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 4: July 25, 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/`

What I told you on Friday

Examples of finite fields are the fields $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ with p elements.

The ring $\mathbf{Z}/n\mathbf{Z}$ has characteristic n: that means that adding 1 less than n times produces a non–zero element of the ring, but adding it n times produces 0:

$$1 + 1 + \cdots + 1 = 0.$$

On the other hand, the characteristic of a field is a prime number. Hence $\mathbf{Z}/n\mathbf{Z}$ is a field if and only if n is a prime number.

Also if n is composite, say $n = ab$ with $a > 1$ and $b > 1$, then the class of a is a zero divisor in $\mathbf{Z}/n\mathbf{Z}$, hence this ring is not a field.

What I told you on Friday (continued)

If F is a field with q elements, then the characteristic of F is a prime number p, which means that F contains $\mathbf{F}_p$, and the number of elements of F is a power of p, say p^s. This number s is the degree of the $\mathbf{F}_p$– vector space F.

Conversely, for any prime number p and any positive integer s, there exists a field F with p^s elements. To construct such a field, we start with an irreducible polynomial $f \in \mathbf{F}_p[X]$ of degree s (there is at least one), one considers the ideal (f) in $\mathbf{F}_p[X]$ generated by f. The field F we are looking for can be viewed as $\mathbf{F}_p[X]/(f)$. If α denotes the class of X modulo f, then $F = \mathbf{F}_p(\alpha) = \mathbf{F}_p[\alpha]$.

For instance the field with 4 elements can be written as

$$\mathbf{F}_4 = \{0,\ 1,\ \alpha,\ \alpha^2\}$$

with $\alpha^2 = \alpha + 1$.

What I told you on Friday (continued)

Given a finite field $\mathbf{F}_q$ with q elements and an element α which is algebraic over $\mathbf{F}_q$ of degree n, the irreducible polynomial of α over $\mathbf{F}_q$ splits completely in the field $\mathbf{F}_q(\alpha)$ into

$$(X - \alpha)(X - \alpha^q) \cdots (X - \alpha^{q^{n-1}}).$$

Hence n is the smallest integer such that $\alpha^{q^n} = \alpha$.
For $i \geq 0$ we write $\mathrm{Frob}_{q^i}(\alpha) = \alpha^{q^i}$.

Now the goal is to find the irreducible polynomials over $\mathbf{F}_q$.
We shall see that they are the irreducible factors of $X^m - X$, where m a power of q. This is a reason to study the polynomials $X^{m-1} - 1$ where $m - 1$ and q are relatively prime.
We first factor them over $\mathbf{Z}$, and after that over $\mathbf{F}_q$.

Cyclotomic Polynomials

Let n be a positive integer. A *n–th root of unity* in a field K is an element of $K^\times$ which satifies $x^n = 1$. This means that it is a torsion element of order dividing n.
A *primitive n–th root of unity* is an element of $K^\times$ of order n: for k in $\mathbf{Z}$, the equality $x^k = 1$ holds if and only if n divides k.
For each positive integer n, the n–th roots of unity in K form a finite subgroup of $K^\times_{\text{tors}}$ having at most n elements. The union of all these subgroups of $K^\times_{\text{tors}}$ is just the torsion group $K^\times_{\text{tors}}$ itself. This group contains 1 and -1, but it could have just one element, like for $\mathbf{F}_2 = \mathbf{Z}/2\mathbf{Z}$ or $\mathbf{F}_2(X)$ for instance.
The torsion subgroup of $\mathbf{R}^\times$ is $\{\pm 1\}$, the torsion subgroup of $\mathbf{C}^\times$ is infinite.

$X^m - 1$ with m multiple of p

Let K be a field of finite characteristic p and let n be a positive integer. Write $n = p^r m$ with $r \geq 0$ and $\mathrm{pgcd}(p, m) = 1$. In $K[X]$, we have

$$X^n - 1 = (X^m - 1)^{p^r}.$$

If $x \in K$ satisfies $x^n = 1$, then $x^m = 1$. Therefore, the order of a finite subgroup of $K^\times$ is prime to p.

It also follows that the study of $X^n - 1$ reduces to the study of $X^m - 1$ with m prime to p.

Cyclotomic polynomials and roots of unity

Let n be a positive integer and Ω be an algebraically closed field of characteristic either 0 or a prime number not dividing n. Then the number of primitive n-th roots of unity in Ω is $\varphi(n)$. These $\varphi(n)$ elements are the generators of the unique cyclic subgroup C_n of order n of $\Omega^\times$, which is the group of n-th roots of unity in Ω:

$$C_n = \{x \in \Omega \,;\, x^n = 1\}.$$

Cyclotomic polynomials over $\mathbf{C}[X]$

The map $\mathbf{C} \to \mathbf{C}^\times$ defined by $z \mapsto e^{2i\pi z/n}$ is a morphism from the additive group $\mathbf{C}$ to the multiplicative group $\mathbf{C}^\times$; this morphism is periodic with period n. Hence, it factors to a morphism from the group $\mathbf{C}/n\mathbf{Z}$ to $\mathbf{C}^\times$: we denote it also by $z \mapsto e^{2i\pi z/n}$. The multiplicative group $(\mathbf{Z}/n\mathbf{Z})^\times$ of the ring $\mathbf{Z}/n\mathbf{Z}$ is the set of classes of integers prime to n. Its order is $\varphi(n)$, where φ is Euler's function.

