有限域 2
Corps finis II
上海/Shanghai, 2015-11[1]

Fabrice ORGOGOZO[2].

version : 642ebab 2019-09-24 21:52:15 +0800
http://fabrice.orgogozo.perso.math.cnrs.fr/articles/Shanghai.pdf

Table des matières

1. Corps finis : premières définitions et quelques applications
1.1. Vocabulaire
1.2. Algèbre de décomposition universelle et corps de décomposition d'un polynôme
1.3. Corps finis : existence, unicité
1.4. ¶ *Nimbres* et construction explicite des $\mathbb{F}_{2^{2^s}}$
1.5. Structure de $\mathbb{F}_q^\times$ et applications
1.6. ¶ Fonction zêta et polynômes sans facteurs carrés dans $\mathbb{F}_p[T]$
1.7. ¶ Nombre moyen de facteurs irréductibles
1.8. Théorème de Chevalley-Warning et suites de de Bruijn
2. Transformation de Fourier discrète ; sommes de Gauß, Jacobi et applications
2.1. Caractères des groupes abéliens finis
2.2. Transformation de Fourier discrète
2.3. Application n°1 : constructibilité à la règle et au compas
2.4. Application n°2 : réciprocité quadratique
2.5. ¶ Application n°3 : courbe de Fermat et sphères sur $\mathbb{F}_p$
3. Factorisation des polynômes
3.1. Généralités
3.2. Critères d'irréductibilité dans les corps finis $\mathbb{F}_q$
3.3. Irréductibilité sur $\mathbb{Q}$ *versus* sur $\mathbb{Z}$: (un) lemme de Gauß
3.4. Bornes explicites sur les coefficients des diviseurs d'un polynôme à coefficients entiers
3.5. Digression : factorisation sans facteur carré et résultant
3.6. Lemme de Hensel
3.7. Algorithme de factorisation
3.8. Astuce de Kronecker et groupe de Galois
Exercices

Le cours oral, plus « concret », *s'appuyant* sur ces notes :
cours n°1 : Galois et de Bruijn
cours n°2 : Frobenius et Berlekamp
cours n°3 : Fourier et Gauß
cours n°4 : Chevalley et van der Waerden
cours n°5 : Mignotte ; résumé des résultats principaux du cours

---

①. Cours : 2015-11-19,20,23,25,26 ; TD : 2015-11-20.
TDs suivants : professeur 陈恭亮 [CHÉN GōngLiàng].

②. « Fabrice Orgogoço »=法布里斯·奥尔戈戈索.

1. Corps finis : premières définitions et quelques applications

1.1. Vocabulaire. Soit k un anneau commutatif [交换环].

Une k-**algèbre** [代数] est un anneau commutatif A muni d'un morphisme (d'anneaux) $k \to A$. Lorsque ce morphisme est *injectif*, on dit que A est une **extension** [扩张] de k.

Un k-**module** [模] est un groupe abélien M muni d'un morphisme d'anneaux $k \to \mathrm{End}(M)$, $\lambda \mapsto (m \mapsto \lambda \cdot m)$. (En particulier, pour tous $\lambda \in k$ et $m, n \in M$, on a $\lambda\cdot(m+n) = \lambda\cdot m+\lambda\cdot n$.) Lorsque M possède une base — condition automatiquement satisfaite si k est un corps —, on dit que M est **libre** [自由] (sur k).

1.2. Algèbre de décomposition universelle et corps de décomposition d'un polynôme.
Références : [Lombardi et Quitté 2011, §3.4], [Bourbaki A, IV §6 n°5], [Pohst et Zassenhaus 1989, §2.2].

1.2.1. Soient k un anneau commutatif et $f = T^d - a_1T^{d-1} + a_2T^{d-2} + \cdots + (-1)^d a_d \in k[T]$ un polynôme unitaire [首一多项式] de degré [次数] d. Considérons l'**algèbre de décomposition universelle** définie comme le quotient A de l'anneau de polynômes $k[X_1, \ldots, X_d]$ par l'idéal engendré par $(\sum_i X_i)-a_1$, $(\sum_{i<j} X_iX_j)-a_2$, etc. c'est-à-dire les $\sigma_r(X_1, \ldots, X_r)-a_r$, $1 \leq r \leq d$, où $\sigma_r := \sum_{1\leq i_1<\cdots<i_r\leq d} X_{i_1}\cdots X_{i_r}$ désigne le **polynôme symétrique** [对称多项式] **élémentaire de degré** r. Par construction, le polynôme f devient *scindé* sur A : on a l'égalité $f = \prod_{i=1}^{d}(T - x_i)$ dans $A[T]$, où les x_i, $1 \leq i \leq d$, désignent les images des X_i dans A par la surjection canonique $k[X_1, \ldots, X_d] \twoheadrightarrow A$. Cette k-algèbre, aussi notée $\mathrm{Adu}_k(f)$ si l'on veut préciser l'anneau de coefficients et le polynôme, est « universelle » pour cette propriété — d'où son nom — : pour toute k-algèbre B telle que f se factorise en $\prod_i(T-y_i)$, il existe un unique morphisme de k-algèbres $A \to B$ envoyant les x_i sur les y_i. En particulier, le groupe $\mathfrak{S}_d$ agit naturellement sur A par k-automorphismes.

1.2.2. De cette propriété universelle, de démonstration immédiate, il résulte que si $k' := k[x_1] \subseteq A$ et $g := f(T)/(T - x_1) \in k'[T]$, le morphisme canonique de k'-algèbres $A = \mathrm{Adu}_k(f) \to \mathrm{Adu}_{k'}(g)$ est un isomorphisme. Ceci entraîne, par récurrence sur le degré d, que le morphisme $k \to A$ est injectif ; mieux : le k-module A est libre de rang $d!$, une base étant constituée des « monômes » $x_1^{e_1}\cdots x_{d-1}^{e_{d-1}}$ avec $e_j \leq d - j$. (En particulier, si k est non nul, il en est de même de l'anneau A.)

1.2.3. D'après l'axiome du choix — sous la forme (équivalente) du théorème de Krull — il existe un idéal maximal $\mathfrak{m}$ de A : l'anneau A (supposé non nul) se surjecte sur le corps $K := A/\mathfrak{m}$. Lorsque k est un corps, on dit que K est un **corps de décomposition** [分裂域] du polynôme f (ou plutôt de son image dans $K[T]$) : le polynôme f est scindé sur K et $K = k(R)$, où R désigne l'ensemble des racines de f dans K. Un tel corps est unique à isomorphisme (non unique) près : cela résulte du fait que deux extensions d'un corps sont toujours coiffées par une troisième.

1.3. Corps finis : existence, unicité.

Références : [Bourbaki A, V §12], [Serre 1977, I §1], [Jacobson 1985, 4.13].

Soient p un nombre premier et K un corps fini de caractéristique p. Les faits suivants sont de démonstration immédiate : (1) K est de cardinal $q = p^d$, où d est la dimension de K vu comme espace vectoriel sur le corps $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ et (2) K est un corps de décomposition du polynôme $X^q - X$. Pour établir (1), remarquer que K est isomorphe, en tant que $\mathbb{F}_p$-espace vectoriel (et, en particulier, ensemblistement) à $\mathbb{F}_p^d$; pour (2), remarquer que le groupe multiplicatif $K^\times$ étant de cardinal $q-1$, chacun de ses éléments est une racine $(q-1)$-ième de l'unité.

Réciproquement, on peut appliquer la construction précédente (d'un corps de décomposition d'un polynôme) au corps $k = \mathbb{F}_p$ et au polynôme $f = X^q - X$ pour établir l'existence d'un tel corps fini. On le note habituellement $\mathbb{F}_q$; il est unique à isomorphisme (*non unique*) près.

Notons qu'un corps de décomposition K de $X^q - X$ sur $\mathbb{F}_p$ est bien de cardinal q. L'ensemble, disons R, des racines de $X^q - X$ dans K est de cardinal exactement q car elles sont *simples* [单根] : le polynôme $X^q - X$ est premier avec sa dérivée $qX^{q-1} - 1 = -1$. D'autre part, R est stable par produit et par addition ; pour ce dernier point on utilise le fait que l'application $\mathrm{Frob}_p : x \mapsto x^p$, ainsi donc que ses puissances, est un *(endo)morphisme* : $(x+y)^p = x^p + y^p$ — égalité valable pour couple (x, y) d'une $\mathbb{F}_p$-algèbre. Ce morphisme est appelé **morphisme de Frobenius** [弗罗贝尼乌斯自同态]. L'ensemble R est donc un *sous-corps* de K ; comme il contient (trivialement) les racines de $X^q - X$, on a $R = K$ et finalement $\#K = q$, comme annoncé. Mise en garde :

> $\mathbb{F}_4$ n'est pas contenu dans $\mathbb{F}_8$: tous deux sont contenus dans $\mathbb{F}_{64}$ et leur intersection est réduite à $\mathbb{F}_2 = \{0, 1\}$.

1.4. ¶ *Nimbres* et construction explicite des $\mathbb{F}_{2^{2^s}}$.

Références : [Conway 2001, chap. 6], [H. W. Lenstra J. 1978], [Siegel 2013, chap. IV, §5] ; article 尼姆数 sur Wikipédia ; suite A051775 de l'OEIS.

1.4.1. Si $S \subsetneq \mathbb{N}$, notons $\mathrm{mex}(S) = \min(\mathbb{N} \smallsetminus S)$ le plus petit entier naturel n'appartenant *pas* à S. Par exemple, $\mathrm{mex}(\varnothing) = 0$. On définit par récurrence pour $x, y \in \mathbb{N}$[①] :

$$x\text{加}y := \mathrm{mex}\big(\{x'\text{加}y : x' < x\} \cup \{x\text{加}y' : y' < y\}\big)$$[②]
$$x\text{乘}y := \mathrm{mex}\big(\{(x'\text{乘}y)\text{加}(x'\text{乘}y')\text{加}(x\text{乘}y') : x' < x, y' < y\}\big)$$[③]

1.4.2. On peut expliciter le calcul de l'addition : x加y est le *ou exclusif* [[逻辑]异或] des écritures binaires de x et y. En d'autres termes, l'addition de deux mêmes nimbres est nulle et l'addition de deux puissances distinctes de 2 est l'addition usuelle. On peut vérifier par récurrence (non immédiate) que la multiplication est quant à elle caractérisée par le fait que le produit de deux nimbres distincts de la

① Plus généralement, on peut définir ces opérations sur les *ordinaux* [序数].

② En d'autres termes, l'addition est définie de la façon la plus simple possible, avec la contrainte que $x\text{加}y \neq x\text{加}y'$ si $y' < y$ et $x\text{加}y \neq x'\text{加}y$ si $x' < x$.

③ En d'autres termes, la multiplication est définie de la façon la plus simple possible avec la contrainte que $(x\text{加}x'\text{乘}(y\text{加}y') \neq 0$ si $x' < x$ et $y' < y$.

forme 2^{2^n} est le produit usuel (c'est-à-dire 2^{2^n}乘$2^{2^m} = 2^{2^n+2^m}$, si $n \neq m$) mais le carré 2^{2^n}乘2^{2^n} est $\frac{3}{2} \times 2^{2^n} = 2^{2^n}$加$2^{2^n-1}$. (Par exemple 4乘4 = 6.)

1.4.3. Pour chaque entier $n \geq 0$, l'ensemble $[2^{2^n}] := \{0, 1, \dots, 2^{2^n} - 1\}$ muni de 加, 乘 est un *corps* (fini, de cardinal 2^{2^n}), et $\mathbb{N}$, muni de ces mêmes lois, est une « clôture quadratique »[①] de $\mathbb{F}_2$. La commutativité, l'associativité, le fait que 0 soit absorbant, etc., se démontrent immédiatement par récurrence. Pour montrer que $[2^{2^n}]$ est un corps, il suffit de montrer que c'est un anneau intègre. L'intégrité de $\mathbb{N}$, et donc de chaque $[2^{2^n}]$, vient du fait que si $x, y > 0$, alors x乘y est le mex d'un ensemble contenant $0 = (0$乘$y)$加$(0$乘$0)$加$(x$乘$0)$. Le fait que ce soit un sous-anneau de $\mathbb{N}$ résulte des formules du paragraphe précédent pour le produit de puissances de 2 de Fermat. (Voir [Siegel 2013, lemme IV.5.6(a)] pour une méthode plus directe.)

À titre d'illustration, voici les tables d'addition et de multiplication de $\mathbb{F}_4 = [4]$.

加	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

et

乘	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

1.4.4. Utilisant les égalités 2^{2^r}乘$2^{2^r} = 2^{2^r}$加$\left(2^{2^{r-1}}$乘$2^{2^{r-2}}$乘$\cdots$乘$2\right)$, on peut montrer qu'il existe un isomorphisme

$$\begin{array}{rcl} ([2^{2^n}], \text{加}, \text{乘}) & \xrightarrow{\sim} & \left(\mathbb{F}_2[X_i : 0 \leq i < n]/(X_i^2 + X_i + \prod_{j<i} X_j, 0 \leq i < n), +, \times\right) \\ \sum_{E \in \mathscr{E}} \prod_{e \in E} 2^{2^e} & \mapsto & \sum_{E \in \mathscr{E}} \prod_{e \in E} x_e \end{array}$$

où $\mathscr{E}$ est un ensemble fini quelconque de parties de $[n]$.

1.5. Structure de $\mathbb{F}_q^\times$ et applications.

Références : [Jacobson 1985, 1.5] (exposant d'un groupe) ; [Hardy et Wright 2007, 16.3-4] (fonction et formule d'inversion de Möbius) ; [Cox 2004, 11.2] (comptage de polynômes irréductibles).

1.5.1. Soient K un corps et G un sous-groupe *fini* du groupe multiplicatif $K^\times$. (Noter que c'est un groupe *abélien* [阿贝尔群].) Soit n le PPCM [最小公倍数] des ordres des éléments de G, appelé **exposant** [指数] de G. Il existe un élément $x \in G$ d'ordre (exactement) n : cela résulte formellement du fait que si deux éléments x_1, x_2 sont d'ordres respectifs n_1, n_2 premiers entre eux, leur produit $x_1 x_2$ est d'ordre $n_1 n_2$. Pour un tel x, le sous-groupe *cyclique* [循环子群] $\langle x \rangle$ de G engendré par x est d'ordre n ; comme d'autre part G, étant d'exposant n, est contenu dans $\mu_n(K) := \{\lambda \in K : \lambda^n = 1\}$ de cardinal au plus n, on a $\langle x \rangle = G$. Nous avons établi le résultat suivant.

Théorème. *Tout sous-groupe fini du groupe multiplicatif d'un corps est cyclique.*

À titre de curiosité, signalons également le fait suivant.

① Cela signifie que tout polynôme de degré 2 est scindé sur ce corps, et qu'il est minimal pour cette propriété.

Proposition. *Si p un nombre premier de la forme $4\ell+1$ où ℓ est un nombre premier, alors 2 est primitif modulo p.*

Cette proposition s'applique par exemple à $p = 13, 29$ ou 53[①].

Démonstration. Un nombre a est primitif modulo p si pour tout premier p' tel que p soit congru à 1 modulo p', $a^{(p-1)/p'}$ n'est pas congru à 1 modulo p. Sous l'hypothèse de la proposition, $p-1$ a deux diviseurs premiers : 2 et ℓ. Puisque ℓ est impair, $4\ell+1$ est congru à 5 modulo 8, de sorte que (exercice 11) $2^{(p-1)/2}$ est congru à -1 modulo p. Enfin, $2^{(p-1)/\ell} = 2^4 \equiv 1$ modulo p entraîne $p = 3$ ou 5. □

Le polynôme irréductible $f = T^4 + T + 1 \in \mathbb{F}_2[T]$ est primitif (sur $\mathbb{F}_2$), c'est-à-dire qu'une quelconque de ses racines engendre $\mathbb{F}_{16}^\times$. Pour se convaincre à la fois du fait qu'il est irréductible et qu'il est primitif, on peut par exemple calculer les puissances successives de la classe t de T modulo f, soit $t^0 = 1$, $t^1 = t$, t^2, t^3, $t^4 = t+1$, $t^5 = t^2+t$, $t^6 = t^3+t^2$, $t^7 = t^3+t+1$, $t^8 = t^2+1$, $t^9 = t^3+t$, $t^{10} = t^2+t+1$, $t^{11} = t^3+t^2+t$, $t^{12} = t^3+t^2+t+1$, $t^{13} = t^3+t^2+1$, $t^{14} = t^3+1$ et $t^{15} = 1$: le fait qu'on ait obtenu un groupe cyclique à 15 éléments, c'est-à-dire tous les éléments non nuls de $\mathbb{F}_2[T]/(f)$, montre d'une part que l'ensemble des éléments non nuls de $\mathbb{F}_2[T]/(f)$ est un groupe (donc que $\mathbb{F}_2[T]/(f)$ est un corps, c'est-à-dire que f est irréductible) et d'autre part que t y est primitif, c'est-à-dire que f est primitif. Par contre, le polynôme irréductible $g = T^4 + T^3 + T^2 + T + 1 \in \mathbb{F}_2[T]$, bien qu'irréductible, n'est pas primitif. En effet, on a $T^5 \equiv T \pmod{f}$, c'est-à-dire que la classe t de T dans $\mathbb{F}_2[T]/(g)$ est d'ordre 5, et cette classe n'engendre donc pas $\mathbb{F}_{16}^\times$.

Ces exemples ont notamment pour but de souligner le fait que tous les polynômes irréductibles ne sont pas nécessairement primitifs ou que, de façon équivalente, le fait qu'un élément $x \in \mathbb{F}_{q^r}$ soit de degré r sur $\mathbb{F}_q$ ne suffit pas à entraîner qu'il soit primitif. (De fait, c'était clair par dénombrement : dans $\mathbb{F}_{16}$ il y a $16-4 = 12$ éléments de degré 4 sur $\mathbb{F}_2$, dont seulement $\varphi(15) = 8$ sont primitifs, c'est-à-dire qu'il y a parmi les polynômes unitaires de degré 4 sur $\mathbb{F}_2$ un total de $\frac{12}{4} = 3$ polynômes irréductibles dont $\frac{8}{4} = 2$ sont primitifs.)

1.5.2. Soit $\mathbb{F}$ un corps fini. Il résulte du théorème précédent que le groupe $\mathbb{F}^\times$ est cyclique. En particulier, si x en est un générateur, on a $\mathbb{F} = \mathbb{F}_p[x]$, où le terme de droite est, par définition, l'ensemble $\{P(x) \,:\, P \in \mathbb{F}_p[T]\}$. Soit Π le **polynôme minimal** [极小多项式] de x sur $\mathbb{F}_p$. C'est l'unique polynôme unitaire tel que le morphisme $\mathbb{F}_p[T] \to \mathbb{F}_p[x]$ envoyant T sur x se factorise à travers un isomorphisme $\mathbb{F}_p[T]/(\Pi) \xrightarrow{\sim} \mathbb{F}_p[x] = \mathbb{F}$. Nécessairement, le degré $\deg(\Pi)$ du polynôme est égal au degré $[\mathbb{F} : \mathbb{F}_p] := \dim_{\mathbb{F}_p} \mathbb{F}$ de l'extension $\mathbb{F} \,/\, \mathbb{F}_p$. Comme on a vu que pour tout entier $d \geq 1$, il existe une extension de $\mathbb{F}_p$ de degré d, on en déduit :

Proposition. *Soit p un nombre premier. Pour tout entier $d \geq 1$, il existe un polynôme irréductible dans $\mathbb{F}_p[T]$ de degré d.*

① On ne sait pas s'il existe une infinité de nombres premiers de la forme $(p-1)/4$. Par contre, la méthode dite du « crible » permet de montrer qu'il existe une infinité de premiers p tels que $(p-1)/4$ soit un produit de deux nombres premiers plus grands que p^θ où θ est une constante strictement supérieure à $\frac{1}{3}$. On peut en déduire (Heath-Brown) que l'un des trois entiers 2, 3 et 5 est primitif pour une infinité de nombres premiers.

1.5.3. *Groupe des automorphismes.* Soit $\mathbb{F}$ un corps fini de cardinal $q = p^d$. On a déjà vu que $\mathrm{Frob}_p : x \mapsto x^p$ est un endomorphisme de $\mathbb{F}$; c'est un automorphisme car tout morphisme de corps est injectif. Le sous-groupe $\langle \mathrm{Frob}_p \rangle$ de $\mathrm{Aut}(\mathbb{F})$ est d'ordre d : sa puissance d-ième Frob_p^d est l'identité et $\mathrm{Frob}_p^a \neq \mathrm{Id}$ si $a < d$, sans quoi $\mathbb{F}$ serait de cardinal $\leq p^a < p^d$. D'autre part, si x est un **élément primitif** [本原元] de $\mathbb{F}$, c'est-à-dire tel que $\mathbb{F} = \mathbb{F}_p[x]$, alors tout automorphisme $\varphi \in \mathrm{Aut}(\mathbb{F})$ est caractérisé par l'image $y = \varphi(x)$ de x. Comme y est une racine du polynôme minimal Π de x, car $0 = \varphi(\Pi(x)) = \Pi(\varphi(x))$, on voit que le cardinal de $\mathrm{Aut}(\mathbb{F})$ est *au plus* d. Finalement, on a démontré le résultat suivant.

Proposition. *Soit $\mathbb{F}$ un corps fini. Le groupe $\mathrm{Aut}(\mathbb{F})$ de ses automorphismes est cyclique engendré par le Frobenius $\mathrm{Frob}_p : x \mapsto x^p$. Les sous-corps de $\mathbb{F}$ sont exactement les ensembles de points fixes d'une puissance de Frob_p.*

1.5.4. *Orbite sous Frobenius.* Soient p un nombre premier, Ω une clôture algébrique de $\mathbb{F}_p$ (qui est la réunion croissante de ses sous-corps de cardinaux $p^{n!}$ pour $n \geq 1$) et $x \in \Omega^\times$, de polynôme minimal Π sur $\mathbb{F}_p$. Notons $d_x := [\mathbb{F}_p(x) : \mathbb{F}_p] = \deg(\Pi)$ le degré de x sur $\mathbb{F}_p$. Puisque $x \in \mathbb{F}_{p^d}$ si et seulement si $\mathrm{Frob}_p^d(x) = x$, on en déduit que d_x est aussi égal au cardinal de l'« orbite » [轨道] (finie) $\{\mathrm{Frob}_p^n(x) : n \geq 0\}$. Puisque, pour chaque $d \geq 1$, on a l'égalité $\mathbb{F}_q^\times = \mu_{q-1}(\Omega) := \{\lambda \in \Omega : \lambda^{q-1} = 1\}$, l'élément x est en particulier une racine $(p^{d_x} - 1)$-ième de l'unité. L'ordre $N = \#\langle x \rangle$ de x, vu comme élément du groupe multiplicatif de Ω, est donc un diviseur de $p^{d_x} - 1$; en particulier, il est premier à p et la condition $\mathrm{Frob}_p^d(x) = x$ devient équivalente à $p^{d_x} \equiv 1 \pmod{N}$. Terminons par le lien entre l'orbite de x sous l'action de l'automorphisme de Frobenius et le polynôme minimal Π. Le polynôme

$$P := \prod_{0 \leq n < d_x} \big(T - \mathrm{Frob}_p^n(x)\big),$$

a priori dans $\Omega[T]$ est en fait dans $\mathbb{F}_p[T]$ car ses coefficients sont fixes sous Frob_p. Comme il est d'autre part unitaire de degré $\deg(\Pi)$ et s'annule en x, on a l'égalité $\Pi = P$.

Pour mémoire, nous résumons ces résultats sous la forme suivante.

Proposition. *Soit $x \neq 0$ un élément de degré fini d_x sur le corps fini $\mathbb{F}_p$. Alors :*

- ***(i)*** *le degré d_x est le cardinal de l'orbite $\{\mathrm{Frob}_p^n x : n \geq 0\}$: c'est le plus petit entier $d \geq 1$ tel que $\mathrm{Frob}_p^d(x) = x$;*
- ***(ii)*** *l'ordre N de x dans $\Omega^\times$ est premier à p et l'entier d_x est l'ordre de p dans $(\mathbb{Z}/N\mathbb{Z})^\times$;*
- ***(iii)*** *le polynôme minimal de x sur $\mathbb{F}_p$ est égal au produit $\prod_{0 \leq n < d_x} \big(T - \mathrm{Frob}_p^n(x)\big)$: les « conjugués » de x (sur $\mathbb{F}_p$) sont exactement les $\mathrm{Frob}_p^n(x)$ avec $0 \leq n < d_x$.*

À titre d'application algébrique, on pourra démontrer l'irréductibilité des polynômes d'Artin-Schreier ; cf. exercice 12. Une application « arithmétique » fait l'objet du paragraphe suivant.

1.5.5. *Polynômes cyclotomiques.* Soit $\Phi_p(T) := T^{p-1} + \cdots + T + 1 \in \mathbb{Z}[T]$ le p-ième polynôme cyclotomique ; il résulte par exemple du critère d'Eisenstein, appliqué à $\Phi_p(X+1)$, que ce polynôme est irréductible. On s'intéresse ici à sa réduction $\overline{\Phi}_p$ modulo un nombre premier $\ell \neq p$. Factorisons la en un produit $P_1 \cdots P_g$ de polynômes irréductibles unitaires, distincts car $\overline{\Phi}_p$ est sans racine multiple, tout comme son multiple $X^p - 1$. Soit x une racine de l'un des P_i dans un surcorps de $\mathbb{F}_\ell$. Puisque x est une racine primitive p-ième de l'unité, le degré de x sur $\mathbb{F}_\ell$ est égal à l'ordre de ℓ dans $\mathbb{F}_p^\times$: cela résulte du (ii) de la proposition précédente. Il en résulte que tous les P_i sont de même degré, que l'on vient de calculer, et que le polynôme $\overline{\Phi}_p \in \mathbb{F}_\ell[T]$:

- est irréductible si et seulement si on a l'égalité $\langle \ell \rangle = \mathbb{F}_p^\times$;
- admet une racine dans $\mathbb{F}_\ell$ si et seulement si $\ell \equiv 1 \bmod p$.

