TC10 / **3. Finite fields**

S. Xambó

- The ring $\mathbb{Z}_n$
- Construction of finite fields
- The Frobenius automorphism
- Splitting field of a polynomial
- Structure of the multiplicative group of a finite field
- Structure of the multiplicative group of a finite field
- The discrete logarithm
- Minimal polynomial
- Uniqueness of the finite fields with the same cardinal
- Factorization of $X^n - 1$ over a finite field $F = \mathbb{F}_q$

The ring $\mathbb{Z}_n$

Set $\mathbb{Z}_n$ to denote the ring $\mathbb{Z}/(n)$ of classs of integers modulo n. We usually represent its elements by the elements of the set $\{0, 1, \dots, n-1\}$, with the operations of sum and product the ordinary sum and product of integers, but reduced modulo n.

We will also set $\mathbb{Z}_n^*$ to denote the multiplicative grup of invertible elements of $\mathbb{Z}_n$.[N1]

An element $k \in \{0, 1, \dots, n-1\}$ is invertible modulo n if and only if $\gcd(k, n) = 1$. In particular we see that $\mathbb{Z}_n$ is a field if and only if n is prime.

We have, therefore, $|\mathbb{Z}_n^*| = \varphi(n)$, where $\varphi(n)$ is Euler's (totient) function (by definition, $\varphi(n)$ is the number of $k \in \{0, 1, \dots, n-1\}$ such that $\gcd(k, n) = 1$). In particular we have

$$a^{\varphi(n)} \equiv 1 \pmod{n} \text{ for any integer } a \text{ such that } \gcd(a, n) = 1 .$$ [N2]

The function $\varphi(n)$ has the following properties:

1. $\varphi(nn') = \varphi(n)\varphi(n')$ if $\mathrm{mcd}(n, n') = 1$.
2. If p is prime, $\varphi(p^r) = p^{r-1}(p-1)$.

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

Construction of finite fields

A. If F is a finite field of cardinal q, then there exists a prime number p and a positive integer r such that $q = p^r$. The number p is called the *characteristic* of F.

B. If F is a finite field and K a subfield of F with cardinal q, then there is positive integer r such that $|F| = q^r$. If L is another subfield of F such that $K \subseteq L$, then $|L| = q^s$, where s *is a divisor of* r.

The converse of **A** is also valid: if p is a prime number and r is a positive integer, then there exist fields of cardinal $q = p^r$. Moreover, two fields of cardinal p^r are isomorphic (not canonically).

Let us summarize the essential ideas that are involved in proving these statements.

If K is a field, and $f = a_0 + a_1X + \cdots + a_{r-1}X^{r-1} + X^r \in K[X]$, then we have the quotient ring $F = K[X]/(f)$. This ring is a K-vector space of dimension r. More explicitely, if $x = [X]_f$ (the class of X mod f), then $1, x, \ldots, x^{r-1}$ is a basis of F over K. In particular we have that if K is finite and $|K| = q$, then $|f| = q^r$.

The ring F is a field if and only if f is irreductible over K. Therefore, we know how to construct a field of p^r elements (p prime and r a positive integer) if we know an irreducible polynomial of degree r over $\mathbb{Z}_p$. Thus we have that the existence of a finite field of cardinal p^r is a consequence of the following result.

Theorem. If K is a finite field, and r is any positive integer, there exist irreducible polynomials over K of degree r.

Remark. For $r = 2$, the number of monic reducible polynomials is $(q+1)q/2$, while the number of monic polynomials of degre 2 is q^2. Hence the number of monic irreducible polynomials of degree 2 over K is $I_2 = q(q-1)/2$.

A similar reasoning is valid for monic polynomial of degree 3. Indeed, there are q^3 monic polynomials of degree 3, while the number of monic reducible polynomials of degree 3 is

$$R_q = \binom{q+2}{3} + \frac{q^2(q-1)}{2} = \frac{2}{3}q^3 + \frac{1}{3}q$$

(the first summand counts polynomials that are the product of three monic linear factors and the second those that are the product of a monic linear factor and monic quadratic factor. It follows that the number of monic irreducible polynomials of degree 3 is

$$I_3 = q^3 - R_q = \frac{q^3}{3} - \frac{q}{3}.$$

Example. $\mathbb{Z}_2[X]/(X^2 + X + 1)$ is a field of 4 elements.

Example. $\mathbb{Z}_2[X]/(X^3 + X + 1)$) is a field of 8 elements.

