Corps de Galois

Jean-François Burnol, 24 septembre 2010

La caractéristique d'un anneau A est l'ordre de 1_A dans le groupe additif de A : le plus petit entier strictement positif n avec $1_A + 1_A + \cdots + 1_A = 0_A$ (n termes 1_A), ou, si un tel n n'existe pas, zéro. Si A est intègre [1], alors caract.(A) est soit nulle, soit un nombre premier p. Dans le premier cas, on peut considérer $\mathbf{Z}$ comme inclus dans A et dans le deuxième c'est $\mathbf{Z}/p\mathbf{Z} \subset A$.

Prenons le cas d'un anneau commutatif intègre A de cardinalité finie. Pour tout $x \in A$ non nul, la multiplication $y \mapsto xy$ est injective donc bijective, donc x a un inverse, et A est en fait un corps. [2] Cela s'applique en particulier à $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ qui est un corps. Tout anneau de caractéristique p est un $\mathbf{F}_p$-espace vectoriel. Un corps fini A sera donc un espace vectoriel sur $\mathbf{F}_p$ de dimension finie $n \geq 1$. Ainsi $\#A = q = p^n$.

Le principal objet de cette fiche est d'établir (pas forcément dans cet ordre) :

1. pour tout p premier et $n \geq 1$ il existe un corps $\mathbf{F}_q$ de cardinalité p^n,
2. deux tels corps $\mathbf{F}_q$ sont toujours isomorphes,
3. si K est une clôture algébrique de $\mathbf{F}_p$ alors il y a inclus dans K un unique sous-corps $\mathbf{F}_q$ de cardinalité $q = p^n$,
4. les sous-corps de $\mathbf{F}_{p^n}$ sont les $\mathbf{F}_{p^m}$ avec m diviseur de n,
5. le corps $\mathbf{F}_q$ a précisément n automorphismes qui sont l'automorphisme de Frobenius $\varphi(x) = x^p$ et ses itérés (avec $\varphi^n = \mathrm{Id}$ sur $\mathbf{F}_q$, en fait $\mathbf{F}_q = \{x \in K, x^{p^n} = x\}$),
6. $K = \bigcup_n \mathbf{F}_{p^n}$. [3]

Au passage on montrera aussi :

7. le groupe multiplicatif $\mathbf{F}_q^*$ est cyclique.

Naïvement on pourrait penser que trouver dans $\mathbf{F}_p[t]$ un polynôme irréductible π de degré n serait une excellente façon de construire un $\mathbf{F}_q$ via $\mathbf{F}_q = \mathbf{F}_p[t]/(\pi)$. Mais ce n'est pas si trivial et/ou immédiat de prouver qu'un tel π existe ! Aller dans cette direction des polynômes irréductibles n'est pas la voie la plus rapide, elle oblige à pas mal travailler et peut d'ailleurs emmener très loin (par exemple jusqu'à l'étude des corps cyclotomiques $\mathbf{Q}[e^{2\pi i \frac{1}{N}}]$ mais il nous faudrait alors absorber la théorie des idéaux d'entiers algébriques ! aïe...). Nous emprunterons donc cette voie seulement dans un deuxième temps, et sans trop pousser. Nous redémontrerons plusieurs fois

1. Dans un anneau intègre on a nécessairement $1_A \neq 0_A$, autrement dit l'anneau nul n'est pas intègre. Cette convention permet de parler du corps des fractions associé à tout anneau intègre et est aussi compatible au fait de ne pas considérer $1 \in \mathbf{Z}$ comme un nombre premier, puisque d'une manière générale on dit qu'un idéal $I \subset A$ est premier si A/I est intègre.

2. Nos corps sont commutatifs ; nous utiliserions la terminologie «corps gauche» pour les corps non-commutatifs. Le théorème de Wedderburn affirme que les corps gauches finis sont commutatifs.

3. Attention, contrairement aux corps finis $\mathbf{F}_q$, le corps K a d'autres automorphismes que les itérés de φ : par exemple φ^{-1} et il y en a même d'autres que les φ^n, $n \in \mathbf{Z}$. cf. infra.

la même chose, abondance ne nuit pas en Mathématiques. Quoi qu'il en soit, quelle que soit l'approche suivie, on ne peut qu'être amené rapidement à LA chose vraiment cruciale, qui est l'**endomorphisme de Frobenius**.

Soit donc k un éventuel corps fini de caractéristique p, de cardinalité $q = p^n$. Le groupe multiplicatif k^* a $q-1$ éléments et par le Théorème de Lagrange :

$$\forall x \in k^* \qquad x^{q-1} = 1 \tag{1}$$

Lorsque $k = \mathbf{F}_p$ c'est le Petit Théorème de Fermat. Il est utile de remettre cette équation sous la forme

$$\forall x \in k \qquad x^q = x \tag{2}$$

Et là, la personne astucieuse se dit : si je peux trouver un corps $L \supset \mathbf{F}_p$ dans lequel $x^q - x$ se factorise entièrement en $x^q - x = \prod (x-\lambda)^{n_\lambda}$, peut-être me suffit-il alors de définir k comme étant l'ensemble des racines λ ? On est alors immédiatement amené à se demander : comment montrer que l'ensemble de ces racines est stable par addition et multiplication ? pour la multiplication, ok, mais pour l'addition, ou plutôt la soustraction, eh bien on doit regarder $(x-y)^q$. Ceci est l'itéré n fois de $x - y \mapsto (x-y)^p$, et au final on est immanquablement amené à découvrir le :

1 Frobenius

Définissons, dans n'importe quel anneau A **commutatif** de caractéristique p une application par

$$\forall y \qquad \varphi(y) = y^p \tag{3}$$

Comme p divise $p! = j!(p-j)!\binom{p}{j}$ et est premier à $j!(p-j)!$ pour $1 \leq j \leq p$, il divise le coefficient du binôme $\binom{p}{j}$ et par conséquent :

$$\forall y_1, y_2 \in A \quad (y_1 - y_2)^p = y_1^p - y_2^p \tag{4}$$

où l'on a utilisé que $(-1)^p$ est toujours égal à -1, soit parce que p est impair, soit parce que $p = 2$ et alors $-1 = 1$ (sic). Comme par ailleurs il est vrai que $(xy)^p = x^p y^p$, on a bien un morphisme d'anneau, qui d'ailleurs est injectif si A est intègre ($y_1^p - y_2^p = 0 \implies (y_1 - y_2)^p = 0$). Il est donc aussi **bijectif** si de plus A est fini (donc un corps).

On dit de φ qu'il est **l'endomorphisme de Frobenius**. Si on applique cela à $\mathbf{F}_p$ on peut redécouvrir le Petit Théorème de Fermat : car il est clair que $\mathbf{F}_p$ a uniquement l'identité comme automorphisme. En effet puisque $\varphi(1) = 1$, il faut $\varphi(2) = \varphi(1) + \varphi(1) = 2$, $\varphi(3) = \varphi(1) + \varphi(2) = 3$, etc...donc $\forall y \in \mathbf{F}_p$ $y^p = \varphi(y) = y$. Notons au passage que cela montre que $\varphi : A \to A$ est aussi un endomorphisme de A comme $\mathbf{F}_p$-espace vectoriel.

