1. Finite Fields

The first examples of finite fields are quotient fields of the ring of integers $\mathbb{Z}$: let $t > 1$ and define $\mathbb{Z}_{/t} = \mathbb{Z}/(t\mathbb{Z})$ to be the ring of congruence classes of integers modulo t: a and b are congruent modulo t when $t divides(a-b)$; in practical terms, we identify the classes with the remainders $\{0, 1, \cdots, t-1\}$ and define the sum and product modulo t. Then $\mathbb{Z}_t$ is a field iff t is a prime (see next paragraph). For a prime q, we denote this field by $\mathbb{F}_q$. Some general properties of these fields are necessarily shared by all finite fields. They are reviewed in the next sections.

1.1. The Additive structure of Finite Fields.

Let $\mathbb{F}$ be any finite field with sum $a+b$ and multiplication ab, for all $a, b \in \mathbb{F}$. There exist necessarily two distinct elements in $\mathbb{F}$, the 0 (defined as the unique element such that $0+a = a+0 = a$ for all $a \in \mathbb{F}$) and the 1 (defined as the unique element such that $1a = a1 = a$ for all $a \in \mathbb{F} \setminus \{0\}$). The multiplicative subgroup of non-zero elements of $\mathbb{F}$ is denoted by $\mathbb{F}^\times$.

There is a naturally defined homomorphism of rings from $\mathbb{Z}$ to $\mathbb{F}$

$$\psi : \mathbb{Z} \to \mathbb{F} : \psi(t) = t \cdot 1 = \begin{cases} \sum_{i=1}^{t} 1 & \text{if } t > 0 \\ -\sum_{i=1}^{-t} 1 & \text{if } t < 0 \\ 0 & \text{if } t = 0 \end{cases}$$

We denote $\psi(t)$ simply as t.

The kernel of ψ is an ideal $q\mathbb{Z} \subset \mathbb{Z}$, with $q > 0$ necessarily a prime, as otherwise, if $q = st$ with both $s > 1$ and $t > 1$, $0 = \psi(st) = \psi(s)\psi(t)$ and $\mathbb{F}$ would contain divisors of zero.

We conclude that there exists a injective homomorphism of $\mathbb{F}_q$ into $\mathbb{F}$ and, identifying $\mathbb{F}_q$ with its image, and we may consider $\mathbb{F}_q$ as a subfield of $\mathbb{F}$; it is called the **prime subfield** of $\mathbb{F}$ and q is the **characteristic** of $\mathbb{F}$.

This implies that $\mathbb{F}$ is a vector space over $\mathbb{F}_q$ of finite dimension m and so $|\mathbb{F}| = q^m$. This field is denoted as $\mathbb{F}_{q^m}$, a notation that hints, implicitly, to the fact that a finite field with that given cardinality is essentially unique. When there is no ambiguity, we will denote this field simply as $\mathbb{F}$, but will use systematically the notation $\mathbb{F}_q$ for the prime fields.

The vector space structure described above completely determines the additive structure of $\mathbb{F}$: it is isomorphic to a direct product of m copies of $\mathbb{F}_q$; given a basis $u_1, \cdots, u_m$, the elements of $\mathbb{F}$ may be identified with the corresponding vectors of coordinates with respect to that basis and sum is performed component wise.

1.2. Multiplicative structure: Orders and Primitive Elements.

Let again $\mathbb{F} = \mathbb{F}_{q^m}$. The understanding of the multiplicative structure of $\mathbb{F}$ starts with the following basic property

Proposition 1 (Fermat/Euler)**.** *For every $a \in \mathbb{F}^\times$, $a^{q^m-1} = 1$. An equivalent statement is that for every $a \in \mathbb{F}$ $a^{q^m} = a$.*

Proof. The equivalence of both statements is obvious. Suppose $a \neq 0$ and let the nonzero elements of the field be indexed as a_i, $1 \leq i < q^m$. The mapping

$$\mathbb{F}^\times \to \mathbb{F}^\times, \qquad a_i \to aa_i$$

is a bijection. So

$$a^{q^m-1}\prod_{i=1}^{q^m-1} a_i = \prod_{i=1}^{q^m-1} aa_i = \prod_{i=1}^{q^m-1} a_i,$$

which implies the result, because $\prod_{i=1}^{q^m-1} a_i \neq 0$. □

Definition 2. *For any $a \in \mathbb{F}^{\times}$, the order of a is defined as*

$$\mathrm{ord}(a) = \min\{k > 0 : a^k = 1\}.$$

Proposition 3. *For any $a, b \in \mathbb{F}^{\times}$,*

i) $\mathrm{ord}(a) \mid (q^m - 1)$;
ii) *if* $a^k = 1$ *then* $\mathrm{ord}(a) \mid k$;
iii) $\mathrm{ord}(a^j) = \frac{\mathrm{ord}(a)}{\gcd(j, \mathrm{ord}(a))}$;
iv) *If* $\mathrm{ord}(a) = s$, $\mathrm{ord}(b) = t$ *and* $\gcd(s, t) = 1$, *then* $\mathrm{ord}(ab) = st$.

Proof. **HW**. □

Remark 4. *The definition and properties of multiplicative order apply for elements of a general commutative finite group. In particular, given a positive integer m, we define, for any a prime to m,*

$$\mathrm{ord}_m(a) = \min\{k > 0 : a^k \equiv 1 \mod m\} = \min\{k > 0 : m \mid (a^k - 1)\}.$$

We now consider the problem of computing the number of elements in a finite field, with a given order. This will be the first application of Möbius Inversion formula; the necessary definitions and theorems are gathered in a section at the end of this file.
For each $t \mid (q^m - 1)$ let $o(t)$ denote the number of elements with order t in a field $\mathbb{F}_{q^m}$ and, for simplicity of notation, $n = q^m - 1$; obviously, $n = \sum_{t|n} o(t)$, and so, by Möbius Inversion formula,

$$o(t) = \sum_{d|t} \mu(d)\frac{t}{d},$$

i.e., $o(t) = \phi(t)$, Euler's function. In particular,

Proposition 5. *If $\mathbb{F} = \mathbb{F}_{q^m}$, there exist exactly $\phi(q^m - 1)$ elements $a \in \mathbb{F}^{\times}$ with order* $\mathrm{ord}(a) = q^m - 1$.

An $\alpha \in \mathbb{F}^{\times}$ with order $\mathrm{ord}(\alpha) = q^m - 1$ is called a **primitive element** or **primitive root** of the field.
The multiplicative structure of $\mathbb{F}$ is in this way completely determined: $\mathbb{F}^{\times}$ is a cyclic group (of order $q^m - 1$) $\{\alpha^i : 0 \leq i < q^m\}$.
When a primitive element α is known, multiplications in the field are turned into sums by means of a "table of logarithms": for any $c, d \in \mathbb{F}^{\times}$

$$cd = \alpha^s \alpha^t = \alpha^{s+t}.$$

Example 6. *2 is a primitive element of $\mathbb{F}_{11}$; the following table presents the correspondence between exponents $0 \leq j < 10$ in the first row and field elements 2^j in the second:*

0	1	2	3	4	5	6	7	8	9
1	2	4	8	5	10	9	7	3	6

The properties of the order imply that if α is a primitive element then α^j is primitive if and only if $\gcd(j, q^m - 1) = 1$.

In order to construct non-prime finite fields and to understand their properties, we need to consider in some detail polynomials in one variable.

1.3. **Polynomials over $\mathbb{F}$.** In this subsection $\mathbb{F}$ denotes a field, not necessarily finite. Denote by $\mathbb{F}[x]$ the ring and $\mathbb{F}$-vector space of polynomials (in a variable x) with coefficients in $\mathbb{F}$:

$$\mathbb{F}[x] = \{p(x) = \sum_{k \geq 0} a_k x^k \,|a_k \in \mathbb{F}; \exists M : a_k = 0 \forall k > M\}$$

If $a_m \neq 0$ and $a_k = 0\ \forall k > m$, $m = \deg(p(x))$ is the **degree** of $p(x)$;
if $m = \deg(p(x))$ and $a_m = 1$, $p(x)$ is **monic**. Obviously, for every nonzero polynomial $p(x) \in \mathbb{F}[x]$ there exists unique $a \in \mathbb{F}^\times$ and monic $g(x)$ such that $p(x) = ag(x)$.

