Ho Chi Minh University of Science HCMUS

Update: April 18, 2009

Finite fields: some applications

Michel Waldschmidt [3]

Third course

April 13, 2009

Errata to the first course.

Page 3, replace

> When F is a field, the ring $F[X]$ of polynomials in one variable over F is a principal domain, hence an Euclidean ring, and therefore a factorial ring.

by

> When F is a field, the ring $F[X]$ of polynomials in one variable over F is a principal domain (since it is an Euclidean ring), and therefore a factorial ring.

Page 3, replace

> The ring **Z** is not an Euclidean ring

by

> The ring $\mathbf{Z}[X]$ is not an Euclidean ring

Page 10, replace

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

by

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

[3]This text is accessible on the author's web site http://www.math.jussieu.fr/~miw/coursVietnam2009.html

3 Cyclotomic Polynomials over finite fields (continued)

Consequences of Corollary 19.

We assume that n is not divisible by the characteristic p of $\mathbf{F}_q$.

1. $\Phi_n(X)$ splits completely in $\mathbf{F}_q[X]$ (into a product of polynomials all of degree 1) if and only if $q \equiv 1 \pmod{n}$. This follows from Corollary 19, but it is also plain from 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 $q \equiv 1 \pmod{n}$.

2. $\Phi_n(X)$ is irreducible in $\mathbf{F}_q[X]$ if and only if the class of q modulo n has order $\varphi(n)$, which is equivalent to saying that 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 $s \geq 1$.

`Recall:` *for $s \geq 2$, $(\mathbf{Z}/2^s\mathbf{Z})^\times$ is the product of a cyclic group of order 2 by a cyclic group of order 2^{s-2}, hence for $s \geq 3$ it is not cyclic.*

3. 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 is $\varphi(q^s-1)/s$, hence 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 $\mathbf{F}_q$.

Example 28. 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 $\mathbf{C}$.

Example 29. 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 (16) 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

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

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

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

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

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

Example 30. 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 (16) 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.

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 $\zeta^6=\eta^2$.

Exercise 31. 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 $\mathbf{F}_3$.

Exercise 32. Check that 2 has order 11 modulo 23 and that $X^{23}-1$ over $\mathbf{F}_2$ is the product of three irreducible polynomials, namely $X-1$,

$$X^{11}+X^{10}+X^6+X^5+X^4+X^2+1$$

and

$$X^{11}+X^9+X^7+X^6+X^5+X+1.$$

Example 33. Assume that q is odd and consider the polynomial $\Phi_4(X)=X^2+1$.

- If $q\equiv 1 \pmod 4$, then X^2+1 has two roots in $\mathbf{F}_q$.
- If $q\equiv -1 \pmod 4$, then X^2+1 is irreducible over $\mathbf{F}_q$.

Example 34. Assume again that q is odd and consider the polynomial $\Phi_8(X)=X^4+1$.

- If $q\equiv 1 \pmod 8$, then X^4+1 has four roots in $\mathbf{F}_q$.
- Otherwise X^4+1 is a product of two irreducible polynomials of degree 2 in $\mathbf{F}_q[X]$.

For instance Example 30 gives over $\mathbf{F}_3$

$$X^4+1=(X^2+X-1)(X^2-X-1).$$

Using the result in the previous example 33, one deduces that in the decomposition of X^8-1 over $\mathbf{F}_q$, there are

8 factors of degree 1 if $q \equiv 1 \pmod 8$,
4 factors of degree 1 and 2 factors of degree 2 if $q \equiv 5 \pmod 8$,
2 factors of degree 1 and 3 factors of degree 2 if $q \equiv -1 \pmod 4$.

Example 35. The group $(\mathbf{Z}/5\mathbf{Z})^\times$ is cyclic of order 4, there are $\varphi(4)=2$ generators which are the classes of 2 and 3. Hence

- If $q \equiv 2$ or $3 \pmod 5$, then Φ_5 is irreducible in $\mathbf{F}_q[X]$,
- If $q \equiv 1 \pmod 5$, then Φ_5 has 4 roots in $\mathbf{F}_q$,
- If $q \equiv -1 \pmod 5$, then Φ_5 splits as a product of two irreducible polynomials of degree 2 in $\mathbf{F}_q[X]$.

