

# 有限域 Corps finis 上海/Shanghai, 2018-11<sup>①</sup>

Fabrice ORGOGOZO<sup>②</sup>.

version : 7b798a7 2019-09-11 21:36:18 +0200

<http://fabrice.orgogozo.perso.math.cnrs.fr/articles/Shanghai4.pdf><sup>③</sup>

## TABLE DES MATIÈRES

1. L'anneau  $\mathbb{Z}/n\mathbb{Z}$ 
  - 1.1. Définition et premières propriétés
  - 1.2. Inversibles de  $\mathbb{Z}/n\mathbb{Z}$
  - 1.3. Le théorème chinois
  - 1.4. Algorithme d'Euclide I
  - 1.5. Groupes cycliques
  - 1.6. RSA
  - 1.7. Notes
  - 1.8. Exercices
2. Corps finis I
  - 2.1. Généralités
  - 2.2. Existence et construction I
  - 2.3. ¶ Fonction zêta
  - 2.4. Notes
  - 2.5. Exercices
3. Théorie des corps : généralités
  - 3.1. Division euclidienne des polynômes
  - 3.2. Rappels terminologiques
  - 3.3. Compléments
  - 3.4. Exercices
4. Corps finis II
  - 4.1. Existence et unicité
  - 4.2. Structure de  $\mathbb{F}_q^\times$  et applications
  - 4.3. Exercices
5. Compléments
  - 5.1. Critères d'irréductibilité dans les corps finis  $\mathbb{F}_q$
  - 5.2. Polynômes cyclotomiques
  - 5.3. ¶ Codes de résidus quadratiques
  - 5.4. ¶ Crypto-système « post-quantique » de McEliece
  - 5.5. Notes
  - 5.6. Exercices

---

①. Cours (séances de 1h40) : 2018-11-13,14,15<sup>2</sup>,16<sup>2</sup>,19,20,21<sup>2</sup>,22

②. « Fabrice Orgogozo » = 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  $\mathbb{Z}/11\mathbb{Z}$ ,  $S_A P_A = \text{Id}$ , 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  $\leq 3$  ;  $(a + b)^p = a^p + b^p$ .
- 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 ;  $\Phi_\ell$  ;  $T^5 - T + 1 \in \mathbb{F}_3[T]$  ; critère de Ben-Or.
- cours n° 11. graphe d'inclusion des corps finis ; cardinal de  $\text{GL}_2(\mathbb{F}_p)$  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 nombres 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<sup>①</sup>  $x \equiv y \pmod{n}$ , 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,

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

Si  $n \geq 1$ , tout entier  $x \in \mathbb{Z}$  s'écrit de façon unique sous la forme  $x = an + b$  avec  $a \in \mathbb{Z}$  et  $0 \leq b < n$  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 :  $\bar{0}, \bar{1}, \dots, \overline{n-1}$ . 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 : «  $\mathbb{Z}$  modulo  $n\mathbb{Z}$  ») des classes de congruences : il suffit de poser

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

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

$$\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}, x \mapsto \bar{x}$$

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]  $\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$  étant surjective – d'où l'usage du symbole «  $\rightarrow$  » –, 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  $n \geq 1$ ) 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  $\bar{2} \cdot \bar{3} = \bar{1}$  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 (mod 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  $n \geq 1$  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,  $\bar{2} \cdot \bar{2} = 0$  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 fautive : 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  $x \mapsto ax$ ,  $A \rightarrow A$  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  $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$  l'est – alors l'entier  $a$  est *premier à  $n$* . En effet, l'existence d'un  $b \in \mathbb{Z}$  tel que  $\bar{a} \cdot \bar{b} = 1_{\mathbb{Z}/n\mathbb{Z}}$  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  $\bar{a} \cdot \bar{u} = \bar{1} (= 1_{\mathbb{Z}/n\mathbb{Z}})$ .

**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  $(\mathbb{Z}/n\mathbb{Z})^\times \subseteq \mathbb{Z}/n\mathbb{Z} \setminus \{0\}$  des inversibles 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<sup>①</sup>. 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]<sup>②</sup>.

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  $\geq 1$  et  $n := n_1 n_2$ . On dispose de deux morphismes d'anneaux  $\mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/n_1\mathbb{Z}$  et  $\mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/n_2\mathbb{Z}$  : 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

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

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  $\text{Ker}(\pi)$ , soit  $a \in \mathbb{Z}$  tel que

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

Par hypothèse, on a donc  $n_1 | a$  et  $n_2 | a$  et on se demande si  $\bar{a} = 0$  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  $n_1, \dots, n_r \geq 1$  des entiers supposés premiers entre eux deux à deux : pour toute paire  $1 \leq i \neq j \leq r$ , on a  $n_i \perp n_j$ . Alors, le morphisme canonique

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

$$a \pmod{n_1 \cdots n_r} \mapsto (a \pmod{n_1}, \dots, a \pmod{n_r})$$

est un isomorphisme.

**1.3.2.** Dans l'exemple ci-dessus, datant de plus de 1700 ans, on cherche un antécédent de  $(\bar{2}, \bar{3}, \bar{2})$  par la surjection  $\mathbb{Z} \rightarrow \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$  ; 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 vu 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* :  $\text{PGCD}(m, n) = \text{PGCD}(a, b)$  (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  $\text{PGCD}(98, 77) = 7$ .

**1.4.2.** Si  $a \perp b$ , c'est-à-dire  $\text{PGCD}(a, b) = 1$ , il existe des entiers  $u$  et  $v$  tels que  $au + bv = 1$  on appelle cette égalité une **relation de Bézout**<sup>①</sup> 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 :

- $(m, n, u, v, u', v') \leftarrow (|a|, |b|, \text{signe}(a), 0, 0, \text{signe}(b))$ .
- 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  $\text{PGCD}(a, b) = d$ , on peut trouver  $u$  et  $v$  tels que  $au + bv = d$  : on a  $\text{PGCD}(\frac{a}{d}, \frac{b}{d}) = 1$ , 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  $\alpha$  et  $\beta$  sont deux entiers relatifs, la somme  $\beta au - abv$  est un entier congru à  $\alpha$  modulo  $a$  et à  $\beta$  modulo  $b$  : on a construit un inverse à l'isomorphisme  $\mathbb{Z}/ab\mathbb{Z} \simeq \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ . (Notons que l'on peut également voir ce qui précède comme un algorithme de calcul de l'inverse de  $a$  dans  $\mathbb{Z}/b\mathbb{Z}$ .)

<sup>①</sup> 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  $O(n^{\log_2(3)}) = O(n^{1,58496\dots})$  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  $O(n^{1,585\dots})$ ).  $\square$

(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<sup>①</sup>  $G$  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  $g$ <sup>②</sup>. Si  $g$  est d'ordre  $n$ , c'est-à-dire si  $G$  est de cardinal  $n$ , on a un isomorphisme  $\mathbb{Z}/n\mathbb{Z} \simeq G$ ,  $r \bmod n \mapsto g^r$ . (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  $|G| \leq 2$ ). Précisément, on a  $\langle g \rangle = \langle g^r \rangle$  si et seulement si  $g \in \langle g^r \rangle$ , si et seulement si il existe un entier  $s$  tel que  $g = g^{rs}$ , ce qui se produit si et seulement si  $rs \equiv 1 \pmod n$ . Il est clairement nécessaire que  $s$  soit premier avec  $n$ . Réciproquement, il résulte du lemme de Bézout que si  $s \perp n$ , il existe  $r$  tel que  $rs \equiv 1 \pmod n$ . 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  $1 \leq s \perp n \leq n$  et l'ensemble des générateurs de  $G$ .

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

Il en résulte que l'on a l'égalité :

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

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

①. Nous supposons cette notion connue et renvoyons à [SERRE 1979], [ŠAFAREVIČ 1997] (magifique 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  $\alpha \geq 1$ . Par multiplicativité de  $\varphi$ , on a donc la minoration  $\varphi(n) \geq \sqrt{n}/2$  pour tout  $n$  et, en particulier,  $\varphi \rightarrow +\infty$ . Des résultats bien plus précis sont établis dans [ibid., 18.4].  $\square$

**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  $X \rightarrow X$ , 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  $y := P_A(x)$  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  $P_A(-) : \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$  est l'élevation  $x \mapsto x^e$  à la puissance  $e$  et, de même, la fonction  $S_A(-) : \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$  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  $(e, n) = P_A$  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  $y = P_A(1070777) = 1473513$  et calcul  $y^d \equiv 1473513^{1051235} \equiv 1070777$ . 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

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

multiplications, où  $v(n)$  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'élevation 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* [孫子算一經卷下第二十六題] 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  $\text{PGCD}(a, b) = \prod_p p^{\min(\alpha_p, \beta_p)}$ . Cependant, factoriser les entiers est algorithmiquement difficile : la meilleure méthode connue (« méthode du crible général de corps de nombres »<sup>①</sup>) 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  $\alpha_p$  et  $\beta_p$  des entiers dont on veut calculer le PGCD est bien moins efficace que l’algorithme d’Euclide, dont le coût est facilement majoré par  $O(\log(n)^2)$ . (Voir par exemple [GATHEN 2015, 15.25 p. 756] pour l’énoncé<sup>②</sup> 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 public 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  $p_1, \dots, p_r$  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  $\ell$  satisfassent quelques conditions arithmétiques — la remarque précédente suppose par exemple l’existence de grands nombres premiers  $\not\equiv 1 \pmod{3}$ <sup>③</sup> — et ainsi que des conditions archimédiennes : par exemple,  $p$  et  $\ell$  doivent être grands (disons au moins 100 chiffres en bases 10) et pas trop proches<sup>④</sup>.

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 «  $O(n^2)$  », 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  $a := \sum_{i=0}^r a_i 10^i$ ,  $0 \leq a_i < 10$ .

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

□ Le nombre 101 étant premier, on a  $\varphi(101) = 100$  et  $a^{100} = 1$  pour tout  $a \in \mathbb{Z}/101\mathbb{Z}^\times = \mathbb{Z}/101\mathbb{Z} \setminus \{0\}$ . Ainsi,  $3^{100} = 3^{200} = \dots = 3^{1\,000\,000} = 1$  dans  $\mathbb{Z}/101\mathbb{Z}$ . L'entier considéré est donc congru à  $3^3 = 27$  modulo 101. □

**1.8.3.** Quelle est la forme simplifiée du caractère traditionnel 贖 ?

□ Le caractère 贖 a pour forme simplifiée 剩 [shèng]. □

**1.8.4.** Nombre de Carmichael.

- (i) Soit  $n$  un entier  $\geq 1$  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  $a^n \equiv a \pmod{n}$  (pour tout  $a$ ) peut-elle servir de test de primalité ?

□

- (i) Commençons par montrer que  $n$  est sans facteur carré. Si  $n = p^2 n'$ , l'élément  $a := 1 + pn' = 1 + \frac{n}{p}$  est d'ordre  $p$  dans le groupe multiplicatif de  $\mathbb{Z}/n\mathbb{Z}$  : calculer  $a^p = (1 + \frac{n}{p})^p$  par la formule du binôme par exemple. Or,  $p$  ne divise pas  $n-1$  ; on ne peut donc avoir  $a^{n-1} = 1$  dans  $(\mathbb{Z}/n\mathbb{Z})^\times$ . (On peut également montrer que pour tout  $p$  premier divisant  $n$ , on a  $p-1 \mid n-1$  : cela résulte immédiatement du théorème chinois et du fait que  $(\mathbb{Z}/p\mathbb{Z})^\times$  est cyclique, établi en 4.2.)
- (ii) Comme l'a montré Carmichael en 1910, l'entier  $561 = 3 \cdot 11 \cdot 17$  satisfait l'hypothèse, car  $3-1 = 2$ ,  $11-1 = 10$  et  $17-1 = 16$  divisent  $561-1 = 560 = 2^4 \cdot 5 \cdot 7$ . Les deux suivants (non premiers) sont 1105 et 1729 ; cf. A002997. Voir [DEMAZURE 2008, §3.3] et [PERRIN-RIOU 2000, p. 26] pour des compléments permettant d'éviter le recours à un ordinateur.

