Kummer theory, support problem, nested radicals

B.Sury
Indian Statistical Institute Bangalore
"Theory if equations" workshop
Delhi
17th October 2014

The support problem

Let x, y be positive integers such that each prime divisor of $x^n - 1$ also divides $y^n - 1$ for every n. What can we say about the relation between x and y?

The support problem

Let x, y be positive integers such that each prime divisor of $x^n - 1$ also divides $y^n - 1$ for every n. What can we say about the relation between x and y?
For instance, if y is a power of x, the above property holds.

The support problem

Let x, y be positive integers such that each prime divisor of $x^n - 1$ also divides $y^n - 1$ for every n. What can we say about the relation between x and y?
For instance, if y is a power of x, the above property holds.
We may ask whether the converse also holds. This problem came to be known as the 'support problem'.

The support problem

Let x, y be positive integers such that each prime divisor of $x^n - 1$ also divides $y^n - 1$ for every n. What can we say about the relation between x and y?
For instance, if y is a power of x, the above property holds.
We may ask whether the converse also holds. This problem came to be known as the 'support problem'.
One calls the 'support' of a natural number a to be the set of its prime divisors.

This will be proved using Kummer theory.

This will be proved using Kummer theory.

What is Kummer theory?

This will be proved using Kummer theory.

What is Kummer theory?

For our purposes in this application, we may think of the following concrete statement as Kummer theory:

Suppose q is a prime number and consider the "field" generated by the q-th roots of unity (namely, all $e^{2ik\pi/p}$ for $0 \leq k < p$).

Suppose q is a prime number and consider the "field" generated by the q-th roots of unity (namely, all $e^{2ik\pi/p}$ for $0 \leq k < p$).
It is usually denoted by $\mathbf{Q}(\zeta_q)$ where ζ_q is $e^{2i\pi/q}$.

Suppose q is a prime number and consider the "field" generated by the q-th roots of unity (namely, all $e^{2ik\pi/p}$ for $0 \leq k < p$).
It is usually denoted by $\mathbf{Q}(\zeta_q)$ where ζ_q is $e^{2i\pi/q}$.
Suppose that a certain non-zero rational number a is a q-th power in this field, Kummer's theorem implies that a is already a q-th power of a rational number.

We mention in passing the more precise version.

We mention in passing the more precise version.
Kummer theory is a correspondence between abelian extensions of a field K and subgroups of the n-th powers of K^*.

We mention in passing the more precise version.
Kummer theory is a correspondence between abelian extensions of a field K and subgroups of the n-th powers of K^*.
If K contains the n-th roots of unity, then abelian extensions L of K whose Galois groups have exponent n correspond bijectively to subgroups Ω of K^* containing $(K^*)^n$ via $L \mapsto K^* \cap (L^*)^n$ and its inverse map $\Omega \mapsto K(\Omega^{1/n})$.

The support problem is:

The support problem is:

Theorem:

Let $x, y \in \mathbb{Q}^*$. If, for all but finitely many primes p and, for all $n \in \mathbb{N}$, one has the implication

$$p \mid (x^n - 1) \Longrightarrow p \mid (y^n - 1),$$

then y is a power of x.

Here p divides a rational number $x = \frac{a}{b}, (a, b) = 1$, means that $p \mid a$.

This is in reality a local-global theorem. To explain:

This is in reality a local-global theorem. To explain:
For a prime p not dividing the numerator and denominators of x and y, look at the order of x mod p; viz.,

This is in reality a local-global theorem. To explain:
For a prime p not dividing the numerator and denominators of x and y, look at the order of x mod p; viz.,
The smallest n such that $p|(x^n - 1)$.

This is in reality a local-global theorem. To explain:
For a prime p not dividing the numerator and denominators of x and y, look at the order of x mod p; viz.,
The smallest n such that $p|(x^n - 1)$.
We have $p|(y^n - 1)$ so that the order of y mod p divides n, the order of x.

This is in reality a local-global theorem. To explain:
For a prime p not dividing the numerator and denominators of x and y, look at the order of x mod p; viz.,
The smallest n such that $p|(x^n - 1)$.
We have $p|(y^n - 1)$ so that the order of y mod p divides n, the order of x.
A simple exercise in the cyclic group $\mathbb{Z}_p^*$ shows that y must be a power of x mod p.

This is in reality a local-global theorem. To explain:
For a prime p not dividing the numerator and denominators of x and y, look at the order of x mod p; viz.,
The smallest n such that $p|(x^n - 1)$.
We have $p|(y^n - 1)$ so that the order of y mod p divides n, the order of x.
A simple exercise in the cyclic group $\mathbb{Z}_p^*$ shows that y must be a power of x mod p.
Therefore, the support theorem says that if, modulo all but finitely many primes p, y is a power of x modulo p, then y is actually a power of x; this is what Kummer theory accomplishes.

We start by very briefly recalling some facts from algebraic number theory.

We start by very briefly recalling some facts from algebraic number theory.
When k is a finite extension field of $\mathbb{Q}$, we have a nice subring called the ring of integers of k.

We start by very briefly recalling some facts from algebraic number theory.
When k is a finite extension field of $\mathbb{Q}$, we have a nice subring called the ring of integers of k.
It is $O_k = \{x \in k : x \text{ is the root of a monic integral polynomial } \}$.

We start by very briefly recalling some facts from algebraic number theory.
When k is a finite extension field of $\mathbb{Q}$, we have a nice subring called the ring of integers of k.
It is $O_k = \{x \in k : x \text{ is the root of a monic integral polynomial } \}$.
For example, if $k = \mathbf{Q}(i)$, $O_k = \mathbb{Z}[i]$.

We start by very briefly recalling some facts from algebraic number theory.
When k is a finite extension field of $\mathbb{Q}$, we have a nice subring called the ring of integers of k.
It is $O_k = \{x \in k : x \text{ is the root of a monic integral polynomial } \}$.
For example, if $k = \mathbf{Q}(i)$, $O_k = \mathbb{Z}[i]$.
More generally, if d is a square-free integer, and $k = \mathbb{Q}(\sqrt{d})$, then $O_k = \mathbb{Z}[\sqrt{d}]$ or $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ according as to whether $d \equiv 2, 3 \bmod 4$ or $1 \bmod 4$.

