Roots of Unity

In the discussion of solution of equations by radicals there is what seems to be an asymmetry in the two steps "adjoin roots of 1" and "adjoin roots of a". For example, when we adjoin $\sqrt[n]{a}$ we assume the nth roots of unity have already been adjoined. But we seem to allow adjoining nth roots of 1 whenever we want, and we never use the symbol $\sqrt[n]{1}$ for a primitive root of unity. Instead we call it some Greek letter, which looks quite different than a symbol like $\sqrt[3]{2}$.

It turns out roots of unity are themselves expressed in terms of more standard iterated radicals. For example, $i = \sqrt{-1}$ and the primitive cube roots of unity are given by the formula $(-1+\sqrt{-3})/2$, where $\sqrt{-3}$ can be interpreted as either of the two square roots. The primitive fifth roots of unity are given by the iterated radical formula $[-1+\sqrt{5}+\sqrt{-10-2\sqrt{5}}]/4$. There are four interpretations: $\sqrt{5}$ has two interpretations, which must be the same both times it appears, and the outer root has two interpretations for each interpretation of $\sqrt{5}$.

Here is the explanation for the fifth root of unity, say ω. Since $\omega^4+\omega^3+\omega^2+\omega+1=0$, it follows that $\alpha = \omega+\omega^4$ satisfies the quadratic equation $\alpha^2+\alpha-1=0$. So $\alpha = (-1+\sqrt{5})/2$. Then $\omega\alpha = \omega^2+1$, and this quadratic relation over $\mathbb{Q}[\alpha]$ leads to the above formula for ω.

A theoretical point of view, which we will generalize below, is that since 2 is a primitive root mod 5, the Galois group of $\mathbb{Q}[\omega]$ over $\mathbb{Q}$, which is cyclic of order 4, is generated by $g(\omega) = \omega^2$. Therefore $\alpha = \omega + g^2(\omega) = \omega+\omega^4$ is fixed by the subgroup of the Galois group of order 2, namely $\langle g^2 \rangle$. This guarantees that α is quadratic over $\mathbb{Q}$.

The complete story here goes back to Gauss. Let's assume for simplicity that the characteristic is 0. Then all roots of unity can be expressed as iterated radicals in a rather controlled manner. In the formulas, only integers appear, along with sums, products, and nested radicals. In the language of towers of field extensions, there is only one type of extension that occurs in the towers. Namely, the adjunction of one root of an irreducible polynomial $X^q - a$, where q is prime and a belongs to the preceding field. (The same is then true for any solvable equation, not just for the roots of unity. That is, the iterated radical towers that eventually contain roots are constructed as a sequence of extensions of this single basic type.) Here is at least a partial explanation, using the concepts of Galois theory and inductive constructions.

First of all, if m and n are relatively prime, then the primitive mnth roots of unity are products of the primitive mth roots of unity and the primitive nth roots of unity. Thus, we only need to construct the primitive p^dth roots for primes p.

The case $p = 2$ is the simplest. The primitive square root of 1 is -1. Then the primitive 4th root of 1 is $\sqrt{-1}$, with two interpretations, obtained by multiplying by the square roots of 1, that is, by $+1$ or -1. The primitive 8th roots are given by $\sqrt{\sqrt{-1}}$, with four interpretations, two inside the outer radical, and then for each of these, two interpretations of the outer radical. Iterate, taking a new outer square root at each stage.

What is happening here? We start with $\mathbb{Q}$. We know if E is obtained from $\mathbb{Q}$ by adjoining all 2^dth roots of unity, then $|E:\mathbb{Q}| = 2^{d-1}$. We have described a tower of radical extensions $\mathbb{Q} = E_1 \subset E_2 \subset \cdots \subset E_d$, where the extension $E_i \subset E_{i+1}$ splits an irreducible quadratic polynomial $X^2 - a_i$, with $a_i \in E_i$, and with a primitive square root of 1 in E_i. Of course, each a_i is a primitive 2^ith root of unity. Inductively, the radical formulas for these roots have exactly the right number of interpretations as distinct elements.