Ce dernier critère a pour corollaire le fait suivant, qui est un cas particulier d'un théorème de Dirichlet.

Proposition. *Soit p un nombre premier. Il existe une infinité de nombres premier ℓ congrus à 1 modulo p.*

(On laisse au lecteur le soin de démontrer le même résultat où l'on remplace p par un entier $n \geq 1$ quelconque.)

La proposition est conséquence immédiate de ce qui précède et du lemme ci-dessous.

Lemme. *Soit $P \in \mathbb{Z}[T]$ un polynôme non constant. Il existe une infinité de nombres premiers ℓ tels que P ait une racine dans $\mathbb{F}_\ell$.*

On peut montrer, mais c'est beaucoup plus difficile (théorème de Frobenius-Čebotarëv), que si P est irréductible de degré ≥ 2, il existe une infinité de ℓ tel que P n'ait *pas* de racine dans $\mathbb{F}_\ell$.

Démonstration. C'est une variante de la méthode d'Euclide pour montrer qu'il existe une infinité de nombres premiers. Commençons par observer que l'on peut supposer que $P(0) = 1$ car, si $a := P(0) \neq 0$, on a $P(aT) = aQ(T)$, où $Q(0) = 1$, et si Q a une racine modulo un nombre premier ℓ, il en est de même de P. Supposons par l'absurde que les $P(n)$, pour $n \in \mathbb{N}$, n'aient qu'un nombre fini de diviseurs premiers $\ell_1, \ell_2, \ldots, \ell_r$. Pour chaque $n \in \mathbb{N}$, l'entier $P(n\ell_1\ell_2 \cdots \ell_r)$ est congru à $P(0) = 1$ modulo chaque ℓ_i. Il en résulte que $P(n\ell_1\ell_2 \cdots \ell_r)$ est premier à chacun des ℓ_i. Or, si n est grand, $P(n\ell_1\ell_2 \cdots \ell_r)$ est grand (en valeur absolue) donc a un diviseur premier. Absurde. □

1.5.6. *Comptage des polynômes irréductibles.* On se propose de donner une formule exacte pour le nombre de polynômes unitaires irréductibles de degré d à coefficients dans $\mathbb{F}_p$[①]. Commençons par une minoration.

Proposition. *Si $p \geq 3$, la proportion des polynômes de degré d dans $\mathbb{F}_p[X]$ qui sont* irréductibles *(resp.* irréductibles unitaires*) est au moins égale à $\frac{1}{3d}$ (resp. $\frac{1}{2d}$).*

① . Pour simplifier les notations, nous nous plaçons dans le cas particulier où le corps de base est $\mathbb{F}_p$ mais les mêmes résultats sont valables sur $\mathbb{F}_q$: remplacer p par q dans les énoncés ci-dessous.

Démonstration. Un élément de $\mathbb{F}_{p^d}$ étant primitif (sur $\mathbb{F}_p$) si et seulement si il n'appartient pas aux sous-corps stricts de $\mathbb{F}_{p^d}$, le nombre de ces éléments est au moins égal à $p^d - \sum_{\substack{m|d \\ m\neq d}} p^m$, que l'on peut minorer par

$$p^d - \sum_{m=1}^{d-1} p^m > p^d - \frac{p^d}{p-1} = p^d \cdot \frac{p-2}{p-1}.$$

Le nombre de polynômes irréductibles *unitaires* de degré d est donc minoré par un d-ième de cette quantité — car chaque polynôme irréductible de degré d a exactement d racines dans $\mathbb{F}_{p^d}$ —, et celui des polynômes irréductibles non nécessairement unitaires (donc de coefficient dominant arbitraire dans $\mathbb{F}_p^\times$) par $p-1$ fois cette dernière quantité. La conclusion résulte alors des inégalités $\frac{p-2}{p-1} \geq \frac{1}{2}$ et $1 - \frac{2}{p} \geq \frac{1}{3}$. □

On appelle **fonction de Möbius** [默比乌斯函数] la fonction $\mu : \mathbb{N} \to \mathbb{Z}$ définie par $\mu(n) = 0$ si n est divisible par un carré $\neq 1$ et $\mu(d) = (-1)^t$ si $d = p_1 \cdots p_t$ avec $p_1, \dots, p_t$ des nombres premiers deux à deux distincts (ainsi, $\mu(1) = 1$, $\mu(2) = -1$, $\mu(3) = -1$, $\mu(4) = 0$, $\mu(5) = -1$, $\mu(6) = 1$, $\mu(7) = -1$, $\mu(8) = 0$, $\mu(9) = 0$, $\mu(10) = 1$). De la formule $\sum_{a|d} \mu(a) = 0$ si $d > 1$ — qu'il suffit d'ailleurs d'établir dans le cas particulier où d est une puissance d'un nombre premier — on tire la *formule d'inversion* [反演公式] suivante : si Γ est un groupe abélien et que $f, g : \mathbb{N}_{>0} \to \Gamma$ sont deux fonctions, on a

$$g(d) = \sum_{a|d} f(a) \text{ pour tout } d > 0 \Leftrightarrow f(d) = \sum_{a|d} \mu\Big(\frac{d}{a}\Big)\, g(a) \text{ pour tout } d > 0.$$

Théorème (Gauß)**.** *Le nombre de polynômes unitaires irréductibles de degré d sur $\mathbb{F}_p$ vaut*

$$\frac{1}{d} \sum_{a|d} \mu\Big(\frac{d}{a}\Big)\, p^a = \frac{1}{d}\Big(p^d - \sum_{\ell_1|d} p^{d/\ell_1} + \sum_{\ell_1,\ell_2|d} p^{d/(\ell_1\ell_2)} - \sum_{\ell_1,\ell_2,\ell_3|d} p^{d/(\ell_1\ell_2\ell_3)} + \cdots\Big).$$

En particulier, il est égal à $\frac{p^d}{d} + O(\frac{p^{d/2}}{d})$.

Démonstration. Soit I_d le nombre — qu'on cherche à calculer — d'unitaires irréductibles de degré d sur $\mathbb{F}_p$. D'après la formule d'inversion précédente, il suffit de prouver $p^d = \sum_{a|d} a\, I_a$. Cela résulte du fait que le polynôme $T^{p^d} - T$ se décompose dans $\mathbb{F}_p[T]$ en le produit des polynômes irréductibles P, unitaires de degré a divisant d : chaque polynôme apparaît une fois car une racine α d'un tel polynôme satisfait $\mathrm{Frob}_p^a(\alpha) = \alpha$ donc *a fortiori* $\mathrm{Frob}_p^d(\alpha) = \alpha$; au plus une fois car les racines de $T^{p^d} - T$ sont simples[①]. Pour ce qui est de l'estimation asymptotique, remarquons que dans la somme exacte, le terme $a = d$ vaut p^d/d, le terme $a = d/2$, s'il existe (c'est-à-dire, si d est pair), vaut $-p^{d/2}/d$, et tous les autres termes, dont le nombre est au plus d, sont chacun $O(p^{d/3}/d)$; leur somme est donc bien $O(p^{d/3}) = O(p^{d/2}/d)$. □

① Par exemple, le polynôme $T^{16} - T$ se factorise sur $\mathbb{F}_2$ comme : $T^{16} - T = T(T+1)(T^2+T+1)(T^4+T+1)(T^4+T^3+1)(T^4+T^3+T^2+T+1)$.

1.6. ¶Fonction zêta et polynômes sans facteurs carrés dans $\mathbb{F}_p[T]$.
Références : [Rosen 2002, chap. 2], [Mignotte et Ştefănescu 1999, 3.7.3] (fonctions zêta/Zêta, polynômes sans facteurs carrés) ; [Hardy et Wright 1979, 17.1-2] et [Serre 1977, VI §2] (séries de Dirichlet) ; [Cartan 1961, I.§1], [Stanley 2012, 1.1] et [TAOCP 1, 1.2.9] (séries formelles).

1.6.1. *Fonction zêta ζ.* Pour tout polynôme unitaire $f \in \mathbb{F}_p[T]$, notons $|f|$ l'entier $p^{\deg(f)}$; en particulier, $|1| = 1$. Pour chaque $s \in \mathbb{C}$ de partie réelle > 1, considérons la série (de Dirichlet) [(狄利克雷)级数]

$$\zeta(s) := \sum_{f \text{ unitaire}} \frac{1}{|f|^s},$$

analogue à la fonction zêta usuelle de Riemann $\zeta_{\mathbb{Z}}(s) := \sum_{n\geq 1} \frac{1}{n^s} = \prod_p \frac{1}{1-p^{-s}}$. Ici aussi, l'existence et l'unicité de la décomposition en produit d'irréductibles entraîne formellement l'égalité (« produit eulérien [欧拉乘积] ») $\zeta(s) = \prod_{P \text{ irr. unit.}} \frac{1}{1-|P|^{-s}}$. En effet, le terme de droite est égal à $\prod_P \left(\sum_{n\geq 1} |P|^{-ns} \right) = \sum_f |f|^{-s}$: si $f = P_1^{n_1} \cdots P_r^{n_r}$, on a $|f|^{-s} = |P_1|^{-n_1 s} \cdots |P_r|^{-n_r s}$. Par contre, à la différence du cas de l'anneau $\mathbb{Z}$, la fonction zêta de $\mathbb{F}_p[T]$ est facile à calculer : $\zeta(s) = \sum_{d\geq 0} \frac{p^d}{p^{ds}} = \frac{1}{1-p\cdot p^{-s}}$ car il y a exactement p^d polynômes unitaires de degré d.

1.6.2. *Fonction Zêta Z.* Il est parfois plus commode de faire le changement de variable $x = p^{-s}$, c'est-à-dire de considérer la série (formelle/entière) [(形式)幂级数]

$$Z(x) := \prod_P \frac{1}{1-x^{\deg(P)}} = \prod_{d\geq 1} \frac{1}{(1-x^d)^{I_d}} \in \mathbb{Z}[[x]],$$

où P parcourt les polynômes irréductibles unitaires de $\mathbb{F}_p[T]$ et I_d désigne le nombre d'entre eux de degré d. Par construction, on a $\zeta(s) = Z(p^{-s})$ et, d'après le calcul du paragraphe précédent, on a $Z(x) = \frac{1}{1-px}$[①]. Notons qu'en prenant la dérivée logarithmique de l'égalité $\prod_{d\geq 1} \frac{1}{(1-x^d)^{I_d}} = \frac{1}{1-px}$, on retrouve les égalités $\sum_{a|d} aI_a = p^d$.

1.6.3. *Polynômes sans facteur carré.* Soit ζ_2 l'analogue de ζ pour les polynômes unitaires *sans facteur carré* [无平方因子] : $\zeta_2(s) := \sum_f |f|^{-s}$ où f parcourt les polynômes unitaires sans facteur carré. On a trivialement $\zeta_2(s) = \prod_P (1+|P|^{-s})$, où P parcourt les polynômes unitaires irréductibles. De l'identité $1+z = \frac{1-z^2}{1-z}$ appliquée aux $z = |P|^{-s}$, on tire l'égalité

$$\zeta_2(s) = \frac{\zeta(s)}{\zeta(2s)}.$$

① Le fait que $Z(x)$ soit une fraction rationnelle n'est pas spécifique à la $\mathbb{F}_p$-algèbre $\mathbb{F}_p[T]$; cf. [Grothendieck 1964].

On peut réécrire cette formule en faisant le changement de variable précédent :

$$Z_2(x) = \frac{Z(x)}{Z(x^2)} = \frac{1-px^2}{1-px}.$$

Comme $Z_2(x) = \sum_d I_d^2\, x^d$, où I_d^2 est le nombre de polynômes unitaires de degré d sans facteur carré, on a $I_d^2 = p^d - p^{d-1} = p^d(1-p^{-1})$ pour chaque $d \geq 2$. On a donc démontré la proposition suivante.

Proposition. *La proportion de polynômes $f \in \mathbb{F}_p[T]$ unitaires de degré $d \geq 2$ sans facteur carré est* $1 - p^{-1} = \dfrac{1}{\zeta(2)}$.

(Il n'est pas difficile de montrer directement qu'à d fixé le nombre de tels polynômes est $1 - o(1)$ lorsque $p \to +\infty$, cf. p. ex. [Tao 2015, lemme 4].)

On pourra comparer ce résultat à celui énoncé dans l'exercice 19.

1.7. ¶Nombre moyen de facteurs irréductibles.

Références : [TAOCP 2, exercice 4.6.2.5], [Flajolet et Sedgewick 2009, exemples I.20, VII.4, IX.21], [Mignotte et Ştefănescu 1999, 3.4.4—6] (nombre moyen de facteurs irréductibles).

1.7.1. Pour tout polynôme unitaire $f \in \mathbb{F}_p[T]$, notons $\lambda(f)$ le nombre de ses facteurs irréductibles (comptés avec multiplicités, avec la convention que $\lambda(1) = 0$) et considérons la série formelle de deux variables

$$Z(x,u) := \prod_{d\geq 1}(1-ux^d)^{-I_d} = \sum_f x^{\deg(f)}u^{\lambda(f)} \in \mathbb{Z}[[x,u]]$$

qui encode les nombres de polynômes unitaires f de degré et nombre de facteurs irréductibles donnés. Elle raffine la fonction Zêta précédente : $Z(x,1) = Z(x)$. Sa dérivée logarithmique par rapport à la nouvelle variable u est égale à $\displaystyle\sum_{d\geq 1} \frac{I_d x^d}{1-ux^d} = \sum_{d\geq 1,k\geq 0} I_d x^{d(k+1)}u^k$ si bien que l'on a l'égalité

$$Z(x,u) = \exp\Big(\sum_{k\geq 1} u^k \frac{I(x^k)}{k}\Big) \text{ où } I(x) := \sum_{d\geq 1} I_d x^d.$$

Pour chaque entier $d \geq 1$, notons $\mathfrak{e}_d$ le nombre moyen de facteurs irréductibles d'un polynôme unitaire de degré d. Par construction et le calcul précédent, on a

$$\sum_{d\geq 1} \mathfrak{e}_d x^d = \frac{\mathrm{d}Z}{\mathrm{d}u}(x/p,u)_{|u=1} = Z(x/p) \times \sum_{k\geq 1} I(x^k/p^k).$$

Or, il résulte de la formule d'inversion de Möbius que l'on a

$$I(x) = -\sum_{m\geq 1} \frac{\mu(m)}{m} \log(1-px^m)$$

d'où, en utilisant $\sum_{m|d} \varphi(m) = d$ et à nouveau la formule d'inversion,

$$\sum_{k\geq 1} I(x^k) = -\sum_{d\geq 1} \frac{\varphi(d)}{d} \log(1-px^d).$$

Finalement, $\sum_{d\geq 1} \mathfrak{e}_d x^d = \frac{1}{1-x}\sum_{d\geq 1}\frac{\varphi(d)}{d}\log(\frac{1}{1-p^{1-d}x^d})$. En développant le logarithme, on en déduit que

$$\mathfrak{e}_d = \big(1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{d}\big) + \sum_{r=1}^{d}\frac{1}{rp^r}\Big(\sum_{\substack{k\geq 2\\ k-1|r}}\varphi(k)\cdot(1-\frac{1}{k})\Big).$$

Le second terme est un $O(\sum_{r=1}^{d} rp^{-r}) = O(p^{-1})$, uniformément en d. On a donc en particulier montré la proposition suivante.

Proposition. *Le nombre moyen de facteurs irréductibles d'un polynôme unitaire de degré d de $\mathbb{F}_p[T]$ est équivalent à $\log(d)$ lorsque $d \to +\infty$, que p soit fixé ou non. De plus, à d fixé, ce nombre est équivalent lorsque $p \to +\infty$ au nombre moyen [=espérance] de cycles[①] d'une permutation de $\mathfrak{S}_d$[②].*

Pour le second point, on a utilisé implicitement le fait classique suivant.

Lemme. *Le nombre moyen de cycles d'une permutation de $\mathfrak{S}_d$ est $1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{d}$.*

Démonstration. On définit des coefficients « d *cycle* c » $\begin{bmatrix} d \\ c \end{bmatrix}$, appelés « nombres de Stirling de première espèce », par la relation $x^{\overline{d}} := x(x+1)\cdots(x+d-1) = \sum_{c=0}^{d}\begin{bmatrix} d \\ c \end{bmatrix}x^c$. On vérifie immédiatement que $\begin{bmatrix} d \\ c \end{bmatrix} = (d-1)\begin{bmatrix} d-1 \\ c \end{bmatrix} + \begin{bmatrix} d-1 \\ c-1 \end{bmatrix}$ et que le nombre de permutations de $\mathfrak{S}_d$ ayant exactement c cycles est $\begin{bmatrix} d \\ c \end{bmatrix}$ car cette dernière quantité satisfait la même relation de récurrence. Il en résulte que la série génératrice $G := \sum_c P(\sharp\text{cycles} = c)x^c = \sum_{c=0}^{d}\begin{bmatrix} d \\ c \end{bmatrix}\frac{x^c}{d!}$ est égale à $\frac{x^{\overline{d}}}{d!} = \prod_{i=1}^{d}\frac{x-1+i}{i}$. Si l'on note G_i chaque facteur du produit, l'espérance $G'(1)$ est égale à $\sum_i G_i'(1) = \sum_{i=1}^{d} i^{-1}$. Ainsi, l'espérance du nombre de cycles est $1+\frac{1}{2}+\cdots+\frac{1}{d}$. (On peut montrer de même que la variance est $G''(1)+G'(1)-G'(1)^2 = \sum_{i=1}^{d} i^{-1} - \sum_{i=1}^{d} i^{-2}$.) □

① On appelle *cycle* [圈/循环] d'une permutation $\sigma \in \mathfrak{S}_d$ une orbite du groupe $\langle\sigma\rangle$ agissant sur $\{1,\ldots,d\}$. Par exemple, le nombre de cycles de $\begin{pmatrix} 1&2&3&4&5&6&7&8 \\ 3&4&5&2&1&8&6&7 \end{pmatrix}$ est 3.

② Ce fait n'est pas spécifique à la $\mathbb{F}_p$-algèbre $\mathbb{Z}[T]/(p) = \mathbb{F}_p[T]$; cf. [Deligne 1980, §3.5], où des résultats généraux d'équidistribution lorsque $p \to +\infty$ sont démontrés. Ils sont également présentés de façon plus accessible mais malgré tout difficile dans [Katz et Sarnak 1999, chap. 9].

1.8. Théorème de Chevalley-Warning et suites de de Bruijn.

1.8.1. *Chevalley-Warning.*
Références : [Chevalley 1935], [Serre 1977, I §2], [Tao 2014, §8].

Soient $\mathbb{F}$ un corps fini et $f_1, \dots, f_e \in \mathbb{F}[T_1, \dots, T_n]$ des polynômes non nuls en n variables à coefficients dans $\mathbb{F}$. On note $\deg(f)$ le *degré* d'un tel polynôme c'est-à-dire le plus grand entier d tel qu'un monôme $T_1^{d_1} \cdots T_n^{d_n}$ avec $d = d_1 + \cdots + d_n$ apparaisse dans la décomposition de f en combinaison linéaire de monômes. (Par convention, $\deg(0) = -\infty$.) On s'intéresse au cardinal de l'ensemble V des *zéros* communs dans $\mathbb{F}^n$ des polynômes $f_1, \dots, f_e$:

$$V := \{(t_1, \dots, t_n) \in \mathbb{F}^n \,:\, f_1(t_1, \dots, t_n) = \cdots = f_e(t_1, \dots, t_n) = 0_{\mathbb{F}}\}.$$

Le point de départ du calcul qui va suivre est que pour tout n-uplet $\underline{t}$ on a :

$$\prod_{i=1}^{e} (1_{\mathbb{F}} - f_i(\underline{t})^{\#\mathbb{F}-1}) = 1_{\mathbb{F}} \text{ si } \underline{t} \in V, \text{ et } 0_{\mathbb{F}} \text{ sinon.}$$

Cela résulte du fait que pour tout $x \in \mathbb{F}$, le scalaire $1_{\mathbb{F}} - x^{\#\mathbb{F}-1}$ vaut $1_{\mathbb{F}}$ si $x = 0_{\mathbb{F}}$, et $0_{\mathbb{F}}$ si $x \neq 0_{\mathbb{F}}$. Il est donc naturel d'introduire le polynôme $P := \prod_{i=1}^{e} (1_{\mathbb{F}} - f_i^{\#\mathbb{F}-1}) \in \mathbb{F}[T_1, \dots, T_n]$, de degré $(\#\mathbb{F} - 1)\big(\deg(f_1) + \cdots + \deg(f_e)\big)$. En effet, d'après ce qui précède on a l'égalité, *dans* $\mathbb{F}$:

$$\#V \cdot 1_{\mathbb{F}} = \sum_{\underline{t} \in \mathbb{F}^n} P(\underline{t}).$$

Ainsi l'entier $\#V$ est déterminé, *modulo la caractéristique* $p > 0$ *de* $\mathbb{F}$, par la somme de droite. Pour évaluer cette somme, le cas crucial est l'étude des sommes $S_{d_1,\dots,d_n} := \sum_{\underline{t} \in \mathbb{F}^n} t_1^{d_1} \cdots t_n^{d_n}$, pour $d_1, \dots, d_n \in \mathbb{N}$, avec la convention que $0_{\mathbb{F}}^0 = 1_{\mathbb{F}}$. Or, $S_{d_1,\dots,d_n} = S_{d_1} \cdots S_{d_n}$ et

$$S_d := \sum_{t \in \mathbb{F}} t^d = 0_{\mathbb{F}}$$

si d n'est pas un multiple non nul de $\#\mathbb{F} - 1$. (En effet, il existe dans ce cas un $\lambda \in \mathbb{F}^\times$ tel que $\lambda^d \neq 1$ si bien que l'égalité $S_d = \lambda^d S_d$, obtenue par le changement de variable $u = \lambda t$, force l'égalité $S_d = 0$.) Il en résulte que si $F \in \mathbb{F}[T_1, \dots, T_n]$ est de degré strictement inférieur à $n(\#\mathbb{F} - 1)$, la somme $\sum_{\underline{t} \in \mathbb{F}^n} F(\underline{t})$ est nulle : chaque monôme de F a au moins un exposant $< \#\mathbb{F} - 1$. Mettant ces observations ensemble, on a démontré le théorème suivant.

Théorème (Chevalley-Warning)**.** *Soient* $\mathbb{F}$ *un corps fini de caractéristique* p *et des polynômes non nuls* $f_1, \dots, f_e \in \mathbb{F}[T_1, \dots, T_n]$ *tels que* $\sum_i \deg(f_i) < n$. *Alors, le cardinal de l'ensemble fini* $\{(t_1, \dots, t_n) \in \mathbb{F}^n \,:\, f_1(t_1, \dots, t_n) = \cdots = f_e(t_1, \dots, t_n) = 0\}$ *est divisible par* p. *En particulier, si les* $f_1, \dots, f_e$ *sont* homogènes *[齐次(多项式)], il existe un zéro commun* non trivial *c'est-à-dire à coordonnées non toutes nulles.*

Ceci montre notamment que toute forme quadratique d'au moins trois variables sur $\mathbb{F}$ a un zéro non trivial.

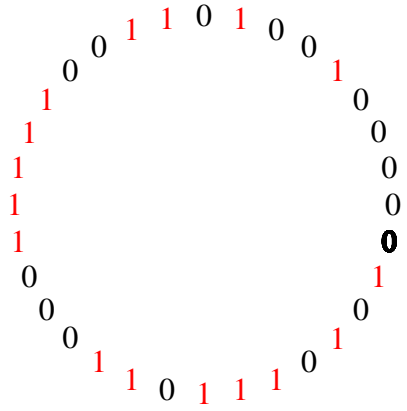
Ce résultat, conjecturé par Emil Artin, a pour conséquence que tout corps (non nécessairement commutatif) fini est commutatif ; c'est l'analogue d'un théorème de Tsen [曾炯=Zēng Jiǒng] où le corps $\mathbb{F}_p$ est remplacé par $\mathbb{C}(t)$.

1.8.2. *Suites de de Bruijn.*
Références : [TAOCP 4A, 7.2.1.1], [TAOCP 1, exercice 2.3.4.2-23], [TAOCP 2, exercice 3.2.2-17], [Flajolet et Sedgewick 2009, exemple V.15], [Stanley 1999, 5.6.15], [Lidl et Niederreiter 1997, chap. 8] ; [Gathen et Gerhard 2003, §12.3] (suites récurrentes linéaires) ; [Diaconis et Graham 2012, chap. 2 et 4] (tour de magie [魔术]).

Soient $\mathfrak{A}$ un ensemble de cardinal a et r un entier. On appelle **suite** — ou bien « cycle », « bracelet » — **de de Bruijn** [də ˈbrœyn] a-aire d'ordre r une suite cyclique u, c'est-à-dire une application $\mathbb{Z}/N\mathbb{Z} \to \mathfrak{A}$ pour un entier $N \geq 1$, telle que pour chaque mot m de longueur r formé sur $\mathfrak{A}$, il existe un unique $i \in \mathbb{Z}/N\mathbb{Z}$ tel que $m = u_{i+1}u_{i+2}\cdots u_{i+r}$. Compte-tenu de l'unicité et du fait qu'il existe a^r mots de longueur r, on a nécessairement $N = a^r$.

Les suites cycliques

et



sont des exemples de suites de de Bruijn binaires d'ordre respectivement 3 et 5 (avec respectivement $N = 8$ et 32). Dans le premier cas, ce sont d'ailleurs les deux seules suites, à rotation près. On peut montrer non seulement qu'il en existe toujours (pour a et r quelconques) mais aussi les compter : le nombre de suites de de Bruijn binaires d'ordre r commençant par $0\cdots0$ [r zéros] est égal à $2^{2^{r-1}-r}$.