For the important class of number fields $k = \mathbb{Q}(\zeta_n)$ generated by the n-th roots of unity - the so-called cyclotomic fields - the ring $O_k = \mathbb{Z}[\zeta_n]$ of all integral polynomial expressions in the n-th roots of unity.

For the important class of number fields $k = \mathbb{Q}(\zeta_n)$ generated by the n-th roots of unity - the so-called cyclotomic fields - the ring $O_k = \mathbb{Z}[\zeta_n]$ of all integral polynomial expressions in the n-th roots of unity.
The rings O_k are a lot like the usual integers but there is one very essential difference - in general, the ideals in O_k are NOT singly generated (unlike $\mathbb{Z}$).

For the important class of number fields $k = \mathbb{Q}(\zeta_n)$ generated by the n-th roots of unity - the so-called cyclotomic fields - the ring $O_k = \mathbb{Z}[\zeta_n]$ of all integral polynomial expressions in the n-th roots of unity.
The rings O_k are a lot like the usual integers but there is one very essential difference - in general, the ideals in O_k are NOT singly generated (unlike $\mathbb{Z}$).
In fact, this fact that, for cyclotomic fields $k = \mathbb{Q}(\zeta_p)$, the ring O_k is not a principal ideal domain when $p \geq 23$, is the serious reason why Fermat's last theorem has no elementary proof using factorization.

Ordinary prime numbers may not exhibit the same property in a bigger ring.

Ordinary prime numbers may not exhibit the same property in a bigger ring.
To explain, look at, for instance, the ring of Gaussian integers $\mathbf{Z}[i]$. The prime number 13 "divides" the product of $1+5i$ and $1-5i$ in this ring but 13 does not divide either of these.

Ordinary prime numbers may not exhibit the same property in a bigger ring.
To explain, look at, for instance, the ring of Gaussian integers $\mathbf{Z}[i]$.
The prime number 13 "divides" the product of $1+5i$ and $1-5i$ in this ring but 13 does not divide either of these.
Why should one care about what happens to ordinary prime numbers in these bigger rings?

Ordinary prime numbers may not exhibit the same property in a bigger ring.
To explain, look at, for instance, the ring of Gaussian integers $\mathbf{Z}[i]$.
The prime number 13 "divides" the product of $1+5i$ and $1-5i$ in this ring but 13 does not divide either of these.
Why should one care about what happens to ordinary prime numbers in these bigger rings?
We'll see that in facts 1,2,3 below.

Although O_k is not a principal ideal domain (PID) in general, it is a so-called Dedekind domain.

Although O_k is not a principal ideal domain (PID) in general, it is a so-called Dedekind domain.
Without getting into technical details, informally a main fact is that multiplication of numbers/elements is replaced by multiplication of ideals in which case unique factorization into prime "ideals" holds.

Although O_k is not a principal ideal domain (PID) in general, it is a so-called Dedekind domain.
Without getting into technical details, informally a main fact is that multiplication of numbers/elements is replaced by multiplication of ideals in which case unique factorization into prime "ideals" holds.
A useful fact to keep in mind is that the ideal pO_k for a prime number p can be a product of at the most d ideals where d is the degree of k.

For instance, the prime number 2 gives in $\mathbb{Z}[i]$ the ideal $2\mathbb{Z}[i]$ which becomes the square of a prime ideal generated by $1+i$.
An odd prime number p which is 3 modulo 4 gives the ideal $p\mathbb{Z}[i]$ which remains a prime ideal.
An odd prime number p which is 1 modulo 4 gives the ideal $p\mathbb{Z}[i]$ which is a product of two different prime ideals generated by complex conjugates $x+iy$ and $x-iy$ for integers x, y; indeed, x, y are obtained from $p = x^2 + y^2$.

For instance, the prime number 2 gives in $\mathbb{Z}[i]$ the ideal $2\mathbb{Z}[i]$ which becomes the square of a prime ideal generated by $1+i$.
An odd prime number p which is 3 modulo 4 gives the ideal $p\mathbb{Z}[i]$ which remains a prime ideal.
An odd prime number p which is 1 modulo 4 gives the ideal $p\mathbb{Z}[i]$ which is a product of two different prime ideals generated by complex conjugates $x+iy$ and $x-iy$ for integers x, y; indeed, x, y are obtained from $p = x^2 + y^2$.

In general, for a quadratic extension $k = \mathbb{Q}(\sqrt{d})$, the decomposition of the ideal pO_k into prime ideals (either two distinct or a single prime ideal or the square of a prime ideal) is an expression of the cases whether d is a square or non-square modulo p or is a multiple of it.

If $k = \mathbb{Q}(\zeta_n)$, the decomposition of an ideal pO_k for a prime number p is governed by what is known as the cyclotomic reciprocity law.

If $k = \mathbb{Q}(\zeta_n)$, the decomposition of an ideal pO_k for a prime number p is governed by what is known as the cyclotomic reciprocity law.
In general, the set of prime numbers p such that pO_k breaks up into the degree $[k : \mathbf{Q}]$ ideals (the maximum possible) determine s the abelian extension field k.

If $k = \mathbb{Q}(\zeta_n)$, the decomposition of an ideal pO_k for a prime number p is governed by what is known as the cyclotomic reciprocity law.
In general, the set of prime numbers p such that pO_k breaks up into the degree $[k : \mathbf{Q}]$ ideals (the maximum possible) determine s the abelian extension field k.
More precisely,

Fact 1 (primes splitting in cyclotomic extensions) :
If p is a prime and $p \not| n$ and ζ_n is a primitive n^{th} root of unity, then p splits completely in $\mathbb{Q}(\zeta_n)$ if and only if $p \equiv 1(\mathrm{mod} n)$.

Fact 1 (primes splitting in cyclotomic extensions) :
If p is a prime and $p \not| n$ and ζ_n is a primitive n^{th} root of unity, then p splits completely in $\mathbb{Q}(\zeta_n)$ if and only if $p \equiv 1(\mathrm{modn})$.

