Updated: *18 février 2016*

Université des Sciences, de Technologie et de Médecine de Nouakchott
École de recherche CIMPA-Mauritanie 15 - 26 février 2016
Algorithmique en Théorie des Nombres et Cryptographie

Arithmétique modulaire, fractions continues, corps finis.

Michel Waldschmidt
This text is available on the internet at the address[1]
http://www.imj-prg.fr/~michel.waldschmidt/

Contents

[1]Les notes sont en anglais, mais les cours seront donnés en français.

1 Background

Among many references for this preliminary section are D.S. Dummit & R.M. Foote [5] and S. Lang [9].

1.1 Group theory

Groups, subgroups. Lagrange's theorem: *the order of a subgroup of a finite group divides the order of the group.* Index of a subgroup in a group.

Additive vs multiplicative notation.

Abelian groups (=commutative groups).

Intersection of subgroups. Subgroup generated by a subset. Finitely generated group. Subgroup generated by an element.

The *order* of an element is the order of the subgroup generated by this element. An element x in a multiplicative group G is *torsion* if it has finite order, that means if there exists $m \geq 1$ such that $x^m = 1$. In this case the order of x is the least of these integers m's. The set of $m \in \mathbf{Z}$ with $x^m = 1$ is a subgroup of $\mathbf{Z}$ which is not 0, hence, it has a unique positive generator d, which is *the order of* x. Therefore, for an element x of order d, we have

$$x^m = 1 \Longleftrightarrow d|m.$$

We stress that the condition $x^m = 1$ does not mean that x has order m, it means that the order of x divides m.

If x is an element in a multiplicative group G and m an integer such that $x^m = 1$, then for i and j in $\mathbf{Z}$ satisfying $i \equiv j \bmod m$ we have $x^i = x^j$. In other terms, the kernel of the morphism

$$\begin{array}{ccc} \mathbf{Z} & \longrightarrow & G \\ j & \mapsto & x^j \end{array}$$

contains $m\mathbf{Z}$. Hence, this morphism factors to $\mathbf{Z}/m\mathbf{Z} \longrightarrow G$, which we denote again by $j \mapsto x^j$. This means that we define x^j for j a class modulo m by selecting any representative of j in $\mathbf{Z}$.

Exercise 1.
(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.

The *torsion subgroup* of a commutative group. *Exponent* of a torsion group G: the smallest integer $m \geq 1$ such that $x^m = 1$ for all $x \in G$. Examples of torsion groups: in additive notation $\mathbf{Z}/n\mathbf{Z}$, $\mathbf{Q}/\mathbf{Z}$. In multiplicative notation: n-th roots of unity, group of all roots of unity in $\mathbf{C}$.

Direct product and *direct sum* of groups (this is the same when there are only finitely many groups).

Morphisms (also called *homomorphisms*) between groups. Isomorphisms, *endomorphisms*, *automorphisms*. *Kernel* of a morphism. *Quotient* of a group by a subgroup.

Theorem of factorisation for morphisms of groups.

Given an surjective morphism of groups $f : G_1 \longrightarrow G_2$ and a morphism of groups $g : G_1 \longrightarrow G_3$, there exists a morphism $h : G_2 \longrightarrow G_3$ such that $h \circ f = g$ if and only if $\ker f \subset \ker g$.

$$\begin{array}{ccc} G_1 & \xrightarrow{\ g\ } & G_3 \\ {\scriptstyle f}\big\downarrow & \nearrow_h & \\ G_2 & & \end{array}$$

If h exists, then h is surjective if and only if g is surjective, and h is injective if and only if $\ker f = \ker g$.

Example: $G_2 = G_1/H$ when G_1 is abelian, H a subgroup of G_1, and f is the canonical morphism.

Cyclic groups. 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 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 whose order 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.

A direct product $G_1 \times G_2$ 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 § 1.4.1).

1.2 Ring theory

Unless otherwise explicitly specified, the rings are commutative, with a unity 1 and $1 \neq 0$. Often, they have no zero divisors (they are called *domains*), but not always: indeed, we will consider quotient rings like $\mathbf{Z}/n\mathbf{Z}$ where n is not a prime number.

Characteristic of a ring.

Intersection of rings. For B a ring, A a subring and E a subset of B, the ring generated by E over A is denoted by $A[E]$. Special case where $E = \{\alpha_1, \ldots, \alpha_n\}$: we denote it by $A[\alpha_1, \ldots, \alpha_n]$.

Morphisms between rings, *isomporhisms*, *endomorphisms*, *automorphisms*. *Ideal* of a ring, *kernel* of a morphism. *Quotient* of a commutative ring by an ideal $\mathcal{I} \neq \{0\}$. Canonical morphism $A \to A/\mathcal{I}$. *Prime ideals, maximal ideals.*

Theorem of factorisation for morphisms of rings. *Given a surjective morphism of rings $f : A_1 \longrightarrow A_2$ and a morphism of rings $g : A_1 \longrightarrow A_3$, there exists a morphism $h : A_2 \longrightarrow A_3$ such that $h \circ f = g$ if and only if* $\ker f \subset \ker g$.

$$\begin{array}{ccc} A_1 & \xrightarrow{\ g\ } & A_3 \\ {\scriptstyle f}\big\downarrow & \nearrow_h & \\ A_2 & & \end{array}$$

If h exists, then h is surjective if and only if g is surjective, and h is injective if and only if $\ker f = \ker g$.

Example: $A_2 = A_1/\mathcal{I}$ when A_1 is commutative, $\mathcal{I}$ an ideal of A_1, and f is the canonical morphism.

Quotient field of a domain.

The ring of polynomials in one variable $A[X]$ or in several variables $A[X_1, \ldots, X_n]$.

The *units* of a ring A are the invertible elements, they form a multiplicative group $A^\times$. A *field* is a ring F such that $F^\times = F \setminus \{0\}$. The torsion elements in the group $A^\times$ are the *roots of unity* in A. Their set

$$A^\times_{\text{tors}} = \{x \in A \mid \text{ there exists } n \geq 1 \text{ such that } x^n = 1\}$$

is the *torsion subgroup* of the group of units $A^\times$.

Euclidean rings, principal rings, factorial rings. Examples: $\mathbf{Z}$, $k[X]$ where k is a field, $A[X]$ where A is a ring, $k[X_1, \ldots, X_n]$ and $A[X_1, \ldots, X_n]$.

Given two rings A_1, B_2, a subring A_2 of B_2, a morphism of rings

$$f : A_1 \to A_2 \subset B_2$$

and elements $y_1, \ldots, y_n$ of B_2, there is a unique morphism

$$F : A_1[X_1, \ldots, X_n] \to A_2[y_1, \ldots, y_n]$$

such that $F(a) = f(a)$ for $a \in A_1$ and $F(X_i) = y_i$ for $1 \leq i \leq n$.

As a consequence, if $f : A_1 \to A_2$ is a morphism of rings, there is a unique morphism of rings $A_1[X_1, \ldots, X_n] \to A_2[X_1, \ldots, X_n]$ which coincides with f on A_1 and maps X_i to X_i for $1 \leq i \leq n$.

A fundamental example is the surjective morphism of rings

$$\Psi_p : \mathbf{Z}[X] \to \mathbf{F}_p[X], \tag{2}$$

which maps X to X and $\mathbf{Z}$ onto $\mathbf{F}_p$ by reduction modulo p of the coefficients. Its kernel is the principal ideal $p\mathbf{Z}[X] = (p)$ of $\mathbf{Z}[X]$ generated by p.

Exercise 3. 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 $x_1, \ldots, x_n$ of B_1 and elements $y_1, \ldots, y_n$ of B_2, a necessary and sufficient condition for the existence of a morphism $F : A_1[x_1, \ldots, x_n] \to A_2[y_1, \ldots, y_n]$ 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 $P \in A_1[X_1, \ldots, X_n]$ such that

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

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

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

Modules over a ring. *Example*: $\mathbf{Z}$–modules are nothing else than the abelian groups.

Structure theorem for finitely generated modules over a principal ring. *Application*: structure theorems for finitely generated abelian groups and for finite groups. *Rank* of a finitely generated abelian group.
Consequence: In a finite abelian group of exponent e, there exists an element of order e.

1.3 Field theory

The characteristic of a field K is either 0 or else a prime number p. In the first case, the *prime field* (smallest subfield of K, which is the intersection of all subfields of K) is $\mathbf{Q}$; in the second case, it is $\mathbf{F}_p := \mathbf{Z}/p\mathbf{Z}$.

Intersection of fields. If L is a field and K a subfield, we say that L is an *extension of* K. Then L is a K–vector space. Further, if E is a subset of L, we denote by $K(E)$ the field generated by E over K: it is the quotient field of $K[E]$. If $E = \{\alpha_1, \ldots, \alpha_n\}$, we write $K(E) = K(\alpha_1, \ldots, \alpha_n)$. If K_1 and K_2 are two subfields of a field L, the *compositum* of K_1 and K_2 is the subfield field $K_1(K_2) = K_2(K_1)$ of L generated by $K_1 \cup K_2$.

A morphism $f : K \to A$, where K is a field and A a ring, is injective.

When L_1 and L_2 are two extensions of K, a *K-morphism* $L_1 \to L_2$ is a field morphism whose restriction to K is the identity. If $f : L_1 \to L_2$ is a field morphism, then L_1 and L_2 have the same characteristic, hence, the same prime field F, and f is a F–morphism.

If L is an extension of K, the K–automorphisms of L form a group denoted $\mathrm{Aut}(L/K)$.

Finitely generated extensions. *Algebraic* and *transcendental* extensions.

Finite extensions, degree $[L : K]$. For $K_1 \subset K_2 \subset K_3$, we have

$$[K_3 : K_1] = [K_3 : K_2][K_2 : K_1].$$

Given an extension $L \supset K$ of fields and an element $\alpha \in L$, there is a unique map $K[X] \to K[\alpha]$, which is the identity on K and maps X to α. Kernel of this map. *Irreducible* (monic) polynomial of an algebraic element over a field K. The field $K[X]/(f) = K(\alpha)$ when α is algebraic over K.

For L an extension of K, an element α in L is algebraic over K if and only if $K[\alpha] = K(\alpha)$, and this is true if and only if $[K(\alpha) : K]$ is finite.

Splitting field of a polynomial over a field. *Algebraic closure* of a field. Two algebraic closures of K are K–isomorphic, but, usually, there is no unicity of such a morphism (since there are many K–automorphisms of the algebraic closure: they constitute the *absolute Galois group* of K).

An element α in an algebraically closed extension Ω of a field K is algebraic over K if and only if the set of $\sigma(\alpha)$, where σ ranges over the K–automorphisms of Ω, is finite.

Given an algebraically closed field Ω, a subfield K of Ω and an element $\alpha \in \Omega$ algebraic over K, the roots in Ω of the irreducible polynomial f of α over K are the *conjugates* of α over K. If $\alpha_1, \ldots, \alpha_m$ are the distinct roots of f in Ω, then there are exactly m K–morphisms $K(\alpha) \to \Omega$, say $\sigma_1, \ldots, \sigma_m$, where σ_i is determined by $\sigma_i(\alpha) = \alpha_i$.

Zeroes of polynomials: *multiplicity* or *order* of a zero of a polynomial in one variable.

1.4 Arithmetic

1.4.1 Residue classes modulo n

Subgroups of $\mathbf{Z}$. Morphism $s_n : \mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$. There exists a morphism $\varphi : \mathbf{Z}/a\mathbf{Z} \to \mathbf{Z}/b\mathbf{Z}$ such that $\varphi \circ s_a = s_b$ if and only if $a\mathbf{Z} \subset b\mathbf{Z}$, which means if and only if b divides a. If φ exists, then φ is unique and surjective. Its kernel is $b\mathbf{Z}/a\mathbf{Z}$ which is isomorphic to $\mathbf{Z}/(a/b)\mathbf{Z}$.

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

The order of the multiplicative group $(\mathbf{Z}/n\mathbf{Z})^\times$ of the ring $\mathbf{Z}/n\mathbf{Z}$ is the number $\varphi(n)$ of integers k in the interval $1 \leq k \leq n$ satisfying $\gcd(n, k) = 1$. The map $\varphi : \mathbf{Z}_{>0} \to \mathbf{Z}$ is *Euler's function* already mentioned in § 1.1. 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 4. *For any positive integer n,*

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

(Compare with (85)).

An *arithmetic function* is a map $f : \mathbf{Z}_{>0} \to \mathbf{Z}$. 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 $(\mathbf{Z}/m\mathbf{Z}) \times (\mathbf{Z}/n\mathbf{Z})$ and the ring $\mathbf{Z}/mn\mathbf{Z}$ 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

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

Primitive roots modulo a prime number p: there are exactly $\varphi(p-1)$ of them in $(\mathbf{Z}/p\mathbf{Z})^\times$. An element $g \in (\mathbf{Z}/p\mathbf{Z})^\times$ 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 $(\mathbf{Z}/n\mathbf{Z})^\times$. In other terms, it is the smallest integer ℓ such that a^ℓ is congruent to 1 modulo n.

Exercise 5. For n a positive integer, check that the multiplicative group $(\mathbf{Z}/n\mathbf{Z})^\times$ 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 $s \geq 2$, $(\mathbf{Z}/2^s\mathbf{Z})^\times$ 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.*

1.4.2 The ring $\mathbf{Z}[X]$

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 $\mathbf{Z}[X]$ is not an Euclidean ring: one cannot divide X by 2 in $\mathbf{Z}[X]$ for instance. But if A and B are in $\mathbf{Z}[X]$ and B is monic, then both the quotient Q and the remainder R of the Euclidean division in $\mathbf{Q}[X]$ of A by B

$$A = BQ + R$$

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

The gcd of the coefficients of a non–zero polynomial $f \in \mathbf{Z}[X]$ 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 $\mathbf{Z}[X]$ can be written in a unique way as $f = c(f)g$ with $g \in \mathbf{Z}[X]$ primitive.

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

Lemma 6 (Gauss's Lemma)**.** *For f and g non–zero polynomials in $\mathbf{Z}[X]$, 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.

Recall the surjective morphism of rings (2) $\Psi_p : \mathbf{Z}[X] \to \mathbf{F}_p[X]$, which is the reduction modulo p. The kernel of Ψ_p 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 $\mathbf{F}_p[X]$ 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 $\mathbf{Z}$ is an Euclidean domain, hence, a principal domain, and, therefore, a factorial ring. It follows that the ring $\mathbf{Z}[X]$ is factorial. The units of $\mathbf{Z}[X]$ are $\{+1, -1\}$. The irreducible elements in $\mathbf{Z}[X]$ are
– the prime numbers $\{2, 3, 5, 7, 11, \dots\}$,
– the irreducible polynomials in $\mathbf{Q}[X]$ with coefficients in $\mathbf{Z}$ and content 1
– and, of course, the product of one of these elements by -1.

From Gauss's Lemma 6, one deduces that if f and g are two monic polynomials in $\mathbf{Q}[X]$ such that $fg \in \mathbf{Z}[X]$, then f and g are in $\mathbf{Z}[X]$.

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

1.4.3 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 7) 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, [13] § 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 4 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 $\mathbf{C}$. 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 7. Let A be a (commutative) 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

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

2 Continued fractions

We first consider generalized continued fractions of the form

$$a_0 + \cfrac{b_1}{a_1 + \cfrac{b_2}{a_2 + \cfrac{b_3}{\ddots}}},$$

which we denote by[2]

$$a_0 + \frac{b_1|}{|a_1} + \frac{b_2|}{|a_2} + \frac{b_3|}{\ddots}.$$

Next we restrict to the special case where $b_1 = b_2 = \cdots = 1$, which yields the simple continued fractions

$$a_0 + \frac{1|}{|a_1} + \frac{1|}{|a_2} + \cdots = [a_0, a_1, a_2, \dots].$$

2.1 Generalized continued fractions

To start with, $a_0, \dots, a_n, \dots$ and $b_1, \dots, b_n, \dots$ will be independent variables. Later, we shall specialize to positive integers (apart from a_0 which may be negative).

