Updated: 22/12/2023

An introduction to the theory of finite fields

Michel Waldschmidt

http://www.imj-prg.fr/~michel.waldschmidt//pdf/FiniteFields.pdf

Contents

1 Sums of two squares

Every odd positive integer which is sum of two squares is congruent to 1 modulo 4: this follows from the fact that a square is congruent to 0 or 1 modulo 4, hence a sum of two squares is congruent to 0, 1 or 2, but not 3, modulo 4. The converse is not true: 21 is congruent to 1 modulo 4 but is not a sum of two squares.

1.1 Prime numbers which are sums of two squares

In this introductory section we will use the following fact related with finite fields:

> *Let p be a finite field and $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ the field with p elements. Then -1 is a sum of two squares in $\mathbb{F}_p$ if and only if p is congruent to 1 modulo 4.*

In the course we will see several proofs of this fact. One of them rests on the properties of the multiplicative group $\mathbb{F}_p^\times$: that -1 is a sum of two squares in $\mathbb{F}_p$ means that this group, the order of which is $p-1$, contains an element of order 4. If there is an element of order 4, then 4 divides the order of the group, which means that p is congruent to 1 modulo 4. For the converse, we may invoke the fact that the multiplicative group $\mathbb{F}_p^\times$ is cyclic of order $p-1$ (Proposition 19), hence if 4 divides the order of the group then it contains an element of order 4.

Another proof involves the quadratic reciprocity law (Exercise 62): condition (ii) means that the Legendre symbol $\left(\frac{-1}{p}\right)$ has the value 1; it also has the value $(-1)^{(p-1)/2}$ (Exercise 13).

Theorem 1 (Fermat)**.** *A prime number p is sum of two squares if and only either $p = 2$ or p is congruent to 1 modulo 4.*

There are many proofs of Theorem 1 — see for instance [Li], [Wiki] — including a one sentence proof by D. Zagier [Z].

It remains to show that a prime number which is congruent to 1 modulo 4 is a sum of two squares. We start with an auxiliary result:

Lemma 2. *Let p be an odd prime number. The following conditions are equivalent.*
(i) p is congruent to 1 modulo 4.
(ii) There exists t is $\mathbb{Z}$ such that t^2 is congruent to -1 modulo p.
(iii) The prime number p is decomposed in the quadratic extension $\mathbb{Q}(i)/\mathbb{Q}$.

Proof of Lemma 2. The equivalence $(i) \iff (ii)$ rests on the preliminary remark. The equivalence with (iii) rests on classical algebraic number theory (for instance [S] §5.4–5.6): if $t \in \mathbb{Z}$ satisfies $-1 \equiv t^2 \pmod{p}$, then the principal ideal $p\mathbb{Z}[i]$ splits as a product of the two ideals $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ of $\mathbb{Z}[i]$ generated by $(t+i)$ and $(t-i)$ respectively.:

$$(p) = \mathfrak{p}\overline{\mathfrak{p}}.$$

□

We now complete the proof of Theorem 1.

Proof of Theorem 1. Here again there are several proofs. For the first one, we use Dirichlet's box principle. Assume condition (ii) of Lemma 2 is satisfied. Let $t \in \mathbb{Z}$ satisfy $t^2 \equiv -1 \mod p$. Consider the set of $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ satisfying $0 \leq x, y < \sqrt{p}$. This set has $(\lfloor \sqrt{p} \rfloor + 1)^2$ elements. Since p is not a square, we have

$$\lfloor \sqrt{p} \rfloor < \sqrt{p} < \lfloor \sqrt{p} \rfloor + 1,$$

hence $(\lfloor \sqrt{p} \rfloor + 1)^2 > p$. Therefore the number of elements (x, y) in this set is $> p$. It follows that there exist (x', y') and (x'', y'') in this set with $(x', y') \neq (x'', y'')$ and $x' - ty' \equiv x'' - ty'' \mod p$. Set $x = x' - x''$ et $y = y' - y''$. We have $x \equiv ty \mod p$, hence

$$x^2 + y^2 \equiv x^2 - t^2 y^2 \equiv (x - ty)(x + ty) \equiv 0 \mod p.$$

We also have

$$0 < x^2 + y^2 < 2p.$$

Since p is the only multiple of p in the interval $[1, 2p - 1]$, we deduce $x^2 + y^2 = p$.

Another proof [S] uses the decomposition of the ideal (p) generated by p in the quadratic field $\mathbb{Q}(i)$ as the product of two conjugate principal prime ideals $\mathfrak{p} = (x + iy)$ and $\overline{\mathfrak{p}} = (x - iy)$, and to take the norm of one of the factors. □

1.2 Positive integers which are sums of two squares

Corollary 3. *A positive integer n is sum of two squares if and only if, in the decomposition of n into prime factors, each prime congruent to 3 modulo 4 occurs with an even exponent.*

Denote by $N_{a,b}$ a positive integer, all prime factor of which are congruent to a modulo b. Then Corollary 3 can be stated as follows: *a positive integer is sum of two squares if and only if it can be written* $2^a N_{1,4} N_{3,4}^2$.

Proof. A number of the form $2^a N_{1,4} N_{3,4}^2$ is a sum of two squares. This follows from the fact that a product of sums of two squares is again a sum of two squares, as shown by the identity

$$(a^2 + b^2)(x^2 + y^2) = (ax - by)^2 + (ay + bx)^2$$

which expresses the fact that the norm from $\mathbb{Q}(i)$ over$\mathbb{Q}$ of a product

$$(a + bi)(x + yi) = (ax - by) + (ay + bx)i$$

is the product of the norms of $a + bi$ and of $x + yi$. This is the special case $d = -1$ of Brahmagupta's identity which is valid for all $d \in \mathbb{Z}$:

$$(a^2 - db^2)(x^2 - dy^2) = (ax - dby)^2 - d(ay + bx)^2.$$

For the converse, we are going to show that if n is a positive integer of the form $x^2 + y^2$ and p an odd prime number, if the exponent $s = v_p(n)$ of p in the decomposition of n into prime factors is odd, then $p \equiv 1 \mod 4$. Let d be the gcd of x and y and let $t = v_p(d)$ be the exponent of p in the decomposition of d into prime factors. Write $x = da$, $y = db$ with a and b relatively prime, so that $n = d^2 m$ with $m = a^2 + b^2$. The exponent $v_p(m)$ of p in the decomposition of m into prime factors is $s - 2t$, and since s is odd we have $s - 2t \geq 1$. Since a and b are relatively prime, one of them is not a multiple of p (as a matter of fact, it is true also for the other since p divides $a^2 + b^2$). Multiplying by its inverse modulo p, we deduce that there exists t in $\mathbb{Z}$ such that $t^2 + 1$ is a multiple of p. From Lemma 2 we deduce that p is congruent to 1 modulo 4. □

Exercise 4. The quadratic form $X^2 + Y^2$ is the homogeneous version of the cyclotomic polynomial $\phi_4(t) = t^2 + 1$. There are only three cyclotomic polynomials of degree 2, $\phi_4(t)$, $\phi_3(t) = t^2 + t + 1$ and $\phi_6(t) = \phi_3(-t)$. The homogeneous version of $\phi_3(t)$ is the quadratic form $X^2 + XY + Y^2$.
(a) Check that a positive integer congruent to 2 modulo 3 cannot be written as $x^2 + xy + y^2$ with integers x, y.
(b) Let p be a prime number, $p \neq 3$. Check that the following conditions are equivalent:
(i) p is congruent to 1 modulo 3.
(ii) There exists t in $\mathbb{Z}$ such that $t^2 + t + 1$ is a multiple of p.
(iii) The prime number p is decomposed in the quadratic field $\mathbb{Q}(j)/\mathbb{Q}$, where j is a primitive cubic root of unity.
(c) Prove that a prime number p can be written as $x^2 + xy + y^2$ if and only if p congruent to 1 modulo 3.
(d) Prove that a positive integer n can be written $n = x^2 + xy + y^2$ with integers x, y if and only if $n = 3^b N_{1,3} N_{2,3}^2$.

References

[Li] Chao Li, From sums of two squares to arithmetic Siegel–Weil formulas. Bull. Amer. Math. Soc. **60** (3), July 2023, 327– 370.

[S] Pierre Samuel, *Algebraic theory of numbers*. Dover Books on Mathematics (2008).

[Wiki] Proof of Fermat's theorem on sums of two squares.
https://en.wikipedia.org/wiki/Proofs_of_Fermat%27s_theorem_on_sums_of_two_squares

[Z] Don Zagier, A one-sentence proof that every prime $p \equiv 1 \pmod 4$ is a sum of two squares. Amer. Math. Monthly 97 (1990), no. 2, 144,
See also
Guillaume Dubach, Fabian Muehlboeck - Formal verification of Zagier's one-sentence proof.
https://arxiv.org/abs/2103.11389

2 Finite projective planes

Here we will use the fact that for a given positive integer q, a field with q elements exists if and only if q is a power of a prime number p.

The easy direction of this equivalence is that if a field F with q elements exists, then q is a power of a prime number p. First, we have $q \geq 2$, since a ring (hence a field) has always at least two elements, $0 \neq 1$. Let p be the characteristic of F; then F is a finite vector space over the prime field $\mathbb{F}_p$, and if r is the dimension then F has p^r elements.

Conversely, let q be a power of a prime. We will prove that for any positive integer r there exists a polynomial of degree r which is irreducible over $\mathbb{F}_p$ (this follows from Theorem 55), hence the field obtained by adjoining a root of this polynomial to $\mathbb{F}_p$ has p^r elements. One may also argue that the set of roots of the polynomial $X^q - X$ in an algebraic closure of $\mathbb{F}_p$ is a field with q elements when q is a power of p (see Theorem 24).

Let $\mathbb{F}_q$ be a finite field with q elements and $n \geq 2$ an integer. The projective space $\mathbb{P}_n(\mathbb{F}_q)$ is the set of lines ($\mathbb{F}_q$ subspaces of dimension 1) of $\mathbb{F}_q^{n+1}$. Hence it is the quotient of $\mathbb{F}_q^{n+1} \setminus \{0\}$ under the equivalence relation

$$(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n) \Longleftrightarrow \text{there exists } \lambda \in \mathbb{F}_q \setminus \{0\} \text{ with } (y_0, \ldots, y_n) = (\lambda x_0, \ldots, \lambda x_n).$$

There are $q^{n+1} - 1$ elements in $\mathbb{F}_q^{n+1} \setminus \{0\}$, each equivalence class contains $q - 1$ elements, hence $\mathbb{P}_n(\mathbb{F}_q)$ has

$$\frac{q^{n+1} - 1}{q - 1} = q^n + q^{n-1} + \cdots + q + 1.$$

elements.

The projective space $\mathbb{P}_n(\mathbb{F}_q)$ of dimension n is the disjoint union of the affine space $\mathbb{F}_q^n$, with q^n elements, and the hyperplane at infinity $\mathbb{P}_{n-1}(\mathbb{F}_q)$ with $(q^n - 1)/(q - 1)$ elements. In particular $\mathbb{P}_2(\mathbb{F}_q)$, the projective plane over $\mathbb{F}_q$, has $q^2 + q + 1$ elements. Each projective line of $\mathbb{P}_2(\mathbb{F}_q)$ contains $q + 1$ points; through each point in $\mathbb{P}_2(\mathbb{F}_q)$ pass $q + 1$ lines.

Definition. *A finite projective plane is a nonempty set X (whose elements are called "points"), along with a nonempty collection L of subsets of X (whose elements are called "lines"), such that:*
- *For every two distinct points, there is exactly one line that contains both points.*
- *The intersection of any two distinct lines contains exactly one point.*
- *There exists a set of four points, no three of which belong to the same line.*

The projective plane of order q has $q^2 + q + 1$ points and $q^2 + q + 1$ lines, each line contains $q + 1$ points, each point belongs to $q + 1$ lines.

The Fano plane is the projective plane of order 2, with 7 points, 7 lines, each line contains 3 points, each point belongs to 3 lines.

If q is a power of a prime, there exists a projective plane of order q: one example is $\mathbb{P}_2(\mathbb{F}_q)$, other examples are known. One conjectures that conversely, if there exists a projective plane of order q, then q is a power of a prime (see Exercise 105). A few partial results are known. Tarry [T] proved that there is no finite projective plane of order 6, by showing that there is no example of two 6×6 orthogonal latin squares (cf. [D-K]). Further, Bruck and Ryser [B-R] proved that for $q \equiv 1 \pmod 4$ or $q \equiv 2 \pmod 4$, if there exists a projective plane of order q, then q is the sum of two squares (one of which may be 0). In 1989, Lam, Thiel and Swiercz [L-T-S] proved that there is no projective plane of order 10. The first open case is $q = 12$.

The card game *dobble* is related with the projective plane of order 7, with $7^2 + 7 + 1 = 57$ elements.

A good reference for the *mutually orthogonal latin squares* (MOL) and the *latin square digraph* (LSD) is [D-K] which come from the *incidence matrix*.

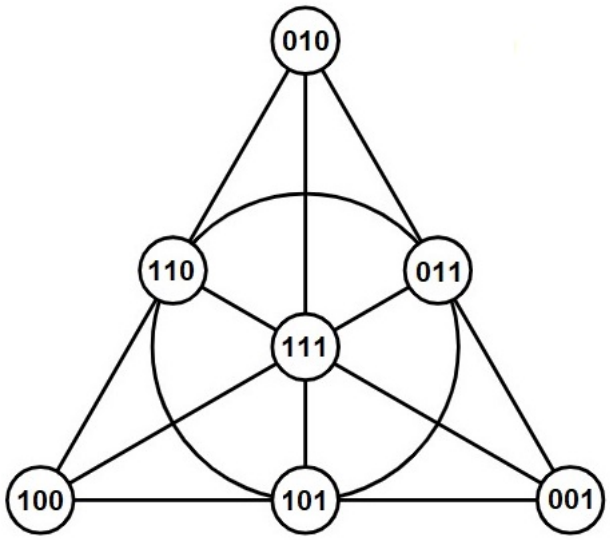
References

[B-R] R.H. Bruck and H.J. Ryser, *The non-existence of certain finite projective planes*, Can. J. Math. **1**, (1949), 88-93.

[D-K] J. Dénes and A.D. Keedwell, *Latin squares and their applications*, Academic Press, (1974, first edition), 547 pages.

[L-T-S] C.W.H. Lam, L. Thiel and S. Swiercz, *The non-existence of finite projective planes of order* 10, Can. J. Math. **XLI**, (1989), 1117-1123.

[T] G. Tarry, *Sur le problème d'Euler des* 36 *officiers*, L'intermédiaire des mathématiciens **7**, (1900), 14-16.



Fano Plane: $\mathbb{P}_2(\mathbb{F}_2)$

	$(1:1:1)$	$(0:1:0)$	$(1:0:1)$	$(1:0:0)$	$(0:1:1)$	$(1:1:0)$	$(0:0:1)$
$x_0 + x_2 = 0$	1	1	1	0	0	0	0
$x_1 + x_2 = 0$	1	0	0	1	1	0	0
$x_0 + x_1 = 0$	1	0	0	0	0	1	1
$x_2 = 0$	0	1	0	1	0	1	0
$x_0 = 0$	0	1	0	0	1	0	1
$x_1 = 0$	0	0	1	1	0	0	1
$x_0 + x_1 + x_2 = 0$	0	0	1	0	1	1	0

Incidence matrix – coordinates $(x_0 : x_1 : x_2)$

3 Background: Arithmetic

3.1 Cyclic groups

If G is a finite multiplicative group and x an element of G, the order of x is the least positive integer n such that $x^n = 1$. For x of order n and for $m \in \mathbb{Z}$, the condition $x^m = 1$ is equivalent to n divides m; in other words, n is the positive generator of the ideal of $\mathbb{Z}$ which consists of the m such that $x^m = 1$.

If x has order n, for $k \in \mathbb{Z}$ the order of x^k is $n/\gcd(n,k)$.

The order of a finite group is the number of elements of this group. A cyclic group is a finite group generated by one element. Two cyclic groups of the same order are isomorphic. For $n \geq 2$, an exemple of a cyclic additive group of order n is the additive group $\mathbb{Z}/n\mathbb{Z}$ of integers modulo n. An example of a cyclic multiplicative group of order n is the group μ_n of complex numbers z which satisfy $z^n = 1$, namely

$$\{1, e^{2i\pi/n}, e^{4i\pi/n}, \dots, e^{2(n-1)i\pi/n}\},$$

the roots of unity of order dividing n. The subgroups and quotients of a cyclic group are cyclic. For any cyclic group of order n and for any divisor d of n, there is a unique subgroup of G of order d; if ζ is a generator of the multiplicative cyclic group G of order n and if d divides n, then $\zeta^{n/d}$ has order d, hence, is a generator of the unique subgroup of G of order d.

In a cyclic group, the order of which is a multiple of d, there are exactly d elements whose orders are divisors of d and these are the elements of the subgroup of order d. In a cyclic group G of order a multiple of d, the set of elements $\{x^d \mid x \in G\}$ is the unique subgroup of G of index d.

The Cartesian product $G_1 \times G_2$ of two groups is cyclic if and only if G_1 and G_2 are cyclic with relatively prime orders.

The number of generators of a cyclic group of order n is $\varphi(n)$, where φ is Euler's function (see § 3.2).

3.2 Residue classes modulo n

The subgroups of the additive group $\mathbb{Z}$ are $n\mathbb{Z}$ with $n \geq 0$. We denote by $s_n : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ the canonical map, which is a morphism of groups with kernel $n\mathbb{Z}$

Given positive integers a and b, there exists a morphism of groups $\varphi_{a,b} : \mathbb{Z}/a\mathbb{Z} \to \mathbb{Z}/b\mathbb{Z}$ such that $\varphi_{a,b} \circ s_a = s_b$ if and only if $a\mathbb{Z} \subset b\mathbb{Z}$, which means if and only if b divides a. If $\varphi_{a,b}$ exists, then $\varphi_{a,b}$ is unique and surjective. Its kernel is $b\mathbb{Z}/a\mathbb{Z}$, the unique subgroup of $\mathbb{Z}/a\mathbb{Z}$ of order a/b, which is cyclic and isomorphic to $\mathbb{Z}/(a/b)\mathbb{Z}$.

The *greatest common divisor* $gcd(a, b)$ of a and b is the positive generator of $a\mathbb{Z}+b\mathbb{Z}$, the *least common multiple* $\operatorname{lcm}(a, b)$ of a and b is the positive generator of $a\mathbb{Z} \cap b\mathbb{Z}$.

For $n \geq 2$, $\mathbb{Z}/n\mathbb{Z}$ is a ring and s_n is a morphism of rings. The order of the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ of the ring $\mathbb{Z}/n\mathbb{Z}$ is the number $\varphi(n)$ of integers k in the interval $1 \leq k \leq n$ satisfying $\gcd(n, k) = 1$. The map $\varphi : \mathbb{Z}_{>0} \to \mathbb{Z}$, with $\varphi(1) = 1$, is *Euler's function* already mentioned in § 3.1. If $\gcd(a, b) = d$, then a/d and b/d are relatively prime. Hence, the partition of the set of integers in $1 \leq k \leq n$ according to the value of $\gcd(k, n)$ yields:

Lemma 5. *For any positive integer n,*

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

(Compare with (44)).

Exercise 6.
(1) Let G be a finite group of order n and let k be a positive integer with $\gcd(n, k) = 1$. Prove that the only solution $x \in G$ of the equation $x^k = 1$ is $x = 1$.
(2) Let G be a cyclic group of order n and let k be a positive integer. Prove that the number of $x \in G$ such that $x^k = 1$ is $\gcd(n, k)$.
(3) Let G be a finite group of order n. Prove that the following conditions are equivalent:
(*i*) G is cyclic

(*ii*) For each divisor d of n, the number of $x \in G$ such that $x^d = 1$ is $\leq d$.
(*iii*) For each divisor d of n, the number of $x \in G$ such that $x^d = 1$ is d.

An *arithmetic function* is a map $f : \mathbb{Z}_{>0} \to \mathbb{Z}$. A *multiplicative function* is an arithmetic function such that $f(mn) = f(m)f(n)$ when m and n are relatively prime. For instance, Euler's φ function is multiplicative: this follows from the ring isomorphim between the ring product $(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$ and the ring $\mathbb{Z}/mn\mathbb{Z}$ when m and n are relatively prime (*Chinese remainder Theorem*). Also, $\varphi(p^a) = p^{a-1}(p-1)$ for p prime and $a \geq 1$. Hence, the value of $\varphi(n)$, for n written as a product of powers of distinct prime numbers, is

$$\varphi(p_1^{a_1} \cdots p_r^{a_r}) = p_1^{a_1-1}(p_1 - 1) \cdots p_r^{a_r-1}(p_r - 1).$$

When p is a prime number, a *primitive root* modulo p is a generator of the cyclic group $(\mathbb{Z}/p\mathbb{Z})^\times$. There are exactly $\varphi(p-1)$ of them in $(\mathbb{Z}/p\mathbb{Z})^\times$. From the definition, it follows that an element $g \in (\mathbb{Z}/p\mathbb{Z})^\times$ is a primitive root modulo p if and only if

$$g^{(p-1)/q} \not\equiv 1 \bmod p$$

for all prime divisors q of $p - 1$.

If a and n are relatively prime integers, the *order of a modulo n* is the order of the class of a in the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$. In other terms, it is the smallest integer ℓ such that a^ℓ is congruent to 1 modulo n.

Exercise 7. For n a positive integer, check that the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic if and only if n is either 2, 4, p^s or $2p^s$, with p an odd prime and $s \geq 1$.

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

3.3 The ring $\mathbb{Z}[X]$

When F is a field, the ring $F[X]$ of polynomials in one variable over F is an Euclidean domain, hence, a principal domain and, therefore, a factorial ring. The ring $\mathbb{Z}[X]$ is not an Euclidean ring: one cannot divide X by 2 in $\mathbb{Z}[X]$ for instance. But if A and B are in $\mathbb{Z}[X]$ and B is monic, then both the quotient Q and the remainder R of the Euclidean division in $\mathbb{Q}[X]$ of A by B

$$A = BQ + R$$

are in $\mathbb{Z}[X]$.

The gcd of the coefficients of a non–zero polynomial $f \in \mathbb{Z}[X]$ is called the *content* of f. We denote it by $c(f)$. A non–zero polynomial with content 1 is called *primitive*. Any non–zero polynomial in $\mathbb{Z}[X]$ can be written in a unique way as $f = c(f)g$ with $g \in \mathbb{Z}[X]$ primitive.

For any non–zero polynomial $f \in \mathbb{Q}[X]$, there is a unique positive rational number r such that rf belongs to $\mathbb{Z}[X]$ and is primitive.

Lemma 8 (Gauss's Lemma)**.** *For f and g non–zero polynomials in $\mathbb{Z}[X]$, we have*

$$c(fg) = c(f)c(g).$$

Proof. It suffices to check that the product of two primitive polynomials is primitive. More generally, let p be a prime number and f, g two polynomials whose contents are not divisible by p. We check that the content of fg is not divisible by p.

We use the surjective morphism of rings

$$\Psi_p : \mathbb{Z}[X] \to \mathbb{F}_p[X], \tag{9}$$

which maps X to X and $\mathbb{Z}$ onto $\mathbb{F}_p$ by reduction modulo p of the coefficients. Its kernel is the principal ideal $p\mathbb{Z}[X] = (p)$ of $\mathbb{Z}[X]$ generated by p: it is the set of polynomials whose content is divisible by p. The assumption is $\Psi_p(f) \neq 0$ and $\Psi_p(g) \neq 0$. Since p is prime, the ring $\mathbb{F}_p[X]$ has no zero divisor, hence, $\Psi_p(fg) = \Psi_p(f)\Psi_p(g) \neq 0$, which shows that fg is not in the kernel of Ψ_p. □

The ring $\mathbb{Z}$ is an Euclidean domain, hence, a principal domain and, therefore, a factorial ring. It follows that the ring $\mathbb{Z}[X]$ is factorial. The units of $\mathbb{Z}[X]$ are $\{+1, -1\}$. The irreducible elements in $\mathbb{Z}[X]$ are
– the prime numbers $\{2, 3, 5, 7, 11, \dots\}$,
– the irreducible polynomials in $\mathbb{Q}[X]$ with coefficients in $\mathbb{Z}$ and content 1
– and, of course, the product of one of these elements by -1.

From Gauss's Lemma 8, one deduces that if f and g are two monic polynomials in $\mathbb{Q}[X]$ such that $fg \in \mathbb{Z}[X]$, then f and g are in $\mathbb{Z}[X]$.

A monic polynomial in $\mathbb{Z}[X]$ is a product, in a unique way, of irreducible monic polynomials in $\mathbb{Z}[X]$.

Exercise 10. Given two rings B_1, B_2, a subring A_1 of B_1, a subring A_2 of B_2, a morphism of ring $f : A_1 \to A_2$,

$$\begin{array}{ccc} B_1 & & B_2 \\ \cup & & \cup \\ A_1 & \xrightarrow[f]{} & A_2 \end{array}$$

elements $x_1, \dots, x_n$ of B_1 and elements $y_1, \dots, y_n$ of B_2, a necessary and sufficient condition for the existence of a morphism $F : A_1[x_1, \dots, x_n] \to A_2[y_1, \dots, y_n]$ such that $F(a) = f(a)$ for $a \in A_1$ and $F(x_i) = y_i$ for $1 \leq i \leq n$ is the following:

For any polynomial $P \in A_1[X_1, \dots, X_n]$ such that

$$P(x_1, \dots, x_n) = 0,$$

the polynomial $Q \in A_2[X_1, \dots, X_n]$, image of P by the extension of f to $A_1[X_1, \dots, X_n] \to A_2[X_1, \dots, X_n]$, satisfies

$$Q(y_1, \dots, y_n) = 0.$$

3.4 Möbius inversion formula

Let f be a map defined on the set of positive integers with values in an additive group. Define another map g by

$$g(n) = \sum_{d|n} f(d).$$

It is easy to check by induction that f is completely determined by g. Indeed, the formula for $n = 1$ produces $f(1) = g(1)$ and for $n \geq 2$, once $f(d)$ is known for all $d \mid n$ with $d \neq n$, one obtains $f(n)$ from the formula

$$f(n) = g(n) - \sum_{\substack{d|n \\ d \neq n}} f(d).$$

We wish to write this formula in a close form. If p is a prime, the formula becomes $f(p) = g(p) - g(1)$. Next, $f(p^2) = g(p^2) - g(p)$. More generally, for p prime and $m \geq 1$,

$$f(p^m) = g(p^m) - g(p^{m-1}).$$

It is convenient to write this formula as

$$f(p^m) = \sum_{h=0}^{m} \mu(p^{m-h}) g(p^h),$$

where $\mu(1) = 1$, $\mu(p) = -1$, $\mu(p^m) = 0$ for $m \geq 2$. In order to extend this formula for writing $f(n)$ in terms of $g(d)$ for $d \mid n$, one needs to extend the function μ and it is easily seen by means of the convolution product (see Exercise 11) that the right thing to do is to require that μ be a *multiplicative function*, namely that $\mu(ab) = \mu(a)\mu(b)$ if a and b are relatively prime.

The *Möbius function* μ (see, for instance, [9] § 2.6) is the map from the positive integers to $\{0, 1, -1\}$ defined by the properties $\mu(1) = 1$, $\mu(p) = -1$ for p prime, $\mu(p^m) = 0$ for p prime and $m \geq 2$ and $\mu(ab) = \mu(a)\mu(b)$ if a and b are relatively prime. Hence, $\mu(a) = 0$ if and only if a has a square factor, while for a squarefree number a, which is a product of s distinct primes we have $\mu(a) = (-1)^s$:

$$\mu(p_1 \cdots p_s) = (-1)^s.$$

One of the many variants of the *Möbius inversion formula* states that, for f and g two maps defined on the set of positive integers with values in an additive group, the two following properties are equivalent:
(i) *For any integer* $n \geq 1$,

$$g(n) = \sum_{d|n} f(d).$$

(ii) *For any integer* $n \geq 1$,

$$f(n) = \sum_{d|n} \mu(n/d) g(d).$$

For instance, Lemma 5 is equivalent to

$$\varphi(n) = \sum_{d|n} \mu(n/d) d \quad \text{for all } n \geq 1.$$

An equivalent statement of the Möbius inversion formula is the following multiplicative version, which deals with two maps f, g from the positive integers into an abelian multiplicative group. The two following properties are equivalent:
(i) *For any integer* $n \geq 1$,

$$g(n) = \prod_{d|n} f(d).$$

(ii) *For any integer* $n \geq 1$,

$$f(n) = \prod_{d|n} g(d)^{\mu(n/d)}.$$

A third form of the Möbius inversion formula (which we will not use here) deals with two functions F and G from $[1, +\infty)$ to $\mathbb{C}$. The two following properties are equivalent:
(i) *For any real number* $x \geq 1$,

$$G(x) = \sum_{n \leq x} F(x/n).$$

(ii) *For any real number* $x \geq 1$,

$$F(x) = \sum_{n \leq x} \mu(n) G(x/n).$$

As an illustration, take $F(x) = 1$ and $G(x) = [x]$ for all $x \in [1, +\infty)$. Then

$$\sum_{n \leq x} \mu(n)[x/n] = 1$$

Exercise 11. Let A be a (commutative, as always) ring and let R denote the set of *arithmetic functions*, namely the set of applications from the positive integers into A. For f and g in R, define the convolution product

$$f \star g(m) = \sum_{ab=m} f(a)g(b).$$

(a) Check that R, with the usual addition and with this convolution product, becomes a commutative ring.
`Hint:`

$$f \star g \star h(m) = \sum_{abc=m} f(a)g(b)h(c).$$

Check that the unity is $\delta \in R$ defined by

$$\delta(a) = \begin{cases} 1 & \text{for } a = 1, \\ 0 & \text{for } a > 1. \end{cases}$$

(b) Check that if f and g are multiplicative, then so is $f \star g$.
(c) Define $\mathbf{1} \in R$ by $\mathbf{1}(x) = 1$ for all $x \geq 1$. Check that μ and $\mathbf{1}$ are inverse each other in R:

$$\mu \star \mathbf{1} = \delta.$$

(d) Check that the formula

$$\mu \star \mathbf{1} \star f = f \quad \text{for all } f \in R$$

is equivalent to Möbius inversion formula.
(e) Define j by $j(n) = n$ and, for $k \geq 0$, $\sigma_k(n) = \sum_{d|n} d^k$. Check

$$\mu \star j = \varphi, \quad j^k \star \mathbf{1} = \sigma_k.$$

4 The theory of finite fields

References:

M. Demazure [2], Chap. 8.
D.S. Dummit & R.M. Foote [3], § 14.3.
S. Lang [6], Chap. 5 § 5.
R. Lidl & H. Niederreiter [7].
V. Shoup [9], Chap. 20.

4.1 Gauss fields

A field with finitely many elements is also called a *Gauss Field*. For instance, given a prime number p, the quotient $\mathbb{Z}/p\mathbb{Z}$ is a Gauss field. Given two fields F and F' with p elements, p prime, there is a unique isomorphism $F \to F'$. Hence, we denote by $\mathbb{F}_p$ the unique field with p elements.

The *characteristic* of a finite field F is a prime number p, hence, its prime field is $\mathbb{F}_p$. Moreover, F is a finite vector space over $\mathbb{F}_p$; if the dimension of this space is s, which means that F is a finite extension of $\mathbb{F}_p$ of degree $[F : \mathbb{F}_p] = s$, then F has p^s elements. Therefore, the number of elements of a finite field is always a power of a prime number p and this prime number is the characteristic of F.

The multiplicative group $F^\times$ of a field with q elements has order $q-1$, hence, $x^{q-1} = 1$ for all x in $F^\times$ and $x^q = x$ for all x in F. Therefore, $F^\times$ is the set of roots of the polynomial $X^{q-1} - 1$, while F is the set of roots of the polynomial $X^q - X$:

$$X^{q-1} - 1 = \prod_{x \in F^\times} (X - x), \qquad X^q - X = \prod_{x \in F} (X - x). \tag{12}$$

Exercise 13. (a) Let F be a finite field with q elements. Denote by $\mathcal{C}$ the set of non–zero squares in F, which is the image of the endomorphism $x \mapsto x^2$ of the multiplicative group $F^\times$:

$$\mathcal{C} = \{x^2 \ \mid \ x \in F^\times\}.$$

Assume q is even; check $\mathcal{C} = F^\times$, hence $X^{q-1} - 1 = \prod_{x \in \mathcal{C}} (X - x)$.
Assume q is odd; check

$$X^{(q-1)/2} - 1 = \prod_{x \in \mathcal{C}} (X - x) \quad \text{and} \quad X^{(q-1)/2} + 1 = \prod_{x \in F^\times \setminus \mathcal{C}} (X - x)$$

(b) Let p be an odd prime. For a in $\mathbb{F}_p$, denote by $\left(\frac{a}{p}\right)$ the Legendre symbol:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } a = 0 \\ 1 & \text{if } a \text{ is a non–zero square in } \mathbb{F}_p \\ -1 & \text{if } a \text{ is not a square in } \mathbb{F}_p. \end{cases}$$

Check

$$X^{(p-1)/2} - 1 = \prod_{a \in \mathbb{F}_p,\, \left(\frac{a}{p}\right) = 1} (X - a)$$

and

$$X^{(p-1)/2}+1=\prod_{a\in\mathbb{F}_p,\ \left(\frac{a}{p}\right)=-1}(X-a).$$

Deduce that for a in $\mathbb{F}_p$,

$$\left(\frac{a}{p}\right)=a^{(p-1)/2}.$$

Exercise 14. Let $\mathbb{F}_q$ be a finite field. A polynomial $f\in\mathbb{F}_q[T]$ *computes squares* if $\alpha=f(\alpha)^2$ for each $\alpha\in\mathbb{F}_q$ which is a square.
(a) Assume q is even. Show that the polynomial $f(T)=T^{q/2}$ computes squares and that no polynomial of degree $<q/2$ computes squares.
(b) Assume that q is odd. Show that no polynomial of degree $<(q+1)/4$ computes squares.
(c) Assume that $q\equiv 3 \mod 4$. Show that the polynomial $f(T)=T^{(q+1)/4}$ computes squares.
(d) Assume that $q\equiv 1 \mod 4$. Show that there exists a polynomial of degree $\leq(q-1)/2$ that computes squares.

Exercise 15. Prove that in a finite field, any element is a sum of two squares.

Exercise 16. Let F be a finite field, q the number of its elements, k a positive integer. Denote by $\mathcal{C}_k$ the image of the endomorphism $x\mapsto x^k$ of the multiplicative group $F^\times$:

$$\mathcal{C}_k=\{x^k \mid x\in F^\times\}.$$

How many elements are there in $\mathcal{C}_k$?

Exercise 17. Find the irreducible polynomial of $\sqrt{2}+\sqrt{3}$ over $\mathbb{Z}$ and prove that it is reducible modulo p for all primes p.

Exercise 18. Prove that if F is a finite field with q elements, then the polynomial X^q-X+1 has no root in F. Deduce that F is not algebraically closed.

Proposition 19. *Any finite subgroup G of the multiplicative group of a field K is cyclic. If n is the order of G, then G is the set of roots of the polynomial X^n-1 in K.*

Proof. Let e be the exponent of G. By Lagrange's theorem, e divides n. Any x in G is a root of the polynomial X^e-1. Since G has order n, we get n roots in the field K of this polynomial X^e-1 of degree $e\leq n$. Hence $e=n$. We conclude by using the fact that there exists in G at least one element of order e, hence, G is cyclic.

The last part of the statement is easy: any element x of G satisfies $x^n=1$ by Lagrange's theorem, hence the polynomial X^n-1, which has degree n, has n roots in K, namely the elements in G. Since K is a field, we deduce

$$X^n-1=\prod_{x\in G}(X-x),$$

which means that G is the set of roots of the polynomial X^n-1 in K. □

Second proof of Proposition 19. The following alternative proof of Proposition 19 does not use the exponent. Let K be a field and G a finite subgroup of $K^\times$ of order n. For each $d\mid n$, the number of elements x in K satisfying $x^d=1$ is at most d (the polynomial X^d-1 has at most d roots in K). The result now follows from exercise 6 (3). □

Recall that when $F = \mathbb{F}_p$, a rational integer a is called a *primitive root modulo* p if a is not divisible by p and if the class of a modulo p is a generator of the cyclic group $(\mathbb{Z}/p\mathbb{Z})^\times$. More generally, when $\mathbb{F}_q$ is a finite field with q elements, a generator of the cyclic group $\mathbb{F}_q^\times$ is called a *primitive root* or a *primitive element* in $\mathbb{F}_q$. A nonzero element α in $\mathbb{F}_q$ is a primitive root in $\mathbb{F}_q$ if and only if α is a primitive $(q-1)$th root of unity. There are $\varphi(q-1)$ primitive roots in $\mathbb{F}_q$. Programs giving primitive roots in $\mathbb{F}_q$ are available online[1].

The discrete logarithm. Let G be a finite cyclic group of order n written multiplicatively and a a generator. Any element of G can be written $x = a^k$, with an integer which is unique modulo n. This integer (or its class in the additive cyclic group $\mathbb{Z}/n\mathbb{Z}$) is called the logarithm of x in basis a. We consider only the case where G is the multiplicative group of the non zero elements of a finite field.

Let $\mathbb{F}_q$ be a finite field and α a primitive root in $\mathbb{F}_q$, so that $\mathbb{F}_q^\times = \{1, \alpha, \alpha^2, \dots, \alpha^{q-2}\}$. Any $\gamma \in \mathbb{F}_q^\times$ can be written in a unique way as α^m for some $0 \le m \le q-2$. This integer m, or the class of m modulo $q-1$, is the *discrete logarithm* in $\mathbb{F}_q$ of γ with respect to α (also called the *index of* γ or the *multiplicative order of* γ with respect to α). We denote it by $\mathrm{Ind}_\alpha \gamma$:

$$\mathrm{Ind}_\alpha(\alpha^n) = n \in \mathbb{Z}/(q-1)\mathbb{Z}, \quad \alpha^{\mathrm{Ind}_\alpha \gamma} = \gamma.$$

For α a primitive root in $\mathbb{F}_q$ and $\gamma, \gamma_1, \gamma_2$ in $\mathbb{F}_q^\times$, we have

$$\mathrm{Ind}_\alpha(\gamma_1\gamma_2) \equiv \mathrm{Ind}_\alpha(\gamma_1) + \mathrm{Ind}_\alpha(\gamma_2) \mod (q-1), \quad \mathrm{Ind}_\alpha(\gamma^{-1}) \equiv -\mathrm{Ind}_\alpha(\gamma) \mod (q-1).$$

If α and β are primitive roots in $\mathbb{F}_q$, then

$$\mathrm{Ind}_\alpha(\beta)\mathrm{Ind}_\beta(\alpha) \equiv 1 \mod (q-1).$$

Example 20 (`The discrete logarithm in` $\mathbb{F}_4$`).` The field $\mathbb{F}_4$ is a quadratic extension of $\mathbb{F}_2$ (see Example 30). Let x be a root of the polynomial $X^2+X+1 \in \mathbb{F}_2[X]$, so that $\mathbb{F}_4 = \mathbb{F}_2(x)$ and $\mathbb{F}_4^\times = \{1, x, x^2\}$. The tables of exponentials in $\mathbb{F}_4^\times$ are

α^n :	$n =$	1	2
	$\alpha = x$	x	x^2
	$\alpha = x^2$	x^2	x

hence the tables of discrete logarithms in $\mathbb{F}_4$ are

$\mathrm{Ind}_\alpha \gamma$:	$\gamma =$	x	x^2
	$\alpha = x$	1	2
	$\alpha = x^2$	2	1

Exercise 21. For each prime $p \le 13$ and also for $p = 31$, list the values $\alpha \in \mathbb{F}_p^\times$ which are primitive roots in $\mathbb{F}_p$. Next, for each α and for $n = 0, 1, 2, \dots, p-2$, compute α^n. Deduce a table of the discrete logarithm in $\mathbb{F}_p$ with respect to the primitive root α.