The notation $p(x) = \sum_{k \geq 0} a_k x^k$ (with no explicit reference to the degree) simplifies the presentation of the formulas for algebraic operations:
If

$$f(x) = \sum_{k \geq 0} a_k x^k, \qquad g(x) = \sum_{k \geq 0} b_k x^k,$$

then

$$(f + g)(x) = \sum_{k \geq 0} (a_k + b_k) x^k,$$

$$f \cdot g(x) = \sum_{k \geq 0} \left(\sum_{j=0}^{k} a_j b_{k-j} \right) x^k;$$

the multiplication by a scalar $c \in \mathbb{F}$ is a particular case ($c \neq 0$ is a polynomial of degree 0):

$$cf(x) = \sum_{k \geq 0} (ca_k) x^k.$$

The well known division algorithm of polynomials shows that

Lemma 7. *For any $f(x), g(x) \in \mathbb{F}[x]$, with $g(x)$ not the zero polynomial, there exist unique polynomials $u(x)$ and $r(x)$ satisfying*

$$f(x) = u(x)g(x) + r(x), \qquad deg(r(x)) < deg(g(x)).$$

If $r(x) = 0$, we say that $g(x)$ divides $f(x)$: $g(x) \mid f(x)$.
On the basis of this division Lemma, an Euclidean algorithm is defined, giving rise to the proof of the existence of the $\gcd(f(x), g(x))$ of two nonzero polynomials, similarly to what happens in $\mathbb{Z}$. If

i) $h(x) \mid f(x), h(x) \mid g(x)$ and

ii) $(v(x) \mid f(x) \wedge v(x) \mid g(x)) \implies v(x) \mid h(x)$,

then also $ch(x)$ has the same property, for any $c \in \mathbb{F}^\times$. We thus define $\gcd(f(x), g(x))$ as the unique monic polynomial satisfying i) and ii).

Again as in $\mathbb{Z}$, there exist polynomials $u(x)$ and $v(x)$ such that

$$\gcd(f(x), g(x)) = u(x)f(x) + v(x)g(x),$$

that may be determined using the **extended Euclidean algorithm**: denoting $r_{-1}(x) = f(x)$ and $r_0(x) = g(x)$, the algorithm computes, applying the division algorithm, a sequence of remainders

$$r_{k+1}(x) = r_{k-1}(x) - q_{k+1}(x)r_k(x),$$

and a pair of sequences $u_k(x)$ and $v_k(x)$ satisfying

$$r_k(x) = u_k(x)f(x) + v_k(x)g(x);$$

by a simple computation and induction argument, it is easy to verify that these may be obtained by the initial conditions and recurrence relations

$$\begin{array}{lll} u_{-1}(x) = 1 & u_0(x) = 0 & u_{k+1}(x) = u_{k-1}(x) - q_{k+1}(x)u_k(x) \\ v_{-1}(x) = 0 & v_0(x) = 1 & v_{k+1}(x) = v_{k-1}(x) - q_{k+1}(x)v_k(x). \end{array}$$

Furthermore,

Lemma 8. *The quotients $q_k(x)$, remainders r_k and coefficients u_k and v_k obtained in the extended Euclidean algorithm applied to $f(x), g(x) in \mathbb{F}[x]$ satisfy, for all k,*

i) $u_k(x)v_{k+1}(x) - u_{k+1}(x)v_k(x) = (-1)^{k+1}$;
ii) $r_k(x)v_{k+1}(x) - r_{k+1}(x)v_k(x) = (-1)^{k+1}f(x)$;
iii) $r_{k+1}(x)u_k(x) - r_k(x)u_{k+1}(x) = (-1)^{k+1}g(x)$;
iv)
- $\deg(u_k(x)) = \sum_{i=2}^{k} \deg(q_i(x))$,
- $\deg(v_k(x)) = \sum_{i=1}^{k} \deg(q_i(x))$,
- $\deg(r_k(x)) = \deg(f(x)) - \sum_{i=1}^{k+1} \deg(q_i(x))$.

Proof. **(HW)**. □

Example 9. *Let $q = 13$ and*

$$f(x) = 7x^6 + 5x^4 + x + 2, \;\; g(x) = 4x^5 + 5x^3 + 3x^2 + 6.$$

The following table presents the simultaneous calculations for the sequence of remainders and of the polynomials $u_k(x)$ and $v_k(x)$:

r_i	q_i	u_i	v_i
$7x^6 + 5x^4 + x + 2$		1	0
$4x^5 + 5x^3 + 3x^2 + 6$		0	1
$6x^4 + 11x^3 + 10x + 2$	$5x$	1	$8x$
$4x^3 + 5x^2 + 8x + 7$	$5x + 6$	$8x + 7$	$12x^2 + 4x + 1$
$8x^2 + 12x + 4$	$8x + 9$	$x^2 + 2x + 3$	$8x^3 + 3x^2 + 3x + 4$
$x + 1$	$7x + 8$	$6x^3 + 4x^2 + 10x + 9$	$9x^4 + 6x^3 + 6x^2 + 4x + 8$
0	$8x + 4$	$4x^4 + 9x^3 + 9x^2 + 7x + 6$	$6x^5 + 7x^4 + x^3 + 12x^2 + x + 11$

We conclude that $d(x) \equiv x+1$ is the greatest common divisor of $f(x)$ and $g(x)$, in the ring $\mathbb{Z}_{/13}[x]$, and we have the equality

$$x+1 \equiv (6x^3+4x^2+10x+9)f(x)+(9x^4+6x^3+6x^2+4x+8)g(x).$$

Definition 10. *$f(x) \in \mathbb{F}[x]$ with positive degree is **irreducible** if $f(x) = g(x)h(x)$ implies that at least one of these factors is a constant (a degree 0 polynomial).*

Monic irreducible polynomials play the same role in $\mathbb{F}[x]$ that primes do in $\mathbb{Z}$. In particular,

Proposition 11. *If $f(x)$ is monic and irreducible, and $f(x) \mid g(x)h(x)$ then $f(x)$ divides one of the factors in the product.*

Proof. **HW**. □

And we have a version of the Fundamental Theorem of Arithmetic:

Theorem 12. *Each monic polynomial has a unique, up to order of the factors, decomposition as a product of monic irreducible polynomials.*

Proof. **HW**. □

Definition 13. *$a \in \mathbb{F}$ is called a root of $f(x) \in \mathbb{F}[x]$ if $f(a) = 0$ (considering $f(x)$ as a function on $\mathbb{F}$) or, equivalently, if $(x-a) \mid f(x)$.*

By induction on the degree, for instance, one proves that

Proposition 14. *If $deg(f(x)) = k > 0$ then $f(x)$ has no more than k roots (counted with multiplicity).*

Proof. **HW**. □

Remark 15. *An obvious corollary is that a degree k polynomial over a field has no more than k distinct roots. This corollary has an independent and almost immediate proof, which is left as an exercise also.*

Later we will study in detail the factorisation of polynomials over finite fields. For the moment, we notice an important special case:

Definition 16. *A polynomial $f(x) \in \mathbb{F}[x]$ is said to **split completely** if it decomposes as a product of distinct linear factors.*

Proposition 17. *If $\mathbb{F}$ is a field with q^m elements, the polynomial $x^{q^m} - x$ splits completely in $\mathbb{F}[x]$*

Proof. **HW**. □

1.4. **Finite Fields: extensions and inclusions.** The existence and explicit construction of finite fields other than the prime fields follows from the next proposition:

Proposition 18. *Let $\mathbb{F}_N$ be a finite field ($N = q^m$ with q prime) and $f(x) \in \mathbb{F}_N[x]$ be an irreducible polynomial of degree t. Then the quotient ring $\mathbb{F}_N[x]/(f(x))$ is a field F with N^t elements.*

Proof. **HW**. □

This field may be seen, in an informal way, as the set of polynomials with coefficients in $\mathbb{F}_N$ and degree less than t (the remainders upon division by $f(x)$), with the operations of sum and product done modulo $f(x)$.
It is more convenient to denote by a new symbol, say β, the congruence class of x in the quotient and identify $\mathbb{F}$ with $\mathbb{F}_N[\beta]$, the field obtained from $\mathbb{F}_N$ by adding the "new" element β; this new element satisfies $f(\beta) = 0$ and this equality determines the operations of sum and product: $1, \beta, \cdots, \beta^{t-1}$ is a basis of $\mathbb{F}$ over $\mathbb{F}_N$; given $a, b \in \mathbb{F}$

$$a = \sum_{i=0}^{t-1} s_i \beta^i, \; b = \sum_{i=0}^{t-1} t_i \beta^i \quad \text{with } a_i, b_i \in \mathbb{F}_N$$

the sum and product are obtained as the usual sum and product of the polynomial expressions; the product, which is a polynomial expression of degree less or equal than $2t - 2$ is then reduced to a linear combination of the powers β^i, $0 \le i < t$, by the repeated use of the equality $f(\beta) = 0$.
It should be noticed, however, that $\mathbb{F} = \mathbb{F}_N[\beta]$ does not imply that β is a primitive element of the field: take, for example, $\mathbb{F}_3[x]/(x^3 + x^2 + 2)$.

