TD ACCQ 201

Julien Béguinot, Duong Hieu Phan

Télécom Paris

1 Reminder

Theorem 1 (Unicity). *Let p be a prime number and $d > 0$. There exist a unique (up to isomorphism) finite field K of cardinality $q = p^d$ denoted $\mathbb{F}_q$ in the sequel. It is termed the **Galois Field** of order q.*

Theorem 2. *$\mathbb{F}_q$ is isomorphic to the splitting field of $X^q - X$ over $\mathbb{Z}_p$.*

Definition 1. A field K is said to be prime if it does not contain any field different from itself. The prime subfield of a field K is the intersection of all the subfield of K.

Theorem 3.
- *$\mathbb{Q}$ is a prime field.*
- *For any prime p, $\mathbb{F}_p$ is a prime field.*

Theorem 4. *Let K be a field, c its characteristic and P its prime subfield.*
- *If $c = 0$, P is isomorphic to $\mathbb{Q}$*
- *If $c \neq 0$, then c is prime and P is isomorphic to $\mathbb{F}_c$.*

Theorem 5. *Let $q = p^d$, $a \in \mathbb{F}_q$ and μ_a its minimal polynomial. Then,*
- *μ_a is irreducible over $\mathbb{F}_p$*
- *$\deg \mu_a \leqslant d$*
- *If a is a root of $P \in \mathbb{F}_p[X]$, then $\mu_a | P$. In particular $\mu_a | X^{p^d} - X$*
- *μ_a is the minimal polynomial of all a^{p^i} for $1 \leqslant i \leqslant d$*

. In particular the product of all disctinct minimal polynomial of element of $\mathbb{F}_q$ is $X^q - X$.

Theorem 6. *Let $q = p^d$, $a \in \mathbb{F}_q$. Let r be the smallest integer such that*

$$a^{p^r} = a$$

i.e. the smallest r such that $p^r \equiv 1 \bmod \operatorname{ord}(a)$. Then $r | d$ and the minimal polynomial of a over $\mathbb{F}_p$ is

$$\mu_a = \prod_{i=0}^{r-1} (X - a^{p^i}).$$

Definition 2 (Cyclotomic Coset). The **cyclotomic coset** of i modulo $p^d - 1$ is

$$C(i) \triangleq \{i, pi, \dots p^{r-1} i\}$$

where r is the smallest integer such that $p^r = \bmod p^d - 1$. By the previous theorems we can then derive all the minimal polynomials of a finite field using the cyclotomic cossets. If α is a primitive element in $\mathbb{F}_q$ then

$$\mu_{a^i} = \prod_{s \in C(i)} X - \alpha^s.$$

Example 1. Let α be a root of $P(X) = X^3 + X + 1 \in \mathbb{F}_2[X]$. And $\mathbb{F}_8$ the coresponding field extension. The cyclotomic cossets are $\{0\}, \{1, 2, 4\}$ and $\{3, 5, 6\}$. The conjugates elements corresponding to each class are $\{1\}$, $\{\alpha, \alpha^2, \alpha^4\}$ and $\{\alpha^3, \alpha^5, \alpha^6\}$. The minimal polynomials are $X + 1, X^3 + X + 1$ and $X^3 + X^2 + 1$.

Definition 3. Let $\mathbb{F}_q$ be a finite field and α a primitive element in $\mathbb{F}_q$ then $\mathbb{F}_q^* = \{1, \alpha, \ldots, \alpha^{q-2}\}$ so we can define a logarithm in base α

$$\log_\alpha : x \in \mathbb{F}_q^* \mapsto i \in \{0, \ldots, q-2\}$$

such that $\alpha^{\log_\alpha(x)} = x$. The value of the logarithm can be stored in a look-up table to speed up computations.

Theorem 7 (Froebenius Mapping)**.**

$$\mathrm{Froeb} : x \in \mathbb{F}_{p^n} \mapsto x^p \in \mathbb{F}_{p^n}$$

is an automorphism of order n. Further $\mathrm{Froeb}(x) = x$ *if and only if* $x \in \mathbb{F}_p$*.*

2 Exercices

Exercice 1 (Construction of $\mathbb{F}_9$)**.** *Construct* $\mathbb{F}_9$ *as an extension of* $\mathbb{F}_3$ *explicitely in two ways:*

- *Consider* $P = X^2 + X + 2 \in \mathbb{F}_3[X]$.
- *Consider* $Q = X^2 + 1 \in \mathbb{F}_3[X]$.

