有限域
Corps finis
上海/Shanghai, 2018-11[1]

Fabrice ORGOGOZO[2].

version : 539202a 2019-09-08 11:40:49 +0200
http://fabrice.orgogozo.perso.math.cnrs.fr/articles/Shanghai4.pdf[3]

Table des matières

① Cours (séances de 1h40) : 2018-11-13,14,15[2],16[2],19,20,21[2],22

② « Fabrice Orgogoço »=法布里斯·奥尔戈戈索.

③ Versions antérieures, contenant des sujets non traités ici :
http://fabrice.orgogozo.perso.math.cnrs.fr/articles/Shanghai3.pdf
http://fabrice.orgogozo.perso.math.cnrs.fr/articles/Shanghai2.pdf
http://fabrice.orgogozo.perso.math.cnrs.fr/articles/Shanghai1.pdf

cours n° 1. $\mathbb{Z}/n\mathbb{Z}$ jusqu'à l'algorithme d'Euclide
cours n° 2. Lamé [Euclide], Karatsuba, groupes cycliques, RSA
cours n° 3. RSA [exemple], exercices : $\varphi(n) \leftrightarrow n = p\ell$, Carmichael [+ mention Granville et collab.], $\mathbb{Z}/9\mathbb{Z}$ et $\mathbb{Z}/11\mathbb{Z}$, $S_A P_A = \mathrm{Id}$, pile ou face à distance [début].
cours n° 4. pile ou face à distance [fin] ; caractéristique ; cardinal des corps finis ; $\mathbb{F}_2[T]/(T^3 + T + 1)$ [début].
cours n° 5. $\mathbb{F}_8$ [fin] ; 2 corps à 49 éléments ; motivation pour $\mathbb{F}_p \subseteq \mathbb{F}_q$; énoncé existence polynômes irréductibles de tous degrés ; $\mathbb{F}_2[T]/(T^4 + T + 1)$ [début].
cours n° 6. $\mathbb{F}_{16}$ [fin] ; polynômes irréductibles de degré $\leqslant 3$; $(a + b)^p = a^p + b^p$.
cours n° 7. rappels sur $k[T]/(f)$ (calcul inverse ; corps si et seulement si f irréductible [$\leftrightarrow \mathbb{Z}/6\mathbb{Z}$, $6 = 2 \cdot 3$], exemple dans $\mathbb{F}_8$), définitions et notations de théorie des corps [k, A corps], stabilité des algébriques par somme et produit [sans démonstration].
cours n° 8. rappels sur les extensions algébriques, base télescopique, corps de décomposition ; existence et unicité corps finis, rappels sur racines simples, structure $K^\times$ [énoncé]
cours n° 9. $K^\times$ cyclique ; applications : $K = k[x]$, existence de polynômes irréductibles ; $\mathbb{F}_q$ comme points fixes ; exercices : $\sqrt{(-1)} \in ?\mathbb{F}_p$.
cours n° 10. $T^4 + T^3 + T^2 + T + 1 \in \mathbb{F}_2[T]$; polynôme minimal et orbite du Frobenius ; Φ_ℓ ; $T^5 - T + 1 \in \mathbb{F}_3[T]$; critère de Ben-Or.
cours n° 11. graphe d'inclusion des corps finis ; cardinal de $\mathrm{GL}_2(\mathbb{F}_p)$ et suite de Fibonacci mod. 2 ; critère de Butler

Remerciements. Quelques exemples et le pseudo-code de l'algorithme d'Euclide sont tirés essentiellement *verbatim* de notes de David Madore, à qui je dois notamment l'idée de présenter le protocole de partage de secret de Shamir, les nimbres de Conway, et le crypto-système de McEliece. La démonstration du théorème de Karatsuba est tirée de notes de Joël Riou. Je les en remercie chaleureusement, ainsi que pour les discussions que nous avons eues sur des sujets connexes.

Les paragraphes ou exercices précédés du pied-de-mouche « ¶ » sont plus difficiles. Comme les notes en fin de sections, on peut en omettre la lecture sans compromettre la compréhension du reste du cours.

1. L'anneau $\mathbb{Z}/n\mathbb{Z}$

1.1. Définition et premières propriétés.

1.1.1. Soit $n \in \mathbb{N} = \{0, 1, 2, 3, \dots\}$ un entier naturel. On dit que deux entiers relatifs $x, y \in \mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ sont **congrus modulo** n, et on note[①] $x \equiv y \pmod{n}$, si leur différence est divisible par n. (Par exemple, deux entiers sont congrus modulo 2 si et seulement si ils ont même *parité*.) On dit aussi que x et y sont dans la même **classe de congruence (modulo n)**, la classe de congruence d'un entier relatif x étant, par définition,

$$\overline{x} := \{y \in \mathbb{Z} : y \equiv x \pmod{n}\} = \{x + kn, k \in \mathbb{Z}\}.$$

Si $n \geqslant 1$, tout entier $x \in \mathbb{Z}$ s'écrit de façon unique sous la forme $x = an + b$ avec $a \in \mathbb{Z}$ et $0 \leqslant b < n$ entier : il est donc congru à un unique entier dans l'ensemble $\{0, 1, \dots, n-1\}$; autrement dit, il y a n classes de congruence : $\overline{0}, \overline{1}, \dots, \overline{n-1}$. La structure d'anneau sur $\mathbb{Z}$, définie par l'addition et la multiplication des entiers relatifs induit de telles opérations sur l'ensemble $\mathbb{Z}/n\mathbb{Z}$ (lire : « Z modulo n Z ») des classes de congruences : il suffit de poser

$$\overline{x} + \overline{y} := \overline{x + y} \text{ et } \overline{x} \cdot \overline{y} := \overline{x \cdot y},$$

où l'addition (resp. la multiplication) à droite du signe « := » est l'opération usuelle, celle à gauche étant l'opération à définir.

1.1.2. Notons que ces définitions n'ont de sens que si l'on vérifie que, si $x \equiv x' \pmod{n}$ et $y \equiv y' \pmod{n}$, alors $x + y$ (resp. $x \cdot y$) est congru à $x' + y'$ (resp. $x' \cdot y'$) modulo n. Ceci est vrai et résulte immédiatement des faits suivants : (a) la somme de deux entiers relatifs multiples de n est un multiple de n (b) le produit d'un multiple de n par un entier relatif quelconque est un multiple de n.

Non seulement l'ensemble $\mathbb{Z}/n\mathbb{Z}$ est ainsi équipé d'une structure d'anneau mais cette structure est compatible, par définition, avec celle de $\mathbb{Z}$: l'application

$$\mathbb{Z} \twoheadrightarrow \mathbb{Z}/n\mathbb{Z}, \ x \mapsto \overline{x}$$

est un *morphisme d'anneaux* (c'est-à-dire : transforme somme en somme, produit en produit et envoie l'unité [pour la multiplication] sur l'unité). (L'application [ensembliste] $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ étant surjective — d'où l'usage du symbole « $\twoheadrightarrow$ » —, c'est même la seule structure d'anneau sur $\mathbb{Z}/n\mathbb{Z}$ compatible au sens précédent avec celle de $\mathbb{Z}$.)

1.1.3. Insistons sur le fait que l'*ensemble* $\mathbb{Z}/n\mathbb{Z}$ est (pour $n \geqslant 1$) en bijection avec l'ensemble $\{0, \dots, n-1\}$ des restes de divisions euclidiennes [欧几里得除法 ou 辗转相除法] par n mais que ce choix de représentants des classes de congruence est arbitraire : on aurait *par exemple* pu choisir les entiers relatifs $1, \dots, n$ ou $-\lfloor \frac{n-1}{2} \rfloor, \dots, \lfloor \frac{n}{2} \rfloor$. D'ailleurs, on ne peut se contenter de manipuler ces seuls représentants lorsque l'on fait des calculs algébriques : par exemple, pour calculer $\overline{2} \cdot \overline{3} = \overline{1}$ dans $\mathbb{Z}/5\mathbb{Z}$, on considère la classe de l'entier $2 \times 3 = 6 \notin \{0, \dots, 4\}$, qui est congru à $1 \pmod{5}$.

① On s'autorise à écrire simplement $x \equiv y$ s'il n'y a pas d'ambiguïté sur le choix de n.

1.1.4. Étudions maintenant quelques propriétés de l'anneau $\mathbb{Z}/n\mathbb{Z}$, où $n \geqslant 1$ est un entier fixé. Tout d'abord, il hérite de $\mathbb{Z}$ la propriété d'être *commutatif* : $ab = ba$ pour toute paire $a, b \in \mathbb{Z}/n\mathbb{Z}$. Par contre, il n'est en général pas **intègre** : le produit de deux éléments non nul peut être nul. Par exemple, $\overline{2} \cdot \overline{2} = 0$ dans $\mathbb{Z}/4\mathbb{Z}$.

Il est ici utile d'introduire le vocabulaire suivant : un élément a d'un anneau A est dit **diviseur de zéro** (resp. **inversible**) s'il existe $b \neq 0$ tel que $ab = 0$ (resp. s'il existe b tel que $ab = 1$; on écrit alors : $a \in A^\times$). Un diviseur de zéro n'est jamais inversible. La réciproque est fausse : un élément non diviseur de zéro n'est pas forcément inversible, par exemple $2 \in \mathbb{Z}$ n'est pas inversible (dans $\mathbb{Z}$).

Cependant, dans un anneau *fini* A — et c'est le cas de $\mathbb{Z}/n\mathbb{Z}$ — un élément a qui n'est pas diviseur de zéro est automatiquement inversible : cela résulte du fait que l'application de multiplication $x \mapsto ax$, $A \to A$ est alors injective donc bijective ; en particulier l'unité 1_A de A est dans l'image.

1.2. Inversibles de $\mathbb{Z}/n\mathbb{Z}$.

1.2.1. Soit $a \in \mathbb{Z}$ un entier. Il est clair que si a est inversible dans $\mathbb{Z}/n\mathbb{Z}$ — c'est-à-dire si son image $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ l'est — alors l'entier a est *premier à* n. En effet, l'existence d'un $b \in \mathbb{Z}$ tel que $\overline{a} \cdot \overline{b} = 1_{\mathbb{Z}/n\mathbb{Z}}$ est équivalente à l'existence d'une paire $(b, k) \in \mathbb{Z}^2$ telle que $ab = 1 + kn$ et tout diviseur commun à a et n divise alors 1.

Réciproquement, si a et n sont **premiers entre eux** [互素] — ce que l'on note classiquement « $(a, n) = 1$ » mais que nous noterons « $a \perp n$ » — il existe une **relation de Bézout** (produite par l'algorithme d'Euclide rappelé plus bas)

$$au + nv = 1$$

entraînant l'égalité $\overline{a} \cdot \overline{u} = \overline{1} (= 1_{\mathbb{Z}/n\mathbb{Z}})$.

1.2.2. Exemple : dans $\mathbb{Z}/10\mathbb{Z}$, les éléments $\bar{1}, \bar{3}, \bar{7}, \bar{9}$ sont inversibles, et leurs inverses sont $\bar{1}^{-1} = \bar{1}, \bar{3}^{-1} = \bar{7}, \bar{7}^{-1} = \bar{3}, \bar{9}^{-1} = \bar{9}$.

1.2.3. En général, on a l'inclusion $(\mathbb{Z}/n\mathbb{Z})^\times \subseteq \mathbb{Z}/n\mathbb{Z} \smallsetminus \{0\}$ des inversible dans l'ensemble des éléments non nuls. S'il y a égalité, on dit que l'anneau est un **corps** : les éléments non nuls sont inversibles[①]. D'après ce qui précède, $\mathbb{Z}/n\mathbb{Z}$ est un corps (ou, de manière équivalente ici, intègre) si et seulement si tous les entiers $0 < a < n$ sont premiers à n, ce qui se produit si et seulement si n est un nombre premier.
Si p est un nombre premier, on note $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$ à p éléments. L'objet de ces notes est d'étudier de tels corps et de présenter quelques-unes de leurs applications.

1.3. Le théorème chinois.

Comme on l'a vu, la structure de l'anneau $\mathbb{Z}/n\mathbb{Z}$ dépend des propriétés arithmétiques de l'entier n ; ce lien est précisé par le **théorème (des restes) chinois** [中国剩余定理][②].

① . Un **corps** [域] est un anneau (commutatif) $k \neq 0$ tel que tout élément non nul soit inversible : $k^\times = k - \{0_k\}$.

② . Voir note **1.7.1**.

1.3.1. Soient n_1 et n_2 deux entiers $\geqslant 1$ et $n \coloneqq n_1 n_2$. On dispose de deux morphismes d'anneaux $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n_2\mathbb{Z}$: si deux entiers sont congrus modulo n, ils sont alors congrus modulo tout diviseur de n, par exemple n_1 et n_2. Le morphisme induit

$$\pi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z},$$

n'est en général pas un isomorphisme d'anneaux (c'est-à-dire : une bijection). Précisons que la structure d'anneau sur le produit cartésien $\mathbb{Z}/n_1\mathbb{Z}\times\mathbb{Z}/n_2\mathbb{Z}$ des couples (x, y), avec $x \in \mathbb{Z}/n_1\mathbb{Z}$ et $y \in \mathbb{Z}/n_2\mathbb{Z}$, est la structure évidente : la somme et le produit se font coordonnée par coordonnée. Les deux anneaux ayant même cardinal, à savoir $n = n_1 n_2$, ce morphisme est injectif si et seulement si il est bijectif. Or, de même qu'une application linéaire est injective si et seulement si son noyau — les antécédents de $\{0\}$ — est réduit au vecteur nul, un morphisme d'anneaux est injectif si son noyau est réduit au singleton $\{0\}$: la même démonstration s'applique (*mutatis mutandis*). Pour étudier ce noyau $\mathrm{Ker}(\pi)$, soit $a \in \mathbb{Z}$ tel que

$$\pi(\overline{a}) = 0_{\mathbb{Z}/n_1\mathbb{Z}\times\mathbb{Z}/n_2\mathbb{Z}} = (0_{\mathbb{Z}/n_1\mathbb{Z}}, 0_{\mathbb{Z}/n_2\mathbb{Z}}).$$

Par hypothèse, on a donc $n_1|a$ et $n_2|a$ et on se demande si $\overline{a} = 0$ c'est-à-dire si n divise a. D'après le lemme de Gauß, il en est ainsi dès que n_1 et n_2 sont *premiers entre eux*. On a donc démontré le théorème chinois, dans le cas de deux facteurs. Par récurrence on démontre le cas général :

Théorème. *Soient $n_1, \ldots, n_r \geqslant 1$ des entiers supposés premiers entre eux deux à deux : pour toute paire $1 \leqslant i \neq j \leqslant r$, on a $n_i \perp n_j$. Alors, le morphisme canonique*

$$\mathbb{Z}/n_1\cdots n_r\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z},$$

$$a \pmod{n_1\cdots n_r} \mapsto \left(a \pmod{n_1}, \ldots, a \pmod{n_r}\right)$$

est un isomorphisme.

1.3.2. Dans l'exemple ci-dessus, datant de plus de 1700 ans, on cherche un antécédent de $(\overline{2}, \overline{3}, \overline{2})$ par la surjection $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$; d'après le théorème chinois, il en existe. (Une infinité : si x est solution, $x \pm 3 \cdot 5 \cdot 7$ aussi.) Dans le paragraphe suivant, nous avons voir comment l'algorithme d'Euclide permet de calculer un inverse explicite à l'isomorphisme du théorème précédent.

1.4. Algorithme d'Euclide I.

1.4.1. Soit à calculer le **plus grand commun diviseur (PGCD)** [最大公因数] de deux entiers a et b. L'algorithme d'Euclide pour ce faire est le suivant :

- Initialiser : $(m, n) \leftarrow (|a|, |b|)$.
- Tant que $n \neq 0$, répéter :
  - Faire $(m, n) \leftarrow (n, r)$ où r est le reste de la division euclidienne $m = nq + r$ de m par n.
- Renvoyer m (le PGCD recherché).

Invariant : $\mathrm{PGCD}(m, n) = \mathrm{PGCD}(a, b)$ (constant) ; l'algorithme termine car n décroît strictement à chaque étape (et reste un entier naturel).

