FINITE FIELDS

PIERRE-LOÏC MÉLIOT

Abstract. In this short note, we prove the fundamental theorem of the theory of finite fields: every prime power $q = p^n$ gives rise to a unique finite field $\mathbb{F}_q$, which can be obtained as a quotient of the ring of polynomials $\mathbb{F}_p[X]$.

Characteristic of a field. Recall that a field k is a commutative ring with $0_k \neq 1_k$, and such that every element $x \neq 0_k$ in k is invertible for the multiplication. Given a field k, there is a unique morphism of rings

$$\begin{aligned} \phi : \mathbb{Z} &\to k \\ m &\mapsto m \cdot 1_k = \underbrace{1_k + 1_k + \cdots + 1_k}_{m \text{ times}}. \end{aligned}$$

The definition of ϕ extends to negative integers by setting $\phi(-m) = -\phi(m)$. The kernel of ϕ is an ideal of $\mathbb{Z}$, so it writes as $\ker \phi = d\mathbb{Z}$ with d non-negative integer. We can then distinguish two cases:

- $d = 0$, ϕ injective. We can then extend ϕ to the field of rational numbers $\mathbb{Q}$:
$$\phi\left(\frac{a}{b}\right) = \frac{\phi(a)}{\phi(b)},$$
because if $b \neq 0$, then $\phi(b) \neq 0_k$ and is invertible in k. We then obtain a morphism of fields $\phi : \mathbb{Q} \to k$, which is injective (remark: any morphism of rings $\phi : k_1 \to k_2$ between fields is injective, because the kernel is an ideal of k_1 and is not k_1 itself, as 1_{k_1} is sent by ϕ to $1_{k_2} \neq 0_{k_2}$; we conclude that $\ker \phi = \{0_{k_1}\}$, since the only ideals of a field k are $\{0_k\}$ and k). In this setting, one says that k is a field **with characteristic 0**, and k contains $\mathbb{Q}$ (called the **prime subfield** of k).
- $d > 0$. We cannot have $d = 1$ since $\phi(1) = 1_k \neq 0_k$. In fact, d is necessarily a prime number: if $d = d_1 d_2$, then $\phi(d_1)\phi(d_2) = 0_k$, so $\phi(d_1) = 0_k$ or $\phi(d_2) = 0_k$, and by minimality of d, $d = d_1$ or $d = d_2$. So, $\ker \phi = p\mathbb{Z}$ for some prime number p, and we then say that k is a field **with characteristic p**. The morphism ϕ descends to a morphism of fields
$$\phi : \mathbb{Z}/p\mathbb{Z} \to k,$$
so k contains as a prime subfield the field $\mathbb{Z}/p\mathbb{Z}$, which we also denote $\mathbb{F}_p$ in the sequel.

If k is a field with finite cardinality, then obviously we cannot have an injective morphism from $\mathbb{Z}$ (infinite) to k, so k has positive characteristic $p \in \mathbb{P}$. This implies the following:

Proposition 1. *Every finite field k has for cardinality a power $p^{n\geq 1}$ of a prime number p.*

Proof. Given two fields $k \subset K$, the larger field K is a k-vector space for the scalar product

$$\begin{aligned} k \times K &\to K \\ (\lambda, x) &\mapsto \lambda \times_K x. \end{aligned}$$

If k is a finite field with characteristic p, then it is a $\mathbb{Z}/p\mathbb{Z}$-vector space with finite dimension $n \geq 1$, whence the result. □

Date: March 16, 2020.

Group of invertibles. Given a finite field k, we denote $k^* = k \setminus \{0_k\}$ the set of non-zero elements, which by definition of a field is a group for the multiplication.

Proposition 2. *If k is a finite field, its group of invertible elements k^* is a cyclic group (isomorphic as a group to $\mathbb{Z}/(q-1)\mathbb{Z}$ if $q = \mathrm{card}\, k$).*

