Denesting Conditions

Sep Thijssen

July 11, 2008

Bachelor Thesis in Mathematics
Department of Mathematics
Radboud University Nijmegen
Supervisor: Wieb Bosma
Second reader: Frans Keune

This paper is a generalization of Chapter 3.2 in *Radical extensions and Galois groups* by Honsbeek [2]. It is about denesting roots. Intuitively this means you try to rewrite an algebraic number so that you get fewer roots of roots. Consider for example the equality:

$$3 \cdot \sqrt{\sqrt[3]{5} - \sqrt[3]{4}} = \sqrt[3]{2} + \sqrt[3]{20} - \sqrt[3]{25}.$$

On the right hand side only single cubic roots appear, but on the left hand side there is a root of two cubic roots. That this equality holds is trivial, to check square both sides and compare terms. This however gives no understanding into why there was a simplification.

This paper determines when roots of roots of a special form can be written in an easier way. To make this precise, we need a definition of what roots of roots are. It is assumed that the reader is familiar with some Galois theory. Often references are made to the work of Honsbeek [2], so it is recommended to keep that work close at hand. One result in particular will be frequently used. For convenience it is stated here:

Corollary 18. Let $n \in \mathbb{Z}_{>0}$ and let K be a field containing a primitive n^{th} root of unity. Let $\alpha, \alpha_1, \ldots, \alpha_k \in \bar{K}^*$ such that $\alpha^n, \alpha_1^n, \ldots, \alpha_k^n \in K$. Then $\alpha \in K(\alpha_1, \ldots, \alpha_k)$ if and only if there are $b \in K^*$ and $l_1, \ldots, l_k \in \mathbb{N}$ such that α can be written in the form

$$\alpha = b \prod_{i=1}^{k} \alpha_i^{l_i}.$$

Definition. Let K be a field and $\bar{K}$ some fixed algebraic closure of K. Let $K^{(0)} = K$ and define $K^{(i)}$ inductively as:

$$K^{(i)} = K(\{\alpha \in \bar{K} \mid \alpha^n \in K^{(i-1)} \text{ for some } n \in \mathbb{N}_{>0}\}).$$

For example, if α and β are elements of $\mathbb{Q}$ and if p is an odd prime, then an obvious element x of $\mathbb{Q}^{(2)}$ is:

$$x = \sqrt{\sqrt[p]{\alpha} + \sqrt[p]{\beta}}.$$

The equality above shows that in some cases x can be rewritten so that it apparently also is an element of $\mathbb{Q}^{(1)}$. This paper will give necessary and sufficient conditions for x to be denestable, i.e. in $\mathbb{Q}^{(1)}$.

Notation. If G is a group, its commutator subgroup is denoted by G', and the second commutator subgroup is $G'' = (G')'$. A primitive n^{th} root of unity is denoted by ζ_n. A field extension of L over K will be denoted by $L : K$. The normal closure of $L : \mathbb{Q}$ will be denoted by L^{norm}. When, for an odd number n, the n^{th} root of a real number x is taken, this will be $\sqrt[n]{x}$, the unique real number such that $(\sqrt[n]{x})^n = x$. Some ambiguity arises for square roots of complex numbers that are not positive real valued. So wherever $\sqrt{\lambda}$ appears in the text you should read: a complex number such that $(\sqrt{\lambda})^2 = \lambda$. There are two such numbers in general, but for our purposes it does not matter which one you take. Throughout the rest of the text we use the following notation:

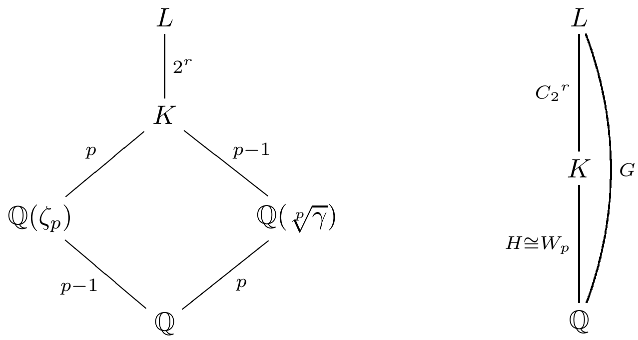
p	An odd prime.
γ	A rational number that is not a p^{th} power.
δ	An element of $\mathbb{Q}(\sqrt[p]{\gamma})\backslash\mathbb{Q}$.
K	The normal closure of $\mathbb{Q}(\delta)$, which is $\mathbb{Q}(\sqrt[p]{\gamma}, \zeta_p)$.
$\delta_0, \delta_1, \ldots, \delta_{p-1}$	The conjugates of $\delta = \delta_0$.
c	The product of all conjugates of δ, which is rational.
μ_i	$\mu_i = c/\delta_i \in K$.

The following lemma and theorem are generalizations of Lemma 101 and Theorem 102 in [2].

Lemma. *Let A be the Galois group of $\mathbb{Q}(\sqrt{\delta}\ )^{\text{norm}} : \mathbb{Q}$, then*

$$A'' = \{1\} \quad \Longrightarrow \quad \sqrt{\mu_0} \in K.$$

Proof. Suppose that $A'' = \{1\}$. Let L be the normal closure $L = K(\sqrt{\mu_0})^{\text{norm}}$. Because the μ_i are the conjugates of μ_0 in $K : \mathbb{Q}$, they are also contained in L. Note that L is a subfield of $\mathbb{Q}(\sqrt{\delta}\ )^{\text{norm}}$. Therefore the group $G = \text{Gal}(L : \mathbb{Q})$ is a factor group of A, and its second commutator subgroup G'' must be trivial as well. The strategy in the proof is to determine the structure of $H = \text{Gal}(K : \mathbb{Q})$, and to show that $\sqrt{\mu_0} \notin K$ contradicts $G'' = \{1\}$.



Because p is a prime, $\mathbb{Q}(\sqrt[p]{\gamma})$ has no subfields in common with $\mathbb{Q}(\zeta_p)$ other than $\mathbb{Q}$. So the order of H is equal to the degree $[K : \mathbb{Q}] = p(p-1)$. Elements of H are determined by the images of ζ_p and $\sqrt[p]{\gamma}$. Let τ be an arbitrary element of H, then it is of the form:

$$\tau(\zeta_p) = \zeta_p^a \qquad \text{and} \qquad \tau(\sqrt[p]{\gamma}) = \zeta_p^b \sqrt[p]{\gamma}.$$

for certain integers a, b such that $0 < a < p$ and $0 \leq b < p$. It is easy to verify that there is an isomorphism $\pi : H \to W_p$ to the group of invertible affine maps on $\mathbb{F}_p$. The image of τ under π would be $\pi(\tau) : x \mapsto ax + b \in W_p$. We may assume that the indexing of the δ_i (and hence of the μ_i) corresponds with the action of W_p on $\mathbb{F}_p$, i.e. such that

$$\tau(\delta_i) = \delta_{\pi(\tau)(i)} \qquad \big(\text{ and } \quad \tau(\mu_i) = \mu_{\pi(\tau)(i)}\ \big).$$

Suppose that $\sqrt{\mu_0}$ is not contained in K. If $\tilde{\tau}$ is an extension automorphism of τ to L, then $\tilde{\tau}(\sqrt{\mu_i})^2 = \tau(\mu_i) = \mu_{\pi(\tau)(i)}$. Hence, the image of $\sqrt{\mu_i}$ under $\tilde{\tau}$ can only be one of $\pm\sqrt{\mu_{\pi(\tau)(i)}}$. If τ is such that $\pi(\tau) : x \mapsto x+i$, then $\tilde{\tau}(\sqrt{\mu_0}) = \pm\sqrt{\mu_i}$, which shows that $\sqrt{\mu_i}$ is not contained in K.