À titre d'exemple, calculons le PGCD de $a = 98$ et $b = 77$:

- $(m, n) = (98, 77)$; division euclidienne $98 = 77 \times 1 + 21$;
- $(m, n) = (77, 21)$; division euclidienne $77 = 21 \times 3 + 14$;
- $(m, n) = (21, 14)$; division euclidienne $21 = 14 \times 1 + 7$;
- $(m, n) = (14, 7)$; division euclidienne $14 = 7 \times 2 + 0$;
- $(m, n) = (7, 0)$; on renvoie $\mathrm{PGCD}(98, 77) = 7$.

1.4.2. Si $a \perp b$, c'est-à-dire $\mathrm{PGCD}(a, b) = 1$, il existe des entiers u et v tels que $au + bv = 1$ on appelle cette égalité une **relation de Bézout**[①] entre a et b. Une telle paire (u, v) est fournie par l'**algorithme d'Euclide étendu**, qui consiste à « remonter » les coefficients dans l'algorithme d'Euclide : la dernière division $m = nq + 1$ donne une relation $1 = m - nq$ puis on remplace n (qui est lui-même un reste de division euclidienne) et ainsi de suite jusqu'à trouver une relation entre les entiers a et b de départ.

Formellement, on procède ainsi :

- $(m, n, u, v, u', v') \leftarrow (|a|, |b|, \mathrm{signe}(a), 0, 0, \mathrm{signe}(b))$.
- Tant que $n \neq 0$, répéter :
  - ♢ Division euclidienne de m par n : soit $m = nq + r$.
  - ♢ Remplacer $(m, n, u, v, u', v') \leftarrow (n, r, u', v', u - qu', v - qv')$.
- Vérifier $m = 1$ (le PGCD est bien 1).
- Les coefficients recherchés sont u et v (on a $au + bv = 1$).

Invariants : à chaque étape, on a $au + bv = m$ et $au' + bv' = n$.

1.4.3. Dans la pratique, à la main, on procède ainsi : pour calculer une relation de Bézout entre 64 et 47, on effectue les divisions euclidiennes successives $64 = 1 \times 47 + 17$, $47 = 2 \times 17 + 13$, $17 = 1 \times 13 + 4$, $13 = 3 \times 4 + 1$ jusqu'à tomber sur le reste 1. Puis on réécrit ce reste en partant de la dernière division $1 = 13 - 3 \times 4$ et en remplaçant successivement le reste de chaque division (lue à l'envers) par une combinaison du dividende et du diviseur : $4 = 17 - 1 \times 13$ donc $1 = 13 - 3 \times (17 - 1 \times 13) = 4 \times 13 - 3 \times 17$ puis $13 = 47 - 2 \times 17$ donc $1 = 4 \times (47 - 2 \times 17) - 3 \times 17 = 4 \times 47 - 11 \times 17$ et enfin $17 = 1 \times 64 - 47$ donc $1 = 4 \times 47 - 11 \times (1 \times 64 - 47) = 15 \times 47 - 11 \times 64$.

1.4.4. **Remarques.**

(i) Naturellement, ajouter b à u et $-a$ à v donne une nouvelle relation de Bézout entre a et b. Donc il n'y a pas unicité.

(ii) Plus généralement, si $\mathrm{PGCD}(a, b) = d$, on peut trouver u et v tels que $au + bv = d$: on a $\mathrm{PGCD}(\frac{a}{d}, \frac{b}{d}) = 1$, et si $\frac{a}{d}u + \frac{b}{d}v = 1$ est une relation de Bézout entre eux, alors on a $au + bv = d$.

1.4.5. Si $au + bv = 1$, et si α et β sont deux entiers relatifs, la somme $\beta au - \alpha bv$ est un entier congru à α modulo a et à β modulo b : on a construit un inverse à l'isomorphisme $\mathbb{Z}/ab\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$. (Notons que l'on peut également voir ce qui précède comme un algorithme de calcul de l'inverse de a dans $\mathbb{Z}/b\mathbb{Z}$.)

① Étienne Bézout (1730–1783), avec un accent aigu.

1.4.6. L'algorithme d'Euclide étendu pour a, b s'effectue en $O(nm)$ opérations élémentaires sur les bits, si a et b ont respectivement n et m bits : cf. [Gathen 2015, 15.33 p. 763]. La recherche d'algorithmes efficaces fait l'objet de nombreuses recherches ; par exemple l'algorithme naïf de multiplication de deux entiers à n chiffres, présenté par exemple en [TAOCP 2, §4.3.1], est en $O(n^2)$ tandis que des algorithmes significativement plus efficaces ont été trouvés relativement récemment (cf. [TAOCP 2, §4.3.3] ; voir aussi [Demazure 2008, §1.3], [Brent et Zimmermann 2011, §1.3] ou [Mullen et Panario 2013, §11.1.5.1]).

Esquissons l'un d'eux. Soit n un entier naturel. Un entier naturel à n bits — c'est-à-dire ayant au plus n chiffres écrit en base 2 — est un entier compris entre 0 et $2^n - 1$: on le représente un entier par le n-uplet $(b_{n-1}, \dots, b_0)$ d'entiers valant 0 ou 1 tel que cet entier soit $\sum_{i=0}^{n-1} b_i 2^i$. On cherche à calculer le produit de deux entiers à n bits (le résultat a au plus $2n$ bits).

Théorème (Karatsuba=Карацуба)**.** *On peut multiplier deux entiers à n bits en $O(n^{\log_2(3)}) = O(n^{1{,}58496\cdots})$ opérations élémentaires sur les bits.*

Démonstration. Soit m un entier. Des entiers à $2m$ bits x et y peuvent être représentés sous la forme $x = a2^m + b$ et $y = c2^m + d$ où a, b, c, d sont des entiers naturels à au plus m bits. On a

$$xy = ac \cdot 2^{2m} + (ad + bc) \cdot 2^m + bd.$$

Un algorithme possible pour faire la multiplication consiste à calculer les quatre produits ac, ad, bc et bd d'entiers à m chiffres, puis faire les opérations faciles (décalage et additions) pour obtenir le résultat xy. Notons c_k le coût en opérations par bits de la multiplication de deux entiers à 2^k bits. En appliquant récursivement la méthode ci-dessus, on obtient une relation de récurrence $c_{k+1} = 4c_k + O(2^k)$. Le quotient $d_k := c_k/4^k$ vérifie une relation $d_{k+1} = d_k + O(2^{-k})$ dont on déduit que la suite (d_k) converge, ainsi $c_k = O(4^k)$. Finalement, on peut en conclure que l'on peut faire le produit d'entiers à n bits en $O(n^2)$ opérations, comme annoncé plus haut. L'algorithme de Karatsuba s'appuie sur le fait que l'on peut déterminer $ac, ad + bc$ et bd en faisant quelques additions et surtout trois multiplications au lieu de quatre. En effet, on peut calculer $N := (a+b)\cdot(c+d)$, ac et bd, et en déduire $ad + bc$ puisqu'on a $ad + bc = N - ac - bd$. Notons c'_k le coût de la multiplication de deux entiers à 2^k bits pour cette méthode. On a cette fois-ci $c'_{k+1} = 3c'_k + O(2^k)$, dont on déduit $c'_k = O(3^k)$. Si n est un entier naturel non nul, on peut considérer la plus petite puissance 2^k de 2 qui lui est supérieure, on a alors $k \leq \log_2 n + 1$. Comme $3^{\log_2 n} = n^{\log_2 3}$, on peut multiplier deux entiers à n bits en $O(n^{\log_2 3})$ (et donc $O(n^{1{,}585})$). □

(On peut améliorer l'exposant $\log_2(3) \approx 1{,}5849625007211$ en n'importe quel nombre > 1.)

1.5. Groupes cycliques.

1.5.1. Un groupe[①] G est dit **cyclique** [循环子群] s'il existe un élément $g \in G$ d'*ordre fini* tel que G coïncide avec le sous-groupe $\langle g \rangle$ engendré par g[②]. Si g est d'ordre n, c'est-à-dire si G est de cardinal n, on a un isomorphisme $\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} G$, $r \bmod n \mapsto g^r$. (Ici, $\mathbb{Z}/n\mathbb{Z}$ désigne le *groupe additif* $(\mathbb{Z}/n\mathbb{Z}, +)$: on oublie momentanément la structure d'anneau.)

Pour tout $h \in G$, on a donc $h^n = e$ et l'ordre de h, c'est-à-dire le plus petit entier $r > 0$ tel que $h^r = e$, est un diviseur de n.

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

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

Leur nombre est noté $\varphi(n)$; la fonction $\varphi : n \mapsto \varphi(n)$ est appelée **indicatrice d'Euler** [欧拉函数]. Puisqu'un entier a est inversible modulo n si et seulement si il est premier à n, on en déduit que $\varphi(n)$ est aussi le cardinal du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ des unités (=éléments inversibles) de l'anneau $\mathbb{Z}/n\mathbb{Z}$.

1.5.3. Proposition.

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

Il en résulte que l'on a l'égalité :

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

Démonstration. Le plus simple est probablement d'observer que, comme on vient de le rappeler, 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 : on a $\mathbb{Z}/nm\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ d'où $(\mathbb{Z}/nm\mathbb{Z})^\times \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times$. (Voir aussi [Hardy et Wright 2007, 16.1], par exemple, pour une démonstration plus élémentaire.) (ii) Il est clair qu'un entier est premier à p^α si et seulement si il n'est pas multiple de p. Le nombre de ces multiples inférieurs à p^α est $p^{\alpha-1}$. (iii) Remarquons que si n est une puissance de 2, on a $\varphi(n) = n/2 \geqslant \sqrt{n}/2$. D'autre part, si $p \geqslant 3$ est un entier, on a $p - 1 \geqslant \sqrt{p}$ si bien que $p^\alpha(1 - p^{-1}) \geqslant p^{\alpha-1/2} \geqslant p^{\alpha/2}$

① Nous supposons cette notion connue et renvoyons à [Serre 1979], [Šafarevič 1997] (magnifique survol), [Rotman 1995], [Perrin 1996] pour des rappels et compléments.

② Cette définition n'est pas universelle : certains auteurs ne supposent pas g d'ordre fini.

pour tout $\alpha \geqslant 1$. Par multiplicativité de φ, on a donc la minoration $\varphi(n) \geqslant \sqrt{n}/2$ pour tout n et, en particulier, $\varphi \to +\infty$. Des résultats bien plus précis sont établis dans [ibid., 18.4]. □

1.5.4. Proposition. *Soit $n > 0$ un entier. Pour tout $x \perp n$, on a*

$$x^{\varphi(n)} \equiv 1 \pmod{n}.$$

En particulier, pour tout nombre premier p, on a $x^{p-1} \equiv 1 \pmod{p}$ lorsque $x \perp p$ et $x^p \equiv x \pmod{p}$ pour tout x.

Cela résulte du fait que dans un groupe de cardinal N, l'ordre des éléments divise N.

1.6. RSA.

1.6.1. *Principe (de la cryptographie à clef publique).* Supposons qu'un individu B souhaite communiquer de façon secrète une information à la personne A : on aimerait qu'un observateur/espion (autre que A) du message transmis par B à A ne puisse pas le décoder en un temps raisonnable mais qu'il soit facile pour A de le faire. On peut formaliser un tel protocole de la façon suivante : A crée une « **clef publique** » P_{A} et une « **clef privée** » S_{A}. Chaque clef définit une fonction $X \to X$, où X est un certain ensemble fini. A rend la clef P_{A} publique — par exemple en la publiant sur sa page internet — mais garde secrète la clef S_{A}. Si B veut envoyer un message à A sous la forme d'une suite d'éléments de X, il applique P_{A} à chaque élément x de son message, et envoie les résultats $y := P_{\mathsf{A}}(x)$ à A, qui applique alors S_{A} à ces y. Bien sûr, il faut que pour tout $x \in X$, on ait $S_A(P_A(x)) = x$, c'est-à-dire que S_A et P_A sont des fonctions inverses l'une de l'autre. Pour que cela entre dans le domaine de la cryptographie, il faut qu'il soit très difficile de déterminer la fonction S_A connaissant la fonction P_A (mais que le calcul de cette dernière soit relativement rapide).

1.6.2. *Le cryptosystème RSA.* Décrivons les ensembles X, les clefs P_A et S_A, et les fonctions $P_A(-)$ et $S_A(-)$ associées. L'individu A choisit deux grands nombres entiers premiers p et $\ell \neq p$, pose $n := p\ell$. L'ensemble X sera $\mathbb{Z}/n\mathbb{Z}$. Il choisit alors un entier naturel $d \perp \varphi(n) = (p-1)(\ell-1)$ et détermine un entier naturel e inverse de d modulo $\varphi(n)$ par l'algorithme d'Euclide étendu. La clef publique P_A est le couple (e, n) et la clef privée S_A est (d, n). La fonction $P_A(-) : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ est l'élévation $x \mapsto x^e$ à la puissance e et, de même, la fonction $S_A(-) : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ est $x \mapsto x^d$.

1.6.3. Voici un exemple, tiré de [Hoffstein, Pipher et Silverman 2014, §3.2] ; il est aisé d'en produire à l'aide d'un ordinateur.

création des clefs A choisit deux nombres premiers secrets $p = 1223$ and $\ell = 1987$. Il calcule le nombre $n = p\ell = 2430101$ puis l'exposant de chiffrement, $e = 948047$ premier avec $(p-1)(\ell-1) = 2426892$; il rend ces deux informations $(e, n) = P_{\mathsf{A}}$ publiques. Connaissant $\varphi(n) = (p-1)(\ell-1)$, il peut trouver un inverse d de e modulo $\varphi(n)$ c'est-à-dire un d tel que $de \equiv 1 \pmod{2426892}$. Il trouve $d = 1051235$.

chiffrement B convertit son message texte en un entier, disons $x = 1070777$ satisfaisant $1 \leq x < n$ (sinon, couper le message en morceaux). Il utilise la clef publique P_{A} pour calculer $y = x^e \pmod n$: il trouve $y \equiv 1070777^{948047} \equiv 1473513$ et envoie cette dernière valeur à A.

décodage A applique S_{A} au message chiffré $y = P_{\mathsf{A}}(1070777) = 1473513$ et calcul $y^d \equiv 1473513^{1051235} = 1070777$. C'est le message que B souhaitait lui envoyer secrètement.

1.6.4. Implicitement, nous supposons que calculer une *racine* e-ième dans $\mathbb{Z}/n\mathbb{Z}$ est plus difficile que de calculer une *puissance* e-ième ou d-ième. Même s'il reste à prouver que le premier problème est difficile, on peut au moins montrer que le second est facile, par le procédé d'**exponentiation rapide**. Nous renvoyons à [TAOCP 2, 4.6.3] pour une discussion détaillée mais signalons simplement qu'en exploitant les égalités

$$x^{2n} = (x^n)^2 \text{ et } x^{2n+1} = (x^n)^2 x,$$

on montre immédiatement que le calcul d'une puissance x^n peut se faire en

$$\lfloor \log_2(n) \rfloor + \nu(n) - 1$$

multiplications, où $\nu(n)$ est le nombre de 1 dans l'écriture de n en base 2.

Pour l'exposant $e = (948047)_{10} = (11100111011101001111)_2$, ayant 20 chiffres en base 2, on voit que le calcul de x^e peut se faire en au plus $19 + 14 - 1 = 32$ multiplications, et non 948046. Explicitement,

$$x^e = xCTCTCCCTCTCTCCTCTCTCCTCCCTCTCTCT,$$

où C est l'opération d'élévation au carré et T est l'opération de multiplication par x. L'expression ci-dessus a été obtenue en remplaçant les 1 (resp. 0) par « CT » (resp. « C ») et suppression du CT de gauche. Pour démontrer que ce procédé calcule bien x^n, procéder par récurrence en écrivant $e = 2e' + \varepsilon$, avec $\varepsilon \in \{0, 1\}$. La formule sur le nombre de multiplications ci-dessus en résulte aussitôt.

1.7. Notes.

1.7.1. La dénomination « théorème chinois » a pour origine le traitement d'un problème d'arithmétique élémentaire dans le Sūnzǐ Suànjīng [孙子算—经卷下第二十六题] dont nous citons le passage pertinent :

今有物，不知其數。三三數之，賸二；五五數之，賸三；七七數之，賸二。
問：物幾何？
答曰：二十三。
術曰：三三數之，賸二，置一百四十；五五數之，賸三，置六十三；七七數之，賸二，置三十。
并之，得二百三十三，以二百一十減之，即得。
凡三三數之，賸一，則置七十；五五數之，賸一，則置二十一；七七數之，賸一，則置十五。
一百六以上，以一百五 減之，即得。

Voir [Needham 1959, p. 119-122] et [TAOCP 2, §4.3.2] pour un historique rapide.

