有限域
Corps finis
上海/Shanghai, 2016-10/11[①]

Fabrice ORGOGOZO[②].

version : 8b86773 2017-08-16 12:19:13 +0200

Table des matières

Le symbole ¶ indique des passages plus difficiles ; leur lecture n'est pas nécessaire à la compréhension du cours oral.

① Cours et TDs : 2016-10-10,11,13,24²,26²,28²,31 ; 2016-11-1.

② « Fabrice Orgogoço »=法布里斯·奥尔戈戈索.

Le cours oral, plus « concret », *s'appuyant* sur ces notes (et n'en couvrant qu'une partie) :

cours n° 1. Groupes (généralités) [**1.2**, **1.3**, **1.4**, **1.9**, **2.1**, **2.2.1**, **2.2.5**]
cours n° 2. Anneaux (généralités) [**3.2**, **3.3**, **3.4.1**, **3.4.2**, **3.7.2**]
cours n° 3. Algèbres [**4.2.1**, **5.1.5**, **5.1.1**, **4.4**, **5.2.2**, **6.1.2**, **6.1.4**]
TD n° 1. Exercices n° 2, 11, 29, 30
cours n° 4. Algèbres [**6.2**, **6.3**]
cours n° 5. Corps finis [**7.6.2**, **7.1**, **7.3.1**]
TD n° 2. Exercices n° 31, 38 [+critère de Ben-Or **8.2.1**], 44
cours n° 6. Corps finis [**7.3.2**, **7.3.3**, **7.3.4**, **7.3.5**, **8.2.2**]
TD n° 3. Exercices n° 48, 53
cours n° 7. Corps finis [exercice n° 47 ; **2.3.2**, **7.7**]
TD n° 4. Résumé du cours et questions.

Merci à 郑维喆 et aux contributeurs de zh.wikipedia.org pour leur aide dans la traduction des termes techniques en chinois, ainsi qu'à Alain Chillès [祁冲], Vésale Nicolas et leurs collègues chinois et français pour leur accueil à Shanghai.

1. Groupes : rappels

Références : [Serre 1978-79], [Šafarevič 1997] (magnifique survol), [Rotman 1995], [Perrin 1996].

Cette section est constituée de brefs rappels sur les groupes ; pour plus de détails, nous renvoyons le lecteur aux références.

1.1. Soit X un ensemble. On note $\mathrm{Aut}(X)$ — ou $\mathrm{Aut}_{\mathtt{Ens}}(X)$ si on veut insister sur le fait que X est un ensemble « nu » c'est-à-dire vu sans structure supplémentaire — l'ensemble des *bijections* $g : X \to X$, c'est-à-dire des applications $g : X \to X$ telles qu'il existe $h : X \to X$ satisfaisant $g \circ h = g \circ h = \mathrm{Id}_X$, l'endomorphisme identité de X, que nous noterons aussi e. Les propriétés suivantes sont immédiates et bien connues :

- **(i)** (loi de composition) pour tout couple $g, h \in \mathrm{Aut}(X)$, on a $g \circ h \in \mathrm{Aut}(X)$;
- **(ii)** (associativité) pour tout triplet $f, g, h \in \mathrm{Aut}(X)$, on a $f \circ (g \circ h) = (f \circ g) \circ h$;
- **(iii)** (élément neutre) l'élément e satisfait $e \circ g = g \circ e = g$ pour tout $g \in \mathrm{Aut}(X)$;
- **(iv)** (inverse) pour tout $g \in \mathrm{Aut}(X)$, il existe un élément h, noté g^{-1}, tel que $g \circ h = h \circ g = e$.

1.2. On appelle **groupe** [群] un ensemble G muni d'un produit $G \times G \to G$, $(g, h) \mapsto g \cdot h$ satisfaisant les propriétés (ii)-(iv) précédentes. Un **morphisme de groupes** [群态射/群同态] $f : (G_1, \cdot_1) \to (G_2, \cdot_2)$ est une application de G_1 dans G_2 respectant la structure de groupes : $f(g \cdot_1 h) = f(g) \cdot_2 f(h)$ pour tout couple $g, h \in G_1$. En particulier, $f(e_1) = e_2$.

Un groupe est dit **abélien** [阿贝尔群] ou **commutatif** si le produit ne dépendant pas de l'ordre des éléments : pour tous $g, h \in G$, on a $g \cdot h = h \cdot g$. (Notons que ce n'est pas le cas du groupe $\mathrm{Aut}(X)$ lorsque X possède au moins trois éléments.)

On peut *définir* un groupe de diverses manières, que nous explicitons ou illustrons dans les paragraphes suivants :

- sous-groupe ;
- quotient ;
- tables de multiplication/Cayley ;
- générateurs et relations.

Bien entendu, on peut aussi définir directement un produit sur un ensemble et vérifier qu'il satisfait les propriétés requises ; c'est parfois non trivial. (Voir par exemple [Šafarevič 1997, §12, exemples 2 et 3].)

1.3. Sous-groupes. Si G est un groupe, un sous-ensemble $H \subseteq G$ est un **sous-groupe** [子群] de G — souvent noté $H \leqslant G$ — si la restriction du produit de $G \times G \to G$ induit une structure de groupe $H \times H \to H$ sur H : si $h_1, h_2 \in H$, l'élément $h_1 \cdot h_2$ *a priori* dans G appartient à H et si $h \in H$, l'élément h^{-1} *a priori* dans G appartient également à H.

Si G est le groupe $\mathrm{Aut}_{\mathtt{Ens}}(X)$ des bijections d'un ensemble X muni d'une structure supplémentaire, un exemple typique est le sous-groupe H des éléments de G respectant cette structure : si X est un espace euclidien, l'ensemble $\mathsf{Isom}(X)$ des

isométries de X est un sous-groupe de $\mathrm{Aut}_{\mathtt{Ens}}(X)$; si X est un espace topologique (par exemple une partie de $\mathbb{R}^n$), l'ensemble des bijections *bicontinues* de X est également un sous-groupe de $\mathrm{Aut}_{\mathtt{Ens}}(X)$.

Si $f : G_1 \to G_2$ est un morphisme de groupes, les sous-ensembles

$$\mathrm{Ker}(f) \coloneqq \{g_1 \in G_1 \,:\, f(g_1) = e_2\} \leqslant G_1$$

et

$$\mathrm{Im}(f) \coloneqq \{f(g_1), g_1 \in G_1\} \leqslant G_2$$

sont respectivement des sous-groupes de G_1 et G_2 appelés **noyau** [核] et **image** [像] du morphisme f.

Tout sous-groupe $H \leqslant G$ est l'image d'un morphisme de groupes ; prendre par exemple l'inclusion $H \hookrightarrow G$.

1.4. **Quotients.** Un sous-groupe $H \leqslant G$ est le noyau d'un morphisme de groupes $f : G \to G'$ si et seulement si H est un **sous-groupe distingué** [正规子群] (on note $H \lhd G$) : pour tout $g \in G$ et tout $h \in H$, le **conjugué** [共轭(元)] ghg^{-1} de h par g *a priori* seulement dans G est dans H.

Une implication est évidente : si $f : G \to G'$ est un morphisme et $h \in \mathrm{Ker}(f)$ alors $f(ghg^{-1}) = f(g)f(h)f(g^{-1}) = f(g)f(g)^{-1} = e$: les conjugués de h appartiennent également au noyau. Pour la réciproque, il faut, donné un sous-groupe *distingué* $H \lhd G$, construire un morphisme $f : G \to G'$ tel que $\mathrm{Ker}(f) = H$. Un tel morphisme « contracte » tous les éléments de H en un seul élément — l'élément neutre de G' — et de même, tous les éléments de $gH \coloneqq \{gh, h \in H\}$ ou Hg sur un seul élément (l'image de g). Il est donc naturel de considérer l'***ensemble*** **quotient** [商集] (voir *infra*) G' de G par la **relation d'équivalence** [等价关系] $g\mathscr{R}_H g'$ si et seulement si $gH = g'H$ et la *structure* de groupe sur G' définie par la condition que l'application $G \twoheadrightarrow G'$, $g \mapsto gH$ soit un morphisme. En d'autres termes, on veut définir un produit satisfaisant $(gH)\cdot(g'H) = gg'H$, quels que soient g, g' dans G. Ceci est possible si et seulement si $Hg' \subseteq g'H$ pour tout $g' \in G$; ou encore (en changeant légèrement les notations) : $gHg^{-1} \subseteq H$ pour tout $g \in G$. Une condition nécessaire et suffisante est donc que H soit distingué dans G.

Si $\mathscr{R} \subseteq E \times E$ est une relation d'équivalence sur un ensemble E, l'ensemble quotient de E par $\mathscr{R}$, noté $E/\mathscr{R}$, est par définition l'ensemble des classes d'équivalences, c'est-à-dire les sous-ensembles de E de la forme $\overline{x} \coloneqq \{y \in E \,:\, x\mathscr{R}y\}$, pour un certain x. Ces classes d'équivalence forment une partition de E et on a une application surjective canonique $E \twoheadrightarrow E/\mathscr{R}$ envoyant x sur $\overline{x}$. (Cette surjection joue un rôle universel parmi les applications de source E envoyant deux éléments en relation sur le même élément du but.) Dans le cas précédent, $\overline{g}$ n'est autre que $gH \subseteq G$ et, ensemblistement, $G/\mathscr{R}_H$ est l'ensemble $\{gH, g \in G\}$ des *classes à gauche*.

En particulier, la construction de l'*ensemble* quotient $G/\mathscr{R}_H$ est possible même lorsque H n'est pas distingué ; seule la structure de groupe (compatible avec celle de G) pourrait lui manquer. Cet ensemble est noté G/H ; s'il est fini, on note $(G : H)$ son cardinal, appelé **indice** [指数] de H dans G.

Du fait que les classes d'équivalence sont toutes en bijection avec H, si bien que G est *ensemblistement* en bijection avec le produit $H \times G/H$, on déduit le théorème de Lagrange : si G est fini, on a l'égalité

$$\operatorname{card} G = (G : H) \operatorname{card} H$$

pour tout sous-groupe $H \leqslant G$; en particulier, le cardinal de H divise celui de G. Si $H = \{e = g^0 = g^\omega, g, g^2, \ldots, g^{\omega-1}\}$ est engendré par un élément g d'ordre fini ω, on en tire que $\omega | \operatorname{card}(G)$: l'ordre d'un élément divise l'ordre du groupe fini G.

1.5. table de multiplication. La donnée d'une loi de composition $G \times G \to G$ peut s'interpréter comme une matrice carrée, éventuellement infinie, indicée par les éléments de $G = \{g : g \in G\}$ et à valeurs dans G : l'élément à la g-ième ligne et h-ième colonne est le produit $g \cdot h$. (Bien que ce soit arbitraire, il faut fixer un ordre.) Par exemple, si G est l'ensemble à 8 éléments notés $1, -1, i, -i, j, -j, k, -k$, on peut définir une loi de composition par la table de multiplication suivante :

$\cdot$	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

On vérifie sans peine que ce produit fait de G un groupe de cardinal 8, dont 1 est l'élément neutre. C'est le groupe des **quaternions** [四元群] souvent noté Q_8 ; c'est l'un des deux groupes non abélien de cardinal 8 (à isomorphisme près).

Il est naturel de penser que l'exemple précédent pourrait être présenté de façon plus compacte : Q_8 est engendré par 4 éléments $-1, i, j, k$ satisfaisant les relations $(-1)^2 = 1$ et $i^2 = j^2 = k^2 = ijk = -1$. Le sens précis à donner à un tel énoncé n'est pas immédiat.

1.6. ¶ Générateurs et relations.
Références : [Artin 1991, chap. 6, §7.9-11], [Šafarevič 1997, §14, p. 134 et §13], [A. Douady et R. Douady 2005, 2.6.2 et 4.7.4], [Magnus, Karrass et Solitar 1966, chap. 1], [Lyndon et Schupp 1977, chap. 1-2], [Rotman 1995, chap. 11].

1.6.1. Commençons par définir la notion de **sous-groupe engendré** [生成的子群] par une partie : si G est un groupe et $(g_x)_{x \in X}$ est une famille d'éléments de G, le sous-groupe (de G) engendré par les g_x est *le* plus petit sous-groupe de G les contenant ; on le note $\langle g_x : x \in X \rangle$. La définition a un sens car l'intersection de sous-groupes contenant les g_x est un tel sous-groupe ; en particulier on peut écrire :

$$\langle g_x : x \in X \rangle = \bigcap_{H \leqslant G} H,$$

où H parcourt les sous-groupes contenant $\{g_x : x \in X\}$.

Dans la construction précédente, on se donne un groupe et tout a lieu dans ce groupe. Une question naturelle est de savoir si, donné un ensemble X, on peut construire un groupe engendré par des éléments e_x (distincts) indicés par X et n'ayant pas d'autres relations que les relations « évidentes » déduites de la structure de groupe : $g \cdot g^{-1} = e$. Un tel groupe existe et est unique à isomorphisme près : on l'appelle le **groupe libre** [自由群] construit sur X, noté L_X. (Si $X = \{1, \dots, n\}$, on le note L_n ou F_n.) On peut par exemple considérer les e_x et e_x^{-1} comme des caractères distincts et définir L_X comme l'ensemble des *mots* (de longueur finie arbitraire, éventuellement nulle) construits sur les e_x et e_x^{-1}, pour $x \in X$, et ne contenant pas de motif $e_x\, e_x^{-1}$ ou $e_x^{-1} e_x$. (Un tel mot est dit *réduit*.) Voir l'exercice 13 pour les détails.

Proposition. *Pour tout groupe G et toute famille $(g_x)_{x\in X}$ d'éléments de G, il existe un unique morphisme $L_X \to G$ envoyant un générateur $e_x \in L_X$ sur g_x.*

1.6.2. Revenons à la question de définir un groupe par « générateurs et relations ». Soit G un groupe et $(g_x)_{x\in X}$ des générateurs : $G = \langle g_x \,:\, x \in X\rangle$. D'après la proposition précédente, il existe un morphisme, nécessairement surjectif, $L_X \twoheadrightarrow G$, envoyant, pour tout $x \in X$, le mot e_x de longueur 1 sur g_x. Soit N le noyau de ce morphisme ; c'est un sous-groupe *distingué* de L_X, a priori infini. Un sous-*ensemble* $R \subseteq N$ est un ensemble de **relations** [关系元] des g_x si N est le plus petit sous-groupe *distingué* de L_X contenant R. On dit que la paire $\langle X | R\rangle$ est une **présentation** de $G \simeq L_X/N$.

1.6.3. **Exemples.** ¶ Notons $\mathrm{SL}_2(\mathbb{Z})$ (resp. $\mathrm{PSL}_2(\mathbb{Z})$) le groupe des matrices à coefficients entiers de déterminant 1 (resp. son quotient par le sous-groupe $\pm\mathrm{Id}$). Les éléments $\begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$ et $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ définissent un morphisme $L_2 \to \mathrm{SL}_2(\mathbb{Z})$ qui induit les présentations

$$\langle s, t | s^3 = t^2, t^4 = 1\rangle \xrightarrow{\sim} \mathrm{SL}_2(\mathbb{Z}) \text{ et } \langle s, t | s^3 = t^2 = 1\rangle \xrightarrow{\sim} \mathrm{PSL}_2(\mathbb{Z}).$$

Le groupe symétrique $\mathfrak{S}_n$ étant engendré par les $n-1$ transposition $\sigma_i := (i, i+1)$, pour $1 \leqslant i \leqslant n-1$, on en déduit un morphisme surjectif $L_{n-1} \twoheadrightarrow \mathfrak{S}_n$ envoyant e_i sur σ_i. Il induit un isomorphisme

$$\langle \sigma_1, \dots, \sigma_{n-1} | \sigma_i^2 = 1, (\sigma_i\sigma_{i+1})^3 = 1, \sigma_i\sigma_j = \sigma_j\sigma_i \text{ si } |i-j| \neq 1\rangle \xrightarrow{\sim} \mathfrak{S}_n.$$

1.6.4. **Remarques.**

(1) D'après un théorème de Pëtr Novikov, il n'existe pas d'algorithme permettant de déterminer, à partir d'une présentation, si le groupe quotient est trivial (voir par exemple [Rotman 1995, chap. 12]).

(2) On montre dans l'exercice 14 que le groupe $\mathrm{SO}_3(\mathbb{R})$ des isométries directes de $\mathbb{R}^3$ admet un sous-groupe libre de rang 2, c'est-à-dire isomorphe à L_2. Cela a des conséquences tout à fait surprenantes (paradoxe de Banach-Tarski).

1.7. **¶ Groupoïdes.** Dans les applications, le concept de groupe est parfois trop restrictif, et est avantageusement remplacée par celui de **groupoïde** [广群] : on se donne un ensemble $\mathcal{G}$, une application $\mathrm{inv} : \mathcal{G} \to \mathcal{G}$ et une application *partielle* $\mathcal{G} \times \mathcal{G} \dashrightarrow \mathcal{G}$, $(a, b) \mapsto a \star b$, définie seulement pour certains couples, telles que

(i) (associativité partielle) si $a \star b$ et $b \star c$ sont définis, il en est de même de $(a \star b) \star c$, $a \star (b \star c)$ et ils sont égaux ; réciproquement, si l'un de ces deux doubles produits est défini, il en est de même de l'autre [et ils sont nécessairement égaux] ;

(ii) (inverse) les produits $\mathrm{inv}(a) \star a$ and $a \star \mathrm{inv}(a)$ sont toujours définis ;

(iii) (identité) si $a \star b$ est défini, alors $a \star b \star \mathrm{inv}(b) = a$ et $\mathrm{inv}(a) \star a \star b = b$.

Un exemple très important est celui du « groupoïde fondamental d'un espace topologique » X, noté $\Pi_1(X)$, dont les éléments sont les applications continues $[0,1] \to X$ « à déformation [=homotopie] près », le produit (partiel) est la composition $\gamma_2 \star \gamma_1$ qui envoie t sur $\gamma_1(2t)$ si $0 \leqslant t \leqslant 1/2$ et sur $\gamma_2(2t-1)$ si $1/2 \leqslant t \leqslant 1$; elle n'est définie que si $\gamma_1(1) = \gamma_2(0)$. Enfin l'application inverse est $\mathrm{inv}(\gamma) : t \mapsto \gamma(1-t)$.

1.8. ¶ **Dévissages.** Pour mieux comprendre un groupe E, on souhaite souvent le « réduire » en composants plus simples : comme on l'a vu en définissant les quotients, si $E \twoheadrightarrow B$ est un morphisme surjectif de noyau F, on peut voir B comme obtenu à partir de E en identifiant les éléments égaux « à F près ». On dispose d'une notation compacte pour dire que l'on a un morphisme surjectif dont on spécifie le noyau :

$$1 \to F \to E \to B \to 1.$$

Ce diagramme s'appelle une **suite exacte** [正合序列] et on dit que le groupe E est une **extension** [(群)扩张] de B par F.

Réciproquement, si on imagine B et F comme étant fixés, la question se pose de la *reconstruction* de E : quels sont les groupes (à isomorphisme près) extension de B par F? Il en existe toujours au moins un : le produit cartésien $B \times F$, avec la loi $(b,f)\cdot(b',f') \coloneqq (bb', ff')$, mais ce n'est en général pas le seul, sauf sous des hypothèses très particulières.

Le groupe F étant distingué dans E, le groupe E *agit* sur F par conjugaison : on a un morphisme $E \to \mathsf{Aut}(F)$, $x \mapsto (f \mapsto xfx^{-1})$. On en déduit par composition un morphisme $E \to \mathsf{Aut}(F) \twoheadrightarrow \mathsf{Autex}(F)$, où $\mathsf{Autex}(F)$ — aussi noté $\mathsf{Out}(F)$ — est le groupe des **automorphismes extérieurs** [外自同构群], quotient de $\mathsf{Aut}(F)$ par le sous-groupe $\mathsf{Int}(F)$ des automorphismes intérieurs (les conjugaisons). Par définition, le sous-groupe $F \leqslant E$ est dans le noyau de ce morphisme composé, qui se factorise donc en

$$B \to \mathsf{Autex}(F).$$

Si F est abélien — auquel cas $\mathsf{Aut}(F) = \mathsf{Autex}(F)$ —, la classification des extensions de B par E induisant ce morphisme est expliquée en [Serre 1978-79, chap. 4]. Ceci permet par exemple de montrer que si B et F sont finis et d'ordre premiers entre eux l'extension E est nécessairement isomorphe au produit cartésien $B \times F$ ([ibid., th. 4.10], [Mac Lane 1963, chap. IV, th. 10.5]). Dans le cas général, une approche assez conceptuelle est présentée en ¶[Baez et Shulman 2010, §1]. (Voir aussi ¶[Breen 2010, §5, ex. 5].)

