Nepal Algebra Project(NAP)
Central Department of Mathematics
Tribhuvan University,Kirtipur, Kathmandu,Nepal
Fields and Galois Theory- Short Note of Module 4 - Lecture 1
Course Instructor: René Schoof and Laura Geatti

NAP: Module -4, Lecture -1, 16:30 – 18:45, Monday, July 3, 2017

Finite fields

Construction of finite fields:

For any prime p one has $\mathbf{F}_p[x]/(f)$, with f irreducible in $\mathbf{F}_p[x]$.

Proposition 1.

(a) the cardinality of a finite field $\mathbf{K}$ of characteristic p is $q = p^n$.

(b) $\mathbf{K}$ contains $\mathbf{F}_p$

(c) the additive group $(\mathbf{K}, +)$ is isomorphic to $(\mathbf{Z}/p\mathbf{Z} \times \ldots \times \mathbf{Z}/p\mathbf{Z}, +)$

(d) the multiplicative group $(\mathbf{K}^*, \cdot)$ of a finite field is cyclic.

Theorem 2. For every prime power $q = p^n$ there exists a field with q elements. It is of the form $\mathbf{F}[x]/(f)$ with f an irreducible polynomial in $\mathbf{F}_p[X]$ of degree n.

Theorem 3. Every finite field of q elements is a splitting field of $x^q - x$ over $\mathbf{F}_p$. Therefore all finite fields with q elements are isomorphic. Notation $\mathbf{F}_q$.

Examples. $\mathbf{F}_4$, $\mathbf{F}_5[\sqrt{2}]$, $\mathbf{F}_9 = \mathbf{F}_3[i] = \mathbf{F}_3[x]/(x^2+1) = \mathbf{F}_3[i+1]$

Theorem 4. $Aut(\mathbf{F}_q) = \langle \phi \rangle$, where ϕ denotes the Frobenius automorphism $\phi(x) = x^p$.