□

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

□ L'idée est simple : le pire cas correspond à la division euclidienne d'un nombre de Fibonacci par son prédécesseur<sup>①</sup>, et on en déduit une majoration en  $\lfloor \log_\varphi((3-\varphi)n) \rfloor$ , où  $\varphi$  est le nombre d'or, soit, plus concrètement, une majoration en  $\lceil 4, 8 \log_{10}(n) - 0, 32 \rceil$ . Plus précisément, on montre par une récurrence immédiate (sur  $r$ ) que si  $0 < y < x$  sont deux entiers de PGCD égal à  $d$  et si l'algorithme d'Euclide s'arrête au bout de  $r$  étapes, alors  $x \geq dF_{r+2}$  et  $y \geq dF_{r+1}$ . Il y a donc au plus  $\frac{3}{2} \log(y) + 1$  pas. (Et,

<sup>①</sup> Fait observé par Lamé en 1844.

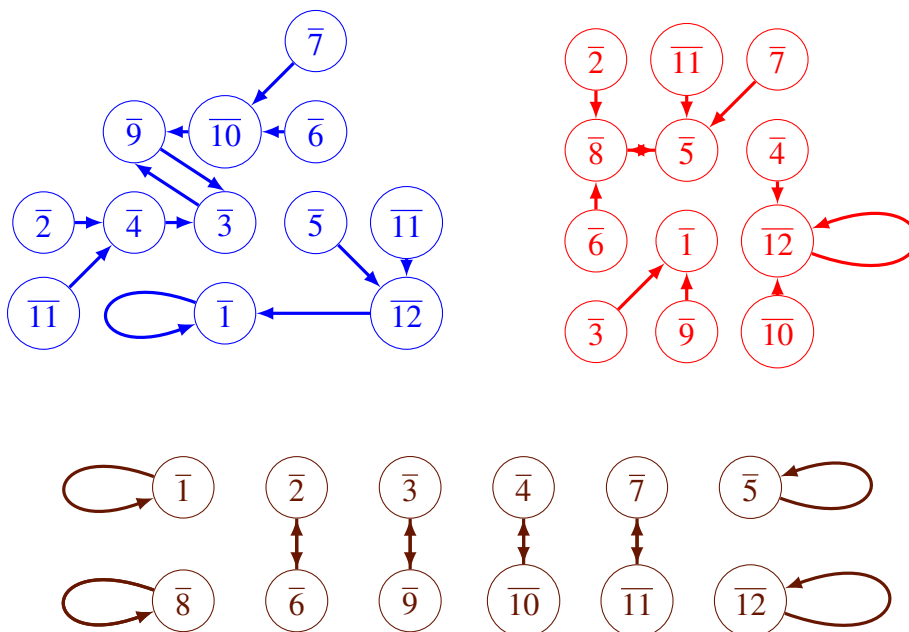
dans le cas du calcul du PGCD de  $F_{r+1}$  et  $F_{r+2}$ , il y a *exactement*  $r$  étapes.) Pour les détails, si nécessaire, sur ce « pire cas », voir [DEMAZURE 2008, 1.4.4]. On trouvera également dans [TAOCP 2, 4.5.3] une analyse plus délicate, « en moyenne » : si deux entiers  $a, b$  sont pris uniformément dans un intervalle  $[1, n]$ , le nombre moyen d'étapes est

$$\frac{12 \log(2)}{\pi^2} \log(n) + C + o(1),$$

où  $C$  est une constante non nulle (explicitée dans [FINCH 2003, §2.18]). Nous verrons plus tard un analogue dans  $\mathbb{F}_p[T]$  ; voir [FLAJOLET et SEDGEWICK 2009, prop. IX.12].□

**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.)

□ On obtient les graphes suivants :



Le cardinal de l'image de l'élevation à la puissance  $r$  est égal à  $(p - 1)/\#\mu_r(\mathbb{F}_p)$  ; pour  $p = 13$ , et  $r \in \{2, 3, 5\}$ , l'ensemble  $\mu_r(\mathbb{F}_p)$  vaut, respectivement,  $\{\pm 1\}$ ,  $\{1, 3, 9\}$ ,  $\{1\}$ .

Une autre façon de voir les choses est de constater que le groupe  $\mathbb{F}_p^\times$  étant cyclique, donc isomorphe à  $\mathbb{Z}/(p - 1)\mathbb{Z}$ , les graphes ci-dessus sont les mêmes que ceux obtenus en considérant non pas  $S_p$  mais  $\mathbb{Z}/(p - 1)\mathbb{Z}$  et non pas l'application  $x \mapsto x^r$  mais l'application  $x \mapsto rx$ . Pour  $p = 13$ , on considère donc la multiplication par  $r \in \{2, 3, 5\}$  sur  $\mathbb{Z}/12\mathbb{Z} \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ . La multiplication par 2 étant une bijection sur le second facteur, et d'image  $2\mathbb{Z}/4\mathbb{Z} \subseteq \mathbb{Z}/4\mathbb{Z}$  dans le premier, on comprend que les flèches touchent la moitié [= 6] des

sommets. De même, la multiplication par 3 touche un tiers [= 4] des sommets tandis que la multiplication par 5 étant bijective (car  $5 \perp 3$  et  $5 \perp 4$ ) on obtient tous les sommets.

Il résulte des congruences  $2^4 \equiv 2^2 \pmod{12}$ ,  $3^3 \equiv 3 \pmod{12}$  et  $5^2 \equiv 1 \pmod{12}$  que l'on a  $[x \mapsto x^2]^{\circ 4} = [x \mapsto x^2]^{\circ 2}$ ,  $[x \mapsto x^3]^{\circ 3} = [x \mapsto x^3]$ , et  $[x \mapsto x^5]^{\circ 2} = \text{Id}$ . En conséquence, on obtient des cycles de longueur [au plus] 2, en appliquant respectivement 2, 1 ou 0 fois l'élevation à la puissance considérée.

□

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

□ D'après le théorème chinois, il s'agit de vérifier que pour tout entier  $x$ , on a  $x^{de} \equiv x \pmod{p}$  (et, de façon équivalente,  $x^{de} \equiv x \pmod{\ell}$ ). Deux cas se présentent :  $x \equiv 0 \pmod{p}$ , et le résultat est trivial, ou bien  $x \perp p$  et alors  $x^{de} \equiv x^1$  car  $de \equiv 1 \pmod{p-1}$  et  $x^{p-1} \equiv 1 \pmod{p}$ . □

**1.8.8.** *Pile ou face à distance.* Soient  $p, \ell$  deux nombres premiers *distincts*, congrus à 3 (mod 4)<sup>①</sup>, 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  $p, \ell$  comme ci-dessus et communique à  $B$  le produit  $n$ .
  - (b)  $B$  choisit un entier  $1 \leq a \leq n-1$  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  $\ell$  [et les donner à  $A$ ], il a gagné ; sinon, il a perdu.

□

- (i) En effet,  $(b^{(p+1)/4})^2 = b^{(p+1)/2} = x^{p+1} = x^{p-1+2} = x^2 = b$  dès lors que  $x^2 = b$ . (Par hypothèse, il existe un tel  $x$ .) Voir [MULLEN et PANARIO 2013, §11.1.116-117] pour d'autres formules et [TAOCP 2, exercice 4.6.2-15] ou [SCHOOF 1985, §4]. Notons également que trouver une racine carrée de  $b \pmod{p}$  revient à factoriser le polynôme  $T^2 - (b \pmod{p}) \in \mathbb{F}_p[T]$  : on peut donc appliquer les techniques générales, et efficaces, de factorisation ([GATHEN et GERHARD 2003, chap. 14] et **5.5.1**).
- (ii) Résoudre l'équation  $x^2 = b$  dans  $\mathbb{Z}/n\mathbb{Z}$  revient à résoudre les deux équations  $x^2 = b \pmod{p}$  et  $x^2 = b \pmod{\ell}$  dans  $\mathbb{F}_p$  et  $\mathbb{F}_\ell$  respectivement : il y a donc  $2 \times 2$  solutions : si  $(x_p, x_\ell)$  est une telle solution de  $x^2 = b$  dans  $\mathbb{F}_p \times \mathbb{F}_\ell$ , l'ensemble des racines carrées est  $\{(\pm x_p, \pm x_\ell)\}$ . (L'entier

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

$\varepsilon := p^{\ell-1} - \ell^{p-1}$  étant envoyé sur  $(-1, 1) \in \mathbb{F}_p \times \mathbb{F}_\ell$ , on en déduit que si  $A$  a calculé une racine carré  $x$  de  $b \pmod{n}$ , les autres sont  $-x$ ,  $\varepsilon x$  et  $-\varepsilon x$ .) Il résulte de ce qui précède que parmi les entiers  $x \in \mathbb{Z}$  tels que  $x^2 = b \pmod{n}$ , il y a en a deux dont la somme  $x + x'$  est divisible par  $p$  mais pas par  $\ell$  : il s'agit des entiers correspondant à une paire  $\{(x_p, x_\ell), (-x_p, x_\ell)\}$  – vue dans  $\mathbb{F}_p \times \mathbb{F}_\ell$  – ou  $\{x, x' = \varepsilon x\}$  – vue dans  $\mathbb{Z}$  –. Ainsi,  $\text{PGCD}(x + x', n) = p$  [et  $\text{PGCD}(x - x', n) = \ell$ ].

- (iii) Si  $A$  a envoyé  $\pm a \pmod{n}$  à  $B$ , cela ne l'avance en rien : il n'obtient aucune information lui permettant de factoriser  $n$ , ce que l'on suppose être difficile. Par contre, si  $A$  a envoyé une des deux autres racines carrées de  $b \pmod{n}$  – ce qui arrive avec probabilité  $\frac{1}{2}$  –, ce qui précède montre que  $B$  peut s'en servir pour calculer rapidement  $p$  et  $\ell$ .

**Remarques.** (a) Une autre façon de formuler ce qui précède est de dire qu'il est aussi difficile de calculer les racines carrées modulo  $n$  que de factoriser  $n$ ; voir [GATHEN 2015, exercices 15.20-21]. (b) Pour une discussion de ce protocole, voir par exemple [SCHROEDER 2006, §19.3], et [ARORA et BARAK 2009, §9.5.3] ou [BONEH et SHOUP 2017, 3.12] pour une présentation générale de ce type de problèmes.

Exemple :

$A$  choisit  $p = 103$ ,  $\ell = 107$  – par exemple en consultant la suite A002145 – de sorte que  $n = 11021$ .  $B$  tire au hasard le nombre  $a = 1234$  et calcule  $b := a^2 \pmod{n}$ , soit [la classe de] 1858, qu'il communique à  $A$ . À l'aide de la factorisation de  $n$ , ce dernier trouve rapidement, en plus de  $\pm 1234 \pmod{n}$  [que  $B$  connaissait déjà mais que  $A$  ignorait], les racines carrées  $\pm 1341 \pmod{n}$ . Précisément :  $A$  calcule  $b$  modulo  $p$  et  $\ell$  [ici :  $1858 \pmod{103} = 4$  et  $1858 \pmod{107} = 39$ ], calcule ensuite dans  $\mathbb{F}_p$  et  $\mathbb{F}_\ell$  les racines carrées par élévation à la puissance [ici :  $4^{26} \equiv 2 =: x_{103}$  et  $39^{27} \equiv 57 =: x_{107}$ ] et relève  $(\pm x_p, \pm x_\ell)$  en  $x_p v \ell + x_\ell u p$  où  $u, v$  satisfait une relation de Bézout  $u p + v \ell = 1$  [ici :  $-27 \times 103 + 26 \times 107 = 1$ ; on trouve notamment  $2 \times 26 \times 107 - 57 \times 27 \times 103 = -152953 \equiv 1341 \pmod{11021}$ ].

$A$  choisit une de ces 4 racines, qu'elle donne à  $B$  : si elle a choisi  $\pm 1234$ ,  $B$  ne peut rien dire d'intéressant sur  $n = 11021$  mais si elle a choisi  $\pm 1341$ ,  $B$  calcule  $1341 + 1234 = 2575 = 5^2 \cdot 103$  et  $1341 - 1234 = 107$ , dont les PGCD avec  $n$  sont respectivement... 103 et 107. Dans ce cas,  $B$  communique ces deux facteurs premiers de  $n$  à  $A$ , qui reconnaît avoir perdu. [Bien entendu, il faut utiliser des nombres premiers beaucoup plus grands, sans quoi le calcul des racines carrées par force brute est instantané.]