Nous allons montrer comment la théorie des corps finis permet de construire de telles suites lorsque le cardinal de l'alphabet $\mathfrak{A}$ est une puissance q d'un nombre premier. (Le cas général s'y ramène d'ailleurs, en décomposant a — donc N — en produit de facteurs premiers et en utilisant le théorème chinois [中国剩余定理].) Fixons une extension $\mathbb{F}_q \subseteq \mathbb{F}_{q^r}$ de corps de cardinaux respectifs q et q^r et considérons un générateur x de $\mathbb{F}_{q^r}^\times$, de polynôme minimal

$$P = T^r - c_1T^{r-1} - c_2T^{r-2}\cdots - c_{r-1}T - c_r \in \mathbb{F}_q[T].$$

(On a vu qu'il existe $\dfrac{\varphi(q^r-1)}{r} > 1$ tels polynômes.)

Considérons la suite u définie de la façon suivante : $u_1 = \cdots = u_{r-1} = 0$, $u_r = c_r$ et, pour $n \in]\!] r, q^r [\![$, définie par récurrence

$$u_n = c_r u_{n-r} + \cdots + c_1 u_{n-1}.$$

La matrice M associée à cette *suite récurrence linéaire* est la matrice compagnon du polynôme P; elle est diagonalisable sur $\mathbb{F}_{q^r}$, de valeurs propres x et ses conjugués, qui sont des racines primitives $q^r - 1$-ièmes de l'unité. On se convainc alors aisément que la suite $u = u_0 u_1 \cdots u_{q^r-1}$, où $u_0 \coloneqq \mathbf{0}$, est une suite de de Bruijn : les images par M^i du vecteur non nul $(u_1, \ldots, u_r)$ parcourent $\mathbb{F}_q^r - \{0\}$ lorsque i parcourt $[\![0, q^r - 1 [\![$ et l'égalité $M^{q^r-1}(u_1, \ldots, u_r) = (u_1, \ldots, u_r)$ montre que la suite est bien cyclique. (Poser $u_0 = \mathbf{0}$ permet d'obtenir le mot nul $0 \cdots 0$ de longueur r.)

Les suites de de Bruijn ont une application à un tour de magie amusant.

Considérons la suite de $2^5 = 32$ cartes

$$8\clubsuit,\ A\clubsuit,\ 2\clubsuit,\ 4\clubsuit,\ A\spadesuit,\ 2\diamondsuit,\ 5\clubsuit,\ 3\spadesuit,\ 6\diamondsuit,\ 4\spadesuit,\ A\heartsuit,\ 3\diamondsuit, 7\clubsuit,\ 7\spadesuit, 7\heartsuit,\ 6\heartsuit,$$

$$4\heartsuit,\ 8\heartsuit,\ A\diamondsuit,\ 3\clubsuit,\ 6\clubsuit, 5\spadesuit, 3\heartsuit,\ 7\diamondsuit,\ 6\spadesuit,\ 5\heartsuit,\ 2\heartsuit,\ 5\diamondsuit,\ 2\spadesuit, 4\diamondsuit,\ 8\spadesuit,\ 8\diamondsuit.$$

Le lien avec la suite de de Bruijn binaire d'ordre 5 ci-dessus (lue dans le sens trigonométrique positif) — associée au polynôme

$$T^5 - T^2 - 1,$$

c'est-à-dire à la relation de récurrence

$$u_n = u_{n-5} + u_{n-3}$$

dans $\mathbb{F}_2$ — est le suivant : à un 5-uplet de bits [位元], on peut associer une couleur (le bit dominant : 0↔noir ; 1↔rouge), majeur ou pas (bit suivant : 0↔♣, ♢ ; 1↔♡, ♠), et un nombre entre 1 et 8 (trois derniers bits, avec la convention que 000↔8). Si on demande à 5 personnes de couper le jeu autant qu'ils veulent, puis de prendre chacun une carte sur le dessus du paquet (cachée du magicien) et d'en indiquer, d'une façon ou d'une autre, la couleur, on peut retrouver chacune de leurs cartes !

Pour d'autres applications ludiques des corps finis, cf. p. ex. [Madore 2015a], [Madore 2015b].

2. Transformation de Fourier discrète ; sommes de Gauß, Jacobi et applications

2.1. Caractères des groupes abéliens finis.

Références : [Serre 1977, VI §1], [Bourbaki A, V §11 n°7], [Ireland et Rosen 1990, §8.1].

2.1.1. Soit G un groupe abélien fini, noté multiplicativement. On appelle **caractère** [特征标] de G un morphisme $\chi : G \to \mathbb{C}^\times$, noté $g \mapsto \chi(g)$ ou parfois $g \mapsto g^\chi$. Observer que si n est l'exposant de G, ce caractère est à valeurs dans le sous-groupe $\mu_n(\mathbb{C})$ des racines n-ièmes de l'unité. L'ensemble $\mathrm{Hom}(G, \mathbb{C}^\times)$ des caractères de G forme un groupe que l'on note $\widehat{G}$, appelé le **dual** [对偶] de G. Soit $H \leq G$ un sous-groupe ; tout caractère $\chi \in \widehat{G}$ induit par restriction un caractère $\chi_{|H} \in \widehat{H}$ de H.

Si G est le groupe *cyclique* $\mathbb{Z}/n\mathbb{Z}$, son dual est isomorphe à $\mu_n(\mathbb{C})$ (également cyclique d'ordre n) : un caractère de G est déterminé par l'image de son générateur $\overline{1}$.

2.1.2. Proposition. *Le morphisme $\widehat{G} \to \widehat{H}$ est* surjectif.

Démonstration. Soit $\chi : H \to \mathbb{C}^\times$ un caractère. Il suffit de montrer que si $H \neq G$ on peut étendre χ à un sous-groupe de G contenant strictement H. Par hypothèse, il existe $g \in G \smallsetminus H$. Soit n le plus petit entier > 1 tel que $g^n = h \in H$. Posons $\zeta = \chi(h)$. Pour toute extension $\widetilde{\chi}$ de χ à G, on a nécessairement $\widetilde{\chi}(g)^n = \zeta$. Considérons donc une racine n-ième ξ de ζ dans $\mathbb{C}^\times$. L'entier n étant minimal, on vérifie immédiatement que $h \mapsto \chi(h)$, $g \mapsto \xi$ s'étend en un caractère de $\langle H, g\rangle$: si $k = hg^i$, le nombre $\chi(h)\xi^i$ ne dépend que de k et pas de la décomposition de k en produit. □

Il en résulte que si $H \leq G$, on a une **suite exacte** [正合序列] $1 \to \widehat{(G/H)} \to \widehat{G} \to \widehat{H} \to 1$. Ceci permet de démontrer par récurrence, en considérant un sous-groupe *cyclique* H, que $\#G = \#\widehat{G}$. Nous allons démontrer un résultat plus fin : les groupes G et $\widehat{G}$ sont (non canoniquement) isomorphes.

2.1.3. *Structure des groupes abéliens finis.* Soit G un groupe abélien fini, d'exposant n. On a vu en **1.5.1** qu'il existe un sous-groupe cyclique $C = \langle x\rangle \leq G$ d'ordre n, d'où — par la proposition précédente — un morphisme [=caractère] $G \to \mu_n(\mathbb{C})$ prolongeant un isomorphisme arbitraire $C \xrightarrow{\sim} \mu_n(\mathbb{C})$. (Le fait que le prolongement soit également à valeurs dans $\mu_n(\mathbb{C})$ tient au choix de n.) Ainsi, il existe une surjection $s : G \twoheadrightarrow C$ telle que le composé $C \to G \to C$ soit l'identité. Il est alors formel d'en déduire que G est isomorphe à $C \times \mathrm{Ker}(s)$ car $C \cap \mathrm{Ker}(s) = \{1\}$. On en déduit par récurrence le théorème suivant. (Bien que cela ne soit pas nécessaire, noter que $\mathrm{Ker}(s)$ est isomorphe au quotient G/C de sorte que la décomposition obtenue se réécrit $G \simeq C \times G/C$.)

Théorème. *Tout groupe abélien fini est isomorphe à un produit de groupes cycliques.*

Comme on a $\widehat{G_1} \times \widehat{G_2} \xrightarrow{\sim} \widehat{G_1 \times G_2}$ (canoniquement), on déduit comme annoncé que $\widehat{G}$ est, non canoniquement, isomorphe à G pour tout groupe abélien fini G. Par contre, le morphisme d'évaluation $\mathrm{ev} : G \to \widehat{\widehat{G}}$, $g \mapsto \big(\mathrm{ev}_g : \chi \mapsto \chi(g)\big)$ est un isomorphisme « canonique ». Cela résulte du fait que ces deux groupes, G et son

bidual, ont même cardinal et que le morphisme ev est injectif : si $x \neq 1$, il existe un caractère χ de G tel que $\chi(x) \neq 1$. (Étendre un caractère non trivial arbitraire de $\langle x \rangle$ à G.)

2.1.4. ¶*Équation $X^n = g$ dans un groupe abélien fini.* Pour tout entier n, notons $G[n] := \{g \in G : g^n = 1\}$ l'ensemble des éléments d'ordre divisant n et $nG = \{g^n : g \in G\}$ l'ensemble des puissances n-ièmes. L'injection $\widehat{G/nG} \hookrightarrow \widehat{G}[n]$, déduite de la surjection $G \twoheadrightarrow G/nG$ par dualité, est un isomorphisme pour des raisons de cardinalité. (On utilise ici le fait que G et $\widehat{G}$ sont (non canoniquement) isomorphes, de sorte que $(\widehat{G} : n\widehat{G}) = (G : nG)$.) Puisque qu'un élément est trivial si et seulement si son image par tout caractère l'est, on en déduit que les conditions suivantes sur un élément $g \in G$ sont équivalentes : $g \in nG$ et $\widehat{G}[n](g) = \{1\}$. Il est parfois utile de préciser ce résultat sous la forme quantitative suivante.

Proposition. *Soient G un groupe abélien fini, $g \in G$ et n un entier. Alors,*

$$\#\{x \in G : x^n = g\} = \sum_{\chi \in \widehat{G}[n]} \chi(g).$$

Démonstration. Le terme de gauche vaut 0 si $g \notin nG$ et $\#G[n]$ sinon car deux solutions diffèrent d'un élément de $G[n]$. Le terme de droite vaut quant à lui $\#\widehat{G}[n] = \#G[n]$ si $g \in nG$; il reste à voir qu'il est nul dans le cas contraire. Or, cette somme se réécrit $\sum_{\tau \in \widehat{G/nG}} \tau(\overline{g})$, où $\overline{g}$ désigne l'image de g dans G/nG. Cette somme est nulle si $\overline{g} \neq 0_{G/nG}$. □

(Voir [Serre 1992, 7.2] pour d'autres équations dans des groupes non nécessairement abéliens finis.)

2.2. Transformation de Fourier discrète.

Références : [Terras 1999, chap. 2, 8-9], [Gathen et Gerhard 2003, §8.2].

2.2.1. Soient p un nombre premier et $\mathbf{e} : \mathbb{F}_p \to \mu_p(\mathbb{C}) \subseteq \mathbb{C}^\times$, $x \mapsto \exp(2\pi i x/p)$, un caractère non trivial du groupe additif de $\mathbb{F}_p$. (On dit que $\mathbf{e}$ est un « *caractère additif* » du corps $\mathbb{F}_p$.) Pour toute fonction f sur $\mathbb{F}_p$ à valeurs complexes, notons pour abréger $\int\!\!\!\!\!\!\int f$ la somme finie $\sum_{t \in \mathbb{F}_p} f(t)$ et définissons le produit hermitien :

$$\langle f, g \rangle := \int\!\!\!\!\!\!\int f\overline{g}.$$

La **transformée de Fourier discrète** [离散傅里叶变换] $\mathscr{F}(f)$ d'une fonction f est la fonction $\mathbb{F}_p \to \mathbb{C}$,

$$\xi \mapsto \langle f, [\times\xi]^\star \mathbf{e} \rangle := \sum_{t \in \mathbb{F}_p} f(t)\mathbf{e}(-t\xi),$$

où, pour toute fonction g, on note $[\times\xi]^\star g$ la translatée multiplicative $t \mapsto g(t\xi)$[①].

Par exemple, pour chaque $x \in \mathbb{F}_p$, on a tautologiquement

$$\mathscr{F}(\delta_{-x}) = [\times x]^\star \mathbf{e}$$

① Le morphisme $\xi \mapsto [\times\xi]^\star \mathbf{e} = \mathbf{e}(\xi\cdot)$, $\mathbb{F}_p \to \widehat{\mathbb{F}_p}$ étant un isomorphisme, on pourrait alternativement voir $\mathscr{F}(f)$ comme une fonction sur $\widehat{\mathbb{F}_p}$.

et

$$\mathscr{F}([\times x]^\star \mathbf{e}) = p\delta_x.$$

(La dernière relation vient de l'orthogonalité des caractères : $\langle [\times x]^\star \mathbf{e}, [\times \xi]^\star \mathbf{e}\rangle = p[x = \xi\,?]$, où $[P?]$ vaut 1 si P est vraie et 0 sinon.) De ces exemples, on déduit que $\mathscr{F}$ est presque une isométrie involutive :

$$\mathscr{F}^2 = p[\times -1]^\star, \text{ c'est-à-dire } \mathscr{F}(\mathscr{F}(f))(x) = pf(-x)$$

et

$$\langle f, g\rangle = \frac{1}{p}\langle \mathscr{F}(f), \mathscr{F}(g)\rangle \text{ [Parseval]},$$

dont on déduit l'égalité $\|\mathscr{F}(f)\| = \sqrt{p}\|f\|$.

2.2.2. *Convolution, sommes de Gauß et Jacobi.*
Références : [Ireland et Rosen 1990, chap. 8], [Davenport 2000, chap. 2] ; [Weil 1974] (survol historique).

Si f et g sont deux fonctions sur $\mathbb{F}_p$, on définit comme dans le cas classique leur **produit de convolution** [卷积/捲積] (additive) : c'est la fonction

$$f \star g : t \mapsto \sum_{u+v=t} f(u)g(v) = \sum_u f(u)g(t-u).$$

La transformation de Fourier transforme produit de convolution en produit usuel :

$$\mathscr{F}(f \star g) = \mathscr{F}(f)\mathscr{F}(g).$$

Soit maintenant χ un caractère *multiplicatif* de $\mathbb{F}_p$, c'est-à-dire un morphisme $\mathbb{F}_p^\times \to \mathbb{C}^\times$, étendu à $\mathbb{F}_p$ en posant $\chi(0) = 0$. On vérifie immédiatement l'égalité

$$\mathscr{F}(\chi) = \mathfrak{g}_\chi \overline{\chi} + [\chi = \mathbf{1}?](p-1)\delta_0,$$

où $\mathbf{1}$ désigne le caractère trivial de $\mathbb{F}_p^\times$ et $\mathfrak{g}_\chi$ est la **somme de Gauß** [高斯和]

$$\mathscr{F}(\chi)(1) = \int_{t\in\mathbb{F}_p^\times} t^\chi \mathbf{e}(-t)\mathrm{d}t = \sum_{t\in\mathbb{F}_p^\times} \chi(t)\exp(2\pi i t/p).$$

En particulier, si $\chi \neq \mathbf{1}$, il résulte de la formule de Parseval que

$$|\mathfrak{g}_\chi| = \sqrt{p}.$$

(Par contre, $\mathfrak{g}_\mathbf{1} = -1$.) Notons que le conjugué $\overline{\mathfrak{g}_\chi}$ de $\mathfrak{g}_\chi$ égal à $\chi(-1)\mathfrak{g}_{\overline{\chi}}$.

Soient χ_1, χ_2 deux caractères multiplicatifs. Par changement de variable, on constate que le produit de convolution f de χ_1 et χ_2 satisfait la relation $f(x) = f(1)\cdot(\chi_1\chi_2)(x)$ pour chaque $x \neq 0$; on a donc l'égalité

$$\chi_1 \star \chi_2 = J(\chi_1, \chi_2)\cdot \chi_1\chi_2 + [\chi_1\chi_2 = \mathbf{1}?]p\chi_1(-1)\cdot\delta_0,$$

où $J(\chi_1, \chi_2)$ est la **somme de Jacobi** [雅可比和]

$$(\chi_1 \star \chi_2)(1) = \sum_{a\in\mathbb{F}_p} \chi_1(a)\chi_2(1-a).$$

En particulier, lorsque $\chi_1\chi_2 \neq \mathbf{1}$, on a $\chi_1 \star \chi_2 = J(\chi_1,\chi_2)\cdot\chi_1\chi_2$, égalité qui devient, en appliquant Fourier :

$$\mathfrak{g}_{\chi_1}\mathfrak{g}_{\chi_2} = J(\chi_1,\chi_2)\mathfrak{g}_{\chi_1\chi_2}\ ①.$$

Plus généralement, on a $\chi_1 \star \cdots \star \chi_r = J(\chi_1,\ldots,\chi_r)\chi_1\cdots\chi_r$, lorsque $\chi_1\cdots\chi_r \neq \mathbf{1}$, où

$$J(\chi_1,\ldots,\chi_r) \coloneqq \chi_1 \star \cdots \star \chi_r(1) = \sum_{a_1+\cdots+a_r=1} \chi_1(a_1)\cdots\chi_r(a_r)$$

et, sous la même hypothèse, $\mathfrak{g}_{\chi_1}\cdots\mathfrak{g}_{\chi_r} = J(\chi_1,\ldots,\chi_r)\mathfrak{g}_{\chi_1\cdots\chi_r}$.

2.3. Application n°1 : constructibilité à la règle et au compas.

Références : [Cox 2004, chap. 10] (généralités), [Ireland et Rosen 1990, chap. 9, §11], [Davenport 2000, chap. 3] ; [Lebesgue 1950, §76], [Eisenbud 2015] (heptadécagone).

2.3.1. Un nombre complexe $z \in \mathbb{C}$ est dit **constructible** [规矩/可造] s'il existe une suite d'extensions *quadratiques* $\mathbb{Q} = K_0 \subset \cdots \subset K_i \subset K_{i+1} \subset \cdots \subset K_n \subset \mathbb{C}$ telle que $z \in K_n$. (« Quadratiques » : $[K_{i+1} : K_i] = 2$.) En particulier, z est algébrique (sur $\mathbb{Q}$) et $[\mathbb{Q}(z) : \mathbb{Q}]$ est une puissance de 2. On vérifie que z, vu comme point du plan complexe $\mathbb{C} = \mathbb{R}^2$, est constructible si et seulement si il est constructible à la règle et au compas à partir des points $0 = (0,0), 1 = (1,0)$ et $i = (0,1)$. Soient p un nombre premier et $\zeta \coloneqq \exp(2\pi i/p) \in \mathbb{C}$ une racine primitive p-ième de l'unité. Il résulte de l'irréductibilité du polynôme cyclotomique Φ_p que si ζ est constructible, alors $p - 1 = \deg(\Phi_p) = [\mathbb{Q}(\zeta) : \mathbb{Q}]$ est une puissance de 2 : le nombre p est un *nombre premier de Fermat* [费马素数]②. Nous allons montrer la réciproque, due à Gauß③. En particulier, les polygones réguliers ci-dessous (pentagone et heptadécagone) sont constructibles à la règle et au compas.

---

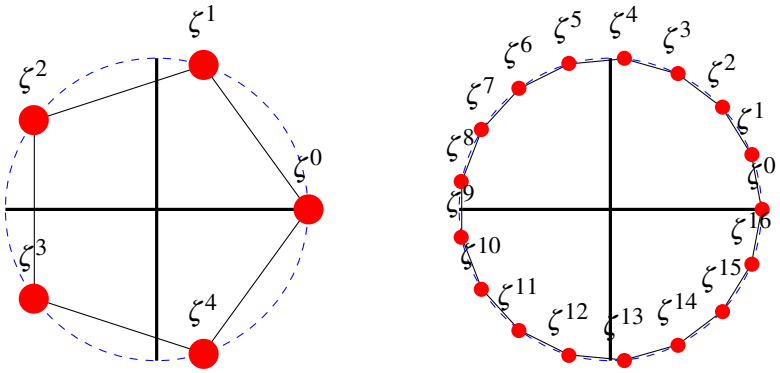
①. Noter les analogies :

$$\begin{aligned}
\mathfrak{g}_\chi &\leftrightarrow \Gamma(\chi) \coloneqq \textstyle\int_{\mathbb{R}_+^\times} t^\chi e^{-t}\frac{\mathrm{d}t}{t} && \text{(fonction Gamma)}\\
J(\chi_1,\chi_2) &\leftrightarrow B(\chi_1,\chi_2) \coloneqq \textstyle\int_{a\in[0,1]} a^{\chi_1}(1-a)^{\chi_2}\mathrm{d}a && \text{(fonction Bêta)}\\
\mathfrak{g}_{\chi_1}\mathfrak{g}_{\chi_2} = J(\chi_1,\chi_2)\mathfrak{g}_{\chi_1\chi_2} &\leftrightarrow \Gamma(\chi_1)\Gamma(\chi_2) = B(\chi_1,\chi_2)\Gamma(\chi_1\chi_2)
\end{aligned}$$

②. Prendre garde au fait qu'il existe des nombres complexes z non constructibles tels que $[\mathbb{Q}(z) : \mathbb{Q}]$ soit une puissance de 2. Par exemple une racine de $T^4 + T^3 - T^2 + T - 1$.

③. Selon la légende, c'est cette découverte — sensationnelle à l'époque — qui aurait décidé Gauß (alors âgé d'un peu moins de 19 ans) à devenir mathématicien, et non linguiste/philologue [语文学家]. Sa démonstration est exposée en détail dans ses *disquisitiones arithmeticæ* (recherches arithmétiques) [Gauß 1807, §7]. La découverte elle-même semble dater du 30 mars 1796. C'est la première entrée dans son fameux *Tagebuch* ([Gauß 2005]) :

> « Principia quibus innititur sectio circuli, ac divisibilitas eiusdem geometrica in septemdecim partes etc. »



2.3.2. Notons $\mathbb{F}$ le corps fini $\mathbb{Z}/p\mathbb{Z}$. La somme $\sum_\chi \mathfrak{g}_\chi = \mathscr{F}(\sum_\chi \chi)(0) - (p-1)$, où χ parcourt l'ensemble $\widehat{\mathbb{F}^\times}$ des caractères multiplicatifs de $\mathbb{F}$, étant égale à $(p-1)\zeta$, il nous suffit de montrer que si p est un nombre de Fermat premier chacune des sommes de Gauß $\mathfrak{g}_\chi$ est constructible. (On utilise ici le fait qu'une somme de nombres constructibles est constructible.) D'autre part, chaque $\mathfrak{g}_\chi$ est constructible si et seulement si $\mathfrak{g}_\chi^{2^r}$ est constructible pour un (resp. chaque) $r \geq 0$: une racine carré d'un nombre constructible est constructible.

Écrivons $p-1 = 2^n$ et considérons $\chi \neq \mathbf{1}$; il est d'ordre 2^m pour un entier $m \leq n$. (La constructibilité de $\mathfrak{g}_\mathbf{1} = -1$ est triviale.) Calculons $\mathfrak{g}_\chi^{2^m}$. Les relations entre sommes de Gauß et sommes de Jacobi montrent que l'on a $\mathfrak{g}_\chi^2 = J(\chi,\chi)\mathfrak{g}_{\chi^2}$, $\mathfrak{g}_\chi^4 = J(\chi,\chi)^2 J(\chi^2,\chi^2)\mathfrak{g}_{\chi^4}$, et plus généralement que $\mathfrak{g}_\chi^{2^r}$, pour $r < m$ est un multiple de $\mathfrak{g}_{\chi^{2^r}}$ par un produit de sommes de Jacobi. (Alternativement, on peut utiliser directement la relation $\mathfrak{g}_\chi^{2^r} = J(\chi,\ldots,\chi)\mathfrak{g}_{\chi^{2^r}}$.) Le caractère multiplicatif χ étant à valeurs dans $\mu_{p-1}(\mathbb{C}) = \mu_{2^n}(\mathbb{C})$, les sommes de Jacobi sont constructibles. Appliquant ce qui précède à $r = m-1$, on voit qu'il suffit donc de montrer que la somme de Gauß $\mathfrak{g}_\chi$ est constructible dans le cas particulier où $\chi^2 = \mathbf{1}$, c'est-à-dire $\chi = \overline{\chi}$. Or, $|\mathfrak{g}_\chi|^2 = p = \mathfrak{g}_\chi \cdot \overline{\mathfrak{g}_\chi} = \chi(-1)\mathfrak{g}_\chi^2 = \pm\mathfrak{g}_\chi^2$. Il en résulte que dans ce cas $\mathfrak{g}_\chi^2 = \pm p$, si bien que $\mathfrak{g}_\chi$ qui est bien constructible. CQFD.

2.3.3. La démonstration précédente permet a priori de faire des calculs explicites. Pour $p = 17$, on peut vérifier l'égalité

$$\begin{aligned}\cos\frac{2\pi}{17} &= -\frac{1}{16} + \frac{1}{16}\sqrt{17} + \frac{1}{8}\sqrt{\frac{17}{2} - \frac{1}{2}\sqrt{17}} \\ &\quad + \frac{1}{4}\sqrt{\frac{17}{4} + \frac{3}{4}\sqrt{17} - \frac{1}{2}\sqrt{\frac{17}{2} - \frac{1}{2}\sqrt{17}} - \sqrt{\frac{17}{2} + \frac{1}{2}\sqrt{17}}},\end{aligned}$$

qui ne fait apparaître que des extractions de racines *carrées*[①].

2.4. Application n°2 : réciprocité quadratique.

Référence : [Ireland et Rosen 1990, chap. 5].

