CIMPA School of Number Theory
in Cryptography and Its Applications
School of Science, Kathmandu University, Dhulikhel, Nepal
July 19th - July 31th, 2010

Finite fields

Michel Waldschmidt

Course 3: July 23, 2010

These notes are extracted from the full text, the pdf of which is available from the web site
http://www.math.jussieu.fr/~miw/

Gauss fields

A field with finitely many elements is also called a *Gauss Field*. For instance, given a prime number p, the quotient $\mathbf{Z}/p\mathbf{Z}$ is a Gauss field. Given two fields F and F' with p elements, p prime, there is a unique isomorphism $F \to F'$. Hence, we denote by $\mathbf{F}_p$ the unique field with p elements.

The characteristic of finite field F is a prime number p, hence, its prime field is $\mathbf{F}_p$. Moreover, F is a finite vector space over $\mathbf{F}_p$; if the dimension of this space is s, which means that F is a finite extension of $\mathbf{F}_p$ of degree $[F : \mathbf{F}_p] = s$, then F has p^s elements. Therefore, the number of elements of a finite field is always a power of a prime number p, and this prime number is the characteristic of F.

Gauss fields

The multiplicative group $F^\times$ of a field with q elements has order $q-1$, hence, $x^{q-1}=1$ for all x in $F^\times$, and $x^q = x$ for all x in F. Therefore, $F^\times$ is the set of roots of the polynomial $X^{q-1}-1$, while F is the set of roots of the polynomial $X^q - X$:

$$(1)\quad X^{q-1}-1 = \prod_{x\in F^\times}(X-x), \qquad X^q - X = \prod_{x\in F}(X-x).$$

Exercise 2.

Prove that if F is a finite field with q elements, then the polynomial $X^q - X + 1$ has no root in F. Deduce that F is not algebraically closed.

Subgroups of the multiplicative group of a field

Proposition 3.

Any finite subgroup of the multiplicative group of a field K is cyclic. If n is the order of G, then G is the set of roots of the polynomial $X^n - 1$ in K.

Proof.

Let K be a field and G a finite subgroup of $K^\times$ of order n and exponent e. By Lagrange's theorem, e divides n. Any x in G is a root of the polynomial $X^e - 1$. Since G has order n, we get n roots in the field K of this polynomial $X^e - 1$ of degree $e \le n$. Hence $e = n$. We conclude by using the fact that there exists in G an element of order e, hence, G is cyclic and is the set of roots of the polynomial $X^n - 1$ in K. □

Lemma 4

Lemma 4.
Let K be a field of characteristic p. For x and y in K, we have $(x+y)^p = x^p + y^p$.

Proof.
When p is a prime number and n an integer in the range $1 \le n < p$, the binomial coefficient

$$\binom{p}{n} = \frac{p!}{n!(p-n)!}$$

is divisible by p. □

Lemma 5: $f \in \mathbf{F}_q[X] \iff f(X^q) = f(X)^q$

We shall use repeatedly the following fact:

Lemma 5.
Let $\mathbf{F}_q$ be a finite field with q elements, F an extension of $\mathbf{F}_q$ and $f \in F[X]$ a polynomial with coefficients in F. Then f belongs to $\mathbf{F}_q[X]$ if and only if $f(X^q) = f(X)^q$.

Proof of $f \in \mathbf{F}_q[X] \iff f(X^q) = f(X)^q$

Proof of Lemma 5.
According to (1), for $a \in F$, the relation $a^q = a$ holds if and only if $a \in \mathbf{F}_q$. Since q is a power of the characteristic p of F, if we write

$$f(X) = a_0 + a_1 X + \cdots + a_n X^n,$$

then, by Lemma 4,

$$f(X)^p = a_0^p + a_1^p X^p + \cdots + a_n^p X^{np}$$

and by induction

$$f(X)^q = a_0^q + a_1^q X^q + \cdots + a_n^q X^{nq}.$$

Therefore, $f(X)^q = f(X^q)$ if and only if $a_i^q = a_i$ for all $i = 0, 1, \ldots, n$. □

Proposition 6

From Lemma 4, we deduce:

Proposition 6.
If F be a finite field of characteristic p, then

$$\begin{array}{rccc} \mathrm{Frob}_p : & F & \to & F \\ & x & \mapsto & x^p \end{array}$$

is an automorphism of F.

The Frobenius automorphism

Proof of proposition 6.

