Arithmétique et compléments d'algèbre linéaire

Pierre de la Harpe

Section de Mathématiques
Université de Genève, C.P. 240
CH-1211 Genève 24, Suisse
Mel : Pierre.delaHarpe@math.unige.ch

Plan du cours (semestre d'hiver)

VII. Arithmétique des nombres entiers.

VIII. Polynômes.

IX. L'homomorphisme $\mathcal{SU}(2) \longrightarrow \mathcal{SO}(3)$.

X. Théorème de Perron-Frobenius et spectres de graphes.

!!! Ce plan est provisoire !!!

(Les chapitres I à VI constituent le cours d'*algèbre linéaire* du semestre d'hiver.)

Table des matières

CHAPITRE VII

Arithmétique des nombres entiers

Le début de ce chapitre a pour but de justifier des résulats avec plusieurs desquels le lecteur est censé être déjà *familier.*

Lecture recommandée pour ce chapitre : le début du livre de G.A. Jones et M.A. Jones, *Elementary number theory* (Springer, 1998).

1. Division euclidienne et pgcd

Dans ce cours,

$$\mathbb{N} = \{0, 1, 2, \ldots\}$$

désigne l'ensemble des *entiers naturels* et

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$

celui des *entiers rationnels.* Ces ensembles sont donnés avec l'*addition* ($3 + 5 = 8$), la *multiplication* ($3 \times 5 = 15$) et la *comparaison* ($3 < 5$) de leurs éléments.

Deux remarques de notation. (a) Le produit de deux entiers $x, y \in \mathbb{Z}$ s'écrit le plus souvent xy ; on n'ajoute un point ou une croix que s'il y a risque de confusion : distinguer $21 \times 4 = 84$, 214 et $2 \times 14 = 28$.

(b) En français mathématique, on dit «x est positif» pour «$x \geq 0$» ; il faut prendre garde que, en anglais, «x is positive» signifie «$x > 0$» et «x is non-negative» signifie «$x \geq 0$». De plus, dans la majorité des livres en anglais, $\mathbb{N}$ désigne l'ensemble $\{1, 2, 3, \ldots\}$, sans le zéro.

1.1. Division euclidienne[1].

THÉORÈME. *Soient $n, d \in \mathbb{Z}$ avec $d > 0$. Il existe deux entiers $q, r \in \mathbb{Z}$ tels que*

$$n = qd + r \quad \textit{et} \quad 0 \leq r < d.$$

De plus q et r sont uniquement déterminés par ces conditions.

PREUVE. *Existence.* Soit S l'ensemble des entiers positifs de la forme $n - kd$, avec $k \in \mathbb{Z}$. Comme S est non vide et minoré, S possède un plus petit élément ; notons-le r. Par définition, il existe $q \in \mathbb{Z}$ tel que $r = n - qd$, et $r \geq 0$. On a aussi $r < d$, sinon, en posant $r' = r - d$, on aurait $r' < r$ et $r' = n - (q+1)d \in S$, contrairement à la définition de r.

Unicité. Supposons que

$$n = q_1 d + r_1 = q_2 d + r_2 \quad \text{et} \quad 0 \leq r_1, r_2 < d.$$

[1] L'invocation d'Euclide pour ce résultat est un peu grandiloquente, mais constitue néanmoins un usage répandu.

Si on avait $q_1 < q_2$, on aurait $r_1 = (q_2 - q_1)d + r_2 \geq d$, ce qui est impossible. De même $q_2 < q_1$ est impossible. Donc $q_1 = q_2$, et par suite $r_1 = r_2$. □

1.2. Définitions et notations. Soient $n, d \in \mathbb{Z}$, avec $d \neq 0$. On dit que d *divise* n, ou que d est un *diviseur* de n, ou que n *est un multiple de* d, et on écrit $d \mid n$, s'il existe $q \in \mathbb{Z}$ tel que $n = qd$. Dans le cas contraire, on écrit $d \nmid n$.

Exemples. $1 \mid 6$, $2 \mid 6$, $3 \mid 6$, $4 \nmid 6$, $5 \nmid 6$, $6 \mid 6$, $7 \nmid 6$, $6 \mid 0$.

1.3. Propriétés immédiates. Si $a, b, c \in \mathbb{Z} \setminus \{0\}$ et $x, y \in \mathbb{Z}$, alors

$$\begin{aligned} a \mid b, \quad a > 0, \quad b > 0 \text{ implique } & 1 \leq a \leq b, \\ a \mid b \text{ et } b \mid c \text{ implique } & a \mid c, \\ a \mid b \text{ implique } & ac \mid bc, \\ a \mid b \text{ et } a \mid c \text{ implique } & a \mid (xb + yc). \end{aligned}$$

1.4. Définitions. Le *plus grand commun diviseur* d'entiers non tous nuls $a_1, \ldots, a_n$ est le plus grand des entiers $k > 0$ qui divisent chacun de ces entiers ; on le note $\operatorname{pgcd}(a_1, \ldots, a_n)$.

On dit que $a_1, \ldots, a_n$ sont *premiers entre eux* si $\operatorname{pgcd}(a_1, \ldots, a_n) = 1$. On dit indifféremment « 8 et 13 sont premiers entre eux » ou « 8 est premier à 13 ».

Exemples. $\operatorname{pgcd}(8, 12) = 4$; les trois entiers $6, 10, 15$ sont premiers entre eux.

Remarques. (i) Si a, k sont deux entiers non nuls, alors $\operatorname{pgcd}(a, ka) = |a|$.

(ii) Si $\epsilon_1, \ldots, \epsilon_n \in \{1, -1\}$, on a $\operatorname{pgcd}(\epsilon_1 a_1, \ldots, \epsilon_n a_n) = \operatorname{pgcd}(a_1, \ldots, a_n)$.

1.5. Lemme. *Soient $n, d \in \mathbb{Z}$ avec $d > 0$ et soient q, r comme au théorème 1.1 : $n = qd + r$ et $0 \leq r < d$. On a*

$$\operatorname{pgcd}(n, d) \;=\; \operatorname{pgcd}(d, r).$$

Preuve. Il suffit de vérifier que l'ensemble des diviseurs communs de n et d coïncide avec l'ensemble des diviseurs communs de d et r, ce qui est immédiat. □

1.6. Algorithme d'Euclide[2].

Proposition. *Le* pgcd *de deux entiers d_1, d_2 tels que $d_1 \geq d_2 > 0$ peut être calculé par l'algorithme suivant.*

Première étape. *Par division euclidienne, on obtient $d_1 = q_1 d_2 + d_3$ avec $q_1 \in \mathbb{N}$ et $0 \leq d_3 < d_2$. Si $d_3 = 0$ alors $d_2 = \operatorname{pgcd}(d_1, d_2)$. Si $d_3 > 0$ on passe à l'étape suivante.*

Deuxième étape. *Par division euclidienne, on obtient $d_2 = q_2 d_3 + d_4$ avec $q_2 \in \mathbb{N}$ et $0 \leq d_4 < d_3$. Si $d_4 = 0$ alors $d_3 = \operatorname{pgcd}(d_1, d_2)$. Si $d_4 > 0$, on recommence ...*

Le nombre des étapes est nécessairement fini car $d_2 > d_3 > d_4 > \cdots \geq 0$.

Si s désigne le plus grand entier tel que $d_s > 0$, alors $d_s = \operatorname{pgcd}(d_1, d_2)$.

[2] Euclide, Livre VII, Propositions 1 et 2.

PREUVE. Notons comme suit le résultat des étapes successives de l'algorithme d'Euclide :

$$\begin{aligned} d_1 &= q_1 d_2 + d_3 \\ d_2 &= q_2 d_3 + d_4 \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ d_{s-2} &= q_{s-2} d_{s-1} + d_s \\ d_{s-1} &= q_{s-1} d_s. \end{aligned}$$

Il résulte du lemme 1.5 que

$$\operatorname{pgcd}(d_1, d_2) = \operatorname{pgcd}(d_2, d_3) = \cdots = \operatorname{pgcd}(d_{s-1}, d_s) = \operatorname{pgcd}(q_{s-1} d_s, d_s)$$

et de la remarque 1.4(ii) que

$$\operatorname{pgcd}(d_1, d_2) = d_s. \qquad \square$$

Le plus grand commun diviseur comme combinaison linéaire entière.

L'algorithme d'Euclide fournit également deux entiers x_1, x_2 tels que

$$\operatorname{pgcd}(d_1, d_2) = x_1 d_1 + x_2 d_2.$$

PREUVE. Démontrons ceci sur l'exemple pour lequel $d_1 = 22$ et $d_2 = 6$. On calcule

$$\begin{aligned} d_1 &= q_1 d_2 + d_3 \quad \text{ou} \quad 22 = 3 \times 6 + 4 \qquad (q_1 = 3, \quad d_3 = 4) \\ d_2 &= q_2 d_3 + d_4 \quad \text{ou} \quad 6 = 1 \times 4 + 2 \qquad (q_2 = 1, \quad d_4 = 2) \\ d_3 &= q_3 d_4 + d_5 \quad \text{ou} \quad 4 = 2 \times 2 + 0 \qquad (q_3 = 2, \quad d_5 = 0) \end{aligned}$$

donc $\operatorname{pgcd}(22, 6) = d_4 = 2$. De plus

$$\begin{aligned} \operatorname{pgcd}(22, 6) = 2 = d_4 &= d_2 - q_2 d_3 = d_2 - q_2(d_1 - q_1 d_2) = -q_2 d_1 + (1 + q_1 q_2) d_2 \\ &= -22 + 4 \times 6. \end{aligned}$$

$\square$

Majoration du nombre d'étapes

PROPOSITION. *Si $s = s(d_1, d_2)$ désigne le nombre d'étapes de l'algorithme d'Euclide alors s est majoré par*

$$s \leq 2 + \frac{\ln(d_2)}{\ln(\theta)} \qquad (*)$$

où $\theta = \frac{1}{2}(1 + \sqrt{5}) \approx 1,618034$ est le nombre d'or.

RAPPEL. Comme $\frac{\log(d_2)}{\log(\theta)} = \frac{\ln(d_2)}{\ln(\theta)}$, la majoration $(*)$ peut aussi s'écrire avec des logarithmes décimaux. Rappelons par ailleurs que $d_1 \geq d_2$.

PREUVE. On constate d'abord que $q_k \geq 1$ pour $k \in \{1, \ldots, s-2\}$, car $d_k > d_{k+2}$, et que $q_{s-1} \geq 2$, car $d_{s-1} > d_s$.

On remarque ensuite que, si a est un diviseur commun de d_1 et d_2, alors $s(d_1/a, d_2/a) = s(d_1, d_2)$. Il suffit donc de montrer $(*)$ lorsque d_1 et d_2 sont premiers entre eux, c'est-à-dire lorsque $d_s = 1$.

Dans ce cas

$$d_k \geq \theta^{s-k} \quad \text{pour tout} \quad k \in \{1, \ldots, s\}.$$

Vérifions ceci par récurrence descendante sur k. D'abord $d_s = 1 = \theta^0$ et $d_{s-1} = q_{s-1} \geq 2 > \theta$. Soit ensuite $k \leq s-2$ et supposons les inégalités $d_{k+2} \geq \theta^{s-k-2}$ et $d_{k+1} \geq \theta^{s-k-1}$ déjà montrées. Alors

$$d_k = q_k d_{k+1} + d_{k+2} \geq d_{k+1} + d_{k+2} \geq \theta^{s-k-2}(\theta + 1) = \theta^{s-k}$$

car $\theta + 1 = \theta^2$.

En particulier $d_2 \geq \theta^{s-2}$. En prenant les logarithmes, on obtient

$$\ln(d_2) \geq (s-2)\ln(\theta)$$

comme annoncé. $\square$

REMARQUE. La preuve ci-dessus indique que, pour obtenir des paires (d_1, d_2) telles que $s(d_1, d_2)$ soit grand, il faut prendre des termes consécutifs de la suite de Fibonacci[3]. Par exemple, si $d_1 = 55$ et $d_2 = 34$, on trouve

$$s = 8 \leq 2 + \frac{\ln(34)}{\ln(\theta)} \approx 9,328.$$

1.7. COROLLAIRE. *Soient $a, b \in \mathbb{Z}$, non tous les deux nuls, et $d = \operatorname{pgcd}(a, b)$. Soit $c \in \mathbb{Z}$. L'équation*

$$ax + by = c$$

a une solution $x, y \in \mathbb{Z}$ si et seulement si $c \in d\mathbb{Z}$. [Voir aussi le corollaire 11.]