The $\varphi(n)$ complex numbers

$$e^{2i\pi k/n}, \qquad k \in (\mathbf{Z}/n\mathbf{Z})^\times,$$

are the primitive roots of unity in $\mathbf{C}$.

Cyclotomic polynomial of index n

For n a positive integer, we define a polynomial $\Phi_n(X) \in \mathbf{C}[X]$ by

(16) $$\Phi_n(X) = \prod_{k \in (\mathbf{Z}/n\mathbf{Z})^\times} (X - e^{2i\pi k/n}).$$

This polynomial is called the *cyclotomic polynomial of index* n; it is monic and has degree $\varphi(n)$. Since

$$X^n - 1 = \prod_{k=0}^{n-1} (X - e^{2i\pi k/n}),$$

the partition of the set of roots of unity according to their order shows that

(17) $$X^n - 1 = \prod_{\substack{1 \le d \le n \\ d \mid n}} \Phi_d(X).$$

A lemma of Euler

The degree of $X^n - 1$ is n, and the degree of $\Phi_d(X)$ is $\varphi(d)$, hence, from (17) one deduces:

Lemma 18.
For any positive integer n,

$$n = \sum_{d \mid n} \varphi(d).$$

Cyclotomy

The name **cyclotomy** comes from the Greek and means *divide the circle*. The complex roots of $X^n - 1$ are the vertices of a regular polygon with n sides.
From (17), it follows that an equivalent definition of the polynomials $\Phi_1, \Phi_2, \dots$ in $\mathbf{Z}[X]$ is by induction on n:

(19) $$\Phi_1(X) = X - 1, \qquad \Phi_n(X) = \frac{X^n - 1}{\prod_{\substack{d \ne n \\ d \mid n}} \Phi_d(X)}.$$

This is the most convenient way to compute the cyclotomic polynomials Φ_n for small values of n.

Möbius function

The *Möbius function* μ (see, for instance, [3] § 2.9) is the map from the positive integers to $\{0, 1, -1\}$ defined by the properties $\mu(1) = 1$, $\mu(p) = -1$ for p prime, $\mu(p^m) = 0$ for p prime and $m \ge 2$, and $\mu(ab) = \mu(a)\mu(b)$ if a and b are relatively prime. Hence, $\mu(a) = 0$ if and only if a has a square factor, while for a squarefree number a which is a product of s distinct primes we have $\mu(a) = (-1)^s$:

$$\mu(p_1 \cdots p_s) = (-1)^s.$$

Möbius inversion formula

There are several variants of the *Möbius inversion formula*. Here is the most classical one:

Lemma 20.

[Möbius inversion formula] Let f and g be two maps defined on the set of positive integers with values in an additive group. Then the two following properties are equivalent:

(i) For any integer $n \geq 1$,

$$g(n) = \sum_{d|n} f(d).$$

(ii) For any integer $n \geq 1$,

$$f(n) = \sum_{d|n} \mu(n/d) g(d).$$

Möbius inversion formula

For instance, Lemma 18

$$\sum_{d|n} \varphi(d) = n \quad \text{for all } n \geq 1$$

is equivalent to

$$\varphi(n) = \sum_{d|n} \mu(n/d) d \quad \text{for all } n \geq 1.$$

Möbius inversion formula (again)

An equivalent statement of the Möbius inversion formula is the following multiplicative version, which deals with two maps f, g from the positive integers into an abelian multiplicative group. The two following properties are equivalent:

(i) *For any integer* $n \geq 1$,

$$g(n) = \prod_{d|n} f(d).$$

(ii) *For any integer* $n \geq 1$,

$$f(n) = \prod_{d|n} g(d)^{\mu(n/d)}.$$

For instance, when G is the multiplicative group $\mathbf{Q}(X)^\times$, we have

$$\Phi_n(X) = \prod_{d|n} (X^d - 1)^{\mu(n/d)}.$$

First examples

One has

$$\Phi_2(X) = \frac{X^2-1}{X-1} = X+1, \quad \Phi_3(X) = \frac{X^3-1}{X-1} = X^2+X+1,$$

and more generally, for p prime

$$\Phi_p(X) = \frac{X^p-1}{X-1} = X^{p-1} + X^{p-2} + \cdots + X + 1.$$

The next cyclotomic polynomials are

$$\Phi_4(X) = \frac{X^4-1}{X^2-1} = X^2+1 = \Phi_2(X^2),$$

$$\Phi_6(X) = \frac{X^6-1}{(X^3-1)(X+1)} = \frac{X^3+1}{X+1} = X^2-X+1 = \Phi_3(-X).$$

Exercise

Exercise 21.

a) Let n be a positive integer. Prove

$$\varphi(2n) = \begin{cases} \varphi(n) & \text{if } n \text{ is odd,} \\ 2\varphi(n) & \text{if } n \text{ is even,} \end{cases}$$

$$\Phi_{2n}(X) = \begin{cases} (-1)^n \Phi_n(-X) & \text{if } n \text{ is odd,} \\ \Phi_n(X^2) & \text{if } n \text{ is even.} \end{cases}$$

`Hint:` For a geometric proof, cut the circle in $2n$ pieces in place of n. Compare the positions on the unit circle of the roots of the two degree n polynomials $X^n - 1$ and $X^n + 1$.