Indeed, this map is a morphism of fields since, by Lemma 4, for x and y in F,

$$\mathrm{Frob}_p(x+y) = \mathrm{Frob}_p(x) + \mathrm{Frob}_p(y)$$

and

$$\mathrm{Frob}_p(xy) = \mathrm{Frob}_p(x)\mathrm{Frob}_p(y).$$

It is injective since $x^p = 0$ implies $x = 0$. It is surjective because it is injective and F is finite. □

Frobenius

This automorphism of F is called the *Frobenius* of F over $\mathbf{F}_p$. It extends to an automorphism of the algebraic closure of F. If s is a non–negative integer, we denote by Frob_p^s or by Frob_{p^s} the iterated automorphism

$$\mathrm{Frob}_p^0 = 1, \quad \mathrm{Frob}_{p^s} = \mathrm{Frob}_{p^{s-1}} \circ \mathrm{Frob}_p \qquad (s \geq 1),$$

so that, for $x \in F$,

$$\mathrm{Frob}_p^0(x) = x, \ \mathrm{Frob}_p(x) = x^p, \ \mathrm{Frob}_{p^2}(x) = x^{p^2}, \dots,$$

$$\mathrm{Frob}_{p^s}(x) = x^{p^s} \quad (s \geq 0).$$

Frobenius

If F has p^s elements, then the automorphism $\mathrm{Frob}_p^s = \mathrm{Frob}_{p^s}$ of F is the identity.

If F is a finite field with q elements and K a finite extension of F, then Frob_q is a F–automorphism of K called the *Frobenius of K over F.*

Frobenius

Let F be a finite field of characteristic p with q elements. According to Proposition 3, the multiplicative group $F^\times$ of F is cyclic of order $q-1$. Let α be a generator of $F^\times$, that means an element of order $q-1$. For $1 \leq \ell < s$, we have $1 \leq p^\ell - 1 < p^s - 1 = q - 1$, hence, $\alpha^{p^\ell - 1} \neq 1$ and $\mathrm{Frob}_p^\ell(\alpha) \neq \alpha$. Therefore, Frob_p has order s in the group of automorphisms of F. It follows that the extension $F/\mathbf{F}_p$ is Galois, with Galois group the cyclic group of order s generated by Frob_p.

As a consequence, if F is a field with q elements and K a finite extension of F, then the extension K/F is Galois with Galois group the cyclic group generated by the Frobenius Frob_q of K over F.

Galois theory for finite fields

Theorem 7.

Let F be a finite field with q elements and K a finite extension of F of degree s. Then there is a bijection between the subfields E of K containing F and the divisors d of s.

$$\begin{array}{ccc} & K & \\ s/d & | & \\ & E & s \\ d & | & \\ & F & \end{array}$$

• *If E is a subfield of K containing F, then the number of elements in E is of the form q^d where d divides s.*
• *Conversely, if d divides s, then K has a unique subfield E with q^d elements, which is the fixed field by Frob_{p^d} and this field E contains F:*

$$E = \{\alpha \in K \; ; \; \mathrm{Frob}_{q^d}(\alpha) = \alpha\}.$$

When does $X^n - 1$ divides $X^m - 1$?

Exercise 8.

Let F be a field, m and n two positive integers, a and b two integers ≥ 2. Prove that the following conditions are equivalent.
(i) n divides m.
(ii) In $F[X]$, the polynomial $X^n - 1$ divides $X^m - 1$.
(iii) $a^n - 1$ divides $a^m - 1$.
(ii') In $F[X]$, the polynomial $X^{a^n} - X$ divides $X^{a^m} - X$.
(iii') $b^{a^n} - b$ divides $b^{a^m} - b$.
Hint *Denote r the remainder of the Euclidean division of m by n. Prove that $a^r - 1$ is the remainder of the Euclidean division of $a^m - 1$ by $a^n - 1$.* See also [3], Theorems 19.2, 19.3, 19.4.

Existence of finite fields with p^s elements

We now prove that for any prime number p and any integer $s \geq 1$, there exists a finite field with p^s elements.

Theorem 9.

Let p be a prime number and s a positive integer. Set $q = p^s$. Then there exists a field with q elements. Two finite fields with the same number of elements are isomorphic. If Ω is an algebraically closed field of characteristic p, then Ω contains one and only one subfield with q elements.

Proof of Theorem 9

Proof.
Let F be a splitting field over $\mathbf{F}_p$ of the polynomial $X^q - X$. Then F is the set of roots of this polynomial, hence, has q elements.
If F' is a field with q elements, then F' is the set of roots of the polynomial $X^q - X$, hence, F' is the splitting field of this polynomial over its prime field, and, therefore, is isomorphic to F.
If Ω is an algebraically closed field of characteristic p, then the unique subfield of Ω with q elements is the set of roots of the polynomial $X^q - X$.

□

Finite subfields of $\overline{\mathbf{F}}_p$

Fix an algebraic closure $\overline{\mathbf{F}}_p$ of $\mathbf{F}_p$. For each $s \geq 1$, denote by $\mathbf{F}_{p^s}$ the unique subfield of Ω with p^s elements. For n and m positive integers, we have the following equivalence:

(10) $$\mathbf{F}_{p^n} \subset \mathbf{F}_{p^m} \iff n \text{ divides } m.$$

If these conditions are satisfied, then $\mathbf{F}_{p^m}/\mathbf{F}_{p^n}$ is cyclic, with Galois group of order m/n generated by Frob_{p^n}.