Remark 19. *This construction of the field $\mathbb{F}$ as a finite algebraic extension of $\mathbb{F}_N$, is no different from the maybe more familiar extensions of the rational field, such as $\mathbb{Q}[\sqrt{2}] \simeq \mathbb{Q}[x]/(x^2 - 2)$, which may appear "more natural" only because we consider, implicitely, $\mathbb{Q}$ as a subfield of the algebraically closed field $\mathbb{C}$, where $\sqrt{2}$ exists, so to speak. However, as in our case, that extension of the rationals is completely independent of this inclusion and is valid also inside other algebraic completions of $\mathbb{Q}$, such as the p-adic fields.*

Example 20. *The simplest of all non-trivial examples of this construction is the following: $x^2 + x + 1 \in \mathbb{F}_2[x]$ is irreducible. We may then represent $\mathbb{F} = \mathbb{F}_2[x]/(x^2 + x + 1)$ as $\mathbb{F} = \{0, 1, \beta, \beta + 1\}$. The sum and product tables are easily deduced: for instance $\beta(\beta + 1) = 1$, etc.*

Example 21. *We consider the field $\mathbb{F}_{27} \simeq \mathbb{F}_3[x]/(x^3 + 2x + 2)$ which can be identified with*

$$\mathbb{F}_3[\alpha] = \{a + b\alpha + c\alpha^2 : a, b, c \in \mathbb{F}_3\}$$

where α satisfies $\alpha^3 = \alpha + 1$.

For example,

$$\alpha(\alpha^2 + \alpha + 1) = \alpha^3 + \alpha^2 + \alpha = \alpha + 1 + \alpha^2 + \alpha = \alpha^2 + 2\alpha + 1.$$

To compute $(\alpha + 1)^{-1}$, we solve $(\alpha + 1)(a + b\alpha + c\alpha^2) = 1$.

$$(\alpha + 1)(a + b\alpha + c\alpha^2) = a + (a + b)\alpha + (b + c)\alpha^2 + c\alpha^3 =$$

$$= a + (a + b)\alpha + (b + c)\alpha^2 + c(\alpha + 1) = (a + c) + (a + b + c)\alpha + (b + c)\alpha^2$$

But

$$(a+c)+(a+b+c)\alpha+(b+c)\alpha^2 = 1 \Leftrightarrow \begin{cases} a+c=1 \\ a+b+c=0 \\ b+c=0 \end{cases}$$

So $(\alpha+1)^{-1} = 2\alpha+\alpha^2$.

The construction of finite extensions of $\mathbb{F}_N$ depends on the existence and knowledge of irreducible polynomials $f(x) \in \mathbb{F}_N[x]$. We will confirm later that there exist irreducible polynomials of any degree over any finite field $\mathbb{F}_N$.

We will now clarify what are the possible inclusions between finite fields. An essential tool is the following

Definition 22 (Frobenius automorphism)**.** *Given a finite field $\mathbb{F}_N$ and an extension $\mathbb{F}_{N^m}$, the Frobenius automorphism of the extension is the mapping*

$$\sigma : \mathbb{F}_{N^m} \to \mathbb{F}_{N^m}, \qquad \sigma(x) = x^N.$$

It satisfies

$$\sigma(x+y) = \sigma(x)+\sigma(y), \qquad \sigma(xy) = \sigma(x)\sigma(y),$$

and

$$\sigma(x) = x \Leftrightarrow x \in \mathbb{F}_N$$

Exercise 23. *Verify that σ has the stated properties. Hint: remember that $N = q^t$ for some prime q and that $\mathbb{F}_q \subset \mathbb{F}_N \subset \mathbb{F}_{N^m}$.*

Remark 24. *Only if we need to identify the extension for which the automorphism is defined, we use the more detailed notation $\sigma_{[\mathbb{F}_{N^m}:\mathbb{F}_N]}$.*

Remark 25. *The Frobenius automorphism of the extension of $\mathbb{F}_N$ by $\mathbb{F}_{N^m}$ induces an automorphism of the ring $\mathbb{F}_{N^m}[x]$, which we denote again by σ, by the formula*

$$\sigma\left(\sum_i a_i x^i\right) = \sum_i \sigma(a_i)x^i.$$

Exercise 26. *Verify that the mapping defined in the previous remark is a ring automorphism*

$$\sigma(g(x)+h(x)) = \sigma(g(x))+\sigma(h(x)), \qquad \sigma(g(x)h(x)) = \sigma(g(x))\sigma(h(x)),$$

and that $\sigma(g(x)) = g(x)$ if and only if $g(x) \in \mathbb{F}_N[x]$.

Proposition 27. *$\mathbb{F}_{q^m}$ contains a unique subfield $\mathbb{F}_{q^d}$ for each $d \mid m$ and these are the only subfields of $\mathbb{F}_{q^m}$.*

Proof. The theorem of Fermat-Euler shows that $x^{q^d}-x$, because it divides $x^{q^m}-x$, splits completely in $\mathbb{F}_{q^m}$ as a product of linear factors. Applying the Frobenius automorphism of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ confirms that the roots of that polynomial are a subfield.
The last statement is an immediate consequence of the properties of the order. $\square$

Example 28. *$x^4 + x^3 + 1 \in \mathbb{F}_2[x]$ is irreducible (**HW**: $x^2 + x + 1$ is the unique degree 2 irreducible polynomial in that ring). So we may define*

$$\mathbb{F}_{16} = \mathbb{F}_2[\lambda] \simeq \mathbb{F}_2[x]/(x^4 + x^3 + 1),$$

*and λ is in fact a primitive element of the field (**HW**). However, $\mathbb{F}_{16}$ is also an extension of $\mathbb{F}_4 = \mathbb{F}_2[\alpha]$ ($\alpha^2 = \alpha + 1$). In fact, the polynomial $f(x) = x^2 + \alpha x + \alpha \in \mathbb{F}_4[x]$ is irreducible, so*

$$\mathbb{F}_{16} =\simeq \mathbb{F}_4[x]/(f(x)).$$

*And it is easy to verify (**HW**) that the roots of $f(x)$ are also roots of $x^4 + x^3 + 1$.*

1.5. **factorisations of Polynomials.** We focus our study of finite fields on the problem of factorisation of polynomials, which is also essential for the applications to follow. This may be done, with advantage, in the framework of a general finite field $\mathbb{F}_N$ (where, of course, N is a prime power) and its extensions.

Given an irreducible polynomial $f(x) \in \mathbb{F}_N[x]$, with degree m, and the corresponding field $\mathbb{F}_N[\beta]$, as above, we have

Claim 29. *$f(x)$ **splits completely** over $\mathbb{F}_N[\beta]$, ie, it decomposes as the product of* distinct *degree* 1 *factors*

$$f(x) = \prod_{s=0}^{m-1} (x - \beta^{N^s}).$$

Proof. **HW**. **Hint:** Use the Frobenius automorphism. □

Proposition 30. *The roots of $f(x)$ have all the same order.*

Proof. Let $\mathrm{ord}(\beta) = d$; we have $\mathrm{ord}(\beta^{N^s}) = \frac{d}{\gcd(N^s, d)}$. But $d \mid (N^m - 1)$ and obviously $N^m - 1$ and N^s are coprime. □

As we will see now, $f(x) \mid (x^{N^m} - x)$:

Proposition 31. *If $h(x) \in \mathbb{F}_N[x]$ is irreducible and $deg(h(x)) = t$ then*

$$h(x) \mid (x^{N^m} - x) \text{ iff } t \mid m.$$

Proof. Let $\mathbb{F} = \mathbb{F}_N[x]/(h(x)) = \mathbb{F}_N[\beta]$ and consider the equality

$$x^{N^m} - x = u(x)h(x) + r(x),$$

with $deg(r(x)) < t$. Suppose first that $t \mid m$. We have that, for any $c \in \mathbb{F}$ and every $j > 0$, $c^{N^{tj}} = c$ (**HW**); in particular, $c^{N^m} = c$ for all $c \in \mathbb{F}$. This implies that the t distinct roots of $h(x)$ in $\mathbb{F}$ must also be roots of $r(x)$, which can happen only if $r(x) = 0$.
Conversely, suppose that $h(x) \mid (x^{N^m} - x)$; this implies that $\sigma^m(\beta) = \beta^{N^m} = \beta$. Let α be a primitive element of $\mathbb{F}$ (ie, an element of $\mathbb{F}$ with order $N^t - 1$); there exist

$v_l \in \mathbb{F}_N$, $0 \le l < t$, such that $\alpha = \sum_{l=0}^{t-1} v_l \beta^l$; applying the Frobenius automorphism again

$$\sigma^m(\alpha) = \sum_{l=0}^{t-1} v_l \sigma^m(\beta^l) = \sum_{l=0}^{t-1} v_l \beta^l = \alpha.$$

So $\alpha^{N^m-1} = 1$ and $(N^t - 1) \mid (N^m - 1)$, which can only happen if $t \mid m$ (**HW**). $\square$

Corollary 32. *In $\mathbb{F}_N[x]$, $x^{N^m} - x = \prod h(x)$ where the product runs over all irreducible polynomials with degree dividing m.*

1.5.1. *Order and degree of irreducible polynomials.* Define the order $o(f)$ of an irreducible polynomial $f(x) \in \mathbb{F}_N[x]$ as the order of any of its roots in $\mathbb{F}_{N^m} = \mathbb{F}_N[x]/(f(x))$.