Examples. If $a \in K$, K a field, $X^2 - a$ is irreducible over K if and only if a is not a square in K. For example, $X^2 + 1$ is irreducible over $\mathbb{Z}_3$, as the squares in $\mathbb{Z}_3$ are 0 and 1. Similarly, the squares of $\mathbb{Z}_7$ are 0, 1, 4 and 2, and hence the polynomials

$$X^2 - 3 = X^2 + 4,\ X^2 - 5 = X^2 + 2,\ X^2 - 6 = X^2 + 1$$

are irreducible over $\mathbb{Z}_7$.

Examples. If $a \in K$, $X^3 - a$ is irreducible over K if and only if a is not a cube in K. Since the cubes in $\mathbb{Z}_7$ are 0, 1 and 6, the polynomials

$X^3 - 2 = X^3 + 5, X^3 - 3 = X^3 + 4, X^3 - 4 = X^3 + 3$ and $X^3 - 5 = X^3 + 2$

are irreducible over $\mathbb{Z}_7$.

The Frobenius automorphism

In a finite field F of characteristic p, the map $F \to F$ such that $x \mapsto x^p$ is an automorphism of F. It is called the *Frobenius automorphism* of F.

The subfield of the elements $x \in F$ such that $x^p = x$ is $\mathbb{Z}_p$.

If K is a subfield of F, and $|K| = q$, the map $F \to F$ such that $x \mapsto x^q$ is an automorphism of F over K. It is called the *Frobenius automorphism of F relative to K*.

The subfield of the elements $x \in F$ such that $x^q = x$ is K.

Splitting field of a polynomial

Theorem. Given a field K and a monic polynomial $f \in K[X]$, there exists a field extension L/K and elements $\alpha_1, \dots, \alpha_r \in L$ such that

$$f = \prod_{j=1}^{r} (X - \alpha_j) \text{ and } L = K(\alpha_1, \dots, \alpha_r).$$

Proof. Let r be the degree of f. If $r = 1$, it is sufficient to set $L = K$. So we may suppose that $r > 1$, and, by induction, that the theorem is true for polynomials of degree $r - 1$.

If every irreducible factor of f has degree 1, then f has r roots in K and again we can set $L = K$. We may suppose, therefore, that f has at least one irreducible factor, say g, of degree > 1. Define $K' = K[X]/(g)$ and $\alpha = [X]$. Then the field extension K'/K and the element $\alpha \in K'$ are such that $K' = K(\alpha)$ and $g(\alpha) = 0$. Since g divides f, we also have $f(\alpha) = 0$, and hence $f' = f/(X - \alpha) \in K'[X]$. Now the proof follows by induction applied to f'. $\square$

A field L that satisfies the conditions of the preceding theorm is called a *splitting field* of f over K.

Theorem (Splitting field of $X^{q^r} - X$). Let K be a finite field and $q = |K|$. Let L be a decomposition field of $h = X^{q^r} - X$ over K. Then $|L| = q^r$.

Proof. By definition of decomposition field, there exist elements $\alpha_i \in L$, $i = 1, \dots, q^r$, such that

$$X^{q^r} - X = \prod_{i=1}^{q^r}(X - \alpha_i) \text{ and } L = K(\alpha_1, \dots, \alpha_{q^r}).$$

The elements α_i are different, for otherwise h and h' would have a common root, which is impossible because $h' = -1$. On the other hand, the set $\{\alpha_1, \dots, \alpha_{q^r}\}$ of roots of h in L is a subfield of L. Indeed, if α and β are roots of h then

$$(\alpha - \beta)^{q^r} = \alpha^{q^r} - \beta^{q^r} = \alpha - \beta \text{ and } (\alpha\beta)^{q^r} = \alpha^{q^r}\beta^{q^r} = \alpha\beta,$$

and if α is a non-zero root of h, then

$$(1/\alpha)^{q^r} = 1/\alpha^{q^r} = 1/\alpha$$

(that is, $\alpha - \beta$, $\alpha\beta$ are roots of h, and so is $1/\alpha$ if $\alpha \neq 0$). Since $\lambda^q = \lambda$ for every $\lambda \in K$, the elements of K are also roots of h. It follows that

$$L = K(\alpha_1, \dots, \alpha_{q^r}) = \{\alpha_1, \dots, \alpha_{q^r}\}$$

and consequently $|L| = q^r$. □

Corollary (Existence of finite fields)**.** If p is a prime number and r a positive integer, there exists a field of cardinal p^r.