1.7.2. En plus de l'algorithme d'Euclide (**1.4**), il en existe un autre, évident, consistant à factoriser les entiers a et b et « lire » le PGCD sur ces factorisations : si $a = \prod_p p^{\alpha_p}$ et $b = \prod_p p^{\beta_p}$ alors $\mathrm{PGCD}(a,b) = \prod_p p^{\min(\alpha_p,\beta_p)}$. Cependant, factoriser les entiers est algorithmiquement difficile : la meilleure méthode connue (« méthode du crible général de corps de nombres »[①]) pour factoriser un entier n a une complexité « attendue » (et heuristique) en

$$\exp\left(\left(\sqrt[3]{\frac{64}{9}}+o(1)\right)(\log n)^{\frac{1}{3}}(\log\log n)^{\frac{2}{3}}\right).$$

Il en résulte qu'utiliser les valuations p-adiques α_p et β_p des entiers dont on veut calculer le PGCD est bien moins efficace que l'algorithme d'Euclide, dont le coût est facilement majoré par $\mathrm{O}(\log(n)^2)$. (Voir par exemple [Gathen 2015, 15.25 p. 756] pour l'énoncé[②] et **1.4.6** pour des précisions.)

1.7.3. Faisons quelques remarques sur le crypto-système RSA.

Si $3 \nmid n$, on pourrait même prendre pour exposant publique l'entier $e = 3$ et obtenir un crypto-système réputé fiable, du moins si l'*entier* $y = x^3$ est $> n$, sans quoi calculer une racine cubique de y modulo n est trivial : prendre la racine cubique usuelle. (Voir [TAOCP 2, p. 404↓] pour une discussion et [TAOCP 2, exercice 4.5.4-32] pour un moyen de contourner ce problème apparent.) Les personnes inquiètent que $e = 3$ ne serait pas un choix sûr semblent préférer en pratique $e = 2^{16} + 1 = 65537$ (cf. [Hoffstein, Pipher et Silverman 2014, p.125]).

On suppose implicitement ici l'existence d'une infinité de nombres premiers, fait connu depuis Euclide (au plus tard) : si $p_1, \ldots, p_r$ sont des nombres premiers, tout facteur premier de $1 + \prod_i p_i$ est différent des p_i. En réalité, on veut plus : que p et ℓ satisfassent quelques conditions arithmétiques — la remarque précédente suppose par exemple l'existence de grands nombres premiers $\not\equiv 1 \pmod 3$[③] — et ainsi que des conditions archimédiennes : par exemple, p et ℓ doivent être grands (disons au moins 100 chiffres en bases 10) et pas trop proches[④].

Enfin, on *conjecture* qu'il est algorithmiquement difficile — en un sens que nous ne précisons pas — de « casser » ce crypto-système. Comme on le verra dans l'exercice **1.8.9** *infra*, on peut au moins montrer que la question — supposée difficile — de factoriser n est essentiellement équivalente à celle du calcul de $\varphi(n)$ (utile au calcul de l'exposant secret d connaissant l'exposant public e).

---

①. Voir [Hoffstein, Pipher et Silverman 2014, §3.7.3] pour une discussion élémentaire informelle.

②. L'usage est plutôt de parler d'algorithme en « $\mathrm{O}(n^2)$ », où n est le nombre de **bits** des données.

③. [Serre 1977, chap. VI] pour un résultat plus général dans ce sens, dû à Dirichlet, et par exemple le paragraphe 7.3.5 des notes de cours de 2016-2017 pour une démonstration, beaucoup plus élémentaire, du fait qu'il existe une infinité de nombres premiers $\equiv 1 \pmod N$ pour tout entier $N > 1$.

④. Voir [TAOCP 2, p. 405], [Gathen 2015, §3.4] et, moins formellement, [Schroeder 2006, §9] pour une discussion de cet aspect.

1.8. Exercices.

1.8.1. Retrouvez en travaillant dans $\mathbb{Z}/9\mathbb{Z}$ et $\mathbb{Z}/11\mathbb{Z}$ les critères classiques de divisibilité par 9 ou 11 d'un entier a en fonction de son écriture décimale $a := \sum_{i=0}^{r} a_i 10^i$, $0 \leqslant a_i < 10$.

1.8.2. Calculer *à la main* $3^{1\,000\,003}$ modulo 101.

1.8.3. Quelle est la forme simplifiée du caractère traditionnel 賸 ?

1.8.4. Nombre de Carmichael.

(i) Soit n un entier $\geqslant 1$ tel que pour tout entier a, on ait $a^n \equiv a \pmod{n}$. Montrer que n est sans facteur carré.

(ii) ¶ L'entier n est-il premier ? En d'autres termes : la congruence $a^n \equiv a$ (pour tout a) peut-elle servir de test de primalité ?

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

1.8.6. Soit p un nombre premier. Considérons le corps $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ et l'ensemble $S_p = \mathbb{F}_p^\times$ de ses éléments inversibles. Pour tout entier r, on considère le graphe orienté $G_{p,r}$ dont l'ensemble des sommets est S_p, d'arêtes les couples (x, y) tels que $y = x^r$. Dessiner les graphes $G_{13,2}$, $G_{13,3}$, et $G_{13,5}$ et expliquer quelques les différences observées. (Par exemple sur la longueur des cycles, le nombre de sommets étant le but d'une arête, etc.)

1.8.7. Vérifier qu'avec les notations du **1.6.2**, on a bien $S_A P_A(x) = x$.

1.8.8. *Pile ou face à distance.* Soient p, ℓ deux nombres premiers *distincts*, congrus à $3 \pmod 4$[①], et $b \in \mathbb{Z}$.

(i) Montrer que si b est un carré modulo p, alors $b^{(p+1)/4}$ en est une racine carrée modulo p.

(ii) Montrer que si b un carré modulo $n := p\ell$ et $b \perp n$, alors b a exactement 4 racines carrées modulo n et que leur connaissance permet de factoriser rapidement n.

(iii) En déduire que le protocole suivant permet à deux personnes A et B de jouer à pile ou face, sans pouvoir tricher, à distance :

(a) A choisit p, ℓ comme ci-dessus et communique à B le produit n.

(b) B choisit un entier $1 \leqslant a \leqslant n-1$ au hasard (mais premier à n) et calcule $b := a^2$ qu'il communique *modulo* n à A.

(c) A envoie à B l'une des 4 racines carrées de $b \pmod n$, qu'il sait calculer rapidement par ce qui précède.

(d) Si B sait calculer p et ℓ [et les donner à A], il a gagné ; sinon, il a perdu.

1.8.9. Soient $n = p\ell, d, e$ comme en **1.6.2**. Montrer que la connaissance de $\varphi(n)$ permet de factoriser n, c'est-à-dire de trouver rapidement p et ℓ.

① Il en existe une infinité : si $p_1, \ldots, p_r$ sont des nombres premiers et ℓ est un nombre premier divisant $N := 4p_1 \cdots p_r - 1$, il est différent des p_i. D'autre parts, de tels ℓ ne peuvent être tous $\equiv 1 \pmod 4$ sans quoi il en serait de même de leur produit N, visiblement congru à $-1 \pmod 4$.

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

2. Corps finis I

2.1. Généralités.

2.1.1. Nous avons vu qu'il existe pour chaque nombre premier p un *corps* à p éléments : $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$. Plusieurs questions se posent :

- **(i)** Est-ce le « seul » corps à p éléments ? [En un sens à préciser.]
- **(ii)** Pour quels entiers n existe-t-il (au moins) un corps à n éléments ?
- **(iii)** Pour de tels n, comment les « construire », de sorte que l'on puisse notamment faire des calculs, à la main ou sur ordinateur, dans un tel corps ?
- **(iv)** Quel est l'intérêt de construire ces corps possiblement « exotiques » pour n non premier ?

Nous allons répondre brièvement à ces questions, en renvoyant généralement aux sections suivantes pour les démonstrations et exemples d'applications.

2.1.2. Soit k un corps, c'est-à-dire un anneau commutatif dans lequel tout élément non nul est inversible (pour le produit). Supposons le *fini*. Il existe un unique morphisme d'anneaux $\mathbb{Z} \to k$, envoyant $n \in \mathbb{N}$ sur $n \cdot 1_k = 1_k + \cdots + 1_k$ (n fois) et $-n$ sur l'opposé de $n \cdot 1_k$. Puisque k est fini, ce morphisme ne peut être injectif et son noyau est engendré par un nombre premier p, appelé **caractéristique** [特征] de k, noté $\mathrm{car.}(k)$. (Voir exercice **2.5.1** ou **3.2.1** pour les détails.)

Il en résulte immédiatement que k contient naturellement le corps $\mathbb{F}_p$ (on dit que s'en est un **sous-corps**) [子域] : $\mathbb{F}_p \subseteq k$, de sorte que k est muni d'une structure de $\mathbb{F}_p$-espace vectoriel : si $\lambda \in \mathbb{F}_p$ et $v \in k$, poser $\lambda v := \lambda \cdot v$ (produit dans k). Par finitude de k, sa dimension $d := \dim_{\mathbb{F}_p}(k)$ en tant que $\mathbb{F}_p$-espace vectoriel est un entier $< +\infty$. En identifiant, non canoniquement, k à $\mathbb{F}_p^d$, on voit que

$$\#k = p^d.$$

Ceci montre que :

- **(i)** si k est de cardinal un nombre premier, alors il est *canoniquement* isomorphe à $\mathbb{F}_p$, pour $p = \mathrm{car.}(k)$;
- **(ii)** si k est de cardinal n, il existe un (unique) nombre premier p, sa *caractéristique*, et un entier $d \geqslant 1$ tels que $n = p^d$.

2.1.3. L'observation précédente ne montre pas que pour chaque puissance q d'un nombre premier il existe un corps de cardinal q : la condition que $\#k$ soit de cette forme est, *a priori*, seulement une condition *nécessaire*. Nous verrons en **2.2** ci-dessous qu'elle est également suffisante. À titre d'exemple, contentons-nous ici de construire un corps à $q = 2^3 = 8$ éléments.

Soit $f(T) := T^3 + T + 1$ le polynôme de degré 3 à coefficients dans $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$. De même que l'on a construit $\mathbb{Z}/n\mathbb{Z}$ à partir de $\mathbb{Z}$ et l'entier n, on peut construire l'anneau $A = \mathbb{F}_2[T]/(f)$ des classes de congruence modulo f [①]. La division euclidienne

① Soit I un **idéal** [理想] d'un anneau (commutatif) A, c'est-à-dire 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 $ai \in I$.

des polynômes — sur laquelle nous reviendrons en **3.1** — nous assure que chaque classe $\overline{g} \in A$ est représentée par un unique polynôme de degré < 3, le *reste* de la division euclidienne de g par f. Les tables d'addition et de multiplication, héritées de $\mathbb{F}_2[T]$, sont les suivantes, où l'on note $t = \overline{T}$ la classe de T dans le quotient :

$+$	$\mathbf{0} = \{000\}$	$\mathbf{1} = \{001\}$	$\mathbf{2} = \{010\}$	$\mathbf{3} = \{011\}$	$\mathbf{4} = \{100\}$	$\mathbf{5} = \{101\}$	$\mathbf{6} = \{110\}$	$\mathbf{7} = \{111\}$
$0 = \mathbf{0} = \{000\}$	$\mathbf{0} = \{000\}$	$\mathbf{1} = \{001\}$	$\mathbf{2} = \{010\}$	$\mathbf{3} = \{011\}$	$\mathbf{4} = \{100\}$	$\mathbf{5} = \{101\}$	$\mathbf{6} = \{110\}$	$\mathbf{7} = \{111\}$
$1 = \mathbf{1} = \{001\}$	$\mathbf{1} = \{001\}$	$\mathbf{0} = \{000\}$	$\mathbf{3} = \{011\}$	$\mathbf{2} = \{010\}$	$\mathbf{5} = \{101\}$	$\mathbf{4} = \{100\}$	$\mathbf{7} = \{111\}$	$\mathbf{6} = \{110\}$
$\bar{t} = \mathbf{2} = \{010\}$	$\mathbf{2} = \{010\}$	$\mathbf{3} = \{011\}$	$\mathbf{0} = \{000\}$	$\mathbf{1} = \{001\}$	$\mathbf{6} = \{110\}$	$\mathbf{7} = \{111\}$	$\mathbf{4} = \{100\}$	$\mathbf{5} = \{101\}$
$\bar{t}+1 = \mathbf{3} = \{011\}$	$\mathbf{3} = \{011\}$	$\mathbf{2} = \{010\}$	$\mathbf{1} = \{001\}$	$\mathbf{0} = \{000\}$	$\mathbf{7} = \{111\}$	$\mathbf{6} = \{110\}$	$\mathbf{5} = \{101\}$	$\mathbf{4} = \{100\}$
$\bar{t}^2 = \mathbf{4} = \{100\}$	$\mathbf{4} = \{100\}$	$\mathbf{5} = \{101\}$	$\mathbf{6} = \{110\}$	$\mathbf{7} = \{111\}$	$\mathbf{0} = \{000\}$	$\mathbf{1} = \{001\}$	$\mathbf{2} = \{010\}$	$\mathbf{3} = \{011\}$
$\bar{t}^2+1 = \mathbf{5} = \{101\}$	$\mathbf{5} = \{101\}$	$\mathbf{4} = \{100\}$	$\mathbf{7} = \{111\}$	$\mathbf{6} = \{110\}$	$\mathbf{1} = \{001\}$	$\mathbf{0} = \{000\}$	$\mathbf{3} = \{011\}$	$\mathbf{2} = \{010\}$
$\bar{t}^2+\bar{t} = \mathbf{6} = \{110\}$	$\mathbf{6} = \{110\}$	$\mathbf{7} = \{111\}$	$\mathbf{4} = \{100\}$	$\mathbf{5} = \{101\}$	$\mathbf{2} = \{010\}$	$\mathbf{3} = \{011\}$	$\mathbf{0} = \{000\}$	$\mathbf{1} = \{001\}$
$\bar{t}^2+\bar{t}+1 = \mathbf{7} = \{111\}$	$\mathbf{7} = \{111\}$	$\mathbf{6} = \{110\}$	$\mathbf{5} = \{101\}$	$\mathbf{4} = \{100\}$	$\mathbf{3} = \{011\}$	$\mathbf{2} = \{010\}$	$\mathbf{1} = \{001\}$	$\mathbf{0} = \{000\}$