Exercise (continued)

b) Deduce

$$\Phi_8(X) = X^4 + 1, \quad \Phi_{12}(X) = X^4 - X^2 + 1$$

and $\Phi_{2^\ell}(X) = X^{2^{\ell-1}} + 1$ for $\ell \geq 1$.

c) Let p be a prime and $m \geq 1$. Prove that if $p|m$, then

$$\Phi_m(X^p) = \Phi_{pm}(X) \quad \text{and} \quad \varphi(pm) = p\varphi(m)$$

while if $\gcd(p, m) = 1$, then

$$\Phi_m(X^p) = \Phi_{pm}(X)\Phi_m(X) \quad \text{and} \quad \varphi(pm) = (p-1)\varphi(m).$$

d) Prove that

$$\Phi_{p^r}(X) = X^{p^{r-1}(p-1)} + X^{p^{r-1}(p-2)} + \cdots + X^{p^{r-1}} + 1$$

when p is a prime and $r \geq 1$.

The cyclotomic polynomial over $\mathbf{Z}$

Theorem 22.

For any positive integer n, the polynomial $\Phi_n(X)$ has its coefficients in $\mathbf{Z}$. Moreover, $\Phi_n(X)$ is irreducible in $\mathbf{Z}[X]$.

$\Phi_n(X) \in \mathbf{Z}[X]$

Proof of the first part of Theorem 22.

We check $\Phi_n(X) \in \mathbf{Z}[X]$ by induction on n. The results holds for $n = 1$, since $\Phi_1(X) = X - 1$. Assume $\Phi_m(X) \in \mathbf{Z}[X]$ for all $m < n$. From the induction hypothesis, it follows that

$$h(X) = \prod_{\substack{d|n \\ d \neq n}} \Phi_d(X)$$

is monic with coefficients in $\mathbf{Z}$. We divide $X^n - 1$ by h in $\mathbf{Z}[X]$: let $Q \in \mathbf{Z}[X]$ be the quotient and $R \in \mathbf{Z}[X]$ the remainder:

$$X^n - 1 = h(X)Q(X) + R(X).$$

We also have $X^n - 1 = h(X)\Phi_n(X)$ in $\mathbf{C}[X]$, as shown by (17). From the unicity of the quotient and remainder in the Euclidean division in $\mathbf{C}[X]$, we deduce $Q = \Phi_n$ and $R = 0$, hence, $\Phi_n \in \mathbf{Z}[X]$. □

Irreducibility of Φ_n over $\mathbf{Z}$

We now show that Φ_n is irreducible in $\mathbf{Z}[X]$. Since it is monic, its content is 1. It remains to check that it is irreducible in $\mathbf{Q}[X]$.
Here is a proof of the irreducibility of the cyclotomic polynomial in the special case where the index is a prime number p. It rests on Eisenstein's Criterion:

Proposition 23 (Eisenstein criterion).

Let

$$C(X) = c_0X^d + \cdots + c_d \in \mathbf{Z}[X]$$

and let p be a prime number. Assume C to be product of two polynomials in $\mathbf{Z}[X]$ of positive degrees. Assume also that p divides c_i for $1 \le i \le d$ but that p does not divide c_0. Then p^2 divides c_d.

Proof of Eisenstein criterion

We denote by Ψ_p the surjective morphism of rings (reduction modulo p):

(24) $$\Psi_p : \mathbf{Z}[X] \to \mathbf{F}_p[X],$$

which maps X to X and $\mathbf{Z}$ onto $\mathbf{F}_p$ by reduction modulo p of the coefficients. Its kernel is the principal ideal $p\mathbf{Z}[X] = (p)$ of $\mathbf{Z}[X]$ generated by p.
Let

$$A(X) = a_0X^n + \cdots + a_n \quad \text{and} \quad B(X) = b_0X^m + \cdots + b_m$$

be two polynomials in $\mathbf{Z}[X]$ of degrees m and n such that $C = AB$. Hence, $d = m + n$, $c_0 = a_0b_0$, $c_d = a_nb_m$.

Proof of Eisenstein criterion (continued)

Write $\tilde{A} = \Psi_p(A)$, $\tilde{B} = \Psi_p(B)$, $\tilde{C} = \Psi_p(C)$,

$$\tilde{A}(X) = \tilde{a}_0X^n + \cdots + \tilde{a}_n, \quad \tilde{B}(X) = \tilde{b}_0X^m + \cdots + \tilde{b}_m$$

and

$$\tilde{C}(X) = \tilde{c}_0X^d + \cdots + \tilde{c}_d.$$

By assumption $\tilde{c}_0 \neq 0$, $\tilde{c}_1 = \cdots = \tilde{c}_d = 0$, hence, $\tilde{C}(X) = \tilde{c}_0X^d = \tilde{A}(X)\tilde{B}(X)$ with $\tilde{c}_0 = \tilde{a}_0\tilde{b}_0 \neq 0$. Now $\tilde{A}$ and $\tilde{B}$ have positive degrees n and m, hence, $\tilde{a}_n = \tilde{b}_m = 0$, which means that p divides a_n and b_m, and, therefore, p^2 divides $c_d = a_nb_m$.

Irreducibility of Φ_p over $\mathbf{Z}$

Proof of the irreducibility of Φ_p over $\mathbf{Z}$.