[1] One of them (in French) is
http://jean-paul.davalan.pagesperso-orange.fr/mots/comb/gfields/index.html
Computation on finite fields can be done also with Pari GP; see
http://wims.unice.fr/~wims/

The theorem of the primitive element for finite fields is:

Proposition 22. *Let F be a finite field and K a finite extension of F. Then there exist $\alpha \in K$ such that $K = F(\alpha)$.*

Proof. Let $q = p^s$ be the number of elements in K, where p is the characteristic of F and K; the multiplicative group $K^\times$ is cyclic (Proposition 19); let α be a generator. Then

$$K = \{0, 1, \alpha, \alpha^2, \dots, \alpha^{q-2}\} = \mathbb{F}_p(\alpha),$$

and, therefore, $K = F(\alpha)$. □

Hence the field K is isomorphic to the quotient $\mathbb{F}_p[X]/(P)$ where $P \in \mathbb{F}_p[X]$ is some irreducible polynomial over $\mathbb{F}_p$ of degree s. We prove below (cf. Theorem 24) that K is isomorphic to the quotient $\mathbb{F}_p[X]/(P)$ where $P \in \mathbb{F}_p[X]$ is any irreducible polynomial over $\mathbb{F}_p$ of degree s.

Lemma 23. *Let K be a field of characteristic p. For x and y in K, we have $(x + y)^p = x^p + y^p$.*

Proof. When p is a prime number and n an integer in the range $1 \leq n < p$, the binomial coefficient

$$\binom{p}{n} = \frac{p!}{n!(p-n)!}$$

is divisible by p. □

We now prove that for any prime number p and any integer $s \geq 1$, there exists a finite field with p^s elements.

Theorem 24. *Let p be a prime number and s a positive integer. Set $q = p^s$. Then there exists a field with q elements. Two finite fields with the same number of elements are isomorphic. If Ω is an algebraically closed field of characteristic p, then Ω contains one and only one subfield with q elements.*

Proof. Let F be a splitting field over $\mathbb{F}_p$ of the polynomial $X^q - X$. Since the derivative of $X^q - X$ is -1, there is no multiple root, hence $X^q - X$ has q distinct roots in F. From Lemma 23 it follows that the set of these roots is a field. Hence this set is F and F has q elements.

If F' is a field with q elements, then F' is the set of roots of the polynomial $X^q - X$, hence, F' is the splitting field of this polynomial over its prime field and, therefore, is isomorphic to F.

If Ω is an algebraically closed field of characteristic p, then the unique subfield of Ω with q elements is the set of roots of the polynomial $X^q - X$. □

According to (12), if $\mathbb{F}_q$ is a finite field with q elements and F an extension of $\mathbb{F}_q$, then for $a \in F$, the relation $a^q = a$ holds if and only if $a \in \mathbb{F}_q$. We will use the following more general fact:

Lemma 25. *Let $\mathbb{F}_q$ be a finite field with q elements, F an extension of $\mathbb{F}_q$ and $f \in F[X]$ a polynomial with coefficients in F. Then f belongs to $\mathbb{F}_q[X]$ if and only if $f(X^q) = f(X)^q$.*

Proof. Since q is a power of the characteristic p of F, if we write

$$f(X) = a_0 + a_1 X + \cdots + a_n X^n,$$

then, by Lemma 23,

$$f(X)^p = a_0^p + a_1^p X^p + \cdots + a_n^p X^{np}$$

and by induction

$$f(X)^q = a_0^q + a_1^q X^q + \cdots + a_n^q X^{nq}.$$

Therefore, $f(X)^q = f(X^q)$ if and only if $a_i^q = a_i$ for all $i = 0, 1, \ldots, n$. □

From Lemma 23, we deduce:

Proposition 26. *Let F be a field of characteristic p.*
(a) The map

$$\begin{array}{rccc} \mathrm{Frob}_p : & F & \to & F \\ & x & \mapsto & x^p \end{array}$$

is an endomorphism of F.
(b) If F is finite, or if F is algebraically closed, then Frob_p is surjective, hence is an automorphism of the field F.

`Remark`. An example of a field of characteristic p for which the endomorphism Frob_p is not surjective is the field $\mathbb{F}_p(X)$ of rational fractions in one variable over the prime field $\mathbb{F}_p$.

Proof. Indeed, this map is a morphism of fields since, by Lemma 23, for x and y in F,

$$\mathrm{Frob}_p(x+y) = \mathrm{Frob}_p(x) + \mathrm{Frob}_p(y)$$

and

$$\mathrm{Frob}_p(xy) = \mathrm{Frob}_p(x)\mathrm{Frob}_p(y).$$

It is injective since it is a morphism of fields. If F is finite, it is surjective because it is injective. If F is algebraically closed, any element in F is a p–th power. □

This endomorphism of F is called the *Frobenius* of F over $\mathbb{F}_p$. It extends to an automorphism of the algebraic closure of F.

If s is a non–negative integer, we denote by Frob_p^s or by Frob_{p^s} the iterated automorphism

$$\mathrm{Frob}_p^0 = 1, \quad \mathrm{Frob}_{p^s} = \mathrm{Frob}_{p^{s-1}} \circ \mathrm{Frob}_p \qquad (s \geq 1),$$

so that, for $x \in F$,

$$\mathrm{Frob}_p^0(x) = x,\ \mathrm{Frob}_p(x) = x^p,\ \mathrm{Frob}_{p^2}(x) = x^{p^2}, \ldots,\ \mathrm{Frob}_{p^s}(x) = x^{p^s} \quad (s \geq 0).$$

If F has p^s elements, then the automorphism $\mathrm{Frob}_p^s = \mathrm{Frob}_{p^s}$ of F is the identity.

If F is a finite field with q elements and K a finite extension of F, then Frob_q is a F–automorphism of K called the *Frobenius of K over F*.

Let F be a finite field of characteristic p with $q = p^r$ elements. According to Proposition 19, the multiplicative group $F^\times$ of F is cyclic of order $q-1$. Let α be a generator of $F^\times$, that means an element of order $q-1$. For $1 \leq \ell < r$, we have $1 \leq p^\ell - 1 < p^r - 1 = q - 1$, hence, $\alpha^{p^\ell - 1} \neq 1$ and $\mathrm{Frob}_p^\ell(\alpha) \neq \alpha$. Since Frob_p^r is the identity on F, it follows that Frob_p has order r in the group of automorphisms of F.

Recall that a finite extension L/K is called *a Galois extension* if the group G of K–automorphisms of L has order $[L : K]$ and in this case the group G is the Galois group of the extension, denoted by $\mathrm{Gal}(L/K)$. It follows that the extension $F/\mathbb{F}_p$ is Galois, with Galois group $\mathrm{Gal}(F/\mathbb{F}_p) = \mathrm{Aut}(F)$ the cyclic group of order s generated by Frob_p.

We extend this result to the more general case where the ground field $\mathbb{F}_p$ is replaced by any finite field.

Theorem 27. *[Galois theory for finite fields]*

Let F be a finite field with q elements and K a finite extension of F of degree s. Then the extension K/F is Galois with Galois group $\mathrm{Gal}(K/F) = \mathrm{Aut}_F(K)$ *the cyclic group generated by the Frobenius* Frob_q. *Define* $G = \mathrm{Gal}(K/F)$.

$$\begin{array}{cc} & K \\ s/d & | \\ & E \\ d & | \\ & F \end{array} \Big) s$$

There is a bijection between
(i) the divisors d of s.
(ii) the subfields E of K containing F
(iii) the subgroups H of G.
• If E is a subfield of K containing F, then the degree $d = [K : E]$ of E over K divides s, the number of elements in E is q^d, the extension K/F is Galois with Galois group the unique subgroup H of G of order d, which is the subgroup generated by Frob_{q^d}*; furthermore, H is the subgroup of G which consists of the elements $\sigma \in G$ such that $\sigma(x) = x$ for all $x \in E$.*
• Conversely, if d divides s, then K has a unique subfield E with q^d elements, which is the fixed field by Frob_{q^d}*:*

$$E = \{\alpha \in K \mid \mathrm{Frob}_{q^d}(\alpha) = \alpha\},$$

this field E contains F and the Galois group of K over E is the unique subgroup H of G of order d.

Proof. Since G is cyclic generated by Frob_q, there is a bijection between the divisors d of s and the subgroups H of G: for $d|s$, the unique subgroup of G of order s/d (which means of index d) is the cyclic subgroup generated by Frob_{q^d}. The fixed field of H, which is by definition the set of x in K satisfying $\sigma(x) = x$ for all $\sigma \in H$, is the fixed field of Frob_{q^d}, hence it is the unique subfield of E with q^d elements; the degree of K over E is therefore d. If E is the subfield of K with q^d elements, then the Galois group of K/E is the cyclic group generated by Frob_{q^d}. □

Under the hypotheses of Theorem 27, the Galois group of E over F is the quotient $\mathrm{Gal}(K/F)/\mathrm{Gal}(K/E)$.

Exercise 28.
Let F be a field, m and n two positive integers.
(a) Let r be the remainder of the Euclidean division of n by m in $\mathbb{Z}$. Prove that the remainder of the Euclidean division of $X^n - 1$ by $X^m - 1$ in $F[X]$ is $X^r - 1$.
(b) Check

$$\gcd(X^n - 1, X^m - 1) = X^{\gcd(m,n)} - 1.$$

(c) Let further a and b be two integers ≥ 2. Prove that the following conditions are equivalent.
(i) n divides m.
(ii) In $F[X]$, the polynomial $X^n - 1$ divides $X^m - 1$.
(iii) $a^n - 1$ divides $a^m - 1$.
(ii') In $F[X]$, the polynomial $X^{a^n} - X$ divides $X^{a^m} - X$.
(iii') $b^{a^n} - b$ divides $b^{a^m} - b$.

Let F be a finite field with q^m elements and let $n \geq 1$. Then F contains a subfield with n elements if and only if n divides m. In this case, such a subfield is unique.

Fix an algebraic closure $\overline{\mathbb{F}}_p$ of $\mathbb{F}_p$. For each $s \geq 1$, denote by $\mathbb{F}_{p^s}$ the unique subfield of Ω with p^s elements. For n and m positive integers, we have the following equivalence:

$$\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m} \iff n \text{ divides } m. \tag{29}$$

If these conditions are satisfied, then $\mathbb{F}_{p^m}/\mathbb{F}_{p^n}$ is cyclic, with Galois group of order m/n generated by Frob_{p^n}.

Let $F \subset \overline{\mathbb{F}}_p$ be a finite field of characteristic p with q elements and let x be an element in $\overline{\mathbb{F}}_p$. The conjugates of x over F are the roots in $\overline{\mathbb{F}}_p$ of the irreducible polynomial of x over F and these are exactly the images of x by the iterated Frobenius Frob_{q^i}, $i \geq 0$.

Two fields with p^s elements are isomorphic (cf. Theorem 24), but if $s \geq 2$, there is no unicity of such an isomorphic, because the set of automorphisms of $\mathbb{F}_{p^s}$ has more than one element (indeed, it has s elements).

`Remarks.`

- The additive group $(F, +)$ of a finite field F with q elements is cyclic if and only if q is a prime number.
- The multiplicative group $(F^\times, \times)$ of a finite field F with q elements is cyclic, hence, is isomorphic to the additive group $\mathbb{Z}/(q-1)\mathbb{Z}$.
- A finite field F with q elements is isomorphic to the ring $\mathbb{Z}/q\mathbb{Z}$ if and only if q is a prime number (which is equivalent to saying that $\mathbb{Z}/q\mathbb{Z}$ has no zero divisor).

Example 30 (`Simplest example of a finite field which is not a prime field).` A field F with 4 elements has two elements besides 0 and 1. These two elements play exactly the same role: the map which permutes them and sends 0 to 0 and 1 to 1 is an automorphism of F: this automorphism is nothing else than Frob_2. Select one of these two elements, call it j. Then j is a generator of the multiplicative group $F^\times$, which means that $F^\times = \{1, j, j^2\}$ and $F = \{0, 1, j, j^2\}$.

Here are the addition and multiplication tables of this field F:

$(F,+)$	0	1	j	j^2
0	0	1	j	j^2
1	1	0	j^2	j
j	j	j^2	0	1
j^2	j^2	j	1	0

$(F,\times)$	0	1	j	j^2
0	0	0	0	0
1	0	1	j	j^2
j	0	j	j^2	1
j^2	0	j^2	1	j

There are 4 polynomials of degree 2 over $\mathbb{F}_2$, three which split in $\mathbb{F}_2$, namely X^2, $X^2+1 = (X+1)^2$ and $X^2 + X = X(X+1)$ and just one which is irreducible, $X^2 + X + 1$, the roots of which are the elements of F other than 0 and 1.

Example 31 (`The field` $\mathbb{F}_5$`).` .

Denote by i and $-i$ the two roots of $X^2 + 1$; one of them is 2, the other is 3. We have $\mathbb{F}_5 = \{0, 1, -1, i, -i\}$. If we do not specify our choice, we cannot tell what is $i + 1$ for instance: it is $-i$ if we select $i = 2$ and it is -1 if we select $i = 3$. Notice that there is no automorphism of $\mathbb{F}_5$ mapping i to $-i$.

Exercise 32. Check the following isomorphisms and give a generator of the multiplicative group of non–zero elements in the field.
(a) $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2 + X + 1)$.
(b) $\mathbb{F}_8 = \mathbb{F}_2[X]/(X^3 + X + 1)$.
(c) $\mathbb{F}_{16} = \mathbb{F}_2[X]/(X^4 + X + 1)$.
(d) $\mathbb{F}_{16} = \mathbb{F}_2[X, Y]/(Y^2 + Y + 1, X^2 + X + Y)$.

Exercise 33. (a) Give the list of all irreducible polynomials of degree ≤ 5 over $\mathbb{F}_2$.
(b) Give the list of all monic irreducible polynomials of degree ≤ 2 over $\mathbb{F}_4$.

Recall (Theorem 27) that any finite extension of a finite field is Galois. Hence, in a finite field F, any irreducible polynomial is separable: *finite fields are perfect*.

Normal basis Theorem

Theorem 34 (Normal basis theorem)**.** *Given a finite extension $L \supset K$ of finite fields, there exists an element α in $L^\times$ such that the conjugates of α over K form a basis of the vector space L over K. With such a basis, the Frobenius map* Frob_q*, where q is the number of elements in K, becomes a shift operator on the coordinates.*

The normal basis Theorem may be viewed as an additive analog of the cyclicity of the multiplicative group of a finite field (cf. Exercise 38).
`Remark`. The normal basis Theorem holds in zero characteriztic: given any finite Galois extension L/K, there exists $\alpha \in L$ such that the conjugates of α give a basis of the K vector space L.

Proof of Theorem 34.
Let σ be a generator of G. The elements of G are distinct characters of $L^\times$, namely homomorphisms of multiplicative groups $L^\times \to L^\times$ and therefore they are linearly independent by Dedekind Theorem (*theorem of linear independence of characters*). We now consider σ as an endomorphism of the K–vector space L: since $1, \sigma, \ldots, \sigma^{d-1}$ are linearly independent over K, with $d = [L : K]$, the minimal polynomial of the endomorphism σ is $X^d - 1$, which is also the characteristic polynomial of this endomorphism. It follows that there is a cyclic vector, which is an element α in L solution of our problem.

For such a basis $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{d-1}}$, an element γ in L has coordinates $a_0, a_1, \ldots, a_{d-1}$ with

$$\gamma = a_0\alpha + a_1\alpha^q + a_2\alpha^{q^2} + \cdots + a_{d-1}\alpha^{q^{d-1}},$$

and the image of γ under the Frobenius map Frob_q is

$$\gamma^q = a_{d-1} + a_0\alpha^q + a_1\alpha^{q^2} + \cdots + a_{d-2}\alpha^{q^{d-1}},$$

the coordinates of which are $a_{d-1}, a_0, a_1, \ldots, a_{d-2}$. Hence the Frobenius is a shift operator on the coordinates. □

`Remark`. For $\alpha \in L$, a necessary and sufficient condition for the conjugates of α to give a basis of L over K is

$$\det\big(\tau^{-1}\sigma(\alpha)\big)_{\tau,\sigma\in G} \neq 0.$$

Exercise 35.
(a) Let G be a group, N be a normal subgroup of finite index in G and H a subgroup of G. Show that the index of $H \cap N$ in H is finite and divides the index of N in G. Deduce that if $H \cap N = \{1\}$, then H is finite and its order divides the index of N in G.
(b) Let L/K be a finite abelian extension and E_1, E_2 two subfields of L containing K. Assume that the compositum of E_1 and E_2 is L. Show that $[L : E_1]$ divides $[E_2 : K]$.
(c) Let F be a finite field, E an extension of F and α, β two elements in E which are algebraic over F of degree respectively a and b. Assume a and b are relatively prime. Prove that $[F(\alpha, \beta) : F] = ab$ and that

$$F(\alpha, \beta) = F(\alpha + \beta).$$

One of the main results of the theory of finite fields is the following:

Theorem 36. *Let F be a finite field with q elements, α an element in an algebraic closure of F. There exist integers $\ell \geq 1$ such that $\alpha^{q^\ell} = \alpha$. Denote by n the smallest:*

$$n = \min\{\ell \geq 1 \ \mid \ \mathrm{Frob}_q^\ell(\alpha) = \alpha\}.$$

Then the field $F(\alpha)$ has q^n elements, which means that the degree of α over F is n and the minimal polynomial of α over F is

$$\prod_{\ell=0}^{n-1} \left(X - \mathrm{Frob}_q^\ell(\alpha)\right) = \prod_{\ell=0}^{n-1} \left(X - \alpha^{q^\ell}\right). \tag{37}$$

Proof. Since F is finite, the set of α^{q^ℓ} with $\ell \geq 0$ is finite, hence there exists $\ell_1 > \ell_2$ such that $\alpha^{q^{\ell_1}} = \alpha^{q^{\ell_2}}$. Recall that the Frobenius Frob_q is an automorphism; we apply $\mathrm{Frob}_q^{-\ell_2}$ and get $\alpha^{q^\ell} = \alpha$ with $\ell = \ell_1 - \ell_2$.

Define $s = [F(\alpha) : F]$. By Theorem 27, the extension $F(\alpha)/F$ is Galois with Galois group the cyclic group of order s generated by Frob_q. The conjugates of α over F are the elements $\mathrm{Frob}_q^i(\alpha)$, $0 \leq i \leq s-1$. Hence $s = n$. □

4.2 Trace and Norm

Let F be a finite field with q elements and let E be a finite extension of degree s of F. For $\alpha \in E$, the *trace of α from E to F* is the sum of the conjugates, while the *norm of α from E to F* is the product of the conjugates of α over F :

$$\mathrm{Tr}_{E/F}(\alpha) = \sum_{i=0}^{s-1} \mathrm{Frob}_q^i(\alpha) = \sum_{i=0}^{s-1} \alpha^{q^i}, \quad \mathrm{N}_{E/F}(\alpha) = \prod_{i=0}^{s-1} \mathrm{Frob}_q^i(\alpha) = \alpha^{(q^s-1)/(q-1)}.$$

For $\alpha \in F$, we have $\mathrm{Tr}_{E/F}(\alpha) = s\alpha$ and $\mathrm{N}_{E/F}(\alpha) = \alpha^s$.

The trace $\mathrm{Tr}_{E/F}$ is a F–linear map from E onto F (a linear form). The kernel is the set of roots of the polynomial $X + X^q + \cdots + X^{q^{s-1}}$ in E, it has at most q^{s-1} elements, hence there exists $\gamma \in E$ such that $\mathrm{Tr}_{E/F}(\gamma) \neq 0$. It follows that this linear form is surjective, hence its kernel has q^{s-1} elements. Therefore for each $\delta \in F$ there are q^{s-1} elements α in E such that $\mathrm{Tr}_{E/F}(\alpha) = \delta$.

Let $\beta \in E$, $\beta \neq 0$; there exists α such that $\alpha\beta$ is not in the kernel of $\mathrm{Tr}_{E/F}$. Hence the linear form $\alpha \mapsto \mathrm{Tr}_{E/F}(\alpha\beta)$ is not 0. It follows that for $\beta_1 \neq \beta_2$ in E, the two linear forms $\alpha \mapsto \mathrm{Tr}_{E/F}(\alpha\beta_1)$ and

$\alpha \mapsto \mathrm{Tr}_{E/F}(\alpha\beta_2)$ are distinct. Hence the set of linear forms $\alpha \mapsto \mathrm{Tr}_{E/F}(\alpha\beta)$ is the set of all linear forms on E, which is the dual of E as an F–vector space. It is an F–vector space of dimension s.

A similar result holds for the norm: the map $\alpha \mapsto \mathrm{N}_{E/F}(\alpha)$ is a homomorphism from the multiplicative group $E^\times$ to $F^\times$, its kernel has at most $(q^r-1)/(q-1)$ elements and its image at most $q-1$ elements, hence the kernel has $(q^r-1)/(q-1)$ elements and the image $q-1$ elements: the norm is surjective, for each $\delta \in F^\times$ there are $(q^r-1)/(q-1)$ elements $\alpha \in E$ such that $\mathrm{N}_{E/F}(\alpha) = \delta$.

Exercise 38. (Hilbert Theorem 90). *This is the version, for finite fields, of a theorem on cyclic extensions due to Kummer (1855), namely the 90th theorem of Hilbert's Zahlbericht (1897).*
Let F be a finite field with q elements and E be a finite extension of F.
(a) *Additive version.*
Prove that for $\alpha \in E$, the condition $\mathrm{Tr}_{E/F}(\alpha) = 0$ is equivalent to the existence of $\beta \in E$ such that $\alpha = \beta^q - \beta$.
(b) *Multiplicative version.*
Prove that for $\alpha \in E^\times$, the condition $\mathrm{N}_{E/F}(\alpha) = 1$ is equivalent to the existence of $\beta \in E^\times$ such that $\alpha = \beta^q/\beta$.

Exercise 39. (Artin–Schreier extensions).
Let p be a prime number, r a positive integer and $\mathbb{F}_q$ a finite field with $q = p^r$ elements.
(a) Denote by u_r and t_r the maps $\mathbb{F}_q \to \mathbb{F}_q$ defined by

$$u_r(\alpha) = \alpha^p - \alpha, \qquad t_r(\alpha) = \alpha + \alpha^p + \cdots + \alpha^{p^{r-1}}.$$

Check that u_r and t_r are $\mathbb{F}_p$–linear endomorphisms of $\mathbb{F}_q$, that $\ker u_r = \mathbb{F}_p$, $\mathrm{im}(u_r) = \ker t_r$ and $\mathrm{im}(t_r) = \mathbb{F}_p$. In other terms the sequence

$$\{0\} \longrightarrow \mathbb{F}_p \longrightarrow \mathbb{F}_q \xrightarrow{u_r} \mathbb{F}_q \xrightarrow{t_r} \mathbb{F}_p \longrightarrow \{0\}$$

is exact.
(b) Check

$$\prod_{a \in \mathbb{F}_p} (X + X^p + \cdots + X^{p^{r-1}} - a) = X^{p^r} - X.$$

(c) Let Ω be an algebraic closure of $\mathbb{F}_q$, let $\gamma \in \Omega$ and let $r = [\mathbb{F}_p(\gamma) : \mathbb{F}_p]$. Prove that
(i) If $t_r(\gamma) = 0$, then the polynomial $X^p - X - \gamma$ splits completely in $\mathbb{F}_{p^r}$.
(ii) If $t_r(\gamma) \neq 0$, then the polynomial $X^p - X - \gamma$ is irreducible over $\mathbb{F}_{p^r}$.
Example. For each $a \in \mathbb{F}_p^\times$, the polynomial $X^p - X - a$ is irreducible over $\mathbb{F}_p$.

Exercise 40. (a) Let F be a finite field, E a finite extension of F and α a generator of the cyclic group $E^\times$. Check that $\mathrm{N}_{E/F}(\alpha)$ is a generator of the cyclic group $F^\times$.
(b) Deduce that the norm $\mathrm{N}_{E/F}$ induces a surjective morphism from $E^\times$ onto $F^\times$.
(c) Given extensions of finite fields $K \subset F \subset E$, check $\mathrm{N}_{E/K} = \mathrm{N}_{E/F} \circ \mathrm{N}_{F/K}$.
(d) For $x \in F$, define

$$\left(\frac{a}{F}\right) = \begin{cases} 0 & \text{if } a = 0 \\ 1 & \text{if } a \text{ is a non–zero square in } F \\ -1 & \text{if } a \text{ is not a square in } F. \end{cases}$$

Hence Legendre symbol (Exercise 13) is

$$\left(\frac{a}{p}\right) = \left(\frac{\alpha}{\mathbb{F}_p}\right)$$

for $a \in \mathbb{Z}$ and $\alpha = a \pmod p \in \mathbb{F}_p$. Check that if F has q elements with q odd, then, for $a \in F$,

$$\left(\frac{a}{F}\right) = a^{(q-1)/2}.$$

Deduce, for $a \in E$,

$$\left(\frac{a}{E}\right) = \left(\frac{\mathrm{N}_{E/F}(a)}{F}\right).$$

Exercise 41. Let $\mathbb{F}_q$ be a finite field of odd characteristic p with $q = p^r$ elements.
(a) Check -1 is a square if and only if $q \equiv 1 \mod 4$.
(b) Assume $p \equiv -1 \mod 4$. Let i be a root of $X^2 + 1$ in $\mathbb{F}_{p^2}$. For a and b in $\mathbb{F}_p$, check

$$(a + ib)^p = a - ib.$$

(Automorphisms of $\mathbb{F}_{p^2}$).
(c) Let p be a Mersenne prime, $p = 2^\ell - 1$ with ℓ prime. Check that for a and b in $\mathbb{F}_p$, $a + ib$ is a generator of the cyclic group $\mathbb{F}_{p^2}^\times$ if and only if $a^2 + b^2$ is a generator of the cyclic group $\mathbb{F}_p^\times$.

Exercise 42. (a) Let $n \geq 1$. Prove that any prime divisor of $2^n + 1$ is congruent to 1 modulo $2n$.
(b) From (a) it follows that the prime divisors of the Fermat number $F_5 = 2^{2^5} + 1$ are congruent to 1 modulo 64. Check that F_5 is divisible by 641, without performing the division $4\,294\,967\,297 = 641 \cdot 6\,700\,417$ but only using $641 = 5^4 + 2^4 = 5 \cdot 2^7 + 1$.

4.3 Cyclotomic polynomials

Let n be a positive integer. A *n–th root of unity* in a field K is an element of $K^\times$ which satifies $x^n = 1$. This means that it is a torsion element of order dividing n.

A *primitive n–th root of unity* is an element of $K^\times$ of order n: for k in $\mathbb{Z}$, the equality $x^k = 1$ holds if and only if n divides k.

For each positive integer n, the n–th roots of unity in F form a finite subgroup of $F_{\mathrm{tors}}^\times$ having at most n elements. The union of all these subgroups of $F_{\mathrm{tors}}^\times$ is just the torsion group $F_{\mathrm{tors}}^\times$ itself. This group contains 1 and -1, but it could have just one element, like for $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{F}_2(X)$ for instance. The torsion subgroup of $\mathbb{R}^\times$ is $\{\pm 1\}$, the torsion subgroup of $\mathbb{C}^\times$ is infinite.

Let K be a field of finite characteristic p and let n be a positive integer. Write $n = p^r m$ with $r \geq 0$ and $\gcd(p, m) = 1$. In $K[X]$, we have

$$X^n - 1 = (X^m - 1)^{p^r}.$$

If $x \in K$ satisfies $x^n = 1$, then $x^m = 1$. Therefore, the order of a finite subgroup of $K^\times$ is prime to p.

It also follows that the study of $X^n - 1$ reduces to the study of $X^m - 1$ with m prime to p.

Let n be a positive integer and Ω be an algebraically closed field of characteristic either 0 or a prime number not dividing n. Then the number of primitive n-th roots of unity in Ω is $\varphi(n)$. These $\varphi(n)$ elements are the generators of the unique cyclic subgroup C_n of order n of $\Omega^\times$, which is the group of n-th roots of unity in Ω:

$$C_n = \{x \in \Omega \mid x^n = 1\}.$$

4.3.1 Cyclotomic polynomials over $\mathbb{C}[X]$

The map $\mathbb{C} \to \mathbb{C}^\times$ defined by $z \mapsto e^{2i\pi z/n}$ is a morphism from the additive group $\mathbb{C}$ to the multiplicative group $\mathbb{C}^\times$; this morphism has kernel $n\mathbb{Z}$. Hence, it factors to an injective morphism from the group $\mathbb{C}/n\mathbb{Z}$ to $\mathbb{C}^\times$: we denote it also by $z \mapsto e^{2i\pi z/n}$. In particular $e^{2i\pi z/n}$ makes sense for $z \in \mathbb{Z}/n\mathbb{Z}$. The unique subgroup of order n in $\mathbb{C}/n\mathbb{Z}$ is $\mathbb{Z}/n\mathbb{Z}$, its image under $z \mapsto e^{2i\pi z/n}$ is $\mu_n \subset \mathbb{C}^\times$.

For n a positive integer, we define a polynomial $\Phi_n(X) \in \mathbb{C}[X]$ by

$$\Phi_n(X) = \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^\times} (X - e^{2i\pi k/n}). \tag{43}$$

This polynomial is called the *cyclotomic polynomial of index* n; it is monic and has degree $\varphi(n)$. Since

$$X^n - 1 = \prod_{k=0}^{n-1} (X - e^{2i\pi k/n}),$$

the partition of the set of roots of unity according to their order shows that

$$X^n - 1 = \prod_{\substack{1 \le d \le n \\ d \mid n}} \Phi_d(X). \tag{44}$$

The degree of $X^n - 1$ is n and the degree of $\Phi_d(X)$ is $\varphi(d)$, hence, Lemma 5 follows also from (44).

The name **cyclotomy** comes from the Greek and means *divide the circle*. The complex roots of $X^n - 1$ are the vertices of a regular polygon with n sides.

From (44), it follows that an equivalent definition of the polynomials $\Phi_1, \Phi_2, \ldots$ in $\mathbb{Z}[X]$ is by induction on n:

$$\Phi_1(X) = X - 1, \qquad \Phi_n(X) = \frac{X^n - 1}{\displaystyle\prod_{\substack{d \ne n \\ d \mid n}} \Phi_d(X)}. \tag{45}$$

This is the most convenient way to compute the cyclotomic polynomials Φ_n for small values of n.

Möbius inversion formula (see the second form in § 3.4 with G the multiplicative group $\mathbb{Q}(X)^\times$) yields

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

Notice that for $m \ge 3$, the polynomial Φ_m has real coefficients (in fact integer coefficients) and no real root, hence its degree $\varphi(m)$ is even.

First examples. One has

$$\Phi_2(X) = \frac{X^2 - 1}{X - 1} = X + 1, \quad \Phi_3(X) = \frac{X^3 - 1}{X - 1} = X^2 + X + 1,$$

and more generally, for p prime

$$\Phi_p(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + X + 1.$$

The next cyclotomic polynomials are

$$\Phi_4(X) = \frac{X^4 - 1}{X^2 - 1} = X^2 + 1 = \Phi_2(X^2),$$

$$\Phi_6(X) = \frac{X^6 - 1}{(X^3 - 1)(X + 1)} = \frac{X^3 + 1}{X + 1} = X^2 - X + 1 = \Phi_3(-X).$$

The next page is reproduced from
https://en.wikipedia.org/wiki/Cyclotomic_polynomial

$$\Phi_1(x) = x - 1$$
$$\Phi_2(x) = x + 1$$
$$\Phi_3(x) = x^2 + x + 1$$
$$\Phi_4(x) = x^2 + 1$$
$$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$$
$$\Phi_6(x) = x^2 - x + 1$$
$$\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$
$$\Phi_8(x) = x^4 + 1$$
$$\Phi_9(x) = x^6 + x^3 + 1$$
$$\Phi_{10}(x) = x^4 - x^3 + x^2 - x + 1$$
$$\Phi_{11}(x) = x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$
$$\Phi_{12}(x) = x^4 - x^2 + 1$$
$$\Phi_{13}(x) = x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$
$$\Phi_{14}(x) = x^6 - x^5 + x^4 - x^3 + x^2 - x + 1$$
$$\Phi_{15}(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$$
$$\Phi_{16}(x) = x^8 + 1$$
$$\Phi_{17}(x) = x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$
$$\Phi_{18}(x) = x^6 - x^3 + 1$$
$$\Phi_{19}(x) = x^{18} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$
$$\Phi_{20}(x) = x^8 - x^6 + x^4 - x^2 + 1$$
$$\Phi_{21}(x) = x^{12} - x^{11} + x^9 - x^8 + x^6 - x^4 + x^3 - x + 1$$
$$\Phi_{22}(x) = x^{10} - x^9 + x^8 - x^7 + x^6 - x^5 + x^4 - x^3 + x^2 - x + 1$$
$$\Phi_{23}(x) = x^{22} + x^{21} + x^{20} + x^{19} + x^{18} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$
$$\Phi_{24}(x) = x^8 - x^4 + 1$$
$$\Phi_{25}(x) = x^{20} + x^{15} + x^{10} + x^5 + 1$$
$$\Phi_{26}(x) = x^{12} - x^{11} + x^{10} - x^9 + x^8 - x^7 + x^6 - x^5 + x^4 - x^3 + x^2 - x + 1$$
$$\Phi_{27}(x) = x^{18} + x^9 + 1$$
$$\Phi_{28}(x) = x^{12} - x^{10} + x^8 - x^6 + x^4 - x^2 + 1$$
$$\Phi_{29}(x) = x^{28} + x^{27} + x^{26} + x^{25} + x^{24} + x^{23} + x^{22} + x^{21} + x^{20} + x^{19} + x^{18} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$
$$\Phi_{30}(x) = x^8 + x^7 - x^5 - x^4 - x^3 + x + 1.$$

It is known that if n has at most two odd prime divisors, then the coefficients of Φ_n are 0, 1 or -1.

The least integer that has three distinct odd prime divisors is 105. In the polynomial Φ_{105}, the coefficients of x^7 and x^{41} are -2:

$$\Phi_{105}(x) = x^{48} + x^{47} + x^{46} - x^{43} - x^{42} - 2x^{41} - x^{40} - x^{39} + x^{36} + x^{35} + x^{34} + x^{33} + x^{32} + x^{31} - x^{28} - x^{26} - x^{24} - x^{22} - x^{20} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} - x^9 - x^8 - 2x^7 - x^6 - x^5 + x^2 + x + 1.$$

Exercise 46.
(a) Let $n \geq 2$ be an integer. Denote by R the radical (maximal square free factor) of n, namely the product of the prime factors of n. Check

$$\phi_n(X) = \phi_R(X^{n/R}). \tag{47}$$

(b) Let p be a prime number and let m_1 a positive integer prime to p. Set $m = pm_1$. Prove

$$\Phi_{m_1}(X^p) = \Phi_m(X)\Phi_{m_1}(X).$$

(c) Let p be a prime number and m a positive integer multiple of p. Write $m = p^r m_1$ with $\gcd(p, m_1) = 1$ and $r \geq 1$. Deduce from (a) and (b)

$$\Phi_{m_1}(X^{p^r}) = \Phi_m(X)\Phi_{m_1}(X^{p^{r-1}}).$$

(d) For $r \geq 0$, p prime and m a multiple of p, check

$$\Phi_{p^r m}(X) = \Phi_m(X^{p^r}) \text{ and } \varphi(p^r m) = p^r \varphi(m).$$

Deduce

$$\Phi_{p^r}(X) = X^{p^{r-1}(p-1)} + X^{p^{r-1}(p-2)} + \cdots + X^{p^{r-1}} + 1 = \Phi_p(X^{p^{r-1}})$$

when p is a prime and $r \geq 1$ (also a consequence of (47)).

(e) Let n be a positive integer. Prove

$$\varphi(2n) = \begin{cases} \varphi(n) & \text{if } n \text{ is odd,} \\ 2\varphi(n) & \text{if } n \text{ is even,} \end{cases}$$

$$\Phi_{2n}(X) = \begin{cases} -\Phi_1(-X) & \text{if } n = 1, \\ \Phi_n(-X) & \text{if } n \text{ is odd and} \geq 3, \\ \Phi_n(X^2) & \text{if } n \text{ is even.} \end{cases}$$

Deduce, for $\ell \geq 1$ and for m odd ≥ 3,

$$\Phi_{2^\ell}(X) = X^{2^{\ell-1}} + 1$$
$$\Phi_{2^\ell m}(X) = \Phi_m(-X^{2^{\ell-1}}),$$
$$\Phi_m(X)\Phi_m(-X) = \Phi_m(X^2).$$

(f) Check, for $n \geq 1$,

$$\Phi_n(1) = \begin{cases} 0 & \text{for } n = 1, \\ p & \text{if } n = p^r \text{ with } p \text{ prime and } r \geq 1; \\ 1 & \text{otherwise.} \end{cases}$$

(g) Check, for $n \geq 1$,

$$\Phi_n(-1) = \begin{cases} -2 & \text{for } n = 1, \\ 1 & \text{if } n \text{ is odd} \geq 3; \\ \Phi_{n/2}(1) & \text{if } n \text{ is even.} \end{cases}$$

In other terms, for $n \geq 3$,

$$\Phi_n(-1) = \begin{cases} p & \text{if } n = 2p^r \text{ with } p \text{ a prime and } r \geq 1; \\ 1 & \text{if } n \text{ is odd or if } n = 2m \text{ where } m \text{ has at least two distinct prime divisors.} \end{cases}$$

Theorem 48. *For any positive integer n, the polynomial $\Phi_n(X)$ has its coefficients in $\mathbb{Z}$. Moreover, $\Phi_n(X)$ is irreducible in $\mathbb{Z}[X]$.*

Proof of the first part of Theorem 48. We check $\Phi_n(X) \in \mathbb{Z}[X]$ by induction on n. The results holds for $n = 1$, since $\Phi_1(X) = X - 1$. Assume $\Phi_m(X) \in \mathbb{Z}[X]$ for all $m < n$. From the induction hypothesis, it follows that

$$h(X) = \prod_{\substack{d|n \\ d \neq n}} \Phi_d(X)$$

is monic with coefficients in $\mathbb{Z}$. We divide $X^n - 1$ by h in $\mathbb{Z}[X]$: let $Q \in \mathbb{Z}[X]$ be the quotient and $R \in \mathbb{Z}[X]$ the remainder:

$$X^n - 1 = h(X)Q(X) + R(X).$$

We also have $X^n - 1 = h(X)\Phi_n(X)$ in $\mathbb{C}[X]$, as shown by (44). From the unicity of the quotient and remainder in the Euclidean division in $\mathbb{C}[X]$, we deduce $Q = \Phi_n$ and $R = 0$, hence, $\Phi_n \in \mathbb{Z}[X]$. □

We now show that Φ_n is irreducible in $\mathbb{Z}[X]$. Since it is monic, its content is 1. It remains to check that it is irreducible in $\mathbb{Q}[X]$.