Can you explicit the isomorphism between these constructions of $\mathbb{F}_3$ *? Find all the minimal polynomials of elements of* $\mathbb{F}_9$*. Give the factorisation of* $X^9 - X$ *as a product of irreducible polynomial in* $\mathbb{F}_3$*.*

Solution 1. First P is an irreducible polynomial in $\mathbb{F}_3[X]$. Indeed if it was not then it would split as a product of two polynomials of degree 1. But then P would have a root in $\mathbb{F}_3[X]$ which is not the case (by computing explictely $P(x)$ for $x = 0, 1, 2$). Let α be a root of P we obtain $\mathbb{F}_9$ by adjoining α to $\mathbb{F}_3$. It turns out that α is a primitive element of $\mathbb{F}_9$ so we can obtain $\mathbb{F}_9^*$ as

$$\langle\alpha\rangle = \{\alpha^0 = 1, \alpha^1, \alpha^2 = 2\alpha + 1, \alpha^3 = 2\alpha + 2, \alpha^4 = 2, \alpha^5 = 2\alpha, \alpha^6 = \alpha + 2, \alpha^7 = \alpha + 1\}.$$

Q is also irreducible in $\mathbb{F}_3[X]$ so we can also obtain $\mathbb{F}_9$ by considering a root β of Q. In this construction we have $\langle\beta\rangle = \{\alpha^0 = 1, \alpha^1, \alpha^2 = 2, \beta^3 = 2\beta\}$ so β is not a primitive element in $\mathbb{F}_9$. Though we know that $\mathbb{F}_9^*$ is cyclic so there must be a primitive element in the field. Because this cyclic group has $\varphi(8) = 4$ generators any other element must be a generator. We obtain a primitive element with $\gamma = \beta + 1$ for instance. Then we have

$$\langle\gamma\rangle = \{\gamma^0 = 1, \gamma = \beta + 1, \gamma^2 = 2\beta, \gamma^3 = 2\beta + 1, \gamma^4 = 2, \gamma^5 = 2\beta + 2, \gamma^6 = \beta, \gamma^7 = \beta + 2\}.$$

. From the two construction we can check directkly that the isomorphism between the two field conbstruction is given by

$$\theta(a\alpha + b) = a\gamma + b$$

The factorization and the minimal polynomials are given by the cyclotomic cosets $\{0\}, \{1, 3\}, \{2, 6\}, \{4\}, \{5, 7\}$. Which yields respectively $X + 2, X^2 + 2X + 2, X^2 + 1, X + 1, X^2 + X + 2$. In particular,

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

Exercice 2. *Construct explicitely $\mathbb{F}_{16}$ with $X^4 + X + 1$.*

Solution 2. Like previous exercice.

Exercice 3 (Trace and Norm)**.** *Let $K \subseteq L$ be a finite field extension. Let $x \in L$ and*

$$m_x : y \in L \mapsto xy \in L.$$

Show that m_x is a K-endomorphism of L. The trace of x is defined as

$$\mathrm{Tr}_{L/K}(x) \triangleq \mathrm{Tr}(m_x).$$

Show that the trace if a K-linear form over L. The norm of x is defined as the determinant of m_x i.e.

$$\mathrm{N}_{L/K}(x) \triangleq \det(m_x).$$

Further show that if $x \in K$ then $\mathrm{Tr}_{L/K}(x) = [L : K]x$ and $\mathrm{N}_{L/K}(x) = x^{[L:K]}$. Show that $\mathrm{Tr}_{\mathbb{C}/\mathbb{R}}(z) = z + \bar{z}$ and $\mathrm{N}_{\mathbb{C}/\mathbb{R}}(z) = z\bar{z}$. Show that

$$\mathrm{Tr}_{\mathbb{F}_{p^m}/\mathbb{F}_p}(x) = x^p + x^{p^2} + \ldots + x^{q^{m-1}} \tag{1}$$

and

$$\mathrm{N}_{\mathbb{F}_{p^m}/\mathbb{F}_p}(x) = x^p x^{p^2} \ldots x^{q^{m-1}}. \tag{2}$$

Solution 3. The first and second questions are clear. For the last point you can observe that in any basis of L as K vectorial space of dimension $[L : K]$ then $m_x = \mathrm{diag}(x, \ldots, x)$ hence the result. The expression of the trace of a complex over the reals is obtained by consodering $\mathbb{C}$ as a $\mathbb{R}$-vectorial space with basis $(1, i)$. We now prove the last two points. Let α be a primitive element of the field. Then the minimal polynomial of α is equal to the charachteristic polynomial of the endomorphism m_α. Let $\xi_\alpha = \prod(X - \lambda_i) = \prod(X - \alpha^{p^i})$. In particular the trace is the sum of the roots of the charachteristic polynomials and the norm if the product of the roots. Now if $x = Q(\alpha)$ for some polynomial Q then $m_x = Q(m_\alpha)$. And the chararcteristic polynomial of m_x is $\xi_x = \prod (X - Q(\lambda_i))$. But since the Frobenius is linear we can commute Q and the iterated froebenius and we have $\xi_x = \prod \left(X - Q(\alpha)^{p^i}\right) = \prod \left(X - x^{p^i}\right)$. This exactly proves the last two points.