Consider the three rational fractions

$$a_0, \qquad a_0 + \frac{b_1}{a_1} \quad \text{and} \quad a_0 + \cfrac{b_1}{a_1 + \cfrac{b_2}{a_2}}.$$

We write them as

$$\frac{A_0}{B_0}, \qquad \frac{A_1}{B_1} \quad \text{and} \quad \frac{A_2}{B_2}$$

with

$$\begin{array}{lll} A_0 = a_0, & A_1 = a_0a_1 + b_1, & A_2 = a_0a_1a_2 + a_0b_2 + a_2b_1, \\ B_0 = 1, & B_1 = a_1, & B_2 = a_1a_2 + b_2. \end{array}$$

[2] Another notation for $a_0 + \frac{b_1|}{|a_1} + \frac{b_2|}{|a_2} + \cdots + \frac{b_n|}{a_n}$ introduced by Th. Muir and used by Perron in [11] Chap. 1 is

$$K\begin{pmatrix} b_1, \dots, b_n \\ a_0, a_1, \dots, a_n \end{pmatrix}$$

Observe that

$$A_2 = a_2A_1 + b_2A_0, \quad B_2 = a_2B_1 + b_2B_0.$$

Write these relations as

$$\begin{pmatrix} A_2 \\ B_2 \end{pmatrix} = \begin{pmatrix} A_1 & A_0 \\ B_1 & B_0 \end{pmatrix} \begin{pmatrix} a_2 \\ b_2 \end{pmatrix}.$$

In order to iterate the process, it is convenient to work with 2×2 matrices and to write

$$\begin{pmatrix} A_2 & A_1 \\ B_2 & B_1 \end{pmatrix} = \begin{pmatrix} A_1 & A_0 \\ B_1 & B_0 \end{pmatrix} \begin{pmatrix} a_2 & 1 \\ b_2 & 0 \end{pmatrix}.$$

Define inductively two sequences of polynomials with positive rational coefficients A_n and B_n for $n \geq 3$ by

$$\begin{pmatrix} A_n & A_{n-1} \\ B_n & B_{n-1} \end{pmatrix} = \begin{pmatrix} A_{n-1} & A_{n-2} \\ B_{n-1} & B_{n-2} \end{pmatrix} \begin{pmatrix} a_n & 1 \\ b_n & 0 \end{pmatrix}. \tag{8}$$

This means

$$A_n = a_nA_{n-1} + b_nA_{n-2}, \qquad B_n = a_nB_{n-1} + b_nB_{n-2}.$$

This recurrence relation holds for $n \geq 2$. It will also hold for $n = 1$ if we set $A_{-1} = 1$ and $B_{-1} = 0$:

$$\begin{pmatrix} A_1 & A_0 \\ B_1 & B_0 \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ b_1 & 0 \end{pmatrix}$$

and it will hold also for $n = 0$ if we set $b_0 = 1$, $A_{-2} = 0$ and $B_{-2} = 1$:

$$\begin{pmatrix} A_0 & A_{-1} \\ B_0 & B_{-1} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a_0 & 1 \\ b_0 & 0 \end{pmatrix}.$$

Obviously, an equivalent definition is

$$\begin{pmatrix} A_n & A_{n-1} \\ B_n & B_{n-1} \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ b_0 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ b_1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_{n-1} & 1 \\ b_{n-1} & 0 \end{pmatrix} \begin{pmatrix} a_n & 1 \\ b_n & 0 \end{pmatrix}. \tag{9}$$

These relations (9) hold for $n \geq -1$, with the empty product (for $n = -1$) being the identity matrix, as always.

Hence $A_n \in \mathbf{Z}[a_0, \ldots, a_n, b_1, \ldots, b_n]$ is a polynomial in $2n + 1$ variables, while $B_n \in \mathbf{Z}[a_1 \ldots, a_n, b_2, \ldots, b_n]$ is a polynomial in $2n - 1$ variables.

Exercise 1. *Check, for $n \geq -1$,*

$$B_n(a_1, \ldots, a_n, b_2, \ldots, b_n) = A_{n-1}(a_1, \ldots, a_n, b_2, \ldots, b_n).$$

Lemma 10. *For $n \geq 0$,*

$$a_0 + \frac{b_1|}{|a_1} + \cdots + \frac{b_n|}{|a_n} = \frac{A_n}{B_n}.$$

Proof. By induction. We have checked the result for $n = 0$, $n = 1$ and $n = 2$. Assume the formula holds with $n - 1$ where $n \geq 3$. We write

$$a_0 + \frac{b_1|}{|a_1} + \cdots + \frac{b_{n-1}|}{|a_{n-1}} + \frac{b_n|}{|a_n} = a_0 + \frac{b_1|}{|a_1} + \cdots + \frac{b_{n-1}|}{|x}$$

with

$$x = a_{n-1} + \frac{b_n}{a_n}.$$

We have, by induction hypothesis and by the definition (8),

$$a_0 + \frac{b_1|}{|a_1} + \cdots + \frac{b_{n-1}|}{|a_{n-1}} = \frac{A_{n-1}}{B_{n-1}} = \frac{a_{n-1}A_{n-2} + b_{n-1}A_{n-3}}{a_{n-1}B_{n-2} + b_{n-1}B_{n-3}}.$$

Since A_{n-2}, A_{n-3}, B_{n-2} and B_{n-3} do not depend on the variable a_{n-1}, we deduce

$$a_0 + \frac{b_1|}{|a_1} + \cdots + \frac{b_{n-1}|}{|x} = \frac{xA_{n-2} + b_{n-1}A_{n-3}}{xB_{n-2} + b_{n-1}B_{n-3}}.$$

The product of the numerator by a_n is

$$\begin{aligned}(a_n a_{n-1} + b_n)A_{n-2} + a_n b_{n-1}A_{n-3} &= a_n(a_{n-1}A_{n-2} + b_{n-1}A_{n-3}) + b_n A_{n-2} \\ &= a_n A_{n-1} + b_n A_{n-2} = A_n\end{aligned}$$

and similarly, the product of the denominator by a_n is

$$\begin{aligned}(a_n a_{n-1} + b_n)B_{n-2} + a_n b_{n-1}B_{n-3} &= a_n(a_{n-1}B_{n-2} + b_{n-1}B_{n-3}) + b_n B_{n-2} \\ &= a_n B_{n-1} + b_n B_{n-2} = B_n.\end{aligned}$$

□

From (9), taking the determinant, we deduce, for $n \geq -1$,

$$A_n B_{n-1} - A_{n-1}B_n = (-1)^{n+1} b_0 \cdots b_n. \tag{11}$$

which can be written, for $n \geq 1$,

$$\frac{A_n}{B_n} - \frac{A_{n-1}}{B_{n-1}} = \frac{(-1)^{n+1} b_0 \cdots b_n}{B_{n-1} B_n}. \tag{12}$$

Adding the telescoping sum, we get, for $n \geq 0$,

$$\frac{A_n}{B_n} = A_0 + \sum_{k=1}^{n} \frac{(-1)^{k+1} b_0 \cdots b_k}{B_{k-1} B_k}. \tag{13}$$

We now substitute for $a_0, a_1, \ldots$ and $b_1, b_2, \ldots$ rational integers, all of which are ≥ 1, apart from a_0 which may be ≤ 0. We denote by p_n (resp. q_n) the value of A_n (resp. B_n) for these special values. Hence p_n and q_n are rational integers, with $q_n > 0$ for $n \geq 0$. A consequence of Lemma 10 is

$$\frac{p_n}{q_n} = a_0 + \frac{b_1|}{|a_1} + \cdots + \frac{b_n|}{|a_n} \quad \text{for} \quad n \geq 0.$$

We deduce from (8),

$$p_n = a_n p_{n-1} + b_n p_{n-2}, \qquad q_n = a_n q_{n-1} + b_n q_{n-2} \quad \text{for} \quad n \geq 0,$$

and from (11),

$$p_n q_{n-1} - p_{n-1} q_n = (-1)^{n+1} b_0 \cdots b_n \quad \text{for} \quad n \geq -1,$$

which can be written, for $n \geq 1$,

$$\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{(-1)^{n+1} b_0 \cdots b_n}{q_{n-1} q_n}. \tag{14}$$

Adding the telescoping sum (or using (13)), we get the alternating sum

$$\frac{p_n}{q_n} = a_0 + \sum_{k=1}^{n} \frac{(-1)^{k+1} b_0 \cdots b_k}{q_{k-1} q_k}. \tag{15}$$

Recall that for real numbers a, b, c, d, with b and d positive, we have

$$\frac{a}{b} < \frac{c}{d} \implies \frac{a}{b} < \frac{a+c}{b+d} < \frac{c}{d}. \tag{16}$$

Since a_n and b_n are positive for $n \geq 0$, we deduce that for $n \geq 2$, the rational number

$$\frac{p_n}{q_n} = \frac{a_n p_{n-1} + b_n p_{n-2}}{a_n q_{n-1} + b_n q_{n-2}}$$

lies between p_{n-1}/q_{n-1} and p_{n-2}/q_{n-2}. Therefore we have

$$\frac{p_2}{q_2} < \frac{p_4}{q_4} < \cdots < \frac{p_{2n}}{q_{2n}} < \cdots < \frac{p_{2m+1}}{q_{2m+1}} < \cdots < \frac{p_3}{q_3} < \frac{p_1}{q_1}. \tag{17}$$

From (14), we deduce, for $n \geq 3$, $q_{n-1} > q_{n-2}$, hence $q_n > (a_n + b_n)q_{n-2}$.

The previous discussion was valid without any restriction, now we assume $a_n \geq b_n$ for all sufficiently large n, say $n \geq n_0$. Then for $n > n_0$, using $q_n > 2b_n q_{n-2}$, we get

$$\left|\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}}\right| = \frac{b_0 \cdots b_n}{q_{n-1}q_n} < \frac{b_n \cdots b_0}{2^{n-n_0} b_n b_{n-1} \cdots b_{n_0+1} q_{n_0} q_{n_0-1}} = \frac{b_{n_0} \cdots b_0}{2^{n-n_0} q_{n_0} q_{n_0-1}}$$

and the right hand side tends to 0 as n tends to infinity. Hence the sequence $(p_n/q_n)_{n\geq 0}$ has a limit, which we denote by

$$x = a_0 + \frac{b_1|}{|a_1} + \cdots + \frac{b_{n-1}|}{|a_{n-1}} + \frac{b_n|}{|a_n} + \cdots$$

From (15), it follows that x is also given by an alternating series

$$x = a_0 + \sum_{k=1}^{\infty} \frac{(-1)^{k+1} b_0 \cdots b_k}{q_{k-1}q_k}.$$

We now prove that x is irrational. Define, for $n \geq 0$,

$$x_n = a_n + \frac{b_{n+1}|}{|a_{n+1}} + \cdots$$

so that $x = x_0$ and, for all $n \geq 0$,

$$x_n = a_n + \frac{b_{n+1}}{x_{n+1}}, \qquad x_{n+1} = \frac{b_{n+1}}{x_n - a_n}$$

and $a_n < x_n < a_n + 1$. Hence for $n \geq 0$, x_n is rational if and only if x_{n+1} is rational, and therefore, if x is rational, then all x_n for $n \geq 0$ are also rational. Assume x is rational. Consider the rational numbers x_n with $n \geq n_0$ and select a value of n for which the denominator v of x_n is minimal, say $x_n = u/v$. From

$$x_{n+1} = \frac{b_{n+1}}{x_n - a_n} = \frac{b_{n+1}v}{u - a_n v} \quad \text{with} \quad 0 < u - a_n v < v,$$

it follows that x_{n+1} has a denominator strictly less than v, which is a contradiction. Hence x is irrational.

Conversely, given an irrational number x and a sequence $b_1, b_2, \dots$ of positive integers, there is a unique integer a_0 and a unique sequence $a_1, \dots, a_n, \dots$ of positive integers satisfying $a_n \geq b_n$ for all $n \geq 1$, such that

$$x = a_0 + \frac{b_1|}{|a_1} + \cdots + \frac{b_{n-1}|}{|a_{n-1}} + \frac{b_n|}{|a_n} + \cdots$$

Indeed, the unique solution is given inductively as follows: $a_0 = \lfloor x \rfloor$, $x_1 = b_1/\{x\}$, and once $a_0, \dots, a_{n-1}$ and $x_1, \dots, x_n$ are known, then a_n and x_{n+1} are given by

$$a_n = \lfloor x_n \rfloor, \quad x_{n+1} = b_{n+1}/\{x_n\},$$

so that for $n \geq 1$ we have $0 < x_n - a_n < 1$ and

$$x = a_0 + \frac{b_1|}{|a_1} + \cdots + \frac{b_{n-1}|}{|a_{n-1}} + \frac{b_n|}{|x_n}.$$

Here is what we have proved.

Proposition 18. *Given a rational integer a_0 and two sequences $a_0, a_1, \dots$ and $b_1, b_2, \dots$ of positive rational integers with $a_n \geq b_n$ for all sufficiently large n, the infinite continued fraction*

$$a_0 + \frac{b_1|}{|a_1} + \cdots + \frac{b_{n-1}|}{|a_{n-1}} + \frac{b_n|}{|a_n} + \cdots$$

exists and is an irrational number.
Conversely, given an irrational number x and a sequence $b_1, b_2, \dots$ of positive integers, there is a unique $a_0 \in \mathbf{Z}$ and a unique sequence $a_1, \dots, a_n, \dots$ of positive integers satisfying $a_n \geq b_n$ for all $n \geq 1$ such that

$$x = a_0 + \frac{b_1|}{|a_1} + \cdots + \frac{b_{n-1}|}{|a_{n-1}} + \frac{b_n|}{|a_n} + \cdots$$

These results are useful for proving the irrationality of π and e^r when r is a non–zero rational number, following the proof by Lambert. See for instance Chapter 7 (Lambert's Irrationality Proofs) of David Angell's course on Irrationality and Transcendence([3]) at the University of New South Wales:

`http://www.maths.unsw.edu.au/~angell/5535/`

The following example is related with Lambert's proof [8]:

$$\tanh z = \frac{z|}{|1} + \frac{z^2|}{|\,3} + \frac{z^2|}{|\,5} + \cdots + \frac{z^2\ \ |}{|2n+1} + \cdots$$

[3] I found this reference from the website of John Cosgrave
`http://staff.spd.dcu.ie/johnbcos/transcendental_numbers.htm`.

Here, z is a complex number and the right hand side is a complex valued function. Here are other examples (see Sloane's Encyclopaedia of Integer Sequences([4]))

$$\frac{1}{\sqrt{e}-1} = 1 + \frac{2|}{|3} + \frac{4|}{|5} + \frac{6|}{|7} + \frac{8|}{|9} + \cdots = 1.541\,494\,082\ldots \qquad \text{(A113011)}$$

$$\frac{1}{e-1} = \frac{1|}{|1} + \frac{2|}{|2} + \frac{3|}{|3} + \frac{4|}{|4} + \cdots = 0.581\,976\,706\ldots \qquad \text{(A073333)}$$

Remark. *A variant of the algorithm of simple continued fractions is the following. Given two sequences $(a_n)_{n\geq 0}$ and $(b_n)_{n\geq 0}$ of elements in a field K and an element x in K, one defines a sequence (possibly finite) $(x_n)_{n\geq 1}$ of elements in K as follows. If $x = a_0$, the sequence is empty. Otherwise x_1 is defined by $x = a_0 + (b_1/x_1)$. Inductively, once $x_1, \ldots, x_n$ are defined, there are two cases:*

- *If $x_n = a_n$, the algorithm stops.*
- *Otherwise, x_{n+1} is defined by*

$$x_{n+1} = \frac{b_{n+1}}{x_n - a_n}, \quad \text{so that} \quad x_n = a_n + \frac{b_{n+1}}{x_{n+1}}.$$

If the algorithm does not stop, then for any $n \geq 1$, one has

$$x = a_0 + \frac{b_1|}{|a_1} + \cdots + \frac{b_{n-1}|}{|a_{n-1}} + \frac{b_n|}{|x_n}.$$

In the special case where $a_0 = a_1 = \cdots = b_1 = b_2 = \cdots = 1$, the set of x such that the algorithm stops after finitely many steps is the set $(F_{n+1}/F_n)_{n\geq 1}$ of quotients of consecutive Fibonacci numbers. In this special case, the limit of

$$a_0 + \frac{b_1|}{|a_1} + \cdots + \frac{b_{n-1}|}{|a_{n-1}} + \frac{b_n|}{|a_n}$$

is the Golden ratio, which is independent of x, of course!

2.2 Simple continued fractions

We restrict now the discussion of § 2.1 to the case where $b_1 = b_2 = \cdots = b_n = \cdots = 1$. We keep the notations A_n and B_n which are now polynomials in $\mathbf{Z}[a_0, a_1, \ldots, a_n]$ and $\mathbf{Z}[a_1, \ldots, a_n]$ respectively, and when we specialize to

[4] `http://www.research.att.com/~njas/sequences/`

integers $a_0, a_1, \ldots, a_n \ldots$ with $a_n \geq 1$ for $n \geq 1$ we use the notations p_n and q_n for the values of A_n and B_n.