Le polynôme $X^p - X$ a p racines distinctes dans $\mathbf{F}_p$ et par conséquent se scinde entièrement en $X(X-1)\cdots(X-p+1)$ dans $\mathbf{F}_p[X]$. Il en résulte que dans tout anneau A de caractéristique p on a

$$\forall y \in A \qquad y^p - y = y(y-1)\cdots(y-p+1) \tag{5}$$

Donc si A est intègre $y^p = y \iff y \in \mathbf{F}_p$.

Soit maintenant $L \supset \mathbf{F}_p$ un corps, et k défini par :

$$k = \{x \in L, \quad x^q = x\} \tag{6}$$

C'est l'ensemble des points fixes de l'automorphisme itéré φ^n de L, **donc certainement k est un sous-corps de L.** La cardinalité de k est le nombre de solutions dans L de l'équation $x^q - x = 0$. Supposons qu'on ait pu choisir L de sorte que le polynôme $P = X^q - X$ se scinde dans l'anneau L[X] :

$$P = X^q - X = \prod (X-\lambda)^{n_\lambda}, \text{ avec des } \lambda \in L. \tag{7}$$

Donc k est l'ensemble des racines λ. Or $P' = -1$, donc $n_\lambda \geq 2$ est impossible. Comme $\deg(P) = q$ on a $\#k = q$ comme espéré.

2 Complétion de la preuve d'existence d'un corps de cardinalité p^n

Il nous suffit donc d'établir le résultat général de la théorie des corps :

Théorème 1. *Soit* K *un corps et* $P \in K[X]$ *un polynôme non constant. Il existe un corps* L *contenant* K *tel que* P *se scinde complètement dans* L[X].

Preuve : soit $n = \deg(P) \geq 1$. On raisonne par récurrence sur n. Parmi les diviseurs non constants Q dans K[X] de P il y en a au moins un dont le degré est minimal. Donc ce Q est irréductible et on sait alors que la K-algèbre quotient $K_1 = K[X]/(Q)$ est un corps (en effet pour tout U non divisible par Q, $\mathrm{pgcd}(U, Q) = 1$ et on a une identité de Bezout $AU + BQ = 1$ qui en passant au quotient donne un inverse de la classe de U). Pour éviter des confusions toujours possibles, on va plutôt prendre une autre indéterminée T et définir $K_1 = K[T]/(Q(T))$. On peut considérer K comme inclus dans K_1. Soit λ égal à l'image de T dans K_1. Par construction $Q(\lambda) = 0$. Par un résultat important cela signifie que $X - \lambda$ divise Q, et donc aussi P, dans l'anneau $K_1[X]$. Ainsi $P = (X-\lambda)P_1$ avec $P_1 \in K_1[X]$. L'hypothèse de récurrence (trivialement vraie pour $n = 1$) permet de conclure.

Résumons :

Théorème 2. *Soit* $n \geq 1$ *et* $q = p^n$. *Il existe un corps de cardinalité* q. *Pour qu'un corps* $L \supset \mathbf{F}_p$ *contienne un sous-corps* k *de cardinalité* q *il est nécessaire et suffisant que* $X^q - X$ *soit scindé sur* L, *et* k *est alors unique et est l'ensemble des racines de* $X^q - X$, *c'est-à-dire l'ensemble des points fixes du* n^e *itéré de l'endomorphisme de Frobenius agissant sur* L.

3 Le groupe multiplicatif d'un corps fini est cyclique

Rappelons qu'un groupe cyclique est un groupe isomorphe au groupe additif $\mathbf{Z}/N\mathbf{Z}$ (cardinalité finie si $N \geq 1$). Notons d'une manière générale $< x >$ le groupe engendré par un élément x d'un groupe quelconque. Pour $\mathbf{Z}/N\mathbf{Z}$ on a $< x >= \mathbf{Z}/N\mathbf{Z}$ si et seulement si il existe $a \in \mathbf{Z}$ avec $ax = 1$ si et seulement si x est premier à N. Le nombre de générateurs est donc $\phi(N)$ (fonction d'Euler). Comptons les éléments x d'ordre d où d est un diviseur de N. L'équation $dx = 0 \bmod N$ signifie $x = 0 \bmod \frac{N}{d}$, donc x est parmi les multiples de $\frac{N}{d}$, $x = k\frac{N}{d}$, $0 \leq k < d$, et $< x > \subset < \frac{N}{d} >$. Pour que $\# < x >= d$ il est nécessaire et suffisant qu'il existe j avec $jx = \frac{N}{d}$, soit $jk\frac{N}{d} = \frac{N}{d} \bmod N$ soit (puisque $\frac{N}{d}$ divise N), $jk = 1 \bmod d$. Il y a donc précisément $\phi(d)$ éléments d'ordre d dans $\mathbf{Z}/N\mathbf{Z}$ et on obtient en particulier l'identité :

$$N = \sum_{d \mid N} \phi(d) \tag{8}$$

Faisons le même genre de décompte directement dans le groupe multiplicatif k^* d'un corps k de cardinalité $q = p^n$. Soit $N = q - 1 = p^n - 1$. Prenons $x \in k^*$ et considérons le groupe cyclique $< x >$ qu'il engendre. Il a cardinalité d avec $d \mid N$ et $x^d - 1 = 0$. On peut factoriser le polynôme $t^d - 1$ dans $k[t]$ en $\prod_{0 \leq j < d}(t - x^j)$ puisque $1, x, \ldots, x^{d-1}$ en sont déjà d racines distinctes dans k. Tout autre $y \in k^*$ d'ordre d vérifie $y^d = 1$, donc est racine de ce polynôme et par conséquent de la forme x^j. Or x^j est d'ordre d si et seulement si j est premier à d (on a un isomorphisme $< x > \simeq \mathbf{Z}/d\mathbf{Z}$ qui fait correspondre j mod d à x^j). Il y a donc précisément $\phi(d)$ éléments y dans k^* d'ordre d dès qu'il y en a au moins un. Notons $\mathcal{D}$ l'ensemble des diviseurs d de $N = q - 1$ pour lesquels on peut trouver un élément d'ordre d. On a donc

$$N = \sum_{d \in \mathcal{D}} \phi(d) \tag{9}$$

La comparaison de (8) et (9) impose la conclusion que $\mathcal{D}$ contient tous les diviseurs de N, en particulier N lui-même. Par conséquent :

Théorème 3. *Le groupe multiplicatif* k^* *d'un corps fini est cyclique.*

4 Existence de polynômes irréductibles de degrés arbitraires

Théorème 4. *Pour chaque* $n \geq 1$ *il existe dans* $\mathbf{F}_p[X]$ *un polynôme irréductible de degré* n.

Preuve : soit k de cardinalité $q = p^n$ et x un générateur du groupe cyclique k^*. Alors le morphisme de k-algèbres $\mathbf{F}_p[X] \to k$ qui envoie X sur x est surjectif, donc le générateur unitaire π de son noyau (polynôme minimal de x) est de degré $\dim_{\mathbf{F}_p} k = n$. Or π est irréductible puisque $\mathbf{F}_p[X]/(\pi) \simeq k$ est un corps.

