

有限域
Corps finis
上海/Shanghai, 2017-9^①

Fabrice ORGOGOZO^②.

version : bb0734d 2019-09-17 19:43:37 +0800

<http://fabrice.orgogozo.perso.math.cnrs.fr/articles/Shanghai3.pdf>

TABLE DES MATIÈRES

1. Groupes : rappels
 2. Transformation de Fourier discrète
 3. Anneaux, corps
 4. Polynômes : généralités
 - 4.1. Propriété universelle
 - 4.2. Algorithme d'Euclide et résultant
 - 4.3. Lemme de Gauß
 5. Factorisations et condition de finitude
 - 5.1. Factorialité et primalité
 - 5.2. Factorialité de $\mathbb{Z}[T]$
 - 5.3. ¶ Noëthérianité
 6. Algèbres
 - 6.1. Algèbre de décomposition universelle et corps de décomposition d'un polynôme
 - 6.2. Éléments entiers
 - 6.3. Extensions de corps et clôture algébrique
 - 6.4. ¶ Application des sommes de Gauß : constructibilité à la règle et au compas [圆规]
 7. Corps finis : premières définitions et quelques applications
 - 7.1. Corps finis : existence, unicité
 - 7.2. ¶ Nombres et construction explicite des \mathbb{F}_{2^s}
 - 7.3. Structure de \mathbb{F}_q^\times et applications
 - 7.4. ¶ Théorème de Chevalley-Waring et suites de de Bruijn
 - 7.5. Réciprocité quadratique
 8. Factorisation des polynômes sur les corps finis et les rationnels
 - 8.1. ¶ Abondance des polynômes irréductibles
 - 8.2. Critères d'irréductibilité dans les corps finis \mathbb{F}_q
 - 8.3. Factorisation sans facteur carré
 - 8.4. Bornes explicites sur les coefficients des diviseurs d'un polynôme à coefficients entiers
- Exercices

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

①. Cours (séances de 1h40) : 2017-9-19,20²,21,22²,25,26,27²,28

②. « Fabrice Orgogozo » = 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, exercice n° 2 (partiellement)

cours n° 2. Groupes cycliques, anneaux (premières définitions)

2.1, 3.2, 3.3, 3.4.1, 3.4.2 (anneau intègre), **3.5**, idéaux de \mathbb{Z} et $\mathbb{R}[T]$ (**4.2.1, 5.1.5**)

cours n° 3. Algèbres, corps (premières définitions)

3.6, 3.7.1, isomorphisme $A/\text{Ker}(f) \simeq \text{Im}(f)$, exercice n° 13

cours n° 4. Morphisme de Frobenius, algèbre de décomposition universelle

3.7.2, 6.1.2

cours n° 5. Extensions algébriques, polynômes minimaux

6.2, toute algèbre intègre de dimension finie sur un corps est un corps (variante de l'exercice n° 19)

cours n° 6. Clôture algébrique ; exercices

6.3, exercices n° 26 (d'Albembert-Gauß) et 38, existence de corps à p^2 et p^3 éléments

cours n° 7. Corps finis : existence et unicité

factorialité de $k[T]$ (**5.1, 7.1, 7.3** (énoncés))

cours n° 8. Corps finis : structure du groupe multiplicatif et du groupe des automorphismes

tour de magie (**7.4.2, 7.3.1, 7.3.2, 7.3.3, 7.3.4** ; exercice n° 32 (début + **8.2.1** [Ben-Or]))

cours n° 9. $\mathbb{F}_p = \text{Fix}(\text{Frob}_p \subset \mathbb{F}_q)$ et $[\mathbb{F}_p(x) : \mathbb{F}_p] = \#\{\text{Frob}_p^n(x), n \geq 0\}$

exercices n° 42, 41

cours n° 10. Polynômes cyclotomiques et critère de Butler

définition des $\Phi_n(T) \in \mathbb{Z}[T]$ et réduction modulo p (généralisation de **7.3.5**), cas de Φ_8 ; **8.2.2**

cours n° 11. Résumé du cours, questions et exercices.

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 $\text{Aut}(X)$ — ou $\text{Aut}_{\text{ENS}}(X)$ 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* $g : X \rightarrow X$, c'est-à-dire des applications $g : X \rightarrow X$ telles qu'il existe $h : X \rightarrow X$ satisfaisant $g \circ h = h \circ g = \text{Id}_X$, 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 $g, h \in \text{Aut}(X)$, on a $g \circ h \in \text{Aut}(X)$;
- (ii) (associativité) pour tout triplet $f, g, h \in \text{Aut}(X)$, 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 $g \in \text{Aut}(X)$;
- (iv) (inverse) pour tout $g \in \text{Aut}(X)$, 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 $G \times G \rightarrow G$, $(g, h) \mapsto g \cdot h$ satisfaisant les propriétés (ii)-(iv) précédentes. Un **morphisme de groupes** [群态射/群同态] $f : (G_1, \cdot_1) \rightarrow (G_2, \cdot_2)$ 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 dépend 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 $\text{Aut}(X)$ 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 [omis].

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 $H \leq G$ — si la restriction du produit de $G \times G \rightarrow G$ induit une structure de groupe $H \times H \rightarrow H$ 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 $\text{Aut}_{\text{ENS}}(X)$ 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 $\text{Isom}(X)$ des

isométries de X est un sous-groupe de $\text{Aut}_{\text{Ens}}(X)$; 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 $\text{Aut}_{\text{Ens}}(X)$.

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

$$\text{Ker}(f) := \{g_1 \in G_1 : f(g_1) = e_2\} \leq G_1$$

et

$$\text{Im}(f) := \{f(g_1), g_1 \in G_1\} \leq G_2$$

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

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

1.4. Quotients. Un sous-groupe $H \leq G$ est le noyau d'un morphisme de groupes $f : G \rightarrow G'$ si et seulement si H est un **sous-groupe distingué** [正规子群] (on note $H \triangleleft G$): 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 $f : G \rightarrow G'$ est un morphisme et $h \in \text{Ker}(f)$ 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* $H \triangleleft G$, construire un morphisme $f : G \rightarrow G'$ tel que $\text{Ker}(f) = H$. 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 $gH := \{gh, h \in H\}$ 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] $g \mathcal{R}_H g'$ si et seulement si $gH = g'H$ et la *structure* de groupe sur G' définie par la condition que l'application $G \rightarrow G', g \mapsto gH$ 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 $\mathcal{R} \subseteq E \times E$ est une relation d'équivalence sur un ensemble E , l'ensemble quotient de E par \mathcal{R} , noté E/\mathcal{R} , est par définition l'ensemble des classes d'équivalences, c'est-à-dire les sous-ensembles de E de la forme $\bar{x} := \{y \in E : x \mathcal{R} y\}$, pour un certain x . Ces classes d'équivalence forment une partition de E et on a une application surjective canonique $E \rightarrow E/\mathcal{R}$ envoyant x sur \bar{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, \bar{g} n'est autre que $gH \subseteq G$ et, ensemblistement, G/\mathcal{R}_H est l'ensemble $\{gH, g \in G\}$ des *classes à gauche*.

En particulier, la construction de l'*ensemble quotient* G/\mathcal{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

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

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

1.5. table de multiplication. La donnée d'une loi de composition $G \times G \rightarrow G$ 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 :

·	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.

1.5.1. 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 $\langle g_x : x \in X \rangle$. C'est le **sous-groupe engendré** [生成的子群]. 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 :

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

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

1.6. ¶ 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 :

$$1 \rightarrow F \rightarrow E \rightarrow B \rightarrow 1.$$

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 $(b, f) \cdot (b', f') := (bb', ff')$, 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 $E \rightarrow \text{Aut}(F)$, $x \mapsto (f \mapsto xfx^{-1})$. On en déduit par composition un morphisme $E \rightarrow \text{Aut}(F) \rightarrow \text{Autex}(F)$, où $\text{Autex}(F)$ — aussi noté $\text{Out}(F)$ — est le groupe des **automorphismes extérieurs** [外自同构群], quotient de $\text{Aut}(F)$ par le sous-groupe $\text{Int}(F)$ des automorphismes intérieurs (les conjugaisons). Par définition, le sous-groupe $F \leq E$ est dans le noyau de ce morphisme composé, qui se factorise donc en

$$B \rightarrow \text{Autex}(F).$$

Si F est abélien — auquel cas $\text{Aut}(F) = \text{Autex}(F)$ —, 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].)

1.7. Action de groupes.

1.7.1. Proposition. *Tout groupe est naturellement le sous-groupe d'un groupe de permutations $\text{Aut}_{\text{Ens}}(X)$ d'un ensemble X . Linéarisation : il est aussi naturellement le sous-groupe d'un groupe d'automorphismes $\text{GL}(V)$ 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 $G \rightarrow \text{Aut}_{\text{Ens}}(G)$, $g \mapsto (x \mapsto gx)$ est un morphisme de groupes, injectif. On a donc le résultat attendu avec $X = G$. Comme d'autre part, $\text{Aut}(X)$ s'injecte dans $\text{GL}(V)$, où $V = \mathbb{Q}^{(X)} = \bigoplus_x \mathbb{Q}e_x$, par l'application $\sigma \in \text{Aut}(X) \mapsto (e_x \mapsto e_{\sigma(x)})$, on a également le résultat. \square

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 $\rho : G \rightarrow \text{Aut}_{\text{Ens}}(X)$, pas nécessairement injectif. Pour chaque $g \in G$, on a donc une bijection $\rho(g) : X \rightarrow X$; 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...

- $\text{Fix}(G \curvearrowright X) = \{x \in X : g \cdot x = x, \forall g \in G\}$ 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 ;
- $G_x = \{g \in G : g \cdot x = x\} \leq G$ 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 $G \rightarrow G \cdot x$, $g \mapsto g \cdot x$, 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.

1.7.2. 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 :*

$$\#X \equiv \#\text{Fix}(G \curvearrowright X) \pmod{p}.$$

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. \square

... et un corollaire (théorème de Cauchy).

1.7.3. 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, \dots, 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 $\text{Fix}(\mathbb{Z}/p\mathbb{Z} \curvearrowright G^p)$ est clairement l'ensemble « diagonal » $G \simeq \{(g, g, \dots, g)\} \subseteq G^p$; il en résulte que $\text{Fix}(\mathbb{Z}/p\mathbb{Z} \curvearrowright X)$ 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. \square

1.7.4. Remarques.

- (1) On a en réalité des résultats beaucoup plus forts : si p^r est la plus grande 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 $p \geq 3$ premier fixé, le nombre de permutations σ de \mathfrak{S}_n telles que $\sigma^p = \text{Id}$ est équivalent, lorsque $n \rightarrow +\infty$, à

$$(n/e)^{n(1-p^{-1})} p^{-1/2} \exp(n^{1/p}).$$

Voir référence citée en [FLAJOLET et SEDGEWICK 2009, exemple VIII.12, p. 569].

- (3) Un point clef de la démonstration de 1.7.2 est l'équation aux classes : si $G \subset X$ 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

$$\text{card}(X) = \sum_i \text{card}(\mathcal{O}_i) = \text{card}(G) \times \sum_i \frac{1}{\text{card } G_{x_i}}.$$

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 $\mathbb{Z}/n\mathbb{Z} \simeq G$, $r \pmod n \mapsto g^r$.

Prendre garde au fait que le choix de g n'est pas canonique/intrinsèque : il y a d'autres générateurs de G (sauf si $|G| \leq 2$). 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 $rs \equiv 1 \pmod n$. 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 $rs \equiv 1 \pmod n$. (Nous reviendrons sur ces questions dans la section sur les anneaux.) En d'autres termes :

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 $1 \leq s \perp n \leq n$ 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) $\varphi(n) \rightarrow +\infty$ lorsque $n \rightarrow +\infty$.

Il en résulte que l'on a l'égalité :

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

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 $\mathbb{Z}/nm\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ d'où $(\mathbb{Z}/nm\mathbb{Z})^\times \simeq (\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times$. (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

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

ces multiples inférieurs à p^α est $p^{\alpha-1}$. (iii) Remarquons que si n est une puissance de 2, on a $\varphi(n) = n/2 \geq \sqrt{n}/2$. D'autre part, si $p \geq 3$ est un entier, on a $p-1 \geq \sqrt{p}$ si bien que $p^\alpha(1-p^{-1}) \geq p^{\alpha-1/2} \geq p^{\alpha/2}$ pour tout $\alpha \geq 1$. Par multiplicativité de φ , on a donc la minoration $\varphi(n) \geq \sqrt{n}/2$ pour tout n et, en particulier, $\varphi \rightarrow +\infty$. Des résultats bien plus précis sont établis dans [ibid., 18.4]. \square

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 $\chi : G \rightarrow \mathbb{C}^\times$, 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 $\text{Hom}(G, \mathbb{C}^\times)$ 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 $\bar{1}$.