En particulier, il existe $x, y \in \mathbb{Z}$ tels que $ax + by = d$. De plus, les diviseurs communs de a et b sont les diviseurs de d.

PREUVE. S'il existe $x, y \in \mathbb{Z}$ tels que $ax + by = c$, nous avons déjà remarqué au numéro 3 tout diviseur commun de a et b divise c, de sorte que d divise c. Donc $c \in d\mathbb{Z}$.

Pour la réciproque, la proposition 1.6 montre qu'il existe $x_0, y_0 \in \mathbb{Z}$ tels que $d = ax_0 + by_0$. Pour tout $c = kd \in \mathbb{Z}$, il suffit de poser $x = kx_0, y = ky_0$ pour que $c = ax + by$. □

1.8. Théorème de Bézout[4]**.** Le théorème suivant (la terminologie est bien établie) n'est qu'un cas particulier du corollaire 1.7.

THÉORÈME. *Deux entiers a, b non tous les deux nuls sont premiers entre eux si et seulement s'il existe des entiers x, y tels que*

$$ax + by = 1.$$

EXEMPLE. Trouver toutes les solutions en nombres entiers de l'équation

$$542 = 17x - 11y.$$

Il s'agit de l'exemple original de Bézout, extrait de son *Cours de Mathématiques à l'usage des Gardes du Pavillon et de la Marine,* en 6 volumes (1764–1769) ; dans ses termes : *On demande en combien de manieres on peut payer* 542 *livres, en donnant des pieces de* 17 *livres & recevant en échange des pieces de* 11 *livres.*

On obtient sans peine $17 \times 2 - 11 \times 3 = 1$, et donc $17 \times 1084 - 11 \times 1626 = 542$. La solution générale est donnée par

$$17 \times (1084 + 11 \times k) - 11 \times (1626 + 17 \times k) = 542 \qquad (k \in \mathbb{Z})$$

---

[3]Rappel : la suite de Fibonacci $(f_n)_{n \geq 0}$ est définie par $f_0 = 1$, $f_1 = 1$ et $f_n = f_{n-1} + f_{n-2}$ pour tout $n \geq 2$. On vérifie facilement par récurrence sur n que

$$f_n = \frac{1}{\sqrt{5}} \left(\theta^{n+1} + (-\theta)^{-n-1}\right) \qquad \text{pour tout} \quad n \geq 0$$

(exercice I.4 du chapitre I). Ici $d_k \geq f_{s-k+1}$ pour tout $k \in \{1, \ldots, s\}$, comme il résulte d'un argument par récurrence descendante sur k ; en particulier $d_2 \geq f_{s-1}$. Ceci montre bien pourquoi le nombre d'or θ joue une rôle dans la majoration de s.

[4]Plusieurs auteurs orthographient « Bezout » , sans accent. Il s'agit pourtant bien d'Étienne Bézout, né à Nemours en 1739, qui fit partie de l'Académie des Sciences dès 1758, et qui est mort en 1783. Il écrivait lui-même son nom avec l'accent aigu, comme en témoigne le fac similé de sa signature paru dans l'article de F. Gramain, *Les degrés des nombres algébriques* $\cos(2\pi/n)$ *et* $\sin(2\pi/n)$, Gazette des mathématiciens **58** (novembre 1993) 29-37.

Ceci dit, ce résultat ne serait pas dû à Bézout, mais à Claude Gaspar Bachet, sieur de Méziriac. Son livre de *Problèmes plaisans et délectables*, dont la seconde édition date de 1624, semble avoir été un grand classique pendant plus de deux siècles, comme en témoignent les très nombreuses éditions ultérieures.

Il est raisonnable de choisir $k = -95$, qui minimise le nombre de «pieces» en jeu, d'où la solution particulière

$$17 \times 39 - 11 \times 11 \;=\; 542.$$

La solution générale écrite sous la forme

$$17 \times (39 + 11 \times s) - 11 \times (11 + 17 \times s) \;=\; 542$$

fait donc intervenir des nombres positifs de pièces si et seulement si $s \in \mathbb{N}$. Comme le dit Bézout : *On peut donc satisfaire à cette question d'une infinité de manieres différentes, qu'on aura toutes en mettant dans les valeurs* [...], *au lieu de* s, *tous les nombres entiers positifs imaginables* [...]. (J'ignore s'il y avait à l'époque de Bézout des pièces de 17 et 11 livres.)

1.9. Les énoncés 1.7 et 1.8 se généralisent comme suit à un nombre $n \geq 2$ d'entiers.

THÉORÈME. *Soient n un entier, $n \geq 2$. Soient $a_1, \ldots, a_{n+1}$ des entiers tels que $a_1, \ldots, a_n$ ne sont pas tous nuls. On pose $d = \operatorname{pgcd}(a_1, \ldots, a_n)$.*

(i) *Les diviseurs communs de $a_1, \ldots, a_n$ sont les diviseurs de d.*

(ii) $\operatorname{pgcd}(a_1, \ldots, a_n, a_{n+1}) = \operatorname{pgcd}(\operatorname{pgcd}(a_1, \ldots, a_n), a_{n+1})$.

(iii) *L'équation*

$$a_1x_1 + \cdots + a_nx_n \;=\; c$$

possède une solution $x_1, \ldots, x_n \in \mathbb{Z}$ si et seulement si $c \in d\mathbb{Z}$.

En particulier, il existe $x_1, \ldots, x_n \in \mathbb{Z}$ tels que $a_1x_1 + \cdots + a_nx_n = d$.

(iv) *Les entiers $a_1, \ldots, a_n$ sont premiers entre eux si et seulement s'il existe des entiers $x_1, \ldots, x_n$ tels que*

$$a_1x_1 + \cdots + a_nx_n \;=\; 1.$$

PREUVE. On procède par récurrence sur n.

Soit d'abord $n = 2$. L'assertion (i) est contenue dans le corollaire 1.7. Il en résulte que l'ensemble des diviseurs communs à a_1, a_2, a_3 coïncide avec l'ensemble des diviseurs communs à $\operatorname{pgcd}(a_1, a_2)$ et a_3, et l'assertion (ii) en résulte. Les assertions (iii) et (iv) sont des répétitions du corollaire 1.7 et du théorème 1.8.

La vérification que les assertions pour $n \geq 3$ résultent des assertions analogues pour $n - 1$ est laissée en exercice au lecteur. □

1.10. PROPOSITION (Gauss [5]). *Soient $a, b \in \mathbb{Z}$ deux entiers premiers entre eux, $a \neq 0$, et $c \in \mathbb{Z}$. Si $a \mid bc$, alors $a \mid c$.*

PREUVE. Puisque $\operatorname{pgcd}(a, b) = 1$, il existe $x, y \in \mathbb{Z}$ tels que $ax + by = 1$. On a donc $acx + bcy = c$.

Vu que a divise évidemment ac, si $a \mid bc$, alors $a \mid (acx + bcy)$, c'est-à-dire $a \mid c$. □

EXEMPLE. $7 \mid 4200$ implique $7 \mid 42$, car $\operatorname{pgcd}(7, 100) = 1$.

[5] Euclide pour a premier.

1.11. Corollaire. *Soient $a, b \in \mathbb{Z} \setminus \{0\}$ et $c \in \mathbb{Z}$; on pose $d = \operatorname{pgcd}(a, b)$. On suppose que l'équation $a\xi + b\eta = c$ (les inconnues étant ξ et η) possède une solution $x \in \mathbb{Z}$, $y \in \mathbb{Z}$, c'est-à-dire que $c \in d\mathbb{Z}$.*

Alors toute solution en entiers de cette équation est de la forme

$$c = a\,(x + kb_1) + b\,(y - ka_1)$$

avec $k \in \mathbb{Z}$, où $a_1 = \frac{a}{d}$ et $b_1 = \frac{b}{d}$.

Preuve. Soient $m, n \in \mathbb{Z}$ tels que $c = a(x + m) + b(y - n)$. On a $am = bn$, donc aussi $a_1 m = b_1 n$ en divisant par d. Vu que a_1, b_1 sont premiers entre eux [6], il résulte de la proposition 1.10 que $l = n/a_1$ et $k = m/b_1$ sont des entiers. En divisant chaque terme de l'égalité $a_1 m = b_1 n$ par $a_1 b_1$, on obtient $k = l$. Par suite $m = kb_1$ et $n = la_1 = ka_1$. □

1.12. Définition. Un sous-ensemble I de $\mathbb{Z}$ est un *idéal* s'il est non vide et si, pour tous $a, b \in I$ et $x \in \mathbb{Z}$, on a $a + b \in I$ et $ax \in I$. [Cette notion d'idéal sera étendue à d'autres anneaux au chapitre VIII.]

Remarque. Tout idéal de $\mathbb{Z}$ contient 0.

Exemples. Pour tout $d \in \mathbb{Z}$, l'ensemble $d\mathbb{Z}$ des multiples entiers de d est un idéal ; de plus, pour $d_1, d_2 \in \mathbb{Z}$, on a $d_1\mathbb{Z} = d_2\mathbb{Z}$ si et seulement si $d_1 \in \{d_2, -d_2\}$. (On écrit parfois aussi (d) pour $d\mathbb{Z}$.)

1.13. Proposition. *Tout idéal de $\mathbb{Z}$ est de la forme $d\mathbb{Z}$ pour $d \in \mathbb{N}$.*

Preuve. Soit I un idéal de $\mathbb{Z}$. Si $I = \{0\}$, il n'y a rien à montrer.

Sinon, il existe $a \in I$, $a \neq 0$; donc $|a| \in I$, $|a| > 0$, et $I_+ = \{b \in I \mid b > 0\}$ n'est pas vide. Soit d le plus petit entier de I_+. On a évidemment $d\mathbb{Z} \subset I$. Par ailleurs, tout $b \in I$ s'écrit $b = qd + r$ avec $q \in \mathbb{Z}$ et $0 \leq r < d$; comme $r \in I$, il résulte de la définition de d que $r = 0$; on en déduit que $I \subset d\mathbb{Z}$, ce qui achève la preuve. □

1.14. Proposition. *Soient $a_1, \ldots, a_n$ des entiers rationnels non tous nuls. On pose*

$$d = \operatorname{pgcd}(a_1, \ldots, a_n) \qquad \text{et}$$
$$I = \{k \in \mathbb{Z} \mid \text{il existe} \quad x_1, \ldots, x_n \in \mathbb{Z} \quad \text{tels que} \quad k = x_1 a_1 + \cdots + x_n a_n\}$$

Alors I est un idéal de $\mathbb{Z}$ et $I = d\mathbb{Z}$.

Preuve. On vérifie immédiatement que I est un idéal de $\mathbb{Z}$. Il résulte du théorème 1.9(iii) que $d \in I$, et de la proposition 1.13 qu'il existe un entier $e > 0$ tel que $I = e\mathbb{Z}$.

L'entier e divise tous les éléments de I, en particulier chacun des a_j. Comme d est le plus grand des diviseurs communs aux a_j, on a $e \leq d$. Par ailleurs, d divise chacun des a_j, donc aussi tous les éléments de I, et en particulier e ; par suite $d \leq e$. Il en résulte que $d = e$. □

[6] A justifier !

Exercices du § VII.1

(VII.1) Ecrire la liste complète des diviseurs de 36, de 59, de 60, et de votre année de naissance.

(VII.2) Pour tout entier $n > 0$, montrer que les entiers $n! + 1$ et $(n + 1)! + 1$ sont premiers entre eux.

(VII.3) On rappelle que les *nombres de Fibonacci* sont définis récursivement par $f_0 = 1$, $f_1 = 1$ et $f_{n+1} = f_n + f_{n-1}$ pour tout $n \geq 2$.