Fact 2 (primes splitting in a radical extension) :
If $a \in \mathbb{N}$, p is a prime not dividing a, then p splits completely in $\mathbb{Q}(\zeta_q, a^{\frac{1}{q}})$ if and only if $p \equiv 1(\mathrm{modq})$ and a is a q^{th} power in $\mathbb{Z}/p\mathbb{Z}$.

Fact 1 (primes splitting in cyclotomic extensions) :
If p is a prime and $p \not| n$ and ζ_n is a primitive n^{th} root of unity, then p splits completely in $\mathbb{Q}(\zeta_n)$ if and only if $p \equiv 1(\mathrm{modn})$.

Fact 2 (primes splitting in a radical extension) :
If $a \in \mathbb{N}$, p is a prime not dividing a, then p splits completely in $\mathbb{Q}(\zeta_q, a^{\frac{1}{q}})$ if and only if $p \equiv 1(\mathrm{modq})$ and a is a q^{th} power in $\mathbb{Z}/p\mathbb{Z}$.

Fact 3 (split primes determine hierarchy) :
If K, L are finite extensions of $\mathbb{Q}$ and $Spl(K)$ and $Spl(L)$ denote the sets of prime integers which split completely in K and L respectively, then $Spl(K) \subseteq Spl(L)$, then $K \supseteq L$.

Proof of the support theorem

,1-¿ Assume x, y are as in the theorem, that is, for all n and all but finitely many primes p, one has

$$p \mid (x^n - 1) \Longrightarrow p \mid (y^n - 1).$$

Proof of the support theorem

,1-¿ Assume x, y are as in the theorem, that is, for all n and all but finitely many primes p, one has

$$p \mid (x^n - 1) \Longrightarrow p \mid (y^n - 1).$$

We us Kummer's theorem which, for our purposes, gives using the facts above:

Proof of the support theorem

,1-¿ Assume x, y are as in the theorem, that is, for all n and all but finitely many primes p, one has

$$p \mid (x^n - 1) \Longrightarrow p \mid (y^n - 1).$$

We us Kummer's theorem which, for our purposes, gives using the facts above:
Let q be an odd prime power. Then the natural map $\mathbb{Q}^*/(\mathbb{Q}^*)^q \to \mathbb{Q}(\zeta_q)^*/(\mathbb{Q}(\zeta_q)^*)^q$ is injective.

Look at our x, y in the support theorem. We can show:

Look at our x, y in the support theorem. We can show:
Let q be a power of a prime l and let ζ_q be a primitive q^{th} root of unity. Then $\mathbb{Q}(\zeta_q, x^{\frac{1}{q}}) \supseteq \mathbb{Q}(\zeta_q, y^{\frac{1}{q}})$.

Look at our x, y in the support theorem. We can show:
Let q be a power of a prime l and let ζ_q be a primitive q^{th} root of unity. Then $\mathbb{Q}(\zeta_q, x^{\frac{1}{q}}) \supseteq \mathbb{Q}(\zeta_q, y^{\frac{1}{q}})$.
This is proved using a generalization of the so-called Hilbert Theorem 90 slightly.

Basically, the hypothesis of the support theorem shows that $y = x^d$ in the group $\mathbb{Q}(\zeta_q)^*/(\mathbb{Q}(\zeta_q)^*)^q$. So, by the last quoted result based on Kummer, we have $y = x^d$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^q$ also.

Basically, the hypothesis of the support theorem shows that $y = x^d$ in the group $\mathbb{Q}(\zeta_q)^*/(\mathbb{Q}(\zeta_q)^*)^q$. So, by the last quoted result based on Kummer, we have $y = x^d$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^q$ also. It is a simple matter to show that this is a power over integers also; I don't say any more about it.

Nested radicals and Ramanujan

The second application of Kummer theory we discuss involves nested systems of taking roots. Let us look at a few.

Nested radicals and Ramanujan

The second application of Kummer theory we discuss involves nested systems of taking roots. Let us look at a few.
We can't help but feel a sense of bewilderment on encountering formulae such as the following:

$$\sqrt[3]{\sqrt[3]{2}-1}=\sqrt[3]{\frac{1}{9}}-\sqrt[3]{\frac{2}{9}}+\sqrt[3]{\frac{4}{9}};$$

$$\sqrt[3]{\sqrt[3]{2}-1}=\sqrt[3]{\frac{1}{9}}-\sqrt[3]{\frac{2}{9}}+\sqrt[3]{\frac{4}{9}};$$

$$\sqrt{\sqrt[3]{28}-\sqrt[3]{27}}=-\frac{1}{3}(-\sqrt[3]{98}+\sqrt[3]{28}+1);$$

$$\sqrt[3]{\sqrt[3]{2}-1}=\sqrt[3]{\frac{1}{9}}-\sqrt[3]{\frac{2}{9}}+\sqrt[3]{\frac{4}{9}};$$

$$\sqrt{\sqrt[3]{28}-\sqrt[3]{27}}=-\frac{1}{3}(-\sqrt[3]{98}+\sqrt[3]{28}+1);$$

$$\sqrt{\sqrt[3]{5}-\sqrt[3]{4}}=\frac{1}{3}(-\sqrt[3]{25}+\sqrt[3]{20}+\sqrt[3]{2});$$

$$\sqrt[3]{\sqrt[3]{2}-1}=\sqrt[3]{\frac{1}{9}}-\sqrt[3]{\frac{2}{9}}+\sqrt[3]{\frac{4}{9}};$$

$$\sqrt{\sqrt[3]{28}-\sqrt[3]{27}}=-\frac{1}{3}(-\sqrt[3]{98}+\sqrt[3]{28}+1);$$

$$\sqrt{\sqrt[3]{5}-\sqrt[3]{4}}=\frac{1}{3}(-\sqrt[3]{25}+\sqrt[3]{20}+\sqrt[3]{2});$$

$$\sqrt[3]{\cos\frac{2\pi}{7}}+\sqrt[3]{\cos\frac{4\pi}{7}}+\sqrt[3]{\cos\frac{8\pi}{7}}=\sqrt[3]{\frac{5-3\sqrt{7}}{2}};$$

