Some slides for 20th Lecture, Algebra 2

Diego Ruano

Department of Mathematical Sciences
Aalborg University
Denmark

18-04-2013

Lemma 4.8.1

Let F be a finite field. Then $|F| = p^n$, where p is a prime number, $n \geq 1$ and there exists and irreducible polynomial $f \in \mathbb{F}_p[X]$ of degree n such that

$$F \cong \mathbb{F}_p[X]/\langle f \rangle$$

Theorem 4.8.2

There exists a unique finite field with p^n elements, where p is a prime number and $n \geq 1$. More precisely, we have

1. There exists an irreducible polynomial in $\mathbb{F}_p[X]$ of degree n.
2. Suppose that F and F' are finite fields with p^n elements. Then there exists a ring isomorphism $F \cong F'$.

Lemma 4.8.3

Let τ, d and n be natural numbers, where $\tau > 1$. Then $\tau^d - 1$ divides $\tau^n - 1$ if and only if d divides n.

Existence of finite fields

Theorem 4.8.5

There exists an irreducible polynomial in $\mathbb{F}_p[X]$ of degree $n \geq 1$. More precisely, if f is an irreducible polynomial dividing Φ_{p^n-1} in $\mathbb{F}_p[X]$ then $\deg(f) = n$.

Uniqueness of finite fields