□

**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  $\ell$ .

□ On a  $\varphi(n) = p\ell - (p + \ell) + 1 = (\pi + 1) - \sigma$ , où  $\pi = n$  et  $\sigma$  sont respectivement le produit et la somme de  $p$  et  $q$ , qui sont donc les racines d'un polynôme unitaire de degré 2 connu :  $X^2 - \sigma X + \pi$ . Ainsi, les problèmes de factoriser  $n$  [réputer difficile] et calculer  $\varphi(n)$  sont essentiellement équivalents. (Mais il n'est pas exclu que l'on puisse casser RSA, c'est-à-dire calculer des racines  $d$ -ièmes, sans calculer  $\varphi(n)$ .)

Pour une discussion de la sécurité de RSA, voir par exemple [GATHEN 2015, §3.5]. [TAOCP 2, §4.5]. Pour d'autres exercices, voir par exemple [HOFFSTEIN, PIPHER et SILVERMAN 2014, ex. 3.10, p. 182] ou [GATHEN et GERHARD 2003, 20.6, p. 582].□

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

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

Voir aussi la suite A060689.□

## 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  $\mathbb{Z} \rightarrow k$ , envoyant  $n \in \mathbb{N}$  sur  $n \cdot 1_k = 1_k + \dots + 1_k$  ( $n$  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  $\text{car.}(k)$ . (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  $p = \text{car.}(k)$  ;



- (ii) si  $k$  est de cardinal  $n$ , il existe un (unique) nombre premier  $p$ , sa *caractéristique*, et un entier  $d \geq 1$  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  $f$ <sup>①</sup>. La division euclidienne des polynômes — sur laquelle nous reviendrons en 3.1 — nous assure que chaque classe  $\bar{g} \in A$  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  $t = \bar{T}$  la classe de  $T$  dans le quotient :

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

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  $ai \in I$ . 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  $A \rightarrow A/I$ , envoyant  $a$  sur sa classe  $\bar{a}$ , soit un morphisme d'anneaux. Formellement,  $A/I$  est l'ensemble quotient de  $A$  par la relation d'équivalence  $\mathcal{R}_I$  définie par :  $x\mathcal{R}_I y$  si et seulement si  $x - y \in I$ . On dit que  $\mathcal{R}_I$  est la relation de **congruence modulo  $I$**  [模 $I$ 同余(关系)] et on note en général  $x \equiv y \pmod{I}$ . L'importance de cette construction vient notamment du slogan suivant :

quotienter, c'est forcer des égalités.

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

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  $\geq 3$ . (La numérotation  $0, 1, \dots, 7$  correspond à l'ordre lexicographique sur les polynôme ; elle n'est restée pas moins arbitraire.) On observe que l'anneau ainsi obtenu est un corps : tout élément  $\neq 0$  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.

**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  $x \in \{3, 5, 6 = -1\}$  —, 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<sup>①</sup> pour construire  $\mathbb{F}_7[\sqrt{3}] \simeq \mathbb{F}_7[\sqrt{-1}]$ . (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  $\sqrt{3} \mapsto -2\sqrt{-1}$ .)

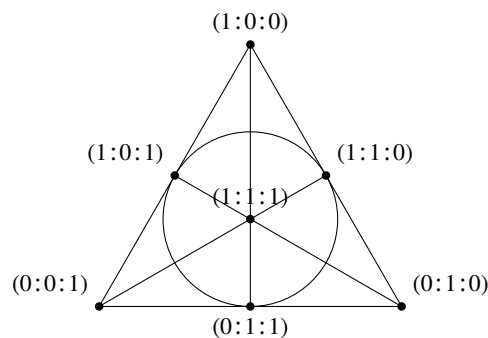
**2.1.5.** La question (iv) de l'intérêt de construire des corps finis plus généraux que les **corps premiers** [素域]  $\mathbb{F}_p$  est, évidemment, celle à laquelle il est le plus difficile de répondre, tant les applications, théoriques ou technologiques, de ces corps sont nombreuses. Certaines font 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

<sup>①</sup>. Voir [MULLEN et PANARIO 2013, théorème 11.7.5] pour une brève discussion et des références sur cette question.

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*<sup>①</sup>  $\mathbf{P}^2(k)$  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).



Pour  $k$  de cardinal 7 on obtient une structure combinatoire à l'origine du jeu *Dobble*<sup>™</sup><sup>②</sup>. 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  $d \geq 1$  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<sup>③</sup>.

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

①. Voir par exemple [DEMAZURE 2008, 7.4] pour une brève discussion.

②. 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.

③. 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  $\deg(a) < \deg(f)$ .

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.

**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  $\prod_P (\sum_{n \geq 1} |P|^{-ns}) = \sum_f |f|^{-s}$  : si  $f = P_1^{n_1} \dots P_r^{n_r}$ , on a  $|f|^{-s} = |P_1|^{-n_1 s} \dots |P_r|^{-n_r s}$ . 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  $P$  parcourt les polynômes irréductibles unitaires de  $\mathbb{F}_p[T]$  et  $I_d$  désigne le nombre d'entre eux de degré  $d$ . Par construction, on a  $\zeta_{\mathbb{F}_p[T]}(s) = Z_{\mathbb{F}_p[T]}(p^{-s})$  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  $d$ )

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

①. Voir 2.4.2.

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

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

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

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

## 2.4. Notes.

**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<sup>①</sup>, signalons également une méthode pour partager un secret en  $N$  « parts » chacune de même longueur que le secret, de manière que  $d + 1$  (avec  $1 \leq d < N$ ) quelconques d'entre elles suffisent à reconstituer le secret mais que  $\leq d$  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**<sup>②</sup> 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  $\leq d$  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  $\leq d$  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  $\leq 255$  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

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.

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'analogie pour les polynômes du résultat difficile énoncé en 1.8.5.

## 2.5. Exercices.

**2.5.1.** Soit  $k$  un corps fini. Vérifier que le morphisme canonique  $\mathbb{Z} \rightarrow k$  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  $F$  ?

□(Voir aussi par exemple [SCHROEDER 2006, §25.3], où le même exemple est traité<sup>①</sup>.)

- (i) Le nombre d'éléments de  $F$  est  $2^{\deg P} = 2^4 = 16$  (comme le nombre de polynômes de degré  $< 4$  sur  $\mathbb{F}_2$ ).
- (ii) On calcule successivement en multipliant par  $T$  et en se rappelant que  $T^4 \equiv T + 1 \pmod{P}$  :

<sup>①</sup>. Ce qui nous amène à nous poser les questions : combien d'autres polynômes auraient donné naissance à un corps à 16 éléments ? [réponse : 3] Combien sont *primitifs*, au sens où l'ordre de  $t$ , la classe de  $T$ , est 15 ? [réponse : 2 ; le polynôme  $T^4 + T^3 + T^2 + T + 1$  n'est pas primitif. En général, leur nombre est  $\varphi(p^d - 1)/d$ , comme on le verra plus tard.]

$i$	$t^i$
0	1
1	$t$
2	$t^2$
3	$t^3$
4	$t^4 = t + 1$
5	$t^2 + t$
6	$t^3 + t^2$
7	$t^4 + t^3 = t^3 + t + 1$
8	$t^4 + t^2 + t = t^2 + 1$
9	$t^3 + t$
10	$t^4 + t^2 = t^2 + t + 1$
11	$t^3 + t^2 + t$
12	$t^4 + t^3 + t^2 = t^3 + t^2 + t + 1$
13	$t^4 + t^3 + t^2 + t = t^3 + t^2 + 1$
14	$t^4 + t^3 + t = t^3 + 1$
15	$t^4 + t = 1$

L'ordre de  $t$  est donc 15 ; celui de  $t^3$  (resp.  $t^5$ ) est 5 (resp. 3).

- (iii) L'inverse de  $t$  est  $t^{14} = t^3 + 1$ . Les puissances de  $t$  étant toutes inversibles, et leur nombre coïncidant avec le cardinal de  $F - \{0\}$ , l'anneau  $F$  est un corps. Le polynôme  $P$  est donc irréductible : si  $P(T) = f(T)g(T)$ , on a  $f(t)g(t) = 0$  dans  $F$  donc  $f(t) = 0$  ou  $g(t) = 0$ , ce qui est impossible si  $f$  ou  $g$  sont non nuls de degré  $< 4$ .
- (iv) Il n'en existe pas pour au moins deux raisons : (a) on aurait l'inclusion de groupes  $K^\times \subseteq F^\times$ , le premier étant de cardinal 7 et le second de cardinal 15 (b) on aurait  $\#F = \#K^d$ , soit  $16 = 8^d$ , où  $d$  est la dimension de  $F$  vu comme  $K$ -espace vectoriel.
- (v) Un sous-corps à 4 éléments ayant un groupe multiplicatif d'ordre 3, son groupe multiplicatif est inclus dans l'ensemble  $\mu_3(F)$  des racines 3-ièmes de l'unité de  $F$ , qui est  $\{1, s, s^2\}$ , où  $s := t^5 = t^2 + t$ . On a  $s^2 = t^4 + t^2 = s + 1$  et le sous-anneau  $\mathbb{F}_2[s] = \{0, 1, s, s + 1\}$  est bien l'unique sous-corps de cardinal 4.

□

#### 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  $\leq 3$ .

□

- (i) On trouve  $f(T) = T^3 + T + 1$  et son palindrome  $g(T) = T^3 f(1/T) = T^3 + T^2 + 1$  : les 6 autres polynômes ont 0 ou 1 pour racine.
- (ii) Nous verrons dans l'exercice 2.5.10 que la réponse est  $\frac{1}{3}p^3 + \frac{1}{2}p^2 + \frac{1}{6}p$  mais il est bon de savoir le faire directement en observant qu'il y a :

- $p$  polynômes unitaires de degré 1 ;
- $p^2 - \binom{p}{2} + p = \binom{p}{2}$  polynômes unitaires irréductibles de degré 2 ;
- $p^3 - \left( \binom{p}{2} \times p + \binom{p}{3} + p(p-1) + p \right) = \frac{1}{3}(p^3 - p)$  de degré 3.

□

**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  $\leq \lfloor \frac{d}{2} \rfloor$ , on a  $g \nmid f$ .

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

**2.5.8.** Soit  $p$  un nombre premier.

- (i) Montrer que si  $n = a_0 + a_1p + \dots + a_r p^r$  est l'écriture de  $n$  en base  $p$ , la plus grande puissance de  $p$  divisant  $n!$  est d'exposant

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

- (ii) En déduire que si  $0 \leq a \leq b$ , la valuation  $p$ -adique  $v_p\left(\binom{b}{a}\right)$  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  $\text{mex}(S) = \min(\mathbb{N} \setminus S)$  le plus petit entier naturel  $n$  appartenant *pas* à  $S$ . Par exemple,  $\text{mex}(\emptyset) = 0$ . On définit par récurrence pour  $x, y \in \mathbb{N}$  :

$$x \oplus y := \text{mex}(\{x' \oplus y : x' < x\} \cup \{x \oplus y' : y' < y\}) \textcircled{1}$$

$$x \otimes y := \text{mex}(\{(x' \otimes y) \oplus (x' \otimes y') \oplus (x \otimes y') : x' < x, y' < y\}) \textcircled{2}$$

- (i) Écrire les tables d'addition et de multiplication induites sur l'ensemble  $[4] := \{0, 1, 2, 3\}$  et vérifier qu'il s'agit d'un corps à 4 éléments.
- (ii) ¶ Faire de même pour  $[16] = \{0, \dots, 15\}$ .

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

□ **Voici les tables pour [4].**

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  $y' < y$ .