$$\sqrt[3]{\sqrt[3]{2}-1}=\sqrt[3]{\frac{1}{9}}-\sqrt[3]{\frac{2}{9}}+\sqrt[3]{\frac{4}{9}};$$

$$\sqrt{\sqrt[3]{28}-\sqrt[3]{27}}=-\frac{1}{3}(-\sqrt[3]{98}+\sqrt[3]{28}+1);$$

$$\sqrt{\sqrt[3]{5}-\sqrt[3]{4}}=\frac{1}{3}(-\sqrt[3]{25}+\sqrt[3]{20}+\sqrt[3]{2});$$

$$\sqrt[3]{\cos\frac{2\pi}{7}}+\sqrt[3]{\cos\frac{4\pi}{7}}+\sqrt[3]{\cos\frac{8\pi}{7}}=\sqrt[3]{\frac{5-3\sqrt{7}}{2}};$$

$$\sqrt[6]{7\sqrt[3]{20}-19}=\sqrt[3]{\frac{5}{3}}-\sqrt[3]{\frac{2}{3}};$$

$$\sqrt[3]{\sqrt[3]{2}-1}=\sqrt[3]{\frac{1}{9}}-\sqrt[3]{\frac{2}{9}}+\sqrt[3]{\frac{4}{9}};$$

$$\sqrt{\sqrt[3]{28}-\sqrt[3]{27}}=-\frac{1}{3}(-\sqrt[3]{98}+\sqrt[3]{28}+1);$$

$$\sqrt{\sqrt[3]{5}-\sqrt[3]{4}}=\frac{1}{3}(-\sqrt[3]{25}+\sqrt[3]{20}+\sqrt[3]{2});$$

$$\sqrt[3]{\cos\frac{2\pi}{7}}+\sqrt[3]{\cos\frac{4\pi}{7}}+\sqrt[3]{\cos\frac{8\pi}{7}}=\sqrt[3]{\frac{5-3\sqrt{7}}{2}};$$

$$\sqrt[6]{7\sqrt[3]{20}-19}=\sqrt[3]{\frac{5}{3}}-\sqrt[3]{\frac{2}{3}};$$

$$\sqrt{8-\sqrt{8+\sqrt{8-\cdots}}}=1+2\sqrt{3}\sin 20^\circ;$$

$$\sqrt{23-2\sqrt{23+2\sqrt{23+2\sqrt{23-\cdots}}}}=1+4\sqrt{3}\sin 20^\circ.$$

Finally, we mention in passing:

Finally, we mention in passing:

$$\frac{e^{-2\pi/5}}{1+}\,\frac{e^{-2\pi}}{1+}\,\frac{e^{-4\pi}}{1+}\,\frac{e^{-6\pi}}{1+}\cdots = \sqrt{\frac{5+\sqrt{5}}{2}} - \frac{\sqrt{5}+1}{2}.$$

Finally, we mention in passing:

$$\frac{e^{-2\pi/5}}{1+}\,\frac{e^{-2\pi}}{1+}\,\frac{e^{-4\pi}}{1+}\,\frac{e^{-6\pi}}{1+}\cdots=\sqrt{\frac{5+\sqrt{5}}{2}}-\frac{\sqrt{5}+1}{2}.$$

The last expressions for the so-called Rogers-Ramanujan continued fraction appeared in Ramanujan's first letter to Hardy. These formulae are among some problems posed by Ramanujan in the Journal of the Indian Mathematical Society.

We notice that radicals are multi-valued and the meaning of expressions where radicals appear has to be made clear.

We notice that radicals are multi-valued and the meaning of expressions where radicals appear has to be made clear. Specially, where there is a ‘nesting’ of radicals, the level of complexity increases exponentially with each radical sign and it is computationally important to have equivalent expressions with the least number of radical signs.

We notice that radicals are multi-valued and the meaning of expressions where radicals appear has to be made clear.
Specially, where there is a ‘nesting’ of radicals, the level of complexity increases exponentially with each radical sign and it is computationally important to have equivalent expressions with the least number of radical signs.
The appropriate language to analyze this type of problem is Kummer theory.

A theorem of Ramanujan

Ramanujan proved :

A theorem of Ramanujan

Ramanujan proved :
If m, n are arbitrary, then

$$\sqrt{m\sqrt[3]{4m-8n}+n\sqrt[3]{4m+n}}=$$

$$\pm\frac{1}{3}(\sqrt[3]{(4m+n)^2}+\sqrt[3]{4(m-2n)(4m+n)}-\sqrt[3]{2(m-2n)^2}).$$

A theorem of Ramanujan

Ramanujan proved :
If m, n are arbitrary, then

$$\sqrt{m\sqrt[3]{4m-8n}+n\sqrt[3]{4m+n}}=$$

$$\pm\frac{1}{3}(\sqrt[3]{(4m+n)^2}+\sqrt[3]{4(m-2n)(4m+n)}-\sqrt[3]{2(m-2n)^2}).$$

This is easy to verify simply by squaring both sides(!) but it is neither clear how this formula was arrived at nor how general it is.

A theorem of Ramanujan

Ramanujan proved :
If m, n are arbitrary, then

$$\sqrt{m\sqrt[3]{4m-8n}+n\sqrt[3]{4m+n}}=$$

$$\pm\frac{1}{3}(\sqrt[3]{(4m+n)^2}+\sqrt[3]{4(m-2n)(4m+n)}-\sqrt[3]{2(m-2n)^2}).$$

This is easy to verify simply by squaring both sides(!) but it is neither clear how this formula was arrived at nor how general it is. Are there more general formulae?

A theorem of Ramanujan

Ramanujan proved :
If m, n are arbitrary, then

$$\sqrt{m\sqrt[3]{4m-8n}+n\sqrt[3]{4m+n}}=$$

$$\pm\frac{1}{3}(\sqrt[3]{(4m+n)^2}+\sqrt[3]{4(m-2n)(4m+n)}-\sqrt[3]{2(m-2n)^2}).$$

This is easy to verify simply by squaring both sides(!) but it is neither clear how this formula was arrived at nor how general it is. Are there more general formulae?
In fact, it turns out that Ramanujan was absolutely on the dot here; the following result shows Ramanujan's result cannot be bettered :

Let $\alpha, \beta \in \mathbf{Q}^*$ such that α/β is not a perfect cube in $\mathbf{Q}$. Then, $\sqrt{\sqrt[3]{\alpha} + \sqrt[3]{\beta}}$ can be denested if and only if there are integers m, n such that $\frac{\alpha}{\beta} = \frac{(4m-8n)m^3}{(4m+n)n^3}$.