2.2.3. Remarque. ¶ Soit G un groupe non nécessairement abélien et $f : G \rightarrow A$ 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 $G \twoheadrightarrow G^{\text{ab}} \xrightarrow{f^{\text{ab}}} A$. 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 $\widehat{G} \rightarrow \widehat{H}$ est surjectif.*

Démonstration. Soit $\chi : H \rightarrow \mathbb{C}^\times$ 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 $g \in G \setminus H$. Soit n le plus petit entier > 1 tel que $g^n = h \in H$. Posons $\zeta = \chi(h)$. Pour toute extension $\tilde{\chi}$ de χ à G , on a nécessairement $\tilde{\chi}(g)^n = \zeta$. 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. \square

Il en résulte que si $H \leq G$, on a une suite exacte (voir 1.6) $1 \rightarrow \widehat{(G/H)} \rightarrow \widehat{G} \rightarrow \widehat{H} \rightarrow 1$. 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] $G \rightarrow \mu_n(\mathbb{C})$ prolongeant un isomorphisme arbitraire $C \simeq \mu_n(\mathbb{C})$. (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 $C \rightarrow G \rightarrow C$ soit l'identité. Il est alors formel d'en déduire que G est isomorphe à $C \times \text{Ker}(s)$ car $C \cap \text{Ker}(s) = \{1\}$. On en déduit par récurrence le théorème suivant. (Bien que cela ne soit pas nécessaire, noter que $\text{Ker}(s)$ 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 $\widehat{G}_1 \times \widehat{G}_2 \simeq \widehat{G_1 \times G_2}$ (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 $\text{ev} : G \rightarrow \widehat{G}$, $g \mapsto (\text{ev}_g : \chi \mapsto \chi(g))$ 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 $G[n] := \{g \in G : g^n = 1\}$ 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 $\sum_{\tau \in \widehat{G/nG}} \tau(\bar{g})$, où \bar{g} désigne l'image de g dans G/nG . Cette somme est nulle si $\bar{g} \neq 0_{G/nG}$. \square

(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 $n \geq 1$ un entier et $\mathbf{e} : \mathbb{Z}/n\mathbb{Z} \rightarrow \mu_n(\mathbb{C}) \subseteq \mathbb{C}^\times$, $x \mapsto \exp(2\pi i x/n)$, 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 abrégier $\int f$ la somme finie $\sum_{t \in \mathbb{Z}/n\mathbb{Z}} f(t)$ et définissons le produit hermitien :

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

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

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

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

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

(où δ_{-x} est la « fonction de Dirac » valant 1 en $-x$ et 0 ailleurs) et

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

(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 \mathcal{F} est presque une isométrie involutive :

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

et

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

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

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 :

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

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

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 $\mathbb{F}_p^\times \rightarrow \mathbb{C}^\times$, étendu à \mathbb{F}_p en posant $\chi(0) = 0$. On vérifie immédiatement l'égalité

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

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

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

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 $\bar{\mathfrak{g}}_\chi$ de \mathfrak{g}_χ égal à $\chi(-1)\mathfrak{g}_{\bar{\chi}}$.

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

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

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 :

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

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

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

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

①. Noter les analogies :

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

3. ANNEAUX, CORPS

3.1. Soit X un espace topologique, par exemple une partie de \mathbb{R}^n . Notons $A = \text{Hom}_{\text{Top}}(X, \mathbb{C})$ 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)** [交換环] 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 multiplication^①.

Il résulte formellement des définitions que l'ensemble

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

des **éléments inversibles** [單位] (ou « unités ») d'un anneau (commutatif) A forment un groupe (commutatif). Par exemple, le groupe des unités de l'anneau $\mathbb{Z}/n\mathbb{Z}$ 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 $x^{\varphi(n)} \equiv 1 \pmod n$. Si n est un nombre premier p , cela se réécrit : $x^{p-1} \equiv 1 \pmod p$ pour tout $x \perp p$, ou encore $x^p \equiv x \pmod p$ pour tout $x \in \mathbb{Z}$ (petit théorème de Fermat ; voir aussi 3.7.2 *infra*).

Un **morphisme d'anneaux** $f : A \rightarrow B$ est une application de A dans B induisant un morphisme de groupes additifs $(A, +) \rightarrow (B, +)$ 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 $A \rightarrow \text{End}(B, +)$, $a \mapsto (b \mapsto f(a)b)$ — 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 .)

^①. 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 12.

3.3. Quotients, idéaux.

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

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

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 $\text{Ker}(A) \hookrightarrow A$ n'est pas un morphisme d'anneaux, car $\mathbf{1}_A$ n'appartient pas à $\text{Ker}(A)$, 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 $\text{Ker}(f)$ 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 \bar{a} , soit un morphisme d'anneaux.

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

L'importance de cette construction vient notamment du slogan suivant :

quotienter, c'est forcer des égalités.

Par exemple, on a $2 \neq 0$ dans \mathbb{Z} mais dans $\mathbb{Z}/2\mathbb{Z}$ on a « forcé » l'égalité $2 = 0$. De même, $T^2 + 1 \neq 0$ dans $\mathbb{R}[T]$ mais dans $\mathbb{R}[T]/(T^2 + 1)$ on a « forcé » l'égalité $t^2 + 1 = 0$ (où t est la classe de T). Dans ce dernier cas, on voit que l'on a formellement ajouté à \mathbb{R} une racine carrée de -1 .

3.3.2. 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 :

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

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 $(e_1, \dots, e_n) = e_1 A + \dots + e_n A$. 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,

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

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 20, 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

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

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

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 $L \geq 0$ et des $s_1, s_2, \dots, s_L \in S$ 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 .) 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 \bar{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 17.)

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 $A \rightarrow A[S^{-1}]$, $a \mapsto (a, \mathbf{1}_A)$, 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 $A \rightarrow A[S^{-1}]$ 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 $\text{Frac}(A)$. 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** [分式环] de A .

Pour une description concrète, lorsque S est engendré par un seul élément, voir l'exercice 15.

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 :

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

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

3.5. Théorème chinois [中国剩余定理].

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

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

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

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 \bar{x} et \bar{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 $z := e_1x + e_2y$ est d'image (\bar{x}, \bar{y}) dans le produit des deux quotients.

Revenons au cas général : $n \geq 2$ et procédons par récurrence. Il est clair que la condition *nécessaire* de l'existence, pour chaque $1 \leq j \leq n$, d'un élément $e_j \in A$ d'image $(\mathbf{0}_{A/\mathfrak{a}_1}, \dots, \mathbf{0}_{A/\mathfrak{a}_{j-1}}, \mathbf{1}_{A/\mathfrak{a}_j}, \mathbf{0}_{A/\mathfrak{a}_{j+1}}, \dots, \mathbf{0}_{A/\mathfrak{a}_n})$ 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 , $1 \leq j < n$ ayant les images voulues dans $\prod_{i < n} A/\mathfrak{a}_i$. Admettons un instant que $(\prod_{i < n} \mathfrak{a}_i) + \mathfrak{a}_n = A$. 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 $e_1 := e'_1(\mathbf{1}_A - e_n), \dots, e_{n-1} := e'_{n-1}(\mathbf{1}_A - e_n), e_n$ 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 $\text{Ker } \pi = \bigcap_i \mathfrak{a}_i$ 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 $x \cdot \prod_{j \neq i} \mathfrak{a}_j \subseteq \prod_i \mathfrak{a}_i$. \square

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 $f : A \rightarrow k$ un morphisme d'anneaux, de but un corps k . Il se factorise en (c'est-à-dire s'écrit comme le composé des morphismes) $A \twoheadrightarrow A/\mathfrak{p} \xrightarrow{\simeq} \text{Im}(f) \subseteq k$, où $\mathfrak{p} := \text{Ker}(f)$. 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 $B \subseteq \text{Frac}(B) \hookrightarrow k$, où $\text{Frac}(B)$ 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.

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 $A \rightarrow A/I$ induit par image inverse une bijection entre les idéaux de A/I et les idéaux de A contenant I .

3.7. Caractéristique, Frobenius.

3.7.1. Soit A un anneau. Il existe un unique morphisme d'anneaux $\mathbb{Z} \rightarrow A$; 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 $n \geq 0$ de $\text{Ker}(\mathbb{Z} \rightarrow k)$, appelé **caractéristique** [特征] de k , est nul ou non. On note $\text{car.}(k)$ cet entier. (¶ Il est aussi parfois commode de considérer l'**exposant caractéristique** [特征指数 (?)] du corps k : $\text{exp.car.}(k) := \text{sup}(1, \text{car.}(k))$.)

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

3.7.2. Proposition. L'application $\text{Frob}_p : k \rightarrow k, a \mapsto a^p$ 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 $n \geq 0$, et tout nombre premier p , on a la congruence

$$n^p \equiv n \pmod{p}.$$

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

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

Il suffit donc de montrer que si $0 < i < p$, on a $\binom{p}{i} \cdot \mathbf{1}_A = 0$, c'est-à-dire que la caractéristique p divise l'entier $\binom{p}{i} = \frac{p!}{i!(p-i)!}$. 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 1.7.2. Pour une troisième démonstration, voir l'exercice 29.) \square

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 $k[T_1, \dots, T_n] := k[T_1, \dots, T_{n-1}][T_n]$ (ou encore en considérant $k[\mathbb{N}^n]$); c'est la k -algèbre des polynômes en n variables à coefficients dans k .

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 $k[T_1, \dots, T_n] \rightarrow A$, 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 $cT_1^{d_1} \dots T_n^{d_n} \in k[T_1, \dots, T_n]$ sur la somme des $ca_1^{d_1} \dots a_n^{d_n} \in A$.

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 JOUANLOU 2006], [LOMBARDI et QUITTÉ 2011, III.§7], ¶[GEL'FAND, KAPRANOV et ZELEVINSKIÏ 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 $\text{cd}(f)$ le coefficient dominant de $f = a_d T^d + \dots + a_1 T + a_0$: si $a_d \neq 0$, on pose $\text{cd}(f) := a_d \in k$. Pour tout polynôme $g = b_e T^e + \dots + b_1 T + b_0$, avec $e \geq d$, l'algorithme d'Euclide^① fournit deux polynômes $u, v \in k[T]$ tels que

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

(Rappelons que l'on note $\deg(v)$ le **degré** [次数] d'un polynôme v .) Dans le cas particulier où $\text{cd}(f) = 1$, 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 ,

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

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 $T^{n-1}g, T^{n-2}g, \dots, g$ par f . Ainsi,

$$(\ddagger) \quad \text{rés}(f, g) = \det(\times g : k[T]/(f) \rightarrow k[T]/(f)).$$

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 $\text{rés}_{n,m}(f, g)$ est inversible ;
- les polynômes f et g sont fortement étrangers.

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

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

c'est le **discriminant** [判别式] de f .

Formulaire :

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

4.3. 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 $a_nT^n + a_{n-1}T^{n-1} + \dots + a_0$ 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 $c_r = \sum_{i+j=r} a_i b_j$. Or, si i et j sont *minimaux* tels que $a_i, b_j \not\equiv 0 \pmod{p}$, le coefficient c_{i+j} est la somme de $a_i b_j$ et de termes $a_{i'} b_{j'}$ avec $i' < i$ ou $j' < j$ donc divisibles par p . Il est donc premier à p . \square

¶ *Cas général, sans l'axiome du choix.* On veut montrer que si $f = a_n T^n + a_{n-1} T^{n-1} + \dots + a_0$ et $g = b_m T^m + b_{m-1} T^{m-1} + \dots + b_0$ sont tels qu'il existe des p_0, \dots, p_n et des q_0, \dots, q_m pour lesquels $\sum_{i=0}^n a_i p_i = 1$ et $\sum_{j=0}^m b_j q_j = 1$, alors, il existe des r_0, \dots, r_{n+m} tels que $\sum_{l=0}^{n+m} c_l r_l = 1$, où les $c_l := \sum_{i+j=l} a_i b_j$ sont les coefficients du produit fg . Un instant de réflexion nous convainc qu'il suffit de démontrer que l'idéal I de l'anneau

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

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

Lemme (McCoy-永田=Nagata). *Soit k un anneau commutatif non nul. Un polynôme $f = a_n T^n + a_{n-1} T^{n-1} + \dots + a_0 \in k[T]$ 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 $g = b_m T^m + b_{m-1} T^{m-1} + \dots + b_0$, 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 $a_d g \neq 0$; considérons le plus grand. Il résulte de l'égalité $fg = (a_d T^d + \dots + a_0)g = 0$ que $a_d b_m = 0$, c'est-à-dire que le degré du polynôme $h := a_d g$ est strictement inférieur au degré m de g . Comme $fh = f \times (a_d g) = 0$, on peut conclure par récurrence sur m . \square

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 $A, B, E_0, \dots, E_{n+m} \in R$ tels que

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

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

5. FACTORISATIONS ET CONDITION 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 \mathcal{P} d'éléments de A tel que tout élément $a \neq 0$ s'écrive de façon unique comme un produit*

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

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

Commençons par établir quelques conséquences de cette propriété.

5.1.2. Pour chaque $p \in \mathcal{P}$, l'application $v_p : A - \{0\} \rightarrow \mathbb{N}$, $a \mapsto v_p(a)$ transforme produit en somme et $a \neq 0$ divise $b \neq 0$ si et seulement si pour tout $p \in \mathcal{P}$, on a $v_p(a) \leq v_p(b)$. 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 \mathcal{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 $p \in \mathcal{P}$ 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 $a \in A - \text{car } p \text{ est irréductible}$ – et est même un idéal *premier* – car p est premier –. Ainsi, l'ensemble d'idéaux (p) , $p \in \mathcal{P}$, est exactement l'ensemble des idéaux ($\neq 0$) premiers principaux de l'anneau intègre A . Il en résulte que l'ensemble \mathcal{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 $(a) \subsetneq (b) \subsetneq (c) \subsetneq \dots$ 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 noethériens introduits ci-après.

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

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

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. \square

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 $t : A - \{0\} \rightarrow \mathbb{N}$ 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 22). 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 $\sum_{n \geq 0} a_n T^n$ est également factoriel.

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, §4.3), 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 $\mathbb{Z}/p\mathbb{Z} \leftarrow \mathbb{Z} \hookrightarrow \mathbb{Q}$ 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 35). 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 noëthérien, 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. ¶ Noëthérianité.