Decomposition of Φ_n into irreducible factors over $\mathbf{F}_q$

As usual, we assume $\gcd(n,q)=1$. Corollary 19 tells us that Φ_n is product of irreducible polynomials over $\mathbf{F}_q$ all of the same degree d. Denote by G the multiplicative group $(\mathbf{Z}/n\mathbf{Z})^\times$. Then d is the order of q in G. Let H be the subgroup of G generated by q:

$$H=\{1,q,q^2,\dots,q^{d-1}\}.$$

Let ζ be any root of Φ_n (in an algebraic closure of $\mathbf{F}_q$, or if you prefer in the splitting field of $\Phi_n(X)$ over $\mathbf{F}_q$). Then the conjugates of ζ over $\mathbf{F}_q$ are its images under the iterated Frobenius σ_q which maps x to x^q. Hence the minimal polynomial of ζ over $\mathbf{F}_q$ is

$$P_H(X)=\prod_{i=0}^{d-1}(X-\zeta^{q^i})=\prod_{h\in H}(X-\zeta^h).$$

This is true for any root ζ of Φ_n. Now fix one of them. Then the others are ζ^m where $\gcd(m,n)=1$. The minimal polynomial of ζ^m is therefore

$$\prod_{i=0}^{d-1}(X-\zeta^{mq^i}).$$

This polynomial can be written

$$P_{mH}(X) = \prod_{h \in mH} (X - \zeta^h)$$

where mH is the class $\{mq^i \ ; \ 0 \le i \le d-1\}$ of m modulo H in G. There are $\varphi(n)/d$ classes of G modulo H, and the decomposition of $\Phi_d(X)$ into irreducible factors over $\mathbf{F}_q$ is

$$\Phi_d(X) = \prod_{mH \in G/H} P_{mH}(X).$$

Factors of $X^n - 1$ *in* $\mathbf{F}_q[X]$
Again we assume $\gcd(n, q) = 1$. We just studied the decomposition over $\mathbf{F}_q$ of the cyclotomic polynomials, and $X^n - 1$ is the product of the $\Phi_d(X)$ for d dividing n. This gives all the information on the decomposition of $X^n - 1$ in $\mathbf{F}_q[X]$. Proposition 36 below follows from these results, but is also easy to prove directly.

Let ζ be a primitive n-th root of unity in an extension F of $\mathbf{F}_q$. Recall that for j in $\mathbf{Z}$, ζ^j depends only on the classe of j modulo n. Hence ζ^i makes sense when i is an element of $\mathbf{Z}/n\mathbf{Z}$:

$$X^n - 1 = \prod_{i \in \mathbf{Z}/n\mathbf{Z}} (X - \zeta^i).$$

For each subset I of $\mathbf{Z}/n\mathbf{Z}$, define

$$Q_I(X) = \prod_{i \in I} (X - \zeta^i).$$

For I ranging over the 2^n subsets of $\mathbf{Z}/n\mathbf{Z}$, we obtain all the monic divisors of $X^n - 1$ in $F[X]$. Lemma 17 implies that Q_I belongs to $\mathbf{F}_q[X]$ if and only if $Q_I(X^q) = Q_I(X)^q$.

Since q and n are relatively prime, the multiplication by q, which we denote by $[q]$, defines a permutation of the cyclic group $\mathbf{Z}/n\mathbf{Z}$:

$$\begin{array}{ccc} \mathbf{Z} & \xrightarrow{[q]} & \mathbf{Z} \\ \downarrow & & \downarrow \\ \mathbf{Z}/n\mathbf{Z} & \xrightarrow{[q]} & \mathbf{Z}/n\mathbf{Z} \\ x & \longmapsto & qx. \end{array}$$

The condition $Q_I(X^q) = Q_I(X)^q$ is equivalent to saying that $[q](I) = I$, which means that multiplication by q induces a permutation of the elements in I. We shall say for brevity that a subset I of $\mathbf{Z}/n\mathbf{Z}$ with this property is *stable under multiplication by* q. Therefore:

Proposition 36. *The map* $I \mapsto Q_I$ *is a bijective map between the subsets* I *of* $\mathbf{Z}/n\mathbf{Z}$ *which are stable under multiplication by* q *on the one hand, and the monic divisors of* $X^n - 1$ *in* $\mathbf{F}_q[X]$ *on the other hand.*

An irreducible factor of $X^n - 1$ over $\mathbf{F}_q$ is a factor Q such that no proper divisor of Q has coefficients in $\mathbf{F}_q$. Hence

Corollary 37. *Under this bijective map, the irreducible factors of* $X^n - 1$ *correspond to the minimal subsets* I *of* $\mathbf{Z}/n\mathbf{Z}$ *which are stable under multiplication by* q.

