Field Review 3

April 14, 2018

40

b)

proposition 1. *The polynomial $x^{p^n} - x$ is precisely the product of all the distinct irreducible polynomials in $F_p[x]$ of degree d where d runs through all divisors of n.*

Proof. Check the notes □

With this proposition, we can get the number of number of irreducible polynomials of degree n. Check the book in page 587-588

So here we have

$$\psi(6) = \frac{1}{6}[\mu(1)p^6 + \mu(2)p^3 + \mu(3)p^2 + \mu(6)p] \tag{1}$$

$$= \frac{1}{6}[p^6 - p^3 - p^2 + p] \tag{2}$$

$\Rightarrow \# \, of \, \beta = 6\psi(6) = p^6 - p^3 - p^2 + p$

Even though I believe this is the correct answer, if we look back to Q39, we should get the conclusion that the number of such $\beta = p^n - p^{n-1}$. Which is less than this, what's wrong with my previous proof?

41

Let $f(x) = x^{3470} - 1$, Suppose f(x) splits in Field F_p^n

$$\Rightarrow f(x)|x^{p^n} - x \tag{3}$$

$$\tag{4}$$

if we can find the smallest n such that $f(x)|x^{p^n} - x$ then we can just say F_{p^n} is the splitting field of f(x) since in finite fields, fields with same degree are isomorphic. Then we can see that n = 4.