Montrer que deux nombres de Fibonacci successifs sont premiers entre eux.

Est-ce que f_m et f_n sont premiers entre eux pour toute paire d'entiers m, n tels que $m < n$?

(VII.4) Vérifier que les trois entiers 6, 10 et 15 sont premiers entre eux et ne sont pas premiers deux à deux.

Trouver $x, y, z \in \mathbb{Z}$ tels que $x6 + y10 + z15 = 1$.

(VII.5) Calculer le plus grand commun diviseur de 1769 et 2378, et l'exprimer comme combinaison linéaire entière de ces deux nombres.

(VII.6) Combien y a-t-il de solutions de l'équation

$$101\,x \;+\; 99\,y \;=\; 30\,000$$

avec $x, y \in \mathbb{N}$?

(VII.7) L'algorithme d'Euclide fournit un *développement en fraction continue* de tout nombre rationnel ; ainsi, avec les notations de la proposition 6 :

$$\frac{d_1}{d_2} \;=\; q_1 + \frac{1}{d_2/d_3} \;=\; q_1 + \frac{1}{q_2 + \dfrac{1}{d_3/d_4}} \;=\; q_1 + \frac{1}{q_2 + \dfrac{1}{q_3 + \cdots \dfrac{1}{q_{s-1}}}}$$

Par exemple :

$$\frac{22}{7} \;=\; 3 + \frac{1}{7}\,.$$

Calculer les développements en fraction continue des nombre $\frac{333}{106}$, $\frac{355}{113}$. [Il s'agit des premiers termes d'une suite classique d'approximations de π. Le terme suivant est la fraction $\frac{103\,993}{33\,102}$.]

(VII.8) Voici une variante du théorème 1.1 : *Soient $r, d \in \mathbb{Z}$ avec $d \neq 0$. Il existe des entiers $q', r' \in \mathbb{Z}$ tels que*

$$n = q'd + r' \qquad et \qquad |r'| \leq \frac{1}{2}|d|$$

(noter toutefois que r' n'est pas toujours uniquement défini par ces conditions lorsque d est pair). Vérifier que les étapes suivantes en fournissent une preuve.

(i) Constater que, pour tout $x \in \mathbb{Q}$, il existe $q' \in \mathbb{Z}$ tel que $|x - q'| \leq \frac{1}{2}$.

(ii) Particulariser à $x = n/d$.

(VII.9) Soient $\mathbb{Q}(i)$ l'ensemble des nombres complexes de la forme $x_1 + ix_2$ avec $x_1, x_2 \in \mathbb{Q}$ et $\mathbb{Z}[i]$ le sous-ensemble de ces nombres[7] pour lesquels $x_1, x_2 \in \mathbb{Z}$.

Pour tout $x \in \mathbb{Q}(i)$, vérifier qu'il existe $q \in \mathbb{Z}[i]$ tel que $|x - q|^2 \leq \frac{1}{2}$. En déduire que, pour $n, d \in \mathbb{Z}[i]$ avec $d \neq 0$, il existe $q, r \in \mathbb{Z}[i]$ tels que

$$n = qd + r \quad \text{et} \quad 0 \leq |r| < |d|$$

(division euclidienne dans $\mathbb{Z}[i]$).

(VII.10) Soient $\mathbb{Q}(\sqrt{-2})$ l'ensemble des nombres complexes de la forme $x_1 + i\sqrt{2}x_2$ avec $x_1, x_2 \in \mathbb{Q}$ et $\mathbb{Z}[\sqrt{-2}]$ le sous-ensemble de ces nombres pour lesquels $x_1, x_2 \in \mathbb{Z}$.

Pour tout $x \in \mathbb{Q}(\sqrt{-2})$, vérifier qu'il existe $q \in \mathbb{Z}[\sqrt{-2}]$ tel que $|x - q|^2 \leq \frac{3}{4}$. En déduire que, pour $n, d \in \mathbb{Z}[\sqrt{-2}]$ avec $d \neq 0$, il existe $q, r \in \mathbb{Z}[\sqrt{-2}]$ tels que

$$n = qd + r \quad \text{et} \quad 0 \leq |r| < |d|$$

(division euclidienne dans $\mathbb{Z}[\sqrt{-2}]$).

(VII.11) Soit $N \geq 3$ un entier premier à 10. Montrer que N divise un entier de la forme $111\cdots1$ (avec $k+1$ chiffres 1 en écriture décimale), c'est-à-dire un entier $u_k = \sum_{j=0}^{k} 10^j$.

[Indication. Soit r_k le reste de la division de u_k par N. Il existe k, l tels que $l > k \geq 1$ et $r_l = r_k$. Alors N divise $10^{-k}(r_l - r_k)$.]

(VII.12) Un sous-ensemble S de l'ensemble $\mathbb{Z}$ des entiers rationnels est dit *périodique de prériode s*, où $s \in \mathbb{Z}$ et $s \geq 1$ si, pour $n \in \mathbb{Z}$, on a $n \in S$ si et seulement si $n + s \in S$.

(i) Observer que, si $S_1, \ldots, S_k$ sont des sous-ensembles périodiques de $\mathbb{Z}$ respectivement de périodes $s_1, \ldots, s_k$, alors la réunion $\cup_{i=1}^{k} S_i$ est périodique d'une période divisant $\prod_{i=1}^{k} s_i$. Observer aussi que le complémentaire d'un sous-ensemble périodique de prériode s est également périodique de prériode s.

[7] $\mathbb{Q}(i)$ est un *corps* pour les règles usuelles d'addition et de multiplication, et $\mathbb{Z}[i]$ est l'anneau des *entiers de Gauss*. De même (exercice suivant), $\mathbb{Q}(\sqrt{-2})$ est un *corps quadratique imaginaire* et $\mathbb{Z}[\sqrt{-2}]$ est son *anneau d'entiers*. L'existence d'une division euclidienne dans un anneau du type $\mathbb{Z}[\sqrt{-d}]$ est un phénomène rare, limité à une courte suite d'entiers (incluant $d = 2$ et $d = 3$).

(ii) Pour tout nombre premier p, notons $S_{(p)}$ l'ensemble des multiples de p (c'est un idéal de $\mathbb{Z}$). Soit S la réunion des $S_{(p)}$ prise sur l'ensemble de tous les nombres premiers. Vériier que le complémentaire de S est l'ensemble $\{-1, 1\}$, et en déduire une preuve de l'infinitude des nombres premiers.

[Cette nouvelle (!) preuve de l'infinitude des nombres premiers est essentiellement due à Harry Furstenberg. Voir son article *On the infinitude of primes,* Amer. Math. Monthly **62** (1955) 353, ainsi que l'article de D. Cass et G. Wildenberg in Math. Magazine **76 :3** (2003) 203.]

2. Nombres premiers

2.1. Définition. Un *nombre premier* est un entier $p > 1$ tel que les seuls diviseurs strictement positifs de p sont 1 et p.

Exemples. Les nombres

2, 3, 5, 7, 11, 13, 17, 19, ..., 1993, 1997, 1999, 2003, 2011, 2017, 2027, 2029, ...

sont premiers.

Remarque. Si p_1, p_2 sont deux nombres premiers distincts, alors $\mathrm{pgcd}(p_1, p_2) = 1$.

2.2. Théorème fondamental de l'arithmétique. *Tout nombre entier $n \geq 2$ est produit de nombres premiers, uniquement déterminés à l'ordre près.*

Preuve de l'existence, par récurrence sur n. Lorsque $n = 2$, l'assertion est évidemment vraie. Supposons désormais $n > 2$, et le théorème vrai pour tout nombre entier n' tel que $1 \leq n' < n$. On distingue deux cas.

Si n est premier, il n'y a rien à montrer. Sinon, il existe deux entiers n_1 et n_2 strictement compris entre 1 et n tels que $n = n_1 n_2$; comme n_1 et n_2 sont produits de nombres premiers par l'hypothèse de récurrence, il en est de même de n. □

2.3. Lemme. *Soient p un nombre premier et $a, b \in \mathbb{Z}$ des entiers. Si p divise ab, alors p divise au moins l'un des deux entiers a, b.*

Preuve. Les diviseurs de p étant 1, -1, p et $-p$, on a ou bien $\mathrm{pgcd}(p, b) = 1$ ou bien $\mathrm{pgcd}(p, b) = p$. Dans le premier cas, p divise a en vertu de la proposition 1.10 ; dans le second cas, p divise b. □

Remarque. C'est une conséquence immédiate du lemme que, pour un nombre premier p et des entiers $a_1, \ldots, a_n \in \mathbb{Z}$, si p divise $\prod_{j=1}^{n} a_j$, alors p divise au moins l'un des a_j.

Preuve de l'unicité pour le théorème fondamental de l'arithmétique. Soient $n \geq 2$ et

$$n = \prod_{i=1}^{k} p_i = \prod_{j=1}^{l} q_j \qquad (*)$$

deux décompositions de n en produit de nombres premiers. On suppose les notations telles que $k \leq l$, et on procède par récurrence sur k.

Si $k = 1$, alors $n = p_1$ est premier, donc $l = 1$ et $p_1 = q_1$.

Si $k \geq 2$, le lemme montre qu'il existe $j \in \{1, \ldots, l\}$ tel que $p_k = q_j$; de plus, on peut supposer les notations telles que $p_k = q_l$. Vu l'hypothèse de récurrence, les décompositions

$$\frac{n}{p_k} = \prod_{i=1}^{k-1} p_i = \prod_{j=1}^{l-1} q_j$$

sont identiques à l'ordre près des facteurs. Il en résulte que les deux décompositions de (∗) sont également identiques à l'ordre près des facteurs. □

2.4. Remarques.

(i) Pour avoir un énoncé simple du théorème fondamental, *il est important de convenir que* 1 *n'est PAS un nombre premier.* Il y a beaucoup d'autres énoncés pour la simplicité desquels la même convention est avantageuse ; voir par exemple le théorème 4.7.

(ii) On convient qu'un *produit vide* est égal au nombre 1. Le théorème fondamental de l'arithmétique vaut donc pour tout entier $n \geq 1$.

(iii) Pour qu'un nombre $n > 1$ soit premier, il faut et il suffit que, pour tout entier d tel que $1 < d \leq \sqrt{n}$, le reste de la division de n par d soit non nul. Cette remarque fournit un critère pour reconnaître les nombres premiers, mais l'usage de ce critère mène à des calculs très longs dès que n est assez grand.

(iv) Un nombre *impair* $n > 1$ est composé, $n = ab$, si et seulement s'il est différence de deux carrés, c'est-à-dire si et seulement s'il est de la forme $n = c^2 - d^2$ avec $c, d \in \mathbb{N}$. [Il suffit de poser $c = \frac{1}{2}(a+b)$ et $d = \frac{1}{2}(a-b)$.] Ceci mène à un algorithme de décomposition qui est efficace chaque fois que n possède deux diviseurs de tailles semblables.

Considérons le cas de $n = 6077$. Si $n = c^2 - d^2$, alors $c \geq \sqrt{6077}$, c'est-à-dire $c \geq 78$. Il s'agit donc de chercher un entier $k \geq 78$ tel que $k^2 - n$ soit un carré. D'où les calculs que voici :

$$\begin{aligned} 78^2 - 6077 &= 7 && \text{n'est pas un carré,} \\ 79^2 - 6077 &= 164 && \text{n'est pas un carré,} \\ 80^2 - 6077 &= 323 && \text{n'est pas un carré,} \\ 81^2 - 6077 &= 484 = 22^2 && \text{est un carré.} \end{aligned}$$

Par suite $6077 = 81^2 - 22^2 = (81 + 22)(81 - 22) = 103 \times 59$.

(v) Il n'est en général pas facile du tout de décomposer un «grand» nombre en produit de nombres premiers. Mais les progrès sont rapides, comme en témoignent par exemple les joutes organisées par les laboratoires RSA de San Mateo (Californie), maîtres ès cryptographies. Il existe un site régulièrement mis à jour informant des progrès dans ce domaine. Voir

http://www.rsasecurity.com/rsalabs/challenges/

ou interroger «google» en écrivant «rsa challenge» .

