SUSAN LANDAU

$\sqrt{2} + \sqrt{3}$: Four Different Views

Introduction

How much time does it take to factor polynomials? How can you efficiently tell if a polynomial has roots expressible in terms of radicals? Is there a fast method to decompose a polynomial into lower-degree components? Suppose it is claimed that

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

how you can check if this is true?

You have to study the underlying algebraic structure, but often the theorems are not conducive to efficient computation, and new understanding—and new results—are needed. In this article I present some theorems that resulted from the effort to find fast methods for algebraic simplification.

It should be no surprise that, in a computational area, conjecture and examples go hand-in-hand—but only after the fact did I realize how closely. Long after I had experimented, conjectured, again experimented, and then proved did I discover that a simple example—$\sqrt{2} + \sqrt{3}$—sheds much light on four seemingly unrelated results. In several cases, the theoretical ideas leap from the simple radical. And that caused me to think more about the role of example.

It is a fact little remarked upon that Euler computed his way to the law of quadratic reciprocity. Gauss's calculations led him to the prime number theorem. Similarly, Dedekind and Frobenius computed their way to conjecture and prove a number of results concerning group representations.

Despite these demonstrations of the power of computation, such calculating fell out favor in the early part of this century. By introducing abstract methods to algebra, Hilbert proved the basis theorem, the syzygy theorem, and the Nullstellensatz. Not long afterward, Noether employed similar abstract methods in her work on ascending chain conditions. Computation went out of vogue, eschewed in favor of abstraction. It was not unusual to see group theory taught without reference to a single concrete group, to find the fundamental theorem of Galois theory proved without the calculation of a single example. There are good reasons to rely on the abstract approach: it is powerful, and for many areas of mathematics, even small examples can be remarkably difficult to compute (commutative algebra is one such).

Yet, examples have much to teach us. Examples can point to a flaw in reasoning, and examples can give students something to hold onto as they attempt to grasp elusive theory. Examples can demonstrate patterns and lead to conjectures. But to those who were mathematically raised in the abstract school, it may be surprising to discover how much examples can guide research.

In this article, I present four results about computational algebra seen from the perspective of $\sqrt{2} + \sqrt{3}$. My main

purpose is illustrating four results in computational algebra, but along the way I hope to demonstrate the power of computation.

Factoring Polynomials

How does one factor a polynomial over the rationals? One might wonder if the problem is decidable; an algorithm from an astronomer in 1793 shows it is.

Let $f(x)$ be a polynomial of degree n over $\mathbb{Z}$. Compute the values $f(0), f(1), \ldots, f(n)$, and then factor each of the $f(i)$. Choose a set of factors $d(0), d(1), \ldots, d(n)$, and interpolate to find a potential factor $d(x)$ of $f(x)$. Integer factorization is decidable, and because there are only finitely many sets of the $d(i)$, factoring is decidable. However, I caution the reader not to implement this algorithm, as it takes exponential time even in the best case, namely when all the $f(i)$ are prime. (Computer scientists define the size of a problem to be the number of bits used to represent the problem. Thus, the input size of "factor the integer n" is $\log n$, as $\log n$ bits are needed to represent n. The standard viewpoint is asymptotic behavior, so I ignore constants, and, in particular, the base for the log function.)

Since the 1970s, the standard method for factoring has been the Berlekamp–Hensel algorithm (see [1, 11]). This works by factoring the polynomial mod p for some suitable choice of a prime p, and then "lifting" the factorization to one mod p^2, then to mod p^4, and so on until the coefficients are sufficiently large that one has a factorization that "resembles" the factorization over the integers. For example, the polynomial

$$x^4 - 8x^3 + x^2 - 24x - 6$$

factors into

$$(x^2 + 2x + 3)(x^2 + 3) \pmod 5$$

and into

$$(x^2 - 8x - 2)(x^2 + 3) \pmod{25}$$

and, finally, into

$$(x^2 - 8x - 2)(x^2 + 3)$$

over the integers.