Now consider an odd prime p. It is quite easy to explain the p^dth roots, once we have the pth roots. Namely, suppose $\mathbb{Q} \subset F = F(p)$ is some field extension containing a primitive pth root of 1, say ω, and such that $|F:\mathbb{Q}|$ is divisible only by primes less than p. We also assume that in F there is an iterated radical formula for ω with exactly $p-1$ interpretations, as the various separate occurring radicals in the formula for ω are interpreted in various allowed ways. Of course, these

$p-1$ interpretations will necessarily correspond to the powers of ω in some order, but that isn't the point here.

Given such an F, we construct the primitive p^dth roots of 1 successively as $\sqrt[p]{\omega}$, $\sqrt[p]{\sqrt[p]{\omega}}$, etc. That is, we build a root tower $F = F_1 \subset F_2 \subset \cdots \subset F_d$, where the extension $F_i \subset F_{i+1}$ is of degree p and splits the polynomial $X^p - a_i$, where $a_i \in F_i$ is a primitive p^ith root of 1. These polynomials must be irreducible at each stage, since we know the degree over $\mathbb{Q}$ of a primitive p^dth root of unity is $p^{d-1}(p-1)$ and $|F : \mathbb{Q}|$ is relatively prime to p. At each stage, our new pth root has p interpretations for each interpretation of a_i, obtained by multiplying any one interpretation by the pth roots of 1. So, the point here is, if we come up with iterated radical formulas for the primitive pth roots of 1 inside a field $F = F(p)$ such that $|F : \mathbb{Q}|$ is divisible only by primes less than p, then we *also* have iterated radical formulas of a controlled type for all p^dth roots of 1, and consequently formulas for nth roots of 1 for any n.

We will construct such fields $F = F(p)$, and iterated radical formulas for the primitive pth roots of 1, $\omega \in F$, using Galois theory and induction on p. We know $\mathbb{Q}[\omega]$ is a cyclic Galois extension of degree $p-1$. Therefore, there is a tower of field extensions $\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_m = \mathbb{Q}[\omega]$, with each successive extension cyclic of order some prime q dividing $p-1$. Now, we would like these extensions to be qth root extensions, but we need to make sure we have qth roots of unity first. So, let $\mathbb{Q} \subset L$ be the extension obtained as the composite of the cyclotomic extensions of $\mathbb{Q}$ corresponding to the qth roots of unity for the primes q that divide $p-1$. It turns out that $|L\mathbb{Q}[\omega] : L| = |\mathbb{Q}[\omega] : \mathbb{Q}| = p-1$. This follows easily from the following lemma.

Lemma 1 *If ζ_n and ζ_m are primitive nth and mth roots of unity with* $\gcd(n, m) = 1$*, then $\mathbb{Q}[\zeta_n]\mathbb{Q}[\zeta_m]$ is the cyclotomic extension generated by the primitive mnth root of unity $\zeta_n\zeta_m$, of degree $\phi(mn) = \phi(m)\phi(n)$ over $\mathbb{Q}$.* □

Now look at the tower $L = L_0 \subset L_1 \subset \cdots \subset L_m$, where $L_i = LK_i$.

Proposition 1 *Each $L_i \subset L_{i+1}$ is a cyclic extension of degree $q_i = |K_{i+1} : K_i|$ obtained by adjoining one (hence all) q_ith roots of some element of L_i. In particular, there is an iterated radical formula for ω in the field $L_m = L\mathbb{Q}[\omega]$, and $|L_m : \mathbb{Q}|$ is divisible only by primes less than p.*

Proof The appropriate auxiliary roots of unity have been placed in L, hence in all the L_i. The successive extensions in the L-tower are cyclic Galois extensions of degree q_i, because in the K-tower the extensions are cyclic of degree q_i, and the total degree from bottom to top of both towers is the same, namely $p-1$. But with appropriate roots of unity in the base field, any cyclic extension is a simple root extension. In every field extension which occurs in the construction of L_m over $\mathbb{Q}$, only primes less than p divide the degree, so $|L_m : \mathbb{Q}|$ is divisible only by primes less than p. ■

The iterated radical formula for ω which is found in the construction of L_m here will contain symbols, not necessarily radical formulas, for various qth roots of unity, $q < p$. But now an induction applied to these roots of unity produces finally a field $F(p)$ containing a radical formula for ω which contains only integers and iterated radical expressions. For example, $F = F(p)$ can be obtained from the field $L_m = L\mathbb{Q}[\omega]$ above by simply adjoining enough radicals to yield radical formulas for the qth roots of unity for each prime q less than p. Note by induction we will have $|F : \mathbb{Q}|$ divisible only by primes less than p.

