

# Re: decomposition of polynomials

---

*Source:* <http://sci.tech--archive.net/Archive/sci.math/2006-03/msg02800.html>

---

- *From:* [rusin@xxxxxxxxxxxxxxxxxxxxxxxx](mailto:rusin@xxxxxxxxxxxxxxxxxxxxxxxx) (Dave Rusin)
  - *Date:* 16 Mar 2006 03:56:12 GMT
- 

In article <Iw72Fz.CL2@xxxxxx>, Peter L. Montgomery <Peter-Lawrence.Montgomery@xxxxxx> wrote:

In article <dv9i9h\$tdu\$1@xxxxxxxxxxxxxxxxxxxx> rusin@xxxxxxxxxxxxxxxxxxxxxxxx (Dave Rusin) writes:

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  $f | (g \circ h)$  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:  
 $x^6+235x^5+1430x^4+1695x^3+270x^2-229x+1$

If we let  $\alpha$  be a root of  $y^3 - y^2 - 2y + 1$ , then the sextic splits over the field  $\mathbb{Q}(\alpha, \sqrt{21})$ .

Ah, good -- thanks for doing the hard work (not sure I remember how you would do that!). Allow me to use this to illustrate my prior remarks.

Peter notes that the intermediate quadratic subfield in the splitting field for this polynomial is  $K = \mathbb{Q}(\sqrt{21})$ . Sure enough, the polynomial factors into two cubics over  $K$ . They are  $p \pm \sqrt{21} q$  where  $p(x) = x^3+235/2x^2+229/2x-1$  and  $q(x) = 49/2x(x+1)$ .

So now if  $x$  is any root of  $f$ , it makes the product of these two sums vanish, so  $p(x)$  is either  $\sqrt{21} q(x)$  or its negative, so that  $p(x)^2 - 21 q(x)^2 = 0$ , i.e.  $(p(x)/q(x))^2 - 21 = 0$ .

If it weren't for that darn  $q(x)$  in there, we would conclude that the sextic is exactly the composite  $f = g \circ p$  where  $g(x) = x^2 - 21$ , because that equation relates two monic sextics with equal roots!

We can do something with the  $q$  there as well, but we don't quite get a decomposition of  $f$ . Note that if as above  $x$  is any of the

## Re: decomposition of polynomials

roots of  $f$ , then  $1/q(x)$  lies in the field  $Q(x)$  generated by  $x$ , but this field is the same as the polynomial ring  $Q[x]$ , so that we may write  $1/q$  as a polynomial in  $x$ . In this particular case that's not too hard: since  $f(x)=0$ ,  $1 = x * ((1-f(x))/x)$ , and that second factor is a polynomial in  $x$ , so we have a polynomial inverse for  $x$  itself; you can do likewise to get an inverse for  $y=x+1$  (first rewrite  $f$  as a polynomial in  $y$ ). Multiply these two inverses together to get an inverse for  $q(x)$  (up to a constant). Don't forget that you can throw away any multiple of  $f(x)$ . Likewise we can then multiply out  $p(x) * 1/q(x)$  and reduce mod  $f$  to get a small polynomial which equals  $p(x)/q(x)$  whenever  $x$  is a root of  $f(x)$ . Carrying out this prescription I get this to be 
$$h(x) = (938x^4 + 5252x^3 + 4x^5 + 4388x^2 + 84x - 225)/49$$

Now we make the same observation as I made above when pretending there was no  $q(x)$ :  $h(x)^2 - 21$  vanishes whenever  $x$  is a root of  $f$ ; except that now  $h^2 - 21$  is of higher degree than  $f$ , so we don't get equality, we get divisibility. Sure enough, you can calculate that if  $h$  is as above and  $g(x) = x^2 - 21$  then  $f \mid g \circ h$  since  $g \circ h = 4/2401 * (4x^4 + 936x^3 + 4785x^2 + 2229x + 51) * f(x)$ .

You can reverse the logic of all this: if you have somehow found two polynomials  $g$  and  $h$  with  $f \mid g \circ h$ , then any root  $x$  of  $f$  would make  $g(h(x))=0$ , i.e.  $h(x)$  is one of the roots  $r_i$  of  $g$ . So the field extension can be done in two steps, first up to the splitting field of  $g$ , then adjoining the solutions to each equation  $h(x) - r_i$ .

This particular sextic happens to have cyclic galois group, so you can view the splitting field either as a cubic extension of a quadratic extension, as I did above, or a quadratic extension of a cubic extension.

Someone suggested using the Chain Rule to decide whether  $f$  is a composite, which is clever but I don't see any way to use that for the broader problem of finding composites which are multiples of  $f$ .

dave

.