$\oplus$	0	1	2	3		$\otimes$	0	1	2	3
0	0	1	2	3		0	0	0	0	0
1	1	0	3	2	et	1	0	1	2	3
2	2	3	0	1		2	0	2	3	1
3	3	2	1	0		3	0	3	1	2

Pour [16] voir [CONWAY 2001, p. 51-52]. Les résultats généraux permettant un calcul rapide de ces tables sont présentés dans [ibid., chap. 6], [LENSTRA 1978], [SIEGEL 2013, chap. IV, §5]. (Voir également l'article 尼姆数 sur Wikipédia et la suite A051775 de l'OEIS.)

On commence par montrer que  $x \oplus y$  est le *ou exclusif* [ [逻辑] 异或 ] des écritures binaires de  $x$  et  $y$ . En d'autres termes, l'addition de deux mêmes « nimbres » est nulle et l'addition de deux puissances distinctes de 2 est l'addition usuelle.

Ensuite, on vérifie par récurrence (non immédiate) que la multiplication est quant à elle caractérisée par le fait que le produit de deux nimbres « de Fermat » (c'est-à-dire de la forme  $2^{2^n}$ ) *distincts* est le produit usuel ( $2^{2^n} \otimes 2^{2^m} = 2^{2^n+2^m}$ , si  $n \neq m$ ) tandis que l'élévation au carré est la multiplication par  $\frac{3}{2}$  : on a  $2^{2^n} \otimes 2^{2^n} = \frac{3}{2} 2^{2^n}$ . (Par exemple  $4 \otimes 4 = 6$ .)

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

Utilisant les égalités  $2^{2^r} \otimes 2^{2^r} = 2^{2^r} \oplus (2^{2^{r-1}} \otimes 2^{2^{r-2}} \otimes \dots \otimes 2)$ , on peut montrer qu'il existe un isomorphisme

$$\begin{aligned} ([2^{2^n}], \oplus, \otimes) &\simeq (\mathbb{F}_2[X_i : 0 \leq i < n] / (X_i^2 + X_i + \prod_{j < i} X_j, 0 \leq i < n), +, \times) \\ \sum_{E \in \mathcal{E}} \prod_{e \in E} 2^{2^e} &\mapsto \sum_{E \in \mathcal{E}} \prod_{e \in E} x_e \end{aligned}$$

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

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

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

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

①. On peut alors en déduire mécaniquement :  $8 \otimes 8 = (4 \otimes 2) \otimes (4 \otimes 2) = (4 \otimes 4) \otimes (2 \otimes 2) = 6 \otimes 3 = \dots = 13$ .

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

*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 le nombre de polynômes unitaires irréductibles de degré  $d$  sur  $\mathbb{F}_p$  vaut

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

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

□ Si nécessaire, voir [HARDY et WRIGHT 2007, 16.3-4] ou [SCHROEDER 2006, §20] pour la formule d'inversion de Möbius (i) et [COX 2004, 11.2] pour une discussion de la formule de Gauß (ii). □

### 2.5.11.

- (i) Utiliser le plan de Fano pour voir comment construire un jeu de *Dobble*<sup>TM</sup> 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.

## 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  $\text{cd}(f)$  le coefficient dominant de  $f = a_d T^d + \dots + a_1 T + a_0$  : si  $a_d \neq 0$ , on pose  $\text{cd}(f) := a_d \in k$ . Pour tout polynôme  $g = b_e T^e + \dots + b_1 T + b_0$ , avec  $e \geq d$ , l'algorithme d'Euclide<sup>①</sup> fournit deux polynômes  $u, v \in k[T]$  tels que

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

(Rappelons que l'on note  $\deg(v)$  le **degré** [次数] d'un polynôme  $v$ .) Dans le cas particulier où  $\text{cd}(f) = 1$ , c'est-à-dire si  $f$  est unitaire, 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<sup>②</sup> 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  $h$ .

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

②. Si nécessaire, voir l'exercice 3.4.1.

(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  $\text{PGCD}(g, f) = \text{PGCD}(f, v)$ . Il en résulte que l'algorithme d'Euclide permet également de calculer  $\text{PGCD}(g, f)$  : on itère  $\text{PGCD}(g, f) = \text{PGCD}(f, v) = \dots$  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 :  $k^\times = k - \{0_k\}$ . 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  $\text{Ker}(\mathbb{Z} \rightarrow k) := \{n \in \mathbb{Z} : n \cdot 1_k = 0\}$  est un idéal de  $\mathbb{Z}$ , engendré par un (unique) entier  $n \geq 0$ , la caractéristique de  $k$ . On note  $\text{car.}(k)$  cet entier, qui est nécessairement nul ou un nombre premier :  $\mathbb{Z}/n\mathbb{Z}$  n'est intègre que dans ces cas.

Si  $\text{car.}(k) = 0$ , l'anneau  $\mathbb{Z}$  s'injecte dans  $k$  ; en particulier,  $k$  est infini. Si  $\text{car.}(k) = p > 0$ , 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  $\mathbb{F}_p \rightarrow k$  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  $\text{Frob}_p : k \rightarrow k, a \mapsto a^p$  est un endomorphisme de  $\mathbb{F}_p$ -algèbre :

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

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

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

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

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

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

Le morphisme  $\text{Frob}_p$  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 retrouvé le **petit théorème de Fermat** (1.5.4) : pour tout entier  $n \geq 0$ , et tout nombre premier  $p$ , on a la congruence

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

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

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

Il suffit donc de montrer que si  $0 < i < p$ , on a  $\binom{p}{i} \cdot \mathbf{1}_A = 0$ , c'est-à-dire que la caractéristique  $p$  divise l'entier  $\binom{p}{i} = \frac{p!}{i!(p-i)!}$ . Cela résulte par exemple du fait que  $i! \perp p$  pour  $0 < i < p$ , et de même pour  $(p-i)!$ .  $\square$

**3.2.3.** Soit  $K$  une  $k$ -algèbre. Si  $k$  est un corps, le morphisme  $k \rightarrow K$  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  $a$  :

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

*A priori*, il n'y a pas de borne sur l'entier  $n$ . Cependant, nous allons voir que si  $a$  est **entier** [整(元)] sur  $k$ , c'est-à-dire s'il existe  $f \in k[T]$  unitaire tel que  $f(a) = 0$ , alors on peut ci-dessus se restreindre aux combinaisons linéaires des  $a^i$  pour  $i < \deg(f)$ . 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  $k[T]/(f) \rightarrow k[a]$ ,  $g \bmod f \mapsto g(a)$ .

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  $k[T] \rightarrow k[a]$ ,  $g \mapsto g(a)$ . 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 :

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

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<sup>①</sup> 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  $k$ .

<sup>①</sup>. 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 –.

**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  $\sum_i \lambda_i x^i = 0$  ( $\lambda_i$  non tous nuls) se réécrit  $f(x) = 0$  avec  $f \in k[T] - \{0\}$ . Puisque  $k$  est un corps, on peut supposer  $f$  unitaire<sup>①</sup>.  $\square$

### 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,  $\lambda a$  le soit pour tout  $\lambda \in k$  est évident : si  $a^n + c_1 a^{n-1} + \dots + c_0 = 0$  alors  $(\lambda a)^n + \lambda c_1 (\lambda a)^{n-1} + \dots + \lambda^n c_0 = 0$ .)

**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  $B := k[a]$  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<sup>②</sup>. 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  $k \rightarrow K$  et  $K \rightarrow L$  sont deux extensions finies, c'est-à-dire telles que  $[K : k], [L : K] < +\infty$ , on a*

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

Ainsi,  $C = k[a, a']$  est une extension finie de  $k$  et pour chaque  $c \in C$ , la sous-algèbre  $k[c]$  est de dimension finie sur  $k$  : la surjection canonique  $k[T] \twoheadrightarrow k[c]$  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  $C$ .

①. 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  $\text{End}_k(V)$  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  $d$ .

②. Par analogie avec les notations  $\mathbb{R}[T]$  et  $\mathbb{R}(T)$  pour, respectivement, l'anneau de polynômes et le corps des fractions rationnelles.

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

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

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

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

**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 un ou des racines. L'exemple classique, mais peut-être pas parfaitement typique<sup>①</sup>, 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  $\mathbb{C} := \mathbb{R}[T]/(T^2 + 1)$ .

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<sup>②</sup> un isomorphisme

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

①. Pourquoi ?

②. C'est l'analogie 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.

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<sup>①</sup>. 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]<sup>②</sup> 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  $g_1$  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  $\prod_{i=1}^d (T - x_i)$ .

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

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

où

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

est un polynôme unitaire de degré  $d$ . On l'appelle l'**algèbre de décomposition universelle**, formellement définie comme le quotient l'anneau de polynômes  $k[X_1, \dots, X_d]$  par l'idéal engendré par les  $\sigma_r(X_1, \dots, X_r) - a_r$ ,  $1 \leq r \leq d$ , où les  $\sigma_1, \dots, \sigma_d \in k[X_1, \dots, X_d]$ , 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,  $\sigma_1 = X_1 + \dots + X_d$  et  $\sigma_d = X_1 \dots X_d$  ; en général, on a

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

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  $k[X_1, \dots, X_d] \twoheadrightarrow A$ .

①. 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.

②. 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.

**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<sup>①</sup>, il suffit de montrer que pour tout  $k$ -algèbre non nulle  $A$ , il existe un  $k$ -morphisme  $A \rightarrow K$ , 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  $\{f_0, f_1, \dots, f_n, \dots\}$ , on obtiendrait (non canoniquement) une suite d'extensions  $k \subseteq K_0 \subseteq K_1 \subseteq \dots \subseteq K_n \subseteq \dots$  telles que  $f_i$  pour  $i \leq n$  soit scindé dans  $K_n$ . Intuitivement, dans le corps  $K_\infty := \bigcup_n K_n$ , 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'analogie de ces unions croissantes dans un contexte plus général —, d'autant plus que, dans nos applications,  $k$  — donc  $k[T]$ , sera dénombrable.
- (b) Le corps  $K_\infty$  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  $K_2 \simeq K'_2$ . Cela résulte des deux observations suivantes :

- (i) si  $f$  est scindé dans une extension  $\Omega$  de  $k$ , il existe un unique corps de décomposition de  $f$  dans  $\Omega$  : c'est la sous-extension de  $\Omega$  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) :

$$\begin{array}{ccccc} & & L_1 & & \\ & \nearrow & & \searrow & \\ k & & & & M \\ & \searrow & & \nearrow & \\ & & L_2 & & \end{array}$$

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



Nous admettons ce fait, non pas qu'il soit difficile<sup>①</sup>, 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.

□ Si l'idéal, disons  $I$ , est non réduit au singleton  $\{0\}$ , considérer  $f$  unitaire de degré minimal appartenant à  $I$ . Tout élément de  $I$  est alors un multiple de  $f$  car les restes des divisions euclidiennes d'éléments de  $I$  sont à la fois dans  $I$  et de degré  $< \deg(f)$ , donc nuls. □

**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 bijectifs.*

□ Ceci peut se voir de deux façons différentes.

- (i) On constate que si  $a \in A$  est non nul, la multiplication  $A \rightarrow A, x \mapsto xa$  est une application  $k$ -linéaire et injective. Comme  $A$  est de dimension finie, cette application linéaire est également surjective et, en particulier, il existe  $y \in A$  tel que  $ya = 1$ . L'élément  $a$  est donc inversible.
- (ii) L'anneau  $A$  est isomorphe au quotient  $k[T]/(f)$ , où  $f$  est le polynôme minimal de  $a$ . Comme  $A$  est intègre, le polynôme  $f$  est irréductible et le quotient  $k[T]/(f)$  est un corps. (Écrire une inclusion  $(f) \subseteq (g)$  et conclure.)

□

**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.

□ Cela revient à montrer que si  $L/K$  est une extension finie,  $L = K$ . En d'autres termes : si  $x$  est algébrique sur  $K$ , il appartient à  $K$ . Or, un tel  $x$  est algébrique sur  $k$  : son polynôme minimal sur  $K$  a un nombre fini de coefficients donc appartient à une extension  $k'$  de  $k$  engendrée par un nombre fini d'éléments algébriques. L'extension  $k'/k$  est donc de degré fini, de même que  $k'[x]/k'$ . Finalement,  $x$  appartient à l'extension finie  $k'[x]$  de  $k$  : l'élément  $x$  est donc algébrique sur  $k$ . Par hypothèse, il appartient à  $K$  car le polynôme minimal de  $x$  sur  $k$  est scindé dans ce corps, et s'en est une racine. □

<sup>①</sup>. ¶ 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  $B := L_1 \otimes_k L_2$ .