Soient p un nombre premier $\neq 2$ et $\mathbb{F}$ le corps fini $\mathbb{Z}/p\mathbb{Z}$. Il existe un unique caractère non trivial $\mathbb{F}^\times \to \{\pm 1\} \subseteq \mathbb{C}^\times$; cela résulte du fait que le groupe multiplicatif $\mathbb{F}^\times$ est (non canoniquement) isomorphe à $\mathbb{Z}/(p-1)\mathbb{Z}$. On note traditionnellement

$$x \mapsto (\frac{x}{p})$$

ce caractère, qui vaut 1 sur les carrés de $\mathbb{F}^\times$ et -1 sinon. (Comme dans le paragraphe précédent, on étend ce caractère multiplicatif à $\mathbb{F}$ tout entier en posant $(\frac{0}{p}) = 0$.) Puisque qu'un élément $x \in \mathbb{F}^\times$ est un carré si et seulement si $x^{\frac{p-1}{2}} = 1_{\mathbb{F}}$, on en déduit en particulier que $(\frac{-1}{p}) = (-1)^{(p-1)/2}$.

Soit maintenant $\ell \neq p$ un autre nombre premier $\neq 2$. Notons ci-dessous pour abréger [②] le caractère $(\frac{\cdot}{p})$. Puisque $^\ell = $ est non trivial, on a (†) $\mathfrak{g}^\ell = J(,\ldots,)\mathfrak{g}$. Comme

$$\mathfrak{g}^2 = (-1)^{(p-1)/2} p,$$

on en déduit en simplifiant (†) par $\mathfrak{g}$ que l'on a l'égalité

$$\left((-1)^{(p-1)/2} p\right)^{\frac{\ell-1}{2}} = \sum_{a_1+\cdots+a_\ell=1} (a_1)\cdots(a_\ell).$$

Le terme de droite, *a priori* complexe, est un entier : c'est une somme de ± 1. Notons que le groupe $\mathbb{Z}/\ell\mathbb{Z}$ agit naturellement sur l'hyperplan affine $\{\underline{a} : a_1 + \cdots + a_\ell = 1\} \subseteq \mathbb{F}^\ell$ par permutation cyclique des coordonnées et l'expression $(a_1)\cdots(a_\ell)$ est invariante sous cette action. Il en résulte que la somme de Jacobi est un entier congru modulo ℓ à $(1/\ell)\cdots(1/\ell) = (\ell)^\ell = (\ell)$, qui est la contribution de l'unique point fixe. Ainsi on a l'égalité modulo ℓ :

$$(-1)^{(\ell-1)(p-1)/4} p^{\frac{\ell-1}{2}} \equiv (\frac{\ell}{p}).$$

Comme $p^{\frac{\ell-1}{2}} \equiv (\frac{p}{\ell}) \pmod{\ell}$, on en déduit le théorème suivant.

Théorème. *Soient p, ℓ deux nombres premiers impairs distincts. On a alors :*

$$(\frac{p}{\ell})(\frac{\ell}{p}) = (-1)^{(p-1)(\ell-1)/4}.$$

---

① Comparer par exemple avec

$$\begin{aligned}\cos\frac{2\pi}{11} \;=\; -\frac{1}{10} \;+\; \frac{1}{40}\sqrt[5]{\frac{11}{4}}\;\times\;&\\ \Big(\;&\left(-1+\sqrt{5}+\sqrt{-10-2\sqrt{5}}\right)\sqrt[5]{-89-25\sqrt{5}-20\sqrt{-10-2\sqrt{5}}+25\sqrt{-10+2\sqrt{5}}}\\ +\;&\left(-1+\sqrt{5}-\sqrt{-10-2\sqrt{5}}\right)\sqrt[5]{-89-25\sqrt{5}+20\sqrt{-10-2\sqrt{5}}-25\sqrt{-10+2\sqrt{5}}}\\ +\;&\left(-1+\sqrt{5}+\sqrt{-10-2\sqrt{5}}\right)\sqrt[5]{-89+25\sqrt{5}-25\sqrt{-10-2\sqrt{5}}-20\sqrt{-10+2\sqrt{5}}}\\ +\;&\left(-1+\sqrt{5}-\sqrt{-10-2\sqrt{5}}\right)\sqrt[5]{-89+25\sqrt{5}+25\sqrt{-10-2\sqrt{5}}+20\sqrt{-10+2\sqrt{5}}}\;\Big)\end{aligned}$$

② Lettre grecque « koppa ».

Autrement dit, $(\frac{\ell}{p}) = (\frac{p}{\ell})$ *sauf si* $p, \ell \equiv -1 \pmod 4$.

On a également la « formule complémentaire » :

$$(\frac{2}{p}) = (-1)^{(p^2-1)/8}.$$

Voir par exemple l'exercice 11 pour une démonstration.

2.5. ¶Application n°3 : courbe de Fermat et sphères sur $\mathbb{F}_p$.
Références : [ibid., chap. 8, 10], [Weil 1949].

2.5.1. Nous nous intéressons ici au nombre de points de la courbe de Fermat (affine) C_n d'équation $X^n+Y^n=1$. Plus précisément, à n fixé, on souhaite estimer, pour p variable (ne divisant pas n pour simplifier) le cardinal de l'ensemble

$$C_n(\mathbb{F}_p) := \{(x,y)\in\mathbb{F}_p^2 \,:\, x^n+y^n=1\}.$$

Comme on l'a vu ci-dessus (**2.1.4**), pour tout $a\in\mathbb{F}_p^\times$ on a l'égalité

$$\#\{x\in\mathbb{F}_p \,:\, x^n=a\} = 1+\sum_{\chi\in\widehat{\mathbb{F}_p^\times}[n]\smallsetminus\{\mathbf{1}\}}\chi(a),$$

où χ parcourt les caractères multiplicatifs non triviaux de $\mathbb{F}_p$, d'ordre divisant n. Puisque le cardinal de $C_n(\mathbb{F}_p)$ est tautologiquement égal à

$$\sum_{a_1+a_2=1}\#\{x\,:\,x^n=a_1\}\cdot\#\{y\,:\,y^n=a_2\},$$

on en déduit que ce cardinal est égal à $p+\sum_{\chi_1,\chi_2\in\widehat{\mathbb{F}_p^\times}[n]\smallsetminus\{\mathbf{1}\}} J(\chi_1,\chi_2)$, où le terme « p », n'est autre que le cardinal de la droite affine $a_1+a_2=1$ dans $\mathbb{F}_p^2$. On obtient en particulier l'estimation :

$$\left|\frac{\#C_n(\mathbb{F}_p)}{p}-1\right| \leq (n-1)^2\times\frac{1}{\sqrt{p}}.$$

On pourrait, comme l'a fait Weil, estimer plus généralement (et plus précisément) le nombre de points modulo p d'une « hypersurface diagonale » d'équation $c_0x_0^{n_0}+c_1x_1^{n_1}+\cdots+c_dx_d^{n_d}=1$.

2.5.2. Intéressons nous maintenant à la sphère S^d d'équation $\sum_{i=0}^d X_i^2=1$, pour d impair[①]. Pour chaque nombre premier $p\neq 2$, on a vu qu'il existe un unique caractère multiplicatif d'ordre 2 de $\mathbb{F}_p$, que nous notons à nouveau . Comme ci-dessus, pour chaque $a\in\mathbb{F}_p$, on a l'égalité $\#\{x\,:\,x^2=a\}=1+(a)$, si bien que $\#S^d(\mathbb{F}_p)=p^d+J(,\ldots,)$ ($d+1$ termes), où le terme « p^d » n'est autre que le cardinal de l'hypersurface $a_0+\cdots+a_d=1$ dans $\mathbb{F}_p^{d+1}$. (On utilise ici le fait que les autres termes qui apparaissent *a priori* sont des multiples de $\sum_a(a)=0$.) Comme la somme de Jacobi est égale à $\mathfrak{g}^d$, dont on connaît le module, on obtient l'estimation :

$$\left|\frac{\#S^d(\mathbb{F}_p)}{p^d}-1\right| \leq 1\times\frac{1}{\sqrt{p}^d}.$$

Ces calculs — joints à l'étude topologique des ensembles $C_n(\mathbb{C})$ (surface de Riemann) et $S^d(\mathbb{C})$ (sphère complexe) — sont à l'origine des célèbres *conjectures de Weil* [Weil[②]猜想] démontrées par Alexander Grothendieck ([**SGA 4**], [**SGA 5**]) et Pierre Deligne ([Deligne 1974]).

① On pourrait, comme l'a fait Weil, estimer plus généralement (et plus précisément) le nombre de points modulo p d'une « hypersurface diagonale » d'équation $c_0x_0^{n_0}+c_1x_1^{n_1}+\cdots+c_dx_d^{n_d}=1$. Le principal ingrédient technique de son article que nous n'abordons pas ici est le théorème de Hasse-Davenport, dont il existe cependant des démonstrations élémentaires (voir par exemple [Ireland et Rosen 1990, chap. 11, §4]). Voir aussi [Sommes trig., 1.15] pour une démonstration conceptuelle.

② « 魏尔 »

3. Factorisation des polynômes

3.1. Généralités.

Référence : [Jacobson 1985, §2.14, §2.16].

3.1.1. Soit k un *corps*. Un polynôme non constant $f \in k[T]$ est dit **irréductible** [不可约] si toute factorisation $f = P_1 P_2$ est *triviale* au sens suivant : l'un des deux polynômes P_1, P_2 est constant. Plus généralement, si A est un anneau *intègre*, on dit qu'un élément $a \in A \smallsetminus \{0\}$ est irréductible si ses seuls diviseurs sont les unités $u \in A^\times$ ou les ua, pour $u \in A^\times$. (Observer que l'on note $A^\times$ l'ensemble des unités [=inversibles] d'un anneau A, à ne pas confondre en général avec l'ensemble $A \smallsetminus \{0\}$ des éléments non nuls.)

Il n'est pas difficile de démontrer que tout polynôme unitaire $f \in k[T]$ se factorise de façon (essentiellement) unique[①] en un produit de polynômes irréductibles ; cela résulte du fait plus général suivant : $k[T]$ est un anneau principal [主理想环] donc factoriel [唯一因子分解整环].

3.1.2. Soient A un anneau intègre, équipé de deux morphismes $A \hookrightarrow K$ et $A \twoheadrightarrow k$ — dont le diagramme $\mathbb{Z}/p\mathbb{Z} \twoheadleftarrow \mathbb{Z} \hookrightarrow \mathbb{Q}$ est un exemple —, et $f \in A[T]$. On peut s'interroger sur les relations entre l'irréductibilité de f dans (l'anneau intègre) $A[T]$ et celle des images $f_K \in K[T]$ et $f_k \in k[T]$ de f. Si l'on ne fait pas d'hypothèse supplémentaire sur f ou A, aucune implication n'est vraie. Par contre, si f est *unitaire*, l'irréductibilité de f_k ou f_K entraîne celle de f. Il résulte du lemme de Gauß (voir **3.3**) que si A est *factoriel* (par exemple : $A = \mathbb{Z}$), on a la réciproque partielle : f (unitaire) irréductible entraîne f_K irréductible. Par contre, f_k n'est pas nécessairement irréductible, même dans les cas les plus simples (voir **1.5.5** et l'exercice 5).

Cependant, on verra, dans le cas particulier où $A = \mathbb{Z}$, que des techniques de « réduction modulo p » sont malgré tout utiles à l'étude de la factorisation des polynômes à coefficients entiers (ou, cela revient essentiellement au même, à coefficients rationnels).

3.1.3. ¶*Abondance des polynômes irréductibles.* À titre de motivation, donnons une première application de techniques de réduction modulo p. (Voir aussi par exemple 31 pour un résultat plus élémentaire dans ce sens.)

Proposition. *Soit $d \geq 1$ un entier. Parmi les polynômes $f \in \mathbb{Z}[T]$ unitaires de degré d à coefficients dans un intervalle $[-N, N]$, la proportion de ceux qui sont* irréductibles *tend vers* 1 *lorsque N tend vers $+\infty$.*

Démonstration. Il suffit de montrer que si $P = p_1 \dots p_r$ est un produit de nombres premiers > 3 distincts (par exemple, $P = 3 \cdot 5 \cdot 7 \cdots$) et $N \geq P$, la proportion des polynômes unitaires réductibles à coefficients dans $[-N, N]$ est majorée par $(\frac{3}{2})^d (1 - \frac{1}{2d})^r$ car cette quantité tend vers 0 lorsque $r \to +\infty$. L'application envoyant un polynôme $f \in \mathbb{Z}[T]$ à coefficients dans $[-N, N]$, unitaire de degré d, sur sa réduction $f \bmod P \in \mathbb{Z}/P\mathbb{Z}[T]$ est à fibres de cardinal au plus $(\frac{2N+1}{P} + 1)^d$, que l'on

① Le *multiensemble* [多重集] des facteurs irréductibles (unitaires) est déterminé par f.

majore par $\frac{3}{2}^d(2N+1)^d P^{-d}$ sous l'hypothèse faite sur N. Elle envoie un polynôme réductible (unitaire, de degré d) sur un polynôme réductible (unitaire, de degré d). D'autre part, il résulte du lemme chinois que l'application $\mathbb{Z}/P\mathbb{Z}[T] \to \mathbb{F}_{p_1}[T] \times \ldots \times \mathbb{F}_{p_r}[T]$ de réduction modulo chacun des p_i est un isomorphisme d'anneaux ; en particulier les conditions « être réductible modulo p_i » sont indépendantes. D'après **1.5.6**, la proportion des polynômes *réductibles* parmi les polynômes de $\mathbb{Z}/P\mathbb{Z}[T]$ unitaires de degré d est donc majorée par $(1-\frac{1}{2d})^r$. Ainsi le nombre de polynômes réductibles comme dans l'énoncé est majoré par $(1-\frac{1}{2d})^r \times P^d \times (\frac{2N+1}{P}+1)^d$, comme annoncé. □

Pour $d = 5$, cette méthode donne N à environ 70 chiffres (en base 10) pour obtenir une proportion d'irréductibles supérieure à 90%. Cependant, un ordinateur calcule en quelques minutes que pour $N = 9$, la proportion est déjà $\frac{113897}{130321} = \frac{7\cdot 53\cdot 307}{19^4} \approx 0,87$.

3.2. Critères d'irréductibilité dans les corps finis $\mathbb{F}_q$.

Références : [TAOCP 2, 4.6.2], [Shoup 2009, chap. 20], [Gathen et Gerhard 2003, §14].

3.2.1. Proposition (Critères de Rabin et Ben-Or). *Un polynôme $f \in \mathbb{F}_q[T]$ de degré d est irréductible si et seulement si il vérifie l'un des deux critères ci-dessous.*

(Rabin) Le polynôme f divise divise $T^{q^d} - T$ et est premier avec $T^{q^r} - T$ pour tout r diviseur strict de d (ou simplement les diviseurs immédiats de d, c'est-à-dire les d/ℓ avec ℓ diviseur premier de d).

(Ben-Or) Le polynôme f est premier avec $T^{q^r} - T$ pour tout $1 \leq r \leq \lfloor \frac{d}{2} \rfloor$.

(La courte démonstration est laissée en exercice au lecteur.)

Faisons quelques remarques. Premièrement, dans le critère de Rabin, on ne peut pas se contenter de vérifier l'une des deux conditions énoncées : l'exemple du polynôme $T^6+T^5+T^4+T^3+T^2+T+1 = (T^3+T^2+1)(T^3+T+1) \in \mathbb{F}_2[T]$, qui n'est pas irréductible mais vérifie la première condition (il divise déjà $T^8 - T$) montre que la première condition, seule, n'assure pas l'irréductibilité ; et l'exemple du polynôme $T^5+T^4+1 = (T^2+T+1)(T^3+T+1) \in \mathbb{F}_2[T]$, qui n'est pas irréductible mais est premier à $T^2 - T$ montre que la seconde condition, seule, n'est pas non plus suffisante. On peut aussi donner l'exemple de $T^6+T^5+T = T(T^2+T+1)(T^3+T+1) \in \mathbb{F}_2[T]$, qui n'est pas irréductible bien qu'il vérifie la première condition et aussi la seconde condition dans laquelle on a affaibli « f est premier avec $T^{q^r} - T$ » en « f ne divise pas $T^{q^r} - T$ » (pour tout diviseur r de d, soit ici $r \in \{1, 2, 3\}$). Enfin, l'un et l'autre de ces critères fournissent un *algorithme* permettant de tester l'irréductibilité d'un polynôme $f \in \mathbb{F}_q[T]$ de degré d en un nombre raisonnable (i.e., polynomial[①] en d) d'opérations dans $\mathbb{F}_q$: en effet, la première condition du critère s'exprime également comme $T^{q^d} \equiv T \pmod f$, ce qui se teste en calculant T^{q^d} dans $\mathbb{F}_q[T]/(f)$ au moyen d'un algorithme d'exponentiation rapide, et la seconde condition, pour un r donné, peut se tester au moyen de l'algorithme d'Euclide étendu (pour calculer le

① On peut par exemple montrer qu'il s'effectue en au pire $O(d^{2+\varepsilon})$ opérations pour tout $\varepsilon > 0$, où la constante impliquée par le O dépend de ε et q.

PGCD), dont la première étape consiste à calculer le reste de la division euclidienne de $T^{q^r} - T$ par f, ce qui peut de nouveau se faire en travaillant dans $\mathbb{F}_q[T]/(f)$.

Appliquons le critère de Ben-Or au polynôme $f = T^5 - T^2 - 1 = T^5 + T^2 + 1 \in \mathbb{F}_2[T]$. Le reste de f modulo $T^2 - T$ et $T^4 - T$ est 1 donc f est irréductible.

3.2.2. *Algèbre de Berlekamp.* Le critère d'irréductibilité suivant utilise, pour sa part, l'algèbre linéaire plutôt que des manipulations de polynômes. Rappelons que toute $\mathbb{F}_q$-algèbre A est munie d'un *endomorphisme* $\mathrm{Frob}_q : A \to A$, $a \mapsto a^q$, qui est la puissance $\log_p(q)$-ième du Frobenius Frob_p. L'ensemble $\mathrm{Fix}(\mathrm{Frob}_q \circlearrowright A) \coloneqq \{a \in A : a^q = a\}$ est donc une *sous-$\mathbb{F}_q$-algèbre* de A, de dimension ≥ 1 (sauf si $A = \{0\}$). Lorsque $A = \mathbb{F}_q[T]/(f)$, où f est un polynôme non nul à coefficients dans $\mathbb{F}_q$, cette algèbre est appelée **algèbre de Berlekamp** de f,

$$B(f) \coloneqq \mathrm{Ker}\left(\mathrm{Frob}_q - \mathrm{Id} : \mathbb{F}_q[T]/(f) \to \mathbb{F}_q[T]/(f)\right).$$

Notons qu'elle est de dimension inférieure ou égale à $\deg(f)$ et que sa dimension est calculable par la méthode du pivot de Gauß : il suffit de calculer le rang de l'application $\mathbb{F}_q$-linéaire $\mathrm{Frob}_q - \mathrm{Id} : A \to A$, que l'on peut écrire explicitement dans la base $1, T, \ldots, T^{\deg(f)-1}$ de A en effectuant les divisions euclidiennes des T^{iq} par f. Lorsque f est irréductible, $\mathbb{F}_q[T]/(f)$ est un corps et $B(f)$ n'est autre que le sous-corps $\mathbb{F}_q \subseteq \mathbb{F}_q[T]/(f)$.

Si $f = \prod_{i=1}^{r} f_i^{e_i}$, où les f_i sont premiers entre eux deux à deux (non constants), on a d'après le théorème chinois un isomorphisme 中 : $B(f) \xrightarrow{\sim} \prod_i B(f_i^{e_i})$ et, en particulier, $\dim_{\mathbb{F}_q} B(f) = \sum_i \dim_{\mathbb{F}_q} B(f_i^{e_i})$ est supérieur ou égal à r. Si les f_i sont irréductibles et que l'on sait *a priori* que les e_i sont égaux à 1, on a équivalence entre : « f est irréductible » et « $\dim_{\mathbb{F}_q} B(f) = 1$ ». (Plus généralement, un facteur non constant g de f est irréductible si et seulement si tous les $y \in B(f)$ se réduisent modulo g en une constante.)

L'hypothèse que les e_i sont égaux à 1 revient à dire que f est sans facteur carré ; lorsque f est un corps fini (ou un corps de caractéristique nulle ; plus généralement un corps « parfait »), cela est équivalent à la propriété suivante : f est premier avec sa dérivée. Un tel polynôme (à coefficients dans un corps quelconque) est un **polynôme séparable** [可分多项式]. Cette condition se teste algorithmiquement par l'algorithme d'Euclide (voir aussi §**3.5**) et est équivalente au fait que les racines de f dans une clôture algébrique de k sont simples. Résumons ces observations sous la forme d'une proposition.

Proposition. *Soit $f \in \mathbb{F}_q[T]$ unitaire* séparable. *Alors, la dimension r sur $\mathbb{F}_q$ de l'algèbre de Berlekamp $B(f)$ de f est égale au nombre de facteurs unitaires irréductibles de f. De plus, pour tout $y \in B(f)$, on a $f = \prod_{c \in \mathbb{F}_q} \mathrm{PGCD}(f, y - c)$.*

Par convention, le PGCD de deux polynômes non tous nuls f, g à coefficients dans un corps, aussi noté $f \wedge g$, est le générateur *unitaire* de l'idéal $(f, g) = (f) + (g)$. (Le complément résulte de ce que $y \in B(f) = \prod_i B(f_i)$ alors $f \wedge y$ est le produit des f_i tels que y soit multiple de f_i c'est-à-dire que la i-ième composante de 中(y) s'annule.)

Corollaire (critère d'irréductibilité de Butler). *Un polynôme séparable $f \in \mathbb{F}_q[T]$ est irréductible si et seulement si* $\dim_{\mathbb{F}_q} \mathrm{Ker}(\mathrm{Frob}_q - \mathrm{Id}) = 1$, *où* $\mathrm{Frob}_q : x \mapsto x^q$ *et* $\mathrm{Id} : x \mapsto x$ *sont vus comme des applications $\mathbb{F}_q$-linéaires sur $\mathbb{F}_q[T]/(f)$.*

Lorsque q est petit, la proposition précédente fournit telle quelle un algorithme de factorisation, dit de Berlekamp, pour les polynômes f sans facteur carré dans $\mathbb{F}_q[T]$: on utilise des techniques d'algèbre linéaire pour trouver une $\mathbb{F}_q$-base $\tau_1, \dots, \tau_s$ de l'algèbre de Berlekamp $B(f) = \mathrm{Ker}(\mathrm{Frob}_q - \mathrm{Id})$ de f, puis, si $s > 1$ de sorte qu'il y a une factorisation non triviale à effectuer, on tire au hasard un élément $y = c_1\tau_1 + \cdots + c_s\tau_s \in B(f)$ (avec $c_i \in \mathbb{F}_q$) et on calcule les $\mathrm{PGCD}(f, y - c)$ pour les différents $c \in \mathbb{F}_q$: ceci fournira une factorisation non triviale de y dès que les composantes de 中(y) ne sont pas toutes égales (où 中 est l'isomorphisme $B_f \xrightarrow{\sim} (\mathbb{F}_q)^s$ déduit de l'isomorphisme chinois), ce qui se produit pour $q^s - q$ des q^s éléments y de B_f.

Lorsque q est grand, la proposition ne peut pas servir en tant que telle. On peut cependant la combiner avec les mêmes idées que celles utilisées dans l'algorithme dit de Cantor-Zassenhaus, que nous ne détaillons pas : une fois tiré y dans B_f, on calcule $t = y^{(q-1)/2}$ (resp. $t = y + y^2 + y^4 + \cdots + y^{q/2}$ en caractéristique 2), et alors $\mathrm{PGCD}(f, t - 1)$ (resp. $\mathrm{PGCD}(f, t)$) a une probabilité raisonnable de fournir un facteur non trivial de f.

Reprenons l'exemple du polynôme $f = T^5 - T^2 - 1 (= T^5 + T^2 + 1) \in \mathbb{F}_2[T]$, en lui appliquant cette fois le critère de Butler : il faut d'abord vérifier que f est séparable, c'est-à-dire, premier avec sa dérivée $f' = T^4$, ce qui se fait en général au moyen de l'algorithme d'Euclide mais est évident ici. On calcule alors la matrice de l'endomorphisme $\mathrm{Frob}_2 - \mathrm{Id}$ sur la base $1, t, t^2, \dots, t^4$ de $\mathbb{F}_2[T]/(f)$, en calculant successivement $T^2, T^4, \dots, T^8$ modulo f :

$$\mathrm{Frob}_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}, \quad \mathrm{Frob}_2 - \mathrm{Id} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

(Les coefficients de la première matrice sont les coefficients des restes de $1, T^2, T^4, T^6, T^8$ modulo f.) En général, on calcule le rang de cette deuxième matrice en appliquant l'algorithme du pivot de Gauß ; ici, on vérifie immédiatement que le bloc 4×4 inférieur droit est inversible. Ceci montre que $\dim_{\mathbb{F}_2} \mathrm{Ker}(\mathrm{Frob}_2 - \mathrm{Id}) = 1$, donc f est bien irréductible.

3.3. Irréductibilité sur $\mathbb{Q}$ *versus* sur $\mathbb{Z}$: (un) lemme de Gauß.

3.3.1. Un polynôme $a_nT^n + a_{n-1}T^{n-1} + \cdots + a_0$ à coefficients dans un anneau k est dit **primitif** [本原多项式] si l'idéal $(a_0, a_1, \dots, a_n) \subseteq k$ engendré par ses coefficients est égal à k tout entier. Si par exemple $k = \mathbb{Z}$, cela revient à dire que leur PGCD est égal 1. La proposition suivante, bien qu'élémentaire, est cruciale.

