Lecture notes of Algebra. Week 8

32. Examples of symmetric systems

A system of equations in x and y is *symmetric* if each of the equations is a symmetric polynomial (or *rational expression,* meaning a quotient of polynomials) in x and y. In that case one expresses both equations in terms of $s = x + y$ and $p = xy$, after which one can try to solve the corresponding system in s and p, and finally recover x and y. Note that if we interchange the values of x and y in any solution (x, y) we get another solution, because a symmetric system does not change if we interchange x and y.

EXAMPLE. To solve the system

$$\begin{cases} x^4 + y^4 = 17 \\ x + y = 3 \end{cases}$$

in the unknowns x and y, we express the left-hand side of the first equation in terms of $x+y$ and xy as we have just learnt, and then substitute the value for $x+y$ obtained from the second equation, obtaining

$$\begin{cases} 3^4 - 4 \cdot 3^2 \cdot xy + 2(xy)^2 = 17 \\ x + y = 3 \end{cases}$$

which becomes

$$\begin{cases} (xy)^2 - 18(xy) + 32 = 0 \\ x + y = 3 \end{cases}$$

Solving the first equation for xy we see that the system is equivalent to

$$\begin{cases} xy = 2 \\ x + y = 3 \end{cases} \quad \text{or} \quad \begin{cases} xy = 16 \\ x + y = 3 \end{cases}$$

Solving these two systems as we learned earlier we find altogether four different solutions in the complex numbers, namely,

$$(x, y) = (2, 1),\ (1, 2),\ \left(\frac{3}{2} + i\frac{\sqrt{55}}{2}, \frac{3}{2} - i\frac{\sqrt{55}}{2}\right),\ \left(\frac{3}{2} - i\frac{\sqrt{55}}{2}, \frac{3}{2} + i\frac{\sqrt{55}}{2}\right).$$

It is also true that sums $x^n + y^n$ with *negative* exponent n can be expressed in terms of $x + y$ and xy, however not as a polynomial in $x + y$ and xy but a quotient of two polynomials (which is called a *rational expression*). For example,

$$x^{-1} + y^{-1} = \frac{1}{x} + \frac{1}{y} = \frac{x + y}{xy}.$$

More generally,

$$x^{-n} + y^{-n} = \frac{1}{x^n} + \frac{1}{y^n} = \frac{x^n + y^n}{(xy)^n},$$

hence if we know how to express $x^n + y^n$, for a positive n, in terms of $x + y$ and xy, then we also know how to express $x^{-n} + y^{-n}$.

EXAMPLE. Find all the complex solutions of the following (symmetric) system:

$$\begin{cases} \dfrac{1}{x} + \dfrac{1}{y} = 1 \\ x + y = 2 \end{cases}$$

After rewriting $1/x + 1/y$ as $(x + y)/(xy)$ in the first equation, multiplying both sides by xy, and substituting into it the value of $x + y$ given by the second equation, we find

$$\begin{cases} xy = 2 \\ x + y = 2 \end{cases}$$

Because according to the first equation xy is nonzero, we did not introduce any more solutions when we multiplied by xy, and so this system is equivalent to the original system. Solving it as usual we find the solutions

$$(x, y) = (1 + i, 1 - i),\ (1 - i, 1 + i).$$

EXAMPLE. Find all the complex solutions of the following symmetric system:

$$\begin{cases} x + y + \dfrac{1}{x} + \dfrac{1}{y} = \dfrac{1}{2} \\ x^2 + y^2 + xy = 3 \end{cases}$$

After multiplying the first equation by xy and expressing everything in terms of the elementary symmetric polynomials $x+y$ and xy, we can write the system in the equivalent form:

$$\begin{cases} 2(x + y)xy + 2(x + y) = xy \\ (x + y)^2 - xy = 3 \end{cases}$$

Note that this is a system of degree $3 \cdot 2 = 6$, because the first equation has degree 3 (the 'combined' degree in x and y, since there is a term x^2y, for example). Obtaining xy from the second equation and then substituting into the first equation we get

$$\begin{cases} 2(x + y)^3 - 4(x + y) = (x + y)^2 - 3 \\ xy = (x + y)^2 - 3 \end{cases}$$

Now the first equation contains only $x + y$, so after setting $z = x + y$ the first equation becomes $2z^3 - z^2 - 4z + 3 = 0$. Using the Rational Root Test it is not hard to find that this polynomial has roots 1, then 1 again, and then $-3/2$ (so the left-hand side of the equation factorises as $2z^3 - z^2 - 4z + 3 = (z - 1)^2(2z + 3)$, with 1 being a double root).