Proposition 33. *Let $f(x) \in \mathbb{F}_N[x]$ be an irreducible polynomial with deg$(f(x)) = m$ and $o(f) = e$.*

a) $o(f) \mid N^m - 1$;
b) $f(x) \mid x^{o(f)} - 1$;
c) $o(f) \mid n \Leftrightarrow f(x) \mid (x^n - 1)$:

Proof. **HW**. $\square$

The order of $f(x)$ determines its degree:

Theorem 34. *Let $f(x) \in \mathbb{F}_N[x]$ be an irreducible polynomial with deg$(f(x)) = m$ and $o(f) = e$. Then $m = \mathrm{ord}_e(N)$, ie, m is the least positive integer satisfying $e \mid (N^m - 1)$.*

Proof. **HW**. $\square$

However, *deg*$(f(x))$ does not determine $o(f)$. Consider for example (**HW**) the polynomials over $\mathbb{F}_2$

$$f(x) = x^4 + x + 1, \qquad g(x) = x^4 + x^3 + x^2 + x + 1.$$

But it is possible to determine $o(f)$ in the following way: $o(f) \mid (N^m - 1)$ so, if $N^m - 1 = \prod_i p_i^{k_i}$ is the prime factor decomposition, we must have $o(f) = \prod_i p_i^{t_i}$ with $t_i \le k_i$; in fact,

$$t_i = k_i - \max\left\{ s : o(f) \mid \frac{N^m - 1}{p_i^s} \right\}.$$

By Proposition 32,

$$o(f) \mid \frac{N^m - 1}{p_i^s} \Leftrightarrow f(x) \mid \left(x^{\frac{N^m-1}{p_i^s}} - 1 \right),$$

and we may determine t_i by a sequence of polynomial divisions.

1.5.2. *Minimal polynomials.*

Definition 35. *Given $a \in \mathbb{F} = \mathbb{F}_{N^m}$, the* ***minimal polynomial*** *of a over $\mathbb{F}_N$ is the (unique) monic polynomial $p_a(x) \in \mathbb{F}_N[x]$ of minimum degree such that $p_a(a) = 0$.*

We state several properties of minimal polynomials:

Proposition 36.
1. *$p_a(x)$ exists and is unique;*
2. *$p_a(x)$ is irreducible;*
3. *If $p(x) \in \mathbb{F}_N[x]$ is a monic irreducible polynomial and $p(a) = 0$ for some $a \in \mathbb{F}$, then $p(x) = p_a(x)$;*
4. *$p_a(x) \mid x^{N^m} - x$ and so $deg(p_a(x)) \mid m$;*
5. *if α is a primitive element of $\mathbb{F}_{N^m}$ then $deg(p_\alpha(x)) = m$.*

Proof. The second part of 4. will be a consequence of a proposition in the next section. The proof of the other statements is left as an exercise. □

The first example of a minimal polynomial was already provided by the construction of $\mathbb{F} = \mathbb{F}_N[\beta] = \mathbb{F}_N[x]/(f(x))$ itself, as it is easily seen that $f(x)$ is the minimal polynomial of β (and of course of the other roots β^{N^s}). More generally, minimal polynomials of elements of $\mathbb{F}_{N^m}$ are exactly the irreducible polynomials with coefficients in $\mathbb{F}_N$ and degree dividing m.

Remark 37. *We notice that, as a consequence of 5. in the previous proposition, the construction of a finite field as the quotient of the polynomial ring $\mathbb{F}_N[x]$ by the ideal generated by a monic irreducible polynomial $f(x)$ of degree m gives rise to all possible finite fields $\mathbb{F}$ of cardinality N^m: suppose $\mathbb{F}$ is a finite extension of $\mathbb{F}_N$ and α a primitive element with minimal polynomial $p(x)$. Then $\mathbb{F} = \mathbb{F}_N[\alpha] \simeq \mathbb{F}_N[x]/(p(x))$.*

At this point, we may clarify the claim of uniqueness of finite fields:

Theorem 38. *Let q be a prime and $m \geq 1$. There exists a unique, up to isomorphism, field $\mathbb{F}_{q^m}$ with cardinality q^m.*

Proof. The existence of the field follows from the existence of an irreducible polynomial $f(x) \in \mathbb{F}_q[x]$ with degree m and will be confirmed later.
As to uniqueness, suppose that $f(x)$ and $g(x)$ are two irreducible polynomials of the same degree m. Let α be a primitive element of $\mathbb{F}_q[x]/(f(x))$ and $\mathbb{F}_q[x]/(g(x)) = \mathbb{F}_q[\beta]$. We have the decomposition into irreducible factors $x^{q^m-1} - 1 = \prod_i p_i(x)$, where the $p_i(x)$ are minimal polynomials of its roots. $g(x)$ divides $x^{q^m-1} - 1$, so we must have $g(x) = p_i(x)$ for some i, ie, $g(x)$ is the minimal polynomial of α^i for some i, ie, $\mathbb{F}_q[\beta] \simeq \mathbb{F}_q[\alpha^i] \subset \mathbb{F}_q[\alpha]$. But the two fields have the same cardinality so we have equality. □

1.5.3. *Counting Irreducible polynomials.* This will be an application of Möbius Inversion formula: denote the number of irreducible polynomials over $\mathbb{F}_N$, of degree m, by $I_N(m)$.
We saw before that $x^{N^m} - x$ factors over $\mathbb{F}_N$ as the product of all monic irreducible polynomials with degree dividing m; equating degrees, we have

$$N^m = \sum_{d|m} dI_N(d).$$

Möbius Inversion formula implies

Proposition 39. *Let N be a prime power. For any $m \in \mathbb{Z}^+$, the number of irreducible polynomials of degree m in $\_N[x]$ is*

$$I_N(m) = \frac{1}{m}\sum_{d|m} \mu(d)N^{m/d}.$$

In particular, $I_N(m) > 0$, thus assuring the existence of irreducible polynomials and so of field extensions of $\mathbb{F}_q$ of any given degree.

We end this section by answering the question of how does an irreducible polynomial over a finite field $\mathbb{F}_N$ factor in an extension of it.

Theorem 40. *Let $\mathbb{F}_N$ be a finite field and $\mathbb{F}_{N^n}$ an extension. Suppose $f(x) \in \mathbb{F}_N[x]$ is an irreducible polynomial with degree t and let $d = \gcd(t, n)$.*
Then $f(x)$ factors in $\mathbb{F}_{N^n}[x]$ as the product of d irreducible polynomials, each with degree t/d.
In particular, $f(x)$ remains irreducible over $\mathbb{F}_{N^n}$ if and only if $\gcd(t, n) = 1$.

Proof. Suppose that $g(x)$ is an irreducible factor of $f(x)$ in $\mathbb{F}_{N^n}[x]$ with degree s. It suffices to show that $s = t/d$.
First, notice that if $\mathbb{F}_{N^{ns}} = \mathbb{F}_{N^n}[x]/(g(x)) = \mathbb{F}_{N^n}[\alpha]$, ie, α is a root of $g(x)$ in $\mathbb{F}_{N^n}[x]/(g(x))$, then α is also a root of $f(x)$ and so $\mathbb{F}_{N^t} = \mathbb{F}_N[x]/(f(x)) = \mathbb{F}_N[\alpha]$ is a subfield of $\mathbb{F}_{N^{ns}} = \mathbb{F}_{N^n}[\alpha]$. In particular, $t \mid (ns)$ which implies $\frac{t}{d} \mid s$.
Now, let $u = \mathrm{ord}(f)$; this implies, by Theorem 38 above, that $t = \mathrm{ord}_u(N)$. But then α has order u, both as an element of $\mathbb{F}_N[x]/(f(x)) = \mathbb{F}_N[\alpha]$ and of $\mathbb{F}_{N^n}[x]/(g(x)) = \mathbb{F}_{N^n}[\alpha]$, implying that $s = \mathrm{ord}_u(N^n)$. But the properties of multiplicative order imply that

$$\mathrm{ord}_u(N^n) = \frac{\mathrm{ord}_u(N)}{\gcd(\mathrm{ord}_u(N), n)} = t/d.$$

□

1.5.4. *Cyclotomic cosets and Factorizaton.* Given a primitive element α of $\mathbb{F}_N$, we may compute the minimal polynomial $p_{\alpha^i}(x)$ (which we will denote now simply by $p_i(x)$) of any other nonzero element, using the notion of cyclotomic cosets:

Definition 41. *For any n co-prime to N, the **cyclotomic coset** of i modulo n, with respect to N, is*

$$C_i = \{iN^j \mod n : j \geq 0\};$$

in other words, C_i is the orbit of $i \in \mathbb{Z}_{/n}$ under the mapping

$$\mathbb{Z}_{/n} \to \mathbb{Z}_{/n} \; x \to xN.$$

Obviously, the cyclotomic cosets partition $\mathbb{Z}_{/n}$; $\{i_1, \cdots, i_s\}$ is called a **complete set of representatives** of cyclotomic cosets if $\{C_{i_1}, \cdots, C_{i_s}\}$ are a partition of $\mathbb{Z}_{/n}$.