The next part of the proof will show that $K(\sqrt{\mu_0}, \sqrt{\mu_1}, \sqrt{\mu_2})$ is of degree eight over K. This can of course only be true if $p > 3$, as $\mu_2 = \mu_0\mu_1$ when $p = 3$. So assume that $p > 3$. The case $p = 3$ is done by Honsbeek in [2].

Suppose that $\sqrt{\mu_i} \in K(\sqrt{\mu_0})$ for some $i \neq 0$. It follows from Corollary 18[2] that $\mu_i = k^2\mu_0^l$ for some $k \in K$, $l \in \mathbb{N}$. Note that l must be odd, for otherwise μ_i would be a square in K. Multiplying by μ_0 and moving squares to the right results in $\delta_0\delta_i = k'^2$ for some $k' \in K$. So the following implication holds:

$$\sqrt{\mu_i} \in K(\sqrt{\mu_0}) \quad \Longrightarrow \quad \delta_0\delta_i \quad \text{is a square in } K.$$

Note that the assumption cannot be true for all $i \neq 0$, as otherwise the product $\prod_{i \neq 0} \delta_0\delta_i$ would also be a square, and removing even powers from this product would result in $\mu_0 \in K^2$ or equivalently $\sqrt{\mu_0} \in K$, contrary to our assumption.

Choose an $i \neq 0$ such that $\sqrt{\mu_i} \notin K(\sqrt{\mu_0})$. Let $j, l \in \mathbb{F}_p$ be two different indices. Note that there is an element of $\tau \in H$ such that $\pi(\tau) : j \mapsto i, l \mapsto 0$. Suppose that $\sqrt{\mu_j} \in K(\sqrt{\mu_l})$. Then $\sqrt{\mu_j} = k + k'\sqrt{\mu_l}$ for some $k, k' \in K$. Applying an extension automorphism $\tilde{\tau}$ to this equation results in $\pm\sqrt{\mu_i} = \tau(k) \pm \tau(k')\sqrt{\mu_0}$, which contradicts $\sqrt{\mu_i} \notin K(\sqrt{\mu_0})$. So for all $j \neq l$ the following holds:

$$\sqrt{\mu_j} \notin K(\sqrt{\mu_l}).$$

Suppose that $\sqrt{\mu_2} \in K(\sqrt{\mu_0}, \sqrt{\mu_1})$. $K(\sqrt{\mu_2})$ is a quadratic subfield of $K(\sqrt{\mu_0}, \sqrt{\mu_1})$. This field cannot be $K(\sqrt{\mu_0})$ or $K(\sqrt{\mu_1})$, so it is $K(\sqrt{\mu_0 \mu_1})$. Because $p > 3$, $\sqrt{\mu_{p-1}} \notin K(\sqrt{\mu_2})$, and hence $\sqrt{\mu_{p-1}} \notin K(\sqrt{\mu_0}, \sqrt{\mu_1})$. Now let $\tau \in H$ such that $\pi(\tau) : x \mapsto -x+1$, then τ interchanges μ_0 and μ_1, and τ also interchanges μ_2 and μ_{p-1}. By applying an extension automorphism $\tilde{\tau}$ in a similar way as before it follows that $\sqrt{\mu_2} \notin K(\sqrt{\mu_0}, \sqrt{\mu_1})$. This is contrary to our previous assumption.

