Simplification of Radicals with Applications to Solving Polynomial Equations

by

Richard Eliot Berman Zippel


SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF SCIENCE at the MASSACHUSETTS INSTITUTE OF TECHNOLOGY May, 1977

Signature of Author 

Signature redacted

Department of Electrical Engineering and Computer Science, May 18, 1977

Certified by 

Signature redacted

Thesis supervisor

Accepted by 

Signature redacted

Chairman, Departmental Committee on Graduate Students

Archives

JUN 29 1977
Simplification of Radicals with Applications to Solving Polynomial Equations

by

Richard Eliot Berman Zippel

Submitted to the Department of Electrical Engineering and Computer Science on May 18, 1977 in partial fulfillment of the requirements for the degree of Master of Science.

ABSTRACT

One aspect of algebraic manipulation which has attracted interest lately is the simplification of expressions involving algebraically dependent variables. Typically one might want to simplify \( \sqrt[5]{\frac{1}{25}} + \sqrt[5]{\frac{3}{25}} - \sqrt[5]{\frac{2}{25}} \) to \( \sqrt[5]{\frac{32}{5}} - \sqrt[5]{\frac{27}{5}} \). More generally, if \( K \) is an algebraic extension of \( k \) of degree \( n \) generated by \( \alpha \) then each element of \( K \) may be expressed in the form \( a_0 + \ldots + a_{n-1} \alpha^{n-1} \) where each of the \( a_i \) are elements of \( k \).

Thus \( \{\alpha^i \mid 0 \leq i < n\} \) forms a basis for \( K \) considered as a \( k \)-algebra. We consider the simplification problem to consist of two distinct parts. The first part is the construction of a \( k \)-linear basis for the desired extension. The second part of the simplification process is to simplify the basis elements. In this thesis we consider only those extensions which can be obtained by the extraction of \( n \)th roots, i.e. solvable extensions. The theorem of the primitive element gives one technique for determining a \( k \)-linear basis, but the basis it provides makes it difficult to recover the original radicals. We present an algorithm for the construction of a \( k \)-linear basis based on Kummer theory which does not have this problem. This result generalizes the previous work of Fateman and Caviness. We also present a partial solution to the second phase of the simplification problem. This phase appears not to have been considered before in print, except for a number of problems given by Ramanujan.

THESIS SUPERVISOR: Joel Moses

TITLE: Associate Professor of Computer Science and Engineering
Chapter I

Introduction

One aspect of algebraic manipulation which has attracted interest lately is the simplification of expressions involving algebraically dependent variables or constants. Typically one might want to recognize that

\[ \sqrt{5 + 2\sqrt{6} - \sqrt{2}} = \sqrt{3} \]

or

\[ \sqrt{x + \sqrt{x^2 - 1}} = \frac{\sqrt{x + 1}}{2} + \frac{\sqrt{x - 1}}{2}. \]

More generally, if \( K \) is an algebraic extension of \( k \) of degree \( n \) generated by \( \alpha \) then each element of \( K \) may be expressed in the form \( a_0 + \ldots + a_{n-1}\alpha^{n-1} \) where each of the \( a_i \) are elements of \( k \). Thus \( \{\alpha^i | 0 \leq i < n\} \) is a \( k \)-linear basis for \( K \) considered as a \( k \)-algebra. We consider the simplification problem to consist of two distinct parts. The first part is the construction of a \( k \)-linear basis for the desired extension. The second part of the process is the simplification of the basis elements.

For \( K \), a purely algebraic extension of \( k \) of degree \( n \), the primitive element theorem says that there is an element \( \gamma \) of \( K \), called a primitive element, such that \( k(\gamma) \) is equal to \( K \). As noted above, \( \{\gamma^i | 0 \leq i < n\} \) is a \( k \)-linear basis for \( K \). A suitable technique is presented in Trager's thesis [20] for computing a primitive element of \( K \).
Let $K = k(\alpha_1, \ldots, \alpha_m)$; then the primitive element of $K$ produced by Trager's algorithm is of the form $\alpha_1 + \ell_2\alpha_2 + \ldots + \ell_m\alpha_m$, where the $\ell_i$ are rational integers. Unfortunately, the polynomials which express $\alpha_i$ in terms of $\gamma$ are substantially more complex. If $K = k(\sqrt[3]{2}, \sqrt[3]{3})$, one can use any of the roots of $x^3 - 10x^2 + 1$ as primitive elements. Thus $\{1, \gamma = \sqrt[3]{2} + \sqrt[3]{3}, \gamma^2, \gamma^3\}$ would be a basis, and

$$\sqrt[3]{2} = \frac{\gamma^3 - 9\gamma}{2} \quad \sqrt[3]{3} = \frac{\gamma^3 - 11\gamma}{2}.$$

From a user's point of view, the basis $\{1, \sqrt[3]{2}, \sqrt[3]{3}, \sqrt[3]{2\sqrt{3}}\}$ would be preferred. By a "preferable" basis for $K$ we mean a basis such that the $\alpha_i$ can be easily expressed in terms of the basis elements. In chapter II we will construct a basis (for radical extensions) wherein each basis element is the product of a number of the $\alpha_i$. This work generalizes the earlier work of Caviness [3] and Fateman [4,5]. It should be noted that most the theorems which appear in chapter II are not new. The main results are nearly one hundred years old.

The second part of the simplification process does not appear to have been considered before, save for a collection of problems due to Ramanujan [13]. Since our basis elements will be products of radicals we only consider those simplifications which pertain to isolated radicals. The type of simplification we consider is called a "de-nesting." The following list of examples should illustrate this type of simplification.

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

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

$$\sqrt[6]{\sqrt[3]{20} - 19} = 3\frac{5}{3} - 3\frac{2}{3}$$
In general nested radicals cannot be "de-nested." In chapter III we present a partial solution to the problem of de-nesting radicals. We are not able to deal with radicals which can be de-nested in fields of higher degree than the degree of definition of the radical itself. It would be interesting to see such a de-nesting if it does exist. We have been unable to produce such an example or show that one does not exist.

We consider the problem of simplifying radicals instead of more general algebraic expressions because this problem is substantially easier and occurs considerably more frequently in algebraic manipulation. While analogues of the results listed above exist for more complex algebraic extensions, it seems doubtful that they would prove useful.

The reader should note that nowhere in this thesis do we depend upon any property of the ground field except the characteristic. Thus our basis algorithm can be used for solvable algebraic function fields, and even solvable extensions of insoluble number (function) fields. For instance, if \( \alpha \) is a zero of \( x^5 - x + 1 \), an irreducible polynomial which generates an insoluble extension of \( \mathbb{Q} \), then we are able to simplify
\[
\frac{\sqrt[6]{60\alpha^3 + 87\alpha^2 + 94\alpha + 73} - \sqrt[6]{-2\alpha^4 + \alpha^3 + \alpha - 1} - \frac{\alpha + 1}{\sqrt[6]{\alpha - 1}}}{6}
\]
to zero by our basis algorithm. Most of the examples given here involve algebraic number fields rather than function fields because the expressions are somewhat simpler and the structure is a bit more transparent.

1. Survey of Previous Work

Some of earliest algorithmic work on the problem of manipulating algebraically dependent variables was done by S. Kleiman [8]. He provided an effective version
of Noether normalization, which depends heavily on resultants. No one appears to have ever implemented his techniques since they appear to be quite costly.

Caviness [3] and later Fateman [5] considered the problem of simplifying un-nested radicals in their theses. This work was recapitulated in [4]. Both Caviness and Fateman base their results on simplification of algebraic expressions on the following results. Let $k$ be a field, $k(\theta)$ an algebraic extension, contained in an algebraically closed field $L$, with minimal polynomial $f(x)$. Let $\alpha$ be an element of $L$ which has $g(x)$ as its minimal polynomial over $k$. If $g(x)$ is irreducible over $k(\theta)$ then $[k(\theta, \alpha): k(\theta)]$ (the degree of the extension) is equal to $\deg (g)$ (the degree of the polynomial $g(x)$) and the monomials in $\theta$ and $\alpha$ of low degree are linearly independent. Thus if we are able to show that $x^2 - 2$ is irreducible over $\mathbb{Q}(\sqrt{3})$ then we will know that $\{1, \sqrt{2}, \sqrt{3}, \sqrt{2}\sqrt{3}\}$ is a $\mathbb{Q}$-linear basis.

In general, Caviness and Fateman need to find conditions for which $x^n - a$ is irreducible over $k$, for some ground field $k$. To do this they appeal to the following well known theorem due to Tchebotarev [19, 9]:

**Theorem:** Let $k$ be a field and $n$ an integer $\geq 2$. Let $a$ be a non-zero element of $k$. Assume for all prime numbers $p$ which divide $n$ we have $a \in k^p$, and if $4$ divides $n$ then $a \notin 4k^4$. Then $x^n - a$ is irreducible in $k[X]$.

In fact the main results of Caviness and Fateman are all easy corollaries of the main theorem of Kummer theory which we prove in the next chapter. Briefly, if $K = k(\sqrt{\alpha_1}, \ldots, \sqrt{\alpha_m})$ is a galois extension of $k$ and $\Delta$ is the multiplicative closure of $\{\alpha_1, \ldots, \alpha_m\}$ then:

**Theorem:** The galois group of $K$ over $k$ is isomorphic to $\Delta$ modulo the elements of $\Delta$ which are perfect $r^{th}$ powers of elements of $k$. 
Caviness' main result is the following easy corollary (we let $\mathbb{Q}$ denote rational numbers and $\mathbb{C}$ denote the complex numbers).

Corollary: Let $\ell$ be a positive integer, $m$ an odd positive integer, and $p_1, \ldots, p_k$ distinct positive prime integers. Then the field $\mathbb{Q}(\omega_\ell, \sqrt[m]{p_1}, \ldots, \sqrt[m]{p_k})$ is of degree $m^k$ over $\mathbb{Q}(\omega_\ell)$ where $\omega_\ell$ is a primitive $\ell^{th}$ root of unity.

Fateman strengthens this by letting the $p_i$ be pairwise relatively prime polynomials and leaving out the roots of unity.

Corollary: Let $m$ be a positive integer, and $B_1, \ldots, B_k$ be non-constant, square-free pairwise relatively prime polynomials over $\mathbb{Q}[x_1, \ldots, x_n]$. Then the field $\mathbb{C}(x_1, \ldots, x_n)(\sqrt[m]{B_1}, \ldots, \sqrt[m]{B_k})$ is of degree $m^k$ over $\mathbb{C}(x_1, \ldots, x_n)$ where $\mathbb{C}$ is the complex numbers and $\sqrt[m]{B_i}$ denotes any one of the roots of $y^m - B_i = 0$.

Notice that both Caviness and Fateman, while restricting themselves to singly nested radicals, are not able to achieve results which differ significantly from what would be indicated by Kummer theory. Indeed their results are corollaries as we show in Chapter II. Caviness and Fateman actually come rather close to producing the main results of Kummer theory in their theses. Had they not restricted themselves to un-nested radicals they might have been able to reproduce Kummer theory. The long and tedious computations which led to their proofs are replaced in this thesis by a simple paragraph. This seems to be a rather persuasive indication of how the appropriate mathematical tools can simplify the solutions of rather tedious problems.
Chapter II

Kummer Theory and Computation with Radicals

Let $r_1, \ldots, r_m$ be rational integers, and $k$ a field with characteristic prime to each of the $r_i$. Consider the elements of the field $K = k(a_1^{1/r_1}, \ldots, a_m^{1/r_m})$ where the $a_i$ are distinct and different from 1. $K$ can be considered to be a $k$-algebra with $n = \prod r_i$ generators: \{${a_1^{s_1/r_1}, \ldots, a_m^{s_m/r_m} | 0 \leq s_1 \leq r_1}$\}. However, the degree of $K$ over $k$ can be less than $n$. For instance, $k(\sqrt{2}, \sqrt{3}, \sqrt{6})$ has degree 4 over $k$ since $\sqrt{6} = \sqrt{2}\sqrt{3}$. In general, if $\{\omega_i\}$ is this set of generators, any of $\{a_1 \omega_1 + \ldots + a_n \omega_n | a_i \in k\}$ could be zero. What we prove in this chapter is that if the $\omega_i$ are multiplicatively independent over $k^m$, for some power $m$, then they are linearly independent. Equivalently, all linear dependencies are generated by linear dependencies of two terms. Thus after eliminating these relatively easy-to-find dependencies it is not difficult to obtain a $k$-linear basis which only involves products of the $a_i^{1/r_i}$.

The theorem upon which this result is based belongs to what is known as Kummer theory. In the first section we summarize the relevant results we need and prove the general structure theorem upon which this chapter rests. For a more thorough study of Kummer theory we suggest [2,10,17]. An elementary version of the proof of the main theorem may be found in Artin's beautiful monograph [1].

The last two sections of this chapter present the basic algorithm for
determining the linearly independent basis and indicates savings which are easily garnered in an implementation.

1. Basic Kummer Theory

We begin with a few comments on group cohomology which permit us to state the theorems which follow succinctly and which simplify the proof of the main theorem. The standard references are [6, 11]. We follow the presentations of Schatz and Serre [16, 17]. Let G be a multiplicative group and A an additive group upon which G acts. We call A a G-module if the map GxA→A which sends (σ, a) to σa satisfies the following conditions.

1. 1·a = a where 1 is the identity element of G.
2. σ(a + a') = σa + σa'
3. (στ)(a) = σ(τa)

Clearly if K is a galois extension of k with galois group G, the action of G on K induces a G-module structure on K.

If 0 → A → B → C → 0 is an exact sequence, then a δ-functor $H^\ast(-)$ gives a corresponding infinite exact sequence

$$
\ldots \rightarrow H^{p-1}(C) \xrightarrow{\delta} H^p(A) \rightarrow H^p(B) \rightarrow H^p(C) \xrightarrow{\delta} H^{p+1}(A) \rightarrow \ldots
$$

There are a number of "efficability conditions" which insure uniqueness of δ-functors. Again see [6, 11]. For our considerations we need only use the following definitions.

Let $C^n(G, A) = \{f \mid G^n \rightarrow A, f \text{ is continuous}\}$ be called the set of n-cochains. We consider $G^0$ to be $\{\emptyset\}$ (the set consisting of one element, the empty set) and give G and A the discrete topology. (In general G is profinite and the topology is not so trivial. In our case the topological considerations can be ignored.) Thus $C^0(G, A)$ is
isomorphic to \( A \). Define the map \( \delta : C^n(G, A) \to C^{n+1}(G, A) \) by

\[
(\delta f)(\sigma_1, \ldots, \sigma_{n+1}) = \sigma_1 f(\sigma_2, \ldots, \sigma_{n+1}) + \sum_{j=1}^{n} (-1)^j f(\sigma_1, \ldots, \sigma_j \sigma_{j+1}, \ldots, \sigma_{n+1}) \\
+ (-1)^{n+1} f(\sigma_1, \ldots, \sigma_1)
\]

By an \( n \)-cocycle we mean an element of the kernel of \( \delta : C^n \to C^{n+1} \) and by an \( n \)-coboundary an element of the image of \( \delta : C^{n-1} \to C^n \). The \( n \)-cocycles \( (Z^n(G, A)) \) and \( n \)-coboundaries \( (B^n(G, A)) \) are groups. Since \( \delta \circ \delta = 0 \), the \( n \)-coboundary group is a subgroup of the \( n \)-cocycle group. The \( n \)th cohomology group \( (H^n(G, A)) \) is the quotient group of the cocycles by the coboundaries.

If \( f \) is an \( 0 \)-cocycle then \( \sigma(f(\sigma)) - f(\sigma) = 0 \). But since \( f \) is also an \( 0 \)-cochain it may be identified with an element of \( A \). By the cocycle condition it is fixed under the action of \( G \) and thus \( H^0(G, A) \approx A^G \), the fixed field of \( A \). If \( f \) is a \( 1 \)-cocycle then

\[ 0 = \delta f(\sigma, \tau) = \sigma f(\tau) - f(\sigma \tau) + f(\sigma), \]

i.e., \( f(\sigma \tau) = \sigma f(\tau) + f(\sigma) \). \( f \) is a coboundary if \( f(\sigma) = \sigma a - a \) for every \( \sigma \) and some fixed \( a \) corresponding to \( f \).

If \( k \) is a field, then \( k^x \) will be used to represent the multiplicative subgroup of \( k \), i.e. the non-zero elements of \( k \). We shall let \( k^n \) represent the set of \( n \)th powers of elements of \( k \). In [7], Hilbert noted the following famous theorem,

**Theorem:** (Hilbert’s theorem 90) Let \( L/K \) be a cyclic normal extension and \( \sigma \) a generator of the galois group of \( L \) over \( K \). If an element \( a \) of \( L \) has norm 1 there is an element \( b \) of \( L \) such that \( a = b/\sigma b \).

The following corollary is often useful.

**Corollary:** If \( k \) contains a primitive \( n \)th root of unity \( \zeta \), and \( K \) is a cyclic normal extension of \( k \) of degree \( n \), then there is an element \( \alpha \) of \( K \), such that \( K = k(\alpha) \) and \( \alpha^n \)
is an element of $k$.

Proof: $f$ has norm 1, therefore there is an $\alpha$ such that $\sigma \alpha = f \alpha$. Since $\alpha$ is of degree $n$ over $k$, $K = k(\alpha)$. $\sigma (\alpha^n) = (f \alpha)^n = \alpha^n$, so $\alpha^n$ is an element of $k$.

Emmy Noether generalized this substantially:

Theorem: Let $L/K$ be normal. If a map $\sigma \rightarrow f(\sigma)$ of $\mathfrak{G}(L/K)$ into $L^*$ satisfies the condition $f(\sigma \tau) = f(\sigma) f(\tau)$ for all $\sigma, \tau \in \mathfrak{G}$ then there is an element $b$ of $L^*$ such that $f(\sigma) = \frac{b}{\sigma b}$.

In view of our definition of the cohomology groups, this theorem may be stated:

Theorem: If $L/K$ is a normal extension with galois group $\mathfrak{G}$, then $H^1(\mathfrak{G}, L^*) = 0$.

Proofs of these theorems are in the standard references [1, 2, 9, 10, 16, 17].

Let $k$ be a field of characteristic $p$, and assume $p$ does not divide $n$. Assume $k$ contains a primitive $n^{th}$ root of unity and let $E_n$ be the subgroup of $k^*$ generated by $n^{th}$ roots of unity in $k$. Let $\Delta$ be a multiplicatively closed subset of $k^*$ which contains $k^*n$ (the $n^{th}$ powers of elements of $k^*$). For instance if $k = \mathbb{Q}$ we might let $n = 2$ and $\Delta = \{ab \mid a \in k, b \in \{1, 2, 3, 6\}\}$ Let $K = k(\Delta^{1/n})$ be the field obtained by adjoining the $n^{th}$ roots of elements of $\Delta$ to $k$. (Thus in our example $K = k(\sqrt{2}, \sqrt{3}, \sqrt{6})$.) Since $k$ contains a primitive $n^{th}$ root of unity, $K$ is normal over $k$.

Let $\mathfrak{G}$ be the galois group of $K$ over $k$. $K$ is generated as a $k$-module by some subset of $\Delta^{1/n}$. Let $\alpha$ be a generator. Then $(\alpha^\sigma)^n = \alpha^n$ so $\alpha^\sigma = f_\sigma \alpha$, where $f_\sigma$ is an $n^{th}$ root of unity. $\alpha^{\sigma \tau} = f_\sigma f_\tau \alpha = \alpha^{\tau \sigma}$ so $\mathfrak{G}$ is abelian. Also, for all $\sigma \in \mathfrak{G}$, $\sigma^n$ is the identity so the exponent of $\mathfrak{G}$ is $n$.

A character of a group $\mathfrak{G}$ is a map $\chi : \mathfrak{G} \rightarrow E_n$ where $n$ is the exponent of the group and $E_n$ is the multiplicative group of the $n^{th}$ roots of unity. Let $\chi$ be a 1-cocycle of $H^1(\mathfrak{G}, E_n)$. Then
Thus $\chi$ is a character of $G$, so we may identify $H^1(G, E_n)$ with the dual group of $G$. If, in addition to being an abelian extension of $k$, $K$ is also of finite degree over $k$, then $H^1(G, E_n) = G$.

We now come to the main theorem of this section. The following proof is a little heavy handed but it is very simple.

**Theorem:** $G$ is isomorphic to $\Delta/k^*$. In particular $[K:k] = (\Delta : k^*)$.

**Proof:** The following sequence is exact

$$0 \to E_n \to K^* \to K^* \to 0$$

where the surjection is the $n$th power map. A piece of the corresponding cohomology sequence is:

$$\cdots \to K^{*G} \to (K^*)^G \to H^1(G, E_n) \to H^1(G, K^*) \to \cdots$$

By Hilbert's theorem 90, $H^1(G, K^*) = 0$. By the previous remarks $G \simeq H^1(G, E_n)$. $K^{*G}$ is $K^*$ by the definition of the galois group. Thus we have the exact sequence

$$\cdots \to K^* \to (K^*)^G \to G \to 0.$$ 

And so $G \simeq (K^*)^G / K^*$ by the definition of exactness. Since $\Delta$ is contained in $(K^*)^G$, 

$$((K^*)^G:K^*) \geq (\Delta : k^*).$$

On the other hand $K$ may be considered as a $k$-module spanned by $\Delta^{1/n}/k^*$. Thus $[K:k] \leq (\Delta^{1/n}:k^*) = (\Delta : k^*)$. Therefore $((K^*)^G:K^*) = (\Delta : K^*)$ and finally

$$\Delta / k^* = (K^*)^G / K^* = G.$$

While this theorem is sufficient for many simplification problems, the following corollary is computationally simpler since it eliminates the use of $n$th roots of unity.

Let $\varphi(r)$ be the Euler $\varphi$-function (the number of integers less than $r$ which are relatively prime to $r$).
Corollary: Let $r$ be a rational integer which is relatively prime to $\varphi(r)$. Let $K = k(\alpha_1^{1/r}, \ldots, \alpha_n^{1/r})$ and let $\Delta = \{x = \alpha_1^{s_1} \cdots \alpha_n^{s_n} | 0 \leq s_i \leq r\}$ and let $S_k = \{a \in \Delta | a \in k^r\}$ then the degree of $K$ over $k$ is $(\Delta : S_k)$.

Proof: Let $k' = k(\zeta_r)$ where $\zeta_r$ is a primitive $r$th root of unity. Let $K'$ be the compositum $KK'$. Since the degree of $k'$ over $k$ is relatively prime to $[K:k]$ the intersection of $K$ and $k'$ is $k$. Applying the last theorem to the extension $K'/k'$ we have the corollary.

2. General Reduction Techniques

In the general case of simplifying multiply nested radicals we have a tower of cyclic extensions which may be refined so that $K = K_m \supset K_{m-1} \supset \ldots \supset K_0 = k$ each of which is of the form $K_i = K_{i-1}(\beta_{i1}^{1/r_i}, \ldots, \beta_{in_i}^{1/r_i})$ where the $\beta_{ij}$ are elements of $K_i$ and we require that $(\varphi(r_i), r_i) = 1$. The algorithm we present relies heavily upon factoring over $K_{i-1}$. Since algebraic factoring is so expensive it is advisable to minimize the height of the tower from $K$ to $k$.

By the main theorem of the previous section we saw that the degree of the extension $K_i/K_{i-1}$ could be computed. In this section we shall show that this computation also leads to the construction of a $K_{i-1}$-algebra basis for $K_i$. Given these bases for each extension in the tower, it is trivial to construct the basis for $K$ over $k$. So we need only consider the simple case of an extension of the form $K = k(\alpha_1^{1/r}, \ldots, \alpha_n^{1/r})$.

Clearly $\Delta_i = \{\alpha_1^{s_1} \cdots \alpha_n^{s_n} | 0 \leq s_i < r\}$ forms a group under multiplication modulo the elements $\alpha_i^{r}$. By the corollary of the last section we can determine the degree
of $K$ over $k$ by determining those elements of $\Delta_1$ which are perfect $r^{th}$ powers as elements of $k$. Determining whether $\alpha \in k$ is a perfect $r^{th}$ power is not difficult when an algebraic factoring algorithm is available. If $x^r - \alpha$ has a linear factor $x - \beta$ then $\alpha = \beta^r$. Algorithms for factoring over algebraic number fields have been presented by Wang [21] and Rothschild and Weinberger [15]. Trager’s algorithm [20], a significant improvement of one presented by van der Waerden [22 vol. I, pp. 136-137], permits factoring in an arbitrary function field.

We now assume that we can actually determine that a certain element of $\Delta_1$ is a perfect $r^{th}$ power. We let $a \sim b$ if $\frac{a}{b}$ is a perfect $r^{th}$ power. Any element which is perfect $r^{th}$ power generates a subgroup of perfect $r^{th}$ powers. Consider the following example: let $n=3$, $r=6$ and assume all the $r_i$ are also 6. $\Delta_1$ has $6 \times 6 \times 6 = 216$ elements. If we can determine that $\alpha_1 \alpha_2^3$ is a perfect sixth power then we also have

$$\begin{align*}
(\alpha_1^2 \alpha_2^3)^2 &\approx \alpha_1^4, \\
(\alpha_1^2 \alpha_2^3)^3 &\approx \alpha_2^3, \\
(\alpha_1^2 \alpha_2^3)^4 &\approx \alpha_1^2.
\end{align*}$$

All are perfect sixth powers; that is, $\alpha_1$ is a perfect cube and $\alpha_2$ is a perfect square. This reduces the size of $\Delta_1$ by a factor of 6.

There are many techniques available for finding the "quotient group" as it is called. We present one which is particularly suggestive in our case. With notation as before, each of the $\alpha_i$ (0 ≤ $i$ ≤ $n$) are of order $r_i$. Let $\alpha_1 \ldots \alpha_n$ be an element of $\Delta_1$ which is a perfect $r^{th}$ power in $k$ and assume $m_i \neq 0$. Let $w = \frac{(r_1, m_1)}{(r_1 - m_1)} \mod r_1$, where the ratio is reduced to lowest terms in $\mathbb{Z}$ and then the division takes place in the finite field. Then

$$(\alpha_2^2 \ldots \alpha_n^{m_n})^w \approx (\alpha_1^{r_1 - m_1})^w \approx \alpha_1^{(r_1, m_1)}$$

and we have reduced $\alpha_1$'s order to $(r_1, m_1)$. Notice that this equation gives a new polynomial which $\alpha_1$ must satisfy of lower degree than any which has occurred
before. We also know that
\[(\alpha_2^{m_2}...\alpha_n^{m_n})^{1/(r_1^{m_1})} \approx 1,\]
so we may repeat the procedure with this new smaller expression and obtain further reductions. The end result will be a sequence of polynomials equalities of the form
\[P_i(\alpha_i) = \alpha_i^{s_i} - f(\alpha_{i+1}, ..., \alpha_n) = 0\]
where the product of the \(s_i\) is the degree of the extension. Thus each of the \(P_i\) must be irreducible.

In summary this algorithm consists of two parts. The first, and most time consuming portion, determines which elements of \(A_1\) are actually perfect \(r^{th}\) powers. The second phase takes each of these elements of \(A_1\) and determines a list of new minimal polynomials for some of the \(\alpha_i\) which comprise the perfect \(r^{th}\) power. The following loose algorithmic description should clarify the details of this algorithm. We define two procedures here, Find-\(r^{th}\)-powers and Reduce-\(A_1\). Find-\(r^{th}\)-powers is the driver; it searches through \(A_1\) to find those elements which are \(r^{th}\) powers and then calls Reduce-\(A_1\) for each \(r^{th}\) power it finds to reduce \(A_1\) modulo that element. To aid in the search Find-\(r^{th}\)-powers maintains an array, \(A\)-table, with one location \(A\)-table(\(\gamma\)) for each element \(\gamma\) of \(A_1\) indicating one of the following

1. \(\gamma\) is known to be a perfect \(r^{th}\) power,
2. \(\gamma\) is known not to be a perfect \(r^{th}\) power or
3. It is not known whether \(\gamma\) is a perfect \(r^{th}\) power or not.

Initially all the elements of \(A\)-table are in state (3). Notice that if \(A\)-table(\(\gamma\)) indicates state (1) then \(A\)-table(\(\gamma\)) = \(A\)-table(\(\gamma^l\)) for all \(l\). If \(A\)-table(\(\gamma\)) indicates state (2) then \(A\)-table(\(\gamma\)) = \(A\)-table(\(\gamma^l\)) for all \(l\) relatively prime to \(r\).
Algorithm Find-$r^\text{th}$-powers

[1] Takes as input: $r$ the exponent of $\Delta_1$, vars a list of the radicals
[2] Initialize the following: $\Delta$-table to state (3) and Min-polys to a list of the minimal polynomials which vars satisfies.
[3] If there is not an element $\gamma$ of $\Delta_1$ such that $\Delta$-table($\gamma$) indicates state (3) then return Min-polys.
[4] If $r^\text{th}$-power($\gamma$) is true then set $\Delta$-table($\gamma'$) to state (1) for all non-negative $i$ less than the order of $\gamma$. Otherwise set $\Delta$-table($\gamma'$) to state (2) for all non-negative $i$ less than the order of $\gamma$ and relatively prime to $r$.
[5] Call Reduce-$\Delta$[\gamma] to reduce the degree of some of the minimal polynomials.

Algorithm Reduce-$\Delta$

[1] Take as argument $\gamma = \alpha_1^{m_1} \ldots \alpha_k^{m_k}$ where the order of the $\alpha_i$ is $r_i$.
[2] If $\gamma$ is 1 then return.
[3] Set $w = (r_1, m_1)/(r_1, m_1) \mod r_1$.
[4] Set $P$ to $x^{(m_1, r_1)} - \alpha_2^{m_2} \ldots \alpha_k^{m_k}$ reduced modulo the relations in Min-Polys.
[5] Change the minimal polynomial of $\alpha_1$ (on Min-Polys) to $P$.
[6] Call Reduce-$\Delta$[(\alpha_2^{m_2} \ldots \alpha_k^{m_k})^\gamma/(m_1, r_1)]

The most time consuming portion of this algorithm is determining which of the elements $\Delta_1$ are actually perfect $n^\text{th}$ powers. In general it will only be necessary to determine if approximately $\prod (1 + d(r_i))$ elements of $\Delta_1$ are perfect $r^\text{th}$ powers where $d(n)$ is the number of divisors of $n$. Thus to find a $k(\alpha_1^{1/r}, \ldots, \alpha_k^{1/r})$ we will need to determine if roughly $(1 + \log r)^k$ elements of $\Delta_1$ are perfect $r^\text{th}$ powers. Since not every element tried will be an $r^\text{th}$ power, it appears that the algebraic factoring step will dominate. So any improvements to step 4 of Find-$r^\text{th}$-powers would lead to
dramatic improvements in the algorithm.

There are several ways in which this process may be improved. It should be clear that if the elements of \( \Delta_1 \) are either constants or polynomials in several variables no two of which differ a multiplicative constant, then we can determine the perfect \( i^{th} \) powers of the polynomials and constants independently. In general if \( \Delta_1 = A \cup B \) and if for every pair \((a, a')\) of elements of \( A \) there is not a \( b \in B \) such that \( ab = a' \) then we can treat \( A \) and \( B \) separately.

If \( k \) is a unique factorization domain in which \( \gcd \)'s may be taken and \( k = k(\sqrt[n]{\alpha_1}, \ldots, \sqrt[n]{\alpha_n}) \) then it is obvious that we can compute the basis by only taking \( \gcd \)'s. This is the type of problem which Caviness and Fateman can handle, and this is the way they handle it. \([4]\) covers this thoroughly, but note that by our theorem their techniques are valid in any unique factorization domain in which \( \gcd \)'s can be computed effectively. If \( k \) is not a unique factorization domain, however, and if \( \rho_1 \rho_2 = \rho_3 \rho_4 \) are four irreducible elements of \( k \), then the four radicals \( \sqrt[4]{\rho_i} \) are not independent. Contrast this with Caviness and Fateman's results in the first chapter.

3. Examples of the Reduction Technique

To illustrate this technique consider our favorite example:

\[
\sqrt{5+2\sqrt{6}} - \sqrt{2}.
\] (1)

We have \( \alpha_1 = 5 + 2\sqrt{6}, \alpha_2 = 2, k = \mathbb{Q} (\sqrt{6}) \). What follows is a solution by MACSYMA \([12]\) of this problem. What follows is a formatted version of a terminal session with MACSYMA. All commands in MACSYMA end with a semi-colon. First we set a few variables TIME:TRUE tells MACSYMA to indicate the time required for the computation of the last command. Setting the switch ALGBRAIC to TRUE in this problem allows
the system to rationalize denominators in step 8.

(C1) (TIME:TRUE, ALGEBRAIC:TRUE);
   time = 1 msec.

(D1) TRUE

(C2) $\alpha_1 : 5 + \sqrt{6}$;
   time = 13 msec.

(D2) $5 + \sqrt{6}$

(C3) $\alpha_2 : 2$;
   time = 1 msec.

(D3) 2

In C2 and C3 we set up $\alpha_1$ and $\alpha_2$. Now we determine which of the three candidates is actually a perfect square. FACTOR is a MACSYMA function which can do algebraic factoring.

(C4) FACTOR($x^2 - \alpha_1$);
   time = 70 msec.

(D4) $x^2 - 2 \sqrt{6} - 5$

(C5) FACTOP($x^2 - \alpha_2$);
   time = 18 msec.

(D5) $x^2 - 2$

(C6) FACTOR($x^2 - \alpha_1 \alpha_2$);
   time = 101 msec.

(D6) $(x - \sqrt{6} - 2) (x + \sqrt{6} + 2)$

Thus we can determine the reduction simplification, and can simplify (1).

(C7) $\sqrt{\alpha_1} \sqrt{\alpha_2} = - \text{EV(PART(D6,1),} x = 0)$;
   time = 58 msec.

(D7) $\sqrt{2} \sqrt{2 + \sqrt{6}} = \sqrt{6} + 2$
In April 1976 H. Stark suggested the author study the following problem due to Shanks [18] (which actually led to the results of this chapter). At SYMSAC '76, Fateman posed the same problem:

\[
\sqrt{11 + 2\sqrt{29}} + \sqrt{16 - 2\sqrt{29} + 2\sqrt{55 + 10\sqrt{29}}} = \sqrt{22 + 2\sqrt{5} + \sqrt{5}}.
\]

The triply nested radical is not a square as an element of \(\mathbb{Q}(\sqrt{29}, \sqrt{55 + 10\sqrt{29}})\), but as an element of \(\mathbb{Q}(\sqrt{5}, \sqrt{29}, \sqrt{55 + 10\sqrt{29}})\) it is:

\[
16 - 2\sqrt{29} + 2\sqrt{55 - 10\sqrt{29}} = (\sqrt{5} + \sqrt{11 - 2\sqrt{29}})^2.
\]

In the next chapter we show how to determine the fields in which to search for perfect powers; what we consider here is the resulting simplification problem:

\[
\sqrt{11 + 2\sqrt{29}} + \sqrt{11 - 2\sqrt{29}} = \sqrt{22 + 2\sqrt{5}}. \quad (2)
\]

Using the technique just described, we have \(\alpha_1 = 11 + 2\sqrt{29}, \alpha_2 = 11 - 2\sqrt{29}, \) and \(\alpha_3 = 22 + 2\sqrt{5}. \) \(\alpha_1\alpha_2 = 5,\) which happens to be a perfect square in \(k.\) This gives the following reduction:

\[
\sqrt{11 - 2\sqrt{29}} = \frac{11 - 2\sqrt{29}}{\sqrt{5}} \sqrt{11 + 2\sqrt{29}}.
\]

Continuing, we get
\[ \alpha_1 \alpha_3 = 242 + 4\sqrt{29} + 22\sqrt{5} + 4\sqrt{5}\sqrt{29} = (\sqrt{5} + 11 + 2\sqrt{29})^2. \]

So finally
\[ \sqrt{22 + 2\sqrt{5}} = 1 + \frac{11 - 2\sqrt{29}}{\sqrt{5}} \sqrt{11 + 2\sqrt{29}}. \]

And thus all the radicals involved in (2) can be expressed in terms of a single quadratic extension of \( \mathbb{Q}(\sqrt{5}, \sqrt{29}) \).
Chapter III

De-nesting Radicals

In the last chapter we presented an algorithm which determined a basis for a field consisting of radicals. This algorithm did not consider possible simplifications of the radicals themselves. What we will do in this section is present the coup de gras of radical simplification, de-nesting radicals. Typical of these very non-trivial simplifications is the following problem of Ramanujan [13]:

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

(1)

To see that \( \sqrt[3]{2} - 1 \) has no perfect cube root in \( \mathbb{Q}(\sqrt{2}) \) we note that \( x^3 - \sqrt[3]{2} + 1 \) is irreducible modulo 31. (\( x^3 - 2 \) splits into linear factors modulo 31. Thus the image of \( \mathbb{Q}(\sqrt[3]{2}) \) in \( \mathbb{Z}/31\mathbb{Z} \) is \( \mathbb{Z}/31\mathbb{Z} \). The images of \( x^3 - \sqrt[3]{2} + 1 \) are all irreducible modulo 31.) Equivalently we could use an algebraic factoring algorithm to show that \( x^3 - \sqrt[3]{2} + 1 \) is irreducible over \( \mathbb{Q}(\sqrt[3]{2}) \).

One of the key points to note about (1) is that while \( \sqrt[3]{2} - 1 \) is not a perfect cube, \( 9\sqrt[3]{2} - 9 \) is a perfect cube. In the first section of this chapter we prove a general structure theorem which make this observation precise. Using this theorem we are able to produce a necessary and sufficient condition for a multiply nested radical to de-nest and we use it as the basis of an algorithm which we present in the second section. Using this algorithm and other heuristics we produce a number of
Interesting examples which are presented in the third section. These examples are general formulae which may be used in place of the more complicated algorithm.

1. The Structure Theorem

In this section we produce a structure theorem which indicates when a field of nesting level \( n \) can be mapped isomorphically to a field of nesting level \( n - 1 \). To be precise consider the following tower of fields:

\[
L = KF \\
K \\
k = KnF
\]

where \( L \) is the compositum of the fields \( K \) and \( F \). The following proposition is useful [9].

**Proposition:** Let \( K, F, k \) and \( L \) be as above, \( L \) galois over \( K \). Then \( F \) is galois over \( k \) and the galois group of \( L \) over \( K \) is isomorphic to the galois group of \( F \) over \( k \).

Now assume that \( L = K(\sqrt[r]{\alpha}) \). We can now prove the main theorem of this section.

**Theorem:** If \( K, F, k \) and \( L \) which satisfy the above conditions and \( k \) contains \( \zeta_r \), a primitive \( r^{th} \) root of unity, then there exists a \( \beta \), an element of \( k \) such that \( \alpha \beta \) is a perfect \( r^{th} \) power of an element of \( K \).

**Proof:** \( L/K \) is a normal extension, and thus \( F/k \) is also normal. Let \( G \) be the galois group of \( L/K \). The automorphisms of \( L \) which fix \( K \) are those which send \( \sqrt[r]{\alpha} \) to \( \zeta_r \sqrt[r]{\alpha} \).

Thus \( F \) is cyclic over \( k \), and by the corollary to Hilbert's Theorem 90, \( F \) is generated by \( \sqrt[r]{\gamma} \) where \( \gamma \) is an element of \( k \). Let \( \sigma \) be a generator of \( G \) such that \( \sigma \sqrt[r]{\alpha} = \zeta_{r} \sqrt[r]{\alpha} \) and \( \sigma \sqrt[r]{\gamma} = \zeta \sqrt[r]{\gamma} \). \( L = K(\sqrt[r]{\gamma}) \) and \( [L : K] \) is equal to \( [F : k] \) so \( \sqrt[r]{\gamma} \) is of degree \( r \) over \( K \).
Therefore \( f \) must be a primitive root of unity. There is an \( m \) such that \( \bar{f}^m f = 1 \) and \( \bar{f}^m \) is a primitive \( n^{th} \) root of unity. Letting \( \sqrt[\gamma]{\beta} \) be \( (\sqrt{\gamma})^m \) we have \( \sigma(\sqrt[\alpha]{\sqrt[\beta]{\gamma}}) = \bar{f}^m \sqrt[\alpha]{\sqrt[\beta]{\gamma}} = \sqrt[\alpha]{\sqrt[\beta]{\gamma}} \). Thus \( \sqrt[\alpha]{\sqrt[\beta]{\gamma}} \) is fixed by \( G \) and must be in \( K \). So \( \alpha \beta \) is an element of \( K^r \). \( \square \)

As an example of the use of this theorem consider \( \sqrt{5 + 2\sqrt{6}} \). Then \( K = \mathbb{Q}(\sqrt{6}) \). The only proper subfield of \( K \) is \( \mathbb{Q} \) so \( K \cap F = \mathbb{Q} = k \). We are looking for a element \( \beta \), of \( \mathbb{Q} \), for which \( \beta(5 + 2\sqrt{6}) \) is a perfect square \( (a + b\sqrt{6})^2 \). We would then have the de-nesting:

\[
\sqrt{5 + 2\sqrt{6}} = \frac{a + b\sqrt{6}}{\sqrt{\beta}}.
\]

Trying a few small integers we see that \( 2(5 + 2\sqrt{6}) = (2 + \sqrt{6})^2 \) and \( 3(5 + 2\sqrt{6}) = (3 + \sqrt{6})^2 \). In the general quadratic case we have

\[
\beta(p + \sqrt{q}) = (a_0 + a_1\sqrt{q})^2.
\]

Since \( a_0 \) and \( \beta \) are elements of a field we may assume \( a_1 = 1 \) and we have the equations

\[
\beta p = a_0^2 + q, \quad \beta = 2a_0
\]
or

\[
\beta^2 - 4\beta p + 4 q = 0.
\]

Since \( \beta \) must be rational \( p^2 - q \) must be a perfect square. Letting \( d^2 = p^2 - q \), we have the following classical formula:

\[
\sqrt{p + \sqrt{q}} = \sqrt{\frac{p + d}{2}} + \sqrt{\frac{p - d}{2}}.
\]

Notice that the de-nestings which are produced by the theorem will occur in \( L \), an extension of degree \( r \) over \( K \). There may be de-nestings which only occur in fields of higher degree. We are unable to exhibit such a de-nesting nor prove that
they do not exist.

2. General De-nesting Formulae

It is easy to extend the techniques of the last section to extensions of \( K \) of arbitrary degree. Unfortunately, the systems of equations can become quite unwieldy when the degree is very large. In general we wish to de-nest the expression \( \sqrt[n]{a_0 + \ldots + a_{n-1} \alpha^{n-1}} \) where \( \alpha \) is an algebraic variable of degree \( n \) and where \( a_0 + \ldots + a_{n-1} \alpha^{n-1} \) is an element of \( K \). Let \( \beta \) be an element of a subfield of \( K \) whose \( r \)th root causes the radical to de-nest. Then we are looking for solutions of the system of equations

\[
\beta (a_0 + \ldots + a_{n-1} \alpha^{n-1}) = (x_0 + \ldots + x_{n-1} \alpha^{n-1})^r
\]

where the \( x_i \) and \( \beta \) must all lie in some proper subfield of \( K \). Since one of the \( x_i \) must be non-zero we may assume it is 1. This would lead to \( n \) equations in the \( n-1 \) variables \( x_i \) and \( \beta \). In general we may not know which of the \( x_i \) is not zero. However, the system of equations is homogeneous. Since we are looking for solutions which lie in a field, the extra indeterminate does not cause any problems. Using the standard elimination techniques, we will be left with a homogeneous polynomial in two variables for which we want a linear factor.

Ramanujan [14] has determined a number of very general formulae along these lines. Among the most interesting are

\[
\frac{3}{9} \left( m^2 + mn + n^2 \right) \left( m-n \right) \left( m+2n \right) \left( 2m+n \right) + 3mn^2 + n^3 - m^3
\]

\[
= \frac{3}{9} \left( m-n \right) \left( m+2n \right) - \frac{3}{9} \left( 2m+n \right) \left( m-n \right) + \frac{3}{9} \left( m+2n \right) \left( 2m+n \right)
\]

(2)
These amazing examples illustrate the skill of one of the greatest algebraic manipulators of all time. Our technique for de-nesting radicals of the form $\sqrt[3]{q} + p$ leads to a polynomial of degree 24, from which we are expected to divine the appropriate polynomials for $p$ and $q$ for which it has a polynomial zero; e.g., a twenty fourth degree polynomial diophantine problem in three variables. Needless to say, there are no general techniques which apply. This is unfortunate since it would be desirable to show that (2) and (3) are the only de-nesting formulae of their type. This was shown in the case of the quadratic de-nesting formula of the previous section.

However, we are able to conjecture how someone with a very fertile imagination might produce formulae like these. Notice that the form $a^2 b + b^2 c + c^2 a$ may be written as

$$\frac{1}{b^2 c} \left[ 1 + \frac{a}{b^3} + \frac{a^2}{b^3 c^3} \right],$$

where $a$ is $abc$. In view of the theorem of the preceding section this looks like a good candidate for a de-nested radical if we let $a$, $b$ and $c$ be cube roots. Replacing $a$, $b$ and $c$ by their cube roots and cubing the resulting form we get

$$3 \sqrt[3]{a} \left( \sqrt[3]{a+b+c} + ab + bc + ac \right) + a^2 b + b^2 c + ac^2 + 6 abc.$$

Thus taking $a + b + c$ to be zero we get an interesting radical which will de-nest, and which is actually a generalization of Ramanujan's.

$$\sqrt[3]{3 \sqrt[3]{ab(a+b)} - (b^3 + 6 ab^2 + 3 ba^2 - a^3)} = \sqrt[3]{a^2 b} - \sqrt[3]{b^2 (a+b)} + \sqrt[3]{a(a+b)^2}$$

Taking $a = m - n$ and $b = m + 2n$ we get (2) after removing a factor of 9 from the left.
hand side. A similar but more difficult derivation is possible for (3).

All of these results may be useful in solving polynomial equations. Consider the fourth degree equation \(x^4 - 2ax^2 + b\). It has

\[\pm \sqrt{a} \pm \sqrt{a^2 - b}\]

as its roots. Sometimes these equations have solutions of the form \(\sqrt{A} + \sqrt{B}\). Examining the de-nesting formula for quadratics we see that the radical de-nests if and only if \(b\) is a perfect square. Assume \(b = c^2\). Then we have

\[\pm \sqrt{a} \pm \sqrt{a^2 - b} = \pm \sqrt{\frac{a + c}{2}} \pm \sqrt{\frac{a + c}{2}}\].

3. Examples of the De-nesting Algorithm

First, we will finish up the solution of Shanks' problem:

\[\sqrt{11 + 2\sqrt{29}} + \sqrt{16 - 2\sqrt{29} + 2\sqrt{55 - 10\sqrt{29}}} = \sqrt{22 + 2\sqrt{5} + \sqrt{5}}\].

With this problem we must be careful as to which field we consider to be \(k\). We will indicate \(k\) by saying \(\alpha\) de-nests over \(k\). We need to de-nest the triply nested radical. (The doubly nested ones cannot be de-nested (over \(\mathbb{Q}\)) by the quadratic formula, and thus they cannot be de-nested at all.) Denote the triply nested radical by \(\alpha\) and the doubly nested radical it contains by \(\beta\). We first notice that \(\beta\) cannot be de-nested over \(\mathbb{Q}\). The field \(\mathbb{Q}(\sqrt{29}, \beta)\) has two subfields. We judiciously try de-nesting \(\alpha\) over \(\mathbb{Q}(\sqrt{29})\). Using the quadratic de-nesting formula

\[d^2 = (16 - 2\sqrt{29})^2 - 4(55 - 10\sqrt{29}) = 152 - 24\sqrt{29}\].

Now all we need do is determine if \(152 - 24\sqrt{29}\) is a perfect square in \(\mathbb{Q}(\sqrt{29})\). Using algebraic factoring (or de-nesting \(\sqrt{152 - 24\sqrt{29}}\) over \(\mathbb{Q}\)) we see that \(d = \pm (6 - 2\sqrt{29})\). Thus

\[\alpha = \sqrt{\frac{16 - 2\sqrt{29} + d}{2}} + \sqrt{\frac{16 - 2\sqrt{29} - d}{2}} = \sqrt{11 - 2\sqrt{29} + \sqrt{5}},\]
as desired.

Consider the first problem given in the introduction: \(3\sqrt[3]{2} - 1\). Here we seek \(x_0, x_1, x_2\) such that

\[
3\sqrt[3]{2} - 1 = \frac{x_0 + x_1\sqrt[3]{2} + x_2\sqrt[4]{4}}{3\beta}.
\]

Assuming \(x_0\) to be 1 and equating like coefficients of \(\sqrt[3]{2}\) we have the following set of equations:

\[
\begin{align*}
-\beta &= 2x_2^3 - 12x_1x_2 - x_1^3 - 4, \\
\beta &= 6x_2^2 - 3x_1^2x_2 - 6x_1, \\
0 &= -3x_1x_2^2 - 6x_2 - 3x_1^2.
\end{align*}
\]

Eliminating \(\beta\) from the first two equations, and then eliminating \(x_2\) from the remaining two equations, we get the following equation which \(x_1\) must satisfy:

\[
x^9 - 9x^7 - 6x^6 + 54x^5 + 36x^4 - 96x^3 - 108x^2 - 36x - 8
\]

whose only rational zeroes are -1 and 2. A similar polynomial may be deduced for \(x_2\). This polynomial has roots 1 and -2. If on the other hand we were to eliminate \(x_1\) and \(x_2\) we would get a polynomial of degree 20. This polynomial has 9, 18 and 36 as its rational zeroes. To get the de-nesting from just this we must factor \(x^3 - 9(\sqrt[3]{2} - 1)\) over \(\mathbb{Q}(\sqrt[3]{2})\).

\[
x^3 - 9(\sqrt[3]{2} - 1) = (x - (1 - \sqrt[3]{2} + \sqrt[4]{4})) \ (x^2 + (1 - \sqrt[3]{2} + \sqrt[4]{4})x + 3\sqrt[4]{4} - 3)
\]

And finally

\[
3\sqrt[3]{2} - 1 = \frac{1}{9} - \frac{2}{9} + \frac{4}{9}.
\]
Chapter IV

Summary

We have presented a general technique for determining a linearly independent basis for a finite solvable algebraic extension. The technique we provide is a natural generalization of earlier techniques presented by Caviness and Fateman and permits one to deal effectively with nested radicals. In addition we have presented a general structure theorem for nested radicals which permits one to de-nest many quite complicated expressions, among which are all the problems given by Ramanujan [13] on nested radicals.

We have hoped to show that the judicious use of higher mathematics can be yield very fruitful results in algebraic manipulation. Even a mathematical structure as complicated as cohomology groups can be useful in algebraic manipulation.

The author would like to acknowledge the many useful discussions he has had with Barry Trager and Dave Barton. Prof. Joel Moses has helped considerably in giving some direction to this work. Prof. Harold Stark has also helped give the author some appreciation of what mathematics is all about.
References