(vi) La litérature traitant des nombres premiers est considérable. Citons le livre de vulgarisation de Marcus du Sautoy : *The music of the primes* (HarperCollins, 2003), et le site compagnon

http://www.musicoftheprimes.com/.

2.5. Théorème (Euclide[8]). *Il existe une infinité de nombres premiers.*

Preuve d'Euclide. On commence par observer qu'il existe au moins un nombre premier, par exemple 2.

Soit alors $\{p_1, \dots, p_k\}$ un ensemble fini de nombres premiers. On considère l'entier

$$n \;=\; 1 \,+\, \prod_{1\le i\le k} p_i.$$

Vu le théorème précédent, il existe un nombre premier p qui divise n. Ce p n'est pas dans $\{p_1, \dots, p_k\}$, sinon il diviserait n et $n-1$, donc aussi $1 = n-(n-1)$, ce qui est absurde. Il en résulte qu'aucun ensemble fini $\{p_1, \dots, p_k\}$ ne peut coïncider avec l'ensemble de *tous* les nombres premiers. □

Autres preuves : voir l'exercice (VII.16) et le numéro 2.6.
Les passages en petites lettres ne font pas partie du programme d'examen.

Remarques. Soit $(p_i)_{i\ge 1}$ la suite croissante des nombres premiers :

$$p_1 = 2, \quad p_2 = 3, \quad p_3 = 5, \quad p_4 = 7, \quad \dots, \quad p_{25} = 97, \quad \dots,$$
$$p_{304} = 2003, \quad p_{305} = 2011, \quad \dots$$

(i) Le nombre $1 + \prod_{i=1}^{k} p_i$ est rarement premier ! Il l'est pour $k \in \{1, 2, 3, 4, 5\}$ et pour précisément cinq autres valeurs de k telles que $k \le 10^5$. En particulier le nombre

$$1 \,+\, \prod_{1\le i\le 6} p_i \;=\; 1 \,+\, 2\times 3\times 5\times 7\times 11\times 13 \;=\; 30031 \;=\; 59\times 509$$

n'est pas premier.

(ii) Illustrons avec la preuve d'Euclide le fait qu'un bon argument montre souvent plus que son objectif premier. La preuve d'Euclide montre en effet que $p_{k+1} \le 1 + \prod_{i=1}^{k} p_i$ (voir aussi l'exercice 2.15), d'où il résulte que

$$p_{k+1} \;\le\; 2^{2^k} \qquad \text{pour tout} \quad k \ge 1 \tag{♯}$$

par une récurrence immédiate.

L'inégalité (♯) peut être elle-même considérablement améliorée (au prix d'efforts plus importants !). Par exemple, le « théorème des nombres premiers » (voir plus bas) équivaut à l'égalité asymptotique

$$\lim_{k\to\infty} \frac{p_k}{k \ln k} \;=\; 1.$$

[8] Euclide, Livre XI, proposition 20.

2.6. Une preuve d'Euler. Il existe de nombreuses autres preuves de l'infinité des nombres premiers. Voir par exemple « Proofs from THE BOOK »[9], pages 3 à 6. Ci-dessous, nous en esquissons brièvement une.

Si $\mathbb{P}$ désigne l'ensemble des nombres premiers, nous allons montrer que le produit sur $\mathbb{P}$ des facteurs $(1-\frac{1}{p})^{-1}$ diverge, au sens où $\lim_{x\to\infty}\prod_{p\le x}\left(1-\frac{1}{p}\right)^{-1}=\infty$ (avec $\prod_{p\le x}$ désignant le produit sur tous les nombres premiers $p\in\mathbb{P}$ tels que $p\le x$).

Le premier pas est de vérifier que

$$\sum_{k=0}^{\infty}\frac{1}{p^k}\;=\;\left(1-\frac{1}{p}\right)^{-1}$$

pour tout $p\in\mathbb{P}$ (somme d'une série géométrique). Il en résulte que

$$\begin{aligned}&\frac{1}{1-\frac12}\;\frac{1}{1-\frac13}\;\frac{1}{1-\frac15}\;\cdots\;\frac{1}{1-\frac1p}\;=\\&\quad\left(1+\frac12+\frac14+\frac18+\cdots\right)\left(1+\frac13+\frac19+\cdots\right)\left(1+\frac15+\cdots\right)\cdots\left(1+\frac1p+\cdots\right)\;>\\&\quad1+\frac12+\frac13+\frac14+\frac15+\frac16+\cdots+\frac{1}{p-1}+\frac1p\end{aligned}$$

où la dernière inégalité est une conséquence du théorème fondamental de l'arithmétique. Plus formellement :

$$\begin{aligned}\prod_{p\in\mathbb{P}}\left(1-\frac1p\right)^{-1}&=\prod_{p\in\mathbb{P}}\sum_{k=0}^{\infty}\frac{1}{p^k}\;=\;\left(\sum_{k=0}^{\infty}\frac{1}{2^k}\right)\left(\sum_{l=0}^{\infty}\frac{1}{3^l}\right)\left(\sum_{m=0}^{\infty}\frac{1}{5^m}\right)\cdots\\&=\;1\;+\sum_{p\in\mathbb{P}}\frac1p\;+\sum_{p_1\le p_2\in\mathbb{P}}\frac{1}{p_1p_2}\;+\sum_{p_1\le p_2\le p_3\in\mathbb{P}}\frac{1}{p_1p_2p_3}\;+\cdots\\&=\;\sum_{n=1}^{\infty}\frac1n\end{aligned}$$

où les $\cdots$ de la première ligne indiquent les termes du produit correspondant aux premiers plus grand ou égaux à 7, et où les $\cdots$ de la deuxième ligne indiquent les termes de la série correspondant aux inverses des nombres entiers produits d'au moins 4 nombres premiers (non nécessairement distincts).

Comme la série harmonique $\sum_{n=1}^{\infty}\frac1n$ diverge (voir le cours d'Analyse I, ou la page 190 du livre de E. Hairer et G. Wanner, *Analysis by its history*, Springer, 1996), le produit $\prod_{p\in\mathbb{P}}\left(1-\frac1p\right)^{-1}$ diverge aussi, et par suite $\mathbb{P}$ est un ensemble infini. □

[En exploitant un peu mieux la même idée, on montre facilement que la fonction π introduite ci-dessous est minorée par

$$\pi(x)\;\ge\;\ln x-1$$

voir « Proofs from THE BOOK » , cité ci-dessus.]

Le résultat d'Euler est équivalent au fait que la série $\sum_{p\in\mathbb{P}}\frac1p$ diverge.

Dirichlet a montré en 1837 que, pour toute paire (a,b) d'entiers premiers entre eux, la série $\sum\frac1p$ diverge encore lorsque la somme porte sur tous les nombres premiers de la forme $ka+b$.

Exercices du § VII.2.

(VII.13) Si p désigne un nombre premier et n le carré d'un nombre entier, montrer que $p\mid n$ implique $p^2\mid n$, que $p^3\mid n$ implique $p^4\mid n$, etc.

Pour tout entier $n\ge0$, montrer l'alternative suivante :

ou bien n est le carré d'un entier ou bien $\sqrt{n}$ est un nombre irrationnel.

(VII.14) On considère un entier $n\ge1$, le coefficient binomial $\binom{2n}{n}=\frac{(2n)!}{n!n!}$ et le produit P des nombres premiers p tels que $n<p<2n$. Montrer que P divise $\binom{2n}{n}$.

[9] M. Aigner et G.M. Ziegler, *Proofs from THE BOOK,* Springer 1988 (existe en traduction française).

(VII.15) Montrer qu'il existe une infinité de nombres premiers de la forme $4k+3$.

[Indication. Choisir un nombre premier $p \geq 2$ et poser $n = (4 \times 3 \times 5 \times \cdots \times p) - 1$ (donc $n+1$ est le produit de 4 et des nombres premiers impairs de 3 à p). Alors la décomposition de n en facteurs premiers fournit au moins un nombre premier $\ell = 4k+3 > p$.]

De même, monter qu'il existe une infinité de nombres premiers de la forme $6k+5$.

[Indication. Choisir $p \geq 5$ et poser $n = 2 \times 3 \times 5 \times \cdots \times p - 1$. Alors la décomposition de n en facteurs premiers fournit au moins un nombre premier $\ell = 6k+5 > p$.]

(VII.16) Pour tout entier $n \geq 0$, on définit le n-ième *nombre de Fermat*

$$F_n = 2^{2^n} + 1.$$

Par exemple :

$$\begin{aligned} F_0 &= 3 & F_1 &= 5 \\ F_2 &= 17 & F_3 &= 257 \\ F_4 &= 65\,537 \\ F_5 &= 641 \times 6\,700\,417 \\ F_6 &= 274\,177 \times 67\,280\,421\,310\,721\,. \end{aligned}$$

(i) Montrer par récurrence sur n que $\prod_{k=0}^{n-1} F_k = F_n - 2$.

(ii) Pour des indices m, n distincts, montrer que F_m et F_n sont premiers entre eux.

(iii) Déduire de (ii) une autre preuve de l'infinitude des nombres premiers.

Remarque. Le lemme 5.10 ci-dessous montre que tout nombre premier impair divisant un nombre de Fermat, et plus généralement un nombre de la forme x^2+1, est de la forme $4k+1$. [Exercice : le vérifier pour $x \leq 15$.] L'argument ci-dessus permet donc de montrer qu'il existe une infinité de nombres premiers de la forme $4k+1$ (proposition 5.11).

Digression historique. Fermat a cru que F_n est premier pour tout n. En 1732, Euler[10] a découvert que F_5 ne l'est pas, et plus précisément que c'est un multiple de 641. En effet, comme

$$2^{2^5} = (641 - 625)\,2^{28} = (641)\,2^{28} - \left(5 \times 2^7\right)^4 = (641)\,2^{28} - (641 - 1)^4$$

on voit que $641 \mid (2^{2^5}+1)$. Aujourd'hui, on ne connaît aucun nombre de Fermat qui soit premier, hormis les cinq connus de Fermat et Euler. On connaît plusieurs nombres de Fermat composés (= non premiers), par exemple celui d'indice 23471 (!). Mais on ne sait ni s'il y a une infinité de nombres de Fermat premiers, ni s'il y en a une infinité de composés.

Digression géométrique. C'est un vieux problème de savoir pour quels entiers $n \geq 3$ un polygone régulier du plan peut être construit à la règle et au compas. Les Grecs de l'antiquité connaissaient des constructions pour $n = 3, 5, 15$, et savaient aussi construire un $(2n)$-gone régulier à partir d'un n-gone régulier. Le 30 mars 1796, à l'âge de 19 ans, Gauss découvrit une construction du 17-gone régulier. C'est aussi à Gauss qu'on doit le théorème suivant : *le n-gone régulier est constructible à la règle et au compas si*[11] *n est de la forme*

$$n = 2^r p_1 \cdots p_s$$

[10] Euler, Opera, Vol. 2, pages 1–5.

[11] En 1837, Wantzel a montré qu'on pouvait écrire «si et seulement si» au lieu de «si» .

où r, s sont des entiers ≥ 0 et où $p_1, \ldots, p_s$ sont des premiers de Fermat distincts.

Il existe une construction pour $n = 257$, et des chercheurs courageux ont même entrepris de trouver une construction du 65537-gone régulier. Pour une preuve du théorème de Gauss, voir par exemple I. Stewart, *Galois theory*, Chapman and Hall, 1973.

EXERCICE. Soient $m, n \geq 2$ des entiers premiers entre eux tels que les polygones réguliers à m et n côtés soient constructibles à la règle et au compas. Montrer qu'il en est de même du polygone régulier à mn côtés.

[*Indication* : Utiliser le théorème de Bézout.]

(VII.17) Pour $a \geq 2$ et $m \geq 2$, montrer que, si $n = a^m + 1$ est premier, alors a est pair et m est une puissance de 2 [de sorte que, si $a = 2$, alors n est un nombre de Fermat].