Hence the degree of $K(\sqrt{\mu_0}, \sqrt{\mu_1}, \sqrt{\mu_2})$ over K is eight. So we can independently choose the images of $\sqrt{\mu_0}, \sqrt{\mu_1}, \sqrt{\mu_2}$ under the action of an element in the Galois group of the normal closure L. Therefore there is a $\rho_0 \in G$ such that:

$$\rho_0(\sqrt{\mu_0}) = -\sqrt{\mu_0}, \qquad \rho_0(\sqrt{\mu_1}) = \sqrt{\mu_1}, \qquad \rho_0(\sqrt{\mu_2}) = \sqrt{\mu_2}.$$

Let ω, ω' be elements of G such that $\pi\left(\omega|_K\right) : x \mapsto -x+1$ and $\pi\left(\omega'|_K\right) : x \mapsto -x+(p+1)/2$. Define $\sigma \in G'$ as the commutator $\sigma = [\omega, \omega']$. Then the corresponding element of σ in W_p is $\pi\left(\sigma|_K\right) = \left[\pi\left(\omega|_K\right), \pi\left(\omega'|_K\right)\right] : x \mapsto x+1$. Let ρ_1 and ρ_2 be the commutators $\rho_1 = [\sigma, \rho_0]$ and $\rho_2 = [\sigma, \rho_1]$. Then:

$$\rho_1 : \sqrt{\mu_1} \overset{\rho_0^{-1}}{\longmapsto} \sqrt{\mu_1} \overset{\sigma^{-1}}{\longmapsto} \pm\sqrt{\mu_0} \overset{\rho_0}{\longmapsto} \mp\sqrt{\mu_0} \overset{\sigma}{\longmapsto} -\sqrt{\mu_1},$$

$$\rho_1 : \sqrt{\mu_2} \overset{\rho_0^{-1}}{\longmapsto} \sqrt{\mu_2} \overset{\sigma^{-1}}{\longmapsto} \pm\sqrt{\mu_1} \overset{\rho_0}{\longmapsto} \pm\sqrt{\mu_1} \overset{\sigma}{\longmapsto} +\sqrt{\mu_2},$$

$$\rho_2 : \sqrt{\mu_2} \overset{\rho_1^{-1}}{\longmapsto} \sqrt{\mu_2} \overset{\sigma^{-1}}{\longmapsto} \pm\sqrt{\mu_1} \overset{\rho_1}{\longmapsto} \mp\sqrt{\mu_1} \overset{\sigma}{\longmapsto} -\sqrt{\mu_2}.$$

But $\rho_2 \in G''$ is a commutator of commutators and should therefore be the identity map, which it clearly is not. This contradiction completes the proof. □

The last part of this proof slightly deviates from the proof for $p = 3$. In that case the entire group $\mathrm{Gal}(L : K)$ is computed and it is shown to be contained in the commutator subgroup G'. In the proof for $p > 3$ the contradiction arises from one element $\rho_2 \in \mathrm{Gal}(L : K)$. To create this element it was sufficient to compute a part of the structure of $L : K$.

Theorem. *Let A be as in the lemma. Then the following are equivalent:*

(i) The element $\sqrt{\delta}$ is contained in $\mathbb{Q}^{(1)}$.

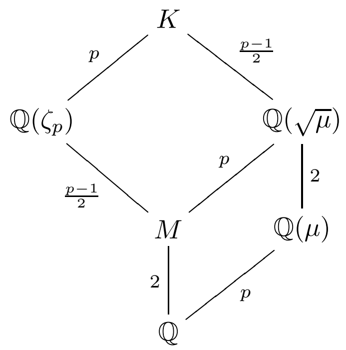
(ii) The group A'' is trivial.

(iii) There exist $c \in \mathbb{Q}$ and $\lambda \in \mathbb{Q}(\delta)$ such that $\delta = c \cdot \lambda^2$.

Proof. Implication $(iii) \Rightarrow (i)$ is trivial. The proof of $(i) \Rightarrow (ii)$ is exactly the same as in the proof of $(i) \Rightarrow (ii)$ in the similar Theorem 102 [2], which will not be repeated here.

Assume that A'' is trivial. Let the μ_i be as in the lemma. Write $\mu = \mu_0$ for simplicity. It would be sufficient to prove that $\sqrt{\mu}$ is an element of $\mathbb{Q}(\delta) = \mathbb{Q}(\mu)$, because we could take $c = \delta \cdot \mu \in \mathbb{Q}$ and $\lambda = \sqrt{\mu}^{-1} \in \mathbb{Q}(\delta)$ so that c and λ are as required.