3.3.2. Proposition (« lemme de Gauß »). *Le produit de deux polynômes primitifs est un polynôme primitif.*

Démonstration, sans l'axiome du choix. On veut montrer que si $f = a_nT^n + a_{n-1}T^{n-1} + \cdots + a_0$ et $g = b_mT^m + b_{m-1}T^{m-1} + \cdots + b_0$ sont tels qu'il existe des $p_0, \dots, p_n$ et

des $q_0, \dots, q_m$ pour lesquels $\sum_{i=0}^{n} a_i p_i = 1$ et $\sum_{j=0}^{m} b_j q_j = 1$, alors, il existe des $r_0, \dots, r_{n+m}$ tels que $\sum_{l=0}^{n+m} c_l r_l = 1$, où les $c_l := \sum_{i+j=l} a_i b_j$ sont les coefficients du produit fg. Un instant de réflexion nous convainc qu'il suffit de démontrer que l'idéal I de l'anneau

$$R := \mathbb{Z}[A_0, \dots, A_n, B_0, \dots, B_m, P_0, \dots, P_n, Q_0, \dots, Q_m]$$

engendré par les éléments $(\sum_i A_i P_i) - 1$, $(\sum_j B_j Q_j) - 1$ et les $C_k := \sum_{i+j=l} A_i B_j$, pour $0 \leq k \leq n+m$, est égal à R tout entier, c'est-à-dire contient l'unité 1_R. (On dit aussi que I est l'« idéal unité ».)[①] Soit S le quotient R/I ; on note en bas de casse les images des variables de R dans S. Soient $f := \sum_i a_i T^i \in S[T]$ et $g := \sum_j b_j T^j$. Par construction, on a : $fg = 0$ (car les images des C_l dans S sont nulles) mais f et g sont primitifs par construction (car on a forcé les relations $\sum_i a_i p_i = 1 = \sum_j b_j q_j$). Si $S \neq 0$, chacun des deux polynômes f, g est (non nul et) diviseur de zéro ; d'après le lemme ci-dessous, il existe notamment $s \in S \smallsetminus \{0\}$ tel $sf = 0$. Ceci est impossible car f est primitif et S supposé $\neq 0$. Ainsi, $S = 0$ et I est bien l'idéal unité de R. □

Lemme (McCoy-永田=Nagata)**.** *Soit k un anneau commutatif non nul. Un polynôme $f = a_n T^n + a_{n-1} T^{n-1} + \cdots + a_0 \in k[T]$ non nul est diviseur de zéro si et seulement si il existe $\lambda \neq 0$ dans k tel que $\lambda f = 0$.*

Démonstration. Par hypothèse, il existe $g = b_m T^m + b_{m-1} T^{m-1} + \cdots + b_0$, avec $b_m \neq 0$, tel que $fg = 0$. On veut montrer que l'on peut trouver un tel g *constant* (non nul). Supposons que $f b_m \neq 0$ sans quoi le résultat est acquis. Il existe donc un entier $d \leq n$ tel que $a_d g \neq 0$; considérons le plus grand. Il résulte de l'égalité $fg = (a_d T^d + \cdots + a_0) g = 0$ que $a_d b_m = 0$, c'est-à-dire que le degré du polynôme $h := a_d g$ est strictement inférieur au degré m de g. Comme $fh = f \times (a_d g) = 0$, on peut conclure par récurrence sur m. □

3.3.3. Proposition. *Un polynôme non constant irréductible de $\mathbb{Z}[T]$ est irréductible dans $\mathbb{Q}[T]$.*

Ainsi — à des variations évidentes près sur ce thème —, l'étude de la factorisation de polynômes à coefficients rationnels se ramène à celle des polynômes à coefficients entiers (relatifs).

Démonstration. Supposons qu'il existe une factorisation $f = g_1 g_2$, avec $g_1, g_2 \in \mathbb{Q}[T]$ non constants. Il existe deux rationnels $c_1, c_2 \in \mathbb{Q}_{>0}$ tels que $g_1 = c_1 G_1$, $g_2 = c_2 G_2$ avec $G_1, G_2 \in \mathbb{Z}[T]$, *primitifs*. Puisque $f = (c_1 c_2) G_1 G_2$ et que $G_1 G_2$ est primitif, de même que f, on a nécessairement $c_1 c_2 = 1$ et $f = G_1 G_2$, qui est une factorisation non triviale de f dans $\mathbb{Z}[T]$. C'est absurde. □

① En effet, s'il existe des polynômes $A, B, E_0, \dots, E_{n+m} \in R$ tels que

$$A \cdot \big(1 - \sum_{i=0}^{n} A_i P_i\big) + B \cdot \big(1 - \sum_{j=0}^{m} B_j Q_j\big) + \sum_{l=0}^{n+m} E_l C_l = 1_{\mathbb{Z}},$$

on a $\sum_l E_l(\underline{a}, \underline{b}, \underline{p}, \underline{q}) \cdot c_l = 1_k$. (L'égalité ayant lieu dans l'anneau k des coefficients des polynômes f et g dont on est parti.)

3.4. Bornes explicites sur les coefficients des diviseurs d'un polynôme à coefficients entiers.

Références : [Mignotte et Ştefănescu 1999, chap. 2, 4], [TAOCP 2, 4.6.2], [Cohen 1993, §3.4-5], [Schinzel 2000, §3.6], [Gathen et Gerhard 2003, §6.6, §14-15], [Lecerf 2013, §2, 4].

3.4.1. *Factorisation des polynômes à coefficients entiers : méthode de Kronecker.* Notre objectif dans ces dernières sections est d'expliquer pourquoi il existe des *algorithmes* de factorisation des polynômes à coefficients entiers. Nous allons conjuguer deux approches : une analytique (ou « archimédienne »), qui consiste à plonger $\mathbb{Z}$ dans $\mathbb{R}$ ou $\mathbb{C}$, et une arithmétique, qui consiste à envoyer $\mathbb{Z}$ sur $\mathbb{F}_p$ pour un ou plusieurs nombres premiers p.

Les méthodes qui suivent sont plus efficaces qu'un des premiers algorithmes, généralement attribué à Kronecker (1882) — mais antérieur (Schubert, 1793) ; voir par exemple [Mignotte et Ştefănescu 2001] —, que nous présentons brièvement[①]. Soient $f \in \mathbb{Z}[T]$ de degré d et g un diviseur de f de degré $r \leq d$. Les *entiers* $v_0 := g(0), v_1 := g(1), \ldots, v_r := g(r)$ divisent les entiers (connus) $f(0), f(1), \ldots, f(r)$, que l'on peut supposer tous non nuls quitte à faire un changement de variable $T \mapsto T + a$, $a \in \mathbb{N}$. Le nombre des possibilités pour les v_i est donc fini. Pour chaque $(r+1)$-uplet $v_0, \ldots, v_r$, il existe un unique polynôme g prenant ces valeurs en les $r+1$ premiers entiers ; une formule explicite est donnée par les « polynômes interpolateurs de Lagrange » [拉格朗日插值多项式]. Le polynôme g appartient donc à une liste finie calculable de polynômes ; on vérifie s'il divise bien f en effectuant la division euclidienne (des polynômes vus dans $\mathbb{Q}[T]$).

3.4.2. Soit $f \in \mathbb{Z}[T]$. Il existe une constante $C \in \mathbb{R}$ majorant, en valeur absolue, les coefficients des polynômes g divisant f : ces derniers sont en nombre fini. Si maintenant p est un nombre premier satisfaisant $p > 2C$, un tel polynôme g est déterminé par sa réduction g_p modulo p : c'est l'unique relèvement de g_p dans $\mathbb{Z}[T]$ qui soit à coefficients compris entre $-p/2$ et $p/2$. Ainsi, si l'on connaît une constante C comme ci-dessus, les diviseurs g de f se déduisent des diviseurs de la réduction f_p de f modulo p. Nous allons établir une borne, meilleure que celle donnée par la méthode de Kronecker, due à Landau et Mignotte.

3.4.3. Factorisons $f = a_n T^n + \cdots + a_0$ sous la forme $a_n(T-\alpha_1)(T-\alpha_2)\cdots(T-\alpha_n)$ dans $\mathbb{C}[X]$ et posons :

$$\begin{aligned} \|f\|_1 &:= \textstyle\sum_i |a_i| \\ \|f\|_2 &:= (\textstyle\sum_i |a_i|^2)^{\frac{1}{2}} \\ \|f\|_\infty &:= \max_i |a_i| \\ M(f) &:= |a_n| \textstyle\prod_{i=1}^n \max(1, |\alpha_i|) \end{aligned}$$

① Par contre, nous n'aborderons pas la « méthode LLL » ([A. K. Lenstra, H. W. Lenstra J. et Lovász 1982]) qui est *en théorie* la plus efficace. Voir par exemple [H. W. Lenstra J. 2008, §13] ou [Gathen et Gerhard 2003, §16.2].

Notons que l'on a les majorations triviales $\|f\|_\infty \leq \|f\|_1$ et $\|f\|_\infty \leq \|f\|_2$. De plus, la « mesure de Mahler » M d'un polynôme est multiplicative au sens suivant :

$$M(gh) = M(g)M(h).$$

Proposition (Landau)**.** *Soit $f \in \mathbb{C}[T]$ un polynôme de degré n. Les inégalités suivantes sont satisfaites :*

(i) $\|f\|_1 \leq 2^n M(f)$;
(ii) $M(f) \leq \|f\|_2$.

Démonstration. (i) Soit $r \in [\![0, n]\!]$. On a

$$a_{n-r} = \pm a_n \sum_{I\,:\#I=r} \alpha_J,$$

où $\alpha_I := \prod_{i\in I} \alpha_i$. Par définition, on a $|a_n||\alpha_I| \leq M(f)$. Il en résulte que $|a_r|$ est majoré par $\binom{n}{r} M(f)$ puis $\|f\|_1 = \sum_r |a_r| \leq 2^n M(f)$. (ii) Commençons par observer que pour tout polynôme g et tout $\alpha \in \mathbb{C}$, on a l'égalité $\|(T-\alpha)g\|_2 = \|(\overline{\alpha}T-1)g\|_2$. En effet, si l'on écrit $g = \sum_{i\in\mathbb{Z}} b_i T^i$, on a $(T-\alpha)g = \sum_i (b_{i-1} - \alpha b_i)T^i$ et $(\overline{\alpha}T-1)g = \sum_i (\overline{\alpha}b_{i-1} - b_i)T^i$. On vérifie alors en développant que $\sum_i |b_{i-1} - \alpha b_i|^2 = \sum_i |\overline{\alpha}b_{i-1} - b_i|^2$. Il en résulte que l'on peut supposer que les racines de f sont de module inférieur ou égal à 1 sans changer $\|f\|_2$. Dans ce cas, $M(f) = |a_n| \leq (\sum_i |a_i|^2)^{\frac{1}{2}} = \|f\|_2$. □

Corollaire (Mignotte)**.** *Soit $f \in \mathbb{Z}[T]$ un polynôme et soit g un diviseur de degré d de f dans l'anneau $\mathbb{Z}[T]$. Alors,*

$$\|g\|_\infty \leq 2^d \|f\|_2.$$

Notons que l'on a trivialement $\|f\|_2 \leq \sqrt{n+1}\|f\|_\infty$, où $n = \deg(f)$.

Démonstration. Si $f = gh$, on a $M(f) = M(g)M(h)$ et $M(h) \geq 1$ car le coefficient dominant de h est un entier. Ainsi, $M(g) \leq M(f)$. D'autre part, on a $\|g\|_\infty \leq \|g\|_1$ et $\|g\|_1 \leq 2^d M(g)$. □

• Soit $f = T^8 + T^6 - 3T^4 - 3T^3 + 8T^2 + 2T - 5$. On a $\|f\|_2 \approx 10,6$. Il résulte de la borne précédente que si g est un diviseur de f de degré au plus 4, ses coefficients sont majorés par $2^4 \times 11 = 176$[①]. Modulo $p = 353 > 2 \times 176$, le polynôme f se décompose en produit de facteurs irréductibles sous la forme :

$$f \equiv (T+111)(T-107)(T^6 - 4T^5 - 108T^4 - 127T^3 - 115T^2 + 94T - 113).$$

D'autre part, $(T+111)(T-107) \equiv T^2 - 4T + 125$. Le polynôme g étant uniquement déterminé par sa réduction modulo p, on en déduit que g est l'un des polynômes $T+111$, $T-107$ ou $T^2 - 4T + 125$. Visiblement, aucun de ces polynômes n'est un diviseur de f, qui est donc irréductible.

• Revenons à notre exemple favori : $f = T^5 - T^2 - 1$. On voit que les coefficients d'un diviseur g de f de degré au plus 2 sont majorés par $\lfloor 2^2\sqrt{3} \rfloor = 6$ si bien qu'il suffit de considérer la réduction $f_{13} \in \mathbb{F}_{13}[T]$. La factorisation $f_{13} = (T+6)(T^2 - 4T + 6)(T^2 - 2T - 4)$ montre immédiatement que f est irréductible par exemple parce qu'aucun des termes constants n'est inversible.

① On pourrait améliorer cette borne (cf. p. ex. [TAOCP 2, exercice 4.6.2-20]) et obtenir une majoration par 34, de sorte que $p = 71$ conviendrait.

3.5. Digression : factorisation sans facteur carré et résultant.

Références : [Gathen et Gerhard 2003, 6.2, 14.6], [Apéry et Jouanolou 2006], [Lombardi et Quitté 2011, III.§7], [Gel'fand, Kapranov et Zelevinskiĭ 1994, chap. 12], [Lang 2004, IV.§8].

3.5.1. Soient k un corps et $f \in k[T]$ un polynôme, supposé unitaire pour simplifier. Si $f = \prod_i f_i^{e_i}$ est la décomposition de f en puissances de polynômes irréductibles unitaires distincts, la **partie sans facteur carré** f_2 est le produit $\prod_i f_i$. (Rappelons qu'un polynôme $f \in k[T]$ est dit sans facteur carré s'il n'existe pas de polynôme non constant g tel que g^2 divise f ; c'est le cas de f_2.) Il est visiblement équivalent de savoir factoriser f ou f_2 mais il n'est pas évident *a priori* de calculer f_2. Notons que si $e_i > 1$, le polynôme $f_i^{e_i-1}$ divise à la fois f et sa dérivée f' de sorte que si $u := f \wedge f'$ (le PGCD de f et f'), on a $\dfrac{f}{u} \mid f_2$. On a même égalité, à moins qu'il n'existe un indice i pour lequel $f_i^{e_i}$ divise f' ; compte tenu de l'égalité $f' = \sum_j e_j f_j' \dfrac{f}{f_j}$, cela revient à supposer que f_i divise $e_i f_i'$ ou encore que $e_i f_i' = 0$. Si k est de caractéristique nulle, cette égalité est impossible et on a donc établi que

$$f_2 = \frac{f}{f \wedge f'}.$$

En particulier, il existe sur k de caractéristique nulle un algorithme permettant de factoriser les polynômes si et seulement si il en existe un factorisant les polynômes *sans facteur carré*.

3.5.2. Remarquons que si $k = \mathbb{F}_q$ est un corps fini de caractéristique $p > 0$ (ou plus généralement « parfait »), on peut adapter l'argument précédent de la façon suivante : donné f, on calcule f' et $u = f \wedge f'$. Si $u = f$ (c'est-à-dire $f' = 0$), alors $f = g^p$ pour un $g \in \mathbb{F}_q[T]$: cela résulte de la surjectivité de $\mathrm{Frob}_p : \mathbb{F}_q \to \mathbb{F}_q$. On est alors ramené au problème de factoriser g, dont le calcul est immédiat (donné f). Si $u \neq f$, deux cas se présentent : soit $u = 1$, auquel cas $f = f_2$ et on a effectué la réduction attendue, soit u est non constant et l'on factorise (récursivement) u et f/u. (Notons au passage que si lorsque k est fini, l'argument précédent montre que si f_i est irréductible, on a nécessairement $f_i' \neq 0$.)

3.5.3. Bien que l'algorithme d'Euclide permette de calculer mécaniquement le PGCD de deux polynômes, il est utile d'avoir un critère numérique permettant de détecter si un polynôme a des racines multiples (dans une clôture algébrique de son corps des coefficients) ou, plus généralement, de savoir si deux polynômes f et g sont premiers entre eux.

Fixons quelques notations. Pour tout anneau non nul k, et tout entier $n \geq 0$, on note $k[T]_{\leq n}$ ou $k[T]_{<n+1}$ l'ensemble des polynômes $f \in k[T]$ de degré inférieur ou égal à n, dont $\{1, T, \ldots, T^n\}$ est une base. Donnés deux polynômes

$$f = \sum_{i=0}^{n} a_i T^i \in k[T]_{\leq n} \quad \text{et} \quad g = \sum_{j=0}^{m} b_j T^j \in k[T]_{\leq m},$$

on appelle **résultant** [结式] (de type (m,n)) de f et g, noté $\mathrm{rés}_{n,m}(f,g)$[①], le déterminant de la matrice carrée de taille $n+m$ (dite « **matrice de Sylvester** »)

$$\begin{pmatrix} a_n & a_{n-1} & \cdots & a_0 & & & & \\ & a_n & a_{n-1} & \cdots & a_0 & & & \\ & & \ddots & \ddots & \ddots & \ddots & & \\ & & & \ddots & \ddots & \ddots & & \\ & & & & a_n & a_{n-1} & \cdots & a_0 \\ b_m & b_{m-1} & \cdots & \cdots & b_1 & b_0 & & \\ & b_m & b_{m-1} & \ddots & \ddots & b_1 & b_0 & \\ & & & \ddots & \ddots & \ddots & & \\ & & b_m & b_{m-1} & \cdots & \cdots & b_1 & b_0 \end{pmatrix}$$

dont les m premières lignes sont constituées des coefficients de f et les n suivantes des coefficients de g. C'est le déterminant de l'application k-linéaire

$$\begin{aligned} k[T]_{<m} \times k[T]_n &\to k[T]_{<n+m} \\ (u,v) &\mapsto uf+vg. \end{aligned}$$

Il résulte de la formule « M fois la transposée de sa comatrice est égal à $\det(M)$ fois l'identité » [=formule de Cramer] qu'il existe toujours un couple $(u,v) \in k[T]_{<m} \times k[T]_{<n}$ tel que $uf+vg = \mathrm{rés}_{n,m}(f,g)$. En symboles : $\mathrm{rés}_{n,m}(f,g) \in (f,g) \cap k$, où l'on note (f,g), ou $(f)+(g)$, l'idéal engendré par f et g, c'est-à-dire l'ensemble $\{uf+vg \ : \ u,v \in k[T]\}$. En particulier, si le résultant est inversible, les polynômes sont **fortement étrangers**[②] : on a l'égalité $(f,g) = (1) (= k[T])$, et les polynômes f et g n'ont de racine commune dans aucune k-algèbre (non nulle).

Si f est *unitaire*, des manipulations élémentaires des lignes de la matrice de Sylvester la transforme en une matrice par blocs $\begin{pmatrix} U & \star \\ 0 & G \end{pmatrix}$, où U est une matrice carrée $m \times m$ triangulaire supérieure unipotente [c'est-à-dire avec des 1 sur la diagonale] et les lignes de la matrice G, carrée de taille $n \times n$, sont coefficients des restes de la division de $X^{n-1}g$, $X^{n-2}g$, ..., g par f. Ainsi,

$$(\ddagger) \qquad \mathrm{rés}(f,g) = \det\big(\times g \ : \ k[T]/(f) \to k[T]/(f) \big).$$

Ceci a pour conséquence que, réciproquement, si $(f,g) = (1)$, le résultant est inversible. En effet, si f et g sont fortement étrangers, l'image de g dans l'anneau quotient $k[T]/(f)$ est une unité et la multiplication par g est donc inversible.

Résumons ces observations :

Proposition. *Soient f un polynôme unitaire de degré n et g un polynôme de degré $\leq m$. On a équivalence entre :*

- *le résultant $\mathrm{rés}_{n,m}(f,g)$ est inversible ;*
- *les polynômes f et g sont fortement premiers entre eux.*

---

①. Lorsque $n = \deg(f)$ et $m = \deg(g)$, on note $\mathrm{rés}(f,g)$ pour $\mathrm{rés}_{n,m}(f,g)$.

②. C'est la terminologie de [Bourbaki AC, III, §4].

3.5.4. Le cas particulier où $g = f'$ est particulièrement intéressant. Si f est unitaire (pour simplifier) de degré n, on pose

$$\mathrm{disc}(f) := (-1)^{n(n-1)/2}\,\mathrm{rés}_{n,n-1}(f, f')\,;$$

c'est le **discriminant** [判别式] de f. On peut montrer l'égalité

$$\mathrm{disc}(f) = \prod_{1\le i<j\le n} (x_i - x_j)^2,$$

où $x_1, \ldots, x_n$ sont les racines de f dans $\mathrm{Adu}_k(f)$ telles que $f = \prod_i (T - x_i)$: cela résulte de la formule générale $\mathrm{rés}(\prod_i (T-a_i), g) = \prod_i g(a_i)$, elle-même conséquence de (‡).

Si f est unitaire à coefficients entiers, sans racine multiple (dans $\mathbb{C}$) alors l'*entier* $\mathrm{disc}(f)$ est non nul. Si $p \nmid \mathrm{disc}(f)$, alors la réduction $f_p \in \mathbb{F}_p[T]$ de f modulo p est sans facteur carré.

Formulaire :

$$\begin{aligned}
\mathrm{disc}(T^2 - a_1T + a_2) &= a_1^2 - 4a_2\\
\mathrm{disc}(T^3 - a_1T^2 + a_2T - a_3) &= a_1^2a_2^2 - 4a_1^3a_3 + 18a_1a_2a_3 - 4a_2^3 - 27a_3^2\\
\mathrm{disc}(T^4 - a_1T^3 + a_2T^2 - a_3T + a_4) &= a_1^2a_2^2a_3^2 - 4a_1^3a_3^3 - 4a_1^2a_2^3a_4 + 18a_1^3a_2a_3a_4\\
&\quad -27a_1^4a_4^2 - 4a_2^3a_3^2 + 18a_1a_2a_3^3 + 16a_2^4a_4\\
&\quad -80a_1a_2^2a_3a_4 - 6a_1^2a_3^2a_4 + 144a_1^2a_2a_4^2\\
&\quad -27a_3^4 + 144a_2a_3^2a_4 - 128a_2^2a_4^2\\
&\quad -192a_1a_3a_4^2 + 256a_4^3\\
\mathrm{disc}(T^n + aT + b) &= (-1)^{n-1}(n-1)^{n-1}a^n + n^nb^{n-1}\\
\mathrm{disc}(T^5 + aT + b) &= 4^4a^5 + 5^5b^4.
\end{aligned}$$

3.6. Lemme de Hensel.

Références : [TAOCP 2, 4.6.2 et exercice 4.6.2-22] et [Gathen et Gerhard 2003, 15.4-6] (aspects algorithmiques) ; [Raynaud 1970, chap. IX], [Bourbaki AC, III, §4, n°3 et 5], [Lombardi et Quitté 2011, III.10] (aspects algébriques).

Plutôt que de considérer le polynôme à factoriser sur $\mathbb{Z}$ modulo un grand nombre premier p, on peut le réduire modulo une grande puissance d'un nombre premier p, ce dernier n'étant pas particulièrement grand par rapport aux données du problème. Cette approche est avantageuse car, sous certaines hypothèses qui rappellent le théorème d'inversion locale (ou la méthode de Newton), nous allons voir qu'il existe un lien entre les factorisations modulo p et modulo p^n, $n \ge 1$.

3.6.1. Soient A un anneau et $I \subseteq A$ un idéal. On dit que la paire (A, I) est **hensélienne** [亨泽尔的] si, pour tout polynôme $F \in A[T]$, toute racine simple de $f := F \bmod I \in A/I[T]$ se relève en une racine de F dans A. En symboles : si $\alpha \in A/I$ satisfait $f(\alpha) = 0_{A/I}$ et $f'(\alpha) \in (A/I)^\times$, il existe $a \in A$ tel que $a \mapsto \alpha$ par $A \twoheadrightarrow A/I$ et $F(a) = 0_A$. Dans ce cas tout élément $a \in A$ d'image inversible dans A/I est inversible : appliquer la définition au polynôme $aT - 1_A$. L'équivalence, pour $a \in A$ d'image $\alpha \in A/I$ entre « a inversible » et « α inversible » est classique lorsque l'idéal I est **nilpotent** [幂零] c'est-à-dire tel $I^{N+1} = 0$ pour un entier $N \ge 0$. Une implication est vraie pour tout morphisme d'anneaux $A \to B$; l'autre résulte du fait que pour tout $\varepsilon \in I$, la « perturbation » (=relèvement de $1_{A/I}$) $1_A - \varepsilon$ de l'unité est inversible, d'inverse $1_A + \varepsilon + \varepsilon^2 + \cdots + \varepsilon^N$. Mieux :

3.6.2. Proposition (Newton, ~1670)**.** *Soient A un anneau et $I \subseteq A$ un idéal* nilpotent*, Alors, la paire (A, I) est hensélienne.*

Démonstration. Il faut montrer que si $a \in A$, d'image $\alpha \in A/I$, est tel que $F(a) \in I$ et $F'(a) \in A^\times$, alors il existe $\varepsilon \in I$ tel que $F(a+\varepsilon) = 0$[①]. Notons que remplacer a par $a+\varepsilon$ (pour $\varepsilon \in I$) préserve les conditions $F(a) \in I$ et $F'(a) \in A^\times$ si bien que l'on peut définir une suite de relèvements de α par $a_0 = a$ et $a_{n+1} = a_n^\star$, où l'on pose $a^\star := a - F'(a)^{-1}F(a)$. La formule $F(a+\varepsilon) - F(a) - F'(a)\varepsilon \in \varepsilon^2 A$ montre que si $F(a) \in I^r$, alors $F(a^\star) \in I^{2r}$. Ainsi, $F(a_n) \in I^{2^n}$ pour tout $n \geq 0$ et, en particulier, $F(a_n) = 0$ si $2^n > N$ (de sorte que $I^{2^n} = 0$)[②]. □

3.6.3. Proposition (Hensel)**.** *Soient (A, I) une paire hensélienne, $F \in A[T]$ un polynôme unitaire et $f = gh$ une factorisation de $f := F \bmod I$ en polynômes unitaires* fortement étrangers*. Alors, il existe une unique paire de relèvements unitaires G et H de g et h tels que $F = GH$.*

Pour une démonstration élémentaire (et algorithmique) dans un cas particulier suffisant pour notre propos, voir par exemple [Gathen et Gerhard 2003, 15.10].