5 Isomorphismes des corps de même cardinalité

Théorème 5. *Deux corps finis de même cardinalité sont isomorphes.*

Preuve : soit k_1 et k_2 deux corps de même cardinalité $q = p^n$. Soit $x \in k_1$ générateur du groupe cyclique k_1^* et soit π son polynôme minimal. C'est un irréductible de $\mathbf{F}_p[X]$ et $\mathbf{F}_p[X]/(\pi) \simeq k_1$ (en envoyant X sur x, la surjectivité puisque x engendre k_1^*). De plus, comme $x_1^q = x_1$, on sait que π divise le polynôme $X^q - X$, disons $X^q - X = \pi T$. Dans k_2, on a $\forall y \in k_2, y^q = y$, donc $\forall y \in k_2, \pi(y)T(y) = 0$. Or $\deg(T) = q - n < q$, donc il existe y dans k_2 avec $T(y) \neq 0$. Par conséquent $\pi(y) = 0$. Mais π est irréductible sur $\mathbf{F}_p$, c'est donc le polynôme minimal de y. Par conséquent on a un isomorphisme $\mathbf{F}_p[X]/(\pi) \to \mathbf{F}_p[y] \subset k_2$ qui envoie X sur y. Ainsi k_1 est isomorphe a un sous-corps de k_2, mais comme $\#k_1 = \#k_2$, c'est que $k_1 \simeq k_2$.

On utilisera la notation $\mathbf{F}_q$ pour désigner tout corps fini de cardinalité q.

6 Automorphismes d'un corps fini $\mathbf{F}_q$

Théorème 6. *Le corps fini* $\mathbf{F}_q$, $q = p^n$, *a précisément* n *automorphismes qui sont* Id, $\varphi, \ldots, \varphi^{n-1}$, *avec* φ *le Frobenius* $x \mapsto x^p$.

Preuve : le Frobenius et ses itérés sont des automorphismes de $\mathbf{F}_q$. On peut considérer le Frobenius φ comme une permutation de l'ensemble fini $\mathbf{F}_q$, et regarder sa décomposition en cycles disjoints, aussi appelés orbites. Comme φ itéré n-fois est l'identité, les orbites ont des longueurs qui sont des diviseurs de n. Prenons en particulier x un générateur du groupe multiplicatif. Alors $x, x^p, \ldots, x^{p^{n-1}}$ sont distincts et l'orbite de x a précisément n éléments. Soit π le polynôme minimal de x, il est de degré n. Comme π est à coefficients dans $\mathbf{F}_p$ on a :

$$\forall y \in k \quad \varphi(\pi(y)) = \pi(\varphi(y)) \tag{10}$$

Donc, non seulement x mais aussi ses images sous φ sont des racines de π. On a n racines, ce sont donc toutes les racines de π. Si σ est un autre automorphisme, avec lui aussi on a

$$\forall y \in k \quad \sigma(\pi(y)) = \pi(\sigma(y)) \tag{11}$$

Donc $\sigma(x)$ est aussi racine de π. Par conséquent il existe un j avec $\sigma(x) = \varphi^j(x)$. Mais alors $\sigma(x^k) = \sigma(x)^k = (\varphi^j(x))^k = \varphi^j(x^k)$ pour tout $k \in \mathbf{Z}$ et donc $\sigma = \varphi^j$ sur $\mathbf{F}_q^*$ et donc sur $\mathbf{F}_q$.

7 Sous-corps d'un $\mathbf{F}_q$

Théorème 7. *Soit* $k = \mathbf{F}_q$, $q = p^n$. *Il existe dans* k *un sous-corps* k_m *de cardinalité* p^m *si et seulement si* m *divise* n *et alors* k_m *est unique.*

Preuve : s'il existe $k_m \subset k$ de cardinalité p^m, on sait en prenant un générateur x_m du groupe multiplicatif k_m^* qu'il existe dans k_m (donc dans k) une orbite du Frobenius φ de longueur m. Ainsi m divise n puisque $\varphi^n = \mathrm{Id}$ sur k. Réciproquement, on sait que pour trouver un tel k_m dans k, qui sera unique, il suffit de montrer que le polynôme $X^{p^m} - X$ est scindé dans k, ou encore que $X^M - 1$, avec $M = p^m - 1$ est scindé dans k. Mais si m divise n alors $M = p^m - 1$ divise $N = p^n - 1$ (exercice), donc $X^M - 1$ divise $X^N - 1$ (exercice) dans $\mathbf{F}_p[X]$. Comme $X^N - 1$ est scindé dans k il en est de même de $X^M - 1$.

8 Clôture algébrique

Si l'on admet l'existence d'une clôture algébrique K de $\mathbf{F}_p$, la preuve de l'existence d'un corps de cardinalité p^n tient en une ligne (modulo le fait de savoir que le Frobenius est un morphisme de corps) :

$$k_n = \{x \in \overline{\mathbf{F}_p}, \quad x^{p^n} = x\} \tag{12}$$

Comme tout élément x de $\overline{\mathbf{F}_p}$ est algébrique sur $\mathbf{F}_p$ il est contenu dans un corps fini et $\overline{\mathbf{F}_p} = \bigcup_{n\geq 1} k_n$.

L'avantage de l'emploi d'une clôture algébrique c'est qu'elle rend la notation $\mathbf{F}_q$ pour les corps de cardinalité q beaucoup plus rigoureuse : en effet chaque $\mathbf{F}_q$ n'est a priori connu qu'à isomorphisme près. Alors qu'une fois qu'un $K = \overline{\mathbf{F}_p}$ est supposé connu, on a pour chaque n un corps de cardinalité p^n bien déterminé.

Théorème 8. *À toute suite* $\sigma = (m_N)_{N\geq 2}$ *de nombres entiers vérifiant les conditions :*

1. $0 \leq m_N < N!$,
2. $\forall N,\ m_{N+1} \equiv m_N \mod N!$.

est associé un unique automorphisme ψ_σ *de* $\overline{\mathbf{F}_p}$ *vérifiant*

$$\forall x \in \mathbf{F}_{p^{N!}} \qquad \psi_\sigma(x) = \varphi^{m_N}(x) \tag{13}$$

et ce sont là tous les automorphismes de $\overline{\mathbf{F}_p}$.

La preuve est laissée au lecteur. En particulier φ^{-1} est obtenu avec $m_N = N! - 1$. Notons que le composé de deux automorphismes ne dépend pas de l'ordre et correspond à additionner les m_N modulo N!. Il est amusant que le groupe des automorphismes ne dépende pas (en tant que groupe abstrait) du nombre premier p.

9 Où l'on repart de zéro (enfin, du Frobenius)

On reprend tout quasiment à zéro, comme si on n'avait rien fait. On aborde le problème via la recherche d'un irréductible π de degré n dans $\mathbf{F}_p[X]$. Procédons

d'abord par conditions nécessaires. Notons x l'image de l'indéterminée X dans $k = \mathbf{F}_p[X]/(\pi)$. Le groupe multiplicatif k^* a cardinalité $q-1$ et donc par le théorème de Lagrange $x^{q-1} = 1$, $x^q = x$. Donc π divise dans $\mathbf{F}_p[X]$ le polynôme $X^q - X$, $q = p^n$.

On est amené à s'intéresser aux diviseurs irréductibles de $X^q - X$. Soit P l'un d'entre eux, de degré m. Considérons le corps $k_1 = \mathbf{F}_p[X]/(P)$, et l'image x_1 de X dans k_1. Utilisons l'automorphisme de Frobenius φ comme une permutation de l'ensemble fini $k_1 = \mathbf{F}_p[x_1]$. Considérons le cycle débutant par x_1, il y a un plus petit M avec $\varphi^M(x_1) = x_1$. On sait aussi que $\varphi^n(x_1) = x_1$ (puisque $\varphi^n(x_1) = x_1^q$), donc M divise n.