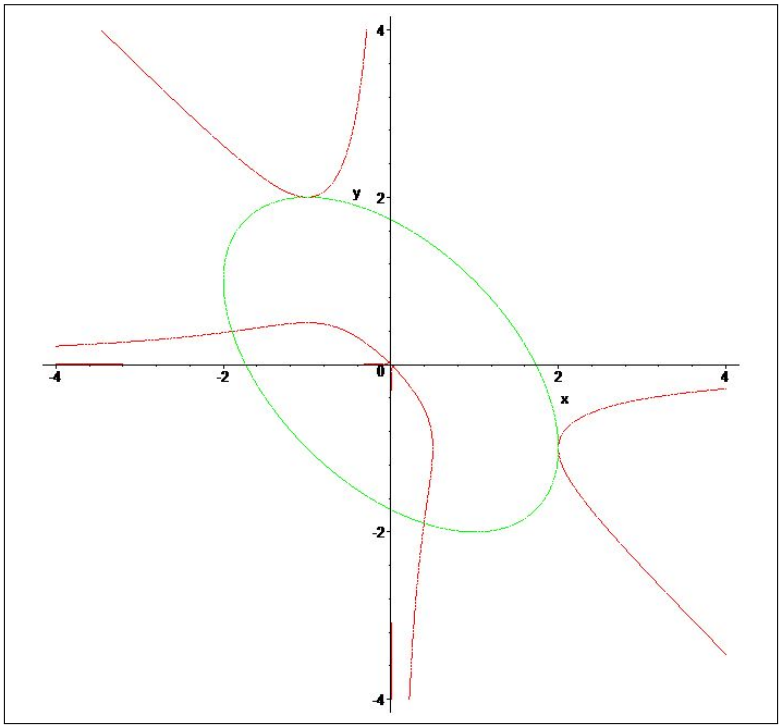
For each of those values of $z = x + y$ one can use the other equation of the system to compute $xy = z^2 - 3$, and so the system is equivalent to

$$\begin{cases} x + y = 1 \\ xy = -2 \end{cases} \quad \text{or} \quad \begin{cases} x + y = -3/2 \\ xy = -3/4 \end{cases}$$

(where each root of the first system should really be counted twice). Solving these two systems as we learned earlier we find altogether four different solutions of the system in the complex numbers, and all four are actually real:

$$(x, y) = (2, -1),\ (-1, 2),\ \left(\frac{-3 + \sqrt{21}}{2}, \frac{-3 - \sqrt{21}}{2}\right),\ \left(\frac{-3 + \sqrt{21}}{2}, \frac{-3 + \sqrt{21}}{2}\right).$$

The first two should actually be counted as *double solutions,* as they came from a double root of the cubic equation, and counting that way we have actually found six solutions of our system of degree six. In the following graph the two equations of our system are represented by the red curve and the green curve, respectively, and we see that the double roots manifest themselves as points where the two curve intersect with the same tangent.



From now on we make a small notational change, using α and β in place of x and y, so we can use x again (rather than z as above) as the indeterminate of our polynomial

$$x^2 - sx + p = (x - \alpha)(x - \beta).$$

Another application of the elementary symmetric polynomials is that they allow us to compute symmetric expressions of the roots of a polynomial (quadratic for now) in terms of the coefficients of the polynomial, without actually computing the roots.