We set $X - 1 = Y$, so that, in $\mathbf{Z}[X]$,

$$\Phi_p(Y+1) = \frac{(Y+1)^p - 1}{Y} = Y^{p-1} + \binom{p}{1}Y^{p-2} + \cdots + \binom{p}{2}Y + p.$$

We observe that p divides all coefficients – but the leading one – of the monic polynomial $\Phi_p(Y+1)$ and that p^2 does not divide the constant term. We conclude by using Eisenstein's Criterion Proposition 23. □

Proof of the irreducibility of Φ_n over $\mathbf{Z}$

We now consider the general case.
Let $f \in \mathbf{Z}[X]$ be an irreducible factor of Φ_n with a positive leading coefficient and let $g \in \mathbf{Z}[X]$ satisfy $fg = \Phi_n$. Our goal is to prove $f = \Phi_n$ and $g = 1$.
Since Φ_n is monic, the same is true for f and g. Let ζ be a root of f in $\mathbf{C}$ and let p be a prime number which does not divide n. Since ζ^p is a primitive n-th root of unity, it is a zero of Φ_n.
The first and main step of the proof is to check that $f(\zeta^p) = 0$. If ζ^p is not a root of f, then it is a root of g. We assume $g(\zeta^p) = 0$ and we shall reach a contradiction.

Proof of the irreducibility of Φ_n over $\mathbf{Z}$ (continued)

Since f is irreducible, f is the minimal polynomial of ζ, hence, from $g(\zeta^p) = 0$, we infer that $f(X)$ divides $g(X^p)$. Write $g(X^p) = f(X)h(X)$ and consider the morphism Ψ_p of reduction modulo p already introduced in (24). Denote by F, G, H the images of f, g, h. Recall that $fg = \Phi_n$ in $\mathbf{Z}[X]$, hence, $F(X)G(X)$ divides $X^n - 1$ in $\mathbf{F}_p[X]$. The assumption that p does not divide n implies that $X^n - 1$ has no square factor in $\mathbf{F}_p[X]$.

Proof of the irreducibility of Φ_n over $\mathbf{Z}$ (continued)

Let $P \in \mathbf{Z}[X]$ be an irreducible factor of F. From $G(X^p) = F(X)H(X)$, it follows that $P(X)$ divides $G(X^p)$. But $G \in \mathbf{F}_p[X]$, hence (see Lemma 5), $G(X^p) = G(X)^p$ and, therefore, P divides $G(X)$. Now P^2 divides the product FG, which is a contradiction.
We have checked that for any root ζ of f in $\mathbf{C}$ and any prime number p which does not divide n, the number ζ^p is again a root of f. By induction on the number of prime factors of m, it follows that for any integer m with $\gcd(m, n) = 1$ the number ζ^m is a root of f. Now f vanishes at all the primitive roots of unity, hence, $f = \Phi_n$ and $g = 1$.

Second proof of Proposition 3

The following alternative proof (not using the exponent) of Proposition 3 is instructive, since it involves cyclotomic polynomials.

Let K be a field and G a finite subgroup of $K^\times$ of order n. For any divisor d of n, denote by $N_G(d)$ the number of elements in G of order d.
By Lagrange's Theorem

$$n = \sum_{d|n} N_G(d). \tag{25}$$

Second proof of Proposition 3 (Continued)

Let d be a divisor of n.
If $N_G(d) > 0$, that is, if there exists an element ζ in G of order d, then the cyclic subgroup of G generated by ζ has order d, hence it has $\varphi(d)$ generators.
These $\varphi(d)$ elements in K are roots of Φ_d and, therefore, they are all the roots of Φ_d in K.
It follows that there are exactly $\varphi(d)$ elements of order d in G.

Second proof of Proposition 3 (Continued)

This proves that $N_G(d)$ is either 0 or $\varphi(d)$.
From (25) and Lemma 18, we deduce

$$n = \sum_{d|n} N_G(d) \leq \sum_{d|n} \varphi(d) = n,$$

hence, $N_G(d) = \varphi(d)$ for all $d|n$.
In particular $N_G(n) > 0$, which means that G is cyclic.

Cyclotomic field of level n

Let n be a positive integer. The *cyclotomic field of level* n *over* $\mathbf{Q}$ is

$$R_n = \mathbf{Q}\big(\{e^{2i\pi k/n}\ ;\ k \in (\mathbf{Z}/n\mathbf{Z})^\times\}\big) \subset \mathbf{C}.$$

This is the splitting field of Φ_n over $\mathbf{Q}$. If $\zeta \in \mathbf{C}$ is any primitive root of unity, then $R_n = \mathbf{Q}(\zeta)$ and $\{1, \zeta, \ldots, \zeta^{\varphi(n)-1}\}$ is a basis of R_n as a $\mathbf{Q}$–vector space.

$\mathrm{Aut}(R_n/\mathbf{Q})$

Proposition 26.
There is a canonical isomorphism between $\mathrm{Aut}(R_n/\mathbf{Q})$ *and the multiplicative group* $(\mathbf{Z}/n\mathbf{Z})^\times$.

Proof.
Let ζ_n be a primitive n-th root of unity. For $\varphi \in \mathrm{Aut}(R_n/\mathbf{Q})$, define $\theta(\varphi) \in (\mathbf{Z}/n\mathbf{Z})^\times$ by

$$\varphi(\zeta_n) = \zeta_n^{\theta(\varphi)}.$$

Then θ is a group isomorphism from $\mathrm{Aut}(R_n/\mathbf{Q})$ onto $(\mathbf{Z}/n\mathbf{Z})^\times$.