Vérifier que $6^2 + 1$ et $6^4 + 1$ sont des nombres premiers, mais que $6^3 + 1$, $6^5 + 1$, $6^6 + 1$ et $6^7 + 1$ sont composés.

[N.B. : on vérifie avec une calculette[12] que $6^{2^3} + 1 = 6^8 + 1$ est divisible par 17.]

(VII.18) Pour $a, m \geq 2$, montrer que, si $n = a^m - 1$ est premier, alors $a = 2$ et m est premier.

Vérifier que les *nombres de Mersenne* $M_p = 2^p - 1$ sont premiers pour quelques-uns des premiers de la liste $p = 2$, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, ..., 216 091, ...

Vérifier que M_p est composé pour au moins un des premiers de la liste $p = 11$, 23, 29, 37, 41, 43, 47, ... [Par exemple $M_{11} = 2047 = 23 \times 89$.]

[Aujourd'hui[13], on connaît 40 nombres de Mersenne qui sont des nombres premiers. Le plus grand d'entre eux est $2^{20996011} - 1$.]

(VII.19) Un nombre entier n est *parfait* s'il est égal à la somme de ses diviseurs stricts (c'est-à-dire à la somme des entiers d tels que $1 \leq d < n$ et $d \mid n$).

(i) Vérifier que 6, 28, 496, 8128 sont parfaits.

(ii) Montrer que, si p est un nombre premier tel que $2^p - 1$ est premier, alors $2^{p-1}(2^p - 1)$ est parfait. (Euclide connaissait une preuve de ce fait. Dix-huit à vingt siècles plus tard, Euler a montré que, réciproquement, tout nombre parfait *pair* est de cette forme.)

---

[12] Voici un autre argument pour le lecteur prêt à se laisser guider ici par le théorème de Fermat (5.7 ci-dessous) plutôt qu'à utilliser une calculette. Comme 6 et 17 sont premiers entre eux,

$$17 \quad \text{divise} \quad 6^{16} - 1 = (6^8 + 1)(6^4 + 1)(6^2 + 1)(6 + 1)(6 - 1)$$
$$= (6^8 + 1) \times 1297 \times 37 \times 7 \times 5.$$

Il est évident que 17 ne divise ni 5, ni 7, ni 37, et il est facile de vérifier qu'il ne divise pas non plus 1297. Il en résulte que le nombre premier 17 divise nécessairement $6^8 + 1$. Le lecteur qui n'aurait pas besoin du théorème de Fermat pour deviner que 17 convient peut aussi utiliser la théorie du § VII.3 et argumenter comme suit : $6^2 \equiv 2 \pmod{17}$, donc $6^8 \equiv 2^4 \equiv -1 \pmod{17}$, donc $6^8 + 1 \equiv 0 \pmod{17}$.

[13] Plus précisément depuis octobre 2003, d'après http://www.utm.edu/research/primes/mersenne/.

On ignore s'il existe une infinité de nombres parfaits, mais on conjecture que c'est le cas. On ignore s'il existe[14] des nombres parfaits impairs.

Les nombres parfaits ont eu une importance historique considérable. Au Moyen Âge, c'est l'un des sujets mathématiques les plus discutés. Beaucoup plus récemment ils occupent une partie du chapitre 1 dans le livre *Triangle de pensées* de A. Connes, A. Lichnerowicz et M.P. Schützenberger (Odile Jacob, 2000).

(VII.20) Contrairement à certaines idées reçues, il existe bel et bien des «formules» qui fournissent les nombres premiers (bien que plusieurs d'entre elles n'aient guère qu'un intérêt anecdotique). Voir le numéro 4.12.

(VII.21) Soit $(p_k)_{k\geq 1}$ la suite croissante des nombres premiers. On choisit un entier k et on pose $N = \prod_{j=1}^{k} p_j$.

(i) Montrer que $N-1$ et $N+1$ sont premiers entre eux.

(ii) Déduire de (i) que $p_{k+2} \leq N+1$.

Compléments au § VII.2

Ces compléments n'entrent pas dans la matière de l'examen.

(1) Pour tout nombre réel $x \geq 1$, on note $\pi(x)$ le nombre des nombres premiers dans l'intervalle $[1, x]$. On a

$$\lim_{x\to\infty} \pi(x) = \infty \qquad \text{(Euclide)},$$

$$\lim_{x\to\infty} \frac{\pi(x)}{x} = 0 \qquad \text{(Legendre, 1808)},$$

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} = 1 \qquad \text{(TNP, Hadamard et de la Vallée Poussin, 1896)}$$

(TNP = théorème des nombres premiers). A la fin du XIXème siècle, il était de bon ton d'affirmer que deviendrait immortel celui qui trouverait une preuve du TNP. Hadamard et de la Vallée Poussin, qui trouvèrent leurs preuves indépendamment l'un de l'autre, ne démentirent que faiblement l'affirmation puisqu'ils moururent respectivement à 98 et presque 96 ans. Leurs preuves utilisent de fortes doses de théorie des fonctions analytiques d'une variable complexe (voir le cours d'Analyse II). En 1949 et à la surprise générale, P. Erdös et A. Selberg ont trouvé (de nouveau indépendamment l'un de l'autre) des preuves dites «élémentaires» (sans théorie des fonctions d'une variable complexe).

On obtient de meilleures approximations de la fonction $\pi(x)$ en la comparant au *logarithme intégral*, défini par

$$Li(x) = \int_2^x \frac{dt}{\ln t},$$

et dont on sait[15] par ailleurs que $\lim_{x\to\infty} \frac{Li(x)}{x/\ln x} = 1$.

---

[14] S'il existe un nombre parfait impair n, on sait qu'il doit être «grand» au sens où $n > 10^{300}$. Voir par exemple http://mathworld.wolfram.com/PerfectNumber.html.

[15] PREUVE. En intégrant par parties, nous avons

$$Li(x) = \int_2^x 1\,\frac{1}{\ln t}\,dt = \frac{x}{\ln x} - \frac{2}{\ln 2} - \int_2^x \frac{dt}{(\ln t)^2}.$$

Il suffit donc de montrer que

$$\lim_{x\to\infty} \frac{\int_2^x \frac{dt}{(\ln t)^2}}{Li(x)} = 0.$$

Soit $\epsilon > 0$. Soient $a, x \in \mathbb{R}$ tels que $a \geq \epsilon^{-1}$ et $x > e^a \geq 2$; on pose $D = \int_2^{e^a} \frac{dt}{(\ln t)^2}$. Alors

$$\int_2^x \frac{dt}{(\ln t)^2} \leq \int_2^{e^a} \frac{dt}{(\ln t)^2} + \int_{e^a}^x \frac{dt}{a \ln t} \leq D + \epsilon \int_{e^a}^x \frac{dt}{\ln t}$$

Les propriétés de la fonction d'une variable réelle $\pi(x)$ sont très étroitement liées à celles de la «fonction dzêta de Riemann» $\zeta(s)$, définie pour tout $s \in \mathbb{C}, s \neq 1$, et analytique dans ce domaine. On en connaît certains zéros : les «zéros triviaux» $-2, -4, -6, \ldots$; on sait aussi qu'il existe une infinité de zéros sur la «droite critique» $\frac{1}{2} + i\mathbb{R}$.

La très célèbre HYPOTHÈSE DE RIEMANN, non démontrée à ce jour, selon laquelle la fonction $\zeta(s)$ n'a pas d'autres zéros que ceux évoqués ci-dessus, impliquerait l'estimation

$$\pi(x) \;=\; Li(x) + O\left(\sqrt{x}\,\ln x\right)$$

et aurait des conséquences importantes en théorie des nombres. L'article original de B. Riemann, *Über die Anzahl der Primzahlen unter einer gegebenen Grösse,* date de 1859.

(2) Pour tout entier $n \geq 1$, il existe un entier $N \geq 1$ tel que l'intervalle $[N, N+n]$ ne contient aucun nombre premier.

Cela résulte de l'exercice facile suivant : pour tout entier $n \geq 2$, vérifier qu'aucun des n entiers

$$(n+1)!+2\,,\ (n+1)!+3\,,\ \ldots\,,\ (n+1)!+n\,,\ (n+1)!+n+1$$

n'est premier.

Pour tout entier n, on sait qu'il existe un nombre premier p tel que $n < p \leq 2n$. Il en résulte que, si p_k désigne le $k$ième nombre premier, on a $p_{k+1} < 2p_k$ pour tout $k \geq 1$. (C'est un résultat connu sous le nom de «postulat de Bertand» , et démontré par Chebyshev en 1852. Voir le chapitre 2 de «Proofs from THE BOOK» .)

On ne sait pas si, pour tout entier $n \geq 1$, il existe un nombre premier compris entre n^2 et $(n+1)^2$. En revanche, on sait qu'il en existe toujours un entre n^3 et $(n+1)^3$.

(3) On ne sait pas s'il existe une infinité de «jumeaux» , c'est-à-dire de paires de nombres premiers de la forme $(p, p+2)$.

Exemples de jumeaux : $(3,5)$, $(41,43)$, $(1997,1999)$, $(2027,2029)$, $(9929,9931)$.

A fortiori, on ne sait pas si (mais on conjecture que) il existe une infinité de triples de nombres premiers de la forme $(p, p+2, p+6)$; idem pour $(p, p+4, p+6)$. [Exercice : recenser les triples de ce type entre 1 et 100.]

(4) On ne sait pas si tout entier ≥ 6 est somme de trois nombres premiers, comme Goldbach en a exprimé la conviction dans une lettre à Euler de 1742. Euler répondit que ceci était vrai si et seulement si

tout entier pair ≥ 4 est somme de deux nombres premiers

(l'équivalence est facile à monter). On ne connaît toujours pas de preuve de cette *conjecture de Goldbach.* Exemples confirmant la conjecture : $96 = 7 + 89$, $98 = 19 + 79$, et

$$100 \;=\; 3+97 \;=\; 11+89 \;=\; 17+83 \;=\; 29+71 \;=\; 41+59 \;=\; 47+53.$$

Depuis les travaux de Hardy & Littlewood (1923) et Vinogradov (1937), on sait que tout entier impair «assez grand» est somme de trois nombres premiers impairs (pour être «assez grand» , il suffit par exemple d'être plus grand que $3^{3^{15}}$).

En 1964, la conjecture de Goldbach a été vérifiée pour tout entier pair inférieur à 33 millions. Le livre de P. Ribenboim[16] mentionne une vérification de la conjecture pour tout entier $n \leq 10^8$.

(5) La «théorie des nombres» permet de poser d'innombrables problèmes d'énoncés élémentaires et de solutions apparemment tout à fait hors d'atteinte. On en trouve par exemple une liste commentée dans le livre de R.K. Guy, *Unsolved problems in number theory* (Springer, 1981), qui commente à juste titre (page vii) : «To pose good unsolved problems is a difficult art. The balance between triviality and hopeless unsolvability is delicate» .

(6) L'une des raisons de la fascination qu'exercent les nombres premiers peut s'énoncer comme suit : d'une part ils sont parfaitement déterminés (et on peut même écrire des formules qui fournissent pour tout n le $n$ième nombre premier – voir 4.15), et d'autre part leur ensemble exhibe de multiples propriétés caractéristiques des ensembles dits aléatoires.

Lecture recommandée : D. Zagier, *The first 50 million prime numbers,* Math. Intelligencer **0** (1977) 7–19.