1.9. Action de groupes.

1.9.1. Proposition. *Tout groupe est naturellement le sous-groupe d'un groupe de permutations* $\mathrm{Aut}_{\mathtt{Ens}}(X)$ *d'un ensemble* X. Linéarisation *: il est aussi naturellement le sous-groupe d'un groupe d'automorphismes* $\mathrm{GL}(V)$ *d'un* $\mathbb{Q}$*-espace vectoriel* V*. Si* G *est fini, on peut supposer* X *fini et* V *de dimension finie.*

Démonstration. En effet, l'application $G \to \mathrm{Aut}_{\mathtt{Ens}}(G)$, $g \mapsto (x \mapsto gx)$ est un morphisme de groupes, injectif. On a donc le résultat attendu avec $X = G$. Comme d'autre part, $\mathrm{Aut}(X)$ s'injecte dans $\mathrm{GL}(V)$, où $V = \mathbb{Q}^{(X)} = \bigoplus_x \mathbb{Q}e_x$, par l'application $\sigma \in \mathrm{Aut}(X) \mapsto \left(e_x \mapsto e_{\sigma(x)}\right)$, on a également le résultat. □

En d'autres termes, tout groupe (resp. fini) « agit » naturellement sur un ensemble X (resp. sur un espace vectoriel de dimension finie V). Plus précisément, on appelle **action** [群作用] un morphisme $\rho : G \to \mathrm{Aut}_{\mathtt{Ens}}(X)$, *pas nécessairement injectif*. Pour chaque $g \in G$, on a donc une bijection $\rho(g) : X \to X$; on la note $x \mapsto g \cdot x$. Avec cette notation, le fait que ρ soit un morphisme de groupes se traduit par les égalités suivantes : $g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x$ pour tous $(g_1, g_2, x) \in G^2 \times X$.

Un peu de vocabulaire et de notations…

- $\mathrm{Fix}(G \circlearrowright X) = \{x \in X : g \cdot x = x, \forall g \in G\}$ est l'ensemble des **points fixes** [不动点] de G agissant sur X ;
- $G \cdot x = \{g \cdot x, g \in G\} \subseteq X$ est l'**orbite** [轨道] de x sous G ;
- $G_x = \{g \in G : g \cdot x = x\} \leqslant G$ est le **stabilisateur** [稳定化子] de x.

On vérifie immédiatement que les orbites distinctes forment une *partition* [集合划分] de X, associée à la relation d'équivalence : $x \sim y$ si et seulement si il existe $g \in G$ tel que $y = g \cdot x$. D'autre part, pour chaque $x \in X$, la surjection canonique $G \twoheadrightarrow G \cdot x$, $g \mapsto g \cdot x$, se factorise en une bijection $gG_x \mapsto g \cdot x$ entre l'*ensemble* quotient G/G_x et l'orbite de x.

Voici une application très utile de ce qui précède.

1.9.2. Proposition. *Soient* X *un ensemble fini et* G *un* p***-groupe****, c'est-à-dire un groupe fini d'ordre une puissance d'un nombre premier* p*. Alors, on a l'égalité modulo* p *:*

$$\#X \equiv \#\,\mathrm{Fix}(G \circlearrowright X) \mod p.$$

Démonstration. Le cardinal de X est la somme des cardinaux des orbites (partition). Il y a deux types d'orbites : celles réduites à des singletons, correspondant aux points fixes, et les autres. Ces dernières sont de cardinal l'indice d'un sous-groupe de G ; cet entier est une puissance de p, non triviale par hypothèse. Les orbites non ponctuelles sont donc en particulier toutes de cardinal divisible par p, ainsi que leur somme. □

… et un corollaire (théorème de Cauchy).

1.9.3. Corollaire. *Soit* G *un groupe fini. Si* p *est un nombre premier divisant l'ordre de* G*, il existe un élément* $g \in G$ *d'ordre* p*.*

Démonstration. Soit X le sous-ensemble du produit cartésien G^p constitué des p-uplets $(g_1, g_2, \ldots, g_p)$ tels que le produit $g_1 g_2 \cdots g_p$ soit le neutre de G. L'action de $\mathbb{Z}/p\mathbb{Z}$ sur G^p par permutation circulaire des indices respecte X. D'autre part, l'ensemble $\mathrm{Fix}(\mathbb{Z}/p\mathbb{Z} \circlearrowright G^p)$ est clairement l'ensemble « diagonal » $G \simeq \{(g, g, \ldots, g)\} \subseteq G^p$; il en résulte que $\mathrm{Fix}(\mathbb{Z}/p\mathbb{Z} \circlearrowright X)$ est en bijection avec $\{g \in G \,:\, g^p = e\}$. D'après la proposition précédente, on a donc les congruences (modulo p)

$$0 \equiv \#G^{p-1} \equiv \#\{g \,:\, g^p = e\}.$$

Ainsi, le terme de droite est divisible par p. Comme d'autre part, il contient l'ensemble $\{g \in G \,:\, g^p = e\}$ contient au moins un élément — le neutre ! —, on a le résultat voulu. □

1.9.4. Remarques.

(1) On a en réalité des résultats beaucoup plus forts : si p^r est la plus grand puissance de p divisant le cardinal d'un groupe fini G, il existe un sous-groupe S de G de cardinal p^r (et leur nombre est congru à 1 modulo p). Voir par exemple [Serre 1978-79, chap. 2].

(2) On peut également améliorer le théorème de Cauchy en calculant/estimant le nombre d'éléments de G d'ordre p. Par exemple, pour chaque $p \geqslant 3$ premier fixé, le nombre de permutations σ de $\mathfrak{S}_n$ telles que $\sigma^p = \mathrm{Id}$ est équivalent, lorsque $n \to +\infty$, à
$$(n/e)^{n(1-p^{-1})} p^{-1/2} \exp(n^{1/p}).$$
Voir référence citée en [Flajolet et Sedgewick 2009, VIII.12].

(3) Un point clef de la démonstration de **1.9.2** est l'**équation aux classes** : si $G \circlearrowright X$ et $X = \coprod_{i=1}^{n} \mathcal{O}_i$ est la décomposition de X en orbites distinctes $\mathcal{O}_i = G \cdot x_i$, on a
$$\mathrm{card}(X) = \sum_i \mathrm{card}(\mathcal{O}_i) = \mathrm{card}(G) \times \sum_i \frac{1}{\mathrm{card}\, G_{x_i}}.$$

Pour une autre application de la congruence ci-dessus, voir par exemple l'exercice 1.

2. Transformation de Fourier discrète

2.1. Groupes cycliques.

2.1.1. Un groupe G est dit **cyclique** [循环子群] s'il existe un élément $g \in G$ d'*ordre fini* tel que $G = \langle g \rangle$[①]. Si g est d'ordre n, c'est-à-dire si G est de cardinal n, on a un isomorphisme $\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} G, r \mod n \mapsto g^r$.

Prendre garde au fait que le choix de g n'est pas canonique/intrinsèque : il y a d'autres générateurs de G (sauf si $|G| \leqslant 2$). Précisément, on a $\langle g \rangle = \langle g^r \rangle$ si et seulement si $g \in \langle g^r \rangle$, si et seulement si il existe un entier s tel que $g = g^{rs}$, ce qui se produit si et seulement si $rs \equiv 1 \mod n$. Il est clairement nécessaire que s soit premier avec n — ce que l'on notera $s \perp n$ —. Réciproquement, il résulte du lemme de Bézout que si $s \perp n$, il existe r tel que $rs \equiv 1 \mod n$. (Nous reviendrons sur ces questions dans la section sur les anneaux.) En d'autres termes :

① Cette définition n'est pas universelle : certains auteurs ne supposent pas g d'ordre fini.

2.1.2. Proposition. *Soit $G = \langle g \rangle$ un groupe cyclique d'ordre n. L'application $s \mapsto g^s$ induit une bijection entre l'ensemble des entiers $1 \leqslant s \perp n \leqslant n$ et l'ensemble des générateurs de G.*

Leur nombre est noté $\varphi(n)$; la fonction $\varphi : n \mapsto \varphi(n)$ est appelée **indicatrice d'Euler** [欧拉函数].

2.1.3. Proposition.

(i) (multiplicativité) si $n \perp m$, on a $\varphi(nm) = \varphi(n)\varphi(m)$;
(ii) si p est un nombre premier, $\varphi(p) = p - 1$ et, plus généralement, $\varphi(p^\alpha) = p^{\alpha-1}(p-1) = p^\alpha(1 - p^{-1})$;
(iii) (comportement asymptotique) $\varphi(n) \to +\infty$ lorsque $n \to +\infty$.

Il en résulte que l'on a l'égalité :

$$\varphi(n) = n \times \prod_{p|n} (1 - \frac{1}{p}).$$

Démonstration. Le plus simple est probablement d'observer que les générateurs du *groupe* $\mathbb{Z}/n\mathbb{Z}$ sont exactement les éléments inversibles (unités) de l'*anneau* $\mathbb{Z}/n\mathbb{Z}$. (i) La multiplicativité résulte alors du théorème chinois **3.5** : on a $\mathbb{Z}/nm\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ d'où $(\mathbb{Z}/nm\mathbb{Z})^\times \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times$. (Voir aussi [Hardy et Wright 2007, 16.1], par exemple, pour une démonstration plus élémentaire.) (ii) Il est clair qu'un entier est premier à p^α si et seulement si il n'est pas multiple de p. Le nombre de ces multiples inférieurs à p^α est $p^{\alpha-1}$. (iii) Remarquons que si n est une puissance de 2, on a $\varphi(n) = n/2 \geqslant \sqrt{n}/2$. D'autre part, si $p \geqslant 3$ est un entier, on a $p - 1 \geqslant \sqrt{p}$ si bien que $p^\alpha(1 - p^{-1}) \geqslant p^{\alpha-1/2} \geqslant p^{\alpha/2}$ pour tout $\alpha \geqslant 1$. Par multiplicativité de φ, on a donc la minoration $\varphi(n) \geqslant \sqrt{n}/2$ pour tout n et, en particulier, $\varphi \to +\infty$. Des résultats bien plus précis sont établis dans [ibid., 18.4]. □

2.2. Caractères des groupes abéliens finis.

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

2.2.1. *Exposant d'un groupe abélien fini.* Soit G un groupe abélien fini, noté multiplicativement. On appelle **exposant** de G [指数] de G le PPCM des ordres d'éléments de G : c'est le plus petit entier n tel que pour tout $g \in G$ on ait $g^n = e$. 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 $n_1 n_2$.

2.2.2. 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. 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 $\overline{1}$.

2.2.3. Remarque. ¶ Soit G un groupe non nécessairement abélien et $f : G \to A$ un morphisme vers un groupe abélien. L'image de f est un sous-groupe abélien donc f se factorise à travers un quotient *abélien* $\overline{G}$ de G. Il existe un plus grand tel quotient — l'**abélianisé** [阿贝尔化] G^{ab} de G — et on vérifie que f se factorise en $G \twoheadrightarrow G^{\mathrm{ab}} \xrightarrow{f^{\mathrm{ab}}} A$. En particulier, l'étude d'un groupe G par ses morphismes vers $\mathbb{C}^\times$ ne peut nous donner d'informations que sur G^{ab}.

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.

2.2.4. 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 (voir **1.8**) $1 \to \widehat{(G/H)} \to \widehat{G} \to \widehat{H} \to 1$. 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.

2.2.5. *Structure des groupes abéliens finis.* Soit G un groupe abélien fini, d'exposant n. On a vu ci-dessus 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.)

Voir [Serre 1978-79, §3.5] pour une autre démonstration.

2.2.6. ¶*Équation $X^n = g$ dans un groupe abélien fini.* Pour tout entier n, notons $G[n] \coloneqq \{g \in G : g^n = 1\}$ 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.)

2.3. Transformation de Fourier discrète.

Références : [Terras 1999, chap. 2, 8-9], [Gathen et Gerhard 2003, §8.2], et ¶[A. Douady et R. Douady 2005, §5.3.1-4] (approche plus conceptuelle).

2.3.1. Soient $n \geqslant 1$ un entier et $\mathbf{e} : \mathbb{Z}/n\mathbb{Z} \to \mu_n(\mathbb{C}) \subseteq \mathbb{C}^\times$, $x \mapsto \exp(2\pi i x/n)$, un caractère non trivial du groupe cyclique $\mathbb{Z}/n\mathbb{Z}$. Pour toute fonction f sur $\mathbb{Z}/n\mathbb{Z}$ à valeurs complexes, notons pour abréger $\int f$ la somme finie $\sum_{t \in \mathbb{Z}/n\mathbb{Z}} f(t)$ et définissons le produit hermitien :

$$\langle f, g \rangle \coloneqq \int f\overline{g}.$$

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

$$\xi \mapsto \langle f, [\times\xi]^\star \mathbf{e} \rangle \coloneqq \sum_{t \in \mathbb{Z}/n\mathbb{Z}} f(t)\mathbf{e}(-t\xi),$$

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

Par exemple, pour chaque $x \in \mathbb{Z}/n\mathbb{Z}$, on a tautologiquement

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

et

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

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

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

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

et

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

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

Si f et g sont deux fonctions sur $\mathbb{Z}/n\mathbb{Z}$, 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 :

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

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

Supposons maintenant que n est un nombre premier, que nous notons dorénavant p, et considérons maintenant un caractère *multiplicatif* χ 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 $\chi_1 \star \cdots \star \chi_r = J(\chi_1,\dots,\chi_r)\chi_1\cdots\chi_r$, lorsque $\chi_1\cdots\chi_r \neq \mathbf{1}$, où

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

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

3. Anneaux, corps

3.1. Soit X un espace topologique, par exemple une partie de $\mathbb{R}^n$. Notons $A = \mathsf{Hom}_{\mathrm{Top}}(X,\mathbb{C})$ l'ensemble des applications continues de X dans $\mathbb{C}$. Les propriétés suivantes sont immédiates et bien connues :

- **(i)** (addition) pour tout $\varphi,\psi \in A$, on a $\varphi+\psi = \psi+\varphi \in A$, $-\varphi \in A$ et $\varphi + \mathbf{0} = \varphi$, où $\mathbf{0}$ désigne la fonction identiquement nulle. ;
- **(ii)** (multiplication) pour tout $\varphi,\psi \in A$, la fonction produit $\varphi\times\psi : x \mapsto \varphi(x)\psi(x)$ appartient à A, la fonction $\mathbf{1}$ constante égale de valeur 1 satisfait $\mathbf{1}\cdot\varphi = \varphi\cdot\mathbf{1} = \varphi$ et ce produit est associatif : $\varphi\times(\psi\times\xi) = (\varphi\times\psi)\times\xi$ pour tout triplet ;
- **(iii)** (distributivité) pour tout triplet φ,ψ,ξ, on a $\varphi\times(\psi+\xi) = \varphi\times\psi + \varphi\times\xi$.
- **(iv)** (commutativité) $\varphi\times\psi = \psi\times\varphi$ pour tout couple φ,ψ.

Gloses :
(i) : $(A,+,\mathbf{0})$ est un groupe abélien ; (ii) $\times$ est une loi de composition interne sur A, d'unité $\mathbf{1}$; (iii) pour chaque φ, l'application $a \mapsto \varphi\times a$ de multiplication à gauche par φ est un endomorphisme du groupe additif $(A,+)$.

3.2. Un **anneau (commutatif)** [交换环] est un ensemble A muni de lois $+,\times$ appelées addition et produit/multiplication satisfaisant les propriétés précédentes. Dans ce texte, nous ne considérons que des anneaux *commutatifs unitaires*, ces deux dernières propriétés portant sur la multiplication②.

Il résulte formellement des définitions que l'ensemble

$$A^\times \coloneqq \{a \in A \,:\, \exists b, ab = ba = \mathbf{1}\}$$

des **éléments inversibles** [单位] (ou « **unités** ») d'un anneau (commutatif) A forment un groupe (commutatif). Par exemple, le groupe des unités de l'anneau $\mathbb{Z}/n\mathbb{Z}$

① . Noter les analogies :

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

② . On ne prétend par contre *pas* que seuls les anneaux commutatifs soient importants — penser par exemple aux endomorphismes d'un espace vectoriel —, ni que la présence d'une unité soit toujours essentielle — penser par exemple à l'espace $L^1(\mathbb{R})$ muni du produit de convolution —. Sur ce dernier point, voir l'exercice 15.

des entiers modulo n est constitué des classes des entiers $x \perp n$; il est de cardinal $\varphi(n)$. En conséquence, pour tout entier $x \perp n$, on a $x^{\varphi(n)} \equiv 1 \mod n$. Si n est un nombre premier p, cela se réécrit : $x^{p-1} \equiv 1 \mod p$ pour tout $x \perp p$, ou encore $x^p \equiv x \mod p$ pour tout $x \in \mathbb{Z}$ (petit théorème de Fermat ; voir aussi 3.7.2 *infra*).

Un **morphisme d'anneaux** $f : A \to B$ est une application de A dans B induisant un morphisme de groupes additifs $(A, +) \to (B, +)$ et respectant produits et unités : pour tous a, a' dans A, on $f(aa') = f(a)f(a')$ et $f(\mathbf{1}_A) = \mathbf{1}_B$. Dans une telle situation, il est souvent commode de considérer B comme un anneau, muni d'une structure supplémentaire — à savoir $A \to \mathrm{End}(B, +)$, $a \mapsto (b \mapsto f(a)b)$ — induite par f : on dit alors que B est une A-**algèbre** [代数] et l'élément $f(a)b$ est simplement noté $a \cdot b$ ou même ab sans que f ne soit nécessairement injective. (Si c'est le cas, on dit que B est une **extension** [扩张] de A.)

3.3. Quotients, idéaux.

3.3.1. Soit $f : A \to B$ un morphisme d'anneaux. Le noyau de f est celui du morphisme de groupes additifs sous-jacents :

$$\mathrm{Ker}(f) = \{a \in A : f(a) = \mathbf{0}_B\}.$$

La principale différence avec la théorie des groupes est que ce sous-ensemble de A, qui est bien un sous-groupe additif, n'est *pas* un sous-anneau (sauf si B est l'anneau nul) : l'application $\mathrm{Ker}(A) \hookrightarrow A$ n'est pas un morphisme d'anneaux, car $\mathbf{1}_A$ n'appartient pas à $\mathrm{Ker}(A)$, sauf si $B = 0$.

Les sous-ensembles de A jouant pour les anneaux le rôle des sous-groupes distingués en théorie des groupes sont appelés idéaux de A. Un **idéal** [理想] $I \subseteq A$ est un sous-ensemble de A stable par addition, et par multiplication par les éléments de A : si $i \in I$ et $a \in A$, on a $ai \in I$. On vérifie immédiatement que le noyau $\mathrm{Ker}(f)$ ci-dessus est un idéal de A et que, réciproquement, tout idéal I de A est le noyau d'un morphisme d'anneaux, de source A. Plus précisément, on peut définir le quotient A/I en identifiant deux éléments de A égaux *à translation par un élément de I près* et vérifier qu'il existe une unique structure d'anneau sur A/I telle que la surjection canonique $A \twoheadrightarrow A/I$, envoyant a sur sa classe $\overline{a}$, soit un morphisme d'anneaux.

Formellement, A/I est l'ensemble quotient de A par la relation d'équivalence $\mathscr{R}_I$ définie par : $x \mathscr{R}_I y$ si et seulement si $x - y \in I$. On dit que $\mathscr{R}_I$ est la relation de **congruence modulo** I [模I同余(关系)] et on note en général $x \equiv y \mod I$.

3.3.2. Remarque. ¶ On peut s'interroger sur l'existence d'un analogue du théorème de Cayley (1.9.1) qui donnerait un caractère universel à la construction faite au début de 3.1. Il n'est pas difficile de se convaincre qu'un anneau n'est pas toujours un (sous-anneau) de fonctions d'un espace topologique vers un corps fixé. La théorie des schémas de Alexander Grothendieck donne cependant ce qui semble être la meilleure réponse à cette question pour un anneau commutatif quelconque. Dans le cas particulier des k-algèbres, on a également des résultats partiels de nature élémentaire (théorie de Gelfand par exemple).

3.3.3. L'**intersection** (finie ou non) d'idéaux étant un idéal, toute partie E de A est contenue dans un plus petit idéal, que l'on appelle **idéal engendré** [生成的理想] par E. Lorsque $E = \{e_1, \dots, e_n\}$, on note habituellement $(e_1, \dots, e_n)$ cet idéal. (Comparer avec la notation $\langle g_1, \dots, g_n \rangle$ pour les groupes.) On en a une description explicite :

$$(e_1, \dots, e_n) = \{a_1 e_1 + \cdots + a_n e_n ; n \in \mathbb{N}, a_1, \dots, a_n \in A^n\}.$$

On dit qu'un idéal est de **type fini** [有限型(理想)] s'il est engendré par un nombre fini d'éléments.

La **somme** (finie ou non) d'idéaux est par définition le plus petit idéal contenant ces idéaux ; c'est l'idéal engendré par leurs éléments. On note $I + J$ la somme de deux idéaux I, J et on vérifie immédiatement que

$$I + J = \{a + b ; a \in I, b \in J\}.$$

Avec cette notation, on a $(e_1, \dots, e_n) = e_1 A + \cdots + e_n A$. Prendre cependant garde au fait que le produit naïf de deux idéaux n'est en général pas un idéal ; le **produit** d'un nombre *fini* d'idéaux $I_1, \dots, I_n$ est donc défini comme l'idéal engendré par les produits $a_1 \cdots a_n$ avec $a_1 \in I_1$, etc. En particulier,

$$IJ = \{\sum_{k=1}^{n} i_k j_k ; n \in \mathbb{N}, i_k \in I, j_k \in J\}.$$

Par définition d'un idéal, on a $IJ \subseteq I \cap J$ et de même avec un nombre (fini) arbitraire de facteurs.