That's not so bad. The real issue is, does this algorithm always work? One can always factor mod p, but will the lifting always be efficient? Are there polyomials for which the factoring blows up? Unfortunately, the answer is yes. Swinnerton-Dyer discovered certain irreducible polynomials that factor into linear or quadratic factors mod m for every integer m. Consider the polynomial

$$x^8 - 40x^6 + 352x^4 - 960x^2 + 576.$$

Over $\mathbb{Q}$, this is irreducible. But it factors into

$$(x^2 + 6x + 6)(x^2 + 6x + 3)(x^2 + x + 6)(x^2 + x + 3) \pmod 7,$$

and into four quadratic factors mod 49, and into four quadratic factors mod 343, and so on. Indeed, this polynomial will factor into linear or quadratic polynomials (mod m) for every integer m.

A polynomial of lower degree with the same property is $x^4 - 10x^2 + 1$. Its zero $\sqrt{2} + \sqrt{3}$ makes it one of a special class of polynomials discovered by Swinnerton-Dyer. These polynomials have zeros of the form

$$\sqrt{p_1} + \sqrt{p_2} + \cdots + \sqrt{p_n},$$

for a set of distinct primes $p_1, \ldots, p_n$. Galois theory explains why they split into so many pieces mod p.

Take an irreducible Swinnerton-Dyer polynomial, say $f(x)$ of degree 2^n. Over $\mathbb{Q}$, it has Galois group $(\mathbb{Z}/2\mathbb{Z})^n$. When p does not divide the discriminant of $f(x)$, the Galois group of $f(x)$ over $\mathbb{Z}/p\mathbb{Z}$ is a subgroup of the Galois group of $f(x)$ over $\mathbb{Q}$ (if p divides the discriminant, the Galois group of $f(x)$ over $\mathbb{Z}/p\mathbb{Z}$ is a homomorphic image of a subgroup of the Galois group of $f(x)$ over $\mathbb{Q}$). Finite extensions of finite fields are always normal (when one root is adjoined, all the roots are), and the Galois group is cyclic. Thus, the Galois group over $\mathbb{Z}/p\mathbb{Z}$ must be $\mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/\mathbb{Z}$. The polynomial $f(x)$ must give rise to an extension of degree at most 2 over $\mathbb{Z}/p\mathbb{Z}$. Thus, $f(x)$ splits into linear or quadratic factors mod p for every p.

Suppose now one takes two Swinnerton-Dyer polynomials, say $f_1(x)$ with zeros $\sqrt{2} + \sqrt{5} + \cdots + \sqrt{p_{2n-1}}$ and $f_2(x)$ with zero $\sqrt{3} + \sqrt{11} + \cdots + \sqrt{p_{2n}}$. Then, $f_1(x)\, f_2(x)$ is of degree $2n$ over $\mathbb{Q}$ but factors into 2^{2n-2}, 2^{2n-1} or 2^{2n} irreducibles (mod p). (One must be careful to stay away from primes that divide the discriminant of the polynomial, as factoring over such primes introduces repeated factors.) Recombining factors to find the factorization of $f_1(x)f_2(x)$ over $\mathbb{Q}$ involves at least 2^{2^n} combinations.

When Does a Polynomial Have Solvable Zeros?

Given an irreducible polynomial over the rationals, how can we tell if its zeros are expressible in terms of radicals? Galois theory gives a technique to discover the answer. That is, in principle. In practice, if $f(x)$ is a polynomial of degree n, Galois's algorithm takes time greater than $2^{n!}$ steps to determine solvability—even with today's computers, the technique is simply not viable for polynomials of degree higher than 5.

There is another well-known method to solve this problem: factor $f(x)$ over $\mathbb{Q}[x]/f(x)$, adjoin a zero of one of the remaining nonlinear irreducible factors, factor $f(x)$ over the new field, adjoin another zero, and stop only when the polynomial splits completely. This is a faster technique than Galois's original method. Ignoring the size of the coefficients of $f(x)$, bootstrapping, as this method is called, takes 2^n steps to find generators for the splitting field of $f(x)$ over $\mathbb{Q}$. Unfortunately, this is exponential in n.