So suppose that $\sqrt{\mu} \notin \mathbb{Q}(\mu)$. By the lemma $\sqrt{\mu}$ is contained in $K = \mathbb{Q}(\delta, \zeta_p)$, so that K equals $\mathbb{Q}(\sqrt{\mu}, \zeta_p)$. Let M be the intersection $M = \mathbb{Q}(\sqrt{\mu}) \cap \mathbb{Q}(\zeta_p)$, then we have the following diagram of extensions:



The degree of $\mathbb{Q}(\mu)$ over $\mathbb{Q}$ is p. Because $\sqrt{\mu}$ is not contained in $\mathbb{Q}(\mu)$ the degree of $\mathbb{Q}(\sqrt{\mu})$ over $\mathbb{Q}$ is $2p$. This divides the total degree $[K:\mathbb{Q}] = p(p-1)$, so that $[K:\mathbb{Q}(\sqrt{\mu})] = \frac{p-1}{2}$. The extension $\mathbb{Q}(\zeta_p):\mathbb{Q}$ is Galois. As a consequence[1] the degree $[\mathbb{Q}(\zeta_p):M]$ equals $[K:\mathbb{Q}(\sqrt{\mu})] = \frac{p-1}{2}$. Therefore M is a subfield of $\mathbb{Q}(\zeta_p)$ of degree two over $\mathbb{Q}$. That field is $M = \mathbb{Q}(\sqrt{\pm p})$, where $\pm = (-1)^{\frac{p-1}{2}}$. So $\sqrt{\mu}$ is contained in $M \cdot \mathbb{Q}(\mu) = \mathbb{Q}(\sqrt{\pm p}, \delta)$. It follows by corollary 18 [2] that $\sqrt{\mu} = \sqrt{\pm p}^i \cdot \theta$ for some $\theta \in \mathbb{Q}(\delta)$ and some integer i. Note that i must be odd, as otherwise $\sqrt{\mu} \in \mathbb{Q}(\delta) = \mathbb{Q}(\mu)$. Let $N : \mathbb{Q}(\delta) \to \mathbb{Q}$ be the norm function of $\mathbb{Q}(\delta):\mathbb{Q}$ sending an element of $\mathbb{Q}(\delta)$ to the product of all its conjugates. Then:

$$N(\sqrt{\mu})^2 = N(\mu) = N(\pm p^i \cdot \theta^2) = \pm p^{ip} \cdot N(\theta)^2.$$

This is a contradiction, as $\pm p^{ip}$ is not a square in $\mathbb{Q}$. □

Note that this theorem is the same as Theorem 102 in [2], but generalized for all odd primes. The proof is almost the same as well, except for one extra step: the implication $\sqrt{\mu} \in \mathbb{Q}(\delta, \zeta_p) \Rightarrow \sqrt{\mu} \in \mathbb{Q}(\delta, \sqrt{\pm p})$.

Application. The theory can now be be applied to all $x \in \mathbb{Q}^{(2)}$ that are of a special form. The use of symbols is the same as before; here is an overview:

$$\begin{aligned} x &= \sqrt{\sqrt[p]{\alpha} + \sqrt[p]{\beta}} & \delta &= 1 + \sqrt[p]{\gamma} \\ \gamma &= \beta/\alpha \ \in \mathbb{Q} & \mu &= c/\delta \\ c &= 1 + \gamma & \lambda &= \sqrt{\mu}^{-1} \end{aligned}$$

Rewrite $x = \sqrt[2p]{\alpha} \cdot \sqrt{\delta}$. If γ is a p^{th} power in $\mathbb{Q}$, then x is obviously denestable. If not, then x is denestable if and only if $\sqrt{\delta}$ is denestable. By the theorem this is so if and only if $\delta = c \cdot \lambda^2$. Here c is the $\mathbb{Q}(\delta):\mathbb{Q}$ norm of δ, which is minus the trailing coefficient of the minimal polynomial $(X-1)^p - \gamma$ of δ. So $c = 1 + \gamma$. It is clear from the proof of the theorem that we can take $\lambda = \sqrt{\mu}^{-1} = \sqrt{\delta/c}$ which is contained in $\mathbb{Q}(\sqrt[p]{\gamma}) \subset \mathbb{Q}^{(1)}$, if $\sqrt{\delta}$ is denestable.