3.4. **Constructions.** Soit A un anneau (commutatif). On peut construire quantité de nouveaux anneaux. (Pour d'autres exemples, voir les exercices 24, etc.)

3.4.1. *Anneau $A[T]$ des polynômes sur A.* L'ensemble $A^{(\mathbb{N})}$ des suites (a_n) à support fini, c'est-à-dire telles que $a_n = \mathbf{0}_A$ pour $n \gg 0$ est naturellement muni d'une structure de groupe additif : $(a_n) + (b_n) := (a_n + b_n)$. On peut également le munir d'un produit (de convolution) : $(a_n) \times (b_n) = (c_n)$, où

$$c_n := \sum_{i+j=n} a_i b_j.$$

Si on note plutôt T^n la suite valant $\mathbf{1}_A$ en n et $\mathbf{0}_A$ en les autres indices, de sorte qu'un élément $a = (a_n)$ se décompose en $a = \sum_n a_n T^n$, on voit que la définition précédente est équivalente à la formule usuelle

$$(\sum_n a_n T^n) \times (\sum_n b_n T^n) = \sum_n (\sum_{i+j=n} a_i b_j) T^n.$$

Nous reviendrons en détail sur cette A-algèbre dans les sections suivantes.

Remarques.

(i) ¶ Plus généralement, si $(M, +)$ est un *monoïde*, on peut définir la A-algèbre $A[M]$ des sommes finies $\sum_m a_m T_m$ munie du produit caractérisé par $(a_m T_m) \cdot (a_{m'} T_{m'}) = (a_m a_{m'}) T_{m+m'}$. Par exemple, $A[\mathbb{N}]$ est isomorphe, comme A-algèbre, à l'anneau de polynômes $A[T]$.

(**ii**) L'hypothèse que les suites soient à support fini, c'est-à-dire dans $A^{(\mathbb{N})}$ et pas seulement dans $A^{\mathbb{N}}$, n'est pas utile pour définir un nouvel anneau (commutatif, unitaire). On en obtient un plus gros, que l'on appelle l'anneau des **séries formelles** [形式幂级数] à coefficients dans A, noté $A[[T]]$. Voir ¶[Cartan 1961, I.§1] pour une introduction. L'anneau quotient $\mathbb{Z}[[T]]/(T-p)$ est l'anneau des nombres p-adiques, que nous n'étudierons pas dans ces notes.

3.4.2. *Localisation, corps des fractions.*

Référence : [Bourbaki AC, II, §2, n°1].

(a) Partant de l'anneau $\mathbb{Z}$ des entiers relatifs, la construction du corps des rationnels, dans lequel tous les entiers non nuls acquièrent un inverse (et minimal en un certain sens pour cette propriété), est bien connue. Plus généralement, si $\{s\}_{s\in S}$ est une collection d'entiers non nuls on peut construire un anneau entre $\mathbb{Z}$ et $\mathbb{Q}$ dans lequel on ajoute « seulement » les inverses des entiers $s \in S$ et ceux qui s'en déduisent, par exemple leurs produits. Cet anneau, qu'il est naturel de noter $\mathbb{Z}[s^{-1}, s \in S]$ est le sous-anneau de $\mathbb{Q}$ constitué des rationnels r tels qu'il existe un entier $L \geqslant 0$ et des $s_1, s_2, \ldots, s_L \in S$ satisfaisant $s_1 s_2 \cdots s_L r \in \mathbb{Z}$.

(b) Nous allons voir qu'il existe une méthode semblable pour construire un anneau $A[S^{-1}]$ (aussi noté $S^{-1}A$) dans lequel les éléments d'un sous-ensemble S d'un anneau A deviennent inversibles et ceci sans supposer avoir construit un grand anneau dans lequel (presque) tous les éléments sont inversibles ($\mathbb{Q}$ dans l'exemple précédent). Supposons pour simplifier que le sous-ensemble S est un sous-monoïde de $(A, \times)$, c'est-à-dire que cette partie est stable par produit fini ; en particulier, $\mathbf{1}_A \in S$. (Un exemple typique d'une telle situation est le cas où $S = \mathbf{1}_A + \mathfrak{a}$, lorsque $\mathfrak{a}$ est un idéal de A. Voir exercice 21.) Notons que cette hypothèse est naturelle car d'une part l'ensemble des unités d'un anneau est un sous-monoïde et, d'autre part, le cas général s'y ramène : remplacer ci-dessous S par le sous-monoïde $\overline{S}$ de $(A, \times)$ engendré par S. La construction est alors relativement évidente : on encode une fraction « as^{-1} » de l'anneau que l'on cherche à construire comme un couple (a, s), $a \in A$, $s \in S$. Cette écriture étant *a priori* non unique — par exemple parce que l'on veut $s_2 \cdot (s_1 s_2)^{-1} = 1 \cdot s_1^{-1}$ dans $A[S^{-1}]$ — on fait l'identification suivante : $(a, s) \sim (a', s')$ si et seulement si il existe un élément t de S tel que $t(as' - a's) = \mathbf{0}_A$. (L'introduction du facteur t permet de montrer que la relation ainsi définie est bien transitive. Elle est inutile si A est intègre mais peut s'avérer nécessaire ; voir l'exercice 20.)

L'ensemble $A[S^{-1}]$, quotient de $A \times S$ par la relation d'équivalence précédente, est naturellement un anneau : poser

$$(a, s) + (a', s') = (as' + a's, ss')$$

et

$$(a, s) \cdot (a', s') = (aa', ss').$$

(On dit que cet anneau est un **localisé** [環的局部化] de A.)

Le morphisme $A \to A[S^{-1}]$, $a \mapsto (a, \mathbf{1}_A)$, fait de $A[S^{-1}]$ une A-algèbre (universelle pour la propriété de rendre les éléments de S inversibles). Prendre garde au

fait que le morphisme $A \to A[S^{-1}]$ n'est pas nécessairement injectif ; par exemple si $\mathbf{0}_A \in S$, l'anneau $A[S^{-1}]$ est l'**anneau nul** [零环] (à un élément, $\mathbf{0} = \mathbf{1}$).

(c) Ceci ne se produit pas si chaque élément $s \in S$ est **non diviseur de zéro** (ou **régulier**) [正则元] : si $sa = \mathbf{0}_A$ alors $a = \mathbf{0}_A$. Un cas particulier important est celui où S est l'ensemble des éléments réguliers ; dans ce cas $A[S^{-1}]$ est appelé **anneau (total) des fractions** [全分式环] de A et on le note $\mathrm{Frac}(A)$. Si A est **intègre** [整环], c'est-à-dire ($A \neq 0$ et) si tout élément non nul est régulier, l'anneau total des fractions est un *corps* (cf. §3.6), appelé **corps des fractions** [分式環] de A.

Pour une description concrète, lorsque S est engendré par un seul élément, voir l'exercice 18.

3.4.3. *Produit cartésien.* Soient maintenant A_1, A_2 deux anneaux. Le produit cartésien $A_1 \times A_2$ est naturellement muni d'une structure d'anneau en effectuant les opérations composante par composante :

$$(a_1, a_2) + (b_1, b_2) = (a_1 +_1 b_1, a_2 + b_2) \text{ et } (a_1, a_2) \times (b_1, b_2) = (a_1 \times_1 b_1, a_2 \times b_2).$$

C'est la seule structure d'anneau telle que les projections $A_1 \times A_2 \twoheadrightarrow A_1$ et $A_1 \times A_2 \twoheadrightarrow A_2$ soient des morphismes d'anneaux.

3.5. Théorème chinois [中国剩余定理].

Proposition. *Soient A un anneau et $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ des idéaux tels que $\mathfrak{a}_i + \mathfrak{a}_j = A$ pour tous $i \neq j$. Le morphisme canonique*

$$\pi : A \to \prod_{i=1}^{n} A/\mathfrak{a}_i,\ a \mapsto (a \mod \mathfrak{a}_i)_i$$

est surjectif, *de noyau l'idéal* $\operatorname{Ker} \pi = \bigcap_i \mathfrak{a}_i = \mathfrak{a}_1 \cdots \mathfrak{a}_n$.

Démonstration. Commençons par démontrer la surjectivité dans le cas particulier $n = 2$. Si $\mathfrak{a}_1$ et $\mathfrak{a}_2$ sont deux idéaux tels que $\mathfrak{a}_1 + \mathfrak{a}_2 = A$, il existe deux éléments de $\mathfrak{a}_1$ et $\mathfrak{a}_2$ de somme égale à $\mathbf{1}_A$. Cela revient à dire qu'il existe deux éléments $e_1, e_2 \in A$ d'image respectivement $(\mathbf{1}, \mathbf{0})$ et $(\mathbf{0}, \mathbf{1})$ dans $A/\mathfrak{a}_1 \times A/\mathfrak{a}_2$. (On peut supposer $e_2 = \mathbf{1}_A - e_1$.) Soient $\overline{x}$ et $\overline{y}$ des éléments respectifs des quotients $A/\mathfrak{a}_1$ et $A/\mathfrak{a}_2$, et $x \in A$, $y \in A$ des éléments les relevant. L'élément $z \coloneqq e_1 x + e_2 y$ est d'image $(\overline{x}, \overline{y})$ dans le produit les deux quotients.

Revenons au cas général : $n \geqslant 2$ et procédons par récurrence. Il est clair que la condition *nécessaire* de l'existence, pour chaque $1 \leqslant j \leqslant n$, d'un élément $e_j \in A$ d'image $(\mathbf{0}_{A/\mathfrak{a}_1}, \ldots, \mathbf{0}_{A/\mathfrak{a}_{j-1}}, \mathbf{1}_{A/\mathfrak{a}_j}, \mathbf{0}_{A/\mathfrak{a}_{j+1}}, \ldots, \mathbf{0}_{A/\mathfrak{a}_n})$ est *suffisante*. (Les rôles des éléments étant symétriques, on pourrait même se contenter de montrer l'existence d'un élément e_1.) Par récurrence (pour $n - 1$), il existe des éléments e'_j, $1 \leqslant j < n$ ayant les images voulues dans $\prod_{i<n} A/\mathfrak{a}_i$. Admettons un instant que $\left(\prod_{i<n} \mathfrak{a}_i\right) + \mathfrak{a}_n = A$. Il existe donc (cas $n = 2$) un élément $e_n \in \mathfrak{a}_n$ tel que $1 - e_n \in \prod_{i<n} \mathfrak{a}_i \subseteq \bigcap_{i<n} \mathfrak{a}_i$. On vérifie immédiatement que la famille $e_1 \coloneqq e'_1(\mathbf{1}_A - e_n), \ldots, e_{n-1} \coloneqq e'_{n-1}(\mathbf{1}_A - e_n), e_n$ répond à la question. Pour démontrer le fait momentanément admis, il suffit de développer l'égalité d'idéaux $\prod_{i<n}(\mathfrak{a}_i + \mathfrak{a}_n) = A$, vraie car pour chaque $i < n$, on a $\mathfrak{a}_i + \mathfrak{a}_n = A$.

Étudions maintenant le noyau. L'égalité $\operatorname{Ker}\pi = \bigcap_i \mathfrak{a}_i$ est tautologique. Il faut par contre montrer que l'inclusion *a priori* $\prod_i \mathfrak{a}_i \subseteq \bigcap_i \mathfrak{a}_i$ est une égalité. Quitte à remplacer e_n ci-dessus par $\mathbf{1}_A - (\sum_{i<n} e_i)$, on peut supposer que la somme $\sum_{i=1}^n e_i$ est égale à $\mathbf{1}_A$. On peut donc écrire tout élément $x \in A$ comme une somme $x = \sum_i x e_i$, qui appartient à l'idéal $\sum_i x \cdot \bigcap_{j\neq i} \mathfrak{a}_j$. Par récurrence, cet idéal est $\sum_i x \cdot \prod_{j\neq i} \mathfrak{a}_j$. Si $x \in \bigcap_i \mathfrak{a}_i$, on a pour chaque i l'inclusion $x \cdot \prod_{j\neq i} \mathfrak{a}_j \subseteq \prod_i \mathfrak{a}_i$. □

Remarque. ¶ Dans le langage géométrique offert par la théorie des schémas de Grothendieck, l'énoncé précédent est essentiellement équivalent à l'observation triviale suivante (reformulée dans un cadre topologique) : si un ensemble X contient des sous-ensembles X_i deux à deux disjoints, toute collection de fonctions sur les X_i s'étend en une fonction sur X.

3.6. Corps. Un **corps** [域] est un anneau (commutatif) $k \neq 0$ tel que tout élément non nul soit inversible : $k^\times = k - \{\mathbf{0}_k\}$.

Les corps jouent un rôle essentiel en algèbre, assez semblable au rôle que jouent les points en géométrie et en topologie. Étant donné un anneau A, il est donc naturel de s'intéresser aux morphismes de A vers un corps k. (Les morphismes d'un corps vers A sont injectifs ; un anneau — par exemple $\mathbb{Z}$ — ne contient pas toujours de corps.) Soit $f : A \to k$ un morphisme d'anneaux, de but un corps k. Il se factorise en (c'est-à-dire s'écrit comme le composé des morphismes) $A \twoheadrightarrow A/\mathfrak{p} \xrightarrow{\sim} \operatorname{Im}(f) \subseteq k$, où $\mathfrak{p} := \operatorname{Ker}(f)$. Tout sous-anneau d'un corps étant intègre, il en est ainsi de $B := A/\mathfrak{p}$. Lorsque qu'un quotient $A/\mathfrak{p}$ est intègre, on dit que $\mathfrak{p}$ est un **idéal premier** [素理想]. Notons que l'on peut encore factoriser le morphisme $B \hookrightarrow k$ en $B \subseteq \operatorname{Frac}(B) \hookrightarrow k$, où $\operatorname{Frac}(B)$ est le corps des fractions de B. Si $B = A/\mathfrak{p}$ est déjà un corps, on dit que l'idéal $\mathfrak{p}$ est **maximal** [极大理想] [①].

On montre (théorème de Krull) que tout anneau non nul possède un — et en général plusieurs ! — idéal maximal. Ce fait est équivalent au célèbre *axiome du choix*. (Voir [Jech 1973] pour une discussion de cet axiome et ¶[Hodges 1979] pour l'équivalence.)

Des exemples classiques de corps sont : $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C} = \mathbb{R}[T]/(T^2+1)$, $\mathbb{Z}/p\mathbb{Z}$ (p premier). Nous verrons plus loin bien d'autres exemples, comme par exemple le corps des nombres algébriques (resp. constructibles) dans $\mathbb{C}$.

La théorie des corps repose de façon cruciale sur la théorie des polynômes et des algèbres, qui font l'objet des deux sections suivantes.

3.7. Caractéristique, Frobenius.

3.7.1. Soit A un anneau. Il existe un unique morphisme d'anneaux $\mathbb{Z} \to A$; son image est contenue dans le **sous-anneau premier**

$$\mathbb{Z}_A := \{n \cdot (m \cdot \mathbf{1}_A)^{-1} : n, m \in \mathbb{Z}, m \cdot \mathbf{1}_A \in A^\times\} \subseteq A.$$

(En particulier, A est naturellement une $\mathbb{Z}_A$-algèbre.)

Si k est un corps, on a nécessairement $\mathbb{Z}_k = \mathbb{Q}$ ou $\mathbb{Z}_k = \mathbb{F}_p$, pour un p premier, selon que le générateur $n \geqslant 0$ de $\operatorname{Ker}(\mathbb{Z} \to k)$, appelé **caractéristique** [特征]

① ¶ Cette terminologie vient du fait qu'un idéal est maximal si et seulement si il l'est pour l'inclusion parmi les idéaux stricts. Plus généralement, il n'est pas difficile de montrer que la surjection $A \to A/I$ induit par image inverse une bijection entre les idéaux de A/I et les idéaux de A contenant I.

de k, est nul ou non. On note car. (k) cet entier. (¶ Il est aussi parfois commode de considérer l'**exposant caractéristique** [特征指数 (?)] du corps k : exp.car.$(k) \coloneqq \sup(1, \text{car.}(k))$.)

Soit k un corps de caractéristique p ou, plus généralement, une $\mathbb{F}_p$-algèbre (commutative).

3.7.2. Proposition. *L'application* $\mathrm{Frob}_p : k \to k, a \mapsto a^p$ *est un endomorphisme de* $\mathbb{F}_p$*-algèbre :*

(i) *pour tous* $a, b \in k$*, on a*

$$(ab)^p = a^p b^p ;$$

(ii) *pour tous* $a, b \in k$*, on a*

$$(a+b)^p = a^p + b^p ;$$

(iii) *pour tout* $a \in k$ *et* $\lambda \in \mathbb{F}_p$*, on a*

$$(\lambda a)^p = \lambda a^p.$$

Le morphisme Frob_p d'élévation à la puissance p s'appelle **morphisme de Frobenius** [弗罗贝尼乌斯自同态], probablement en l'honneur du célèbre article [Frobenius 1896].

Notons au passage que d'après (iii), on a le **petit théorème de Fermat** : pour tout entier $n \geqslant 0$, et tout nombre premier p, on a la congruence

$$n^p \equiv n \mod p.$$

Démonstration. L'égalité (i) est triviale — l'anneau k est commutatif — ; quant à (ii), elle est équivalente à l'égalité $\lambda^p = \lambda$ pour $\lambda \in \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Cette dernière résulte par récurrence de l'égalité (ii) appliquée aux multiples de $\mathbf{1}_A$. On est donc ramené à démontrer (ii). D'après la formule du binôme de Newton, on a

$$(a+b)^p = \sum_{i=0}^{p} \binom{i}{p} \cdot a^i b^{p-i} = a^p + \Big(\sum_{0<i<p} \binom{i}{p} \cdot a^i b^{p-i} \Big) + b^p.$$

Il suffit donc de montrer que si $0 < i < p$, on a $\binom{i}{p} \cdot \mathbf{1}_A = 0$, c'est-à-dire que la caractéristique p divise l'entier $\binom{i}{p} = \frac{p!}{i!(p-i)!}$. Cela résulte par exemple du fait que $i! \perp p$ pour $0 < i < p$, et de même pour $(p-i)!$. (Alternativement, on peut remarquer que ce coefficient binomial est le cardinal de l'ensemble des parties à i éléments de $\mathbb{Z}/p\mathbb{Z}$, que l'on peut munir d'une action par translation du p-groupe $\mathbb{Z}/p\mathbb{Z}$. Elle est sans point fixe (pour $i \neq 0, p$), de sorte que la conclusion résulte de 1.9.2. Pour une troisième démonstration, voir l'exercice 35.) □

4. Polynômes : généralités

4.1. Propriété universelle. Soit k un anneau (commutatif) ; on a rappelé en 3.4.1 la définition de la k-algèbre $k[T]$ des polynômes en une variable à coefficients dans k. On peut itérer cette construction en posant $k[T_1, \ldots, T_n] \coloneqq k[T_1, \ldots, T_{n-1}][T_n]$ (ou encore en considérant $k[\mathbb{N}^n]$) ; c'est la k-algèbre des polynômes en n variables

à coefficients dans k. Elle joue pour les k-algèbres le rôle que le groupe libre L_n joue pour les groupes (cf. proposition de §1.6).

Proposition. *Pour toute k-algèbre A et toute famille $(a_i)_{i=1,\dots,n}$ d'éléments de A, il existe un unique morphisme de k-algèbres $k[T_1,\dots,T_n] \to A$, envoyant la variable T_i sur a_i.*

La démonstration est formelle et le morphisme en question n'est pas mystérieux : il faut (et suffit d') envoyer un polynôme somme de monômes $cT_1^{d_1}\cdots T_n^{d_n} \in k[T_1,\dots,T_n]$ sur la somme des $ca_1^{d_1}\cdots a_n^{d_n} \in A$.

4.2. Algorithme d'Euclide et résultant.

Références : [TAOCP 2, 4.6.1], [Bourbaki A, IV.10], et [Gathen et Gerhard 2003, §3] pour une analyse du nombre d'opérations nécessaires (algorithme d'Euclide) ; [ibid., 6.2], [Apéry et Jouanolou 2006], [Lombardi et Quitté 2011, III.§7], ¶[Gel'fand, Kapranov et Zelevinskiĭ 1994, chap. 12], [Lang 2004, IV.§8] (résultant).