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 **noëthérien** [诺特环] si pour toute suite croissante $I_0 \subseteq I_1 \subseteq \dots \subseteq I_n \subseteq I_{n+1} \subseteq \dots$ 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 noëthérien, 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 $J \cap A[T]_{\leq n}$ de $A[T]$ des éléments de J (nul ou) de degré au plus n et I_n l'ensemble $\{\text{cd}(f) : f \in J_n\}$, qui est un idéal de A si l'on fait la convention que $\text{cd}(0) = 0$. 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 noëthérianité de A , l'idéal $I := \bigcup_n I_n$ de A est engendré par un nombre fini d'éléments : il existe un ensemble fini $F \subseteq I$ tel que $I = (\text{cd}(f), f \in F)$ et, plus précisément, que pour tout n , on ait $I_n = (\text{cd}(f), f \in F \cap J_n)$. 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 $g \in J \setminus J'$, de degré minimal, noté d . Puisque $\text{cd}(g) \in I_d$, 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 $g - g' \in J \setminus J'$ est de degré $< d$. Absurde. \square

6. ALGÈBRES

6.1. Algèbre de décomposition universelle et corps de décomposition d'un polynôme.

Références : [ibid., §3.4], [Bourbaki A, IV §6 n°5], [POHST et ZASSENHAUS 1989, §2.2], [BHARGAVA et SATTRIANO 2014, §6].

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

Les **fonctions symétriques élémentaires** [初等对称函数/初等对称多项式] $\sigma_1, \dots, \sigma_n \in k[X_1, \dots, X_n]$, 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, $\sigma_1 = X_1 + \dots + X_n$ et $\sigma_n = X_1 \cdots X_n$; en général, on a

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

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

Démonstration. On munit les monômes de l'ordre lexicographique : $X_1^{a_1} \cdots X_n^{a_n} < X_1^{b_1} \cdots X_n^{b_n}$ (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, \dots, r_n des entiers, considérons le polynôme symétrique $\sigma_1^{r_1} \cdots \sigma_n^{r_n}$: son monôme maximal est $X_1^{r_1+r_2+\dots+r_n} X_2^{r_2+\dots+r_n} \cdots X_n^{r_n}$. 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 $a_1 \geq a_2 \geq \dots \geq a_n$, sans quoi on pourrait permuter deux variables et obtenir un monôme supérieur. Soit r_1, \dots, r_n les (uniques) entiers *positifs* tels que $r_1 + r_2 + \dots + r_n = a_1, r_2 + \dots + r_n = a_2, \dots, r_n = a_n$. 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. \square

6.1.2. Soient k un anneau commutatif non nul et

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

un polynôme unitaire de degré d . Considérons l'**algèbre de décomposition universelle** définie comme le quotient A de l'anneau de polynômes $k[X_1, \dots, X_d]$ par l'idéal engendré par les $\sigma_r(X_1, \dots, X_r) - a_r, 1 \leq r \leq d$:

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

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 $k[X_1, \dots, X_d] \twoheadrightarrow A$. Cette k -algèbre, aussi notée $\text{Adu}_k(f)$ 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 $A \rightarrow B$ 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

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

où x_1, \dots, x_n sont les racines de f dans $\text{Adu}_k(f)$ telles que $f = \prod_i (T - x_i)$: cela résulte de la formule générale $\text{rés}(\prod_i (T - a_i), g) = \prod_i g(a_i)$, 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 $A = \text{Adu}_k(f) \rightarrow \text{Adu}_{k'}(g)$ est un isomorphisme. Ceci entraîne, par récurrence sur le degré d , que le morphisme $k \rightarrow A$ est injectif. ¶ Mieux : le k -module A est libre de rang $d!$, une base étant constituée des « monômes » $x_1^{e_1} \dots x_{d-1}^{e_{d-1}} x_d^{e_d}$ 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 $k \rightarrow A$ 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 :

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

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 $i < \text{deg}(f)$. 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 $k[T]/(f) \twoheadrightarrow k[a]$, $g \bmod f \mapsto g(a)$.

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 :

$$k[T]/(f) \simeq k[a].$$

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 $a^n + c_1 a^{n-1} + \dots + c_0 = 0$ alors $(\lambda a)^n + \lambda c_1 (\lambda a)^{n-1} + \dots + \lambda^n c_0 = 0$.)

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 $B \rightarrow B$, $x \mapsto xb$ 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 $k \rightarrow K$ et $K \rightarrow L$ 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 $k[T] \rightarrow k[c]$ 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

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

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 . \square

Par exemple, le nombre $z = \sqrt[3]{3} + \sqrt[3]{2} \in \mathbb{R}$, somme des deux réels positifs $\sqrt[3]{3}$, $\sqrt[3]{2}$ 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 $\sqrt[3]{3}$ 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 $k[X, Y] \rightarrow k[a, b]$ 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 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

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

$i < n, j < m$. (Le même résultat vaut pour A : c'est un k -module libre.) Les applications K -linéaires $u : B \rightarrow B$ et $v : B \rightarrow B$ 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 annihilées 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.

6.2.6. 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 $\text{Hom}_k(K, A)$ des morphismes de k -algèbres $K \rightarrow A$. Commençons par un cas particulier.

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

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

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 $\text{Hom}_k(K, A)$ est non vide.

Démonstration. L'ensemble des morphismes d'une sous- k -algèbre de K vers A est naturellement muni d'un ordre partiel : $\varphi \leq \psi$ 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 $K_0 \rightarrow A$. (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 $\text{Hom}_k(k[x], A)$ est non vide. Absurde par maximalité. \square

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 $1 \leq i \leq d$, par les relations $\sigma_j(X_{f,1}, \dots, X_{f,d}) = a_{f,j} \in k$, défini par $f = X^d + \sum_{j < d} (-1)^j a_{f,j} X^{d-j}$. Cette k -algèbre $\text{Adu}_k(F)$ scinde chaque polynôme de F ; elle est non nulle car il en est ainsi de chaque $\text{Adu}_k(f)$. 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 -morphisms $\Omega_1 \rightarrow \Omega_2$ et $\Omega_2 \rightarrow \Omega_1$. 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*

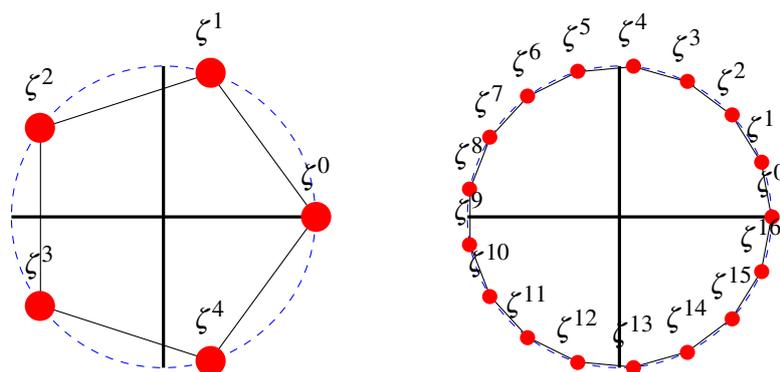
part, deux telles clôtures algébriques sont nécessairement k -isomorphes, quoique de façon éventuellement non unique.

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.

6.4. ¶ 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).

6.4.1. Un nombre complexe $z \in \mathbb{C}$ est dit **constructible** [规矩/可造] s'il existe une suite d'extensions quadratiques $\mathbb{Q} = K_0 \subset \dots \subset K_i \subset K_{i+1} \subset \dots \subset K_n \subset \mathbb{C}$ 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 $\Phi_p := \frac{T^p - 1}{T - 1} = 1 + T + \dots + T^{p-1}$ (exercice 25) 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 arithmeticae* (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. »

6.4.2. Notons \mathbb{F} le corps fini $\mathbb{Z}/p\mathbb{Z}$. La somme $\sum_{\chi} \mathfrak{g}_{\chi} = \mathcal{F}(\sum_{\chi} \chi)(0) - (p-1)$, 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}_{χ} est constructible. (On utilise ici le fait qu'une somme de nombres constructibles est constructible.) D'autre part, chaque \mathfrak{g}_{χ} 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 $\chi \neq 1$; il est d'ordre 2^m pour un entier $m \leq n$. (La constructibilité de $\mathfrak{g}_1 = -1$ 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 $\mathfrak{g}_{\chi}^{2^r} = J(\chi, \dots, \chi)\mathfrak{g}_{\chi^{2^r}}$.) 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}_{χ} est constructible dans le cas particulier où $\chi^2 = 1$, c'est-à-dire $\chi = \bar{\chi}$. Or, $|\mathfrak{g}_{\chi}|^2 = p = \mathfrak{g}_{\chi} \cdot \bar{\mathfrak{g}}_{\chi} = \chi(-1)\mathfrak{g}_{\chi}^2 = \pm\mathfrak{g}_{\chi}^2$. Il en résulte que dans ce cas $\mathfrak{g}_{\chi}^2 = \pm p$, si bien que \mathfrak{g}_{χ} est constructible. CQFD.

6.4.3. 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.

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

①. Comparer par exemple avec

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

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 $\text{Frob}_p : x \mapsto x^p$, 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. ¶ Nombres et construction explicite des $\mathbb{F}_{2^{2^s}}$.

Références : [John Horton 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.

7.2.1. Si $S \subsetneq \mathbb{N}$, notons $\text{mex}(S) = \min(\mathbb{N} \setminus S)$ le plus petit entier naturel n appartenant pas à S . Par exemple, $\text{mex}(\emptyset) = 0$. On définit par récurrence pour $x, y \in \mathbb{N}$ ^① :

$$\begin{aligned} x \text{ 加 } y &:= \text{mex}(\{x' \text{ 加 } y : x' < x\} \cup \{x \text{ 加 } y' : y' < y\})^{\textcircled{2}} \\ x \text{ 乘 } y &:= \text{mex}(\{(x' \text{ 乘 } y) \text{ 加 } (x \text{ 乘 } y') \text{ 加 } (x \text{ 乘 } y') : x' < x, y' < y\})^{\textcircled{3}} \end{aligned}$$

7.2.2. On peut expliciter le calcul de l'addition : $x \text{ 加 } y$ est le *ou exclusif* [[逻辑]异或] des écritures binaires de x et y . En d'autres termes, l'addition de deux mêmes nombres est nulle et l'addition de deux puissances distinctes de 2 est l'addition usuelle. On peut vérifier par récurrence (non immédiate) que la multiplication est quant à elle caractérisée par le fait que le produit de deux nombres distincts de la forme 2^{2^n} est le produit usuel (c'est-à-dire $2^{2^n} \text{ 乘 } 2^{2^m} = 2^{2^n+2^m}$, si $n \neq m$) mais le carré $2^{2^n} \text{ 乘 } 2^{2^n}$ est $\frac{3}{2} \times 2^{2^n} = 2^{2^n} \text{ 加 } 2^{2^n-1}$. (Par exemple $4 \text{ 乘 } 4 = 6$.)

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 »^④ 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} ,

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 $y' < y$.

④. Cela signifie que tout polynôme de degré 2 est scindé sur ce corps, et qu'il est minimal pour cette propriété.

et donc de chaque $[2^{2^n}]$, vient du fait que si $x, y > 0$, alors $x \text{ 乘 } y$ est le mex d'un ensemble contenant $0 = (0 \text{ 乘 } y) \text{ 加 } (0 \text{ 乘 } 0) \text{ 加 } (x \text{ 乘 } 0)$. 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		乘	0	1	2	3
0	0	1	2	3		0	0	0	0	0
1	1	0	3	2	et	1	0	1	2	3
2	2	3	0	1		2	0	2	3	1
3	3	2	1	0		3	0	3	1	2

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

$$([2^{2^n}], \text{加}, \text{乘}) \cong (\mathbb{F}_2[X_i : 0 \leq i < n] / (X_i^2 + X_i + \prod_{j < i} X_j, 0 \leq i < n), +, \times)$$

$$\sum_{E \in \mathcal{E}} \prod_{e \in E} 2^{2^e} \mapsto \sum_{E \in \mathcal{E}} \prod_{e \in E} x_e$$

où \mathcal{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.

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,

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.

$4\ell + 1$ est congru à 5 modulo 8, de sorte que (exercice 41) $2^{(p-1)/2}$ est congru à -1 modulo p . Enfin, $2^{(p-1)/\ell} = 2^4 \equiv 1$ modulo p entraîne $p = 3$ ou 5 . \square

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 $T^5 \equiv T \pmod{g}$, 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 $\mathbb{F}_p[T] \rightarrow \mathbb{F}_p[x]$ envoyant T sur x se factorise à travers un isomorphisme $\mathbb{F}_p[T]/(\Pi) \simeq \mathbb{F}_p[x] = \mathbb{F}$. 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 .*

7.3.3. Groupe des automorphismes. Soit \mathbb{F} un corps fini de cardinal $q = p^d$. On a déjà vu que $\text{Frob}_p : x \mapsto x^p$ est un endomorphisme de \mathbb{F} ; c'est un automorphisme car tout morphisme de corps est injectif. Le sous-groupe $\langle \text{Frob}_p \rangle$ de $\text{Aut}(\mathbb{F})$ est d'ordre d : sa puissance d -ième Frob_p^d est l'identité et $\text{Frob}_p^a \neq \text{Id}$ 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 $\varphi \in \text{Aut}(\mathbb{F})$ 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 $\text{Aut}(\mathbb{F})$ est *au plus* d . Finalement, on a démontré le résultat suivant.

Proposition. *Soit \mathbb{F} un corps fini. Le groupe $\text{Aut}(\mathbb{F})$ de ses automorphismes est cyclique engendré par le Frobenius $\text{Frob}_p : x \mapsto x^p$. 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 $\text{Frob}_p^d(x) = x$, on en déduit que d_x est aussi égal au cardinal de l'« orbite » (finie) $\{\text{Frob}_p^n(x) : n \geq 0\}$. 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 $\text{Frob}_p^d(x) = x$ 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

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

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 $\{\text{Frob}_p^n x : n \geq 0\}$: c'est le plus petit entier $d \geq 1$ tel que $\text{Frob}_p^d(x) = x$;*
- (ii) *l'ordre N de x dans Ω^\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 $\prod_{0 \leq n < d_x} (T - \text{Frob}_p^n(x))$: les « conjugués » de x (sur \mathbb{F}_p) sont exactement les $\text{Frob}_p^n(x)$ avec $0 \leq n < d_x$.*

À titre d'application algébrique, on pourra démontrer l'irréductibilité des polynômes d'Artin-Schreier ; cf. exercice 42. Une application « arithmétique » fait l'objet du paragraphe suivant.