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

□ L'idée est que chacun des deux nombres dont on considère la somme est valeur propre de la matrice compagnon associée à son polynôme minimal, de degré respectivement 2 et 3. Le problème est que les deux espaces vectoriels correspondant sont distincts ; on veut les « mettre ensemble ». On peut le faire par le procédé général expliqué ci-dessous ; *in fine*, on trouve la matrice

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

dont le polynôme caractéristique est  $T^6 - 9T^4 - 4T^3 + 27T^2 - 36T - 23$  ; par construction (*infra*), il s'annule en la valeur attendue.

**Procédé général.** Soient  $a, b$  deux éléments algébriques sur un corps  $k$ , ici  $\mathbb{Q}$ . On souhaite montrer que  $a+b$  et  $ab$  sont entiers et calculer des polynômes annulateurs. Par hypothèse, il existe deux polynômes unitaires  $f = X^n + \sum_{i < n} c_i X^i \in k[X]$  et  $g = Y^m + \sum_{j < m} d_j Y^j \in k[Y]$  tels que  $f(a) = g(b) = 0$ . (Dans l'exemple de l'exercice, il s'agit de  $X^2 - 3$  et  $Y^3 - 2$ .) Soient  $V_a := k[X]/(f(X))$  et  $V_b := k[Y]/(g(Y))$  : tautologiquement, le polynôme minimal de la multiplication par  $x := X \pmod{f}$  agissant sur  $V_a$  (resp. la multiplication par  $y := Y \pmod{g}$  agissant sur  $V_b$ ) est  $f$  (resp.  $g$ ). En particulier,  $a$  et  $b$  sont racines des polynômes caractéristiques des matrices correspondantes, exprimées par exemple dans les bases  $\{1, x, \dots, x^{n-1}\}$  et  $\{1, y, \dots, y^{m-1}\}$ . Un  $k$ -espace vectoriel sur lequel on peut faire agir *simultanément* la multiplication par  $x$  et par  $y$  est

$$W_{a,b} := k[X, Y]/(f(X), g(Y)).$$

(C'est le *produit tensoriel*  $V_a \otimes_k V_b$ , mais il est inutile de le savoir ici.) Une base naturelle de  $W_{a,b}$  est constituée des produits  $x^i y^j$ ,  $0 \leq i < n$ ,  $0 \leq j < m$  ; c'est un  $k$ -espace vectoriel de dimension  $nm$ . Il est immédiat de calculer, dans cette base, la matrice de la multiplication par  $x$  (resp. par  $y$ ) ; en particulier, on peut calculer la matrice, dans cette base, de l'endomorphisme  $\sigma : W_{a,b} \rightarrow W_{a,b}$  de multiplication par  $x+y$ . D'après le théorème de Cayley-Hamilton, l'endomorphisme  $\sigma$  est annulé par son polynôme caractéristique. (Dans le cas de l'exemple ci-dessus, on trouve la matrice  $6 \times 6$  et le polynôme annoncés.) Il reste à se convaincre que si  $P$  est un polynôme unitaire tel que  $P(\sigma) = 0$  (endomorphisme nul de  $W_{a,b}$ ) alors  $P(a+b) = 0$  (dans la  $k$ -algèbre à laquelle appartiennent  $a$  et  $b$ ). Il suffit que  $a+b$  soit valeur propre de  $\sigma$ , ce qui est le cas, comme nous allons le voir. Pour le vérifier, on peut toujours remplacer  $k$  par un corps plus grand (une extension ; ici  $\mathbb{Q}(\sqrt{3}, \sqrt[3]{2})$  convient). On peut donc supposer qu'il existe  $0 \neq v_a = \sum_i c_i x^i \in V_a$  et  $0 \neq v_b =$

$\sum_j d_j y^j \in W_b$  tels que  $xv_a = av_a$  et  $yv_b = bv_b$ . Soit  $w_{a,b} := \sum_{i,j} c_i d_j x^i y^j$ ; il est clair que  $xw_{a,b} = aw_{a,b}$  et  $yw_{a,b} = bw_{a,b}$ . On a donc  $\sigma(w_{a,b}) = (a+b)w_{a,b}$ ; comme  $w_{a,b} \neq 0$ , on a montré que ce que l'on souhaitait.

Le même procédé permet bien sûr de trouver un polynôme annulateur du produit  $ab$  : considérer l'endomorphisme  $\pi$  de multiplication par  $xy$  dans  $W_{a,b}$ .  $\square$

**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.*

$\square$ Euclide : si  $x_1, \dots, x_n$  sont des éléments d'un anneau, tout facteur de  $y := 1 + x_1 \cdots x_n$  est premier avec les  $x_i$ . Ceci nous incite à considérer le polynôme  $f := 1 + \prod_{a \in k} (T - a)$  à coefficients dans le corps fini  $k$ ; il n'a pas de racine dans ce corps.

Cela résulte aussi du fait qu'il existe des polynômes irréductibles sur  $\mathbb{F}_p$  de degré quelconque. Il est instructif d'en vérifier les détails.  $\square$

**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  $\text{SF}(Y)$  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  $\deg(y_1, \dots, y_k) = \sum_i \deg(y_i)$  et  $e(y_1, \dots, y_k) = k$  la longueur de la suite.

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

(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

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

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) Dédurre 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  $v = 0$ .)

□

- (i) Soit  $(v, u) \in E$ . Posons  $u_0 := u$  et  $u_1 = v$  et faisons la division euclidienne étendu de  $u$  par  $v$  pour calculer le PGCD de  $u$  et  $v$ . Cet algorithme nous donne une suite finie de polynômes  $u_n$  et de polynômes  $q_n$  définis par  $u_n = q_{n+1}u_{n+1} + u_{n+2}$ ; il s'arrête, après  $e$  étapes, lorsque  $u_{e+1} = 0$ : la première division est  $u_0 = q_1u_1 + u_2$  et la dernière  $u_{e-1} = q_eu_e + 0$ . La bijection est donnée par  $(v, u) \mapsto ((q_1, \dots, q_e), u'_e := u_e / \text{cd}(u_e))$ . En effet, si on part du PGCD (unitaire)  $u'_e$  et que l'on « remonte » à l'aide des quotients, on retrouve  $(u_1, u_0)$ , quitte à multiplier par un (unique) scalaire non nul pour que  $u_0$  soit unitaire.
- (ii) Il faut se convaincre, sans calcul, que c'est la traduction analytique d'un fait combinatoire élémentaire.
- (iii) La bijection de la première question, compatible avec les degrés et les longueurs/nombres d'étapes, se traduit sous la forme :

$$Z_E(T, \lambda) = Z_{\text{SF}(\mathbb{F}_p[T]_{>0})}(T, \lambda) \cdot Z_{\mathbb{F}_p[T]_1}(T).$$

On trouve donc

$$\left( \frac{1}{1 - \lambda \frac{p(p-1)T}{1-pT}} - 1 \right) \cdot \frac{1}{1 - pT}.$$

- (iv) Par définition de la moyenne et des séries, l'espérance du nombre d'étapes est la valeur en  $\lambda = 1$  du coefficient de  $T^n$  dans  $\frac{\partial}{\partial \lambda} Z_E(T, \lambda)$ , divisé par le nombre de paires avec  $u$  unitaire, soit  $p^{2n}$ . Ce qui précède permet de faire un calcul *exact*, dont l'équivalent est un corollaire immédiat. Plus précisément, l'évaluation en  $\lambda = 1$  de la dérivée par rapport à  $\lambda$  donne

$$p(p-1)T \frac{1}{(1-p^2T)^2} = \sum_n np^{2n-1}(p-1)T^n.$$

La moyenne est donc  $np^{2n-1}(p-1)/p^{2n} = (1-p^{-1})n$ . CQFD.

Voir [FLAJOLET et SEDGEWICK 2009, prop. IX.12, p. 663] pour une présentation de ce résultat comme conséquence de faits plus généraux et [MA et GATHEN 1990] pour des compléments, par une approche plus *ad hoc*. □

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

Mise en garde :

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

**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  $\langle x \rangle \leq G \leq \mu_n(K) := \{\lambda \in K : \lambda^n = 1\}$  ; 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<sup>①</sup>, n'est pas primitif. En effet, on a  $T^5 \equiv T \pmod{g}$ , c'est-à-dire que la classe  $t$  de  $T$  dans  $\mathbb{F}_2[T]/(g)$  est d'ordre 5, et cette classe n'engendre donc pas  $\mathbb{F}_{16}^\times$ .

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

**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  $\Pi$  le polynôme minimal de  $x$  sur  $\mathbb{F}_p$ . C'est l'unique polynôme unitaire tel que le morphisme  $\mathbb{F}_p[T] \rightarrow \mathbb{F}_p[x]$  envoyant  $T$  sur  $x$  se factorise à travers un isomorphisme  $\mathbb{F}_p[T]/(\Pi) \simeq \mathbb{F}_p[x] = \mathbb{F}$ . Nécessairement, le degré  $\deg(\Pi)$  du polynôme est égal au degré  $[\mathbb{F} : \mathbb{F}_p] := \dim_{\mathbb{F}_p} \mathbb{F}$  de l'extension  $\mathbb{F} / \mathbb{F}_p$ . Comme on a vu que pour tout entier  $d \geq 1$ , il existe une extension de  $\mathbb{F}_p$  de degré  $d$ , on en déduit 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  $\text{Frob}_p : x \mapsto x^p$  est un endomorphisme de  $\mathbb{F}$ ; c'est un automorphisme car tout morphisme de corps est injectif. Le sous-groupe  $\langle \text{Frob}_p \rangle$  de  $\text{Aut}(\mathbb{F})$  est d'ordre  $d$  : sa puissance  $d$ -ième  $\text{Frob}_p^d$  est l'identité et  $\text{Frob}_p^a \neq \text{Id}$  si  $a < d$ , sans quoi  $\mathbb{F}$  serait de cardinal  $\leq p^a < p^d$ . D'autre part, si  $x$  est un **élément primitif** [本原元] de  $\mathbb{F}$ , c'est-à-dire tel que  $\mathbb{F} = \mathbb{F}_p[x]$ , alors tout automorphisme  $\varphi \in \text{Aut}(\mathbb{F})$  est caractérisé par l'image  $y = \varphi(x)$  de  $x$ . Comme  $y$  est une racine du polynôme minimal  $\Pi$  de  $x$ , car  $0 = \varphi(\Pi(x)) = \Pi(\varphi(x))$ , on voit que le cardinal de  $\text{Aut}(\mathbb{F})$  est *au plus*  $d$ . Finalement, on a démontré le résultat suivant.

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

<sup>①</sup> C'est la réduction modulo 2 du polynôme  $\Phi_5$  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,  $\Omega$  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  $\Pi$  sur  $\mathbb{F}_p$ . Notons  $d_x := [\mathbb{F}_p(x) : \mathbb{F}_p] = \deg(\Pi)$  le degré de  $x$  sur  $\mathbb{F}_p$ . Puisque  $x \in \mathbb{F}_{p^d}$  si et seulement si  $\text{Frob}_p^d(x) = x$ , on en déduit que  $d_x$  est aussi égal au cardinal de l'« orbite » (finie)  $\{\text{Frob}_p^n(x) : n \geq 0\}$ . Puisque, pour chaque  $d \geq 1$ , on a l'égalité  $\mathbb{F}_q^\times = \mu_{q-1}(\Omega) := \{\lambda \in \Omega : \lambda^{q-1} = 1\}$ , l'élément  $x$  est en particulier une racine  $(p^{d_x} - 1)$ -ième de l'unité. L'ordre  $N = \#\langle x \rangle$  de  $x$ , vu comme élément du groupe multiplicatif de  $\Omega$ , est donc un diviseur de  $p^{d_x} - 1$ ; en particulier, il est premier à  $p$  et la condition  $\text{Frob}_p^d(x) = x$  devient équivalente à  $p^{d_x} \equiv 1 \pmod{N}$ . Terminons par le lien entre l'orbite de  $x$  sous l'action de l'automorphisme de Frobenius et le polynôme minimal  $\Pi$ . Le polynôme

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

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

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

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

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

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

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  $\prod_{i < d} (T - \text{Frob}_\infty^i(z))$ , où  $\text{Frob}_\infty$  est la conjugaison complexe  $z \mapsto \bar{z}$  et  $d > 0$  est minimal pour la propriété que  $\text{Frob}_\infty^d(z) = z$ . Bien entendu,  $d = 1$  ou  $2$ , selon que  $z$  soit réel ou non — de sorte que le polynôme minimal est  $T - z$  ou  $(T - z)(T - \bar{z}) = T^2 - 2\Re(z)T + |z|^2$ . 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  $\text{CF}_{p,N}$  le graphe orienté dont les sommets sont les entiers  $1 \leq a \leq N$  et les arêtes sont définies par :  $a \rightarrow b$  s'il existe un plongement  $\mathbb{F}_{p^a} \hookrightarrow \mathbb{F}_{p^b}$ .