4.2.1. *Division euclidienne [欧几里得除法/辗转相除法].* Soient k un anneau et $f \in k[T]$ un polynôme non nul. Notons $\mathrm{cd}(f)$ le coefficient dominant de $f = a_dT^d + \cdots + a_1T + a_0$: si $a_d \neq 0$, on pose $\mathrm{cd}(f) := a_d \in k$. Pour tout polynôme $g = b_eT^e + \cdots + b_1T + b_0$, avec $e \geqslant d$, l'algorithme d'Euclide[①] fournit deux polynômes $u, v \in k[T]$ tels que

$$\mathrm{cd}(f)^{e-d+1} \cdot g = uf + v, \quad \deg(v) < d.$$

(Rappelons que l'on note $\deg(v)$ le **degré** [次数] d'un polynôme v.) Dans le cas particulier où $\mathrm{cd}(f) = 1$, c'est-à-dire si f est **unitaire** [首一多项式], on retrouve la division euclidienne usuelle : $g = uf + v$.

4.2.2. *PGCD.* Supposons dans ce paragraphe que k est un corps, de sorte que le coefficient d'un polynôme non nul est inversible. Comme nous le verrons en 5.1.5, il résulte de ce qui précède que tout idéal I de $k[T]$ est principal : il existe un polynôme h tel que I soit l'idéal $(h) = h\,k[T]$ engendré par h. Notons que h n'est pas unique mais qu'il le devient si on lui impose d'être unitaire (ou nul).

En particulier, donnés deux polynômes $f, g \in k[T]$, il existe un unique polynôme unitaire ou nul h tel que l'idéal (f, g) engendré par f et g soit égal à (h). On appelle h le **plus grand commun diviseur (PGCD)** [最大公因数] de f et g, parfois noté $f \wedge g$. Si ce PGCD est égal à 1, on dit que f et g sont **premiers entre eux** [互素].

Si $g = uf + v$, on a trivialement $(g, f) = (f, v)$. Il en résulte que l'algorithme d'Euclide permet également de calculer le PGCD $g \wedge f$: on itère $(g, f) = (f, v) = \cdots$ jusqu'à obtenir un reste v nul.

① Rappelons que la première étape de l'algorithme consiste à écrire $\mathrm{cd}(f)g = b_eT^{e-d}f + r$, où $r = c_{e-1}T^{e-1} + \cdots$; on procède alors par récurrence sur e.

4.2.3. Bien que l'algorithme d'Euclide permette (si l'anneau des coefficients est un corps) de calculer mécaniquement le PGCD de deux polynômes, il est utile d'avoir un critère numérique permettant de détecter si deux polynômes f et g sont premiers entre eux. (En particulier, si k est un corps, cela permettrait de savoir si un polynôme a des *racines multiples* dans un sur-corps de k.)

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 $\text{rés}_{n,m}(f, g)$[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 dét(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 $uf + vg = \text{rés}_{n,m}(f, g)$. En symboles : $\text{rés}_{n,m}(f, g) \in (f, g) \cap k$, 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 $T^{n-1}g$, $T^{n-2}g$, ..., g par f. Ainsi,

$$(\ddagger) \qquad \text{rés}(f, g) = \text{dét}\left(\times g \,:\, k[T]/(f) \to k[T]/(f) \right).$$

---

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

②. C'est la terminologie de [Bourbaki AC, III, §4]. Si k est un corps, on dit plutôt qu'ils sont premiers entre eux.

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.*

4.2.4. 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.

Formulaire :

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

4.3. 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).

4.3.1. 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 $f(\alpha) = \mathbf{0}_{A/I}$ et $f'(\alpha) \in (A/I)^\times$, il existe $a \in A$ tel que $a \mapsto \alpha$ par $A \twoheadrightarrow A/I$ et $F(a) = \mathbf{0}_A$. Dans ce cas tout élément $a \in A$ d'image inversible dans A/I est inversible : appliquer la définition au polynôme $aT - \mathbf{1}_A$. 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 $N \geq 0$. 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 $\mathbf{1}_{A/I}$) $\mathbf{1}_A - \varepsilon$ de l'unité est inversible, d'inverse $\mathbf{1}_A + \varepsilon + \varepsilon^2 + \cdots + \varepsilon^N$. Mieux :

4.3.2. 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 $F(a+\varepsilon) = \mathbf{0}$[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 $F(a+\varepsilon) - F(a) - F'(a)\varepsilon \in \varepsilon^2 A$, qui est une incarnation de la *formule de Taylor*, 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, $F(a_n) = \mathbf{0}$ si $2^n > N$ (de sorte que $I^{2^n} = 0$)[②]. □

4.3.3. 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 $F = GH$.*

Rappelons que les conditions « f et g sont fortement étrangers » (c'est-à-dire $(f)+(g) = (\mathbf{1})$) 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 $\mathbf{1}$.

Nous utiliserons cette proposition sous la forme suivante, dont on peut donner une démonstration élémentaire (et algorithmique). Voir par exemple [Gathen et Gerhard 2003, 15.10].

4.3.4. 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* $\mathrm{rés}(g, h) \in \mathbb{F}_p$ *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 $\underline{A}$ l'anneau quotient A/I et $B := \mathrm{Adu}_A(F)$ (resp. $\underline{B} := \mathrm{Adu}_{\underline{A}}(g, h)$) l'algèbre de décomposition universelle du polynôme F sur A (resp. des polynômes g, h), définie en **6.1.2** (resp. **6.3.2**). Par définition, on a des décompositions $F(T) = \prod_{i=1}^{n}(T - x_i)$ dans $B[T]$ et $g(T) = \prod_{i\leq d}(T - \underline{x}_i)$, $h(T) = \prod_{i>d}(T - \underline{x}_i)$ dans $\underline{B}[T]$. Il existe un unique morphisme de A-algèbres $\varphi : B \twoheadrightarrow \underline{B}$ envoyant x_i sur $\underline{x}_i$: 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 $F = G_1H_1$. Il n'y a pas de raison qu'ils soient dans le sous-anneau $A[T]$ de $B[T]$. Soient z l'image dans B d'un polynôme $Z \in$

① En d'autres termes, si $F(a)$ est petit et $F'(a)$ pas trop petit, il existe une solution de $F = \mathbf{0}$ 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.

$A[X_1,\dots,X_n]$ invariant par $\mathfrak{S}_{d,n-d}$ et $P(Y)$ le polynôme $\prod_{\sigma\in\mathfrak{S}_n/\mathfrak{S}_{d,n-d}}(Y-z^\sigma)$, qui s'annule tautologiquement en z. Il est de degré $N := \binom{n}{d}$ et à coefficients dans A car c'est l'image dans $B[T]$ du polynôme $\prod_{\sigma\in\mathfrak{S}_n/\mathfrak{S}_{d,n-d}}(Y-Z^\sigma)\in A[\sigma_1,\dots,\sigma_n,Y]$[①]. On montre immédiatement en développant 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 $P(y)=\mathbf{0}$ 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 η un relèvement arbitraire de h dans $A[T]$. Nous allons appliquer ce qui précède à $z:=\eta(x_1)\cdots\eta(x_d)\in B$, image de $Z=\eta(X_1)\cdots\eta(X_d)$. Comme $h(\underline{x}_i)=\mathbf{0}$ si $i>d$, l'image $p(Y)\in\underline{A}[Y]$ par φ du polynôme $P(Y)$ est $Y^{N-1}(Y-\underline{z})$, où l'image $\underline{z}$ de z dans $\underline{A}\subseteq\underline{B}$, est égale au produit $h(\underline{x}_1)\cdots h(\underline{x}_d)$. Puisque $(g)+(h)=(\mathbf{1})$, pour chaque racine $\underline{x}_i$ ($i\leq d$) de g dans $\underline{B}$, on a $h(\underline{x}_i)\in\underline{B}^\times$, si bien que $z\in\underline{A}^\times$. (On a $\underline{A}\cap\underline{B}^\times=\underline{A}^\times$ car $\underline{A}$ 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 $\underline{A}$.

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, $G_1=G_2$. □

4.4. Lemme de Gauß.

Références : [Perrin 1996, II.§4], [TAOCP 2, 4.6.1], [Gathen et Gerhard 2003, §6.2], [Lombardi et Quitté 2011], [Messing et Reiner 2013].

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.

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

Esquisse de démonstration lorsque $k=\mathbb{Z}$. Il s'agit de montrer que si un nombre premier p ne divise pas tous les a_i ni tous les b_j alors, il ne divise pas tous les $c_r=\sum_{i+j=r}a_ib_j$. Or, si i et j sont *minimaux* tels que $a_i,b_j\perp p$, le coefficient c_{i+j} est la somme de a_ib_j et de termes $a_{i'}b_{j'}$ avec $i'<i$ ou $j'<j$ donc divisibles par p. Il est donc premier à p. □

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

¶ *Cas général, 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 $p_0, \ldots, p_n$ et des $q_0, \ldots, q_m$ pour lesquels $\sum_{i=0}^{n} a_ip_i = 1$ et $\sum_{j=0}^{m} b_jq_j = 1$, alors, il existe des $r_0, \ldots, r_{n+m}$ tels que $\sum_{l=0}^{n+m} c_lr_l = 1$, où les $c_l := \sum_{i+j=l} a_ib_j$ sont les coefficients du produit fg. Un instant de réflexion nous convainc qu'il suffit de démontrer que l'idéal I de l'anneau

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

engendré par les éléments $(\sum_i A_iP_i) - 1$, $(\sum_j B_jQ_j) - 1$ et les $C_k := \sum_{i+j=l} A_iB_j$, 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 $f := \sum_i a_iT^i \in S[T]$ et $g := \sum_j b_jT^j$. 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 $\sum_i a_ip_i = 1 = \sum_j b_jq_j$). 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 $s \in S\setminus\{0\}$ 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 $f = a_nT^n + a_{n-1}T^{n-1} + \cdots + a_0 \in k[T]$ non nul est diviseur de zéro si et seulement si il existe $\lambda \neq 0$ dans k tel que $\lambda f = 0$.*

(On pourra comparer ce résultat avec [Watkins 2007, th. 12.2].)

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

Remarque. ¶ Le lemme de Gauß signifie que l'ensemble $\mathscr{P} \subseteq k[T]$ des polynômes primitifs est un sous-monoïde (multiplicatif) de sorte que l'on peut définir le localisé $k(T) := k[T][\mathscr{P}^{-1}]$ par un calcul de fractions (§3.4.2). D'après le lemme de McCoy-Nagata, les éléments de $\mathscr{P}$sont réguliers ; il en résulte que le morphisme de localisation $k[T] \to k(T)$ est injectif. L'anneau $k(T)$ est appelé « gonflement » ou « localisation de Nagata » de k. (Si k est un corps, $k(T)$ est le corps des fractions rationnelles à coefficients dans k.)

Nous utiliserons le lemme de Gauß dans la section suivante pour montrer notamment que l'anneau $\mathbb{Z}[T]$ est *factoriel*.

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

$$A \cdot \big(1 - \sum_{i=0}^{n} A_iP_i\big) + B \cdot \big(1 - \sum_{j=0}^{m} B_jQ_j\big) + \sum_{l=0}^{n+m} E_lC_l = 1_{\mathbb{Z}},$$

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.)

5. Factorisations et conditions de finitude

5.1. Factorialité et principalité.

Références : [Jacobson 1985, §2.14, §2.16], [Artin 1991, chap. 11], [A. Douady et R. Douady 2005, §3.2, 3.7], ¶[Samuel 1968] (bref survol) et ¶[Lombardi et Quitté 2011, XI.§1-3] pour une autre approche.

La définition ci-dessous est une généralisation de la propriété bien connue de l'anneau $\mathbb{Z}$ des entiers relatifs.

5.1.1. Définition. *Un anneau intègre A est dit* ***factoriel*** *[唯一因子分解整环] s'il existe un ensemble $\mathscr{P}$ d'éléments de A tel que tout élément $a \neq 0$ s'écrive* de façon unique *comme un produit*

$$a = u \cdot \prod_{p \in \mathscr{P}} p^{v_p(a)},$$

où $u \in A^\times$ et les $v_p(a)$ sont des entiers $\geqslant 0$ presque tous nuls.

Commençons par établir quelques conséquences de cette propriété.

5.1.2. Pour chaque $p \in \mathscr{P}$, l'application $v_p : A - \{0\} \to \mathbb{N}$, $a \mapsto v_p(a)$ transforme produit en somme et $a \neq 0$ divise $b \neq 0$ si et seulement si pour tout $p \in \mathscr{P}$, on a $v_p(a) \leqslant v_p(b)$. Il en résulte que deux éléments non nuls ont un **plus grand diviseur commun** (PGCD) et un **plus petit multiple commun** (PPCM) [最小公倍数], que l'on peut définir par les formules suivantes :

$$a \wedge b = \prod_p p^{\min\{v_p(a), v_p(b)\}} \text{ et } a \vee b = \prod_p p^{\max\{v_p(a), v_p(b)\}}.$$

(Ces éléments de A dépendent, à une unité près, de l'ensemble $\mathscr{P}$; cf. *infra*.)

Prendre garde au fait qu'en général, on a seulement l'inclusion entre les idéaux $(a, b) \subseteq (a \wedge b)$: dans $\mathbb{Q}[X, Y]$, on a $(X, Y) \subsetneq (X \wedge Y) = \mathbb{Q}[X, Y]$.

5.1.3. Un élément $p \in \mathscr{P}$ est nécessairement **irréductible** [不可约] : toutes ses décompositions en produit ab sont triviales au sens où l'un des deux facteurs a, b est une unité. Il satisfait même la propriété en général plus forte suivante : si $p \mid ab$, on a $p \mid a$ ou $p \mid b$. (On dit que p est un élément **premier**.) En termes d'idéaux, $(p) = Ap$ est *maximal parmi les idéaux principaux*, c'est-à-dire de la forme (a), pour $a \in A$ — car p est irréductible — et est même un idéal *premier* — car p est premier —. Ainsi, l'ensemble d'idéaux (p), $p \in \mathscr{P}$, est exactement l'ensemble des idéaux ($\neq 0$) premiers principaux de l'anneau intègre A. Il en résulte que l'ensemble $\mathscr{P}$ est uniquement caractérisé par la propriété de la définition ci-dessus, à multiplication par des unités près. (On utilise le fait que dans un anneau *intègre*, l'égalité $(a) = (b)$ force l'existence d'une unité $u \in A^\times$ telle que $b = ua$.)

Comment montrer qu'un anneau intègre donné est factoriel ?

5.1.4. Commençons par chercher des conditions suffisantes pour l'*existence* d'une factorisation en irréductibles ; la question de l'unicité est plus délicate (et moins souvent satisfaite en pratique). Fixons a. Trouver un diviseur non trivial de a revient à trouver un b tel que $(a) \subsetneq (b) \subsetneq A$: on a alors $a = bb'$ et l'on peut alors s'interroger sur la possibilité de factoriser b et b', etc. On entrevoit que la question de l'existence d'une factorisation en irréductibles est liée à la non-existence d'une

suite strictement croissante $(a) \subsetneq (b) \subsetneq (c) \subsetneq \cdots$ d'idéaux principaux de A. Une telle propriété, dont on prouve sans difficulté qu'elle est bien suffisante pour obtenir l'existence de factorisations en irréductibles[①], est satisfaite par une large classe d'anneaux, en particulier les anneaux nœthériens introduits ci-après.

Introduisons maintenant une propriété très utile — quoique très restrictive — qui garantit qu'il *n'existe pas* de chaîne strictement croissante

$$(a_1) \subsetneq (a_2) \subsetneq \cdots \subsetneq (a_n) \subsetneq \cdots$$

d'idéaux principaux. Un anneau intègre A est dit **principal** [主理想环] si tout idéal $\mathfrak{a}$ de A est principal : il existe $a \in A$ tel que $\mathfrak{a} = (a)$. Si (a_n) est une suite comme ci-dessus, la réunion $\mathfrak{a} := \bigcup_n (a_n)$ est un idéal de A, donc de la forme (a) pour un $a \in A$. Or, un tel a doit appartenir à l'un des (a_n), ce qui a pour conséquence l'inclusion $\mathfrak{a} = (a) \subseteq (a_n)$. C'est absurde.

Comment montrer qu'un anneau est principal ? Voyons tout d'abord un exemple.

5.1.5. **Proposition.** *Si k est un corps, l'anneau $k[T]$ est principal.*

Par contre, l'anneau $\mathbb{Q}[X, Y]$ — et bien d'autres — n'est pas principal. (Considérer par exemple l'idéal (X, Y).)

Démonstration. Soit $I \subseteq k[T]$ un idéal, que l'on peut supposer non nul. Nous allons montrer que si $f \in I$ est un élément non nul de degré minimal, I est l'idéal principal engendré par f. Si $g \in I$, on peut effectuer la division euclidienne de g par f et écrire $g = uf + v$, avec $\deg(v) < \deg(f)$. (On fait la convention que $\deg(0) = -\infty$ est plus petit que tous les entiers naturels.) Comme $v = g - uf$ appartient lui-aussi à I, on a nécessairement $v = 0$ (par définition de f) et donc $g = uf \in (f)$. CQFD. □

Le même argument, où l'on remplace le degré par la valeur absolue, permet de montrer que l'anneau $\mathbb{Z}$ est principal. Plus généralement, on peut définir la notion d'anneau **euclidien** [欧几里得整环] A, muni d'une fonction $t : A - \{0\} \to \mathbb{N}$ encodant la « taille » des éléments et pour lequel il existe pour tous a, b non nuls une écriture $a = ub + v$ avec $v = 0$ ou $t(v) < t(b)$. Un anneau euclidien est principal.

Revenons maintenant au problème de vérifier qu'un anneau est factoriel.

5.1.6. Nous avons vu que dans un anneau factoriel, un élément irréductible est premier. (On a déjà dit que dans un anneau intègre tout élément premier est irréductible.) Cela suffit, une fois que l'on a l'existence d'une décomposition :

Proposition. *Soit A un anneau intègre dans lequel tout élément non nul s'écrit comme un produit d'une unité et d'éléments irréductibles. L'anneau A est factoriel si et seulement si tout élément irréductible est premier.*

Or, dans un anneau (intègre) principal, tout élément irréductible est premier (voir exercice 27). On a donc :

Théorème. *Un anneau (intègre) principal est factoriel.*

① Voir par exemple [Jacobson 1985, 2.14] ou [Artin 1991, chap. 11, prop. 2.3].

En particulier, si k est un corps, l'anneau $k[T]$ est factoriel : tout polynôme non nul $f \in k[T]$ s'écrit de façon unique comme le produit d'une constante non nulle et d'un produit de polynômes unitaires irréductibles. Qu'en est-il des anneaux *non principaux* $\mathbb{Q}[X,Y]$ ou $\mathbb{Z}[T]$ par exemple ? Ces deux anneaux sont factoriels ; c'est un corollaire d'un résultat général d'après lequel si A est factoriel, il en est de même de $A[T]$.

Remarque. On pourra comparer ce résultat, dû à Gauß, au théorème de Hilbert 5.3.2. ¶ Il faut cependant se garder de croire que la factorialité est aussi stable qu'on pourrait l'espérer par des opérations « naturelles ». Par exemple, si A est factoriel, il n'est pas vrai que l'anneau $A[[T]]$ des séries formelles $\sum_{n\geqslant 0} a_n T^n$ est également factoriel.

Liste des $\mathbb{Z}[\sqrt{d}]$ qui sont euclidiens/principaux/factoriels ? [Goldfeld ; Stark ; [Hardy et Wright 2007, §14.7-9]. Même si $h_k \neq 1$, on peut avoir unicité de la longueur : si et seulement si $h_K = 2$; voir Narkiewicz, chap. IX [th. Carlitz]

5.2. Factorialité de $\mathbb{Z}[T]$.

5.2.1. Dans ce paragraphe, on démontre un cas particulier du théorème de Gauß ; la démonstration du cas général n'est guère plus difficile et ne nous sera pas utile dans ces notes. L'idée principale est simplement de se ramener à la factorialité de $\mathbb{Q}[T]$, connue car c'est un anneau principal.

Pour cela, on commence par comparer les irréductibles ; pour passer de $\mathbb{Q}[T]$ à $\mathbb{Z}[T]$, on « chasse les dénominateurs ».

5.2.2. Proposition. *Un polynôme non constant de $\mathbb{Z}[T]$ est irréductible si et seulement si il est primitif et irréductible dans $\mathbb{Q}[T]$.*

(Ce résultat nous sera également utile pour, *a contrario*, ramener des questions sur les polynômes à coefficients rationnels au cas plus « arithmétique » des polynômes à coefficients entiers.)

Démonstration. Soit f un polynôme non constant irréductible dans $\mathbb{Z}[T]$. Il est nécessaire primitif, sinon on pourrait factoriser le PGCD, non inversible, des coefficients. Pour montrer qu'il est irréductible dans $\mathbb{Q}[T]$, considérons une factorisation $f = g_1 g_2$, avec $g_1, g_2 \in \mathbb{Q}[T]$ non constants. Il existe deux rationnels $c_1, c_2 \in \mathbb{Q}^\times$ 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 (lemme de Gauß, §4.4), de même que f, on a nécessairement $c_1 c_2 \in \mathbb{Z}^\times = \{\pm 1\}$ et $f = \pm G_1 G_2$, qui est une factorisation non triviale de f dans $\mathbb{Z}[T]$. C'est absurde. Réciproquement, si $f \in \mathbb{Z}[T]$ est non constant, primitif et irréductible dans $\mathbb{Q}[T]$, il est irréductible dans $\mathbb{Z}[T]$ car toute factorisation non triviale $f = g_1 g_2$ dans $\mathbb{Z}[T]$ est une factorisation en polynômes non constants qui contredit l'irréductibilité dans $\mathbb{Q}[T]$. □

Il en résulte que les irréductibles de $\mathbb{Z}[T]$ sont : les irréductibles de $\mathbb{Z}$ (c'est-à-dire les $\pm p$, avec p premier) et les polynômes primitifs, irréductibles dans $\mathbb{Q}[T]$.