Comme P est à coefficients dans $\mathbf{F}_p$, on a $\forall y\ \varphi(P(y)) = P(\varphi(y))$. Par conséquent x_1 et ses M itérés distincts sous φ sont des racines de P et le degré de P est ainsi au moins égal à M. Mais considérons le polynôme de degré M :

$$(14) \qquad Q(X) = (X - x_1)(X - \varphi(x_1)) \cdots (X - \varphi^{M-1}(x_1)) = X^M - a_1 X^{M-1} + \cdots + (-1)^M a_M$$

Les coefficients sont $a_j = \sigma_j(x_1, \varphi(x_1), \ldots, \varphi^{M-1}(x_1))$ où σ_j est le j^e polynôme symétrique en M lettres, réduit modulo p. Comme φ permute les racines, $\varphi(a_j) = a_j$, et donc $a_j \in \mathbf{F}_p$. Donc $Q \in \mathbf{F}_p[X]$, et comme $Q(x_1) = 0$, Q est divisible par P et par conséquent le degré de P est au plus M.

Au final le degré m de P est M et **est donc un diviseur de n**. De plus comme $\varphi^m(x_1) = x_1$, on en déduit que P divise le polynôme $X^{p^m} - X$. Nous avons réuni les informations suivantes : tous les facteurs irréductibles P de $X^q - X$ ont leurs degrés parmi les diviseurs de n (avec $q = p^n$). Si $\deg(P) = m$ alors P divise aussi $X^{p^m} - X$.

Cela va nous permettre de prouver qu'il existe un facteur irréductible de $X^q - X$ de degré n via des calculs sur $\mathbf{C}$! Visiblement on doit s'intéresser à des racines de l'unité d'ordre $p^a - 1$ pour des entiers a parcourant les diviseurs de n. Toute racine M^e de l'unité avec $M = p^m - 1$ est aussi une racine N^e de l'unité avec $N = p^n - 1$ lorsque m divise n, puisqu'alors $p^m - 1$ divise $p^n - 1$.

Notons que chaque polynôme unitaire $X^M - 1$ n'a que des racines simples dans $\mathbf{C}$ donc ses facteurs irréductibles unitaires Q_j dans $\mathbf{Z}[X]$ sont distincts. Prenons la collection de tous les diviseurs m de n, **sauf** n, et les $M = p^m - 1$ associés. Le PPCM des polynômes $X^M - 1$ est le produit, sans répétition, de tous les Q_j qui interviennent dans un au moins des $X^M - 1$. Notons-le U. Il divise $X^N - 1$ dans $\mathbf{Z}[X]$, car chacun des Q_j est aussi dans la décomposition de $X^N - 1$ en produits d'irréductibles puisque chaque $X^M - 1$ divise $X^N - 1$.

De plus on a $\deg(U) < N$. En effet toute racine complexe de U est un zéro de l'un des Q_j donc de l'un au moins des $X^M - 1$. Par conséquent, le nombre complexe $e^{2\pi i \frac{1}{N}}$ qui annule $X^N - 1$ n'est pas racine de U. Réduisons modulo p la relation $X^N - 1 = UV$ valable dans $\mathbf{Z}[X]$. On a $\deg \widetilde{U} = \deg U < N$. Mais comme U est multiple dans $\mathbf{Z}[X]$ de chaque $X^M - 1$, il en est de même pour $\widetilde{U}$ dans $\mathbf{F}_p[X]$. Donc $X\widetilde{U}$ est multiple de chaque $X(X^M - 1) = X^{p^m} - X$, m diviseur de n, $m \neq n$ et de plus $\deg(X\widetilde{U}) < \deg(X^{p^n} - X)$. La décomposition de $P = X^{p^n} - X$ en facteurs irréductibles unitaires de $\mathbf{F}_p[X]$ n'a

aucune multiplicité, car $\pi^2 \mid P \implies \pi \mid P'$ or $P' = -1$. Si l'on écrit $P = X\widetilde{U}\prod_j \pi_j$ les irréductibles π_j sont donc premiers avec $X\widetilde{U}$ et par conséquent premiers avec chaque $X^{p^m} - X$, m diviseur de n, $m \neq n$. D'après ce qui précède on a $\deg \pi_j = n$ pour chaque j. À ce stade nous avons donc (re)-prouvé qu'il existe bel et bien (au moins) un corps de cardinalité $q = p^n$!

10 Structure des corps finis (on recommence encore une fois)

Reprenons à nouveau à zéro. Nous avons juste besoin de savoir que $\varphi : y \mapsto y^p$ est un automorphisme du corps k de cardinalité $q = p^n$. Le groupe multiplicatif k^* a $q - 1$ éléments, et par le Théorème de Lagrange, $x^{q-1} = 1$ pour tout $x \neq 0$ et donc $x^q = x$ pour tout x et par conséquent $\varphi^n = \mathrm{Id}$. En effet φ^2 est $x \mapsto x^{p^2}$, etc...

On peut considérer le morphisme $\mathbf{Z} \to \mathrm{Aut}(k)$, $m \mapsto \varphi^m$ et il existe un plus petit $m \geq 1$ qui engendre le noyau, donc m divise n. Cependant $\varphi^m = \mathrm{Id}$ dit que $x^{p^m} = x$ pour tout x, or cette équation a au plus p^m racines distinctes, donc en fait $m = n$. On a donc trouvé n automorphismes de k, à savoir Id, φ, ..., φ^{n-1}.

Un lemme classique d'Artin nous dit que k automorphismes $\sigma_1, \ldots, \sigma_k$ distincts d'un corps k sont toujours linéairement indépendants sur k, au sens où si

$$\forall x \qquad \alpha_1\sigma_1(x) + \cdots + \alpha_k\sigma_k(x) = 0 \tag{15}$$

alors $\alpha_1 = \cdots = \alpha_k = 0$. Montrons le par récurrence. C'est vrai pour $k = 1$. Supposons le vrai pour $k - 1 \geq 1$. Soit y avec $\sigma_1(y) \neq \sigma_k(y)$, alors

$$\forall x \qquad \alpha_1\sigma_1(y)\sigma_1(x) + \cdots + \alpha_k\sigma_k(y)\sigma_k(x) = 0 \tag{16}$$

En multipliant la première équation par $\sigma_k(y)$ et en soustrayant :

$$\alpha_1(\sigma_k(y)-\sigma_1(y))\sigma_1(x)+\alpha_2(\sigma_k(y)-\sigma_2(y))\sigma_1(x)+\cdots+\alpha_{k-1}(\sigma_k(y)-\sigma_{k-1}(y))\sigma_1(x) = 0 \tag{17}$$

Par l'hypothèse de récurrence $\alpha_1(\sigma_k(y) - \sigma_1(y)) = 0$ et donc $\alpha_1 = 0$. Puis $\alpha_2 = \cdots = \alpha_k = 0$ à nouveau par l'hypothèse de récurrence.