Proof. The cardinal of the splitting field of $X^{p^r} - X$ over $\mathbb{Z}_p$ is p^r. □

Corollary. Given a field L such that $|L| = p^r$ and a divisor s of r, there exists a unique subfield of L of cardinal p^s.

Proof. If $r = st$ and we set $q = p^s$, then $|L| = p^r = p^{st} = q^t$. If there is a subfield K of L of cardinal q, it must be $K = \{\alpha \in L \mid \alpha^q = \alpha\}$. Let, then, $K = \{\alpha \in L \mid \alpha^q = \alpha\}$. Since the elements of K are the elements of L

that are fixed by the automorphism $\alpha \mapsto \alpha^q$, K is a subfield of L. To see that the cardinal of K is q, notice that $X^{p^r} - X$ is divisible by $X^q - X$:

$$X^{p^r} - X = X^{q^t} - X = X\left(X^{q^t-1} - 1\right) = X\left(X^{(q-1)m} - 1\right) = X(X^{q-1} - 1)(\cdots)$$

Thus $X^q - X$ has q roots in L and this completes the proof. □

Structure of the multiplicative group of a finite field

Order of an element. If K is a finite field and α is a non-zero element of K, the *order* of α, $\mathrm{ord}(\alpha)$, is the least positive integer r such that $\alpha^r = 1$. Note that r exists and that it is a divisor of $q - 1$ (q the cardinal of K). Moreover, $r > 1$ except for $\alpha = 1$.

Example. In $\mathbb{Z}_5$ we have $\mathrm{ord}(2) = \mathrm{ord}(3) = 4$ and $\mathrm{ord}(4) = 2$.

Proposition. Let K be a finite field, $\alpha \in K - \{0\}$ and $r = \mathrm{ord}(\alpha)$.

1. If $x \in K - \{0\}$ is such that $x^r = 1$, then there exists an integer k such that $x = \alpha^k$.

2. For every integer k, $\mathrm{ord}(\alpha^k) = r/\gcd(k, r)$.

3. The elements of order r of K have the form α^k, with $\gcd(k, r) = 1$. In particular we have that if there exists an element of order r, then there are exactly $\varphi(r)$ elements of order r.

Proof. Consider the polynomial $f = X^r - 1 \in K[X]$. Since f has degree r and K is a field, f has at most r roots in K. Since r is the order of α, all the elements of the subgroup

$$R = \{1, \alpha, \dots, \alpha^{r-1}\}$$

are roots of f and hence f has no roots other than the elements of R. Since x is a root of f by hypothesis, $x \in R$. This settles point 1.

To establish 2, let $d = \gcd(r, k)$ and $s = r/d$. We want to see that α^k has order s. If $\left(\alpha^k\right)^m = 1$, then $\alpha^{km} = 1$ and hence $r|km$. Dividing by d we see that $s|\big(m(k/d)\big)$. As s and k/d have no common primer divisors, it follows that $s|m$. Finally it is clear that

$$\left(\alpha^k\right)^s = \alpha^{k(r/d)} = \alpha^{r(k/d)} = 1$$

and this completes the proof of 2.

Finally 3 is a direct consequence of 1, 2 and the definition of $\varphi(r)$. □

Primitive roots. A non-zero element α of a finite field K of cardinal $q = p^r$ is said to be a *primitive root* (or a *primitive element*) of K if $\mathrm{ord}(\alpha) = q - 1$. In this case it is clear that

$$K^* = \{1, \alpha, \dots, \alpha^{q-2}\}.$$

This representation of the elements of K is called *exponential representation* relative to a primitive root α. With this representation, the product of elements of K is particularly easy to obtain:

$$\alpha^i \alpha^j = \alpha^k, \text{ where } k = i + j \bmod q - 1 .$$

Examples. The elements 2 and 3 are the primitive roots of $\mathbb{Z}_5$.

Theorem. Let K be a finite field of cardinal q and d a positive integer. If $d|(q-1)$, then K contains exactly $\varphi(d)$ elements of order d.