- (i) Représenter  $CF_{p,N}$  pour de petites valeurs de  $p, N$ .
- (ii) Comprendre que  $CF_{p,N}$  ne dépend pas de  $p$  en l'identifiant à un graphe simple.

□ Tout revient à comprendre que  $\mathbb{F}_{q_1}$  s'injecte dans  $\mathbb{F}_{q_2}$  si et seulement si  $q_2$  est une puissance de  $q_1$ . Nous avons déjà vu, plusieurs fois, que c'est une condition nécessaire :  $\mathbb{F}_{q_2}$  est, notamment, un  $\mathbb{F}_{q_1}$ -espace vectoriel (de dimension finie) donc ensemblistement en bijection avec une puissance cartésienne de  $\mathbb{F}_{q_1}$ . Réciproquement, nous avons aussi vu que  $\mathbb{F}_{q^r}$  contient un sous-corps de cardinal  $q$  : le sous-ensemble des racines de  $T^q - T$ , polynôme qui divise  $T^{q^r} - T$ .

Ainsi, le graphe  $CF_{p,N}$  est simplement le graphe sur  $\{1, \dots, N\} \subseteq \mathbb{N}$ , avec une arête  $a \rightarrow b$  si et seulement si  $a|b$ . □

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

□

- (i) Le polynôme caractéristique de  $A$  est  $T^2 - T - 1$ , dont les racines sont le nombre d'or  $\varphi = (1 + \sqrt{5})/2$  et son inverse. Elle est donc diagonalisable et  $A^n$  est semblable à  $\text{diag}(\varphi^n, \varphi^{-n})$  qui n'est l'identité que si  $n = 0$ . On peut également remarquer, en calculant  $A^n$  que ses coefficients sont des entiers positifs croissants. D'ailleurs, si l'on définit la suite de Fibonacci par  $F_0 = 0, F_1 = 1$  et  $F_{n+2} = F_{n+1} + F_n$  pour  $n \geq 0$ , on voit immédiatement que  $A^n(0, 1) = (F_n, F_{n+1})$  et on retrouve ainsi la formule  $F_n = \frac{1}{\sqrt{5}}(\varphi^n - \varphi^{-n})$  utilisée en 1.8.5.
- (ii) La matrice  $B$  est de déterminant  $1 \in \mathbb{F}_2$  ; elle appartient donc au groupe  $\text{GL}_2(\mathbb{F}_2)$  des matrices  $2 \times 2$  inversibles. Ce groupe est fini de cardinal  $6 = (p^2 - 1)(p^2 - p)$ , où  $p = 2$ . On a donc nécessairement  $B^6 = \text{Id}$ . Compte tenu de l'interprétation précédente, cela montre que la suite  $(F_n \pmod{2})$  est périodique de période un diviseur de 6. En effet, on constate que cette suite à valeurs dans  $\mathbb{F}_2$  est  $0, 1, 1, 0, 1, 1, 0, 1, 1, \dots$

□

**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  $P = T^r - c_1 T^{r-1} - c_2 T^{r-2} \dots - c_{r-1} T - c_r \in \mathbb{F}_q[T]$  un polynôme irréductible primitif : si  $x$  est une racine de  $P$  dans  $\mathbb{F}_{q'}$ , on a  $\langle x \rangle = \mathbb{F}_{q'}$ .

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



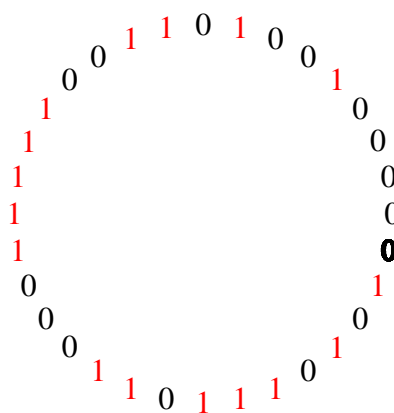
- (ii) Soit  $u$  la suite  $q'$ -périodique à valeurs dans  $\mathbb{F}_q$  définie par façon suivante :  $u_0 = u_1 = \dots = u_{r-1} = 0$ ,  $u_r = c_r$  et, pour  $r < n < q'$ , définie par récurrence

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

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

*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  $n \geq 1$ , il existe une suite de de Bruijn  $a^n$ -périodique à valeurs dans  $\mathfrak{A}$ .

□

- (i) Il en existe  $\varphi(q' - 1)/r$ . Pour des exemples de tels polynômes et leur importance dans le contexte de l'exercice, voir par exemple [TAOCP 4A, 7.2.1.1].
- (ii) Il suffit de montrer que pour tout vecteur  $v \in \mathbb{F}_q^r - \{0\}$ , l'ensemble  $\{M^i v\}$ ,  $0 \leq i < q' - 1$  est de cardinal  $q' - 1 = \text{card}(\mathbb{F}_q^r - \{0\})$  : tous les vecteurs non nuls à  $r$  coordonnées sont obtenus. En d'autres termes, on veut que  $M^i v \neq M^j v$  si  $0 \leq i \neq j < q' - 1$ , ou encore :  $\text{Ker}(M^i - \text{Id}) = \{0\}$  pour  $0 < i < q' - 1$ . Or, la matrice  $M$  est diagonalisable sur  $\mathbb{F}_q$ , ses valeurs propres sont toutes des racines primitives  $(q' - 1)$ -ièmes de l'unité. (Pour une discussion générale des suites récurrentes dans le cas des corps finis, voir par exemple [LIDL et NIEDERREITER 1997, chap. 8].)
- (iii) C'est un simple calcul. Pour une application ludique — un tour de magie —, voir par exemple le paragraphe 7.4.2 des notes de cours de 2017-2018 et les références citées.
- (iv) Si  $a = q_1 q_2 \dots q_t$ , où les  $q_i$  sont des puissances de nombres premiers distincts, et  $\mathfrak{A} = \mathbb{Z}/a\mathbb{Z}$  (ce que l'on peut supposer), le théorème chinois nous

ramène au problème de construire  $t$  suites  $q_i^n$ -périodiques de de Bruijn à valeurs dans les  $\mathbb{Z}/q_i\mathbb{Z}$ , qui sont en bijection (ensembliste) avec les  $\mathbb{F}_{q_i}$ .

□

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

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

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

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

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

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

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

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

**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].

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

#### 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  $n \rightarrow +\infty$ . (Indication : on pourra choisir les  $p_n$  tels que  $p_n - 1$  soit divisible par de plus en plus de nombres premiers et utiliser le fait que  $\prod_{\ell} (1 - \ell^{-1}) = 0$ , où  $\ell$  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  $\mathbb{F}_{3^5}^\times$ .

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

Remarques :

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

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

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

□

**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.

□

- (i) Si  $\delta | d$  et  $t$  est la classe de  $T$  dans  $\mathbb{F}$ , l'unique sous-corps de  $\mathbb{F}$  de degré  $\delta$  sur  $\mathbb{F}_p$  (c'est-à-dire de cardinal  $p^\delta$ ) est  $\mathbb{F}_p[s]$ , où  $s := t^{(p^d-1)/(p^\delta-1)}$ .  
(ii) On peut toujours procéder par force brute : ne serait-ce parce que les ensembles sont finis et les tables d'addition et de multiplication sont connues. On peut bien entendu faire un peu mieux mais le problème de faire *vraiment* plus rapide est délicat. Par exemple, comme énoncé en [MULLEN et PANARIO 2013, §11.1.1.3], aucune méthode efficace n'est connue si l'on ne connaît pas à l'avance une factorisation de  $p^d - 1$ .

□

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

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

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

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

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

□

**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  $n$ .

□ Il s'agit essentiellement de l'argument donné en 4.3.5 pour minorer la proportion de polynômes irréductibles. Le nombre d'éléments de  $\mathbb{F}_{q^n}$  de degré  $< n$  est majoré par la somme des cardinaux des  $\mathbb{F}_{q^d}$  pour  $d | n$ . Au moins deux arguments

possibles. (1) On remarque que  $\sum_{d|n, d \neq n} q^d \leq \sum_{d < n} q^d < q^n$ , par exemple par unicité de l'écriture en base  $q$ . (2) On remarque que chaque  $q^d$  est majoré par  $\leq q^{n/2}$  et leur nombre est  $\leq n$ , par conséquent cette somme de cardinaux est inférieure ou égale à  $nq^{n/2}$ . Pour avoir la conclusion souhaitée, il suffit d'avoir  $q^n > nq^{n/2}$ , soit  $q^{n/2} > n$ , ce qui se produit dès que  $2^n > n^2$ , donc dès que  $n > 4$ . Pour les valeurs plus petites de  $n$ , on constate que  $q^4 > q^2 + q$  et  $q^3 > q$  et  $q^2 > q$  (et  $q > 0 \dots$ ) pour tout  $q \geq 2$ .  $\square$

#### 4.3.13.

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

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

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

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

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

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

(ii) Puisque qu'aucun de ces polynômes n'est à coefficients rationnels et que  $\Phi_8$  n'a visiblement pas de racine dans  $\mathbb{Q}$  (ni dans  $\mathbb{R}$ ), il est bien irréductible.

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

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.  $\P$  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  $r, s \geq 0$ .

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

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

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

(ii) Le polynôme  $T^2 + T + 1 \in \mathbb{F}_2[T]$  est irréductible, par exemple parce qu'il n'a pas de racine dans  $\mathbb{F}_2$  ou, de façon un peu pédante, d'après l'exercice 4.3.3 ci-dessus. Le quotient  $\mathbb{F}_2[T]/(T^2 + T + 1)$  est donc un corps de cardinal 4 et la classe  $j$  de  $T$  est bien comme annoncé. D'après le critère précédent, pour vérifier que les polynômes de degré 5 de l'énoncé sont irréductibles, il faut vérifier qu'ils n'ont pas de racine dans  $\mathbb{F}_2$  — ce qui résulte du fait que leur terme constant est non nul et qu'ils ont un nombre impair de monôme — ni dans  $\mathbb{F}_4$ . (On utilise le fait que  $\lfloor 5/2 \rfloor = 2$ .) On vérifie par le calcul que pour chacun de ces polynômes  $f$ , on a  $f(j) \neq 0$ . Comme  $f(j^2) = f(j)^2$ , on a aussi  $f(j^2) \neq 0$  sans avoir besoin de refaire le calcul. L'exercice demande de vérifier que ces polynômes sont les seuls qui soient irréductibles de degré 5. Il résulte de la formule de Gauß (§ 2.5.10) qu'il y en a  $\frac{1}{5}(2^5 - 5) = 6$ . On les a donc tous trouvés. Plus simplement, on peut faire une liste des autres polynômes et vérifier qu'ils ont une racine dans  $\mathbb{F}_2$  ou  $\mathbb{F}_4$ . (Ici  $\mathbb{F}_2 \subseteq \mathbb{F}_4$  donc il s'agit en fait de chercher des racines dans  $\mathbb{F}_4$  mais on rappelle qu'en général l'inégalité  $a \leq b$  n'entraîne pas l'existence d'un plongement  $\mathbb{F}_{p^a} \subseteq \mathbb{F}_{p^b}$ .) □

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

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

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

□

**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  $d \leq 7$ .

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

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

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

**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  $2^d$ .

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

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

**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  $q \rightarrow 1$  (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  $q - \frac{q-1}{d}$ .