$\times$	$\mathbf{0} = \{000\}$	$\mathbf{1} = \{001\}$	$\mathbf{2} = \{010\}$	$\mathbf{3} = \{011\}$	$\mathbf{4} = \{100\}$	$\mathbf{5} = \{101\}$	$\mathbf{6} = \{110\}$	$\mathbf{7} = \{111\}$
$0 = \mathbf{0} = \{000\}$	$\mathbf{0} = \{000\}$	$\mathbf{0} = \{000\}$	$\mathbf{0} = \{000\}$	$\mathbf{0} = \{000\}$	$\mathbf{0} = \{000\}$	$\mathbf{0} = \{000\}$	$\mathbf{0} = \{000\}$	$\mathbf{0} = \{000\}$
$1 = \mathbf{1} = \{001\}$	$\mathbf{0} = \{000\}$	$\mathbf{1} = \{001\}$	$\mathbf{2} = \{010\}$	$\mathbf{3} = \{011\}$	$\mathbf{4} = \{100\}$	$\mathbf{5} = \{101\}$	$\mathbf{6} = \{110\}$	$\mathbf{7} = \{111\}$
$\bar{t} = \mathbf{2} = \{010\}$	$\mathbf{0} = \{000\}$	$\mathbf{2} = \{010\}$	$\mathbf{4} = \{100\}$	$\mathbf{6} = \{110\}$	$\mathbf{3} = \{011\}$	$\mathbf{1} = \{001\}$	$\mathbf{7} = \{111\}$	$\mathbf{5} = \{101\}$
$\bar{t}+1 = \mathbf{3} = \{011\}$	$\mathbf{0} = \{000\}$	$\mathbf{3} = \{011\}$	$\mathbf{6} = \{110\}$	$\mathbf{5} = \{101\}$	$\mathbf{7} = \{111\}$	$\mathbf{4} = \{100\}$	$\mathbf{1} = \{001\}$	$\mathbf{2} = \{010\}$
$\bar{t}^2 = \mathbf{4} = \{100\}$	$\mathbf{0} = \{000\}$	$\mathbf{4} = \{100\}$	$\mathbf{3} = \{011\}$	$\mathbf{7} = \{111\}$	$\mathbf{6} = \{110\}$	$\mathbf{2} = \{010\}$	$\mathbf{5} = \{101\}$	$\mathbf{1} = \{001\}$
$\bar{t}^2+1 = \mathbf{5} = \{101\}$	$\mathbf{0} = \{000\}$	$\mathbf{5} = \{101\}$	$\mathbf{1} = \{001\}$	$\mathbf{4} = \{100\}$	$\mathbf{2} = \{010\}$	$\mathbf{7} = \{111\}$	$\mathbf{3} = \{011\}$	$\mathbf{6} = \{110\}$
$\bar{t}^2+\bar{t} = \mathbf{6} = \{110\}$	$\mathbf{0} = \{000\}$	$\mathbf{6} = \{110\}$	$\mathbf{7} = \{111\}$	$\mathbf{1} = \{001\}$	$\mathbf{5} = \{101\}$	$\mathbf{3} = \{011\}$	$\mathbf{2} = \{010\}$	$\mathbf{4} = \{100\}$
$\bar{t}^2+\bar{t}+1 = \mathbf{7} = \{111\}$	$\mathbf{0} = \{000\}$	$\mathbf{7} = \{111\}$	$\mathbf{5} = \{101\}$	$\mathbf{2} = \{010\}$	$\mathbf{1} = \{001\}$	$\mathbf{6} = \{110\}$	$\mathbf{4} = \{100\}$	$\mathbf{3} = \{011\}$

La vérification de ces tableaux est immédiate : pour l'addition, il suffit d'additionner les 3 coordonnées bit par bit ; pour la multiplication, on calcule le produit des polynômes puis on effectue la division euclidienne par f s'il est de degré $\geqslant 3$. (La numérotation $\mathbf{0}, \mathbf{1}, \ldots, \mathbf{7}$ correspond à l'ordre lexicographique sur les polynôme ; elle n'est reste pas moins arbitraire.) On observe que l'anneau ainsi obtenu est un corps : tout élément $\neq \mathbf{0}$ a un inverse ; comme nous le verrons, cela résulte de l'*irréductibilité* du polynôme f dans $\mathbb{F}_2[T]$. Nous donnerons par la suite (**2.3**,**4.2.2**) plusieurs démonstrations du fait que pour chaque nombre premier p et chaque entier d il existe un polynôme irréductible de degré d dans $\mathbb{F}_p[T]$; cela nous permettra d'étendre la construction précédente à toutes les valeurs possibles de q et de répondre positivement à la question (**iii**) ci-dessus.

Signalons cependant que d'autres constructions sont possibles : voir par exemple la construction d'un corps à 4 éléments, ou plus généralement 2^{2^n} éléments, esquissée dans l'exercice **2.5.9**.

On peut définir le **quotient** A/I en identifiant deux éléments de A égaux *à translation par un élément de I près* et vérifier qu'il existe une unique structure d'anneau sur A/I telle que la surjection canonique $A \twoheadrightarrow A/I$, envoyant a sur sa classe $\overline{a}$, soit un morphisme d'anneaux. Formellement, A/I est l'ensemble quotient de A par la relation d'équivalence $\mathscr{R}_I$ définie par : $x \mathscr{R}_I y$ si et seulement si $x - y \in I$. On dit que $\mathscr{R}_I$ est la relation de **congruence modulo** I [模I同余(关系)] et on note en général $x \equiv y \mod I$. 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.

2.1.4. Dans la discussion précédente, nous avons omis la discussion de la possible « unicité » des corps à q éléments, pour q non premier. *A priori*, ce n'est pas évident : pour construire par exemple un corps à $49 = 7^2$ éléments, on a plutôt « trop » de choix. En effet, pour chaque élément $x \in \mathbb{F}_7$ qui n'est pas un carré — c'est-à-dire $x \in \{\bar{3}, \bar{5}, \bar{6} = -\bar{1}\}$ —, le quotient $\mathbb{F}_7[T]/(T^2 - x)$ convient. Ainsi, par exemple,

$$\mathbb{F}_7[\sqrt{-1}] := \mathbb{F}_7[T]/(T^2 + 1) = \{a + \sqrt{-1}b \,:\, a, b \in \mathbb{F}_7\}$$

et

$$\mathbb{F}_7[\sqrt{3}] := \mathbb{F}_7[T]/(T^2 - 3) = \{a + \sqrt{3}b \,:\, a, b \in \mathbb{F}_7\}$$

sont deux corps à 49 éléments, isomorphes si et seulement si 3 est un carré dans $\mathbb{F}_7[\sqrt{-1}]$ (ou -1 un carré dans $\mathbb{F}_7[\sqrt{3}]$). La théorie générale nous dira qu'il doit en être ainsi mais ne donne pas de recette[①] pour construire $\mathbb{F}_7[\sqrt{3}] \xrightarrow{\sim} \mathbb{F}_7[\sqrt{-1}]$. (Ici, on peut vérifier que $\sqrt{3} \mapsto 2\sqrt{-1}$ convient.) Par contre, on verra qu'une fois un tel isomorphisme construit, on en déduit immédiatement tous les autres. (Ici, c'est évidemment $\sqrt{3} \mapsto -2\sqrt{-1}$.)

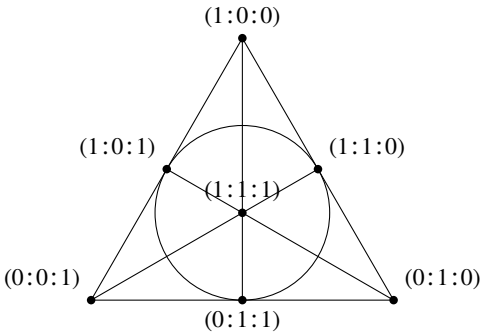
2.1.5. La question (**iv**) de l'intérêt de construire des corps finis plus généraux que les **corps premiers** [素域] $\mathbb{F}_p$ est, évidemment, celle à laquelle il est le plus difficile de répondre, tant les applications, théoriques ou technologiques, de ces corps sont nombreuses. Certaines font l'objet de ces notes mais, pour motiver ce qui va suivre, mentionnons d'ores et déjà les faits suivants.

a) De même que l'étude de phénomènes réels — par exemple, la compréhension d'équations différentielles linéaires à coefficients dans $\mathbb{R}$ — est grandement simplifiée par l'adjonction de nombres non réels (ici : l'adjonction à $\mathbb{R}$ de $\sqrt{-1}$, obtenant ainsi le corps $\mathbb{C}$ dans lequel toutes les valeurs propres des matrices sont présentes), l'étude de l'arithmétique/algèbre/dynamique/géométrie sur $\mathbb{F}_p$ est grandement simplifiée par l'introduction de corps $\mathbb{F}_q \supseteq \mathbb{F}_p$. Les applications sont innombrables : voir par exemple **4.3.6** pour un exemple en arithmétique ou **4.3.4** en combinatoire/algèbre linéaire.

b) La géométrie sur les corps finis est une source, qui semble inépuisable, d'objets remarquables — qu'il s'agisse par exemple de groupes finis ou de structures combinatoires — : se restreindre aux seuls corps ayant un nombre premier d'éléments nous ferait perdre une grande partie de cette richesse. Comme construction géométrico-combinatoire élémentaire, signalons le *plan projectif*[②] $\mathbf{P}^2(k)$ sur un corps k : c'est l'ensemble à $n := (\#k)^2 + \#k + 1$ éléments des droites dans l'espace affine $\mathbf{A}^3(k) = k^3$. Pour k de cardinal 2, on obtient le **plan de Fano**, dont on représente ci-dessous les 7 points et 7 droites (dont une d'allure courbe).

① . Voir [Mullen et Panario 2013, théorème 11.7.5] pour une brève discussion et des références sur cette question.

② . Voir par exemple [Demazure 2008, 7.4] pour une brève discussion.



Pour k de cardinal 7 on obtient une structure combinatoire à l'origine du jeu *Dobble*™[①]. Il est probablement clair à ce stade de la discussion qu'il serait évidemment inutilement restrictif de se restreindre aux corps de cardinal un nombre premier.

2.2. Existence et construction I.

2.2.1. Soient p un nombre premier et $d \geqslant 1$ un entier. Une condition suffisante pour l'existence d'un corps fini à $q = p^d$ éléments est l'existence d'un polynôme **unitaire** [首一多项式] $f \in \mathbb{F}_p[T]$ qui soit **irréductible** [不可约], c'est-à-dire tel que toute factorisation $f = gh$, où $g, h \in \mathbb{F}_p[T]$, soit « triviale » : l'un des facteurs g, h est une constante (c'est-à-dire un polynôme de degré 0). Ceci entraîne en effet que l'anneau quotient $\mathbb{F}_p[T]/(f)$, construit de manière semblable au corps à 8 éléments ci-dessus, est un corps à q éléments[②].

2.2.2. Pour établir l'existence d'un tel polynôme, l'approche la plus simple — celle qui est traditionnellement suivie — est de montrer, *par d'autres arguments*, l'existence d'un corps fini de cardinal q… La section suivante est donc consacrée à la présentation des généralités sur les corps et leurs extensions ; ces résultats, abstraits et élégants, donneront immédiatement le résultat attendu ; mieux ils permettent de montrer l'*unicité* du corps à q éléments, en un sens que nous préciserons plus tard. Une autre approche, plus combinatoire, est présentée en **2.3** ci-dessous : elle n'établit que l'*existence*.

2.2.3. La question de construire *explicitement* un corps à q éléments, en exhibant un polynôme irréductible fera l'objet d'une partie de la suite du cours, dans laquelle on présentera des algorithmes pour tester l'irréductibilité des polynômes.

2.3. ¶ Fonction zêta.

①. Voir [Madore 2015a] ou le site image des mathématiques. Voir également [Madore 2015b] pour une variante de ce jeu, ou [Mullen et Panario 2013, 14.3-5] pour d'autres constructions combinatoires.

②. D'ailleurs, tout élément non nul $a(t) = \sum_{i<d} a_i t^i \in \mathbb{F}_p[T]/(f)$ est d'inverse $u(t)$, dès lors que l'on a une relation de Bézout $au + fv = 1$, dont l'existence et le calcul sont fournis par l'algorithme d'Euclide, pour les polynômes : on utilise ici le fait que le polynôme $a(T)$ est premier à $f(T)$ car f est irréductible et $\deg(a) < \deg(f)$.

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

$$\zeta_{\mathbb{F}_p[T]}(s) := \sum_{f \text{ unitaire}} \frac{1}{|f|^s},$$

analogue à la fonction zêta usuelle de Riemann $\zeta_{\mathbb{Z}}(s) := \sum_{n\geq 1} \frac{1}{n^s} = \prod_p \frac{1}{1-p^{-s}}$[①]. Ici aussi, l'existence et l'unicité de la décomposition en produit d'irréductibles entraîne formellement l'égalité (« produit eulérien [欧拉乘积] »)

$$\zeta_{\mathbb{F}_p[T]}(s) = \prod_{P \text{ irr. unit.}} \frac{1}{1-|P|^{-s}}.$$

En effet, le terme de droite est égal à $\prod_P \left(\sum_{n\geq 1} |P|^{-ns}\right) = \sum_f |f|^{-s}$: si $f = P_1^{n_1}\cdots P_r^{n_r}$, on a $|f|^{-s} = |P_1|^{-n_1 s}\cdots|P_r|^{-n_r s}$. Par contre, à la différence du cas de l'anneau $\mathbb{Z}$, la fonction zêta de $\mathbb{F}_p[T]$ est facile à calculer : $\zeta(s) = \sum_{d\geq 0} \frac{p^d}{p^{ds}} = \frac{1}{1-p\cdot p^{-s}}$ car il y a exactement p^d polynômes unitaires de degré d.

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

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

où Pparcourt les polynômes irréductibles unitaires de $\mathbb{F}_p[T]$ et I_d désigne le nombre d'entre eux de degré d. Par construction, on a $\zeta_{\mathbb{F}_p[T]}(s) = Z_{\mathbb{F}_p[T]}(p^{-s})$ et, d'après le calcul du paragraphe précédent, on a $Z_{\mathbb{F}_p[T]}(x) = \frac{1}{1-px}$. Notons qu'en prenant la dérivée logarithmique $\frac{d}{dt}\circ\log$ de l'égalité $\prod_{d\geq 1} \frac{1}{(1-x^d)^{I_d}} = \frac{1}{1-px}$, on trouve les égalités (valables pour tout d)

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

On veut montrer que, pour tout $d \geqslant 1$, le nombre I_d — ou, de façon équivalente, son multiple $x_d := d I_d$ — est non nul. La formule $\sum_{a|d} x_a = p^d$ montre que $x_a \leqslant p^a$ pour tout a et donc

$$x_d = p^d - \sum_{\substack{a|d\\ a\neq d}} x_a \geqslant p^d - \sum_{\substack{a|d\\ a\neq d}} p^a \geqslant p^d - \sum_{a<d} p^a > 0,$$

où la dernière minoration résulte, par exemple, de l'unicité de l'écriture en base p.

Notons que la quantité $x_d := d I_d$ correspond au nombre de « racines des polynômes irréductibles de degré d ». Lorsque nous aurons vu les rudiments de théorie des corps, la minoration $x_d \geqslant p^d - \sum_{\substack{a|d\\ a\neq d}} p^a$ deviendra triviale : voir **4.3.5**.

2.4. Notes.

① Voir **2.4.2**.

2.4.1. En plus des applications aux codes correcteurs d'erreurs — qui feront l'objet de la fin de ce cours — et à la cryptographie[①], signalons également une méthode pour partager un secret en N « parts » chacune de même longueur que le secret, de manière que $d+1$ (avec $1 \leqslant d < N$) quelconques d'entre elles suffisent à reconstituer le secret mais que $\leqslant d$ parts n'apportent *absolument aucune* information sur le secret autre que sa longueur, même si on dispose de moyens de calculs illimités. Le principe général du **partage de secret de Shamir**[②] est d'identifier le secret à un élément z d'un corps fini k à q éléments, où q est strictement supérieur au nombre de parts/individus. (On peut donc fixer des éléments distincts $x_1, \dots, x_N \in k^\times$.) Pour chaque tel z, on considère le polynôme de degré $\leqslant d$ tel que $f(0)$ soit la valeur z du secret et que les autres d coefficients de f soit tirés au hasard uniformément dans k. Les parts seront $(x_1, f(x_1)), \dots, (x_N, f(x_N))$. Notons que, comme un polynôme de degré $\leqslant d$ est complètement déterminé par la donnée de $d+1$ valeurs de celui-ci, elles permettent de retrouver le secret $z = f(0)$. Pour implémenter ce principe élémentaire — il s'agit de l'interpolation de Lagrange ! — on a besoin que : (A) on puisse couper le secret en « valeurs » représentables sur un nombre entier de bits (donc il doit y avoir 2^r « valeurs » possibles), (B) on puisse travailler avec ces « valeurs » comme sur les réels (donc elles doivent constituer un corps), et (C) on ait $N < 2^r$ pour pouvoir fabriquer les parts du secret. Ce qui impose dans la pratique de travailler avec le corps fini à 2^8 éléments — le message étant découpé en octets — (pour partager un secret en $\leqslant 255$ parts).

2.4.2. La démonstration donnée en **2.3** de l'existence de polynômes irréductibles de tout degré peut être précisée pour obtenir une formule exacte, due à Gauß : voir l'exercice **2.5.10**. Signalons que l'idée de considérer une « fonction zêta » n'est pas surprenante : qu'il existe « beaucoup » de nombres premiers [les irréductibles de $\mathbb{Z}$] résulte de la divergence de $\sum_p p^{-1}$, elle-même conséquence de la divergence de $\zeta_{\mathbb{Z}}(1) = \sum_{n>0} n^{-1} = \prod_p (1-p^{-1})^{-1}$. L'argument présenté est une variante dans le cas, semblable mais *beaucoup* plus simple, des polynômes. Voir [Hardy et Wright 2007, théorème 19] pour une démonstration élémentaire de $\sum_p p^{-1} = +\infty$ et [Ireland et Rosen 1990, chap. 2, §3], où il est également démontré que $\sum_{\substack{P \in \mathbb{F}_p[T] \\ \text{irréd}}} |P|^{-1} = +\infty$.