Here is a proof of the irreducibility of the cyclotomic polynomial in the special case where the index is a prime number p. It rests on Eisenstein's Criterion:

Proposition 49 (Eisenstein criterion)**.** *Let*

$$C(X) = c_0X^d + \cdots + c_d \in \mathbb{Z}[X]$$

and let p be a prime number. Assume C to be product of two polynomials in $\mathbb{Z}[X]$ of positive degrees. Assume also that p divides c_i for $1 \leq i \leq d$ but that p does not divide c_0. Then p^2 divides c_d.

Proof. Let

$$A(X) = a_0X^n + \cdots + a_n \quad \text{and} \quad B(X) = b_0X^m + \cdots + b_m$$

be two polynomials in $\mathbb{Z}[X]$ of degrees m and n such that $C = AB$. Hence, $d = m + n$, $c_0 = a_0b_0$, $c_d = a_nb_m$. We use the morphism (9) of reduction modulo p, namely $\Psi_p : \mathbb{Z}[X] \longrightarrow \mathbb{F}_p[X]$. Write $\tilde{A} = \Psi_p(A)$, $\tilde{B} = \Psi_p(B)$, $\tilde{C} = \Psi_p(C)$,

$$\tilde{A}(X) = \tilde{a}_0X^n + \cdots + \tilde{a}_n, \quad \tilde{B}(X) = \tilde{b}_0X^m + \cdots + \tilde{b}_m$$

and

$$\tilde{C}(X) = \tilde{c}_0 X^d + \cdots + \tilde{c}_d.$$

By assumption $\tilde{c}_0 \neq 0$, $\tilde{c}_1 = \cdots = \tilde{c}_d = 0$, hence, $\tilde{C}(X) = \tilde{c}_0 X^d = \tilde{A}(X)\tilde{B}(X)$ with $\tilde{c}_0 = \tilde{a}_0\tilde{b}_0 \neq 0$. Now $\tilde{A}$ and $\tilde{B}$ have positive degrees n and m, hence, $\tilde{a}_n = \tilde{b}_m = 0$, which means that p divides a_n and b_m and, therefore, p^2 divides $c_d = a_n b_m$. □

Proof of the irreducibility of Φ_p over $\mathbb{Z}$ in Theorem 48 for p prime. We set $X - 1 = Y$, so that

$$\Phi_p(Y+1) = \frac{(Y+1)^p - 1}{Y} = Y^{p-1} + \binom{p}{1} Y^{p-2} + \cdots + \binom{p}{2} Y + p \in \mathbb{Z}[Y].$$

We observe that p divides all coefficients – but the leading one – of the monic polynomial $\Phi_p(Y+1)$ and that p^2 does not divide the constant term. We conclude by using Eisenstein's Criterion Proposition 49. □

We now complete the proof of Theorem 48.

Proof of the irreducibility of Φ_n over $\mathbb{Z}$ in Theorem 48 for all n. Let $f \in \mathbb{Z}[X]$ be an irreducible factor of Φ_n with a positive leading coefficient and let $g \in \mathbb{Z}[X]$ satisfy $fg = \Phi_n$. Our goal is to prove $f = \Phi_n$ and $g = 1$.

Since Φ_n is monic, the same is true for f and g. Let ζ be a root of f in $\mathbb{C}$ and let p be a prime number which does not divide n. Since ζ^p is a primitive n-th root of unity, it is a zero of Φ_n.

The first and main step of the proof is to check that $f(\zeta^p) = 0$. If ζ^p is not a root of f, then it is a root of g. We assume $g(\zeta^p) = 0$ and we will reach a contradiction.

Since f is irreducible, f is the minimal polynomial of ζ, hence, from $g(\zeta^p) = 0$, we infer that $f(X)$ divides $g(X^p)$. Write $g(X^p) = f(X)h(X)$ and consider the morphism Ψ_p of reduction modulo p already introduced in (9). Denote by F, G, H the images of f, g, h. Recall that $fg = \Phi_n$ in $\mathbb{Z}[X]$, hence, $F(X)G(X)$ divides $X^n - 1$ in $\mathbb{F}_p[X]$. The assumption that p does not divide n implies that $X^n - 1$ has no square factor in $\mathbb{F}_p[X]$.

Let $P \in \mathbb{Z}[X]$ be an irreducible factor of F. From $G(X^p) = F(X)H(X)$, it follows that $P(X)$ divides $G(X^p)$. But $G \in \mathbb{F}_p[X]$, hence (see Lemma 25), $G(X^p) = G(X)^p$ and, therefore, P divides $G(X)$. Now P^2 divides the product FG, which is a contradiction.

We have checked that for any root ζ of f in $\mathbb{C}$ and any prime number p which does not divide n, the number ζ^p is again a root of f. By induction on the number of prime factors of m, it follows that for any integer m with $\gcd(m, n) = 1$ the number ζ^m is a root of f. Now f vanishes at all the primitive n–th roots of unity, hence, $f = \Phi_n$ and $g = 1$. □

Let n be a positive integer. The *cyclotomic field of level n over $\mathbb{Q}$* is

$$R_n = \mathbb{Q}\big(\{e^{2i\pi k/n} \mid k \in (\mathbb{Z}/n\mathbb{Z})^\times\}\big) \subset \mathbb{C}.$$

This is the splitting field of Φ_n over $\mathbb{Q}$. If $\zeta \in \mathbb{C}$ is any primitive n–th root of unity, then $R_n = \mathbb{Q}(\zeta)$ and $\{1, \zeta, \ldots, \zeta^{\varphi(n)-1}\}$ is a basis of R_n as a $\mathbb{Q}$–vector space.

For example we have

$$R_1 = R_2 = \mathbb{Q}, \quad R_3 = R_6 = \mathbb{Q}(j), \quad R_4 = \mathbb{Q}(i),$$

where j is a root of the polynomial $X^2 + X + 1$. It is easy to check that for $n \geq 1$ we have $\varphi(n) = 1$ if and only if $n \in \{1, 2\}$, $\varphi(n) = 2$ if and only if $n \in \{3, 4, 6\}$ and $\varphi(n)$ is even and ≥ 4 for $n \geq 5$ with $n \neq 6$. That $\varphi(n)$, the degree of R_n, tends to infinity with n can be checked in an elementary way.

Exercise 50. *Check*

$$n \leq 2.685\varphi(n)^{1.161}$$

for all $n \geq 1$.

Proposition 51. *There is a canonical isomorphism between* $\mathrm{Gal}(R_n/\mathbb{Q})$ *and the multiplicative group* $(\mathbb{Z}/n\mathbb{Z})^\times$.

Proof. Let ζ_n be a primitive n-th root of unity and let μ_n be the group of n-th roots of unity, which is the subgroup of $\mathbb{C}^\times$ generated by ζ_n. The map $\mathbb{Z} \longrightarrow \mu_n$ which maps m to ζ_n^m is a group homomorphism of kernel $n\mathbb{Z}$. When c is a class modulo n, we denote by ζ^c the image of c under the isomorphism $\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \mu_n$.

For $\sigma \in \mathrm{Gal}(R_n/\mathbb{Q})$, define $\theta(\sigma) \in (\mathbb{Z}/n\mathbb{Z})^\times$ by

$$\sigma(\zeta_n) = \zeta_n^{\theta(\sigma)}.$$

Then θ is well defined and is a group isomorphism from $\mathrm{Gal}(R_n/\mathbb{Q})$ onto $(\mathbb{Z}/n\mathbb{Z})^\times$. □

Example 52. The element τ in $\mathrm{Gal}(R_n/\mathbb{Q})$ such that $\theta(\tau) = -1$ satisfies $\tau(\zeta_n) = \zeta_n^{-1}$. But ζ_n^{-1} is the complex conjugate of ζ_n, since $|\zeta_n| = 1$. Hence τ is the (restriction to R_n of the) complex conjugation.

Assume $n \geq 3$. The subfield of R_n fixed by the subgroup $\theta^{-1}(\{1, -1\})$ of $\mathrm{Gal}(R_n/\mathbb{Q})$ is the maximal real subfield of R_n:

$$R_n^+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1}) = \mathbb{Q}\big(\cos(2\pi/n)\big) = R_n \cap \mathbb{R}$$

with $[R_n : R_n^+] = 2$.

4.3.2 Cyclotomic Polynomials over a finite field

Since Φ_n has coefficients in $\mathbb{Z}$, for any field K, we can view $\Phi_n(X)$ as an element in $K[X]$: in zero characteristic, this is plain since K contains $\mathbb{Q}$; in finite characteristic p, one considers the image of Φ_n under the morphism Ψ_p introduced in (9): we denote again this image by Φ_n.

Proposition 53. *Let* K *be a field and let* n *be a positive integer. Assume that* K *has characteristic either* 0 *or else a prime number* p *prime to* n. *Then the polynomial* $\Phi_n(X)$ *is separable over* K *and its roots in* K *are exactly the primitive* n*–th roots of unity which belong to* K.

Proof. The derivative of the polynomial $X^n - 1$ is nX^{n-1}. In K, we have $n \neq 0$ since p does not divide n, hence, $X^n - 1$ is separable over K. Since $\Phi_n(X)$ is a factor of $X^n - 1$, it is also separable over K. The roots in K of $X^n - 1$ are precisely the n–th roots of unity contained in K. A n-th root of unity is primitive if and only if it is not a root of Φ_d when $d|n$, $d \neq n$. From (45), this means that it is a root of Φ_n. □

Recall that when $n = p^r m$ with $r \geq 0$ and $m \geq 1$, in characteristic p we have

$$X^n - 1 = (X^m - 1)^{p^r}.$$

Therefore, if p divides n, there is no primitive n–th root of unity in a field of characteristic p.

Exercise 54.
The polynomials below are over a field of characteristic p.
(a) Prove that for $r \geq 0$ and $m \geq 1$ with $p \not| m$,

$$\Phi_{p^r m}(X) = \Phi_m(X)^{\varphi(p^r)} \quad \text{with} \quad \varphi(p^r) = \begin{cases} 1 & \text{if } r = 0, \\ p^r - p^{r-1} & \text{if } r \geq 1. \end{cases}$$

(b) Deduce that if p divides m, then in characteristic p we have

$$\Phi_{p^r m}(X) = \Phi_m(X)^{p^r}.$$

According to (12), given $q = p^r$, the unique subfield of $\overline{\mathbb{F}}_p$ with q elements is the set $\mathbb{F}_q$ of roots of $X^q - X$ in $\overline{\mathbb{F}}_p$. The set $\{X - x \mid x \in \mathbb{F}_q\}$ is the set of all monic degree 1 polynomials with coefficients in $\mathbb{F}_q$. Hence, (12) is the special case $n = 1$ of the next statement.

Theorem 55. *Let F be a finite field with q elements and let n be a positive integer.The polynomial $X^{q^n} - X$ is the product of all monic irreducible polynomials in $F[X]$ whose degree divides n. In other terms, for any $n \geq 1$,*

$$X^{q^n} - X = \prod_{d|n} \prod_{f \in E_q(d)} f(X)$$

where $E_q(d)$ is the set all monic irreducible polynomials in $\mathbb{F}_q[X]$ of degree d.

Proof. The derivative of $X^{q^n} - X$ is -1, which has no root, hence, $X^{q^n} - X$ has no multiple factor in characteristic p.

Let $f \in \mathbb{F}_q[X]$ be an irreducible factor of $X^{q^n} - X$, d its degree and α a root of f in $\overline{\mathbb{F}}_p$. The polynomial $X^{q^n} - X$ is a multiple of f, therefore, it vanishes at α, hence, $\alpha^{q^n} = \alpha$, which means $\alpha \in \mathbb{F}_{q^n}$. From the field extensions

$$\mathbb{F}_q \subset \mathbb{F}_q(\alpha) \subset \mathbb{F}_{q^n},$$

we deduce that the degree of α over $\mathbb{F}_q$ divides the degree of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, that is d divides n.

Conversely, let f be an irreducible polynomial in $\mathbb{F}_q[X]$ of degree d where d divides n. Let α be a root of f in $\overline{\mathbb{F}}_p$. The field $\mathbb{F}_q(\alpha)$ has degree d over $\mathbb{F}_q$, hence it has q^d elements; since d divides n, it is a subfield of $\mathbb{F}_{q^n}$, hence $\alpha \in \mathbb{F}_{q^n}$ satisfies $\alpha^{q^n} = \alpha$ and, therefore, f divides $X^{q^n} - X$.

This shows that $X^{q^n} - X$ is a multiple of all irreducible polynomials of degree dividing n.

In the factorial ring $\mathbb{F}_q[X]$, the polynomial $X^{q^n} - X$, having no multiple factor, is the product of the monic irreducible polynomials which divide it. Theorem 55 follows. □

Denote by $N_q(d)$ the number of elements in $E_q(d)$, that is the number of monic irreducible polynomials of degree d in $\mathbb{F}_q[X]$. Theorem 55 yields, for $n \geq 1$,

$$q^n = \sum_{d|n} d N_q(d). \tag{56}$$

From Möbius inversion formula (§ 3.4), one deduces:

$$N_q(n) = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d}.$$

For instance, when ℓ is a prime number,

$$N_q(\ell) = \frac{q^\ell - q}{\ell}. \tag{57}$$

Exercise 58. Let F be a finite field with q elements.
(a) Give the values of $N_2(n)$ for $1 \leq n \leq 6$.
(b) Check, for $n \geq 2$,

$$\frac{q^n}{2n} \leq N_q(n) \leq \frac{q^n}{n}.$$

(c) More precisely, check, for $n \geq 2$,

$$\frac{q^n - q^{\lfloor n/2 \rfloor + 1}}{n} < N_q(n) \leq \frac{q^n - q}{n}.$$

(d) Let F be a finite field of characteristic p. Denote by $\mathbb{F}_p$ the prime subfield of F. Check that more than half of the elements α in F satisfy $F = \mathbb{F}_p(\alpha)$.
(e) Check that when p^n tends to infinity, the probability that a polynomial of degree n over $\mathbb{F}_p$ be irreducible in $\mathbb{F}_p[X]$ tends to $1/n$.

`Remark`. From (c) one deduces that the number $N_q(n)$ of monic irreducible polynomials of degree n over $\mathbb{F}_q$ satisfies

$$N_q(n) = \frac{q^n}{n} + O\left(\frac{q^{n/2}}{n}\right).$$

This *Prime Polynomial Theorem* is the analog for polynomials of the *Prime Number Theorem* which asserts that the number $\pi(x)$ of primes $p \leq x$ is asymptotically equal to

$$\mathrm{Li}(x) = \int_2^x \frac{dt}{\log t} \sim \frac{x}{\log x},$$

while the Riemann Hypothesis is equivalent to the assertion that the remainder term $\pi(x) - \mathrm{Li}(x)$ is bounded above by $x^{1/2+o(1)}$. This analogy takes into account the fact that x is the number of integers $\leq x$ while q^n is the number of monic polynomials of degree n over $\mathbb{F}_q$.

The abstract of the lecture by Will Sawin on *The distribution of prime polynomials over finite fields* on October 29, 2020 at the Number Theory Web Seminar https://www.ntwebseminar.org/ starts with: *Many conjectures in number theory have analogues for polynomials in one variable over a finite field. In recent works with Mark Shusterman, we proved analogues of two conjectures about prime numbers - the twin primes conjecture and the conjecture that there are infinitely many primes of the form $n^2 + 1$.* The analogy is:

Number Theory		*Polynomials*
$\mathbb{Z}$	$\longleftrightarrow$	$\mathbb{F}_q[T]$
$\mathbb{Z}^\times = \{\pm 1\}$	$\longleftrightarrow$	$\mathbb{F}_q[T]^\times = \mathbb{F}_q^\times$
$\mathbb{N}$	$\longleftrightarrow$	monic polynomials
prime numbers	$\longleftrightarrow$	irreducible monic polynomials

4.4 Decomposition of cyclotomic polynomials over a finite field

In all this section, we assume that n is not divisible by the characteristic p of $\mathbb{F}_q$.

We apply Theorem 36 to the cyclotomic polynomials.

Theorem 59. *Let $\mathbb{F}_q$ be a finite field with q elements and let n be a positive integer not divisible by the characteristic of $\mathbb{F}_q$. Then the cyclotomic polynomial Φ_n splits in $\mathbb{F}_q[X]$ into a product of irreducible factors, all of the same degree d, where d is the order of q modulo n.*

Recall (see § 3.2) that the order of q modulo n is by definition the order of the class of q in the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ (hence, it is defined if and only if n and q are relatively prime), it is the smallest integer ℓ such that q^ℓ is congruent to 1 modulo n.

Proof. Let ζ be a root of Φ_n in a splitting field K of the polynomial Φ_n over $\mathbb{F}_q$. The order of ζ in the multiplicative group $K^\times$ is n. According to Theorem 36, the degree of ζ over $\mathbb{F}_q$ is the smallest integer $\ell \geq 1$ such that $\zeta^{q^\ell} = \zeta$, that is $\zeta^{q^\ell - 1} = 1$. Hence it is the smallest positive integer ℓ such that n divides $q^\ell - 1$ and this is the order of the image of q in the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$. □

Since an element $\zeta \in \overline{\mathbb{F}}_p^\times$ has order n in the multiplicative group $\overline{\mathbb{F}}_p^\times$ if and only if ζ is a root of Φ_n, an equivalent statement to Theorem 59 is the following.

Corollary 60. *If $\zeta \in \overline{\mathbb{F}}_p^\times$ has order n in the multiplicative group $\overline{\mathbb{F}}_p^\times$, then its degree $d = [\mathbb{F}_q(\zeta) : \mathbb{F}_q]$ over $\mathbb{F}_q$ is the order of q modulo n.*

The special case $d = 1$ of corollary 60 produces the next result:

Corollary 61. *The polynomial $\Phi_n(X)$ splits completely in $\mathbb{F}_q[X]$ (into a product of linear polynomials) if and only if $q \equiv 1 \bmod n$.*

This follows from Theorem 59, but it is also plain from Proposition 19 and the fact that the cyclic group $\mathbb{F}_q^\times$ of order $q-1$ contains a subgroup of order n if and only if n divides $q-1$, which is the condition $q \equiv 1 \bmod n$.

Exercise 62. Let p and q be two distinct odd primes with at least one of them congruent to 1 modulo 4. Assume that the polynomial $X^q - 1$ splits completely in the finite field $\mathbb{F}_p$. Show that the polynomial $X^2 - q$ splits in $\mathbb{F}_p$.

`Hint.` One may use the Legendre reciprocity law: for p and q distinct odd primes,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}.$$

`Remark`. *Class Field Theory elaborates on such results.*

The special case $d = \varphi(n)$ of corollary 60 produces the next result:

Corollary 63. *The following conditions are equivalent:*
(i) *The polynomial $\Phi_n(X)$ is irreducible in $\mathbb{F}_q[X]$.*
(ii) *The class of q modulo n has order $\varphi(n)$.*
(iii) *q is a generator of the group $(\mathbb{Z}/n\mathbb{Z})^\times$.*

This can be true only when this multiplicative group is cyclic, which means (see Exercise 7) that n is either

$$2,\ 4,\ \ell^s,\ 2\ell^s$$

where ℓ is an odd prime and $s \geq 1$. Any cyclotomic polynomial Φ_n with $n \geq 2$ not in this list is reducible over any finite field (including the fields with characteristic p which divides n - see Exercise 54) while it irreducible over $\mathbb{Z}$.

Exercise 64. What are the degrees of the irreducible factors of the polynomials $\Phi_8(X) = X^4 + 1$ and $\Phi_{12}(X) = X^4 - X^2 + 1$ over a finite field $\mathbb{F}_q$?

Corollary 65. *Let q be a power of a prime, s a positive integer and $n = q^s - 1$. Then q has order s modulo n. Hence, Φ_n splits in $\mathbb{F}_q[X]$ into irreducible factors, all of which have degree s.*

Notice that the number of factors in this decomposition is $\varphi(q^s - 1)/s$, hence it follows that s divides $\varphi(q^s - 1)$.

Numerical examples

Recall that we fix an algebraic closure $\overline{\mathbb{F}}_p$ of the prime field $\mathbb{F}_p$ and for q a power of p we denote by $\mathbb{F}_q$ the unique subfield of $\overline{\mathbb{F}}_p$ with q elements. Of course, $\overline{\mathbb{F}}_p$ is also an algebraic closure of $\mathbb{F}_q$.

Example 66. The field $\mathbb{F}_4$, quadratic extension of $\mathbb{F}_2$ *(see also Example 30).* We consider the quadratic extension $\mathbb{F}_4/\mathbb{F}_2$. There is a unique irreducible polynomial of degree 2 over $\mathbb{F}_2$, which is $\Phi_3 = X^2 + X + 1$. Denote by ζ one of its roots in $\mathbb{F}_4$. The other root is ζ^2 with $\zeta^2 = \zeta + 1$ and

$$\mathbb{F}_4 = \{0,\ 1,\ \zeta,\ \zeta^2\}.$$

If we set $\eta = \zeta^2$, then the two roots of Φ_3 are η and η^2, with $\eta^2 = \eta + 1$ and

$$\mathbb{F}_4 = \{0,\ 1,\ \eta,\ \eta^2\}.$$

There is no way to distinguish these two roots, they play the same role. It is the same situation as with the two roots $\pm i$ of $X^2 + 1$ in $\mathbb{C}$.

In $\mathbb{F}_4$ there are two elements of trace 0 over $\mathbb{F}_2$, namely 0 and 1, and two elements of trace 1, namely ζ and ζ^2. The three elements of $\mathbb{F}_4^\times$ have norm 1 over $\mathbb{F}_2$.

Example 67. The field $\mathbb{F}_8$, cubic extension of $\mathbb{F}_2$. We consider the cubic extension $\mathbb{F}_8/\mathbb{F}_2$. There are 6 elements in $\mathbb{F}_8$ which are not in $\mathbb{F}_2$, each of them has degree 3 over $\mathbb{F}_2$, hence, there are two irreducible polynomials of degree 3 in $\mathbb{F}_2[X]$. Indeed, from (57), it follows that $N_2(3) = 2$. The two irreducible factors of Φ_7 are the only irreducible polynomials of degree 3 over $\mathbb{F}_2$:

$$X^8 - X = X(X + 1)(X^3 + X + 1)(X^3 + X^2 + 1).$$

The $6 = \varphi(7)$ elements in $\mathbb{F}_8^\times$ of degree 3 are the six roots of Φ_7, hence, they have order 7. If ζ is any of them, then

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

Since $[\mathbb{F}_8 : \mathbb{F}_2] = 3$, there are three automorphisms of $\mathbb{F}_8$, namely the identity, Frob_2 and $\mathrm{Frob}_4 = \mathrm{Frob}_2^2$. If ζ is a root of $Q_1(X) = X^3 + X + 1$, then the two other roots are ζ^2 and ζ^4, while the roots of

$Q_2(X) = X^3 + X^2 + 1$ are ζ^3, ζ^5 and ζ^6. Notice that $\zeta^6 = \zeta^{-1}$ and $Q_2(X) = X^3 Q_1(1/X)$. Set $\eta = \zeta^{-1}$. Then

$$\mathbb{F}_8 = \{0,\ 1,\ \eta,\ \eta^2,\ \eta^3,\ \eta^4,\ \eta^5,\ \eta^6\}$$

and

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

For transmission of data, it is not the same to work with ζ or with $\eta = \zeta^{-1}$. For instance, the map $x \mapsto x + 1$ is given by

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

and by

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

In $\mathbb{F}_8$ there are four elements of trace 0 over $\mathbb{F}_2$, namely 0 and the three roots of $X^3 + X + 1$, and four elements of trace 1, namely 1 and the three roots of $X^3 + X^2 + 1$. The seven elements of $\mathbb{F}_8^\times$ have norm 1 over $\mathbb{F}_2$.

Exercise 68. List the values $\alpha \in \mathbb{F}_8^\times$ which are primitive roots in $\mathbb{F}_8$. Next, for each α and for $n = 0, 1, 2, \ldots, 6$, write the table of the discrete logarithm in $\mathbb{F}_8$ with respect to the primitive root α.

Example 69. The field $\mathbb{F}_9$, quadratic extension of $\mathbb{F}_3$. We consider the quadratic extension $\mathbb{F}_9/\mathbb{F}_3$. Over $\mathbb{F}_3$,

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

In $\mathbb{F}_9^\times$, there are $4 = \varphi(8)$ elements of order 8 (the four roots of Φ_8) which have degree 2 over $\mathbb{F}_3$. There are two elements of order 4, which are the roots of Φ_4; they are also the squares of the elements of order 8 and they have degree 2 over $\mathbb{F}_3$, their square is -1. There is one element of order 2, namely -1 and one of order 1, namely 1. From (57), it follows that $N_3(2) = 3$: the three monic irreducible polynomials of degree 2 over $\mathbb{F}_3$ are Φ_4 and the two irreducible factors of Φ_8.

Since $[\mathbb{F}_9 : \mathbb{F}_3] = 2$, there are two automorphisms of $\mathbb{F}_9$, namely the identity and Frob_3. Let ζ be a root of $X^2 + X - 1$ and let $\eta = \zeta^{-1}$. Then $\eta = \zeta^7$, $\eta^3 = \zeta^5$ and

$$X^2 + X - 1 = (X - \zeta)(X - \zeta^3), \quad X^2 - X - 1 = (X - \eta)(X - \eta^3).$$

We have

$$\mathbb{F}_9 = \{0,\ 1,\ \zeta,\ \zeta^2,\ \zeta^3,\ \zeta^4,\ \zeta^5,\ \zeta^6,\ \zeta^7\}$$

and also

$$\mathbb{F}_9 = \{0,\ 1,\ \eta,\ \eta^2,\ \eta^3,\ \eta^4,\ \eta^5,\ \eta^6,\ \eta^7\}.$$

The element $\zeta^4 = \eta^4 = -1$ is the element of order 2 and degree 1 and the two elements of order 4 (and degree 2), roots of $X^2 + 1$, are $\zeta^2 = \eta^6$ and $\zeta^6 = \eta^2$.

In $\mathbb{F}_9$ there are three elements of trace 0 over $\mathbb{F}_3$, namely 0 and the two roots of $X^2 + 1$, three elements of trace 1, namely 1 and the two roots of $X^2 - X - 1$ and three elements of trace -1, namely -1 and the two roots of $X^2 + X - 1$. There are four elements of norm 1 over $\mathbb{F}_3$, namely 1, -1 and the two roots of $X^2 + 1$ and four elements of norm -1, namely the roots of $X^2 - X - 1$ and $X^2 + X - 1$.

Exercise 70. List the values $\alpha \in \mathbb{F}_9^\times$ which are primitive roots in $\mathbb{F}_9$. Next, for each α and for $n = 0, 1, 2, \ldots, 7$, write the table of the discrete logarithm in $\mathbb{F}_9$ with respect to the primitive root α.

Exercise 71. Check that 3 has order 5 modulo 11 and that

$$X^{11} - 1 = (X-1)(X^5 - X^3 + X^2 - X - 1)(X^5 + X^4 - X^3 + X^2 - 1)$$

is the decomposition of $X^{11} - 1$ into irreducible factors over $\mathbb{F}_3$.
Remark. Compare with § 5.9.2.

Exercise 72. Check that 2 has order 11 modulo 23 and that $X^{23} - 1$ over $\mathbb{F}_2$ is the product of three irreducible polynomials, namely $X - 1$,

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

and

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

Remark. Compare with § 5.9.1.

Example 73. Assume that q is odd and consider the polynomial $\Phi_4(X) = X^2 + 1$. Corollary 61 implies:

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

Example 74. Assume again that q is odd and consider the polynomial $\Phi_8(X) = X^4 + 1$.

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

(see Exercise 64).

For instance, Example 69 gives over $\mathbb{F}_3$

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

Using Example 73, one deduces that in the decomposition of $X^8 - 1$ over $\mathbb{F}_q$, there are

8 linear factors if $q \equiv 1 \bmod 8$,
4 linear factors and 2 quadratic factors if $q \equiv 5 \bmod 8$,
2 linear factors and 3 quadratic factors if $q \equiv -1 \bmod 4$.

Exercise 75. (a) Check that the polynomials $X^4 + 1$ and $X^4 - X^2 + 1$ are irreducible over $\mathbb{Q}$ but that they are reducible over $\mathbb{F}_p$ for all prime numbers p.
(b) Show that a polynomial in $\mathbb{Z}[X]$ which is irreducible modulo p for all p has degree 1.

Exercise 76. Let n be an odd positive integer of the form $x^4 + y^4$ with x and y in $\mathbb{Z}$. Show that there are two integers N and M such that $n = NM^4$, where N is the product of odd prime numbers congruent to 1 modulo 8 and M is a product of odd prime numbers congruent to 3, 5 or 7 modulo 8.

Example 77. The group $(\mathbb{Z}/5\mathbb{Z})^\times$ is cyclic of order 4, there are $\varphi(4) = 2$ generators which are the classes of 2 and 3. Hence,

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

Exercise 78. Let $\mathbb{F}_q$ be a finite field with q elements. What are the degrees of the irreducible factors of the cyclotomic polynomial Φ_{15} over $\mathbb{F}_q$? For which values of q is Φ_{15} irreducible over $\mathbb{F}_q$?

Exercise 79. Let p be a prime number, r a positive integer, $q = p^r$. Denote by $\mathbb{F}_{q^2}$ a field with q^2 elements.
(a) Consider the homomorphism of multiplicative groups $\mathbb{F}_{q^2}^\times \longrightarrow \mathbb{F}_{q^2}^\times$ which maps x to x^{q-1}. What is the kernel? What is the image?
(b) Show that there exists $\alpha \in \mathbb{F}_{q^2}$ such that α^{q-1} is not in $\mathbb{F}_q$. Deduce that (α, α^q) is a basis of the $\mathbb{F}_q$–vector space $\mathbb{F}_{q^2}$.

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

As usual, we assume $\gcd(n, q) = 1$. Theorem 59 tells us that Φ_n is product of irreducible polynomials over $\mathbb{F}_q$ all of the same degree d. Denote by G the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$. Then d is the order of q in G. Let H be the subgroup of G generated by q:

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

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

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

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

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

This polynomial can be written

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

where mH is the class of m modulo H in G:

$$mH = \{mq^i \mid 0 \leq i \leq d-1\}.$$

There are $\varphi(n)/d$ classes of G modulo H and the decomposition of $\Phi_n(X)$ into irreducible factors over $\mathbb{F}_q$ is

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

Factors of $X^n - 1$ in $\mathbb{F}_q[X]$

Again we assume $\gcd(n, q) = 1$. We just studied the decomposition over $\mathbb{F}_q$ of the cyclotomic polynomials and $X^n - 1$ is the product of the $\Phi_d(X)$ for d dividing n. This gives all the information on the decomposition of $X^n - 1$ in $\mathbb{F}_q[X]$. Proposition 80 below follows from these results, but is also easy to prove directly.

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

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

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

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

For I ranging over the 2^n subsets of $\mathbb{Z}/n\mathbb{Z}$, we obtain all the monic divisors of $X^n - 1$ in $F[X]$. Lemma 25 implies that Q_I belongs to $\mathbb{F}_q[X]$ if and only if $Q_I(X^q) = Q_I(X)^q$.

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

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

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

Proposition 80. *The map $I \mapsto Q_I$ is a bijective map between the subsets I of $\mathbb{Z}/n\mathbb{Z}$ which are stable under multiplication by q on the one hand and the monic divisors of $X^n - 1$ in $\mathbb{F}_q[X]$ on the other hand.*

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

Corollary 81. *Under this bijective map, the irreducible factors of $X^n - 1$ correspond to the minimal nonempty subsets I of $\mathbb{Z}/n\mathbb{Z}$ which are stable under multiplication by q.*

This bijective map is not canonical: it depends on a choice of a primitive n–th root of unity ζ.

Here are some examples:

1. For $I = \emptyset$, $Q_\emptyset(X) = 1$.
2. For $I = \{0\}$, $Q_0(X) = X - 1$.

3. For $I = \mathbb{Z}/n\mathbb{Z}$, $Q_{\mathbb{Z}/n\mathbb{Z}}(X) = X^n - 1$.

4. For $I = (\mathbb{Z}/n\mathbb{Z})^\times$, $Q_{(\mathbb{Z}/n\mathbb{Z})^\times}(X) = \Phi_n(X)$. Recall that the order of ζ^k is $n/\gcd(n,k)$; hence ζ^k is a generator of the multiplicative group $\{1, \zeta, \zeta^2, \ldots, \zeta^{n-1}\}$ if and only if $\gcd(n,k) = 1$, meaning that k modulo n is a generator of the additive group $\mathbb{Z}/n\mathbb{Z}$, or equivalently that k modulo n belongs to $(\mathbb{Z}/n\mathbb{Z})^\times$.

5. For $I = (\mathbb{Z}/n\mathbb{Z})\backslash\{0\}$, $Q_I(X) = 1+X+X^2+\cdots+X^{n-1} = (X^n-1)/(X-1)$.

6. If n is even (and q odd, of course), then for $I = \{n/2\}$, $Q_{\{n/2\}}(X) = X+1$.

7. Let r be a divisor of n. There is a unique subgroup C_r of order r in the cyclic additive group $\mathbb{Z}/n\mathbb{Z}$. This subgroup is generated by the class of n/r, it is the set of $k \in \mathbb{Z}/n\mathbb{Z}$ such that $rk = 0$, it is stable under multiplication by any element prime to n. Then $Q_{C_r}(X) = X^r - 1$.

8. Let m be a divisor of n and let E_m be the set of generators of C_m: this set has $\varphi(m)$ elements which are the elements of order m in the cyclic additive group $\mathbb{Z}/n\mathbb{Z}$. This subset of $\mathbb{Z}/n\mathbb{Z}$ is stable under multiplication by any element prime to n. Then Q_{E_m} is the cyclotomic polynomial Φ_m of degree $\varphi(m)$.

For instance the minimal nonempty subsets of $\mathbb{Z}/7\mathbb{Z}$ which are stable under multiplication by 2 are $\{0\}$, $\{1,2,4\}$, $\{3,5,6\}$. This is related with the fact that the decomposition of $X^7 - 1$ over $\mathbb{F}_2$ is

$$(X-1)(X^3+X+1)(X^3+X^2+1)$$

(cf Example 67).

For q odd, the following 8 subsets of $\mathbb{Z}/4\mathbb{Z}$ are stable under multiplication by q:

$$\emptyset,\ \{0\},\ \{0,1,2,3\},\ \{1,3\},\ \{1,2,3\},\ \{2\},\ \{0,2\},\ \{0,1,3\}.$$

The subsets $\{1\}$ and $\{3\}$ are stable under multiplication by q if and only if $q \equiv 1 \mod 4$. For $q \equiv 1 \mod 4$ the polynomial $X^4 - 1$ splits into linear factors over $\mathbb{F}_q$, in which case all the 16 subsets of $\mathbb{Z}/4\mathbb{Z}$ are stable under multiplication by q, and the minimal nonempty ones are $\{0\}, \{1\}, \{2\}, \{3\}$. If $q \equiv 3 \mod 4$, the decomposition of $X^4 - 1$ into irreducible polynomials over $\mathbb{F}_q$ is $(X-1)(X+1)(X^2+1)$, in which case the minimal nonempty subsets of $\mathbb{Z}/4\mathbb{Z}$ stable under multiplication by q are $\{0\}, \{2\}, \{1,3\}$; among the 16 subsets of $\mathbb{Z}/4\mathbb{Z}$, only 8 are stable under multiplication by q .

Example 82. The field $\mathbb{F}_{16}$, quartic extension of $\mathbb{F}_2$. Take $n = 15$, $q = 2$. The minimal nonempty subsets of $\mathbb{Z}/15\mathbb{Z}$ which are stable under multiplication by 2 modulo 15 are the classes of

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

We recover the fact that in the decomposition

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

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

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

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

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

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

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

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

Let ζ is a primitive 15-th root of unity (that is, a root of Φ_{15}). Then $\zeta^{15}=1$ is the root of Φ_1, ζ^5 and ζ^{10} are the roots of Φ_3 (these are the primitive cube roots of unity, they belong to $\mathbb{F}_8$), while $\zeta^3, \zeta^6, \zeta^9, \zeta^{12}$ are the roots of Φ_5 (these are the primitive 5-th roots of unity). One of the two irreducible factors of Φ_{15} has the roots $\zeta, \zeta^2, \zeta^4, \zeta^8$, the other has the roots $\zeta^7, \zeta^{11}, \zeta^{13}, \zeta^{14}$. Also, we have

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

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

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

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

Example 83. The field $\mathbb{F}_{27}$, cubic extension of $\mathbb{F}_3$.
We have $X^{26}-1 = (X^{13}-1)(X^{13}+1)$ with

$$X^{13}-1 = (X-1)\Phi_{13}(X), \qquad X^{13}+1 = (X+1)\Phi_{26}(X) \quad \text{and} \quad \Phi_{26}(X) = \Phi_{13}(-X).$$

Since 3 has order 3 modulo 13 and modulo 26 and since Φ_{13} and Φ_{26} have degree 12, over $\mathbb{F}_3$ the polynomial $\Phi_{26}(X)$ is a product of four irreducible polynomials of degree 3, say $\Phi_{26} = f_1f_2f_3f_4$ and $\Phi_{13} = f_5f_6f_7f_8$, where $f_{4+i}(X) = -f_i(-X)$ $(i=1,2,3,4)$. The roots of f_1, f_2, f_3, f_4 are the $12 = \varphi(26)$ generators of the cyclic group $\mathbb{F}_{27}^\times = C_{26}$, the roots of f_5, f_6, f_7, f_8 are the $12 = \varphi(13)$ elements of order 13, each of which generates the unique cyclic subgroup of $\mathbb{F}_{27}^\times$ of order 13.

We are going to exhibit the set $\{f_1, \ldots, f_8\}$ by looking at the degree 3 irreducible polynomials over $\mathbb{F}_3$.

In order to get the decomposition of $X^{13}+1$, we write the table of discrete logarithms for $\mathbb{F}_{27}$. For this we need a generator, which means to select one of the four factors of Φ_{26}. Let us take a root α of X^3-X+1. With this choice we have

$$\begin{array}{lll}
\alpha^3=\alpha-1 & \alpha^4=\alpha^2-\alpha & \alpha^5=-\alpha^2+\alpha-1\\
\alpha^6=\alpha^2+\alpha+1 & \alpha^7=\alpha^2-\alpha-1 & \alpha^8=-\alpha^2-1\\
\alpha^9=\alpha+1 & \alpha^{10}=\alpha^2+\alpha & \alpha^{11}=\alpha^2+\alpha-1\\
\alpha^{12}=\alpha^2-1 & \alpha^{13}=-1 & \alpha^{14}=-\alpha\\
\alpha^{15}=-\alpha^2 & \alpha^{16}=-\alpha+1 & \alpha^{17}=-\alpha^2+\alpha\\
\alpha^{18}=\alpha^2-\alpha+1 & \alpha^{19}=-\alpha^2-\alpha-1 & \alpha^{20}=-\alpha^2+\alpha+1\\
\alpha^{21}=\alpha^2+1 & \alpha^{22}=-\alpha-1 & \alpha^{23}=-\alpha^2-\alpha\\
\alpha^{24}=-\alpha^2-\alpha+1 & \alpha^{25}=-\alpha^2+1 & \alpha^{26}=1.
\end{array}$$

Hence the roots of X^3-X+1 are α, $\alpha^3=\alpha-1$ and $\alpha^9=\alpha+1$. We deduce that the roots of the reciprocal polynomial X^3+X^2+1 are $\alpha^{-1}=\alpha^{25}=-\alpha^2+1$, $\alpha^{-3}=\alpha^{23}=-\alpha^2-\alpha$ and $\alpha^{-9}=\alpha^{17}=-\alpha^2+\alpha$.

We compute the irreducible polynomial of $\alpha^7=\alpha^2-\alpha-1$, which is also the irreducible polynomial of $\alpha^{21}=\alpha^2+1$ and of $\alpha^{63}=\alpha^{11}=\alpha^2+\alpha+1$, we find X^3+X^2-X+1.