5.2.3. Remarque. ¶ Soient plus généralement 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. La démonstration précédente montre que si A est *factoriel*, on a la réciproque partielle : f non constant, unitaire (ou plus généralement primitif) irréductible entraîne f_K irréductible. Par contre, f_k n'est pas nécessairement irréductible, même dans les cas les plus simples (voir **7.3.5** et l'exercice 41). 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).

5.2.4. Soit $f \neq 0 \in \mathbb{Z}[T]$. Comme observé dans la démonstration précédente, tout polynôme non constant de $\mathbb{Q}[T]$ est multiple rationnel d'un polynôme primitif de $\mathbb{Z}[T]$, uniquement défini si l'on impose par exemple à son coefficient dominant d'être > 0. (Ce que nous faisons.) Il existe donc une factorisation de f dans $\mathbb{Q}[T]$ en $f = c \cdot \prod_i P_i$, où chaque $P_i \in \mathbb{Z}[T]$ est primitif irréductible, non constant. Nécessairement, $c \in \mathbb{Z}$ car le produit $\prod_i P_i$ est primitif (lemme de Gauß) si bien que c est un PGCD des coefficients de f. L'anneau $\mathbb{Z}$ étant factoriel, on a existence et unicité de la factorisation de c en produit de nombres premiers. Ceci montre l'existence d'une factorisation en produit d'irréductibles. (¶ Comme expliqué ci-dessus, cela résulte aussi du fait que $\mathbb{Z}[T]$ est nœthérien, notion introduite ci-dessous !) Pour terminer de montrer que l'anneau $\mathbb{Z}[T]$ est factoriel, il faut vérifier que l'on a unicité (à une unité près) des P_i. Or, les P_i sont exactement les représentants primitifs (de coefficient dominant > 0) des facteurs irréductibles de f dans $\mathbb{Q}[T]$ qui, eux, sont bien uniques. (Alternativement, on peut établir l'unicité de la décomposition en vérifiant qu'un élément irréductible de $\mathbb{Z}[T]$ est premier.)

5.3. ¶ Conditions de finitude.

Références : [Atiyah et Macdonald 1969, chap. 6-7], ¶[Bourbaki A, VIII, §1], [Lombardi et Quitté 2011, II.§3].

5.3.1. Définition. *Un anneau A est dit* ***nœthérien*** *[诺特环] si pour toute suite croissante $I_0 \subseteq I_1 \subseteq \cdots \subseteq I_n \subseteq I_{n+1} \subseteq \ldots$ d'idéaux de A, il existe un entier n tel que $I_n = I_{n+1}$.*

On peut montrer que cela est équivalent aux propriétés suivantes :

- **(i)** toute suite croissante d'idéaux de A est stationnaire, c'est-à-dire constante à partir d'un certain rang ;
- **(ii)** tout idéal de A est de type fini.

On a le résultat fondamental de stabilité suivant.

5.3.2. Théorème (Hilbert)**.** *Si A est un anneau nœthérien, il en est de même de l'anneau $A[T]$ des polynômes à coefficients dans A.*

Démonstration. Soit J un idéal de $A[T]$. Pour tout entier n, notons J_n le sous-groupe $J \cap A[T]_{\leqslant n}$ de $A[T]$ des éléments de J (nul ou) de degré au plus n et I_n l'ensemble $\{\mathrm{cd}(f) : f \in J_n\}$, qui est un idéal de A si l'on fait la convention que

$\mathrm{cd}(0) = 0$. La suite $(I_n)_n$ est croissante car si $f \in J_n$, le produit $Tf \in J_{n+1}$ est de même coefficient dominant. Par nœthérianité de A, l'idéal $I := \bigcup_n I_n$ de A est engendré par un nombre fini d'éléments : il existe un ensemble fini $F \subseteq J$ tel que $I = (\mathrm{cd}(f), f \in F)$ et, plus précisément, que pour tout n, on ait $I_n = (\mathrm{cd}(f), f \in F \cap J_n)$. Montrons que, sous ces hypothèses, on a $J = (f, f \in F)$. Notons à cet effet J' l'idéal de droite, clairement contenu dans J, et supposons qu'il existe $g \in J \smallsetminus J'$, de degré minimal, noté d. Puisque $\mathrm{cd}(g) \in I_d$, il existe une somme finie $g' := \sum_{f \in F' \subseteq F} a_f T^{d-\deg(f)} f$ de même monôme dominant que g. Par construction $g' \in J'$ et $g - g' \in J \smallsetminus J'$ est de degré $< d$. Absurde. □

5.3.3. Remarque. ¶ Noter que l'on n'établit pas directement la nœthérianité de $A[T]$ telle qu'énoncée dans la définition mais plutôt la condition (équivalente) (ii). Ceci est une incarnation du caractère imparfaitement constructif de la nœthérianité. (Voir [Mines, Richman et Ruitenburg 1988, VIII.§1] pour une discussion.)

5.3.4. Soit k un corps. Pour toute famille $v_1, \ldots, v_n$ de vecteurs d'un k-espace vectoriel V, l'ensemble $\{(x_1, \ldots, x_n) \in k^n : \sum_i x_i v_i = 0_V\}$ des relations entre ces vecteurs est un sous-k-espace vectoriel. Il est donc engendré par un nombre fini d'éléments de k^n. Dans le cas d'un anneau k quelconque, la notion de cohérence permet de garantir un contrôle analogue sur l'ensemble des solutions d'un système linéaire homogène.

5.3.5. Définition. *Un anneau k est dit* ***cohérent*** *[凝聚(环)] si pour toute application k-linéaire $\varphi : k^n \to k^m$, $x \mapsto \sum_i x_i v_i$, correspondant à une matrice $k^{m\times n}$, il existe une application k-linéaire $u : k^s \to k^n$, correspondant à une matrice $k^{n\times s}$, telle que $\mathrm{Ker}(\varphi) = \mathrm{Im}(u)$: un élément $x \in k^n$ satisfait $\sum_i x_i v_i = 0$ si et seulement si il existe $y \in k^s$ tel que $x = u(y)$.*

(On obtiendrait la même condition en ne considérant que les *formes linéaires* $\varphi : k^n \to k$.)

Cette condition est plus faible que la nœthérianité : par exemple, la clôture intégrale $\overline{\mathbb{Z}}$ de $\mathbb{Z}$ dans $\overline{\mathbb{Q}}$, définie en **6.2** ou l'anneau des polynômes $\mathbb{Z}[X_1, \ldots, X_n, \ldots]$ en une infinité de variables, sont des anneaux cohérents non nœthériens. C'est parfois un substitut utile.

On peut montrer qu'un anneau est cohérent si et seulement si les deux conditions suivantes sont satisfaites :

- **(i)** l'intersection de deux idéaux de type fini est de type fini ;
- **(ii)** l'annulateur $\mathrm{Ann}(x) := \{a \in A : ax = \mathbf{0}_A\}$ d'un élément $x \in A$ est de type fini.

(La seconde condition est automatiquement satisfaite si A est intègre.)

6. Algèbres

6.1. 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], ¶[Bhargava et Satriano 2014, §6].

6.1.1. *Polynômes symétriques.* Soient k un anneau et $n \geqslant 1$ un entier. Un polynôme $f \in k[X_1, \ldots, X_n]$ est dit **symétrique** [对称多项式] si pour tout $\sigma \in \mathfrak{S}_n$, le polynôme $\sigma \cdot f := f(X_{\sigma(1)}, \ldots, X_{\sigma(n)})$ est égal à f. En d'autres termes, $f \in \mathrm{Fix}(\mathfrak{S}_n \circlearrowright k[X_1, \ldots, X_n])$, où $\mathfrak{S}_n$ agit sur $k[X_1, \ldots, X_n]$ par $\sigma(X_i) = X_{\sigma(i)}$.

Les **fonctions symétriques élémentaires** [初等对称函数/初等对称多项式] $\sigma_1, \ldots, \sigma_n \in k[X_1, \ldots, X_n]$, définies par l'égalité

$$\prod_{i=1}^{n}(T + X_i) = T^n + \sum_{i=1}^{n} \sigma_i T^{n-i}$$

sont symétriques. Par exemple, $\sigma_1 = X_1 + \cdots + X_n$ et $\sigma_n = X_1 \cdots X_n$; en général, on a

$$\sigma_r := \sum_{1 \leq i_1 < \cdots < i_r \leq d} X_{i_1} \cdots X_{i_r}.$$

Théorème. *L'inclusion $k[\sigma_1, \ldots, \sigma_n] \subseteq \mathrm{Fix}(\mathfrak{S}_n \circlearrowright k[X_1, \ldots, X_n])$ est une égalité : toute fonction symétrique est un polynôme en les fonctions symétriques élémentaires.*

Démonstration. 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. □

Remarques. ¶ Avec un peu de soin cet argument montre même que l'écriture $f = g(\sigma_1, \ldots, \sigma_n)$ est unique : les $(\sigma_i)_{1 \leqslant i \leqslant n}$ sont *algébriquement indépendants* au sens où si $g(\sigma_1, \ldots, \sigma_n) = 0$ alors $g = 0$. On peut également montrer que l'inclusion $A = k[\sigma_1, \ldots, \sigma_n] \to B = k[X_1, \ldots, X_n]$ fait de B un « A-module de type fini », libre de base les $X_1^{e_1} \cdots X_n^{e_n}$ avec $0 \leqslant e_i \leqslant i - 1$. (La notion de *module* est une généralisation de la notion d'espace vectoriel lorsque les scalaires appartiennent à un anneau qui n'est pas forcément un corps : un **A-module** [模] est un groupe abélien M muni d'un morphisme d'anneaux $A \to \mathrm{End}(M)$, $\lambda \mapsto (m \mapsto \lambda \cdot m)$. (En particulier, pour tous $\lambda \in A$ 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 A est un corps —, on dit que M est **libre** [自由] (sur A).)

6.1.2. Soient k un anneau commutatif non nul et

$$f = T^d - a_1 T^{d-1} + a_2 T^{d-2} + \cdots + (-1)^d a_d \in k[T]$$

un polynôme unitaire de degré 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 les $\sigma_r(X_1, \ldots, X_r) - a_r$, $1 \leq r \leq d$:

$$A := k[X_1, \ldots, X_d] / \Big((\sum_i X_i) - a_1, (\sum_{i<j} X_i X_j) - a_2, \ldots, \prod_i X_i - a_n \Big).$$

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.

Remarque. ¶ On peut montrer l'égalité

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

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 l'égalité (‡) du paragraphe 4.2.3.

6.1.3. 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 » $x_1^{e_1} \cdots x_{d-1}^{e_{d-1}} x_d^{e_d}$ avec $e_j \leq d - j$. (En particulier, $e_d = 0$ donc la variable x_d n'apparaît pas dans les éléments de cette base.)

6.1.4. Le morphisme $k \to A$ étant injectif, l'anneau A est non nul (car $k \neq 0$). Il possède donc un idéal maximal $\mathfrak{m}$ (cf. 3.6) : l'anneau A 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 est engendrée comme k-algèbre par l'ensemble R des racines de f dans K (ce que l'on écrit $K = k[R]$). 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, comme nous le verrons dans les paragraphes suivants.

6.2. Éléments entiers.

6.2.1. Soit A une k-algèbre. Pour tout élément $a \in A$, on note $k[a]$ la sous-k-algèbre de A engendrée par a :

$$k[a] := \{ \sum_{i=0}^{n} \lambda_i a^i \ : \ n \geqslant 0, (a_i) \in A^{n+1} \}.$$

A priori, il n'y a *pas* de borne sur l'entier n. Cependant, nous allons voir que si a est **entier** [整(元)] sur k, c'est-à-dire s'il existe $f \in k[T]$ *unitaire* tel que $f(a) = 0$, alors on peut ci-dessus se restreindre aux combinaisons linéaires des a^i pour $i < \deg(f)$. Tout élément de $k[a]$ s'écrit $g(a)$ pour un $g \in k[T]$ (non unique). Faisons la division euclidienne de g par le polynôme f ; c'est possible car f est

unitaire. On a donc $g = uf + v$, où $\deg(v) < \deg(f)$. En évaluant en a, on trouve $g(a) = u(a)f(a) + v(a) = v(a)$ car $f(a) = 0$.

Formellement, on a établi une surjection $k[T]/(f) \twoheadrightarrow k[a]$, $g \mod f \mapsto g(a)$.

6.2.2. Dans le cas particulier important où k est un corps, on peut pour tout élément entier a trouver un f tel que la surjection précédente soit un *isomorphisme*. Considérons à cet effet le morphisme surjectif $k[T] \twoheadrightarrow k[a]$, $g \mapsto g(a)$. Son noyau $I \neq 0$ est un idéal de l'anneau $k[T]$, principal car k est un corps : il existe un polynôme f, que l'on peut supposer unitaire, tel que $I = (f)$. Par propriété universelle du quotient, on a bien :

$$k[T]/(f) \xrightarrow{\sim} k[a].$$

Le polynôme f s'appelle le **polynôme minimal** [极小多项式] de l'élément a : c'est le polynôme unitaire de plus petit degré tel que $f(a) = 0$.

Par exemple, l'élément $\sqrt{2} \in \mathbb{R}$ est entier sur $\mathbb{Q}$, de polynôme minimal $X^2 - 2$. (Il n'y a pas de polynôme de degré 1 à coefficient rationnel l'annulant car ce nombre est irrationnel.)

Une k-algèbre A est dite **entière** [整扩张] sur k si tout élément de A est entier sur k. Lorsque k et A sont des *corps*, on dit plutôt que l'extension est **algébrique** [代数扩张] .

6.2.3. Théorème. *Soient k un anneau et A une k-algèbre. L'ensemble des éléments de A* entiers *sur k est une sous-k-algèbre de A : si a et b sont entiers, $a + b$ et ab sont entiers.*

On appelle cette k-algèbre la **clôture intégrale** [整闭包] de k dans A.

(Le fait que si a est entier, λa le soit pour tout $\lambda \in k$ est évident : si $a^n + c_1 a^{n-1} + \cdots + c_0 = 0$ alors $(\lambda a)^n + \lambda c_1 (\lambda a)^{n-1} + \cdots + \lambda^n c_0 = 0$.)

La démonstration de ce résultat important fait l'objet des deux paragraphes suivants.

6.2.4. *Démonstration de 6.2.3 : cas particulier où k est un corps et A intègre.* Si k est un corps, on peut utiliser les techniques de l'algèbre linéaire usuelle. En particulier, tout k-module=k-espace vectoriel a une base et la notion de dimension est toujours définie.

Si $a \in A$ est entier, alors $k[a]$ est de dimension finie, égale au degré de son polynôme minimal. (Cet entier s'appelle le **degré** de a sur k.) De plus, le sous-anneau $B := k[a]$ de A est intègre (car A l'est) et de dimension finie sur k ; c'est donc un corps. Ceci peut se voir de deux façons différentes. (1) On constate que si $b \in B$ est non nul, la multiplication $B \to B$, $x \mapsto xb$ est une application k-linéaire et injective. Comme B est de dimension finie, cette application linéaire est également surjective et, en particulier, il existe $y \in B$ tel que $yb = 1$. L'élément b est donc inversible. (2) L'anneau B est isomorphe au quotient $k[T]/(f)$, où f est le polynôme minimal de a. Comme B est intègre, l'idéal (f) est *premier*. (C'est tautologique.) Or, dans un anneau principal, un idéal premier est maximal : le quotient est un corps. (Écrire une inclusion $(f) \subseteq (g)$ et conclure.)

On a donc montré que — sous nos hypothèses — $k[a]$ est un corps, que l'on note aussi $k(a)$ pour mettre en valeur ce fait. Soit maintenant $a' \in A$ un autre élément entier. Soit C la sous-k-algèbre $k[a,a'] = B[a']$ de A engendrée par a et a'. Puisque a' est entier sur k, il est *a fortiori* entier sur (le corps) B et C est de dimension finie sur B. D'autre part, B est de dimension finie sur k. Or, on a le fait général suivant, où l'on note $[K : k]$ pour $\dim_k(K)$, etc.

Proposition. *Si $k \to K$ et $K \to L$ sont deux* extensions finies*, c'est-à-dire telles que $[K : k], [L : K] < +\infty$, on a*

$$[L : k] = [L : K][K : k] < +\infty.$$

Ainsi, $C = k[a,a']$ est une extension finie de k et pour chaque $c \in C$, la sous-algèbre $k[c]$ est de dimension finie sur k : la surjection canonique $k[T] \twoheadrightarrow k[c]$ a un noyau non nul et il existe un polynôme unitaire annulant c. On applique ceci à $a + a'$ et aa', qui sont bien deux éléments de C.

Démonstration de la proposition. Soient $y_1, \dots, y_n$ une base de L sur K et $x_1, \dots, x_m$ une base de K sur k. On vérifie immédiatement que la famille $z_{ij} := x_i y_j$, $(i,j) \in [1,m] \times [1,n]$, est une base de L sur k : il suffit de développer l'expression

$$\sum_{j=1}^{n} \lambda_j y_j = \sum_{j=1}^{n} \Big(\sum_{i=1}^{m} \lambda_{ij} x_i \Big) y_j$$

d'un élément de L vu d'abord comme une combinaison linéaire à coefficients λ_j dans K des y_j, puis en exprimant à leur tour les coefficients λ_j comme combinaison k-linéaire des x_i. □

Par exemple, le nombre $z = \sqrt[2]{3} + \sqrt[3]{2} \in \mathbb{R}$, somme des deux réels positifs $\sqrt{3}$, $\sqrt[3]{2}$ entiers sur $\mathbb{Q}$, est entier sur $\mathbb{Q}$. (On parle de **nombre algébrique**.) L'argument précédent permet de voir qu'il est de degré au plus 6 mais ne donne pas, du moins pas immédiatement, de procédé pour *construire* un polynôme annulant z à partir de la donnée de polynômes annulant $\sqrt{3}$ et $\sqrt[3]{2}$ (par exemple $T^2 - 3$ et $T^3 - 2$). La démonstration ci-dessous, qui ne fait pas appel à la notion de dimension, a l'avantage d'être plus constructive.

6.2.5. ¶ *Démonstration de 6.2.3 : cas général (esquisse).* Soient a, b deux éléments de A entiers sur k. On souhaite montrer que $a + b$ et ab sont entiers. Par hypothèse, il existe deux polynômes unitaires $f = X^n + \sum_{i<n} c_i X^i \in k[X]$ et $g = Y^m + \sum_{j<m} d_j Y^j \in k[Y]$ tels que $f(a) = g(b) = 0$. Il en résulte que l'unique k-morphisme $k[X,Y] \twoheadrightarrow k[a,b]$ envoyant X sur a et Y sur b se factorise à travers le quotient $k[X,Y]/(f(X), g(Y))$. On peut donc supposer que A est ce quotient : les classes x et y de X et Y sont entières et l'image d'un élément entier sur k par un morphisme de k-algèbres est entier. Il faut alors montrer que $x + y$ et xy sont entiers sur k. Si on le souhaite, on peut également supposer l'anneau k *intègre*, de corps des fractions que nous notons K[①]. (Cette réduction n'est pas nécessaire

① . En effet, les coefficients des polynômes f et g induisent un morphisme $\mathbb{Z}[C_i, D_j\,; i < n, j < m] \to k$, $C_i \mapsto c_i$, $D_j \mapsto d_j$; le même argument que précédemment nous ramène au cas particulier $k = \mathbb{Z}[C_i, D_j\,; i < n, j < m]$.

mais psychologiquement rassurante lorsque l'on ne connaît pas la théorie des modules.) La k-algèbre $A = k[X,Y]/(f(X), g(Y))$ est contenue dans la K-algèbre $B := K[X,Y]/(f(X), g(Y))$. C'est un K-espace vectoriel de base les $x^i y^j$ pour $i < n, j < m$. (Le même résultat vaut pour A : c'est un k-module libre.) Les applications K-linéaires $u : B \to B$ et $v : B \to B$ de multiplication par $x + y$ et xy, correspondant à deux matrices à coefficients dans le sous-anneau k du corps K. D'après le théorème de Cayley-Hamilton, ces matrices sont annulées par leur polynôme caractéristique, qui est unitaire et à coefficients dans k. Ainsi, on a deux polynômes $P_+, P_\times \in k[T]$ tels que $P_+(u) = P_\times(v) = 0$ (endomorphisme nul de B). C'est équivalent à dire que $P_+(x + y)$ et $P_\times(xy)$ sont nuls. CQFD.