L'utilisation de fonctions génératrices — appelées fonctions zêta dans ce contexte — est extrêmement fécond : par exemple, on peut calculer la proportion de polynômes unitaires dans facteurs carré. (Voir le paragraphe 7.4.3 des notes de cours de 2016-2017.) Pour une autre application de ces techniques, voir aussi l'exercice **3.4.6**, qui est l'analogue pour les polynômes du résultat difficile énoncé en **1.8.5**.

2.5. Exercices.

① En informatique, il est souvent utile de travailler avec *exactement* 2^r valeurs, notamment pour $r = 8$ (256 valeurs), de sorte qu'un corps fini à 2^r éléments est très utile en pratique, notamment pour le chiffrement AES. (Voir [Gathen 2015, §6.1] pour une présentation simplifiée et [Hoffstein, Pipher et Silverman 2014, §8.12] pour un bref historique.)

② Voir [TAOCP 2, p. 505] ou [Stinson 2006, §13.1] pour des exemples.

2.5.1. Soit k un corps fini. Vérifier que le morphisme canonique $\mathbb{Z} \to k$ induit un morphisme injectif de corps $\mathbb{Z}/p\mathbb{Z} \hookrightarrow k$.

2.5.2. Vérifier que le morphisme $x \mapsto x^2$ est un automorphisme du corps à 8 éléments $k := \mathbb{F}_2[T]/(T^3+T+1)$ construit en **2.1.3**. En déduire que t^2 est également une racine du polynôme f puis déterminer tous les automorphismes de k, c'est-à-dire les permutations de k respectant l'addition et la multiplication.

2.5.3. Soit $P := T^4 + T + 1 \in \mathbb{F}_2[T]$.

- **(i)** Combien d'éléments a $F := \mathbb{F}_2[T]/(P)$?
- **(ii)** Dresser la liste des puissances successives de $t := \bar{T}$ dans F. Quel est l'ordre multiplicatif de t ? De t^3, t^5 ?
- **(iii)** Quel est l'inverse de t ? L'anneau quotient F est-il un corps ? Qu'en déduire sur le polynôme P?
- **(iv)** Existe un sous-corps K de F de cardinal 8 ?
- **(v)** Quels sont les sous-corps à 4 éléments contenus dans F?

2.5.4.

- **(i)** Faire une liste des polynômes irréductibles de degré 3 sur $\mathbb{F}_2$.
- **(ii)** Soit p un nombre premier. Déterminer le nombre de polynômes irréductibles unitaires de $\mathbb{F}_p[X]$ de degré ≤ 3.

2.5.5. Montrer qu'un polynôme $f \in \mathbb{F}_p[T]$ de degré d est irréductible si et seulement si pour tout $0 \neq g \in \mathbb{F}_p[T]$ de degré $\leqslant \lfloor \frac{d}{2} \rfloor$, on a $g \perp f$.

2.5.6. Montrer que dans un corps fini, tout élément est somme de 2 carrés.

2.5.7. 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 $\binom{p}{i} \equiv 0 \mod p$.

2.5.8. Soit p un nombre premier.

- **(i)** Montrer que si $n = a_0 + a_1 p + \cdots + a_r p^r$ est l'écriture de n en base p, la plus grande puissance de p divisant $n!$ est d'exposant
$$v_p(n!) = \frac{n - \sum_i a_i}{p-1}.$$
- **(ii)** En déduire que si $0 \leqslant a \leqslant b$, la valuation p-adique $v_p(\binom{b}{a})$ du coefficient binomial est la somme des retenues de l'addition de a avec $b-a$, écrits en base p.

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

$$x \oplus y \coloneqq \mathrm{mex}\big(\{x' \oplus y \,:\, x' < x\} \cup \{x \oplus y' \,:\, y' < y\}\big)^{①}$$
$$x \otimes y \coloneqq \mathrm{mex}\big(\{(x' \otimes y) \oplus (x' \otimes y') \oplus (x \otimes y') \,:\, x' < x, y' < y\}\big)^{②}$$

(i) Écrire les tables d'addition et de multiplication induites sur l'ensemble $[4] \coloneqq \{0, 1, 2, 3\}$ et vérifier qu'il s'agit d'un corps à 4 éléments.

(ii) ¶ Faire de même pour $[16] = \{0, \ldots, 15\}$.

On pourra utiliser un ordinateur ou commencer par établir des résultats généraux.

2.5.10. On appelle **fonction de Möbius** [默比乌斯函数] la fonction $\mu : \mathbb{N} \to \mathbb{Z}$ définie par $\mu(n) = 0$ si n est divisible par un carré $\neq 1$ et $\mu(d) = (-1)^t$ si $d = p_1 \cdots p_t$ avec $p_1, \ldots, p_t$ des nombres premiers deux à deux distincts (ainsi, $\mu(1) = 1$, $\mu(2) = -1$, $\mu(3) = -1$, $\mu(4) = 0$, $\mu(5) = -1$, $\mu(6) = 1$, $\mu(7) = -1$, $\mu(8) = 0$, $\mu(9) = 0$, $\mu(10) = 1$).

(i) Établir la *formule d'inversion* [反演公式] suivante : si Γ est un groupe abélien et que $f, g : \mathbb{N}_{>0} \to \Gamma$ sont deux fonctions, on a

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

Indication : on remarquera qu'il suffit d'établir la formule $\sum_{a|d} \mu(a) = 0$, *pour* $d > 1$, *qui se ramène elle-même au cas particulier où* d *est une puissance d'un nombre premier.*

(ii) En déduire que e nombre de polynômes unitaires irréductibles de degré d sur $\mathbb{F}_p$ vaut

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

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

2.5.11.

(i) Utiliser le plan de Fano pour voir comment construire un jeu de *Dobble*™ à 7 cartes.

(ii) Le jeu précédent a trop peu de cartes ! Comment en construire un à 21 cartes ?

(iii) Trouver un moyen d'identifier les cartes manquantes dans la version commercialisée du jeu qui, au lieu des $57 = 7^2 + 7 + 1$ cartes attendues, n'en a que 55.

---

①. En d'autres termes, l'addition est définie de la façon la plus simple possible, avec la contrainte que $x \oplus y \neq x \oplus y'$ si $y' < y$ et $x \oplus y \neq x' \oplus y$ si $x' < x$.

②. En d'autres termes, la multiplication est définie de la façon la plus simple possible avec la contrainte que $(x \oplus x') \otimes (y \oplus y') \neq 0$ si $x' < x$ et $y' < y$.

3. Théorie des corps : généralités

3.1. Division euclidienne des polynômes. Soient k un anneau et $f \in k[T]$ un polynôme non nul. Notons $\mathrm{cd}(f)$ le coefficient dominant de $f = a_d T^d + \cdots + a_1 T + a_0$: si $a_d \neq 0$, on pose $\mathrm{cd}(f) := a_d \in k$. Pour tout polynôme $g = b_e T^e + \cdots + b_1 T + b_0$, avec $e \geqslant d$, l'algorithme d'Euclide[①] fournit deux polynômes $u, v \in k[T]$ tels que

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

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

Nous allons maintenant rappeler brièvement les résultats analogues à ceux que nous avons vus, sur $\mathbb{Z}$, dans les sections **1.2** et **1.4**.

3.1.1. *PGCD.* Supposons dans ce paragraphe que k est un corps, de sorte que le coefficient d'un polynôme non nul est inversible. Il résulte de ce qui précède[②] que

> tout idéal I de $k[T]$ est principal : il existe un polynôme h tel que I soit l'idéal $(h) = h \cdot k[T]$ 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 $(f, g) = \{af + bg \ : \ a, b \in k[T]\}$ engendré par f et g soit égal à (h) : c'est le PGCD de f et g.

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

3.2. Rappels terminologiques.

3.2.1. On rappelle qu'un corps est un anneau (commutatif) $k \neq 0$ tel que tout élément non nul soit inversible : $k^\times = k - \{\mathbf{0}_k\}$. 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). Si k est un corps, le noyau $\mathrm{Ker}(\mathbb{Z} \to k) := \{n \in \mathbb{Z} \ : \ n \cdot 1_k = 0\}$ est un idéal de $\mathbb{Z}$, engendré par un (unique) entier $n \geqslant 0$, la caractéristique de k. On note $\mathrm{car.}(k)$ cet entier, qui est nécessairement nul ou un nombre premier : $\mathbb{Z}/n\mathbb{Z}$ n'est intègre que dans ces cas.

Si $\mathrm{car.}(k) = 0$, l'anneau $\mathbb{Z}$ s'injecte dans k ; en particulier, k est infini. Si $\mathrm{car.}(k) = p > 0$, le corps $\mathbb{F}_p$ s'injecte — de façon unique — dans k, en faisant ainsi une **$\mathbb{F}_p$-algèbre** [代数], ce qui est une autre façon de dire que l'on a un morphisme d'anneaux $\mathbb{F}_p \to k$ ou, plus simplement peut-être, que k est un anneau dans lequel $p = 0$.

3.2.2. Proposition. *Soit k un corps de caractéristique p ou, plus généralement, une $\mathbb{F}_p$-algèbre (commutative). L'application $\mathrm{Frob}_p : k \to k$, $a \mapsto a^p$ est un endomorphisme de $\mathbb{F}_p$-algèbre :*

---

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

② Si nécessaire, voir l'exercice **3.4.1**.

(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 retrouve le **petit théorème de Fermat** (1.5.4) : pour tout entier $n \geqslant 0$, et tout nombre premier p, on a la congruence

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

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

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

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 $(p-i)!$. □

3.2.3. Soit K une k-algèbre. Si k est un corps, le morphisme $k \to K$ est nécessairement injectif car tout élément non nul du noyau est inversible dans k, de même que son image dans K, supposée nulle. Si K est aussi un corps, on dit aussi que K est une **extension** [扩张] de k, ce qui est justifié par la remarque précédente : on peut voir K comme un sur-corps de k.

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

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

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

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

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 $k[T]$; comme k est un corps, il est principal, c'est-à-dire de la forme $(f) = f \cdot k[T]$. Par « propriété universelle du quotient » — c'est-à-dire ici le fait que $g(a)$ ne dépende que du reste de la division euclidienne de g par f —, on a bien :

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

où le terme de gauche est l'ensemble des classes de polynômes modulo f. (On rappelle que, sauf si $f = 0$, toute classe est représentée par un unique polynôme de degré $< \deg(f)$.) 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 $f(a) = 0$. Il est *irréductible* si A est un corps[①] car, dans ce cas, toute décomposition $f = gh$ est triviale : si $f(a) = g(a)h(a) = 0$, on a $g(a) = 0$ ou $h(a) = 0$.

Par exemple, l'élément $\sqrt{2} \in \mathbb{R}$ est entier sur $\mathbb{Q}$, de polynôme minimal $T^2 - 2$. (Il n'y a pas de polynôme de degré 1 à coefficient rationnel l'annulant car ce nombre est irrationnel.) En conséquence, l'anneau $\mathbb{Q}[\sqrt{2}] \subseteq \mathbb{R}$ est isomorphe à $\mathbb{Q}[T]/(T^2 - 2)$.

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] ; de même, ses éléments sont en général dits *algébriques* sur k.

3.2.5. Proposition. *Une extension de degré finie est algébrique.*

Démonstration. Soient K/k une extension de degré fini et $x \in K$. La famille des puissances $\{1, x, x^2, \dots\}$ de x appartient au k-espace vectoriel *de dimension finie* K ; elle est donc liée. Une relation $\sum_i \lambda_i x^i = 0$ (λ_i non tous nuls) se réécrit $f(x) = 0$ avec $f \in k[T] - \{0\}$. Puisque k est un corps, on peut supposer f unitaire[②]. □

3.3. Compléments.

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

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

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

---

①. Si $k[a]$ est un corps, on le note également $k(a)$, par analogie avec la distinction entre $k[T] = \{P(T)\}$ — l'anneau des polynômes — et $k(T) = \{P(T)/Q(T)\}$ — le *corps* des fractions rationnelles —.

②. On observera que la démonstration est essentiellement identique à celle du fait que pour tout endomorphisme u d'un k-espace vectoriel V de dimension finie d, il existe un polynôme non nul $f \in k[T]$ tel que $f(u) = 0$: cela résulte du fait que $\mathrm{End}_k(V)$ est de dimension finie (d^2) sur k. (D'ailleurs, en appliquant ce fait à l'endomorphisme de multiplication par $x \in K$, on obtient le résultat de la proposition.) Le théorème de Cayley-Hamilton améliore la borne d^2 sur le degré de f en d.

3.3.2. Donnons la démonstration dans le cas particulier où k est un corps et A intègre : c'est le cas essentiel. Pour une autre approche, plus générale et plus algorithmique, voir l'exercice **3.4.4**. Puisque k est maintenant un corps, on peut utiliser les techniques de l'algèbre linéaire usuelle. En particulier, tout 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 $B \coloneqq k[a]$ de A est intègre (car A l'est) et de dimension finie sur k ; c'est donc un corps (cf. exercice **3.4.2**).

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[①]. 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 (« base télescopique »). *Si $k \to K$ et $K \to L$ sont deux* extensions finies*, c'est-à-dire telles que $[K : k], [L : K] < +\infty$, on a*

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

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

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

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

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

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

3.3.3. *Adjonction de racines.* Dans le paragraphe précédent, on se donnait un ou des éléments d'une k-algèbre et on considérait les polynômes à coefficients dans k s'annulant en ces éléments. Réciproquement, on peut se demander si, partant d'un polynôme à coefficients dans k, on peut trouver une k-algèbre dans laquelle il a

① Par analogie avec les notations $\mathbb{R}[T]$ et $\mathbb{R}(T)$ pour, respectivement, l'anneau de polynômes et le corps des fractions rationnelles.

un ou des racines. L'exemple classique, mais peut-être pas parfaitement typique[①], étant le polynôme $T^2+1 \in \mathbb{R}[T]$: on ajoute une racine carré de -1 — c'est-à-dire une racine de T^2+1 — en considérant le quotient $\mathbb{C} \coloneqq \mathbb{R}[T]/(T^2+1)$.

Plusieurs questions naturelles se posent :

(i) Que donne cette construction $k[T]/(f)$ pour un polynôme arbitraire $f \in k[T]$?

(ii) Cette construction fournit un anneau dans lequel le polynôme de départ a *une* racine ; est-il possible de construire explicitement un anneau dans lequel le polynôme de départ serait *scindé*, c'est-à-dire aurait *toutes* ses racines ?

(iii) Dans l'exemple $\mathbb{R}[\sqrt{-1}] = \mathbb{R}[T]/(T^2+1)$, le corps $\mathbb{C}$ obtenu est **algébriquement clos** [代数闭(域)] : les polynômes non constants à coefficients dans $\mathbb{C}$ sont scindés ; existe-t-il pour tout corps k une extension qui soit algébriquement close ?

Considérons ces questions dans l'ordre.

(i) 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[②] un isomorphisme

$$k[T]/(f) \xrightarrow{\sim} \prod_i k[T]/(f_i^{e_i}),$$

de sorte que notre k-algèbre est un produit d'algèbre du même type, pour f ayant un unique facteur irréductible g c'est-à-dire tel que $f = g^e$, avec g irréductible. Si $e = 1$, le quotient $k[T]/(f) = k[T]/(g)$ est un corps ; si $e > 1$, c'est un anneau non intègre car l'élément $g \pmod f$ est *nilpotent* : $g(t)^e = 0$. En particulier, si f est sans facteur carré, on voit que la k-algèbre $k[T]/(f)$ est isomorphe à un produit fini d'extensions finies de k.

