Nepal Algebra Project(NAP)
Central Department of Mathematics
Tribhuvan University,Kirtipur, Kathmandu,Nepal
Fields and Galois Theory- Short Note of Module 4 - Lecture 2
Course Instructor: René Schoof and Laura Geatti

NAP: Module -4, Lecture -2, 16:30 – 18:45, Tuesday, July 4, 2017

Finite fields

Subfields.

Lemma 1. Let p be a prime. Let $f \in \mathbf{F}_p[x]$ be an irreducible polynomial of degree n. Let α be a zero of f. Then

(a) $\alpha^{p^n} = \alpha$;
(b) n is the smallest positive integer for which (a) holds.

Proposition 2. Let $f \in \mathbf{F}_p[x]$ be an irreducible polynomial of degree n. Let α be a zero of f. Then

$$f(x) = (x-\alpha)(x-\alpha^p)\dots(x-\alpha^{p^{n-1}}).$$

Corollary 3. Every finite extension of a finite field is a Galois extension.

Theorem 4. $Aut(\mathbf{F}_{p^n})$ is a cyclic group isomorphic to $\mathbf{Z}/n\mathbf{Z}$, generated by the Frobenius automorphism ϕ.

Proposition 5.

(a) If $\mathbf{K}$ is a subfield of $\mathbf{F}_{p^n}$, then the cardinality of $\mathbf{K}$ is equal to p^d, for some divisor d of n.
(b) For every divisor d of n, there exists a unique subfield of cardinality p^d.

The Galois correspondence in the case of finite fields:
Fix p prime and the finite field $\mathbf{F}_{p^n}$.
$Aut(\mathbf{F}_{p^n}) = \langle\phi\rangle = Gal(\mathbf{F}_{p^n}/\mathbf{F}_p) \cong \mathbf{Z}/n\mathbf{Z}$.
For every d divisor of n, there is a unique subfield $\mathbf{F}_{p^d} \subset \mathbf{F}_{p^n}$.
For every d divisor of n, there is a unique subgroup G_d of $Gal(\mathbf{F}_{p^n}/\mathbf{F}_p)$ of index d, namely the subgroup generated by ϕ^d.
One has $\mathbf{F}_{p^d} = \{x \in \mathbf{F}_{p^n} \mid g(x) = x, \forall g \in G_d\}$.
Conversely $G_d = \{g \in Gal(\mathbf{F}_{p^n}/\mathbf{F}_p) \mid g(x) = x,\ \forall x \in \mathbf{F}_{p^d}\}$.
Example: $\mathbf{F}_{3^4}$.

Excercise 1.

(a) Find an irreducible polynomial f of degree 2 in $\mathbf{F}_3[x]$. Then $\mathbf{F}_9 = \mathbf{F}_3[x]/(f)$.
(b) Which elements of $\mathbf{F}_9$ are generators of its multiplicative group $\mathbf{F}_9^*$?
(c) Which elements of $\mathbf{F}_9$ have square roots in $\mathbf{F}_9$?
(d) Prove that the product of all elements of $\mathbf{F}_9^*$ is 2.
(e) Show that the additive group of $\mathbf{F}_9$ is not cyclic.

Excercise 2.

Draw the Hasse diagrams of the subfields of each $\mathbf{F}_{2^k}$ for $k = 1, .., 6$..