The recurrence relations (8) are now, for $n \geq 0$,

$$\begin{pmatrix} A_n & A_{n-1} \\ B_n & B_{n-1} \end{pmatrix} = \begin{pmatrix} A_{n-1} & A_{n-2} \\ B_{n-1} & B_{n-2} \end{pmatrix} \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix}, \tag{19}$$

while (9) becomes, for $n \geq -1$,

$$\begin{pmatrix} A_n & A_{n-1} \\ B_n & B_{n-1} \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_{n-1} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix}. \tag{20}$$

From Lemma 10 one deduces, for $n \geq 0$,

$$[a_0, \ldots, a_n] = \frac{A_n}{B_n}.$$

Taking the determinant in (20), we deduce the following special case of (11)

$$A_n B_{n-1} - A_{n-1} B_n = (-1)^{n+1}.$$

The specialization of these relations to integral values of $a_0, a_1, a_2 \ldots$ yields

$$\begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} = \begin{pmatrix} p_{n-1} & p_{n-2} \\ q_{n-1} & q_{n-2} \end{pmatrix} \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \qquad \text{for } n \geq 0, \tag{21}$$

$$\begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_{n-1} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \qquad \text{for } n \geq -1, \tag{22}$$

$$[a_0, \ldots, a_n] = \frac{p_n}{q_n} \qquad \text{for } n \geq 0$$

and

$$p_n q_{n-1} - p_{n-1} q_n = (-1)^{n+1} \qquad \text{for } n \geq -1. \tag{23}$$

From (23), it follows that for $n \geq 0$, the fraction p_n/q_n is in lowest terms: $\gcd(p_n, q_n) = 1$.

Transposing (22) yields, for $n \geq -1$,

$$\begin{pmatrix} p_n & q_n \\ p_{n-1} & q_{n-1} \end{pmatrix} = \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_{n-1} & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix}$$

from which we deduce, for $n \geq 1$,

$$[a_n, \ldots, a_0] = \frac{p_n}{p_{n-1}} \quad \text{and} \quad [a_n, \ldots, a_1] = \frac{q_n}{q_{n-1}}$$

Lemma 24. *For $n \geq 0$,*

$$p_n q_{n-2} - p_{n-2} q_n = (-1)^n a_n.$$

Proof. We multiply both sides of (21) on the left by the inverse of the matrix

$$\begin{pmatrix} p_{n-1} & p_{n-2} \\ q_{n-1} & q_{n-2} \end{pmatrix} \quad \text{which is} \quad (-1)^n \begin{pmatrix} q_{n-2} & -p_{n-2} \\ -q_{n-1} & p_{n-1} \end{pmatrix}.$$

We get

$$(-1)^n \begin{pmatrix} p_n q_{n-2} - p_{n-2} q_n & p_{n-1} q_{n-2} - p_{n-2} q_{n-1} \\ -p_n q_{n-1} + p_{n-1} q_n & 0 \end{pmatrix} = \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix}$$

□

2.2.1 Finite simple continued fraction of a rational number

Let u_0 and u_1 be two integers with u_1 positive. The first step in Euclid's algorithm to find the gcd of u_0 and u_1 consists in dividing u_0 by u_1:

$$u_0 = a_0 u_1 + u_2$$

with $a_0 \in \mathbf{Z}$ and $0 \leq u_2 < u_1$. This means

$$\frac{u_0}{u_1} = a_0 + \frac{u_2}{u_1},$$

which amonts to dividing the rational number $x_0 = u_0/u_1$ by 1 with quotient a_0 and remainder $u_2/u_1 < 1$. This algorithms continues with

$$u_m = a_m u_{m+1} + u_{m+2},$$

where a_m is the integral part of $x_m = u_m/u_{m+1}$ and $0 \leq u_{m+2} < u_{m+1}$, until some $u_{\ell+2}$ is 0, in which case the algorithms stops with

$$u_\ell = a_\ell u_{\ell+1}.$$

Since the gcd of u_m and u_{m+1} is the same as the gcd of u_{m+1} and u_{m+2}, it follows that the gcd of u_0 and u_1 is $u_{\ell+1}$. This is how one gets the regular continued fraction expansion $x_0 = [a_0, a_1, \ldots, a_\ell]$, where $\ell = 0$ in case x_0 is a rational integer, while $a_\ell \geq 2$ if x_0 is a rational number which is not an integer.

Exercise 2. *Compare with the geometrical construction of the continued fraction given in the beamer presentation.*
Give a variant of this geometrical construction where rectangles are replaced by segments.

Proposition 25. *Any finite regular continued fraction*

$$[a_0, a_1, \dots, a_n],$$

where $a_0, a_1, \dots, a_n$ are rational numbers with $a_i \geq 2$ for $1 \leq i \leq n$ and $n \geq 0$, represents a rational number. Conversely, any rational number x has two representations as a continued fraction, the first one, given by Euclid's algorithm, is

$$x = [a_0, a_1, \dots, a_n]$$

and the second one is

$$x = [a_0, a_1, \dots, a_{n-1}, a_n - 1, 1].$$

If $x \in \mathbf{Z}$, then $n = 0$ and the two simple continued fractions representations of x are $[x]$ and $[x-1, 1]$, while if x is not an integer, then $n \geq 1$ and $a_n \geq 2$. For instance the two continued fractions of 1 are $[1]$ and $[0, 1]$, they both end with 1. The two continued fractions of 0 are $[0]$ and $[-1, 1]$, the first of which is the unique continued fraction which ends with 0.

We shall use later (in the proof of Lemma 30 in § 3.2) the fact that any rational number has one simple continued fraction expansion with an odd number of terms and one with an even number of terms.

2.2.2 Infinite simple continued fraction of an irrational number

Given a rational integer a_0 and an infinite sequence of positive integers $a_1, a_2, \dots$, the continued fraction

$$[a_0, a_1, \dots, a_n, \dots]$$

represents an irrational number. Conversely, given an irrational number x, there is a unique representation of x as an infinite simple continued fraction

$$x = [a_0, a_1, \dots, a_n, \dots]$$

Definitions The numbers a_n are the *partial quotients*, the rational numbers

$$\frac{p_n}{q_n} = [a_0, a_1, \dots, a_n]$$

are the *convergents* (in French *réduites*), and the numbers

$$x_n = [a_n, a_{n+1}, \ldots]$$

are the *complete quotients.*

From these definitions we deduce, for $n \geq 0$,

$$x = [a_0, a_1, \ldots, a_n, x_{n+1}] = \frac{x_{n+1}p_n + p_{n-1}}{x_{n+1}q_n + q_{n-1}}. \tag{26}$$

Lemma 27. *For $n \geq 0$,*

$$q_n x - p_n = \frac{(-1)^n}{x_{n+1}q_n + q_{n-1}}.$$

Proof. From (26) one deduces

$$x - \frac{p_n}{q_n} = \frac{x_{n+1}p_n + p_{n-1}}{x_{n+1}q_n + q_{n-1}} - \frac{p_n}{q_n} = \frac{(-1)^n}{(x_{n+1}q_n + q_{n-1})q_n}.$$

□

Corollary 28. *For $n \geq 0$,*

$$\frac{1}{q_{n+1} + q_n} < |q_n x - p_n| < \frac{1}{q_{n+1}}.$$

Proof. Since a_{n+1} is the integral part of x_{n+1}, we have

$$a_{n+1} < x_{n+1} < a_{n+1} + 1.$$

Using the recurrence relation $q_{n+1} = a_{n+1}q_n + q_{n-1}$, we deduce

$$q_{n+1} < x_{n+1}q_n + q_{n-1} < a_{n+1}q_n + q_{n-1} + q_n = q_{n+1} + q_n.$$

□

In particular, since $x_{n+1} > a_{n+1}$ and $q_{n-1} > 0$, one deduces from Lemma 27

$$\frac{1}{(a_{n+1} + 2)q_n^2} < \left| x - \frac{p_n}{q_n} \right| < \frac{1}{a_{n+1}q_n^2}. \tag{29}$$

Therefore any convergent p/q of x satisfies $|x - p/q| < 1/q^2$ (compare with (i) $\Rightarrow$ (v) in Proposition 60). Moreover, if a_{n+1} is large, then the approximation p_n/q_n is sharp. Hence, large partial quotients yield good rational approximations by truncating the continued fraction expansion just before the given partial quotient.

2.3 Continued fractions and cryptography

We refer to section 6 of the course *Cryptoalgomaple* by Abderrahmane Nitaj for a connection between continued fractions and cryptanalysis:

`http://www.math.unicaen.fr/~nitaj/cimpamaure/Documents.htm`

Cryptanalyse de RSA par les Fractions Continues
Les fractions continues
Définitions et propriétés
Cryptanalyse de RSA par les fractions continues
L'attaque de Wiener.

3 Continued fractions and Pell's Equation

3.1 The main lemma

The theory which follows is well–known (a classical reference is the book [11] by O. Perron), but the point of view which we develop here is slightly different from most classical texts on the subject. We follow [1, 2, 14]. An important role in our presentation of the subject is the following result (Lemma 4.1 in [12]).

Lemma 30. *Let $\epsilon = \pm 1$ and let a, b, c, d be rational integers satisfying*

$$ad - bc = \epsilon$$

and $d \geq 1$. Then there is a unique finite sequence of rational integers $a_0, \ldots, a_s$ with $s \geq 1$ and $a_1, \ldots, a_{s-1}$ positive, such that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_s & 1 \\ 1 & 0 \end{pmatrix} \tag{31}$$

These integers are also characterized by

$$\frac{b}{d} = [a_0, a_1, \ldots, a_{s-1}], \quad \frac{c}{d} = [a_s, \ldots, a_1], \quad (-1)^{s+1} = \epsilon. \tag{32}$$

For instance, when $d = 1$, for b and c rational integers,

$$\begin{pmatrix} bc+1 & b \\ c & 1 \end{pmatrix} = \begin{pmatrix} b & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} c & 1 \\ 1 & 0 \end{pmatrix}$$

and

$$\begin{pmatrix} bc-1 & b \\ c & 1 \end{pmatrix} = \begin{pmatrix} b-1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} c-1 & 1 \\ 1 & 0 \end{pmatrix}.$$

Proof. We start with unicity. If $a_0, \dots, a_s$ satisfy the conclusion of Lemma 30, then by using (31), we find $b/d = [a_0, a_1, \dots, a_{s-1}]$. Taking the transpose, we also find $c/d = [a_s, \dots, a_1]$. Next, taking the determinant, we obtain $(-1)^{s+1} = \epsilon$. The last equality fixes the parity of s, and each of the rational numbers b/d, c/d has a unique continued fraction expansion whose length has a given parity (cf. Proposition 25). This proves the unicity of the factorisation when it exists.

For the existence, we consider the simple continued fraction expansion of c/d with length of parity given by the last condition in (32), say $c/d = [a_s, \dots, a_1]$. Let a_0 be a rational integer such that the distance between b/d and $[a_0, a_1, \dots, a_{s-1}]$ is $\leq 1/2$. Define a', b', c', d' by

$$\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_s & 1 \\ 1 & 0 \end{pmatrix}.$$

We have

$$d' > 0, \quad a'd' - b'c' = \epsilon, \quad \frac{c'}{d'} = [a_s, \dots, a_1] = \frac{c}{d}$$

and

$$\frac{b'}{d'} = [a_0, a_1, \dots, a_{s-1}], \quad \left| \frac{b'}{d'} - \frac{b}{d} \right| \leq \frac{1}{2}.$$

From $\gcd(c, d) = \gcd(c', d') = 1$, $c/d = c'/d'$ and $d > 0$, $d' > 0$ we deduce $c' = c$, $d' = d$. From the equality between the determinants we deduce $a' = a + kc$, $b' = b + kd$ for some $k \in \mathbf{Z}$, and from

$$\frac{b'}{d'} - \frac{b}{d} = k$$

we conclude $k = 0$, $(a', b', c', d') = (a, b, c, d)$. Hence (31) follows.

□

Corollary 33. *Assume the hypotheses of Lemma 30 are satisfied.*
a) If $c > d$, then $a_s \geq 1$ and

$$\frac{a}{c} = [a_0, a_1, \dots, a_s].$$

b) If $b > d$, then $a_0 \geq 1$ and

$$\frac{a}{b} = [a_s, \dots, a_1, a_0].$$

The following examples show that the hypotheses of the corollary are not superfluous:

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} b & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

$$\begin{pmatrix} b-1 & b \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} b-1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

and

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

Proof of Corollary 33. Any rational number $u/v > 1$ has two continued fractions. One of them starts with 0 only if $u/v = 1$ and the continued fraction is $[0, 1]$. Hence the assumption $c > d$ implies $a_s > 0$. This proves part a), and part b) follows by transposition (or repeating the proof). □

Another consequence of Lemma 30 is the following classical result (Satz 13 p. 47 of [11]).

Corollary 34. *Let a, b, c, d be rational integers with $ad - bc = \pm 1$ and $c > d > 0$. Let x and y be two irrational numbers satisfying $y > 1$ and*

$$x = \frac{ay + b}{cy + d}.$$

Let $x = [a_0, a_1, \ldots]$ be the simple continued fraction expansion of x. Then there exists $s \geq 1$ such that

$$a = p_s, \quad b = p_{s-1}, \quad c = q_s, \quad r = q_{s-1}, \quad y = x_{s+1}.$$

Proof. Using lemma 30, we write

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a'_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a'_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a'_s & 1 \\ 1 & 0 \end{pmatrix}$$

with $a'_1, \ldots, a'_{s-1}$ positive and

$$\frac{b}{d} = [a'_0, a'_1, \ldots, a'_{s-1}], \quad \frac{c}{d} = [a'_s, \ldots, a'_1].$$

From $c > d$ and corollary 33, we deduce $a'_s > 0$ and

$$\frac{a}{c} = [a'_0, a'_1, \ldots, a'_s] = \frac{p'_s}{q'_s}, \quad x = \frac{p'_s y + p'_{s-1}}{q'_s y + q'_{s-1}} = [a'_0, a'_1, \ldots, a'_s, y].$$

Since $y > 1$, it follows that $a'_i = a_i$, $p'_i = q'_i$ for $0 \leq i \leq s$ and $y = x_{s+1}$.

□

Remark.
In [6], § 4, there is a variant of the matrix formula (21) for the simple continued fraction of a real number.

Given integers $a_0, a_1, \ldots$ with $a_i > 0$ for $i \geq 1$ and writing, for $n \geq 0$, as usual, $p_n/q_n = [a_0, a_1, \ldots, a_n]$, one checks, by induction on n, the two formulae

$$\left.\begin{array}{ll} \begin{pmatrix} 1 & a_0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ a_1 & 1 \end{pmatrix} \cdots \begin{pmatrix} 1 & a_n \\ 0 & 1 \end{pmatrix} & = \begin{pmatrix} p_{n-1} & p_n \\ q_{n-1} & q_n \end{pmatrix} \quad \text{if } n \text{ is even} \\ \begin{pmatrix} 1 & a_0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ a_1 & 1 \end{pmatrix} \cdots \begin{pmatrix} 1 & 0 \\ a_n & 1 \end{pmatrix} & = \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} \quad \text{if } n \text{ is odd} \end{array}\right\} \tag{35}$$

Define two matrices U (up) and L (low) in $\mathrm{GL}_2(\mathbf{R})$ of determinant $+1$ by

$$U = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad L = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

For p and q in $\mathbf{Z}$, we have

$$U^p = \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad L^q = \begin{pmatrix} 1 & 0 \\ q & 1 \end{pmatrix},$$

so that these formulae (35) are

$$U^{a_0} L^{a_1} \cdots U^{a_n} = \begin{pmatrix} p_{n-1} & p_n \\ q_{n-1} & q_n \end{pmatrix} \quad \text{if } n \text{ is even}$$

and

$$U^{a_0} L^{a_1} \cdots L^{a_n} = \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} \quad \text{if } n \text{ is odd.}$$

The connexion with Euclid's algorithm is

$$U^{-p} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a - pc & b - pd \\ c & d \end{pmatrix} \quad \text{and} \quad L^{-q} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c - qa & d - qb \end{pmatrix}.$$

The corresponding variant of Lemma 30 is also given in [6], § 4: *If a, b, c, d are rational integers satisfying $b > a > 0$, $d > c \geq 0$ and $ad - bc = 1$, then there exist rational integers $a_0, \ldots, a_n$ with n even and $a_1, \ldots, a_n$ positive, such that*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & a_0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ a_1 & 1 \end{pmatrix} \cdots \begin{pmatrix} 1 & a_n \\ 0 & 1 \end{pmatrix}$$

These integers are uniquely determined by $b/d = [a_0, \ldots, a_n]$ with n even.

3.2 Simple Continued fraction of $\sqrt{D}$

An infinite sequence $(a_n)_{n\geq 1}$ is *periodic* if there exists a positive integer s such that

$$a_{n+s} = a_n \quad \text{for all } n \geq 1. \tag{36}$$

In this case, the finite sequence $(a_1, \ldots, a_s)$ is called a *period* of the original sequence. For the sake of notation, we write

$$(a_1, a_2, \ldots) = (\overline{a_1, \ldots, a_s}).$$

If s_0 is the smallest positive integer satisfying (36), then the set of s satisfying (36) is the set of positive multiples of s_0. In this case $(a_1, \ldots, a_{s_0})$ is called *the fundamental period* of the original sequence.