(ii) Notons tout d'abord que la question se pose : si $k = \mathbb{Q}$ et $f = T^3 - 2$, le corps $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$ ne contient pas les deux autres racines, qui ne sont pas réelles[③]. La construction $f \mapsto k[T]/(f)$ construit une k-algèbre dans laquelle le polynôme unitaire f a un zéro tautologique : si $t \in k[T]/(f)$ est la classe de T modulo f, on a $f(t) = 0$. Il est donc facile de construire une k-algèbre dans laquelle f a [au moins][④] *une* racine ; et c'est un corps, appelé **corps de rupture**, si f est *irréductible*.

Pour obtenir une k-algèbre dans laquelle f est *scindé*, c'est-à-dire se factorise en produit de polynômes de degré 1, on peut itérer le processus précédent : construire une k-algèbre A_1 dans laquelle f s'écrit $(T - x_1)g_1$, puis une A_1-algèbre A_2 dans laquelle g se factorise en $(T-x_2)g_2$ pour aboutir à une k-algèbre A_d, où $d = \deg(f)$, dans laquelle f se factorise en $\prod_{i=1}^{d}(T - x_i)$.

---

①. Pourquoi ?

②. C'est l'analogue du théorème chinois usuel sur $\mathbb{Z}$, que l'on démontre de la même façon. [Il faut cependant remplacer l'argument de « même cardinalité » par un argument de « même dimension ».] Pour un énoncé plus général, inutile ici, voir par exemple le paragraphe 3.5 des notes de cours de 2016-2017.

③. On verra cependant, *a posteriori* que si k est fini, un polynôme irréductible ayant une racine dans une extension est automatiquement scindé dans cette extension.

④. On verra plus tard que si k est un corps fini et f irréductible, s'il a une racine dans une k-algèbre, il les a toutes.

On peut également construire directement une telle k-algèbre en posant :

$$A \coloneqq k[X_1, \ldots, X_d]/\big((\sum_i X_i) - a_1, (\sum_{i<j} X_i X_j) - a_2, \ldots, \prod_i X_i - a_d\big),$$

où

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

est un polynôme unitaire de degré d. On l'appelle l'**algèbre de décomposition universelle**, formellement définie comme le quotient l'anneau de polynômes $k[X_1, \ldots, X_d]$ par l'idéal engendré par les $\sigma_r(X_1, \ldots, X_r) - a_r$, $1 \leq r \leq d$, où les $\sigma_1, \ldots, \sigma_d \in k[X_1, \ldots, X_d]$,sont les **fonctions symétriques élémentaires** [初等对称函数 / 初等对称多项式] définies par l'égalité

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

Par exemple, $\sigma_1 = X_1 + \cdots + X_d$ et $\sigma_d = X_1 \cdots X_d$; en général, on a

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

Par construction, le polynôme f devient *scindé* sur A : on a l'égalité

$$f = \prod_{i=1}^{d}(T - x_i)$$

dans $A[T]$, où les x_i, $1 \leq i \leq d$, désignent les images des X_i dans A par la surjection canonique $k[X_1, \ldots, X_d] \twoheadrightarrow A$.

Remarque. Dans la discussion précédente, les k-algèbres considérées ne sont pas nécessairement des *corps* ; si l'on veut montrer que, donné un polynôme unitaire $f \in k[T]$ (non constant), il existe une extension K de k dans laquelle il est scindé[①], il suffit de montrer que pour tout k-algèbre non nulle A, il existe un k-morphisme $A \to K$, où K est un corps. C'est ce qu'affirme le « théorème de Krull », dont la démonstration est très élémentaire mais formelle et peu éclairante pour la suite du cours.

(iii) De même que l'on peut itérer la construction du (i) pour répondre à la question (ii), on peut itérer (ii) pour répondre à la question (iii) : si on pouvait énumérer les polynômes unitaires de k en une suite $\{f_0, f_1, \ldots, f_n, \ldots\}$, on obtiendrait (non canoniquement) une suite d'extensions $k \subseteq K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n \subseteq \cdots$ telles que f_i pour $i \leqslant n$ soit scindé dans K_n. Intuitivement, dans le corps $K_\infty \coloneqq \bigcup_n K_n$, tous les polynômes à coefficients dans k sont scindés. Cet argument présente au moins deux difficultés :

(a) L'ensemble $k[T]$ n'est pas nécessairement dénombrable. Ce n'est pas une difficulté sérieuse — la théorie des ensembles permet de considérer l'analogue de ces unions croissantes dans un contexte plus général —, d'autant plus que, dans nos applications, k — donc $k[T]$, sera dénombrable.

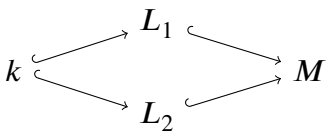
① On dit que K est un **corps de décomposition** [分裂域] de f si elle est de plus engendrée par les racines de f.

(b) Le corps K_∞ obtenu a la propriété de scinder tout polynôme non constant de k, mais les polynômes de K sont-ils eux aussi scindés sur K ? Oui : cf. exercice 3.4.3.

3.3.4. *Unicité.* Soit f un polynôme à coefficients dans un corps k. On a vu ci-dessus, qu'il existe un corps de rupture K_1 et un corps de décomposition K_2 de f. Lorsque f est irréductible, il est clair que le premier est unique à k-isomorphisme près : il est isomorphe à $k[T]/(f)$; mais si f possède deux facteurs irréductibles distincts, il ne peut y avoir unicité. Par contre, le corps de décomposition est toujours unique, à isomorphisme (non unique) près : si K_2 et K_2' sont deux corps de décomposition d'un polynôme f, il existe un k-isomorphisme $K_2 \xrightarrow{\sim} K_2'$. Cela résulte des deux observations suivantes :

(i) si f est scindé dans une extension Ω de k, il existe un unique corps de décomposition de f dans Ω : c'est la sous-extension de Ω engendrée par les racines de f ;

(ii) Toutes paires d'extensions est « coiffée » par une troisième : si L_1 et L_2 sont deux extensions de k, il existe une k-extension M dominant L_1 et L_2, c'est-à-dire un diagramme « commutatif » (l'image d'un élément de k dans M ne dépend pas du chemin choisi, par le haut ou par le bas) :



Nous admettons ce fait, non pas qu'il soit difficile[①], mais parce que la démonstration n'est pas particulièrement éclairante dans le cadre de ce cours.

3.4. Exercices.

3.4.1. Vérifier que tout idéal de $k[T]$, où k est un corps, est principal, c'est-à-dire engendré par un élément.

3.4.2. Montrer que si k est un corps et A une k-algèbre intègre, de dimension finie sur k, alors A est un *corps*.

Indication : on pourra s'inspirer de la démonstration du fait qu'en dimension finie, les endomorphismes injectifs sont bijectif.

3.4.3. Soit $K \,/\, k$ une extension *algébrique* telle que tout polynôme non constant à coefficients dans k soit scindé sur K. Montrer que K est algébriquement clos.

3.4.4. Trouver une matrice carrée 6×6 à coefficients rationnels dont le polynôme caractéristique s'annule en $\sqrt[2]{3} + \sqrt[3]{2}$.

---

①. ¶ Indication de preuve : d'après le théorème de Krull sus-mentionné, il suffit de construire une k-algèbre B [non nulle] recevant L_1 et L_2. Un procédé général permet de le faire : considérer le *produit tensoriel* $B \coloneqq L_1 \otimes_k L_2$.

3.4.5. Montrer qu'un corps fini n'est pas algébriquement clos.

Indication : on pourra s'inspirer de la démonstration d'Euclide de l'existence d'une infinité de nombres premiers.

3.4.6. ¶ Soit p un nombre premier. On note $\mathbb{F}_p[T]_1 \subseteq \mathbb{F}_p[T]$ l'ensemble des polynômes unitaires, $\mathbb{F}_p[T]_{>0}$ ceux de degré > 0 et enfin E l'ensemble des paires (v, u), où $u \in \mathbb{F}_p[T]_1$ et $v \in \mathbb{F}_p[T]$ satisfait $v \neq 0$ ou $\deg(v) < \deg(u)$. (Ceux pour lesquels on peut faire une division euclidienne de u par v.) Par convention, on pose $\deg((v, u)) := \deg(u)$.

Pour tout ensemble $Y \subseteq \mathbb{F}_p[T]$, on note $\mathrm{SF}(Y)$ désigne l'ensemble des suites de longueur finie > 0 à valeurs dans un ensemble Y : c'est l'ensemble des k-uplets d'éléments de Y, pour k variable. On pose également $\deg(y_1, \ldots, y_k) = \sum_i \deg(y_i)$ et $e(y_1, \ldots, y_k) = k$ la longueur de la suite.

(i) Montrer que l'algorithme d'Euclide étendu induit une bijection entre l'ensemble E et l'ensemble $\mathrm{SF}\big(\mathbb{F}_p[T]_{>0}\big) \times \mathbb{F}_p[T]_1$. Vérifier qu'elle respecte le degré : si (v, u) correspond à un élément $\big((y_1, \ldots, y_k), f\big)$, on a $\deg(v, u) = \deg(y_1, \ldots, y_k) + \deg(f)$.

(ii) Soient $Y \subseteq \mathbb{F}_p[T]$ un ensemble et $Z_Y(T)$ la série génératrice associée :

$$Z_Y(T) := \sum_{f \in Y} T^{\deg(f)}.$$

Montrer que la série génératrice

$$Z_{\mathrm{SF}(Y)}(T, \lambda) := \sum_{s \in \mathrm{SF}(Y)} \lambda^{e(s)} T^{\deg(s)}$$

est égale à $\sum_{k>0} \lambda^k Z_Y(T)^k = \frac{\lambda Z_Y(T)}{1 - \lambda Z_Y(T)}$.

(iii) Soit $Z_{\mathbb{F}_p[T]_{>0}}(T) := \sum_{f \in \mathbb{F}_p[T]_{>0}} T^{\deg(f)}$, l'analogue de la fonction Zêta considérée en 2.3. Montrer que $Z_{\mathbb{F}_p[T]_{>0}}(T) = \frac{p(p-1)T}{1-pT}$.

(iv) Déduire la série génératrice

$$Z_E(T, \lambda) := \sum_{(v,u) \in E} \lambda^{e(u,v)} T^{\deg(u)},$$

où $e(u, v)$ est le nombre d'étapes du calcul du PGCD de (v, u) par l'algorithme d'Euclide.

(v) En déduire que le nombre moyen d'étapes dans le calcul du PGCD d'une paire de polynômes $(v, u) \in \mathbb{F}_p[T]$ avec $\deg(v) < \deg(u) = n$ est $(1 - \frac{1}{p})n$. (On considère qu'il n'y a aucune étape si $v = 0$.)

4. Corps finis II

4.1. Existence et unicité.

4.1.1. Soient p un nombre premier et K un corps fini de caractéristique p. Les faits suivants sont de démonstration immédiate : (1) K est de cardinal $q = p^d$, où d est la dimension de K vu comme espace vectoriel sur le corps $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ et (2) K est un corps de décomposition du polynôme $X^q - X$. Pour établir (1) — qui n'est mis ici que pour mémoire (cf. 2.1.2) —, 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.

4.1.2. Réciproquement, on peut appliquer la construction (3.3.3) 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 (3.2.2) que l'application $\mathrm{Frob}_p : x \mapsto x^p$, ainsi donc que ses puissances, est un *(endo)morphisme* : $(x+y)^p = x^p + y^p$ — égalité valable pour couple (x, y) d'une $\mathbb{F}_p$-algèbre. L'ensemble R est donc un *sous-corps* de K ; comme il contient (trivialement) les racines de $X^q - X$, on a $R = K$ et finalement $\#K = q$, comme annoncé.

Mise en garde :

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

4.1.3. Notons qu'il résulte de la construction qu'un corps K de cardinal q^d contient un unique sous-corps de cardinal q, qui coïncide avec l'ensemble des racines de $T^q - T$ dans K.

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

4.2.1. 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. Il existe un élément $x \in G$ d'ordre exactement n.

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 $n_1 n_2$. Pour un tel x, le sous-groupe *cyclique* $\langle x \rangle$ de G engendré par x est d'ordre n.

Supposons maintenant que G soit un sous-groupe du groupe multiplicatif $K^\times$ d'un corps K. On a alors l'inclusion on a $\langle x \rangle \leqslant G \leqslant \mu_n(K) := \{\lambda \in K : \lambda^n = 1\}$; le terme de gauche est de cardinal exactement n et celui de droite de cardinal *au plus* n : un polynôme de degré n, comme $T^n - 1$, a au plus n racines. On en déduit que $\langle x \rangle = G = \mu_n(K)$. En particulier, G est cyclique.

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

Ceci précise l'idée déjà évoquée que

> si K est un corps fini de cardinal q, le groupe multiplicatif $K^\times$ « ressemble » au groupe $\mu_{q-1}(\mathbb{C})$ des racines $(q-1)$-ièmes de l'unité.

(Ils sont même abstraitement isomorphes.)

On a vu en 2.5.3 que le polynôme irréductible $f = T^4 + T + 1 \in \mathbb{F}_2[T]$ est **primitif** (sur $\mathbb{F}_2$), au sens où l'une quelconque de ses racines engendre $\mathbb{F}_{16}^\times$. Par contre, le polynôme irréductible $g = T^4 + T^3 + T^2 + T + 1 \in \mathbb{F}_2[T]$, bien qu'irréductible[①], n'est pas primitif. En effet, on a $T^5 \equiv T \pmod{f}$, c'est-à-dire que la classe t de T dans $\mathbb{F}_2[T]/(g)$ est d'ordre 5, et cette classe n'engendre donc pas $\mathbb{F}_{16}^\times$.

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

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

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.*

(*Mutatis mutandis*, on a le même résultat sur les $\mathbb{F}_q$. Pour un raffinement quantitatif, voir l'exercice 4.3.5.)

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

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

① C'est la réduction modulo 2 du polynôme Φ_5 considérée en 5.2 : on pourrait utiliser le fait que $\langle 2 \rangle = \mathbb{F}_5^\times$, même s'il est plus simple de vérifier qu'il est premier à T, $T+1$ et T^2+T+1.

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

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

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

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

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

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

(*Mutatis mutandis*, on a le même résultat sur les $\mathbb{F}_q$, en remplaçant p par q, et notamment Frob_p par $\mathrm{Frob}_q : y \mapsto y^q$.)

À titre d'application algébrique, on pourra démontrer l'irréductibilité des polynômes d'Artin-Schreier ; cf. exercice **4.3.3**. Voir aussi l'étude de la réduction modulo p des polynômes cyclotomiques (**5.2**).

Remarque. La proposition précédente est à rapprocher du fait que si $z \in \mathbb{C}$, son polynôme minimal sur $\mathbb{R}$ est $\prod_{i<d} \big(T - \mathrm{Frob}_\infty^i(z)\big)$, où Frob_∞ est la conjugaison complexe $z \mapsto \overline{z}$ et $d > 0$ est minimal pour la propriété que $\mathrm{Frob}_\infty^d(z) = z$. Bien entendu, $d = 1$ ou 2, selon que z soit réel ou non — de sorte que le polynôme minimal est $T - z$ ou $(T - z)(T - \overline{z}) = T^2 - 2\Re(z)T + |z|^2$. Cette formulation alambiquée a pour but d'insister sur le fait important :

> L'automorphisme de Frobenius $x \mapsto x^q$ joue pour les corps finis,
> un rôle semblable à la conjugaison complexe.

4.3. Exercices.

4.3.1. Soient p un nombre premier et N un entier. Notons $\mathrm{CF}_{p,N}$ le graphe orienté dont les sommets sont les entiers $1 \leqslant a \leqslant N$ et les arêtes sont définies par : $a \to b$ s'il existe un plongement $\mathbb{F}_{p^a} \hookrightarrow \mathbb{F}_{p^b}$.

(i) Représenter $\mathrm{CF}_{p,N}$ pour de petites valeurs de p, N.

(ii) Comprendre que $\mathrm{CF}_{p,N}$ ne dépend pas de p en l'identifiant à un graphe simple.

4.3.2.

(i) Soit $A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \in M_2(\mathbb{R})$. Existe-t-il $n > 0$ tel que $A^n = \mathrm{Id}$?

(ii) Soit $B = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \in M_2(\mathbb{F}_2)$. Existe-t-il $n > 0$ tel que $B^n = \mathrm{Id}$?

4.3.3. 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 4.2.4.