Let $\alpha, \beta \in \mathbf{Q}^*$ such that α/β is not a perfect cube in $\mathbf{Q}$. Then, $\sqrt{\sqrt[3]{\alpha} + \sqrt[3]{\beta}}$ can be denested if and only if there are integers m, n such that $\frac{\alpha}{\beta} = \frac{(4m-8n)m^3}{(4m+n)n^3}$.

For instance, it follows by this theorem that $\sqrt{\sqrt[3]{3} + \sqrt[3]{2}}$ cannot be denested.

By the denesting of a nested radical one means rewriting it with fewer radical symbols.

By the denesting of a nested radical one means rewriting it with fewer radical symbols.
The usual convention used in fixing the values of radical expressions is:
$\sqrt[3]{t}$ for a real number t will stand for the unique real cube root and, if s is a positive real number, $\sqrt{s}$ stands for the value which is the positive square root.

By the denesting of a nested radical one means rewriting it with fewer radical symbols.
The usual convention used in fixing the values of radical expressions is:
$\sqrt[3]{t}$ for a real number t will stand for the unique real cube root and, if s is a positive real number, $\sqrt{s}$ stands for the value which is the positive square root.
For example, the expression $\sqrt[3]{\sqrt{5}+2}-\sqrt[3]{\sqrt{5}-2}$ has value 1 !

By the denesting of a nested radical one means rewriting it with fewer radical symbols.
The usual convention used in fixing the values of radical expressions is:
$\sqrt[3]{t}$ for a real number t will stand for the unique real cube root and, if s is a positive real number, $\sqrt{s}$ stands for the value which is the positive square root.
For example, the expression $\sqrt[3]{\sqrt{5}+2}-\sqrt[3]{\sqrt{5}-2}$ has value 1 !
Indeed, if t is the value (according to the agreed-upon convention above), then t is seen to be a (real) root of the polynomial X^3+3X-4. As $X^3+3X-4=(X-1)(X^2+X+4)$, the only real root is 1.

An element $x \in \overline{K}$ is a nested radical over K if and only if there exists a Galois extension L of K and a chain of intermediate fields

$$K \subset K_1 \subset \cdots \subset K_n = L$$

such that K_i is generated by radicals over K_{i-1} and $x \in L$.

An element $x \in \overline{K}$ is a nested radical over K if and only if there exists a Galois extension L of K and a chain of intermediate fields

$$K \subset K_1 \subset \cdots \subset K_n = L$$

such that K_i is generated by radicals over K_{i-1} and $x \in L$.
Normally, if an element x is a nested radical over K, one obtains a chain as above successively generated by radicals such that $x \in L$ but L may not be automatically a Galois extension.

An element $x \in \overline{K}$ is a nested radical over K if and only if there exists a Galois extension L of K and a chain of intermediate fields

$$K \subset K_1 \subset \cdots \subset K_n = L$$

such that K_i is generated by radicals over K_{i-1} and $x \in L$.
Normally, if an element x is a nested radical over K, one obtains a chain as above successively generated by radicals such that $x \in L$ but L may not be automatically a Galois extension.
Why is it so important/useful to have a Galois extension ?

An element $x \in \overline{K}$ is a nested radical over K if and only if there exists a Galois extension L of K and a chain of intermediate fields

$$K \subset K_1 \subset \cdots \subset K_n = L$$

such that K_i is generated by radicals over K_{i-1} and $x \in L$.
Normally, if an element x is a nested radical over K, one obtains a chain as above successively generated by radicals such that $x \in L$ but L may not be automatically a Galois extension.
Why is it so important/useful to have a Galois extension ?
Galois's famous theorem tells us that $x \in \overline{K}$ is a nested radical if and only if the Galois closure of $K(x)$ over K has a solvable Galois group.

An element $x \in \overline{K}$ is a nested radical over K if and only if there exists a Galois extension L of K and a chain of intermediate fields

$$K \subset K_1 \subset \cdots \subset K_n = L$$

such that K_i is generated by radicals over K_{i-1} and $x \in L$.
Normally, if an element x is a nested radical over K, one obtains a chain as above successively generated by radicals such that $x \in L$ but L may not be automatically a Galois extension.
Why is it so important/useful to have a Galois extension ?
Galois's famous theorem tells us that $x \in \overline{K}$ is a nested radical if and only if the Galois closure of $K(x)$ over K has a solvable Galois group.
Thus, if the successive extensions above are Galois extensions, they have an abelian Galois group and this theory is well-studied under Kummer theory.

One may adjoin enough roots of unity at the first step of the chain to get a chain of Galois extensions and may apply Kummer theory.

One may adjoin enough roots of unity at the first step of the chain to get a chain of Galois extensions and may apply Kummer theory.
Recall:
If K contains the n-th roots of unity, then abelian extensions L of K whose Galois groups have exponent n correspond bijectively to subgroups Ω of K^* containing $(K^*)^n$ via $L \mapsto K^* \cap (L^*)^n$ and its inverse map $\Omega \mapsto K(\Omega^{1/n})$.

One may adjoin enough roots of unity at the first step of the chain to get a chain of Galois extensions and may apply Kummer theory.
Recall:
If K contains the n-th roots of unity, then abelian extensions L of K whose Galois groups have exponent n correspond bijectively to subgroups Ω of K^* containing $(K^*)^n$ via $L \mapsto K^* \cap (L^*)^n$ and its inverse map $\Omega \mapsto K(\Omega^{1/n})$.
The following consequence of the above theorem will be a key to denesting radicals.