Suppose we want to make the above inductive construction quite explicit. The key step, really, is the step where a cyclic extension with roots of unity in the ground field is shown to be a simple root adjunction. The rest is arithmetic, although of course it gets complicated. Now, in the abstract, this result about cyclic extensions is not proved so constructively. Some Lagrange resolvant enters, but what Lagrange resolvant? Often Hilbert's Theorem 90 is used, or linear independence of characters, as in my Paragraph 26. But perhaps this is a disservice to students. It is not all that hard to exhibit explicit non-zero Lagrange resolvants in the presence of primitive elements.

Here is the story for $\mathbb{Q}[\omega]$. In the K-tower above between $\mathbb{Q}$ and $\mathbb{Q}[\omega]$, each field K_i in the tower can rather easily be seen to be generated over $\mathbb{Q}$ by an element γ that is a sum of some number of distinct powers of ω. In fact, exactly $(p-1)/d$ such powers, if $|K_i : \mathbb{Q}| = d$. This is easy Galois theory, exploiting the cyclic Galois group of $\mathbb{Q}[\omega]$ over $\mathbb{Q}$, generated by $g(\omega) = \omega^r$, where r is some primitive root mod p, that is, a generator of the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$. One takes $\gamma = \omega + g^d\omega + g^{2d}\omega + \cdots + g^{p-1-d}\omega$. Then $g^d\gamma = \gamma$. Gauss called these elements γ *periods* of the cyclotomic equation. So γ will certainly be a primitive element for K_i over the immediately preceding field in the K-tower, and also γ will be a primitive element for $L_i = LK_i$ over the preceding field in the L-tower. Let ζ be an appropriate qth root of unity for this cyclic extension step in the L-tower. The prime q will be a divisor of d. Then $\gamma + \zeta g(\gamma) + \cdots + \zeta^{q-1}g^{q-1}(\gamma)$ is an appropriate Lagrange resolvant here, a *non-zero* element of L_i whose qth power falls in the preceding field. The key word is *non-zero.* One reason this Lagrange resolvant is non-zero is precisely because all the powers $\{\omega, \omega^2, \ldots, \omega^{p-1}\}$ are linearly independent over $\mathbb{Q}[\zeta]$, by the lemma above. The Lagrange resolvant in question is seen to be a linear combination over $\mathbb{Q}[\zeta]$ of exactly $q(p-1)/d$ powers of ω, hence it is non-zero. Brute force will compute the qth power of this Lagrange resolvant as a specific element of the preceding field in the tower.

This concludes the discussion about radical formulas for roots of unity. But here is a general result about non-zero Lagrange resolvants, which makes the general discussion of solving equations by radicals more constructive than it appears from proofs which use linear independence of characters or Hilbert's Theorem 90 at the crucial point.

Proposition 2 *Suppose F is a field containing primitive qth roots of unity, q prime, and suppose $F \subset F[\gamma]$ is a cyclic Galois extension of degree q, with Galois group generated by an automorphism g. Then for at least one of the $q-1$ primitive qth roots of 1 in F, say ζ, the Lagrange resolvant $\rho = \rho(\zeta, \gamma) = \gamma + \zeta g(\gamma) + \cdots + \zeta^{q-1}g^{q-1}(\gamma)$ is non-zero. Thus $g(\rho) = \zeta^{-1}\rho$, $\rho q = r \in F$, and $F[\gamma] = F[\rho]$.* □

I won't give the proof here, but it is relatively simple linear algebra. A non-zero Vandermonde determinant enters the argument at some point, but that is as hard as it gets. The significance of the Proposition is that one has only $q-1$ elements ρ to compute. Brute force arithmetic will find the powers $\rho q = r \in F$ in terms of powers of ζ and elements of F obtained from the coefficients of the minimal polynomial of γ. Note that the elements $g^j(\gamma)$ are the conjugates of γ, the other roots of its minimal polynomial over F. More linear algebra then finds formulas for γ and its conjugates in terms of elements of F obtained from the coefficients of its minimal polynomial, powers of ζ, and powers of $\rho = \sqrt[q]{r}$.