4.3.4. Soient q un puissance d'un nombre premier, $r > 0$ un entier, $q' = q^r$ et $P = T^r - c_1 T^{r-1} - c_2 T^{r-2} \cdots - c_{r-1} T - c_r \in \mathbb{F}_q[T]$ un polynôme irréductible *primitif* : si x est une racine de P dans $\mathbb{F}_{q'}$, on a $\langle x \rangle = \mathbb{F}_{q'}^\times$.

(i) Vérifier qu'un tel polynôme existe. Combien y en a-t-il ?

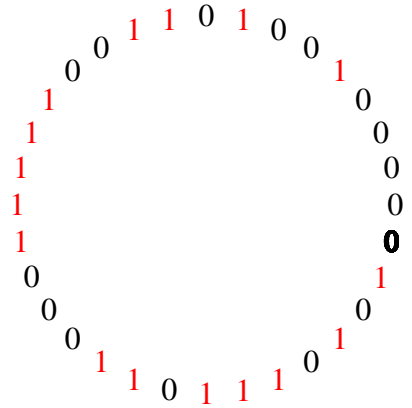
(ii) Soit u la suite q'-périodique à valeurs dans $\mathbb{F}_q$ définie par façon suivante : $u_0 = u_1 = \cdots = u_{r-1} = 0$, $u_r = c_r$ et, pour $r < n < q'$, définie par récurrence

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

Montrer que la suite u est une **suite de de Bruijn** à valeurs dans $\mathbb{F}_q$: pour chaque r-uplet $(m_1, \ldots, m_r) \in \mathbb{F}_q^r$, il existe un unique $0 \leqslant \alpha < q'$ tel que $m_i = u_{\alpha+i}$ pour chaque $1 \leqslant i \leqslant r$.

Indication : on pourra commencer par introduire la matrice compagnon M associée au polynôme P et montrer qu'elle est diagonalisable de valeurs propres des racines primitives $q' - 1$-ièmes de l'unité, dont x.

(iii) Vérifier que pour $q = 2$ et $q' = 2^5 = 32$, le polynôme $T^5 + T^2 + 1 \in \mathbb{F}_2[T]$ convient et que la suite obtenue est



(iv) Montrer, en utilisant la construction précédente, que pour tout ensemble fini $\mathfrak{A}$ de cardinal a et tout entier $n \geqslant 1$, il existe une suite de de Bruijn a^n-périodique à valeurs dans $\mathfrak{A}$.

4.3.5. Montrer que 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. $\frac{1}{2d}$).

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

(i) Rappeler pourquoi $\mathbb{F}_p = \{x \in \Omega : \mathrm{Frob}_p(x) = x\}$.

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

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

4.3.7.

(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].

4.3.8.

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

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

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

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

4.3.10. Soient $f \in \mathbb{F}_p[T]$ un polynôme irréductible de degré d et $\mathbb{F} = \mathbb{F}_p[T]/(f)$ le corps fini associé.

(i) Comment décrire les sous-corps de $\mathbb{F}$, lorsque f est primitif ?

(ii) ¶ Cas général.

4.3.11. 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 $p := \mathrm{car.}(\mathbb{F})$) dont une racine α est primitive et écrire les puissances de α comme un polynôme en α de degré minimal.

4.3.12. 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.

4.3.13.

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

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

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

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

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

4.3.14. 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.

4.3.15. ¶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 $r, s \geq 0$.

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

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

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

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

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

4.3.18. 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 $d \leq 7$.

4.3.19. 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.

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

4.3.21. 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 $q - \frac{q-1}{d}$.

5. Compléments

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

Pour toute puissance q d'un nombre premier p, on note $\mathbb{F}_q$ un corps de cardinal q.

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

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

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

(La courte démonstration est laissée en exercice au lecteur, qui remarquera l'analogue entre la condition $r \leqslant d/2$ et le fait que si un entier n n'a pas de facteur premier $p \leqslant n^{1/2}$, alors il est premier.)

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.

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

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

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

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

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

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

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

(Le complément résulte de ce que $y \in B(f) = \prod_i B(f_i)$, de relèvement $Y \in \mathbb{F}_q[T]$ de degré $< \deg(f)$, alors $\mathrm{PGCD}(f, Y)$ est le produit des f_i tels que Y soit multiple de f_i c'est-à-dire que la i-ième composante de $\text{中}(y)$ s'annule.)

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

Reprenons l'exemple du polynôme $f = T^5 - T^2 - 1 (= T^5 + T^2 + 1) \in \mathbb{F}_2[T]$, considéré en 4.3.4, en lui appliquant cette fois le critère de Butler : il faut d'abord vérifier que f est séparable, c'est-à-dire, premier avec sa dérivée $f' = T^4$, ce qui se fait en général au moyen de l'algorithme d'Euclide mais est évident ici. On calcule alors la matrice de l'endomorphisme $\mathrm{Frob}_2 - \mathrm{Id}$ sur la base $1, t, t^2, \ldots, t^4$ de $\mathbb{F}_2[T]/(f)$, en calculant successivement $T^2, T^4, \ldots, T^8$ modulo f :

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

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

5.2. Polynômes cyclotomiques.

5.2.1. Soient ℓ un nombre premier et $\Phi_\ell(T) := T^{\ell-1} + \cdots + T + 1 \in \mathbb{Z}[T]$ le ℓ-ième polynôme cyclotomique, dont les racines complexes sont les racines ℓ-ièmes de l'unité. (Il n'est pas difficile de vérifier qu'il est irréductible, mais nous n'en ferons pas usage.) On s'intéresse ici à sa réduction $\overline{\Phi}_\ell$ modulo un nombre premier $p \neq \ell$. Factorisons la en un produit $P_1 \cdots P_g$ de polynômes irréductibles unitaires, distincts car $\overline{\Phi}_\ell$ est sans racine multiple, tout comme son multiple $T^\ell - 1$. Soit x une racine de l'un des P_i dans un surcorps de $\mathbb{F}_p$. Puisque x est une racine primitive ℓ-ième de l'unité, le degré de x sur $\mathbb{F}_p$ est égal à l'ordre de p dans $\mathbb{F}_\ell^\times$: cela résulte du (ii) de la proposition du 4.2.4. Ainsi, tous les P_i sont de même degré, que l'on vient de calculer, et le polynôme $\overline{\Phi}_\ell \in \mathbb{F}_p[T]$:

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

5.2.2. Supposons maintenant $\ell \neq 2$ et que p soit un carré modulo ℓ. Si $p = 2$, cela signifie que $\ell \equiv \pm 1 \pmod 8$, d'après le résultat de l'exercice 4.3.6. Fixons $\zeta \neq 1$ une racine ℓ-ième de l'unité dans une extension finie $\mathbb{F}$ de $\mathbb{F}_p$. La décomposition

$$T^\ell - 1 = (T-1)\overline{\Phi_\ell} = (T-1)\prod_{i \in \mathbb{F}_\ell^\times} (T - \zeta^i)$$

dans $\mathbb{F}[T]$ induit une décomposition $T^\ell - 1 = (T-1) f(T) f^\perp(T)$ dans $\mathbb{F}_p[T]$, où

$$f := \prod_{i \in \mathcal{Q}} (T - \zeta^i),$$

(resp. $f^\perp$) est le produit correspondant aux exposants non nuls appartenant à l'ensemble $\mathcal{Q}$ des carrés modulo ℓ (resp. son complémentaire). C'est bien un polynôme à coefficients dans $\mathbb{F}_p$ car l'ensemble des ζ^i, pour i carré modulo ℓ, est stable par Frobenius : l'ensemble $\mathcal{Q}$ est stable par produit et $p \in \mathcal{Q}$ par hypothèse.

5.2.3. Si $\ell \equiv -1 \pmod 4$, c'est-à-dire si -1 n'est pas un carré modulo ℓ, l'application $x \mapsto -x$ induit une bijection entre l'ensemble des carrés de $\mathbb{F}_\ell^\times$ et des non-carrés. En conséquence, on a $f^\perp(T) = T^{(\ell-1)/2} f(1/T)$: c'est le polynôme f « lu » en sens inverse. Par exemple, pour $p = 3$, $\ell = 11$, on trouve $f(T) = T^5 + T^4 - T^3 + T^2 - 1$ et $f^\perp(T) = T^5 - T^3 + T^2 - T - 1$.

La variante suivante est également utile : soit n un entier qui n'est pas un carré modulo ℓ. L'endomorphisme de $\mathbb{F}_p[T]$ défini par $T^i \mapsto T^{ni}$ induit un automorphisme $c \mapsto c_n$ de $\mathbb{F}_p[T]/(T^\ell - 1)$, transformant $f(T) \pmod{T^\ell - 1}$ en $f^\perp(T) \pmod{T^\ell - 1}$. Cet automorphisme correspond à une *permutation* de la base canonique ; en particulier, il ne change pas le poids des vecteurs, c'est-à-dire le nombre de coordonnées non nulles.

5.3. ¶ Codes de résidus quadratiques.

5.3.1. La construction précédente est utile en théorie des communications : on veut envoyer un message, découpé en mots codés comme éléments d'un espace vectoriel de dimension finie sur un corps, de sorte que l'on puisse corriger un maximum d'erreurs faites sur les coordonnées lors de la transmission. Pour une discussion de la problématique générale, voir [Shannon 1948] ; pour un survol historique des débuts de la théorie des codes correcteurs d'erreurs, voir [Thompson 1983, chap. 1].

5.3.2. Soient $V_{p,\ell} := \mathbb{F}_p[T]/(T^\ell - 1)$ et $C_{p,\ell} := (f) \subseteq V$ le sous-espace vectoriel des multiples de f ; ils sont respectivement de dimension ℓ et $(\ell+1)/2$ sur $\mathbb{F}_p$. Notons que dans la base « canonique » $\{1, t, \ldots, t^{\ell-1}\}$ de $V_{p,\ell}$, le sous-espace $C_{p,\ell}$ a la propriété d'être stable par permutation cyclique des coordonnées : si $c = (c_0, \ldots, c_{\ell-1})$ appartient à $C_{p,\ell}$ — correspondant à un polynôme $h(T) \pmod f$ —, il en est de même de $(c_{\ell-1}, c_0, \ldots, c_{\ell-2})$, qui correspond au polynôme $T \cdot h(T)$. Pour vérifier que la classe $c \in V_{p,\ell}$ d'un polynôme $h(T) = \sum_{i<\ell} c_i T^i$ appartient à $C_{p,\ell}$, il suffit de vérifier l'une des deux conditions équivalentes suivantes :

(i) $h(\zeta^{x^2}) = 0$, pour $x \in \mathbb{F}_\ell^\times$;
(ii) le produit $h(T)(T-1)f^\perp(T)$ est nul dans $V_{p,\ell}$.

5.3.3. Dans la terminologie des **code correcteur d'erreurs**[①], un tel sous-espace vectoriel $\mathbb{F}_p^{(\ell+1)/2} \simeq C_{p,\ell} \subseteq V \simeq \mathbb{F}_p^\ell$ est un **code linéaire cyclique** de **longueur** ℓ et de **dimension** $(\ell+1)/2$, appelé **code de résidus quadratiques**, auquel [MacWilliams et Sloane 1977, chap. 16] et [Huffman et Pless 2003, §6.6] sont consacrés.

5.3.4. Soit d le nombre minimal de coefficients non nuls d'un vecteur non nul de C (dans la base canonique). Le code $C_{p,\ell}$ détecte donc des erreurs de poids $< d$ — c'est-à-dire ayant strictement moins de d coordonnées non nulles — et en corrige $\lfloor \frac{d-1}{2} \rfloor$. La borne générale, et élémentaire, de Singleton affirme que $d \leqslant \ell - (\ell+1)/2 + 1 = (\ell+1)/2$. Lorsque $p = 2$, on dispose également de la *minoration* suivante.

Proposition. *Si $p = 2$, la distance minimale d du code $C_{p,\ell}$ satisfait : $d \geqslant \lfloor \sqrt{\ell} \rfloor$.*

① Voir [Demazure 2008] pour une introduction et [MacWilliams et Sloane 1977] pour un traitement encyclopédique.

Au cours de la démonstration, nous utiliserons — en l'admettant — le fait suivant : l'entier d est *impair*[①]

Démonstration. Soit $c \in C_{2,\ell}$ un élément non nul de poids d. L'élément c_n défini en **5.2.3** est également de poids d. D'autre part, le polynôme C_n de degré $< \ell$ de $\mathbb{F}_2[T]$ correspondant est un multiple de $f^\perp$: cela résulte du fait que c correspond à un multiple C de f et que $f(t)_n = f^\perp(t)$. Considérons le produit $P \coloneqq C \cdot C_n \in \mathbb{F}_2[T]$ de ces deux polynômes ; son poids est majoré par d^2, le nombre maximal de monômes pouvant apparaître en développant le produit. Soit $\overline{P}$ l'image de P dans le quotient $V_{2,\ell}$. Comme il est obtenu en substituant les $T^{\ell+i}$ par les T^i, il a un poids inférieur ou égal à celui de P, donc majoré par d^2. Pour conclure, il suffit de montrer que $\overline{P} = \Phi_\ell(t)$, ce dernier étant de poids exactement ℓ. Or, $P \in \mathbb{F}_2[T]$ est un multiple $\Phi_\ell(T)a(T)$ de $\Phi_\ell(T)$; comme, par construction, $t\Phi_\ell(t) = \Phi_\ell(t)$ dans $V_{2,\ell}$, on a $t^i\Phi_\ell(t) = \Phi_\ell(t)$ pour tout $i \geqslant 0$ et, finalement, $\overline{P} = \Phi_\ell(t)a(1_{\mathbb{F}_2})$. Il suffit donc d'observer que $a(1_{\mathbb{F}_2}) \neq 0$; cela résulte du fait que $C(1_{\mathbb{F}_2}) = C_n(1_{\mathbb{F}_2})$ est la classe de d modulo 2, donc $\neq 0$. □

Remarque. La même démonstration permet de montrer, lorsque $\ell \equiv -1 \pmod 4$ que $d^2 - d + 1 \geqslant \ell$: remplacer $C_n(T)$ par son palindrome $T^{(\ell-1)/2}C(1/T)$.

5.3.5. *Exemples.*

(i) Le code binaire $C_{2,23}$, habituellement noté G_{23} est parmi les plus célèbres des codes[②]. Les carrés de $\mathbb{F}_{23}^\times$ étant $\{1, 2, 3, 4, 6, 8, 12, 13, 16, 18\}$, on vérifie que ce code correspond à la factorisation de $T^{23} - 1$ sur $\mathbb{F}_2$ en

$$(T-1)(1+T+T^5+T^6+T^7+T^9+T^{11})(1+T^2+T^4+T^5+T^6+T^{10}+T^{11}).$$

En d'autres termes, le sous-espace G_{23} de $\mathbb{F}_2^{23}$ est engendré par le vecteur de coordonnées $(1,1,0,0,0,1,1,1,0,1,0,1,0^{11})$ et ses 11 translatés à droite. (On note 0^{11} les 11 dernières coordonnées nulles.)
L'entier 2 est bien un carré : on a $5^2 \equiv 2 \pmod{23}$ et les racines 23-ièmes de l'unité appartiennent à une extension de degré 11 de $\mathbb{F}_2$. Sa distance minimale est $d = 7$.

(ii) Le code ternaire $C_{3,11}$ peut être défini par le polynôme

$$-1 + T^2 - T^3 + T^4 + T^5 \in \mathbb{F}_3[T]$$

L'entier 3 est bien un carré : on a $6^2 \equiv 3 \pmod{11}$ et les racines 11-ièmes de l'unité appartiennent à une extension de degré 5 de $\mathbb{F}_3$. Sa distance minimale est $d = 5$.

(iii) Le code binaire $C_{2,7}$ est appelé « code de Hamming[③] » noté parfois H_7 (ou H_3), dont $1 + T + T^3$ est un générateur. Les racines 7-ièmes de l'unité appartiennent à une extension de degré 3 de $\mathbb{F}_2$. Sa distance minimale est 3.

---

①. Voir note **5.5.3**.

②. Découvert par Golay, il a notamment été utilisé — ou plutôt la variante « étendue » $G_{24} \coloneqq \overline{G}_{23}$ — pour envoyer les images de Jupiter et Saturne des sondes Voyager 1 et 2.

③. Voir [Thompson 1983, chap. 1, §2] pour une présentation élémentaire et le contexte historique.