Example 42. *The cyclotomic cosets modulo* 26 *with respect to* 3 *are*

$$\{0\},\ \{1,3,9\},\ \{2,6,18\},\ \{4,12,10\},\ \{5,15,19\},$$
$$\{7,21,11\},\ \{8,24,20\},\ \{13\}, \{14,16,22\}, \{17,25,23\}.$$

The cyclotomic cosets modulo 16 *with respect to* 3 *are*

$$\{0\},\ \{1,3,9,11\},\ \{2,6\},\ \{4,12\},\ \{5,15,13,7\},\ \{8\},\ \{10,14\}.$$

The cyclotomic cosets modulo 13 *with respect to* 4 *are*

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

Remark 43. *The elements in each cyclotomic coset are written in the order they "appear" in the orbit of the mapping, but that is irrelevant for the definition and use of the cosets.*

Remark 44. *Let m be the order of N in $\mathbb{Z}^{\times}_{/n}$, ie m, the minimal positive integer such that $n \mid (N^m - 1)$. If C_i is the cyclotomic coset of i modulo n, with respect to N, it is clear that $|C_i| = u$ where u is the least positive integer such that*

$$i(N^u - 1) \equiv 0 \mod n;$$

it follows that $|C_i| = m$ if $\gcd(i, n) = 1$; on the other hand, if $\gcd(i, n) = v > 1$ and $n_1 = n/v$, then we get from the same equation that $|C_i| = p$ where p is the order of N in $\mathbb{Z}_{n_1}$ and so, in any case, $p \mid m$.
Also, if C is the cyclotomic polynomial modulo n with respect to N, containing i, and $|C| = k$, it is easy to see that the cyclotomic coset C_1 modulo n with respect to N^j, containing i, has k/d elements, where $d = \gcd(k, j)$.
In fact, cyclotomic cosets modulo n, with respect to N, are nothing but cycles of a permutation of $\{0, 1, \cdots, n-1\}$ (the one induced by multiplication by N), and all the properties stated above generalise to this situation.

The next theorem generalizes the factorisation of $f(x)$ in $\mathbb{F}_N[x]/(f(x))$ identified before:

Theorem 45. *Let α be a primitive element of $\mathbb{F}_{N^m}$. The minimal polynomial of α^i over $\mathbb{F}_N$ is*

$$p_i(x) = \prod_{j \in C_i} (x - \alpha^j),$$

where C_i is the cyclotomic coset of i modulo $N^m - 1$, with respect to N.

Proof. α^i is obviously a root of the given polynomial. We verify, with the help of the Frobenius automorphism, that

$p_i(x) \in \mathbb{F}_N[x]$;
$p_i(x)$ has no multiple roots;
any polynomial $f(x)$ that has α^i as a root is divisible by $p_i(x)$.

□

The details of the proof are left as an exercise (**HW**).

Corollary 46. *Let α be a primitive element of $\mathbb{F}_{q^m}$ and $\{i_1, \cdots, i_r\}$ a complete set of representatives of the cyclotomic cosets modulo $q^m - 1$, with respect to q. Then*

$$x^{q^m-1} - 1 = \prod_{k=1}^{r} p_{i_k}(x).$$

Example 47. *$p(x) = x^3 + 2x + 1$ is irreducible over $\mathbb{F}_3$, so we may take $\mathbb{F}_{27}$ to be $\mathbb{F}_3[\alpha]$ where α is a root of $p(x)$. It turns out that α is also a primitive element. The following table gives the correspondence between powers of α and the expression of the same element on the basis $1, \alpha, \alpha^2$:*

0	1	9	$\alpha+1$	18	$\alpha^2+2\alpha+1$
1	α	10	$\alpha^2+\alpha$	19	$2\alpha^2+2\alpha+2$
2	α^2	11	$\alpha^2+\alpha+2$	20	$2\alpha^2+\alpha+1$
3	$\alpha+2$	12	α^2+2	21	α^2+1
4	$\alpha^2+2\alpha$	13	2	22	$2\alpha+2$
5	$2\alpha^2+\alpha+2$	14	2α	23	$2\alpha^2+2\alpha$
6	$\alpha^2+\alpha+1$	15	$2\alpha^2$	24	$2\alpha^2+2\alpha+1$
7	$\alpha^2+2\alpha+2$	16	$2\alpha+1$	25	$2\alpha^2+1$
8	$2\alpha^2+2$	17	$2\alpha^2+\alpha$		

The cyclotomic cosets found before allow us to factor $x^{26} - 1$ over $\mathbb{F}_3$:

$$\begin{array}{rl}
\{0\} & x-1 \\
\{1,3,9\} & (x-\alpha)(x-\alpha^3)(x-\alpha^9) = x^3+2x+1 \\
\{2,6,18\} & (x-\alpha^2)(x-\alpha^6)(x-\alpha^{18}) = x^3+x^2+x+2 \\
\{4,12,10\} & (x-\alpha^4)(x-\alpha^{12})(x-\alpha^{10}) = x^3+x^2+2 \\
\{5,15,19\} & (x-\alpha^5)(x-\alpha^{15})(x-\alpha^{19}) = x^3+2x^2+x+1 \\
\cdots & \cdots
\end{array}$$

Example 48 (Example 28 continued)**.** *Computing cyclotomic cosets modulo 15, with respect to 2, and using λ as a primitive element of $\mathbb{F}_{16}$, we know that*

$$x^4 + x^3 + 1 = (x-\lambda)(x-\lambda^2)(x-\lambda^4)(x-\lambda^8);$$

cyclotomic cosets modulo 15, with respect to 4 show that over $\mathbb{F}_4$

$$x^4 + x^3 + 1 = f_1(x) f_2(x), \qquad f_1(x) = (x-\lambda)(x-\lambda^4), \qquad f_2 = (x-\lambda^2)(x-\lambda^8);$$

now

$$f_1(x) = x^2 + (\lambda + \lambda^4)x + \lambda^5 = x^2 + \lambda^5 x + \lambda^5$$

and

$$f_2(x) = x^2 + (\lambda^2 + \lambda^8)x + \lambda^{10} = x^2 + \lambda^{10} x + \lambda^{10},$$

confirming that λ^5 and λ^{10}, being the two elements with order 3, are α and α^2.

Remark 49. *Notice that there is no intrinsic way to decide between the possibilities $\lambda^5 = \alpha$ and $\lambda^5 = \alpha^2$.*

1.5.5. *Roots of unity and factorisation of $x^n - 1$.*

Definition 50. *An element $a \in \mathbb{F}^\times$ is a n-root of unity if $a^n = 1$ and a primitive n-root of unity if $ord(a) = n$.*

The following facts are an easily verified (**HW**) consequence of the definition and of the multiplicative structure of finite fields:

- If $\mathbb{F} = \mathbb{F}_{q^m}$ then the multiplicative group $\mathbb{F}^\times$ contains as a subgroup the n-roots of unity if and only if $n \mid (q^m - 1)$. In particular, $\gcd(n, q) = 1$;.
- If $n = q^t u$ with $\gcd(u, q) = 1$, a n-root of unity in $\mathbb{F}$ is also a u-root of unity.
- The smallest extension of $\mathbb{F}_q$ containing the n-roots of unity is $\mathbb{F}_{q^m}$ with $m = \mathrm{ord}_n(q)$. If β is a primitive element (ie a primitive $q^m - 1$ root of unity) the primitive n-roots of unity are (**HW**)
$$\{\beta^k | k = \frac{q^m - 1}{n} t; 1 \leq t < n; \gcd(t, n) = 1\}.$$
- Let $m = \mathrm{ord}_n(q)$; if $N = q^s$, and $\gcd(m, s) = d$. Then $\mathrm{ord}_n(N) = m/d$ and so the extensions of $\mathbb{F}_N$ containing the group of n-roots of unit are $\mathbb{F}_{N^t}$ for t a multiple of m/d.