Theorem 37. *Let D be a positive integer which is not a square. Write the simple continued fraction of $\sqrt{D}$ as $[a_0, a_1, \ldots]$ with $a_0 = \lfloor \sqrt{D} \rfloor$.*
a) The sequence $(a_1, a_2, \ldots)$ is periodic.
b) Let (x, y) be a positive integer solution to Pell's equation $x^2 - Dy^2 = \pm 1$. Then there exists $s \geq 1$ such that $x/y = [a_0, \ldots, a_{s-1}]$ and

$$(a_1, a_2, \ldots, a_{s-1}, 2a_0)$$

is a period of the sequence $(a_1, a_2, \ldots)$. Further, $a_{s-i} = a_i$ for $1 \leq i \leq s-1$. One says that the word $a_1, \ldots, a_{s-1}$ is a palindrome. [5]
c) Let $(a_1, a_2, \ldots, a_{s-1}, 2a_0)$ be a period of the sequence $(a_1, a_2, \ldots)$. Set $x/y = [a_0, \ldots, a_{s-1}]$. Then $x^2 - Dy^2 = (-1)^s$.
d) Let s_0 be the length of the fundamental period. Then for $i \geq 0$ not multiple of s_0, we have $a_i \leq a_0$.

If $(a_1, a_2, \ldots, a_{s-1}, 2a_0)$ is a period of the sequence $(a_1, a_2, \ldots)$, then

$$\sqrt{D} = [a_0, \overline{a_1, \ldots, a_{s-1}, 2a_0}] = [a_0, a_1, \ldots, a_{s-1}, a_0 + \sqrt{D}].$$

[5] Note (2016). As kindly pointed out to me by Yoishi Motohashi, the fact that the word $a_1, \ldots, a_{s-1}$ is a palindrom is proved in 'Essai sur la théorie des nombres' by Legendre (1798).
In his first paper published at the age of 17 by Evariste Galois, it is proved that if the expansion of a quadratic irrational α is purely periodic, then the same is true for the conjugate α' of α, and the continued fraction of α' is obtained by reversing the order of the continued fraction of α. Besides, this continued fraction is a palindrom if and only if $\alpha\alpha' = -1$.
É. Galois, *Démonstration d'un théorème sur les fractions continues périodiques.*
Annales de Mathématiques Pures et Appliquées, **19** (1828-1829), p. 294-301.
`http://archive.numdam.org/article/AMPA_1828-1829__19__294_0.pdf`
For more information on these contributions by Galois, see
`https://www.bibnum.education.fr/mathematiques/algebre/demonstration-d-un-theoreme-sur-les-fractions-continues-periodiques`

Consider the fundamental period $(a_1, a_2, \ldots, a_{s_0-1}, a_{s_0})$ of the sequence $(a_1, a_2, \ldots)$. By part b) of Theorem 37 we have $a_{s_0} = 2a_0$, and by part d), it follows that s_0 is the smallest index i such that $a_i > a_0$.

From b) and c) in Theorem 37, it follows that the fundamental solution (x_1, y_1) to Pell's equation $x^2 - Dy^2 = \pm 1$ is given by $x_1/y_1 = [a_0, \ldots, a_{s_0-1}]$, and that $x_1^2 - Dy_1^2 = (-1)^{s_0}$. Therefore, if s_0 is even, then there is no solution to the Pell's equation $x^2 - Dy^2 = -1$. If s_0 is odd, then (x_1, y_1) is the fundamental solution to Pell's equation $x^2 - Dy^2 = -1$, while the fundamental solution (x_2, y_2) to Pell's equation $x^2 - Dy^2 = 1$ is given by $x_2/y_2 = [a_0, \ldots, a_{2s-1}]$.

It follows also from Theorem 37 that the $(ns_0 - 1)$-th convergent

$$x_n/y_n = [a_0, \ldots, a_{ns_0-1}]$$

satisfies

$$x_n + y_n\sqrt{D} = (x_1 + y_1\sqrt{D})^n. \tag{38}$$

We shall check this relation directly (Lemma 42).

Proof. Start with a positive solution (x, y) to Pell's equation $x^2 - Dy^2 = \pm 1$, which exists according to Proposition 61. Since $Dy \geq x$ and $x > y$, we may use lemma 30 and corollary 33 with

$$a = Dy, \quad b = c = x, \quad d = y$$

and write

$$\begin{pmatrix} Dy & x \\ x & y \end{pmatrix} = \begin{pmatrix} a'_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a'_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a'_s & 1 \\ 1 & 0 \end{pmatrix} \tag{39}$$

with positive integers $a'_0, \ldots, a'_s$ and with $a'_0 = \lfloor \sqrt{D} \rfloor$. Then the continued fraction expansion of Dy/x is $[a'_0, \ldots, a'_s]$ and the continued fraction expansion of x/y is $[a'_0, \ldots, a'_{s-1}]$.

Since the matrix on the left hand side of (39) is symmetric, the word $a'_0, \ldots, a'_s$ is a palindrome. In particular $a'_s = a'_0$.

Consider the periodic continued fraction

$$\delta = [a'_0, \overline{a'_1, \ldots, a'_{s-1}, 2a'_0}].$$

This number δ satisfies

$$\delta = [a'_0, a'_1, \ldots, a'_{s-1}, a'_0 + \delta].$$

Using the inverse of the matrix

$$\begin{pmatrix} a_0' & 1 \\ 1 & 0 \end{pmatrix} \quad \text{which is} \quad \begin{pmatrix} 0 & 1 \\ 1 & -a_0' \end{pmatrix},$$

we write

$$\begin{pmatrix} a_0' + \delta & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} a_0' & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \delta & 1 \end{pmatrix}$$

Hence the product of matrices associated with the continued fraction of δ

$$\begin{pmatrix} a_0' & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1' & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_{s-1}' & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_0' + \delta & 1 \\ 1 & 0 \end{pmatrix}$$

is

$$\begin{pmatrix} Dy & x \\ x & y \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \delta & 1 \end{pmatrix} = \begin{pmatrix} Dy + \delta x & x \\ x + \delta y & y \end{pmatrix}.$$

It follows that

$$\delta = \frac{Dy + \delta x}{x + \delta y},$$

hence $\delta^2 = D$. As a consequence, $a_i' = a_i$ for $0 \leq i \leq s-1$ while $a_s' = a_0$, $a_s = 2a_0$.

This proves that if (x, y) is a non–trivial solution to Pell's equation $x^2 - Dy^2 = \pm 1$, then the continued fraction expansion of $\sqrt{D}$ is of the form

$$\sqrt{D} = [a_0, \overline{a_1, \ldots, a_{s-1}, 2a_0}] \tag{40}$$

with $a_1, \ldots, a_{s-1}$ a palindrome, and x/y is given by the convergent

$$x/y = [a_0, a_1, \ldots, a_{s-1}]. \tag{41}$$

Consider a convergent $p_n/q_n = [a_0, a_1, \ldots, a_n]$. If $a_{n+1} = 2a_0$, then (29) with $x = \sqrt{D}$ implies the upper bound

$$\left| \sqrt{D} - \frac{p_n}{q_n} \right| \leq \frac{1}{2a_0 q_n^2},$$

and it follows from Proposition 62 that (p_n, q_n) is a solution to Pell's equation $p_n^2 - Dq_n^2 = \pm 1$. This already shows that $a_i < 2a_0$ when $i+1$ is not the length of a period. We refine this estimate to $a_i \leq a_0$.

Assume $a_{n+1} \geq a_0 + 1$. Since the sequence $(a_m)_{m \geq 1}$ is periodic of period length s_0, for any m congruent to n modulo s_0, we have $a_{m+1} > a_0$. For these m we have

$$\left| \sqrt{D} - \frac{p_m}{q_m} \right| \leq \frac{1}{(a_0 + 1) q_m^2}.$$

For sufficiently large m congruent to n modulo s we have

$$(a_0+1)q_m^2 > q_m^2\sqrt{D}+1.$$

Proposition 62 implies that (p_m, q_m) is a solution to Pell's equation $p_m^2 - Dq_m^2 = \pm 1$. Finally, Theorem 37 implies that $m+1$ is a multiple of s_0, hence $n+1$ also.

□

3.3 Connection between the two formulae for the n-th positive solution to Pell's equation

Lemma 42. *Let D be a positive integer which is not a square. Consider the simple continued fraction expansion $\sqrt{D} = [a_0, \overline{a_1, \ldots, a_{s_0-1}, 2a_0}]$ where s_0 is the length of the fundamental period. Then the fundamental solution (x_1, y_1) to Pell's equation $x^2 - Dy^2 = \pm 1$ is given by the continued fraction expansion $x_1/y_1 = [a_0, a_1, \ldots, a_{s_0-1}]$. Let $n \geq 1$ be a positive integer. Define (x_n, y_n) by $x_n/y_n = [a_0, a_1, \ldots, a_{ns_0-1}]$. Then $x_n + y_n\sqrt{D} = (x_1 + y_1\sqrt{D})^n$.*

This result is a consequence of the two formulae we gave for the n-th solution (x_n, y_n) to Pell's equation $x^2 - Dy^2 = \pm 1$. We check this result directly.

Proof. From Lemma 30 and relation (39), one deduces

$$\begin{pmatrix} Dy_n & x_n \\ x_n & y_n \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_{ns_0-1} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Since

$$\begin{pmatrix} Dy_n & x_n \\ x_n & y_n \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -a_0 \end{pmatrix} = \begin{pmatrix} x_n & Dy_n - a_0x_n \\ y_n & x_n - a_0y_n \end{pmatrix},$$

we obtain

$$\begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_{ns_0-1} & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} x_n & Dy_n - a_0x_n \\ y_n & x_n - a_0y_n \end{pmatrix}. \qquad (43)$$

Notice that the determinant is $(-1)^{ns_0} = x_n^2 - Dy_n^2$. Formula (43) for $n+1$ and the periodicity of the sequence $(a_1, \ldots, a_n, \ldots)$ with $a_{s_0} = 2a_0$ give :

$$\begin{pmatrix} x_{n+1} & Dy_{n+1} - a_0x_{n+1} \\ y_{n+1} & x_{n+1} - a_0y_{n+1} \end{pmatrix} = \begin{pmatrix} x_n & Dy_n - a_0x_n \\ y_n & x_n - a_0y_n \end{pmatrix} \begin{pmatrix} 2a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_{s_0-1} & 1 \\ 1 & 0 \end{pmatrix}.$$

Take first $n = 1$ in (43) and multiply on the left by

$$\begin{pmatrix} 2a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -a_0 \end{pmatrix} = \begin{pmatrix} 1 & a_0 \\ 0 & 1 \end{pmatrix}.$$

Since

$$\begin{pmatrix} 1 & a_0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 & Dy_1 - a_0x_1 \\ y_1 & x_1 - a_0y_1 \end{pmatrix} = \begin{pmatrix} x_1 + a_0y_1 & (D - a_0^2)y_1 \\ y_1 & x_1 - a_0y_1 \end{pmatrix}.$$

we deduce

$$\begin{pmatrix} 2a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_{s_0-1} & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} x_1 + a_0y_1 & (D - a_0^2)y_1 \\ y_1 & x_1 - a_0y_1 \end{pmatrix}.$$

Therefore

$$\begin{pmatrix} x_{n+1} & Dy_{n+1} - a_0x_{n+1} \\ y_{n+1} & x_{n+1} - a_0y_{n+1} \end{pmatrix} = \begin{pmatrix} x_n & Dy_n - a_0x_n \\ y_n & x_n - a_0y_n \end{pmatrix} \begin{pmatrix} x_1 + a_0y_1 & (D - a_0^2)y_1 \\ y_1 & x_1 - a_0y_1 \end{pmatrix}.$$

The first column gives

$$x_{n+1} = x_nx_1 + Dy_ny_1 \qquad \text{and} \qquad y_{n+1} = x_1y_n + x_ny_1,$$

which was to be proved.

□

3.4 Examples of simple continued fractions

The three first examples below are special cases of results initiated by O. Perron [11] and related with real quadratic fields of Richaud-Degert type.

Example 1. Take $D = a^2b^2 + 2b$ where a and b are positive integers. A solution to

$$x^2 - (a^2b^2 + 2b)y^2 = 1$$

is $(x, y) = (a^2b + 1, a)$. As we shall see, this is related with the continued fraction expansion of $\sqrt{D}$ which is

$$\sqrt{a^2b^2 + 2b} = [ab, \overline{a, 2ab}]$$

since

$$t = \sqrt{a^2b^2 + 2b} \Longleftrightarrow t = ab + \cfrac{1}{a + \cfrac{1}{t + ab}}.$$

This includes the examples $D = a^2 + 2$ (take $b = 1$) and $D = b^2 + 2b$ (take $a = 1$). For $a = 1$ and $b = c - 1$, this includes the example $D = c^2 - 1$.

Example 2. Take $D = a^2b^2 + b$ where a and b are positive integers. A solution to

$$x^2 - (a^2b^2 + b)y^2 = 1$$

is $(x, y) = (2a^2b + 1, 2a)$. The continued fraction expansion of $\sqrt{D}$ is

$$\sqrt{a^2b^2 + b} = [ab, \overline{2a, 2ab}]$$

since

$$t = \sqrt{a^2b^2 + b} \Longleftrightarrow t = ab + \frac{1}{2a + \dfrac{1}{t + ab}}\cdot$$

This includes the example $D = b^2 + b$ (take $a = 1$).

The case $b = 1$, $D = a^2 + 1$ is special: there is an integer solution to

$$x^2 - (a^2 + 1)y^2 = -1,$$

namely $(x, y) = (a, 1)$. The continued fraction expansion of $\sqrt{D}$ is

$$\sqrt{a^2 + 1} = [a, \overline{2a}]$$

since

$$t = \sqrt{a^2 + 1} \Longleftrightarrow t = a + \frac{1}{t + a}\cdot$$

Example 3. Let a and b be two positive integers such that $b^2 + 1$ divides $2ab + 1$. For instance $b = 2$ and $a \equiv 1 \pmod 5$. Write $2ab + 1 = k(b^2 + 1)$ and take $D = a^2 + k$. The continued fraction expansion of $\sqrt{D}$ is

$$[a, \overline{b, b, 2a}]$$

since $t = \sqrt{D}$ satisfies

$$t = a + \frac{1}{b + \dfrac{1}{b + \dfrac{1}{a + t}}} = [a, b, b, a + t].$$

A solution to $x^2 - Dy^2 = -1$ is $x = ab^2 + a + b$, $y = b^2 + 1$.

In the case $a = 1$ and $b = 2$ (so $k = 1$), the continued fraction has period length 1 only:

$$\sqrt{5} = [1, \overline{2}].$$

Example 4. Integers which are *Polygonal numbers* in two ways are given by the solutions to quadratic equations.

Triangular numbers are numbers of the form

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2} \quad \text{for } n \geq 1;$$

their sequence starts with

1, 3, 6, 10, 15, 21, 28, 36, 45, 55, 66, 78, 91, 105, 120, 136, 153, 171, ...

`http://www.research.att.com/~njas/sequences/A000217`.

Square numbers are numbers of the form

$$1 + 3 + 5 + \cdots + (2n+1) = n^2 \quad \text{for } n \geq 1;$$

their sequence starts with

1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144, 169, 196, 225, 256, 289, ...

`http://www.research.att.com/~njas/sequences/A000290`.

Pentagonal numbers are numbers of the form

$$1 + 4 + 7 + \cdots + (3n+1) = \frac{n(3n-1)}{2} \quad \text{for } n \geq 1;$$

their sequence starts with

1, 5, 12, 22, 35, 51, 70, 92, 117, 145, 176, 210, 247, 287, 330, 376, 425, ...

`http://www.research.att.com/~njas/sequences/A000326`.

Hexagonal numbers are numbers of the form

$$1 + 5 + 9 + \cdots + (4n+1) = n(2n-1) \quad \text{for } n \geq 1;$$

their sequence starts with

1, 6, 15, 28, 45, 66, 91, 120, 153, 190, 231, 276, 325, 378, 435, 496, 561, ...

`http://www.research.att.com/~njas/sequences/A000384`.

For instance, numbers which are at the same time triangular and squares are the numbers y^2 where (x, y) is a solution to Pell's equation with $D = 8$. Their list starts with

$$0, 1, 36, 1225, 41616, 1413721, 48024900, 1631432881, 55420693056, \ldots$$

See `http://www.research.att.com/~njas/sequences/A001110`.

Example 5. Integer rectangle triangles having sides of the right angle as consecutive integers a and $a+1$ have an hypothenuse c which satisfies $a^2+(a+1)^2=c^2$. The admissible values for the hypothenuse is the set of positive integer solutions y to Pell's equation $x^2-2y^2=-1$. The list of these hypothenuses starts with

$$1, 5, 29, 169, 985, 5741, 33461, 195025, 1136689, 6625109, 38613965,$$

See `http://www.research.att.com/~njas/sequences/A001653`.

3.5 Records

For large D, Pell's equation may obviously have small integer solutions. Examples are

for $D=m^2-1$ with $m\geq 2$, the numbers $x=m$, $y=1$ satisfy $x^2-Dy^2=1$,

for $D=m^2+1$ with $m\geq 1$, the numbers $x=m$, $y=1$ satisfy $x^2-Dy^2=-1$,

for $D=m^2\pm m$ with $m\geq 2$, the numbers $x=2m\pm 1$, $y=2$ satisfy $x^2-Dy^2=1$,

for $D=t^2m^2+2m$ with $m\geq 1$ and $t\geq 1$, the numbers $x=t^2m+1$, $y=t$ satisfy $x^2-Dy^2=1$.