Exemple. Si on applique ce qui précède à $\sqrt[2]{3} + \sqrt[3]{2}$, on trouve que la matrice de l'endomorphisme de multiplication par cet élément est

$$\begin{pmatrix} 0 & 0 & 2 & 3 & 0 & 0 \\ 1 & 0 & 0 & 0 & 3 & 0 \\ 0 & 1 & 0 & 0 & 0 & 3 \\ 1 & 0 & 0 & 0 & 0 & 2 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

Son polynôme caractéristique est $T^6 - 9T^4 - 4T^3 + 27T^2 - 36T - 23$.

6.3. Extensions de corps et clôture algébrique.

6.3.1. *Prolongement des morphismes.* Soient k un corps et K, A deux k-algèbres. On s'intéresse à l'ensemble $\mathsf{Hom}_k(K, A)$ des morphismes de k-algèbres $K \to A$. Commençons par un cas particulier.

Lemme. *Soit $f \in k[T]$. L'application $\varphi \mapsto \varphi(T \mod f)$ induit une bijection*

$$\mathsf{Hom}_k(k[T]/(f), A) \xrightarrow{\sim} \{a \in A : f(a) = 0\}.$$

En particulier, cet ensemble est non vide si et seulement si f a (au moins) une racine dans A.

Corollaire. *Soient k un corps et K/k une extension algébrique. Si chacun des polynômes minimaux sur k des éléments de K ont (au moins) une racine dans A, l'ensemble $\mathsf{Hom}_k(K, A)$ est non vide.*

Démonstration. L'ensemble des morphismes d'une sous-k-algèbre de K vers A est naturellement muni d'un ordre partiel : $\varphi \leqslant \psi$ si φ est une restriction de ψ. Il existe donc — par l'axiome du choix sur la forme du lemme de Zorn — un k-morphisme maximal $K_0 \to A$. (Nécessairement K_0 est un corps : c'est une k-algèbre intègre, entière.) On veut montrer que $K = K_0$. Pour simplifier les notations, on peut supposer que $k = K_0$: A et K sont des K_0-algèbres, K est algébrique sur K_0 et les polynômes minimaux sur K_0 des éléments de K divisent les polynômes minimaux sur k. Or, si $K \neq k$, il existe $x \in K - k$. Comme $k[x] \subseteq K$ est isomorphe à $k[T]/(f)$, où f est le polynôme minimal de x, le lemme précédent et l'hypothèse montrent que $\mathsf{Hom}_k(k[x], A)$ est non vide. Absurde par maximalité. □

6.3.2. Il est naturel de se poser la question suivante : si k est un corps, existe-t-il une k-algèbre A telle que tout polynôme non constant à coefficients dans k ait une racine dans A ? Ou, mieux, soit *scindé* sur A. On a vu en **6.1.2** que pour chaque polynôme (unitaire) non constant f, il existe une k-algèbre scindant f. La construction s'applique à un ensemble quelconque $F \subseteq k[T]$ de polynômes unitaires (non constants) : considérer le quotient de l'algèbre de polynômes $k[X_{f,i}]$, où f parcourt F et $1 \leqslant i \leqslant d$, par les relations $\sigma_j(X_{f,1}, \ldots, X_{f,d}) = a_{f,j} \in k$, défini par $f = X^d + \sum_{j<d}(-1)^j a_{f,j} X^{d-j}$. Cette k-algèbre $\mathrm{Adu}_k(F)$ scinde chaque polynôme de F ; elle est non nulle car il en est ainsi de chaque $\mathrm{Adu}_k(f)$. En particulier, elle se surjecte (Krull ; §**3.6**) sur un *corps*, extension de k, dans lequel chaque polynôme de F est scindé. C'est un corps de décomposition de la famille F de polynômes. Si on applique ce résultat au plus gros F possible, c'est-à-dire à l'ensemble de *tous* les polynômes unitaires non constants, on voit que l'on a répondu positivement à la question.

6.3.3. Soit Ω un corps de décomposition de l'ensemble des polynômes unitaires non constants de $k[T]$, tel que construit au paragraphe précédent. Il satisfait les propriétés suivantes :

- **(i)** Ω/k est une extension *algébrique* ;
- **(ii)** tout polynôme non constant de $k[T]$ est scindé sur Ω.

Un corps satisfaisant ces propriétés est appelé une **clôture algébrique** de k.

La propriété (ii) peut être renforcée de la façon suivante :

- (ii′) tout polynôme non constant de $\Omega[T]$ est scindé.

Il suffit de montrer que tout polynôme irréductible de $\Omega[T]$ est de degré 1 ou, de façon équivalente, que toute extension finie de Ω est triviale. Or, si ω est un élément d'un sur-corps de Ω, algébrique sur Ω, il est aussi algébrique sur k. Son polynôme minimal sur k est scindé dans Ω ; en particulier, $\omega \in \Omega$. CQFD.

Un corps satisfaisant la propriété (ii′) est dit **algébriquement clos** [代数闭(域)]. C'est une propriété *absolue*, c'est-à-dire qui ne fait pas référence à un sous-corps k.

6.3.4. On a vu que pour tout corps k, il existe un sur-corps Ω qui en est une *clôture algébrique*. La construction n'est pas canonique : elle utilise le théorème de Krull, c'est-à-dire le *choix* d'un idéal maximal dans un anneau gigantesque. Il n'est donc pas exclu *a priori* qu'il existe d'autres clôtures algébriques « différentes » : ici, cela voudrait dire non k-isomorphes. Les résultats sur les prolongements des morphismes (**6.3.1**) montrent qu'il n'en est rien : si Ω_1 et Ω_2 sont deux clôtures algébriques de k, il existe des k-morphismes $\Omega_1 \to \Omega_2$ et $\Omega_2 \to \Omega_1$. Ce sont des *isomorphismes*. En effet, (1) l'image d'une clôture algébrique par un k-plongement de corps est une clôture algébrique et (2) toute extension algébrique d'un corps algébriquement clos est triviale.

En résumé, nous avons notamment démontré le théorème suivant, attribué à Steinitz.

6.3.5. **Théorème.** *Soit k un corps. Il existe une clôture algébrique de k, c'est-à-dire un corps algébrique sur k et scindant tous les polynômes non constants de k. D'autre*

part, deux telles clôtures algébriques sont nécessairement k-isomorphes, quoique de façon éventuellement non unique.

Si on omet la condition d'être algébrique sur k, on perd l'unicité. Par exemple, $\mathbb{Q}$ est contenu dans sa clôture intégrale $\overline{\mathbb{Q}}$ dans $\mathbb{C}$ — qui est dénombrable — mais aussi dans le corps algébriquement clos $\mathbb{C}$ — qui est indénombrable —, ce dernier étant inclus dans une clôture algébrique de $\mathbb{C}(T)$, etc.

Remarques. ¶ Il existe d'autres types, importants, de clôtures : la clôture parfaite (ou radicielle) et les clôtures séparables. Nous n'en ferons pas usage ici. Enfin, signalons que la construction de $\mathrm{Adu}_k(f_1, \ldots, f_r)$ à partir de celle des $\mathrm{Adu}_k(f_i)$ pourrait s'expliquer plus naturellement à l'aide de la notion, essentielle, de *produit tensoriel* (fini) de k-algèbres.

6.4. ¶ Discriminant : approche « galoisienne » et cas de la caractéristique 2. Références : [Bourbaki A, V, exercices, §10, n°23] et [Knus et collab. 1998, chap. V, §18.23].

6.4.1. Soient k un corps, $n \geqslant 1$ et $L := k(X_1, \ldots, X_n)$ le corps des fractions rationnelles en les indéterminées $X_1, \ldots, X_n$: c'est le corps des fractions de l'anneau $k[X_1, \ldots, X_n]$. Le groupe symétrique $\mathfrak{S}_n$ agit sur L et il résulte de l'égalité $\mathrm{Fix}(\mathfrak{S}_n \circlearrowright k[X_1, \ldots, X_n]) = k[\sigma_1, \ldots, \sigma_n]$ que l'on a $\mathrm{Fix}(\mathfrak{S}_n \circlearrowright L) = K := k(\sigma_1, \ldots, \sigma_n)$. D'après la remarque faite en **6.1.1**, l'extension L/K est de degré $n!$[①]. Soit $K^+ := \mathrm{Fix}(\mathfrak{A}_n \circlearrowright L)$; le groupe quotient $\mathfrak{S}_n/\mathfrak{A}_n \xrightarrow{\sim} \mathbb{Z}/2\mathbb{Z}$ agit naturellement sur K^+ et on a tautologiquement $\mathrm{Fix}(\mathbb{Z}/2\mathbb{Z} \circlearrowright K^+) = K$. Il en résulte que l'extension K^+/K est de degré au plus 2.

6.4.2. Soit $\delta_{2'} \in k[X_1, \ldots, X_n]$ l'élément $\prod_{1 \leqslant i < j \leqslant n}(X_i - X_j)$. Pour tout $\sigma \in \mathfrak{S}_n$, $\sigma(\delta_{2'}) = \varepsilon_{2'}(\sigma) \cdot \delta_{2'}$, où $\varepsilon_{2'} : \mathfrak{S}_n \twoheadrightarrow \{\pm 1\} \subseteq k$ est la signature. En particulier,

$$\Delta_{2'} = \delta_{2'}^2 = \prod_{1 \leqslant i < j \leqslant d} (X_i - X_j)^2$$

appartient à $k[\sigma_1, \ldots, \sigma_n]$. C'est le **discriminant** de l'équation générique de degré n (voir remarque en §**6.1.2**). Si la caractéristique de k est différente de 2, il résulte de ce calcul que $\delta_{2'} \in K^+ - K$: il est invariant par le groupe alterné $\mathfrak{A}_n$ mais pas par le groupe symétrique entier $\mathfrak{S}_n$. Ainsi, on a

$$\mathrm{Fix}(\mathfrak{A}_n \circlearrowright k(X_1, \ldots, X_n)) = k(\sigma_1, \ldots, \sigma_n)[\delta_{2'}],$$

avec $\delta_{2'}$ racine du polynôme $T^2 - \Delta_2 \in k[T]$.

6.4.3. *Cas de la caractéristique 2.* Il est naturel de se demander si, lorsque k est de caractéristique 2, c'est-à-dire si $1 = -1$, si on a encore l'égalité $[K^+ : K] = 2$ et, le cas échéant, de trouver un élément δ_2 tel que $K^+ = K(\delta_2)$. L'égalité des degrés est vraie et s'explique le plus naturellement dans le langage de la *théorie de Galois* (de même qu'une partie de ce qui précède). On peut vérifier par le calcul[②] que l'élément

$$\delta_2 := \sum_{1 \leqslant i < j \leqslant n} \frac{X_j}{X_i - X_j}$$

① C'est un fait général, connu sous le nom de « lemme d'Artin » : l'extension obtenue en prenant les invariants sous un groupe fini d'automorphisme est de degré le cardinal du groupe.

② Regarder le nombre d'inversions et calculer $\sigma(\delta_2) = \sum_{\sigma(i)<\sigma(j)} \ldots + \sum_{\sigma(i)>\sigma(j)} \ldots$.

appartient à K^+ et que pour tout $\sigma \in \mathfrak{S}_n$, on a $\sigma(\delta_2) = \delta_2 + \varepsilon_2(\sigma)$, où $\varepsilon_2 : \mathfrak{S}_n \twoheadrightarrow \mathbb{F}_2$ est la signature. En conséquence,

$$\Delta_2 := \delta_2(\delta_2 - 1) = \sum_{1 \leqslant i < j \leqslant n} \frac{X_i X_j}{X_i^2 + X_j^2}$$

appartient à K et on a

$$\mathrm{Fix}(\mathfrak{A}_n \circlearrowright k(X_1, \ldots, X_n)) = k(\sigma_1, \ldots, \sigma_n)[\delta_2],$$

avec δ_2 racine du polynôme $T^2 - T - \Delta_2 \in k[T]$.

Remarque. Plutôt que δ_2, on aurait pu considérer l'image dans $k[X_1, \ldots X_n]$ de l'élément $\frac{1}{2}\big(\prod_{i<j}(X_i - X_j) + \prod_{i+j}(X_i + X_j)\big)$. À vérifier !

6.5. ¶ Application des sommes de Gauß : constructibilité à la règle et au compas [圆规].

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

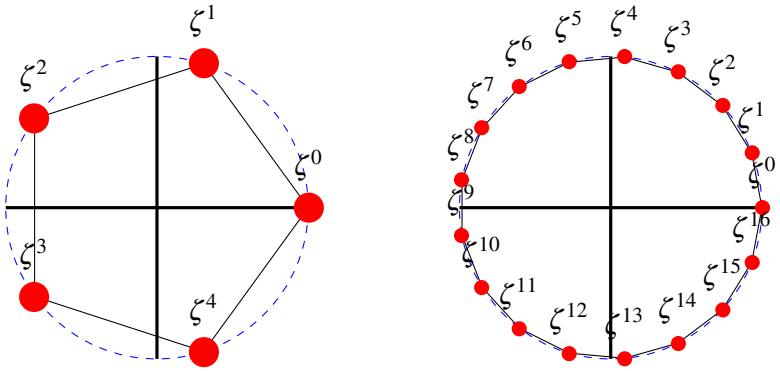
6.5.1. Un nombre complexe $z \in \mathbb{C}$ est dit **constructible** [规矩/可造] s'il existe une suite d'extensions *quadratiques* $\mathbb{Q} = K_0 \subset \cdots \subset K_i \subset K_{i+1} \subset \cdots \subset K_n \subset \mathbb{C}$ telle que $z \in K_n$. (« Quadratiques » : $[K_{i+1} : K_i] = 2$.) En particulier, z est algébrique (sur $\mathbb{Q}$), c'est-à-dire appartient à la clôture algébrique $\overline{\mathbb{Q}}$ de $\mathbb{Q}$ dans $\mathbb{C}$ et, plus précisément, $[\mathbb{Q}(z) : \mathbb{Q}]$ est une puissance de 2 : cela résulte de la multiplicativité du degré des extensions (**6.2.4**). Ces nombres algébriques forment un sous-corps de $\overline{\mathbb{Q}}$. La terminologie vient du fait suivant : un élément 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 $\zeta := \exp(2\pi i/p) \in \mathbb{C}$ une racine primitive p-ième de l'unité. Il résulte de l'irréductibilité du polynôme cyclotomique $\Phi_p := \frac{T^p - 1}{T - 1} = 1 + T + \cdots T^{p-1}$ (exercice 30) 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][①]. Nous allons montrer la réciproque, due à Gauß[②]. En particulier, les polygones réguliers ci-dessous (pentagone et heptadécagone) sont constructibles à la règle et au compas.

---

①. 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 $T^4 + T^3 - T^2 + T - 1$.

②. 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. »



6.5.2. 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 $\mathfrak{g}_\chi$ est constructible. CQFD.

6.5.3. La démonstration précédente permet même de faire des calculs explicites, quoique fastidieux. 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].

① Comparer par exemple avec

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

7. Corps finis : premières définitions et quelques applications

7.1. 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 (**6.1.4**) 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 (**3.7.2**) 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. 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 $\mathbb{F}_2 = \{0, 1\}$.

7.2. ¶ *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.

Ajouter exposé de David et peut-être référence à exercices de Knuth sur $2^{2^n} \otimes 2^{2^n}$.

7.2.1. 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] :

$$x \text{加} y := \mathrm{mex}\left(\{x' \text{加} y : x' < x\} \cup \{x \text{加} y' : y' < y\}\right)$$[②]

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

7.2.2. 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

---

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 $y' < y$.

quant à elle caractérisée par le fait que le produit de deux nimbres distincts de la 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.)

7.2.3. 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

7.2.4. Utilisant les égalités 2^{2^r}乘$2^{2^r} = 2^{2^r}$加$\left(2^{2^{r-1}}\text{乘}2^{2^{r-2}}\text{乘}\cdots\text{乘}2\right)$, 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 $[n]$.

7.3. 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).

7.3.1. Soient K un corps et G un sous-groupe *fini* du groupe multiplicatif $K^\times$. (Noter que c'est un groupe abélien.) Soit n le PPCM des ordres des éléments de G, c'est-à-dire l'*exposant* de G. On a vu en **2.2.1** qu'il existe un élément $x \in G$ d'ordre exactement n.

Pour un tel x, le sous-groupe *cyclique* $\langle x \rangle$ 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 47) $2^{(p-1)/2}$ 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.)

7.3.2. 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 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.

7.3.3. *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.*

7.3.4. *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 » (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 48. Une application « arithmétique » fait l'objet du paragraphe suivant.

7.3.5. *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 $\Phi_p(T+1)$, que ce polynôme est irréductible (cf. exercices 29, 30). 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 $T^p - 1$. 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. □

7.3.6. *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*

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

où les ℓ_i sont des nombres premiers. *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 : $T^{16} - T = T(T+1)(T^2+T+1)(T^4+T+1)(T^4+T^3+1)(T^4+T^3+T^2+T+1)$.

7.4. ¶Fonction zêta et polynômes sans facteur carré dans $\mathbb{F}_p[T]$.
Références : [Rosen 2002, chap. 2], [Mignotte et Ştefănescu 1999, 3.7.3] (fonctions zêta/Zêta, polynômes sans facteur carré) ; [Hardy et Wright 2007, 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).

7.4.1. *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.

7.4.2. *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 $\sum_{a|d} a I_a = p^d$.

7.4.3. *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 55.

Notons que 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.

7.5. ¶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).

7.5.1. 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 $\{1,\dots,d\}$. 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].

7.5.2. *Nombre moyen de racines.* Il est immédiat que le nombre moyen de racines d'un polynôme unitaire de degré $d \geqslant 1$, *comptées sans multiplicités*, est égal à 1. En effet, si X_i, pour $i \in \mathbb{F}_p$, est la variable aléatoire valant 1 si i est racine et 0 sinon, l'espérance à calculer satisfait les égalités :

$$\mathbb{E}(\sum_i X_i) = \sum_i \mathbb{E}(X_i) = p\mathbb{E}(X_0) = p\frac{p^{d-1}}{p^d}.$$

Si l'on tient en compte les multiplicités, un calcul analogue — quoiqu'un peu plus laborieux — donne sauf erreur un nombre moyen égal à $(1-p^{-d})/(1-p^{-1})$.

Remarque. On peut bien sûr se poser la question sur $\mathbb{R}$: on fixe le degré $d \geqslant 1$ et on considère les polynômes $a_0T^d + a_1T^{d-1} + \cdots + a_d$ de degré $\leqslant d$. Si les coefficients a_i sont *indépendants* et suivent une *loi normale standard* (moyenne $\mu = 0$; variance $\sigma^2 = 1$ [pour fixer les idées]), on montre que l'espérance du nombre de racines *réelles* est

$$\frac{1}{\pi}\int_{-\infty}^{+\infty}\sqrt{\frac{1}{(x^2-1)^2} - \frac{(d+1)^2x^{2d}}{(x^{2d+2}-1)^2}}dx \sim_{d\to+\infty} \frac{2}{\pi}\log(d).$$

(Voir [Edelman et Kostlan 1995, §2] pour une démonstration géométrique de la formule intégrale, due à Mark Kac. Si la moyenne des coefficients est non nulle, on a un équivalent en $\pi^{-1}\log(d)$.)

7.6. ¶ Théorème de Chevalley-Warning et suites de de Bruijn.

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

Soient $\mathbb{F}$ un corps fini et $f_1, \ldots, f_e \in \mathbb{F}[T_1, \ldots, T_n]$ 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 $f_1, \ldots, f_e$:

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

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 $P \coloneqq \prod_{i=1}^{e}(1_{\mathbb{F}} - f_i^{\#\mathbb{F}-1}) \in \mathbb{F}[T_1, \ldots, T_n]$, 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 $S_{d_1,\ldots,d_n} \coloneqq$

$\sum_{\underline{t}\in\mathbb{F}^n} t_1^{d_1}\cdots t_n^{d_n}$, 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

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

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 $\mathbb{C}(t)$.

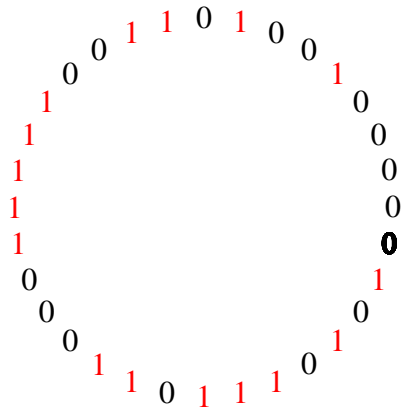
7.6.2. *Suites de de Bruijn.*

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.) 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

$$P = T^r - c_1 T^{r-1} - c_2 T^{r-2} \cdots - c_{r-1} T - c_r \in \mathbb{F}_q[T].$$

(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 $u_0 := \mathbf{0}$, 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 $0\cdots0$ 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].