Proof. Let $p(d)$ be the number of elements of K that have order d. It is clear that

$$\sum_{d|(q-1)} p(d) = q - 1 ,$$

as the order of any non-zero element is a divisor of $q-1$. Now observe that $p(d) = \varphi(d)$ if $p(d) \neq 0$ and that $\sum_{d|(q-1)} \varphi(d) = q - 1$, with which the proof is easily completed. □

Proposition. Let L be a finite field, K a subfield of L and $q = |K|$. Let r be the positive integer such that $|L| = q^r$. If α is a primitive element of L, then $1, \alpha, \ldots, \alpha^{r-1}$ is a basis of L as a K-vector space.

Proof. If $\alpha \in L$ and $1, \alpha, \ldots, \alpha^{r-1}$ are linearly dependent over K, there would exist $a_0, \ldots, a_{r-1} \in K$, not all zero, such that

$$a_0 + a_1\alpha + \cdots a_{r-1}\alpha^{r-1} = 0.$$

If we let

$$h = a_0 + a_1X + \cdots a_{r-1}X^{r-1} \in K[X],$$

then h is a polynomial of positive degree $< r$ such that $h(\alpha) = 0$. It follows that there exists a monic irreducible polynomial $f \in K[X]$ of degree $< r$ such that $f(\alpha) = 0$. This implies that the kernel of the homomorphism $K[X] \to L$ such that $g \mapsto g(\alpha)$ is the ideal (f) and therefore that there is an inclusion of the field $K' = K[X]/(f)$ in L that is the identity on K and such that it maps $x = [X]_f$ to α.

But then the order of α divides $|K'| - 1 = q^{\deg(f)} - 1 < q^r - 1$ and α would not be a primitive root. □

Primitive polynomials. If f is an irreducible polynomial of degree r over $\mathbb{Z}_p$, p a prime, then

$$\mathbb{Z}_p(x) = \mathbb{Z}_p[X]/(f)$$

is a field of cardinal p^r, where x is the class of X mod f. The element x may be primitive or not. In the case $\mathbb{Z}_2(x) = \mathbb{Z}_2[X]/(X^2 + X + 1)$, for example, it is primitive, but in the case $\mathbb{Z}_3(x) = \mathbb{Z}_3[X]/(X^2 + 1)$, $\mathrm{ord}(x) = 4$.

Proposition. Let K be a finite field and $f \in K[X]$ a monic irreducible polynomial, $f \neq X$. Let x be the class of X in $L = K[X]/(f)$. If $m = \deg(f)$, then $\mathrm{ord}(x)$ is the least divisor d of $q^m - 1$ such that $f|(X^d - 1)$.

Proof. The order of x is the least divisor d of

$$|L| - 1 = q^m - 1$$

such that $x^d = 1$. But this is equivalent to say that $X^d - 1$ is $0 \bmod f$, which is the same as asserting that $X^d - 1$ is a multiple of f. □

If x is a primitive root, we say that f is *primitive* over $\mathbb{Z}_p$. The least divisor d of $q^m - 1$ such that $f|(X^d - 1)$ is called the *period* (or *exponent*) of *f*.

The discrete logarithm

Suppose that L is a finite field and that $\alpha \in L$ is a primitive element of L. Let K be a subfield of L and let $q = |K|$, $r = \dim_K(L)$. We know that $1, \alpha, \dots, \alpha^{r-1}$ form a basis of L over K, so that the elements of L can be uniquely written in the form

$$a_0 + a_1\alpha + \cdots a_{r-1}\alpha^{r-1}, \;\; a_0, \dots, a_{r-1} \in K.$$

This representation of the elements of L is called *additive representation* over K relative to the primitive root α.

With the additive representation the sum of two elements of L is reduced to the sum of two vectors of K^r. To calculate products, however, it is more convenient to use the exponential representation with respect to the primitive element α. More concretely, if $x, y \in L^*$ and we know the exponents i, j such that $x = \alpha^i, y = \alpha^j$, then

$$xy = \alpha^{i+j} = \alpha^k, \;\; k = i + j \bmod q - 1, \;\; q = |L|.$$

Given x, we write $\operatorname{ind}(x)$ to indicate the exponent i (defined mod $q-1$) such that $x = \alpha^i$ and we say that it is the *index* or *discrete logarithm* of x with respect to α.

In order to be able to use the additive and exponential representations at the same time, it is convenient to tabulate the additive form of the powers α^i ($r \leq i \leq q-2$),

$$\alpha^i = a_{i0} + a_{i1}\alpha + \cdots a_{i,r-1}\alpha^{r-1},$$

as this allows us to pass from the exponential form to the additive form and conversely. This table is often completed by assigning a conventional symbol (say $-$ or ∞) as the index of 0.