Par conséquent il est impossible de trouver $\alpha_0, \ldots, \alpha_{n-1}$ non tous nuls avec

$$\forall x \in k \qquad \alpha_0 x + \alpha_1\varphi(x) + \cdots + \alpha_{n-1}\varphi^{n-1}(x) = 0 \tag{18}$$

Ceci est en particulier vrai si l'on se restreint à $\alpha_j \in \mathbf{F}_p$, $0 \leq j \leq n - 1$ et dit que le polynôme minimal de φ comme $\mathbf{F}_p$-endomorphisme du $\mathbf{F}_p$-espace vectoriel k est au moins de degré n. Ce polynôme minimal M_φ est donc précisément $X^n - 1$.

Or, nous savons par la théorie de la réduction des endomorphismes qu'il existe un x tel que M_φ soit aussi le polynôme minimal annulateur de x. L'espace cyclique

engendré par x sous φ a dimension $\deg M_\varphi = n = \dim k$, et par conséquent k a comme base vectorielle $(x, x^p, x^{p^2}, \ldots, x^{p^{n-1}})$.

Soit $f : k \to k$ l'endomorphisme $y \mapsto xy$. On remarque que k est engendré comme $\mathbf{F}_p$ espace vectoriel par 1, $f(1) = x$, $f(x) = x^2$, ..., puisqu'il est engendré par x, x^p, ..., $x^{p^{n-1}}$. Donc k est cyclique pour f, de vecteur générateur 1. Soit π le polynôme minimal unitaire de f, c'est le polynôme unitaire de plus bas degré avec $\pi(x) = 0$. Il est donc irréductible. Le morphisme d'anneaux $\mathbf{F}_p[X] \mapsto k$ qui envoie X sur x est surjectif (puisque k est engendré par 1, x, x^2, ...), son noyau est l'idéal engendré par π et on a un isomorphisme d'anneaux $\mathbf{F}_p[X]/(\pi) \to k$. De plus $n = \dim \mathbf{F}_p[X]/(\pi) = \deg \pi$.

Comme π est à coefficients dans $\mathbf{F}_p$, de $\pi(x) = 0$ résulte $\varphi(\pi(x)) = \pi(\varphi(x)) = 0$, puis $\pi(\varphi^2(x)) = 0$, etc...Donc π s'annule sur x, x^p, ..., $x^{p^{n-1}}$ et par conséquent :

$$\pi = \prod_{0 \le j \le n-1} (t - x^{p^j}) \qquad \pi \in \mathbf{F}_p[t] \tag{19}$$

Si σ est un autre automorphisme de k, on remarque tout d'abord que $\sigma(y^p) = \sigma(y)^p$ pour tout y, donc que σ commute nécessairement avec φ. De plus de $0 = \sigma(\pi(x)) = \pi(\sigma(x))$ résulte qu'il existe un j avec $\sigma(x) = \varphi^j(x)$. Mais alors $\sigma(\varphi^m(x)) = \varphi^m(\sigma(x)) = \varphi^{j+m}(x) = \varphi^j(\varphi^m(x))$, pour tout m. Comme $(x, x^p, x^{p^2}, \ldots, x^{p^{n-1}})$, engendre k comme $\mathbf{F}_p$-espace vectoriel, il en résulte que $\sigma(y) = \varphi^j(y)$ pour tout élément de k. On a donc montré $\sigma = \varphi^j$ et par conséquent les seuls automorphismes de k sont Id, φ, ..., φ^{n-1}.

Soit maintenant $k' \subset k$ un sous-corps. Il aura cardinalité p^m avec $m \le n$. Notons Ψ la restriction de φ à k'. On sait par ce qui précède que l'ordre de Ψ dans le groupe des automorphismes de k' est précisément m. Or $\varphi^n = \mathrm{Id}_k \implies \Psi^n = \mathrm{Id}_{k'}$, donc n est un multiple de m. De plus les éléments de k', en nombre p^m, vérifient $\Psi^m(x) = x$, autrement dit sont solutions de $x^{p^m} - x = 0$, équation qui a au plus p^m solutions. Ainsi, nécessairement :

$$k' = \{y \in k, y^{p^m} = y\} \tag{20}$$

Réciproquement, l'ensemble ainsi défini est bien un sous-corps car il est stable par différence et division. Cependant le fait que $\#k' = p^m$ demande démonstration (d'ailleurs on peut définir ainsi un k' pour tout m entier et c'est seulement lorsque m divise n que l'on aura $\#k' = p^m$.)

Pour cette justification, soit donc le corps $k' = \{y \in k, \varphi^m(y) = y\}$ et $a = \frac{n}{m}$. reprenons notre x déjà utilisé tel que les n éléments x, x^p, ..., $x^{p^{n-1}}$ forment une $\mathbf{F}_p$-base de k. Considérons

$$0 \le j < m \qquad y_j := x^{p^j} + x^{p^{m+j}} + x^{p^{2m+j}} + \cdots + x^{p^{(a-1)m+j}} \tag{21}$$

Comme il n'y aucun x^{p^r} commun à l'écriture de deux y_j avec des indices distincts, certainement $(y_0, \ldots, y_{m-1})$ est un système $\mathbf{F}_p$-linéairement indépendant (on notera

par ailleurs que $y_1 = y_0^p$, $y_2 = y_0^{p^2}$, ...). Il est de plus clair que $y_j^{p^m} = y_j$, car élever à la puissance p (ou p^m) commute avec les sommes et $ma = n$, $x^{p^n} = x$. La dimension de k' comme $\mathbf{F}_p$-espace vectoriel est donc au moins m et $\#k' \geq p^m$. Or $\#k' \leq p^m$ car l'équation $y^{p^m} - y = 0$ a au plus autant de solutions que son degré. En conclusion on a $\#k' = p^m$.

À ce stade on a donc trouvé la liste complète des sous-corps de k et montré que deux sous-corps de la même cardinalité sont égaux. Cependant dans cette approche on n'a pas montré qu'un k de cardinalité $q = p^n$ existe, on a juste étudié ses propriétés. On pourrait alors, dans une tentative désespérée de sauvetage, invoquer le deux ex machina «clôture algébrique», puis obtenir notre k via $k = \{x \in \overline{\mathbf{F}_p}, \quad x^{p^n} = x\}$.

11 Combinatoire et polynômes cyclotomiques

On peut étudier d'un peu plus près certains aspects combinatoires des groupes cycliques X de cardinalité N, $N \geq 2$. Soit $p_1, \ldots, p_r$ les diviseurs premiers distincts de N. Notons $A_j \subset X$ les éléments $y \in X$ dont l'ordre e(y) divise N/p_j. Vu dans $\mathbf{Z}/N\mathbf{Z}$ (une fois choisi un générateur de X) ce sont simplement les multiples de p_j. L'union des A_j est donc précisément le complémentaire de l'ensemble $Y \subset X$ des générateurs de X. La formule d'inclusion-exclusion donne l'identité de fonctions indicatrices :

$$\mathbf{1}_Y = 1 - \sum_j \mathbf{1}_{A_j} + \sum_{j_1<j_2} \mathbf{1}_{A_{j_1}\cap A_{j_2}} - \cdots + (-1)^r \mathbf{1}_{A_1\cap\cdots\cap A_r} \tag{22}$$

Comme $A_{j_1} \cap \cdots \cap A_{j_k}$ vu dans $\mathbf{Z}/N\mathbf{Z}$ est simplement l'ensemble des multiples de $p_{j_1} \ldots p_{j_k}$, c'est aussi précisément l'ensemble des y dont l'ordre e(y) divise $N/p_{j_1} \ldots p_{j_k}$. On va écrire notre formule (22) de manière plus sophistiquée via l'emploi de la