7.7. Réciprocité quadratique.

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

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

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

ce caractère, qui vaut 1 sur les carrés de $\mathbb{F}_p^\times$ et -1 sinon. (Comme dans le paragraphe précédent, on étend ce caractère multiplicatif à $\mathbb{F}_p$ tout entier en posant $(\frac{0}{p}) = 0$.) Puisque qu'un élément $x \in \mathbb{F}_p^\times$ est un carré si et seulement si $x^{\frac{p-1}{2}} = 1_{\mathbb{F}_p}$, 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 [①] 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 $\{\underline{a} : a_1 + \cdots + a_\ell = 1\} \subseteq \mathbb{F}_p^\ell$ 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 :

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

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

① Lettre grecque « koppa ».

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

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

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 47 pour une démonstration.

Ajouter que c'est multiplicatif : trivial mais à dire !

7.8. ¶ Courbe de Fermat et sphères sur $\mathbb{F}_p$ [esquisse].

Références : [Ireland et Rosen 1990, chap. 8, 10], [Weil 1949].

7.8.1. 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 (**2.2.6**), pour tout $a \in \mathbb{F}_p^\times$ on a l'égalité

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

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 $p + \sum_{\chi_1, \chi_2 \in \widehat{\mathbb{F}_p^\times}[n] \setminus \{1\}} J(\chi_1, \chi_2)$, 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 :

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

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 $c_0 x_0^{n_0} + c_1 x_1^{n_1} + \cdots + c_d x_d^{n_d} = 1$.

7.8.2. 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

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 $c_0 x_0^{n_0} + c_1 x_1^{n_1} + \cdots + c_d x_d^{n_d} = 1$. 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.

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 $\#S^d(\mathbb{F}_p) = p^d + J(,\dots,)$ ($d+1$ 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[①]猜想] démontrées par Alexander Grothendieck ([**SGA 4**], [**SGA 5**]) et Pierre Deligne ([Deligne 1974]).

8. Factorisation des polynômes sur les corps finis et les rationnels

8.1. ¶Abondance des polynômes irréductibles. À titre de motivation, donnons une première application de techniques de réduction modulo p. (Voir aussi par exemple l'exercice 65 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 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 $\mathbb{Z}/P\mathbb{Z}[T] \to \mathbb{F}_{p_1}[T] \times \dots \times \mathbb{F}_{p_r}[T]$ 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 **7.3.6**, 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 $\frac{113897}{130321} = \frac{7\cdot 53\cdot 307}{19^4} \approx 0,87$.

8.2. 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].

① . « 魏尔 »

8.2.1. 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 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 premier avec irréductible.

8.2.2. *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}

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.

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 $\text{中} : B(f) \xrightarrow{\sim} \prod_i B(f_i^{e_i})$ 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, $f \perp f'$, se teste algorithmiquement par l'algorithme d'Euclide (voir aussi §**4.2**) 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 $\text{中}(y)$ 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 $\text{中}(y)$ 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 PGCD($f, t-1$) (resp. 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 $1, t, t^2, \ldots, t^4$ de $\mathbb{F}_2[T]/(f)$, en calculant successivement $T^2, T^4, \ldots, T^8$ 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.

8.3. Factorisation sans facteur carré.

Référence : [Gathen et Gerhard 2003, 14.6].

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*.

8.3.1. 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 $f_i' \neq 0$.)

8.4. 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].

8.4.1. *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 $\mathbb{Q}[T]$).

8.4.2. 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.

8.4.3. 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 $f_{13} = (T+6)(T^2 - 4T + 6)(T^2 -$

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.

$2T - 4$) montre immédiatement que f est irréductible par exemple parce qu'aucun des termes constants n'est inversible.

8.5. Algorithme de factorisation. 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), il existe un lien entre les factorisations modulo p et modulo p^n, $n \geq 1$. C'est ce que nous avons fait en **4.3**.

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

(2) ($\leftrightarrow$ 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) ($\leftrightarrow$ 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.

8.6. ¶ 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).

8.6.1. *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 $f \in \mathbb{Q}[X_0, \ldots, X_n]$. 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 »)

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

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.

8.6.2. *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 $x_1, \ldots, x_d$ les racines distinctes de f dans K (uniques à numérotation près). Pour tout sous-groupe $G \leq \mathfrak{S}_d$, posons

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

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 $k[X, \Lambda_1, \ldots, \Lambda_d]$) est appelé **groupe de Galois** [伽罗瓦群] du polynôme f. Le morphisme (injectif) de restriction $\mathrm{Aut}_k(K) \to \mathfrak{S}_d$, $\sigma \mapsto \sigma_{|\{x_1,\ldots,x_d\}}$, 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.

8.6.3. *Reformulation.* Le groupe de Galois $\mathrm{Gal}(f \,/\, k)$ de f est conjugué au stabilisateur d'un facteur irréductible $h \in k[X, \Lambda_1, \ldots, \Lambda_d]$ de la résolvante de Kronecker, où l'action de $\mathfrak{S}_d$ se fait par permutation des (indices des) Λ_i, $i = 1, \ldots, d$[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.

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, $\mathrm{Gal}(T^3 + T^2 - 2T - 1 \;/\; \mathbb{Q}) = \mathbb{Z}/3\mathbb{Z}$.

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.

8.6.4. *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 $\mathbb{K} := \mathrm{Frac}(A/\mathbb{0})$ et $\mathbb{F} := A/\mathbb{p}$ 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 $s = 1$.

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.

SGA 4½ — Pierre Deligne (1977). *Cohomologie étale.* Lecture Notes in Mathematics **569**. Avec la collaboration de J.-F. Boutot, A. Grothendieck, L. Illusie et J.-L. Verdier. Springer-Verlag, iv+312 pages.

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.

Autres références

Apéry, François et Jean-Pierre Jouanolou (2006). *Résultant et sous-résultants. Le cas d'une variable*. Hermann, x+477 pages (↑ p. 19).

Artin, Michael (1991). *Algebra*. Prentice Hall, xviii+618 pages (↑ p. 3, 25, 26).

Atiyah, Michael F. et Ian G. Macdonald (1969). *Introduction to commutative algebra*. Addison-Wesley, ix+128 pages (↑ p. 28).

Baez, John C. et Michael Shulman (2010). « Lectures on *n*-categories and cohomology ». *Towards higher categories*. **152**. IMA Vol. Math. Appl. Springer, 1–68 (↑ p. 5).

Bhargava, Manjul et Matthew Satriano (2014). « On a notion of "Galois closure" for extensions of rings ». *J. Eur. Math. Soc. (JEMS)* **16**.(9), 1881–1913 (↑ p. 29).

Breen, Lawrence (2010). « Notes on 1- and 2-gerbes ». *Towards higher categories*. **152**. IMA Vol. Math. Appl. Springer, 193–235 (↑ p. 5).

Buhler, J. P. et P. Stevenhagen, éds. (2008). *Surveys in algorithmic number theory*. Mathematical Sciences Research Institute Publications **44**. Cambridge University Press, x+652 pages.

Cartan, Henri (1961). *Théorie élémentaire des fonctions analytiques d'une ou plusieurs variables complexes*. Hermann, 232 pages (↑ p. 15, 45).

Chevalley, Claude (1935). « Démonstration d'une hypothèse de M. Artin ». *Abh. Math. Sem. Univ. Hamburg* **11**.(1), 73–75 (↑ p. 48).

Cohen, Henri (1993). *A course in computational algebraic number theory*. Graduate Texts in Mathematics **138**. Springer-Verlag, xii+534 pages (↑ p. 57).

Conway, John Horton (2001). *On numbers and games*. 2e éd. A K Peters, xii+242 pages (↑ p. 39).

Cox, David A. (2004). *Galois theory*. John Wiley & Sons, xx+559 pages (↑ p. 37, 40, 59).

Davenport, Harold (2000). *Multiplicative number theory*. 3e éd. Graduate Texts in Mathematics **74**. Springer-Verlag, xiv+177 pages (↑ p. 11, 37).

Deligne, Pierre (1974). « La conjecture de Weil. I ». *Publications mathématiques de l'IHÉS* **43**, 273–307 (↑ p. 53).

– (1980). « La conjecture de Weil. II ». *Publications mathématiques de l'IHÉS* **52**, 137–252 (↑ p. 47).

Diaconis, Persi et Ron Graham (2012). *Magical mathematics*. The mathematical ideas that animate great magic tricks. Princeton University Press, xiv+244 pages (↑ p. 49).

Douady, Adrien et Régine Douady (2005). *Algèbre et théories galoisiennes*. Cassini (↑ p. 3, 10, 25, 69).

Edelman, Alan et Eric Kostlan (1995). « How many zeros of a random polynomial are real ? ». *Bull. Amer. Math. Soc.* **32**.(1), 1–37 (↑ p. 48).

Eisenbud, David (2015). « The Amazing Heptadecagon ». Youtube 87uo2TPrsl8 (↑ p. 37).

Flajolet, Philippe et Robert Sedgewick (2009). *Analytic combinatorics*. Cambridge University Press, xiv+810 pages (↑ p. 7, 46, 49).

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 (↑ p. 18, 59).

Gathen, Joachim von zur et Jürgen Gerhard (2003). *Modern computer algebra*. 2e éd. Cambridge University Press, xiv+785 pages (↑ p. 10, 19, 21–23, 49, 53, 56, 57).

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 (↑ p. 37).

– (2005). *Mathematisches Tagebuch, 1796—1814*. 5e éd. Ostwalds Klassiker der Exakten Wissenschaften. Bilingue latin-allemand (avec commentaires en allemand). Verlag Harri Deutsch, 235 pages (↑ p. 37).

Gel'fand, Israel M., Mikhail M. Kapranov et Andrei V. Zelevinskiĭ (1994). *Discriminants, resultants, and multidimensional determinants*. Birkhäuser, x+523 pages (↑ p. 19).

Grothendieck, Alexander (1964). « Formule de Lefschetz et rationalité des fonctions L ». *Séminaire Bourbaki*, exp. nº 279, 41–55 (↑ p. 45).

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 (↑ p. 8, 27, 40, 45).

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] (↑ p. 73).

Hodges, Wilfrid (1979). « Krull implies Zorn ». *J. London Math. Soc.* **19**.(2), 285–287 (↑ p. 17).

Ireland, Kenneth et Michael Rosen (1990). *A classical introduction to modern number theory*. Graduate Texts in Mathematics **84**. Springer-Verlag, xiv+389 pages (↑ p. 8, 11, 37, 51, 52).

Jacobson, Nathan (1985). *Basic algebra. I*. 2e éd. W. H. Freeman and Company, xviii+499 pages (↑ p. 25, 26, 39, 40).

Jech, Thomas J. (1973). *The axiom of choice*. Studies in Logic and the Foundations of Mathematics, Vol. 75. North-Holland, xi+202 pages (↑ p. 17, 69).

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] (↑ p. 73).

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 (↑ p. 47).

Knus, Max-Albert et collab. (1998). *The book of involutions*. American Mathematical Society Colloquium Publications **44**. American Mathematical Society, xxii+593 pages (↑ p. 36).

Lang, Serge (2002). *Algebra*. 3e éd. Graduate Texts in Mathematics **211**. Springer-Verlag, xvi+914 pages.

– (2004). *Algèbre. Cours et exercices*. Traduction française de [Lang 2002]. Dunod, 944 pages (↑ p. 19).

Lebesgue, Henri (1950). *Leçons sur les constructions géométriques*. Gauthier-Villars, vi+304 pages (↑ p. 37).

Lecerf, Grégoire (2013). « Factorisation des polynômes à plusieurs variables ». *Les cours du CIRM* **3**.(1), 1–85 (↑ p. 57).

Lenstra, A. K., H. W. Lenstra Jr. et L. Lovász (1982). « Factoring polynomials with rational coefficients ». *Math. Ann.* **261**.(4), 515–534 (↑ p. 57).

Lenstra Jr., H. W. (1978). « Nim multiplication ». *Séminaire de théorie des nombres, Talence 1977–1978*, exp. nº 11 (↑ p. 39).

– (2008). « Lattices ». Dans [Buhler et Stevenhagen 2008], 127–181 (↑ p. 57).

Lenstra Jr., H. W. et P. Stevenhagen (1996). « Chebotarëv and his density theorem ». *Math. Intelligencer* **18**.(2), 26–37 (↑ p. 59).

Lidl, Rudolf et Harald Niederreiter (1997). *Finite fields*. 2e éd. Encyclopedia of Mathematics and its Applications **20**. Cambridge University Press, xiv+755 pages (↑ p. 49).

Lombardi, Henri et Claude Quitté (2011). *Algèbre commutative (Méthodes constructives)*. Mathématiques en devenir. Calvage & Mounet, xxxi+991 pages (↑ p. 19, 21, 23, 25, 28, 29).

Lyndon, Roger C. et Paul E. Schupp (1977). *Combinatorial group theory*. Ergebnisse der Mathematik und ihrer Grenzgebiete **89**. Springer-Verlag, xiv+339 pages (↑ p. 3).

Mac Lane, Saunders (1963). *Homology*. Die Grundlehren der mathematischen Wissenschaften **114**. Springer-Verlag, x+422 pages (↑ p. 5).

Madore, David A. (2015a). « Le jeu de cartes Dobble et la géométrie projective expliquée aux enfants ». Blog (↑ p. 51).

– (2015b). « Comment faire un jeu de *Tribble* ». Blog (↑ p. 51).

Magnus, Wilhelm, Abraham Karrass et Donald Solitar (1966). *Combinatorial group theory : Presentations of groups in terms of generators and relations*. Interscience Publishers, xii+444 pages (↑ p. 3).

Messing, William et Victor Reiner (2013). « A universal coefficient theorem for Gauss's lemma ». *J. Commut. Algebra* **5**.(2), 299–307 (↑ p. 23).

Mignotte, Maurice et Doru Ştefănescu (1999). *Polynomials. An algorithmic approach*. Springer-Verlag, xii+306 pages (↑ p. 45, 46, 57).

– (2001). « La première méthode générale de factorisation des polynômes. Autour d'un mémoire de F.T. Schubert ». *Rev. histoire math.* **7**.(1), 67–89 (↑ p. 57).

Mines, Ray, Fred Richman et Wim Ruitenburg (1988). *A course in constructive algebra*. Universitext. Springer-Verlag, xii+344 pages (↑ p. 29).

Perrin, Daniel (1996). *Cours d'algèbre*. Ellipse (↑ p. 1, 23).

Pohst, Michael et Hans Zassenhaus (1989). *Algorithmic algebraic number theory*. Encyclopedia of Mathematics and its Applications **30**. Cambridge University Press, xiv+465 pages (↑ p. 29).

Raynaud, Michel (1970). *Anneaux locaux henséliens*. Lecture Notes in Mathematics, Vol. 169. Springer-Verlag, v+129 pages (↑ p. 21).

Rosen, Michael (2002). *Number theory in function fields*. Graduate Texts in Mathematics **210**. Springer-Verlag, xii+358 pages (↑ p. 45).

Rotman, Joseph J. (1995). *An introduction to the theory of groups*. Quatrième édition. Graduate Texts in Mathematics **148**. Springer-Verlag, xvi+513 pages (↑ p. 1, 3, 4).

Šafarevič, Igor R. [Игорю Р. Шафаревичу] (1997). *Basic notions of algebra*. Springer-Verlag, iv+258 pages (↑ p. 1, 3).

Samuel, Pierre (1968). « Unique factorization ». *Amer. Math. Monthly* **75**, 945–952 (↑ p. 25).

Schinzel, Andrzej (2000). *Polynomials with special regard to reducibility*. Encyclopedia of Mathematics and its Applications **77**. Cambridge University Press, x+558 pages (↑ p. 57, 59).

Serre, Jean-Pierre (1978-79). « Groupes finis ». Notes d'un cours à l'ÉNSJF ; `arXiv :0503154v6` (↑ p. 1, 5, 7, 9).

– (1977). *Cours d'arithmétique*. 2e éd. Presses universitaires de France, 188 pages (↑ p. 8, 39, 45, 48).

– (1992). *Topics in Galois theory*. **1**. Research Notes in Mathematics. Jones et Bartlett Publishers, xvi+117 pages (↑ p. 10).

– (2003). « On a theorem of Jordan ». *Bull. Amer. Math. Soc.* **40**.(4), 429–440 (↑ p. 59).

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 (↑ p. 53).

Siegel, Aaron N. (2013). *Combinatorial game theory*. Graduate Studies in Mathematics **146**. American Mathematical Society, xiv+523 pages (↑ p. 39, 40).

Stanley, Richard P. (1999). *Enumerative combinatorics. Vol. 2*. Cambridge Studies in Advanced Mathematics **62**. Cambridge University Press, xii+581 pages (↑ p. 49).

– (2012). *Enumerative combinatorics. Vol. 1*. 2e éd. Cambridge Studies in Advanced Mathematics **49**. Cambridge University Press, xiv+626 pages (↑ p. 45).

Tao, Terence (2009). « Amenability, the ping-pong lemma, and the Banach-Tarski paradox ». blog (↑ p. 69).

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 (↑ p. 48).

– (2015). « Cycles of a random permutation, and irreducible factors of a random polynomial ». blog (↑ p. 46).

Terras, Audrey (1999). *Fourier analysis on finite groups and applications*. London Mathematical Society Student Texts **43**. Cambridge University Press, x+442 pages (↑ p. 10).

Waerden, Bartel Leendert van der (1937). *Moderne Algebra. Erster Teil*. 2e éd. Springer-Verlag, x+272 pages (↑ p. 59).

Watkins, John J. (2007). *Topics in commutative ring theory*. Princeton University Press, xii+215 pages (↑ p. 24).

Weil, André (1949). « Numbers of solutions of equations in finite fields (Œuvres [1949b]) ». *Bull. Amer. Math. Soc.* **55**, 497–508 (↑ p. 52).

– (1974). « La cyclotomie jadis et naguère ». *Séminaire Bourbaki*, exp. no 452 (↑ p. 11).

Exercices

Groupes

Exercice 1. Soient p un nombre premier et G un p-groupe. Montrer que le **centre** $Z(G) \coloneqq \{g \,:\, \forall x, gx = xg\}$ de G est un sous-groupe *non trivial.*

(*Indication : on pourra utiliser* ***1.9.2*** *à G agissant sur lui-même par conjugaison.*)

Exercice 2. Faire la liste, à isomorphisme près, des groupes de cardinal inférieur ou égal à 10. Combien ne sont pas abéliens ?

Exercice 3. Si G est un groupe abélien, tous ses sous-groupes sont distingués. La réciproque est-elle vraie ?

(*Indication : on pourra regarder des groupes de petits ordres pour se faire une idée de la réponse.*)

Exercice 4. Montrer que tout sous-groupe de $\mathbb{Z}$ est de la forme $n\mathbb{Z}$ pour un unique entier $n \geqslant 0$. En déduire que les quotients finis de $\mathbb{Z}$ sont les groupes $\mathbb{Z}/n\mathbb{Z}$.

Exercice 5. Soit G un groupe fini de cardinal n.

- **(i)** Montrer qu'il existe une suite $(a_1, \ldots, a_m)$ telle que $\langle a_1, \ldots, a_m\rangle = G$ et $a_i \notin \langle a_1, \ldots, a_{i-1}\rangle$ pour tout $1 \leqslant i \leqslant m$.
- **(ii)** Montrer que $2^m \leqslant n$ et en déduire que $\#\mathrm{Aut}(G) \leqslant n^{\log_2(n)}$.

Exercice 6. Soit $f : G \to G'$ un morphisme de groupes. Montrer que s'il est *simplifiable à gauche* — c'est-à-dire si pour tout groupe T, l'application $\mathrm{Hom}(T, G) \to \mathrm{Hom}(T, G')$, $\varphi \mapsto f \circ \varphi$ est injective — alors le morphisme f est injectif.

Exercice 7. Montrer que l'on peut plonger tout groupe fini G d'ordre n dans le groupe orthogonal $\mathbf{O}(n, \mathbb{R})$.

(*Indication : si $G \leqslant \mathrm{GL}(n, \mathbb{R})$, on pourra considérer la forme quadratique définie positive q obtenue en faisant la « moyenne » (sur G) des formes quadratiques translatées $q_g \coloneqq g \cdot \|\|^2$, de la forme quadratique usuelle $\sum_i x_i^2$ sur $\mathbb{R}^n$.*)

Exercice 8. Soit $T \subseteq \mathfrak{S}_n$ un *ensemble* de transpositions, c'est-à-dire de permutations (a, b) échangeant deux éléments $a \neq b$ et laissant invariants les autres. On associe à T un graphe G_T sur $\{1, \ldots, n\}$ de la façon suivante : x et y sont liés par une arête si et seulement si ($x \neq y$ et) la transposition (x, y) appartient à T.

Montrer que $\langle T\rangle = \mathfrak{S}_n$ si et seulement si le graphe G_T est *connexe* : pour tous $x \neq y$, il existe un chemin joignant x à y.

Exercice 9. Soient G un groupe fini, H un sous-groupe et E le G-ensemble G/H. Montrer que le cardinal de $\mathrm{Aut}_{G\text{-}\mathrm{Ens}}(E)$ est au plus $(G : H)$ avec égalité si et seulement si $H \lhd G$.

Exercice 10.