There is, however, a polynomial-time algorithm for the problem. The idea is quite simple: divide the the solvability question up into lots of smaller solvability problems.

Let α be a zero of the polynomial $f(x)$. Suppose there is a field $\mathbb{Q}(\beta)$ between $\mathbb{Q}$ and $\mathbb{Q}(\alpha)$, $\mathbb{Q} \subset \mathbb{Q}(\beta) \subset \mathbb{Q}(\alpha)$. Then, α is expressible in radicals over $\mathbb{Q}$ if and only if α is expressible in radicals over $\mathbb{Q}(\beta)$ and β is expressible in terms of radicals over $\mathbb{Q}$. There's no reason why one should stop with one intermediate field.

Suppose I could find a maximal chain of fields $\mathbb{Q} = \mathbb{Q}(\beta_0) \subset \mathbb{Q}(\beta_1) \subset \cdots \subset \mathbb{Q}(\beta_n) \subset \mathbb{Q}(\alpha) = \mathbb{Q}(\beta_{n+1})$, where $\mathbb{Q}(\beta_i) \subset F \subset \mathbb{Q}(\beta_{i+1})$ implies $F = \mathbb{Q}(\beta_i)$ or $F = \mathbb{Q}(\beta_{i+1})$. Then, α is expressible in radicals over $\mathbb{Q}$ if and only if α is expressible in radicals over $\mathbb{Q}(\beta_n)$ and β_n is expressible in radicals over $\mathbb{Q}(\beta_{n-1})$ and . . . and β_1 is expressible in radicals over $\mathbb{Q}(\beta_0) = \mathbb{Q}$.

In terms of group theory, I am looking at subgroups of G_α, the subgroup of the Galois group that fixes α. Let G act on a set $\Omega = \{\alpha_1, \ldots, \alpha_n\}$. $\Delta \subset \Omega$ is a *block of imprimitivity* if for all $\sigma \in G$, $\sigma(\Delta) \cap \Delta = \varnothing$ or Δ. The singleton sets and the full set Ω are always blocks; if these are the only blocks of imprimitivity, then the group is acting *primitively* on Ω. To say that there is no field between $\mathbb{Q}(\beta_i)$ and $\mathbb{Q}(\beta_{i+1})$ is equivalent to saying the Galois group of the splitting field of $\mathbb{Q}(\beta_{i+1})$ over $\mathbb{Q}(\beta_i)$ acts primitively on the set of zeros of the minimal polynomial of $\mathbb{Q}(\beta_{i+1})$ over $\mathbb{Q}(\beta)$.

Primitive solvable permutation groups are small. In 1982, Pálfy showed that a primitive solvable permutation group acting on n elements has no more than $n^{3.25}$ elements [8]. So, if one could construct those intermediate fields, the Galois group that is constructed would be acting primitively on the roots. If the extensions were also solvable, by Pálfy's result they would be small, and thus could be computed quickly even by brute force.

Gary Miller and I found a polynomial-time algorithm for finding maximal subfields between $\mathbb{Q}$ and $\mathbb{Q}(\alpha)$ [6]; iterating this gives a method for finding a maximal chain of subfields. Here, I will present Hendrik Lenstra's implementation of the Landau–Miller algorithm [7]. Let $f(x)$ be the irreducible polynomial of α over $\mathbb{Q}$. Suppose $f(x)$ factors into irreducible factors $\Pi h_i(x)$ in $L = \mathbb{Q}[x]/f(x) \simeq \mathbb{Q}(\alpha)$, where α is a zero of $f(x)$. Then, for each irreducible factor $h(x)$ of $f(x)$ in L, we define the field L_h as follows:

If $h(x) = (x - \gamma)$ is a linear factor (i.e., if γ can be written as a polynomial in α with coefficients in $\mathbb{Q}$), let σ be the unique automorphism in the Galois group that takes α to γ, and let L_h be the field of invariants of σ. Otherwise, if γ is a zero of $h(x)$, a nonlinear factor of $f(x)$ in $\mathbb{Q}[x]/f(x)$, then $L_h = \mathbb{Q}(\alpha) \cap \mathbb{Q}(\gamma)$. All the maximal subfields of L occur among the L_h; they are those subfields of highest degree over $\mathbb{Q}$ ([7], p. 224). This follows from the simple observation that if G is a finite group with $H \subset J \subset G$ subgroups with $H \neq J$, and no subgroup I of G such that $H \subset I \subset J$ with $H \neq I \neq J$, then there exists $\sigma \in G - H$ such that

$$< H, \sigma > = J \quad \text{if } \sigma H \sigma^{-1} = H,$$
$$< H, \sigma H \sigma^{-1} > = J \quad \text{if } \sigma H \sigma^{-1} \neq H.$$

One can repeat this procedure [substituting $\mathbb{Q}(\beta_i)$ for $\mathbb{Q}(\alpha)$] to determine a maximal chain of subfields between $\mathbb{Q}$ and $\mathbb{Q}(\alpha)$. Not only have we determined solvability, but we have also given a technique for determining all subfields of a given field.

Let us take a simple Galois extension but one with some subfield structure. An obvious example to choose is $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3}) \simeq \mathbb{Q}[x^4 - 10x^2 + 1]/x$; as we know, the polynomial $x^4 - 10x^2 + 1$ has zeros $\pm\sqrt{2} \pm \sqrt{3}$. Factoring that polynomial over the field $\mathbb{Q}(\sqrt{2} + \sqrt{3})$, the polynomial splits completely:

$$\begin{aligned} & x^4 - 10x^2 + 1 \\ &= (x - 10(\sqrt{2} + \sqrt{3}) + (\sqrt{2} + \sqrt{3})^3)(x + 10(\sqrt{2} + \sqrt{3}) \\ &\quad -(\sqrt{2} + \sqrt{3})^3)(x + \sqrt{2} + \sqrt{3})(x - (\sqrt{2} + \sqrt{3})) \\ &= (x + \sqrt{2} - \sqrt{3})(x - \sqrt{2} + \sqrt{3})(x - \sqrt{2} - \sqrt{3}) \cdot \\ &\quad (x + \sqrt{2} + \sqrt{3}). \end{aligned}$$

There are three 2-element block decompositions.

The block decomposition $\{(\sqrt{2} + \sqrt{3}, \sqrt{2} - \sqrt{3}), (-\sqrt{2} + \sqrt{3}, -\sqrt{2} - \sqrt{3})\}$ gives rise to the polynomials $x^2 - 2\sqrt{2}x - 1$ and $x^2 + 2\sqrt{2}x - 1$ and corresponds to the field $\mathbb{Q}(\sqrt{2})$. The block decomposition $\{(\sqrt{2} + \sqrt{3}, -\sqrt{2} + \sqrt{3}), (\sqrt{2} - \sqrt{3}, -\sqrt{2} - \sqrt{3})\}$ corresponds to polynomial factors $x^2 - 2\sqrt{3}x + 1$ and $x^2 + 2\sqrt{3}x + 1$ and the field $\mathbb{Q}(\sqrt{3})$. And the block decomposition $\{(\sqrt{2} + \sqrt{3}, -\sqrt{2} - \sqrt{3}), (-\sqrt{2} + \sqrt{3}, \sqrt{2} - \sqrt{3})\}$ corresponds to polynomial factors $x^2 - 5 - 2\sqrt{6}$ and $x^2 - 5 + 2\sqrt{6}$ and the intermediate field $\mathbb{Q}(\sqrt{6})$.