Given a table of discrete logarithms, we can form the *Zech* (or *Jacobi*) table, which by definition associates the index $Z(i) = \operatorname{ind}(1+\alpha^i)$ to the exponent i. With this we can get exponential representation of a sum $\alpha^i + \alpha^j$ as $\alpha^i\left(1+\alpha^{j-i}\right) = \alpha^{i+Z(j-i)}$.

x	$\mathrm{ind}(x)$
0000	–
0001	0
0010	1
0011	4
0100	2
0101	8
0110	5
0111	10

x	$\mathrm{ind}(x)$
1000	3
1001	14
1010	9
1011	7
1100	6
1101	13
1110	11
1111	12

k	α^k	$Z(k)$
–	0000	0
0	0001	–
1	0010	4
2	0100	8
3	1000	14
4	0011	1
5	0110	10
6	1100	13

k	α^k	$Z(k)$
7	1011	9
8	0101	2
9	1010	7
10	0111	5
11	1110	12
12	1111	11
13	1101	6
14	1001	3

Discrete logaritme and Zech table of $\mathbb{Z}_2(\alpha) = \mathbb{Z}_2[X]/(X^4 + X + 1)$

Minimal polynomial

Let L be finite field and K a subfield. Let $q = |K|$. Then $|L| = q^m$, for some positive integer m.

Given $\alpha \in L$, the $m + 1$ elements $1, \alpha, \dots, \alpha^m$ are linearly dependent over K. Hence there exist $a_0, \dots, a_m \in K$ not all zero such that

$$a_0 + a_1\alpha + \cdots a_m\alpha^m = 0 .$$

This means that if

$$f = a_0 + a_1X + \cdots a_mX^m,$$

then $f \neq 0$ and

$$f(\alpha) = 0.$$

Proposition. There exists a unique monic polynomial $p \in K[X]$ that satisfies the following two conditions:

1. $p(\alpha) = 0$.
2. If $f \in K[X]$ satisfies $f(\alpha) = 0$, then $p|f$.

The polynomial p is irreducible and satisfies

3. $\deg(p) \leq m$.

Proof. Among all the monic polynomials that satisfy $f(\alpha) = 0$, pick one, say p, of least degree. It is clear that $\deg(p) \leq m$, as we have observed that there exist non-zero polynomials f of degree $\leq m$ such that $f(\alpha) = 0$. If now f is any polynomial such that $f(\alpha) = 0$, let g and r be the quotient and remainder of the integer division of f by p:

$$f = gp + r, \text{ with } r = 0 \text{ or } \deg(r) < \deg(p).$$

Since $f(\alpha) = p(\alpha) = 0$, we also have $r(\alpha) = 0$. It follows that $r = 0$, for otherwise we would have a contradiction with the definition of p. But this means that $p|f$, which is the property 2.

To see that p is unique, let p' be another monic polynomial that satisfies 1 and 2. Then $p|p'$ (we can apply 2 to p', as $p'(\alpha) = 0$). Similarly, $p'|p$. This implies that $p' = \lambda p$, for some $\lambda \in K^*$. Since p and p' are monic, we conclude that $p = p'$.

To prove that p is irreducible, suppose that $p = gh,\ g, h \in K[X]$. Then $g(\alpha) = 0$ or $h(\alpha) = 0$. Without loss of generality we may assume that $g(\alpha) = 0$. Then $g = pg'$ for some polynomial g'. Thus $p = gh = pg'h$ and hence $g'h$ is a constant polynomial. Consequently g' and h are constants and therefore the factorization $p = gh$ is not proper. Hence p is irreducible. □

The polynomial p of last proposition is called the *minimal polynomial* of α over K, and usually will be denoted p_α. The degree of p_α is also called *degree of* α, and is denoted $\deg(\alpha)$.

Remark. Note that $\deg(\alpha)$ is the least positive integer r such that $\alpha^r \in \langle 1, \alpha, \dots, \alpha^{r-1} \rangle_K$.

Remark. There exists a unique K-isomorphism

$$K[X]/(p_\alpha) \simeq K[\alpha] \text{ such that } x \mapsto \alpha,$$

where $x = [X]$. Thus we see that the degree of α coincides with the dimension of $K[\alpha]$ over K. For example, if α is a primitive element of L, then $\deg(\alpha) = m$, as $K[\alpha] = L$.