7.3.5. Polynômes cyclotomiques. Soit $\Phi_p(T) := T^{p-1} + \dots + T + 1 \in \mathbb{Z}[T]$ 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 24, 25). 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}_ℓ . Puisque x est une racine primitive p -ième de l'unité, le degré de x sur \mathbb{F}_ℓ 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}_ℓ si et seulement si $\ell \equiv 1 \pmod{p}$.

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 premiers 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}_ℓ .

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}_ℓ .

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 $\ell_1, \ell_2, \dots, \ell_r$. 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. \square

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. $\frac{1}{2d}$).

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 $p^d - \sum_{m \mid d, m \neq d} p^m$, 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 $1 - \frac{2}{p} \geq \frac{1}{3}$. \square

On appelle **fonction de Möbius** [默比乌斯函数] la fonction $\mu : \mathbb{N} \rightarrow \mathbb{Z}$ définie par $\mu(n) = 0$ si n est divisible par un carré $\neq 1$ et $\mu(d) = (-1)^j$ si $d = p_1 \cdots p_j$ avec

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.

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 $f, g : \mathbb{N}_{>0} \rightarrow \Gamma$ sont deux fonctions, on a

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

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

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

où les ℓ_i sont des nombres premiers. En particulier, il est égal à $\frac{p^d}{d} + \mathcal{O}\left(\frac{p^{d/2}}{d}\right)$.

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 $\text{Frob}_p^a(\alpha) = \alpha$ donc *a fortiori* $\text{Frob}_p^d(\alpha) = \alpha$; 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 $\mathcal{O}(p^{d/3}/d)$; leur somme est donc bien $\mathcal{O}(p^{d/3}) = \mathcal{O}(p^{d/2}/d)$. \square

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

7.4.1. Chevalley-Warning.

Références : [CHEVALLEY 1935], [SERRE 1977, I §2], [TAO 2014, §8].

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

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

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

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

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

Cela résulte du fait que pour tout $x \in \mathbb{F}$, le scalaire $1_{\mathbb{F}} - x^{\#\mathbb{F}-1}$ vaut $1_{\mathbb{F}}$ si $x = 0_{\mathbb{F}}$, et $0_{\mathbb{F}}$ si $x \neq 0_{\mathbb{F}}$. Il est donc naturel d'introduire le polynôme

$$P := \prod_{i=1}^e (1_{\mathbb{F}} - f_i^{\#\mathbb{F}-1}) \in \mathbb{F}[T_1, \dots, T_n],$$

de degré $(\#\mathbb{F} - 1)(\deg(f_1) + \dots + \deg(f_e))$. En effet, d'après ce qui précède on a l'égalité, dans \mathbb{F} :

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

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

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

si d n'est pas un multiple non nul de $\#\mathbb{F} - 1$. (En effet, il existe dans ce cas un $\lambda \in \mathbb{F}^\times$ tel que $\lambda^d \neq 1$ si bien que l'égalité $S_d = \lambda^d S_d$, obtenue par le changement de variable $u = \lambda t$, force l'égalité $S_d = 0$.) Il en résulte que si $F \in \mathbb{F}[T_1, \dots, T_n]$ est de degré strictement inférieur à $n(\#\mathbb{F} - 1)$, la somme $\sum_{t \in \mathbb{F}^n} F(t)$ 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 $\{(t_1, \dots, t_n) \in \mathbb{F}^n : f_1(t_1, \dots, t_n) = \dots = f_e(t_1, \dots, t_n) = 0\}$ 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 $\mathbb{C}(t)$.

7.4.2. 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 'brœyn] a -aire d'ordre r une suite cyclique u , c'est-à-dire une application $\mathbb{Z}/N\mathbb{Z} \rightarrow \mathfrak{A}$ 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 $m = u_{i+1}u_{i+2} \dots u_{i+r}$. Compte-tenu de l'unicité et du fait qu'il existe a^r mots de longueur r , on a nécessairement $N = a^r$.

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

8♣, A♣, 2♣, 4♣, A♠, 2♦, 5♣, 3♠, 6♦, 4♠, A♥, 3♦, 7♣, 7♠, 7♥, 6♥,
4♥, 8♥, A♦, 3♣, 6♣, 5♠, 3♥, 7♦, 6♠, 5♥, 2♥, 5♦, 2♠, 4♦, 8♠, 8♦.

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 : $0 \leftrightarrow$ noir ; $1 \leftrightarrow$ rouge), majeur ou pas (bit suivant : $0 \leftrightarrow$ ♣, ♦ ; $1 \leftrightarrow$ ♥, ♠), et un nombre entre 1 et 8 (trois derniers bits, avec la convention que $000 \leftrightarrow 8$). 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].

7.5. Réciprocité quadratique.

Référence : [IRELAND et ROSEN 1990, chap. 5].

Soit p un nombre premier $\neq 2$. Il existe un unique caractère non trivial $\mathbb{F}_p^\times \rightarrow \{\pm 1\} \subseteq \mathbb{C}^\times$; 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 $\left(\frac{0}{p}\right) = 0$.) 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 $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.

Soit maintenant $\ell \neq p$ un autre nombre premier $\neq 2$. Notons ci-dessous pour abrégé \mathfrak{h}^\circledast le caractère $\left(\frac{\cdot}{p}\right)$. Puisque $\mathfrak{h}^\ell = \mathfrak{h}$ est non trivial, on a

$$(\dagger) \quad \mathfrak{g}_{\mathfrak{h}^\ell} = J(\mathfrak{h}, \dots, \mathfrak{h})\mathfrak{g}_{\mathfrak{h}}.$$

Comme

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

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

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

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 $\{\underline{a} : a_1 + \dots + a_\ell =$

①. Lettre grecque « koppa ».

$1\} \subseteq \mathbb{F}_p^\ell$ par permutation cyclique des coordonnées et l'expression $\mathfrak{h}(a_1)\cdots\mathfrak{h}(a_\ell)$ est invariante sous cette action. Il en résulte que la somme de Jacobi est un entier congru modulo ℓ à $\mathfrak{h}(1/\ell)\cdots\mathfrak{h}(1/\ell) = \mathfrak{h}(\ell)^\ell = \mathfrak{h}(\ell)$, 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 $p^{\frac{\ell-1}{2}} \equiv \left(\frac{p}{\ell}\right) \pmod{\ell}$, on en déduit le théorème suivant.

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

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

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

On a également la « formule complémentaire » :

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

Voir par exemple l'exercice 41 pour une démonstration.

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 56 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, $P = 3 \cdot 5 \cdot 7 \dots$) 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 $r \rightarrow +\infty$. 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 $\frac{3^d}{2} (2N+1)^d P^{-d}$ 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 $\mathbb{Z}/P\mathbb{Z}[T] \rightarrow \mathbb{F}_{p_1}[T] \times \dots \times \mathbb{F}_{p_r}[T]$ 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. \square

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

calculé 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].

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 $T^{q^d} - T$ 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* $\text{Frob}_q : A \rightarrow A, a \mapsto a^q$, qui est la puissance $\log_p(q)$ -ième du Frobenius Frob_p . L'ensemble $\text{Fix}(\text{Frob}_q \subset A) := \{a \in A : a^q = a\}$ est donc une *sous- \mathbb{F}_q -algèbre* de A , de dimension ≥ 1 (sauf si $A = \{0\}$).

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

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 ,

$$B(f) := \text{Ker}(\text{Frob}_q - \text{Id} : \mathbb{F}_q[T]/(f) \rightarrow \mathbb{F}_q[T]/(f)).$$

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 $\text{Frob}_q - \text{Id} : A \rightarrow A$, que l'on peut écrire explicitement dans la base $1, T, \dots, T^{\deg(f)-1}$ de A en effectuant les divisions euclidiennes des T^{iq} par f . Lorsque f est irréductible, $\mathbb{F}_q[T]/(f)$ est un corps et $B(f)$ n'est autre que le sous-corps $\mathbb{F}_q \subseteq \mathbb{F}_q[T]/(f)$.

Si $f = \prod_{i=1}^r f_i^{e_i}$, où les f_i sont premiers entre eux deux à deux (non constants), on a d'après le théorème chinois un isomorphisme $\# : B(f) \simeq \prod_i B(f_i^{e_i})$ 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 $f = \prod_{c \in \mathbb{F}_q} \text{PGCD}(f, y - c)$.*

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 $\#(y)$ s'annule.)

Corollaire (critère d'irréductibilité de Butler). *Un polynôme séparable $f \in \mathbb{F}_q[T]$ est irréductible si et seulement si $\dim_{\mathbb{F}_q} \text{Ker}(\text{Frob}_q - \text{Id}) = 1$, où $\text{Frob}_q : x \mapsto x^q$ et $\text{Id} : x \mapsto x$ sont vues 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 τ_1, \dots, τ_s de l'algèbre de Berlekamp $B(f) = \text{Ker}(\text{Frob}_q - \text{Id})$ de f , puis, si $s > 1$ de sorte qu'il y a une factorisation non triviale à effectuer, on tire au hasard un élément $y = c_1 \tau_1 + \dots + c_s \tau_s \in B(f)$ (avec $c_i \in \mathbb{F}_q$) et on calcule les 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 $\#(y)$ ne sont pas toutes égales (où $\#$ est l'isomorphisme $B_f \simeq (\mathbb{F}_q)^s$ 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. $t = y + y^2 + y^4 + \dots + y^{q/2}$ en caractéristique 2), et alors $\text{PGCD}(f, t - 1)$ (resp. $\text{PGCD}(f, t)$) 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 $\text{Frob}_2 - \text{Id}$ sur la base $1, t, t^2, \dots, t^4$ de $\mathbb{F}_2[T]/(f)$, en calculant successivement T^2, T^4, \dots, T^8 modulo f :

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

(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 $\dim_{\mathbb{F}_2} \text{Ker}(\text{Frob}_2 - \text{Id}) = 1$, donc f est bien irréductible.

8.3. Factorisation sans facteur carré.

Référence : [ibid., 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 $\frac{f}{u} \mid f_2$. 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 $f' = \sum_j e_j f_j' \frac{f}{f_j}$, 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 $\text{Frob}_p : \mathbb{F}_q \rightarrow \mathbb{F}_q$. 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 ȘTEFĂNESCU 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 ȘTEFĂNESCU 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 $v_0 := g(0), v_1 := g(1), \dots, v_r := g(r)$ divisent les entiers (connus) $f(0), f(1), \dots, f(r)$, 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, \dots, 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.

^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].

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

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

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 $r \in \llbracket 0, n \rrbracket$. On a

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

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 $\|(T - \alpha)g\|_2 = \|(\bar{\alpha}T - 1)g\|_2$. 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 $(\bar{\alpha}T - 1)g = \sum_i (\bar{\alpha} b_{i-1} - b_i) T^i$. On vérifie alors en développant que $\sum_i |b_{i-1} - \alpha b_i|^2 = \sum_i |\bar{\alpha} b_{i-1} - b_i|^2$. 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, $M(f) = |a_n| \leq (\sum_i |a_i|^2)^{\frac{1}{2}} = \|f\|_2$. \square

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 $\|g\|_1 \leq 2^d M(g)$. \square

• 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 :

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

^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.

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

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

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*. 3^e éd. Addison-Wesley, xx+650 pages.
- TAOCP 2 Donald E. KNUTH (1998). *The art of computer programming. Vol. 2. Seminumerical algorithms*. 3^e éd. Addison-Wesley, xiv+762 pages.
- TAOCP 4A Donald E. KNUTH (2011). *The art of computer programming. Vol. 4A. Combinatorial algorithms, part 1*. Addison-Wesley, xvi+883 pages.

AUTRES RÉFÉRENCES

- APÉRY, François et Jean-Pierre JOUANOLOU (2006). *Résultant et sous-résultants. Le cas d'une variable*. Hermann, x+477 pages.
- ARTIN, Michael (1991). *Algebra*. Prentice Hall, xviii+618 pages.
- ATIYAH, Michael F. et Ian G. MACDONALD (1969). *Introduction to commutative algebra*. Addison-Wesley, ix+128 pages.
- BAEZ, John C. et Michael SHULMAN (2010). « [Lectures on \$n\$ -categories and cohomology](#) ». *Towards higher categories*. **152**. IMA Vol. Math. Appl. Springer, 1-68.
- BHARGAVA, Manjul et Matthew SARIANO (2014). « [On a notion of "Galois closure" for extensions of rings](#) ». *J. Eur. Math. Soc. (JEMS)* **16**(9), 1881-1913.
- BREEN, Lawrence (2010). « [Notes on 1- and 2-gerbes](#) ». *Towards higher categories*. **152**. IMA Vol. Math. Appl. Springer, 193-235.
- CHEVALLEY, Claude (1935). « [Démonstration d'une hypothèse de M. Artin](#) ». *Abh. Math. Sem. Univ. Hamburg* **11**(1), 73-75.
- COHEN, Henri (1993). *A course in computational algebraic number theory*. Graduate Texts in Mathematics **138**. Springer-Verlag, xii+534 pages.
- CONWAY, John H., Heiko DIETRICH et E. A. O'BRIEN (2008). « [Counting groups : gnus, moas, and other exotica](#) ». *Math. Intelligencer* **30**(2), 6-18.
- CONWAY, John Horton (2001). *On numbers and games*. 2^e éd. A K Peters, xii+242 pages.
- COX, David A. (2004). *Galois theory*. John Wiley & Sons, xx+559 pages.
- DAVENPORT, Harold (2000). *Multiplicative number theory*. 3^e éd. Graduate Texts in Mathematics **74**. Springer-Verlag, xiv+177 pages.
- DIACONIS, Persi et Ron GRAHAM (2012). *Magical mathematics*. The mathematical ideas that animate great magic tricks. Princeton University Press, xiv+244 pages.
- DOUADY, Adrien et Régine DOUADY (2005). *Algèbre et théories galoisiennes*. Cassini.
- EISENBUD, David (2015). « [The Amazing Heptadecagon](#) ». Youtube [87uo2TPrsl8](#).
- FLAJOLET, Philippe et Robert SEDGEWICK (2009). *Analytic combinatorics*. Cambridge University Press, xiv+810 pages.