On the other hand, relatively small values of D may lead to large fundamental solutions. Tables are available on the internet[6].

For D a positive integer which is not a square, denote by $S(D)$ the base 10 logarithm of x_1, when (x_1,y_1) is the fundamental solution to $x^2-Dy^2=1$. The number of decimal digits of the fundamental solution x_1 is the integral part of $S(D)$ plus 1. For instance, when $D=61$, the fundamental solution (x_1,y_1) is

$$x_1=1\,766\,319\,049, \quad y_1=226\,153\,980$$

and $S(61)=\log_{10} x_1=9.247\,069\ldots$

An integer D is a *record holder* for S if $S(D')<S(D)$ for all $D'<D$.

Here are the record holders up to 1021:

D	2	5	10	13	29	46	53	61	109
$S(D)$	0.477	0.954	1.278	2.812	3.991	4.386	4.821	9.247	14.198

[6]For instance:
Tomás Oliveira e Silva: Record-Holder Solutions of Pell's Equation
`http://www.ieeta.pt/~tos/pell.html`.

D	181	277	397	409	421	541	661	1021
$S(D)$	18.392	20.201	20.923	22.398	33.588	36.569	37.215	47.298

Some further records with number of digits successive powers of 10:

D	3061	169789	12765349	1021948981	85489307341
$S(D)$	104.051	1001.282	10191.729	100681.340	1003270.151

3.6 Periodic continued fractions

An infinite sequence $(a_n)_{n\geq 0}$ is said to be *ultimately periodic* if there exists $n_0 \geq 0$ and $s \geq 1$ such that

$$a_{n+s} = a_n \quad \text{for all } n \geq n_0. \tag{44}$$

The set of s satisfying this property (3.6) is the set of positive multiples of an integer s_0, and $(a_{n_0}, a_{n_0+1}, \ldots, a_{n_0+s_0-1})$ is called *the fundamental period*.

A continued fraction with a sequence of partial quotients satisfying (44) will be written

$$[a_0, a_1, \ldots, a_{n_0-1}, \overline{a_{n_0}, \ldots, a_{n_0+s-1}}].$$

Example. For D a positive integer which is not a square, setting $a_0 = \lfloor \sqrt{D} \rfloor$, we have by Theorem 37

$$a_0 + \sqrt{D} = [\overline{2a_0, a_1, \ldots, a_{s-1}}] \quad \text{and} \quad \frac{1}{\sqrt{D} - a_0} = [\overline{a_1, \ldots, a_{s-1}, 2a_0}].$$

Lemma 45 (Euler 1737)**.** *If an infinite continued fraction*

$$x = [a_0, a_1, \ldots, a_n, \ldots]$$

is ultimately periodic, then x is a quadratic irrational number.

Proof. Since the continued fraction of x is infinite, x is irrational. Assume first that the continued fraction is periodic, namely that (44) holds with $n_0 = 0$:

$$x = [\overline{a_0, \ldots, a_{s-1}}].$$

This can be written

$$x = [a_0, \ldots, a_{s-1}, x].$$

Hence

$$x = \frac{p_{s-1}x + p_{s-2}}{q_{s-1}x + q_{s-2}}.$$

It follows that

$$q_{s-1}X^2 + (q_{s-2} - p_{s-1})X - p_{s-2}$$

is a non–zero quadratic polynomial with integer coefficients having x as a root. Since x is irrational, this polynomial is irreducible and x is quadratic.

In the general case where (44) holds with $n_0 > 0$, we write

$$x = [a_0, a_1, \ldots, a_{n_0-1}, \overline{a_{n_0}, \ldots, a_{n_0+s-1}}] = [a_0, a_1, \ldots, a_{n_0-1}, y],$$

where $y = [\overline{a_{n_0}, \ldots, a_{n_0+s-1}}]$ is a periodic continued fraction, hence is quadratic. But

$$x = \frac{p_{n_0-1}y + p_{n_0-2}}{q_{n_0-1}y + q_{n_0-2}},$$

hence $x \in \mathbf{Q}(y)$ is also quadratic irrational.

□

Lemma 46 (Lagrange, 1770)**.** *If x is a quadratic irrational number, then its continued fraction*

$$x = [a_0, a_1, \ldots, a_n, \ldots]$$

is ultimately periodic.

Proof. For $n \geq 0$, define $d_n = q_n x - p_n$. According to Corollary 28, we have $|d_n| < 1/q_{n+1}$.

Let $AX^2 + BX + C$ with $A > 0$ be an irreducible quadratic polynomial having x as a root. For each $n \geq 2$, we deduce from (26) that the convergent x_n is a root of a quadratic polynomial $A_nX^2 + B_nX + C_n$, with

$$\begin{aligned}
A_n &= Ap_{n-1}^2 + Bp_{n-1}q_{n-1} + Cq_{n-1}^2,\\
B_n &= 2Ap_{n-1}p_{n-2} + B(p_{n-1}q_{n-2} + p_{n-2}q_{n-1}) + 2Cq_{n-1}q_{n-2},\\
C_n &= A_{n-1}.
\end{aligned}$$

Using $Ax^2 + Bx + C = 0$, we deduce

$$\begin{aligned}
A_n &= (2Ax + B)d_{n-1}q_{n-1} + Ad_{n-1}^2,\\
B_n &= (2Ax + B)(d_{n-1}q_{n-2} + d_{n-2}q_{n-1}) + 2Ad_{n-1}d_{n-2}.
\end{aligned}$$

There are similar formulae expressing A, B, C as homogeneous linear combinations of A_n, B_n, C_n, and since $(A, B, C) \neq (0, 0, 0)$, it follows that $(A_n, B_n, C_n) \neq (0, 0, 0)$. Since x_n is irrational, one deduces $A_n \neq 0$.

From the inequalities

$$q_{n-1}|d_{n-2}| < 1, \quad q_{n-2}|d_{n-1}| < 1, \quad q_{n-1} < q_n, \quad |d_{n-1}d_{n-2}| < 1,$$

one deduces

$$\max\{|A_n|,\ |B_n|/2, |C_n|\} < A + |2Ax + B|.$$

This shows that $|A_n|$, $|B_n|$ and $|C_n|$ are bounded independently of n. Therefore there exists $n_0 \geq 0$ and $s > 0$ such that $x_{n_0} = x_{n_0+s}$. From this we deduce that the continued fraction of x_{n_0} is purely periodic, hence the continued fraction of x is ultimately periodic. □

A *reduced quadratic irrational number* is an irrational number $x > 1$ which is a root of a degree 2 polynomial $ax^2 + bx + c$ with rational integer coefficients, such that the other root x' of this polynomial, which is the *Galois conjugate of* x, satisfies $-1 < x' < 0$. If x is reduced, then so is $-1/x'$.

Lemma 47. *A continued fraction*

$$x = [a_0, a_1, \ldots, a_n \ldots]$$

is purely periodic if and only if x is a reduced quadratic irrational number. In this case, if $x = [\overline{a_0, a_1, \ldots, a_{s-1}}]$ and if x' is the Galois conjugate of x, then

$$-1/x' = [\overline{a_{s-1}, \ldots, a_1, a_0}]$$

Proof. Assume first that the continued fraction of x is purely periodic:

$$x = [\overline{a_0, a_1, \ldots, a_{s-1}}].$$

From $a_s = a_0$ we deduce $a_0 > 0$, hence $x > 1$. From $x = [a_0, a_1, \ldots, a_{s-1}, x]$ and the unicity of the continued fraction expansion, we deduce

$$x = \frac{p_{s-1}x + p_{s-2}}{q_{s-1}x + q_{s-2}} \quad \text{and} \quad x = x_s.$$

Therefore x is a root of the quadratic polynomial

$$P_s(X) = q_{s-1}X^2 + (q_{s-2} - p_{s-1})X - p_{s-2}.$$

This polynomial P_s has a positive root, namely $x > 1$, and a negative root x', with the product $xx' = -p_{s-2}/q_{s-1}$. We transpose the relation

$$\begin{pmatrix} p_{s-1} & p_{s-2} \\ q_{s-1} & q_{s-2} \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_{s-1} & 1 \\ 1 & 0 \end{pmatrix}$$

and obtain

$$\begin{pmatrix} p_{s-1} & q_{s-1} \\ p_{s-2} & q_{s-2} \end{pmatrix} = \begin{pmatrix} a_{s-1} & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Define

$$y = [\overline{a_{s-1}, \ldots, a_1, a_0}],$$

so that $y > 1$,

$$y = [a_{s-1}, \ldots, a_1, a_0, y] = \frac{p_{s-1}y + q_{s-1}}{p_{s-2}y + q_{s-2}}$$

and y is the positive root of the polynomial

$$Q_s(X) = p_{s-2}X^2 + (q_{s-2} - p_{s-1})X - q_{s-1}.$$

The polynomials P_s and Q_s are related by $Q_s(X) = -X^2 P_s(-1/X)$. Hence $y = -1/x'$.

For the converse, assume $x > 1$ and $-1 < x' < 0$. Let $(x_n)_{n \geq 1}$ be the sequence of complete quotients of x. For $n \geq 1$, define x'_n as the Galois conjugate of x_n. One deduces by induction that $x'_n = a_n + 1/x'_{n+1}$, that $-1 < x'_n < 0$ (hence x_n is reduced), and that a_n is the integral part of $-1/x'_{n+1}$.

If the continued fraction expansion of x were not purely periodic, we would have

$$x = [a_0, \ldots, a_{h-1}, \overline{a_h, \ldots, a_{h+s-1}}]$$

with $a_{h-1} \neq a_{h+s-1}$. By periodicity we have $x_h = [a_h, \ldots, a_{h+s-1}, x_h]$, hence $x_h = x_{h+s}$, $x'_h = x'_{h+s}$. From $x'_h = x'_{h+s}$, taking integral parts, we deduce $a_{h-1} = a_{h+s-1}$, a contradiction. □

Corollary 48. *If $r > 1$ is a rational number which is not a square, then the continued fraction expansion of $\sqrt{r}$ is of the form*

$$\sqrt{r} = [a_0, \overline{a_1, \ldots, a_{s-1}, 2a_0}]$$

with $a_1, \ldots, a_{s-1}$ a palindrome and $a_0 = \lfloor \sqrt{r} \rfloor$.
Conversely, if the continued fraction expansion of an irrational number $t > 1$ is of the form

$$t = [a_0, \overline{a_1, \ldots, a_{s-1}, 2a_0}]$$

with $a_1, \ldots, a_{s-1}$ a palindrome, then t^2 is a rational number.

Proof. If $t^2 = r$ is rational > 1, then for and $a_0 = \lfloor \sqrt{t} \rfloor$ the number $x = t + a_0$ is reduced. Since $t' + t = 0$, we have

$$-\frac{1}{x'} = \frac{1}{x - 2a_0}.$$

Hence

$$x = [\overline{2a_0, a_1, \ldots, a_{s-1}}], \quad -\frac{1}{x'} = [\overline{a_{s-1}, \ldots, a_1, 2a_0}]$$

and $a_1, \ldots, a_{s-1}$ a palindrome.

Conversely, if $t = [a_0, \overline{a_1, \ldots, a_{s-1}, 2a_0}]$ with $a_1, \ldots, a_{s-1}$ a palindrome, then $x = t + a_0$ is periodic, hence reduced, and its Galois conjugate x' satisfies

$$-\frac{1}{x'} = [\overline{a_1, \ldots, a_{s-1}, 2a_0}] = \frac{1}{x - 2a_0},$$

which means $t + t' = 0$, hence $t^2 \in \mathbf{Q}$. □

Lemma 49 (Serret, 1878)**.** *Let x and y be two irrational numbers with continued fractions*

$$x = [a_0, a_1, \ldots, a_n \ldots] \quad \text{and} \quad y = [b_0, b_1, \ldots, b_m \ldots]$$

respectively. Then the two following properties are equivalent.

(i) *There exists a matrix* $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *with rational integer coefficients and determinant* ± 1 *such that*

$$y = \frac{ax + b}{cx + d}.$$

(ii) *There exists* $n_0 \geq 0$ *and* $m_0 \geq 0$ *such that* $a_{n_0+k} = b_{m_0+k}$ *for all* $k \geq 0$.

Condition (i) means that x *and* y *are equivalent modulo the action of* $\mathrm{GL}_2(\mathbf{Z})$ *by homographies.*

Condition (ii) means that there exists integers n_0, m_0 and a real number $t > 1$ such that

$$x = [a_0, a_1, \ldots, a_{n_0-1}, t] \quad \text{and} \quad y = [b_0, b_1, \ldots, b_{m_0-1}, t].$$

Example.

$$\text{If } x = [a_0, a_1, x_2], \text{ then} \quad -x = \begin{cases} [-a_0 - 1, 1, a_1 - 1, x_2] & \text{if } a_1 \geq 2, \\ [-a_0 - 1, 1 + x_2] & \text{if } a_1 = 1. \end{cases} \tag{50}$$

Proof. We already know by (26) that if x_n is a complete quotient of x, then x and x_n are equivalent modulo $\mathrm{GL}_2(\mathbf{Z})$. Condition (ii) means that there is a partial quotient of x and a partial quotient of y which are equal. By transitivity of the $\mathrm{GL}_2(\mathbf{Z})$ equivalence, (ii) implies (i).

Conversely, assume (i):

$$y = \frac{ax+b}{cx+d}.$$

Let n be a sufficiently large number. From

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} = \begin{pmatrix} u_n & u_{n-1} \\ v_n & v_{n-1} \end{pmatrix}$$

with

$$\begin{aligned} u_n &= ap_n + bq_n, \quad u_{n-1} = ap_{n-1} + bq_{n-1}, \\ v_n &= cp_n + dq_n, \quad v_{n-1} = cp_{n-1} + dq_{n-1}, \end{aligned}$$

we deduce

$$y = \frac{u_n x_{n+1} + u_{n-1}}{v_n x_{n+1} + v_{n-1}}.$$

We have $v_n = (cx+d)q_n + c\delta_n$ with $\delta_n = p_n - q_n x$. We have $q_n \to \infty$, $q_n \geq q_{n-1} + 1$ and $\delta_n \to 0$ as $n \to \infty$. Hence, for sufficiently large n, we have $v_n > v_{n-1} > 0$. From part 1 of Corollary 33, we deduce

$$\begin{pmatrix} u_n & u_{n-1} \\ v_n & v_{n-1} \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_s & 1 \\ 1 & 0 \end{pmatrix}$$

with $a_0, \ldots, a_s$ in $\mathbf{Z}$ and $a_1, \ldots, a_s$ positive. Hence

$$y = [a_0, a_1, \ldots, a_s, x_{n+1}].$$

□

A computational proof of (i) ⇒ (ii). Another proof is given by Bombieri [1] (Theorem A.1 p. 209). He uses the fact that $\mathrm{GL}_2(\mathbf{Z})$ is generated by the two matrices

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

The associated fractional linear transformations are K and J defined by

$$K(x) = x + 1 \quad \text{and} \quad J(x) = 1/x.$$

We have $J^2 = 1$ and

$$K([a_0, t]) = [a_0 + 1, t], \quad K^{-1}([a_0, t]) = [a_0 - 1, t].$$

Also $J([a_0,t]) = [0,a_0,t]$ if $a_0 > 0$ and $J([0,t]) = \lfloor t \rfloor$. According to (50), the continued fractions of x and $-x$ differ only by the first terms. This completes the proof. [7]

□

3.7 Diophantine approximation and simple continued fractions

Lemma 51 (Lagrange, 1770)**.** *The sequence* $(|q_n x - p_n|)_{n\geq 0}$ *is strictly decreasing: for* $n \geq 1$ *we have*

$$|q_n x - p_n| < |q_{n-1} x - p_{n-1}|.$$

Proof. We use Lemma 27 twice: on the one hand

$$|q_n x - p_n| = \frac{1}{x_{n+1} q_n + q_{n-1}} < \frac{1}{q_n + q_{n-1}}$$

because $x_{n+1} > 1$, on the other hand

$$|q_{n-1} x - p_{n-1}| = \frac{1}{x_n q_{n-1} + q_{n-2}} > \frac{1}{(a_n+1) q_{n-1} + q_{n-2}} = \frac{1}{q_n + q_{n-1}}$$

because $x_n < a_n + 1$. □

Corollary 52. *The sequence* $(|x - p_n/q_n|)_{n\geq 0}$ *is strictly decreasing: for* $n \geq 1$ *we have*

$$\left| x - \frac{p_n}{q_n} \right| < \left| x - \frac{p_{n-1}}{q_{n-1}} \right|.$$

Proof. For $n \geq 1$, since $q_{n-1} < q_n$, we have

$$\left| x - \frac{p_n}{q_n} \right| = \frac{1}{q_n} |q_n x - p_n| < \frac{1}{q_n} |q_{n-1} x - p_{n-1}| = \frac{q_{n-1}}{q_n} \left| x - \frac{p_{n-1}}{q_{n-1}} \right| < \left| x - \frac{p_{n-1}}{q_{n-1}} \right|.$$

□

Here is the *law of best approximation* of the simple continued fraction.