Rappelons que les conditions « f et g sont fortement étrangers » (c'est-à-dire $(f)+(g) = (1)$) et « f et g sont de résultant inversible » sont équivalentes. De plus, si A/I est un corps, cela revient à supposer que le PGCD (unitaire) $f \wedge g$ est égal à 1.

3.6.4. Corollaire. *Soit $F \in \mathbb{Z}[T]$ un polynôme unitaire. Soient p un nombre premier, et $(g, h) \in \mathbb{F}_p[T]$ deux polynômes unitaires tels que si l'on note f la classe de F dans $\mathbb{F}_p[T]$ on ait $f = gh$. On suppose* rés$(g, h) \in \mathbb{F}_p$ *non nul. Alors, pour tout entier $e \geq 1$, il existe d'uniques polynômes unitaires G et H dans $\mathbb{Z}/p^e\mathbb{Z}[T]$ se réduisant sur g et h modulo p tels que l'on ait l'égalité $F \bmod p^e = GH$ dans $\mathbb{Z}/p^e\mathbb{Z}[T]$.*

¶*Démonstration de la proposition.* Soient F, g, h comme dans l'énoncé, de degrés respectifs n, d et $n-d$. Notons $\overline{A}$ l'anneau quotient A/I et B (resp. $\underline{B}$) l'algèbre de décomposition universelle du polynôme F sur A (resp. des polynômes g, h), si bien que l'on a des décompositions $F(T) = \prod_{i=1}^{n}(T - X_i)$ dans $B[T]$ et $g(T) = \prod_{i\leq d}(T - x_i)$, $h(T) = \prod_{i>d}(T - x_i)$ dans $\underline{B}[T]$. Il existe un unique morphisme de A-algèbres $\varphi : B \twoheadrightarrow \underline{B}$ envoyant X_i sur x_i : cela résulte du fait que l'image $f = gh$ de F dans $\underline{B}[T]$ est scindée. Rappelons que le groupe $\mathfrak{S}_n$ agit naturellement sur B par permutation des X_i ($i \leq n$) et que, de même, son sous-groupe $\mathfrak{S}_{d,n-d}$ des permutations préservant globalement $\{i : i \leq d\}$ et $\{i : i > d\}$ agit naturellement sur $\underline{B}$. Soient $G_1(T) := \prod_{i\leq d}(T - X_i)$ et $H_1(T) := \prod_{i>d}(T - X_i)$; ce sont des relèvements dans $B[T]$ de g et h, invariants par $\mathfrak{S}_{d,n-d}$, tels que $F = G_1H_1$. Soient Z l'image dans B d'un polynôme invariant par $\mathfrak{S}_{d,n-d}$ et $P(Y)$ le polynôme

① En d'autres termes, si $F(a)$ est petit et $F'(a)$ pas trop petit, il existe une solution de $F = 0$ proche de a. C'est exactement ce qu'affirme la méthode de Newton(-Raphson) : si par exemple f est une fonction réelle deux fois dérivable telle que $\|ff''/f'^2\|_\infty < 1$ alors $x \mapsto x^\star := x - f'(x)^{-1}f(x)$ est contractante si bien que toute suite récurrente $x_{n+1} = x_n^\star$ tend vers un zéro (unique) de f. [Le même type de résultat vaut sur un intervalle borné.]

② On retrouve la « convergence quadratique » bien connue dans le cas réel.

$\prod_{\sigma\in\mathfrak{S}_n/\mathfrak{S}_{d,n-d}}(Y-Z^\sigma)$ à coefficients dans A[①] s'annulant en Z. (Il est de degré $N:=\binom{n}{d}$.) Un calcul immédiat montre que l'on a l'égalité

$$\Big(\sum_{\sigma\in\mathfrak{S}_n/\mathfrak{S}_{d,n-d}}\frac{P(Y)}{Y-Z^\sigma}G_1^\sigma\Big)\cdot\Big(\sum_{\sigma\in\mathfrak{S}_n/\mathfrak{S}_{d,n-d}}\frac{P(Y)}{Y-Z^\sigma}H_1^\sigma\Big)=$$
$$P'(Y)^2F(T)-P(Y)\Big(\sum_{\sigma\neq\tau}\frac{P(Y)}{(Y-Z^\sigma)(Y-Z^\tau)}(F(T)-G_1^\sigma H_1^\tau)\Big)$$

où les trois polynômes G_Y, H_Y et R_Y entre parenthèses appartiennent à $A[Y,T]$. En particulier, si $y\in A$ satisfait $P(y)=0$ et $P'(y)\in A^\times$, on obtient en évaluant en $Y=y$ une factorisation unitaire $F=(P'(y)^{-1}G_y)(P'(y)^{-1}H_y)$ dans $A[T]$. Soit $\widetilde{H}$ un relèvement arbitraire de h dans $A[T]$. Nous allons appliquer ce qui précède à $Z:=\widetilde{H}(X_1)\cdots\widetilde{H}(X_d)\in B$. Comme $h(x_i)=0$ si $i>d$, l'image $p(Y)\in\overline{A}[Y]$ par φ du polynôme $P(Y)$ est $Y^{N-1}(Y-z)$, où l'image z de Z dans $\overline{A}\subseteq\underline{B}$, est égale au produit $h(x_1)\cdots h(x_d)$. Puisque $(g)+(h)=(1)$, pour chaque racine x_i $(i\leq d)$ de g dans $\underline{B}$, on a $h(x_i)\in\underline{B}^\times$, si bien que $z\in\overline{A}^\times$. (On a $\overline{A}\cap\underline{B}^\times=\overline{A}^\times$ car $\overline{A}$ est un facteur direct de $\underline{B}$.) Ainsi, z est une racine simple de $p(Y)$. Par définition, il existe bien une racine y de P relevant z ; la dérivée $P'(y)$ est inversible car d'image inversible dans $\overline{A}$.

Vérifions maintenant l'unicité de G et H. On considère pour cela deux factorisations $F=G_1H_1=G_2H_2$ comme dans l'énoncé. On a $(G_1)+(H_2)=(1)$ car le résultant de ces deux polynômes est inversible. (Il en est ainsi modulo I.) Il existe donc deux polynômes a,b tels que $aG_1+bH_2=1$. En multipliant par H_1 et en utilisant $G_1H_1=G_2H_2$, on obtient : $(aG_2+bH_1)H_2=H_1$. Ainsi, le polynôme unitaire H_2 divise H_1. On a donc égalité $H_1=H_2$ et, de même, $G_1=G_2$. □

3.7. Algorithme de factorisation.

Proposition. *Soit $F\in\mathbb{Z}[T]$ de degré n, supposé unitaire et de discriminant non nul (c'est-à-dire sans facteur carré). On va déterminer la factorisation de F dans $\mathbb{Z}[T]$ en produits de polynômes unitaires irréductibles.*

(1) (↔ Mignotte) On choisit un nombre premier p ne divisant pas $\mathrm{disc}(F)$ *et un entier $e\geq 1$ tels que $p^e>2^{n+1}\|F\|_2$.*

(2) (↔ Berlekamp) On détermine la factorisation unitaire $F_p=f_1\cdots f_r\in\mathbb{F}_p[T]$ de la réduction modulo p de F.

(3) (↔ Hensel) On relève la factorisation précédente en une factorisation unitaire $F_{p^e}=F_{1,e},\ldots,F_{r,e}\in\mathbb{Z}/p^e\mathbb{Z}[T]$ de la réduction modulo p^e de F.

(4) (test des candidats) Pour toute partie $\varnothing\neq R\subsetneq\{1,\ldots,r\}$, on calcule $F_{R,e}:=\prod_{i\in R}F_{i,e}\in\mathbb{Z}/p^e\mathbb{Z}[T]$ et on teste si le représentant unitaire $F_R\in\mathbb{Z}[T]$ de $F_{R,e}$ tel $\|F_R\|_\infty\leq\lfloor\frac{p^e}{2}\rfloor$ divise F.

Si oui, on a déterminé un facteur non trivial de F dans $\mathbb{Z}[T]$ (et si aucun F_S pour S contenu strictement dans R ne vérifie déjà cela, alors F_R est irréductible et on peut continuer à examiner les parties de $\{1,\ldots,r\}$ contenues dans le complémentaire de R pour déterminer les autres facteurs irréductibles). Si aucun polynôme F_R ne fournit un facteur non trivial de F, alors $F\in\mathbb{Z}[T]$ est irréductible.

① On ne prétend pas que $\mathrm{Fix}(\mathfrak{S}_n\circlearrowright B)=A$.

3.8. Astuce de Kronecker et groupe de Galois.

Références : [Schinzel 2000, §1.6] (substitution de Kronecker) ; [Waerden 1937, §61], [Cox 2004, §13.4.A] (groupe de Galois) ; [Frobenius 1896], [Serre 2003], [H. W. Lenstra J. et Stevenhagen 1996] (théorème de Frobenius-Čebotarëv).

3.8.1. *Factorisation des polynômes en plusieurs variables.* On vient de voir qu'il existe un algorithme de factorisation des polynômes en une seule variable à coefficients rationnels. Nous allons voir comment, en principe, ceci permet de factoriser les polynômes (à coefficients rationnels) en plusieurs variables.

Soit $f \in \mathbb{Q}[X_0, \dots, X_n]$. On choisit un entier e strictement supérieur au degré de f dans n'importe laquelle des variables X_i et on calcule (« substitution de Kronecker »)

$$S_e(f) \coloneqq f(T, T^e, T^{e^2}, \dots, T^{e^n}) \in \mathbb{Q}[T].$$

Si f possède un facteur g non-trivial, alors manifestement $S_e(g)$ divise $S_e(f)$. Supposant qu'on sait factoriser le polynôme univarié $S_e(f)$, on peut vérifier pour chacun de ses facteurs s'il est susceptible de s'écrire sous la forme $S_e(g)$ avec g de degré inférieur à e en chaque variable : le polynôme g se retrouve de façon unique en remplaçant chaque monôme $T^{i_0+i_1e+i_2e^2+\cdots+i_ne^n}$ (l'exposant étant écrit en base e) par $X_0^{i_0}\cdots X_n^{i_n}$; on teste alors si g divise f. Si un diviseur de f existe, il sera nécessairement trouvé par cet algorithme.

3.8.2. *Groupe de Galois.* Soient k un corps et $f \in k[T]$ un polynôme séparable de degré d. Fixons un corps de décomposition K de f (unique à isomorphisme non unique près) et $x_1, \dots, x_d$ les racines distinctes de f dans K (uniques à numérotation près). Pour tout sous-groupe $G \leq \mathfrak{S}_d$, posons

$$F_G \coloneqq \prod_{\sigma \in G} \left(X - \sum_i \Lambda_i x_{\sigma(i)}\right) \in K[X, \Lambda_1, \dots, \Lambda_d].$$

Lorsque $G = \mathfrak{S}_d$, ce polynôme (appelé « résolvante de Kronecker ») est en fait à coefficients dans k : cela résulte du théorème sur les fonctions symétriques. Le plus petit sous-groupe G tel que F_G soit à coefficients dans k et *irréductible* (dans $k[X, \Lambda_1, \dots, \Lambda_d]$) est appelé **groupe de Galois** [伽罗瓦群] du polynôme f. Le morphisme (injectif) de restriction $\mathrm{Aut}_k(K) \to \mathfrak{S}_d$, $\sigma \mapsto \sigma_{|\{x_1,\dots,x_d\}}$, induit une bijection entre le groupe des automorphismes k-linéaires de K et le groupe de Galois de f tel que nous l'avons défini.

3.8.3. *Reformulation.* Le groupe de Galois $\mathrm{Gal}(f \,/\, k)$ de f est conjugué au stabilisateur d'un facteur irréductible $h \in k[X, \Lambda_1, \dots, \Lambda_d]$ de la résolvante de Kronecker, où l'action de $\mathfrak{S}_d$ se fait par permutation des (indices des) Λ_i, $i = 1, \dots, d$[①]. Dit ainsi, il est clair (compte tenu des résultats du paragraphe précédent) que, lorsque $k = \mathbb{Q}$, on dispose d'un *algorithme* permettant — en principe — de calculer le groupe de Galois d'un polynôme.

① Plus précisément, c'est le stabilisateur du facteur irréductible s'annulant en $\sum_i \Lambda_i x_i$; les autres facteurs correspondent à une renumérotation des racines, qui a pour effet de donner un sous-groupe conjugué.

Par exemple, lorsque $f = T^3 + T^2 - 2T - 1$, on peut vérifier que

$$\begin{aligned} F_{\mathfrak{S}_3} = \Big(& X^3 - (\Lambda_1 + \Lambda_2 + \Lambda_3)X^2 \\ & + \big(-2(\Lambda_1^2 + \Lambda_2^2 + \Lambda_3^2) + 3(\Lambda_1\Lambda_2 + \Lambda_2\Lambda_3 + \Lambda_3\Lambda_1)\big)X \\ & + \big((\Lambda_1^3 + \Lambda_2^3 + \Lambda_3^3) + 3(\Lambda_1^2\Lambda_2 + \Lambda_2^2\Lambda_3 + \Lambda_3^1\Lambda_1) \\ & \quad -4(\Lambda_1\Lambda_2^2 + \Lambda_2\Lambda_3^2 + \Lambda_3\Lambda_1^2) - \Lambda_1\Lambda_2\Lambda_3\big)\Big) \\ \cdot \Big(& X^3 - (\Lambda_1 + \Lambda_2 + \Lambda_3)X^2 \\ & + \big(-2(\Lambda_1^2 + \Lambda_2^2 + \Lambda_3^2) + 3(\Lambda_1\Lambda_2 + \Lambda_2\Lambda_3 + \Lambda_3\Lambda_1)\big)X \\ & + \big((\Lambda_1^3 + \Lambda_2^3 + \Lambda_3^3) - 4(\Lambda_1^2\Lambda_2 + \Lambda_2^2\Lambda_3 + \Lambda_3^1\Lambda_1) \\ & \quad +3(\Lambda_1\Lambda_2^2 + \Lambda_2\Lambda_3^2 + \Lambda_3\Lambda_1^2) - \Lambda_1\Lambda_2\Lambda_3\big)\Big) \end{aligned}$$

L'existence de cette factorisation prouve que le groupe de Galois de f est contenu dans $\mathbb{Z}/3\mathbb{Z}$ opérant cycliquement sur les racines ; et le fait que ces deux facteurs soient irréductibles est équivalent au fait que le groupe de Galois de f n'est pas strictement plus petit (c'est-à-dire, que f n'est pas scindé). Ainsi, $\mathrm{Gal}(T^3 + T^2 - 2T - 1 \ / \ \mathbb{Q}) = \mathbb{Z}/3\mathbb{Z}$.

3.8.4. *Théorème de spécialisation du groupe de Galois.* D'un point de vue pratique, l'algorithme précédent de calcul du groupe de Galois d'un polynôme à coefficients rationnels est sans intérêt. Par contre, on peut en déduire le fait fondamental suivant, où les corps finis réapparaissent.

Théorème (Dedekind)**.** *Soit $f \in \mathbb{Q}[T]$ un polynôme unitaire à coefficients rationnels de degré d et soit p un nombre premier, ne divisant le dénominateur d'aucun coefficient de f, tel que la réduction $f_p \in \mathbb{F}_p[T]$ de f modulo p soit séparable. Alors le groupe de Galois de f sur $\mathbb{Q}$ contient un élément qui, vu comme élément de $\mathfrak{S}_d$ par son action sur les racines de f (nécessairement distinctes), se décompose comme produit de r cycles de longueurs $(d_1, \ldots, d_r)$, où $d_1, \ldots, d_r$ sont les degrés des facteurs irréductibles (distincts) de f_p.*

Démonstration. Supposons pour simplifier f unitaire à coefficients entiers. Soit A l'algèbre de décomposition universelle de f sur $\mathbb{Z}$, de sorte qu'on a en particulier la décomposition $f = \prod_{i=1}^{d}(T - x_i)$. Il existe deux idéaux premiers $\mathbb{0} \subsetneq \mathbb{p}$ de A au-dessus des idéaux $(0) \subsetneq (p)$ de $\mathbb{Z}$: on a $\mathbb{0} \cap \mathbb{Z} = (0)$ et $\mathbb{p} \cap \mathbb{Z} = (p)$. Posons $h \in A[\Lambda_1, \ldots, \Lambda_d][X]$ le produit $\prod_{\sigma \in G_{\mathbb{0}}}(X - \sigma \cdot c)$, où $c \in A[\Lambda_1, \ldots, \Lambda_d]$ est la combinaison linéaire générique $\Lambda_1 x_1 + \cdots + \Lambda_d x_d$ et $G_{\mathbb{0}}$ est le groupe de Galois de f sur $\mathbb{Q}$, vu comme un sous-groupe de $\mathfrak{S}_d$ agissant par permutation des (indices des) variables $\Lambda_1, \ldots, \Lambda_d$. Si $\mathbb{K} \coloneqq \mathrm{Frac}(A/\mathbb{0})$ et $\mathbb{F} \coloneqq A/\mathbb{p}$ sont les corps de décomposition de f sur $\mathbb{Q}$ et $\mathbb{F}_p$ correspondants aux idéaux choisis, on peut considérer les images $c_{\mathbb{0}}$, $x_{i\mathbb{p}}$, etc. des différents objets sur A déduits des deux morphismes composés $A \twoheadrightarrow A/\mathbb{0} \hookrightarrow \mathbb{K}$ et $A \twoheadrightarrow A/\mathbb{0} \twoheadrightarrow \mathbb{F}$. Le morphisme $A/\mathbb{0} \twoheadrightarrow \mathbb{F}$ induit une bijection $x_{i\mathbb{0}} \mapsto x_{i\mathbb{p}}$ entre les racines de f dans $\mathbb{K}$ et celles de f_p dans $\mathbb{F}$: cela résulte du fait que le polynôme f_p est séparable (c'est-à-dire : les $x_{i\mathbb{p}}$ sont distincts). Ainsi, $A/\mathbb{0}[\Lambda_1, \ldots, \Lambda_d] \twoheadrightarrow \mathbb{F}[\Lambda_1, \ldots, \Lambda_d]$ induit une bijection entre les racines $\sigma \cdot c_{\mathbb{0}}$ de $h_{\mathbb{0}}$ (pour $\sigma \in G_{\mathbb{0}}$) et les racines $\sigma \cdot c_{\mathbb{p}}$ de $h_{\mathbb{p}}$. Puisque $h_{\mathbb{p}}(c_{\mathbb{p}}) = 0$ et $h_{\mathbb{p}} \in \mathbb{F}_p(\Lambda_1, \ldots, \Lambda_d)[X]$, le polynôme minimal de $c_{\mathbb{p}}$ *divise* $h_{\mathbb{p}}$. Comme ses racines sont les $\tau \cdot c_{\mathbb{p}}$ pour τ appartenant au groupe de Galois $G_{\mathbb{p}}$ de f sur $\mathbb{F}_p$, on en

déduit que $G_{\mathbb{p}}$ est un sous-groupe de $G_{\mathbb{0}}$: *le groupe de Galois de f modulo p s'injecte dans le groupe de Galois de f*, de façon compatible aux actions sur les racines $\{x_{1\mathbb{0}}, \ldots, x_{d\mathbb{0}}\}$ et $\{x_{1\mathbb{p}}, \ldots, x_{d\mathbb{p}}\}$. La conclusion résulte alors du fait que si $g \in \mathbb{F}_p[T]$ est un polynôme irréductible de degré e, le groupe de Galois de g est engendré par le morphisme de Frobenius, qui agit par permutation cyclique des e racines. (On applique ceci aux facteurs irréductibles de f_p de degrés respectifs $d_1, \ldots, d_r$.) □

On a montré que pour chaque nombre premier p ne divisant pas le discriminant d'un polynôme unitaire $f \in \mathbb{Z}[T]$, on peut définir une classe de conjugaison φ_p de son groupe de Galois G, obtenue en factorisant f modulo p. Une question naturelle est de savoir si toute classe de conjugaison (dans $\mathfrak{S}_d$) d'un élément $g \in G$ est de ce type. C'est ce qu'affirme un théorème de Frobenius, amélioré par Čebotarëv. Le point clef de la démonstration est le fait suivant de théorie analytique des nombres : si f est irréductible et $n_p(f)$ désigne le nombre de racines de f modulo p alors $\sum_p n_p(f)p^{-s}$ est équivalent à $\log((s-1)^{-1})$ au voisinage de $s = 1^+$[①] : *le nombre moyen de racines modulo p d'un polynôme irréductible est égal à* 1.

① Ce résultat est conséquence du fait que la « fonction zêta du corps (de nombres) $\mathbb{K}$ » a un pôle simple en $s = 1$.

Bibliographie

Sigles

Éléments de mathématique

Bourbaki A — Nicolas Bourbaki (1970-2012). *Éléments de mathématique. Algèbre.* Chap. 1 à 3 (1970), chap. 4 à 7 (1981), chap. 8 (2012), chap. 9 (1959), chap. 10 (1980). Springer-Verlag.

Bourbaki AC — Nicolas Bourbaki (1968-1998). *Éléments de mathématique. Algèbre.* Chap. 1 à 4 (1968), chap. 5 à 7 (1975), chap. 8 et 9 (1983), chap. 10 (1998). Springer-Verlag.

The art of computer programming

TAOCP 1 — Donald E. Knuth (1997). *The art of computer programming. Vol. 1. Fundamental algorithms.* 3e éd. Addison-Wesley, xx+650 pages.

TAOCP 2 — Donald E. Knuth (1998a). *The art of computer programming. Vol. 2. Seminumerical algorithms.* 3e éd. Addison-Wesley, xiv+762 pages.

TAOCP 3 — Donald E. Knuth (1998b). *The art of computer programming. Vol. 3. Sorting and searching.* 2e éd. Addison-Wesley, xiv+780 pages.

TAOCP 4A — Donald E. Knuth (2011). *The art of computer programming. Vol. 4A. Combinatorial algorithms, part 1.* Addison-Wesley, xvi+883 pages.

Séminaires de géométrie algébrique

SGA 4 — Alexander Grothendieck, Michael Artin et Jean-Louis Verdier (1972—1973). *Théorie des topos et cohomologie étale des schémas. Séminaire de géométrie algébrique du Bois-Marie, 1963—1964.* Lecture Notes in Mathematics **269, 270, 305**. Springer-Verlag. ☞.

Sommes trig. — Pierre Deligne (p. d.). « Applications de la formule des traces aux sommes trigonométriques ».

SGA 5 — Alexander Grothendieck (1977). *Cohomologie ℓ-adique et fonctions L. Séminaire de géometrie algébrique du Bois-Marie, 1965—1966.* Lecture Notes in Mathematics **589**. Springer-Verlag, xii+484 pages.

. ↑ p. … = cité page(s) …

☞ : librement accessible en ligne

Autres références

Apéry, François et Jean-Pierre Jouanolou (2006). *Résultant et sous-résultants. Le cas d'une variable*. Hermann, x+477 pages.

Cartan, Henri (1961). *Théorie élémentaire des fonctions analytiques d'une ou plusieurs variables complexes*. Hermann, 232 pages.

Chevalley, Claude (1935). « Démonstration d'une hypothèse de M. Artin ». *Abh. Math. Sem. Univ. Hamburg* **11**.(1), 73-75.

Cohen, Henri (1993). *A course in computational algebraic number theory*. Graduate Texts in Mathematics **138**. Springer-Verlag, xii+534 pages.

Conway, John Horton (2001). *On numbers and games*. 2e éd. A K Peters, xii+242 pages.

Cox, David A. (2004). *Galois theory*. John Wiley & Sons, xx+559 pages.

Davenport, Harold (2000). *Multiplicative number theory*. 3e éd. Graduate Texts in Mathematics **74**. Springer-Verlag, xiv+177 pages.

Deligne, Pierre (1974). « La conjecture de Weil. I ». *Publications mathématiques de l'IHÉS* **43**, 273-307. ☞.

– (1980). « La conjecture de Weil. II ». *Publications mathématiques de l'IHÉS* **52**, 137-252.

Diaconis, Persi et Ron Graham (2012). *Magical mathematics*. The mathematical ideas that animate great magic tricks. Princeton University Press, xiv+244 pages.

Eisenbud, David (2015). « The Amazing Heptadecagon ». Youtube 87uo2TPrsl8.

Flajolet, Philippe et Robert Sedgewick (2009). *Analytic combinatorics*. Cambridge University Press, xiv+810 pages. ☞.

Frobenius, Ferdinand Georg (1896). « Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe ». *Sitz. Akad. Wiss. Berlin.* (= Ges. Abh., II, 719–733), 689-703.

Gathen, Joachim von zur et Jürgen Gerhard (2003). *Modern computer algebra*. 2e éd. Cambridge University Press, xiv+785 pages.

Gauß, Carl Friedrich (1807). *Recherches arithmétiques (*Disquisitiones arithmeticae*)*. Traduit du latin par A.-C.M. Poullet-Delisle. Réédité chez Jacques Gabay et disponible sur gallica.bnf.fr.

– (2005). *Mathematisches Tagebuch, 1796—1814*. 5e éd. Ostwalds Klassiker der Exakten Wissenschaften. Bilingue latin-allemand (avec commentaires en allemand). Verlag Harri Deutsch, 235 pages.

Gel'fand, Israel M., Mikhail M. Kapranov et Andrei V. Zelevinskiĭ (1994). *Discriminants, resultants, and multidimensional determinants*. Birkhäuser, x+523 pages.

Grothendieck, Alexander (1964). « Formule de Lefschetz et rationalité des fonctions L ». *Séminaire Bourbaki*, exp. nº 279, 41-55. ☞.

Hardy, Godfrey Harold et Edward Maitland Wright (1979). *An introduction to the theory of numbers*. 5e éd. Oxford University Press, xvi+426 pages.