EXAMPLE. Compute $\alpha^2+\beta^2$, $\alpha^3+\beta^3$, and $\alpha^{-2}+\beta^{-2}$, where α and β are the roots of the polynomial x^2-5x+3. A direct approach based on finding expressions for α and β first, which are $(5\pm\sqrt{13})/2$, would involve complicated calculations with radicals, which would eventually simplify and give rational numbers as final answers (actually, integers in this case). It is much better to use the fact that $\alpha+\beta=5$ and $\alpha\beta=3$, whence

$$\alpha^2+\beta^2=(\alpha+\beta)^2-2\alpha\beta=25-2\cdot 3=19,$$

$$\alpha^3+\beta^3=(\alpha+\beta)^3-3\alpha\beta(\alpha+\beta)=125-3\cdot 3\cdot 5=80,$$

$$\alpha^{-2}+\beta^{-2}=\frac{\alpha^2+\beta^2}{(\alpha\beta)^2}=\frac{(\alpha+\beta)^2-2\alpha\beta}{(\alpha\beta)^2}=\frac{5^2-2\cdot 3}{3^2}=\frac{19}{9}.$$

This last one could also be found by looking at the reciprocal polynomial $3x^2-5x+1$, whose roots are $1/\alpha$, $1/\beta$, $1/\gamma$:

$$\frac{1}{\alpha^2}+\frac{1}{\beta^2}=\left(\frac{1}{\alpha}+\frac{1}{\beta}\right)^2-2\frac{1}{\alpha}\frac{1}{\beta}=\left(\frac{5}{3}\right)^2-2\cdot\frac{1}{3}=\frac{19}{9}.$$

33. (Optional) Expressing a sum of two equal powers in terms of symmetric polynomials

A systematic and instructive way of expressing $\alpha^n+\beta^n$ in terms of $\alpha+\beta=s$ and $\alpha\beta=p$ is as follows. We start with the fundamental equations

$$\alpha^2-s\alpha+p=0 \quad \text{and} \quad \beta^2-s\beta+p=0.$$

which we can rewrite in the equivalent form

$$\alpha^2=s\alpha-p \quad \text{and} \quad \beta^2=s\beta-p.$$

Adding them together we obtain

$$\alpha^2+\beta^2=s(\alpha+\beta)-2p=s^2-2p.$$

If instead of adding the two equations together we first multiply them by α and β, respectively,

$$\alpha^3=s\alpha^2-p\alpha \quad \text{and} \quad \beta^3=s\beta^2-p\beta,$$

and then add them together, we find

$$\alpha^3+\beta^3=s(\alpha^2+\beta^2)-p(\alpha+\beta)=s(s^2-2p)-ps=s^3-3sp.$$

If, instead, we multiply the resulting two equations again by α and β, respectively, and then add them together, we find

$$\alpha^4+\beta^4=s(\alpha^3+\beta^3)-p(\alpha^2+\beta^2)=s(s^3-3sp)-p(s^2-2p)=s^3-4s^2p+2p^2,$$

and so on.

We can also state what we have found as follows. If we set $c_n = \alpha^n + \beta^n$, the sequence of numbers c_n satisfies the (quadratic) *linear recurrence relation* [15]

$$c_n = s \cdot c_{n-1} - p \cdot c_{n-2},$$

which may also write as $c_n - sc_{n-1} + pc_{n-2} = 0$ if we prefer. (Note that the coefficients are the same as those of our polynomial $x^2 - sx + 1$.) The whole sequence is then completely (and explicitly) determined by this linear recurrence relation together with the *initial conditions*

$$c_1 = \alpha + \beta = s, \quad \text{and} \quad c_2 = \alpha^2 + \beta^2 = s^2 - 2p,$$

or, even better,

$$c_0 = \alpha^0 + \beta^0 = 1 + 1 = 2, \quad \text{and} \quad c_1 = \alpha + \beta = s.$$

The relation can also be used backwards, to compute sums $\alpha^n + \beta^n$ for negative n (as long as $\alpha\beta \neq 0$).

EXAMPLE. Let α and β be the complex roots of $x^2 + x + 1$. Hence $\alpha + \beta = -1$ and $\alpha\beta = 1$. Proceeding as we have seen above we have

$$\alpha^2 = -\alpha - 1 \quad \text{and} \quad \beta^2 = -\beta - 1.$$

Adding them together we obtain

$$\alpha^2 + \beta^2 = -\alpha - \beta - 2 = -(-1) - 2 = -1.$$

If instead of adding the two equations together we first multiply them by α and β, respectively,

$$\alpha^3 = -\alpha^2 - \alpha \quad \text{and} \quad \beta^3 = -\beta^2 - \beta,$$

and then add them together, we find

$$\alpha^3 + \beta^3 = -(\alpha^2 + \beta^2) - (\alpha + \beta) = -(-1) - (-1) = 2.$$