The irreducible polynomial of $\alpha^5=-\alpha^2+\alpha-1$, which is also the irreducible polynomial of $\alpha^{15}=-\alpha^2$ and of $\alpha^{45}=\alpha^{19}=-\alpha^2-\alpha-1$ is the reciprocal polynomial of the previous one, namely X^3-X^2+X+1.

Therefore

$$X^{13}+1=(X+1)(X^3-X+1)(X^3-X^2+1)(X^3+X^2-X+1)(X^3-X^2+X+1).$$

The roots of X^3-X+1 are α, α^3, α^9.
The roots of X^3-X^2+1 are α^{25}, α^{23}, α^{17}.
The roots of X^3+X^2-X+1 are α^7, α^{21}, α^{11}.
The roots of X^3-X^2+X+1 are α^{19}, α^5, α^{15}.
This gives the list of 12 generators of $\mathbb{F}_{27}^\times$.

The twelve elements of order 13 in $\mathbb{F}_{27}^\times$ are the roots of $(X^{13}-1)/(X-1)$, where

$$X^{13}-1=(X-1)(X^3-X-1)(X^3-X^2-1)(X^3-X^2-X-1)(X^3+X^2+X-1).$$

Exercise: list the three roots of each of the four factors of $(X^{13}-1)/(X-1)$ over $\mathbb{F}_3$ (they are the 12 elements of order 13).
`Hint`: consider the change of variable $x\mapsto -x$ using $-1=\alpha^{13}$.

Exercise 84. The field $\mathbb{F}_{16}$, quadratic extension of $\mathbb{F}_4$.

Write $\mathbb{F}_4=\mathbb{F}_2(j)$ with j root of X^2+X+1.
(1) List the irreducible polynomials of degree 2 over $\mathbb{F}_4$.
(2) Decompose the 6 irreducible polynomials of $\mathbb{F}_2$ of degree 4 into irreducible factors of degree 2 over $\mathbb{F}_2$.
(Explain why it should be so)
(3) Select a generator of $\mathbb{F}_{16}^\times$ and an irreducible polynomial of degree 2 over $\mathbb{F}_4$ of which α is a root in $\mathbb{F}_{16}$. Write the discrete logarithm table of $\mathbb{F}_{16}^\times$ with basis α. For each of the 15 elements α^k with $0\le k\le 14$, tell which one is the irreducible polynomial of α^k.

Exercise 85. The field $\mathbb{F}_{64}$ is an extension of degree 6 of the prime field $\mathbb{F}_2$.
(a) List the subfields of $\mathbb{F}_{64}$.
(b) Decompose $X^{64} - X$ into irreducible polynomials over $\mathbb{F}_2$. Check the correspondence between the minimal subsets of $\mathbb{Z}/63\mathbb{Z}$ which are stable under multiplication by 2 and the irreducible factors of $X^{63} - 1$ over $\mathbb{F}_2$.
(c) Which are the degrees of the elements $\alpha \in \mathbb{F}_{64}$ with $\mathrm{Tr}_{\mathbb{F}_{64}/\mathbb{F}_2}(\alpha) = 0$?

Exercise 86. Let $\mathbb{F}_q$ be a finite field with q elements of characteristic p. Show that the following conditions are equivalent.
(i) Any element α in $\mathbb{F}_q$ such that $\mathbb{F}_q = \mathbb{F}_p(\alpha)$ is a generator of the cyclic group $\mathbb{F}_q^\times$.
(ii) The number $q - 1$ is a prime number.

4.5 Infinite Galois theory

Let p be a prime number. For each pair (n, m) of positive integers such that n divides m, there exists a field homomorphism from $\mathbb{F}_{p^n}$ into $\mathbb{F}_{p^m}$. Such a morphism is not unique if $n < m$: if we compose it with the Frobenius over $\mathbb{F}_p$, we get another one. For each $n|m$, we choose one of them, say $\iota_{n,m}$, which allow us to consider $\mathbb{F}_{p^n}$ as a subfield of $\mathbb{F}_{p^m}$.Then one checks that the union of the increasing family of fields $\mathbb{F}_{p^{n!}}$ is an algebraic closure of $\mathbb{F}_p$.

Let $\overline{\mathbb{F}}_p$ be an algebraic closure of $\mathbb{F}_p$. The extension $\overline{\mathbb{F}}_p/\mathbb{F}_p$ is algebraic, infinite, normal and separable: it is an *infinite Galois extension*. Its *Galois group* $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ is the group of automorphisms of $\mathbb{F}_p$. It is the projective limit of the Galois groups of the finite extensions of $\mathbb{F}_p$ contained in $\overline{\mathbb{F}}_p/\mathbb{F}_p$:

$$\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) = \varprojlim_{[L:\mathbb{F}_p]<\infty} \mathrm{Gal}(L/\mathbb{F}_p).$$

This group $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ is

$$\hat{\mathbb{Z}} := \varprojlim_{n\to\infty} \mathbb{Z}/n\mathbb{Z}.$$

The projective limite is the set of $(a_n)_{n\geq 1}$ in the Cartesian product $\prod_{n\geq 1} \mathbb{Z}/n\mathbb{Z}$ which satisfy $s_{nm}(a_n) = a_m$ for all pairs of positive integers (n, m) where m divides n, where

$$s_{n,m} : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$$

lis the canonical surjective morphism.

We also have

$$\hat{\mathbb{Z}} := \prod_p \mathbb{Z}_p \quad \text{with} \quad \mathbb{Z}_p = \varprojlim_{r\to\infty} \mathbb{Z}/p^r\mathbb{Z}.$$

See, for instance, [3] exercise 19 p. 635. and [4] Appendice p. 288.

5 Error correcting codes

From http://en.wikipedia.org/wiki/Coding_theory

> *Coding theory is an approach to various science disciplines – such as information theory, electrical engineering, digital communication,*

mathematics, and computer science – which helps design efficient and reliable data transmission methods so that redundancy can be removed and errors corrected.

Channel encoding adds extra data bits to make the transmission of data more robust to disturbances present on the transmission channel.

Error detection is the ability to detect the presence of errors caused by noise or other impairments during transmission from the transmitter to the receiver.
Error correction is the additional ability to reconstruct the original, error–free data.

5.1 Some historical dates

Among important dates are the following

• 1949: Marcel Golay (specialist of radars): produced two remarkably efficient codes.

• 1950: Richard W. Hamming, *Error detecting and error correcting codes*, The Bell System Technical Journal **26** (April 1950), N° 2, 147–160.

• 1955: Convolutional codes.

• 1959: Bose Chaudhuri Hocquenghem codes (BCH codes).

• 1960: Reed Solomon codes.

• 1963 John Leech uses Golay's ideas for sphere packing in dimension 24 - classification of finite simple groups

• 1971: no other perfect code than the two found by Golay.

• 1970: Goppa codes.

• 1981: Algebraic geometry codes.

5.2 Hamming distance

The *Hamming distance* on the set $\mathbb{F}_q^n$ is

$$d(\underline{x}, \underline{y}) = \#\{i\ ; 1 \leq i \leq n,\ x_i \neq y_i\}$$

for $\underline{x} = (x_1, \ldots, x_n)$ and $\underline{y} = (y_1, \ldots, y_n)$. It satisfies, as it should with the name *distance* (see, for instance, [1], Prop. 10.D),

$$d(\underline{x}, \underline{y}) = 0 \Longleftrightarrow \underline{x} = \underline{y}$$

and

$$d(\underline{y}, \underline{x}) = d(\underline{x}, \underline{y})$$

for $\underline{x}$ and $\underline{y}$ in $\mathbb{F}_q^n$, as well as the triangle inequality for $\underline{x}$, $\underline{y}$ and $\underline{z}$ in $\mathbb{F}_q^n$,

$$d(\underline{x}, \underline{z}) \leq d(\underline{x}, \underline{y}) + d(\underline{y}, \underline{z}).$$

We define the *minimum distance* $d(\mathcal{C})$ of a code $\mathcal{C} \subset \mathbb{F}_q^n$ by

$$d(\mathcal{C}) = \min\{d(\underline{x}, \underline{y})\ ;\ \underline{x}, \underline{y} \in \mathcal{C},\ \underline{x} \neq \underline{y}\}.$$

The *Hamming weight* $w(\underline{x})$ of an element of $\mathbb{F}_q^n$ is its Hamming distance with 0: for $\underline{x} = (x_1, \ldots, x_n)$:

$$w(\underline{x}) = \#\{i \ ; \ 1 \leq i \leq n, \ x_i \neq 0\}.$$

Hence, for $\underline{x}$ and $\underline{y}$ in $\mathbb{F}_q^n$,

$$d(\underline{x}, \underline{y}) = w(\underline{x} - \underline{y}).$$

For t a non–negative integer, the *Hamming ball* $B(\underline{c}, t)$ of center $\underline{c} \in \mathbb{F}_q^n$ and radius t is the set of elements of $\mathbb{F}_q^n$ having Hamming distance to $\underline{c}$ at most t:

$$B(\underline{c}, t) = \{\underline{x} \in \mathbb{F}_q^n \ ; \ d(\underline{x}, \underline{c}) \leq t\}.$$

The number of elements in $B(\underline{c}, t)$ is 1 for $t = 0$, it is $1 + n(q-1)$ for $t = 1$, and more generally

$$\#B(\underline{c}, t) = 1 + \binom{n}{1}(q-1) + \cdots + \binom{n}{t}(q-1)^t \qquad \text{for } t \geq 0. \tag{87}$$

As usual, $\binom{a}{b}$ is defined as 0 when $a < b$. For $t \geq n$ the formula (87) reduces to $\#B(\underline{c}, n) = q^n$.

5.3 Codes

A *code* of *length* n on a finite alphabet A with q elements is a subset $\mathcal{C}$ of A^n. A *word* is an element of A^n, a *codeword* is an element of $\mathcal{C}$. We speak of a q-ary code as a reference to the number of elements of the alphabet; it is a binary code for $q = 2$, a ternary code for $q = 3$.

Here we will assume A is a finite field $\mathbb{F}_q$ and $\mathcal{C}$ is a $\mathbb{F}_q$–vector subspace of $\mathbb{F}_q^n$. A *linear code* over a finite field $\mathbb{F}_q$ of length n and *dimension* d is a $\mathbb{F}_q$–vector subspace of $\mathbb{F}_q^n$ of dimension d (such a code is also called a $[n, d]$–code). Its *rate* is defined as d/n, the number $n - d$ is the redundancy.

A subspace $\mathcal{C}$ of $\mathbb{F}_q^n$ of dimension d can be described by giving a basis $e_1, \ldots, e_d$ of $\mathcal{C}$ over $\mathbb{F}_q$, so that

$$\mathcal{C} = \{m_1 e_1 + \cdots + m_d e_d \ ; \ (m_1, \ldots, m_d) \in \mathbb{F}_q^d\}.$$

An alternative description of a subspace $\mathcal{C}$ of $\mathbb{F}_q^n$ of codimension $n-d$ is by giving $n-d$ linearly independent linear forms $L_1, \ldots, L_{n-d}$ in n variables $\underline{x} = (x_1, \ldots, x_n)$ with coefficients in $\mathbb{F}_q$, such that

$$\mathcal{C} = \ker L_1 \cap \cdots \cap \ker L_{n-d}.$$

The sender replaces his message $(m_1, \ldots, m_d) \in \mathbb{F}_q^d$ of length d by the longer message $m_1 e_1 + \cdots + m_d e_d \in \mathcal{C} \subset \mathbb{F}_q^n$ of length n. The receiver checks whether the message $\underline{x} = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$ belongs to $\mathcal{C}$ by computing the $n - d$–tuple $\underline{L}(\underline{x}) = (L_1(\underline{x}), \ldots, L_{n-d}(\underline{x})) \in \mathbb{F}_q^{n-d}$. If there is no error during the transmission, then $\underline{x} \in \mathcal{C}$ and $L_1(\underline{x}) = \cdots = L_{n-d}(\underline{x}) = 0$. On the opposite, if the receiver observes that some $L_i(\underline{x})$ is non–zero, he knows that the received message has at least one error. The message with was sent was an element $\underline{c}$ of the code $\mathcal{C}$, the message received $\underline{x}$ is not in $\mathcal{C}$, the error is $\underline{\epsilon} = \underline{x} - \underline{c}$. The values of $\underline{L}(\underline{x})$ may enable him to correct the errors in case there are not too many of them. We give a few examples.

For a linear code $\mathcal{C}$, the minimum distance $d(\mathcal{C})$ equals the minimal weight of a non–zero element in $\mathcal{C}$.

5.4 First examples

Trivial codes of length n are $\mathcal{C} = \{0\}$ of dimension 0 and $\mathcal{C} = \mathbb{F}_q^n$ of dimension n.

We now take $q = 2$ (binary codes).

Example 88. Repetition $[2, 1]$ code detecting one error.

$n = 2$, $d = 1$, rate $= 1/2$.

$$\mathcal{C} = \big\{(0,0),\ (1,1)\big\}, \qquad e_1 = (1,1), \qquad L_0(x_0, x_1) = x_0 + x_1.$$

Example 89. Repetition $[3, 1]$ code correcting one error.

$n = 3$, $d = 1$, rate $= 1/3$.

$$\mathcal{C} = \big\{(0,0,0),\ (1,1,1)\big\}, \qquad e_1 = (1,1,1),$$

$$L_1(\underline{x}) = x_1 + x_3,\ L_2(\underline{x}) = x_2 + x_3.$$

If the message which is received is correct, it is either $(0, 0, 0)$ or $(1, 1, 1)$, and the two numbers $L_1(\underline{x})$ and $L_2(\underline{x})$ are 0 (in $\mathbb{F}_2$). If there is exactly one mistake, then the message which is received is either one of

$$(0,0,1),\ (0,1,0),\ (1,0,0),$$

or else one of

$$(1,1,0),\ (1,0,1),\ (0,1,1).$$

In the first case the message which was sent was $(0, 0, 0)$, in the second case it was $(1, 1, 1)$.

A message with a single error is obtained by adding to a codeword one of the three possible errors

$$(1,0,0),\ (0,1,0),\ (0,0,1).$$

If the mistake was on x_1, which means that $\underline{x} = \underline{c} + \underline{\epsilon}$ with $\underline{\epsilon} = (1, 0, 0)$ and $\underline{c} \in \mathcal{C}$ a codeword, then $L_1(\underline{x}) = 1$ and $L_2(\underline{x}) = 0$. If the mistake was on x_2, then $\underline{\epsilon} = (0, 1, 0)$ and $L_1(\underline{x}) = 0$ and $L_2(\underline{x}) = 1$. Finally if the mistake was on x_3, then $\underline{\epsilon} = (0, 0, 1)$ and $L_1(\underline{x}) = L_2(\underline{x}) = 1$. Therefore, the three possible values for the pair $\underline{L}(\underline{x}) = (L_1(\underline{x}), L_2(\underline{x}))$ other than $(0, 0)$ correspond to the three possible positions for a mistake. We will see that this is a *perfect one error correcting code* (see the definition after Theorem 101).

More generally, for $n \geq 2$ and $d = 1$ the repetition $[n, 1]$ codeis the subspace generated by $(1, 1, \ldots, 1)$, with only two elements. It is the intersection of the $n - 1$ hyperplanes which are the kernels of the linear forms

$$x_0 + x_1, x_0 + x_2, \ldots, x_0 + x_{n-1}$$

(for instance).

Example 90. Parity bit $[3, 2]$ code detecting one error.

$n = 3$, $d = 2$, rate $= 2/3$.

$$\mathcal{C} = \big\{(0,0,0),(0,1,1),(1,0,1),(1,1,0)\big\} = \big\{(m_1, m_2, m_1 + m_2)\ ;\ (m_1, m_2) \in \mathbb{F}_2^2\big\} \subset \mathbb{F}_2^3,$$

$$e_1 = (1,0,1),\ e_2 = (0,1,1), \qquad L_1(x_1, x_2, x_3) = x_1 + x_2 + x_3.$$

This is the easiest example of the *bit parity check.*

Example 91. A one error linear correcting $[5,2]$ code using the parity bit idea.
$n=5$, $d=2$, rate $=2/5$.

$$\begin{aligned}\mathcal{C} &= \big\{(0,0,0,0,0),(0,1,0,1,1),(1,0,1,0,1),(1,1,1,1,0)\big\}\\ &= \big\{(m_1,m_2,m_1,m_2,m_1+m_2)\ ;\ (m_1,m_2)\in\mathbb{F}_2^2\big\}\subset\mathbb{F}_2^5,\end{aligned}$$

$$e_1=(1,0,1,0,1),\ e_2=(0,1,0,1,1),$$

$$L_1(\underline{x})=x_1+x_3,\ L_2(\underline{x})=x_2+x_4,\ L_3(\underline{x})=x_1+x_2+x_5,$$

The possible values for the triple $\underline{L}(\underline{x})$ corresponding to a single error are displayed in the following table.

$\underline{x}$	x_1	x_2	x_3	x_4	x_5
$\underline{L}(\underline{x})$	$(1,0,1)$	$(0,1,1)$	$(1,0,0)$	$(0,1,0)$	$(0,0,1)$

Therefore, when there is a single error, the value of $\underline{L}(\underline{x})$ enables one to correct the error.

One may observe that a single error will never produce the triple $(1,1,0)$ nor $(1,1,1)$ for $\underline{L}(\underline{x})$: there are 8 elements $\underline{x}\in\mathbb{F}_2^5$ which cannot be received starting from a codeword and adding at most one mistake, namely $(x_1,x_2,x_1+1,x_2+1,x_5)$, with $(x_1,x_2,x_5)\in\mathbb{F}_2^3$.

Example 92. A one error correcting $[6,3]$ codeusing the parity bit idea.
$n=6$, $d=3$, rate $=1/2$.

$$\begin{aligned}\mathcal{C} &= \big\{(m_1,m_2,m_3,m_2+m_3,m_1+m_3,m_1+m_2)\ ;\ (m_1,m_2,m_3)\in\mathbb{F}_2^3\big\}\\ &= \big\{(0,0,0,0,0,0),\quad (0,0,1,0,1,1),\quad (0,1,0,1,0,1),\quad (0,1,1,1,1,0),\\ &\quad (1,0,0,1,1,0),\quad (1,0,1,1,0,1),\quad (1,1,0,0,1,1),\quad (1,1,1,0,0,0)\big\}\quad\subset\mathbb{F}_2^7,\end{aligned}$$

$$e_1=(1,0,0,0,1,1),\ e_2=(0,1,0,1,0,1),\ e_3=(0,0,1,1,1,0),$$

$$L_1(\underline{x})=x_2+x_3+x_4,\ L_2(\underline{x})=x_1+x_3+x_5,\ L_3(\underline{x})=x_1+x_2+x_6.$$

The possible values for the triple $\underline{L}(\underline{x})$ corresponding to a single error are displayed in the following table.

$\underline{x}$	x_1	x_2	x_3	x_4	x_5	x_6
$\underline{L}(\underline{x})$	$(0,1,1)$	$(1,0,1)$	$(1,1,0)$	$(1,0,0)$	$(0,1,0)$	$(0,0,1)$

Therefore, when there is a single error, the value of $\underline{L}(\underline{x})$ enables one to correct the error.

One may observe that a single error will never produce the triple $(1,1,1)$ for $\underline{L}(\underline{x})$: there are 8 elements $\underline{x}\in\mathbb{F}_2^5$ which cannot be received starting from a codeword and adding at most one mistake, namely:

$$(x_1,x_2,x_3,x_2+x_3+1,x_1+x_3+1,x_1+x_2+1)\quad\text{with}\quad(x_1,x_2,x_3)\in\mathbb{F}_2^3.$$

Example 93. Hamming $[7,4]$ binary code correcting one error.
$n=7$, $d=4$, rate $=7/4$, *corrects one error.*
$\mathcal{C}$ is the set of

$$(m_0,m_0+m_1,m_1+m_2,m_0+m_2+m_3,,m_1+m_3,m_2,m_3)\in\mathbb{F}_2^7$$

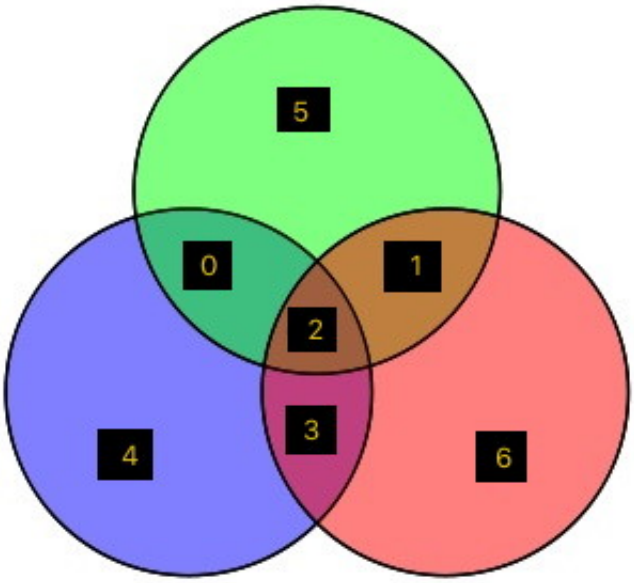
where (m_0, m_1, m_2, m_3) ranges over $\mathbb{F}_2^4$. A basis of $\mathcal{C}$ is

$$e_0 = (1,1,0,1,0,0,0), \quad e_1 = (0,1,1,0,1,0,0),$$
$$e_2 = (0,0,1,1,0,1,0), \quad e_3 = (0,0,0,1,1,0,1)$$

and $\mathcal{C}$ is also the intersection of the hyperplanes defined as the kernels of the linear forms

$$L_1(\underline{x}) = x_0 + x_2 + x_3 + x_4,\ L_2(\underline{x}) = x_0 + x_1 + x_2 + x_5,\ L_3(\underline{x}) = x_1 + x_2 + x_3 + x_6.$$

This corresponds to the next picture from
http://en.wikipedia.org/wiki/Hamming_code



Hamming [7,4] code

The possible values for the triple $\underline{L}(\underline{x})$ corresponding to a single error are displayed in the following table.

$\underline{x}$	x_0	x_1	x_2	x_3	x_4	x_5	x_6
$\underline{L}(\underline{x})$	$(1,1,0)$	$(0,1,1)$	$(1,1,1)$	$(1,0,1)$	$(1,0,0)$	$(0,1,0)$	$(0,0,1)$

This table gives a bijective map between the set $\{1,2,3,4,5,6,7\}$ of indices of the unique wrong letter in the word $\underline{x}$ which is received with a single mistake on the one hand, the set of values of the triple

$$\underline{L}(\underline{x}) = (L_1(\underline{x}), L_2(\underline{x}), L_3(\underline{x})) \in \mathbb{F}_2^3 \setminus \{0\}$$

on the second hand.

This is a *perfect* 1*–error correcting code.*

Exercise 94. Let $n \in \{1, 2, 3, 4\}$. Among 2^n playing cards, you select one without telling me which one it is. I display some of them and I ask you whether the card you selected is one of them. You answer yes or no.

1. How many questions should I ask in order to know which card you selected?
2. Same problem, but now you are allowed to give me at most one wrong answer, and I want to decide whether or not all you answers were right. If you gave always the right answer, I want to know which card you selected.
3. Same problem, again you are allowed to give me at most one wrong answer, but now, I want to know which card you selected, even if one of your answers was wrong.

Exercise 95. Three people are in a room, each has a hat on his head, the colour of which is black or white. Hat colours are chosen randomly. Everybody sees the colour of the hat of everyone else, but not on one's own. People do not communicate with each other. Everyone tries to guess (by writing on a piece of paper) the colour of their hat. They may write: Black/White/Abstain.

The people in the room win together or lose together as a team. The team wins if at least one of the three persons does not abstain, and everyone who did not abstain guessed the colour of their hat correctly.

1. What could be the strategy of the team to get the highest probability of winning? What is this probability?
2. Same questions with seven people.

5.5 Cyclic codes

A *cyclic code* $\mathcal{C}$ of length n over an alphabet with q elements is a $\mathbb{F}_q$–vector subspace of $\mathbb{F}_q^n$ such that, for any $(a_0, a_1, \ldots, a_{n-1}) \in \mathcal{C}$, the element $(a_{n-1}, a_0, a_1, \ldots, a_{n-2})$ also belongs to $\mathcal{C}$.

The codes from Examples 88, 89 and 93 are cyclic, while the codes from Examples 90, 91 and 92 are not cyclic.

We denote by $T : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$ the linear map (*right shift* – T for *translation*[2])

$$T(a_0, a_1, \ldots, a_{n-1}) = (a_{n-1}, a_0, \ldots, a_{n-2});$$

In the group of automorphism of the $\mathbb{F}_q$–vector space $\mathbb{F}_q^n$, this element T satisfies $T^n = I$ (the unit of $\mathrm{Aut}(\mathbb{F}_q^n/\mathbb{F}_q)$, namely the identity map). This is how the polynomial $X^n - 1$ comes into the picture.

Assume $\gcd(n, q) = 1$. A natural basis of the $\mathbb{F}_q$–space $\mathbb{F}_q[X]/(X^n - 1)$ is given by the classes modulo $X^n - 1$ of $1, X, \ldots, X^{n-1}$. This gives a $\mathbb{F}_q$–isomorphism

$$\begin{array}{rccc} \Psi : & \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q[X]/(X^n - 1) \\ & (a_0, a_1, \ldots, a_{n-1}) & \longmapsto & a_0 + a_1 X + \cdots + a_{n-1} X^{n-1}. \end{array}$$

Hence,

$$\Psi \circ T(a_0, a_1, \ldots, a_{n-1}) = X(a_0 + a_1 X + \cdots + a_{n-1} X^{n-1}) \mod (X^n - 1),$$

[2]The translation into French of *shift* is *translation*.

which is $\Psi \circ T = X\Psi$. As a consequence, a subset $\mathcal{C}$ of $\mathbb{F}_q^n$ is stable under the shift T if and only if $\Psi(\mathcal{C})$ is stable under multiplication by X in $\mathbb{F}_q[X]/(X^n-1)$.

A vector subspace $\mathcal{I}$ of $\mathbb{F}_q[X]/(X^n-1)$ is stable under multiplication by X if and only if $\mathcal{I}$ is an ideal of the quotient ring $\mathbb{F}_q[X]/(X^n-1)$. Furthermore, there is a bijective map between the ideals of $\mathbb{F}_q[X]/(X^n-1)$ and the ideals of $\mathbb{F}_q[X]$ which contain X^n-1. Since the ring $\mathbb{F}_q[X]$ is principal, the ideals containing X^n-1 are the ideals (Q) generated by a divisor Q of X^n-1. Given such an ideal, there is a single generator Q which is monic. If r is the degree of Q, then the ideal of $\mathbb{F}_q[X]/(X^n-1)$ generated by the class of Q modulo X^n-1 is a $\mathbb{F}_q$–vector space of dimension $d=n-r$: a basis of $(Q)/(X^n-1)$ is $Q, XQ, \ldots, X^{d-1}Q$. Also, the following sequence of $\mathbb{F}_q$–linear maps is exact:

$$0 \longrightarrow \frac{(Q)}{(X^n-1)} \longrightarrow \frac{\mathbb{F}_q[X]}{(X^n-1)} \longrightarrow \frac{\mathbb{F}_q[X]}{(Q)} \longrightarrow 0.$$

The dimensions of these three vector spaces are d, n and r respectively, with $n=r+d$, as it should. Combining these results with Proposition 80, we deduce

Proposition 96. *Given a finite field $\mathbb{F}_q$ and an integer n with $\gcd(n,q)=1$, there are bijective maps between the following subsets.*
(i) The cyclic codes $\mathcal{C}$ of length n over $\mathbb{F}_q$.
(ii) The ideals $\mathcal{I}$ of $\mathbb{F}_q[X]/(X^n-1)$.
(iii) The monic divisors Q of X^n-1 in $\mathbb{F}_q[X]$.
(iv) The subsets I of $\mathbb{Z}/n\mathbb{Z}$ which are stable under multiplication by q.
Under this correspondence, the dimension d of the code is the dimension of the $\mathbb{F}_q$–vector space $\mathcal{I}$, the degree of Q is $r=n-d$, and the number of elements in I is r.

The code $\mathcal{C}$ is the set of $(a_0, a_1, \ldots, a_{n-1})$ in $\mathbb{F}_q^n$ such that $a_0 + a_1X + \cdots + a_{n-1}X^{n-1}$ belongs to $\mathcal{I}$. The ideal $\mathcal{I}$ is the ideal generated by the class of Q modulo X^n-1. The correspondence given by Proposition 80 between I and Q depends on a choice of a primitive n–th root of unity ζ.

Here are some examples:

1. For the empty subset $I=\emptyset$ of $\mathbb{Z}/n\mathbb{Z}$, we have $r=0$, $d=n$, $Q_\emptyset(X)=1$, $\mathcal{I}=(1)=\mathbb{F}_q[X]/(X^n-1)$ and $\mathcal{C}$ is the full $[n,n]$ code $\mathbb{F}_q^n$.
2. For $I=\{0\}$, we have $r=1$, $d=n-1$, $Q_0(X)=X-1$, $\mathcal{I}=(X-1)$, $\mathcal{C}$ is the parity bit check $[n,n-1]$ codewhich is the hyperplane of equation $x_1+\cdots+x_n=0$ in $\mathbb{F}_q^n$.
3. For $I=\mathbb{Z}/n\mathbb{Z}$, we have $r=n$, $d=0$, $Q_I(X)=X^n-1$, $\mathcal{I}=(0)$ and $\mathcal{C}$ is the trivial code $\{0\}$.
4. For $I=(\mathbb{Z}/n\mathbb{Z})^\times$, we have $r=\varphi(n)$ and $Q_I(X)=\Phi_n(X)$.
5. For $I=(\mathbb{Z}/n\mathbb{Z})\setminus\{0\}$, we have $r=n-1$, $d=1$, Q_I is the divisor
$$\frac{X^n-1}{X-1}=1+X+\cdots+X^{n-1}$$
of X^n-1, $\mathcal{I}$ is the ideal $\big((X^n-1)/(X-1)\big)$ of $\mathbb{F}_q[X]/(X^n-1)$ and $\mathcal{C}$ is the repetition $[n,1]$ code $\{(a,a,\ldots,a)\ ;\ a\in\mathbb{F}_q\}\subset\mathbb{F}_q^n$, generalising Examples 88 and 89.

6. If n is even, for $I = \{n/2\}$, we have $Q_I(X) = X + 1$, hence $\mathcal{C}$ is the $(n, n-1)$ code which is the set of $(a_0, a_1, \ldots, a_{n-1}) \in \mathcal{C}$ such that

$$a_0 - a_1 + a_2 - \cdots + a_{n-2} - a_{n-1} = 0.$$

7. For r a divisor of n and $I = C_r$ the additive subgroup of $\mathbb{Z}/n\mathbb{Z}$ of order r, we have $Q_I(X) = X^r - 1$. The associated code $\mathcal{C} \subset \mathbb{F}_q^n$ is the intersection of the r hyperplanes

$$\left\{ (a_0, a_1, \ldots, a_{n-1}) \in \mathbb{F}_q^n \;\mid\; \sum_{i=0}^{(n/r)-1} a_{j+ir} = 0 \quad \text{for} \quad j = 0, 1, \ldots, r-1 \right\}$$

(see Exercise 98 (b)).

8. For m a divisor of n and $I = E_m$ the set of elements of order m in the additive group $\mathbb{Z}/n\mathbb{Z}$, we have $Q_I(X) = \Phi_m(X)$ and $r = \varphi(m)$. The code $\mathcal{C} \subset \mathbb{F}_q^n$ is the set of $(a_0, a_1, \ldots, a_{n-1})$ such that

$$a_0 + a_1\zeta^{jn/m} + a_2\zeta^{2jn/m} + \cdots + a_{n-1}\zeta^{(n-1)jn/m} = 0$$

for $j = 0, 1, \ldots, m-1$ with $\gcd(j, m) = 1$.

Example 97. Take $n = 4$ and, of course, q odd. Here are some subsets I of $\mathbb{Z}/4\mathbb{Z}$ which are stable under multiplication by q, the associated polynomial Q_I, the degree r of Q_I and the dimension $d = 4 - r$ of the associated code $\mathcal{C} \subset \mathbb{F}_q^4$.

	(1)	(2)	(3)	(4)	(5)	(6, 8)	(7)
$I =$	$\emptyset$	$\{0\}$	$\{0, 1, 2, 3\}$	$\{1, 3\}$	$\{1, 2, 3\}$	$\{2\}$	$\{0, 2\}$
$Q_I =$	1	$X - 1$	$X^4 - 1$	$X^2 + 1$	$X^3 + X^2 + X + 1$	$X + 1$	$X^2 - 1$
$r =$	0	1	4	2	3	1	2
$d =$	4	3	0	2	1	3	2

For $I = \{1, 3\}$ we have $\mathcal{C} = \{(a_0, a_1, a_0, a_1) \mid (a_0, a_1) \in \mathbb{F}_q^2\}$.
For $I = \{0, 2\}$ we have $\mathcal{C} = \{(a_0, a_1, -a_0, -a_1) \mid (a_0, a_1) \in \mathbb{F}_q^2\}$.

Exercise 98.
(a) For q odd, write the code in $\mathbb{F}_q^4$ associated with the subset $I = \{0, 1, 3\}$ of $\mathbb{Z}/4\mathbb{Z}$.
(b) For q prime to n and r a divisor of n, let C_r be the cyclic subgroup of $\mathbb{Z}/n\mathbb{Z}$ of order r. Write the cyclic code in $\mathbb{F}_q^n$ associated with the subset $I = C_r$ of $\mathbb{Z}/n\mathbb{Z}$ as an intersection of r hyperplanes with coefficients in $\mathbb{F}_q$.
(c) For q prime to n and ℓ a prime divisor of n, let E_ℓ be the set of elements of order ℓ in the additive group $\mathbb{Z}/n\mathbb{Z}$. Write the cyclic code in $\mathbb{F}_q^n$ associated with the subset $I = E_\ell$ of $\mathbb{Z}/n\mathbb{Z}$ as an intersection of $\ell - 1$ hyperplanes with coefficients in $\mathbb{F}_q$.

5.6 Detection, correction and minimal distance

A *transmission with at most t errors* is a mapping $f : \mathcal{C} \longrightarrow \mathbb{F}_q^n$ such that for all $\underline{c} \in \mathcal{C}$,

$$d\big(f(\underline{c}), \underline{c}\big) \leq t.$$

The *error* is $\epsilon(\underline{c}) = f(\underline{c}) - \underline{c}$. The message which is sent is $\underline{c}$, a codeword, the message which is received is $f(\underline{c})$.

The first question is to detect if an error occurred, that means to detect whether $\epsilon(\underline{c})$ is zero or not. A code $\mathcal{C}$ *can detect* t *errors* if for all $\underline{c} \in \mathcal{C}$,

$$B(\underline{c}, t) \cap \mathcal{C} = \{\underline{c}\}.$$

This means that for a transmission $f : \mathcal{C} \longrightarrow \mathbb{F}_q^n$ with at most t errors, $f(\underline{c}) \in \mathcal{C}$ if and only if $\epsilon(\underline{c}) = 0$. The receiver checks whether $f(\underline{c})$ is in $\mathcal{C}$ or not (for instance, by using a check matrix H). If $f(\underline{c}) \in \mathcal{C}$, if the code is t–error detecting and if the transmission had at most t errors, then $\epsilon(\underline{c}) = 0$: there was no error.

A code $\mathcal{C}$ of length n over $\mathbb{F}_q$ *can correct* t *errors* (one also says that it is t–*error correcting*) if for all $\underline{x} \in \mathbb{F}_q^n$,

$$\#B(\underline{x}, t) \cap \mathcal{C} \leq 1.$$

This means that any transmission $f : \mathcal{C} \longrightarrow \mathbb{F}_q^n$ with at most t errors is injective: for all $\underline{y} \in f(\mathcal{C})$ there is a single $\underline{c}$ such that $\underline{y} = f(\underline{c})$. After receiving $\underline{y} = f(\underline{c})$, knowing that the transmission had at most t errors, the receiver computes the unique $\underline{c}$ for which $d(y; \underline{c}) \leq t$. Then he knows that $f(\underline{c}) = \underline{y}$ and he also knows the error $\epsilon(\underline{c}) = f(\underline{c}) - \underline{y}$.

Lemma 99. *A code $\mathcal{C}$ of length n over $\mathbb{F}_q$ can detect t errors if and only if $d(\mathcal{C}) \geq t+1$. The code $\mathcal{C}$ can correct t errors if and only if $d(\mathcal{C}) \geq 2t+1$.*

Proof. The condition $d(\mathcal{C}) \geq t+1$ means that a word at Hamming distance at most t from an element $\underline{c}$ of $\mathcal{C}$ and distinct from $\underline{c}$ does not belong to $\mathcal{C}$. This is equivalent to saying that $\mathcal{C}$ can detect t errors.

For the second part of Lemma 99, assume first that $d(\mathcal{C}) \geq 2t+1$. Let $\underline{x} \in \mathbb{F}_q^n$ and let $\underline{c}_1$ and $\underline{c}_2$ in $\mathcal{C}$ satisfy $d(\underline{x}, \underline{c}_1) \leq t$ and $d(\underline{x}, \underline{c}_2) \leq t$. Then by the triangle inequality

$$d(\underline{c}_1, \underline{c}_2) \leq 2t < d(\mathcal{C}).$$

Therefore, $\underline{c}_1 = \underline{c}_2$.
Conversely, assume $d(\mathcal{C}) \leq 2t$: there is a non–zero element $\underline{c}$ in $\mathcal{C}$ with $w(\underline{c}) \leq 2t$, hence, $\underline{c}$ has at most $2t$ non–zero components. Split the set of indices of the non–zero components of $\underline{c}$ into two disjoint subsets I_1 and I_2 having each at most t elements. Next define $\underline{x} \in \mathbb{F}_q^n$ as the point having the same components x_i as $\underline{c}$ for $i \in I_1$ and 0 for i not in I_1. Then in the Hamming ball of center $\underline{x}$ and radius t there are at least two points of $\mathcal{C}$, namely 0 and $\underline{c}$. Hence, $\mathcal{C}$ is not t–error correcting. □

Proposition 100. *For a $[n, d]$ code $\mathcal{C}$, the minimum distance is bounded by*

$$d(\mathcal{C}) \leq n + 1 - d.$$

Proof. The subspace

$$V = \{(x_1, \ldots, x_{n+1-d}, 0, \ldots, 0) \; ; \; (x_1, \ldots, x_{n+1-d}) \in \mathbb{F}_q^{n+1-d}\}$$

of $\mathbb{F}_q^n$ has dimension $n+1-d$, the sum of this dimension with the dimension d of $\mathcal{C}$ exceeds the dimension n of the ambient space $\mathbb{F}_q^n$, hence, there is a non–zero element in the intersection. This is a non–zero element of $\mathcal{C}$ with weight $\leq n + 1 - d$. □

A $[n, d]$ code $\mathcal{C}$for which $d(\mathcal{C}) = n + 1 - d$ is called MDS (*Maximal Distance Separable*). Examples 88, 89 and 90 are MDS codes.

Hamming $[7, 4]$ code (Example 93 and § 5.7) has minimum distance 3, hence, is not MDS.

From (87), we deduce Hamming's bound on the error correcting capacity of a $[n, d]$ code over $\mathbb{F}_q$ (see [8] Theorem 3.3.1).