- FROBENIUS, Ferdinand Georg (1896). « Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe ». *Sitz. Akad. Wiss. Berlin.* (= Ges. Abh., II, 719–733), 689–703.
- GATHEN, Joachim von zur et Jürgen GERHARD (2003). *Modern computer algebra*. 2^e éd. Cambridge University Press, xiv+785 pages.
- GAUß, Carl Friedrich (1807). *Recherches arithmétiques* (Disquisitiones arithmeticae). Traduit du latin par A.-C.M. Pouillet-Delisle. Réédité chez Jacques Gabay et disponible sur gallica.bnf.fr.
- (2005). *Mathematisches Tagebuch, 1796–1814*. 5^e éd. Ostwalds Klassiker der Exakten Wissenschaften. Bilingue latin-allemand (avec commentaires en allemand). Verlag Harri Deutsch, 235 pages.
- GEL'FAND, Israel M., Mikhail M. KAPRANOV et Andrei V. ZELEVINSKIÏ (1994). *Discriminants, resultants, and multidimensional determinants*. Birkhäuser, x+523 pages.
- HARDY, Godfrey Harold et Edward Maitland WRIGHT (2007). *Introduction à la théorie des nombres*. Traduction française de [Hardy-Wright] par François Sauvageot. Vuibert & Springer, xxxviii+569 pages.
- HIRAMATU, Toyokazu [平松豊一] (1998). 数論を学ぶ人のための相互法則入門 [Introduction aux lois de réciprocités supérieures...] 牧野書店 [Makino-shoten].
- HODGES, Wilfrid (1979). « Krull implies Zorn ». *J. London Math. Soc.* **19**(2), 285–287.
- IRELAND, Kenneth et Michael ROSEN (1990). *A classical introduction to modern number theory*. Graduate Texts in Mathematics **84**. Springer-Verlag, xiv+389 pages.
- JACOBSON, Nathan (1985). *Basic algebra. I*. 2^e éd. W. H. Freeman and Company, xviii+499 pages.
- JECH, Thomas J. (1973). *The axiom of choice*. Studies in Logic and the Foundations of Mathematics, Vol. 75. North-Holland, xi+202 pages.
- KATO, Kazuya [加藤和也] (2009). 類体論と非可換類体論. 1 [Théorie du corps de classes et théorie non commutative du corps de classes. 1]. 岩波書店 [Iwanami-shoten].
- LANG, Serge (2004). *Algèbre. Cours et exercices*. Traduction française de [Algebra/Lang]. Dunod, 944 pages.
- LEBESGUE, Henri (1950). *Leçons sur les constructions géométriques*. Gauthier-Villars, vi+304 pages.
- LECERF, Grégoire (2013). « Factorisation des polynômes à plusieurs variables ». *Les cours du CIRM* **3**(1), 1–85.
- LENSTRA, A. K., H. W. LENSTRA Jr. et L. LOVÁSZ (1982). « Factoring polynomials with rational coefficients ». *Math. Ann.* **261**(4), 515–534.
- LENSTRA Jr., H. W. (1978). « Nim multiplication ». *Séminaire de théorie des nombres, Talence 1977–1978*, exp. n° 11.
- (2008). « Lattices ». Dans [Surveys//Buhler-Steinhagen], 127–181.
- LIDL, Rudolf et Harald NIEDERREITER (1997). *Finite fields*. 2^e éd. Encyclopedia of Mathematics and its Applications **20**. Cambridge University Press, xiv+755 pages.
- LOMBARDI, Henri et Claude QUITTÉ (2011). *Algèbre commutative (Méthodes constructives)*. Mathématiques en devenir. Calvage & Mounet, xxxi+991 pages.
- MAC LANE, Saunders (1963). *Homology*. Die Grundlehren der mathematischen Wissenschaften **114**. Springer-Verlag, x+422 pages.
- MADORE, David A. (15 juil. 2015a). « Le jeu de cartes Dobble et la géométrie projective expliquée aux enfants ». Blog.

- (27 juil. 2015b). « Comment faire un jeu de *Tribble* ». Blog.
- MESSING, William et Victor REINER (2013). « A universal coefficient theorem for Gauss's lemma ». *J. Commut. Algebra* 5.(2), 299-307.
- MIGNOTTE, Maurice et Doru ȘTEFĂNESCU (1999). *Polynomials. An algorithmic approach*. Springer-Verlag, xii+306 pages.
- (2001). « La première méthode générale de factorisation des polynômes. Autour d'un mémoire de F.T. Schubert ». *Rev. histoire math.* 7.(1), 67-89.
- PERRIN, Daniel (1996). *Cours d'algèbre*. Ellipse.
- POHST, Michael et Hans ZASSENHAUS (1989). *Algorithmic algebraic number theory*. Encyclopedia of Mathematics and its Applications 30. Cambridge University Press, xiv+465 pages.
- ROTMAN, Joseph J. (1995). *An introduction to the theory of groups*. Quatrième édition. Graduate Texts in Mathematics 148. Springer-Verlag, xvi+513 pages.
- ŠAFAREVIČ, Igor R. [Игорю Р. Шафаревичу] (1997). *Basic notions of algebra*. Springer-Verlag, iv+258 pages.
- SAMUEL, Pierre (1968). « Unique factorization ». *Amer. Math. Monthly* 75, 945-952.
- SCHINZEL, Andrzej (2000). *Polynomials with special regard to reducibility*. Encyclopedia of Mathematics and its Applications 77. Cambridge University Press, x+558 pages.
- SERRE, Jean-Pierre (1977). *Cours d'arithmétique*. 2^e éd. Presses universitaires de France, 188 pages.
- (1992). *Topics in Galois theory*. 1. Research Notes in Mathematics. Jones et Bartlett Publishers, xvi+117 pages.
- (1978-79). « Groupes finis ». Notes d'un cours à l'ÉNSJF ; [arXiv :0503154v6](https://arxiv.org/abs/0503154v6).
- SHOUP, Victor (2009). *A computational introduction to number theory and algebra*. 2^e éd. (Sous licence CC BY-NC-ND). Cambridge University Press, xviii+580 pages.
- SIEGEL, Aaron N. (2013). *Combinatorial game theory*. Graduate Studies in Mathematics 146. American Mathematical Society, xiv+523 pages.
- STANLEY, Richard P. (1999). *Enumerative combinatorics. Vol. 2*. Cambridge Studies in Advanced Mathematics 62. Cambridge University Press, xii+581 pages.
- 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.
- TERRAS, Audrey (1999). *Fourier analysis on finite groups and applications*. London Mathematical Society Student Texts 43. Cambridge University Press, x+442 pages.
- WATKINS, John J. (2007). *Topics in commutative ring theory*. Princeton University Press, xii+215 pages.
- WEIL, André (1974). « La cyclotomie jadis et naguère ». *Séminaire Bourbaki*, exp. n° 452.

EXERCICES

Groupes

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

(Indication : on pourra utiliser 1.7.2 à G agissant sur lui-même par conjugaison.)

□ Le point clef est que l'ensemble des points fixes sous cette action est exactement $Z(G)$. Il en résulte que l'on a la congruence

$$\#G \equiv \#Z(G) \pmod{p},$$

soit $p \mid Z(G)$. Ceci est équivalent à la non trivialité de $Z(G)$ (qui est nécessairement un p -groupe lui aussi). □

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

□ Pour chaque entier n , notons $\text{gnu}(n)$ le nombre de groupes d'ordre n .

(i) Si p est un nombre premier, tout groupe d'ordre p est cyclique :

$$\text{gnu}(p) = 1.$$

En particulier, il existe [à isomorphisme non unique près] un seul groupe d'ordre 2, 3, 5 ou 7.

(ii) Si p est un nombre premier, tout groupe d'ordre p^2 est abélien :

$$\text{gnu}(p^2) = 2.$$

(En effet, le centre Z d'un tel groupe G est non trivial – voir exercice 1 – et si $x \in G - Z$, on a $G = \langle Z, x \rangle$ qui est nécessairement abélien.) En particulier, il existe deux groupes d'ordre $2^2 = 4$ (resp. $3^2 = 9$), qui sont $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/4\mathbb{Z}$ (resp. $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ et $\mathbb{Z}/9\mathbb{Z}$).

(iii) Si $\ell < p$ sont deux nombres premiers, on a

$$\text{gnu}(\ell p) = 1 + [p \equiv 1(\ell)].$$

En particulier, il existe deux groupes d'ordre 6 : le groupe cyclique $\mathbb{Z}/6\mathbb{Z} = \langle x \mid x^6 = 1 \rangle$ et le groupe $S_3 \simeq D_3 \simeq \text{GL}_2(\mathbb{F}_2) \simeq \langle c, \tau \mid c^3 = \tau^2 = 1, \tau c \tau = c \rangle$, et deux groupes d'ordre 10 : le groupe cyclique $\mathbb{Z}/10\mathbb{Z}$ et le groupe diédral D_5 des isométries du pentagone. Pour vérifier l'énoncé, on commence par remarquer que G est une extension scindée de $\mathbb{Z}/\ell\mathbb{Z}$ par $\mathbb{Z}/p\mathbb{Z}$; cela résulte du théorème de Cauchy et du fait que le p -sous-groupe de G est distingué (par un théorème de Sylow, ou de façon *ad hoc* pour les valeurs considérées ici : un sous-groupe d'indice 2 est toujours distingué). L'action $\mathbb{Z}/\ell\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Z}/p\mathbb{Z}) = (\mathbb{Z}/p\mathbb{Z})^\times$ est nécessairement triviale si $p \not\equiv 1(\ell)$. Dans le cas contraire, on a $G = \langle x, y \rangle$ avec $x^p = 1$, $y^\ell = 1$ et $y^{-1}xy = x^a$, où a appartient à l'ensemble $(\mathbb{Z}/p\mathbb{Z})^\times[\ell]$. Les différentes actions non triviales (\leftrightarrow choix de a) diffèrent par [composition avec] un automorphisme de $\mathbb{Z}/\ell\mathbb{Z}$ et induisent donc des groupes isomorphes (cf. p. ex. [PERRIN 1996, I.7.12] ou [John H. CONWAY, DIETRICH et O'BRIEN 2008, §5]). Remarquons – c'est un fait général – que si $n = 6$, et $H = \langle \tau \rangle$ est un sous-groupe d'ordre 2, on a un morphisme naturel $G \rightarrow S_{G/H} \simeq S_3$,

correspondant à l'action par translations sur les classes gH . Dans le cas non abélien, c'est un isomorphisme car H n'est pas distingué.

- (iv) Si p est un nombre premier, il existe 3 groupes abéliens d'ordre p^3 — $\mathbb{Z}/p^3\mathbb{Z}$, $\mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ et $(\mathbb{Z}/p\mathbb{Z})^3$ — et deux groupes non abéliens :

$$\text{gnu}(p^3) = 5.$$

(Voir par exemple [ROTMAN 1995, exercice 4.32 et exemple 7.16] ou [PERRIN 1996, chap. I, exercice 8] pour une discussion de ce résultat, dû à Hölder.) En particulier, il existe deux groupes non abéliens d'ordre 8 : le groupe diédral D_4 et le groupe Q_8 des quaternions. Vérifions ce fait. Soit G un groupe non abélien d'ordre 8. Nécessairement il existe un élément d'ordre 4 : si les ordres étaient ≤ 2 , G serait abélien. Notons $H = \langle x \rangle = \{1, x, x^2, x^3 = x^{-1}\}$; il est d'indice 2 donc distingué dans $G = H \cup \tau H$, pour tout $\tau \notin H$. On a $\tau^{-1}x\tau \in H$; si G n'est pas abélien, cet élément ne peut être x , ni x^2 (qui a un ordre différent de x). On a donc $\tau^{-1}x\tau = x^3 = x^{-1}$. L'élément τ^2 appartient au centre Z de G , qui est de cardinal 2. (Si $\#Z = 4$, on aurait $G = \langle Z, y \rangle$ pour tout $y \notin Z$, et G serait abélien.) Ainsi $Z = \{1, x^2\}$ et $\tau^2 \in Z$. Notons -1 l'élément x^2 . Si $\tau^2 = 1$, le groupe obtenu est le groupe diédral $D_4 \simeq \langle x, \tau \mid x^4 = 1, \tau^2 = 1, x\tau x = \tau \rangle$. Si $\tau^2 = -1$, l'élément τ est également d'ordre 4, $\tau x = -x\tau$ et on vérifie que le groupe $\langle x, \tau \mid x^4 = 1, \tau^2 = x^2, x\tau x = \tau \rangle$ obtenu est le groupe Q_8 des quaternions. Les groupes D_4 et Q_8 ne sont pas isomorphes.

□

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 $n \geq 0$. 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, \dots, a_m) telle que $\langle a_1, \dots, a_m \rangle = G$ et $a_i \notin \langle a_1, \dots, a_{i-1} \rangle$ pour tout $1 \leq i \leq m$.
- (ii) Montrer que $2^m \leq n$ et en déduire que $\#\text{Aut}(G) \leq n^{\log_2(n)}$.