□

Example 27.
The subfield of R_n *fixed by the element* $\theta^{-1}(\{1, -1\})$ *of* $\mathrm{Aut}(R_n/\mathbf{Q})$ *is the maximal real subfield of* R_n.

Cyclotomic Polynomials over a finite field

Since Φ_n has coefficients in $\mathbf{Z}$, for any field K, we can view $\Phi_n(X)$ as an element in $K[X]$: in zero characteristic, this is plain since K contains $\mathbf{Q}$; in finite characteristic p, one considers the image of Φ_n under the morphism Ψ_p introduced in (24): we denote again this image by Φ_n.

Exercise 28.
Prove that in characteristic p, for $r \geq 1$ and $m \geq 1$,

$$\Phi_{mp^r}(X) = \Phi_m(X)^{p^{r-1}(p-1)}.$$

Roots of $\Phi_n(X)$

Proposition 29.
Let K be a field and let n be a positive integer. Assume that K has characteristic either 0 or else a prime number p prime to n. Then the polynomial $\Phi_n(X)$ is separable over K and its roots in K are exactly the primitive n–th roots of unity which belong to K.

Proof.
The derivative of the polynomial $X^n - 1$ is nX^{n-1}. In K, we have $n \neq 0$ since p does not divide n, hence, $X^n - 1$ is separable over K. Since $\Phi_n(X)$ is a factor of $X^n - 1$, it is also separable over K. The roots in K of $X^n - 1$ are precisely the n–th roots of unity contained in K. A n-th root of unity is primitive if and only if it is not a root of Φ_d when $d|n$, $d \neq n$. From (19), this means that it is a root of Φ_n.

$X^{q^n} - X$ over $\mathbf{F}_q$

According to (1), given $q = p^r$, the unique subfield of $\overline{\mathbf{F}}_p$ with q elements is the set $\mathbf{F}_q$ of roots of $X^q - X$ in $\overline{\mathbf{F}}_p$. The set $\{X - x \; ; \; x \in \mathbf{F}_q\}$ is the set of all monic degree 1 polynomials with coefficients in $\mathbf{F}_q$. Hence, (1) is the special case $n = 1$ of the next statement.

Theorem 30.
Let F be a finite field with q elements and let n be a positive integer.The polynomial $X^{q^n} - X$ is the product of all irreducible polynomials in $F[X]$ whose degree divides n. In other terms, for any $n \geq 1$,

$$X^{q^n} - X = \prod_{d|n} \prod_{f \in E_q(d)} f(X)$$

where $E_q(d)$ is the set all monic irreducible polynomials in $\mathbf{F}_q[X]$ of degree d.

Proof of Theorem 30

The derivative of $X^{q^n} - X$ is -1, which has no root, hence, $X^{q^n} - X$ has no multiple factor in characteristic p.
Let $f \in \mathbf{F}_q[X]$ be an irreducible factor of $X^{q^n} - X$ and α be a root of f in $\overline{\mathbf{F}}_p$. The polynomial $X^{q^n} - X$ is a multiple of f, therefore, it vanishes at α, hence, $\alpha^{q^n} = \alpha$ which means $\alpha \in \mathbf{F}_{q^n}$. From the field extensions

$$\mathbf{F}_q \subset \mathbf{F}_q(\alpha) \subset \mathbf{F}_{q^n},$$

we deduce that the degree of α over $\mathbf{F}_q$ divides the degree of $\mathbf{F}_{q^n}$ over $\mathbf{F}_q$, that is d divides n.

Proof of Theorem 30 (Continued)

Conversely, let f be an irreducible polynomial in $\mathbf{F}_q[X]$ of degree d where d divides n. Let α be a root of f in $\overline{\mathbf{F}}_p$. Since d divides n, the field $\mathbf{F}_q(\alpha)$ is a subfield of $\mathbf{F}_{q^n}$, hence, $\alpha \in \mathbf{F}_{q^n}$ satisfies $\alpha^{q^n} = \alpha$, and, therefore, f divides $X^{q^n} - X$.
Since d divides n, the polynomial $X^{q^n} - X$ is a multiple of $X^{q^d} - X$, hence (see exercise 8), a multiple of f. This shows that $X^{q^n} - X$ is a multiple of all irreducible polynomials of degree dividing n.
In the factorial ring $\mathbf{F}_q[X]$, the polynomial $X^{q^n} - X$, having no multiple factor, is the product of the monic irreducible polynomials which divide it. Theorem 30 follows.

$N_q(d)$

Denote by $N_q(d)$ the number of elements in $E_q(d)$, that is the number of monic irreducible polynomials of degree d in $\mathbf{F}_q[X]$.
Theorem 30 yields, for $n \geq 1$,

$$q^n = \sum_{d|n} dN_q(d).$$

From Möbius inversion formula (Lemma 20), one deduces:

$$N_q(n) = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d}.$$

For instance, when ℓ is a prime number not equal to the characteristic p of $\mathbf{F}_q$,

(31) $$N_q(\ell) = \frac{q^\ell - q}{\ell}.$$

Exercise

Exercise 32.
Let F be a finite field with q elements.

a) Give the values of $N_2(n)$ for $1 \leq n \leq 6$.

b) Check
$$\frac{q^n}{2n} \leq N_q(n) \leq \frac{q^n}{n}.$$

c) Denote by p the characteristic of F and by $\mathbf{F}_p$ the prime subfield of F. Check that more than half of the elements α in F satisfy $F = \mathbf{F}_p(\alpha)$.

