irreducible polynomials over finite field

Canonical name	IrreduciblePolynomialsOverFiniteField
Date of creation	2013-03-22 17:43:14
Last modified on	2013-03-22 17:43:14
Owner	pahio (2872)
Last modified by	pahio (2872)
Numerical id	7
Author	pahio (2872)
Entry type	Theorem
Classification	msc 12E20
Classification	msc 11T99
Related topic	FiniteField

Theorem. Over a finite field F, there exist irreducible polynomials of any degree.

Proof. Let n be a positive integer, p be the characteristic of F, $\mathbb{F}_p$ be the prime subfield, and p^r be the `http://planetmath.org/FiniteField`order of the field F. Since p^r-1 is a divisor of $p^{rn}-1$, the zeros of the polynomial $X^{p^r}-X$ form in $G := \mathbb{F}_{p^{rn}}$ a subfield isomorphic to F. Thus, one can regard F as a subfield of G. Because

$$[G:F] = \frac{[G:\mathbb{F}_p]}{[F:\mathbb{F}_p]} = \frac{rn}{r} = n,$$

the minimal polynomial of a primitive element of the field extension G/F is an irreducible polynomial of degree n in the ring $F[X]$.