Fonction de Moebius

Définissons-la comme fonction de $\mathbf{N}^*$ vers $\{-1, 0, +1\}$ par les formules $\mu(1) = 1$, $\mu(p_1 \ldots p_r) = (-1)^r$ pour un produit de r premiers distincts et $\mu(n) = 0$ pour tous les autres. L'équation (22) devient (avec une notation multiplicative pour la loi de groupe) :

$$\mathbf{1}_Y = \sum_{d \mid N} \mu(d) \mathbf{1}_{\{y\in X, y^{\frac{N}{d}}=1\}} \tag{23}$$

Polynômes cyclotomiques

Nous appliquerons ce qui précède à deux groupes particuliers : le groupe des racines N^e de l'unité dans le plan complexe, et le groupe multiplicatif $\mathbf{F}_q^*$, avec $N = q-1$. Dans le premier cas Y est l'ensemble des racines N^e primitives de l'unité, dans le second

cas Y est l'ensemble des générateurs du groupe cyclique $\mathbf{F}_q^*$. Soit d un diviseur de N. Dans l'un comme l'autre cas nous savons que

$$t^{N/d} - 1 = \prod_{y \in X, y^{N/d}=1} (t - y) \tag{24}$$

Regardons maintenant la fraction rationnelle, dans le premier cas dans $\mathbf{C}(t)$ dans le deuxième cas dans $\mathbf{F}_q(t)$:

$$\prod_{d \mid N} (t^{N/d} - 1)^{\mu(d)} \tag{25}$$

Chaque terme $t^{N/d}-1$ se factorise entièrement dans $\mathbf{C}$, respectivement dans $\mathbf{F}_q$ en le produit des $t-y$ pris sur les N/d éléments y avec $y^{N/d} = 1$. La contribution complète d'un $t-y$ est $(t-y)^{a(y)}$ avec $a(y) = \sum_{d \mid N, y^{N/d}=1} \mu(d)$. Par la relation (23) $a(y) = 0$ sauf si $y \in Y$ auquel cas $a(y) = 1$. En conclusion :

$$\prod_{d \mid N} (t^{N/d} - 1)^{\mu(d)} = \prod_{y \in Y} (t - y) \tag{26}$$

Le polynôme de droite est appelé, dans le cas complexe, le N^e polynôme cyclotomique et est noté Φ_N. Il s'écrit, dans $\mathbf{C}[t]$:

$$\Phi_N = \prod_{0 \leq j < N,\ \mathrm{pgcd}(j,N)=1} (t - e^{2\pi i \frac{j}{N}}) \tag{27}$$

La somme débute à $j = 0$ uniquement pour gérer $N = 1$ (on a bien $\mathrm{pgcd}(0,1) = 1$). Considérons dans ce cas complexe les polynômes à coefficients entiers :

$$A = \prod_{d \mid N, \mu(d)=-1} (t^{N/d} - 1) \qquad B = \prod_{d \mid N, \mu(d)=+1} (t^{N/d} - 1) \tag{28}$$

Ainsi

$$A\Phi_N = B \tag{29}$$

vaut dans $\mathbf{C}[t]$ avec A et B à coefficients entiers, et A unitaire. Il en résulte par un argument simple (voir l'annexe) que Φ_N lui-même qui a priori est dans $\mathbf{C}[t]$ est en fait dans $\mathbf{Z}[t]$. On peut de plus prouver que **le polynôme cyclotomique Φ_N est irréductible dans $\mathbf{Q}[t]$**. Réfléchissez-y, c'est un bel énoncé. Par conformisme, je donne l'une des preuves classiques en annexe. Ainsi :

Théorème 9. *Pour chaque $N \geq 1$ le N^e polynôme cyclotomique Φ_N est à coefficients entiers et est irréductible sur $\mathbf{Q}$ (et dans $\mathbf{Z}[t]$). La factorisation (qui n'a pas de multiplicités)*

$$t^N - 1 = \prod_{d \mid N} \Phi_d \tag{30}$$

est la factorisation de $t^N - 1$ en irréductibles de $\mathbf{Q}[t]$ (ou de $\mathbf{Z}[t]$).

Preuve pour la factorisation : toute racine N^e de l'unité est une racine primitive d^e de l'unité pour un unique diviseur d de N. On notera le corollaire suivant :

Corollaire. *On a :* $\mathrm{pgcd}(t^n-1, t^m-1) = t^{\mathrm{pgcd}(n,m)}-1$.

Preuve directe simple : si $n = 0$ ou $m = 0$ (mais pas les deux) l'énoncé est vrai bien qu'assez spécial. Si $n \geq m > 0$ alors de $t^n - 1 = t^{n-m}(t^m-1) + t^{n-m} - 1$ résulte $\mathrm{pgcd}(t^n-1, t^m-1) = \mathrm{pgcd}(t^{n-m}-1, t^m-1)$ et la conclusion en découle par récurrence sur la valeur de $n+m$. L'argument fonctionne dans A[t] pour n'importe quel anneau intègre A (commutatif unitaire) : car il montre que tout diviseur commun divise $t^{\mathrm{pgcd}(n,m)}-1$. Celui-ci est lui-même un diviseur commun, donc il existe un pgcd dans ce cas.

Dans le cas de $k^* = \mathbf{F}_q^*$, et $N = q-1$, nous avons aussi dans k[t] :

$$\prod_{d\,|\,N,\mu(d)=-1} (t^{N/d}-1) \cdot \prod_{y\in k^*,e(y)=N} (t-y) = \prod_{d\,|\,N,\mu(d)=+1} (t^{N/d}-1) \tag{31}$$

La même relation vaut en remplaçant $\prod_{y\in k^*,e(y)=N}(t-y)$ par la réduction modulo p de Φ_N. Comme k[t] est intègre, c'est donc que

$$\prod_{y\in k^*,e(y)=N} (t-y) \equiv \Phi_N \mod p \tag{32}$$

En particulier le polynôme de gauche est un élément de $\mathbf{F}_p[t]$ (alors qu'a priori il est dans $\mathbf{F}_q[t]$). Tout générateur x de $\mathbf{F}_q^*$ vérifie donc $\Phi_N(x) = 0$, et son polynôme unitaire minimal $\pi \in \mathbf{F}_p[t]$, $\pi(x) = 0$ est un diviseur de Φ_N mod p.

Comme x n'est inclus dans aucun sous-corps propre de $\mathbf{F}_q$, l'orbite qu'il engendre sous le Frobenius est de cardinalité n. On peut donc partitionner les $\phi(N)$ générateurs en $\frac{1}{n}\phi(N)$ orbites de chacune n éléments (si x est un générateur, clairement $\varphi(x)$ l'est aussi). À chaque orbite est associée (cf equation (19)) le polynôme unitaire π qui a les éléments de l'orbite comme racines. On obtient ainsi $\frac{1}{n}\phi(N)$ polynômes unitaires π_α irréductibles distincts de degrés n qui divisent chacun Φ_N, donc Φ_N (modulo p) est le produit de ces π_α.