Decomposition of cyclotomic polynomials over a finite field

In all this section, we assume that n is not divisible by the characteristic p of $\mathbf{F}_q$.
We apply Theorem 14 to the cyclotomic polynomials.

Theorem 33.
Let $\mathbf{F}_q$ be a finite field with q elements and let n be a positive integer not divisible by the characteristic of $\mathbf{F}_q$. Then the cyclotomic polynomial Φ_n splits in $\mathbf{F}_q[X]$ into a product of irreducible factors, all of the same degree d, where d is the order of q modulo n.

Proof of Theorem 33

By definition, the *order of q modulo n* is the order of the class of q in the multiplicative group $(\mathbf{Z}/n\mathbf{Z})^\times$ (hence, it is defined if and only if n and q are relatively prime), it is the smallest integer ℓ such that q^ℓ is congruent to 1 modulo n.

Proof.
Let ζ be a root of Φ_n in a splitting field K of the polynomial Φ_n over $\mathbf{F}_q$. The order of ζ in the multiplicative group $K^\times$ is n. According to Theorem 14, the degree of ζ over $\mathbf{F}_q$ is he smallest integer $s \geq 1$ such that $\zeta^{q^s-1} = 1$. Hence it is the smallest positive integer s such that n divides $q^s - 1$, and this is the order of the image of q in the multiplicative group $(\mathbf{Z}/n\mathbf{Z})^\times$. □

Corollaries

Since an element $\zeta \in \overline{\mathbf{F}}_p^\times$ has order n in the multiplicative group $\overline{\mathbf{F}}_p^\times$ if and only if ζ is a root of Φ_n, an equivalent statement to Theorem 33 is the following.

Corollary 34.
If $\zeta \in \overline{\mathbf{F}}_p^\times$ has order n in the multiplicative group $\overline{\mathbf{F}}_p^\times$, then its degree $d = [\mathbf{F}_q(\zeta) : \mathbf{F}_q]$ over $\mathbf{F}_q$ is the order of q modulo n.

Corollary 35.
The polynomial $\Phi_n(X)$ splits completely in $\mathbf{F}_q[X]$ (into a product of polynomials all of degree 1) if and only if $q \equiv 1 \bmod n$.

This follows from Theorem 33, but it is also plain from Proposition 3 and the fact that the cyclic group $\mathbf{F}_q^\times$ of order $q-1$ contains a subgroup of order n if and only if n divides $q-1$, which is the condition $q \equiv 1 \bmod n$.

Irreducible cyclotomic polynomials

Corollary 36.
The following conditions are equivalent:
(i) *The polynomial $\Phi_n(X)$ is irreducible in $\mathbf{F}_q[X]$.*
(ii) *The class of q modulo n has order $\varphi(n)$.*
(iii) *q is a generator of the group $(\mathbf{Z}/n\mathbf{Z})^\times$.*

This can be true only when this multiplicative group is cyclic, which means n is either

$$2,\ 4,\ \ell^s,\ 2\ell^s$$

where ℓ is an odd prime and $s \geq 1$.

s divides $\varphi(q^s-1)$

Corollary 37.
Let q be a power of a prime, s a positive integer, and $n = q^s - 1$. Then q has order s modulo n. Hence, Φ_n splits in $\mathbf{F}_q[X]$ into irreducible factors, all of which have degree s.

Notice that the number of factors in this decomposition is $\varphi(q^s-1)/s$, hence it follows that s divides $\varphi(q^s-1)$.

Numerical examples

Recall that we fix an algebraic closure $\overline{\mathbf{F}}_p$ of the prime field $\mathbf{F}_p$, and for q a power of p we denote by $\mathbf{F}_q$ the unique subfield of $\overline{\mathbf{F}}_p$ with q elements. Of course, $\overline{\mathbf{F}}_p$ is also an algebraic closure of $\mathbf{F}_q$.

$\mathbf{F}_4$

Example 38.

We consider the quadratic extension $\mathbf{F}_4/\mathbf{F}_2$. There is a unique irreducible polynomial of degree 2 over $\mathbf{F}_2$, which is $\Phi_3 = X^2 + X + 1$. Denote by ζ one of its roots in $\mathbf{F}_4$. The other root is ζ^2 with $\zeta^2 = \zeta + 1$ and

$$\mathbf{F}_4 = \{0,\ 1,\ \zeta,\ \zeta^2\}.$$

If we set $\eta = \zeta^2$, then the two roots of Φ_3 are η and η^2, with $\eta^2 = \eta + 1$ and

$$\mathbf{F}_4 = \{0,\ 1,\ \eta,\ \eta^2\}.$$

There is no way to distinguish these two roots, they play the same role. It is the same situation as with the two roots $\pm i$ of $X^2 + 1$ in $\mathbf{C}$.

$\mathbf{F}_8$

Example 39.