□ (Esquisse)

(i) Le fait que  $c_i(t)$  soit de degré au plus  $di$  est évident. La fonction  $c_i$  est constante sur  $\mathbb{F}^\times$  ; si son degré est  $< q - 1$ , le polynôme  $c_i$  est constant, égal à  $c_i(0)$ . Si  $i \neq 0$ , on a  $c_i(0) = 0$  (car  $P(0) = 0$ ).

- (ii) L'égalité entre l'image de  $P$  et l'ensemble des zéros de  $Q$  ou  $R := Q - (X^q - X)$  est évidente. D'après ce qui précède, le polynôme  $R$  est de degré  $\leq q - \frac{q-1}{d}$ . S'il est nul,  $P(\mathbb{F}) = \mathbb{F}$ , sinon l'ensemble de ses zéros est de cardinal majoré par son degré.

□

## 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  $T^{q^d} - T$  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  $d/\ell$  avec  $\ell$  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'analogie entre la condition  $r \leq d/2$  et le fait que si un entier  $n$  n'a pas de facteur premier  $p \leq n^{1/2}$ , 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<sup>①</sup> 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.

<sup>①</sup>. On peut par exemple montrer qu'il s'effectue en au pire  $O(d^{2+\epsilon})$  opérations pour tout  $\epsilon > 0$ , où la constante impliquée par le  $O$  dépend de  $\epsilon$  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*  $\text{Frob}_q : A \rightarrow A, a \mapsto a^q$ , qui est la puissance  $\log_p(q)$ -ième du Frobenius  $\text{Frob}_p$ . L'ensemble  $\text{Fix}(\text{Frob}_q \subset A) := \{a \in A : a^q = a\}$  est donc une *sous- $\mathbb{F}_q$ -algèbre* de  $A$ , de dimension  $\geq 1$  (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  $f$ ,

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

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

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

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

**Proposition.** Soit  $f \in \mathbb{F}_q[T]$  unitaire séparable. Alors, la dimension  $r$  sur  $\mathbb{F}_q$  de l'algèbre de Berlekamp  $B(f)$  de  $f$  est égale au nombre de facteurs unitaires irréductibles de  $f$ . De plus, pour tout  $y \in B(f)$ , on a  $f = \prod_{c \in \mathbb{F}_q} \text{PGCD}(f, Y - c)$ , 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  $\text{PGCD}(f, Y)$  est le produit des  $f_i$  tels que  $Y$  soit multiple de  $f_i$  c'est-à-dire que la  $i$ -ième composante de  $\#(y)$  s'annule.)

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

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  $\text{Frob}_2 - \text{Id}$  sur la base  $1, t, t^2, \dots, t^4$  de  $\mathbb{F}_2[T]/(f)$ , en calculant successivement  $T^2, T^4, \dots, T^8$  modulo  $f$  :

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

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

## 5.2. Polynômes cyclotomiques.

**5.2.1.** Soient  $\ell$  un nombre premier et  $\Phi_\ell(T) := T^{\ell-1} + \dots + T + 1 \in \mathbb{Z}[T]$  le  $\ell$ -ième polynôme cyclotomique, dont les racines complexes sont les racines  $\ell$ -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  $\ell$ -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  $p \equiv 1 \pmod{\ell}$ .

**5.2.2.** Supposons maintenant  $\ell \neq 2$  et que  $p$  soit un carré modulo  $\ell$ . 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  $\ell$ -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  $\ell$  (resp. son complémentaire). C'est bien un polynôme à coefficients dans  $\mathbb{F}_p$  car l'ensemble des  $\zeta^i$ , pour  $i$  carré modulo  $\ell$ , 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  $\ell$ , 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  $\ell$ . 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  $\ell$  et  $(\ell + 1)/2$  sur  $\mathbb{F}_p$ . Notons que dans la base « canonique »  $\{1, t, \dots, t^{\ell-1}\}$  de  $V_{p,\ell}$ , le sous-espace  $C_{p,\ell}$  a la propriété d'être stable par permutation cyclique des coordonnées : si  $c = (c_0, \dots, c_{\ell-1})$  appartient à  $C_{p,\ell}$  — correspondant à un polynôme  $h(T) \pmod{f}$  —, il en est de même de  $(c_{\ell-1}, c_0, \dots, c_{\ell-2})$ , 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** <sup>①</sup>, 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**  $\ell$  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  $d \leq \ell - (\ell + 1)/2 + 1 = (\ell + 1)/2$ . Lorsque  $p = 2$ , on dispose également de la *minoration* suivante.

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

<sup>①</sup>. 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*<sup>①</sup>

*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  $P := C \cdot C_n \in \mathbb{F}_2[T]$  de ces deux polynômes ; son poids est majoré par  $d^2$ , le nombre maximal de monômes pouvant apparaître en développant le produit. Soit  $\bar{P}$  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  $\bar{P} = \Phi_\ell(t)$ , ce dernier étant de poids exactement  $\ell$ . 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  $i \geq 0$  et, finalement,  $\bar{P} = \Phi_\ell(t)a(1_{\mathbb{F}_2})$ . 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  $\neq 0$ .  $\square$

**Remarque.** La même démonstration permet de montrer, lorsque  $\ell \equiv -1 \pmod{4}$  que  $d^2 - d + 1 \geq \ell$  : 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<sup>②</sup>. 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 23 est bien un carré : on a  $5^2 \equiv 23 \pmod{23}$  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<sup>③</sup> » 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 »  $G_{24} := \bar{G}_{23}$  — 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)  $M : \mathbb{F}_2^m \rightarrow \mathbb{F}_2^n$  une matrice injective d'image un code (linéaire) pour lequel elle sait efficacement faire un décodage avec au plus  $t$  erreurs ;
- (iii)  $S \in \text{GL}_m(\mathbb{F}_2)$  une matrice inversible choisie aléatoirement ;
- (iv)  $\sigma \in \mathfrak{S}_n$  une permutation aléatoire, de matrice associée  $P_\sigma \in \text{GL}_n(\mathbb{F}_2)$  ;

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  $B(f) = \text{Ker}(\text{Frob}_q - \text{Id})$  de  $f$ , puis, si  $s > 1$  de sorte qu'il y a une factorisation non triviale à effectuer, on tire au hasard un élément  $y = c_1\tau_1 + \dots + c_s\tau_s \in B(f)$  (avec  $c_i \in \mathbb{F}_q$ ) et on calcule les PGCD( $f, y - c$ ) pour les différents  $c \in \mathbb{F}_q$  : ceci fournira une factorisation non triviale de  $y$  dès que les composantes de  $\#(y)$  ne sont pas toutes égales (où  $\#$  est l'isomorphisme  $B(f) \simeq (\mathbb{F}_q)^s$  déduit de l'isomorphisme chinois), ce qui se produit pour  $q^s - q$  des  $q^s$  éléments  $y$  de  $B(f)$ .

Lorsque  $q$  est grand, la proposition ne peut pas servir en tant que telle. On peut cependant la combiner avec les mêmes idées que celles utilisées dans l'algorithme dit de Cantor-Zassenhaus, que nous ne détaillons pas : une fois tiré  $y$  dans  $B(f)$ , on calcule  $z := y^{(q-1)/2}$  (resp.  $z := y + y^2 + y^4 + \dots + y^{q/2}$  en caractéristique 2), et alors PGCD( $f, z - 1$ ) (resp. 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  $\zeta$ , 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  $\text{Aut}(C)$  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,  $\text{Aut}(C)$  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  $\text{Aut}(\overline{C}_{2,\ell})$  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<sup>①</sup>.

---

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

□

- (i)  $p = 5$ . La question revient à déterminer le plus petit  $p$  tel que le polynôme cyclotomique  $\Phi_{23} = (T^{23} - 1)/(T - 1)$  soit irréductible sur  $\mathbb{F}_p$ . D'après 5.2, on veut donc que  $p$  soit un générateur de  $(\mathbb{Z}/23\mathbb{Z})^\times$ . Pour  $p = 2$ , les puissances sont 1, 2, 8, 16, 32, 64, 128, 256 = 3, 6, 12, 24 = 1 ; pour  $p = 3$ , on a 1, 3, 27 = 4, 12, 36 = 13, 39 = 16, 48 = 2, 6, 18 = -5, -15 = 8, 24 = 1. Dans ces deux cas, l'ordre n'est pas 22. Par contre, c'est le cas si  $p = 5$ .
- (ii)  $p = 2, 3, 5, 11, 13, 19, 29, 37, 53, 59, \dots$  On se demande maintenant pour quels  $p$  le polynôme  $\Phi_p$  est irréductible sur  $\mathbb{F}_2$ , c'est-à-dire quand 2 est primitif dans  $(\mathbb{Z}/p\mathbb{Z})^\times$ . On vérifie à la main que  $p = 3, 5$  conviennent mais pas 7 (car  $2^3 = 1$ ), ni 17 (car  $2^4 = -1$ ). On trouve par des calculs semblables les valeurs ci-dessus.

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

□

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

□

- (i) Ben-Or : si un polynôme de degré  $d$  n'est pas irréductible, il a au moins un facteur irréductible de degré  $\leq d/2$  donc une racine dans un corps  $\mathbb{F}_{q^r}$  pour un  $r \leq \lfloor d/2 \rfloor$ . Cette dernière condition implique qu'il n'est pas premier avec  $T^{q^r} - T$  dont  $\mathbb{F}_{q^r}$  est un corps de décomposition.
- (ii) Il faut d'abord vérifier que  $f$  est séparable, c'est-à-dire premier avec sa dérivée  $f' = T^5 - T^3 + 2T^2 - 2T - 1$ , ce qui se fait au moyen de l'algorithme d'Euclide :

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

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

□

**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.

□

- (i) Résulte du fait que le PGCD de  $\varphi(p^2) = p(p-1)$  et  $p^2 - 1 = (p+1)(p-1)$  est  $p-1$ . (Ou, plus simplement peut-être,  $p^2 - 1 - \varphi(p^2) = p-1$  donc  $b^{p^2-1} \equiv 1$  entraîne  $b^{p-1} \equiv 1$ .)
- (ii) En utilisant  $x^2 - 1 = (x-1)(x+1)$ , on voit que  $2^{2^n-2} - 1$  est divisible par  $2^{2^{n-1}-1} - 1$ . Comme l'exposant  $2^{n-1} - 1$  est un multiple de  $n$ , l'entier  $x^n - 1$  divise  $x^{2^{n-1}-1} - 1$  pour tout  $x$ . En particulier pour  $x = 2$ . Noter que  $2^n - 1$  est bien composé (=non premier) car  $n$  l'est.

□

**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*. 3<sup>e</sup> éd. Addison-Wesley, xiv+762 pages.
- TAOCP 4A Donald E. KNUTH (2011). *The art of computer programming. Vol. 4A. Combinatorial algorithms, part 1*. Addison-Wesley, xvi+883 pages.