5.4. ¶ Crypto-système « post-quantique » de McEliece. On présente ici brièvement un crypto-système ne reposant pas sur la difficulté de factoriser des entiers, ni de résoudre un problème du logarithme discret pour une autre structure de groupe.

5.4.1. *Clef publique.* La personne A, qui souhaite recevoir des messages chiffrés, fixe :

(i) $n > m$ deux entiers ;
(ii) $M : \mathbb{F}_2^m \to \mathbb{F}_2^n$ une matrice injective d'image un code (linéaire) pour lequel elle sait efficacement faire un décodage avec au plus t erreurs ;
(iii) $S \in \mathrm{GL}_m(\mathbb{F}_2)$ une matrice inversible choisie aléatoirement ;
(iv) $\sigma \in \mathfrak{S}_n$ une permutation aléatoire, de matrice associée $P_\sigma \in \mathrm{GL}_n(\mathbb{F}_2)$;

Elle calcule la matrice $M' := P_\sigma M S$ et rend publique la clef (t, M').

5.4.2. *Chiffrement.* La personne B qui souhaite envoyer à A un message, ou un bout de message, $x \in \mathbb{F}_2^m$ procède ainsi :

(i) choisit aléatoirement un vecteur $\varepsilon \in \mathbb{F}_2^n$ de poids t ;
(ii) calcule $y := M'(x) + \varepsilon$ et l'envoie à A.

5.4.3. *Décodage.* Pour retrouver x à partir de y, la personne A procède ainsi : elle calcule $P_\sigma^{-1}(y) = MS(x) + P_\sigma^{-1}(\varepsilon)$. Puisque $P_\sigma^{-1}(\varepsilon)$ est de poids t, et $MS(x)$ est dans le code linéaire, elle peut retrouver $MS(x)$ — ou, de façon équivalente, $S(x)$ — et enfin x en appliquant l'inverse de S.

5.5. Notes.

5.5.1. Lorsque q est petit, la proposition du paragraphe 5.1.2 fournit telle quelle un algorithme de factorisation, dit de Berlekamp, pour les polynômes f sans facteur carré dans $\mathbb{F}_q[T]$: on utilise des techniques d'algèbre linéaire pour trouver une $\mathbb{F}_q$-base $\tau_1, \dots, \tau_s$ de l'algèbre de Berlekamp $B(f) = \mathrm{Ker}(\mathrm{Frob}_q - \mathrm{Id})$ de f, puis, si $s > 1$ de sorte qu'il y a une factorisation non triviale à effectuer, on tire au hasard un élément $y = c_1\tau_1 + \cdots + c_s\tau_s \in B(f)$ (avec $c_i \in \mathbb{F}_q$) et on calcule les $\mathrm{PGCD}(f, y - c)$ pour les différents $c \in \mathbb{F}_q$: ceci fournira une factorisation non triviale de y dès que les composantes de $中(y)$ ne sont pas toutes égales (où 中 est l'isomorphisme $B(f) \xrightarrow{\sim} (\mathbb{F}_q)^s$ déduit de l'isomorphisme chinois), ce qui se produit pour $q^s - q$ des q^s éléments y de $B(f)$.

Lorsque q est grand, la proposition ne peut pas servir en tant que telle. On peut cependant la combiner avec les mêmes idées que celles utilisées dans l'algorithme dit de Cantor-Zassenhaus, que nous ne détaillons pas : une fois tiré y dans $B(f)$, on calcule $z := y^{(q-1)/2}$ (resp. $z := y + y^2 + y^4 + \cdots + y^{q/2}$ en caractéristique 2), et alors $\mathrm{PGCD}(f, z - 1)$ (resp. $\mathrm{PGCD}(f, z)$) a une probabilité raisonnable de fournir un facteur non trivial de f. Pour une discussion détaillée, voir par exemple [Shoup 2009, chap. 20] ou [Gathen et Gerhard 2003, §14].

5.5.2. Si $p = 2$ et $\ell \equiv -1 \pmod 8$, il n'est pas difficile de vérifier que, pour un bon choix de ζ, le polynôme

$$e_{\square} := \sum_{i \in \mathcal{Q}} T^i$$

est un multiple du polynôme f introduit en **5.2.2** et que l'inclusion d'idéaux $(e_{\square}) \subseteq (f) =: C_{2,\ell}$ qui en résulte est une égalité. (Voir [Demazure 2008, §10.4.5, 13.1.2] pour les détails.) Ceci nous donne un moyen rapide de décrire le code $C_{2,\ell}$: il est engendré par le vecteur de $\mathbb{F}_2^\ell$ correspondant à la fonction caractéristique de l'ensemble $\mathcal{Q}$ des carrés non nuls de $\mathbb{F}_\ell$, ainsi que par ses décalés. (Pour $\ell = 7$, les carrés sont $\{1, 2, 4\}$; les vecteurs sont donc $(0, 1, 1, 0, 1, 0, 0)$, $(1, 1, 0, 1, 0, 0, 0)$, etc. Le code obtenu est le code de Hamming.) Cette approche permet de voir que $C_{2,\ell}$ est naturellement isomorphe au code binaire de parties de $\mathbb{F}_\ell$ (la somme étant la différence symétrique), engendré par $\mathcal{Q} \subseteq \mathbb{F}_\ell$ et ses translatés $\mathcal{Q} + x$, $x \in \mathbb{F}_\ell$.

5.5.3. Le *groupe des automorphismes* $\mathrm{Aut}(C)$ d'un code correcteur d'erreurs $C \subseteq V$ joue un rôle essentiel à la fois dans la théorie des codes, mais aussi dans l'ensemble des mathématiques. Par exemple, les groupes des automorphismes (= de symétrie) des codes G_{23} et G_{24} sont respectivement les « groupes de Mathieu » M_{23} et M_{24}, qui font partie des « briques élémentaires » des groupes finis.

Par définition, $\mathrm{Aut}(C)$ est le sous-groupe des permutations — notion ensembliste — de V, qui transforment tout mot de code [élément de C] en un mot de code. Comme expliqué dans [ibid., §7.6], il est immédiat que, pour montrer que la distance minimale d'un code binaire C est impaire, il suffit de vérifier que le groupe des automorphismes du **code étendu** $\overline{C}$ agit transitivement, c'est-à-dire qu'un mot code peut être envoyé sur n'importe quel autre mot code via un automorphisme du code. Par définition, le code $\overline{C} \subseteq V \oplus \mathbb{F}_2$ est obtenu en ajoutant une dernière coordonnée, qui est la somme des précédentes : c'est un bit de contrôle. Ainsi, pour montrer que la distance minimal des codes $C_{2,\ell}$ est impaire, il « suffit » de calculer $\mathrm{Aut}(\overline{C_{2,\ell}})$ ou, plus simplement, de montrer qu'il a assez d'éléments pour agir transitivement. Voir par exemple [ibid., §13.1.4] pour une telle minoration et [MacWilliams et Sloane 1977, chap. 20] pour la détermination exacte lorsque $\ell = 23$.

5.5.4. Dans la proposition originale de McEliece, usage était fait d'un code (de Goppa) de paramètres $(n, m, t) = (1024, 524, 50)$, mais d'autres paramètres (plus grands) sont maintenant envisagés pour qu'il soit sûr.

Notons que l'on dispose d'algorithmes efficaces de décodage des codes de résidus quadratiques — cf. [ibid., chap. 16, §9] — et que le crypto-système précédente repose sur l'idée que le décodage d'un code linéaire aléatoire est difficile[①].

① Voir par exemple la discussion dans [Berlekamp, McEliece et Tilborg 1978].

5.6. Exercices.

5.6.1.

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

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

5.6.2.

(i) Démontrer les critères de Butler et Ben-Or énoncés en §**5.1**.

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

5.6.3.

(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.

5.6.4. 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 ?

Sigles

The art of computer programming

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

Autres références

Berlekamp, Elwyn R., Robert J. McEliece et Henk C. A. van Tilborg (1978). « On the inherent intractability of certain coding problems ». *IEEE Trans. Information Theory* **IT-24**.(3), 384-386 (↑ p. 39).

Brent, Richard P. et Paul Zimmermann (2011). *Modern computer arithmetic*. Cambridge Monographs on Applied and Computational Mathematics **18**. Cambridge University Press, xvi+221 pages (↑ p. 5).

Demazure, Michel (2008). *Cours d'algèbre*. 2e éd. Cassini (↑ p. 5, 13, 36, 39).

Frobenius, Ferdinand Georg (1896). « Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe ». *Sitz. Akad. Wiss. Berlin.* (= Ges. Abh., II, 719–733), 689-703 (↑ p. 20).

Gathen, Joachim von zur (2015). *CryptoSchool*. Springer-Verlag, 888 pages (↑ p. 5, 9, 16).

Gathen, Joachim von zur et Jürgen Gerhard (2003). *Modern computer algebra*. 2e éd. Cambridge University Press, xiv+785 pages (↑ p. 38).

Hardy, Godfrey Harold et Edward Maitland Wright (1979). *An introduction to the theory of numbers*. 5e éd. Oxford University Press, xvi+426 pages (↑ p. 41).

– (2007). *Introduction à la théorie des nombres*. Traduction française de [Hardy et Wright 1979] par François Sauvageot. Vuibert & Springer, xxxviii+569 pages (↑ p. 6, 7, 16).

Hoffstein, Jeffrey, Jill Pipher et Joseph H. Silverman (2014). *An introduction to mathematical cryptography*. 2e éd. Undergraduate Texts in Mathematics. Springer, xviii+538 pages (↑ p. 7, 9, 16).

Huffman, W. Cary et Vera Pless (2003). *Fundamentals of error-correcting codes*. Cambridge University Press, xviii+646 pages (↑ p. 36).

Ireland, Kenneth et Michael Rosen (1990). *A classical introduction to modern number theory*. Graduate Texts in Mathematics **84**. Springer-Verlag, xiv+389 pages (↑ p. 16).

MacWilliams, F. J. et N. J. A. Sloane (1977). *The theory of error-correcting codes*. North-Holland, 762 pages (↑ p. 36, 39).

Madore, David A. (15 juil. 2015a). « Le jeu de cartes Dobble et la géométrie projective expliquée aux enfants ». Blog (↑ p. 14).

– (27 juil. 2015b). « Comment faire un jeu de *Tribble* ». Blog (↑ p. 14).

Mullen, Gary L. et Daniel Panario, éd. (2013). *Handbook of finite fields*. Discrete Mathematics and its Applications. CRC Press, xxxvi+1033 pages (↑ p. 5, 13, 14).

Needham, Joseph (1959). *Mathematics and the sciences of the heavens and the earth [数学、天学和地学]*. Science and civilisation in China [中国科学技术史] **3**. Cambridge University Press, 877 pages (↑ p. 8).

Perrin, Daniel (1996). *Cours d'algèbre*. Ellipse (↑ p. 6).

Rotman, Joseph J. (1995). *An introduction to the theory of groups*. Quatrième édition. Graduate Texts in Mathematics **148**. Springer-Verlag, xvi+513 pages (↑ p. 6).

Šafarevič, Igor R. [Игорь Ростиславович Шафаревичу] (1997). *Basic notions of algebra*. Springer-Verlag, iv+258 pages (↑ p. 6).

Schroeder, Manfred (2006). *Number theory in science and communication*. 4e éd. Springer Series in Information Sciences **7**. With applications in cryptography, physics, digital information, computing, and self-similarity. Springer-Verlag, xxvi+367 pages (↑ p. 9).

Serre, Jean-Pierre (1977). *Cours d'arithmétique*. 2e éd. Presses universitaires de France, 188 pages (↑ p. 9).

– (1979). « Groupes finis ». Notes d'un cours à l'ÉNSJF ; arXiv :0503154v6 (↑ p. 6).

Shannon, Claude E. (1948). « The Mathematical Theory of Communication ». *Bell System Technical Journal* (↑ p. 36).

Shoup, Victor (2009). *A computational introduction to number theory and algebra*. 2e éd. (Sous licence CC BY-NC-ND). Cambridge University Press, xviii+580 pages (↑ p. 38).

Stinson, Douglas R. (2006). *Cryptography. Theory and practice*. 3e éd. Discrete Mathematics and its Applications. Chapman & Hall/CRC, xviii+593 pages (↑ p. 16).

Thompson, Thomas M. (1983). *From error-correcting codes through sphere packings to simple groups*. Carus Mathematical Monographs **21**. Mathematical Association of America, xiv+228 pages (↑ p. 36, 37).

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 $\mathbb{F}_9 \to \mathbb{F}_{27}$?

   □ 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 $\mathbb{F}_{256} \to \mathbb{F}_{65536}$?

   □ 0 □ 1 □ 2 □ 4 ■ **8** □ 16 □ 256 □ 65536

Examen 2015-2016

Exercice 1.

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

Exercice 2.

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

Exercice 3.

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

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

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

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

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

Exercice 6.

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

Examen 2016-2017

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

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

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

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

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

(On ne demande pas de calculer ce polynôme.)

(*Indication : on pourra s'inspirer du §3.4.4.*)

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

- **(i)** Montrer, *en utilisant la loi de réciprocité quadratique* (§7.7 [du poly de 2017-2018]), qu'il existe $x \in \mathbb{F}_p$ tel que $x^2 = -3$ si et seulement si p est congru à 1 modulo 3.
- **(ii)** Donner une démonstration de ce fait *sans utiliser la réciprocité quadratique.*

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

Exercice 5.

- **(i)** Soit p un nombre premier. Quelle est la probabilité qu'un élément de $\mathbb{F}_p^\times$ tiré (uniformément) au hasard soit un générateur de ce groupe multiplicatif ?
- **(ii)** ¶ Montrer qu'il existe une suite de nombres premiers (p_n) telle que cette probabilité tende vers 0 quand $n \to +\infty$.

  (*Indication : on pourra choisir les* p_n *tels que* $p_n - 1$ *soit divisible par de plus en plus de nombres premiers (par une petite généralisation de §7.3.5 [du poly de 2017-2018]) et utiliser le fait suivant que l'on admettra :* $\prod_{\ell < x} \left(1 - \ell^{-1}\right) \to 0$ *lorsque* $x \to +\infty$*, où* ℓ *parcourt les nombres premiers.*)

Exercice 6. Soit p un nombre premier.

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

Examen 2017-2018[①]

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 $\{a \in A \,:\, a^3 = 1\}$.

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* $A \twoheadrightarrow K$?

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.

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 $T^q + T + a$.

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 $n \geqslant 1$. On définit une matrice carrée $M_f = (a_{i,j})$ de taille $n \times n$ à coefficients dans $\mathbb{F}_q$ par les relations :

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

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

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

① exceptés deux exercices sur les codes correcteurs d'erreurs.

Examen 2018-2019[①]

Exercice 6. Calculer le cardinal de l'intersection

$$\mu_{196560}(\mathbb{C}) \cap \mu_{55}(\mathbb{C}),$$

où, pour tout entier $r > 0$, on note $\mu_r(\mathbb{C})$ l'ensemble $\{z \in \mathbb{C} : z^r = 1\}$.
(*Indication : on pourra utiliser le fait que* $196560 = 2^4 \cdot 3^3 \cdot 5 \cdot 7 \cdot 13$.)

Exercice 7. Soit $f := T^5 - T^2 - T - 1 \in \mathbb{F}_3[T]$.

(i) Quel est le cardinal n de l'anneau $A := \mathbb{F}_3[T]/(f)$? Factoriser $n - 1$.
(ii) L'anneau A est-il un corps ?
(iii) Calculer le cardinal de l'ensemble $\{a \in A : a^{11} = 1\}$.

Exercice 8. Soit $A \subseteq M_2(\mathbb{F}_3)$ le sous-ensemble des matrices à coefficients dans le corps $\mathbb{F}_3$ de la forme

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix},$$

pour $a, b \in \mathbb{F}_3$. Montrer que A, muni de la somme et du produit déduits de $M_2(\mathbb{F}_3)$, est un corps à 9 éléments.

Exercice 9. Soit (F_n) la suite d'entiers définie par $F_0 = 0$, $F_1 = 1$ et $F_{n+2} = F_{n+1} + F_n$ pour $n \geqslant 0$.
Quel est le nombre d'entiers $0 \leqslant n \leqslant 999$ tels que 5 divise F_n ?

① exceptés deux exercices sur les codes correcteurs d'erreurs.