We consider the cubic extension $\mathbf{F}_8/\mathbf{F}_2$. There are 6 elements in $\mathbf{F}_8$ which are not in $\mathbf{F}_2$, each of them has degree 3 over $\mathbf{F}_2$, hence, there are two irreducible polynomials of degree 3 in $\mathbf{F}_2[X]$. Indeed, from (31), it follows that $N_2(3) = 2$. The two irreducible factors of Φ_7 are the only irreducible polynomials of degree 3 over $\mathbf{F}_2$:

$$X^8 - X = X(X+1)(X^3+X+1)(X^3+X^2+1).$$

The $6 = \varphi(7)$ elements in $\mathbf{F}_8^\times$ of degree 3 are the six roots of Φ_7, hence, they have order 7. If ζ is any of them, then

$$\mathbf{F}_8 = \{0,\ 1,\ \zeta,\ \zeta^2,\ \zeta^3,\ \zeta^4,\ \zeta^5,\ \zeta^6\}.$$

$\mathbf{F}_8$ (Continued)

If ζ is a root of $Q_1(X) = X^3 + X + 1$, then the two other roots are ζ^2 and ζ^4, while the roots of $Q_2(X) = X^3 + X^2 + 1$ are ζ^3, ζ^5 and ζ^6. Notice that $\zeta^6 = \zeta^{-1}$ and $Q_2(X) = X^3 Q_1(1/X)$. Set $\eta = \zeta^{-1}$. Then

$$\mathbf{F}_8 = \{0,\ 1,\ \eta,\ \eta^2,\ \eta^3,\ \eta^4,\ \eta^5,\ \eta^6\}$$

and

$$Q_1(X) = (X-\zeta)(X-\zeta^2)(X-\zeta^4),$$
$$Q_2(X) = (X-\eta)(X-\eta^2)(X-\eta^4).$$

$\mathbf{F}_8$ (Continued)

For transmission of data, it is not the same to work with ζ or with $\eta = \zeta^{-1}$. For instance, the map $x \mapsto x + 1$ is given by

$$\zeta + 1 = \zeta^3,\ \zeta^2 + 1 = \zeta^6,\ \zeta^3 + 1 = \zeta,$$

$$\zeta^4 + 1 = \zeta^5,\ \zeta^5 + 1 = \zeta^4,\ \zeta^6 + 1 = \zeta^2$$

and by

$$\eta + 1 = \eta^5,\ \eta^2 + 1 = \eta^3,\ \eta^3 + 1 = \eta^2,$$
$$\eta^4 + 1 = \eta^6,\ \eta^5 + 1 = \eta,\ \eta^6 + 1 = \eta^4.$$

$\mathbf{F}_9$

Example 40.

We consider the quadratic extension $\mathbf{F}_9/\mathbf{F}_3$. Over $\mathbf{F}_3$,

$$X^9 - X = X(X-1)(X+1)(X^2+1)(X^2+X-1)(X^2-X-1).$$

In $\mathbf{F}_9^\times$, there are $4 = \varphi(8)$ elements of order 8 (the four roots of Φ_8) which have degree 2 over $\mathbf{F}_3$. There are two elements of order 4, which are the roots of Φ_4; they are also the squares of the elements of order 8 and they have degree 2 over $\mathbf{F}_3$, their square is -1. There is one element of order 2, namely -1, and one of order 1, namely 1. From (31), it follows that $N_3(2) = 3$: the three monic irreducible polynomials of degree 2 over $\mathbf{F}_3$ are Φ_4 and the two irreducible factors of Φ_8.

$\mathbf{F}_9$ (continued)

Let ζ be a root of $X^2 + X - 1$ and let $\eta = \zeta^{-1}$. Then $\eta = \zeta^7$, $\eta^3 = \zeta^5$ and

$$X^2+X-1 = (X-\zeta)(X-\zeta^3), \quad X^2-X-1 = (X-\eta)(X-\eta^3).$$

We have

$$\mathbf{F}_9 = \{0,\ 1,\ \zeta,\ \zeta^2,\ \zeta^3,\ \zeta^4,\ \zeta^5,\ \zeta^6,\ \zeta^7\}$$

and also

$$\mathbf{F}_9 = \{0,\ 1,\ \eta,\ \eta^2,\ \eta^3,\ \eta^4,\ \eta^5,\ \eta^6,\ \eta^7\}.$$

The element $\zeta^4 = \eta^4 = -1$ is the element of order 2 and degree 1, and the two elements of order 4 (and degree 2), roots of $X^2 + 1$, are $\zeta^2 = \eta^6$ and $\zeta^6 = \eta^2$.

Decomposition of Φ_{11} over $\mathbf{F}3$

Exercise 41.

Check that 3 has order 5 modulo 11 and that

$$X^{11}-1 = (X-1)(X^5-X^3+X^2-X-1)(X^5+X^4-X^3+X^2-1)$$

is the decomposition of $X^{11} - 1$ into irreducible factors over $\mathbf{F}_3$.

References

W. Chen – *Discrete Mathematics*, 201 pp. (web edition, 2008).

http://www.maths.mq.edu.au/~wchen/ln.html/

M. Demazure, *Cours d'algèbre*, Nouvelle Bibliothèque Mathématique [New Mathematics Library], 1, Cassini, Paris, 1997.
Primalité. Divisibilité. Codes. [Primality. Divisibility. Codes].

D. S. Dummit & R. M. Foote, *Abstract algebra*, John Wiley & Sons Inc., Hoboken, NJ, third ed., 2004.

S. Lang – *Algebra*, vol. 211 of Graduate Texts in Mathematics, Springer-Verlag, New York, third ed., 2002. In French: *Algèbre*, Third edition, Dunod, 2004.