□ Le (i) est évident. Si $H_1 < H_2$ est une inclusion stricte de sous-groupes de G , le cardinal de H_2 est au moins le double de celui de H_1 . (Plus précisément : $\text{card } H_2 = (H_2 : H_1) \times \text{card}(H_1)$.) Si on applique cette observation à la suite strictement croissante $\langle e \rangle < \langle a_1 \rangle < \dots < \langle a_1, \dots, a_m \rangle = G$, on obtient : $\text{card } G \geq 2^m \text{card} \langle e \rangle = 2^m$. Enfin, un automorphisme de G (et même un endomorphisme) est caractérisé par l'image de ses générateurs. Ici, on a au plus n choix pour chacun des m éléments a_1, \dots, a_m , d'où $\#\text{Aut}(G) \leq n^m \leq n^{\log_2(n)}$. □

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

□ Soient H le noyau de f et $h, h' \in H$. Les morphismes $\mathbb{Z} \rightarrow G, 1 \mapsto h$ et $1 \mapsto h'$ ont même image dans $\text{Hom}(T, G/H)$, et en particulier dans $\text{Hom}(T, G')$. Si f est simplifiable à gauche on a donc $h = h'$: le sous-groupe $H \leq G$ est donc trivial. □

Exercice 7. 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 $\{1, \dots, n\}$ 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 8. Soient G un groupe fini, H un sous-groupe et E le G -ensemble G/H . Montrer que le cardinal de $\text{Aut}_{G\text{-Ens}}(E)$ est au plus $(G : H)$ avec égalité si et seulement si $H \triangleleft G$.

Exercice 9.

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

□(i) On écrit $M = 1 + 3^a S$ avec S à coefficients entiers et a maximal (c'est-à-dire S non divisible par 3). On a $(1 + 3^a S)^3 = 1 + 3 \cdot 3^a S + 3 \cdot 3^{2a} S^2 + 3^{3a} S^3 = 1$ donc $S = -3^a S^2 - 3^{2a-1} S^3$ est divisible par 3 ; absurde.

(ii) Il suffit de montrer que $M^p \neq \text{Id}$ pour tout nombre premier p car $(\text{Id} + 3R)^a$ est du même type que M pour tout $a \geq 1$. Pour $p = 3$, on vient de le faire. Supposons donc $p \neq 3$. On factorise à nouveau la plus grande puissance de 3 et on écrit

$$(1 + 3^a S)^p = 1 + p3^a S + \binom{p}{2} 3^{2a} S^2 + \dots + 3^{pa} S^p = 1.$$

On a donc

$$pS = -\binom{p}{2} 3^a S^2 - \dots - 3^{(p-1)a} S^p,$$

qui est divisible par 3. Absurde.

(iii) D'après ce qui précède, $\text{GL}_n(\mathbb{Z}) \twoheadrightarrow \text{GL}_n(\mathbb{F}_3)$ est de noyau sans torsion donc tout sous-groupe fini de $\text{GL}_n(\mathbb{Z})$ s'injecte dans $\text{GL}_n(\mathbb{F}_3)$, qui est fini. □

Exercice 10. Soient n_1, \dots, n_r et m_1, \dots, m_s des entiers ≥ 2 . À quelle condition les groupes $\mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_r\mathbb{Z}$ et $\mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_s\mathbb{Z}$ sont-ils isomorphes ?

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

Voir aussi la suite [A060689](#). □

Exercice 11. 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 $\bigcup_g (gHg^{-1} - \{e\})$ est de cardinal au plus $(G : H) \times (\#H - 1)$.)

□ Voir [SERRE 1978-79, §6.1]. □

Anneaux

Exercice 12. 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 13. Montrer qu'il y a 4 classes d'isomorphie d'anneaux de cardinal 4.

□ Il s'agit des anneaux \mathbb{F}_2^2 , $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{F}_2[x]/(x^2)$, $\mathbb{F}_4 \simeq \mathbb{F}_2[x]/(x^2 + x + 1)$. En effet, un tel anneau A est isomorphe à $\mathbb{Z}/4\mathbb{Z}$ ou bien est une \mathbb{F}_2 -algèbre et $A = \mathbb{F}_2[a]$ pour n'importe quel $a \in A \setminus \mathbb{F}_2$. Notons f le polynôme minimal de a ; trois cas se présentent : (1) f est irréductible – et $A \simeq \mathbb{F}_4$ –, (2) f est scindé à racines simples – et $A \simeq \mathbb{F}_2[x]/(x(x-1)) \simeq \mathbb{F}_2^2$ –, et (3) f est scindé à racine double – et $A \simeq \mathbb{F}_2[x]/(x^2)$. Le même argument montre qu'il y a 4 classes d'isomorphie d'anneau de cardinal p^2 , où p est un nombre premier. □

Exercice 14. Montrer que le sous-ensemble $\mathbb{Z}[s^{-1}]$ de \mathbb{Q} considéré en 3.4.2 est bien un sous-anneau.

Exercice 15. 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 16. Soient A un anneau et $S \subseteq A$. Montrer que le morphisme $\iota_S : A \rightarrow A[S^{-1}]$ est un épimorphisme, c'est-à-dire qu'il est simplifiable à droite : si $f \circ \iota_S = g \circ \iota_S$ alors $f = g$.

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

Exercice 17.

(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 ?

□ (i) En effet, si $(a, s)\mathcal{R}(a', s')$ signifie que $as' = a's$ dans A , on a $(0, 2)\mathcal{R}(0, 4)$ et $(0, 4)\mathcal{R}(3, 8)$ mais on n'a pas $(0, 2)\mathcal{R}(3, 8)$.

(ii) Je n'ai pas vérifié. (Noter que les valeurs de $n \leq 12$ pour lesquelles il y a plus d'un anneau de cardinal n – c'est-à-dire un autre anneau que $\mathbb{Z}/n\mathbb{Z}$ – sont : 4, 8, 9, 12.) □

Exercice 18.

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

Fixons un entier $n \geq 1$. 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 $G \rightarrow \mathbb{C}$, dont le produit \star est le *produit de convolution*.

- (ii) Montrer que l'ensemble X est naturellement en bijection avec le groupe \hat{G} des caractères de G .
- (iii) Montrer que la transformation de Gelfand $A = (\mathbb{C}[G], \star) \rightarrow \mathbb{C}^X$, $a \mapsto \hat{a}$, est un isomorphisme de \mathbb{C} -algèbres.
- (iv) Comprendre le lien avec la transformation de Fourier considérée en §2.

□ Voir [A. DOUADY et R. DOUADY 2005, 5.3.2-5]. □

Exercice 19. 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 20. Soient p un nombre premier et A une \mathbb{F}_p -algèbre. Montrer que le produit cartésien A^2 , muni des deux opérations :

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

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

□ Il est clair que le pire cas correspond à la division euclidienne d'un nombre de Fibonacci par son prédécesseur. On en déduit une majoration en $\lfloor \log_{\varphi}((3-\varphi)n) \rfloor$, où φ est le nombre d'or, soit, plus concrètement, une majoration en $\lceil 4, 8 \log_{10}(n) - 0, 32 \rceil$. Voir [TAOCP 2, 4.5.3] pour ce résultat et une analyse en moyenne ; pour un analogue dans $\mathbb{F}_p[T]$, voir [FLAJOLET et SEDGEWICK 2009, prop. IX.12]. □

Exercice 22. Montrer que dans un anneau principal, un élément irréductible est premier.

Exercice 23. 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.

□ On prend $A = \mathbb{Z}$, $K = \mathbb{Q}$ et $k = \mathbb{F}_p$ pour p premier.

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.

- (i) Le polynôme $T^2 + p$ est irréductible sur \mathbb{Z} mais pas sur \mathbb{F}_p .
- (ii) Le polynôme $pT^2 + T$ est irréductible sur \mathbb{F}_p mais pas sur \mathbb{Z} .
- (iii) Le polynôme pT est irréductible sur \mathbb{Q} mais pas sur \mathbb{Z} .
- (iv) Le polynôme p est irréductible sur \mathbb{Z} mais pas sur \mathbb{Q} .

□

Exercice 24. Soient p un nombre premier et $f = T^d + a_1 T^{d-1} + \dots + a_d \in \mathbb{Z}[T]$ un polynôme tel que $p \mid a_i$ pour chaque $0 < i \leq d$ mais $p^2 \nmid a_d$. Montrer que f est irréductible dans $\mathbb{Q}[T]$. (Il s'agit du « **critère d'Eisenstein** ».)

□ D'après le lemme de Gauß, il suffit de montrer que le polynôme primitif f est irréductible dans $\mathbb{Z}[T]$. Or, une factorisation $f = gh$ donne par réduction modulo p une factorisation de T^d , nécessairement de la forme $T^r \cdot T^{d-r}$ avec $0 < r < d$. En particulier, $g(0)$ et $h(0)$ sont divisibles par p . Pourtant $g(0)h(0) = f(0) = a_d$ n'est pas divisible par p^2 . Absurde. □

Exercice 25. 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).)

□ En effet, $\Phi_p(X + 1) = ((1 + T)^p - 1)/T$ a ses coefficients divisibles par p , excepté le coefficient dominant, et son terme constant est $(T^p)'(1) = p$. On peut donc lui appliquer le critère d'Eisenstein. □

Exercice 26. Montrer que \mathbb{C} est algébriquement clos.

(Indication : on pourra commencer par montrer que si $f = 1 + z^r + a_{r+1}z^{r+1} + \dots + a_n z^n$, il existe $z \in \mathbb{C}$ tel que $|f(z)| < 1$.)

Exercice 27. Soit $n \geq 2$ un entier. Montrer que le discriminant du polynôme $T^n + aT + b$ est

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

(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 $\prod_i (ux_i + v) = \sum_i u^i \sigma_i(x_1, \dots, x_n) v^{n-i}$ où les σ_j sont les fonctions symétriques élémentaires.)

Exercice 28. 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.

Corps finis

Exercice 29. 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

$$\binom{i}{p} \equiv 0 \pmod{p}.$$

Exercice 30. Soit p un nombre premier.

- (i) Montrer que si $n = a_0 + a_1p + \dots + a_r p^r$ 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 $0 \leq a \leq b$, la valuation p -adique $v_p\left(\binom{a}{b}\right)$ du coefficient binomial est la somme des retenues de l'addition de a avec $b - a$, écrits en base p .

Exercice 31.

- (i) Trouver le plus petit nombre premier p tel que $\sum_{i=0}^{22} T^i$ soit irréductible dans $\mathbb{F}_p[T]$.
- (ii) Trouver les dix plus petits nombres premiers p tels que $\sum_{i=0}^{p-1} T^i$ soit irréductible dans $\mathbb{F}_2[T]$.

□(i) $p = 5$. La question revient à déterminer le plus petit p tel que le polynôme cyclotomique $\Phi_{23} = (T^{23} - 1)/(T - 1)$ soit irréductible sur \mathbb{F}_p . D'après 7.3.5, on veut donc que p soit un générateur de $(\mathbb{Z}/23\mathbb{Z})^\times$. Pour $p = 2$, les puissances sont $1, 2, 8, 16, 32, 64, 128, 256 = 3, 6, 12, 24 = 1$; pour $p = 3$, on a $1, 3, 27 = 4, 12, 36 = 13, 39 = 16, 48 = 2, 6, 18 = -5, -15 = 8, 24 = 1$. Dans ces deux cas, l'ordre n'est pas 22. Par contre, c'est le cas si $p = 5$.

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

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

Exercice 32. Montrer, ou expliquer comment montrer, que $T^5 - T + 1$ est un polynôme primitif sur \mathbb{F}_3 , c'est-à-dire un polynôme irréductible dont chaque racine est un générateur du groupe multiplicatif $\mathbb{F}_{3^5}^\times$.

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

Remarques :

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

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

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

□

Exercice 33. Pour $\mathbb{F} = \mathbb{F}_4, \mathbb{F}_8, \mathbb{F}_{27}$ ou \mathbb{F}_{25} , trouver un polynôme irréductible dans $\mathbb{F}_p[T]$ (où $p := \text{car.}(\mathbb{F})$) dont une racine α est primitive et écrire les puissances de α comme un polynôme en α de degré minimal.

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

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

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

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

□

Exercice 34. Soit $\mathbb{F}_{q^n} / \mathbb{F}_q$ une extension de degré $n \geq 1$. Montrer en comptant le nombre d'éléments de \mathbb{F}_{q^n} de degré $< n$ sur \mathbb{F}_q qu'il existe au moins un polynôme $f \in \mathbb{F}_q[T]$ irréductible degré n .

□ Il s'agit essentiellement de l'argument donné en 7.3.6 pour minorer la proportion de polynômes irréductibles. Le nombre d'éléments de \mathbb{F}_{q^n} de degré $< n$ est majoré par la somme des cardinaux des \mathbb{F}_{q^d} pour $d|n$. Au moins deux arguments possibles. (1) On remarque que $\sum_{d|n, d \neq n} q^d \leq \sum_{d < n} q^d < q^n$, par exemple par unicité de l'écriture en base q . (2) On remarque que chaque q^d est majoré par $\leq q^{n/2}$ et leur nombre est $\leq n$, par conséquent cette somme de cardinaux est inférieure ou égale à $nq^{n/2}$. Pour avoir la conclusion souhaitée, il suffit d'avoir $q^n > nq^{n/2}$, soit $q^{n/2} > n$, ce qui se produit dès que $2^n > n^2$, donc dès que $n > 4$. Pour les valeurs plus petites de n , on constate que $q^4 > q^2 + q$ et $q^3 > q$ et $q^2 > q$ (et $q > 0 \dots$) pour tout $q \geq 2$. □

Exercice 35.

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

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

- (ii) En déduire que $T^4 + 1$ est irréductible dans $\mathbb{Q}[X]$.
 (iii) Montrer que $T^4 + 1$ est réductible dans $\mathbb{F}_p[X]$ pour tout nombre premier p .
 (Indication : on rappelle que l'ensemble des carrés de \mathbb{F}_p^\times est un sous-groupe d'indice 2 de sorte que si $a, b \in \mathbb{F}_p$, alors a, b ou ab est un carré dans \mathbb{F}_p .)

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

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

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

Exercice 36. 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 37. ¶ Montrer que $T^{4n} + T^n + 1$ est irréductible sur \mathbb{F}_2 si et seulement si $n = 3^r 5^s$ pour des entiers $r, s \geq 0$.

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

Exercice 38. 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 $\frac{1}{3}p^3 + \frac{1}{2}p^2 + \frac{1}{6}p$.