[7] Bombieri in [1] gives formulae for $J([a_0,t])$ when $a_0 \leq -1$. He distinguishes eight cases, namely four cases when $a_0 = -1$ ($a_1 > 2$, $a_1 = 2$, $a_1 = 1$ and $a_3 > 1$, $a_1 = a_3 = 1$), two cases when $a_0 = -2$ ($a_1 > 1$, $a_1 = 1$) and two cases when $a_0 \leq -3$ ($a_1 > 1$, $a_1 = 1$). Here, (50) enables us to simplify his proof by reducing to the case $a_0 \geq 0$.

Lemma 53. *Let $n \geq 0$ and $(p, q) \in \mathbf{Z} \times \mathbf{Z}$ with $q > 0$ satisfy*

$$|qx - p| < |q_n x - p_n|.$$

Then $q \geq q_{n+1}$.

Proof. The system of two linear equations in two unknowns u, v

$$\begin{cases} p_n u + p_{n+1} v &= p \\ q_n u + q_{n+1} v &= q \end{cases} \tag{54}$$

has determinant ± 1, hence there is a solution $(u, v) \in \mathbf{Z} \times \mathbf{Z}$.

Since $p/q \neq p_n/q_n$, we have $v \neq 0$.

If $u = 0$, then $v = q/q_{n+1} > 0$, hence $v \geq 1$ and $q \geq q_{n+1}$.

We now assume $uv \neq 0$.

Since q, q_n and q_{n+1} are > 0, it is not possible for u and v to be both negative. In case u and v are positive, the desired result follows from the second relation of (54). Hence one may suppose u and v of opposite signs. Since $q_n x - p_n$ and $q_{n+1} x - p_{n+1}$ also have opposite signs, the numbers $u(q_n x - p_n)$ and $v(q_{n+1} x - p_{n+1})$ have same sign, and therefore

$$|q_n x - p_n| \leq |u(q_n x - p_n)| + |v(q_{n+1} x - p_{n+1})| = |qx - p| < |q_n x - p_n|,$$

which is a contradiction.

□

A consequence of Lemma 53 is that the sequence of p_n/q_n produces the best rational approximations to x in the following sense: any rational number p/q with denominator $q < q_n$ has $|qx - p| > |q_n x - p_n|$. This is sometimes referred to as *best rational approximations of type* 0.

Corollary 55. *The sequence $(q_n)_{n \geq 0}$ of denominators of the convergents of a real irrational number x is the increasing sequence of positive integers for which*

$$\|q_n x\| < \|qx\| \quad \textit{for} \quad 1 \leq q < q_n.$$

As a consequence,

$$\|q_n x\| = \min_{1 \leq q \leq q_n} \|qx\|.$$

The theory of continued fractions is developed starting from Corollary 55 as a definition of the sequence $(q_n)_{n \geq 0}$ in Cassels's book [3].

Corollary 56. *Let $n \geq 0$ and $p/q \in \mathbf{Q}$ with $q > 0$ satisfy*

$$\left| x - \frac{p}{q} \right| < \left| x - \frac{p_n}{q_n} \right|.$$

Then $q > q_n$.

Proof. For $q \leq q_n$ we have

$$\left| x - \frac{p}{q} \right| = \frac{1}{q}|qx - p| > \frac{1}{q}|q_n x - p_n| \frac{q_n}{q} \left| x - \frac{p_n}{q_n} \right| \geq \left| x - \frac{p_n}{q_n} \right|.$$

□

Corollary 56 shows that the denominators q_n of the convergents are also among the *best rational approximations of type* 1 in the sense that

$$\left| x - \frac{p}{q} \right| > \left| x - \frac{p_n}{q_n} \right| \quad \text{for} \quad 1 \leq q < q_n,$$

but they do not produce the full list of them: to get the complete set, one needs to consider also some of the rational fractions of the form

$$\frac{p_{n-1} + ap_n}{q_{n-1} + aq_n}$$

with $0 \leq a \leq a_{n+1}$ (*semi–convergents*) – see for instance [11], Chap. II, § 16.

Lemma 57 (Vahlen, 1895)**.** *Among two consecutive convergents p_n/q_n and p_{n+1}/q_{n+1}, one at least satisfies $|x - p/q| < 1/2q^2$.*

Proof. Since $x - p_n/q_n$ and $x - p_{n-1}/q_{n-1}$ have opposite signs,

$$\left| x - \frac{p_n}{q_n} \right| + \left| x - \frac{p_{n-1}}{q_{n-1}} \right| = \left| \frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} \right| = \frac{1}{q_n q_{n-1}} < \frac{1}{2q_n^2} + \frac{1}{2q_{n-1}^2}.$$

The last inequality is $ab < (a^2 + b^2)/2$ for $a \neq b$ with $a = 1/q_n$ and $b = 1/q_{n-1}$. Therefore,

$$\text{either} \quad \left| x - \frac{p_n}{q_n} \right| < \frac{1}{2q_n^2} \quad \text{or} \quad \left| x - \frac{p_{n-1}}{q_{n-1}} \right| < \frac{1}{2q_{n-1}^2}.$$

□

Lemma 58 (É. Borel, 1903)**.** *Among three consecutive convergents p_{n-1}/q_{n-1}, p_n/q_n and p_{n+1}/q_{n+1}, one at least satisfies $|x - p/q| < 1/\sqrt{5}q^2$.*

Compare with the implication (i) $\Rightarrow$ (vi) in the irrationality criterion below (Proposition 60.

That the constant $\sqrt{5}$ cannot be replaced by a larger one follows from Proposition 63. This is true for any number with a continued fraction expansion having all but finitely many partial quotients equal to 1 (which means the Golden number Φ and all rational numbers which are equivalent to Φ modulo $\mathrm{GL}_2(\mathbf{Z})$).

Proof. Recall Lemma 27: for $n \geq 0$,

$$q_n x - p_n = \frac{(-1)^n}{x_{n+1}q_n + q_{n-1}}.$$

Therefore $|q_n x - p_n| < 1/\sqrt{5}q_n$ if and only if $|x_{n+1}q_n + q_{n-1}| > \sqrt{5}q_n$. Define $r_n = q_{n-1}/q_n$. Then this condition is equivalent to $|x_{n+1} + r_n| > \sqrt{5}$.

Recall the inductive definition of the convergents:

$$x_{n+1} = a_{n+1} + \frac{1}{x_{n+2}}.$$

Also, using the definitions of r_n, r_{n+1}, and the inductive relation $q_{n+1} = a_{n+1}q_n + q_{n-1}$, we can write

$$\frac{1}{r_{n+1}} = a_{n+1} + r_n.$$

Eliminate a_{n+1}:

$$\frac{1}{x_{n+2}} + \frac{1}{r_{n+1}} = x_{n+1} + r_n.$$

Assume now

$$|x_{n+1} + r_n| \leq \sqrt{5} \quad \text{and} \quad |x_{n+2} + r_{n+1}| \leq \sqrt{5}.$$

We deduce

$$\frac{1}{\sqrt{5} - r_{n+1}} + \frac{1}{r_{n+1}} \leq \frac{1}{x_{n+2}} + \frac{1}{r_{n+1}} = x_{n+1} + r_n \leq \sqrt{5},$$

which yields

$$r_{n+1}^2 - \sqrt{5}r_{n+1} + 1 \leq 0.$$

The roots of the polynomial $X^2 - \sqrt{5}X + 1$ are $\Phi = (1+\sqrt{5})/2$ and $\Phi^{-1} = (\sqrt{5}-1)/2$. Hence $r_{n+1} > \Phi^{-1}$ (the strict inequality is a consequence of the irrationality of the Golden ratio). .

This estimate follows from the hypotheses $|q_n x - p_n| < 1/\sqrt{5}q_n$ and $|q_{n+1}x - p_{n+1}| < 1/\sqrt{5}q_{n+1}$. If we also had $|q_{n+2}x - p_{n+2}| < 1/\sqrt{5}q_{n+2}$, we would deduce in the same way $r_{n+2} > \Phi^{-1}$. This would give

$$1 = (a_{n+2} + r_{n+1})r_{n+2} > (1 + \Phi^{-1})\Phi^{-1} = 1,$$

which is impossible.

□

Lemma 59 (Legendre, 1798)**.** *If $p/q \in \mathbf{Q}$ satisfies $|x - p/q| \leq 1/2q^2$, then p/q is a convergent of x.*

Proof. Let r and s in $\mathbf{Z}$ satisfy $1 \leq s < q$. From

$$1 \leq |qr - ps| = |s(qx-p) - q(sx-r)| \leq s|qx-p| + q|sx-r| \leq \frac{s}{2q} + q|sx-r|$$

one deduces

$$q|sx - r| \geq 1 - \frac{s}{2q} > \frac{1}{2} \geq q|qx - p|.$$

Hence $|sx - r| > |qx - p|$ and therefore Lemma 53 implies that p/q is a convergent of x.

□

3.8 Appendix

The proof of the following results are left as exercises.

Proposition 60. *Let ϑ be a real number. The following conditions are equivalent:*
(i) *ϑ is irrational.*
(ii) *For any $\epsilon > 0$, there exists $(p, q) \in \mathbf{Z}^2$ such that $q > 0$ and*

$$0 < |q\vartheta - p| < \epsilon.$$

(iii) *For any $\epsilon > 0$, there exist two linearly independent linear forms in two variables*

$$L_0(X_0, X_1) = a_0X_0 + b_0X_1 \quad \textit{and} \quad L_1(X_0, X_1) = a_1X_0 + b_1X_1,$$

with rational integer coefficients, such that

$$\max\left\{|L_0(1,\vartheta)|\ ,\ |L_1(1,\vartheta)|\right\} < \epsilon.$$

(iv) *For any real number $Q > 1$, there exists an integer q in the range $1 \leq q < Q$ and a rational integer p such that*

$$0 < |q\vartheta - p| < \frac{1}{Q}\cdot$$

(v) *There exist infinitely many $p/q \in \mathbf{Q}$ such that*

$$\left|\vartheta - \frac{p}{q}\right| < \frac{1}{q^2}\cdot$$

(vi) *There exist infinitely many $p/q \in \mathbf{Q}$ such that*

$$\left|\vartheta - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2}\cdot$$

Proposition 61. *Given a positive integer D which is not a square, there exists $(x, y) \in \mathbf{Z}^2$ with $x > 0$ and $y > 0$ such that $x^2 - Dy^2 = 1$.*

Proposition 62. *Let D be a positive integer which is not a square. Let x and y be positive rational integers. The following conditions are equivalent:*
(i) $x^2 - Dy^2 = \pm 1$.
(ii) $\left|\sqrt{D} - \dfrac{x}{y}\right| < \dfrac{1}{2y^2\sqrt{D} - 1}\cdot$
(iii) $\left|\sqrt{D} - \dfrac{x}{y}\right| < \dfrac{1}{y^2\sqrt{D} + 1}\cdot$

Proposition 63. *For any $q \geq 1$ and any $p \in \mathbf{Z}$,*

$$\left|\Phi - \frac{p}{q}\right| > \frac{1}{\sqrt{5}q^2 + (q/2)}\cdot$$

On the other hand

$$\lim_{n\to\infty} F_{n-1}^2 \left|\Phi - \frac{F_n}{F_{n-1}}\right| = \frac{1}{\sqrt{5}}\cdot$$

4 The theory of finite fields

References:

M. Demazure [4], Chap. 8.
D.S. Dummit & R.M. Foote [5], § 14.3.
S. Lang [9], Chap. 5 § 5.
R. Lidl & H. Niederreiter [10].
V. Shoup [13], 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 $\mathbf{Z}/p\mathbf{Z}$ 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 $\mathbf{F}_p$ the unique field with p elements.

The characteristic of finite field F is a prime number p, hence, its prime field is $\mathbf{F}_p$. Moreover, F is a finite vector space over $\mathbf{F}_p$; if the dimension of this space is s, which means that F is a finite extension of $\mathbf{F}_p$ of degree $[F : \mathbf{F}_p] = s$, 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 $X^q - X$:

$$X^{q-1} - 1 = \prod_{x \in F^\times} (X - x), \qquad X^q - X = \prod_{x \in F} (X - x). \tag{64}$$

Exercise 65. (a) Let F be a finite field with q elements, where q is odd. 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 $F^\times$:

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

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 $\mathbf{F}_p$, denote by $\left(\frac{a}{p}\right)$ the Legendre symbol:

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

Check

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

and

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

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

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

Exercise 66. Prove that in a finite field, any element is a sum of two squares.

Exercise 67. 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 68. *Any finite subgroup 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. 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

Let e be the exponent go 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. □

Second proof of Proposition 68. The following alternative proof of Proposition 68 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 1 (3). □

Programs giving a generator of the cyclic group $\mathbf{F}_q^\times$, also called a *primitive root* or a *primitive element* in $\mathbf{F}_q$, are available online[8].

[8]One of them (in French) is

Exercise 69. 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 $\mathcal{C}_k$?

When $F = \mathbf{F}_p$, 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 $(\mathbf{Z}/p\mathbf{Z})^\times$. More generally, when $\mathbf{F}_q$ is a finite field with q elements, a nonzero element α in $\mathbf{F}_q$ is a generator of the cyclic group $\mathbf{F}_q^\times$ if and only if α is a primitive $(q-1)$th root of unity.

The theorem of the primitive element for finite fields is:

Proposition 70. *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 68); let α be a generator. Then

$$K = \left\{0, 1, \alpha, \alpha^2, \ldots, \alpha^{q-2}\right\} = \mathbf{F}_p(\alpha),$$

and, therefore, $K = F(\alpha)$.

□

Hence the field K is isomorphic to the quotient $\mathbf{F}_p[X]/(P)$ where $P \in \mathbf{F}_p[X]$ is some irreducible polynomial over $\mathbf{F}_p$ of degree s. We prove below (cf. Theorem 72) that K is isomorphic to the quotient $\mathbf{F}_p[X]/(P)$ where $P \in \mathbf{F}_p[X]$ is any irreducible polynomial over $\mathbf{F}_p$ of degree s.

Lemma 71. *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. □

`http://jean-paul.davalan.pagesperso-orange.fr/mots/comb/gfields/index.html`
Computation on finite fields can be done also with
`http://wims.unice.fr/~wims/`

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 72. *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 $\mathbf{F}_p$ of the polynomial $X^q - X$. Then F is the set of roots of this polynomial, hence, 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 (64), if $\mathbf{F}_q$ is a finite field with q elements and F an extension of $\mathbf{F}_q$, then for $a \in F$, the relation $a^q = a$ holds if and only if $a \in \mathbf{F}_q$. We will use the following more general fact:

Lemma 73. *Let $\mathbf{F}_q$ be a finite field with q elements, F an extension of $\mathbf{F}_q$ and $f \in F[X]$ a polynomial with coefficients in F. Then f belongs to $\mathbf{F}_q[X]$ 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 71,

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

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 71, we deduce:

Proposition 74. *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 Frob_p is not surjective is the field $\mathbf{F}_p(X)$ of rational fractions in one variable over the prime field $\mathbf{F}_p$.

Proof. Indeed, this map is a morphism of fields since, by Lemma 71, 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 $\mathbf{F}_p$. 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 68, 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 $F/\mathbf{F}_p$ is Galois, with Galois group $\mathrm{Gal}(F/\mathbf{F}_p) = \mathrm{Aut}(F)$ the cyclic group of order s generated by Frob_p.

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

Theorem 75. *[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 75, the Galois group of E over F is the quotient $\mathrm{Gal}(K/F)/\mathrm{Gal}(K/E)$.

Exercise 76.
(a) Let F be a field, m and n two positive integers, a and b 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 $b^{a^m} - b$.
(b) Let m, n and a be positive integers with $a \geq 2$. Check

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

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

$$\mathbf{F}_{p^n} \subset \mathbf{F}_{p^m} \iff n \text{ divides } m. \tag{77}$$

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

Let $F \subset \overline{\mathbf{F}}_p$ be a finite field of characteristic p with q elements, and let x be an element in $\overline{\mathbf{F}}_p$. The conjugates of x over F are the roots in $\overline{\mathbf{F}}_p$ 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 72), but if $s \geq 2$, there is no unicity of such an isomorphic, because the set of automorphisms of $\mathbf{F}_{p^s}$ 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 $\mathbf{Z}/(q-1)\mathbf{Z}$.

- A finite field F with q elements is isomorphic to the ring $\mathbf{Z}/q\mathbf{Z}$ if and only if q is a prime number (which is equivalent to saying that $\mathbf{Z}/q\mathbf{Z}$ has no zero divisor).

