Solution in radicals of polynomials of degree ≤ 4

developed as a series of exercises

The idea of these exercises can be motivated as follows. Suppose u and v are the roots of a quadratic equation $x^2 + ax + b = 0$. The quadratic formula expresses these roots as $u = A_0 + A_1$, $v = A_0 - A_1$, where A_0 is a polynomial in the coefficients of the given equation, and A_1 is the square root of such a polynomial; this is clearly consistent with the fact that A_0 is the same in both expressions, while A_1 changes sign. And in fact, if we solve the above pair of equations for A_0 and A_1 and then write out the resulting expressions for A_0 and A_1^2 and compare with the expressions for the coefficients a and b of the given quadratic equation in terms of u and v, we immediately see that we can express A_0 and A_1^2 in terms of a and b, allowing us to rederive the quadratic formula.

Below, we will seek to generalize this idea to get cubic and quartic formulas as well.

Throughout these exercises:

n will denote one of the values 2, 3, 4 (the degree of the equation we seek to solve),

F will be a field which contains primitive mth roots of unity for all $m \leq n$, hence has characteristic either 0 or $> n$,

$u_1, \dots, u_n$ will be elements of F (which we will later take to be roots of a polynomial; but to begin with, they will just be arbitrary elements on which we will perform some interesting manipulations)

ω (when used) will denote a primitive cube root of unity assumed to lie in F,

i (when used) will denote a primitive fourth root of unity assumed to lie in F.

(1) For each of the systems of equations (a)-(d) below, assuming the the existence in F of the roots of unity occurring in those equations, verify that $u_1, \dots, u_n$ can be written in the form shown, for unique $A_0, \dots, A_{n-1} \in F$. You may assume results of undergraduate linear algebra. (Suggestion: Write each of these systems of equations as a matrix equation, and compute the *square* of the matrix in question. You can simplify your computation by noting certain properties of the rows and columns which force most columns to have zero product with most rows. Also recall the condition on the characteristic, mentioned in the definition of F above.)

(a) $n = 2$

$$\begin{aligned} u_1 &= A_0 + A_1 \\ u_2 &= A_0 - A_1. \end{aligned}$$

(b) $n = 3$

$$\begin{aligned} u_1 &= A_0 + A_1 + A_2 \\ u_2 &= A_0 + \omega A_1 + \omega^2 A_2 \\ u_3 &= A_0 + \omega^2 A_1 + \omega A_2. \end{aligned}$$

(c) $n = 4$

$$\begin{aligned} u_1 &= A_0 + A_1 + A_2 + A_3 \\ u_2 &= A_0 + iA_1 - A_2 - iA_3 \\ u_3 &= A_0 - A_1 + A_2 - A_3 \\ u_4 &= A_0 - iA_1 - A_2 + iA_3. \end{aligned}$$

(d) $n = 4$

$$\begin{aligned} u_1 &= A_0 + A_1 + A_2 + A_3 \\ u_2 &= A_0 + A_1 - A_2 - A_3 \\ u_3 &= A_0 - A_1 + A_2 - A_3 \\ u_4 &= A_0 - A_1 - A_2 + A_3. \end{aligned}$$

(2) Suppose we perform a permutation σ on the elements $u_1, \dots, u_n$, writing $u_i' = u_{\sigma(i)}$, and obtain a representation of the new elements u_i' in terms of elements $A_i' \in F$, using the same systems of equations as above. Show that in all four of cases (a-d), we get $A_0' = A_0$, and that in *three* of the four cases, but not in the remaining one, we can say that the elements $A_1', \dots, A_{n-1}'$ are obtained from $A_1, \dots, A_{n-1}$ by a combination of a permutation, and multiplication by certain mth roots of unity, for some $m \leq n$. (Suggestion: *either* verify the result for a certain small number of permutations $\sigma \in S_n$ and show that the whole result follows, *or* note certain conditions characterizing the set of expressions giving the A's, i.e., the rows of your inverse matrix, verify that any permutation of the u's, i.e., the columns, will approximately preserve those conditions, and deduce that such a permutation will have the asserted affect on the A's.)

(3) Deduce that in each of the three ''good'' cases, the $n-1$ elementary symmetric polynomials in A_1^m, ... , A_{n-1}^m can be expressed as polynomials in the n elementary symmetric polynomials in $u_1, \dots, u_n$. Here m, which depends on n, is as in the preceding question.

(4) Deduce from this that for $2 \leq n \leq 4$, we can find formulas for the solution of polynomial equations of degree n if we have such formulas for polynomial equations of degree $n-1$, and can take mth roots (for the same m as in the last two questions). More precisely, you should show that under those assumptions, we can get formulas associating to a polynomial equation of degree n a finite set of elements, possibly more than n of them, among which the n roots must lie.

In the next two parts, you get to put the above theory into practice! Note that though (6) deals with a harder case than (5), it asks for less: only that you go through the reduction, and not that you grind out an explicit formula.

Before doing either or both of these, you might look ahead at (7), and see whether you wish to incorporate the idea thereof into your calculations. Alternatively, you could do (7) afterwards and show retroactively how it can be used to sharpen the results you get in (5) and/or (6).

(5) Carry out the procedure outlined in (1-4) for $n = 3$, culminating in a formula for solving the general monic cubic equation $x^3 + ax^2 + bx + c = 0$.

(6) Carry out the *reduction* outlined above for $n = 4$. That is, derive formulas which can be used to solve a quartic equation $x^4 + ax^3 + bx^2 + cx + d = 0$ in terms of the roots of an appropriate cubic. Suggestion: begin by showing how you can reduce to the case $u_1 + u_2 + u_3 + u_4 = 0$.

We now return to the problem noted in (4), that our procedure gives us a set of ''candidate roots'', which may be larger than the set of actual roots of our polynomial. You might prepare for the next problem by determining how many ''candidate roots'' it gives in each case. Be careful; some cases that may look at first as though they are different will turn out to be the same.

(7) Verify that in the ''good'' cases of (2) arising in the solution of the cubic and quartic equations, one has $A_1' \dots A_{n-1}' = A_1 \dots A_{n-1}$. Translate this into a statement about symmetric polynomials, and show how it allows us to modify our procedures so as to get exactly the set of roots of the given equation.

(8) (Assumes the student has seen a presentation of the *resolvant cubic* of a quartic polynomial; e.g., Hungerford, Lemmas V.4.9 and V.4.10.) In the $n = 4$ case, suppose the coefficients of the given monic quartic equation lie in a field $K \subseteq F$. Show that for A_1, A_2, A_3 defined as in (1)(d), the extension fields $K(A_1^2)$, $K(A_2^2)$, $K(A_3^2)$ are the fields generated over K by the three roots of the resolvant cubic of the given quartic.