If, instead, we multiply the two equations again by α and β, respectively, and then add them together, we find

$$\alpha^4 + \beta^4 = -(\alpha^3 + \beta^3) - (\alpha^2 + \beta^2) = -2 - (-1) = -1,$$

and so on. Continuing this way we will find

$$\alpha^5 + \beta^5 = -(\alpha^4 + \beta^4) - (\alpha^3 + \beta^3) = -(-1) - 2 = -1,$$

and

$$\alpha^6 + \beta^6 = -(\alpha^5 + \beta^5) - (\alpha^4 + \beta^4) = -(-1) - (-1) = 2,$$

[15] This is a sort of discrete version of a linear differential equation of the second order, such as $y'' + ay' + b = 0$, and a similar theory can be developed.

Hence $\alpha^k + \beta^k$, for $k = 1, \ldots, 6$, takes the values -1, -1, 2, -1, -1, 2. We may suspect that this would continue periodically, and this is in fact correct.

One way to see that if we set $c_n = \alpha^n + \beta^n$ as done earlier, the sequence of numbers c_n satisfies the (quadratic) linear recurrence relation

$$c_n = -c_{n-1} - c_{n-2},$$

with the initial values

$$c_1 = \alpha + \beta = -1, \quad \text{and} \quad c_2 = \alpha^2 + \beta^2 = -1.$$

We may use the recurrence to compute c_3, c_4, and c_5. At this point we see that $c_4 = c_1 = -1$ and $c_5 = c_2 = -1$, and because each term of the sequence only depends on the previous two we may conclude that the sequence repeats periodically, every three steps.

Another explanation is that our polynomial $x^2 + x + 1$ is a very special polynomial: because $x^2 + x + 1 = (x^3 - 1)/(x - 1)$, its roots $\alpha = (-1 + i\sqrt{3})/2$ and $\beta = (-1 - i\sqrt{3})/2$ satisfy $\alpha^3 = 1$ and $\beta^3 = 1$. (They are the *primitive cubic roots of* 1, and $x^2 + x + 1$ is a *cyclotomic polynomial*.) Also, $\alpha^2 = -\alpha - 1 = \beta$. This explains why the value of $\alpha^k + \beta^k$ repeats periodically every three steps: it does so because the (complex) value of each term, α^k and β^k, repeats periodically every three steps.

34. Symmetric functions of the roots of a cubic polynomial

What we have seen about symmetric functions of the roots of quadratic polynomials generalizes nicely to polynomials of higher degree. We start with the case of a cubic polynomial. After dividing by the leading coefficients we may always assume the polynomial to be monic, and we conveniently write it in the form $x^3 - sx^2 + rx - p$, with alternating signs. If the polynomial factorises as the product of three linear factors over some field we will have

$$\begin{aligned} x^3 - sx^2 + rx - p &= (x - \alpha)(x - \beta)(x - \gamma) \\ &= x^3 - (\alpha + \beta + \gamma)x^2 + (\alpha\beta + \alpha\gamma + \beta\gamma)x - \alpha\beta\gamma, \end{aligned}$$

and so

$$\begin{aligned} \alpha + \beta + \gamma &= s, \\ \alpha\beta + \alpha\gamma + \beta\gamma &= r, \\ \alpha\beta\gamma &= p. \end{aligned}$$

Those expressions at the left-hand sides (hence the sum of the three roots, a new expression in the second equation, and the product of the three roots) are the *elementary symmetric polynomials* in α, β, γ, when those are viewed as indeterminates. More generally, a polynomial $f(\alpha, \beta, \gamma)$ in three (independent) indeterminates α, β, γ is called

symmetric if it is unchanged after *permuting* (that is, swapping around, rearranging) the three indeterminates, in any of the six possible ways:

$$f(\alpha,\beta,\gamma) = f(\beta,\alpha,\gamma) = f(\alpha,\gamma,\beta) = f(\gamma,\beta,\alpha) = f(\beta,\gamma,\alpha) = f(\gamma,\alpha,\beta).$$

In order to verify that a polynomial is symmetric it is actually sufficient to check that

$$f(\alpha,\beta,\gamma) = f(\beta,\alpha,\gamma) = f(\alpha,\gamma,\beta)$$

(interchanging the first two indeterminates, and interchanging the last two), because the remaining permutations of α, β, and γ, can be realised by appropriately repeating those two simple exchanges (called *transpositions*) in some order. As in the quadratic case one can prove that arbitrary symmetric polynomials can always be expressed in terms of the elementary ones.

