Re: irredicuble polynomials

Source: http://sci.tech−archive.net/Archive/sci.math/2005−11/msg03910.html

- *From*: Gerry Myerson <gerry@xxxxxxxxxxxxxxxxxxxxxxxxxx>
- *Date*: Fri, 25 Nov 2005 01:05:48 GMT

In article
<6753587.1132828228028.JavaMail.jakarta@xxxxxxxxxxxxxxxxxxxxxx>,
eugene <jane1806@xxxxxxx> wrote:

> I am stuck with the proof of the following fact:
>
> Prove that for every prime power q, one has that for all n there exists and
> irreducible polynomial of degree n.
>
> At the begginning the proof suggest the following identity
>
> \product_{k=1^\infty} (1/(1−x^k)^I(k))=\sum_{n=1}^{\infty}q^n x^n
>
> where I(k)−the number of irredicuble polynomials of degree k(we are working
> in our field F_q).
> Could you please explain me this identity.
> Thanks in advance

I hate to harp on typos, but the word you are looking for
is "irreducible."

Anyway, the right side of the identity, the coefficient of x^n
is the number of monic polynomials of degree n, right? Now, each
such polynomial has a unique expression as a product of (monic)
irreducible polynomials, right?

On the left side,

1 / (1 − x^k)^I(k) = (1 + x^k + x^(2k) + ...)^I(k)

Now all you have to do is identify each term in the expansion of
product_{k = 1 to infinity} (1 + x^k + x^(2k) + ...)^I(k)
with a factorization into irreducibles. Can you see it?

−−
Gerry Myerson (gerry@xxxxxxxxxxxxxxx) (i −> u for email)
.

- ***References***:
  - ***irredicuble polynomials***
    - ◊ *From:* eugene

- Prev by Date: ***Re: Group actions***
- Next by Date: ***AX+BY+CXY+D=A'X'+B'Y'+C'X'Y'+D'***
- Previous by thread: ***irredicuble polynomials***
- Next by thread: ***sparse matrix inversion algorithm***
- Index(es):
  - ***Date***
  - ***Thread***