For calculating examples, a computer algebra system is indispensable. The first naive strategy is to pick some non trivial integers α, β, i.e. not both a p^{th} power. To calculate the field extension $\mathbb{Q}(\sqrt[p]{\gamma})$, and to check whether λ is contained in it. For most choices of α, β there are no solutions. Here are some exceptions.

Example 1. For $p = 3$, take $\alpha = 5$ and $\beta = -4$. Then λ is a zero of $X^2 - \delta/c = X^2 - 1/5 \cdot (1 + \sqrt[3]{\gamma})$, which splits into linear factors over $\mathbb{Q}(\sqrt[3]{\gamma})$. When recovering x by the formula $x = \sqrt[6]{\alpha} \cdot \sqrt{c} \cdot \lambda$, it does matter which root of $X^2 - \lambda^2$ is taken. The right choice is $\lambda = 5/6 \cdot \sqrt[3]{\gamma}^2 - 5/3 \cdot \sqrt[3]{\gamma} - 5/3 = 1/3 \cdot (\sqrt[3]{10} + \sqrt[3]{100} - 5)$, leading to the equality:

$$3 \cdot \sqrt{\sqrt[3]{5} - \sqrt[3]{4}} = \sqrt[3]{2} + \sqrt[3]{20} - \sqrt[3]{25}.$$

Example 2. For $p = 3$, take $\alpha = 3^7$ and $\beta = 20$. Then λ is a zero of $X^2 - \delta/c = X^2 - 3 \cdot 11^2/343 \cdot (1 + \sqrt[3]{\gamma})$, which has two roots in $\mathbb{Q}(\sqrt[3]{\gamma})$. The right one is $\lambda = 343/66 \cdot \sqrt[3]{\gamma}^2 + 49/66 \cdot \sqrt[3]{\gamma} - 7/33 = 7/33 \cdot (\sqrt[3]{10} + \sqrt[3]{20} - 1)$. Using $x = \sqrt[6]{\alpha} \cdot \sqrt{c} \cdot \lambda$ to recover x leads to the equality:

$$\sqrt{3} \cdot \sqrt{7 + \sqrt[3]{20}} = \sqrt[3]{10} + \sqrt[3]{20} - 1.$$

You might have noticed that some strange factors appear in the calculation that are not in the final equality. A part of this is explained by:

$$\sqrt[2p]{\alpha} \cdot \sqrt{c} = \sqrt[2p]{\alpha} \cdot \sqrt{1 + \frac{\beta}{\alpha}} = \frac{\sqrt{\alpha + \beta}}{\sqrt[p]{\alpha^{(p-1)/2}}}.$$

[1] See for example Theorem 29 of Chapter II in [1]

The denominator is a power of $\sqrt[p]{\alpha}$, which can be merged with the $\sqrt[p]{\gamma}$ terms in λ. It is not so clear why the numerator has the right factors. Let's calculate some more examples for other primes first.