- **(i)** Soit $R \in M_n(\mathbb{R})$ une matrice non nulle *à coefficients entiers* et $M = \mathrm{Id} + 3R$. Montrer $M^3 \neq \mathrm{Id}$.
- **(ii)** Montrer que pour tout $n \geq 1$, $M^n \neq \mathrm{Id}$.
- **(iii)** En déduire qu'il existe un nombre fini de classes d'isomorphismes de sous-groupes finis de $\mathrm{GL}_n(\mathbb{Z})$.

Exercice 11. 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 ?

Exercice 12. Soient G un groupe fini et H un sous-groupe strict. Montrer que l'inclusion $\bigcup_{g\in G} gHg^{-1} \subseteq G$ est stricte : G n'est pas recouvert par les conjugués de H.

(*Indication : on pourra montrer que* $\bigcup_g \left(gHg^{-1} - \{e\}\right)$ *est de cardinal au plus* $(G : H) \times (\#H - 1)$.)

Exercice 13. Soit M l'ensemble des mots de longueur $\geqslant 0$ construits sur les 4 lettres à, á, ù, ú. On note ε le mot « vide » de longueur nulle. On munit M d'une loi de composition interne $M \times M \to M$, envoyant (m_1, m_2) sur $m_1 \cdot m_2 \coloneqq m_1 m_2$. Par exemple ùà · á = ùàá et àà · ε = àà. Un mot de M est dit **réduit** s'il ne contient aucun des 4 sous-mots suivants : àá, áà, ùú, úù. On dit qu'un mot réduit $\overline{m}$ est une **forme réduite** de $m \in M$ s'il s'obtient en effectuant une suite finie d'effacements de ces 4 motifs à partir de m. Par exemple, úá est une forme réduite de úáúùàá.

- **(i)** Montrer que, bien qu'il y ait en général plusieurs façon de procéder aux effacements, tout mot possède une *unique* forme réduite.
- **(ii)** En déduire que l'ensemble des mots réduits, muni du produit $m_1 \times m_2 = \overline{m_1 \cdot m_2}$ est un groupe, d'élément neutre ε, pour lequel $\grave{a}^{-1} = \acute{a}$, etc.

Exercice 14.

- **(i)** Soit $L = \langle a, b\rangle$ le groupe libre à deux générateurs. Montrer qu'il existe une décomposition paradoxale de L au sens suivant : $L = E_1 \amalg E_2 \amalg E_3 \amalg E_4$ avec $L = E_1 \amalg aE_2$ et $L = E_3 \amalg bE_4$.
- **(ii)** Soient $\varphi, \psi \in \mathrm{SO}_3(\mathbb{R})$ agissant : trivialement sur respectivement l'axe $\mathbb{R}e_3$ des z et l'axe $\mathbb{R}e_1$ des x ; par une rotation d'angle θ satisfaisant $\cos(\theta) = \frac{1}{3}$ sur l'orthogonal.
  - (a) Écrire les matrices de φ et ψ dans la base canonique.
  - (b) Soit w un produit de longueur arbitraire des 4 rotations $\varphi, \varphi^{-1}, \psi, \psi^{-1}$. Montrer que $w(1, 0, 0)$ est de la forme $\frac{1}{3^n}(a, b\sqrt{2}, c)$, où a, b, c et n sont des entiers.
  - (c) Montrer que si w est sans simplification, c'est-à-dire sans $\varphi^{\pm}\varphi^{\mp}$ ou $\psi^{\pm}\psi^{\mp}$ consécutifs, et se termine par $\varphi^{\pm 1}$, alors b est non nul.

Il existe donc un sous-groupe libre à deux générateurs dans $\mathrm{SO}_3(\mathbb{R})$ et un tel groupe (dénombrable) est « paradoxal ». Ceci permet de démontrer le fameux *paradoxe de Banach-Tarski*. Voir [Tao 2009], [Jech 1973, §1.3] ou [A. Douady et R. Douady 2005, exercice 5, p. 4-5] pour des détails.

Anneaux

Exercice 15. Soit A un anneau non nécessairement unitaire et considérons $A' = \mathbb{Z} \times A$ muni de l'addition terme à terme et de la multiplication $(n, a) \times (m, b) = (nm, nb{+}ma{+}ab)$. Montrer que A' est un anneau unitaire et que A est naturellement un idéal de A'.

Exercice 16. Montrer qu'il y a 4 classes d'isomorphie d'anneaux de cardinal 4.

Exercice 17. Montrer que le sous-ensemble $\mathbb{Z}[s^{-1}]$ de $\mathbb{Q}$ considéré en **3.4.2** est bien un *sous-anneau*.

Exercice 18. Soient A un anneau et $s \in S$. Notons $S \subseteq A$ le sous-monoïde $\{s^n : n \in \mathbb{N}\}$ de $(A, \times)$ des puissances de S (avec la convention que $s^0 = \mathbf{1}_A$). Montrer que le localisé $A[S^{-1}]$ (aussi noté $A[1/a]$) est isomorphe comme A-algèbre au quotient $A[T]/(sT - \mathbf{1}_A)$.

Exercice 19. Soient A un anneau et $S \subseteq A$. Montrer que le morphisme $\imath_S : A \to A[S^{-1}]$ est un *épimorphisme*, c'est-à-dire qu'il est simplifiable à droite : si $f \circ \imath_S = g \circ \imath_S$ alors $f = g$.

(On peut montrer que si $a \in A$, il en est de même du morphisme $A \to A[a^{-1}] \times A/(a)$.)

Exercice 20.

(i) Montrer que l'introduction du facteur t dans la construction du localisé d'un anneau (3.4.2) est nécessaire pour que la relation soit *transitive*.

(*Indication : on pourra considérer l'anneau* $A = \mathbb{Z}/12\mathbb{Z}$ *et le monoïde* $S = \langle 2 \rangle = \{1, 2, 4, 8\}$.)

(ii) ¶ L'anneau A est-il du plus petit cardinal possible ?

Exercice 21. Soient A un anneau et $\mathfrak{a}$ un idéal. Posons $S := 1 + \mathfrak{a}$, $B := A[S^{-1}]$ et $\mathfrak{b}$ l'image de $\mathfrak{a}$ par le morphisme canonique $j : A \to B$.

(i) Montrer que $A/\mathfrak{a} \to B/\mathfrak{b}$ est un isomorphisme.

(ii) Montre que pour tout $n, r \geqslant 0$, le morphisme j induit un isomorphisme $\mathfrak{a}^n/\mathfrak{a}^{n+r} \xrightarrow{\sim} \mathfrak{b}^n/\mathfrak{b}^{n+r}$.

Exercice 22.

(i) Soient k un corps, A une k-algèbre et $X := \mathsf{Hom}_{k-\mathtt{Alg}}(A, k)$. Montrer que le morphisme $A \to k^X$, $a \mapsto \hat{a} := \big(\varphi \mapsto \varphi(a)\big)$, appelé *transformation de Gelfand*, est un morphisme de k-algèbres.

Fixons un entier $n \geqslant 1$. Notons G le groupe cyclique $\mathbb{Z}/n\mathbb{Z}$ et considérons le cas particulier où A est la $\mathbb{C}$-algèbre $\mathbb{C}[G]$ des fonctions de $G \to \mathbb{C}$, dont le produit $\star$ est le *produit de convolution*.

(ii) Montrer que l'ensemble X est naturellement en bijection avec le groupe $\widehat{G}$ des caractères de G.

(iii) Montrer que la transformation de Gelfand $A = (\mathbb{C}[G], \star) \to \mathbb{C}^X$, $a \mapsto \hat{a}$, est un isomorphisme de $\mathbb{C}$-algèbres.

(iv) Comprendre le lien avec la transformation de Fourier considérée en §2.

Exercice 23. Montrer qu'un anneau fini A *intègre* est un corps.

Indication : cela revient à montrer que pour tout $a \in A$ *non nul, l'application* $x \mapsto ax$ *est surjective.*

Exercice 24. Soient p un nombre premier et A une $\mathbb{F}_p$-algèbre. Montrer que le produit cartésien A^2, muni des deux opérations :

$$(a, a') \oplus (b, b') := \Big(a + b, a' + b' - \sum_{i=1}^{p-1} \frac{(-1)^i}{i} a^i b^{p-i}\Big)$$

et

$$(a, a') \otimes (b, b') := (ab, a'b^p + b'a^p)$$

est un anneau commutatif[①]. Est-ce une $\mathbb{F}_p$-algèbre ?

Polynômes et factorialité

Exercice 25. Soient a, b deux entiers $\leqslant n$. Donner un majorant du nombre maximal de boucles effectuées dans l'algorithme d'Euclide pour calculer le PGCD de a et b.

Exercice 26. Comprendre la démonstration de la proposition du §**4.4**.

Exercice 27. Montrer que dans un anneau principal, un élément irréductible est premier.

Exercice 28. Donner des contre-exemples aux implications possibles entre « $f \in A[T]$ irréductible », « $f_K \in K[T]$ » irréductible » et « $f_k \in k[T]$ irréductible », dont l'existence a été annoncée en **5.2.3**.

Exercice 29. Soient p un nombre premier et $f = T^d + a_1 T^{d-1} + \cdots + a_d \in \mathbb{Z}[T]$ un polynôme tel que $p \mid a_i$ pour chaque $0 < i \leqslant d$ mais $p^2 \nmid a_d$. Montrer que f est irréductible dans $\mathbb{Q}[T]$. (Il s'agit du « **critère d'Eisenstein** ».)

Exercice 30. Montrer que $\Phi_p := \frac{T^p-1}{T-1} \in \mathbb{Z}[T]$ est irréductible dans $\mathbb{Q}[T]$.
(*Indication : on pourra utiliser le critère d'Eisenstein (exercice précédent).*)

Exercice 31. Montrer que $\mathbb{C}$ est algébriquement clos.
(*Indication : on pourra commencer par montrer que si* $f = 1 + z^r + a_{r+1} z^{r+1} + \cdots + a_n z^n$, *il existe* $z \in \mathbb{C}$ *tel que* $|f(z)| < 1$.)

Exercice 32. 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 33. 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 34. Montrer que dans la définition d'un couple hensélien, le relèvement a de α est nécessairement unique.

Corps finis

① On le note habituellement $W_2(A)$: c'est l'anneau des **vecteurs de Witt** [维特向量] tronqué à l'ordre 2.

Exercice 35. Soit p un nombre premier. Montrer, *sans utiliser le morphisme de Frobenius*, que le polynôme $(1+X)^p - (1+X^p) \in \mathbb{F}_p[X]$ est nul.

Indication : on pourra étudier la fonction polynomiale associée et utiliser le fait que $\mathbb{F}_p^\times$ *est de cardinal* $p-1$.

En déduire une autre démonstration du fait que pour tout $0 < i < p$, on a $\binom{i}{p} \equiv 0 \mod p$.

Exercice 36. Soit p un nombre premier.

(i) Montrer que si $n = a_0 + a_1 p + \cdots + a_r p^r$ est l'écriture de n en base p, la plus grande puissance de p divisant $n\,!$ est d'exposant

$$v_p(n!) = \frac{n - \sum_i a_i}{p-1}.$$

(ii) En déduire que si $0 \leqslant a \leqslant b$, la valuation p-adique $v_p(\binom{a}{b})$ du coefficient binomial est la somme des retenues de l'addition de a avec $b-a$, écrits en base p.

Exercice 37.

(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 $\mathbb{F}_2[T]$.

Exercice 38. 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 $\mathbb{F}_{3^5}^\times$.

Exercice 39. 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 $p \coloneqq \text{car.}(\mathbb{F})$) dont une racine α est primitive et écrire les puissances de α comme un polynôme en α de degré minimal.

Exercice 40. 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.

Exercice 41.

(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* $\mathbb{F}_p$.)

Exercice 42. 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 43. ¶ 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 $r, s \geq 0$.

Exercice 44. Montrer, sans utiliser la formule de Gauß (§7.3.6), que le nombre de polynômes irréductibles unitaires de $\mathbb{F}_p[X]$ de degré ≤ 3 est $\frac{1}{3}p^3 + \frac{1}{2}p^2 + \frac{1}{6}p$.

Exercice 45. Détailler les démonstrations des faits suivants, énoncés en 7.3.

(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 46. 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 47. 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].

Exercice 48. 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 7.3.4.*)

Exercice 49.

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

---

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

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

(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 $(P, X^{p^2} - X) = 1$.

Exercice 51. Montrer que $T^6+T^4+T+1 \in \mathbb{F}_2[T]$ est le produit de trois polynômes irréductibles distincts.

Exercice 52. 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 $d \leq 7$.

Exercice 53.

(i) Démontrer les critères de Butler et Ben-Or énoncés en §**8.2**.

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

Exercice 54. (Amélioration du lemme de §**7.3.5**.) ¶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* $A \coloneqq \mathrm{Adu}_{\mathbb{Z}}(P)$ *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.*)

Exercice 55. ¶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 **7.4.3**.)

Exercice 56. 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.

Exercice 57. (« 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 $\{1, \ldots, e\}$ tel que $2E \subseteq E$.

(i) Montrer que $f(T) \coloneqq \prod_{i \in E}(T - x^i) \in \mathbb{F}[T]$ 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.

Exercice 58. 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

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

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

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

Exercice 59. 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 60. 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 $q - \frac{q-1}{d}$.

Exercice 61. 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 7.7.

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

Exercice 63.

(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 ?

---

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

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

Exercice 64.

(i) Soit p un nombre premier. Quelle est la probabilité qu'un élément de $\mathbb{F}_p^\times$ tiré au hasard 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 tende 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 65. Soit $f \in \mathbb{Z}[T]$ un polynôme unitaire, se réduisant modulo deux nombres premiers distincts en un produit de polynômes irréductibles de degrés $(d_1, \dots, d_r)$ et $(e_1, \dots, e_s)$. 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 $I = \{1, \dots, r\}$ et $J = \{1, \dots, s\}$, alors f est irréductible.

Exercice 66.

(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.

Exercice 67. (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 $\mathbb{F}_p^\times$.

Exercice 68. ¶ Soient $a_1, \dots, a_n \in \mathbb{Z}$ distincts et $n \geq 2$ un entier. Montrer que $(T - a_1) \cdots (T - a_n) - 1$ est irréductible dans $\mathbb{Z}[T]$.

Exercice 69. (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 ?

Examen 2015-2016

Exercice 1.

(a) A-t-on $\mathbb{F}_{32} \subseteq \mathbb{F}_{64}$?
(b) Si oui, quel est le nombre de $\alpha \in \mathbb{F}_{64}$ tels que $\mathbb{F}_{64} = \mathbb{F}_{32}(\alpha)$?

Exercice 2.

(a) Le groupe additif $\mathbb{Z}/16\mathbb{Z}$ peut-il être muni d'une structure de $\mathbb{F}_2$-espace vectoriel ?
(b) Les groupes additifs $\mathbb{Z}/16\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ sont-ils isomorphes ?
(c) L'anneau $\mathbb{Z}/16\mathbb{Z}$ est-il un corps ?

Exercice 3.

(a) Soient $p \neq 2$ un nombre premier et $a \in \mathbb{F}_p^\times$. Montrer que si l'équation $x^2 = a$ admet au moins une solution dans $\mathbb{F}_p$, elle en a exactement 2.
(b) Soit p un nombre premier, congru à 1 modulo 3. Montrer que l'ensemble $\{x \in \mathbb{F}_p \,:\, x^3 = 2\}$ est de cardinal 0 ou 3.

Exercice 4. Soient $p \neq 2$ un nombre premier et $f := T^4 + 1 \in \mathbb{F}_p[T]$.

(a) Calculer le PGCD de f et f'.
(b) En distinguant les 4 cas : p de la forme $8k+1$, $8k+3$, $8k+5$ ou $8k+7$, déterminer le nombre de facteurs irréductibles de f dans $\mathbb{F}_p[T]$ en considérant l'algèbre de Berlekamp $\boldsymbol{B}(f)$ de f.

Exercice 5. Soit $f \in \mathbb{Z}[T]$ tel que les entiers $f(0)$ et $f(1)$ soient impairs, c'est-à-dire congrus à 1 modulo 2.

(a) Montrer que f n'a pas de racine dans $\mathbb{Z}$.
(b) Est-il également vrai que f n'a pas de racine dans $\mathbb{Q}$? Si c'est le cas, le démontrer ; dans le cas contraire, donner un contre-exemple.

Exercice 6.

(a) Trouver les entiers relatifs $a, b \in \mathbb{Z}$ de valeurs absolues minimales tels que $a \equiv 2 \pmod 3$, $a \equiv 4 \pmod 5$ et $b \equiv 2 \pmod 3$, $b \equiv 2 \pmod 5$.
(b) Soit $f := T^5 + T^4 + T^2 + T + 2 \in \mathbb{Z}[T]$. On admet que $f_3 := f \pmod 3 \in \mathbb{F}_3[T]$ et $f_5 := f \pmod 5 \in \mathbb{F}_5[T]$ ont les factorisations en produits de polynômes irréductibles suivantes :
$$f_3 = (T+2)^2(T^3+2T+2) \quad \text{et} \quad f_5 = (T^2+T+1)(T^3+4T+2).$$
En déduire un $g \in \mathbb{Z}[T]$ unitaire de degré 3 qui pourrait diviser f.
(c) Effectuer la division euclidienne de f par g et factoriser f sur $\mathbb{Z}$.
(d) Vérifier que $\omega := \exp(2\pi i/3) \in \mathbb{C}$ est une racine de f.

Examen 2016-2017

Exercice 1. Soit p un nombre premier. Montrer que si $A = \mathbb{Z}$, $K = \mathrm{Frac}(A) = \mathbb{Q}$ et k le quotient $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ de A, aucune des implications suivantes n'est vraie :

- **(i)** si $f \in A[T]$ est irréductible, son image dans $k[T]$ l'est aussi ;
- **(ii)** si l'image de $f \in A[T]$ dans $k[T]$ est irréductible, f l'est aussi dans $A[T]$;
- **(iii)** si $f \in A[T]$ est irréductible, son image dans $K[T]$ l'est aussi ;
- **(iv)** si l'image de $f \in A[T]$ dans $K[T]$ est irrédctible, f l'est aussi dans $A[T]$.

Exercice 2. Soient $d \geqslant 4$ un entier, $f \in \mathbb{Z}[T]$ un polynôme unitaire de degré d et p_1, p_2 deux nombres premiers distincts. On note $f_1 \in \mathbb{F}_{p_1}[T]$ (resp. $f_2 \in \mathbb{F}_{p_2}[T]$) la réduction modulo p_1 (resp. p_2) de f.

Supposons que $f_1 = g_1 h_1$, avec $g_1, h_1 \in \mathbb{F}_{p_1}[T]$ irréductibles de degrés 1 et $d-1$, et $f_2 = g_2 h_2$, avec $g_2, h_2 \in \mathbb{F}_{p_2}[T]$ irréductibles de degrés 2 et $d-2$. Montrer que f est irréductible dans $\mathbb{Z}[T]$.

Exercice 3. Soient k un corps, A une k-algèbre et $x, y \in A$ entiers sur k : on suppose qu'il existe $a, b, c, d \in k$ tels que $x^2 - ax - b = 0 = y^2 - cy - d$. Trouver une matrice 4×4 à coefficients dans k dont le polynôme caractéristique P satisfait l'égalité $P(x + y) = 0$.

(On ne demande pas de calculer ce polynôme.)

(*Indication : on pourra s'inspirer de §6.2.5.*)

Exercice 4. Soit $p > 3$ un nombre premier.

- **(i)** Montrer, *en utilisant la loi de réciprocité quadratique* (§7.7), qu'il existe $x \in \mathbb{F}_p$ tel que $x^2 = -3$ si et seulement si p est congru à 1 modulo 3.
- **(ii)** Donner une démonstration de ce fait *sans utiliser la réciprocité quadratique.*

  (*Indication : on pourra s'inspirer de l'exercice du polycopié sur* $(\frac{2}{p})$ *et du fait que, dans* $\mathbb{C}$, $\sqrt{-3} = i\sqrt{3}$ *s'exprime simplement en terme d'une racine troisième* $j \neq 1$ *de l'unité.*)

Exercice 5.

- **(i)** Soit p un nombre premier. Quelle est la probabilité qu'un élément de $\mathbb{F}_p^\times$ tiré (uniformément) au hasard soit un générateur de ce groupe multiplicatif ?
- **(ii)** ¶ Montrer qu'il existe une suite de nombres premiers (p_n) telle que cette probabilité tende 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 (par une petite généralisation de §7.3.5) et utiliser le fait suivant que l'on admettra :* $\prod_{\ell < x} \left(1 - \ell^{-1}\right) \to 0$ *lorsque* $x \to +\infty$*, où* ℓ *parcourt les nombres premiers.*)

Exercice 6. Soit p un nombre premier.

- **(i)** Expliciter 4 anneaux [commutatifs, unitaires] de cardinal p^2 deux-à-deux non isomorphes.
- **(ii)** Combien d'entre-eux sont des corps ?
- **(iii)** ¶ Montrer que le nombre de classes d'isomorphie d'anneaux de cardinal p^2 est égal à 4.