References

R. Lidl & H. Niederreiter – *Introduction to finite fields and their applications*, Cambridge Univ. Press, 1994.

http://www.amazon.com/gp/reader/0521460948/ref=sib_dp_ptu#re

G.L. Mullen, C. Mummert – *Finite Fields and Applications*, Student mathematical library, **41**, AMS 2007.

V. Shoup – *A Computational Introduction to Number Theory and Algebra* (Version 2) second print editon, Fall 2008.

http://shoup.net/ntb/

On projective planes of order n (after Claude Levesque)

The rows of the incidence matrix of a projective plane of order n form a code.

Definition. Let $n \geq 2$ be an integer. A projective plane of order n is given by n^2+n+1 *points* and n^2+n+1 *lines* with the property that
• Each line contains exactly $n+1$ points,
• Each point belongs to exactly $n+1$ lines,
• Two different lines intersect in exactly one point,
• There exist four points no three of which belong to the same line.

Latin squares

Definition. A *latin square* of order n is a $n \times n$ matrix with entries in $\{1, 2, \dots, n\}$ with the property that
• Each line contains n different elements,
• Each column contains n different elements,

NOTE. Instead of $\{1, 2, \dots, n\}$ one can use a set of n elements.

Orthogonal latin squares

Definition. The two latin squares $A = (a_{ij})$ and $B = (b_{ij})$ of order n are said to be *orthogonal* if the cardinality of

$$\{(a_{ij}, b_{ij})\ ;\ 1 \le i \le n,\ 1 \le j \le n\}$$

is equal to n^2.

EXAMPLE

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{pmatrix}$$

are orthogonal.

Mutually orthogonal latin squares

EXAMPLE. Let

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{pmatrix} \quad B = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

and

$$C = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \end{pmatrix}.$$

Then $\{A,\ B,\ C\}$ is a set of three mutually orthogonal latin squares.

Two theorems, one conjecture

Theorem 42.
There exists a projective finite plane of order n if and only if there exist $n-1$ mutually orthogonal latin squares $n \times n$.

Conjecture. If there exist $n-1$ mutually orthogonal latin squares $n \times n$, then $n = p^s$ with p prime and $s \ge 1$.

Theorem 43.
Suppose that $q = p^s$ with p prime and $s \ge 1$. Then there exist $q-1$ mutually orthogonal latin squares $q \times q$.

Proof of Theorem 43

Let

$$\mathbf{F}_q = \{a_0 = 0,\ a_1 = 1,\ a_2, \ldots, a_{q-1}\}$$

be the field with q elements. Let us define $q-1$ matrices $M^{(s)}$ of size $q \times q$ by specifying that

$$M_{ij}^{(s)} = a_i a_s + a_j$$

for $1 \le s \le q-1$, $0 \le i \le q-1$, $0 \le j \le q-1$. We want to prove that $M^{(1)}, \ldots, M^{(q-1)}$ form a set of $q-1$ mutually orthogonal latin squares $q \times q$.

Proof of Theorem 43: latin squares

(i) Let us consider a given $s \in \{1, \dots, q-1\}$ and let us prove that $M^{(s)}$ is a latin square.
It is clear that for any given row, say the i–th row, its elements

$$a_i a_s + a_0,\ a_i a_s + a_1, \dots, a_i a_s + a_{q-1}$$

are all different. Similarly, for a given column, say the j–th column, its elements

$$a_0 a_s + a_j,\ a_1 a_s + a_j, \dots, a_{q-1} a_s + a_j$$

are all different.

Proof of Theorem 43: orthogonality

(ii) Now, let us prove that for s_1, s_2 in $\{1, \dots, q-1\}$ with $s_1 \neq s_2$, the couples of latin squares $M^{(s_1)}$ and $M^{(s_2)}$ are mutually orthogonal, namely let us prove that the couples

$$\left\{ \left(M_{ij}^{(s_1)}, M_{ij}^{(s_2)}\right) ;\ 0 \leq i \leq q-1,\ 0 \leq j \leq q-1 \right\}$$

are all different. We will do it by contradiction. So let us suppose that there exist i, j, u, v in $\{1, \dots, q-1\}$ such that $(i,j) \neq (u,v)$ and

$$\left(M_{ij}^{(s_1)}, M_{ij}^{(s_2)}\right) = \left(M_{uv}^{(s_1)}, M_{uv}^{(s_2)}\right).$$

Hence there exist i, j, u, v in $\{1, \dots, q-1\}$ such that

$$M_{ij}^{(s_1)} = M_{uv}^{(s_1)} \quad \text{and} \quad M_{ij}^{(s_2)} = M_{uv}^{(s_2)}.$$

End of the proof of Theorem 43

Hence

$$\begin{cases} a_i a_{s_1} + a_j = a_u a_{s_1} + a_v \\ a_i a_{s_2} + a_j = a_u a_{s_2} + a_v, \end{cases}$$

namely

$$a_{s_1}(a_i - a_u) = a_v - a_j = a_{s_2}(a_i - a_u).$$

If $a_i = a_u$, then $a_v = a_j$, a contradiction. So suppose $a_i \neq a_u$.
Then, after cancellation, $a_{s_1} = a_{s_2}$, a contradiction.

Reference for finite projective planes

D. Stinson – *Combinatorial designs. Constructions and analysis.* Springer-Verlag, New York, 2004.