– (2007). *Introduction à la théorie des nombres*. Traduction française de [Hardy et Wright 1979] par François Sauvageot. Vuibert & Springer, xxxviii+569 pages.

Hiramatu, Toyokazu [平松豊一] (1998). 数論を学ぶ人のための相互法則入門 *[Introduction aux lois de réciprocités supérieures…]* 牧野書店 [Makino-shoten].

Ireland, Kenneth et Michael Rosen (1990). *A classical introduction to modern number theory*. Graduate Texts in Mathematics **84**. Springer-Verlag, xiv+389 pages.

Jacobson, Nathan (1985). *Basic algebra. I.* 2e éd. W. H. Freeman and Company, xviii+499 pages.
Kato, Kazuya [加藤和也] (2009). 類体論と非可換類体論. 1 *[Théorie du corps de classes et théorie non commutative du corps de classes. 1]*. 岩波書店 [Iwanami-shoten].
Katz, Nicholas M. et Peter Sarnak (1999). *Random matrices, Frobenius eigenvalues, and monodromy*. American Mathematical Society Colloquium Publications **45**. American Mathematical Society, xii+419 pages.
Lang, Serge (2004). *Algèbre. Cours et exercices*. Traduction française de [**Algebra//Lang**]. Dunod, 944 pages.
Lebesgue, Henri (1950). *Leçons sur les constructions géométriques*. Gauthier-Villars, vi+304 pages.
Lecerf, Grégoire (2013). « Factorisation des polynômes à plusieurs variables ». *Les cours du CIRM* **3**.(1), 1-85.
Lenstra, A. K., H. W. Lenstra Jr. et L. Lovász (1982). « Factoring polynomials with rational coefficients ». *Math. Ann.* **261**.(4), 515-534.
Lenstra Jr., H. W. (1978). « Nim multiplication ». *Séminaire de théorie des nombres, Talence 1977–1978*, exp. nº 11.
– (2008). « Lattices ». Dans [**Surveys//Buhler-Stevenhagen**], 127-181.
Lenstra Jr., H. W. et P. Stevenhagen (1996). « Chebotarëv and his density theorem ». *Math. Intelligencer* **18**.(2), 26-37.
Lidl, Rudolf et Harald Niederreiter (1997). *Finite fields*. 2e éd. Encyclopedia of Mathematics and its Applications **20**. Cambridge University Press, xiv+755 pages.
Lombardi, Henri et Claude Quitté (2011). *Algèbre commutative (Méthodes constructives)*. Mathématiques en devenir. Calvage & Mounet, xxxi+991 pages.
Madore, David A. (15 juil. 2015a). *Le jeu de cartes Dobble et la géométrie projective expliquée aux enfants*. Blog. ☞.
– (27 juil. 2015b). *Comment faire un jeu de* Tribble. Blog. ☞.
Mignotte, Maurice et Doru Ştefănescu (1999). *Polynomials. An algorithmic approach*. Springer-Verlag, xii+306 pages.
– (2001). « La première méthode générale de factorisation des polynômes. Autour d'un mémoire de F.T. Schubert ». *Rev. histoire math.* **7**.(1), 67-89.
Pohst, Michael et Hans Zassenhaus (1989). *Algorithmic algebraic number theory*. Encyclopedia of Mathematics and its Applications **30**. Cambridge University Press, xiv+465 pages.
Raynaud, Michel (1970). *Anneaux locaux hensséliens*. Lecture Notes in Mathematics, Vol. 169. Springer-Verlag, v+129 pages.
Rosen, Michael (2002). *Number theory in function fields*. Graduate Texts in Mathematics **210**. Springer-Verlag, xii+358 pages.
Schinzel, Andrzej (2000). *Polynomials with special regard to reducibility*. Encyclopedia of Mathematics and its Applications **77**. Cambridge University Press, x+558 pages.
Serre, Jean-Pierre (1977). *Cours d'arithmétique*. 2e éd. Presses universitaires de France, 188 pages.
– (1992). *Topics in Galois theory*. **1**. Research Notes in Mathematics. Jones et Bartlett Publishers, xvi+117 pages.
– (2003). « On a theorem of Jordan ». *Bull. Amer. Math. Soc.* **40**.(4), 429-440.
Shoup, Victor (2009). *A computational introduction to number theory and algebra*. 2e éd. (Sous licence CC BY-NC-ND). Cambridge University Press, xviii+580 pages. ☞.

Siegel, Aaron N. (2013). *Combinatorial game theory*. Graduate Studies in Mathematics **146**. American Mathematical Society, xiv+523 pages.

Stanley, Richard P. (1999). *Enumerative combinatorics. Vol. 2*. Cambridge Studies in Advanced Mathematics **62**. Cambridge University Press, xii+581 pages.

– (2012). *Enumerative combinatorics. Vol. 1*. 2e éd. Cambridge Studies in Advanced Mathematics **49**. Cambridge University Press, xiv+626 pages.

Tao, Terence (2014). « Algebraic combinatorial geometry : the polynomial method in arithmetic combinatorics, incidence combinatorics, and number theory ». *EMS Surv. Math. Sci.* **1**.(1), 1-46. ☞.

– (2015). *Cycles of a random permutation, and irreducible factors of a random polynomial*. blog. ☞.

Terras, Audrey (1999). *Fourier analysis on finite groups and applications*. London Mathematical Society Student Texts **43**. Cambridge University Press, x+442 pages.

Waerden, Bartel Leendert van der (1937). *Moderne Algebra. Erster Teil*. 2e éd. Springer-Verlag, x+272 pages.

Weil, André (1949). « Numbers of solutions of equations in finite fields (Œuvres [1949b]) ». *Bull. Amer. Math. Soc.* **55**, 497-508.

– (1974). « La cyclotomie jadis et naguère ». *Séminaire Bourbaki*, exp. no 452. ☞.

Exercices

Exercice 1.

(i) Trouver le plus petit nombre premier p tel que $\sum_{i=0}^{22} T^i$ soit irréductible dans $\mathbb{F}_p[T]$.

(ii) Trouver les dix plus petits nombres premiers p tels que $\sum_{i=0}^{p-1} T^i$ soit irréductible dans $\mathbb{F}_2[T]$.

□(i) $p = 5$. La question revient à déterminer le plus petit p tel que le polynôme cyclotomique $\Phi_{23} = (T^{23} - 1)/(T - 1)$ soit irréductible sur $\mathbb{F}_p$. D'après **1.5.5**, on veut donc que p soit un générateur de $(\mathbb{Z}/23\mathbb{Z})^\times$. Pour $p = 2$, les puissances sont $1, 2, 8, 16, 32, 64, 128, 256 = 3, 6, 12, 24 = 1$; pour $p = 3$, on a $1, 3, 27 = 4, 12, 36 = 13, 39 = 16, 48 = 2, 6, 18 = -5, -15 = 8, 24 = 1$. Dans ces deux cas, l'ordre n'est pas 22. Par contre, c'est le cas si $p = 5$.

(ii) $p = 2, 3, 5, 11, 13, 19, 29, 37, 53, 59, \ldots$ On se demande maintenant pour quels p le polynôme Φ_p est irréductible sur $\mathbb{F}_2$, c'est-à-dire quand 2 est primitif dans $(\mathbb{Z}/p\mathbb{Z})^\times$. On vérifie à la main que $p = 3, 5$ conviennent mais pas 7 (car $2^3 = 1$), ni 17 (car $2^4 = -1$). On trouve par des calculs semblables les valeurs ci-dessus.

Remarque : on a vu dans le cours que si $p = 4\ell + 1$ avec ℓ premier, alors 2 est primitif et que cela s'applique en particulier à $p = 13, 29$ et 53.□

Exercice 2. Montrer, ou expliquer comment montrer, que $T^5 - T + 1$ est un polynôme primitif sur $\mathbb{F}_3$, c'est-à-dire un polynôme irréductible dont chaque racine est un générateur du groupe multiplicatif $\mathbb{F}_{3^5}^\times$.

□On peut montrer que ce polynôme est irréductible en constatant qu'il est premier à $T^3 - T$ et $T^9 - T$. (On vérifie par exemple que les équations $\alpha^5 = \alpha - 1$ et $\alpha^3 = \alpha$ [resp. $\alpha^9 = \alpha$] sont incompatibles.) Pour montrer qu'il est primitif, il faut montrer que toute racine α est un générateur de $\mathbb{F}_{3^5}^\times = \mathbb{F}_{243}^\times$, cyclique de cardinal $242 = 2 \cdot 11^2$. Il n'est pas difficile de vérifier à la main que $\alpha^{22} \neq 1$: on a $\alpha^{15} = \alpha^3 - 1$ (Frobenius) donc $\alpha^{22} = (\alpha^3 - 1)(\alpha^7 = \alpha^3 - \alpha^2)$, etc. Montrer que $\alpha^{121} \neq 1$ ou, de façon équivalente, $\alpha^{121} = -1$ est plus fastidieux. On peut faire la division euclidienne de T^{121} par $T^5 - T + 1$, probablement avec un ordinateur si on n'a pas la patience de faire le calcul[①].

Remarques :

(i) Le polynôme $T^5 - T + 1$ est un *polynôme de Conway* : il est minimal et bien adapté aux calculs en un certain sens que l'on ne précise pas ici.

(ii) On insiste sur le fait qu'un polynôme irréductible n'est pas nécessairement primitif : environ $\frac{1}{5}$-ième [plus exactement $\frac{1}{5}(1-3^{-4})$ des polynômes unitaires de degré 5 sur $\mathbb{F}_3$ sont irréductibles mais la proportion des primitifs est environ moitié moindre [plus exactement : $\frac{1}{5} \times \varphi(2 \times 11^2)/3^5 = \frac{1}{5} \times \frac{11 \times 10}{243}$].

□

① Sur $\mathbb{Z}$, on trouve $-16269333T^4 + 18952107T^3 - 22128873T^2 + 25880583T - 13951852$, qui se réduit bien modulo $2 = -1$ sur $\mathbb{F}_3$.

Exercice 3. Pour $\mathbb{F} = \mathbb{F}_4, \mathbb{F}_8, \mathbb{F}_{27}$ ou $\mathbb{F}_{25}$, trouver un polynôme irréductible dans $\mathbb{F}_p[T]$ (où $p := \text{car.}(\mathbb{F})$) dont une racine α est primitive et écrire les puissances de α comme un polynôme en α de degré minimal.

□$\mathbb{F}_4 : T^2 + T + 1$; α, $\alpha^2 = \alpha + 1$, $\alpha^3 = 1$. (Remarque : il n'y a qu'un polynôme irréductible de degré 2.)

$\mathbb{F}_8 : T^3 + T + 1$; α, α^2, $\alpha^3 = \alpha + 1$, $\alpha^2 + \alpha$, $\alpha^2 + \alpha + 1$, $\alpha^2 + 1$, 1. (Remarque : il n'y a que $2 = \frac{1}{3}(2^3 - 2)$ polynômes irréductibles [unitaires] de degré 3.)

$\mathbb{F}_{27} : T^3 - T + 1$; α, α^2, $\alpha - 1$, $\alpha^2 - \alpha$, $-\alpha^2 + \alpha - 1$, $\alpha^2 + \alpha + 1$, $\alpha^2 - \alpha - 1$, $-\alpha^2 - 1$, $\alpha + 1$, $\alpha^2 + \alpha$, $\alpha^2 + \alpha - 1$, $\alpha^2 - 1$, $\alpha^{13} = -1$, $-\alpha$, $-\alpha^2$, $-\alpha + 1$, $-\alpha^2 + \alpha$, $\alpha^2 - \alpha + 1$, $-\alpha^2 - \alpha - 1$ $-\alpha^2 + \alpha + 1$, $\alpha^2 + 1$, $-\alpha - 1$, $-\alpha^2 - \alpha$, $-\alpha^2 - \alpha + 1$, $-\alpha^2 + 1$, $\alpha^{26} = 1$

$\mathbb{F}_{25} : T^2 - T + 2$; α, $\alpha + 3$, $-\alpha + 3$, $2\alpha + 2$, $-\alpha + 1$, 2, 2α, $2\alpha + 1$, $3\alpha + 1$, $-\alpha - 1$, $3\alpha + 2$, $\alpha^{12} = -1$, $-\alpha$, $-\alpha + 2$, $\alpha + 2$, $3\alpha + 3$, $\alpha - 1$, 3, 3α, $3\alpha - 1$, $2\alpha - 1$, $\alpha + 1$, $2\alpha + 3$, $\alpha^{24} = 1$

□

Exercice 4. Soit $\mathbb{F}_{q^n} / \mathbb{F}_q$ une extension de degré $n \geq 1$. Montrer en comptant le nombre d'éléments de $\mathbb{F}_{q^n}$ de degré $< n$ sur $\mathbb{F}_q$ qu'il existe au moins un polynôme $f \in \mathbb{F}_q[T]$ irréductible degré n.

□Il s'agit essentiellement de l'argument donné en **1.5.6** pour minorer la proportion de polynômes irréductibles. Le nombre d'éléments de $\mathbb{F}_{q^n}$ de degré $< n$ est majoré par la somme des cardinaux des $\mathbb{F}_{q^d}$ pour $d|n$. Au moins deux arguments possibles. (1) On remarque que $\sum_{d|n, d\neq n} q^d \leq \sum_{d<n} q^d < q^n$, par exemple par unicité de l'écriture en base q. (2) On remarque que chaque q^d est majoré par $\leq q^{n/2}$ et leur nombre est $\leq n$, par conséquent cette somme de cardinaux est inférieure ou égale à $nq^{n/2}$. Pour avoir la conclusion souhaitée, il suffit d'avoir $q^n > nq^{n/2}$, soit $q^{n/2} > n$, ce qui se produit dès que $2^n > n^2$, donc dès que $n > 4$. Pour les valeurs plus petites de n, on constate que $q^4 > q^2 + q$ et $q^3 > q$ et $q^2 > q$ (et $q > 0$...) pour tout $q \geq 2$.□

Exercice 5.

(i) Vérifier les factorisations dans $\mathbb{C}[T]$

$$T^4+1 = (T^2+i)(T^2-i) = (T^2-\sqrt{2}T+1)(T^2+\sqrt{2}T+1) = (T^2+i\sqrt{2}T-1)(T^2-i\sqrt{2}-1).$$

(ii) En déduire que $T^4 + 1$ est irréductible dans $\mathbb{Q}[X]$.

(iii) Montrer que T^4+1 est réductible dans $\mathbb{F}_p[X]$ pour tout nombre premier p.

(Indication : on rappelle que l'ensemble des carrés de $\mathbb{F}_p^\times$ est un sous-groupe d'indice 2 de sorte que si $a, b \in \mathbb{F}_p$, alors a, b ou ab est un carré dans $\mathbb{F}_p$.)

□(i) On a la factorisation de $\Phi_8 = T^4+1$ en $\prod_\zeta (T-\zeta)$ où ζ parcourt les 4 racines primitives 8-ièmes de l'unité. Suivant que l'on regroupe les racines par paquets de deux diamétralement opposées, conjuguée l'une de l'autre, ou symétriques par rapport à l'axe imaginaire on obtient les factorisations ci-dessus.

(ii) Puisque qu'aucun de ces polynômes n'est à coefficients rationnels et que Φ_8 n'a visiblement pas de racine dans $\mathbb{Q}$ (ni dans $\mathbb{R}$), il est bien irréductible.

(iii) Pour $p = 2$, c'est clair. Si $p \neq 2$, on remarque (cf. indication) que l'un au moins des trois éléments $-1, 2, -2$ est le carré d'un élément dans $\mathbb{F}_p$, que l'on note i, $\sqrt{2}$ ou $\sqrt{2}i$. Il en résulte que l'une des trois factorisations ci-dessus est à coefficients dans $\mathbb{F}_p$.□

Exercice 6. Soit p un nombre premier de Fermat différent de 5. Montrer que 5 est primitif dans $\mathbb{F}_p^\times$. (*Indication : on pourra observer que tout élément qui n'est pas un carré est primitif.*)

Exercice 7. ¶Montrer que $T^{4n} + T^n + 1$ est irréductible sur $\mathbb{F}_2$ si et seulement si $n = 3^r 5^s$ pour des entiers $r, s \geq 0$.

□Soit β une racine de $T^4 + T + 1$ dans $\mathbb{F}_{16}$. C'est une racine primitive 15-ième de l'unité. Une racine α du polynôme est une racine n-ième de β. (Notons que n est nécessairement impair sinon le polynôme est un carré.) C'est une racine primitive $15n$-ième de l'unité. L'élément α est de degré $4n$ sur $\mathbb{F}_2$ si et seulement si l'ordre de 2 dans $(\mathbb{Z}/15n\mathbb{Z})^\times$ est égal à $4n$. Notons que $\varphi(15n) = 8n \times \prod(1 - p^{-1})$, où $p|n$, $p \neq 3, 5$. Il est nécessaire que $4n|\varphi(15n)$, ce qui se produit si et seulement si $2\prod(1-p^{-1})$ est un entier, c'est-à-dire que seuls 3 et 5 divisent n. Réciproquement, si $n = 3^r 5^s$, (la classe de) 2 est générateur de $(\mathbb{Z}/3^{r+1}\mathbb{Z})^\times$ et de $(\mathbb{Z}/5^{s+1}\mathbb{Z})^\times$ (car il l'est modulo 3 et 5) donc son ordre est le ppcm de $\varphi(3^{r+1})$ et $\varphi(5^{s+1})$, soit $4n$.□

Exercice 8. Montrer, sans utiliser la formule de Gauß (§**1.5.6**), que le nombre de polynômes irréductibles unitaires de $\mathbb{F}_p[X]$ de degré ≤ 3 est $\frac{1}{3}p^3 + \frac{1}{2}p^2 + \frac{1}{6}p$.

□Il y a p polynômes unitaires de degré 1, $p^2 - \left(\binom{p}{2} + p\right) = \binom{p}{2}$ unitaires irréductibles de degré 2 et $p^3 - \left(\binom{p}{2} \times p + \binom{p}{3} + p(p-1) + p\right) = \frac{1}{3}(p^3 - p)$ de degré 3.□

Exercice 9. Détailler les démonstrations des faits suivants, énoncés en **1.5**.

- **(i)** Un sous-groupe fini G du groupe multiplicatif d'un corps K est cyclique.
- **(ii)** $g(d) = \sum_{a|d} f(a)$ pour tout $d > 0$ si et seulement si $f(d) = \sum_{a|d} \mu\left(\frac{d}{a}\right) g(a)$ pour tout $d > 0$.
- **(iii)** Si $q = p^d$, le polynôme $T^q - T$ est le produit des polynômes $P \in \mathbb{F}_p[T]$ irréductibles unitaires de degré divisant d.

Exercice 10. Soit $A = \mathbb{Z}[\zeta_n \,:\, n \geq 1]$ le sous-anneau de $\mathbb{C}$ engendré par les racines de l'unité $\zeta_n := \exp(2\pi i/n)$.

- **(i)** Montrer que pour tout nombre premier p, on a $pA \subsetneq A$.
  (*Indication : on pourra observer que si a et n sont des entiers ≥ 1, le rationnel $1/a$ n'appartient pas à $\mathbb{Z}[\zeta_n]$.*)
- **(ii)** Soit $\mathfrak{p}$ un idéal maximal de A contenant p. Montrer que $A/\mathfrak{p}$ est une clôture algébrique de $\mathbb{F}_p$.

Exercice 11. On fixe une clôture algébrique Ω de $\mathbb{F}_p$.

- **(i)** Rappeler pourquoi $\mathbb{F}_p = \{x \in \Omega \,:\, \mathrm{Frob}_p(x) = x\}$.
- **(ii)** (p impair) Montrer qu'il existe $\zeta \in \Omega$ tel que $\zeta^2 = -1$. En déduire que -1 est un carré dans $\mathbb{F}_p$ si et seulement si $p \equiv 1 \bmod 4$.

(iii) (p impair) Montrer qu'il existe $\zeta \in \Omega$ tel que $\zeta^4 = -1$. En considérant l'élément $\zeta + \zeta^{-1}$, montrer que 2 est un carré dans $\mathbb{F}_p$ si et seulement si $p \equiv \pm 1 \bmod 8$ [①].

□Dans un cas comme dans l'autre, l'existence de ζ vient du fait que Ω est algébriquement clos et il s'agit de savoir si « $\sqrt{-1}$ » $= \zeta$ ou « $\sqrt{2}$ » $= \zeta + \zeta^{-1}$ — car $(\zeta+\zeta^{-1})^2 = 2+\zeta^2+\zeta^{-2} = 2$ — appartient à $\mathbb{F}_p$, c'est-à-dire est fixe par Frobenius. Dans le second cas par exemple, on a $\mathrm{Frob}_p(\zeta + \zeta^{-1}) = \zeta^p + \zeta^{-p}$, qui ne dépend que de $\pm p$ modulo 8. On vérifie immédiatement que $\zeta + \zeta^{-1} \neq \zeta^3 + \zeta^{-3}$.□

Exercice 12. Montrer que si p est premier et $a \in \mathbb{F}_p^\times$, alors $T^p - T + a$ est irréductible dans $\mathbb{F}_p[T]$.

(*Indication : on pourra utiliser les résultats du paragraphe* ***1.5.4****.*)

□D'après ce critère, il s'agit de montrer que l'orbite d'une racine α sous le Frobenius Frob_p est de cardinal exactement p. Or, par construction, $\mathrm{Frob}_p(\alpha) := \alpha^p$ est égal à $\alpha + (-a)$, un translaté de α par un élément non nul. Son orbite est donc bien de cardinal p.□

Exercice 13.

(i) Soient p un nombre premier et $n \geq 1$ un entier. Montrer qu'une matrice $A \in M_2(\mathbb{Z}/p^n\mathbb{Z})$ est inversible si et seulement si son image dans $M_2(\mathbb{F}_p)$ est inversible.

(ii) Calculer le cardinal de ce groupe $\mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$ en fonction de p et n.

(iii) Peut-on en déduire un calcul de $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ pour $N \geq 1$?

Exercice 14. Soit $P \in \mathbb{F}_p[X]$ un polynôme de degré d.

(i) Montrer que P est irréductible dans $\mathbb{F}_p[X]$ si et seulement si P n'a pas de racine dans $\mathbb{F}_{p^r}$ pour tout $r \leq \frac{d}{2}$.

(ii) (Application) Montrer que $\mathbb{F}_4 = \{0, 1, j, j^2\}$ avec $j^2 = 1 + j$. En déduire que les polynômes $1 + X^2 + X^5$, $1 + X^3 + X^5$, $1 + X + X^2 + X^3 + X^5$, $1 + X + X^2 + X^4 + X^5$, $1 + X + X^3 + X^4 + X^5$ et $1 + X^2 + X^3 + X^4 + X^5$ sont les polynômes irréductibles de degré 5 de $\mathbb{F}_2[X]$.

(iii) (Une variante) Supposons $d \leq 5$. Montrer que P est irréductible dans $\mathbb{F}_p[X]$ si et seulement si $(P, X^{p^2} - X) = 1$.

□(i) P est irréductible si et seulement si il n'a pas de factorisation $P = gh$ avec $\deg(g), \deg(h) > 0$ ou encore — puisque $a + b = d$ entraîne $\min\{a, b\} \leq d/2$ — s'il n'existe pas de polynôme g non constant de degré $r \leq d/2$ tel que $g | P$. Or, un tel g a une racine dans $\mathbb{F}_{p^r}$ et, réciproquement, si $\alpha \in \mathbb{F}_{p^r}$ est une racine de P, son polynôme minimal (sur $\mathbb{F}_p$) divise P — car $P(\alpha) = 0$ — et est de degré $\leq r$.

① L'étude des nombres premiers p pour lesquels 2 est un *cube* est plus délicate et s'insère naturellement dans la « théorie non abélienne du corps de classes » (ou « programme de Langlands »). On démontre ([平松 1998, §3.2], [加藤 2009, exemple 3.1]) que le nombre de solutions dans $\mathbb{F}_p$ de l'équation $x^3 = 2$ est $1 + a_p$, où les a_n sont les coefficients de la série formelle

$$x \prod_{n=1}^{\infty} \left((1 - x^{6n})(1 - x^{18n})\right) = \sum_{n=1}^{\infty} a_n x^n.$$

(ii) Le polynôme $T^2+T+1 \in \mathbb{F}_2[T]$ est irréductible, par exemple parce qu'il n'a pas de racine dans $\mathbb{F}_2$ ou, de façon un peu pédante, d'après l'exercice 12 ci-dessus. Le quotient $\mathbb{F}_2[T]/(T^2+T+1)$ est donc un corps de cardinal 4 et la classe j de T est bien comme annoncé. D'après le critère précédent, pour vérifier que les polynômes de degré 5 de l'énoncé sont irréductibles, il faut vérifier qu'ils n'ont pas de racine dans $\mathbb{F}_2$ — ce qui résulte du fait que leur terme constant est non nul et qu'ils ont un nombre impair de monômes — ni dans $\mathbb{F}_4$. (On utilise le fait que $\lfloor 5/2 \rfloor = 2$.) On vérifie par le calcul que pour chacun de ces polynômes f, on a $f(j) \neq 0$. Comme $f(j^2) = f(j)^2$, on a aussi $f(j^2) \neq 0$ sans avoir besoin de refaire le calcul. L'exercice demande de vérifier que ces polynômes sont les seuls qui soient irréductibles de degré 5. Il résulte de la formule de Gauß (§ **1.5.6**) qu'il y en a $\frac{1}{5}(2^5-5) = 6$. On les a donc tous trouvés. Plus simplement, on peut faire une liste des autres polynômes et vérifier qu'ils ont une racine dans $\mathbb{F}_2$ ou $\mathbb{F}_4$. (Ici $\mathbb{F}_2 \subseteq \mathbb{F}_4$ donc il s'agit en fait de chercher des racines dans $\mathbb{F}_4$ mais on rappelle qu'en général l'inégalité $a \leq b$ n'entraîne *pas* l'existence d'un plongement $\mathbb{F}_{p^a} \subseteq \mathbb{F}_{p^b}$.)□

Exercice 15. Montrer que $T^6+T^4+T+1 \in \mathbb{F}_2[T]$ est le produit de trois polynômes irréductibles distincts.