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

Exercice 39. 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 40. 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 41. On fixe une clôture algébrique Ω de \mathbb{F}_p .

- (i) Rappeler pourquoi $\mathbb{F}_p = \{x \in \Omega : \text{Frob}_p(x) = x\}$.
(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 $p \equiv 1 \pmod{4}$.
(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 $p \equiv \pm 1 \pmod{8}$ ^①.

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

Exercice 42. 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.)

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

Exercice 43.

- (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 $\text{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$ en fonction de p et n .
(iii) Peut-on en déduire un calcul de $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})$ pour $N \geq 1$?

Exercice 44. Soit $P \in \mathbb{F}_p[X]$ un polynôme de degré d .

- (i) Montrer que P est irréductible dans $\mathbb{F}_p[X]$ si et seulement si P n'a pas de racine dans \mathbb{F}_{p^r} pour tout $r \leq \frac{d}{2}$.
(ii) (Application) Montrer que $\mathbb{F}_4 = \{0, 1, j, j^2\}$ avec $j^2 = 1 + j$. En déduire que les polynômes $1 + X^2 + X^5$, $1 + X^3 + X^5$, $1 + X + X^2 + X^3 + X^5$, $1 + X + X^2 + X^4 + X^5$, $1 + X + X^3 + X^4 + X^5$ et $1 + X^2 + X^3 + X^4 + X^5$ sont les polynômes irréductibles de degré 5 de $\mathbb{F}_2[X]$.

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

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

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

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

(ii) Le polynôme $T^2 + T + 1 \in \mathbb{F}_2[T]$ est irréductible, par exemple parce qu'il n'a pas de racine dans \mathbb{F}_2 ou, de façon un peu pédante, d'après l'exercice 42 ci-dessus. Le quotient $\mathbb{F}_2[T]/(T^2 + T + 1)$ est donc un corps de cardinal 4 et la classe j de T est bien comme annoncé. D'après le critère précédent, pour vérifier que les polynômes de degré 5 de l'énoncé sont irréductibles, il faut vérifier qu'ils n'ont pas de racine dans \mathbb{F}_2 – ce qui résulte du fait que leur terme constant est non nul et qu'ils ont un nombre impair de monôme – ni dans \mathbb{F}_4 . (On utilise le fait que $\lfloor 5/2 \rfloor = 2$.) On vérifie par le calcul que pour chacun de ces polynômes f , on a $f(j) \neq 0$. Comme $f(j^2) = f(j)^2$, on a aussi $f(j^2) \neq 0$ sans avoir besoin de refaire le calcul. L'exercice demande de vérifier que ces polynômes sont les seuls qui soient irréductibles de degré 5. Il résulte de la formule de Gauß (§ 7.3.6) qu'il y en a $\frac{1}{5}(2^5 - 5) = 6$. On les a donc tous trouvés. Plus simplement, on peut faire une liste des autres polynômes et vérifier qu'ils ont une racine dans \mathbb{F}_2 ou \mathbb{F}_4 . (Ici $\mathbb{F}_2 \subseteq \mathbb{F}_4$ donc il s'agit en fait de chercher des racines dans \mathbb{F}_4 mais on rappelle qu'en général l'inégalité $a \leq b$ n'entraîne pas l'existence d'un plongement $\mathbb{F}_{p^a} \subseteq \mathbb{F}_{p^b}$.) □

Exercice 45. Montrer que $T^6 + T^4 + T + 1 \in \mathbb{F}_2[T]$ est le produit de trois polynômes irréductibles distincts.

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

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

□

Exercice 46. Soit p un nombre premier fixé. Quelle est la probabilité qu'un polynôme unitaire $f \in \mathbb{F}_p[T]$ de degré d soit un produit de polynômes irréductibles de degrés 1 ou 2 ? Évaluer ces nombres (rationnels) pour $p = 2$ et $d \leq 7$.

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

$$\sum_{a+2b=d} \binom{n_1}{a} \binom{n_2}{b}$$

où $\binom{n}{r} = \binom{r+n-1}{r}$ est le cardinal des multiensembles de cardinal r pris dans un ensemble de cardinal n . Par exemple, pour $d = 3$, on trouve $\frac{2}{3}p^3 + \frac{1}{3}p$, qui est

bien égal à $p^3 - \frac{1}{3}(p^3 - p)$ (cf. 7.3.6). La probabilité est donc $\frac{2}{3} + \frac{1}{3p^2}$. Lorsque $p = 2$ et d quelconque, on trouve $2^{-d} \sum_{a+2b=d} (a+1)$. Par exemple, pour $d = 3$, on (re)trouve $\frac{3}{4}$. Le calcul des autres valeurs est laissé au lecteur intéressé. \square

Exercice 47.

- (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 $T^6 - 2T^4 + 3T^3 - T^2 - T - 2 \in \mathbb{F}_7[T]$.

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

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

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

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

\square

Exercice 48. (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 $P \pmod{\ell}$ soit scindé.

(Indication : on se ramène à montrer que si $A := \text{Adu}_{\mathbb{Z}}(P)$ 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.)

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

Exercice 49. Calculer le nombre de solutions de $y^2 + y = x^3$ dans \mathbb{F}_2 et \mathbb{F}_4 . Montrer que si d est impair, le nombre de solutions dans \mathbb{F}_{2^d} est 2^d .

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

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

Exercice 50. 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 $q \rightarrow 1$ (dans les réels) ?

Exercice 51. Soient \mathbb{F} un corps fini de cardinal q et $P \in \mathbb{F}[T]$ un polynôme de degré d , supposé tel que $P(0) = 0$ pour simplifier.

(i) Soit $Q(X) := \prod_{\lambda \in \mathbb{F}} (X - P(\lambda))$. Montrer que les coefficients de Q de degré $q - i$ tel que $0 < di < q - 1$ sont nuls.

(Indication : on pourra considérer $\prod_{\lambda \in \mathbb{F}} (X - P(t\lambda)) = \sum_i c_i(t) X^{q-i}$, où $c_i \in \mathbb{F}[t]$ est de degré $\leq di$, et remarquer que la fonction c_i est constante sur \mathbb{F}^\times .)

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

□ (Esquisse)

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

Exercice 52. 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 $p - \left(\frac{-ab}{p}\right)$, où le terme de droite désigne le symbole de Legendre considéré en 7.5.

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

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

Exercice 54.

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

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

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

Exercice 55.

- (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 $n \rightarrow +\infty$. (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 $\prod_{\ell} (1 - \ell^{-1}) = 0$, 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 56. 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 57.

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

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

(ii) En utilisant $x^2 - 1 = (x - 1)(x + 1)$, on voit que $2^{2^n-2} - 1$ est divisible par $2^{2^{n-1}-1} - 1$. Comme l'exposant $2^{n-1} - 1$ est un multiple de n , l'entier $x^n - 1$ divise

$x^{2^{n-1}-1} - 1$ pour tout x . En particulier pour $x = 2$. Noter que $2^n - 1$ est bien composé (=non premier) car n l'est. \square

Exercice 58. (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 .

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

Exercice 59. ¶ 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 $\mathbb{Z}[T]$.

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

Exercice 60. (amusement) 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.

□(b) Sous l'hypothèse faite, $\mu_3(\mathbb{F}_p)$ est de cardinal 3 : c'est l'unique sous-groupe de \mathbb{F}_p^\times de cardinal 3. Si $x^3 = 2$, les autres solutions sont les ζx pour $\zeta \in \mu_3(\mathbb{F}_p)$. La conclusion en résulte aussitôt. □

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 $B(f)$ de f .

□ Si t est la classe de T dans $\mathbb{F}_p[T]/(f)$, on a $t^8 = 1$ et $t^4 = -1$. On vérifie immédiatement que la matrice de Frob_p dans la base $1, t, t^2, t^3$ est l'identité si $p \equiv 1 \pmod{8}$, $\text{diag}(1, -1, 1, -1)$ si $p \equiv 5 \pmod{8}$, etc. □

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.

□(a) L'image de $f(\mathbb{Z})$ dans \mathbb{F}_2 est $\{1\}$. (b) Considérer par exemple $2T - 1$. □

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 .

□(a) $a = -1$, $b = 2$. (b) $g = T^3 - T + 2$. (c) $f(\omega) = \omega^2 + \omega + \omega^2 + \omega + 2 = 2(\omega^2 + \omega + 1) = 0$. □

Examen 2016-2017

Exercice 1. Soit p un nombre premier. Montrer que si $A = \mathbb{Z}$, $K = \text{Frac}(A) = \mathbb{Q}$ 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 irréductible, f l'est aussi dans $A[T]$.

□

- (i) Le polynôme $T^2 + p$ est irréductible sur \mathbb{Z} mais pas sur \mathbb{F}_p .
- (ii) Le polynôme $pT^2 + T$ est irréductible sur \mathbb{F}_p mais pas sur \mathbb{Z} .
- (iii) Le polynôme p est irréductible sur \mathbb{Z} mais pas sur \mathbb{Q} .
- (iv) Le polynôme pT est irréductible sur \mathbb{Q} mais pas sur \mathbb{Z} .

□

Exercice 2. Soient $d \geq 4$ 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 $\mathbb{Z}[T]$.

□ On raisonne par l'absurde. Si f n'est pas irréductible, il existe une factorisation $f = uv$ avec $u, v \in \mathbb{Z}[T]$, unitaires de degrés > 0 . En réduisant modulo p_1 et p_2 , on obtient $u_1 v_1 = g_1 h_1$ et $u_2 v_2 = g_2 h_2$. Les termes de droite étant des factorisations en polynômes irréductibles unitaires, on a nécessairement $\{u_1, v_1\} = \{g_1, h_1\}$ et $\{u_2, v_2\} = \{g_2, h_2\}$. En particulier, en passant aux degrés, on a $\{\deg(u), \deg(v)\} = \{1, d - 1\} = \{2, d - 2\}$. C'est impossible lorsque $d \geq 4$. □

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.)

□ On trouve la matrice, dans une base e_1, e_x, e_y, e_{xy} ,

$$\begin{pmatrix} 0 & b & d & 0 \\ 1 & a & 0 & d \\ 1 & 0 & c & b \\ 0 & 1 & 1 & a+c \end{pmatrix}$$

de polynôme caractéristique (sauf erreur) égal à $T^4 + (-2a - 2c)T^3 + (a^2 + 3ac + c^2 - 2b - 2d)T^2 + (-a^2c - ac^2 + 2ab + 2bc + 2ad + 2cd)T - abc - bc^2 - a^2d - acd + b^2 - 2bd + d^2$. □

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.)

□

- (i) On a $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{(p-1)/2} \times \left(\frac{p}{3}\right) \times (-1)^{(3-1)/2 \cdot (p-1)/2}$. La conclusion en résulte aussitôt.
Attention : on ne peut pas appliquer la réciprocité quadratique à $\ell = -3$, qui n'est pas un nombre premier.
- (ii) (esquisse) On a $(2j+1)^2 = -3$ et $2j+1$, vu dans une clôture algébrique, appartient à \mathbb{F}_p si et seulement si $j \in \mathbb{F}_p$, si et seulement si $j^p = j$, etc.

□

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 $n \rightarrow +\infty$.
(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 : $\prod_{\ell < x} (1 - \ell^{-1}) \rightarrow 0$ lorsque $x \rightarrow +\infty$, où ℓ parcourt les nombres premiers.)

□

- (i) La probabilité est $\varphi(p-1)/(p-1)$. En effet, $\#\mathbb{F}_p^\times$ est de cardinal $p-1$. Parmi ses éléments, $\varphi(p-1)$ d'entre eux sont générateurs : le nombre de générateurs du groupe cyclique $\mathbb{Z}/n\mathbb{Z}$ est $\varphi(n)$ (cf. 2.1.2).
- (ii) (esquisse) Si $p-1 = \ell_1 \cdots \ell_r n$, on a $\varphi(p-1)/(p-1) = \prod_{\ell \mid \ell_1 \cdots \ell_r n} (1 - \ell^{-1}) \leq (1 - \ell_1^{-1}) \cdots (1 - \ell_r^{-1})$.
On utilise alors le fait admis et la proposition du §7.3.5.

□

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.

□

- (i) $\mathbb{Z}/p^2\mathbb{Z}$, $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p^2$, \mathbb{F}_p , $\mathbb{F}_p[T]/(T^2)$.
- (ii) Seulement 1. (À isomorphisme près, il n'y a qu'un corps fini de cardinal q .)
- (iii) En effet, un tel anneau A est isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$ ou bien est une \mathbb{F}_p -algèbre et $A = \mathbb{F}_p[x]$ pour n'importe quel $x \in A \setminus \mathbb{F}_p$. Notons f le polynôme minimal de x ; trois cas se présentent : (1) f est irréductible — et $A \simeq \mathbb{F}_{p^2}$ —, (2) f est scindé à racines simples — et $A \simeq \mathbb{F}_p[X]/(X-a)(X-b) \simeq \mathbb{F}_p^2$ —, et (3) f est scindé à racine double — et $A \simeq \mathbb{F}_p[X]/((X-a)^2) \simeq \mathbb{F}_p[X]/(X^2)$.

□

QCM

1. Existe-t-il un corps à 25 éléments ?
 oui non
2. L'anneau $\mathbb{Z}/25\mathbb{Z}$ est-il un corps ?
 oui **non**
3. Le groupe abélien $\mathbb{Z}/12\mathbb{Z}$ est-il isomorphe au groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$?
 oui **non**
4. Le groupe abélien $\mathbb{Z}/12\mathbb{Z}$ est-il isomorphe au groupe $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$?
 oui non
5. Existe-t-il un morphisme de corps $\mathbb{F}_9 \rightarrow \mathbb{F}_{27}$?
 oui **non**
6. Soit $p > 3$ un nombre premier. La somme $\sum_{x \in \mathbb{F}_p} x^2$ est égale à
 -1 **0** 1 2 cela dépend de p
7. Parmi les six polynômes ci-dessous de $\mathbb{F}_2[T]$ combien sont irréductibles ?
 $1+T^2+T^5, 1+T^3+T^5, 1+T^2+T^4, 1+T+T^2, 1+T+T^4+T^6, 1+T+T^3.$
 0 1 2 3 **4** 5 6
8. Combien existe-t-il de morphismes de corps de $\mathbb{F}_{256} \rightarrow \mathbb{F}_{65536}$?
 0 1 2 4 **8** 16 256 65536

Examen 2017-2018

Exercice 1. Soient $k = \mathbb{F}_{16}$ un corps à 16 éléments et $A = \mathbb{Z}/16\mathbb{Z}$.