Remark. If $f \in K[X]$ is a monic irreducible polynomial and α is a root of f in an extension L of K, then f is the minimal polynomial of α over K. Note, in particular, that if $K[x] = K[X]/(f)$, then f is the minimal polynomial of x over K.

Example. Let $K = \mathbb{Z}_2$, $K' = K[X]/(X^2 + X + 1)$, $x = [X]$, $L = K'[Y]/(Y^2 + xY + 1)$, $y = [Y]$. Then $y^2 = xy + 1 \in \langle 1, y \rangle_{K'}$, which amounts to rediscovering that the minimal polynomial of y over K' is $Y^2 + xY + 1$. But $y^2 \notin \langle 1, y \rangle_K$, so that the minimal polynomial of y over K has degree > 2. Since $y^3 = xy + x \notin \langle 1, y, y^2 \rangle_K$ and $y^4 = y^3 + y^2 + y + 1$, the minimal polynomial of y over K is

$$Y^4 + Y^3 + Y^2 + Y + 1.$$

Notice that this polynomial is not primitive, as $\operatorname{ord}(y) = 5$.

Conjugates of an element. The set C_α of *conjugates* over K of an element $\alpha \in L$ is defined as

$$C_\alpha = \left\{\alpha, \alpha^q, \alpha^{q^2}, \dots, \alpha^{q^{r-1}}\right\},$$

where r is the least positive integer such that

$$\alpha^{q^r} = \alpha.$$

Proposition. $p_\alpha = \prod_{\beta \in C_\alpha}(X - \beta)$.

Proof. We will use the extension of the Frobenius automorphism of L/K to the automorphism of the ring $L[X]$ such that

$$a_0 + a_1 X + \cdots + a_n X^n \mapsto a_0^q + a_1^q X + \cdots + a_n^q X^n.$$

The polynomial

$$f = \prod_{\beta \in C_\alpha}(X - \beta)$$

is invariant by this automorphism, as $\beta \to \beta^q$ permutes the elements of C_α. Hence $f \in K[X]$. Now observe that if $\beta \in L$ is a root of p_α, then β^q is also a root of p_α, as seen by applying the Frobenius automorfisme of L/K to the relation $p_a(\beta) = 0$. Applying this observation repeatedly beginning with the root α of p_α, we obtain that $p_\alpha(\beta) = 0$ for any $\beta \in C_\alpha$. Hence, $f | p_\alpha$. But since p_α is irreducible and f has positive degree, we conclude that $f = p_\alpha$, inasmuch as both polynomials are monic. □

Uniqueness of the finite fields with the same cardinal

Theorem. If K and K' are finite fields with the same cardinal q, then there exists an isomorphism $\varphi: K \to K'$.

Proof. If $q = p^r$, $\mathbb{Z}_p$ is a subfield of K and of K'. Consider the polynomial

$$X^q - X \in \mathbb{Z}_p[X].$$

Regarded as a polynomial with coefficients in K, we have

$$X^q - X = \prod_{\alpha \in K}(X - \alpha)\ .$$

Analogously,

$$X^q - X = \prod_{\alpha' \in K'}(X - \alpha')\ .$$

Let α be a primitive element of K and $f \in \mathbb{Z}_p[X]$ its minimal polynomial. We know that $\deg(f) = r$. Since all the roots of f are in K, we also have

$$f \mid \left(X^{p^r - 1} - 1\right)$$

as polynomials with coefficients in K. But since these polynomials are monic and with coefficients in $\mathbb{Z}_p$, the relation $f|\left(X^{p^r-1}-1\right)$ is also valid as polynomials with coefficients in $\mathbb{Z}_p$. The polynomial $X^{p^r-1}-1$ also factors completely in K' and thereby f has a root $\alpha' \in K'$. From this it follows that there is a unique isomorphism

$$\mathbb{Z}_p[X]/(f) \simeq \mathbb{Z}_p[\alpha'] = K'$$

such that $x = [X] \mapsto \alpha'$. But there is also a unique isomorphism

$$\mathbb{Z}_p[X]/(f) \simeq \mathbb{Z}_p[\alpha] = K$$

such that $x = [X] \mapsto \alpha$. As a result, there is a unique isomorphism $K \simeq K'$ such that $\alpha \mapsto \alpha'$. □

Factorization of $X^n - 1$ over a finite field $F = \mathbb{F}_q$

The solution of this question turns out to be of fundamental importance for the study of cyclic codes. If $q = p^r$, p prime, and we put $n = p^k n'$, $p \nmid n'$, then we have

$$X^n - 1 = \left(X^{n'} - 1\right)^{p^k}.$$

This shows that we can assume that n is not divisible by p.