Proof. Consider a finite commutative group G, and denote e the least common multiple of all the orders of the elements of G. We claim that G contains an element with order e. In order to prove this, consider the prime numbers $p_1, \ldots, p_s$ that appear as factors of the orders of the elements of G, and denote $r_1, \ldots, r_s \geq 1$ the maximal powers of these prime numbers as factors of orders of elements. By considering adequate powers of elements of G, we therefore have for each i an element $g_i \in G$ with order equal to $(p_i)^{r_i}$, and on the other hand,

$$e = (p_1)^{r_1}(p_2)^{r_2} \cdots (p_s)^{r_s}.$$

It now suffices to prove that if g and h have orders $\omega(g)$ and $\omega(h)$ which are coprime, then gh has order $\omega(g)\,\omega(h)$. By applying this result recursively to the g_i's, we shall then obtain an element $g = g_1 g_2 \cdots g_r$ with order e. Obviously, given g and h with $\omega(g) \wedge \omega(h) = 1$, we have

$$(gh)^{\omega(g)\,\omega(h)} = (g^{\omega(g)})^{\omega(h)}\,(h^{\omega(h)})^{\omega(g)} = e_G\, e_G = e_G,$$

so $\omega(gh)$ divides $\omega(g)\,\omega(h)$. Conversely, note that

$$g^{\omega(h)\,\omega(gh)} = (gh)^{\omega(h)\,\omega(gh)}\,h^{-\omega(h)\,\omega(gh)} = e_G\, e_G = e_G,$$

so $\omega(h)\,\omega(gh)$ divides $\omega(g)$. Since $\omega(g)$ and $\omega(h)$ are coprime, $\omega(gh)$ divides $\omega(g)$, and by symmetry it also divides $\omega(h)$, so $\omega(gh)$ divides $\omega(g)\,\omega(h)$. We conclude that $\omega(gh) = \omega(g)\,\omega(h)$.

Let us consider the group of invertibles $G = k^*$ of a finite field with cardinality q, and let us use the existence of an element g with maximal order e with respect to the relation of divisibility. We have for any element $x \in k \setminus \{0\}$ the identity $x^e = 1_k$. This is a polynomial equation in a field, so its number of solutions is smaller than the degree e. Therefore, $q - 1 \leq e$, and we have proved the existence of an element g with multiplicative order at least equal to $q - 1$. As $q - 1 = \mathrm{card}\, k^*$, e cannot be larger, so $e = q - 1$ and g is a cyclic generator of k^*. □

This result can be used to prove the first part of the fundamental theorem on finite fields. In the sequel, we call a polynomial $P(X)$ with coefficients in $\mathbb{F}_q$ **monic** if its leading term $X^n + \cdots$ has coefficient 1, and **irreducible** if it is not the product of two polynomials with degree larger than 1.

Theorem 3. *Let q be a prime power $p^{n \geq 1}$.*

(1) If $P(X)$ is a monic irreducible polynomial with degree n in $\mathbb{F}_p[X]$, then the quotient ring $\mathbb{F}_p[X]/(P)$ is a finite field with cardinality $q = p^n$.

(2) Conversely, if k is a finite field with cardinality $q = p^n$, then there exists a monic polynomial P with degree n and irreducible in $\mathbb{F}_p[X]$ and an isomorphism of fields $k \simeq \mathbb{F}_p[X]/(P)$.

Note that at this point, we do not know whether there exists for each $n \geq 1$ an irreducible polynomial with degree n in $\mathbb{F}_p[X]$. This existence result will be shown later (Theorem 7).

Proof. The first part of the theorem is an immediate consequence of the existence of Bezout relations. Consider a non-zero element $[Q]$ in the quotient ring $\mathbb{F}_p[X]/(P)$, with P monic irreducible polynomial of degree n. It is represented by a non-zero polynomial Q with degree $\deg Q \in [\![0, n-1]\!]$. Since P is irreducible, P and Q are coprime and there exists a Bezout relation

$$UP + VQ = 1.$$

If we project this relation in $\mathbb{F}_p[X]/(P)$, we obtain $[V][Q] = [1]$, so $[Q]$ is invertible and the quotient ring $\mathbb{F}_p[X]/(P)$ is a field. Its number of elements is the number of polynomials over $\mathbb{F}_p$ with degree smaller than $n-1$, that is p^n.