If one wants a simple example of Galois theory, the field $\mathbb{Q}(\sqrt{2} + \sqrt{3})$ over $\mathbb{Q}$ is a nice one; it has a slightly complex subfield structure, with three nontrivial subfields. And the block decomposition of the four zeros $\pm\sqrt{2} \pm \sqrt{3}$ gives a simple but effective demonstration of some elementary results in primitive permutation groups. Another aspect of $\sqrt{2} + \sqrt{3}$ has surfaced.

Polynomial Decomposition

Multiplication is a fundamental mathematical operation; factoring, its reverse. But polynomials are functions and have another operation akin to multiplication, namely composition, $f(x) = g(x) \circ h(x)$ or, equivalently, $g(h(x))$. Composition is interesting for a number of reasons, including the fact that in composition, unlike polynomial multiplication, the degrees multiply. That complexity made polynomial composition a potential candidate for an RSA-type cryptosystem. (RSA is a "public key" cryptosystem in which "easy" parts of the computation are public, and difficult-to-compute portions are private, thus providing security. See [9].) The problem is also made more interesting by Lüroth's theorem [10], which tells us that if k is an arbitrary field, the fields between $k(f(x))$ and $k(x)$ are in one-to-one correspondence with the decompositions of $f(x)$; each field between $k(f(x))$ and $k(x)$ can be written as $k(h(x))$ for some (right) composition factor of $f(x)$.

These were among the motivations that Dexter Kozen and I had when we looked at the issue of decomposition. Previous algorithms had relied on factorization; a theorem of Evyater and Scott, Dorey and Whaples, and Fried and MacRae showed that the univariate polynomial $f(x)$ is decomposable into $g(h(x))$ if and only if the multivariate polynomial $h(y) - h(x)$ divides $f(y) - f(x)$. Barton and Zippel (and independently Alagar and Thanh[1]) used this to decompose: factor $f(y) - f(x)$, compute potential decomposition factors from divisors of $f(y) - f(x)$. If $f(y) - f(x)$

[1] I am presenting the Barton and Zippel algorithm.

splits into many factors of small degree, the algorithm takes exponential time to compute a decomposition. It is the old recombination of factors problem again.

Kozen and I discovered a simple way to decompose polynomials $f(x)$ when the degree is not divisible by the characteristic of the field [3]. We also found an elegant structure theorem that gives a method for decomposition. The theorem gives an effective technique for decomposition over finite fields; the theorem also applies in characteristic 0.

We began by generalizing the concept of polynomial decomposition. Let k be a field of arbitrary characteristic and let $f(x) \in k[x]$ be of degree $n = rs$, not necessarily irreducible or separable. Let $\hat{k}$ be the splitting field of $f(x)$ over k, and let $\mathcal{G}$ denote the Galois group of $\hat{k}$ over k.

Definition 1. *A block decomposition for f is a multiset Δ of multisets of elements of k such that,*

- $f = \Pi_{A\in\Delta} \Pi_{\alpha\in A}(x - \alpha)$,
- *if $\alpha \in A \in \Delta$, $\beta \in B \in \Delta$, and $\sigma \in \mathcal{G}$ such that $\sigma(\alpha) = \beta$, then*

$$B = \sigma(A) = \{\sigma(\gamma) | \gamma \in A\}.$$

A block decomposition Δ is an $r \times s$ block decomposition if $|\Delta| = r$ and $|A| = s$ for all $A \in \Delta$.

This generalization of block decomposition to multisets is useful in decomposition, where polynomials are not necessarily irreducible and may have repeated zeros.

Let c_j^m denote the jth elementary symmetric function on m-element multisets:

$$c_j^m(A) = \sum_{B\subseteq A, |B|=j} \prod_{\beta\in B} \beta.$$

We let $c_0^m = 1$.

Theorem 2 (Kozen and Landau [3]) *Let $f(x) \in k[x]$ be monic of degree $n = rs$. The following two statements are equivalent:*

- *$f = g \circ h$ for some $g, h \in k[x]$ of degree r and s, respectively.*
- *There exists an $r \times s$ block decomposition Δ for f such that*

$$c_j^s(A) = c_j^s(B) \in k \quad \text{for all } A, B \in \Delta,\ 0 \le j \le s - 1.$$

In the proof of Theorem 2, g and h are explicitly constructed from A, B, and Δ by

$$h = \sum_{j=0}^{s-1} (-1)^k c_j^s(A) x^{s-j},$$

with g determined either explicitly from

$$g(x) = \prod_{A\in\Delta} [x - (-1)^{s+1} c_s^s(A)]$$

or by the fact that $f(x) = g(h(x))$.

What is the simplest polynomial that we can use to illustrate Theorem 2? Because degrees multiply when polynomials are composed, the lowest-degree polynomial that has a nontrivial decomposition would be one of degree 4. The polynomial $x^4 - 10x^2 + 1$ fits the requirements of Theorem 2, and indeed, we get a block decomposition

A	B
$\sqrt{2} + \sqrt{3}$	$\sqrt{2} - \sqrt{3}$
$-\sqrt{2} - \sqrt{3}$	$-\sqrt{2} + \sqrt{3}$

We have

$$\begin{aligned}
\Delta &= \{\sqrt{2} + \sqrt{3}, \sqrt{2} - \sqrt{3}, -\sqrt{2} + \sqrt{3}, -\sqrt{2} - \sqrt{3}\},\\
c_0^2(A) &= 1 = c_0^2(B),\\
c_1^2(A) &= \sqrt{2} + \sqrt{3} + (-\sqrt{2} - \sqrt{3}) = 0 = -\sqrt{2} + \sqrt{3} + \sqrt{2} - \sqrt{3} = c_1^2(B),\\
c_2^2(A) &= -5 - 2\sqrt{6},\\
c_2^2(B) &= -5 + 2\sqrt{6},\\
h(x) &= x^2 - 0x = x^2,\\
g(x) &= [x - (-1)^3(-5 - 2\sqrt{6})][x - (-1)^3(-5 + 2\sqrt{6})]\\
&= x^2 - 10x + 1.
\end{aligned}$$

Thus, we have a decomposition of $x^4 - 10x^2 + 1$—a decomposition that the observant reader may have already noticed.[2]

At this point, I might have realized that I should investigate $\sqrt{2} + \sqrt{3}$ for any algebraic investigation I might try—but I did not. Instead, I first explored a number of radical expressions, and only then realized that my familiar example was a particularly easy one with which to illustrate the theorem.

Denesting Radicals

Ramanujan discovered that

$$\sqrt[3]{\sqrt[3]{2} - 1} = \sqrt[3]{1/9} - \sqrt[3]{2/9} + \sqrt[3]{4/9},$$
$$\sqrt{\sqrt[3]{5} - \sqrt[3]{4}} = 1/3(\sqrt[3]{2} + \sqrt[3]{20} - \sqrt[3]{25}),$$
$$\sqrt[6]{7\sqrt[3]{20} - 19} = \sqrt[3]{5/3} - \sqrt[3]{2/3}.$$

How can we simplify nested radicals, going from complex equations as displayed on the left-hand side to the simpler, *denested* version on the right-hand side?

Following [2], a *formula* over a field k and its *depth of nesting* are defined as follows:

- An element of k is a formula of depth 0 over k.
- An arithmetic combination (A + B, A × B, A/B) of formulas A and B is a formula whose depth over k is max(depth(A), depth(B)).
- A root $\sqrt[n]{A}$ of a formula A is a formula whose depth over k is 1+ depth(A).

Such a formula is a nested radical. A nesting of α means any formula A that can take α as a value. Note that nth roots are multivalued, so ambiguity is an issue. See [5] or [4] for further details.

[2]Although in the previous section we had three different block decompositions [corresponding to the fields $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{6})$], under the more restrictive requirements of Theorem 2 that $c_j^s(A) \in k$, we have only one block decomposition, corresponding to the single polynomial decomposition.

The formula A *can be denested over the field k* if there is a formula B of lower nesting depth than A such that A = B. Formula A *can be denested in the field L* if there is a formula B = A of lower nesting depth than A with all of the terms (subexpressions) of B lying in L. Define the *depth* of α over k to be the depth of the minimum depth expression for α. When given a formula A for α such that A can be denested, I will sometimes say that α can be denested. And I will cheat a little by writing a primitive nth root of unity as a special symbol ζ_n rather than as a nested radical; this defines the depth of nesting to be 1 for a primitive root of unity that is not already in the field.

Under what circumstances can a radical be expressed in terms of radicals with a lower depth of nesting? I discovered that each time I computed subfields of $\mathbb{Q}(\alpha)$, where α was a nested radical, the subfields corresponded to a denesting.

Theorem 3. *Suppose α is a nested radical over k, where k is a field of characteristic 0 containing all roots of unity. Then, there is a minimal depth nesting of α with each of its terms lying in the splitting field of the minimal polynomial of α over k.*

All roots of unity is a rather large extension over $\mathbb{Q}$; in particular, it is an infinite extension. From a computational standpoint, such an extension is not viable. Roots of unity are needed to make the field extensions between k and L Galois. However, we can limit ourselves to adding only those roots of unity that are necessary, thus trading optimality of denesting for finiteness of the extension over $\mathbb{Q}$. Let ζ_l denote the lth root of unity.

Theorem 4. *Suppose α is a nested radical over k, where k is a field of characteristic 0. Let L be the splitting field of $k(\alpha)$ over k, with Galois group G. Let l be the least common multiple of the exponents of the derived series of G. If there is a denesting of α such that each of the terms has depth no more than t, then there is a denesting of α over $k(\zeta_l)$ with each of the terms having depth no more than $t + 1$ and lying in $L(\zeta_l)$.*

We can restore optimality by allowing some additional roots of unity, those that arise from the original expression for α:

Corollary 5. *Let k, α, L, G, l, and t be as in Theorem 4. Let m be the least common multiple of the (m_{ij}), where the m_{ij} are the indices of the roots in the given nested expression for α. Let r be the least common multiple of (m, l). Then, there is a minimal depth nesting of α over $k(\zeta_r)$ with each of its terms lying in $L(\zeta_r)$.*

One of the simplest nested radicals is $\sqrt{5 + 2\sqrt{6}}$; consider the field extension $\mathbb{Q}(\sqrt{5 + 2\sqrt{6}})$ over $\mathbb{Q}$. As we already know, the algebraic number $\sqrt{5 + 2\sqrt{6}}$ satisfies the irreducible polynomial $x^4 - 10x^2 + 1$ over $\mathbb{Q}$. The field $\mathbb{Q}(\sqrt{5 + 2\sqrt{6}})$ is of degree 4 over $\mathbb{Q}$, and it has $\{1, \sqrt{5 + 2\sqrt{6}}, 5 + 2\sqrt{6}, (\sqrt{5 + 2\sqrt{6}})^3\}$ as a basis over $\mathbb{Q}$. This basis is of a nice mathematical form: $\{1,\alpha,\alpha^2,\alpha^3\}$. But because

$$\sqrt{5 + 2\sqrt{6}} = \sqrt{2} + \sqrt{3}$$

and 1, $\sqrt{2}$, $\sqrt{3}$, and $\sqrt{6}$ are linearly independent over $\mathbb{Q}$, $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is also a basis for $\mathbb{Q}(\sqrt{5 + 2\sqrt{6}})$ over $\mathbb{Q}$. Many people prefer the second basis; it seems more natural to them.

Thus, $\sqrt{2} + \sqrt{3}$ provides a practical reason for investigating denesting, namely designating procedures for a symbolic computation system like *Maple* to simplify nested radicals, and thus, for example, to transform the basis $\{1, \sqrt{5 + 2\sqrt{6}}, 5 + 2\sqrt{6}, (\sqrt{5 + 2\sqrt{6}})^3\}$ into $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$. In computational algebra, the practical and the theoretical often go very much hand in hand.

What Is the Significance of All This?

$\sqrt{2} + \sqrt{3}$ is one of the simplest combined radicals that exists, yet it provides a wealth of information about algebraic structure. For example, studying it demonstrates the relationship between intermediate subfields and decomposition—a relationship that led to the discovery of Theorem 2.

In one sense, I have presented a curiosity: one simple equation that illustrates results about factoring polynomials over $\mathbb{Q}$, finding subfields using minimal blocks of imprimitivity, determining decompositions of polynomials, and denesting. But I think there is a deeper issue here.

For many of us, computation has gone the way of the slide rule. We use it occasionally to illustrate a theorem. Yet the tools of such symbolic computation packages as *Maple*, *MacCauley*, *Grobner*, and *AXIOM* make such algebraic computations far easier to perform than they have ever been. When, in the 1920s, the Hilbert and Noether school made the transition to abstract methods, it was greatly beneficial to mathematics. The multivariate computations in commutative algebra were too large to be done by hand, and the abstract methods achieved what computation could not. Unfortunately, the transition went much farther. Algebraists and mathematicians of many flavors pursued abstraction, and concrete examples rarely appeared. The result was a gain—and a loss. We have a chance to recoup that now. The computational tools recently introduced by computer scientists and mathematicians enable us to solve much harder problems, in extensions of higher degree, with many variables.

I am convinced that had I fully examined $\sqrt{2} + \sqrt{3}$, results in decomposition and denesting would have jumped out at me—or others—years earlier. Proof is the backbone of mathematics. Examples can light the way. We should use them for teaching, exploring, and research.

Acknowledgments

Warm thanks to John Cremona, Donald Goldberg, and Ann Trenk; their suggestions greatly improved this article.

Supported by NSF grant CCR-9204630 and CDA-

9753055, and a grant from Sun Microsystems. This work was partially done while the author was visiting Cornell University.

REFERENCES

[1] E. Berlekamp, Factoring polynomials over finite fields, *Bell Syst. Tech. J.* 46 (1967), 1853–1859.

[2] A. Borodin, R. Fagin, J. Hopcroft, and M. Tompa, Decreasing the nesting depth of expressions involving square roots, *J. Symbol. Comput.* 1 (1985), 169–188.

[3] D. Kozen and S. Landau, Polynomial decomposition algorithms, *J. Symbol. Comput.* 7 (1989), 445–456.

[4] S. Landau, How to tangle with a nested radical, *Math. Intell.* 16, no. 2 (1994), 49–55.

[5] S. Landau, Simplification of nested radicals, *SIAM J. Comput.* 21 (1992), 85–110.

[6] S. Landau and G. Miller, Solvability by radicals is in polynomial time, *J. Comput. Syst. Sci.* 30(2) (1985), 179–208.

[7] H.W. Lenstra, Jr., Algorithms in algebraic number theory, *Bull. AMS* 26(2) (1992), 211–244.

[8] P. Pálfy, A polynomial bound for the orders of primitive solvable groups, *J. Algebra* 77 (1982), 127–137.

[9] R. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public key cryptosystems, *Communications of the ACM* 21(1978), 120–126.

[10] B.L. van der Waerden, *Algebra*, Frederick Ungar Publishing Co. (1977).

[11] H. Zassenhaus, On Hensel factorization I, *J. Number Theory* 1 (1969), 291–311.

AUTHOR

SUSAN LANDAU
Department of Computer Science
University of Massachusetts
Amherst, MA 01003 USA
e-mail: landau@cs.umass.edu

Susan Landau received her Ph.D. from MIT in 1983. Since then, she has taught at Wesleyan University and at the University of Massachusetts at Amherst. Her research interests include cryptography, algebraic algorithms, symbolic computation, and cryptography policy. Susan Landau and Whitfield Diffie recently wrote *Privacy on the Line: The Politics of Wiretapping and Encryption* (MIT Press). When she is not proving theorems or reading mail, she likes to attend the theater or the New York City Ballet, or to go hiking with her husband, two children, and dog.