Field of decomposition of $X^n - 1$**.** The condition $p \nmid n$ tells us that $[q]_n \in \mathbb{Z}_n^*$. Hence we may consider the order m of $[q]_n$ in $\mathbb{Z}_n^*$. By definition, m is the least positive integer such that

$$q^m \equiv 1 \ (n).$$

In other words, m is the least positive integer such that

$$n | (q^m - 1) .$$

We write $e_n(q)$ to denote it.

Let now $h \in F[X]$ be any monic irreducible polynomial of degree $m = e_n(q)$ and define

$$F' = F[X]/(h) \quad (F' \simeq \mathbb{F}_{q^m}).$$

Let α be a primitive element of F' (if we chose h primitive, we can take $\alpha = [X]_h$). Then, by definition of m, $\mathrm{ord}(\alpha) = q^m - 1$ is divisible by n. Set

$$r = (q^m - 1)/n \text{ and } \omega = \alpha^r.$$

Proposition. Over F' we have

$$X^n - 1 = \prod_{j=0}^{n-1}(X - \omega^j).$$

Proof. Since

$$\mathrm{ord}(\omega) = (q^m - 1)/r = n\,,$$

the set

$$R = \{\omega^j \mid 0 \leq j \leq n-1\}$$

has cardinal n. Moreover, ω^j is a root of $X^n - 1$ for all j, because

$$\left(\omega^j\right)^n = (\omega^n)^j = 1\,.$$

Hence the set R contains n distinct roots of $X^n - 1$. It follows that $\prod_{j=0}^{n-1}(X - \omega^j)$ is a monic polynomial of degree n that divides $X^n - 1$. Since both polynomials are monic of degree n, they must coincide.

***Proposition*.** $F' = F[\omega]$ and so F' is the splitting field of $X^n - 1$ over F.

Proof. Indeed, if $|F[\omega]| = q^s$, then $n = \mathrm{ord}(\omega)$ must divide $q^s - 1$ and, by definition of m, we get $s = m$.

Cyclotomic classes

Given an integer j in $0..(n-1)$, the q-*cyclotomic class* of $j \bmod n$ is the set

$$C_j = \{j, qj, \dots, q^{t-1}j\},$$

where t is the least positive integer such that $q^t j \equiv j \pmod{n}$.

If C is a q-cyclotomic class mod n, we define

$$f_C = \prod_{j\in C}(X - \omega^j).$$

Lemma. The polynomial f_C has coefficients in F for every q-cyclotomic class C.

Proof. It is enough to note that f_C is invariant by the Frobenius automorphism.

Theorem. The correspondence $C \mapsto f_C$ is a bijection between the set of q-cyclotomic classes mod n and the set of monic irreducible factors of $X^n - 1$ over F.

Proof. The fact that the q-cyclotomic classes $\mathrm{mod}\, n$ form a partition of $\{0,1,\ldots,n-1\}$, and the factoritzation $f_C = \prod_{j\in C}(X-\omega^j)$, imply that the factorization $X^n - 1 = \prod_C f_C$, where C runs over the q-cyclotomic classes mod n. It is therefore enough to show that $f_C \in F[X]$ is irreducible for any class C. To see this, note that

$$\{\omega^j | j \in C\}$$

is the set of conjugates of anyone of its elements, so that f_C is the minimal polynomial of ω^j for any $j \in C$.

Notes

N1. If A is a ring with multiplicative unit (usually dented 1, or 1_A), then the set A^* of invertible elements of A forms a grup with the product operation of A.

Examples. $\mathbb{Z}^* = \{\pm 1\}$. A is a field if and only if $A^* = A - \{0\}$. If K is a field, $K[X]^* = K^*$. If $M_n(K)$ is the ring of square matrices of dimension n, then $M_n(K)^* = GL(n, K)$, the linear grup over K of dimension n.

N2. If G is a finite grup of order n, then $a^n = e$ for any $a \in G$ (e denotes the identity element of G). Indeed, there is a least positive integer r such that $a^r = e$. Since $\{e = a^0, a, \dots, a^{r-1}\}$ is a subgroup of order r of G, we know that $r|n$ (Lagrange lemma) and this clearly implies the assertion.