As an illustration of this entire discussion, let's look at the final result for the roots, γ, of a cubic $X^3 + pX - q$ with cyclic Galois group of order 3. Here is a radical formula for 3γ, hence γ, essentially Cardan's formula:

$$3\gamma = \alpha + \beta = \sqrt[3]{\frac{27q}{2} - \frac{3\sqrt{-3}\sqrt{-4p^3 - 27q^2}}{2}} + \sqrt[3]{\frac{27q}{2} + \frac{3\sqrt{-3}\sqrt{-4p^3 - 27q^2}}{2}}$$

where the two cube roots α and β are related by $\alpha\beta = -3p$.

Here are some features of this amazing formula, which illustrate very general points. First, the coefficients p and q of the minimal polynomial of γ occur in the formula. Second, other, more subtle, elements of the ground field occur, specifically the square root of the discriminant, which must be in the ground field since the Galois group is cyclic. Third, the primitive cube roots of unity ζ and ζ^2 occur, specifically $\sqrt{-3} = \zeta - \zeta^2$. Fourth, each of the two distinct square roots in the formula are allowed to be interpreted in two ways, that is, the signs can be changed, but such sign changes do not change the final expression, except for possibly switching α and β. Finally, the two big cube roots α and β would independently have three interpretations each. But the constraint $\alpha\beta = -3p$, reduces the total number of allowed interpretations of the formula to three, not nine. The occurrence of both cube roots α and β is only an aesthetic convenience. In an iterated root tower producing the radical formula for γ, one would *stop* when α is created, since then $\beta = -3p/\alpha$ is there for the taking.

Without going through the entire derivation of the Cardan formula for the roots of a cubic, it is relevant to point out that the cube roots α and β are exactly the Lagrange resolvants $\alpha = \gamma + \zeta g(\gamma) + \zeta^2 g^2(\gamma)$ and $\beta = \gamma + \zeta^2 g(\gamma) + \zeta g^2(\gamma)$, where g generates the cyclic Galois group. Brute force leads to formulas for $\alpha^3 + \beta^3$ and $\alpha^3 - \beta^3$, specifically, $\alpha^3 + \beta^3 = 27q$ and $\alpha^3 - \beta^3 = 3(\zeta^2 - \zeta)\sqrt{D}$, where D is the discriminant. This immediately gives the desired formulas for α^3 and β^3 in the ground field.

Finally, here is the strongest possible statement of the general phenomenon, at least in characteristic 0. A polynomial with solvable Galois group has an iterated radical formula for its roots obtainable in an iterated root tower each step of which adjoins one, hence all, roots of an *irreducible* polynomial $X^q - r$, q prime, where the element r and the qth roots of unity are in the preceding field. Every root $\rho = \sqrt[q]{r}$ which is adjoined in the tower can be chosen to be a Lagrange resolvant associated to an arbitrary primitive element of that particular extension in the tower. An occurrence of $\rho = \sqrt[q]{r}$ in the iterated radical formula is allowed *all possible interpretations*, q of them, although multiple occurrences of this same ρ must be interpreted identically. The set of distinct field elements obtained by *all* the different interpretations of the basic roots ρ which occur is *exactly* the set of distinct roots of the polynomial.

As an example, a universal tower for an irreducible reduced cubic $X^3 + pX - q$ would be $F \subset F[\sqrt{D}] \subset F[\sqrt{D}, \sqrt{-3}] \subset F[\sqrt{D}, \sqrt{-3}, \alpha]$, where D is the discriminant and α is as above. (One or both of the first two extensions might be trivial, hence would not occur as separate steps in a minimal root tower.)