Théorème 10. *Soit* $N = p^n-1$. *La réduction modulo* p *du* N^e *polynôme cyclotomique est le produit de* $\frac{1}{n}\phi(N)$ *polynômes unitaires irréductibles distincts, tous de degrés* n. *Leurs racines dans une clôture algébrique de* $\mathbf{F}_p$ *sont les générateurs du groupe multiplicatif de* $\mathbf{F}_q$.

Exemple 1 : $p = 7$, $n = 1$, $N = 6$, $\phi(6) = 2$, $\Phi_6(t) = \frac{(t^6-1)(t-1)}{(t^3-1)(t^2-1)} = t^2 - t + 1$, $\Phi_6(t) \equiv (t-3)(t-5) \mod 7$. Parmi les 7 irréductibles unitaires de degré 1 seuls 2 correspondent à des générateurs du groupe multiplicatif de $\mathbf{Z}/7\mathbf{Z}$: $t-3$ et $t-5$.

Exemple 2 : $p = 3$, $n = 2$, $N = 9-1 = 8$, $\phi(8) = 4$, $\Phi_8(t) = t^4 + 1$ se factorise modulo 3 en $(t^2+t-1)(t^2-t-1)$. Mais il y a un troisième irréductible de degré 2 qui est t^2+1.

12 Combinatoire des polynômes irréductibles

La méthode d'inclusion-exclusion permet de compter combien il y a de polynômes irréductibles unitaires dans $\mathbf{F}_p[X]$ de degré n. Soit C_n ce nombre. Soit $\mathbf{F}_q$ un corps de cardinalité $q = p^n$. On sait que $X^q - X$ est scindé (sans multiplicité) par $\mathbf{F}_q$ et aussi que tout polynôme irréductible π de degré n divise $X^q - X$, donc en particulier a n racines dans $\mathbf{F}_q$. Pour chaque telle racine x, on a $\mathbf{F}_p[x] = \mathbf{F}_q$ et réciproquement.

Soit $q_1, q_2, \ldots, q_s$ la liste des diviseurs premiers distincts de l'entier n. Soit, pour $1 \leq j \leq s$, $A_j \subset \mathbf{F}_q$ l'ensemble des y tels que la dimension sur $\mathbf{F}_p$ de $\mathbf{F}_p[y]$ divise $\frac{1}{q_j}n$. En fait, A_j est $\mathbf{F}_{p^m}$, $m = \frac{1}{q_j}n$. Le complémentaire de l'union des A_j est précisément l'ensemble Z des éléments $x \in \mathbf{F}_q$ avec $\mathbf{F}_q = \mathbf{F}_p[x]$, ensemble qui par ce qui précède a nC_n éléments. Par ailleurs pour $j_1 < j_2 < \cdots < j_l$, l'intersection des A_{j_i} est l'ensemble des y tels que $\dim \mathbf{F}_p[y]$ divise $m = \frac{1}{q_{j_1} \cdots q_{j_l}}n$, c'est donc en fait précisément le sous-corps $\mathbf{F}_{p^m}$ de $\mathbf{F}_q$ qui a cardinalité p^m. La formule de comptage par inclusion-exclusion donne donc :

$$p^n - nC_n = \sum_j p^{\frac{1}{q_j}n} - \sum_{j_1<j_2} p^{\frac{1}{q_{j_1}q_{j_2}}n} + \cdots - (-1)^s p^{\frac{1}{q_{j_1}\cdots q_{j_s}}n} \tag{33}$$

Avec la fonction de Moebius, cela donne la formule plus compacte :

Théorème 11. *Le nombre* C_n *des polynômes irréductibles unitaires de degré* n *dans* $\mathbf{F}_p[X]$ *est donné par :*

$$nC_n = \sum_{d \mid n} \mu(d) p^{\frac{n}{d}} \tag{34}$$

Je laisse en exercice la formule duale :

$$p^n = \sum_{d \mid n} dC_d \tag{35}$$

Solution : oui, bon je devrais plus laisser réfléchir les gens. Définissez une fonction qui va de $\mathbf{F}_q$ vers l'ensemble des diviseurs d de n, via $d(x) = \dim \mathbf{F}_p[x]$. Nos arguments précédents montrent qu'il y a précisément dC_d éléments x avec $d(x) = d$. Ou alors, vous déduisez cette formule de la précédente par « inversion de Moebius ». Ou encore il suffit de dire que $X^q - X$ est le produit sans répétition de tous les irréductibles unitaires de degré un diviseur de n ($q = p^n$).

Je laisse pour conclure en exercice le théorème plus précis suivant, que vous pourrez prouver via l'emploi de fonctions indicatrices, et en imitant les preuves du chapitre précédent :

Théorème 12. *Le produit de tous les irréductibles unitaires de degré* n *de* $\mathbf{F}_p[X]$ *est donné par la formule* $\prod_{d \mid n}(X^{p^{n/d}} - X)^{\mu(d)}$.

Ce produit est nécessairement un multiple dans $\mathbf{F}_p[X]$ de la réduction modulo p du polynôme cyclotomique $\Phi_N(X)$, $N = p^n - 1$ puisque nous savons que ce dernier est le produit sans répétition des polynômes irréductibles ayant pour racines les générateurs du groupe cyclique $\mathbf{F}_q^*$.

13 Annexe : factorialité de Z[t] et irréductibilité de Φ_N

J'ai utilisé ou indiqué à plusieurs reprises que $\mathbf{Z}[t]$ est un anneau factoriel. Je rappelle plusieurs aspects ou préliminaires. Si $P = \sum_{0\leq j\leq n} a_j t^j$ est un polynôme non nul de $\mathbf{Z}[t]$ son contenu $c(P)$ est $\mathrm{pgcd}(a_0, \ldots, a_n)$.

Lemme 1 (Gauss)**.**

$$\forall P, Q \neq 0 \qquad c(PQ) = c(P)c(Q) \tag{36}$$

Preuve : on trouve le Lemme plus souvent sous la forme de son cas particulier $c(P) = c(Q) = 1 \implies c(PQ) = 1$, qui entraîne le cas général, puisque $c(nP) = |n|\, c(P)$ pour tout entier n non nul. Pour montrer le cas particulier il suffit de prouver que si le premier p divise PQ alors il divise P ou Q, car alors $c(PQ) > 1$ implique $c(P) > 1$ ou $c(Q) > 1$. Et finalement il suffit de dire que $\mathbf{Z}/p\mathbf{Z}[t]$ est un anneau intègre pour conclure.

Lemme 2. *Si* $P = P_1P_2$ *dans* $\mathbf{Q}[t]$ *avec* $P, P_1 \in \mathbf{Z}[t]$ *et* $c(P_1) = 1$*, alors* $P_2 \in \mathbf{Z}[t]$.

Preuve : si $P_2 = 0$ c'est ok. On peut donc supposer $P, P_2 \neq 0$. Soit $d \geq 1$ avec $dP_2 \in \mathbf{Z}[t]$. Alors

$$dP = P_1 dP_2 \implies c(dP) = c(P_1)c(dP_2) = c(dP_2) \implies d \mid c(dP_2) \implies P_2 \in \mathbf{Z}[t] \tag{37}$$

Lemme 3. *Si* $P = P_1P_2$ *dans* $\mathbf{C}[t]$ *avec* $P, P_1 \in \mathbf{Z}[t]$ *et* $c(P_1) = 1$*, alors* $P_2 \in \mathbf{Z}[t]$.