## AUTRES RÉFÉRENCES

- ARORA, Sanjeev et Boaz BARAK (2009). *Computational complexity. A modern approach*. Cambridge University Press, xxiv+579 pages (↑ p. 13).
- 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. 52).
- BONEH, Dan et Victor SHOUP (2017). « **A Graduate Course in Applied Cryptography** ». Tapuscrit (version 0.4) (↑ p. 13).
- 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).
- CONWAY, John Horton (2001). *On numbers and games*. 2<sup>e</sup> éd. A K Peters, xii+242 pages (↑ p. 23).
- COX, David A. (2004). *Galois theory*. John Wiley & Sons, xx+559 pages (↑ p. 24).
- DEMAZURE, Michel (2008). *Cours d'algèbre*. 2<sup>e</sup> éd. Cassini (↑ p. 5, 10, 11, 17, 49, 52).
- FINCH, Steven R. (2003). *Mathematical constants*. Encyclopedia of Mathematics and its Applications **94**. Cambridge University Press, xx+602 pages (↑ p. 11).
- FLAJOLET, Philippe et Robert SEDGEWICK (2009). *Analytic combinatorics*. Cambridge University Press, xiv+810 pages (↑ p. 11, 34).
- 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. 25).
- GATHEN, Joachim von zur (2015). *CryptoSchool*. Springer-Verlag, 888 pages (↑ p. 5, 9, 13, 14, 19).
- GATHEN, Joachim von zur et Jürgen GERHARD (2003). *Modern computer algebra*. 2<sup>e</sup> éd. Cambridge University Press, xiv+785 pages (↑ p. 12, 14, 51).
- HARDY, Godfrey Harold et Edward Maitland WRIGHT (2007). *Introduction à la théorie des nombres*. Traduction française de [Hardy-Wright] par François Sauvageot. Vuibert & Springer, xxxviii+569 pages (↑ p. 6, 7, 20, 24).
- HOFFSTEIN, Jeffrey, Jill PIPHER et Joseph H. SILVERMAN (2014). *An introduction to mathematical cryptography*. 2<sup>e</sup> éd. Undergraduate Texts in Mathematics. Springer, xviii+538 pages (↑ p. 7, 9, 14, 19).
- HUFFMAN, W. Cary et Vera PLESS (2003). *Fundamentals of error-correcting codes*. Cambridge University Press, xviii+646 pages (↑ p. 49).
- IRELAND, Kenneth et Michael ROSEN (1990). *A classical introduction to modern number theory*. Graduate Texts in Mathematics **84**. Springer-Verlag, xiv+389 pages (↑ p. 20).
- LENSTRA JR., H. W. (1978). « Nim multiplication ». *Séminaire de théorie des nombres, Talence 1977-1978*, exp. n° 11 (↑ p. 23).

- LIDL, Rudolf et Harald NIEDERREITER (1997). *Finite fields*. 2<sup>e</sup> éd. Encyclopedia of Mathematics and its Applications **20**. Cambridge University Press, xiv+755 pages (↑ p. 39).
- MA, Keju et Joachim von zur GATHEN (1990). « Analysis of Euclidean algorithms for polynomials over finite fields ». *J. Symbolic Comput.* **9**(4), 429-455 (↑ p. 34).
- MACWILLIAMS, F. J. et N. J. A. SLOANE (1977). *The theory of error-correcting codes*. North-Holland, 762 pages (↑ p. 49, 52).
- MADORE, David A. (15 juil. 2015a). « Le jeu de cartes Dobble et la géométrie projective expliquée aux enfants ». Blog (↑ p. 17).
- (27 juil. 2015b). « Comment faire un jeu de Tribble ». Blog (↑ p. 17).
- MULLEN, Gary L. et Daniel PANARIO, éd. (2013). *Handbook of finite fields*. Discrete Mathematics and its Applications. CRC Press, xxxvi+1033 pages (↑ p. 5, 12, 16, 17, 42).
- 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-RIOU, Bernadette (2000). *Algèbre, arithmétique et Maple*. Cassini (↑ p. 10).
- 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).
- SCHOOF, René (1985). « Elliptic curves over finite fields and the computation of square roots mod  $p$  ». *Math. Comp.* **44**(170), 483-494 (↑ p. 12).
- SCHROEDER, Manfred (2006). *Number theory in science and communication*. 4<sup>e</sup> 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, 13, 20, 24).
- SERRE, Jean-Pierre (1977). *Cours d'arithmétique*. 2<sup>e</sup> éd. Presses universitaires de France, 188 pages (↑ p. 9).
- (1979). « Groupes finis ». Notes d'un cours à l'ÉNSJF ; [arXiv :0503154v6](https://arxiv.org/abs/0503154v6) (↑ p. 6).
- SHANNON, Claude E. (1948). « The Mathematical Theory of Communication ». *Bell System Technical Journal* (↑ p. 49).
- SHOUP, Victor (2009). *A computational introduction to number theory and algebra*. 2<sup>e</sup> éd. (Sous licence CC BY-NC-ND). Cambridge University Press, xviii+580 pages (↑ p. 51).
- SIEGEL, Aaron N. (2013). *Combinatorial game theory*. Graduate Studies in Mathematics **146**. American Mathematical Society, xiv+523 pages (↑ p. 23).
- STINSON, Douglas R. (2006). *Cryptography. Theory and practice*. 3<sup>e</sup> éd. Discrete Mathematics and its Applications. Chapman & Hall/CRC, xviii+593 pages (↑ p. 19).
- 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. 49, 50).

# QCM

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

## Examen 2015-2016

### Exercice 1.

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

### Exercice 2.

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

### Exercice 3.

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

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

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

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

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

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

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

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

### Exercice 6.

- (a) Trouver les entiers relatifs  $a, b \in \mathbb{Z}$  de valeurs absolues minimales tels que  $a \equiv 2 \pmod{3}$ ,  $a \equiv 4 \pmod{5}$  et  $b \equiv 2 \pmod{3}$ ,  $b \equiv 2 \pmod{5}$ .  
 (b) Soit  $f := T^5 + T^4 + T^2 + T + 2 \in \mathbb{Z}[T]$ . On admet que  $f_3 := f \pmod{3} \in \mathbb{F}_3[T]$  et  $f_5 := f \pmod{5} \in \mathbb{F}_5[T]$  ont les factorisations en produits de polynômes irréductibles suivantes :

$$f_3 = (T + 2)^2(T^3 + 2T + 2) \quad \text{et} \quad f_5 = (T^2 + T + 1)(T^3 + 4T + 2).$$

En déduire un  $g \in \mathbb{Z}[T]$  unitaire de degré 3 qui pourrait diviser  $f$ .

- (c) Effectuer la division euclidienne de  $f$  par  $g$  et factoriser  $f$  sur  $\mathbb{Z}$ .  
 (d) Vérifier que  $\omega := \exp(2\pi i/3) \in \mathbb{C}$  est une racine de  $f$ .

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

### Examen 2016-2017

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

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

□

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

□

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

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

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

**Exercice 3.** Soient  $k$  un corps,  $A$  une  $k$ -algèbre et  $x, y \in A$  entiers sur  $k$  : on suppose qu'il existe  $a, b, c, d \in k$  tels que  $x^2 - ax - b = 0 = y^2 - cy - d$ . Trouver une matrice  $4 \times 4$  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.)

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

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

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

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

- (i) Montrer, en utilisant la loi de réciprocité quadratique (§7.7 [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.)

□

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

□

**Exercice 5.**

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

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

□

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

□

**Exercice 6.** Soit  $p$  un nombre premier.

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

□

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

□

**Examen 2017-2018**<sup>①</sup>

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

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

□

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

□

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

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

□

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

□

**Exercice 3.**

- (i) Soit  $k$  un corps fini de caractéristique 2. Tout élément de  $k$  est-il un carré, c'est-à-dire de la forme  $x^2$ , pour un  $x \in k$  ? (Démontrer ce résultat ou donner un contre-exemple.)
- (ii) Soit  $k$  un corps fini de caractéristique  $\neq 2$ . Tout élément de  $k$  qui n'est pas un carré est-il nécessairement primitif, c'est-à-dire générateur du groupe multiplicatif  $k^\times$  ? (Démontrer ce résultat ou donner un contre-exemple.)
- (iii) Soit  $p = 65537 = 2^{24} + 1$ . Montrer que 5 est primitif, c'est-à-dire que  $\langle 5 \rangle = \mathbb{F}_p^\times$ .  
Indication : on pourra admettre que 5 est un carré modulo  $p$  si et seulement si  $p$  est un carré modulo 5.

□

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

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

□

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

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

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

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

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

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

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

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



### Examen 2018-2019<sup>①</sup>

**Exercice 1.** 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  $196560 = 2^4 \cdot 3^3 \cdot 5 \cdot 7 \cdot 13$ .)

□ On commence par observer que  $\mu_a \cap \mu_b = \mu_c$ , où  $c = \text{PGCD}(a, b)$ . Ici,  $c = \text{PGCD}(196560, 55)$ , que l'on pourrait calculer par division euclidienne ou bien en utilisant la factorisation indiquée, qui montre que le PGCD est 5. On a donc  $\mu_{196560}(\mathbb{C}) \cap \mu_{55}(\mathbb{C}) = \mu_5(\mathbb{C})$ , qui est de cardinal 5. □

**Exercice 2.** 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  $\{a \in A : a^{11} = 1\}$ .

□

- (i) Le cardinal est  $p^{\deg(f)}$ , avec  $p = 3$  et  $\deg(f) = 5$ , soit  $243 = 2 \times 11^2 + 1$ .
- (ii) Le polynôme  $f$  se factorise en  $(T^2 + 1)(T^3 - T - 1)$ ; l'anneau  $A$  n'est donc pas un corps.
- (iii) Les deux facteurs  $T^2 + 1$  et  $T^3 - T - 1$  étant irréductibles, l'anneau  $A$  est isomorphe à  $\mathbb{F}_9 \times \mathbb{F}_{27}$  : cela résulte du théorème chinois. En conséquence, le cardinal de l'ensemble demandé est :

$$\text{card}\{x \in \mathbb{F}_9 : x^{11} = 1\} \times \text{card}\{y \in \mathbb{F}_{27} : y^{11} = 1\}.$$

Les groupes  $\mathbb{F}_9^\times$  et  $\mathbb{F}_{27}^\times$  sont cycliques d'ordres respectivement  $9 - 1 = 8 = 2^3$  et  $27 - 1 = 2 \times 13$ . Ces ordres étant premiers avec l'exposant 11, les ensembles  $\{x \in \mathbb{F}_9 : x^{11} = 1\}$  et  $\{y \in \mathbb{F}_{27} : y^{11} = 1\}$  sont réduits au singleton  $\{1\} \subseteq \mathbb{F}_3$ . La réponse est donc que le cardinal demandé est 1. (Si  $A$  avait été un corps de cardinal 243, il y aurait eu des racines 11-ièmes non triviales de l'unité.)

□

**Exercice 3.** 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.

□ Tout d'abord, il est clair que  $\text{card}(A) = 9$ , le cardinal des couples  $(a, b) \in \mathbb{F}_3^2$ . C'est d'ailleurs le sous- $\mathbb{F}_3$  espace vectoriel engendré par

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \text{Id} =: \mathbf{1},$$

et

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} =: u.$$

En conséquence,  $A$  est un sous-groupe (additif) de  $M_2(\mathbb{F}_3)$ . La matrice  $u$  satisfait l'équation  $u^2 = -1$ , de sorte que  $A$  est stable par produit. Enfin, parmi les matrices de  $A$ , la seule non inversible est la matrice nulle : si le déterminant  $a^2 + b^2$  s'annule, alors  $(a, b) = (0, 0)$ . (En effet,  $a^2, b^2 \in \{0, 1\}$ ; leur somme

<sup>①</sup>. exceptés deux exercices sur les codes correcteurs d'erreurs.

n'est nulle que s'ils sont simultanément nuls.) On a donc montré que  $A$  est un corps, de cardinal 9. (Explicitement,  $A = \mathbb{F}_3[u] \subseteq M_2(\mathbb{F}_3)$ , avec  $u^2 = -1$ , de sorte que  $A$  est naturellement isomorphe à  $\mathbb{F}_3(\sqrt{-1})$ .)  $\square$

**Exercice 4.** 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  $n \geq 0$ . Quel est le nombre d'entiers  $0 \leq n \leq 999$  tels que 5 divise  $F_n$  ?

$\square$  La suite  $(F_n \pmod{5})$  est une suite périodique à valeurs dans  $\mathbb{F}_5$  ; sa période divise  $\#GL_2(\mathbb{F}_5) = (5^2 - 1)(5^2 - 5) = 24 \times 20$ . (Même argument que celui vu en classe pour  $(F_n \pmod{2})$ .) Un calcul immédiat montre que les premières valeurs de la suite modulo 5 sont :

0, 1, 1, 2, 3, 0, 3, 3, 1, 4, 0, 4, 4, 3, 2, 0, 2, 2, 4, 1, 0, 1, 1, 2, 3, ...

La période est donc exactement 20. Parmi les 20 premières valeurs, 4 sont égales à 0 (mod 5), soit un cinquième des valeurs. Comme 1000 est un multiple de 20, on en déduit que la réponse est  $1000 \times \frac{1}{5} = 200$ .

$\square$