Example 3. For $p = 5$, take $\alpha = 4$ and $\beta = -3$. Then similarly $\lambda = -8/5 \cdot \sqrt[5]{\gamma}^4 - 4/5 \cdot \sqrt[5]{\gamma}^3 + 8/5 \cdot \sqrt[5]{\gamma}^2 + 4/5 \cdot \sqrt[5]{\gamma} + 2/5$. Notice that $\sqrt{\alpha+\beta} = 1$ and $\sqrt[p]{\alpha^{(p-1)/2}} = \sqrt[5]{16}$. Using $x = \sqrt[6]{\alpha} \cdot \sqrt{c} \cdot \lambda$ to recover x leads to the equality:

$$5 \cdot \sqrt{\sqrt[5]{4} - \sqrt[5]{3}} = -\sqrt[5]{648} + \sqrt[5]{27} + 2 \cdot \sqrt[5]{36} - \sqrt[5]{48} + \sqrt[5]{2}.$$

Example 4. For $p = 5$, take $\alpha = -7^5$ and $\beta = 12 \cdot 11^5$. Then there is an ugly solution for λ in $\mathbb{Q}(\sqrt[p]{\gamma})$. But when written in a basis of the same field $\mathbb{Q}(\sqrt[5]{12})$ it becomes readable: $\lambda = 49/6190 \cdot (-\sqrt[5]{12}^4 + \sqrt[5]{12}^3 - 2 \cdot \sqrt[5]{12}^2 + 8 \cdot \sqrt[5]{12} + 10)$. Notice that $\sqrt{\alpha+\beta} = 619 \cdot \sqrt{5}$ and $\sqrt[p]{\alpha^{(p-1)/2}} = 49$. So altogether there is a surprisingly nice equality:

$$\sqrt{5} \cdot \sqrt{11 \cdot \sqrt[5]{12} - 7} = -\sqrt[5]{648} + \sqrt[5]{54} - \sqrt[5]{144} + 4 \cdot \sqrt[5]{12} + 5.$$

Example 5. For $p = 7$ take $\alpha = 64$ and $\beta = -1$. Then there is a solution for λ. When written in a basis of $\mathbb{Q}(\sqrt[7]{2})$ this is $\lambda = 4/21 \cdot (-2 \cdot \sqrt[7]{2}^5 + \sqrt[7]{2}^4 + 2 \cdot \sqrt[7]{2}^3 - 2 \cdot \sqrt[7]{2}^2 - 2)$. In this case $\sqrt{\alpha+\beta} = 3 \cdot \sqrt{7}$ and $\sqrt[p]{\alpha^{(p-1)/2}} = 4 \cdot \sqrt[7]{16}$. Again factors disappear, with the result:

$$\sqrt{7} \cdot \sqrt{\sqrt[7]{64} - 1} = 2 \cdot \sqrt[7]{2} + \sqrt[7]{8} + \sqrt[7]{32} - \sqrt[7]{64} - 1.$$

These examples were not found by choosing α and β randomly. There is a very useful method based on solving equations for λ in the field $\mathbb{Q}(\sqrt[p]{\gamma})$ seen as a p-dimensional vector space. See for example Chapter 3.3 in [2]. This leads to an infinite family of denesting examples for $p = 3$. For larger primes however the results are less satisfactory. Calculation time rises very quickly too, making it hard to use this method for primes larger then seven.

Another way to find denesting examples is by using what you might have noticed before: in all the examples calculated so far $\alpha + \beta$ is a square up to a factor at most $\pm p$. I have not been able to prove this in general, but I think the following is true.

Conjecture. Let $\alpha, \beta \in \mathbb{Z}$ be relatively prime integers that are not both a p^{th} power. Write $\alpha + \beta = n \cdot m^2$ for integers n, m such that n is squarefree. Then the following implication holds:

$$\sqrt{\sqrt[p]{\alpha} + \sqrt[p]{\beta}} \quad \text{is denestable} \quad \Longrightarrow \quad n \in \{\pm 1, \pm p\}.$$

Assuming the conjecture is true we have a strong condition on the pair α, β so that denesting examples can be found much quicker. There is however still essentially only one known example for $p = 7$ (given above), and there are none know for bigger primes.

References

[1] Emil Artin, *Galois Theory*, Notre Dame: University of Notre Dame Press, 1971 (sixth printing)

[2] Mascha Honsbeek, *Radical extensions and Galois groups*, Nijmegen: Radboud University Nijmegen, 2005