Theorem 101. *For a $[n, d]$ code $\mathcal{C}$ which is t–error correcting,*

$$1 + \binom{n}{1}(q-1) + \cdots + \binom{n}{t}(q-1)^t \leq q^{n-d}.$$

A t–error correcting code over $\mathbb{F}_q$ of length n is *perfect* if this upper bound is an equality, meaning that $\mathbb{F}_q^n$ is the disjoint union of the balls of radius t around the codewords in $\mathcal{C}$.

For a perfect 1–error correcting $[n, d]$ code over $\mathbb{F}_q$, the union of the q^d Hamming balls of radius 1 gives a packing of the set $\mathbb{F}_q^n$ with q^n elements, hence,

$$q^d\big(1 + n(q-1)\big) = q^n.$$

We set $d = n - r$, so that $n = (q^r - 1)/(q - 1)$. One easily checks that the order of q modulo n is r. According to Theorem 59, the polynomial $\Phi_n(X)$, splits into irreducible factors of degree r. Each of these factors gives a cyclic code which is Hamming q-ary $[n, d]$ code of length n and dimension d.

For instance, take $q = 2$. For $r = 2$ we have $n = 3$, $d = 1$ and this is the repetition $[3, 1]$ code $\{(0, 0, 0)\ ,\ (1, 1, 1)\}$ of Example 89. For $r = 3$ we have $n = 7$, $d = 4$ which are the parameters of Hamming $[7, 4]$ code considered in Example 93 and § 5.7.

5.7 Hamming codes

From http://en.wikipedia.org/wiki/Hamming_code

> *In telecommunication, a Hamming code is a linear error-correcting code named after its inventor, Richard Hamming. Hamming codes can detect up to two simultaneous bit errors, and correct single-bit errors; thus, reliable communication is possible when the Hamming distance between the transmitted and received bit patterns is less than or equal to one. By contrast, the simple parity code cannot correct errors, and can only detect an odd number of errors.*
>
> *Hamming worked at Bell Labs in the 1940s on the Bell Model V computer, an electromechanical relay-based machine with cycle times in seconds. Input was fed in on punch cards, which would invariably have read errors. During weekdays, special code would find errors and flash lights so the operators could correct the problem. During after-hours periods and on weekends, when there were no operators, the machine simply moved on to the next job.*
>
> *Hamming worked on weekends, and grew increasingly frustrated with having to restart his programs from scratch due to the unreliability*

of the card reader. Over the next few years he worked on the problem of error-correction, developing an increasingly powerful array of algorithms. In 1950 he published what is now known as Hamming Code, which remains in use in some applications today.

Let $\mathbb{F}_q$ be a finite field with q elements and let r be a positive integer. Define

$$n = \frac{q^r - 1}{q - 1} = 1 + q + q^2 + \cdots + q^{r-1}.$$

Therefore, q is prime to n and the class of q in $(\mathbb{Z}/n\mathbb{Z})^\times$ has order r. The subset $I = \{1, q, q^2, \ldots, q^{r-1}\}$ of $\mathbb{Z}/n\mathbb{Z}$ is stable under multiplication by q. This defines a cyclic $[n, d]$ code of length n and dimension $d = n - r$ over $\mathbb{F}_q$.

Hamming $[7, 4]$ *binary code.*

We first develop the special case already considered in Example 93, where $r = 3$, $q = 2$, hence, $n = 7$ and $d = 4$. We have seen in Example 67 that the decomposition of Φ_7 over $\mathbb{F}_2$ is

$$\Phi_7(X) = (X^3 + X + 1)(X^3 + X^2 + 1).$$

We choose $Q(X) = 1 + X + X^3$. The vector of its coordinates in the basis $1, X, X^2, X^3, X^4, X^5, X^6$ is $e_0 = (1, 1, 0, 1, 0, 0, 0) \in \mathbb{F}_2^7$. Next define e_1, e_2 and e_3 by taking the coordinates in the same basis of XQ, X^2Q, X^3Q:

$$\begin{array}{rl} Q(X) = 1 + X + X^3 & e_0 = (1, 1, 0, 1, 0, 0, 0), \\ XQ(X) = X + X^2 + X^4, & e_1 = (0, 1, 1, 0, 1, 0, 0) = Te_0, \\ X^2Q(X) = X^2 + X^3 + X^5, & e_2 = (0, 0, 1, 1, 0, 1, 0) = Te_1, \\ X^3Q(X) = X^3 + X^4 + X^6, & e_3 = (0, 0, 0, 1, 1, 0, 1) = Te_2. \end{array}$$

We have $e_1 = Te_0$, $e_2 = T^2e_0$, $e_3 = T^3e_0$, $T^7 = 1$.

The components of e_0, e_1, e_2, e_3 in $\mathbb{F}_2^7$ are the rows of the following matrix

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

The elements in the code $\mathcal{C}$ are the 16 elements

$$m_0e_0 + m_1e_1 + m_2e_2 + m_3e_3$$

with $(m_0, m_1, m_2, m_3) \in \mathbb{F}_2^4$. This subspace $\mathcal{C}$ of $\mathbb{F}_2^7$ has dimension 4, hence, it is an intersection of 3 hyperplanes. Let us recall how to find a basis of the $\mathbb{F}_q$–vector space of linear forms vanishing on a subspace V of F^n given by a basis with d elements. We write the $d \times n$ matrix whose rows are the coordinates of the given basis. We add one further row with the variables $x_1, \ldots, x_n$. By elementary columns operations (replacing a column by its sum with a linear combination of the other columns, which corresponds to the multiplication on the right by a regular $n \times n$ matrix), we get a matrix of the form

$$\begin{pmatrix} & I_d & & 0 & \ldots & 0 \\ y_1 & y_2 & \ldots & y_d & y_{d+1} & \ldots & y_n \end{pmatrix}$$

where I_d is the identity $d \times d$ matrix and $y_1, \ldots, y_n$ are linearly independent linear forms in $x_1, \ldots, x_n$. Then the $(n-d)$–tuple $y_{d+1}, \ldots, y_n$ is a basis of the space of linear forms vanishing on V. This can be checked by reducing to the simple case of a hyperplane $x_n = t_1 x_1 + \cdots + t_{n-1} x_{n-1}$ with $d = n-1$ and the matrix

$$\begin{pmatrix} & & & t_1 \\ & I_{n-1} & & \vdots \\ & & & t_{n-1} \\ x_1 & x_2 & \ldots & x_{n-1} & x_n \end{pmatrix}$$

We perform this process with the matrix G above: therefore, we introduce

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ x_0 & x_1 & x_2 & x_3 & x_4 & x_5 & x_6 \end{pmatrix}.$$

Here is the last row of the successive matrices obtained by the triangulation process (we work over $\mathbb{F}_2$)

x_0	x_1	x_2	x_3	x_4	x_5	x_6
x_0	$x_1 + x_0$	x_2	$x_3 + x_0$	$x_4 + x_0 + x_1$	x_5	x_6
x_0	$x_1 + x_0$	$x_2 + x_0 + x_1$	$x_3 + x_0$	$x_4 + x_0 + x_1$	x_5	x_6
x_0	$x_1 + x_0$	$x_2 + x_0 + x_1$	$x_3 + x_1 + x_2$	$x_4 + x_0 + x_1$	$x_5 + x_0 + x_1 + x_2$	x_6
x_0	$x_1 + x_0$	$x_2 + x_0 + x_1$	$x_3 + x_1 + x_2$	$x_4 + x_0 + x_2 + x_3$	$x_5 + x_0 + x_1 + x_2$	x_6
x_0	$x_1 + x_0$	$x_2 + x_0 + x_1$	$x_3 + x_1 + x_2$	$x_4 + x_0 + x_2 + x_3$	$x_5 + x_0 + x_1 + x_2$	$x_6 + x_1 + x_2 + x_3$

Hence, we introduce the three linear forms

$$\begin{aligned} L_0(\underline{x}) &= x_0 + x_2 + x_3 + x_4 \\ L_1(\underline{x}) &= x_0 + x_1 + x_2 + x_5 \\ L_2(\underline{x}) &= x_1 + x_2 + x_3 + x_6. \end{aligned}$$

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} \tag{102}$$

The 7 column vectors are all the non–zero elements in $\mathbb{F}_2^3$. The product $G \cdot {}^tH$ of G with the transpose of H is the zero 4×3 matrix.

Hamming $[n, n-r]$ code with $n = (q^r - 1)/(q-1)$.

The same construction can be performed in the general case of $\mathbb{F}_q^n$ with $n = (q^r - 1)/(q-1)$. Let Q be an irreducible factor of Φ_n over $\mathbb{F}_q$. Since q has order r modulo n, the degree of Q is r. The *Hamming $[n, d]$ code of length n and dimension $d = n - r$ over $\mathbb{F}_q$* is the code $\mathcal{C}$ associated to Q by Proposition 96: it is the set of $\underline{x} = (x_0, \ldots, x_{n-1}) \in \mathbb{F}_q^n$ such that $Q(X)$ divides $x_0 + x_1 X + \cdots + x_{n-1} X^{n-1}$ in $\mathbb{F}_q[X]$.

Let ζ be a root of Q (in a splitting field). Since Q divides Φ_n, ζ is a primitive n–th root of unity. The code $\mathcal{C}$is the set of $\underline{x} = (x_0, \ldots, x_{n-1}) \in \mathbb{F}_q^n$ such that $\sum_{i=0}^{n-1} x_i \zeta^i = 0$. We have

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

where $I = \{1, q, q^2, \ldots, q^{r-1}\}$. The ideal $\mathcal{I}$ of $\mathbb{F}_q[X]/(X^n - 1)$ generated by the class of Q modulo $X^n - 1$ is the $\mathbb{F}_q$–vector space of dimension $d = n - r$ spanned by the classesmodulo $X^n - 1$ of $Q, XQ, \ldots, X^{d-1}Q$.

Since ζ has degree r over $\mathbb{F}_q$, given $(m_r, \dots, m_{n-1}) \in \mathbb{F}_q^d$, there is a unique $(m_0, \dots, m_{r-1}) \in \mathbb{F}_q^r$, so that

$$m_0 + m_1\zeta + \cdots + m_{r-1}\zeta^{r-1} = -m_r\zeta^r - \cdots - m_{n-1}\zeta^{n-1}.$$

From $\sum_{i=0}^{n-1} m_i\zeta^i$ we deduce that $\underline{c} = (m_0, \dots, m_{n-1}) \in \mathbb{F}_q^n$ is a codeword. In other words, the projection $\mathbb{F}_q^n \to \mathbb{F}_q^d$ on the last d coordinates induces a bijective map $\mathcal{C} \to \mathbb{F}_q^d$.

Given $\underline{x} = (x_0, \dots, x_{n-1}) \in \mathbb{F}_q^n$, if the sum $\sum_{i=0}^{n-1} x_i\zeta^i$ is nonzero and if $\underline{c} \in \mathcal{C}$ satisfies $d(\underline{x}, \underline{c}) \leq 1$, then the error $\epsilon = \underline{x} - \underline{c} = (0, \dots, 0, \epsilon_k, 0, \dots, 0) \in \mathbb{F}_q^n$ has its nonzero component in position k with

$$\epsilon_k\zeta^k = \sum_{i=0}^{n-1} x_i\zeta^i.$$

Since $\epsilon_k\zeta^k \neq \epsilon_h\zeta^h$ for $k \neq h$, if there is such a c, it is unique. Now there are q^d elements in the code, each Hamming ball of radius 1 in $\mathbb{F}_q^n$ contains $1 + n(q-1)$ elements. We have $q^r - 1 = n(q-1)$, the number of elements in $\mathbb{F}_q^n$ is $q^n = q^d(n(q-1)+1)$, hence for each $\underline{x} \in \mathbb{F}_q^n$ there is a unique $\underline{c} \in \mathcal{C}$ with $d(\underline{x}, \underline{c}) \leq 1$: the unit balls of radius 1 centred at the elements in the code give a partition of $\mathbb{F}_q^n$, which means that $\mathcal{C}$ is a perfect 1–error correcting code.

The code $\mathcal{C}$ is the kernel of a linear map $\mathbb{F}_q^n \to \mathbb{F}_q^r$ which is given by r independent linear forms in n variables $L_0, \dots, L_{r-1}$.

Let H be the $r \times n$ matrix, the rows of which are the components of the linear forms $L_0, \dots, L_{r-1}$. Any two rows of H are linearly independent over $\mathbb{F}_q$. The columns of H define n elements of $\mathbb{F}_q^n$, no two of them lie on the same line. In $\mathbb{F}_q^r$, there are $q^r - 1$ non–zero elements, each of them defines a line ($\mathbb{F}_q$–subspace of dimension 1) having $q-1$ non–zero elements and, therefore, there are n lines in $\mathbb{F}_q^r$, which are the 1-dimensional subspaces spanned by the columns of H.

The tuple $(L_0(\underline{x}), \dots, L_{r-1}(\underline{x}))$ takes q^r different values when $\underline{x}$ ranges over $\mathbb{F}_q^n$, with $q^r = 1 + n(q-1)$; the value $(0, \dots, 0)$ for this tuple corresponds to a code word, any of the other $n(q-1)$ values tells, for an element $\underline{x}$ not in the code, the position i of the error $\underline{x} - \underline{m}$ and the value of the coordinate m_i for $\underline{m}$ the unique element in the code at Hamming distance 1 of $\underline{x}$.

5.8 Generator matrix and check matrix

Among many others, a reference for this section is [8], Chapter 3.

Given a linear $[n, d]$ code $\mathcal{C}$over $\mathbb{F}_q$, a *generator matrix* is a $d \times n$ matrix G with coefficients in $\mathbb{F}_q$, the rows of which are the components of a basis of $\mathcal{C}$. The code is the set of elements $\underline{m}G$ where $\underline{m}$ ranges over $\mathbb{F}_q^d$ (viewed as a $1 \times d$ row vector). From the definition, it follows that G has rank d.

A *check matrix* is a $(n-d) \times n$ matrix H with coefficients in $\mathbb{F}_q$, the rows of which are the components of a basis of the space of linear forms vanishing on $\mathcal{C}$. The code $\mathcal{C}$ is the set of elements $\underline{c}$ in $\mathbb{F}_q^n$ such that $H \cdot {}^t\underline{c} = 0$, where ^{t} denotes the transposition, so that ${}^t\underline{c}$ is a $n \times 1$ column vector in $\mathbb{F}_q^n$. Therefore,

$$G \cdot {}^tH = 0$$

where G is a $d \times n$ matrix of rank d and H a $r \times n$ matrix of rank $r = n - d$.

The code is said to be *in systematic form* if $H = \begin{pmatrix} A & I_r \end{pmatrix}$, where I_r is the identity $r \times r$ matrix and A is a $r \times d$ matrix.

Two codes are *isomorphic* if they have the same check matrix in suitable bases - for instance, the two descriptions that we gave of the Hamming $[7, 4]$ code in Example 93 and § 5.7 are isomorphic.

5.9 Further examples

5.9.1 The binary Golay $[23, 12]$ code

A perfect code with $q = 2$, $n = 23$, $d = 12$ and minimal distance 7 (hence, it is 3–error correcting but not MDS) has been constructed by Golay as follows.

We have $2^{11} - 1 = 23 \times 89 = 2047$, which is the smallest integer of the form $M_p = 2^p - 1$ with p prime but which is not itself a prime (primes of the form $M_p = 2^p - 1$ are called *Mersenne primes*). We take the multiplicative subset I of $(\mathbb{Z}/23\mathbb{Z})^\times$ generated by 2, which is

$$I = \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}.$$

The decomposition of Φ_{23} over $\mathbb{F}_2$ has been given in Exercise 72.

There are 2^{12} codewords, for each of them the Hamming ball of radius 3 has

$$\binom{23}{0} + \binom{23}{1} + \binom{23}{2} + \binom{23}{3} = 1 + 23 + 253 + 1771 = 2048 = 2^{11}$$

elements, these balls are disjoint and the total number of elements in their union is $2^{11}2^{12} = 2^{23}$.

5.9.2 The ternary Golay $[11, 6]$ code

An other perfect code constructed by Golay has the parameters $q = 3$, $n = 11$, $d = 6$ and minimal distance 5 (it is 2–error correcting not MDS). We have $3^5 - 1 = 11 \times 23$. We take the multiplicative subset I of $(\mathbb{Z}/11\mathbb{Z})^\times$ generated by 3, which is $I = \{1, 3, 4, 5, 9\}$. The decomposition of Φ_{11} over $\mathbb{F}_3$ has been given in Exercise 71.

There are 3^6 codewords, for each of them the Hamming ball of radius 2 has

$$\binom{11}{0} + 2\binom{11}{1} + 2^2\binom{11}{2} = 1 + 22 + 220 = 243 = 3^5$$

elements, they are disjoint the total number of elements in $\mathbb{F}_3^{11}$ is $3^6 3^5 = 3^{11}$.

5.9.3 BCH (Bose–Chaudhuri–Hocquenghem) codes

Given a finite field $\mathbb{F}_q$ and an integer r, let n be a divisor of $q^r - 1$. Hence, the order of q modulo n divides r. Let $\zeta \in \mathbb{F}_q^r$ be a primitive n-th root of unity and let $\delta \geq 2$ be an integer. Consider the morphism of rings

$$\begin{array}{ccc} \mathbb{F}_q[X]/(X^n - 1) & \longrightarrow & \mathbb{F}_q^{\delta-1} \\ P & \longmapsto & \big(P(\zeta^j)\big)_{1 \leq j \leq \delta - 1} \end{array}$$

The kernel is a cyclic q–ary code of length n and minimal distance δ, the generating polynomial is the lcm of the minimal polynomials over $\mathbb{F}_q$ of the elements ζ^j, $1 \leq j \leq \delta - 1$: the subset I of $\mathbb{Z}/n\mathbb{Z}$ is the smallest subset containing $\{1, \ldots, q\}$ and stable under multiplication by q.

5.9.4 Reed–Solomon code

The Reed–Solomon codes are special cases of BCH codes. Let $q = 2^m$, $n = q - 1$ and let ζ be a primitive n–th–th root of unity, that means a generator of $\mathbb{F}_q^\times$. For $1 \leq d \leq n$ the code associated with the subset $I = \{1, 2, 3, \ldots, n - d\}$ of $\mathbb{Z}/n\mathbb{Z}$ and to the polynomial

$$\prod_{i=1}^{n-d} (X - \zeta^i)$$

has dimension d and minimal distance $q - d$. This code is MDS; it is used in CD's. This code is specially efficient when errors occur often consecutively, since the words here have length m.

It is known that the only perfect codes are

- *The trivial code with a single element* 0.
- *The full code* $\mathbb{F}_q^n$.
- *A binary repetition code with odd length (see [8] Exercise 3.12).*
- *For* $r \geq 2$*, the* q*-ary Hamming code of length* $n = (q^r - 1)/(q - 1)$*, dimension* $n - r$ *and minimal distance* 3.
- *The ternary Golay code over* $\mathbb{F}_3$ *of length* 11*, dimension* 6 *and minimal distance* 5.
- *The binary Golay code over* $\mathbb{F}_2$ *of length* 23*, dimension* 12 *and minimal distance* 7.

5.10 Minimum distance of a code

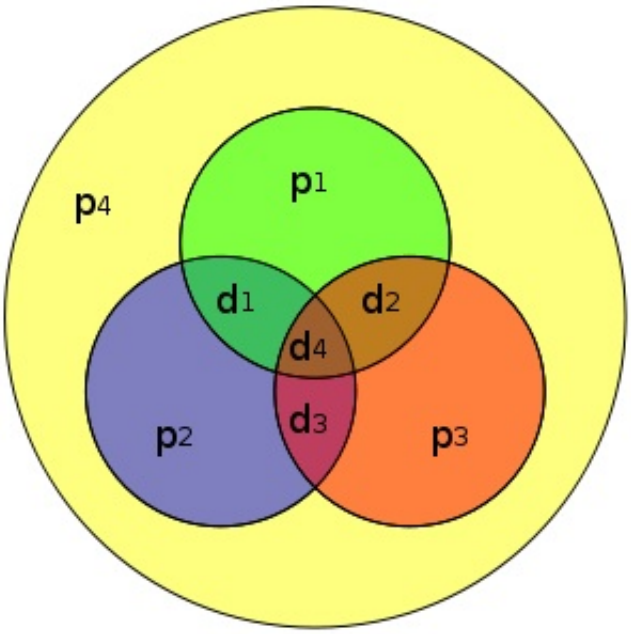
We state two results which are useful tools to compute the minimum distance of a code. For the first one, see [1], Prop. 11C.

Proposition 103. *Let* $\mathcal{C}$ *be a linear code over* $\mathbb{F}_q$ *of length* n *with check matrix* H *and let* s *be a positive integer. Then* $\mathcal{C}$ *has minimum distance* $\geq s+1$ *if and only if any* s *columns of* H *are linearly independent over* $\mathbb{F}_q$.

As a consequence, if any s columns of H are linearly independent over $\mathbb{F}_q$, and if further there exists $s + 1$ columns of H which are linearly dependent over $\mathbb{F}_q$, then $d(\mathcal{C}) = s + 1$. This enables one to check that Hamming code has minimum distance 3. Indeed in the matrix (102) all rows are non–zero and distinct (hence, any two rows are linearly independent over $\mathbb{F}_2$), but there are sets of three rows which are linearly dependent. If we add a row with 1's, then for the new matrix any sum of an odd number of rows is non–zero, hence, any three rows are linearly independent. This means that we extend the code of Hamming of lenth 7 to a code of length 8 by adding a parity check bit.

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{pmatrix}. \qquad H = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

This code has, therefore, minimum distance 4, it cannot correct more than one error, but it can detect up to 3 errors.



Hamming extended $[8, 4]$ code

To any code $\mathcal{C} \subset \mathbb{F}_q^n$ we can associate an *extended code* $\widetilde{\mathcal{C}} \subset \mathbb{F}_q^{n+1}$ by adding a parity bit:

$$\widetilde{\mathcal{C}} = \{(x_1, \dots, x_{n+1}) \in \mathcal{C} \times \mathbb{F}_q \; ; \; (x_1, \dots, x_n) \in \mathcal{C}, \; x_1 + \cdots + x_{n+1} = 0\} \subset \mathbb{F}_q^{n+1}.$$

One can check $d(\mathcal{C}) \leq d(\widetilde{\mathcal{C}}) \leq d(\mathcal{C})$.

A variant is to take the *even subcode*

$$\mathcal{C}' = \{(x_1, \dots, x_n) \in \mathcal{C} \; ; \; x_1 + \cdots + x_n = 0\} \subset \mathbb{F}_q^n.$$

Then $d(\mathcal{C}) \leq d(\mathcal{C}')$.

Proposition 104. *Let $\mathcal{C}$ be a cyclic linear code of length n over $\mathbb{F}_q$ associated with a subset I of $\mathbb{Z}/n\mathbb{Z}$ stable under multiplication by q. Assume that there exist i and s such that $\{i+1, i+2, \dots, i+s\} \subset I$. Then $d(\mathcal{C}) \geq s+1$.*

For instance, Hamming code is associated with the subset $I = \{1, 2, 4, \dots, 2^{r-1}\}$ of $\mathbb{Z}/n\mathbb{Z}$, with two consecutive elements, hence, its distance is at least 3 (and here it is just 3).

6 Further exercises

Exercise 105. Latin squares

Given n symbols $z_1, \ldots, z_n$, a *latin square* of order n is a square $n \times n$ matrix with entries in $\{z_1, \ldots, z_n\}$ such that each row contains each symbol exactly once, and each column contains each symbol exactly once. Two latin squares of the same order $(a_{ij})_{1 \leq i,j \leq n}$ and $(b_{ij})_{1 \leq i,j \leq n}$ are *orthogonal* if the set of couples (a_{ij}, b_{ij}) for $1 \leq i, j \leq n$ has n^2 elements: they are the n^2 elements (z_h, z_k), $1 \leq h, k \leq n$.
(a) Check that a set of mutually orthogonal latin squares of order n has at most $n-1$ elements.
(b) Let $\mathbb{F}_q$ be a finite field with q elements. Write $\mathbb{F}_q = \{x_0, x_1, \ldots, x_{q-1}\}$ with $x_0 = 0$ and $x_1 = 1$. check that for $s = 1, 2, \ldots, q-1$,

$$A_s = \big(x_i x_s + x_j\big)_{0 \leq i,j \leq q-1}, \quad s = 1, 2, \ldots, q-1$$

are $q-1$ mutually orthogonal latin squares of order q.
(c) Give an example of two mutually orthogonal latin squares of order 3 and an example of three mutually orthogonal latin squares of order 4.
`Remark.` *For each $n \geq 3$ with $n \neq 6$, there exists a pair of orthogonal latin squares of order n. However it is not known whether there exists an integer n which is not a power of a prime for which there exist $n-1$ mutually orthogonal latin squares of order n.*

Exercise 106. (a) Write the decomposition of the polynomial $X^{12} - 1$ into irreducible factors over $\mathbb{Z}$.
(b) Write the decomposition of the polynomial $X^{12} - 1$ into irreducible factors over the finite field $\mathbb{F}_5$ with 5 elements.
(c) How many elements are there in the splitting field over $\mathbb{F}_5$ of the polynomial $X^{12} - 1$?
(d) Let p be a prime number and $\mathbb{F}_p$ the finite field with p elements. What are the degrees of the irreducible factors of $X^{12} - 1$ over $\mathbb{F}_p$?

Exercise 107. (a) What are the degrees of the irreducible factors of the cyclotomic polynomials Φ_5, Φ_7 and Φ_{11} over $\mathbb{F}_2$? Over $\mathbb{F}_3$?
(b) Decompose the polynomial Φ_{15} into irreducible factors over $\mathbb{F}_2$.
(c) Is the polynomial $X^4 + X + 1$ irreducible over $\mathbb{F}_4$? over $\mathbb{F}_8$?
(d) For each of the fields $\mathbb{F}_2$, $\mathbb{F}_4$, $\mathbb{F}_8$ and $\mathbb{F}_{16}$, give the list of irreducible cyclotomic polynomials.

Exercise 108. Let $\mathbb{F}_q$ the finite field with q elements. Show that the number of squarefree monic polynomials in $\mathbb{F}_q[X]$ of degree n is

$$\begin{cases} 1 & \text{for } n = 0, \\ q & \text{for } n = 1, \\ q^n - q^{n-1} & \text{for } n \geq 2. \end{cases}$$

Exercise 109. Check that over the field $\mathbb{F}_3$ with 3 elements, the cyclotomic polynomial Φ_{728} splits into a product of 48 irreducible factors, each of which has degree 6.

Exercise 110. Check that if α is any root of the polynomial $X^3 + X + 1$ in characteristic 5, then 2α is a primitive root of the cubic extension $\mathbb{F}_{5^3}$ of $\mathbb{F}_5$.

Exercise 111. Let $\mathbb{F}_q$ be a finite field with q elements of characteristic p.
(a) Let K be a field containing $\mathbb{F}_q$ and let $\zeta \in K$ satisfy $\zeta^{q-1} = -1$. Check $\zeta^2 \in \mathbb{F}_q^\times$.
(b) How many irreducible factors are there in the decomposition of the polynomial $X^{2q-1} - X$ over $\mathbb{F}_q$? Which are their degrees?
`Hint.` *Consider separately the case where $p = 2$ is even and the case where it is odd.*

Exercise 112. Given a finite field F with q elements, determine all integers n such that $x \mapsto x^n$ is an automorphism of F.

Exercise 113. (a) Let p and q be two prime numbers. Assume q divides $2^p - 1$. Check $q \equiv 1 \bmod p$.
(b) Let n be a positive integer and q a prime number. Assume that q divides $2^{2^n} + 1$. Check $q \equiv 1 \bmod 2^{n+1}$.

Exercise 114. Let p be a prime number and $f \in \mathbb{Z}[X]$ a polynomial. Check that the following conditions are equivalent.
(i) For all $a \in \mathbb{Z}$, $f(a) \equiv 0 \bmod p$.
(ii) There exist two polynomials g and h in $\mathbb{Z}[X]$ such that

$$f(X) = (X^p - X)g(X) + ph(X).$$

Exercise 115. Let p be a prime number Consider the endomorphism f of the multiplicative group $(\mathbb{Z}/p^2\mathbb{Z})^\times$ given by $x \to x^p$:

$$\begin{array}{rccc} f: & (\mathbb{Z}/p^2\mathbb{Z})^\times & \longrightarrow & (\mathbb{Z}/p^2\mathbb{Z})^\times \\ & x & \longmapsto & x^p \end{array}$$

What are the image and kernel (and their number of elements)?

Exercise 116.
(a) Check that any element in $\mathrm{GL}_n(\mathbb{F}_q)$ has order $\leq q^n - 1$. Give an example where the order does not divide $q^n - 1$.
(b) Show that for $A \in \mathrm{GL}_n(\mathbb{F}_q)$, the following conditions are equivalent:
(i) A has order $q^n - 1$
(ii) The subring $\mathbb{F}_q[A]$ of $\mathrm{Mat}_{n\times n}(\mathbb{F}_q)$ generated by A is a field and A is a primitive element in this field.
(iii) The characteristic polynomial $\det(XI_n - A) \in \mathbb{F}_q[X]$ of A is a primitive polynomial (see the definition in Exercise 118).

Exercise 117. Let $m \in \mathbb{Z}$, $1 \leq m \leq 12$. Does there exist a domain A (commutative ring without zero divisor) such that the group of units of A has m elements?

Exercise 118. Let $\mathbb{F}_q$ be a finite field and $f \in \mathbb{F}_q[X]$ be a monic irreducible polynomial with $f(X) \neq X$.
(a) Show that the roots α of f in $\overline{\mathbb{F}}_p$ all have the same order in the multiplicative group $\overline{\mathbb{F}}_p^\times$. We denote this order by $p(f)$ and call it the *period* of f.
(b) For ℓ a positive integer, check that $p(f)$ divides ℓ if and only if $f(X)$ divides $X^\ell - 1$.
(c) Check that if f has degree n, then $p(f)$ divides $q^n - 1$. Deduce that q and $p(f)$ are relatively prime.
(d) A monic irreducible polynomial f is *primitive* if its degree n and its period $p(f)$ are related by $p(f) = q^n - 1$. Explain the definition.
(e) Recall that $X^2 + X + 1$ is the unique irreducible polynomials of degree 2 over $\mathbb{F}_2$, that there are two irreducible polynomials of degree 3 over $\mathbb{F}_2$:

$$X^3 + X + 1, \quad X^3 + X^2 + 1,$$

three irreducible polynomials of degree 4 over $\mathbb{F}_2$:

$$X^4 + X^3 + 1, \quad X^4 + X + 1, \quad X^4 + X^3 + X^2 + X + 1$$

and three monic irreducible polynomials of degree 2 over $\mathbb{F}_3$:

$$X^2+1, \quad X^2+X-1, \quad X^2-X-1.$$

For each of these 9 polynomials compute the period. Which ones are primitive?
(f) Which are the irreducible polynomials over $\mathbb{F}_2$ of period 15? Of period 5?

Exercise 119. Let $\mathbb{F}_p$ be the prime field with p elements and let ℓ be a prime number. Show that if $a \in \mathbb{F}_p$ is not an ℓ–th power in $\mathbb{F}_p$, then $x^\ell - a$ is irreducible over $\mathbb{F}_p$.

Exercise 120. *(Galois Theorem)* Let p be a prime number and P a polynomial of $\mathbb{F}_p[X]$ of degree $n \geq 1$ such that $P(0) \neq 0$. The goal is to prove that there exist $m < p^n$ such that P divides $X^m - 1$.
(a) Using Euclidean division, show that there exists k with $1 \leq k \leq p^n$ such that P divides $X^k - 1$.
(b) Show that one may select $k < p^n$.
(c) Find the integer $m < 8$ such that $X^3 + X + 1$ divides $X^m - 1$ in $\mathbb{F}_2[X]$.

Exercise 121. Let $u \in \mathbb{F}_p^\times$. Denote by m the order of u in $\mathbb{F}_p^\times$. Set $k = (p-1)/m$.
(a) Show that in the decomposition of the polynomial $X^{p-1} - u$ into irreducible polynomials over $\mathbb{F}_p$, all factors have degree m
(b) Show that there are k elements $v_1, \ldots, v_k$ in $\mathbb{F}_p^\times$ such that $v_i^k = u$.
(c) Write the the decomposition of the polynomial $X^{p-1} - u$ into irreducible polynomials over $\mathbb{F}_p$.

Exercise 122. Decompose the polynomial $X^{p+1} - 1$ into irreducible polynomials over $\mathbb{F}_p$.

Exercise 123. How many $(x, y) \in \mathbb{F}_8^2$ are there satisfying

$$x^3y + y^3 + x = 0?$$

Exercise 124. For each of the following values of p (a prime number), r (a positive integer, $q = p^r$) and n a positive integer,
(1) Give the list of monic irreducible polynomials of degree n over the field $\mathbb{F}_q$
(2) Select a primitive root of unity of order $q^n - 1$ in $\mathbb{F}_{q^n}$ and write the table of discrete logarithms of basis α
(3) For each of the polynomials listed in (1), give the list of its roots in $\mathbb{F}_{q^n}$
(4) If $r \neq 1$, decompose each polynomials of degree rn over $\mathbb{F}_p$ into irreducible factors over $\mathbb{F}_q$.

p	r	n
2	1	2
3	1	2
5	1	2
7	1	2
2	1	3
3	1	3
2	2	2
3	2	2
2	3	2

Exercise 125. Let $\mathbb{F}_q$ be a finite field with q elements of characteristic $\neq 5$. How many cyclic codes are there on $\mathbb{F}_q$ of dimension 5? What are their dimensions?

Exercise 126. Let r be a positive integer. Denote by n_r the least positive integer such that $2^{n-r} \geq 1+n$.
(a) Show that for $n < n_r$ there is no 1–error correcting code on $\mathbb{F}_{2^n}$ of dimension r.
(b) For each of the values $r = 0, 1, 2, 3, 4$, give an example of a 1–error correcting code on $\mathbb{F}_{2^{n_r}}$ of dimension r.

Exercise 127. What is the least positive integer n such that there exists a 1–error correcting code of length n?

Exercise 128. Let $f : \mathbb{F}_3^2 \to \mathbb{F}_3^4$ be the linear map

$$F(a, b) = (a, b, a + b, a - b)$$

and $\mathcal{C}$ be the image of f.
(a) What are the length and the dimension of the code $\mathcal{C}$? How many elements are there in $\mathcal{C}$? List them.
(b) What is the minimum distance $d(\mathcal{C})$ of $\mathcal{C}$? How many errors can the code $\mathcal{C}$ detect? How many errors can the code $\mathcal{C}$ correct? Is it a MDS code?
(c) How many elements are there in a Hamming ball of $\mathbb{F}_3^4$ of radius 1? Write the list of elements in the Hamming ball of $\mathbb{F}_3^4$ of radius 1 centred at $(0, 0, 0, 0)$.
(d) Check that for any element $\underline{x}$ in $\mathbb{F}_3^4$, there is a unique $\underline{c} \in \mathcal{C}$ such that $d(\underline{c}, \underline{x}) \leq 1$.
What is $\underline{c}$ when $\underline{x} = (1, 0, -1, 1)$?

Exercise 129. Let $\mathbb{F}_q$ be a finite field with q elements. Assume $q \equiv 3 \bmod 7$. How many cyclic codes of length 7 are there on $\mathbb{F}_q$? For each of them describe the code: give its dimension, the number of elements, a basis, a basis of the space of linear forms vanishing on it, its minimum distance, the number of errors it can detect or correct and whether it is MDS or not.

Exercise 130. Let $(P_i)_{i \in I}$ be a family of polynomials with coefficients in $\mathbb{Z}$. Show that the following properties are equivalent.
(a) The P_i 's have a common zero in $\mathbb{C}$.
(b) There exists an infinite set of primes p such that the P_i 's have a common zero in $\mathbb{F}_p$.
(c) For every prime p, except a finite number, there exists a field of characteristic p in which the P_i's have a common zero.
Example with a family having a single element P. Show that for the polynomial $P(X) = X^2 - 5$ there are infinitely many p for which the congruence $P(x) \equiv 0 \bmod p$ has a solution $x \in \mathbb{Z}$ and there are also infinitely many p for which the congruence $P(x) \equiv 0 \bmod p$ has no solution $x \in \mathbb{Z}$.
`Reference`: Jean-Pierre Serre, *How to use finite fields for problems concerning infinite fields*,
http://arxiv.org/abs/0903.0517
`Hint.`
Let n be the number of variables.
`(a) implies (b).` Assume (a). Show that there is a number field K in which the P_i's have a common zero $\underline{\alpha} \in K^n$. Using Chebotarev density Theorem, show that there exist infinitely many prime numbers p totally split in K such that the reduction of $\underline{\alpha}$ modulo a prime ideal above p in K is well defined and produces a common zero of the P_i's in $\mathbb{F}_p^n$. Deduce (b).
`(a) implies (c).` Use the same argument but without the condition that p splits completely in K.
`(b) or (c) implies (a).` Assume that the P_i's have no common zero in $\mathbb{C}^n$. Using Hilbert Nullstellensatz, deduce that the ideal of $\mathbb{Z}[X_1, \ldots, X_n]$ generated by the P_i's contains a nonzero integer m. For F a field of characteristic not dividing m, check that the P_i's have no common root in F^n.
`Remark.` A special case (namely with a single polynomial $P(X) = X^2 - a$) is quoted by Serre in his *Course in arithmetic*, §4.4.

7 Solutions of some Exercises

Solution to Exercise 4.
(a) For x and y in $\mathbb{Z}$, the integer x^2+xy+y^2 is congruent to 0 or 1 modulo 3.
(b) The group $\mathbb{F}_p^\times$ is cyclic of order $p-1$. It contains an element of order 3 if and only if p is congruent to 1 modulo 3. Hence $(i) \Leftrightarrow (ii)$.

The equivalence with (iii) uses algebraic number theory – see for instance [S] §5.4.
(c) If $p = x^2+xy+y^2$, then either $p=3$ or p is congruent to 1 modulo 3.

For the converse, assume p is congruent to 1 modulo 3. Using (b), let $t \in \mathbb{Z}$ satisfy $t^2-t+1 \equiv 0 \mod p$. From Dirichlet's box principle it follows that there exist x and y in $\mathbb{Z}$ such that $0 \leq x < \sqrt{p}$, $0 \leq y < \sqrt{p}$, $(x,y) \neq (0,0)$ and $x \equiv ty \mod p$. From

$$-p < x^2 - xy + y^2 < 2p$$

with $x^2-xy+y^2 \neq 0$ we deduce $x^2-xy+y^2 = p$.

Another proof is to use the fact that the ring of integers $\mathbb{Z}[j]$ of the quadratic field $\mathbb{Q}(j)$ is principal. A generator of the ideal $\mathfrak{p}$ can be written $x+jy$ with x and y in $\mathbb{Z}$. Hence

$$p = (x+yj)(x+yj^2) = x^2+xy+y^2.$$

(d) The fact that a positive integer of the form $3^b N_{1,3} N_{2,3}^2$ can be written x^2+xy+y^2 follows from the identity

$$(a^2+ab+b^2)(x^2+xy+y^2) = u^2+uv+v^2$$

with

$$u = ax-by,\ v = bx+(a-b)y,$$

which expresses the fact that the norm from $\mathbb{Q}(j)$ to $\mathbb{Q}$ (where $j^2+j+1=0$) of the product

$$(a+bj)(x+yj) = (ax-by)+(ay+bx-by)j$$

is the product of the norms of $a+bj$ and $x+yj$.

For the converse, let $n = x^2+xy+y^2$ and let p be a prime number $\neq 3$. Let $s = v_p(n)$ be the exponent of p in the prime decomposition of n. Assume that s is odd. We need to show $p \equiv 1 \mod 3$.