Conversely, consider a finite field k with cardinality $q = p^n$, and an element α_0 in k which is a cyclic generator of k^*. We have a morphism of rings

$$\begin{aligned} \psi : \mathbb{F}_p[X] &\to k \\ P &\mapsto P(\alpha_0). \end{aligned}$$

This morphism is surjective, because every non-zero element of k is a power of α_0, hence attained by ψ; of course, 0_k is also attained as $\psi(0)$. The kernel of ψ is an ideal of $\mathbb{F}_p[X]$, hence of the form $(P) = P(X)\,\mathbb{F}_p[X]$; we can assume without loss of generality that P is monic. The polynomial P is necessarily irreducible, because if $P = P_1P_2$, then $P_1(\alpha_0)\,P_2(\alpha_0) = 0_k$, so $P_1(\alpha_0) = 0_k$ or $P_2(\alpha_0) = 0_k$. The morphism ψ descends to an isomorphism of rings (and in fact of fields) between $\mathbb{F}_p[X]/(P)$ and k. $\square$

Automorphisms. We now investigate the group of automorphisms $\mathrm{Aut}(k)$ of a finite field k with characteristic p and cardinality $q = p^n$.

Lemma 4. *Consider the* ***Frobenius morphism*** $F : x \mapsto x^p$*. It is an automorphism of the field* k*.*

Proof. This map sends 0_k to 0_k, 1_k to 1_k, and it is obviously compatible with the multiplication. The compatibility with the addition is a bit more surprising, and it is due to the positive characteristic. Given x and y, we have

$$F(x+y) = (x+y)^p = x^p + y^p + \sum_{k=1}^{p-1} \binom{p}{k} x^k y^{p-k}.$$

However, all the non-trivial binomial coefficients above vanish in characteristic p:

$$\binom{p}{k} = \frac{p(p-1)\cdots(p-k+1)}{1\,2\cdots k}$$

contains p in the numerator, and no number larger than or equal to p in the denominator, so it is divisible by p; hence, $F(x+y) = F(x) + F(y)$. $\square$

We have $F^{\circ n} = \mathrm{id}_k$: for any $x \neq 0_k$, $x^{q-1} = 1_k$, so $F^{\circ n}(x) = x^q = x$, and this is also true if $x = 0_k$. On the other hand, if $m < n$, then we do not have $F^{\circ m} = \mathrm{id}_k$, because this would amount to a polynomial equation with degree p^m and p^n solutions. So, we have a group of automorphisms

$$\langle F \rangle = \{\mathrm{id}_k,\, F,\, F^{\circ 2}, \dots, F^{\circ(n-1)}\}$$

with n distinct maps, which is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ as a group (for the operation of composition of automorphisms).

Proposition 5. *The set above is the full group of automorphisms of* k*:* $\mathrm{Aut}(k) \simeq \mathbb{Z}/n\mathbb{Z}$*, and it consists of the powers of the Frobenius morphism.*

Proof. We already have the inclusion $\langle F \rangle \subset \mathrm{Aut}(k)$, so we have to prove that conversely, if $G \in \mathrm{Aut}(k)$, then it is equal to some power of the Frobenius morphism. Consider as in the proof of Theorem 3 an element α_0 which spans the cyclic group k^*, and its minimal polynomial P (monic polynomial which spans the ideal of polynomials of $\mathbb{F}_p[X]$ which vanish on α_0). We write $P(X) =$

$X^n + c_{n-1}X^{n-1} + \cdots + c_0$, with the c_i's in $\mathbb{F}_p$. Note that if $x \in k$ is a root of P, then the same holds for $F(x)$, because:

$$0_k = F(0_k) = F(P(x)) = \sum_{k=0}^{n} F(c_k\,x^k) = \sum_{k=0}^{n} c_k\,(F(x))^k = P(F(x)).$$

Indeed, if $c \in \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, then $F(c) = c^p = c$ by the Fermat theorem. It follows that $\alpha_1 = F(\alpha_0)$, $\alpha_2 = F^{\circ 2}(\alpha_0)$, *etc.*, $\alpha_{n-1} = F^{\circ(n-1)}(\alpha_0)$ are roots of P. All these roots are distinct, because otherwise α_0 would have a multiplicative order smaller than $q-1$. Therefore, the factorisation of P viewed as a polynomial in $k[X] \supset \mathbb{F}_p[X]$ is:

$$P(X) = \prod_{i=0}^{n-1} (X - F^{\circ i}(\alpha_0)).$$

Consider now an automorphism G of k. Notice that it must be the identity on the prime subfield $\mathbb{F}_p$, because $G(m \cdot 1_k) = m \cdot 1_k$ for any $m \in \mathbb{N}$. As a consequence, if x is a root of P, then for the same reasons as above, $G(x)$ is again a root of P. In particular, there is an index $i \in [\![0, n-1]\!]$ such that $G(\alpha_0) = \alpha_i = (\alpha_0)^{p^i}$. But then, for any power of α_0, we have

$$G((\alpha_0)^m) = (G(\alpha_0))^m = (\alpha_0)^{p^i m} = F^{\circ i}((\alpha_0)^m).$$