THEOREM 41. *Every symmetric polynomial $f(\alpha,\beta,\gamma)$ (with coefficients in any field F) can be expressed as a polynomial in the elementary symmetric polynomials $e_1(\alpha,\beta,\gamma) = \alpha+\beta+\gamma$, $e_2(\alpha,\beta,\gamma) = \alpha\beta+\alpha\gamma+\beta\gamma$, and $e_3(\alpha,\beta,\gamma) = \alpha\beta\gamma$.*

Hence if $f(\alpha,\beta,\gamma)$ is a symmetric polynomial in α, β, and γ, then

$$f(\alpha,\beta,\gamma) = g(\alpha+\beta+\gamma, \alpha\beta+\alpha\gamma+\beta\gamma, \alpha\beta\gamma),$$

for some polynomial $g(s,r,p)$ in three indeterminates s, r, and p. As in the quadratic case, more is true: if $f(\alpha,\beta,\gamma)$ has integer coefficients, then $g(s,r,p)$ has integer coefficients as well. For example, we have

$$\alpha^2+\beta^2+\gamma^2 = (\alpha+\beta+\gamma)^2 - 2(\alpha\beta+\alpha\gamma+\beta\gamma) = s^2 - 2r.$$

EXAMPLE. Suppose we want to express $\alpha^2\beta+\alpha^2\gamma+\beta^2\gamma+\alpha\beta^2+\alpha\gamma^2+\beta\gamma^2$ in terms of the elementary symmetric polynomials in α,β,γ. First of all, note that this is actually a symmetric polynomial, so Theorem 41 really applies. In fact, if we take one of the terms, say $\alpha^2\beta$, then by applying to it all permutations of α,β,γ we obtain precisely all terms of the sum (and each exactly once in this case). Hence according to Theorem 41 it must be possible to express this polynomial as a polynomial in the elementary symmetric polynomials $s = \alpha+\beta+\gamma$, $r = \alpha\beta+\alpha\gamma+\beta\gamma$, $p = \alpha\beta\gamma$.

Because $\alpha^2\beta$ can be written as the product of $\alpha\beta$ (which is a term of r) and α (which is a term of s), this suggests considering the product rs:

$$\begin{aligned}(\alpha\beta+\alpha\gamma+\beta\gamma)(\alpha+\beta+\gamma) = {}& \alpha^2\beta+\alpha^2\gamma+\alpha\beta\gamma \\ & +\alpha\beta^2+\alpha\beta\gamma+\beta^2\gamma \\ & +\alpha\beta\gamma+\alpha\gamma^2+\beta\gamma^2.\end{aligned}$$

Hence we conclude that

$$\alpha^2\beta+\alpha^2\gamma+\beta^2\gamma+\alpha\beta^2+\alpha\gamma^2+\beta\gamma^2 = (\alpha\beta+\alpha\gamma+\beta\gamma)(\alpha+\beta+\gamma) - 3\alpha\beta\gamma = rs - 3p.$$

EXAMPLE. Let α, β and γ be the complex roots of the polynomial $x^3 + x^2 - 2x - 5$. Compute $\alpha^2 + \beta^2 + \gamma^2$ and $\alpha^{-2} + \beta^{-2} + \gamma^{-2}$.