[On peut entre autre y lire une preuve, essentiellement découverte par Chebyshev en 1850, des inégalités suivantes :

$$\frac{2}{3}\;\frac{x}{\ln x} \;<\; \pi(x) \;<\; 1,7\;\frac{x}{\ln x}$$

---

et

$$\frac{\int_2^x \frac{dt}{(\ln t)^2}}{Li(x)} \;\leq\; \frac{D}{Li(x)} + \epsilon.$$

La conclusion en résulte. □

[16] *The book of prime number records,* second edition, Springer, 1989

pour tout $x \geq 1$ (voir ci-dessus l'énoncé du TNP). L'exercice 8 consistant à montrer qu'un certain produit P de nombres premiers divise $\binom{2n}{n}$ est l'une des étapes de cette preuve pour l'inégalité de droite. En effet, on a d'une part

$$\binom{2n}{n} < \sum_{j=0}^{2n} \binom{2n}{j} = (1+1)^{2n} = 2^{2n},$$

et d'autre part

$$P = \prod_{\substack{n<p<2n \\ p \text{ premier}}} p > n^{\pi(2n)-\pi(n)},$$

de sorte que

$$n^{\pi(2n)-\pi(n)} \leq P \leq \binom{2n}{n} < 2^{2n}$$

ou encore en prenant les logarithmes

$$\pi(2n) - \pi(n) < \frac{2n \ln 2}{\ln n} < 1,39 \frac{n}{\ln n}. \qquad (*)$$

Pour la preuve en question de $\pi(x) < 1,7 \frac{x}{\ln x}$, on vérifie [17] d'abord l'inégalité «à la main» pour $x < 1200$, puis on procède par récurrence à l'aide de l'inégalité $(*)$.]

(7) La fascination déjà mentionnée est certainement due pour une bonne part à la *cohérence interne* (ou la profondeur, ou la beauté, ...) de la théorie. Mais il existe par ailleurs de nombreuses *applications* de cette théorie, notamment à la cryptographie (transmission de messages secrets, sécurité de cartes bancaires, etc., voir § VII.7 et § VII.8).

3. Congruences

Ce paragraphe a pour but d'exposer la notion de *congruence*. Nous répétons d'abord quelques définitions du § II.6.

3.1. Définitions. Une *relation d'équivalence* sur un ensemble E est une partie R de l'ensemble produit $E \times E$ ayant les propriétés suivantes, où x, y, z sont des éléments quelconques de E et où on écrit $x \sim y$ pour $(x, y) \in R$:

$$x \sim x \quad \text{(réflexivité)},$$
$$\text{si} \quad x \sim y \quad \text{alors} \quad y \sim x \quad \text{(symétrie)},$$
$$\text{si} \quad x \sim y \quad \text{et} \quad y \sim z \quad \text{alors} \quad x \sim z \quad \text{(transitivité)}.$$

Soit R une telle relation. Pour tout $x \in E$, la *classe* de x est le sous-ensemble C_x de E des éléments $y \in E$ tels que $y \sim x$, et tout $y \in C_x$ est un *représentant* de la classe C_x. Pour deux éléments x, y de E, ou bien $C_x = C_y$, ou bien les classes C_x et C_y sont des sous-ensembles *disjoints* de E.

L'ensemble des classes est l'*ensemble quotient ;* on le note souvent $E/\sim$ ou E/R. L'*application canonique*, appelée aussi *projection canonique*, est $\begin{cases} E & \longrightarrow & E/R \\ x & \longmapsto & C_x \end{cases}$.

Exemples. (i) Sur l'ensemble E des 8 sommets d'un cube centré à l'origine O de $\mathbb{R}^3$, la relation R pour deux sommets d'être sur une même droite passant par O est une relation d'équivalence pour laquelle l'ensemble E/R a 4 éléments ; ainsi $C_x = \{x, -x\}$ pour tout $x \in E$. On peut identifier ce quotient E/R à l'ensemble des 4 diagonales du cube.

(ii) Sur l'ensemble E des parties finies d'un ensemble infini, la relation R définie par ARB s'il existe une bijection de A sur B est une relation d'équivalence. L'ensemble quotient E/R s'identifie naturellement à l'ensemble $\mathbb{N}$ des entiers positifs.

[17] J'avoue ne pas avoir effectué cette vérification.

(iii) Soit $\mathbb{S}^2$ une sphère marquée de deux points antipodaux N et S. On définit une relation d'équivalence sur $\mathbb{S}^2$ en posant : xRy s'il existe une rotation ρ de la sphère fixant N et S telle que $y = \rho(x)$. Cette relation définit deux classes réduites à un point, à savoir $\{N\}$ et $\{S\}$, et toutes les autres classes sont infinies – ce sont des latitudes. L'ensemble quotient $\mathbb{S}^2/R$ peut être identifié à l'intervalle d'extrémités N et S, et la projection canonique $\mathbb{S}^2 \longrightarrow \mathbb{S}^2/R$ à la projection orthogonale de la sphère sur ce segment.

(iv) Sur l'ensemble E des paires d'entiers rationnels $(p, q) \in \mathbb{Z}^2$ tels que $q \neq 0$, la relation R définie par $(p, q)R(p', q')$ si $pq' = p'q$ est une relation d'équivalence. L'ensemble quotient s'identifie naturellement à l'ensemble $\mathbb{Q}$ des nombres rationnels.

(v) Pour un entier $n \geq 0$ et un corps $\mathbb{K}$, on définit une relation R sur $\mathbb{K}^{n+1} \setminus \{0\}$ (c'est-à-dire sur l'espace vectoriel $\mathbb{K}^{n+1}$ privé de l'origine) en posant : xRy s'il existe $\lambda \in \mathbb{K}^*$ tel que $x = \lambda y$. C'est une relation d'équivalence, et l'ensemble quotient $\mathbb{P}^n_{\mathbb{K}}$ est *l'espace projectif de dimension n sur le corps* $\mathbb{K}$. En particulier, $\mathbb{P}^0_{\mathbb{K}}$ est réduit à un point, $\mathbb{P}^1_{\mathbb{K}}$ est la *droite projective sur* $\mathbb{K}$, et $\mathbb{P}^2_{\mathbb{K}}$ le *plan projectif sur* $\mathbb{K}$.

(vi) Sur le plan euclidien $E = \mathbb{R}^2$, la relation R pour deux points d'être à distance de 0 ou 1 mètre l'un de l'autre est symétrique, réflexive et non transitive. Ce *n'est pas* une relation d'équivalence.

Sur la droite $\mathbb{R}$, la relation pour deux nombres x, y de satisfaire $x \leq y$ est réflexive, transitive et non symétrique. Ce *n'est pas* une relation d'équivalence.

3.2. Exemple fondamental pour l'arithmétique. Pour tout entier naturel $d > 0$, on définit pour $x, y \in \mathbb{Z}$ la relation «être congru modulo d» , ou «de congruence modulo d» , par

$$x \equiv y \pmod{d} \quad \text{lorsque} \quad d \quad \text{divise} \quad y - x.$$

On laisse au lecteur le soin de vérifier qu'il s'agit bien d'une relation d'équivalence sur $\mathbb{Z}$.

La classe d'un entier x est alors le sous-ensemble

$$[x]_d \;=\; \{y \in \mathbb{Z} \mid \text{il existe} \quad k \in \mathbb{Z} \quad \text{tel que} \quad y = x + kd\} \;=\; x + d\mathbb{Z}$$

de $\mathbb{Z}$. Le théorème 1.1 implique qu'il y a exactement d classes, c'est-à-dire que l'ensemble quotient contient exactement d éléments, ayant pour représentants (par exemple) les entiers $0, 1, \ldots, d-1$. On note cet ensemble quotient $\mathbb{Z}/d\mathbb{Z}$, ou parfois $\mathbb{Z}/d$.

Attention à l'écriture : $[x]_d \subset \mathbb{Z}$ et $[x]_d \in \mathbb{Z}/d\mathbb{Z}$! ! !

Dans le cas particulier où $d = 2$, un entier $x \in \mathbb{Z}$ est *pair* si $x \equiv 0 \pmod 2$ et *impair* si $x \equiv 1 \pmod 2$.

Exemples numériques :

$$[7]_{10} \;=\; \{\ldots, -13, -3, 7, 17, 27, \ldots\}\,, \quad [2]_{10} \;=\; \{\ldots, -18, -8, 2, 12, 22, \ldots\}\,,$$
$$[7]_5 \;=\; \{\ldots, -8, -3, 2, 7, 12, 17, \ldots\} \;=\; [7]_{10} \cup [2]_{10} \quad \text{(réunion disjointe)}.$$

3.3. Définitions. Soient E un ensemble, R une relation d'équivalence sur E et

$$\mu \,:\, E \times E \ni (x,y) \;\longmapsto\; x * y \in E$$

une loi de composition. La loi μ et la relation R sont dites *compatibles* si, pour x, x', y, y' dans E,

$$xRx' \quad \text{et} \quad yRy' \quad \text{impliquent} \quad (x*y)R(x'*y').$$

Lorsque c'est le cas, l'ensemble E/R est muni d'une loi de composition

$$E/R \times E/R \ni (C_x, C_y) \;\longmapsto\; C_{x*y} \in E/R$$

qui, à une paire de classes représentées par des éléments x et y, fait correspondre la classe de $x * y$; cette loi s'appelle le *quotient* de la loi $*$ par R.

3.4. Exemple fondamental. Soit d un entier strictement positif, comme à 3.2.

L'addition $\mathbb{Z} \times \mathbb{Z} \ni (x,y) \longmapsto x+y \in \mathbb{Z}$ est compatible avec la congruence modulo d. En d'autres termes, pour $x, x', y, y' \in \mathbb{Z}$:

$$x \equiv x' \pmod d \quad \text{et} \quad y \equiv y' \pmod d \quad \text{impliquent} \quad x+y \equiv x'+y' \pmod d$$

(comme on le vérifie immédiatement à partir des définitions). On appelle encore « addition » et on note « + » la loi de composition quotient sur l'ensemble quotient $\mathbb{Z}/d\mathbb{Z}$.

De même la mutliplication $\mathbb{Z} \times \mathbb{Z} \ni (x,y) \longmapsto xy \in \mathbb{Z}$ est compatible avec la congruence modulo d. En d'autres termes, pour $x, x', y, y' \in \mathbb{Z}$:

$$x \equiv x' \pmod d \quad \text{et} \quad y \equiv y' \pmod d \quad \text{impliquent} \quad xy \equiv x'y' \pmod d$$

(en effet, si $x' - x = kd$ et $y' - y = ld$ sont des multiples de d, alors $x'y' - xy = x'(y'-y) + (x'-x)y = (x'l + ky)d$ est aussi un multiple de d).

On appelle encore « multiplication » la loi de composition quotient sur l'ensemble quotient $\mathbb{Z}/d\mathbb{Z}$.

Exemples numériques. (i) Si $d = 6$, la relation de congruence modulo 6 a 6 classes que nous notons ici $[0]_6, [1]_6, [2]_6, [3]_6, [4]_6, [5]_6$ et qui sont donc les éléments de l'ensemble quotient $\mathbb{Z}/6$. (Bien distinguer : $[x]_6 \subset \mathbb{Z}$ et $[x]_6 \in \mathbb{Z}/6$.) Pour l'addition, on a par exemple

$$[3]_6 + [4]_6 \;=\; [1]_6 \qquad \text{et} \qquad [5]_6 + [5]_6 \;=\; [4]_6.$$

Pour la multiplication, on a par exemple

$$[3]_6[5]_6 \;=\; [3]_6 \qquad \text{et} \qquad [2]_6[3]_6 \;=\; [0]_6.$$

(ii) Notons $\{[0]_5, [1]_5, [2]_5, [3]_5, [4]_5\}$ les 5 classes de la relation de congruence modulo 5. La table de multiplication dans $\mathbb{Z}/5\mathbb{Z}$ est donnée par

$$\begin{array}{lllll}
[0]_5[0]_5 = [0]_5 & [0]_5[1]_5 = [0]_5 & [0]_5[2]_5 = [0]_5 & [0]_5[3]_5 = [0]_5 & [0]_5[4]_5 = [0]_5 \\
[1]_5[0]_5 = [0]_5 & [1]_5[1]_5 = [1]_5 & [1]_5[2]_5 = [2]_5 & [1]_5[3]_5 = [3]_5 & [1]_5[4]_5 = [4]_5 \\
[2]_5[0]_5 = [0]_5 & [2]_5[1]_5 = [2]_5 & [2]_5[2]_5 = [4]_5 & [2]_5[3]_5 = [1]_5 & [2]_5[4]_5 = [3]_5 \\
[3]_5[0]_5 = [0]_5 & [3]_5[1]_5 = [3]_5 & [3]_5[2]_5 = [1]_5 & [3]_5[3]_5 = [4]_5 & [3]_5[4]_5 = [2]_5 \\
[4]_5[0]_5 = [0]_5 & [4]_5[1]_5 = [4]_5 & [4]_5[2]_5 = [3]_5 & [4]_5[3]_5 = [2]_5 & [4]_5[4]_5 = [1]_5.
\end{array}$$

Nous reviendrons sur une différence importante entre les exemples (i) et (ii) : dans le premier cas, il existe des « diviseurs non nuls de zéro » : $[2]_6[3]_6 = [0]_6$; dans le second cas, il n'en existe pas : si $[x]_5 \neq [0]_5, [y]_5 \neq [0]_5$, alors $[x]_5[y]_5 \neq [0]_5$.