Let d be the gcd of x and y and let $t = v_p(d)$ be the exponent of p in the prime decomposition of d. Write $x = da$, $y = db$ with a and b relatively prime, so that $n = d^2 m$ with $m = a^2+ab+b^2$. Since s is odd, the number $v_p(m) = s-2t$ is ≥ 1. One at least of the two integers a, b is not multiple of p; it has an inverse modulo p, and therefore there exists t in $\mathbb{Z}$ such that t^2+t+1 is congruent to 0 modulo p. From (c) we deduce that p is congruent to 1 modulo 3. □

Solution to Exercise 6.
(1) Let a and b be two integers satisfying $an+bk=1$. For $x \in G$, we have $x^n = 1$. Hence $x^k = 1$ implies $x = (x^n)^a (x^k)^b = 1$.
(2) If d divides n, G has a unique subgroup of order d and the elements x in this subgroup are the solutions $x \in G$ of the equation $x^d = 1$.
In general, write $an+bk = d$. Since $x^n = 1$ for any $x \in G$, an element $x \in G$ satisfies $x^k = 1$ if and only

if $x^d = 1$. Hence the number of such x is d.
(3)
$(i) \Rightarrow (iii)$ From (2), we deduce that if G is a cyclic group of order n, then for each divisor d of n, the number of $x \in G$ such that $x^d = 1$ is d. If ζ is a generator of the cyclic group G, these d elements are $\zeta^{jn/d}$ for $j = 0, 1, \ldots, d-1$.
$(iii) \Rightarrow (ii)$ is obvious.
$(ii) \Rightarrow (i)$ Assume that G is a finite group of order n such that, for each divisor d of n, the number of $x \in G$ such that $x^d = 1$ is $\leq d$.

By Lagrange's Theorem, any element in G has an order d dividing n; the order yields a partition of G. When d is a divisor of n, denote by $N(d)$ the number of elements of G of order d. Hence

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

Let $d \mid n$. If $N(d) \geq 1$, then G has at least one cyclic subgroup H of order d, all the elements x in this subgroup H satisfy $x^d = 1$, hence the hypothesis implies that there is a single cyclic subgroup of order d. The elements in G of order d are the generators of H, therefore $N(d) = \varphi(d)$. Therefore for any d dividing n, the number $N(d)$ is either 0 or $\varphi(d)$. In any case $N(d) \leq \varphi(d)$. Using Lemma 5, we deduce

$$n = \sum_{d|n} N(d) \leq \sum_{d|n} \varphi(d) = n,$$

which implies $N(d) = \varphi(d)$ for all $d \mid n$. In particular $N(n) \geq 1$, which means that G is cyclic. □

Solution to Exercise 7. (Following [9], § 10.2).
From the Chinese Remainder Theorem, it follows that for $n = p_1^{e_1} \cdots p_r^{e_r}$, the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ is isomorphic to the product of the multiplicative groups $(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times$, of orders $p^{e_i-1}(p_i - 1)$. If $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic, then each of these factors is a cyclic group and their orders are pairwise relatively prime. It follows that n is either a power of a prime ($r = 1$), or twice a power of an odd prime ($r = 2$, $p_1 = 2$, $e_1 = 1$). It remains to show that $(\mathbb{Z}/2\mathbb{Z})^\times$, $(\mathbb{Z}/4\mathbb{Z})^\times$, $(\mathbb{Z}/p^e\mathbb{Z})^\times$ and $(\mathbb{Z}/2p^reZ)^\times$ are cyclic when p is an odd prime and $e \geq 1$, and that $(\mathbb{Z}/2^e\mathbb{Z})^\times$ is not cyclic if $e \geq 3$.

Clearly the groups $(\mathbb{Z}/2\mathbb{Z})^\times$ and $(\mathbb{Z}/4\mathbb{Z})^\times$, of order 1 and 2 respectively, are cyclic.

For p an odd prime and for $e \geq 1$ the groups $(\mathbb{Z}/p^e\mathbb{Z})^\times$ and $(\mathbb{Z}/2p^e\mathbb{Z})^\times$ are isomorphic of order $\varphi(p^e) = p^{e-1}(p-1)$.

For p an odd prime number, the fact that $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic follows from Proposition 19. Assume now $e \geq 2$. Let $x \in \mathbb{Z}$ be a primitive root of unity modulo p. The class of x modulo p^e has an order which is a multiple of $p-1$, hence $(\mathbb{Z}/p^e\mathbb{Z})^\times$ contains a cyclic subgroup of order $p-1$. From the congruences

$$(1+p)^{p^j} \equiv 1 + p^{j+1} \mod p^{j+2}$$

for $j = 0, 1, \ldots, e-1$, which are easy to check by induction, one deduces that the class of $1+p$ modulo p^e has order p^{e-1}. Hence $(\mathbb{Z}/p^e\mathbb{Z})^\times$ contains also a cyclic subgroup of order p^{e-1}; it follows that it is cyclic, as the direct product of two cyclic groups of relatively prime orders.

Finally we deal with $(\mathbb{Z}/2^e\mathbb{Z})^\times$ for $e \geq 3$. In the group $(\mathbb{Z}/8\mathbb{Z})^\times$, the 3 elements 3, 5, 7 have order 2, hence this group is isomorphic the (additive) Klein group $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ of order 4, which is not cyclic. In general, for $e \geq 3$, using the congruences

$$5^{2^j} = (1+4)^{2^j} \equiv 1 + 2^{j+2} \mod 2^{j+3}$$

for $j = 1, \dots, e-2$, we deduce that 5 has order 2^{e-2} modulo 2^e and that $5^{2^{e-3}}$ is not congruent to -1 modulo 2^e. It follows that $(\mathbb{Z}/2^e\mathbb{Z})^\times$ is the direct product of a cyclic group of order 2 and a cyclic group of order 2^{e-2}, hence is not cyclic. □

Solution to Exercise 10.
Let φ be the morphism of algebras $A_1[X_1, \dots, X_n] \to A_2[y_1, \dots, y_n]$ which maps X_i to y_i and whose restriction to A_1 is f. The kernel of φ is the set of polynomials P in $A_1[X_1, \dots, X_n]$ such that the polynomial $Q \in A_2[X_1, \dots, X_n]$, image of P by the extension of f to $A_1[X_1, \dots, X_n] \to A_2[X_1, \dots, X_n]$, satisfies

$$Q(y_1, \dots, y_n) = 0.$$

The kernel of the morphism $\psi : A_1[X_1, \dots, X_n] \to A_1[x_1, \dots, x_n]$, which maps X_i to x_i and whose restriction to A_1 is the identity, is the set of polynomials P in $A_1[X_1, \dots, X_n]$ such that $P(x_1, \dots, x_n) = 0$. The result is that F exists if and only if $\ker \psi \subset \ker \varphi$. □

Solution to Exercise 11.
See, for instance, [9] § 2.6. □

Solution to Exercise 13.
(a) The kernel of the endomorphism $x \mapsto x^2$ of the multiplicative group $F^\times$ is $\{\pm 1\}$. If q is even, that means in characteristic 2, we have $-1 = +1$, this endomorphism is an automorphism (namely the Frobenius Frob_2).

When q is odd, the kernel is a subgroup with 2 elements of $F^\times$, hence the image $\mathcal{C}$, which is the set of non–zero squares in F, has index 2 in $F^\times$: there are $(q-1)/2$ squares and $(q-1)/2$ nonsquares in $F^\times$. Each square is a root of $X^{(q-1)/2} - 1$; therefore

$$X^{(q-1)/2} - 1 = \prod_{x \in \mathcal{C}} (X - x).$$

Since

$$\prod_{a \in F^\times} (X - a) = X^{q-1} - 1 = (X^{(q-1)/2} - 1)(X^{(q-1)/2} + 1),$$

we deduce

$$X^{(q-1)/2} + 1 = \prod_{x \in F^\times \setminus \mathcal{C}} (X - x).$$

(b) From (a) we deduce

$$X^{(p-1)/2} - 1 = \prod_{a \in \mathbb{F}_p,\, \left(\frac{a}{p}\right) = 1} (X - a)$$

and

$$X^{(p-1)/2} + 1 = \prod_{a \in \mathbb{F}_p,\, \left(\frac{a}{p}\right) = -1} (X - a).$$

It follows that for a in $\mathbb{F}_p$,

$$\left(\frac{a}{p}\right) = a^{(p-1)/2}.$$

□

Solution to Exercise 14.
(a) In a finite field $\mathbb{F}_q$ of characteristic 2, any element α satisfies $\alpha^q = \alpha$, hence $\alpha = \beta^2$ with $\beta = \alpha^{q/2}$. Therefore any element is a square (in a unique way since $\beta^2 = \gamma^2$ implies $\beta = \gamma$).
If a polynomial $g \in \mathbb{F}_q[T]$ of degree $< q/2$ satisfies $g(\alpha) = \alpha^2$, then the polynomial $g(T)^2 - T^{q/2}$ is non zero, it has degree $< q$ and vanishes on $\mathbb{F}_q$, hence has q roots, which is not possible
(b) Assume q is odd and let $g \in \mathbb{F}_q[T]$ satisfies $g(\alpha) = \alpha^2$ for each α in $\mathbb{F}_q$ which is a square. There are $(q-1)/2$ non zero squares in $\mathbb{F}_q$ and $(q+1)/2$ squares (including 0). Hence the polynomial $g(T)^2 - T$ has $(q+1)/2$ zeros in $\mathbb{F}_q$. Since T is not a square in $\mathbb{F}_q[T]$, this polynomial is not zero, hence its degree is $\geq (q+1)/2$. Therefore g has degree $\geq (q+1)/4$.
(c) Assume $q \equiv 3 \mod 4$. Let $f(T) = T^{(q+1)/4}$ and let α be a square in $\mathbb{F}_q$, say $\alpha = \beta^2$ with $\beta \in \mathbb{F}_q$. From $\beta^q = \beta$ we deduce

$$f(\alpha)^2 = \alpha^{(q+1)/2} = \beta^{q+1} = \beta^2 = \alpha.$$

(d) For each $\alpha \in \mathbb{F}_q$ which is a square, select $\beta_\alpha \in \mathbb{F}_q$ such that $\alpha = \beta_\alpha^2$. We claim that there exists a polynomial $f \in \mathbb{F}_q[T]$ of degree $\leq (q-1)/2$ which satisfies the $(q+1)/2$ conditions $f(\alpha) = \beta_\alpha$ for the $(q+1)/2$ elements $\alpha \in \mathbb{F}_q$ which are squares. Such a polynomial computes the squares.
`Proof of the claim`. More generally, given a field F, $d+1$ distinct elements $\alpha_0, \alpha_1, \ldots, \alpha_d$ in F and $d+1$ elements $\beta_0, \beta_1, \ldots, \beta_d$ in F, there is a unique polynomial $f \in F[T]$ which satisfies $f(\alpha_i) = \beta_i$ for $i = 0, \ldots, d$. Indeed, the linear map

$$\begin{array}{ccc} \mathbb{F}_q[T]_{\leq d} & \longrightarrow & \mathbb{F}_q^{d+1} \\ f & \longmapsto & (f(\alpha_i))_{0 \leq i \leq d} \end{array}$$

is injective, hence surjective.
`Reference:` [5] □

Solution to Exercise 15.
Since 0 is a square, any square is the sum of two squares.

If F is a finite field of characteristic 2, the Frobenius $x \mapsto x^2$ is an automorphism of F, hence any element is a square in a unique way.

Assume F is a finite field with odd characteristic and with q elements. Consider the partition $F = Q \bigcup N$ where Q is the set of squares and N the set of non squares.

According to Exercise 13, the squares in F are the roots of

$$X(X^{(q-1)/2} - 1) = X^{(q+1)/2} - X,$$

hence Q has $(q+1)/2$ elements while N has $(q-1)/2$ elements.

Let $t \in F$. The set $t - Q$ has $(q+1)/2$ elements with $(q+1)/2 > (q-1)/2$, therefore one at least of these elements, say $t - x$ with $x \in Q$, is not in N – hence it is in Q. Let $y = t - x$. We have written $t = x + y$ as a sum of two squares. □

Solution to Exercise 16.
The kernel of the endomorphism $x \mapsto x^k$ of the cyclic multiplicative group $F^\times$ is the set of k–th roots of unity in F. According to Exercise 6 (ii), the number of its elements is $\gcd(k, q-1)$, hence the number of elements in $\mathcal{C}_k$ is

$$\frac{q-1}{\gcd(k, q-1)}.$$

□

Solution to Exercise 17. The complex conjugates of $\sqrt{2}+\sqrt{3}$ are $\pm\sqrt{2}\pm\sqrt{3}$. A simple computation yields

$$\begin{aligned}(X-\sqrt{2}-\sqrt{3})(X-\sqrt{2}+\sqrt{3})(X+\sqrt{2}-\sqrt{3})(X+\sqrt{2}+\sqrt{3}) &= X^4-10X^2+1\\ &= (X^2-1)^2-8X^2\\ &= (X^2+1)^2-12X^2\\ &= (X^2-5)^2-24.\end{aligned}$$

Notice also that this polynomial is $g(X^2)$ where $g(Y)=Y^2-10Y+1$ has discriminant $96=4^2 6$ and roots $5\pm 2\sqrt{6}$. Indeed, $\sqrt{2}+\sqrt{3}=\sqrt{5+2\sqrt{6}}$.

If 2 is a square in $\mathbb{F}_p$, then

$$X^4-10X^2+1=(X^2-2\sqrt{2}X-1)(X^2+2\sqrt{2}X-1).$$

If 3 is a square in $\mathbb{F}_p$, then

$$X^4-10X^2+1=(X^2-2\sqrt{3}X+1)(X^2+2\sqrt{3}X+1).$$

If neither 2 not 3 are squares in $\mathbb{F}_p$, then 6 is a square and

$$X^4-10X^2+1=(X^2-(5+2\sqrt{6}))(X^2-(5-2\sqrt{6})).$$

□

Solution to Exercise 18.
In a field F with q elements, any element x satisfies $x^q=x$, hence $x^q-x+1\neq 0$. This proves that F is not algebraically closed. □

Solution to Exercise 21. For each primitive root α modulo p, we give the table of the exponentials in basis α, namely α^n for $n=0,1,\ldots,p-2$. One can view the values of n modulo $p-1$, while the values of α^n are modulo p. It is plain to deduce the table of the logarithms with respect to the primitive root α. We give explicitly this table only for $p=31$ and $\alpha=3$.

1. $p=2$, $\alpha=1$
2. $p=3$, $\alpha=1$ or $\alpha=2$.
3. $p=5$, $\alpha=2$ or $\alpha=3$.

	$n=$	0	1	2	3
α^n :	$\alpha=2$	1	2	4	3
	$\alpha=3$	1	3	4	2

4. $p = 7$, $\alpha = 3$ or $\alpha = 5$.

	$n =$	0	1	2	3	4	5
α^n	$\alpha = 3$	1	3	2	6	4	5
	$\alpha = 5$	1	5	4	6	2	3

5. $p = 11$

From $2^5 = 32 \equiv -1 \pmod{11}$ it follows that 2 is a primitive root modulo 11 (a generator of the cyclic group $\mathbb{F}_{11}^{\times}$):

$n =$	0	1	2	3	4	5	6	7	8	9
$2^n =$	1	2	4	8	5	10	9	7	3	6

We have $\varphi(10) = 4$, $(\mathbb{Z}/10\mathbb{Z})^{\times} = \{1, 3, 7, 9\}$, the primitive roots modulo 11 are 2, $2^3 = 8$, $2^7 = 7$, $2^9 = 6$.

To get the table of exponentials 8^n we take the shift of the table for 2^n by 3:

$n =$	0	1	2	3	4	5	6	7	8	9
$8^n =$	1	8	9	6	4	10	3	2	5	7

To get the table of exponentials 7^n we reverse the order of the table for 8^n (since $7 = 8^{-1}$):

$n =$	0	1	2	3	4	5	6	7	8	9
$7^n =$	1	7	5	2	3	10	4	6	9	8

To get the table of exponentials 6^n we reverse the order of the table for 2^n (since $6 = 2^{-1}$):

$n =$	0	1	2	3	4	5	6	7	8	9
$6^n =$	1	6	3	7	9	10	5	8	4	2

6. $p = 13$

We have $\varphi(12) = 4$, the primitive roots modulo 13 are 2, $2^5 = 6$, $2^7 = 11$, $2^{11} = 7$.

The table of 2^n for $n = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11$ is

$n =$	0	1	2	3	4	5	6	7	8	9	10	11
$2^n =$	1	2	4	8	3	6	12	11	9	5	10	7

The table for 6^n is obtained by shifting by 5 the table for 2^n:

$$6^n : \quad 1, 6, 10, 8, 9, 2, 12, 7, 3, 5, 4, 11.$$

The table for 11^n is the reverse of the table for 6^n:

$$11^n : \qquad 1,\ 11,\ 4,\ 5,\ 3,\ 7,\ 12,\ 2,\ 9,\ 8,\ 10,\ 6.$$

The table for 7^n is the reverse of the table for 2^n:

$$7^n : \qquad 1,\ 7,\ 10,\ 5,\ 9,\ 11,\ 12,\ 6,\ 3,\ 8,\ 4,\ 2.$$

7. $p = 31$

Since $\varphi(30) = 8$, there are 8 primitive roots modulo 31.

From $2^5 \equiv 1 \pmod{31}$, it follows that 2 has order 5 in $\mathbb{F}_{31}^{\times}$, hence is not a primitive root modulo 31.

A primitive root modulo 31 is 3. The table of 3^n for $n = 1, 2, \ldots, 30$ is given by

$n =$	0	1	2	3	4	5	6	7	8	9
$3^n =$	1	3	9	27	19	26	16	17	20	29

$n =$	10	11	12	13	14	15	16	17	18	19
$3^n =$	25	13	8	24	10	30	28	22	4	12

$n =$	20	21	22	23	24	25	26	27	28	29
$3^n =$	5	15	14	11	2	6	18	23	7	21

The primitive roots modulo 31 are

$$3,\ 3^7 = 17,\ 3^{11} = 13,\ 3^{13} = 24,\ 3^{17} = 22,\ 3^{19} = 12,\ 3^{23} = 11,\ 3^{29} = 21.$$

One checks indeed that the numbers

$$3 \times 21 = 63,\ 17 \times 11 = 187,\ 13 \times 12 = 156,\ 24 \times 22 = 528$$

are congruent to 1 modulo 31.

The table for 17^n is the shift by 7 of the table for 3^n, the table for 13^n is the shift by 4 of the table for 17^n, the table for 24^n is the shift by 2 of the table for 13^n, and we get the other tables by reversing the order.

The table of the discrete logarithms with respect to 3 modulo 31 is the following (the first row is 3^n modulo 31, the second row is n modulo 30):

1	2	3	4	5	6	7	8	9	10
0	24	1	18	20	25	28	12	2	14

11	12	13	14	15	16	17	18	19	20
23	19	11	22	21	6	7	26	4	8

21	22	23	24	25	26	27	28	29	30
29	17	27	13	10	5	3	16	9	15

□

Solution to Exercise 28.
(a) Let $n = ms + r$ with $0 \leq r < m$ be the Euclidean division of n by m in $\mathbb{Z}$, with quotient s and remainder r. From

$$X^n - 1 = (X^{ms} - 1)X^r + X^r - 1$$

we deduce that

$$X^n - 1 = (X^m - 1)S + X^r - 1$$

is the Euclidean division of $X^n - 1$ by $X^m - 1$ in $\mathbb{Z}[X]$, with quotient

$$S(X) = \frac{X^{ms} - 1}{X^m - 1}X^r = X^{m(s-1)+r} + X^{m(s-2)+r} + \cdots + X^{m+r} + X^r$$

and remainder $X^r - 1$.
(b) For $n = ms + r$, we deduce from (a) that

$$\gcd(X^n - 1, X^m - 1) = \gcd(X^m - 1, X^r - 1).$$

The result follows by induction on $\max\{n, m\}$.
(c) From (a) we deduce that the remainder of the Euclidean division of $a^n - 1$ by $a^m - 1$ is $a^r - 1$, and from (b) that the gcd of $a^n - 1$ and $a^m - 1$ is $a^d - 1$ where $d = \gcd(n, m)$. The result easily follows. □

Solution to Exercise 32.
(a) (See Example 66).
(b) (See Example 67).
(c) (See Example 82).
(d) According to Example 82, we have

$$\mathbb{F}_4 = \mathbb{F}_2[Y]/(Y^2 + Y + 1),$$

hence $\mathbb{F}_4 = \mathbb{F}_2(j)$ where $j^2 = j + 1$. Over $\mathbb{F}_4 = \mathbb{F}_2(j)$, the polynomial $X^2 + X + j$ is irreducible. □

Solution to Exercise 33.
(a) Irreducible polynomials over $\mathbb{F}_2$:
degree 1: X, $X + 1$
degree 2: $X^2 + X + 1$ (see see Example 66)
degree 3: $X^3 + X + 1$ and $X^3 + X^2 + 1$ (see Example 67)
degree 4: $X^4 + X + 1$, $X^4 + X^3 + 1$, Φ_5 (see Example 82)
degree 5: there are six of them: write $P(0) \neq 0$, $P(1) \neq 0$ and omit

$$(X^2 + X + 1)(X^3 + X + 1) = X^5 + X^4 + 1 \quad \text{and} \quad (X^2 + X + 1)(X^3 + X^2 + 1) = X^5 + X + 1.$$

Remain:

$$X^2 + aX^4 + bX^3 + cX^2 + (a + b + c + 1)X + 1$$

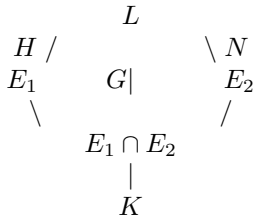
with a, b, c in $\mathbb{F}_2$ omitting $(1, 0, 0)$ and $(0, 0, 0)$.
(b) Write $\mathbb{F}_4 = \{0, 1, j, j^2\}$. The four irreducible polynomials of degree 1 over $\mathbb{F}_4$ are X, $X - 1$, $X - j$, $X - j^2$. For the 6 irreducible polynomials of degree 2 over $\mathbb{F}_4$, see Exercise 84. □

Solution to Exercise 35.
a) Let $s : G \to G/N$ be the canonical surjective morphism of groups with kernel N. The restriction of s to H has kernel $H \cap N$ and image $s(H) = (H + N)/N$, hence

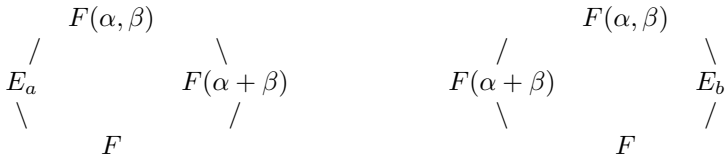
$$s(H) = \frac{H+N}{N} \simeq \frac{H}{H \cap N}.$$

Since $s(H)$ is a subgroup of G/N, its order, which is the index of $H \cap N$ in H, divides the order of G/N, which is the index of N in G.

If $H \cap N = \{1\}$, then the index of $H \cap N$ in H is the order of H.
(b) We apply (a) with G the Galois group of the extension $L/E_1 \cap E_2$, which is a finite abelian group, H the Galois group of L/E_1 and N the Galois group of L/E_2. The order of H is $[L : E_1]$ while the index of N in G is $[E_2 : E_1 \cap E_2]$. The conclusion follows from the remark that $[E_2 : E_1 \cap E_2]$ divides $[E_2 : K]$:



c) Let $E_a = F(\alpha + \beta) \cap F(\alpha)$ and $E_b = F(\alpha + \beta) \cap F(\beta)$. We apply (b) with $L = F(\alpha, \beta)$, $K = F$, $E_1 = F(\alpha)$ or $F(\beta)$, $E_2 = F(\alpha + \beta)$:



The first diagram shows that $[F(\alpha, \beta) : F(\alpha + \beta)]$ divides $[E_a : F] = a$, while the second diagram shows that $[F(\alpha, \beta) : F(\alpha + \beta)]$ divides $[E_b : F] = b$, hence $[F(\alpha, \beta) : F(\alpha + \beta)] = 1$ and therefore $F(\alpha, \beta) = F(\alpha + \beta)$. □

Solution to Exercise 38.
Let $r = [E : F]$.
(a) If $\alpha = \beta^q - \beta$ with $\beta \in E$, then from $\mathrm{Tr}(\beta^q) = \mathrm{Tr}(\beta)$ we deduce $\mathrm{Tr}_{E/F}(\alpha) = \mathrm{Tr}_{E/F}(\beta^q) - \mathrm{Tr}_{E/F}(\beta) = 0$.

Conversely, assume $\mathrm{Tr}_{E/F}(\alpha) = 0$. Let β be a root of the polynomial $X^q - X - \alpha$ in an extension of E (the number of roots of this polynomial is q). Then $\alpha = \beta^q - \beta$ and

$$\begin{aligned}
\mathrm{Tr}_{E/F}(\alpha) =& \alpha + \alpha^q + \cdots + \alpha^{q^{r-1}} \\
=& (\beta^q - \beta) + (\beta^q - \beta)^q + \cdots + (\beta^q - \beta)^{q^{r-1}} \\
=& (\beta^q - \beta) + (\beta^{q^2} - \beta^q) + \cdots + (\beta^{q^r} - \beta^{q^{r-1}}) = \beta^{q^r} - \beta,
\end{aligned}$$

hence $\beta^{q^r} = \beta$, which means that β is in E.
Here is another proof using the normal basis Theorem 34. Let $\gamma \in E$ be such that $\gamma, \gamma^q, \gamma^{q^2}, \dots, \gamma^{q^{r-1}}$ is a basis of E as an F–vector space. Any $\alpha \in E$ can be written in a unique way

$$\alpha = a_0\gamma + a_1\gamma^q + a_2\gamma^{q^2} + \cdots + a_{r-1}\gamma^{q^{r-1}},$$

with $a_j \in F$ $(0 \leq j < r)$. We have $\mathrm{Tr}_{E/F}(\alpha) = (a_0 + a_1 + \cdots + a_{r-1})\mathrm{Tr}_{E/F}(\gamma)$. Since the trace is not the zero map, we deduce $\mathrm{Tr}_{E/F}(\gamma) \neq 0$.

Assume $\mathrm{Tr}_{E/F}(\alpha) = 0$: hence $a_0 + a_1 + \cdots + a_{r-1} = 0$. We are looking for an element $\beta \in E$ such that $\alpha = \beta^q - \beta$; write

$$\beta = b_0\gamma + b_1\gamma^q + b_2\gamma^{q^2} + \cdots + b_{r-1}\gamma^{q^{r-1}}$$

with $b_j \in F$ $(0 \leq j < r)$. From

$$\beta^q - \beta = (b_{r-1} - b_0)\gamma + (b_0 - b_1)\gamma^q + (b_1 - b_2)\gamma^{q^2} + \cdots + (b_{r-2} - b_{r-1})\gamma^{q^{r-1}},$$

it follows that the equation $\alpha = \beta^q - \beta$ is equivalent to a linear system in $b_0, b_1, b_2, \dots, b_{r-1}$:

$$b_0 - b_1 = a_1,\ b_1 - b_2 = a_2, \dots, b_{r-2} - b_{r-1} = a_{r-1},\ b_{r-1} - b_0 = a_0.$$

Thanks to the assumption $a_0 + a_1 + \cdots + a_{r-1} = 0$, this system has q solutions: given $b_0 \in F$, the corresponding solution $(b_0, b_1, b_2, \dots, b_{r-1}) \in F^r$ is given by

$$b_i = b_0 - a_1 - a_2 - \cdots - a_i \qquad (i = 1, 2, \dots, r-1).$$

(b) If $\alpha = \beta^{q-1}$ with $\beta \in E^\times$, then from $\beta^{q^r} = \beta$ we deduce $\mathrm{N}_{E/F}(\alpha) = \alpha^{(q^r-1)/(q-1)} = \beta^{q^r-1} = 1$.

Conversely, assume $\mathrm{N}_{E/F}(\alpha) = 1$. Let β be a root of the polynomial $X^{q-1} - \alpha$ in an extension of E (the number of roots is $q-1$). Then $\alpha = \beta^{q-1}$ and

$$\mathrm{N}_{E/F}(\alpha) = \alpha^{(q^r-1)/(q-1)} = \beta^{q^r-1} = 1,$$

hence $\beta^{q^r} = \beta$ and therefore $\beta \in E$.
Here is a variant of this proof. Assume $\alpha^{(q^r-1)/(q-1)} = 1$. Let ζ be a generator of the cyclic group $E^\times$. Write $\alpha = \zeta^m$, with $0 \leq m \leq q^r - 1$. Since ζ is of order $q^r - 1$ and since $\zeta^{m(q^r-1)/(q-1)} = 1$, we deduce that $q^r - 1$ divides $m(q^r-1)/(q-1)$, hence $q-1$ divides m. Therefore the $q-1$ roots β of the polynomial $X^{q-1} - \alpha$ belong to E. □

Solution to Exercise 39.
(a) One readily checks that u_r and t_r are $\mathbb{F}_p$ linear, that $\ker(u_r) = \mathbb{F}_p$ and that $\mathrm{im}(t_r) \subset \mathbb{F}_p$. The kernel of t_r has at most p^{r-1} elements (namely the roots of the polynomial $X + X^p + \cdots + X^{p^{r-1}}$), hence the image of t_r is $\mathbb{F}_p$, and this polynomial has p^{r-1} roots in $\mathbb{F}_q$.

If $\alpha = u_r(\beta)$ with $\beta \in \mathbb{F}_q$, then

$$\alpha^{p^j} = \beta^{p^j} - \beta^{p^{j-1}}$$

for all $j \geq 1$ and therefore

$$t_r(\alpha) = (\beta^p - \beta) + (\beta^{p^2} - \beta^p) + \cdots + (\beta^{p^r} - \beta^{p^{r-1}}) = \beta^{p^r} - \beta = 0,$$

from which one deduces $\mathrm{im}(u_r) = \ker(u_r)$.
(b) The polynomial

$$\prod_{a\in\mathbb{F}_p} (X + X^p + \cdots + X^{p^{r-1}} - a)$$

has degree p^r, its derivative is 1 and its zeroes are the p^r elements of $\mathbb{F}_q$.
(c) Write $q = p^r$ so that $\mathbb{F}_p(\gamma) = \mathbb{F}_q$.
(i) If $t_r(\gamma) = 0$, then $\gamma \in \mathrm{im}(u_r)$ and the polynomial $X^p - X - \gamma$ has a root α in $\mathbb{F}_q$. In this case the p roots of $X^p - X - \gamma$, namely $\alpha + a$, $a \in \mathbb{F}_p$, are in $\mathbb{F}_q$.
(ii) Assume $t_r(\gamma) \neq 0$. Hence $\gamma \notin \mathrm{im}(u_r)$ and the polynomial $X^p - X - \gamma$ has no root in $\mathbb{F}_q$. Let α be a root in Ω. For $\ell \geq 0$ we have

$$\alpha^{p^\ell} - \alpha = \gamma + \gamma^p + \cdots + \gamma^{p^{\ell-1}},$$

hence

$$\alpha^q - \alpha = a$$

with $a = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\gamma) \in \mathbb{F}_p$. From $\alpha \notin \mathbb{F}_q$ we deduce $\alpha^q \neq \alpha$, hence $a \neq 0$. It follows that the p elements

$$\alpha^{q^j} = \alpha + ja \quad (j = 0, 1, \ldots, p-1)$$

are pairwise distinct, hence $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = p$. □

Solution to Exercise 40.
Let q be the number of elements in F and n the degree of the extension E/F. Hence the field E has q^n elements. We have

$$\mathrm{N}_{E/F}(\alpha) = \alpha^{(q^n-1)/(q-1)}.$$

If $\mathrm{N}_{E/F}(\alpha)$ has order $< q-1$ in $F^\times$, then there exists an integer ℓ with $1 \leq \ell < q-1$ such that $\mathrm{N}_{E/F}(\alpha)^\ell = 1$, hence $\alpha^{(q^n-1)\ell/(q-1)} = 1$. Since

$$0 < \frac{(q^n-1)\ell}{q-1} < q^n - 1,$$

it follows that α has order $< q^n - 1$ in $E^\times$. □

Solution to Exercise 41.
(a) See Example 73.
(b) This is a special case of Exercise 40. Indeed, The norm over $\mathbb{F}_q$ of $a + ib \in \mathbb{F}_q(i)$ is

$$a^2 + b^2 = (a + ib)(a - ib) = (a + ib)^{p+1},$$

hence if $a + ib$ is a primitive root in $\mathbb{F}_{p^2}$ then $a^2 + b^2$ is a primitive root in $\mathbb{F}_p$.

Conversely, assume that $a^2 + b^2$ has order $p-1$ in the multiplicative group $\mathbb{F}_p^\times$. If $(a+ib)^m = 1$, then $(a - ib)^m = 1$ and $(a^2 + b^2)^m = 1$, therefore $p - 1$ divides m, which means that the order of $a + ib$ is a multiple of $p - 1$.

Also, we have

$$(a^2 + b^2)^{(p-1)/2} = (a + ib)^{(p-1)(p+1)/2} = -1,$$

hence the order of $a + ib$ does not divide $(p^2 - 1)/2$.
(c) Assume now that p is a Mersenne prime. Using the fact that $p + 1$ is a power of 2, we deduce that the only multiple of $p - 1$ which divides $p^2 - 1$ but does not divide $(p^2 - 1)/2$ is $p^2 - 1$ itself. □

Solution to Exercise 42.
(See also exercise 113).
(a) If a prime number p divides 2^n+1, then p is odd and 2 has order $n+1$ modulo p.
(b) We have $5^4 \equiv -2^4 \mod 641$ and $5 \equiv -2^{-7} \mod 641$, hence $-2^4 \equiv 2^{-28} \mod 641$. Therefore $2^{32} \equiv -1 \mod 641$. □

Solution to Exercise 46.
(a) Recall that Euler totient function φ is a multiplicative arithmetic function: $\varphi(ab) = \varphi(a)\varphi(b)$ when $\gcd(a,b) = 1$. For $n = p_1^{r_1} \cdots p_s^{r_s}$ where $p_1, \ldots, p_s$ are distinct odd primes and $r_i \geq 1$, we have

$$\varphi(n) = p_1^{r_1-1}(p_1-1) \cdots p_s^{r_s-1}(p_s-1),$$

while for the radical R of n we have

$$R = p_1 \cdots p_s \quad \text{and} \quad \varphi(R) = (p_1-1) \cdots (p_s-1),$$

hence

$$R\varphi(n) = n\varphi(R).$$

If ζ is a primitive root of unity of order n and if d divides n, then $\zeta^{n/d}$ is a primitive root of unity of order d. If, further, $d\varphi(n) = n\varphi(d)$, then the polynomial $\Phi_d(X^{n/d})$ is monic, of degree $\varphi(n)$ and vanishes at the primitive n–th roots of unity; hence it is $\Phi_n(X)$. This completes the proof of (a).
(b) If ζ is a primitive root of unity of order pm_1, then ζ^p is a primitive root of unity of order m_1. Since m_1 and p are relatively prime, if ζ is a primitive root of unity of order m_1, then ζ^p is also a primitive root of unity of order m_1. Now the polynomial $\Phi_{m_1}(X^p)$ has a simple zero at all primitive roots of unity of order m and at all primitive roots of unity of order m_1 and has the same degree as $\Phi_m(X)\Phi_{m_1}(X)$, namely $p\varphi(m_1) = \varphi(m) + \varphi(m_1)$; hence these two polynomials are the same.
(c) Denote by R_1 the radical of m_1. The radical of m is pR_1. Using (a) and (b) we deduce

$$\Phi_{p^r m_1}(X) = \Phi_{pR_1}(X^{p^{r-1}m_1/R_1}) = \frac{\Phi_{R_1}(X^{p^r m_1/R_1})}{\Phi_{R_1}(X^{p^{r-1}m_1/R_1})} = \frac{\Phi_{m_1}(X^{p^r})}{\Phi_{m_1}(X^{p^{r-1}})}.$$

(d) follows from (c).
(e) If n is odd, the map $\zeta \mapsto -\zeta$ is a bijective map from the set of primitive n-th roots of unity to the set of primitive $2n$-th roots of unity. Hence $\Phi_{2n}(X) = \Phi_n(-X)$ for n odd ≥ 3.

Assume now n is even. The relation $\Phi_{2n}(X) = \Phi_n(X^2)$ follows from (c) (and also from (a)). Notice that the map $\zeta \mapsto \zeta^2$ from μ_{2n} to μ_n is a surjective homomorphism of kernel $\{\pm 1\}$.
(f) We have $\Phi_1(1) = 0$. Assume now $n \geq 2$. From

$$X^{n-1} + X^{n-2} + \cdots + X + 1 = \prod_{d|n, d\geq 2} \Phi_d(X)$$

we deduce

$$\prod_{d|n, d\geq 2} \Phi_d(1) = n.$$

The von Mangoldt function is defined for $n \geq 1$ as

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^r \text{ with } p \text{ prime and } r \geq 1; \\ 0 & \text{otherwise.} \end{cases}$$

It satisfies, for $n \geq 2$,

$$\sum_{d|n, d\geq 2} \Lambda(d) = \log n,$$

which means

$$\prod_{d|n, d\geq 2} e^{\Lambda(d)} = n.$$

Since $\Phi_p(1) = p = e^{\Lambda(p)}$ when p is prime, it follows by induction that

$$\Phi_n(1) = e^{\Lambda(n)}$$

for all $n \geq 2$.

(g) We have $\Phi_1(-1) = -2$, $\Phi_2(-1) = 0$. Assume now $n \geq 3$.

Assume first that n is odd. Using the formula

$$X^n - 1 = (X-1) \prod_{d|n, d\geq 3} \Phi_d(X),$$

we deduce by induction $\Phi_n(-1) = 1$.

Assume n is even, say $n = 2^r m$ where $r \geq 1$ while m is odd. Then $\Phi_n(X) = \Phi_{2m}(X^{2^{r-1}})$. Hence $\Phi_n(-1) = \Phi_{2m}(1) = e^{\Lambda(2m)} = e^{\Lambda(n/2)}$. □

Solution to Exercise 50. Write the decomposition of n into prime factors

$$n = p_1^{a_1} \cdots p_k^{a_k}.$$

We have

$$\frac{\varphi(n)}{n} = \frac{p_1}{p_1 - 1} \cdots \frac{p_k}{p_k - 1}.$$

Set

$$\lambda = 1 - \frac{\log 4}{\log 5},$$

so that

$$\frac{p_i}{p_i - 1} \leq \frac{5}{4} \leq p_i^{\lambda} \quad \text{for} \quad i \geq 3.$$

Thus

$$\frac{\varphi(n)}{n} \leq 3(p_3 \cdots p_k)^{\lambda} \leq 2.341(p_1 \cdots p_k)^{\lambda} \leq 2.341 n^{\lambda},$$

so that

$$n \leq \big(3.341\varphi(n)\big)^{1/(1-\lambda)} \leq 2.685\varphi(n)^{1.161}$$

for all $n \geq 1$.