Example (`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 $\mathbf{F}_2$, three of them split in $\mathbf{F}_2$, 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 (`The field` $\mathbf{F}_5$`).` .

We could write $\mathbf{F}_5 = \{0, 1, -1, i, -i\}$ with i and $-i$ the two roots of X^2+1, one of them is 2, the other is 3. Notice that there is no automorphism of $\mathbf{F}_5$ mapping i to $-i$.

Exercise 78. Check the following isomorphisms, and give a generator of the multiplicative group of non–zero elements in the field.
(a) $\mathbf{F}_4 = \mathbf{F}_2[X]/(X^2+X+1)$.
(b) $\mathbf{F}_8 = \mathbf{F}_2[X]/(X^3+X+1)$.
(c) $\mathbf{F}_{16} = \mathbf{F}_2[X]/(X^4+X+1)$.
(d) $\mathbf{F}_{16} = \mathbf{F}_2[X,Y]/(Y^2+Y+1, X^2+X+Y)$.

Exercise 79. (a) Give the list of all irreducible polynomials of degree ≤ 5 over $\mathbf{F}_2$.
(b) Give the list of all monic irreducible polynomials of degree ≤ 2 over $\mathbf{F}_4$.

Recall (Theorem 75) 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.*

Theorem 80 (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.*

`Remark`. The normal basis Theorem holds for any finite Galois extension L/K: 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. We first give a proof of this result when K is infinite, and then a proof for a cyclic extension L/K. The second proof will give the result for finite fields.

Let $G = \mathrm{Gal}(L/K)$. The conjugates of α over K are the elements $\sigma(\alpha)$. Consider a linear relation with coefficients in K among such numbers, for an arbitrary $\alpha \in L$:

$$\sum_{\sigma \in G} a_\sigma \sigma(\alpha) = 0.$$

For each $\tau \in G$, we also have

$$\sum_{\sigma \in G} a_\sigma \tau^{-1}\sigma(\alpha) = 0.$$

Hence, for $\alpha \in L$; a necessary and sufficient condition for the conjugates of α to give a basis of L over K is

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

Since L/K is a finite separable extension, there exists an element β in L such that $L = K(\beta)$ (*theorem of the primitive element*). Let f be the irreducible polynomial of β over K:

$$f(X) = \prod_{\sigma \in G} (X - \sigma(\beta)).$$

For $\sigma \in G$, define $g^\sigma(X) \in L[X]$ by

$$g^\sigma(X) = \frac{f(X)}{X - \sigma(\beta)} = \prod_{\tau \in G \setminus \{\sigma\}} (X - \tau(\beta)).$$

We have $g^\sigma(\beta) \neq 0$ for $\sigma = 1$ and $g^\sigma(\beta) = 0$ for $\sigma \neq 1$, hence the determinant

$$\mathrm{d}(X) = \det\bigl(g^{\tau^{-1}\sigma}(X)\bigr)_{\tau,\sigma\in G}$$

does not vanish at β; this shows that $\mathrm{d}(X)$ is not the zero polynomial

Assume now that the field K is infinite: hence there exists $\gamma \in L$ such that $\mathrm{d}(\gamma) \neq 0$. Set

$$\alpha = \frac{f(\gamma)}{\gamma - \beta}.$$

Then one checks that α and its conjugates give a basis of L over K.

However this argument does not work for a finite field, which is the case we are interested in. In this case a different argument is used, which works more generally for a cyclic extension.

Proof of Theorem 80.
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.

□

Exercise 81.
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

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

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

Theorem 82. *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

$$\prod_{\ell=0}^{n-1} \left(X - \mathrm{Frob}_q^\ell(\alpha)\right) = \prod_{\ell=0}^{n-1} \left(X - \alpha^{q^\ell}\right). \tag{83}$$

Proof. Define $s = [F(\alpha) : F]$. By Theorem 75, the extension $F(\alpha)/F$ is Galois with Galois group the cyclic group of order s generated by Frob_q. The conjugates of αover F are the elements $\mathrm{Frob}_q^i(\alpha)$, $0 \leq i \leq s-1$. Hence $s = n$.

□

4.2 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 $\mathbf{Z}$, 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 $F^\times_{\mathrm{tors}}$ having at most n elements. The union of all these subgroups of $F^\times_{\mathrm{tors}}$ is just the torsion group $F^\times_{\mathrm{tors}}$ itself. This group contains 1

and -1, but it could have just one element, like for $\mathbf{F}_2 = \mathbf{Z}/2\mathbf{Z}$ or $\mathbf{F}_2(X)$ for instance. The torsion subgroup of $\mathbf{R}^\times$ is $\{\pm 1\}$, the torsion subgroup of $\mathbf{C}^\times$ 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:

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

4.2.1 Cyclotomic polynomials over $\mathbf{C}[X]$

The map $\mathbf{C} \to \mathbf{C}^\times$ defined by $z \mapsto e^{2i\pi z/n}$ is a morphism from the additive group $\mathbf{C}$ to the multiplicative group $\mathbf{C}^\times$; this morphism is periodic with period n. Hence, it factors to a morphism from the group $\mathbf{C}/n\mathbf{Z}$ to $\mathbf{C}^\times$: we denote it also by $z \mapsto e^{2i\pi z/n}$. The multiplicative group $(\mathbf{Z}/n\mathbf{Z})^\times$ of the ring $\mathbf{Z}/n\mathbf{Z}$ is the set of classes of integers prime to n. Its order is $\varphi(n)$, where φ is Euler's function.

The $\varphi(n)$ complex numbers

$$e^{2i\pi k/n} \qquad k \in (\mathbf{Z}/n\mathbf{Z})^\times$$

are the primitive roots of unity in $\mathbf{C}$.

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

$$\Phi_n(X) = \prod_{k \in (\mathbf{Z}/n\mathbf{Z})^\times} (X - e^{2i\pi k/n}). \tag{84}$$

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

$$X^n - 1 = \prod_{\substack{1 \le d \le n \\ d|n}} \Phi_d(X). \tag{85}$$

The degree of $X^n - 1$ is n, and the degree of $\Phi_d(X)$ is $\varphi(d)$, hence, Lemma 4 follows also from (85).

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

$$\Phi_1(X) = X - 1, \qquad \Phi_n(X) = \frac{X^n - 1}{\prod_{\substack{d \ne n \\ d|n}} \Phi_d(X)}. \tag{86}$$

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 § 1.4.3 with G the multiplicative group $\mathbf{Q}(X)^\times$) yields

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

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

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

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

Exercise 87.
(a) Let p be a prime number and let $m \geq 1$. Prove

$$\begin{cases} \Phi_m(X^p) = \Phi_{pm}(X) & \text{and} \quad \varphi(pm) = p\varphi(m) & \text{if } p|m, \\ \Phi_m(X^p) = \Phi_{pm}(X)\Phi_m(X) & \text{and} \quad \varphi(pm) = (p-1)\varphi(m) & \text{if } \gcd(p,m) = 1. \end{cases}$$

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 $r \geq 1$.
(b) 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,

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

Theorem 88. *For any positive integer n, the polynomial $\Phi_n(X)$ has its coefficients in $\mathbf{Z}$. Moreover, $\Phi_n(X)$ is irreducible in $\mathbf{Z}[X]$.*

Proof of the first part of Theorem 88. We check $\Phi_n(X) \in \mathbf{Z}[X]$ by induction on n. The results holds for $n = 1$, since $\Phi_1(X) = X - 1$. Assume $\Phi_m(X) \in \mathbf{Z}[X]$ 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 $\mathbf{Z}$. We divide $X^n - 1$ by h in $\mathbf{Z}[X]$: let $Q \in \mathbf{Z}[X]$ be the quotient and $R \in \mathbf{Z}[X]$ the remainder:

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

We also have $X^n - 1 = h(X)\Phi_n(X)$ in $\mathbf{C}[X]$, as shown by (85). From the unicity of the quotient and remainder in the Euclidean division in $\mathbf{C}[X]$, we deduce $Q = \Phi_n$ and $R = 0$, hence, $\Phi_n \in \mathbf{Z}[X]$. □

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

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 89 (Eisenstein criterion)**.** *Let*

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

and let p be a prime number. Assume C to be product of two polynomials in $\mathbf{Z}[X]$ 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 $\mathbf{Z}[X]$ 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 (2) of reduction modulo p, namely $\Psi_p : \mathbf{Z}[X] \longrightarrow \mathbf{F}_p[X]$. 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

$$\tilde{C}(X) = \tilde{c}_0X^d + \cdots + \tilde{c}_d.$$

By assumption $\tilde{c}_0 \neq 0$, $\tilde{c}_1 = \cdots = \tilde{c}_d = 0$, hence, $\tilde{C}(X) = \tilde{c}_0X^d = \tilde{A}(X)\tilde{B}(X)$ 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 $c_d = a_nb_m$. □

Proof of the irreducibility of Φ_p over $\mathbf{Z}$ in Theorem 88 for p prime. We set $X - 1 = Y$, so that

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

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 89. □

We now consider the general case.

Proof of the irreducibility of Φ_n *over* $\mathbf{Z}$ *in Theorem* 88 *for all* n. Let $f \in \mathbf{Z}[X]$ be an irreducible factor of Φ_n with a positive leading coefficient and let $g \in \mathbf{Z}[X]$ 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 $\mathbf{C}$ 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 (2). Denote by F, G, H the images of f, g, h. Recall that $fg = \Phi_n$ in $\mathbf{Z}[X]$, hence, $F(X)G(X)$ divides $X^n - 1$ in $\mathbf{F}_p[X]$. The assumption that p does not divide n implies that $X^n - 1$ has no square factor in $\mathbf{F}_p[X]$.

Let $P \in \mathbf{Z}[X]$ be an irreducible factor of F. From $G(X^p) = F(X)H(X)$, it follows that $P(X)$ divides $G(X^p)$. But $G \in \mathbf{F}_p[X]$, hence (see Lemma 73), $G(X^p) = G(X)^p$ 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 $\mathbf{C}$ 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* $\mathbf{Q}$ is

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

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

For example we have

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

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 90. *Check*

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

for all $n \geq 1$.

Proposition 91. *There is a canonical isomorphism between* $\mathrm{Gal}(R_n/\mathbf{Q})$ *and the multiplicative group* $(\mathbf{Z}/n\mathbf{Z})^\times$.

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 $\mathbf{C}^\times$ generated by ζ_n. The map $\mathbf{Z} \longrightarrow \mu_n$ which maps m to ζ_n^m is a group homomorphism of kernel $n\mathbf{Z}$. When c is a class modulo n, we denote by ζ^c the image of c under the isomorphism $\mathbf{Z}/n\mathbf{Z} \simeq \mu_n$.

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

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

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

□

Example. The element τ in $\mathrm{Gal}(R_n/\mathbf{Q})$ 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 $\mathrm{Gal}(R_n/\mathbf{Q})$ is the maximal real subfield of R_n:

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

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

4.2.2 Cyclotomic Polynomials over a finite field

Since Φ_n has coefficients in $\mathbf{Z}$, 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 $\mathbf{Q}$; in finite characteristic p, one considers the image of Φ_n under the morphism Ψ_p introduced in (2): we denote again this image by Φ_n.

Proposition 92. *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 (86), this means that it is a root of Φ_n.

□

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 93.
Consider the following polynomials 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 (64), given $q = p^r$, the unique subfield of $\overline{\mathbf{F}}_p$ with q elements is the set $\mathbf{F}_q$ of roots of $X^q - X$ in $\overline{\mathbf{F}}_p$. The set $\{X - x \mid x \in \mathbf{F}_q\}$ is the set of all monic degree 1 polynomials with coefficients in $\mathbf{F}_q$. Hence, (64) is the special case $n = 1$ of the next statement.

Theorem 94. *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 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 $\mathbf{F}_q[X]$ 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 $f \in \mathbf{F}_q[X]$ be an irreducible factor of $X^{q^n} - X$ and α be a root of f in $\overline{\mathbf{F}}_p$. The polynomial $X^{q^n} - X$ is a multiple of f, therefore, it vanishes at α, hence, $\alpha^{q^n} = \alpha$ which means $\alpha \in \mathbf{F}_{q^n}$. From the field extensions

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

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

Conversely, let f be an irreducible polynomial in $\mathbf{F}_q[X]$ of degree d where d divides n. Let α be a root of f in $\overline{\mathbf{F}}_p$. Since d divides n, the field $\mathbf{F}_q(\alpha)$ is a subfield of $\mathbf{F}_{q^n}$, hence $\alpha \in \mathbf{F}_{q^n}$ 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 $\mathbf{F}_q[X]$, the polynomial $X^{q^n} - X$, having no multiple factor, is the product of the monic irreducible polynomials which divide it. Theorem 94 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 $\mathbf{F}_q[X]$. Theorem 94 yields, for $n \geq 1$,

$$q^n = \sum_{d|n} dN_q(d). \tag{95}$$

From Möbius inversion formula (§ 1.4.3), one deduces:

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

For instance, when ℓ is a prime number,

$$N_q(\ell) = \frac{q^\ell - q}{\ell}. \tag{96}$$

Exercise 97. 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 $\mathbf{F}_p$ the prime subfield of F. Check that more than half of the elements α in F satisfy $F = \mathbf{F}_p(\alpha)$.
(e) Check that when p^n tends to infinity, the probability that a polynomial of degree n over $\mathbf{F}_p$ be irreducible in $\mathbf{F}_p[X]$ tends to $1/n$.

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

4.3 Decomposition of cyclotomic polynomials over a finite field

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

We apply Theorem 82 to the cyclotomic polynomials.

Theorem 98. *Let $\mathbf{F}_q$ be a finite field with q elements and let n be a positive integer not divisible by the characteristic of $\mathbf{F}_q$. Then the cyclotomic polynomial Φ_n splits in $\mathbf{F}_q[X]$ into a product of irreducible factors, all of the same degree d, where d is the order of q modulo n.*

Recall (see § 1.4.1) that the order of q modulo n is by definition the order of the class of q in the multiplicative group $(\mathbf{Z}/n\mathbf{Z})^\times$ (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 $\mathbf{F}_q$. The order of ζ in the multiplicative group $K^\times$ is n. According to Theorem 82, the degree of ζ over $\mathbf{F}_q$ is he smallest integer $s \geq 1$ such that $\zeta^{q^s-1} = 1$. Hence it is the smallest positive integer s such that n divides $q^s - 1$, and this is the order of the image of q in the multiplicative group $(\mathbf{Z}/n\mathbf{Z})^\times$. □

Since an element $\zeta \in \overline{\mathbf{F}}_p^\times$ has order n in the multiplicative group $\overline{\mathbf{F}}_p^\times$ if and only if ζ is a root of Φ_n, an equivalent statement to Theorem 98 is the following.

Corollary 99. *If $\zeta \in \overline{\mathbf{F}}_p^\times$ has order n in the multiplicative group $\overline{\mathbf{F}}_p^\times$, then its degree $d = [\mathbf{F}_q(\zeta) : \mathbf{F}_q]$ over $\mathbf{F}_q$ is the order of q modulo n.*

The special case $d = 1$ of corollary 99 produces the next result:

Corollary 100. *The polynomial $\Phi_n(X)$ splits completely in $\mathbf{F}_q[X]$ (into a product of linear polynomials) if and only if $q \equiv 1 \bmod n$.*

This follows from Theorem 98, but it is also plain from Proposition 68 and the fact that the cyclic group $\mathbf{F}_q^\times$ of order $q - 1$ contains a subgroup of order n if and only if n divides $q - 1$, which is the condition $q \equiv 1 \bmod n$.

The special case $d = \varphi(n)$ of corollary 99 produces the next result:

Corollary 101. *The following conditions are equivalent:*
(i) *The polynomial $\Phi_n(X)$ is irreducible in $\mathbf{F}_q[X]$.*
(ii) *The class of q modulo n has order $\varphi(n)$.*
(iii) *q is a generator of the group $(\mathbf{Z}/n\mathbf{Z})^\times$.*

This can be true only when this multiplicative group is cyclic, which means (see Exercise 5) that n is either

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

where ℓ is an odd prime and $s \geq 1$.

Corollary 102. *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 $\mathbf{F}_q[X]$ 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 $\overline{\mathbf{F}}_p$ of the prime field $\mathbf{F}_p$, and for q a power of p we denote by $\mathbf{F}_q$ the unique subfield of $\overline{\mathbf{F}}_p$ with q elements. Of course, $\overline{\mathbf{F}}_p$ is also an algebraic closure of $\mathbf{F}_q$.

Example. The field $\mathbf{F}_4$, quadratic extension of $\mathbf{F}_2$ *(see also example* 4.1*).* We consider the quadratic extension $\mathbf{F}_4/\mathbf{F}_2$. There is a unique irreducible polynomial of degree 2 over $\mathbf{F}_2$, which is $\Phi_3 = X^2 + X + 1$. Denote by ζ one of its roots in $\mathbf{F}_4$. The other root is ζ^2 with $\zeta^2 = \zeta + 1$ and

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

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

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

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 $\mathbf{C}$.

