

Re: decomposition of polynomials

Source: <http://sci.tech-archive.net/Archive/sci.math/2006-03/msg02672.html>

- *From:* rusin@xxxxxxxxxxxxxxxxxxxxxxxx (Dave Rusin)
 - *Date:* 15 Mar 2006 17:18:41 GMT
-

In article <slrne1g080.36i.a282244@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>, Helmut Richter <hhr-m@xxxxxx> wrote:

Let f be a polynomial over Z . It is a well-known task with smart known solutions to find polynomials g and h over Z such that $f(x)=g(x)h(x)$ if such g and h exist. But I have never seen solutions to the problem to find polynomials g and h over Z such that $f(x)=g(h(x))$ if such g and h exist.

That's a big "if", in the following sense.

Suppose I hand you a polynomial of degree 6. I do so by giving you 7 integers, or equivalently 6 rational numbers -- you might as well assume that f , g , and h are monic polynomials in $Q[x]$ because you can move around the constant terms from factor to factor. Now, for you to factor f as $g h$, you have to come up with, say, a quadratic factor and a quartic factor, or two cubics, etc. In each case, you need to come up with a total of 6 rational numbers -- the coefficients of g and h , partitioned according to the degrees you think g and h have. You can if you like treat this as a set of 6 equations (one for each coefficient in f) in 6 unknowns (one for each coefficient in g and h). As you may know, this typically has a finite solution set over the complex numbers, which of course makes perfect sense here -- there is a unique (up to order) factorization of f into monic linear factors over C , and those factors can be grouped in just a few ways to make g and h .

Now let's play the game again but trying to "factor" f as $g \circ h$. (Again we start with f of degree 6.) The key difference now is that the degree of $g \circ h$ is the product of the degrees of g and h . So we have fewer possible pairs of degrees to consider, and they are smaller degrees. You might consider, for example, the possibility that g is a quadratic and h is a cubic. Well, again you can write out the equations which state that $f = g \circ h$ and compare coefficients. You again have 6 equations, one for each coefficient in f , but now only 5 unknown coefficients in g and h . That's very different from the previous paragraph -- 6 equations in 5

Re: decomposition of polynomials

unknowns are likely to be contradictory, meaning that there are no solutions at all. (It's actually a little worse than this -- the equations are also a little redundant in the sense that if one factorization is possible then there are multiple factorizations since we can compose g and h with linear functions; so after solving just 4 of the equations, you'll already run out of variables.) In this way we conclude that most polynomials of any fixed degree are likely to be irreducible -- over any field, not just Q -- in the sense that $f = g \circ h \implies \deg(g)=1$ or $\deg(h)=1$.

(A sextic $x^6 + q_5 x^5 + \dots$ is decomposable as cubic o quadratic iff $-q_5^5 + 3q_5^3 q_4 + 81q_1 - 27q_2 q_5 = -27q_3 - 5q_5^3 + 18q_5 q_4 = 0$ and it's decomposable the other way iff $5q_5^4 - 24q_5^2 q_4 + 16q_4^2 - 64q_2 + 32q_5 q_3 = -64q_1 - q_5^5 + 8q_5^3 q_4 - 16q_5 q_4^2 - 8q_3 q_5^2 + 32q_3 q_4 = 0$.)

More high-falutin' responses are also possible. Look for "polynomial decomposition", "primitive Galois group", and widen your search to the more general problem of finding g, h with $f \mid (g \circ h)$ instead of $f = g \circ h$.

If you'd like to try your hand at this, consider the following interesting example proposed when this question was asked in July 2001: $x^6 + 235x^5 + 1430x^4 + 1695x^3 + 270x^2 - 229x + 1$

See also these news articles by Bill Dubuque, which also give citations to the literature:

<y8zn06nl4kr.fsf@xxxxxxxxxxxxxxxxxxxx>
<y8zy8yy9500.fsf@xxxxxxxxxxxxxxxxxxxx>

dave

.