We express the desired quantities in terms of

$$\alpha + \beta + \gamma = -1, \quad \alpha\beta + \alpha\gamma + \beta\gamma = -2, \quad \text{and} \quad \alpha\beta\gamma = 5.$$

For the former quantity we have

$$\alpha^2 + \beta^2 + \gamma^2 = (\alpha + \beta + \gamma)^2 - 2(\alpha\beta + \alpha\gamma + \beta\gamma) = (-1)^2 - 2 \cdot (-2) = 5.$$

For the latter quantity, where negative powers of the roots appear, we consider the reciprocal polynomial $-5x^3 - 2x^2 + x + 1$, whose roots are α^{-1}, β^{-1}, and γ^{-1}. From the coefficients of the reciprocal polynomial we see that

$$\frac{1}{\alpha} + \frac{1}{\beta} + \frac{1}{\gamma} = -\frac{2}{5}, \quad \frac{1}{\alpha\beta} + \frac{1}{\alpha\gamma} + \frac{1}{\beta\gamma} = -\frac{1}{5}, \quad \text{and} \quad \frac{1}{\alpha\beta\gamma} = \frac{1}{5}.$$

Consequently, we have

$$\frac{1}{\alpha^2} + \frac{1}{\beta^2} + \frac{1}{\gamma^2} = \left(\frac{1}{\alpha} + \frac{1}{\beta} + \frac{1}{\gamma}\right)^2 - 2\left(\frac{1}{\alpha\beta} + \frac{1}{\alpha\gamma} + \frac{1}{\beta\gamma}\right) = \left(-\frac{2}{5}\right)^2 - 2 \cdot \left(-\frac{1}{5}\right) = \frac{14}{25}.$$

Note that one may also compute $\alpha^{-2} + \beta^{-2} + \gamma^{-2}$ without passing through the reciprocal polynomial, by directly expressing it in terms of the elementary symmetric polynomials:

$$\begin{aligned} \frac{1}{\alpha^2} + \frac{1}{\beta^2} + \frac{1}{\gamma^2} &= \frac{\alpha^2\beta^2 + \alpha^2\gamma^2 + \beta^2\gamma^2}{(\alpha\beta\gamma)^2} \\ &= \frac{(\alpha\beta + \alpha\gamma + \beta\gamma)^2 - 2(\alpha\beta\gamma)(\alpha + \beta + \gamma)}{(\alpha\beta\gamma)^2} \\ &= \frac{(-2)^2 - 2 \cdot 5 \cdot (-1)}{5^2} = \frac{14}{25}. \end{aligned}$$

However, this procedure appears a little more complicated than using the reciprocal polynomial (despite being equivalent to that).

35. (Optional) Symmetric polynomials in many indeterminates

Symmetric polynomials can be defined similarly for an arbitrary number n of indeterminates. The general definition of elementary symmetric polynomials, and the fundamental theorem of symmetric polynomials, are then as follows.

DEFINITION 42. If $x_1, \ldots, x_n$ and x are independent indeterminates, then the *elementary symmetric polynomials* $e_k = e_k(x_1, \ldots, x_n)$, for $k = 1, \ldots, n$, are defined by the identity

$$(x - x_1)(x - x_2) \cdots (x - x_n) = x^n - e_1 x^{n-1} + e_2 x^{n-2} - e_3 x^{n-3} + \cdots + (-1)^n e_n.$$

Hence e_k is the coefficient of x^{n-k} in the polynomial $(x-x_1)(x-x_2)\cdots(x-x_n)$ (once this is expanded into powers of x, its standard form). One can see that

$$e_k(x_1,\ldots,x_n) = \sum_{1\le j_1<j_2<\cdots<j_k\le n} x_{j_1}x_{j_2}\cdots x_{j_k}.$$

In particular, e_k is a *homogeneous* polynomial of degree k, and $e_1(x_1,\ldots,x_n) = x_1 + \cdots + x_n$, and $e_n(x_1,\ldots,x_n) = x_1\cdots x_n$. (A *homogeneous polynomial* of degree k is a polynomial (in several indeterminates) where each term alone has the same degree k.) More generally, according to the above formula $e_k(x_1,\ldots,x_n)$ is the sum of all distinct products of k distinct indeterminates taken from $x_1,\ldots,x_n$. The number of such distinct products equals the binomial coefficient $\binom{n}{k}$ (see one of the next sections).

THEOREM 43 (The fundamental theorem of symmetric polynomials). *Every symmetric polynomial $f(x_1,\ldots,x_n)$ with integer coefficients can be expressed as a polynomial with integer coefficients in the elementary symmetric polynomials $e_k(x_1,\ldots,x_n)$, with $k = 1,\ldots,n$.*