Since α_0 is a cyclic generator, G and F^i correspond on k^*; they also obviously correspond on 0_k. Thus, $G = F^i$. $\square$

An important argument used in the proof above is that if $P \in \mathbb{F}_p[X]$, then the Frobenius morphism acts by permutation of the roots of P in k. Above, the action was cyclic; for a general polynomial P (not necessarily irreducible over $\mathbb{F}_p$), the action can split in several orbits.

Classification of the subfields. Consider a finite field K with cardinality $q = p^{n \geq 1}$; it contains the prime subfield $k = \mathbb{Z}/p\mathbb{Z}$. We want to describe all the intermediary subfields L with $k \subset L \subset K$. In the setting of finite fields, this is easy:

Proposition 6. *If L is an intermediary subfield with cardinality p^d, then d divides n. Conversely, for any divisor d of n, there exists a unique subfield L of K, which can be obtained as the set of fixed points of $F^{\circ d} : K \to K$.*

Proof. If $k \subset L \subset K$, then $\mathrm{card}\, L$ is a power p^d of p, and as K is a L-vector field, p^n is a power of p^d, so d must divide n. Notice then that the relation $x^{p^d} = x$ holds for any $x \in L$, so we have the inclusion

$$L \subset \mathrm{Fix}(F^{\circ d}).$$

Since we are looking at a set determined by a polynomial equation with degree d, the cardinality of the right-hand side is at most p^d, so by cardinality, $L = \mathrm{Fix}(F^{\circ d})$. This proves the uniqueness of a subfield with cardinality p^d, and it remains to prove that for every divisor d of n, the set $\mathrm{Fix}(F^{\circ d})$ has exactly cardinality p^d (this is the existence part of the proof). Equivalently, we need to show that the polynomial $X^{p^d} - X$ splits over K, with simple roots. However, we already know that this is true for $d = n$, because the set of roots of this polynomial is K. It suffices then to see that if d divides n, then $X^{p^d} - X$ divides $X^{p^n} - X$ in $\mathbb{F}_p[X]$:

$$X^{p^n} - X = (X^{p^d} - X)\left(\sum_{k=0}^{\frac{p^n - p^d}{p^d - 1}} X^{(p^d-1)k}\right). \qquad \square$$

Note that the divisors of n correspond bijectively to the subgroups of the group of automorphisms $\mathrm{Aut}(K) \simeq \mathbb{Z}/n\mathbb{Z}$. Therefore, the previous proposition can be restated as a correspondence between intermediary subfields $k \subset L \subset K$, and intermediary subgroups $\mathbb{Z}/n\mathbb{Z} \supset \mathbb{Z}/\frac{n}{d}\mathbb{Z} \supset \{1\}$, the correspondence being

$$L \mapsto \mathrm{Fix}(L) = \{G \in \mathrm{Aut}(K) \,|\, G(l) = l \text{ for all } l \in L\}.$$

In pompous terms, we have an anti-equivalence of categories; in the diagram below, the arrows correspond to injective morphisms (of fields or of groups), and the correspondence reverses the arrows. This is a particular case of the **Galois correspondence** between field extensions and groups of automorphisms.

$$\begin{tikzcd}
K = \mathbb{F}_{p^n} & & & \mathrm{Fix}(K) = \{\mathrm{id}_K\} \arrow[dd] \arrow[dr] & \\
& L = \mathbb{F}_{p^d} \arrow[ul] & & & \mathrm{Fix}(L) = \langle F^{\circ d} \rangle \arrow[dl] \\
k = \mathbb{F}_p \arrow[uu] \arrow[ur] & & & \mathrm{Fix}(k) = \langle F \rangle = \mathbb{Z}/n\mathbb{Z} &
\end{tikzcd}$$

The main identity. We are now ready to prove the remaining part of the fundamental theorem:

Theorem 7. *For every prime power $q = p^{n\geq 1}$, there exists a finite field with cardinality q, and it is unique up to isomorphisms. We denote it $\mathbb{F}_q$.*