Proposition.
Let K denote a field extension of $\mathbf{Q}$ containing the n-th roots of unity. Suppose $a, b_1, b_2, \cdots, b_r \in \overline{\mathbf{Q}}^*$ are so that $a^n, b_1^n, \cdots, b_r^n \in K$.
Then, $a \in K(b_1, \cdots, b_r)$ if, and only if, there exist $b \in K^*$ and natural numbers $m_1, m_2, \cdots, m_r$ such that

$$a = b \prod_{i=1}^{r} b_i^{m_i}.$$

Proof.

The 'if' part is easily verified. Let us assume that $a \in L := K(b_1, \cdots, b_r)$. The subgroup Ω of L^* generated by the n-th powers of elements of (K^*) along with $b_1^n, \cdots, b_r^n$ satisfies $L = K(\Omega^{1/n})$ by Kummer theory. So, $a^n \in (L^*)^n \cap K^* = \Omega$. Thus, there exists $c \in K^*$ so that

$$a^n = c^n \prod_{i=1}^{r} b_i^{m_i n}.$$

Taking n-th roots on both sides and multiplying by a suitable n-th root of unity (remember they are in K), we get

$$a = b \prod_{i=1}^{r} b_i^{m_i}$$

for some $b \in K^*$. The proof is complete.

The following technical result from Galois theory which uses the above proposition is crucial in the denesting of $\sqrt{1+\sqrt[3]{\beta/\alpha}}$ over $\mathbf{Q}$.

Let c be a rational number which is not a perfect cube. Let $\delta \in \mathbf{Q}(\sqrt[3]{c})$ and let G denote the Galois group of the Galois-closure M of $\mathbf{Q}(\sqrt{\delta})$ over $\mathbf{Q}$. Then, the nested radical $\sqrt{\delta}$ can be denested over $\mathbf{Q}$ if, and only if, the second commutator group G'' of G is trivial. Further, these conditions are equivalent to the existence of $f \in \mathbf{Q}^*$ and some $e \in \mathbf{Q}(\delta)$ so that $\delta = fe^2$.

The following technical result from Galois theory which uses the above proposition is crucial in the denesting of $\sqrt{1+\sqrt[3]{\beta/\alpha}}$ over $\mathbf{Q}$.

Theorem.

Let c be a rational number which is not a perfect cube. Let $\delta \in \mathbf{Q}(\sqrt[3]{c})$ and let G denote the Galois group of the Galois-closure M of $\mathbf{Q}(\sqrt{\delta})$ over $\mathbf{Q}$. Then, the nested radical $\sqrt{\delta}$ can be denested over $\mathbf{Q}$ if, and only if, the second commutator group G'' of G is trivial. Further, these conditions are equivalent to the existence of $f \in \mathbf{Q}^*$ and some $e \in \mathbf{Q}(\delta)$ so that $\delta = fe^2$.

Sketch of Proof.

The essential part is to show that when G'' is trivial, then there are $f \in \mathbf{Q}^*$ and $e \in \mathbf{Q}(\delta)$ with $\delta = fe^2$.

We consider the field $K = \mathbf{Q}(\delta, \zeta_3)$, the smallest Galois extension of $\mathbf{Q}$ which contains δ. If δ_2, δ_3 are the other Galois-conjugates of δ in K, the **main claim** is that if $\delta_2\delta_3$ is not a square in K, then G'' is not trivial. To see this, suppose $\delta_2\delta_3$ (and hence its Galois-conjugates $\delta\delta_3, \delta\delta_2$) are non-squares as well. Then, $\sqrt{\delta\delta_2}$ cannot be contained in $K(\sqrt{\delta_2\delta_3})$ because of the above proposition. So, the extension $L = K(\sqrt{\delta\delta_2}, \sqrt{\delta_2\delta_3})$ has degree 4 over K and is contained in the Galois closure M of $\mathbf{Q}(\sqrt{\delta})$ over $\mathbf{Q}$. The Galois group Gal (L/K) is the abelian Klein 4-group V_4. Indeed, its nontrivial elements are $\rho_1, \rho_2, \rho_1\rho_2$ where :

ρ_1 fixes $\sqrt{\delta\delta_2}$ and sends $\sqrt{\delta_2\delta_3}$ and $\sqrt{\delta\delta_3}$ to their negatives;

ρ_2 fixes $\sqrt{\delta_2\delta_3}$ and sends $\sqrt{\delta\delta_2}$ and $\sqrt{\delta\delta_3}$ to their negatives.

Also, Gal $(K/\mathbf{Q})$ is the full permutation group on $\delta, \delta_2, \delta_3$. We also put δ_1 instead of δ for convenience.

Suppose, if possible, $G'' = \{1\}$. Now, the second commutator subgroup of Gal $(L/\mathbf{Q})$ is trivial as it is a subgroup of G''. In other words, the commutator subgroup of Gal $(L/\mathbf{Q})$ is abelian.
Consider the action of Gal$(K/\mathbf{Q})$ on Gal (L/K) defined as :

$$(\sigma, \tau) \mapsto \sigma_L \tau \sigma_L^{-1}$$

where, for $\sigma \in$Gal $(K/\mathbf{Q})$, the element $\sigma_L \in$Gal $(L/\mathbf{Q})$ which restricts to K as σ.
The following computation shows that the commutator subgroup of Gal $(L/\mathbf{Q})$ cannot be abelian.
If π :Gal $(L/\mathbf{Q}) \to$Gal$(K/\mathbf{Q})$ is the restriction map, look at any lifts a, b, c of $(12), (13), (23)$ respectively. For any $d \in$Gal (L/K), the commutator $ada^{-1}d^{-1}$ is defined independently of the choice of the lift a since Gal (L/K) is abelian. An easy computation gives :

$$a\rho_2 a^{-1}\rho_2^{-1} = \rho_1$$

$$b\rho_1 b^{-1}\rho_1^{-1} = \rho_1\rho_2$$

$$c(\rho_1\rho_2)c^{-1}(\rho_1\rho_2)^{-1} = \rho_2.$$

Therefore, the whole of Gal (L/K) is contained in the commutator subgroup of Gal $(L/\mathbf{Q})$. Now $(123) = (13)(23)(13)(23)$ implies that $d = bcb^{-1}c^{-1}$ which is in the commutator subgroup of Gal $(L/\mathbf{Q})$ is a lift of (123). Thus, $dgd^{-1}g^{-1} = Id$ for any $g \in$Gal (L/K) as Gal (L/K) is contained in the commutator subgroup of Gal $(L/\mathbf{Q})$ (an abelian group). But note that $d\rho_1 d^{-1}$ fixes $\sqrt{\delta_2\delta_3}$ and hence, cannot be equal to ρ_1. Thus, we have a contradiction to the assumption that $G'' = \{1\}$ while $\delta_2\delta_3$ is a nonsquare in K; the claim follows.