For the applications of finite fields to coding theory it is essential to know the factorisation, over some $\mathbb{F}$, of the polynomials $x^n - 1$. The case $n = N^t - 1$ was dealt with in theorem 45, generalised in the following

Theorem 51. *Suppose that $\gcd(N, n) = 1$, t is the order of N in $\mathbb{Z}_n^\times$, and $k = \frac{N^t - 1}{n}$. Let α be a primitive element of $\mathbb{F}_{N^t}$.*
Then, if $\{C_1, \cdots, C_r\}$ denote the cyclotomic cosets modulo n, with respect to N, with representatives $a_i, \cdots, a_r$, the following factorisation holds in $F_N[x]$:
$$x^n - 1 = \prod_{i=1}^{r} p_{ki}(x),$$
where $p_{ki}(x)$ is the minimal polynomial of α^{ki}, ie,
$$p_{ki}(x) = \prod_{j \in C_i} (x - \alpha^{kj}).$$

Proof. Being a factor of $x^{N^t - 1} - 1$, the polynomial $x^n - 1$ is, by Theorem 45, a product of irreducible polynomials $p_i(x)$, each one corresponding to a cyclotomic coset modulo $N^t - 1$, with respect to N:
$$p_i(x) = \prod_{j \in C_i} (x - \alpha^j);$$
α^j is a n-root of unit if and only if $k \mid j$, and this property is shared by all elements of a cyclotomic coset.
Classes modulo $N^t - 1$, that are multiples of k are in bijection, through division by k, with classes modulo n, and this bijection preserves multiplication by N, ie, under this bijection cyclotomic cosets modulo $N^t - 1$ are mapped to cyclotomic cosets modulo n, both with respect to N. $\square$

The details of this proof are left as an exercise (**HW**); the following examples illustrate the application of the theorem.

Example 52. *Consider the polynomial* $x^{16} - 1 \in \mathbb{F}_3[x]$*; a complete system of representatives for the cyclotomic cosets modulo* 16*, with respect to* $q = 3$*, was obtained above:* $\{0, 1, 2, 4, 5, 8, 10\}$*. As* $3^4 - 1 = 16 \times 5$*, we must use a primitive element* α *of* $\mathbb{F}_{81}$*.*
Define $\mathbb{F}_{81} = \mathbb{F}_3[x]/(x^4 + x + 2) = \mathbb{F}_3[\alpha]$*. By the previous theorem, we have the factorisation*

$$x^{16} - 1 = p_0(x)p_5(x)p_{10}(x)p_{20}(x)p_{25}(x)p_{40}(x)p_{50}(x),$$

where $p_l(x)$ *denotes the minimal polynomial of* α^l*; for instance,*

$$p_0(x) = (x - \alpha^0) = x - 1$$

while

$$p_{10}(x) = (x - \alpha^{10})(x - \alpha^{30}) = x^2 - (\alpha^{10} + \alpha^{30})x + \alpha^{40} = x^2 + x + 2$$

*The computation of the other factors is left as an exercise (**HW**).*

Example 53. *Factorisation of* $x^9 - 1$ *over* $\mathbb{F}_4 = \mathbb{F}_2[\alpha]$*. The cyclotomic cosets modulo* 9*, with respect to* 4*, are*

$$(0), (1, 4, 7), (2, 8, 5), (3), (6);$$

so $\mathrm{ord}_9(4) = 3$ *and* $\frac{4^3-1}{9} = 7$*. We find that, using a notation similar to the one in the previous example,*

$$x^9 - 1 = p_0(x)p_7(x)p_{14}(x)p_{21}(x)p_{42}(x),$$

where

$$p_0(x) = x - 1; \qquad p_7(x) = (x - \lambda^7)(x - \lambda^{28})(x - \lambda^{49});$$

$$p_{14}(x) = (x - \lambda^{14})(x - \lambda^{56})(x - \lambda^{35}); \qquad p_{21}(x) = x - \lambda^{21}; \qquad p_{42}(x) = x - \lambda^{42},$$

and λ *is a primitive element of* $\mathbb{F}_{64}$*.*
The polynomial $f(x) = x^3 + \alpha x^2 + \alpha^2 x + \alpha$ *is irreducible over* $\mathbb{F}_4$ *and in* $\mathbb{F}_4[x]/(f(x)) \simeq \mathbb{F}_4[\lambda] = \mathbb{F}_{64}$ λ *is a primitive element. We find then that*

$$p_7(x) = x^3 + \alpha, \qquad p_{14}(x) = x^3 + \alpha^2, \qquad p_{21}(x) = x + \alpha, \qquad p_{42}(x) = x + \alpha^2.$$

The method of cyclotomic cosets to factor polynomials $x^n - 1$, with $n \mid (N^m - 1)$ into irreducible factors (which are minimal polynomials of their roots) has the disadvantage of depending on computations involving a primitive element of the extension field. This disadvantage is stressed by the fact that there is no general method to find primitive elements, even for prime fields.
The next two subsections are devoted to the application of other mathematical concepts and theories to the problem of determining irreducible polynomials.

1.5.6. *Cyclotomic Polynomials.* It is possible to obtain partial factorisations of $x^n - 1$ working only in $\mathbb{F}_q[x]$ using the theory of cyclotomic polynomials.
Let $\mathbb{F}$ be any field containing the group of n-th roots of unity, or more precisely an isomorphic copy of it. This may be $\mathbb{C}$ but it may also be $\mathbb{F}_{q^m}$ for m such that $n \mid q^m - 1$.

Definition 54. *Let $n \mid (q^m - 1)$. The n-th cyclotomic polynomial over $\mathbb{F}_{q^m}$ is defined as $\Phi_n(x) = \prod_{a:\mathrm{ord}(a)=n}(x - a)$.*

Although our definition depends on the extension field containing the n-roots of unity, we'll see that the cyclotomic polynomials do not depend on that choice. We start with the following result:

Theorem 55. *$\Phi_n(x) \in \mathbb{F}_q[x]$ and its degree is $\phi(n)$. Moreover $x^n - 1 = \prod_{d|n} \Phi_d(x)$.*

Proof. **HW**. □

The same argument used in the proof of the second version of Möbius Inversion Formula gives us an explicit formula for the cyclotomic polynomials:

Proposition 56. *For $n \in \mathbb{Z}^+$,*

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

Proof. **HW**. □

This formula implies that the cyclotomic polynomials have rational coefficients. The following classical result, stated here without proof, shows they in fact $\Phi_n(x) \in \mathbb{Z}[x]$:

Lemma 57 (Gauss)**.** *Suppose that $f(x), g(x) \in \mathbb{Q}[x]$ and that $f\dot{g}(x) \in \mathbb{Z}[x]$. Then $f(x), g(x) \in \mathbb{Z}[x]$.*

Corollary 58. *For every $n \in \mathbb{Z}+$, $\Phi_n(x) \in \mathbb{Z}[x]$.*

Proof. (**HW**) **Hint**: use induction. □

As a consequence, we have

Lemma 59. *Let p be prime and $n, k \in \mathbb{Z}+$. Then*

1. $\Phi_{pn}(x) = \begin{cases} \Phi_n(x^p) \ \textit{if } p \mid n \\ \frac{\Phi_n(x^p)}{\Phi_n(x)} \ \textit{if } p \nmid n \end{cases}$
2. $\Phi_{p^k n}(x) = \begin{cases} \Phi_n(x^{p^k}) \ \textit{if } p \mid n \\ \frac{\Phi_n(x^{p^k})}{\Phi_n(x^{p^{k-1}})} \ \textit{if } p \nmid n \end{cases}$

Proof. **HW**. **Hint:** In 1. apply the Inversion Formula for cyclotomic polynomials. In the case $p \mid n$, notice that if $d \mid pn$ then either $d \mid n$ or $d \nmid n$ and $p^2 \mid d$; in the case $p \nmid n$, notice that the divisors of pn are either divisors of n or of the for pd with $d \mid n$.
2. is a easy consequence of 1. □

We have also the following theorem, which we state without proof:

Theorem 60. *For $n \in \mathbb{Z}^+$, $\Phi_n(x)$ is irreducible over $\mathbb{Z}$.*

However, the cyclotomic polynomials $\Phi_n(x)$ are not, in general, irreducible over $\mathbb{F}_q$: consider, for example, the case $n = q^m - 1$; then, assuming that α is a primitive element in $\mathbb{F} = \mathbb{F}_{q^m}$, we have the factorisation

$$\Phi_n(x) = \prod_{0<i<q^m-1;\gcd(i,q^m-1)=1} (x - \alpha^i);$$

but the minimal polynomial of each of these α^i over $\mathbb{F}_q$ has degree m. We conclude that, over this field, $\Phi_{q^m-1}(x)$ factors as a product of degree m irreducible polynomials.
But the fact that a degree m irreducible polynomial $f(x) \in \mathbb{F}_q[x]$ totally splits in $\mathbb{F}_{q^m}$ (or in any extension field containing it) and that all its roots have the same order, implies that if $f(x)$ is a factor of some $x^n - 1$ then it must be a factor of one of the cyclotomic polynomials $\Phi_d(x)$ with $d \mid n$.