`Remark`. It is known that for any $\epsilon > 0$, there exists an integer $n_0 > 0$ such that, for $n \geq n_0$,

$$n \leq (e^{\gamma} + \epsilon)\varphi(n) \log\log \varphi(n)$$

where γ is Euler's constant. Equivalently,

$$\varphi(n) \geq (e^{-\gamma} - \epsilon)\frac{n}{\log\log n}$$

for sufficiently large n. □

Solution to Exercise 54.
(a) Assume p does not divide m. We prove the relation in characteristic p:

$$\Phi_{p^r m}(X) = \Phi_m(X)^{\varphi(p^r)}$$

by induction on $p^r m$. We have

$$X^{p^r m} - 1 = (X^m - 1)^{p^r}. \tag{131}$$

Writing a divisor of $p^r m$ as $p^k d$ with d dividing m and $0 \leq k \leq r$, using the induction hypothesis and the equality

$$\sum_{k=0}^{r} \varphi(p^k) = p^r,$$

we see that the left hand side of (131) is

$$\begin{aligned}
\prod_{d|p^r m} \Phi_d(X) &= \prod_{k=0}^{r} \prod_{d|m} \Phi_{p^k d}(X) \\
&= \Phi_{p^r m}(X) \left(\prod_{k=0}^{r-1} \Phi_{m p^k}(X) \right) \left(\prod_{d|m, d\neq m} \prod_{k=0}^{r} \Phi_{p^k d}(X) \right) \\
&= \Phi_{p^r m}(X) \left(\prod_{k=0}^{r-1} \Phi_m(X)^{\varphi(p^k)} \right) \left(\prod_{d|m, d\neq m} \prod_{k=0}^{r} (\Phi_d(X))^{\varphi(p^r)} \right) \\
&= \Phi_{p^r m}(X) \Phi_m(X)^{p^{r-1}} \prod_{d|m, d\neq m} (\Phi_d(X))^{p^r}
\end{aligned}$$

while the right hand side of (131) is

$$\prod_{d|m} (\Phi_d(X))^{p^r}.$$

This completes the proof of (a)
(b) If $m = m_1 p^k$ with $k \geq 1$ and $\gcd(m_1, p) = 1$, then

$$\Phi_m(X) = \Phi_{m_1 p^k}(X) = \Phi_{m_1}(X)^{p^k - p^{k-1}},$$

$$\Phi_{p^r m}(X) = \Phi_{m_1 p^{r+k}}(X) = \Phi_{m_1}(X)^{p^{r+k} - p^{r+k-1}},$$

hence

$$\Phi_{p^r m}(X) = \Phi_m(X)^{p^r}.$$

□

Solution to Exercise 58.
(a) From (56) it follows that the number $N_2(n)$ of irreducible polynomials of degree n over $\mathbb{F}_2$ satisfies

the following relations.

$$\begin{aligned}
2^1 = N_2(1), &\quad \text{hence} \quad N_2(1) = 2.\\
2^2 = 4 = N_2(1) + 2N_2(2), &\quad \text{hence} \quad N_2(2) = 1.\\
2^3 = 8 = N_2(1) + 3N_2(3), &\quad \text{hence} \quad N_2(3) = 2.\\
2^4 = 16 = N_2(1) + 2N_2(2) + 4N_2(4), &\quad \text{hence} \quad N_2(4) = 3.\\
2^5 = 32 = N_2(1) + 5N_2(5), &\quad \text{hence} \quad N_2(5) = 6.\\
2^6 = 64 = N_2(1) + 2N_2(2) + 3N_2(3) + 6N_2(6), &\quad \text{hence} \quad N_2(6) = 9.
\end{aligned}$$

(b) and (c) The upper bound

$$N_q(n) \leq \frac{1}{n}(q^n - q)$$

for $n > 1$ can be checked as follows. On the one hand, each irreducible polynomial of degree n over $\mathbb{F}_q$ has n roots in $\mathbb{F}_{q^n}$. On the other hand, since $n > 1$, the number of elements in $\mathbb{F}_{q^n}$ having degree n over $\mathbb{F}_q$ is $\leq q^n - q$; each of these elements has n conjugates over $\mathbb{F}_q$. Therefore the number of roots in $\mathbb{F}_{q^n}$ of the irreducible polynomials of degree n over $\mathbb{F}_q$ is $\leq q^n - q$. It follows that the number of irreducible polynomials of degree n over $\mathbb{F}_q$ is $\leq (q^n - q)/n$.

On the other hand from (56) we deduce

$$q^n - nN_q(n) = \sum_{d|n, d<n} dN_q(d) \leq \sum_{d|n, d<n} q^d \leq \sum_{0 \leq k \leq n/2} q^k = \frac{q^{\lfloor n/2 \rfloor + 1} - 1}{q - 1} < q^{\lfloor n/2 \rfloor + 1}.$$

Hence

$$N_q(n) > \frac{q^n - q^{\lfloor n/2 \rfloor + 1}}{n}.$$

(See also [9], Theorem 19.10).
(d) As soon as

$$q^n \geq 4q^{n/2},$$

more than half of the elements α in $\mathbb{F}_q$ satisfy $\mathbb{F}_q = \mathbb{F}_p(\alpha)$.
(e) There are q^n monic polynomials of degree n in $\mathbb{F}_q[X]$. Since

$$\lim_{q^n \to \infty} \frac{nN_q(n)}{q^n} = 1,$$

the number $N_q(n)$ of monic irreducible polynomials of degree n in $\mathbb{F}_q[X]$ is asymptotically q^n/n. □

Solution to Exercise 62.
From Corollary 61 it follows that the polynomial $X^q - 1 = (X - 1)\Phi_q(X)$ splits completely in the finite field $\mathbb{F}_p$ if and only if p is congruent to 1 modulo q, in which case p is a square modulo q. Using the Legendre reciprocity law and the assumption that at least one of p, q, is congruent to 1 modulo 4, we deduce that q is a square modulo p, hence that $X^2 - q$ splits in $\mathbb{F}_p$. □

Solution to Exercise 64.
(a) Over a field of characteristic 2, $\Phi_8(X) = X^4 + 1 = (X+1)^4$ splits into linear factors.

Let $\mathbb{F}_q$ be a finite field of odd characteristic. Over $\mathbb{F}_q$, the cyclotomic polynomial Φ_8 splits into irreducible factors, all of the same degree d, which is the order of q modulo 8. The number $q^2 - 1 = (q-1)(q+1)$ is a multiple of 8 (each of $q-1$ and $q+1$ is even, one of them is divisible by 4). Hence $q^2 \equiv 1 \mod 8$, which proves that the order d of $q \mod 8$ is 1 or 2.

Notice that $d = 1$ if and only if $q \equiv 1 \mod 8$. Indeed, $\mathbb{F}_q^\times$ contains a subgroup of order 8 if and only 8 divides $q-1$. Hence $d = 2$ for q congruent to 3, 5 or 7 modulo 8.

For $q = p^r$ with p an odd prime, over $\mathbb{F}_q$ the polynomial Φ_8 splits into 4 linear factors if either $p \equiv 1 \mod 8$ or r is even, and into 2 irreducible quadratic factor if p is congruent to 3, 5 or 7 modulo 8 and r is odd.

(b) Over $\mathbb{F}_2$ we have $\Phi_{12}(X) = (X^2 + X + 1)^2$, the square of an irreducible quadratic polynomial. Hence over $\mathbb{F}_{2^r}$ the polynomial Φ_{12} splits into 4 linear factors if r is even, into 2 irreducible quadratic factor if r is odd.

Over $\mathbb{F}_3$ we have $\Phi_{12}(X) = (X^2 + 1)^2$. Hence over $\mathbb{F}_{3^r}$ the polynomial Φ_{12} splits into 4 linear factors if r is even, into 2 irreducible quadratic factor if r is odd.

For $p \geq 5$, the product $(q-1)(q+1)$ is divisible by 12. Since $5, 7, 11$ have order 2 modulo 12, the polynomial Φ_{12} splits into 4 linear factors in $\mathbb{F}_q$ when $q \equiv 1 \mod 12$ and is a product of 2 irreducible quadratic factors otherwise. □

Solution to Exercise 68.
The field $\mathbb{F}_8$ is a cubic extension of $\mathbb{F}_2$ (see Example 67). Let ζ be a root of the polynomial $X^3 + X + 1 \in \mathbb{F}_2[X]$, so that $\mathbb{F}_8 = \mathbb{F}_2(\zeta)$ and

$$\mathbb{F}_8 = \{a + b\zeta + c\zeta^2 \mid (a,b,c) \in \mathbb{F}_2^3\}.$$

The group $\mathbb{F}_8^\times$ is cyclic of order 7, there are 6 generators (primitive roots in $\mathbb{F}_8$), namely

$$\{\zeta, \zeta^2, \zeta + \zeta^2, 1 + \zeta, 1 + \zeta^2, 1 + \zeta + \zeta^2\}.$$

The table of exponentials in $\mathbb{F}_8^\times$ with respect to ζ is

$n =$	0	1	2	3	4	5	6
$\zeta^n =$	1	ζ	ζ^2	$1+\zeta$	$\zeta+\zeta^2$	$1+\zeta+\zeta^2$	$1+\zeta^2$

and this gives the table of discrete logarithms with respect to ζ, since $n = \mathrm{Ind}_\zeta(\zeta^n)$. In the same way we deduce the following table for $\mathrm{Ind}_{\zeta^n}\gamma$:

$\gamma =$	1	ζ	ζ^2	$1+\zeta$	$1+\zeta^2$	$\zeta+\zeta^2$	$1+\zeta+\zeta^2$
$n = 1$	0	1	2	3	6	4	5
$n = 2$	0	4	1	5	3	2	6
$n = 3$	0	5	3	1	2	6	4
$n = 4$	0	2	4	6	5	1	3
$n = 5$	0	3	6	2	4	5	1
$n = 6$	0	6	5	4	1	3	2

Given $m \in \{1, 2, 3, 4, 5, 6\}$ and $\gamma \in \mathbb{F}_8^\times$ with $\gamma \neq 1$, there is a unique n modulo 7 such that $\mathrm{Ind}_{\zeta^n}\gamma = m$, i.e. such that $\zeta^{nm} = \gamma$. □

Solution to Exercise 70.
The field $\mathbb{F}_9$ is a quadratic extension of $\mathbb{F}_3$ (see Example 69). Since $\varphi(8) = 4$, there are 4 primitive roots in $\mathbb{F}_9$. Let $i \in \mathbb{F}_9$ be a root of $X^2 + 1$ and let $\zeta = 1 + i$, so that

$$\zeta = 1 + i, \quad \zeta^2 = -i, \quad \zeta^3 = 1 - i, \quad \zeta^4 = -1, \quad \zeta^5 = -1 - i, \quad \zeta^6 = i, \quad \zeta^7 = -1 + i.$$

The roots in $\mathbb{F}_9$ of the polynomial $X^2 + X - 1 \in \mathbb{F}_3[X]$ are ζ and ζ^3. Let $\eta = -1 + i$, so that $\eta = \zeta^7$ and $\eta^3 = \zeta^5 = -1 - i$. The roots in $\mathbb{F}_9$ of the polynomial $X^2 - X - 1 \in \mathbb{F}_3[X]$ are η and η^3. The 4 primitive roots in $\mathbb{F}_9$ are ζ, ζ^3, η, η^3.

The table of discrete logarithms in $\mathbb{F}_9$ is the following

$\gamma =$	1	-1	i	$-i$	$1+i$	$-1+i$	$1-i$	$-1-i$
$\mathrm{Ind}_\zeta \gamma =$	0	4	6	2	1	7	3	5
$\mathrm{Ind}_{\zeta^3} \gamma =$	0	4	2	6	3	5	1	7
$\mathrm{Ind}_\eta \gamma =$	0	4	2	6	7	1	5	3
$\mathrm{Ind}_{\eta^3} \gamma =$	0	4	6	2	5	3	7	1

□

Solution to Exercise 71.
From

$$3^5 = 243 = 22 \times 11 + 1$$

we deduce that the class of 3 has order 5 modulo 11. Hence Φ_{11}, which has degree $\varphi(11) = 10$, splits into two irreducible polynomials of degree 5 over $\mathbb{F}_3$:

$$\Phi_{11}(X) = f(X)g(X)$$

where

$$f(X) = X^5 + X^4 - X^3 + X^2 - 1 \quad \text{and} \quad g(X) = X^5 f(1/X) = X^5 - X^3 + X^2 - X - 1.$$

□

Solution to Exercise 72.
The group $(\mathbb{Z}/23\mathbb{Z})^\times$ is cyclic of order 22, the elements have order 1, 2, 11 or 22. Clearly 2 is not of order 1 nor 2. Compute 2^{11} modulo 23:

$$2^6 = 64 \equiv -5 \pmod{23}, \quad 2^9 \equiv -40 \pmod{23}, \quad 2^{10} \equiv 12 \pmod{23},$$

hence $2^{11} \equiv 1 \pmod{23}$ and 2 has order 11 modulo 23. It follows that Φ_{23}, which has degree $\varphi(23) = 22$, is the product of two polynomials of degree 11 over $\mathbb{F}_2$. □

Solution to Exercise 75.
(Compare with 64).
(a) The polynomial $\Phi_8(X) = X^4 + 1$ has no root in $\mathbb{Q}$ and is not the product of two degree 2 polynomials. Hence it is irreducible over $\mathbb{Q}$.

We have seen in Exercise 64 that over $\mathbb{F}_2$, $X^4+1=(X+1)^4$ splits into linear factors, while over $\mathbb{F}_p$ with p an odd prime, Φ_8 splits into 4 linear factors if $p\equiv 1 \mod 8$ and into 2 quadratic factors if $p\equiv 3,5,7 \mod 8$. Hence X^4+1 is always reducible over $\mathbb{F}_p$.

The same for $\Phi_{12}(X)=X^4-X^2+1$.

(b) If a polynomial of degree >1 were irreducible modulo p for each p, then its values at the integers would be only ± 1, which is not possible. □

Solution to Exercise 76.

Let p be a prime divisor of $n=x^4+y^4$. If p^4 does not divide n, then p does not divide xy, hence in $\mathbb{F}_p$ there is an element t such that $t^4=-1$. This t has order 8 in $\mathbb{F}_p^\times$, hence 8 divides $p-1$. □

Solution to Exercise 78.

The group $(\mathbb{Z}/15\mathbb{Z})^\times$ is a product $C_2\times C_4$ of a cyclic group of order 2 by a cyclic group of order 4, hence there are 4 elements of order 4 (namely the classes of 2, 7, 8, 13) and 3 elements of order 2 (namely the classes of 4, 11 and 14).

Since the group $(\mathbb{Z}/15\mathbb{Z})^\times$ is not cyclic, Φ_{15} is always reducible over $\mathbb{F}_q$.

If $\gcd(15,q)=1$, then Φ_{15} decomposes over $\mathbb{F}_q$ into a product of

- 8 factors of degree 1 if $q\equiv 1 \pmod{15}$,
- 4 factors of degree 2 if $q\equiv 4,\ 11,\ 14 \pmod{15}$,
- 2 factors of degree 4 if $q\equiv 2,\ 7,\ 8,\ 13 \pmod{15}$.

In characteristic 3, $\Phi_{15}(X)=\Phi_5(X)^2$. Recall Example 77. Since 3 has order 4 modulo 5, if $q=3^r$, then over $\mathbb{F}_q$, the polynomial Φ_5

- splits into 4 linear factors if $r\equiv 0 \pmod 4$ (hence Φ_{15} splits completely),
- splits into 2 factors of degree 2 if $r\equiv 2 \pmod 4$ (hence Φ_{15} splits into 4 quadratic factors),
- is irreducible if $r\equiv 1$ or $3 \pmod 4$ (hence Φ_{15} splits into 2 factors of degree 4).

In characteristic 5, $\Phi_{15}(X)=\Phi_3(X)^4$. Assume $q=5^r$. If r is odd, then over $\mathbb{F}_q$, the polynomial Φ_3 is irreducible and Φ_{15} splits into 4 quadratic factors, while if r is even, then over $\mathbb{F}_q$, the polynomial Φ_3 splits into two linear factors and Φ_{15} splits completely into 8 linear factors. □

Solution to Exercise 79.

(a) The kernel of the homomorphism of multiplicative groups $f:\mathbb{F}_{q^2}^\times\longrightarrow\mathbb{F}_{q^2}^\times$ which maps x to x^{q-1} is $\mathbb{F}_q^\times$, it has $q-1$ elements; the image of f is the set of roots of $X^{q+1}-1$, it has $q+1$ elements.

(b) Since the image of f has $q+1$ elements, there exists $\gamma\in\mathbb{F}_{q^2}$ in the image of f, say $\gamma:=\alpha^{q-1}$, which is not in $\mathbb{F}_q$. The two elements 1 and α^{q-1} are lineary independent over $\mathbb{F}_q$, which means (since $\alpha\neq 0$) that (α,α^q) are linearly independent over $\mathbb{F}_q$. □

Solution to Exercise 84.

Write $\mathbb{F}_4=\{0,1,j,j^2\}$ with $j^2+j+1=0$. There 16 elements in $\mathbb{F}_{16}$, two of degree 1 over $\mathbb{F}_2$ (the elements of $\mathbb{F}_2$), two of degree 2 (the elements of $\mathbb{F}_4\setminus\mathbb{F}_2$) and 12 of degree 4 (the elements of $\mathbb{F}_{16}\setminus\mathbb{F}_4$). In the cyclic group $\mathbb{F}_{16}^\times$ of order 15 there are $\varphi(15)=6$ elements of order 15, $\varphi(5)=4$ elements of order 5 (namely the roots of Φ_5), 2 elements of order 3, namely j and j^2.

The 12 elements of $\mathbb{F}_{16}$ of degree 4 over $\mathbb{F}_2$ have degree 2 over $\mathbb{F}_4$. Among them, there are 8 elements of order 15 and 4 elements of order 5 in the group $\mathbb{F}_{16}^\times$. The 4 elements of order 5 are the roots of Φ_5 which is irreducible over $\mathbb{F}_2$ and which splits into 2 quadratic factors over $\mathbb{F}_4$. The 6 irreducible quadratic

polynomials of $\mathbb{F}_4[X]$ come in pairs of conjugate polynomials over $\mathbb{F}_2$ (notice that Frob_2 permutes j and j^2):

$$\begin{aligned} &X^2+jX+1, \quad X^2+j^2+1\\ &X^2+X+j, \quad X^2+X+j^2,\\ &X^2+jX+j, \quad X^2+j^2X+j^2. \end{aligned}$$

Notice that

$$(A+jB)(A+j^2B) = A^2+AB+B^2,$$

hence

$$\begin{aligned} &(X^2+jX+1)(X^2+j^2+1) = X^4+X^3+X^2+X+1 = \Phi_5(X),\\ &(X^2+X+j)(X^2+X+j^2) = X^4+X+1,\\ &(X^2+jX+j)(X^2+j^2X+j^2) = X^4+X^3+1. \end{aligned}$$

These products are the three irreducible polynomials of degree 4 over $\mathbb{F}_2$.

Let α be a root of X^2+X+j. The other is α^4.

Taking the conjugate over $\mathbb{F}_2$, we deduce that the roots of X^2+X+j^2 are α^2 and α^6. The roots of $X^2+j^2X+j^2$ are α^{-1} and α^{-4}. Again, taking the conjugate over $\mathbb{F}_2$, we deduce that the roots of X^2+jX+j are α^{-2} and α^{-6}

The 4 elements of order 5 are α^3, α^{12} (they are conjugate) and α^6, α^9 (they are conjugate).

We have

$$\alpha^2 = \alpha+j, \quad \alpha^3 = \alpha+j+j\alpha, \quad \alpha^6 = j\alpha,$$

hence α^3 and α^{12} are the roots of X^2+j^2X+1, while α^6, α^9 are the roots of X^2+jX+1. □

Solution to Exercise 85.
(a) The divisors of 6 are 1, 2, 3 and 6, Hence $\mathbb{F}_{2^6}$ has four subfields, $\mathbb{F}_2$, $\mathbb{F}_{2^2} = \mathbb{F}_4$, $\mathbb{F}_{2^3} = \mathbb{F}_8$ and $\mathbb{F}_{64} = \mathbb{F}_{2^6}$.
(b) Since $63 = 3^2 \cdot 7$, the divisors of 63 are $1, 3, 7, 9, 21$ and 63, and the decomposition of $X^{64}-X$ into irreducible polynomials over $\mathbb{Z}$ is

$$X^{64}-X = X\Phi_1(X)\Phi_3(X)\Phi_7(X)\Phi_9(X)\Phi_{21}(X)\Phi_{63}(X).$$

The degrees are respectively $1, 1, 2, 6, 6, 12, 36$, the total of which is 64. Over $\mathbb{F}_2$, there is one irreducible polynomial of degree 2, there are two irreducible polynomials of degree 3 and nine of order 6 (cf Exercise 58).

The zeroes of $X^4-X = X\Phi_1(X)\Phi_3(X)$ are the elements of $\mathbb{F}_4$, the polynomial Φ_3 is irreducible of degree 2 over $\mathbb{F}_2$.

The zeroes of $X^8-X = X\Phi_1(X)\Phi_7(X)$ are the elements of $\mathbb{F}_8$, the polynomial Φ_7 splits over $\mathbb{F}_2$ into a product of two polynomials of degree 3:

$$X^6+X^5+X^4+X^3+X^2+X+1 = (X^3+X^2+1)(X^3+X+1).$$

There are 54 zeroes of $\Phi_9(X)\Phi_{21}(X)\Phi_{63}(X)$ in $\mathbb{F}_{64}$, each has degree 6 over $\mathbb{F}_2$, hence is a primitive element of $\mathbb{F}_{64}$ over $\mathbb{F}_2$. Therefore this polynomial splits into 9 irreducible polynomials over $\mathbb{F}_2$, each of degree 6.

The roots of Φ_9 are the 6 primitive roots of order 9, the roots of Φ_{21} are the 12 primitive roots of order 21, the roots of Φ_{63} are the 36 primitive roots of order 63, namely the generators of the cyclic group $\mathbb{F}_{63}^\times$.

Finally $X^{64} - X$ has
- two factors of degree 1, namely X and $X + 1$;
- one factors of degree 2, namely $X^2 + X + 1$ which is Φ_3;
- two factors of degree 3, namely $X^3 + X^2 + 1$ and $X^3 + X + 1$, which are the two factors of Φ_7;
- nine factors of degree 6, one of which is $\Phi_9(X) = X^6 + X^3 + 1$, two of which are the two factors of Φ_{21}, and the six others are the factors of Φ_{63}.

The nonempty minimal subsets of $\mathbb{Z}/63\mathbb{Z}$ which are stable under multiplication by 2 are

$$\begin{aligned}\{0\}\\ \{21, 42\}\\ \{9, 18, 36\}\\ \{27, 45, 54\}\end{aligned}$$

and 9 subsets having 6 elements each.

(c) Altogether in $\mathbb{F}_{64}$ there are 32 elements of trace 0 and 32 elements of trace 1. Since $[\mathbb{F}_{64} : \mathbb{F}_8] = 2$ is even, the 8 elements $\alpha \in \mathbb{F}_8$, have $\mathrm{Tr}_{\mathbb{F}_{64}/\mathbb{F}_2}(\alpha) = 0$. The two elements in $\mathbb{F}_4$ not in $\mathbb{F}_2$ have trace 1. Hence in $\mathbb{F}_{64} \setminus (\mathbb{F}_8 \cup F_4)$ there are $32 - 8 = 24$ elements of trace 0 and $32 - 2 = 30$ elements of trace 1.

The roots of $X^6 + X^3 + 1$ have trace 0. Among the 12 roots of Φ_{21}, six have trace 0 and six have trace 1. Two of the six factors of Φ_{63} have trace 0 and four have trace 1. □

Solution to Exercise 86.

Write $q = p^r$. If $q - 1$ is a prime number, then $q - 1$ is a Mersenne prime, the characteristic p is 2 and r is prime. Since $[\mathbb{F}_q : \mathbb{F}_2] = r$ is prime, any element in $\mathbb{F}_q \setminus \mathbb{F}_2$ is a generator of the extension $\mathbb{F}_q/\mathbb{F}_2$. Since $\mathbb{F}_q^\times$ is a cyclic group of prime order, any element in $\mathbb{F}_q \setminus \mathbb{F}_2$ is a generator of the cyclic group $\mathbb{F}_q^\times$.

Conversely, assume that any element α in $\mathbb{F}_q$ such that $\mathbb{F}_q = \mathbb{F}_p(\alpha)$ is a generator of the cyclic group $\mathbb{F}_q^\times$. Since $\varphi(p - 1) < p$, we have $r \geq 2$. The number of generators of the cyclic group $\mathbb{F}_q^\times$ is $\varphi(N)$ with $N = q - 1$. Using the notation and the results of Exercise 58, we deduce that the number of elements in $\mathbb{F}_q$ of degree r over $\mathbb{F}_p$ is $rN_p(r)$ and satisfies $rN_p(r) > N/2$. By assumption $rN_p(r) = \varphi(N)$, hence $\varphi(N) > N/2$. Therefore N is odd and consequently the characteristic p is 2.

If $N = 2^r - 1$ is not prime, then

$$\varphi(N) \leq N - \lfloor \sqrt{N} \rfloor.$$

Indeed, N has a prime factor $\leq \sqrt{N}$, hence there are at least $\lfloor \sqrt{N} \rfloor$ integers in $[1, N]$ which are not prime to N.

On the other hand, according to Exercise 58, the number of elements in $\mathbb{F}_{2^r}$ of degree r over $\mathbb{F}_2$ is $rN_2(r)$ and satisfies

$$rN_2(r) \geq 2^r - 2 \cdot 2^{r/2}.$$

Recall the assumption $rN_2(r) = \varphi(N)$. We do not yet deduce the desired contradiction, but we can improve one at least of these inequalities.

If r is odd, the solution of Exercise 58 provides a refinement of this last inequality, namely

$$rN_2(r) \geq 2^r - 2 \cdot 2^{r/3}.$$

If r is even, $r = 2k$, then $N = (2^k - 1)(2^k + 1)$ has at least one prime divisor $\leq \sqrt{2^k + 1}$ (notice that for $k \geq 3$ one at least of the two numbers $2^k - 1$, $2^k + 1$ is composite). In this case

$$\varphi(N) \leq N - \lfloor \sqrt[4]{N} + 1 \rfloor.$$

These estimates are sufficient to complete the proof. □

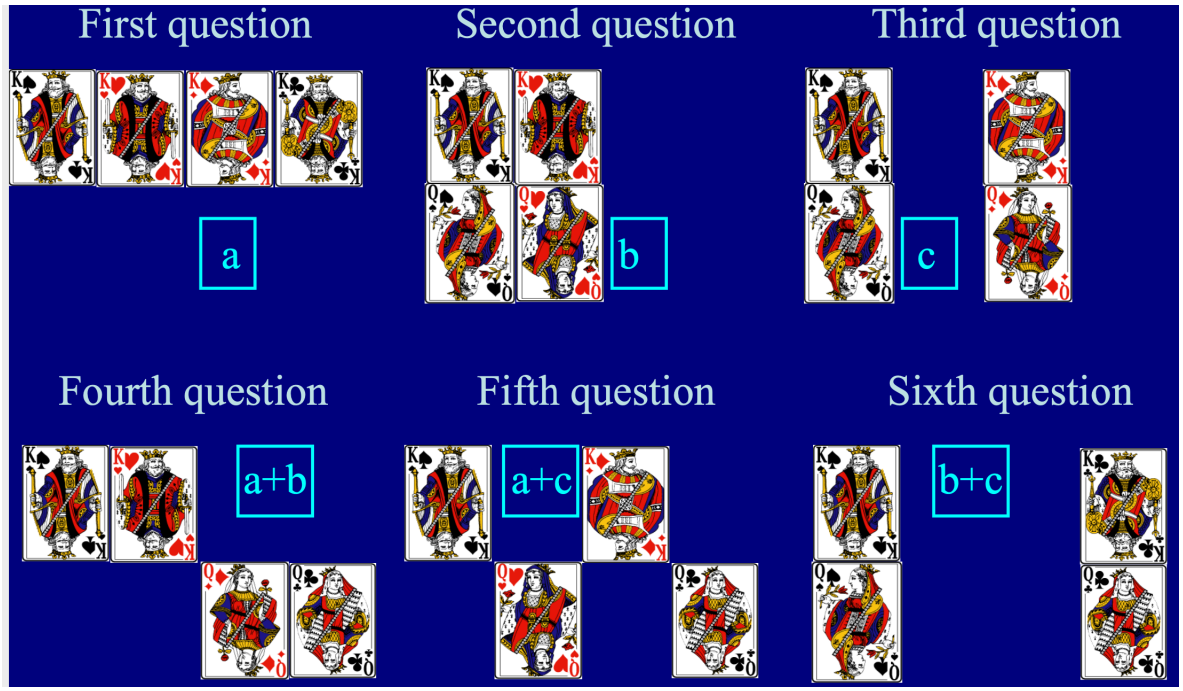
Solution to Exercise 94.

1. Given 2^n card, label them starting from 0 to $2^n - 1$; write the labels in binary form. Ask n questions, for the k–th one, display the cards having a label with 1 for the k–th binary digit. The sequence of yes and no gives you the binary expansion of the answer, with the digit 1 for yes and 0 for no.

2. In order to detect a wrong answer, ask one more question using the parity bit. The number of questions is $n + 1$.

3. In order to correct a wrong answer, use an error correcting code.
   • For $n = 1$ and 2 cards, ask 3 questions using the repetition code (display the same card 3 times). The corresponding error correcting code is the repetition $[3, 1]$ code (Example 89).
   • For $n = 2$ and 4 cards, ask 5 questions: repeat twice the two questions which give the solution when there is no wrong answer, and for the last one use the parity bit. The corresponding error correcting code is the $[5, 2]$ code of Example 91.
   • For $n = 3$ and 8 cards, ask 6 questions: questions 1,2,3 are the ones which give the solution when there is no wrong answer, the next 3 questions are the parity bits between questions (1 and 2), (2 and 3), (1 and 3). The corresponding error correcting code is the $[6, 3]$ code of Example 92.

   .



• For $n = 4$ and 16 cards, ask 7 questions only using Hamming $[7, 4]$ code (Example 93).

The optimality is proved by counting the number of Hamming balls of radius 1 and the number of points in each such ball. □

Solution to Exercise 95.

1. The idea is to use the repetition $[3, 1]$ code (Example 89).

   With three people, one solution is that the team bets that the three colours are not the same. When they see twice the same colour on the heads of the two other people, they bet that their own hat is not of that colour. If they see two different colours, they abstain.

   There are 8 possible distributions of the colours, two of them where the hats have all the same colours (white–white–white or black–black–black); in this case they all bet the wrong colour and the team looses. In the remaining 6 cases, the team wins. Hence the probability of winning is $3/4 = 75\%$.

   This is the best probability for this game, but there are other equivalent strategies: they select two distributions of colours which have no common element, like white–black–white and black–white–black, and they bet that these two distributions do not correspond to the correct answer.

2. With seven people, use the Hamming $[7,4]$ code in place of the repetition $[3,1]$ code. Replace the two colours by 0 and 1, so that the distribution of colours corresponds to an element in $\mathbb{F}_2^7$. The team bets that the distribution of colours is not an element of the Hamming code. When one member of the team sees the 6 other colours, he or she looks at the two possible elements in $\mathbb{F}_2^7$ which correspond to the distribution of hats. If one of them lies in the Hamming code, he or she writes the colour corresponding to the other element. Otherwise, the two possible answers correspond to elements which lie in two different Hamming balls of radius 1, this person does not know which is the center of the Hamming ball containing the right solution and in this case he or she abstains. The team looses in 16 cases, there are $2^7 = 128$ possible distributions, so he wins in $2^7 - 2^4 = 128 - 16 = 112$ cases, the probability of winning is $7/8 = 87.5\%$, and this is optimal.

The optimality is proved by counting the number of Hamming balls of radius 1 and the number of points in each such ball. □

Solution to Exercise 98.
(a) For $n = 4$ and q odd, the polynomial Q_I associated with the subset $I = \{0, 1, 3\}$ of $\mathbb{Z}/4\mathbb{Z}$ is $(X - 1)(X^2 + 1) = X^3 - X^2 + X - 1$, the dimension of the codeis 1. This code is the line $\mathbb{F}_q(1, -1, 1, -1)$.
(b) For r a divisor of n, say $n = mr$,and $I = C_r$ the additive subgroup of $\mathbb{Z}/n\mathbb{Z}$ of order r, we have $Q_I(X) = X^r - 1$. Since the roots of Q_I are ζ^{km} for $k = 0, 1, \ldots, r-1$, the associated code $\mathcal{C} \subset \mathbb{F}_q^n$ is the set of $(a_0, a_1, \ldots, a_{n-1})$ such that

$$a_0 + a_1\zeta^{km} + a_2\zeta^{2km} + \cdots + a_{n-1}\zeta^{(n-1)km} = 0 \quad \text{for} \quad k = 0, 1, \ldots, r-1.$$

Since $\zeta^n = 1$, these equations can be written

$$\sum_{j=0}^{r-1} \left(\sum_{i=0}^{m-1} a_{j+ir} \right) \zeta^{jkm} = 0 \quad \text{for} \quad k = 0, 1, \ldots, r-1.$$

Since the determinant $\left(\zeta^{jkm}\right)_{0 \le j,k \le r-1}$ does not vanish, these equations are equivalent to

$$\sum_{i=0}^{m-1} a_{j+ir} = 0 \quad \text{for} \quad j = 0, 1, \ldots, r-1.$$

(c) Let $m = n/\ell$. The set E_ℓ of elements of order ℓ in the additive group $\mathbb{Z}/n\mathbb{Z}$ has $\varphi(\ell) = \ell - 1$ elements. The associated code has dimension $n - \ell + 1$, it is the intersection of the $\ell - 1$ hyperplanes

$$\sum_{i=0}^{m-1} a_{i\ell} = \sum_{i=0}^{m-1} a_{1+i\ell} = \cdots = \sum_{i=0}^{m-1} a_{\ell-1+i\ell}$$

in $\mathbb{F}_q^n$. □

Solution to Exercise 105.
(a) Let $A_1, A_2, \dots, A_t$ be t mutually orthogonal latin squares of order n. Without loss of generality we may assume that the symbols are $1, 2, \dots, n$ and that the first row of each A_i is $1, 2, \dots, n$. Let x_i the first element in the second row of A_i. Since 1 is already in the first column and A_i is orthogonal, no x_i can be 1. Since A_i and A_j are mutually orthogonal and have the same first row, we also have $x_i \neq x_j$ for $i \neq j$. Hence $t \leq n-1$.
(b) For $s = 1, 2, \dots, q-1$ and $0 \leq i, j_1, j_2 \leq q-1$, the conditions

$$x_i x_s + x_{j_1} = x_i x_s + x_{j_2}$$

imply $x_{j_1} = x_{j_2}$, hence $j_1 = j_2$.

For $s = 1, 2, \dots, q-1$ and $0 \leq i_1, i_2, j \leq q-1$, since $x_s \neq 0$, the conditions

$$x_{i_1} x_s + x_j = x_{i_2} x_s + x_j$$

imply $x_{i_1} = x_{i_2}$, hence $i_1 = i_2$. Hence A_s is a latin square.

For $1 \leq s_1, s_2 \leq q-1$ and $0 \leq i_1, i_2, j_1, j_2 \leq q-1$ with $(i_1, j_1) \neq (i_2, j_2)$, the conditions

$$x_{i_1} x_{s_1} + x_{j_1} = x_{i_2} x_{s_1} + x_{j_2} \quad \text{and} \quad x_{i_1} x_{s_2} + x_{j_1} = x_{i_2} x_{s_2} + x_{j_2}$$

imply $s_1 = s_2$.
(c) Taking $q = 3$ and replacing the symbols $\{x_0, x_1, x_2\}$ respectively with $\{1, 2, 3\}$, one deduces the following couple of mutually orthogonal latin squares of order 3:

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{pmatrix}, \quad \text{so that} \quad (A, B) = \begin{pmatrix} (1,1) & (2,2) & (3,3) \\ (2,3) & (3,1) & (1,2) \\ (3,2) & (1,3) & (2,1) \end{pmatrix}.$$

Taking $q = 4$ and replacing the symbols $\{x_0, x_1, x_2, x_3\}$ respectively with $\{1, 2, 3, 4\}$, one deduces the following 3 mutually orthogonal latin squares of order 4:

$$(A, B, C) = \begin{pmatrix} (1,1,1) & (2,2,2) & (3,3,3) & (4,4,4) \\ (2,3,4) & (1,4,3) & (4,1,2) & (3,2,1) \\ (3,4,3) & (4,3,4) & (1,2,1) & (2,1,2) \\ (4,2,2) & (3,1,1) & (2,4,4) & (1,3,3) \end{pmatrix}.$$

□

Solution to Exercise 106.
(a) The divisors of 12 are $1, 2, 3, 4, 6$ and 12, hence,

$$X^{12} - 1 = \Phi_1(X)\Phi_2(X)\Phi_3(X)\Phi_4(X)\Phi_6(X)\Phi_{12}(X)$$

with

$$\Phi_1(X) = X - 1, \quad \Phi_2(X) = X + 1, \quad \Phi_3(X) = X^2 + X + 1,$$
$$\Phi_4(X) = \Phi_2(X^2) = X^2 + 1, \quad \Phi_6(X) = \Phi_3(-X) = X^2 - X + 1,$$

and

$$\Phi_{12} = \Phi_6(X^2) = X^4 - X^2 + 1.$$

(b) According to Theorem 59, the polynomial $\Phi_n(X)$ splits in the finite field with q elements into a product of irreducible polynomials, all of the same degree d, where d is the order of q modulo n. We have

$$5 \equiv 1 \bmod 1, \quad 5 \equiv 1 \bmod 2, \quad 5 \equiv 1 \bmod 4,$$

$$5 \not\equiv 1 \bmod 3, \quad 5 \not\equiv 1 \bmod 6, \quad 5 \not\equiv 1 \bmod 12,$$

$$5^2 \equiv 1 \bmod 3, \quad 5^2 \equiv 1 \bmod 6, \quad 5^2 \equiv 1 \bmod 12,$$

which means that 5 has order 1 modulo 1, 2 and 4, order 2 modulo 3, 6 and 12. Therefore, in $\mathbb{F}_5[X]$, the polynomial $\Phi_4(X)$ is product of two linear polynomials:

$$X^2 + 1 = (X + 2)(X + 3) \quad \text{in } \mathbb{F}_5[X],$$

$\Phi_3(X)$, $\Phi_6(X)$ are irreducible and $\Phi_{12}(X)$ is product of two irreducible quadratic factors:

$$X^4 - X^2 + 1 = (X^2 + 2X - 1)(X^2 + 3X - 1).$$

Hence, in $\mathbb{F}_5[X]$, the polynomial $X^{12} - 1$ is a product of six linear polynomials and three irreducible quadratic polynomials.
(c) Let K be the splitting field over $\mathbb{F}_5$ of $X^{12} - 1$. The root of any of the three irreducible quadratic factors in $\mathbb{F}_5$ of $X^{12} - 1$ generates over $\mathbb{F}_5$ the unique quadratic extension of $\mathbb{F}_5$ contained in K. Hence, $[K : \mathbb{F}_5] = 2$ and K has 25 elements.

(d) Over $\mathbb{F}_2$, the polynomial $X^2 + X + 1$ is irreducible and

$$X^{12} - 1 = (X^3 - 1)^4 = (X - 1)^4(X^2 + X + 1)^4$$

is the product of four linear polynomials and four irreducible quadratic polynomials.

Over $\mathbb{F}_3$, the polynomial $X^2 + 1$ is irreducible and

$$X^{12} - 1 = (X^4 - 1)^3 = (X - 1)^3(X + 1)^3(X^2 + 1)^3$$

is the product of six linear polynomials and three irreducible quadratic polynomials.