Now, assume that G'' is trivial. We would like to use the claim proved above to show that there are $f \in \mathbf{Q}^*$ and $e \in \mathbf{Q}(\delta)$ with $\delta = fe^2$.

Start with some $\eta \in K$ with $\delta_2\delta_3 = \eta^2$. We would like to show that $\eta \in \mathbf{Q}(\delta)$. This will prove our assertion, for then,

$$\delta = \frac{\delta_1\delta_2\delta_3}{\delta_2\delta_3} = \frac{\delta_1\delta_2\delta_3}{\eta^2} = fe^2$$

where $f = \delta_1\delta_2\delta_3 \in \mathbf{Q}$ and $e = \eta^{-1} \in \mathbf{Q}(\delta)$.
Suppose $\eta \notin \mathbf{Q}(\delta)$. Since the product $\delta_2\delta_3 \in \mathbf{Q}(\delta)$, on applying the above proposition to $K = \mathbf{Q}(\delta, \zeta_3) = \mathbf{Q}(\delta, \sqrt{-3})$, we get $\sqrt{\delta_2\delta_3} = \sqrt{-3}\theta$ for some $\theta \in \mathbf{Q}(\delta)$; that is,

$$\eta^2 = \delta_2\delta_3 = -3\theta^2.$$

Taking norms over $\mathbf{Q}$, we get $N(\eta) = (-3)^3 N(\theta)^2$ which is a contradiction since $(-3)^3$ is not a square in $\mathbf{Q}$. Therefore, η indeed belongs to $\mathbf{Q}(\delta)$ and we are done.

We determine conditions under which elements e, f as in the above theorem exist.

We determine conditions under which elements e, f as in the above theorem exist.
For any non-zero α, β in $\mathbf{Q}$, the polynomial

$$F_{\beta/\alpha}(t) = t^4 + 4t^3 + 8\frac{\beta}{\alpha}t - 4\frac{\beta}{\alpha}$$

plays a role in determining the denestability of the nested radical $\sqrt{\sqrt[3]{\alpha} + \sqrt[3]{\beta}}$ over $\mathbf{Q}$.

Let $\alpha, \beta \in \mathbf{Q}^*$ such that α/β is not a perfect cube in $\mathbf{Q}$. Then, $\sqrt{\sqrt[3]{\alpha} + \sqrt[3]{\beta}}$ can be denested if and only if the polynomial $F_{\beta/\alpha}$ has a root in $\mathbf{Q}$.

We determine conditions under which elements e, f as in the above theorem exist.
For any non-zero α, β in $\mathbf{Q}$, the polynomial

$$F_{\beta/\alpha}(t) = t^4 + 4t^3 + 8\frac{\beta}{\alpha}t - 4\frac{\beta}{\alpha}$$

plays a role in determining the denestability of the nested radical $\sqrt{\sqrt[3]{\alpha} + \sqrt[3]{\beta}}$ over $\mathbf{Q}$.

Lemma.

Let $\alpha, \beta \in \mathbf{Q}^*$ such that α/β is not a perfect cube in $\mathbf{Q}$. Then, $\sqrt{\sqrt[3]{\alpha} + \sqrt[3]{\beta}}$ can be denested if and only if the polynomial $F_{\beta/\alpha}$ has a root in $\mathbf{Q}$.

Proof.

Now $\sqrt{\sqrt[3]{\alpha}+\sqrt[3]{\beta}}$ can be denested if and only if $\sqrt{1+\sqrt[3]{\beta/\alpha}}$ can be denested.

Proof.

Now $\sqrt{\sqrt[3]{\alpha}+\sqrt[3]{\beta}}$ can be denested if and only if $\sqrt{1+\sqrt[3]{\beta/\alpha}}$ can be denested.

By the theorem, this happens if and only if there exists $f, x, y, z \in \mathbf{Q}$ with

$$1+\sqrt[3]{\beta/\alpha} = f(x+y\sqrt[3]{\beta/\alpha}+z\sqrt[3]{\beta^2/\alpha^2})^2 \cdots\cdots \diamondsuit$$

Proof.

Now $\sqrt{\sqrt[3]{\alpha}+\sqrt[3]{\beta}}$ can be denested if and only if $\sqrt{1+\sqrt[3]{\beta/\alpha}}$ can be denested.

By the theorem, this happens if and only if there exists $f, x, y, z \in \mathbf{Q}$ with

$$1+\sqrt[3]{\beta/\alpha} = f(x+y\sqrt[3]{\beta/\alpha}+z\sqrt[3]{\beta^2/\alpha^2})^2 \cdots\cdots \diamondsuit$$

Assume that denesting can be done.

Proof.

Now $\sqrt{\sqrt[3]{\alpha}+\sqrt[3]{\beta}}$ can be denested if and only if $\sqrt{1+\sqrt[3]{\beta/\alpha}}$ can be denested.

By the theorem, this happens if and only if there exists $f, x, y, z \in \mathbf{Q}$ with

$$1+\sqrt[3]{\beta/\alpha} = f(x+y\sqrt[3]{\beta/\alpha}+z\sqrt[3]{\beta^2/\alpha^2})^2 \cdots\cdots \diamondsuit$$

Assume that denesting can be done.

The elements $1, \sqrt[3]{\beta/\alpha}, \sqrt[3]{\beta^2/\alpha^2}$ are linearly independent over $\mathbf{Q}$.

Proof.

Now $\sqrt{\sqrt[3]{\alpha}+\sqrt[3]{\beta}}$ can be denested if and only if $\sqrt{1+\sqrt[3]{\beta/\alpha}}$ can be denested.