1.5.7. *Minimal polynomials by Linear Algebra.* A Linear Algebra approach to the computation of irreducible polynomials over finite fields is as follows: let $\alpha \in \mathbb{F}_q[\beta] = \mathbb{F}_q[x]/(f(x))$, where $f(x)$ is an irreducible polynomial of degree m. As it was seen above, $1, \beta, \cdots, \beta^{m-1}$ is a basis of the $\mathbb{F}_q$ vector space $\mathbb{F}_q[\beta]$. In particular, we have a matrix M such that

$$(1, \alpha, \alpha^2, \cdots, \alpha^m) = (1, \beta, \cdots, \beta^{m-1})M.$$

It is then clear (**HW**) that a polynomial $p(x) = \sum_{i=0}^m a_i x^i \in \mathbb{F}_q[x]$ satisfies $p(\alpha) = 0$ if and only if

$$M \begin{pmatrix} a_0 \\ \vdots \\ a_m \end{pmatrix} = 0.$$

So to find the minimal polynomial of α corresponds to determine the solution $(a_0, \cdots, a_m)^t$ of this last equation such that there exists k for which $a_k = 1$, $a_i = 0$ for $i > k$, with k minimal. This can be done applying row-reduction to M, obtaining a matrix of the form

$$\begin{bmatrix} I & U \\ 0 & V \end{bmatrix}$$

Nwhere I is the k-dimensional identity matrix, and the first column of U is nonzero. The solution wanted is then easily obtained (**HW**).

Exercise 61. *Let $\mathbb{F}_3[\beta]$ be defined by $\beta^3 = \beta + 2$, and $\alpha = \beta^2 + \beta + 2$. Compute the minimal polynomial of α by the method described in this subsection.*
In an example above, it was seen, by a direct computation, that β (denoted as α in that example) is in fact a primitive element of the field. Use the table given there and the rsults about cyclotomic cosets to confirm the result.

1.5.8. *Rabin's Criterion for Irreducibility.* Although the results in previous sections may help in identifying irreducibility, they do not provide a general criterion and/or method. One such criterion was proposed by Rabin:

Proposition 62. *Let $f(x) \in \mathbb{F}_N[x]$ be a degree m polynomial, $\{p_1, \cdots, p_t\}$ the primes dividing m, and $m_i = \frac{m}{p_i}$. Then $f(x)$ is irreducible if and only if*

i) $f(x) \mid (x^{N^m} - x)$;
ii) *For all* $1 \leq i \leq t$, $\gcd(f(x), x^{N^{m_i}} - x) = 1$.

Proof. Suppose $f(x)$ is irreducible; then it obviously satisfies i) and ii) (**HW**). Suppose, on the other hand that $f(x)$ satisfies i) and ii). Then, by Fermat-Euler Theorem, $f(x)$ totally splits in $\mathbb{F}_{N^m}$; if $f(x)$ has an irreducible factor $g(x)$ with degree $n < m$ then $\mathbb{F}_{N^n} = \mathbb{F}_N[x]/(g(x))$ is a subfield of $\mathbb{F}_{N^m}$ and so $n \mid m$. But then $n \mid m_i$ for some $1 \leq i \leq t$; this would imply $\mathbb{F}_{N^n} \subset \mathbb{F}_{N^{m_i}}$ and in particular $g(x) \mid \gcd(f(x), x^{N^{m_i}} - x)$, contradicting ii).
The details of the argument are left as an exercise (**HW**). $\square$

1.6. **Automorphisms, Norm and Trace.** This subsection collects some basic results on the group of automorphisms of an extension F_{N^m} of a prime field $\mathbb{F}_N$ and on the Norm and Trace maps associated to it. Many details are left as an exercise.

Recall that a map $\tau : F_{N^m} \to F_{N^m}$ is an automorphism if it is a bijection satisfying

$$\tau(x+y) = \tau(x) + \tau(y), \qquad \tau(xy) = \tau(x)\tau(y), \qquad \forall x, y \in \mathbb{F}_{N^m}.$$

Definition 63. *$Gal(F_{N^m}/\mathbb{F}_N)$ denotes the group of automorphisms of F_{N^m} that leave the points of $\mathbb{F}_N$ fixed.*

As we saw above, an example of such an automorphism is the Frobenius automorphism σ. We will see that in fact $Gal(F_{N^m}/\mathbb{F}_N) = \{\sigma^k : 0 \leq k < m\}$, where, of course, σ^k denotes de k-fold composition of σ.

By definition, each $\varphi \in Gal(F_{N^m}/\mathbb{F}_N)$ is a linear invertible transformation of F_{N^m}, as a vector space over $\mathbb{F}_N$ (**HW**). The set $L(F_{N^m})$ of all $\mathbb{F}_N$-linear transformations of F_{N^m} is also a vector space over F_{N^m}, and we have

Lemma 64. *The automorphisms in $Gal(F_{N^m}/\mathbb{F}_N)$ are linearly independent over $\mathbb{F}_{N^m}$ (as elements of $L(F_{N^m})$).*

Proof. Assume $\varphi_1, \cdots, \varphi_r \in Gal(F_{N^m}/\mathbb{F}_N)$ and $a_1, \cdots, a_r \in \mathbb{F}_{N^m}^{\times}$. are such that

$$a_1\varphi_1 + \cdots + a_r\varphi_r = 0$$

is a shortest nontrivial linear relation. Obviously $r > 1$ and the φ_i are all distinct. Let $x \in \mathbb{F}_{N^m}$ be some element such that $\varphi_1(x) \neq \varphi_2(x)$. Then, for any $y \in \mathbb{F}_{N^m}$,

$$\sum_{i=1}^{r} a_i\varphi_i(xy) = \sum_{i=1}^{r} a_i\varphi_i(x)\varphi_i(y) = 0$$

which implies that $\sum_{i=1}^{r} a_i\varphi_i(x)\varphi_i = 0$ is also a linear relation. But then

$$\sum_{i=2}^{r} a_i(\varphi_i(x) - \varphi_1(x))\varphi_i = 0$$

is a shorter linear relation, a contradiction. $\square$

As a consequence,

Lemma 65. *$Gal(F_{N^m}/\mathbb{F}_N)$ contains at most m elements.*

Proof. Suppose that this is not the case and let $\varphi_1, \cdots, \varphi_n$ be distinct elements of $Gal(F_{N^m}/\mathbb{F}_N)$, with $n > m$. If $v_1, \cdots, v_m$ is a basis of $\mathbb{F}_{N^m}$ over $\mathbb{F}_N$, then the system of m linear equations (over $\mathbb{F}_{N^m}$) in n variables

$$\begin{pmatrix} \varphi_1(v_1) & \varphi_2(v_1) & \cdots & \varphi_n(v_1) \\ \vdots & \vdots & \ddots & \vdots \\ \varphi_1(v_m) & \varphi_2(v_m) & \cdots & \varphi_n(v_m) \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

must have a nontrivial solution $(a_1, \cdots, a_n)$. This implies that $\sum_{i=1}^n a_i \varphi_i(y) = 0$, for any $y \in \mathbb{F}_{N^m}$, ie, the automorphisms φ_i are linearly dependent, contradicting the result in the previous lemma. $\square$

Corollary 66. *$Gal(F_{N^m}/\mathbb{F}_N) = \{\sigma^k : 0 \le k < m\}$, where σ is the Frobenius automorphism*

$$\sigma : \mathbb{F}_{N^m} \to \mathbb{F}_{N^m}, \qquad \sigma(x) = x^N.$$

The norm and trace maps associated to the extension are fundamental in the theory of finite fields and will play also a role in the applications to coding.
Their definition and main properties are listed in the propositions below.

Proposition 67. *The **Trace** map, defined by*

$$Tr(a) = \sum_{j=0}^{m-1} a^{N^j} = \sum_{j=0}^{m-1} \sigma^j(a),$$

satisfies

i) $Tr(a) \in \mathbb{F}_N \ \forall a \in \mathbb{F}_{N^m}$;
ii) $Tr(a+b) = Tr(a) + Tr(b) \ \forall a, b \in \mathbb{F}_{N^m}$;
iii) $Tr(ta) = tTr(a) \ \forall t \in \mathbb{F}_N, \ \forall a \in \mathbb{F}_{N^m}$;
iv) *For each* $t \in \mathbb{F}_N$, $Tr(x) = t$ *has* N^{m-1} *distinct solutions.*
v) $Tr(x) = 0 \Leftrightarrow x = y - y^N$, *for some* $y \in \mathbb{F}_{N^m}$.

Proof. (**HW**). $\square$

In other words, Tr is a surjective linear mapping from the $\mathbb{F}_N$-vector space $\mathbb{F}_{N^m}$ to $\mathbb{F}_N$, with kernel

$$y - y^N : y \in \mathbb{F}_{N^m}.$$

Proposition 68. *The **Norm** map, defined by*

$$N(a) = \prod_{j=0}^{m-1} \sigma^j(a), \qquad \forall$$

is a surjective homomorphism from $\mathbb{F}_{N^m}^\times$ to $\mathbb{F}_N^\times$ (both multiplicative groups) with kernel

$$\{\frac{x}{\sigma(x)} : x \in \mathbb{F}_{N^m}^\times\}.$$

Proof. (**HW**). $\square$

Definition 69. *A function $f : \mathbb{N} \to \mathbb{C}$ is* ***multiplicative*** *if $f(mn) = f(m)f(n)$ for any* coprime *integers m and n.*

Proposition 70. *If $f : \mathbb{N} \to \mathbb{C}$ is a multiplicative function, then*

$$F : \mathbb{N} \to \mathbb{C}, \qquad F(n) = \sum_{d|n} f(d)$$

is also multiplicative.