Preuve : clair si P_1 est constant (donc ± 1). Sinon, on fait la division euclidienne dans $\mathbf{Q}[t]$: $P = P_1Q + R$, $\deg(R) < \deg(P_1)$. Alors $P_1P_2 = P_1Q + R$ puis $R = P_1(P_2 - Q)$ dans $\mathbf{C}[t]$ d'où $R = 0$ (en regardant les degrés). Ainsi $P_2 = Q \in \mathbf{Q}[t]$. Le Lemme précédent donne alors $P_2 \in \mathbf{Z}[t]$.

Le cas particulier du Lemme avec P_1 unitaire est plus élémentaire. En effet pour **tout** anneau commutatif (unitaire) A, le théorème d'existence et d'unicité pour la division euclidienne $M = P_1Q + R$, $\deg(R) < \deg(P_1)$, est valable dans $A[t]$ lorsque P_1 est **unitaire**, avec la preuve usuelle. Si l'on revient au Lemme ci-dessus, dans le cas avec P_1 unitaire dans $\mathbf{Z}[t]$, on fait la division euclidienne $P = P_1Q + R$ dans $\mathbf{Z}[t]$, et par unicité de la division euclidienne dans $\mathbf{C}[t]$ il en résulte $P_2 = Q$, $R = 0$. Donc $P_2 \in \mathbf{Z}[t]$.

Prenons à titre d'exemple les polynômes cyclotomiques, définis dans $\mathbf{C}[t]$ par :

$$\Phi_N = \prod_{0\leq j<N, \mathrm{pgcd}(j,N)=1} (t - e^{2\pi i \frac{j}{N}}) \tag{38}$$

Comme toute racine N^e de l'unité est une racine primitive d^e de l'unité pour un unique diviseur d de N, on a dans $\mathbf{C}[t]$: $t^N - 1 = \prod_{d \mid N} \Phi_d$. Supposons alors par hypothèse de récurrence que l'on sache que tous les Φ_M, $M < N$ sont dans $\mathbf{Z}[t]$. Alors : $t^N - 1 = \Phi_N P$ avec P unitaire dans $\mathbf{Z}[t]$. Comme P est unitaire, le cas particulier du Lemme ci-dessus, utilisant la division euclidienne dans $\mathbf{Z}[t]$, montre que Φ_N est à coefficients entiers.

Théorème 13. *Si un polynôme* $P \in \mathbf{Z}[t]$ *est irréductible, et non constant, alors il est irréductible dans* $\mathbf{Q}[t]$.

Preuve : supposons $P = P_1 P_2$ dans $\mathbf{Q}[t]$ avec $\deg(P_1) > 0$, $\deg(P_2) > 0$. Soit $m \geq 1$ avec $mP_1 \in \mathbf{Z}[t]$, et posons $Q_1 = \frac{1}{c(mP_1)} mP_1$, et $Q_2 = \frac{c(mP_1)}{m} P_2$, de sorte que $P = Q_1 Q_2$ et Q_1 est à coefficients entiers et de contenu 1. Par le lemme, Q_2 est à coefficients entiers. Comme $\deg(Q_1) > 0$, Q_1 n'est pas un inversible de $\mathbf{Z}[t]$ (c'est-à-dire il n'est pas la constante ± 1) et idem pour Q_2. Donc P est réductible dans $\mathbf{Z}[t]$.

La liste complète des irréductibles de $\mathbf{Z}[t]$ est donnée par :

1. les nombres premiers (et leurs opposés), qui sont les irréductibles de degré nul,
2. les polynômes entiers de degrés strictement positifs, de contenu 1, qui sont irréductibles dans $\mathbf{Q}[t]$.

En utilisant que $\mathbf{Z}$ et $\mathbf{Q}[t]$ sont factoriels on aboutit alors au fait que $\mathbf{Z}[t]$ est factoriel.

Preuve de l'irréductibilité sur $\mathbf{Q}[t]$ de Φ_N : il suffit donc de la prouver dans $\mathbf{Z}[t]$. On peut supposer $N \geq 2$. On raisonne par l'absurde. Supposons que $\Phi_N = MU$ dans $\mathbf{Z}[t]$ avec M irréductible, $\deg(M) > 0$, $\deg(U) > 0$ (comme $c(\Phi_N) = 1$ c'est la seule possibilité de factorisation éventuelle).

Soit z une racine complexe de M. On commence par montrer que tout polynôme de $\mathbf{Z}[t]$ qui s'annule sur z est divisible par M dans $\mathbf{Z}[t]$. Considérons l'idéal dans $\mathbf{Q}[t]$ des A avec $A(z) = 0$. Il est engendré par un polynôme D que l'on peut prendre dans $\mathbf{Z}[t]$ et de contenu 1. Comme $M(z) = 0$, on a $M = DE$ avec $E \in \mathbf{Q}[t]$. Comme M et D sont entiers et que $c(D) = 1$ on sait que nécessairement $E \in \mathbf{Z}[t]$. Comme M est irréductible, c'est que $E = \pm 1$. Donc on peut prendre $D = M$. Tout polynôme A de $\mathbf{Z}[t]$ qui s'annule sur z est donc multiple dans $\mathbf{Q}[t]$ de M. En utilisant à nouveau notre fameux Lemme (on note que l'irréductible M est de contenu 1), on a comme annoncé : $A \in \mathbf{Z}[t], A(z) = 0 \implies A = MP$ avec $P \in \mathbf{Z}[t]$.

Soit maintenant p un nombre premier, qui ne divise pas N. Alors z^p est aussi une racine primitive N^e de l'unité. Supposons $U(z^p) = 0$. Par ce qui vient d'être prouvé :

$$U(t^p) = M(t)P(t) \tag{39}$$

dans l'anneau $\mathbf{Z}[t]$. Modulo p on a la relation $U(t^p) \equiv U(t)^p \mod p$ (encore notre Frobenius ! l'observation fondamentale étant que l'action du Frobenius sur l'anneau

commutatif $\mathbf{F}_p[t]$ est identique à la substitution $t \mapsto t^p$). Ainsi

$$U^p \equiv MP \mod p \tag{40}$$

Soit maintenant π un facteur irréductible unitaire de M mod p dans l'anneau factoriel $\mathbf{F}_p[t]$ (remarquez que $\deg(M \bmod p) > 0$, car M est nécessairement de coefficient dominant ± 1). Comme π divise U^p il divise U. Mais alors de $t^N - 1 = MU$ résulte que π^2 divise $t^N - 1$ dans $\mathbf{F}_p[t]$. Donc π divise la dérivée Nt^{N-1}. Comme on a pris p non diviseur de N, $N \not\equiv 0 \mod p$ donc π est le monôme t, mais ce dernier ne divise pas $t^N - 1$, contradiction.

Au final $U(z^p) = 0$ a mené à une contradiction et c'est donc qu'en fait $M(z^p) = 0$. Ainsi $M(z) = 0 \implies M(z^p) = 0$ lorsque $p \not| N$. Mais tout entier positif j premier à N est un produit de nombres premiers premiers à N, par conséquent, en itérant on finit par établir que $M(z^j) = 0$. Mais alors M a toutes les racines primitives N^e de l'unité comme racines, donc $\deg(M) = \deg(\Phi_N)$ et $\deg(U) = 0$ contredisant notre point de départ.