By the theorem, this happens if and only if there exists $f, x, y, z \in \mathbf{Q}$ with

$$1+\sqrt[3]{\beta/\alpha} = f(x+y\sqrt[3]{\beta/\alpha}+z\sqrt[3]{\beta^2/\alpha^2})^2 \cdots\cdots \diamondsuit$$

Assume that denesting can be done.

The elements $1, \sqrt[3]{\beta/\alpha}, \sqrt[3]{\beta^2/\alpha^2}$ are linearly independent over $\mathbf{Q}$.

Thus, we may compare like powers of $\sqrt[3]{\beta^2/\alpha^2}$ in $\diamondsuit$ to get

$$1 + \sqrt[3]{\beta/\alpha} = f(x + y\sqrt[3]{\beta/\alpha} + z\sqrt[3]{\beta^2/\alpha^2})^2$$

implies

$$1/f = x^2 + \frac{2yz\beta}{\alpha}$$

$$0 = y^2 + 2xz$$

$$1/f = \frac{\beta z^2}{\alpha} + 2xy$$

$$1 + \sqrt[3]{\beta/\alpha} = f(x + y\sqrt[3]{\beta/\alpha} + z\sqrt[3]{\beta^2/\alpha^2})^2$$

implies

$$1/f = x^2 + \frac{2yz\beta}{\alpha}$$

$$0 = y^2 + 2xz$$

$$1/f = \frac{\beta z^2}{\alpha} + 2xy$$

After a simple calculation, it is easy to see that $z \neq 0$ and that y/z is a root of $F_{\beta/\alpha}$.

$$1+\sqrt[3]{\beta/\alpha}=f(x+y\sqrt[3]{\beta/\alpha}+z\sqrt[3]{\beta^2/\alpha^2})^2$$

implies

$$1/f=x^2+\frac{2yz\beta}{\alpha}$$

$$0=y^2+2xz$$

$$1/f=\frac{\beta z^2}{\alpha}+2xy$$

After a simple calculation, it is easy to see that $z\neq 0$ and that y/z is a root of $F_{\beta/\alpha}$.
Conversely, suppose $F_{\beta/\alpha}$ has a rational root s. Then, working backwards, a denesting is given as :

$$\sqrt{\sqrt[3]{\alpha}+\sqrt[3]{\beta}}=\pm\frac{1}{\sqrt{f}}(-\frac{s^2\sqrt[3]{\alpha^2}}{2}+s\sqrt[3]{\alpha\beta}+\sqrt[3]{\beta^2})$$

where $f=\beta-s^3\alpha$. The proof is complete.

Examples 4.

For $\alpha = 5, \beta = -4$ we get $s = -2$ to be the rational root of $F_{-4/5}(t) = t^4 + 4t^3 - \frac{32}{5}t + \frac{16}{5} = 0$. Thus, $f = -4 + 40 = 36$ and we have

$$\sqrt{\sqrt[3]{5} - \sqrt[3]{4}} = \frac{1}{6}(-2\sqrt[3]{25} - 2\sqrt[3]{-20} + \sqrt[3]{16})$$

$$= \frac{1}{3}(-\sqrt[3]{25} + \sqrt[3]{20} + \sqrt[3]{2}).$$

Similarly, for $\alpha = 28, \beta = 27$, we have $s = -3$ and $f = 27^2$ and we get

$$\sqrt{\sqrt[3]{28} - \sqrt[3]{27}} = -\frac{1}{27}(-\frac{9}{2}\sqrt[3]{28^2} - 3\sqrt[3]{(-27)(28)} + \sqrt[3]{27^2})$$

$$= -\frac{1}{3}(-\sqrt[3]{98} + \sqrt[3]{28} + 1).$$

Connection with Ramanujan's denesting

We saw that denesting of $\sqrt{\sqrt[3]{\alpha} + \sqrt[3]{\beta}}$ involved the rational root of a certain related polynomial.

Connection with Ramanujan's denesting

We saw that denesting of $\sqrt{\sqrt[3]{\alpha} + \sqrt[3]{\beta}}$ involved the rational root of a certain related polynomial.
The connection with Ramanujan's denesting comes while trying to characterize the α, β for which the polynomial $F_{\beta/\alpha}$ has a root in $\mathbf{Q}$. This is easy to see as follows :

Lemma.
Let $\alpha, \beta \in \mathbf{Q}^*$ where the ratio is not a cube. Then $\sqrt{\sqrt[3]{\alpha} + \sqrt[3]{\beta}}$ can be denested over $\mathbf{Q}$ if, and only if, $F_{\beta/\alpha}$ has a root s in $\mathbf{Q}$ which is if, and only if, there are integers m, n so that

$$\frac{\alpha}{\beta} = \frac{(4m - 8n)m^3}{(4m + n)n^3}.$$

Of course, we need to prove only the second 'if and only if' and, even there, it suffices to prove the 'only if' part as the other implication is obvious. Now
$s^4 + 4s^3 + 8s\beta/\alpha - 4\beta/\alpha = 0$ **implies (on taking** $s = n/m$**) that**

$$\frac{\beta}{\alpha} = \frac{s^3(s+4)}{4 - 8s} = \frac{(4m + n)n^3}{(4m - 8n)m^3}.$$

Lemma.
Let $\alpha, \beta \in \mathbf{Q}^*$ where the ratio is not a cube. Then $\sqrt{\sqrt[3]{\alpha} + \sqrt[3]{\beta}}$ can be denested over $\mathbf{Q}$ if, and only if, $F_{\beta/\alpha}$ has a root s in $\mathbf{Q}$ which is if, and only if, there are integers m, n so that

$$\frac{\alpha}{\beta} = \frac{(4m - 8n)m^3}{(4m + n)n^3}.$$

Proof.
Of course, we need to prove only the second 'if and only if' and, even there, it suffices to prove the 'only if' part as the other implication is obvious. Now
$s^4 + 4s^3 + 8s\beta/\alpha - 4\beta/\alpha = 0$ **implies (on taking** $s = n/m$**) that**

$$\frac{\beta}{\alpha} = \frac{s^3(s+4)}{4 - 8s} = \frac{(4m + n)n^3}{(4m - 8n)m^3}.$$