□Si ce polynôme est réductible, il a un facteur irréductible de degré 1, 2 ou 3, c'est-à-dire une racine dans $\mathbb{F}_2$, $\mathbb{F}_4 \smallsetminus \mathbb{F}_2$ ou $\mathbb{F}_8 \smallsetminus \mathbb{F}_2$. Il y a deux polynômes unitaires irréductible de degré 1 T et $T+1$ —, et un polynôme unitaire irréductible de degré 2 : T^2+T+1. On trouve donc immédiatement que T^6+T^4+T+1 est divisible par $(T+1)(T^2+T+1)$. Le quotient, T^3+T+1 — calculé par exemple par division euclidienne —, est irréductible (par exemple car il n'a pas de racine dans $\mathbb{F}_2$). La décomposition en facteurs irréductibles est donc

$$T^6+T^4+T+1 = (T+1)(T^2+T+1)(T^3+T+1).$$

□

Exercice 16. Soit p un nombre premier fixé. Quelle est la probabilité qu'un polynôme unitaire $f \in \mathbb{F}_p[T]$ de degré d soit un produit de polynômes irréductibles de degrés 1 ou 2 ? Évaluer ces nombres (rationnels) pour $p = 2$ et $d \leq 7$.

□Soient $n_1 = p$ et $n_2 = \binom{p}{2}$ les nombres de polynômes unitaires irréductibles de degré respectivement 1 et 2. Alors, le nombre cherché est

$$\sum_{a+2b=d} \left(\!\binom{n_1}{a}\!\right)\left(\!\binom{n_2}{b}\!\right)$$

où $\left(\!\binom{n}{r}\!\right) = \binom{r+n-1}{r}$ est le cardinal des multiensembles de cardinal r pris dans un ensemble de cardinal n. Par exemple, pour $d = 3$, on trouve $\frac{2}{3}p^3 + \frac{1}{3}p$, qui est bien égal à $p^3 - \frac{1}{3}(p^3-p)$ (cf. **1.5.6**). La probabilité est donc $\frac{2}{3} + \frac{1}{3p^2}$. Lorsque $p = 2$ et d quelconque, on trouve $2^{-d}\sum_{a+2b=d}(a+1)$. Par exemple, pour $d = 3$, on (re)trouve $\frac{3}{4}$. Le calcul des autres valeurs est laissé au lecteur intéressé.□

Exercice 17.

(i) Démontrer les critères de Butler et Ben-Or énoncés en §**3.2**.

(ii) Vérifier à la main le critère de Butler pour le polynôme $T^6-2T^4+3T^3-T^2-T-2 \in \mathbb{F}_7[T]$.

□(i) Ben-Or : si un polynôme de degré d n'est pas irréductible, il a au moins un facteur irréductible de degré $\leq d/2$ donc une racine dans un corps $\mathbb{F}_{q^r}$ pour un $r \leq \lfloor d/2 \rfloor$. Cette dernière condition implique qu'il n'est pas premier avec $T^{q^r} - T$ dont $\mathbb{F}_{q^r}$ est un corps de décomposition.

(ii) Il faut d'abord vérifier que f est séparable, c'est-à-dire premier avec sa dérivée $f' = T^5 - T^3 + 2T^2 - 2T - 1$, ce qui se fait au moyen de l'algorithme d'Euclide :

$$\begin{aligned}
f &\equiv -3T^4 - 2T^3 - 3T^2 - 2T - 2 \pmod{f'} \\
f' &\equiv -2T^3 + 2T^2 - T - 3 \pmod{-3T^4 - 2T^3 - 3T^2 - 2T - 2} \\
-3T^4 - 2T^3 - 3T^2 - 2T - 2 &\equiv -3T^2 - 2T + 2 \pmod{-2T^3 + 2T^2 - T - 3} \\
-2T^3 + 2T^2 - T - 3 &\equiv -3T \pmod{-3T^2 - 2T + 2} \\
-3T^2 - 2T + 2 &\equiv 2 \pmod{-3T}
\end{aligned}$$

$$\mathrm{Frob}_7 = \begin{pmatrix} 1 & 0 & 2 & -1 & 0 & 3 \\ 0 & 2 & 2 & 0 & 2 & -2 \\ 0 & 1 & 2 & -1 & 0 & 0 \\ 0 & 1 & 2 & -3 & -2 & -2 \\ 0 & -3 & -2 & 3 & -3 & -3 \\ 0 & 2 & -3 & -2 & 3 & 1 \end{pmatrix}, \quad \mathrm{Frob}_7 - \mathrm{Id} = \begin{pmatrix} 0 & 0 & 2 & -1 & 0 & 3 \\ 0 & 1 & 2 & 0 & 2 & -2 \\ 0 & 1 & 1 & -1 & 0 & 0 \\ 0 & 1 & 2 & 3 & -2 & -2 \\ 0 & -3 & -2 & 3 & 3 & -3 \\ 0 & 2 & -3 & -2 & 3 & 0 \end{pmatrix}$$

□

Exercice 18. (Amélioration du lemme de §**1.5.5**.) ¶Soit $P \in \mathbb{Z}[T]$. Montrer qu'il existe une infinité de nombres premiers ℓ tels que $P \mod \ell$ soit *scindé*.

(*Indication : on se ramène à montrer que si* $A := \mathrm{Adu}_{\mathbb{Z}}(P)$ *est l'algèbre de décomposition universelle de P, il existe une infinité de* ℓ *pour lesquels on ait une surjection* $A \twoheadrightarrow \mathbb{F}_\ell$. *C'est un fait général pour toute algèbre disons libre de type fini comme* $\mathbb{Z}$*-module.*)

□(Esquisse) Soit $\mathfrak{p}_{\mathbb{Q}}$ un idéal premier de $A_{\mathbb{Q}} := \mathrm{Adu}_{\mathbb{Q}}(P)$. Quitte à remplacer A par $A/\mathfrak{p}$, où $\mathfrak{p} := \mathfrak{p}_{\mathbb{Q}} \cap A$, on peut supposer l'anneau A *intègre*, de corps des fractions noté K. Soit $P \in \mathbb{Q}[T]$ le polynôme minimal d'un élément primitif de l'extension finie $K/\mathbb{Q}$. Il existe un entier $n \geq 1$ tel (P soit à coefficients dans $\mathbb{Z}[1/n]$ et) que l'anneau $A[1/n]$ soit isomorphe à $\mathbb{Z}[1/n][T]/(P)$. Il suffit donc de démontrer le résultat attendu pour ce dernier anneau ; cela résulte du lemme que l'on souhaite généraliser.□

Exercice 19. ¶Montrer que le nombres entiers plus petits que x *dans facteur carré* est équivalent à $x/\zeta_{\mathbb{Z}}(2) = \frac{6}{\pi^2}x$ lorsque $x \to +\infty$. (Comparer avec la proposition de **1.6.3**.)

□Voir [Hardy et Wright 2007, démonstration du théorème 333].□

Exercice 20. Calculer le nombre de solutions de $y^2 + y = x^3$ dans $\mathbb{F}_2$ et $\mathbb{F}_4$. Montrer que si d est *impair*, le nombre de solutions dans $\mathbb{F}_{2^d}$ est 2^d.

□Si d est impair, l'application $x \mapsto x^3$ est une bijection de $\mathbb{F}_{2^d}$ car le groupe multiplicatif $\mathbb{F}_{2^d}^\times$ est d'ordre premier à 3. D'autre part, l'endomorphisme $\wp : y \mapsto y^2 + y$ du groupe additif de $\mathbb{F}_{2^d}$ est de noyau $\mathbb{F}_2 = \{0, 1\}$ donc d'image d'indice 2. On a donc $2^{d-1} \times 2$ solutions.

Remarque : il s'agit d'une *courbe elliptique* sur $\mathbb{F}_2$ à laquelle on a retiré un point à l'infini. Sa « fonction Zêta » (non définie dans ce cours) est $(1+2T^2)/(1-T)(1-2T)$.□

Exercice 21. (« hachage » [TAOCP 3, exercice 6.4-7]) Soient $n \geq e \geq 1$ deux entiers et r tel que $n \mid 2^r - 1$. Notons $\mathbb{F}$ un corps à 2^r éléments et fixons un élément $x \in \mathbb{F}^\times$ d'ordre (exactement) n. Soit enfin $E \subseteq \mathbb{Z}/n\mathbb{Z}$ le plus petit ensemble contenant $\{1, \dots, e\}$ tel que $2E \subseteq E$.

(i) Montrer que $f(T) := \prod_{i \in E}(T - x^i) \in \mathbb{F}[T]$ est à coefficients dans $\mathbb{F}_2$.

(ii) Montrer que si $g(T) = \sum_{0 \leq j < n} a_i T^i \in \mathbb{F}_2[T]$ est un polynôme non nul ayant au plus e coefficients non nuls alors $f \nmid g$.

Voir [TAOCP 3, §6.4] pour le lien avec le hachage.

□(Esquisse)
(i) Par hypothèse, l'ensemble des x^i, pour $i \in E$, est stable par Frob_2 ; les coefficients de f sont donc fixes par Frob_2. (ii) Écrivons $g(T) = T^{d_1} + \cdots + T^{d_s}$ avec $d_1 > \cdots > d_s \geq 0$ et $s \leq e$. Choisissons arbitrairement $e - s$ entiers $d_{s+1}, \dots, d_e$ tels que les $d_1, \dots, d_e$ soient distincts et strictement inférieurs à n. Alors, la matrice de Vandermonde (x^{id_j}), $1 \leq i, j \leq e$, est inversible — car les x^{d_j} sont distincts — mais la somme de ses s premières colonnes est nulle si $f \mid g$ car les x^i sont alors des racines de g.□

Exercice 22. Soient $n_1, \dots, n_r$ et $m_1, \dots, m_s$ des entiers ≥ 2. À quelle condition les groupes $\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$ et $\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_s\mathbb{Z}$ sont-ils isomorphes ?

□On se ramène immédiatement, par le théorème chinois au cas particulier où les n_i et les m_j sont des puissances d'un même nombre premier p : c'est-à-dire $n_i = p^{e_i}$ et $m_j = p^{f_j}$. Les groupes sont alors isomorphes si et seulement si pour tout entier $e \geq 1$, les ensembles $\{i : e_i = e\}$ et $\{j : f_j = e\}$ sont de même cardinal. En d'autres termes, ils sont isomorphes si et seulement si pour tout p et tout e, les ensembles $\{i : v_p(n_i) = e\}$ et $\{j : v_p(m_j) = e\}$ sont égaux, où $v_p(n)$ désigne l'exposant de la plus grande puissance de p divisant n.□

Exercice 23. Soient $p \neq 2$ un nombre premier et le caractère quadratique de $\mathbb{F}_p^\times$.

(i) Rappeler pourquoi pour chaque $a \in \mathbb{F}_p^\times$, on a $|\mathscr{F}()(a)| = \sqrt{p}$.

(ii) Montrer que pour tout *entier* n et tout entier $1 \leq a < p$, on a

$$\sum_{1 \leq k \leq n} \exp(2\pi i a k/p) = O(\|a/p\|^{-1}),$$

où $\|x\|$ est la distance de x à l'entier le plus proche.

(iii) En déduire, via la formule d'inversion de Fourier, que l'on a

$$|\sum_{1 \leq k \leq n} (k)| = O(\sqrt{p}\log(p))^{①}.$$

① En étant plus précis, on peut montrer l'inégalité de Pólya-Виноградов=Vinogradov : $|\sum_{1 \leq k \leq n} (k)| \leq \sqrt{p}\log(p)$

□(Esquisse)
(ii) En calculant la somme géométrique, on se ramène à montrer que $|1-\exp(2\pi i\theta)| \geq c\cdot\theta$, pour une constante $c>0$, lorsque $\theta \in [0, \frac{1}{2}]$. Cela résulte par exemple de la minoration $\sin(\theta) \geq \frac{2}{\pi}\theta$ pour θ un angle aigu.
Il résulte de cette majoration que le nombre de résidus quadratiques modulo p dans $[a,b]$ est $\frac{1}{2}(b-a)+O(\sqrt{p}\log(p))$.□

Exercice 24. Montrer que le nombre de sous-espaces de dimension $d \leq n$ de $\mathbb{F}_q^n$ est $\binom{n}{d}_q := \prod_{i=1}^{n}(q^i-1)\prod_{i=1}^{d}(q^i-1)^{-1}\prod_{i=1}^{n-d}(q^i-1)^{-1}$. Équivalent lorsque $q\to 1$ (dans les *réels*) ?

Exercice 25. Soient $\mathbb{F}$ un corps fini de cardinal q et $P\in\mathbb{F}[T]$ un polynôme de degré d, supposé tel que $P(0)=0$ pour simplifier.

(i) Soit $Q(X) := \prod_{\lambda\in\mathbb{F}}(X-P(\lambda))$. Montrer que les coefficients de Q de degré $q-i$ tel que $0<di<q-1$ sont nuls.
(*Indication : on pourra considérer* $\prod_{\lambda\in\mathbb{F}}(X-P(t\lambda)) = \sum_i c_i(t)X^{q-i}$, *où* $c_i\in\mathbb{F}[t]$ *est de degré* $\leq di$, *et remarquer que la* fonction c_i *est constante sur* $\mathbb{F}^\times$.)

(ii) Montrer que $P(\mathbb{F})\subseteq\mathbb{F}$ est l'ensemble des zéros du polynôme $Q-(X^q-X)$ et en déduire le théorème suivant de Wan Daqing [万大庆] : ou bien $P(\mathbb{F})=\mathbb{F}$ ou bien $P(\mathbb{F})$ est de cardinal au plus $q-\frac{q-1}{d}$.

□(Esquisse)
(i) Le fait que $c_i(t)$ soit de degré au plus di est évident. La *fonction* c_i est constante sur $\mathbb{F}^\times$; si son degré est $<q-1$, le polynôme c_i est constant, égal à $c_i(0)$. Si $i\neq 0$, on a $c_i(0)=0$ (car $P(0)=0$). (ii) L'égalité entre l'image de P et l'ensemble des zéros de Q ou $R := Q-(X^q-X)$ est évidente. D'après ce qui précède, le polynôme R est de degré $\leq q-\frac{q-1}{d}$. S'il est nul, $P(\mathbb{F})=\mathbb{F}$, sinon l'ensemble de ses zéros est de cardinal majoré par son degré.□

Exercice 26. Soit $p\neq 2$ un nombre premier. Montrer que pour tous $a,b\in\mathbb{F}_p$, le nombre de solutions de l'équation $ax^2+by^2=1$ est $p-(\frac{-ab}{p})$, où le terme de droite désigne le symbole de Legendre considéré en **2.4**.
(*Indications. [Première méthode] On pourra résoudre dans* $\mathbb{F}_{p^2}$ *puis voir quelles sont les solutions qui sont dans* $\mathbb{F}_p$. *[Seconde méthode] On pourra commencer par montrer qu'il existe une solution puis en déduire que que l'ensemble des solutions de* $aX^2+bY^2=Z^2$ *dans* $\mathbb{P}^2(\mathbb{F}_p)$ *est* $p+1$. *On obtient alors le résultat en comptant le « nombre de points à l'infini », solutions de l'équation* $ax^2+by^2=0$.)

Exercice 27. Soit $u=(u_n)$ une suite récurrente à valeurs dans $\mathbb{F}_q$ satisfaisant les égalités $u_n = f(u_{n-1},u_{n-2},\dots,u_{n-r})$ pour un $r\geq 1$ et une fonction $f:\mathbb{F}_q\to\mathbb{F}_q$. Montrer que u est *périodique*.

□C'est un fait général qui n'est pas spécifique aux corps finis. L'ensemble $\mathbb{F}_p^r$ étant fini, il existe forcément [...]□

Exercice 28.

(i) Soit p un nombre premier. Montrer qu'une suite à valeurs dans $\mathbb{F}_p \cup \{\infty\}$ satisfaisant la relation de récurrence $u_{n+1} = au_n^{-1} + b$ — avec la convention que $0^{-1} = \infty$, $\infty^{-1} = 0$, $\infty + x = \infty$ —, a pour période $p+1$ si et seulement si le polynôme $f(T) = T^2 - bT - a$ satisfait les deux propriétés suivantes : (i) T^{p+1} est congru modulo f à une constante non nulle (ii) $T^{p+1/\ell} \pmod f$ est de degré 1 pour tout nombre premier $\ell \mid p+1$.

(ii) Quel est le nombre de (a, b) tels que ces propriétés soient satisfaites ?

Voir [TAOCP 2, 3.2.2] pour le lien avec la génération de « nombres aléatoires » [随机数生成].

□[Esquisse] On veut que la matrice $g \in \mathrm{PGL}_2(\mathbb{F}_p)$ image de $G := \begin{pmatrix} 0 & 1 \\ a & b \end{pmatrix}$ soit d'ordre $p+1$. Comme le polynôme caractéristique de G est f, on a immédiatement le résultat. Le polynôme $T^{p+1} - \lambda$ ayant une unique racine, simple, dans $\mathbb{F}_p$ pour chaque $\lambda \neq 0$, un polynôme f satisfaisant (i) est nécessairement irréductible. Le nombre cherché est la moitié du nombre des $x \in \mathbb{F}_{p^2}^\times$ d'ordre exactement $p+1$ dans $\mathbb{F}_{p^2}^\times / \mathbb{F}_p^\times$ soit encore $\frac{1}{2}(p-1)$ multiplié par le cardinal des éléments d'ordre exactement $p+1$ de $\mathbb{F}_{p^2}^\times / \mathbb{F}_p^\times$. Comme ce dernier est cyclique d'ordre $p+1$, le résultat est $\frac{1}{2}(p-1)\varphi(p+1)$.□

Exercice 29.

(i) Soit p un nombre premier. Quelle est la probabilité qu'un élément de $\mathbb{F}_p^\times$ soit *primitif* (c'est-à-dire générateur [multiplicatif] de ce groupe [multiplicatif]) ?

(ii) ¶ Montrer qu'il existe une suite de nombres premiers (p_n) telle que cette probabilité tend vers 0 quand $n \to +\infty$. (*Indication : on pourra choisir les p_n tels que $p_n - 1$ soit divisible par de plus en plus de nombres premiers et utiliser le fait que $\prod_\ell \left(1 - \ell^{-1}\right) = 0$, où ℓ parcourt les nombres premiers.*)

(iii) Même question, lorsque l'on cherche les p_n de la forme p^{f_n} pour un nombre premier p fixé.

Exercice 30. Contre-exemples aux implications possibles entre « $f \in A[T]$ irréductible », « $f_K \in K[T]$ » irréductible » et « $f_k \in k[T]$ irréductible ».

Exercice 31. Soit $f \in \mathbb{Z}[T]$ un polynôme unitaire, se réduisant modulo deux nombres premiers distincts en un produit de polynômes irréductibles de degrés $(d_1, \ldots, d_r)$ et $(e_1, \ldots, e_s)$. Montrer que si ces décompositions sont *incompatibles*, au sens où $\sum_{i \in I} d_i = \sum_{j \in J} e_j$ si et seulement si $I = \{1, \ldots, r\}$ et $J = \{1, \ldots, s\}$, alors f est irréductible.

Exercice 32.

(i) Un nombre composé $n \geq 2$ est dit **pseudo-premier** [伪素数] en base b (ou b-pseudo-premier) si b^{n-1} est congru à 1 modulo n. Montrer que p^2 est pseudo-premier en base b si et seulement si $b^{p-1} \equiv 1 \pmod{p^2}$.

(ii) Montrer que si n est 2-pseudo-premier, l'entier $2^n - 1$ aussi.

□(i) Résulte du fait que le PGCD de $\varphi(p^2) = p(p-1)$ et $p^2 - 1 = (p+1)(p-1)$ est $p-1$. (Ou, plus simplement peut-être, $p^2 - 1 - \varphi(p) = p - 1$ donc $b^{p^2-1} \equiv 1$ entraîne $b^{p-1} \equiv 1$.)

(ii) En utilisant $x^2 - 1 = (x-1)(x+1)$, on voit que $2^{2^n-2} - 1$ est divisible par $2^{2^{n-1}-1} - 1$. Comme l'exposant $2^{n-1} - 1$ est un multiple de n, l'entier $x^n - 1$ divise $x^{2^{n-1}-1} - 1$ pour tout x. En particulier pour $x = 2$. Noter que $2^n - 1$ est bien composé (=non premier) car n l'est.□

Exercice 33. ¶Soient k un anneau et $n \geq 1$ un entier. On rappelle que les *fonctions symétriques élémentaires* $\sigma_1, \ldots, \sigma_n \in k[X_1, \ldots, X_n]$ sont définies par l'égalité $\prod_{i=1}^{n}(T - X_i) = T^n + \sum_{i=1}^{n}(-1)^i \sigma_i T^{n-i}$. Montrer que $\mathrm{Fix}(\mathfrak{S}_n \circlearrowright k[X_1, \ldots, X_n]) = k[\sigma_1, \ldots, \sigma_n]$, où $\mathfrak{S}_n$ agit sur les X_i par permutation des indices.

(*Indication : on pourra procéder par récurrence lexicographique sur le monôme de plus haut degré dans l'expression symétrique.*)

□On munit les monômes de l'ordre lexicographique : $X_1^{a_1} \cdots X_n^{a_n} \prec X_1^{b_1} \cdots X_n^{b_n}$ (inégalité stricte) si et seulement si $a_1 < b_1$ ou ($a_1 = b_1$ et $a_2 < b_2$) ou ($a_1 = b_1$, $a_2 = b_2$ et $a_3 < b_3$) etc. Pour $r_1, \ldots, r_n$ des entiers, considérons le polynôme symétrique $\sigma_1^{r_1} \cdots \sigma_n^{r_n}$: son monôme maximal est $X_1^{r_1+r_2+\cdots+r_n} X_2^{r_2+\cdots+r_n} \cdots X_n^{r_n}$. Soit maintenant un polynôme symétrique f arbitraire et $\lambda X_1^{a_1} \cdots X_n^{a_n}$ son monôme maximal ($\lambda \in k - \{0\}$). Puisque f symétrique, on a $a_1 \geq a_2 \geq \ldots \geq a_n$, sans quoi on pourrait permuter deux variables et obtenir un monôme supérieur. Soit $r_1, \ldots, r_n$ les (uniques) entiers *positifs* tels que $r_1 + r_2 + \cdots + r_n = a_1$, $r_2 + \cdots + r_n = a_2$, ..., $r_n = a_n$. Alors, $f - \lambda \sigma_1^{r_1} \cdots \sigma_n^{r_n}$ est encore symétrique mais son monôme maximal est strictement inférieur à celui de f. On peut alors conclure par récurrence. (Remarquer que l'on n'a pas besoin que k soit un corps.)□

Exercice 34. Soit $n \geq 2$ un entier. Montrer que le discriminant du polynôme $T^n + aT + b$ est

$$(-1)^{\frac{n(n-1)}{2}} \left(n^n b^{n-1} + (1-n)^{n-1} a^n\right).$$

(*Indication : on pourra utiliser le fait que le discriminant est égal à* $(-1)^{\frac{n(n-1)}{2}} \prod_i f'(x_i)$, *où les* x_i *sont les racines de* f, *et utiliser la formule* $\prod_i (ux_i + v) = \sum_i u^i \sigma_i(x_1, \ldots, x_n) v^{n-i}$ *où les* σ_j *sont les fonctions symétriques élémentaires.*)

Exercice 35. Soit p un nombre premier impair.

- **(i)** Montrer que le discriminant de $X^p - 1$ est $(-1)^{\frac{p-1}{2}} p^p$.
- **(ii)** En déduire que $\mathbb{Q}(\sqrt{(-1)^{\frac{p-1}{2}} p}) \subseteq \mathbb{Q}(\zeta_p)$.
- **(iii)** Lien avec les sommes de Gauß ?
- **(iv)** En déduire que toute extension quadratique (=de degré 2) de $\mathbb{Q}$ se plonge dans une extension cyclotomique.

Exercice 36. (Stickelberger, 1897) ¶Soient $p \neq 2$ un nombre premier et $f \in \mathbb{F}_p[T]$ unitaire de degré d, supposé de discriminant $\Delta \neq 0$. Montrer que le nombre de facteurs irréductibles de f dans $\mathbb{F}_p[T]$ est congru à d modulo 2 si et seulement si Δ est un carré dans $\mathbb{F}_p^\times$.

□La signature de Frob_p agissant sur les racines de $f = f_1 \cdots f_r$ (décomposition irréductible) dans une clôture algébrique est égale à $(-1)^{d_1 - 1} \cdots (-1)^{d_r - 1} = (-1)^{d-r}$. Or, cette signature est égale à 1 si et seulement si Frob_p est une permutation paire, ce qui est équivalent au fait que le discriminant soit un carré.□

Exercice 37. ¶Soient $a_1, \ldots, a_n \in \mathbb{Z}$ distincts et $n \geq 2$ un entier. Montrer que $(T - a_1) \cdots (T - a_n) - 1$ est irréductible dans $\mathbb{Z}[T]$.

□Soit gh une factorisation non triviale. On peut supposer ces deux polynômes unitaires. Puisque $g(a_i)h(a_i) = -1$, on a $(g+h)(a_i) = 0$. Or, le polynôme $g+h$ est non nul, de degré $< n$. Il est absurde qu'il ait n racines distinctes.□

Exercice 38. Montrer que dans la définition d'un couple hensélien, le relèvement a de α est nécessairement unique.

Exercice 39. (amusette) Soit n un entier. On suppose que l'on a $2n+1$ pierres telles que pour toute pierre, l'ensemble des $2n$ pierres restantes puisse être divisé en deux tas de même masse de n pierres. Les pierres ont-elles toutes même masse ?