Finite subfields of $\overline{\mathbf{F}}_p$ (continued)

Let $F \subset \overline{\mathbf{F}}_p$ be a finite field of characteristic p with q elements, and let x be an element in $\overline{\mathbf{F}}_p$. The conjugates of x over F are the roots in $\overline{\mathbf{F}}_p$ of the irreducible polynomial of x over F, and these are exactly the images of x by the iterated Frobenius Frob_{q^i}, $i \geq 0$.

Two fields with p^s elements are isomorphic (cf. Theorem 9), but if $s \geq 2$, there is no unicity of such an isomorphic, because the set of automorphisms of $\mathbf{F}_{p^s}$ has more than one element (indeed, it has s elements).

Remarks

- The additive group $(F, +)$ of a finite field F with q elements is cyclic, generated by 1, hence, is isomorphic to $\mathbf{Z}/q\mathbf{Z}$.
- The multiplicative group $(F^\times, \times)$ of a finite field F with q elements is cyclic, hence, is isomorphic to the additive group $\mathbf{Z}/(q-1)\mathbf{Z}$.
- A finite field F with q elements is isomorphic to the ring $\mathbf{Z}/q\mathbf{Z}$ if and only if q is a prime number (which is equivalent to saying that $\mathbf{Z}/q\mathbf{Z}$ has no zero divisor).

Simplest example of a finite field $\neq \mathbf{F}_p$

A field F with 4 elements has two elements besides 0 and 1. These two elements play exactly the same role: the map which permutes them and sends 0 to 0 and 1 to 1 is an automorphism of F: this is nothing else than Frob_2. Select one of these two elements, call it α. Then α is a generator of the multiplicative group $F^\times$, which means that $F^\times = \{1, \alpha, \alpha^2\}$ and $F = \{0, 1, \alpha, \alpha^2\}$.
Here is the addition table of this field F:

$(F,+)$	0	1	α	α^2
0	0	1	α	α^2
1	1	0	α^2	α
α	α	α^2	0	1
α^2	α^2	α	1	0

Theorem of the primitive element

Recall (Theorem 7) that any finite extension of a finite field is Galois. Hence, in a finite field F, any irreducible polynomial is separable: *finite fields are perfect.*

Proposition 11.

Let F be a finite field and K a finite extension of F. Then there exist $\alpha \in K$ such that $K = F(\alpha)$.

Proof.

Let $q = p^s$ be the number of elements in K, where p is the characteristic of F and K; the multiplicative group $K^\times$ is cyclic (Proposition 3); let α be a generator. Then

$$K = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{q-2}\} = \mathbf{F}_p(\alpha),$$

and, therefore, $K = F(\alpha)$.

□

Exercises

Exercise 12.

Prove the *normal basis Theorem*: given a finite extension $F_1 \subset F_2$ of finite fields, there exists an element β in $F_2^\times$ such that the conjugates of β over F_1 form a basis of the vector space F_2 over F_1.
Prove that, with such a basis, the Frobenius map Frob_{q_1} (where q_1 is the number of elements in F_1) becomes a shift operator on the coordinates.

Exercise 13.

Let F be a finite field, E an extension of F and α, β two elements in E which are algebraic over F of degree respectively a and b. Assume a and b are relatively prime. Prove that

$$F(\alpha, \beta) = F(\alpha + \beta).$$

Fundamental result

One of the main results of the theory of finite fields is the following :

Theorem 14.

Let F be a finite field with q elements, α an element in an algebraic closure of F. There exist integers $\ell \geq 1$ such that $\alpha^{q^\ell} = \alpha$. Denote by n the smallest:

$$n = \min\{\ell \geq 1 \; ; \; \mathrm{Frob}_q^\ell(\alpha) = \alpha\}.$$

Then the field $F(\alpha)$ has q^n elements, which means that the degree of α over F is n, and the minimal polynomial of α over F is

$$\prod_{\ell=0}^{n-1}(X - \mathrm{Frob}_q^\ell(\alpha)) = \prod_{\ell=0}^{n-1}\left(X - \alpha^{q^\ell}\right). \tag{15}$$

Galois theory

Proof of Theorem 14.

Define $s = [F(\alpha) : F]$. By Theorem 7, the extension $F(\alpha)/F$ is Galois with Galois group the cyclic group of order s generated by Frob_q. The conjugates of αover F are the elements $\mathrm{Frob}_q^i(\alpha)$, $0 \leq i \leq s-1$. Hence $s = n$.

□