Here are some examples:

- For $I = \emptyset$, $Q_\emptyset = 1$.
- For $I = \mathbf{Z}/n\mathbf{Z}$, $Q_{\mathbf{Z}/n\mathbf{Z}} = \Phi_n$.
- For $I = \{0\}$, $Q_0(X) = X - 1$.
- If n is even (and q odd, of course), then for $I = \{n/2\}$, $Q_{n/2}(X) = X + 1$.
- Let d be a divisor of n. There is a unique subgroup C_d of order d in the cyclic group $\mathbf{Z}/n\mathbf{Z}$. This subgroup is generated by the class of n/d, it is the set of $k \in \mathbf{Z}/n\mathbf{Z}$ such that $dk = 0$, it is stable under multiplication by any element prime to n. Then $Q_{C_d}(X) = X^d - 1$.
- Let again d be a divisor of n and let E_d be the set of generators of C_d: this set has $\varphi(d)$ elements which are the elements of order d in the cyclic group $\mathbf{Z}/n\mathbf{Z}$. Again this subset of $\mathbf{Z}/n\mathbf{Z}$ is stable under multiplication by any element prime to n. Then Q_{E_d} is the cyclotomic polynomial Φ_d of degree $\varphi(d)$.

Example 38. Take $n = 15$, $q = 2$. The minimal subsets of $\mathbf{Z}/15\mathbf{Z}$ which are stable under multiplication by 2 modulo 15 are the classes of

$$\{0\},\ \{5, 10\},\ \{3, 6, 9, 12\},\ \{1, 2, 4, 8\},\ \{7, 11, 13, 14\}.$$

We recover the fact that in the decomposition

$$X^{15} - 1 = \Phi_1(X)\Phi_3(X)\Phi_5(X)\Phi_{15}(X)$$

over $\mathbf{F}_2$, the factor Φ_1 is irreducible of degree 1, the factors Φ_3 and Φ_5 are irreducible of degree 2 and 4 respectively, while Φ_{15} splits into two factors of degree 4 (use the fact that 2 has order 2 modulo 3, order 4 modulo 5 and also order 4 modulo 15).

It is easy to find the two factors of Φ_{15} of degree 4 over $\mathbf{F}_2$. There are four polynomials of degree 4 over $\mathbf{F}_2$ without roots in $\mathbf{F}_2$ (the number of monomials with coefficient 1 should be odd, hence 3 or 5) and $\Phi_3^2 = X^4 + X^2 + 1$ is reducible; hence there are three irreducible polynomials of degree 4 over $\mathbf{F}_2$:

$$X^4 + X^3 + 1, \quad X^4 + X + 1, \quad \Phi_5(X) = X^4 + X^3 + X^2 + X + 1.$$

Therefore, in $\mathbf{F}_2[X]$,

$$\Phi_{15}(X) = (X^4 + X^3 + 1)(X^4 + X + 1).$$

We check the result by computing Φ_{15}: we divide $(X^{15} - 1)/(X^5 - 1) = X^{10} + X^5 + 1$ by $\Phi_3(X) = X^2 + X + 1$ and get in $\mathbf{Z}[X]$:

$$\Phi_{15}(X) = X^8 - X^7 + X^5 - X^4 + X^3 - X + 1.$$

Let ζ is a primitive 15-th root of unity (that is, a root of Φ_{15}). Then $\zeta^{15} = 1$ is the root of Φ_1, ζ^5 and ζ^{10} are the roots of Φ_3 (these are the primitive cube roots of unity, they belong to $\mathbf{F}_4$), while $\zeta^3, \zeta^6, \zeta^9, \zeta^{12}$ are the roots of Φ_5 (these are the primitive 5-th roots of unity). One of the two irreducible factors of Φ_{15} has the roots $\zeta, \zeta^2, \zeta^4, \zeta^8$, the other has the roots $\zeta^7, \zeta^{11}, \zeta^{13}, \zeta^{14}$. Also we have

$$\{\zeta^7, \zeta^{11}, \zeta^{13}, \zeta^{14}\} = \{\zeta^{-1}, \zeta^{-2}, \zeta^{-4}, \zeta^{-8}\}.$$

The splitting field over $\mathbf{F}_2$ of any of the three irreducible factors of degree 4 of $X^{15} - 1$ is the field F_{16} with 2^4 elements, but for one of them (namely Φ_5) the 4 roots have order 5 in $F_{16}^\times$, while for the two others the roots have order 15.

Hence we have checked that in $\mathbf{F}_{16}^\times$, there are

- 1 element of order 1 and degree 1 over $\mathbf{F}_2$, namely $\{1\} \subset \mathbf{F}_2$,
- 2 elements of order 3 and degree 2 over $\mathbf{F}_2$, namely $\{\zeta^5,\ \zeta^{10}\} \subset \mathbf{F}_4$,
- 4 elements of order 5 and degree 4 over $\mathbf{F}_2$, namely $\{\zeta^3,\ \zeta^6,\ \zeta^9,\ \zeta^{12}\}$,
- 8 elements of order 15 and degree 4 over $\mathbf{F}_2$.