- (i) Calculer le cardinal de l'ensemble $\{x \in k : x^3 = 1\}$.
- (ii) Calculer le cardinal de l'ensemble $\{a \in A : a^3 = 1\}$.

□

- (i) Il est clair que le cardinal de $\mu_3(k)$ est égal à 3. Par exemple parce qu'il est en bijection avec l'ensemble $\{x \in \mathbb{Z}/15\mathbb{Z} : 3x = 0\}$.
- (ii) Le groupe A^\times est de cardinal $\varphi(16) = 8$ donc il n'y a qu'une seule solution : $a = 1$.

□

Exercice 2. Soient $k = \mathbb{F}_{16}$ un corps à 16 éléments et $A = \mathbb{Z}/16\mathbb{Z}$.

- (i) Quel est le nombre de sous-corps (non nécessairement stricts) de k ?
- (ii) Pour chacun de ces sous-corps k_i , trouver un polynôme unitaire $f_i \in \mathbb{F}_2[T]$ tel que k_i soit isomorphe à $\mathbb{F}_2[T]/(f_i)$.
- (iii) Quel est le nombre de sous-corps de A ?
- (iv) Quel est le nombre de corps K (à isomorphisme près) pour lesquels il existe un morphisme surjectif $A \twoheadrightarrow K$?

□

- (i) Il y a exactement 3 sous-corps, de cardinal 2, 4 et 16.
- (ii) Les polynômes $T, T^2 + T + 1$ et $T^4 + T + 1$ conviennent (cf. photocopié).
- (iii) Il n'y a pas de sous-corps (nécessairement de caractéristique deux) car un morphisme de corps $K \rightarrow A$, devrait envoyer 1_K sur 1_A et donc $2 \cdot 1_K = 0_K$ sur $2 \cdot 1_A \neq 0_A$.
- (iv) Il y a un seul quotient qui soit un corps : $A/2A = \mathbb{F}_2$.

□

Exercice 3.

- (i) Soit k un corps fini de caractéristique 2. Tout élément de k est-il un carré, c'est-à-dire de la forme x^2 , pour un $x \in k$? (Démontrer ce résultat ou donner un contre-exemple.)
- (ii) Soit k un corps fini de caractéristique $\neq 2$. Tout élément de k qui n'est pas un carré est-il nécessairement primitif, c'est-à-dire générateur du groupe multiplicatif k^\times ? (Démontrer ce résultat ou donner un contre-exemple.)
- (iii) Soit $p = 65537 = 2^{2^4} + 1$. Montrer que 5 est primitif, c'est-à-dire que $\langle 5 \rangle = \mathbb{F}_p^\times$.
Indication : on pourra admettre que 5 est un carré modulo p si et seulement si p est un carré modulo 5.

□

- (i) Oui : l'endomorphisme de Frobenius est injectif donc surjectif.
- (ii) Non : -1 n'est souvent pas un carré (par exemple dans \mathbb{F}_7 , car $p \equiv -1 \pmod{4}$) mais il est d'ordre 2 (et n'engendre donc pas \mathbb{F}_7^\times).
- (iii) Le nombre $p - 1$ étant une puissance de 2, tout élément qui n'est pas un carré est primitif : dans $(\mathbb{Z}/2^n\mathbb{Z}, +)$ les générateurs correspondent aux nombres impairs, c'est-à-dire non multiples de 2. Il suffit donc de montrer que 5 n'est pas un carré modulo p , ou encore d'après le fait admis (réciprocité quadratique) que $65537 \equiv 2 \pmod{5}$ n'est pas un carré modulo 5. Modulo 5, les seuls carrés sont 1 et -1 .

□

Exercice 4. Soient q une puissance d'un nombre premier, \mathbb{F}_q un corps de cardinal q et $f(T) = T^2 + aT + b \in \mathbb{F}_q[T]$. Montrer que f est irréductible dans $\mathbb{F}_q[T]$ si et seulement si il divise $T^q + T + a$.

□ Si f , factorisé en $(T - \alpha)(T - \beta)$ dans un surcorps, est irréductible alors β est différent de α et égal à son conjugué $\text{Frob}_q(\alpha) = \alpha^q$. Ainsi, l'égalité $\alpha + \beta = -a$ (relation coefficients-racines) devient $\alpha^q + \alpha + a = 0$: le polynôme minimal f de α divise donc le polynôme $T^q + T + a$.

Réciproquement, si f divise $T^q + T + a$ il est à racines simples (car $(T^q + T + a)' = 1$) et si α est une racine de f , on a $\alpha^q = -\alpha - a = \beta$. Comme $\beta \neq \alpha$, on a donc $\alpha \notin \mathbb{F}_q$ (car il n'est pas fixe sous le Frobenius) et f est bien irréductible. □

Exercice 5. Soient q une puissance d'un nombre premier, \mathbb{F}_q un corps de cardinal q et $f \in \mathbb{F}_q[T]$ un polynôme unitaire de degré $n \geq 1$. On définit une matrice carrée $M_f = (a_{i,j})$ de taille $n \times n$ à coefficients dans \mathbb{F}_q par les relations :

$$T^{iq} \equiv \sum_{j=0}^{n-1} a_{i,j} T^j \pmod{f}.$$

Montrer que si f est irréductible, alors le polynôme caractéristique de M_f est $X^n - 1$.

Indication : on pourra admettre que pour tout $d \geq 1$, il existe $\alpha \in \mathbb{F}_{q^d}$ tel que les $1, \alpha, \alpha^q, \alpha^{q^2}, \dots, \alpha^{q^{d-1}}$ forment une base de \mathbb{F}_{q^d} sur \mathbb{F}_q .

□ Puisque $\mathbb{F}_q[T]/(f)$ est isomorphe à \mathbb{F}_{q^n} , la question revient à montrer que l'endomorphisme de Frobenius $\text{Frob}_q : \mathbb{F}_{q^n} \rightarrow \mathbb{F}_{q^n}$ a pour polynôme caractéristique (vu comme application \mathbb{F}_q -linéaire) $X^n - 1$. Trivialement, on a $\text{Frob}_q^n = \text{Id}$. Pour conclure, il suffit de montrer que le polynôme minimal de Frob_q est $X^n - 1$. L'indépendance linéaire de $\text{Id}, \text{Frob}_q, \dots, \text{Frob}_q^{n-1}$ — qui résulte de l'indication — l'entraîne immédiatement. □

Exercice 6.

Sur \mathbb{F}_2 , on considère le code linéaire C de matrice génératrice :

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

- (i) Déterminer la dimension et la longueur de C .
- (ii) Coder le message $(1, 0, 1, 0)$.
- (iii) Déterminer une matrice de contrôle du code.
- (iv) Quelle est la distance minimale du code ? Combien d'erreurs permet-il de détecter ? Combien d'erreurs permet-il de corriger ?
- (v) En déduire une table de décodage.
- (vi) Le mot $(1, 1, 0, 0, 1, 0, 0, 1)$ est reçu.
 - (a) Quel est son syndrome ? Est-ce un mot du code ?
 - (b) En faisant les hypothèses nécessaires, quel est le message initialement envoyé ?
- (vii) On considère l'extension paire de C . Quelle est la distance minimale du nouveau code ?

□

- (i) La matrice G est de taille 8,4 donc C est de dimension 4 et de longueur 8.
(ii) On réalise le produit matriciel

$$G \cdot \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}.$$

Le mot de code est alors $(1, 0, 1, 0, 0, 1, 1, 1)$.

- (iii) La matrice G est donnée sous forme systématique, une matrice de contrôle est alors :

$$H = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

- (iv) Une ou deux colonnes de H sont toujours linéairement indépendantes et les colonnes 1 4 et 7 sont linéairement dépendantes. La distance minimale du code est 3. On peut donc détecter 2 erreurs et en corriger une.
(v) Pour cela, on détermine les syndromes de tous les mots de poids 1 :

Mots non nuls de poids ≤ 1	Syndrome associé
$(1,0,0,0,0,0,0,0)$	$(1,0,1,1)$
$(0,1,0,0,0,0,0,0)$	$(0,1,1,0)$
$(0,0,1,0,0,0,0,0)$	$(1,1,0,0)$
$(0,0,0,1,0,0,0,0)$	$(1,0,0,1)$
$(0,0,0,0,1,0,0,0)$	$(1,0,0,0)$
$(0,0,0,0,0,1,0,0)$	$(0,1,0,0)$
$(0,0,0,0,0,0,1,0)$	$(0,0,1,0)$
$(0,0,0,0,0,0,0,1)$	$(0,0,0,1)$

- (vi) (a) On a :

$$H \cdot \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}.$$

Le syndrome n'est pas nul, ce n'est pas un mot de code.

- (b) Pour pouvoir décoder, il faut supposer qu'une seule erreur a été commise (le code est 1-correcteur). Le mot de poids 1 ayant le même syndrome que le mot reçu est alors l'erreur commise. Le mot de code est donc :

$$(1, 1, 0, 0, 1, 0, 0, 1) + (0, 0, 0, 0, 0, 1, 0, 0) = (1, 1, 0, 0, 1, 1, 0, 1).$$

Comme le codage est systématique, le message initial est :

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

- (vii) On est dans le cas binaire et la distance de C est 3 qui est impaire donc la distance du code étendu est 4.

□

Exercice 7.

On considère le polynôme g de $\mathbb{F}_2[X]$ suivant :

$$g = X^3 + X^2 + 1.$$

- (i) Montrer que g est irréductible sur \mathbb{F}_2 .
(ii) Justifier que le polynôme cyclotomique Φ_7 est :

$$X^6 + X^5 + X^4 + X^3 + X^2 + X + 1.$$

- (iii) Montrer que g divise Φ_{7, \mathbb{F}_2} , l'image de $\Phi_7 \in \mathbb{Z}[X]$ dans $\mathbb{F}_2[X]$.
(iv) Soit α un élément primitif d'un corps à 8 éléments. On suppose que α est une racine de g . Pour tout $l \in \llbracket 0, 6 \rrbracket$, exprimer α^l en fonction de $1, \alpha, \alpha^2$.
(v) On considère le code cyclique C de longueur 7 et de polynôme générateur g . On suppose que les messages sont codés en utilisant la méthode de codage efficace.
(a) Quelle est la dimension du code ?
(b) Montrer que C est un code BCH et déterminer sa distance prescrite.
(c) Coder le message $(1, 0, 1, 0)$.
(d) Le mot $(0, 1, 0, 0, 0, 0, 1)$ est reçu. En faisant les hypothèses nécessaires, déterminer le message envoyé.

□

- (i) g est de degré 3 et ne possède pas de racine dans \mathbb{F}_2 donc est irréductible.
(ii) On sait que $X^7 - 1 = \Phi_1 \times \Phi_7$ et $\Phi_1 = X - 1$. Donc,

$$\Phi_7 = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1.$$

- (iii) On a :

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

Donc g divise Φ_7 .

- (iv) En utilisant la relation $\alpha^3 + \alpha + 1 = 0$, on a :

$$\begin{array}{ll} \alpha^0 = 1 & \alpha^4 = \alpha^2 + \alpha + 1 \\ \alpha^1 = \alpha & \alpha^5 = \alpha + 1 \\ \alpha^2 = \alpha^2 & \alpha^6 = \alpha^2 + \alpha \\ \alpha^3 = \alpha^2 + 1 & \end{array}$$

- (v) (a) g est de degré 3 donc C est de dimension $7 - 3 = 4$.
(b) D'après la question (iv), on a :

$$g = (X - \alpha) \times (X - \alpha^2) \times (X - \alpha^4).$$

Le polynôme g correspond donc à la classe cyclotomique $\{1, 2, 4\}$ de $\mathbb{Z}/7\mathbb{Z}$. On en déduit que C est un code BCH de distance prescrite 3.

- (c) Ce mot est associé au polynôme $X^2 + 1$, on fait alors la division euclidienne de $X^3 \times (X^2 + 1)$ par g :

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

Le mot de code est donc $(0, 1, 1, 1, 0, 1, 0)$.

- (d) Le polynôme associé est $m(X) = 1 + X^5$. On calcule ses syndromes :

$$\begin{array}{ll} m(\alpha) & = 1 + \alpha^5 = \alpha \\ m(\alpha^2) & = 1 + \alpha^{10} = \alpha^2. \end{array}$$

Un des syndromes de m n'est pas nul donc des erreurs ont été commises.

Pour pouvoir retrouver le message initial, on suppose que le nombre d'erreurs est inférieur à $\delta/2$. On suppose donc qu'une seule erreur a été commise.

Le polynôme syndrome est : $S(Z) = \alpha + \alpha^2.Z$. Pour déterminer le polynôme localisateur, on applique l'algorithme d'Euclide.

$$Z^2 = (\alpha^2.Z + \alpha) \times (\alpha^5.Z + \alpha^4) + \alpha^5 + 1.$$

Le degré du reste est inférieur strictement à 1, donc le polynôme localisateur est :

$$\alpha^{-4} \times (\alpha^5.Z + \alpha^4) = \alpha.Z + 1.$$

La seule racine du polynôme localisateur est α^{-1} . Il y a donc eu une erreur en position 1. Le mot de code envoyé est :

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

Comme le codage est celui qui permet de retrouver le message à la fin du mot de code, le message envoyé est :

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

□