(iii) Un *carré parfait* est un entier $x \geq 0$ pour lequel il existe $y \in \mathbb{N}$ tel que $x = y^2$. Dans l'écriture usuelle (en base 10), le dernier chiffre d'un carré parfait ne peut être 2, 3, 7 ou 8. En effet, si $y = 10q + r$ avec $r \in \{0, 1, \ldots, 9\}$, alors $y^2 \equiv r^2 \pmod{10}$ et r^2 est congru modulo 10 à l'un de $0, 1, 4, 9, 6, 5$. [On peut s'économiser le calcul de r^2 pour $6 \leq r \leq 9$ en remarquant que $(10 - r)^2 \equiv r^2 \pmod{10}$.]

(iv) Le même genre d'argument montre que 7 853 683 n'est pas un carré parfait. En effet, si $y = 2q + r$ avec $r \in \{0, 1\}$, alors $y^2 \equiv r^2 \pmod{4}$ et r^2 est congru modulo 4 ou bien à 0 ou bien à 1. Comme $7\,853\,683 \equiv 83 \equiv 3 \pmod{4}$, la conclusion en résulte.

Ainsi, 8 968 n'est pas un carré parfait par (iii) et 6 137 586 n'est pas un carré parfait par (iv). Noter que (iii) ne permet aucune conclusion pour 6 137 586 et (iv) aucune conclusion pour 8 968.

A propos de (iii) et (iv), voir aussi l'exercice (VII.24).

3.5. Tests de divisibilité. Soit

$$x = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0$$

un nombre entier d'écriture décimale $a_k a_{k-1} \cdots a_0$.

On sait bien que x a la même parité que a_0, ce qui s'écrit $x \equiv a_0 \pmod{2}$; en particulier, x est divisible par 2 si et seulement si $a_0 \in \{0, 2, 4, 6, 8\}$. De même $x \equiv a_0 \pmod{5}$; en particulier, x est divisible par 5 si et seulement si $a_0 \in \{0, 5\}$. On laisse au lecteur le soin de formuler les conditions ad hoc pour la divisibilité de x par $4, 8, 16, \ldots$ et par $5, 125, \ldots$.

Voici quelques autres cas.

Divisibilité par 3. Comme $10 \equiv 1 \pmod{3}$, et donc $10^j \equiv 1 \pmod{3}$ pour tout entier $j \geq 0$, on voit que

$$x \equiv a_k + a_{k-1} + \cdots + a_0 \pmod{3}.$$

Par exemple $3 \mid 282$ car $282 \equiv (2 + 8 + 2) \equiv 12 \equiv 1 + 2 \equiv 0 \pmod{3}$, alors que $3 \nmid 283$ car $283 \equiv 1 \pmod{3}$.

Divisibilité par 9. Comme $10 \equiv 1 \pmod{9}$, et donc $10^j \equiv 1 \pmod{9}$ pour tout entier $j \geq 0$, on voit que

$$x \equiv a_k + a_{k-1} + \cdots + a_0 \pmod{9}.$$

Divisibilité par 11. Comme $10 \equiv -1 \pmod{11}$, et donc $10^j \equiv (-1)^j \pmod{11}$ pour tout entier $j \geq 0$, on voit que

$$x \equiv (-1)^k a_k + (-1)^{k-1} a_{k-1} + \cdots - a_1 + a_0 \pmod{11}.$$

Par exemple 949762 est divisible par 11, car $949762 \equiv -9 + 4 - 9 + 7 - 6 + 2 \equiv -11 \equiv 0 \pmod{11}$.

EXERCICE. Vérifier *de tête* (donc sans effectuer la division !) que $99 \mid 2\,411\,046$.

Divisibilité par 7, 11 et 13. Notons que $7 \times 11 \times 13 = 1001$ et que $1000 \equiv -1 \pmod{1001}$. Par suite

$$x \equiv (a_0 + 10a_1 + 100a_2) - (a_3 + 10a_4 + 100a_5) + - \cdots \pmod{1001}.$$

A fortiori

$$x \equiv (a_0 + 10a_1 + 100a_2) - (a_3 + 10a_4 + 100a_5) + \cdots \pmod{7};$$
$$x \equiv (a_0 + 10a_1 + 100a_2) - (a_3 + 10a_4 + 100a_5) + \cdots \pmod{11};$$
$$x \equiv (a_0 + 10a_1 + 100a_2) - (a_3 + 10a_4 + 100a_5) + \cdots \pmod{13}.$$

Par exemple, $59\,358\,208 \equiv (208 - 358 + 59) \pmod{1001} \equiv -91 \mod 1001$, de sorte que

$$59\,358\,208 \equiv 0 \pmod{7}$$
$$59\,358\,208 \equiv 0 \pmod{13}$$
$$59\,358\,208 \equiv -3 \not\equiv 0 \pmod{11}.$$

3.6. Preuve par 9. Pour un produit $xy = z$ de nombres entiers, la classe modulo 9 de z est égale au produit des classes modulo 9 de x et y, d'où une vérification des calculs numériques qu'on appelle «la preuve par 9» . Ainsi, pour le produit $239 \times 241 = 57\,599$, on vérifie bien que $5 \times 7 \equiv 8 \pmod{9}$. Cette «preuve» permet de déceler certaines erreurs, par exemple $239 \times 241 \neq 56\,599$, mais bien sur pas toutes ($239 \times 241 \neq 57\,509$ survit à la preuve par 9).

Remarque. La «preuve par deux» fonctionne aussi : elle dit précisément que le produit de deux nombres impairs est impair, et que tout autre produit est pair. On laisse au lecteur le soin de formuler une «preuve par trois» , une «preuve par cinq» et une «preuve par onze» .

Exercices du § VII.3

(VII.22) Soient m, n deux entiers strictement positifs.

(i) Vérifier que, pour deux matrices $s, t \in M_{m,n}(\mathbb{R})$, la relation d'être *semblables* (voir § III.5) est une relation d'équivalence.

(ii) Vérifier que, pour deux matrices $a, b \in M_n(\mathbb{R})$, la relation d'être *équivalentes* (voir § III.7) est une relation d'équivalence.

(iii) Dans $M_2(\mathbb{R})$, exhiber deux matrices semblables non conjuguées.

(VII.23) Vérifier que $366 \equiv 2 \pmod{7}$. Sachant que le 25 mars 2004 est un jeudi, en déduire quel jour de la semaine (lundi, mardi, ..., dimanche) était le 25 mars 2003.

De même pour $365 \equiv 1 \pmod{7}$ et le 25 mars 2005.

Remarque. Les calculs de «calendrier perpétuel» sont basés sur des considérations de ce type. Il faut prendre garde au fait que, dans le calendrier actuel (= grégorien), les années bissextiles sont les multiples de 4, sauf celles divisibles par 100 mais pas par 400. Ainsi, les années 1904, ..., 1996, 2000, 2004, ... sont bissextiles, alors que 1900, ..., 2001, 2002, 2003, 2005, ... ne le sont pas. Le pape Grégoire XIII adopta le calendrier actuel en date du vendredi 15 octobre 1582 (lendemain du jeudi ... 4 octobre 1582).

(VII.24) Pour $a \in \mathbb{Z}$, vérifier que $a^2 \equiv 0 \pmod 4$ si a est pair et $a^2 \equiv 1 \pmod 4$ si a est impair. En déduire que, pour tout entier de la forme $n = a^2 + b^2$, avec $a, b \in \mathbb{Z}$, on a $n \not\equiv 3 \pmod 4$.

Faire la liste de tous les nombres premiers p tels que $p \leq 100$ et $p \equiv 1 \pmod 4$, et vérifier que chacun d'eux est une somme de deux carrés parfaits.

[Un théorème de Fermat montre que *tout* nombre premier congru à 1 modulo 4 est une somme de deux carrés, et plus généralement qu'un nombre entier ≥ 2 dont la décomposition en facteurs premiers s'écrit $\prod p_i^{a_i}$ (où les p_i sont distincts deux à deux) est une somme de deux carrés si et seulement si l'exposant a_i est pair pour tout i tel que $p_i \equiv 3 \pmod 4$.

Exercice. Vérifier ceci pour n « petit » .]

(VII.25) On se propose d'explorer quels sont les entiers qui sont sommes de trois carrés.

(i) Pour $a \in \mathbb{Z}$ et $r \in \{0, 1, \ldots, 7\}$ tels que $a^2 \equiv r \pmod 8$, vérifier que $r \in \{0, 1, 4\}$.

(ii) Déduire de (i) que, pour tout entier de la forme $n = a^2+b^2+c^2$, avec $a, b, c \in \mathbb{Z}$, on a $n \not\equiv 7 \pmod 8$.

(iii) Soit n un entier de la forme $n = a^2 + b^2 + c^2$, avec $a, b, c \in \mathbb{Z}$, tel que $n \equiv 0 \pmod 4$. Vérifier que a, b et c sont tous pairs.

(iv)$^\sharp$ Déduire des pas précédents que, pour qu'un entier positif n soit somme de trois carrés, il faut qu'il ne soit pas de la forme $n = 4^k(8l + 7)$.

(v) Pour les entiers $n \leq 30$, vérifier que la condition de (iv$^\sharp$)est également suffisante.

[La condition de (iv$^\sharp$) est en fait suffisante : c'est un théorème de Gauss. Un théorème de Lagrange montre que tout entier positif est une somme de quatre carrés.

Exercice. Vérifier ces énoncés pour n « petit » .]

(VII.26) Montrer les congruences suivantes :

$$\begin{aligned} 2^{2n} - 1 &\equiv 0 \pmod 3 \\ 2^{3n} - 1 &\equiv 0 \pmod 7 \\ 2^{4n} - 1 &\equiv 0 \pmod{15} \\ n^3 &\equiv -1,\ 0 \text{ ou } 1 \pmod 9 \end{aligned}$$

pour tout $n \geq 0$.

(VII.27) Montrer que l'équation $x^3+2y^3 = 4z^3$ n'a aucune solution en nombres entiers non nuls, c'est-à-dire aucune solution $(x, y, z) \in (\mathbb{Z} \setminus \{0\})^3$.

[*Indication* : Vérifier d'abord que, s'il existait une solution (x, y, z), alors x, y, z seraient les trois pairs, et qu'on obtiendrait une autre solution $(x/2)^3 + 2(y/2)^3 = 4(z/2)^3$. Montrer que cela conduirait à une contradiction.]

Montrer plus généralement que, pour tout entier $n \geq 3$ et pour tout nombre premier p, l'équation $x^n + py^n = p^2z^n$ n'a aucune solution $(x, y, z) \in (\mathbb{Z} \setminus \{0\})^3$.

(VII.28) On se propose de montrer que la seule solution $(x, y, z) \in \mathbb{Z}^3$ de l'équation

$$x^2 + y^2 - 7z^2 = 0$$

est la solution banale $x = y = z = 0$, selon le schéma suivant.

(i) Pour tout $a \in \{0, 1, 2, 3, 4, 5, 6\}$, calculer $s \in \{0, 1, 2, 3, 4, 5, 6\}$ tel que $a^2 \equiv s \pmod 7$.

(ii) Soient $a, b \in \{0, 1, 2, 3, 4, 5, 6\}$ tels que $a^2 + b^2 \equiv 0 \pmod 7$. Montrer que $a \equiv b \equiv 0 \pmod 7$.