Assume now $p \geq 5$. Since p does not divide 12, the polynomial $X^{12} - 1$ has no multiple factor. There are always two degree 1 factors, namely $\Phi_1(X) = X - 1$ and $\Phi_2(X) = X + 1$. For each of the other factors $\Phi_d(X)$ with d a divisor of 12 and $d > 2$ (hence, $d = 3$, 4, 6 or 12), if m is the order of p modulo d, then Φ_d splits over $\mathbb{F}_p$ into a product of polynomials, all of degree m. Since $\varphi(3) = \varphi(4) = \varphi(6) = 2$ and $\varphi(12) = 4$, for $d = 3, 4$ or 6 the polynomial Φ_d modulo p is either irreducible of degree 2 or product of two linear factors, while $\varphi(12)$ is either product of two irreducible quadratic factors or product of four linear factors[3].

Here is the result: the first row gives the 4 possible classes of p modulo 12, the next rows deduces the classes of p modulo 3, 4, 6 and the order of p modulo the divisors of 12, hence the degrees of the

[3] As a matter of fact, Φ_{12} is irreducible over $\mathbb{Q}$ but reducible over $\mathbb{F}_p$ for all primes p - see Exercise 64

irreducible factors.

p modulo 12	1	5	-5	-1
p modulo 3	1	-1	1	-1
p modulo 4	1	1	-1	-1
p modulo 6	1	-1	1	-1
order of p modulo 12	1	2	2	2
order of p modulo 3	1	2	1	2
order of p modulo 4	1	1	2	2
order of p modulo 6	1	2	1	2

Since Φ_{12} has degree 4 and Φ_3, Φ_4, Φ_6 degree 2, it follows that $X^{12}-1$ is product of

- twelve linear factors (it splits completely over $\mathbb{F}_p$) if $p \equiv 1 \bmod 12$,
- four linear factors and four irreducible quadratic factors if $p \equiv 5 \bmod 12$,
- six linear factors and three irreducible quadratic factors if $p \equiv 7 \bmod 12$,
- two linear factors and five irreducible quadratic factors if $p \equiv 11 \bmod 12$. □

Solution to Exercise 107.
(a) The order of 2 and of 3 modulo 5 is $4 = \varphi(5)$, hence the cyclotomic polynomial

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

is irreducible over $\mathbb{F}_2$ and over $\mathbb{F}_3$. (See Example 77).

The order of 2 modulo 7 is 3, hence Φ_7 splits into a product of two irreducible polynomials of degree 3 over $\mathbb{F}_2$.

The order of 3 modulo 7 is $6 = \varphi(7)$, hence Φ_7 is irreducible over $\mathbb{F}_3$.

The order of 2 modulo 11 is $10 = \varphi(11)$, hence Φ_{11} is irreducible over $\mathbb{F}_2$.

The order of 3 modulo 11 is 5, hence Φ_{11} splits into a product of two irreducible polynomials of degree 5 over $\mathbb{F}_2$.

(b) The order of 2 modulo 15 is 4, the degree of Φ_{15} is $\varphi(15) = 8$, hence Φ_{15} splits into a product of two irreducible polynomials of degree 4 over $\mathbb{F}_2$:

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

(See Example 82).
(c) The polynomial $X^4 + X + 1$ is irreducible over $\mathbb{F}_2$, over $\mathbb{F}_4 = \{0, 1, j, j^2\}$ with $1 + j + j^2 = 0$ it splits into two irreducible quadratic factors

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

(See Exercise 84). Since $[\mathbb{F}_8 : \mathbb{F}_2] = 3$ and $\gcd(2, 3) = 1$, it follows that $X^4 + X + 1$ is irreducible over $\mathbb{F}_8$.
(d) The polynomials $\Phi_1(X) = X - 1$ and $\Phi_2(X) = X + 1$ are irreducible over any field. The polynomial $\Phi_4(X) = X^2 + 1$ splits into $(X + 1)^2$ in characteristic 2.

Let Φ_n be a cyclotomic polynomial which is irreducible over $\mathbb{F}_q$ where $q \in \{1,\ 2,\ 4,\ 8,\ 16\}$. Then the class of q modulo n is a generator of $(\mathbb{Z}/n\mathbb{Z})^\times$, in particular this group is cyclic, hence (exercise 7) $n \in \{2, 4, p^s, p^{2s}\}$ where p is an odd prime and $s \geq 1$. Since $\Phi_{2p^s}(X) = \Phi_{p^s}(-X)$ (see Exercise 46), it only remains to use the fact that for $n = p^s$ with p odd prime and $s \geq 1$,

- Φ_n is irreducible over $\mathbb{F}_2$ if and only if 2 is a generator of the cyclic group $(\mathbb{Z}/n\mathbb{Z})^\times$,
- Φ_n is irreducible over $\mathbb{F}_4$ if and only if 4 is a generator of the cyclic group $(\mathbb{Z}/n\mathbb{Z})^\times$,
- Φ_n is irreducible over $\mathbb{F}_8$ if and only if 8 is a generator of the cyclic group $(\mathbb{Z}/n\mathbb{Z})^\times$,
- Φ_n is irreducible over $\mathbb{F}_{16}$ if and only if 16 is a generator of the cyclic group $(\mathbb{Z}/n\mathbb{Z})^\times$.

The polynomial $\Phi_3(X) = 1 + X + X^2$ is irreducible over $\mathbb{F}_2$ and $\mathbb{F}_8$, it splits into linear factors over $\mathbb{F}_4$ hence also over $\mathbb{F}_{16}$.

The polynomial Φ_5 is irreducible over $\mathbb{F}_2$ hence over $\mathbb{F}_8$ (it has degree 4 prime to $[\mathbb{F}_8 : \mathbb{F}_2] = 3$), it is reducible over $\mathbb{F}_4$ (since 4 has order 2 modulo 5), hence also over $\mathbb{F}_{16}$.

The polynomial Φ_7 is reducible over $\mathbb{F}_2$ (since 2 has order 3 modulo 7), hence also over $\mathbb{F}_4$, $\mathbb{F}_8$ and $\mathbb{F}_{16}$.

The polynomial Φ_{11} is irreducible over $\mathbb{F}_2 \ldots$

$n = p^s$, $\varphi(n) = p^{s-1}(p-1)$, $(\mathbb{Z}/p^s\mathbb{Z})^\times$ is a product of a cyclic group of order p^{s-1} and a cyclic group of order $p-1$. If Φ_n is irreducible over $\mathbb{F}_2$, then the class of 2 modulo p has order $p-1$, hence $2^{(p-1)/2} \equiv -1 \pmod p$ which means that the Legendre symbol $\left(\frac{2}{p}\right)$ is -1, which means $p \equiv 3$ or $5 \pmod 8$.

It follows that for $p \equiv 1$ or $-1 \pmod 8$, Φ_p is reducible in characteristic 2.

Let ζ be a primitive p-th root of unity in characteristic 2.

If $p \equiv 5 \pmod 8$, then $p \equiv 1 \pmod 4$, Φ_p is reducible over $\mathbb{F}_4$.

If $p \equiv 3 \pmod 8$, then Φ_p is irreducible over $\mathbb{F}_4$.

Over $\mathbb{F}_8$, the condition is 3 divides $(p-1)/2$, hence $p \equiv 1 \pmod 6$.

Over $\mathbb{F}_{16}$, the condition is 4 divides $(p-1)/2$, hence $p \equiv 1 \pmod 8$. Hence Φ_n is always reducible over $\mathbb{F}_{16}$. □

Solution to Exercise 108.
Denote by $\mathcal{N}_q(n)$ the number of squarefree monic polynomials in $\mathbb{F}_q[X]$ of degree n. Clearly $\mathcal{N}_q(0) = 1$ and $\mathcal{N}_q(1) = q$.

Any monic polynomial in $\mathbb{F}_q[X]$ of degree n can be written in a unique way A^2B, where A is a monic polynomial of degree, say, d, with $0 \le d \le n/2$ and B is a monic squarefree polynomial of degree $n - 2d$. This yields a partition of the set of monic polynomials of degree n, which implies

$$\begin{aligned} q^n &= \sum_{0 \le d \le n/2} q^d \mathcal{N}_q(n-2d) \\ &= \mathcal{N}_q(n) + q\mathcal{N}_q(n-2) + q^2\mathcal{N}_q(n-4) + \cdots + \begin{cases} q^{n/2}\mathcal{N}_q(0) & \text{if } n \text{ is even,} \\ q^{(n-1)/2}\mathcal{N}_q(1) & \text{if } n \text{ is odd.} \end{cases} \end{aligned}$$

The formula $\mathcal{N}_q(n) = q^n - q^{n-1}$ for $n \ge 2$ follows by induction on n (telescoping sum). □

Solution to Exercise 109.
Since $728 = 3^6 - 1$, the order of 3 modulo 728 is 6. We also check

$$728 = 2^3 \cdot 7 \cdot 13 \quad \text{and therefore} \quad \varphi(728) = 2^5 \cdot 3^2 = 48 \cdot 6.$$

Hence, over the field $\mathbb{F}_3$, the cyclotomic polynomial Φ_{728} splits into a product of 48 irreducible factors, each of which has degree 6. □

Solution to Exercise 110.
The polynomial X^3+X+1 is irreducible over $\mathbb{F}_5$. Let α be a root of this polynomial in $\mathbb{F}_{5^3}$. One checks

$$\alpha^5 = -\alpha^2+\alpha+1, \quad \alpha^{15} = \alpha^2-\alpha-2, \quad \alpha^{30} = \alpha^2+1,$$

$$\alpha^{31} = -1, \quad (2\alpha)^{31} = -2, \quad (2\alpha)^{62} = -1.$$

It follows that 2α has order $124 = 5^3-1$, hence is a generator of the cyclic group $\mathbb{F}_{5^3}^\times$. □

Solution to Exercise 111.
(a) If $\zeta \in K$ satisfies $\zeta^{q-1} = -1$, then $\zeta^q = -\zeta$ and $(\zeta^2)^q = (\zeta^q)^2 = \zeta^2$, hence $\zeta^2 \in \mathbb{F}_q^\times$.
(b) Assume first $p = 2$. Then

$$X^{2q-1} - X = X(X^{q-1}-1)^2$$

splits into $2q-1$ linear factors (degree 1) in $\mathbb{F}_q$.

Next assume q is odd. According to (a), the polynomial $X^{q-1}+1$ has no root in $\mathbb{F}_q$, but it splits into linear factors in $\mathbb{F}_{q^2}$. Hence we have

$$X^{2q-1} - X = X(X^{q-1}-1)(X^{q-1}+1),$$

where $X(X^{q-1}-1)$ is a product of q linear factors in $\mathbb{F}_q$, while $X^{q-1}+1$ is a product of $(q-1)/2$ quadratic factors in $\mathbb{F}_q$. □

Solution to Exercise 112. Let p be the characteristic of F and $q = p^r$ the number of elements of F. Denote by σ_n the map $x \mapsto x^n$ from F to F.

If $n \equiv p^\ell \pmod{(q-1)}$ for some ℓ with $0 \leq \ell \leq r-1$, then for $x \in F^\times$ we have $\sigma_n(x) = \mathrm{Frob}_p^\ell(x)$, hence $\sigma_n = \mathrm{Frob}_p^\ell$, which is an automorphism of F.

Conversely, assume σ_n is an automorphism of F. Hence σ is an element of the Galois group of F over $\mathbb{F}_p$, which means that there exist ℓ with $0 \leq \ell \leq r-1$ such that $\sigma = \mathrm{Frob}_p^\ell$. Let m be the class of n modulo $(q-1)$: hence $0 \leq m \leq q-2$ and $m-n$ is a multiple of $q-1$. Therefore $\sigma_n = \sigma_m$, where σ_m is the map $x \mapsto x^m$ from F to F. From $x^{p^\ell} = x^m$ for all $x \in F$ we deduce that the polynomial $X^q - X$ divides $X^{p^\ell} - X^m$. However $p^\ell < q$ and $m < q$, hence $m = p^\ell$.

Therefore the set of n such that σ_n is an automorphism of F is the set of integers congruent to a power of p modulo $q-1$. □

Solution to Exercise 113.
(a) Since q divides 2^p-1, it follows that q is odd and that the order of the class of 2 in $(\mathbb{Z}/q\mathbb{Z})^\times$ is p, hence p divides $q-1$.
(b) Since q divides $2^{2^n}+1$, it follows that q is odd and that the order of the class of 2 in $(\mathbb{Z}/q\mathbb{Z})^\times$ is 2^{n+1}, hence 2^{n+1} divides $q-1$.
(See also exercise 42). □

Solution to Exercise 114.
Since $a^p \equiv a \bmod p$, if $f(X) = (X^p - X)g(X) + ph(X)$, then, for all $a \in \mathbb{Z}$, the number p divides $f(a)$.

Conversely, assume that for any $a \in \mathbb{Z}$, the number p divides $f(a)$. Divide the polynomial f by $X^p - X$ in $\mathbb{Z}[X]$:

$$f(X) = (X^p - X)g(X) + r(X),$$

with g and r in $\mathbb{Z}[X]$, and r either zero, or else of degree $< p$. Then $r(a) \equiv 0 \bmod p$ for all $a \in \mathbb{Z}$, hence, the image of r in $\mathbb{F}_p[X]$ is zero. This means that there exists $h \in \mathbb{Z}[X]$ such that $r = ph$.

One can also argue as follows: when K is a field of characteristic p, we have

$$X^p - X = \prod_{\alpha \in \mathbb{F}_p} (X - \alpha),$$

hence, for $F \in K[X]$, the condition
(i)' For all $a \in \mathbb{F}_p$, $F(a) = 0$
is equivalent to
(ii)' There exists a polynomial $G \in \mathbb{F}_p[X]$ such that $F(X) = (X^p - X)G(X)$.
The statement of the exercise is a reformulation of this equivalence (take $K = \mathbb{F}_p$, and F, G are the reductions modulo p of f and g). □

Solution to Exercise 115.

We show that the kernel of f has p elements, which are the classes modulo p^2 of the integers $\equiv 1 \pmod{p^2}$, while the image of f has $p - 1$ elements, which are the roots of $X^{p-1} - 1$ in $(\mathbb{Z}/p^2\mathbb{Z})^\times$.

For $p = 2$, we have $(\mathbb{Z}/4\mathbb{Z})^\times = \{1, -1\}$, the kernel of the homomorphism $f : x \mapsto x^2$ of this group is $(\mathbb{Z}/4\mathbb{Z})^\times$ and has two elements, the image of f is $\{1\}$, which is the set of roots of $X - 1$ and has one elements,

Assume now that p is odd. Since $p^2\mathbb{Z} \subset p\mathbb{Z}$, the canonical surjective homomorphism $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ factors as $\mathbb{Z} \to \mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$:

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z}/p\mathbb{Z} \\ \downarrow & \nearrow \varphi & \\ \mathbb{Z}/p^2\mathbb{Z} & & \end{array}$$

Let $\phi : (\mathbb{Z}/p^2\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$ be the restriction of φ to $(\mathbb{Z}/p^2\mathbb{Z})^\times$. Since $(1 + pt)^p \equiv 1 \pmod{p^2}$, any $x \in \ker \phi$ satisfies $x^p = 1$ and there are p such elements, namely the classes modulo p^2 of

$$1, 1 + p, \ldots, 1 + (p - 1)p.$$

It follows that $\ker f$ has p elements; therefore, since $(\mathbb{Z}/p^2\mathbb{Z})^\times$ has $p(p - 1)$ elements, $\mathrm{Im} f$ has $p - 1$ elements. Further, any element $y = x^p$ in the image of f satisfies $y^{p-1} = 1$, hence $\mathrm{Im} f$ is the set of roots of $X^{p-1} - 1$. □

Solution to Exercise 116.
(a) Let $f \in \mathbb{F}_q[X]$ be the minimal polynomial of A over $\mathbb{F}_q$. The degree of f is at most n. The subring $\mathbb{F}_q[A]$ of $\mathrm{Mat}_{n\times n}(\mathbb{F}_q)$ generated by A is $\mathbb{F}_q[X]/(f)$. Let G be the subgroup of $\mathbb{F}_q[A]^\times$ generated by the class of A modulo f. The order of G divides the order of $\mathbb{F}_q[A]^\times$, and the order of $\mathbb{F}_q[A]^\times$ is at most $q^n - 1$.

Take for instance $n = q = 2$. Over $\mathbb{F}_2$, the 2×2 matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ has order 2 which does not divide $2^n - 1 = 3$.

(b) If A has order $q^n - 1$, then (with the above notations) the group $G = \mathbb{F}_q[A]^\times$ has $q^n - 1$ elements, hence $\mathbb{F}_q[A]$ is a field with q^n elements and A is a generator of G. Hence $(i) \Rightarrow (ii)$.

If $\mathbb{F}_q[A]$ is a field with q^n elements and A is a primitive element in this field, then the characteristic polynomial of A is a primitive polynomial. Hence $(ii) \Rightarrow (iii)$.

If the characteristic polynomial of A is a primitive polynomial, since it has degree n, it is the minimal polynomial f of A; the class of X in $\mathbb{F}_q[X]/(f)$ is a generator of the cyclic group $\mathbb{F}_q[A]^\times$, hence $\mathbb{F}_q[A]$ is a field with q^n elements and A has order $q^n - 1$. Hence $(iii) \Rightarrow (i)$. □

Solution to Exercise 117.

Notice first that if there is a domain A such that $A^\times$ has order m, then the same is true for other domains like $A[X]$ - hence there is not unicity.

Also, if $A^\times$ is a finite group, then it is cyclic (being a finite subgroup of the multiplicative group of the quotient field of A).

The answer is yes for $m = p^r - 1$, hence for $m = 1, 2, 3, 4, 6, 7, 8, 10$, by taking for A the field with p^m elements. Let us show that the answer is no for $m = 5, 9$ and 11.

Assume $A^\times$ has order m with $m \in \{5, 9, 11\}$. Since m is odd, if follows that -1, which is a unit, cannot have order 2; therefore $-1 = 1$, which means that A has characteristic 2.

The ring A contains the m–th roots of unity, hence contains $\mathbb{F}_2(\zeta)$ where ζ is a primitive m–th root of unity. The degree d of ζ is the order of 2 modulo m, hence $d = 4$ for $m = 5$, $d = 6$ for $m = 9$ and $d = 10$ for $m = 11$. Now $A^\times$ contains $\mathbb{F}_2(\zeta)^\times$ which is a group having $2^d > m$ elements. This is a contradiction. □

Solution to Exercise 118.

(a) Two conjugate elements α and $\sigma(\alpha)$ have the same order, since $\alpha^m = 1$ if and only if $\sigma(\alpha)^m = 1$.

(b) Let α be a root of f. Since α has order $p(f)$ in the multiplicative group $\mathbb{F}_q(\alpha)^\times$ we have

$$p(f)|\ell \Longleftrightarrow \alpha^\ell = 1 \Longleftrightarrow f(X)|X^\ell - 1.$$

(c) The n conjugates of a root α of f over $\mathbb{F}_q$ are its images under the iterated Frobenius $x \mapsto x^q$, which is the generator of the cyclic Galois group of $\mathbb{F}_q(\alpha)/\mathbb{F}_q$. From $\alpha^{q^n} = \alpha$, we deduce that f divides the polynomial $X^{q^n} - X$ (see also Theorem 55). Since $f(X) \neq X$ we deduce $\alpha \neq 0$, hence, f divides the polynomial $X^{q^n - 1} - 1$. As we have seen in question (b), it implies that $p(f)$ divides $q^n - 1$. The fact that the characteristic p does not divide $p(f)$ is then obvious.

(d) An irreducible monic polynomial $f \in \mathbb{F}_q[X]$ is primitive if and only if any root α of f in $\overline{\mathbb{F}}_p$ is a generator of the cyclic group $\mathbb{F}_q(\alpha)^\times$.

(e) Here is the answer:

q	d	$f(X)$	$p(f)$	primitive
2	2	X^2+X+1	3	yes
2	3	X^3+X+1	7	yes
2	3	X^3+X^2+1	7	yes
2	4	X^4+X^3+1	15	yes
2	4	X^4+X+1	15	yes
2	4	$X^4+X^3+X^2+X+1$	5	no
3	2	X^2+1	4	no
3	2	X^2+X-1	8	yes
3	2	X^2-X-1	8	yes

(f) The two irreducible polynomials of period 15 over $\mathbb{F}_2$ are the two factors X^4+X^3+1 and X^4+X+1 of Φ_{15}. The only irreducible polynomial of period 5 over $\mathbb{F}_2$ is $\Phi_5(X) = X^4+X^3+X^2+X+1$. □

Solution to Exercise 119.
If $\ell = 2$ and p is odd, the assumption that a is not a square in $\mathbb{F}_p$ implies that $X^2 - a$ is irreducible over $\mathbb{F}_p$.

If ℓ is odd and $p = 2$, then for any $a \in \mathbb{F}_2$ the polynomial $X^\ell - a$ is reducible over $\mathbb{F}_2$.

If $p = \ell$, since the Frobenius $x \mapsto x^p$ is an automorphism of $\mathbb{F}_p$, any element in $\mathbb{F}_p$ is a p-th power and again the result is trivial.

Assume now that ℓ and p are distinct odd primes. Let ζ be an element of order $p-1$ in the multiplicative group $\mathbb{F}_p^\times$. If ℓ does not divide $p-1$, then ζ is a ℓ-th power (if m is the inverse of ℓ in the group $(\mathbb{Z}/(p-1)\mathbb{Z})^\times$, then $\zeta = \gamma^\ell$ with $\gamma = \zeta^m$); in this case any element in $\mathbb{F}_p$ is a ℓ-th power. Therefore we need to consider only the prime numbers ℓ which divide $p-1$. In this case the ℓ–th roots of unity are in $\mathbb{F}_p$. Let $\zeta \in \mathbb{F}_p$ be a primitive ℓ-th root of unity. Let γ be a root of the polynomial $X^\ell - a$ in an extension of $\mathbb{F}_p$ and let $E = \mathbb{F}_p(\gamma)$. Since a is not an ℓ–th power in $\mathbb{F}_p$, we have $E \neq \mathbb{F}_p$. Also,

$$X^\ell - a = \prod_{j=0}^{\ell-1} (X - \zeta^j \gamma).$$

For $0 \leq j \leq \ell - 1$, we have $\mathbb{F}_p(\gamma) = \mathbb{F}_p(\gamma\zeta^j)$, hence all $\gamma\zeta^j$ have the same degree $d \geq 2$ over $\mathbb{F}_p$, hence this degree divides ℓ. Given that ℓ is prime, we deduce $d = \ell$. □

Solution to Exercise 120.
The division of $(X+1)^k$ by $f(X) = X^3+X+1$ in $\mathbb{F}_2[X]$ is given by

$$\begin{aligned}
X+1 &= 0f + X + 1\\
(X+1)^2 &= 0f + X^2 + 1\\
(X+1)^3 &= f + X\\
(X+1)^4 &= Xf + X^2 + X + 1\\
(X+1)^5 &= (X^2+1)f + X^2 + X\\
(X+1)^6 &= (X^3+X+1)f + X^2\\
(X+1)^7 &= (X^4+X^2+X+1)f,
\end{aligned}$$

hence the least integer k such that $(X+1)^k$ is multiple of f is $k=7$.

Let $f \in \mathbb{F}_p[X]$ of degree n with $f(0) \neq 0$. For $1 \leq \ell \leq p^n$, write

$$X^\ell - 1 = f(X)Q_\ell(X) + R_\ell$$

with R_ℓ of degree $< n$. There are p^n polynomials of degree $< n$ over $\mathbb{F}_p$. If the R_ℓ are all distinct, one of them is 0; then f divides the corresponding $X^\ell - 1$. If two of the R_ℓ are the same, say $R_\ell = R_k$ with $1 \leq \ell < k \leq p^n$, then $X^k - X^\ell = (X^{k-\ell} - 1)X^\ell$ divides f; since X does not divide f, we deduce that $X^{k-\ell} - 1$ divides f while we have $1 \leq k - \ell \leq p^n - 1$.

The only case where this proof does not yield an exponent $< p^n$ is when the only ℓ where R_ℓ is 0 is p^n (and all the other R_ℓ are pairwise distinct). But in this case $X^{p^n} - 1 = (X-1)^{p^n}$ divides f, hence $f(X) = (X-1)^n$, but since $n \leq p^{n-1}$ it follows that $X^{p^{n-1}} - 1$ divides f. (So this case never happens). □

Solution to Exercise 121.
(a) Let x be a root of $X^{p-1} - u$ in an extension of $\mathbb{F}_p$. Then

$$x^{p^r} = u^r x$$

for all $r \geq 0$. Since u has order m in $\mathbb{F}_p^\times$, the least r such that $x^{p^r} = x$ is $r = m$. Since $k = (p-1)/m$, the orbit of x under the iterated of Frob_p has m elements, hence (Theorem 36) x has degree m over $\mathbb{F}_p$. Since all roots of $X^{p-1} - u$ have the same degree m over $\mathbb{F}_p$, in the decomposition of the polynomial $X^{p-1} - u$ into irreducible polynomials over $\mathbb{F}_p$, all factors have degree m.
(b) The multiplicative group H generated by u is the unique subgroup of $\mathbb{F}_p^\times$ of order m. The morphism

$$\begin{array}{ccc} \mathbb{F}_p^\times & \to & H \\ x & \mapsto & x^{(p-1)/m} \end{array}$$

is surjective, its kernel has $(p-1)/m$ elements, say $v_1, \ldots, v_k$, which are the solutions in $\mathbb{F}_p^\times$ of $v_i^k = u$.
(c) Since $X^m - v_i \in \mathbb{F}_p[X]$, we deduce that

$$X^{p-1} - u = \prod_{i=1}^{k} (X^m - v_i)$$

is the decomposition of $X^{p-1} - u$ into irreducible factors over $\mathbb{F}_p$. □

Solution to Exercise 122.
For $p = 2$, we have $X^3 - 1 = (X-1)(X^2 + X + 1)$.

Assume that p is odd. We show that $X^{p+1} - 1$ is the product of $(X-1)(X+1)$ by $(p-1)/2$ quadratic polynomials $X^2 + aX + 1$ where a ranges over the set of elements in $\mathbb{F}_p$ such that $a^2 - 4$ is not a square modulo p.

Indeed, let x is a root of $X^{p+1} - 1$ in an extension of $\mathbb{F}_p$. If $x \in \mathbb{F}_p$, then $x^p = x$, which implies $x = \pm 1$. Assume now $x \notin \mathbb{F}_p$. From $x^p = x^{-1}$ we deduce $x^{p^2} = x^{-p} = x$, hence x is quadratic over $\mathbb{F}_p$ and its irreducible polynomial over $\mathbb{F}_p$ is

$$(X - x)(X - x^p) = X^2 + aX + 1$$

with $a = x + x^p$ and the discriminant $a^2 - 4$ is not a square. Conversely, if x is a root of such a polynomial, then its norm is $x^{p+1} = 1$. □

Solution to Exercise 123.
Let $(x,y) \in \mathbb{F}_8^2$ satisfy $x^3y + y^3 + x = 0$. If $x = 0$ the $y = 0$. If $y = 0$ then $x = 0$. Assume $(x,y) \neq (0,0)$. Then $x \neq 0$ and $y \neq 0$. Write $\mathbb{F}_8 = \mathbb{F}_2(\alpha)$ with $\alpha^3 = \alpha + 1$ (see Example 67). We can write

$$y = \alpha^j, \qquad x = \alpha^{3j}\beta$$

with $0 \leq j \leq 6$ and $\beta \in \mathbb{F}_8^\times$. We deduce

$$\alpha^{10j}\beta^3 + \alpha^{3j} + \alpha^{3j}\beta = 0.$$

Since $\alpha^7 = 1$, dividing by α^{3j}, we get

$$\beta^3 + \beta + 1 = 0,$$

hence β is a Galois conjugale to α. Since α has three conjugate, we obtain 21 points in $(F_8^\times)^2$. Counting the point $(0,0)$, we conclude that there are 22 solutions in $\mathbb{F}_8^2$.
`Remark.` *The curve* $X^3Y + Y^3 + X = 0$ *is an affine version of Klein quartic*

$$X^3Y + Y^3Z + XZ^3 = 0.$$

□

Solution to Exercise 124.
`Hint:` use a software like Sage. See also the examples and exercise:

p	r	n	Reference
2	1	2	30, 66
3	1	2	69
5	1	2	
7	1	2	
2	1	3	67
3	1	3	83
2	2	2	84
3	2	2	
2	3	2	

□

Solution to Exercise 125. (see Example 77).
If $q \equiv 1 \bmod 5$, the polynomial $\Phi_5(X) = X^4 + X^3 + X^2 + X + 1$ splits completely in $\mathbb{F}_q$ into a product of 4 degree 1 polynomials, the polynomial $X^5 - 1$ is a product of 5 irreducible polynomials, therefore, it has $2^5 = 32$ divisors, 1 of degree 0 and 1 of degree 5, 5 of degree 1 and also 5 of degree 4, 10 of degree 2 and 10 of degree 3.
If $q \equiv -1 \bmod 5$, the polynomial Φ_5 is a product of two irreducible degree 2 polynomials in $\mathbb{F}_q[X]$, $X^5 - 1$ is a product of 3 polynomials, hence, it has $2^3 = 8$ monic divisors, 1 of degree 0 and 1 of degree 5, 1 of degree 1 and also 1 of degree 4, 2 of degree 2 and 2 of degree 3.
If $q \equiv 2$ or $3 \bmod 5$, the polynomial Φ_5 is irreducible in $\mathbb{F}_q[X]$, $X^5 - 1$ is a product of 2 polynomials, hence, it has $2^2 = 4$ monic divisors, they have degree 0, 1, 4 and 5.

Number of cyclic codes of length 5 and of a given dimension over $\mathbb{F}_q$

dimension	0	1	2	3	4	5
$q \equiv 1 \bmod 5$	1	5	10	10	5	1
$q \equiv -1 \bmod 5$	1	1	2	2	1	1
$q \equiv 2$ or $3 \bmod 5$	1	1	0	0	1	1

□

Solution to Exercise 126.
From Theorem 101 with $r = 2$ and $t = 1$, one deduces that if there is a 1–error correcting code on $\mathbb{F}_{q^n}$ of dimension r, then $1 + n(q-1) \leq q^{n-r}$. For $q = 2$ this is $n \geq n_r$.

For $r = 1$ we have $n_1 = 3$ and the corresponding code on $\mathbb{F}_{2^3}$ of dimension 1 is the repetition code of Example 89.

For $r = 2$ we have $n_2 = 5$ and a binary 1–error correcting code of length 5 and dimension 2 is the code of Example 91.

For $r = 3$ we have $n_2 = 6$ and a binary 1–error correcting code of length 6 and dimension 3 is the code of Example 92.

For $r = 4$ we have $n_2 = 7$ and a binary 1–error correcting code of length 7 and dimension 4 is Hamming's code of Example 93. □

Solution to Exercise 127.
From Theorem 101 with $q = 3$, $r = 2$ and $t = 1$, one deduces that if there is a 1–error correcting code on $\mathbb{F}_{3^n}$ of dimension 2, then $1 + 2n \leq 3^{n-2}$, hence, $n \geq 4$.

An example of a ternary 1–error correcting $[4, 2]$ codeis given in Exercise 128. □

Solution to Exercise 128.
(a) This ternary code has length 4, dimension 2, the number of elements is $3^2 = 9$, the elements are

$$\begin{array}{lll} (0,0,0,0) & (0,1,1,-1) & (0,-1,-1,1) \\ (1,0,1,1) & (1,1,-1,0) & (1,-1,0,-1) \\ (-1,0,-1,-1) & (-1,1,0,1) & (-1,-1,1,0) \end{array}$$

(b) Any non–zero element in $\mathcal{C}$ has three non–zero coordinates, which means that the minimum weight of a non–zero element in $\mathcal{C}$ is 3. Since the code is linear, its minimum distance is 3. Hence, it can detect two errors and correct one error. The Hamming balls of radius 1 centred at the elements in $\mathcal{C}$ are pairwise disjoint.

Recall that a MDS code is a linear code $\mathcal{C}$ of length n and dimension d for which $d(\mathcal{C}) = n + 1 - d$. Here $n = 4$, $d = 2$ and $d(\mathcal{C}) = 3$, hence, this code $\mathcal{C}$ is MDS.
(c) The elements at Hamming distance ≤ 1 from $(0,0,0,0)$ are the elements of weight ≤ 1. There are 9 such elements, namely the center $(0,0,0,0)$ plus $2 \times 4 = 8$ elements having three coordinates 0 and the other one 1 or -1:

$$\begin{array}{llll} (1,0,0,0), & (-1,0,0,0), & (0,1,0,0), & (0,-1,0,0), \\ (0,0,1,0), & (0,0,-1,0), & (0,0,0,1), & (0,0,0,-1). \end{array}$$

A Hamming ball $B(\underline{x}, 1)$ of center $\underline{x} \in \mathbb{F}_3^4$ and radius 1 is nothing but the translate $\underline{x} + B(0,1)$ of the Hamming ball $B(0,1)$ by $\underline{x}$, hence, the number of elements in $B(\underline{x}, 1)$ is also 9.

(d) The 9 Hamming balls of radius 1 centred at the elements of $\mathcal{C}$ are pairwise disjoint, each of them has 9 elements and the total number of elements in the space $\mathbb{F}_3^4$ is 81. Hence, these balls give a perfect packing: each element in $\mathbb{F}_3^4$ belongs to one and only one Hamming ball centred at $\mathcal{C}$ and radius 1.
For instance, the unique element in the code at distance ≤ 1 from $\underline{x} = (1, 0, -1, 1)$ is $(1, 0, 1, 1)$. □

Solution to Exercise 129.
The class of 3 in $(\mathbb{Z}/7\mathbb{Z})^\times$ is a generator of this cyclic group of order $6 = \phi(7)$:

$$(\mathbb{Z}/7\mathbb{Z})^\times = \{3^0 = 1,\ 3^1 = 3,\ 3^2 = 2,\ 3^3 = 6,\ 3^4 = 4,\ 3^5 = 5\}.$$

The condition $q \equiv 3 \bmod 7$ implies that q has order 6 in $(\mathbb{Z}/7\mathbb{Z})^\times$, hence, Φ_7 is irreducible in $\mathbb{F}_q[X]$. The polynomial $X^7 - 1 = (X - 1)\Phi_7$ has exactly 4 monic divisors in $\mathbb{F}_3[X]$, namely

$$Q_0(X) = 1, \quad Q_1(X) = X - 1,$$

$$Q_2(X) = \Phi_7(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1, \quad Q_3(X) = X^7 - 1.$$

Hence, there are exactly 4 cyclic codes of length 7 over $\mathbb{F}_q$.

The code $\mathcal{C}_0$ associated to the factor $Q_0 = 1$ has dimension 7, it is the full code $\mathbb{F}_q^7$ with q^7 elements. A basis of $\mathcal{C}_0$ is any basis of $\mathbb{F}_q^7$, for instance, the canonical basis. The space of linear forms vanishing on $\mathcal{C}$ has dimension 0 (a basis is the empty set). The minimum distance is 1. It cannot detect any error. Since $d(\mathcal{C}) = 1 = n + 1 - d$, the code $\mathcal{C}_0$ is MDS.

The code $\mathcal{C}_1$ associated to the factor $Q_1 = X - 1$ has dimension 6, it is the hyperplane of equation $x_0 + \cdots + x_6 = 0$ in $\mathbb{F}_q$, it has q^6 elements. Let $T : \mathbb{F}_q^7 \to \mathbb{F}_q^7$ denote the right shift

$$T(a_0, a_1, a_2, a_3, a_4, a_5, a_6) = (a_6, a_0, a_1, a_2, a_3, a_4, a_5).$$

A basis (with 6 elements, as it should) of $\mathcal{C}_1$ is

$$\begin{array}{lllllllll}
e_0 = & & (1, & -1, & 0, & 0, & 0, & 0, & 0), \\
e_1 = & Te_0 = & (0, & 1, & -1, & 0, & 0, & 0, & 0), \\
e_2 = & T^2e_0 = & (0, & 0, & 1, & -1, & 0, & 0, & 0), \\
e_3 = & T^3e_0 = & (0, & 0, & 0, & 1, & -1, & 0, & 0), \\
e_4 = & T^4e_0 = & (0, & 0, & 0, & 0, & 1, & -1, & 0), \\
e_5 = & T^5e_0 = & (0, & 0, & 0, & 0, & 0, & 1, & -1).
\end{array}$$

Notice that $T^6e_0 = (-1, 0, 0, 0, 0, 0, 1)$ and

$$e_0 + Te_0 + T^2e_0 + T^3e_0 + T^4e_0 + T^5e_0 + T^6e_0 = 0.$$

This is related to

$$1 + X + X^2 + X^3 + X^4 + X^5 + X^6 = \Phi_7(X) = \frac{X^7 - 1}{X - 1}.$$

The minimum distance of $\mathcal{C}_1$ is 2, it is a MDS code. It can detect one error (it is a parity bit check) but cannot correct any error.

The code $\mathcal{C}_2$ associated to the factor Q_2 has dimension 1 and q elements:

$$\mathcal{C}_2 = \{(a, a, a, a, a, a, a)\ ;\ a \in \mathbb{F}_q\} \subset \mathbb{F}_q^7.$$

It is the repetition code of length 7, which is the line given by the equations

$$X_1 = X_2 = X_3 = X_4 = X_5 = X_6 = X_7$$

spanned by $(1, 1, 1, 1, 1, 1, 1)$ in $\mathbb{F}_q^7$, there are q elements in the code. It has dimension 1, its minimum distance is 7, hence, is MDS. It can detect 6 errors and correct 3 errors.

The code $\mathcal{C}_3$ associated to the factor Q_3 is the trivial code of dimension 0, it contains only one element, a basis is the empty set, a basis of the space of linear forms vanishing on $\mathcal{C}_3$ is $x_0, x_1, x_2, x_3, x_4, x_5, x_6$. Its minimum distance is not defined, it is not considered as a MDS code. □

References

[1] W. Chen – *Discrete Mathematics*, 201 pp. (web edition, 2008).
http://rutherglen.science.mq.edu.au/wchen/lndmfolder/lndm.html/

[2] M. Demazure, *Cours d'algèbre*, Nouvelle Bibliothèque Mathématique [New Mathematics Library], 1, Cassini, Paris, 1997. Primalité. Divisibilité. Codes. [Primality. Divisibility. Codes].

[3] D. S. Dummit & R. M. Foote, *Abstract algebra*, John Wiley & Sons Inc., Hoboken, NJ, third ed., 2004.

[4] M. Hindry, *Arithmetics. Primality and codes, analytic number theory, Diophantine equations, elliptic curves. (Arithmétique. Primalité et codes, théorie analytique des nombres, équations diophantiennes, courbes elliptiques.)*, Paris: Calvage et Mounet. xvi, 328 p., 2008.

[5] K. Kedlaya & S. Kopparty – *On the degree of polynomials computing square roots mod p* , 2023. http://arxiv.org/abs/2311.10956v1

[6] S. Lang – *Algebra*, vol. 211 of Graduate Texts in Mathematics, Springer-Verlag, New York, third ed., 2002.
In French: *Algèbre*, troisième édition, Dunod, 2004.

[7] R. Lidl & H. Niederreiter – *Introduction to finite fields and their applications*, Cambridge Univ. Press, 1994.
http://www.amazon.com/gp/reader/0521460948/ref=sib_dp_ptu#reader-link

[8] G.L. Mullen & C. Mummert – *Finite Fields and Applications*, Student mathematical library, **41**, AMS 2007.

[9] V. Shoup – *A Computational Introduction to Number Theory and Algebra* (Version 2) second print editon, Fall 2008. http://shoup.net/ntb/

Michel WALDSCHMIDT
Sorbonne Université and Université de Paris
CNRS, IMJ–PRG
75005 Paris, France
e-mail: michel.waldschmidt@imj-prg.fr
URL: http://www.imj-prg.fr/~michel.waldschmidt/