Example. The field $\mathbf{F}_8$, cubic extension of $\mathbf{F}_2$. We consider the cubic extension $\mathbf{F}_8/\mathbf{F}_2$. There are 6 elements in $\mathbf{F}_8$ which are not in $\mathbf{F}_2$, each of them has degree 3 over $\mathbf{F}_2$, hence, there are two irreducible polynomials of degree 3 in $\mathbf{F}_2[X]$. Indeed, from (96), it follows that $N_2(3) = 2$. The two irreducible factors of Φ_7 are the only irreducible polynomials of degree 3 over $\mathbf{F}_2$:

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

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

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

Since $[\mathbf{F}_8 : \mathbf{F}_2] = 3$, there are three automorphisms of $\mathbf{F}_8$, 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

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

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

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

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

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

In $\mathbf{F}_9^\times$, there are $4 = \varphi(8)$ elements of order 8 (the four roots of Φ_8) which have degree 2 over $\mathbf{F}_3$. 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 $\mathbf{F}_3$, their square is -1. There is one element of order 2, namely -1, and one of order 1, namely 1. From (96), it follows that $N_3(2) = 3$: the three monic irreducible polynomials of degree 2 over $\mathbf{F}_3$ are Φ_4 and the two irreducible factors of Φ_8.

Since $[\mathbf{F}_9 : \mathbf{F}_3] = 2$, there are two automorphisms of $\mathbf{F}_9$, 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

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

and also

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

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 $\zeta^6 = \eta^2$.

Exercise 103. 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 $\mathbf{F}_3$.

Exercise 104. Check that 2 has order 11 modulo 23 and that $X^{23}-1$ over $\mathbf{F}_2$ is the product of three irreducible polynomials, namely $X-1$,

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

and

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

Example. Assume that q is odd and consider the polynomial $\Phi_4(X) = X^2+1$. Corollary 100 implies:

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

Example. 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 $\mathbf{F}_q$.
- Otherwise X^4+1 is a product of two irreducible polynomials of degree 2 in $\mathbf{F}_q[X]$.

For instance, Example 4.3 gives over $\mathbf{F}_3$

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

Using Example 4.3, one deduces that in the decomposition of X^8-1 over $\mathbf{F}_q$, 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 105. Check that the polynomial X^4+1 is irreducible over $\mathbf{Q}$ but that it is reducible over $\mathbf{F}_p$ for all prime numbers p.

Example. The group $(\mathbf{Z}/5\mathbf{Z})^\times$ 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 $\mathbf{F}_q[X]$,
- If $q \equiv 1 \bmod 5$, then Φ_5 has 4 roots in $\mathbf{F}_q$,
- If $q \equiv -1 \bmod 5$, then Φ_5 splits as a product of two irreducible polynomials of degree 2 in $\mathbf{F}_q[X]$.

Exercise 106. Let $\mathbf{F}_q$ be a finite field with q elements. What are the degrees of the irreducible factors of the cyclotomic polynomial Φ_{15} over $\mathbf{F}_q$? For which values of q is Φ_{15} irreducible over $\mathbf{F}_q$?

Exercise 107. Let p be a prime number, r a positive integer, $q = p^r$. Denote by $\mathbf{F}_{q^2}$ a field with q^2 elements.
(a) Consider the homomorphism of multiplicative groups $\mathbf{F}_{q^2}^\times \longrightarrow \mathbf{F}_{q^2}^\times$ which maps x to x^{q-1}. What is the kernel? What is the image?
(b) Show that there exists $\alpha \in \mathbf{F}_{q^2}$ such that α^{q-1} is not in $\mathbf{F}_q$. Deduce that (α, α^q) is a basis of the $\mathbf{F}_q$–vector space $\mathbf{F}_{q^2}$.

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

As usual, we assume $\gcd(n, q) = 1$. Theorem 98 tells us that Φ_n is product of irreducible polynomials over $\mathbf{F}_q$ all of the same degree d. Denote by G the multiplicative group $(\mathbf{Z}/n\mathbf{Z})^\times$. 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 $\mathbf{F}_q$, or if you prefer in the splitting field of $\Phi_n(X)$ over $\mathbf{F}_q$). Then the conjugates of ζ over $\mathbf{F}_q$ are its images under the iterated Frobenius Frob_q which maps x to x^q. Hence, the minimal polynomial of ζ over $\mathbf{F}_q$ 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 $\{mq^i \mid 0 \le i \le d-1\}$ of m modulo H in G. There are $\varphi(n)/d$ classes of G modulo H, and the decomposition of $\Phi_d(X)$ into irreducible factors over $\mathbf{F}_q$ is

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

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

Again we assume $\gcd(n, q) = 1$. We just studied the decomposition over $\mathbf{F}_q$ 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 $\mathbf{F}_q[X]$. Proposition 108 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 $\mathbf{F}_q$. Recall that for j in $\mathbf{Z}$, ζ^j depends only on the classe of j modulo n. Hence, ζ^i makes sense when i is an element of $\mathbf{Z}/n\mathbf{Z}$:

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

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

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

For I ranging over the 2^n subsets of $\mathbf{Z}/n\mathbf{Z}$, we obtain all the monic divisors of $X^n - 1$ in $F[X]$. Lemma 73 implies that Q_I belongs to $\mathbf{F}_q[X]$ 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 $\mathbf{Z}/n\mathbf{Z}$:

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

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 $\mathbf{Z}/n\mathbf{Z}$ with this property is *stable under multiplication by q*. Therefore:

Proposition 108. *The map $I \mapsto Q_I$ is a bijective map between the subsets I of $\mathbf{Z}/n\mathbf{Z}$ which are stable under multiplication by q on the one hand, and the monic divisors of $X^n - 1$ in $\mathbf{F}_q[X]$ on the other hand.*

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

Corollary 109. *Under this bijective map, the irreducible factors of $X^n - 1$ correspond to the minimal subsets I of $\mathbf{Z}/n\mathbf{Z}$ which are stable under multiplication by q.*

Here are some examples:

- For $I = \emptyset$, $Q_\emptyset = 1$.
- For $I = \mathbf{Z}/n\mathbf{Z}$, $Q_{\mathbf{Z}/n\mathbf{Z}} = X^n - 1$.
- For $I = (\mathbf{Z}/n\mathbf{Z})^\times$, $Q_{(\mathbf{Z}/n\mathbf{Z})^\times} = \Phi_n$.
- For $I = \{0\}$, $Q_0(X) = X - 1$.
- If n is even (and q odd, of course), then for $I = \{n/2\}$, $Q_{\{n/2\}}(X) = X + 1$.
- Let d be a divisor of n. There is a unique subgroup C_d of order d in the cyclic group $\mathbf{Z}/n\mathbf{Z}$. This subgroup is generated by the class of n/d, it is the set of $k \in \mathbf{Z}/n\mathbf{Z}$ such that $dk = 0$, it is stable under multiplication by any element prime to n. Then $Q_{C_d}(X) = X^d - 1$.
- Let again d be a divisor of n and let E_d be the set of generators of C_d: this set has $\varphi(d)$ elements which are the elements of order d in the cyclic group $\mathbf{Z}/n\mathbf{Z}$. Again this subset of $\mathbf{Z}/n\mathbf{Z}$ is stable under multiplication by any element prime to n. Then Q_{E_d} is the cyclotomic polynomial Φ_d of degree $\varphi(d)$.

Example. The field $\mathbf{F}_{16}$, quartic extension of $\mathbf{F}_2$. Take $n = 15$, $q = 2$. The minimal subsets of $\mathbf{Z}/15\mathbf{Z}$ 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 $\mathbf{F}_2$, 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 $\mathbf{F}_2$. There are four polynomials of degree 4 over $\mathbf{F}_2$ without roots in $\mathbf{F}_2$ (the number of

monomials with coefficient 1 should be odd, hence should be 3 or 5) and $\Phi_3^2 = X^4+X^2+1$ is reducible; hence, there are three irreducible polynomials of degree 4 over $\mathbf{F}_2$:

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

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

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

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 $\mathbf{Z}[X]$:

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

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 $\mathbf{F}_4$), 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 $\mathbf{F}_2$ 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 $\mathbf{F}_{16}^\times$, there are

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

Example. The field $\mathbf{F}_{27}$, cubic extension of $\mathbf{F}_3$. Let us write, in $\mathbf{F}_3[X]$,

$$X^{27} - X = X(X^{13} - 1)(X^{13} + 1),$$

$$X^{13} + 1 = (X + 1)f_1f_2f_3f_4, \qquad X^{13} - 1 = (X - 1)f_5f_6f_7f_8$$

with f_i of degree 3. The roots of f_1, f_2, f_3, f_4 are the $12 = \varphi(26)$ generators of the cyclic group $\mathbf{F}_{27}^\times = C_{26}$, the roots of f_5, f_6, f_7, f_8 are the $12 = \varphi(13)$ elements of order 13 which generate the unique cyclic subgroup of $\mathbf{F}_{27}^\times$ of order 13, the root of $X + 1$ is the unique element of order 2.

We are going to exhibit the set $\{f_1, \ldots, f_8\}$ by looking at the degree 3 irreducible polynomials over $\mathbf{F}_3$. We will first describe the set $\{f_1, \ldots, f_4\}$. Then we can take $f_{4+i}(X) = -f_i(-X)$ (replace X^{2j} by $-X^{2j}$ and keep the sign for X^{2j+1}).

In order to get the decomposition of $X^{13} + 1$, we write the table of discrete logarithms for $\mathbf{F}_{27}$. We need a generator. One among 4 solutions is to take a root α of $X^3 - X + 1$.
Exercise: check $\alpha^{13} = -1$.
`Hint.` Check $\alpha^3 = \alpha - 1$, $\alpha^9 = \alpha^3 - 1 = \alpha + 1$, $\alpha^{12} = \alpha^2 - 1$.

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 $\alpha^{-1} = \alpha^{19} - \alpha^2 - \alpha - 1$, $\alpha^{-3} = \alpha^{23} = -\alpha - 1$ 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 $\alpha^5 = \alpha^{-21} = -\alpha^2 + \alpha + 1$, which is also the irreducible polynomial of $\alpha^{15} = \alpha^{-11} = 2\alpha^2$ and of $\alpha^{45} = \alpha^{19} = \alpha^7 = -\alpha^2 - \alpha - 1$ 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 $\alpha^{-1} = \alpha^{25}$, $\alpha^{-3} = \alpha^{23}$, $\alpha^{-9} = \alpha^{17}$
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 $\alpha^{-7} = \alpha^{19}$, $\alpha^{-21} = \alpha^5$, $\alpha^{-11} = \alpha^{15}$.
This gives the list of 12 generators of $\mathbf{F}_{27}^\times$.

The twelve elements of order 13 in $\mathbf{F}_{27}^\times$ 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: give the list of the three roots of each of the four factors of $(X^{13} - 1)/(X - 1)$ over $\mathbf{F}_3$.
`Hint`: consider the change of variable $x \mapsto -x$ using $-1 = \alpha^{13}$.

Exercise 110. Let $\mathbf{F}_q$ be a finite field with q elements of characteristic p. Show that the following conditions are equivalent.
(i) Any element α in $\mathbf{F}_q$ such that $\mathbf{F}_q = \mathbf{F}_p(\alpha)$ is a generator of the cyclic group $\mathbf{F}_q^\times$.
(ii) The number $q-1$ is a prime number.

4.4 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 *norm of α from E to F* is the product of the conjugates of α over F, while the *trace of α from E to F* is the sum of the conjugates:

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

For $\alpha \in F$, we have $\mathrm{N}_{E/F}(\alpha) = \alpha^s$ and $\mathrm{Tr}_{E/F}(\alpha) = s\alpha$. The norm $\mathrm{N}_{E/F}$ induces a surjective morphism from $E^\times$ onto $F^\times$. The trace $\mathrm{Tr}_{E/F}$ is a F–linear surjective map from E onto F, the kernel of which is the set of roots of the polynomial $X + X^q + \cdots + X^{q^{s-1}}$.

Exercise 111. (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 65) is

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

for $a \in \mathbf{Z}$ and $\alpha = a \pmod p \in \mathbf{F}_p$. 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 112. The field $\mathbf{F}_{16}$, quadratic extension of $\mathbf{F}_4$.

Write $\mathbf{F}_4 = \mathbf{F}_2(j)$ with j root of $X^2 + X + 1$.

(1) List the irreducible polynomials of degree 2 over $\mathbf{F}_4$.

(2) Decompose the 6 irreducible polynomials of $\mathbf{F}_2$ of degree 4 into irreducible factors of degree 2 over $\mathbf{F}_2$.

(Explain why it should be so)

(3) Select a generator of $\mathbf{F}_{16}^\times$ and an irreducible polynomial of degree 2 over $\mathbf{F}_4$ of which α is a root in $\mathbf{F}_{16}$. Write the discrete logarithm table of $\mathbf{F}_{16}^\times$ with basis α. For each of the 15 elements α^k with $0 \leq k \leq 14$, tell which one is the irreducible polynomial of α^k.

Exercise 113. Let $\mathbf{F}_q$ 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 $\mathbf{F}_{p^2}$. For a and b in $\mathbf{F}_p$, check

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

(Automorphisms of $\mathbf{F}_{p^2}$).

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

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 $\mathbf{F}_{p^n}$ into $\mathbf{F}_{p^m}$. Such a morphism is not unique if $n < m$: if we compose it with the Frobenius over $\mathbf{F}_p$, we get another one. For each $n|m$, we choose one of them, say $\iota_{n,m}$, which allow us to consider $\mathbf{F}_{p^n}$ as a subfield of $\mathbf{F}_{p^m}$.Then one checks that the union of the increasing family of fields $\mathbf{F}_{p^{n!}}$ is an algebraic closure of $\mathbf{F}_p$.

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

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

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

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

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

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

lis the canonical surjective morphism.

We also have

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

See, for instance, [5] exercise 19 p. 635. and [7] Appendice.

References

[1] E. Bombieri, *Continued fractions and the Markoff tree*, Expo. Math., 25 (2007), pp. 187–213.

[2] E. Bombieri and A. J. van der Poorten, *Continued fractions of algebraic numbers*, in Computational algebra and number theory (Sydney, 1992), vol. 325 of Math. Appl., Kluwer Acad. Publ., Dordrecht, 1995, pp. 137–152.

[3] J. W. S. Cassels, *An introduction to Diophantine approximation*, Hafner Publishing Co., New York, 1972. Facsimile reprint of the 1957 edition, Cambridge Tracts in Mathematics and Mathematical Physics, No. 45.

[4] M. Demazure, *Cours d'algèbre*, Nouvelle Bibliothèque Mathématique [New Mathematics Library], 1, Cassini, Paris, 1997. Primalité. Divisibilité. Codes. [Primality. Divisibility. Codes].

[5] D. S. Dummit and R. M. Foote, *Abstract algebra*, John Wiley & Sons, Inc., Hoboken, NJ, third ed., 2004.

[6] P. Flajolet, B. Vallée, and I. Vardi, *Continued fractions from euclid to the present day.* 44p.
`http://www.lix.polytechnique.fr/Labo/Ilan.Vardi/continued_fractions.ps`.

[7] M. Hindry, *Arithmetics*, Universitext, Springer, London, 2011. Translated from the 2008 French original.

[8] H. Lambert, *Mémoire sur quelques propriétés remarquables des quantités transcendantes circulaires et logarithmiques*, Mémoires de l'Académie des Sciences de Berlin, 17 (1768), pp. 265–322. Math. Werke, t. II
http://www.bibnum.education.fr/mathematiques/theorie-des-nombres/lambert-et-l-irrationalite-de-n-1761.

[9] S. Lang, *Algebra*, vol. 211 of Graduate Texts in Mathematics, Springer-Verlag, New York, third ed., 2002.

[10] R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications*, Cambridge University Press, Cambridge, first ed., 1994.

[11] O. Perron, *Die Lehre von den Kettenbrüchen. Dritte, verbesserte und erweiterte Aufl. Bd. II. Analytisch-funktionentheoretische Kettenbrüche*, B. G. Teubner Verlagsgesellschaft, Stuttgart, 1957.

[12] D. Roy, *On the continued fraction expansion of a class of numbers*, in Diophantine approximation, vol. 16 of Dev. Math., SpringerWienNewYork, Vienna, 2008, pp. 347–361.
http://arxiv.org/abs/math/0409233.

[13] V. Shoup, *A computational introduction to number theory and algebra*, Cambridge University Press, Cambridge, second ed., 2009. http://shoup.net/ntb/.

[14] A. J. van der Poorten, *An introduction to continued fractions*, in Diophantine analysis (Kensington, 1985), vol. 109 of London Math. Soc. Lecture Note Ser., Cambridge Univ. Press, Cambridge, 1986, pp. 99–138.

Michel WALDSCHMIDT
Sorbonne Universités
UPMC Univ Paris 06, UMR 7586-IMJ
F–75005 Paris France
michel.waldschmidt@imj-prg.fr