(iii) Soient $x, y \in \mathbb{Z}$ tels que $x^2 + y^2 - 7z^2 = 0$. Montrer qu'il existe $x', y', z' \in \mathbb{Z}$ tels que $x = 7x'$, $y = 7y'$, $z = 7z'$ et $x'^2 + y'^2 - 7z'^2 = 0$.

(iv) Montrer l'énoncé du début.

(VII.29) On pose $f(x) = x^5 - x^2 + x - 3$. Montrer que l'équation $f(x) = 0$ n'a pas de solution entière.

[*Indication* : Calculer $f(j)$ pour $j = -1, 0, 1, 2$, puis raisonner modulo 4.]

4. Anneaux et corps

Ce paragraphe est essentiellement terminologique. Le résultat important apparaît au théorème 4.7. Pour les notions de groupes et homomorphismes de groupes, voir le § IV.1 du semestre d'hiver.

4.1. Définition. Un *sous-groupe* H d'un groupe G est une partie de G telle que $1_G \in H$, $a \in H$ implique $a^{-1} \in H$ et $a, b \in H$ implique $ab \in H$.

Notation : « $H \leq G$ » pour « H est un sous-groupe de G » .

Exemples de sous-groupes. (i) Voici d'abord une suite de sous-groupe du groupe additif des nombres complexes : $d\mathbb{Z} \leq \mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$ (où d est un entier strictement positif) et trois suites de sous-groupes du groupe multiplicatif des nombres complexes non nuls : $\{1, -1\} \leq \mathbb{R}^* \leq \mathbb{C}^*$, et $\mathbb{R}_+^* \leq \mathbb{R}^* \leq \mathbb{C}^*$, ainsi que $\mu(d) \leq \{z \in \mathbb{C} \,|\, |z| = 1\} \leq \mathbb{C}^*$ (comme à l'exercice IV.1, $\mu(d)$ désigne ici le groupe des racines d-ièmes de l'unité).

(ii) Les groupes symétriques (voir § IV.2) fournissent plusieurs exemples, dont $\mathrm{Sym}(n) \leq \mathrm{Sym}(n + 1)$. Il y a plusieurs inclusions possibles ; préciser !

(iii) Tout sous-groupe de $\mathbb{Z}$ est de la forme $d\mathbb{Z}$ (voir la proposition 1.13).

Le groupe $GL(n,\mathbb{R})$[18] possède un sous-groupe noté $SL(n,\mathbb{R})$ formé des matrices de déterminant 1, un sous-groupe noté $O(n)$ formé des matrices orthogonales, un sous-groupe formé des matrices diagonales (et bien d'autres sous-groupes).

(iv) Si G est un groupe et $g \in G$ un élément, l'ensemble des puissances g^n ($n \in \mathbb{Z}$) constitue un sous-groupe de G. (Attention : ces puissances peuvent être distinctes deux à deux, comme c'est le cas pour $g = 2$ et $G = \mathbb{C}^*$, ou non, comme c'est le cas pour $g = i$ et le même groupe $G = \mathbb{C}^*$.)

(v) Tout groupe G a deux sous-groupes « évidents » : $\{1\} \leq G$ et $G \leq G$.

Nous répétons aussi la définition de « anneau », déjà introduite en prologue au chapitre V.

4.2. Définitions. Un *anneau* est un ensemble A muni de deux opérations internes, une *addition* et une *multiplication,* satisfaisant les propriétés suivantes :

(i) avec l'addition, A est un groupe commutatif (et on note toujours 0 l'élément neutre correspondant),

(ii) la multiplication est associative ($(ab)c = a(bc)\ \forall\ a,b,c \in A$), et possède un élément neutre[19] noté 1 ($1a = a1 = a\ \forall\ a \in A$),

(iii) de plus $(a+b)c = ac + bc$ et $a(b+c) = ab + ac\ \forall\ a,b,c \in A$ (distributivité).

L'anneau est *commutatif* si de plus $ab = ba$ pour tous $a, b \in A$.

Si A et A' sont deux anneaux, un *homomorphisme d'anneaux* est une application $\phi : A \longrightarrow A'$ telle que[20] :

$$\begin{aligned} \phi(a+b) &= \phi(a) + \phi(b) \quad \text{et} \quad \phi(0_A) = 0_{A'} \\ \phi(ab) &= \phi(a)\phi(b) \quad \text{et} \quad \phi(1_A) = 1_{A'} \end{aligned}$$

pour tous $a, b \in A$. Le *noyau* d'un tel homomorphisme d'anneaux est son noyau comme homomorphisme de groupes additifs, c'est-à-dire l'image inverse $\phi^{-1}(0_{A'})$ du zéro de l'anneau but. [Dans la pratique, on écrit 0 pour 0_A et $0_{A'}$, indifféremment ; de même pour $1 = 1_A = 1_{A'}$.]

Exemples d'anneaux. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des anneaux pour les opérations usuelles. L'anneau de tous les endomorphismes linéaires d'un espace vectoriel est un anneau pour la somme et la composition des endomorphismes.

---

[18] La notation $GL(n,\mathbb{R})$ a été introduite au § IV.1.

[19] En algèbre, presque tous les auteurs imposent aux anneaux d'avoir une telle *unité*. L'usage est toutefois différent sur ce point en analyse où, par exemple, l'ensemble $\mathcal{C}_0(\mathbb{R})$ des fonctions continues $f : \mathbb{R} \longrightarrow \mathbb{R}$ telles que $\lim_{|t|\to\infty} f(t) = 0$ est un « anneau » SANS unité. Notons que $\mathcal{C}_0(\mathbb{R})$ se plonge naturellement dans l'anneau (avec unité !) des fonctions continues $f : \mathbb{R} \longrightarrow \mathbb{R}$ telles que $\lim_{t\to\infty} f(t)$ et $\lim_{t\to-\infty} f(t)$ existent et sont égales.

[20] La condition $\phi(0_A) = 0_{A'}$ résulte des autres ; en effet $\phi(a) = \phi(a + 0_A) = \phi(a) + \phi(0_A)$ implique $\phi(0_A) = 0_{A'}$. En revanche, la condition $\phi(1_A) = 1_{A'}$ ne peut être omise, comme le montre l'exemple de l'application $\phi : \mathbb{R} \longrightarrow M_2(\mathbb{R})$ définie par $\phi(a) = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$.

4.3. Exemple d'anneau fondamental pour l'arithmétique : les entiers modulo d. Pour tout entier $d \geq 1$, l'ensemble $\mathbb{Z}/d\mathbb{Z}$ des classes modulo d est naturellement un anneau.

Répétons que l'addition est bien définie dans $\mathbb{Z}/d\mathbb{Z}$ puisque, pour $m, n \in \mathbb{Z}$, la classe $[m+n]_d$ de $m+n$ modulo d ne dépend que des classes modulo d de m et n (n^o 3.5) ; on a donc $[m]_d + [n]_d = [m+n]_d$. Il en est de même pour la multiplication : $[m]_d[n]_d = [mn]_d$.

Il faut bien sûr *vérifier* que ces opérations possèdent les propriétés de la définition et font de $\mathbb{Z}/d\mathbb{Z}$ un anneau ; il s'agit là de vérifications de routine que nous ne détaillons pas (comme déjà dit au numéro 3.4).

4.4. Exemples d'homomorphismes d'anneaux : les homomorphismes canoniques de réduction modulo d.

(i) Pour tout entier $d \geq 2$, l'application $\phi_d : \mathbb{Z} \longrightarrow \mathbb{Z}/d\mathbb{Z}$ qui applique un entier n sur sa classe $[n]_d$ est un homomorphisme d'anneaux, de noyau $d\mathbb{Z}$.

Par exemple, si $d = 2$, cet homomorphisme applique tous les entiers pairs sur l'élément neutre pour l'addition (le 0) du groupe $\mathbb{Z}/2\mathbb{Z}$ et tous les entiers impairs sur l'autre élément de $\mathbb{Z}/2\mathbb{Z}$.

(ii) Pour des entiers $c, d \geq 2$ tels que $d \mid c$, l'application $\pi : \mathbb{Z}/c\mathbb{Z} \longrightarrow \mathbb{Z}/d\mathbb{Z}$ qui applique la classe modulo c d'un entier sur la classe modulo d de cet entier est un homomorphisme d'anneaux[21] , dont le noyau est formé des classes $[0]_c$, $[d]_c$, $[2d]_c$, …, $[c-d]_c$. Par exemple, si $d = 2$ et $c = 4$, l'image de $[0]_4$ (respectivement $[1]_4$, $[2]_4$, $[3]_4$) est $[0]_2$ (respectivement $[1]_2$, $[0]_2$, $[1]_2$).

(iii) Pour l'homomorphisme $\phi_9 : \mathbb{Z} \longrightarrow \mathbb{Z}/9\mathbb{Z}$ de réduction modulo 9 et un entier $n = \sum_{j=0}^{k} a_j (10)^j \in \mathbb{Z}$ (avec $a_0, \ldots, a_k \in \{0, \ldots, 9\}$), nous avons $\phi_9(n) = \phi_9\left(\sum_{j=0}^{k} a_j\right)$; ceci est à la base de la « preuve par 9 » (voir le numéro 3.6).

(iv) Pour l'homomorphisme $\phi_{11} : \mathbb{Z} \longrightarrow \mathbb{Z}/(11\mathbb{Z})$ de réduction modulo 11 et n comme ci-dessus, nous avons $\phi_{11}(n) = \phi_{11}\left(\sum_{j=0}^{k} (-1)^j a_j\right)$.

4.5. Définition. Un anneau commutatif A est un *corps* s'il n'est pas réduit à $\{0\}$ et si tout élément $a \neq 0$ dans A possède un *inverse* a^{-1} tel que $aa^{-1} = a^{-1}a = 1$, c'est-à-dire si l'ensemble de ses éléments non nuls est un groupe pour la multiplication.

---

[21] Il faut bien sûr d'abord vérifier que l'application π est bien définie. Ensuite, pour vérifier que π est un homomorphisme d'anneaux, on peut procéder comme suit. Soient $\xi, \eta \in \mathbb{Z}/c\mathbb{Z}$. Choisissons x et y dans $\mathbb{Z}$ tels que $\xi = [x]_c$ et $\eta = [y]_c$. Alors $\pi(\xi) = [x]_d$ et $\pi(\eta) = [y]_d$. Par suite

$$\pi(\xi + \eta) \;=\; \pi([x+y]_c) \;=\; [x+y]_d \;=\; [x]_d + [y]_d \;=\; \pi(\xi) + \pi(\eta).$$

Des vérifications analogues montrent que $\pi(\xi\eta) = \pi(\xi)\pi(\eta)$ et $\pi([1]_c) = [1]_d$.

4.6. Lemme. *On considère un entier $d \geq 2$ et un entier $a \in \mathbb{Z}$. Pour que $[a]_d$ soit inversible dans l'anneau $\mathbb{Z}/d\mathbb{Z}$, il faut et il suffit que a et d soient premiers entre eux.*

Preuve. Supposons d'abord que $[a]_d$ possède un inverse dans $\mathbb{Z}/d\mathbb{Z}$, c'est-à-dire qu'il existe $b \in \mathbb{Z}$ tel que $[a]_d[b]_d = [1]_d$. En d'autres termes, il existe $k \in \mathbb{Z}$ tel que $ab + kd = 1$; par suite a et d sont premiers entre eux.

Réciproquement, si a et d sont premiers entre eux, il existe en vertu du théorème de Bézout deux entiers b et k tels que $ab + kd = 1$, et par suite $[b]_d = ([a]_d)^{-1} \in \mathbb{Z}/d\mathbb{Z}$. □

4.7. Théorème. *Pour un entier $d \geq 2$, l'anneau $\mathbb{Z}/d\mathbb{Z}$ est un corps si et seulement si d est premier.*

Preuve. L'anneau $\mathbb{Z}/d\mathbb{Z}$ est un corps si et seulement si tous ses éléments non nuls sont inversibles, donc si et seulement si $[a]_d$ est inversible pour tout $a \in \{1, \ldots, d-1\}$, ou encore (vu le lemme) si et seulement si d est premier. □

4.8. