Solutions to "Algebraic identities, polynomials" problems

1. [2004-B1] Let $k$ be an integer, $0 \leq k \leq n - 1$. Since $P(r)/r^k = 0$, we have

$$c_nr^{n-k} + c_{n-1}r^{n-k+1} + \ldots + c_{k+1}r = -(c_k + c_{k-1}r^{-1} + \ldots + c_0r^{-k}).$$

Write $r = p/q$ where $p$ and $q$ are relatively prime. Then the left hand side of the above equation can be written as a fraction with denominator $q^{n-k}$, while the right hand side is a fraction with denominator $p^k$. Since $p$ and $q$ are relatively prime, both sides of the equation must be an integer, and the result follows.

**Remark:** If we write $r = a/b$ in lowest terms, then $P(x)$ factors as $(bx-a)Q(x)$, where the polynomial $Q$ has integer coefficients because you can either do the long division from the left and get denominators divisible only by primes dividing $b$, or do it from the right and get denominators divisible only by primes dividing $a$. The numbers given in the problem are none other than $a$ times the coefficients of $Q$. More generally, if $P(x)$ is divisible, as a polynomial over the rationals, by a polynomial $R(x)$ with integer coefficients, then $P/R$ also has integer coefficients; this is known as “Gauss’s lemma” and holds in any unique factorization domain.

2. [2004-A4] It suffices to verify that

$$x_1 \cdots x_n = \frac{1}{2^n n!} \sum_{e_i \in \{-1, 1\}} (e_1 \cdots e_n)(e_1x_1 + \cdots + e_nx_n)^n.$$

To check this, first note that the right side vanishes identically for $x_1 = 0$, because each term cancels the corresponding term with $e_1$ flipped. Hence the right side, as a polynomial, is divisible by $x_1$; similarly it is divisible by $x_2, \ldots, x_n$. Thus the right side is equal to $x_1 \cdots x_n$ times a scalar. (Another way to see this: the right side is clearly odd as a polynomial in each individual variable, but the only degree $n$ monomial in $x_1, \ldots, x_n$ with that property is $x_1 \cdots x_n$.) Since each summand contributes $\frac{1}{n!}x_1 \cdots x_n$ to the sum, the scalar factor is 1 and we are done.

**Remark:** Several variants on the above construction are possible; for instance,

$$x_1 \cdots x_n = \frac{1}{n!} \sum_{e_i \in \{0, 1\}} (-1)^{n-e_1-\cdots-e_n}(e_1x_1 + \cdots + e_nx_n)^n$$

by the same argument as above.

**Remark:** These construction work over any field of characteristic greater than $n$ (at least for $n > 1$). On the other hand, no construction is possible over a field of characteristic $p \leq n$, since the coefficient of $x_1 \cdots x_n$ in the expansion of $(e_1x_1 + \cdots + e_nx_n)^n$ is zero for any $e_i$.

**Remark:** Richard Stanley asks whether one can use fewer than $2^n$ terms, and what the smallest possible number is.


**First solution:** Suppose the contrary. By setting $y = -1, 0, 1$ in succession, we see that the polynomials $1 - x + x^2, 1 + x + x^2$ are linear combinations of $a(x)$ and $b(x)$. But these three polynomials are linearly independent, so cannot all be written as linear combinations of two other polynomials, contradiction.

Alternate formulation: the given equation expresses a diagonal matrix with 1, 1, 1 and zeroes on the diagonal, which has rank 3, as the sum of two matrices of rank 1. But the rank of a sum of matrices is at most the sum of the ranks of the individual matrices.

**Second solution:** It is equivalent (by relabeling and rescaling) to show that $1 + xy + x^2y^2$ cannot be written as $a(x)d(y) - b(x)c(y)$. Write $a(x) = \sum a_ix^i, b(x) = \sum b_ix^i, c(y) = \sum c_jy^j, d(y) = \sum d_jy^j$. We now start comparing coefficients of $1 + xy + x^2y^2$. By comparing coefficients of $1 + xy + x^2y^2$ and $a(x)d(y) - b(x)c(y)$, we get

$$\begin{align*}
1 &= a_id_i - b_ic_i \quad (i = 0, 1, 2) \\
0 &= a_id_j - b_ic_j \quad (i \neq j).
\end{align*}$$
The first equation says that \( a_i \) and \( b_i \) cannot both vanish, and \( c_i \) and \( d_i \) cannot both vanish. The second equation says that \( a_i/b_i = c_j/d_j \) when \( i \neq j \), where both sides should be viewed in \( R \cup \{ \infty \} \) (and neither is undetermined if \( i, j \in \{ 0, 1, 2 \} \)). But then

\[
a_0/b_0 = c_1/d_1 = a_2/b_2 = c_0/d_0
\]

contradicting the equation \( a_0d_0 - b_0c_0 = 1 \).

**Third solution:** We work over the complex numbers, in which we have a primitive cube root \( \omega \) of 1. We also use without further comment unique factorization for polynomials in two variables over a field. And we keep the relabeling of the second solution.

Suppose the contrary. Since \( 1 + xy + x^2 y^2 = (1 - xy/\omega)(1 - xy/\omega^2) \), the rational function \( a(\omega/y)d(y) - b(\omega/y)c(y) \) must vanish identically (that is, coefficient by coefficient). If one of the polynomials, say \( a \), vanished identically, then one of \( b \) or \( c \) would also, and the desired inequality could not hold. So none of them vanish identically, and we can write

\[
\frac{c(y)}{d(y)} = \frac{a(\omega/y)}{b(\omega/y)}.
\]

Likewise,

\[
\frac{c(y)}{d(y)} = \frac{a(\omega^2/y)}{b(\omega^2/y)}.
\]

Put \( f(x) = a(x)/b(x) \); then we have \( f(\omega x) = f(x) \) identically. That is, \( a(x)b(\omega x) = b(x)a(\omega x) \). Since \( a \) and \( b \) have no common factor (otherwise \( 1 + xy + x^2 y^2 \) would have a factor divisible only by \( x \), which it doesn’t since it doesn’t vanish identically for any particular \( x \) ), \( a(x) \) divides \( a(\omega x) \). Since they have the same degree, they are equal up to scalars. It follows that one of \( a(x) \), \( xa(x) \), \( x^2 a(x) \) is a polynomial in \( x^3 \) alone, and likewise for \( b \) (with the same power of \( x \)).

If \( xa(x) \) and \( xb(x) \), or \( x^2 a(x) \) and \( x^2 b(x) \), are polynomials in \( x^3 \), then \( a \) and \( b \) are divisible by \( x \), but we know \( a \) and \( b \) have no common factor. Hence \( a(x) \) and \( b(x) \) are polynomials in \( x^3 \). Likewise, \( c(y) \) and \( d(y) \) are polynomials in \( y^3 \). But then \( 1 + xy + x^2 y^2 = a(x)d(y) - b(x)c(y) \) is a polynomial in \( x^3 \) and \( y^3 \), contradiction.

**Note:** The third solution only works over fields of characteristic not equal to 3, whereas the other two work over arbitrary fields. (In the first solution, one must replace \(-1\) by another value if working in characteristic 2.)

4.[2003-B4] **First solution:** Put \( g = r_1 + r_2, \ h = r_3 + r_4, \ u = r_1 r_2, \ v = r_3 r_4 \). We are given that \( g \) is rational. The following are also rational:

\[
\begin{align*}
\frac{-b}{a} &= g + h \\
\frac{c}{a} &= gh + u + v \\
\frac{-d}{a} &= gv + hu
\end{align*}
\]

From the first line, \( h \) is rational. From the second line, \( u + v \) is rational. From the third line, \( g(u + v) - (gv + hu) = (g - h)u \) is rational. Since \( g \neq h \), \( u \) is rational, as desired.

**Second solution:** This solution uses some basic Galois theory. We may assume \( r_1 \neq r_2 \), since otherwise they are both rational and so then is \( r_1 r_2 \).

Let \( \tau \) be an automorphism of the field of algebraic numbers; then \( \tau \) maps each \( r_i \) to another one, and fixes the rational number \( r_1 + r_2 \). If \( \tau(r_1) \) equals one of \( r_1 \) or \( r_2 \), then \( \tau(r_2) \) must equal the other one, and vice versa. Thus \( \tau \) either fixes the set \( \{ r_1, r_2 \} \) or moves it to \( \{ r_3, r_4 \} \). But if the latter happened, we would have \( r_1 + r_2 = r_3 + r_4 \), contrary to hypothesis. Thus \( \tau \) fixes the set \( \{ r_1, r_2 \} \) and in particular the number \( r_1 r_2 \). Since this is true for any \( \tau \), \( r_1 r_2 \) must be rational.

**Note:** The conclusion fails if we allow \( r_1 + r_2 = r_3 + r_4 \). For instance, take the polynomial \( x^4 - 2 \) and label its roots so that \( (x - r_1)(x - r_2) = x^2 - \sqrt{2} \) and \( (x - r_3)(x - r_4) = x^2 + \sqrt{2} \).
5.[2002-A1] By differentiating \( \frac{P_n(x)}{(x^k - 1)^{n+1}} \), we find that \( P_{n+1}(x) = (x^k - 1)P'_n(x) - (n+1)kx^{k-1}P_n(x) \); substituting \( x = 1 \) yields \( P_{n+1}(1) = -(n+1)kP_n(1) \). Since \( P_0(1) = 1 \), an easy induction gives \( P_n(1) = (-k)^n n! \) for all \( n \geq 0 \).

**Note:** one can also argue by expanding in Taylor series around 1. Namely, we have

\[
\frac{1}{x^k - 1} = \frac{1}{k(x-1)} + \ldots = \frac{1}{k} (x-1)^{-1} + \ldots,
\]

so

\[
\frac{d^n}{dx^n} \frac{1}{x^k - 1} = \frac{(-1)^n n!}{k(x-1)^{n-1}}
\]

and

\[
P_n(x) = (x^k - 1)^{n+1} \frac{d^n}{dx^n} \frac{1}{x^k - 1} = (k(x-1) + \ldots)^{n+1} \left( \frac{(-1)^n n!}{k} (x-1)^{-n-1} + \ldots \right) = (-k)^n n! + \ldots.
\]

6.[2001-A3] By the quadratic formula, if \( P_m(x) = 0 \), then \( x^2 = m \pm 2\sqrt{2m} + 2 \), and hence the four roots of \( P_m \) are given by \( S = \{ \pm \sqrt{m} \pm \sqrt{2} \} \). If \( P_m \) factors into two nonconstant polynomials over the integers, then some subset of \( S \) consisting of one or two elements form the roots of a polynomial with integer coefficients.

First suppose this subset has a single element, say \( \sqrt{m} \pm \sqrt{2} \); this element must be a rational number. Then \( (\sqrt{m} \pm \sqrt{2})^2 = 2 + m \pm 2\sqrt{2m} \) is an integer, so \( m \) is twice a perfect square, say \( m = 2n^2 \). But then \( \sqrt{m} \pm \sqrt{2} = (n \pm 1)\sqrt{2} \) is only rational if \( n = \pm 1 \), i.e., if \( m = 2 \).

Next, suppose that the subset contains two elements; then we can take it to be one of \( \{ \sqrt{m} \pm \sqrt{2}, \sqrt{2} \pm \sqrt{m} \} \) or \( \{ \pm (\sqrt{m} + \sqrt{2}) \} \). In all cases, the sum and the product of the elements of the subset must be a rational number. In the first case, this means \( 2\sqrt{m} \in Q \), so \( m \) is a perfect square. In the second case, we have \( 2\sqrt{2} \in Q \), contradiction. In the third case, we have \( (\sqrt{m} + \sqrt{2})^2 \in Q \), or \( m + 2 + 2\sqrt{2m} \in Q \), which means that \( m \) is twice a perfect square.

We conclude that \( P_m(x) \) factors into two nonconstant polynomials over the integers if and only if \( m \) is either a square or twice a square.

**Note:** a more sophisticated interpretation of this argument can be given using Galois theory. Namely, if \( m \) is neither a square nor twice a square, then the number fields \( Q(\sqrt{m}) \) and \( Q(\sqrt{2}) \) are distinct quadratic fields, so their compositum is a number field of degree 4, whose Galois group acts transitively on \( \{ \pm \sqrt{m} \pm \sqrt{2} \} \). Thus \( P_m \) is irreducible.

7.[2001-B2] By adding and subtracting the two given equations, we obtain the equivalent pair of equations

\[
\begin{align*}
2/x &= x^4 + 10x^2y^2 + 5y^4 \\
1/y &= 5x^4 + 10x^2y^2 + y^4.
\end{align*}
\]

Multiplying the former by \( x \) and the latter by \( y \), then adding and subtracting the two resulting equations, we obtain another pair of equations equivalent to the given ones,

\[
3 = (x + y)^5, \quad 1 = (x - y)^5.
\]

It follows that \( x = (3^{1/5} + 1)/2 \) and \( y = (3^{1/5} - 1)/2 \) is the unique solution satisfying the given equations.

8.[1999-A2] First solution: First factor \( p(x) = q(x)r(x) \), where \( q \) has all real roots and \( r \) has all complex roots. Notice that each root of \( q \) has even multiplicity, otherwise \( p \) would have a sign change at that root. Thus \( q(x) \) has a square root \( s(x) \).

Now write \( r(x) = \prod_{j=1}^k (x - a_j)(x - \overline{a_j}) \) (possible because \( r \) has roots in complex conjugate pairs). Write \( \prod_{j=1}^k (x - a_j) = t(x) + iu(x) \) with \( t, x \) having real coefficients. Then for \( x \) real,

\[
p(x) = q(x)r(x) = s(x)^2(t(x) + iu(x))(t(x) + iu(x)) = (s(x)t(x))^2 + (s(x)u(x))^2.
\]
(Alternatively, one can factor \( r(x) \) as a product of quadratic polynomials with real coefficients, write each as a sum of squares, then multiply together to get a sum of many squares.)

**Second solution:** We proceed by induction on the degree of \( p \), with base case where \( p \) has degree 0. As in the first solution, we may reduce to a smaller degree in case \( p \) has any real roots, so assume it has none. Then \( p(x) > 0 \) for all real \( x \), and since \( p(x) \to \infty \) for \( x \to \pm \infty \), \( p \) has a minimum value \( c \). Now \( p(x) - c \) has real roots, so as above, we deduce that \( p(x) - c \) is a sum of squares. Now add one more square, namely \((\sqrt{c})^2\), to get \( p(x) \) as a sum of squares.

9,[1999-A3] **First solution:** Computing the coefficient of \( x^{n+1} \) in the identity \( (1 - 2x - x^2) \sum_{m=0}^{\infty} a_m x^m = 1 \) yields the recurrence \( a_{n+1} = 2a_n + a_{n-1} \); the sequence \( \{a_n\} \) is then characterized by this recurrence and the initial conditions \( a_0 = 1, a_1 = 2 \).

Define the sequence \( \{b_n\} \) by \( b_{2n} = a_{2n-1}^2 + a_{2n}^2, \ b_{2n+1} = a_n(a_{n-1} + a_{n+1}) \). Then

\[
2b_{2n+1} + b_{2n} = 2a_n a_{n+1} + 2a_n + 2a_{n-1} a_n + a_{n-1} a_{n+1} + a_n^2 = a_{n+1}^2 + a_n^2 = b_{2n+2},
\]

and similarly \( 2b_{2n} + b_{2n-1} = b_{2n+1} \), so that \( \{b_n\} \) satisfies the same recurrence as \( \{a_n\} \). Since further \( b_0 = 1, b_1 = 2 \) (where we use the recurrence for \( \{a_n\} \) to calculate \( a_{-1} = 0 \)), we deduce that \( b_n = a_n \) for all \( n \). In particular, \( a_0^2 + a_1^2 = b_{2n+2} = a_{2n+2} \).

**Second solution:** Note that

\[
\frac{1}{1 - 2x - x^2} = \frac{1}{2\sqrt{2}} \left( \frac{\sqrt{2} + 1}{1 - (1 + \sqrt{2}) x} + \frac{\sqrt{2} - 1}{1 - (1 - \sqrt{2}) x} \right)
\]

and that

\[
\frac{1}{1 + (1 + \sqrt{2}) x} = \sum_{n=0}^\infty (1 + \sqrt{2})^n x^n,
\]

so that

\[
a_n = \frac{1}{2\sqrt{2}} \left( (\sqrt{2} + 1)^{n+1} - (1 - \sqrt{2})^{n+1} \right).
\]

A simple computation (omitted here) now shows that \( a_n^2 + a_{n+1}^2 = a_{2n+2} \).

10,[1999-B2] **First solution:** Suppose that \( P \) does not have \( n \) distinct roots; then it has a root of multiplicity at least 2, which we may assume is \( x = 0 \) without loss of generality. Let \( x^k \) be the greatest power of \( x \) dividing \( P(x) \), so that \( P(x) = x^k R(x) \) with \( R(0) \neq 0 \); a simple computation yields

\[
P''(x) = (k^2 - k) x^{k-2} R(x) + 2k x^{k-1} R'(x) + x^k R''(x).
\]

Since \( R(0) \neq 0 \) and \( k \geq 2 \), we conclude that the greatest power of \( x \) dividing \( P''(x) \) is \( x^{k-2} \). But \( P(x) = Q(x) P''(x) \), and so \( x^2 \) divides \( Q(x) \). We deduce (since \( Q \) is quadratic) that \( Q(x) \) is a constant \( C \) times \( x^2 \); in fact, \( C = 1/(n(n-1)) \) by inspection of the leading-degree terms of \( P(x) \) and \( P''(x) \).

Now if \( P(x) = \sum_{j=0}^n a_j x^j \), then the relation \( P(x) = C x^2 P''(x) \) implies that \( a_j = C(j-1) a_j \) for all \( j \); hence \( a_j = 0 \) for \( j < n-1 \), and we conclude that \( P(x) = a_n x^n \), which has all identical roots.

**Second solution (by Greg Kuperberg):** Let \( f(x) = P''(x)/P(x) = 1/Q(x) \). By hypothesis, \( f \) has at most two poles (counting multiplicity).

Recall that for any complex polynomial \( P \), the roots of \( P' \) lie within the convex hull of \( P \). To show this, it suffices to show that if the roots of \( P \) lie on one side of a line, say on the positive side of the imaginary axis, then \( P' \) has no roots on the other side. That follows because if \( r_1, \ldots, r_n \) are the roots of \( P \),

\[
\frac{P'(z)}{P(z)} = \sum_{i=1}^n \frac{1}{z - r_i}
\]

and if \( z \) has negative real part, so does \( 1/(z - r_i) \) for \( i = 1, \ldots, n \), so the sum is nonzero.
The above argument also carries through if \( z \) lies on the imaginary axis, provided that \( z \) is not equal to a root of \( P \). Thus we also have that no roots of \( P' \) lie on the sides of the convex hull of \( P \), unless they are also roots of \( P \).

From this we conclude that if \( r \) is a root of \( P \) which is a vertex of the convex hull of the roots, and which is not also a root of \( P' \), then \( f \) has a single pole at \( r \) (as \( r \) cannot be a root of \( P'' \)). On the other hand, if \( r \) is a root of \( P \) which is also a root of \( P' \), it is a multiple root, and then \( f \) has a double pole at \( r \).

If \( P \) has roots not all equal, the convex hull of its roots has at least two vertices.