Proof. **HW**. □

A basic example of a multiplicative function is $d(n)$, the number of positive divisors of n (**HW**). Another one is Euler's *phi* function, defined, for any positive integer n, as the number of $0 < k < n$ that are co-prime to n.

Definition 71 (Möbius Function)**.** *The Möbius function $\mu : \mathbb{N} \to \{-1, 0, 1\}$ is defined as*

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ (-1)^k & \text{if } n \text{ is squarefree with } k \text{ distinct prime factors} \\ 0 & \text{otherwise} \end{cases}$$

The function μ is obviously multiplicative and it satisfies the following

Theorem 72. *For any $n \in \mathbb{N}$*

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise} \end{cases}$$

Proof. For $n = 1$ the result is obvious. Suppose that $n > 1$ and, if n has the prime factorisation $n = \prod_{i=1}^{t} p_i^{k_i}$ (with $k_i > 0$), define $rad(n) = \prod_{i=1}^{t} p_i$. It is clear

$$\sum_{d|n} \mu(d) = \sum_{d|rad(n)} \mu(d)$$

as for other divisors of n the corresponding summand is zero by definition. This sum may be written, taking the number of factor primes of d as a parameter, as

$$\sum_{d|rad(n)} \mu(d) = \sum_{j=0}^{t} \binom{t}{j} (-1)^j = 0$$

by Newton's Binomial formula. □

The main property of the Möbius function is expressed in the following fundamental result:

Theorem 73 (Möbius Inversion Formula)**.** *Given $f : \mathbb{N} \to \mathbb{N}$,*

$$F(n) = \sum_{d|n} f(d) \Leftrightarrow f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right).$$

Proof. The proof consists in a straightforward computation:

$$\sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \sum_{t|n/d} f(t) = \sum_{t|n} f(t) \sum_{d|n/t} \mu(d) = f(n)$$

as a consequence of the previous theorem.
The converse is proved in the same way. □

Reciprocally,

Theorem 74. *If $f(n) = \sum_{d|n} \mu(d) F(n/d)$ for every positive integer n, then $F(n) = \sum_{d|n} f(d)$.*

Proof. **HW**. □

Example 75. *It is easy to see that Euler's function satisfies, for any n,*

$$n = \sum_{d|n} \phi(d) :$$

if we denote by $s(d)$ the set of numbers $0 < k \leq n$ such that $gcd(n, k) = d$ it is obvious that these sets partition $\{1, \cdots, n\}$; moreover, $k \in s(d)$ if and only if $k = jd$ for some j satisfying $1 \leq j \leq n/d$ and $gcd(j, n/d) = 1$, the number of these j is exactly $\phi(n/d)$ and we obtain a different formulation of the equality.
Now the Inversion Formula implies

$$\phi(n) = \sum_{d|n} \mu(d) \frac{n}{d} = n \sum_{d|n} \frac{\mu(d)}{d},$$

and, as the function in the sum is multiplicative, we recover the fact that ϕ is also multiplicative. Also, if $rad(n) = \prod i = 1^t p_i$, the properties of Möbius function give

$$\phi(n) = n \sum_{d|rad(n)} \frac{\mu(d)}{d} = n \sum_{j=0}^{t} (-1)^j \sum_{d} \frac{1}{d},$$

where the inner sum is over the divisors d of $rad(n)$ with j prime factors. This is equal to

$$\phi(n) = n \prod_{i=1}^{t} (1 - 1/p_i) ;$$

if $n = \prod_{i=1}^{t} p_i^{k_i}$, this formula may be written as

$$\phi(n) = \prod_{i=1}^{t} \left(p_i^{k_i} - p_i^{k_i - 1}\right),$$

an expression that can be obtained directly from the knowledge that phi is multiplicative.

A similar argument proves

Theorem 76. *Given $f : \mathbb{N} \to \mathbb{N}$,*

$$F(n) = \prod_{d|n} f(d) \Leftrightarrow f(n) = \prod_{d|n} \left(F\left(\frac{n}{d}\right)\right)^{\mu(d)}.$$

Proof. **HW**. □

The inversion formula is used to disclose several relations between arithmetic functions and is used frequently in these notes.

2.1. **Supplementary Results and Problems.**

Lemma 77. *For any $a, u, v > 1$, $\gcd(a^u - 1, a^v - 1) = a^{\gcd(u,v)} - 1$.*

Proof. **HW**. **Hint:** Assume $u \leq v$ and $v = tu + r$; find the expression of the remainder of the division of $a^v - 1$ by $a^u - 1$ and analise the application of Euclides's algorithm to the two pairs of integers □

Problem 78. *Find a primitive element and construct a logarithmic table for (some isomorphic copy of) $\mathbb{F}_{25}$.*

Problem 79. *Find the irreducible factors of $x^{24} - 1$ over $\mathbb{Z}$ and over $\mathbb{F}_7$.*

Problem 80. *Find the smallest finite field containing an element of order 6 and an element of order 8.*

Problem 81. *Verify if each one of the following polynomials is irreducible over $\mathbb{F}_2$:*

a) $x^4 + x^3 + 1$;
b) $x^8 + x^7 + x^6 + x^5 + x^4 + x + 1$.

Problem 82. *Compute the decomposition $x^9 - 1 = \prod_{d|9} \Phi_d(x)$.*
Compute the cyclotomic cosets modulo $n = 9$ with respect to $q = 2$ and use them to justify that the factors in the previous decomposition are irreducible in $\mathbb{F}_2[x]$.

Problem 83. *The application of Rabin's result to determine if a given polynomial is irreducible may involve computations with polynomials of reasonably large degree, requiring a computer. Sometimes a more elementary approach solves the problem. Verify that the polynomial $p(x) = x^4 + x^2 + 2$ is irreducible over $\mathbb{F}_5$:*

i) *Verify that $p(x)$ has no factors of degree 1;*
ii) *Write $p(x)$ as a product of two degree 2 polynomials and derive a contradiction.*

Repeat the exercise for $p(x) = x^4 + x^3 + 1$.

Problem 84. *Determine the order of each one of following polynomials*

a) $x^6 + x + 1 \in \mathbb{F}_2[x]$;
b) $x^6 + x^4 + x^2 + x + 1 \in \mathbb{F}_2[x]$;
c) $x^4 + x + 2 \in F_3[x]$;

d) $x^5 + 2x + 1 \in F_3[x]$:

Problem 85. *Let $\mathbb{F}_2[\alpha]$ be defined as $\mathbb{F}_2[x]/(x^5 + x^2 + 1)$ (ie, $\alpha^5 + \alpha^2 + 1 = 0$). Is this a field? Is it a direct sum of fields?*
Rewrite as a sum of monomials with coefficients in $\mathbb{F}_2$ the polynomial

$$(x - \alpha)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8)(x - \alpha^{16}).$$

2.1.1. *Codes over non prime fields.*

Problem 86. *Let $\mathbb{F}_9 = \mathbb{F}_3[\alpha]$, where $\alpha^2 = \alpha + 1$, and C be the code over $\mathbb{F}_9$ with generator matrix*

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & \alpha & \alpha \\ 0 & 1 & 0 & \alpha & 1 & \alpha \\ 0 & 0 & 1 & \alpha & \alpha & 1 \end{pmatrix}$$

a) *Encode $u = \begin{pmatrix} \alpha+2 & \alpha^2 & 2\alpha+1 \end{pmatrix}$.*
b) *Compute a parity-check matrix and determine the minimal distance of C.*
c) *Decode $r = \begin{pmatrix} \alpha & 1 & 2\alpha & 0 & \alpha+2 & 2 \end{pmatrix}$.*

2.1.2. *Hermitian Inner product.* It is possible to define other inner products other than the canonical one. An example is the following

Definition 87. *Let $\mathbb{F}_4 = \mathbb{F}_2[\alpha]$ where $\alpha^2 = \alpha + 1$. Define the conjugate map $a \to \bar{a}$ by*

$$\bar{0} = 0, \qquad \bar{1} = 1, \qquad \bar{\alpha} = \alpha^2, \qquad \bar{\alpha^2} = \alpha.$$

Given $x, y \in \mathbb{F}_4^n$, their Hermitian inner product is

$$< x, y >_H = \sum_i x_i \bar{y_i}.$$

Exercise 88. *Prove that $<,>_H$ has the properties of an inner product.*

The **hexacode** is the $[6, 3, 4]$ code over $\mathbb{F}_4$ with generator

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & \alpha & \alpha \\ 0 & 1 & 0 & \alpha & 1 & \alpha \\ 0 & 0 & 1 & \alpha & \alpha & 1 \end{bmatrix}$$

Exercise 89. *Prove that the hexacode is not self-dal with respect to the usual inner product but is self-dual with respect to the Hermitian inner product.*