Lemma 8. *Denote* $\mathrm{Irr}(n, \mathbb{F}_p)$ *the set of monic irreducible polynomials with degree n over $\mathbb{F}_p$. We have the following factorisation in $\mathbb{F}_p[X]$:*

$$X^{p^n} - X = \prod_{d\,|\,n} \prod_{P \in \mathrm{Irr}(d,\mathbb{F}_p)} P(X).$$

Proof. Notice first that $Q(X) = X^{p^n} - X$ does not have a multiple irreducible factor. Indeed, we can compute the greatest common divisor of Q and Q':

$$\gcd(Q, Q') = \gcd(X^{p^n} - X, -1) = 1.$$

Let P be an irreducible factor of Q in $\mathbb{F}_p[X]$. In the finite field $k_P = \mathbb{F}_p[X]/(P)$, we have the relation $[X^{p^n} - X] = 0$, so, if $\alpha = [X]$, then $F^{\circ n}(\alpha) = \alpha$. The same relation holds for $\alpha^2, \alpha^3, \ldots, \alpha^{n-1}$ since the Frobenius morphism F is a morphism of fields. Therefore, $F^{\circ n} = \mathrm{id}_{k_P}$ holds over the $\mathbb{F}_p$-linear basis

$$\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$$

of k_P; therefore, $F^{\circ n} = \mathrm{id}_{k_P}$. This implies that the dimension $d = \deg P$ of k_P over $\mathbb{F}_p$ divides n (by using the description of the group of automorphisms of a finite field). Conversely, if $P \in \mathrm{Irr}(d, \mathbb{F}_p)$ with $d \,|\, n$, then we have the relation $x^{p^d} = x$ in k_P, so in particular, $[X^{p^d} - X] = [0]$. In other words, $P(X)$ divides $X^{p^d} - X$. *A fortiori*, it divides $X^{p^n} - X$, because we have seen that $X^{p^d} - X$ divides $X^{p^n} - X$ if d divides n. $\square$

Proof of Theorem 7. Let $I(d, p)$ be the cardinality of $\mathrm{Irr}(d, \mathbb{F}_p)$. The main identity implies that

$$\forall n \geq 1, \;\; p^n = \sum_{d\,|\,n} d\, I(d, p)$$

by looking at the degrees. We can invert this relation by using the **Möbius function**

$$\mu(n) = \begin{cases} (-1)^r & \text{if } n = p_1 p_2 \cdots p_r \text{ has no square factor,} \\ 0 & \text{otherwise.} \end{cases}$$

Thus,

$$I(n,p) = \frac{1}{n} \sum_{d \,|\, n} \mu\left(\frac{n}{d}\right) p^d.$$

In particular, by isolating the term $d = n$, we see that

$$I(n,p) \geq \frac{1}{n} \left(p^n - \sum_{\substack{d \,|\, n \\ d<n}} p^d \right) \geq \frac{p^n - (1 + p + \cdots + p^{n-1})}{n} > 0.$$

So, for any $p \in \mathbb{P}$ and any $n \geq 1$, there exists at least one irreducible polynomial over $\mathbb{F}_p$ with degree n, hence a finite field with cardinality p^n.

It remains to prove the unicity up to isomorphisms. To this purpose, let us modify a bit the proof of Theorem 3. We fix a finite field k with cardinality p^n and an arbitrary polynomial $P \in \mathrm{Irr}(n, \mathbb{F}_p)$, and we are going to exhibit an isomorphism of fields $k \simeq \mathbb{F}_p[X]/(P)$. The polynomial $X^{p^n} - X$ splits over k, and it has simple roots (all the elements of k). Because of the main identity, the same is true for P: there exists distinct elements $\alpha_0, \ldots, \alpha_{n-1}$ such that $P(X) = \prod_{i=0}^{n-1}(X - \alpha_i)$ in $k[X]$. Consider then the morphism of rings

$$\begin{aligned} \psi : \mathbb{F}_p[X] &\to k \\ R &\mapsto R(\alpha_0). \end{aligned}$$

It vanishes on the ideal spanned by P, hence it descends to a morphism of fields between $\mathbb{F}_p[X]/(P)$ and k. This morphism is necessarily injective (morphism of fields), and it is also surjective by a cardinality argument, so it is an isomorphism. $\square$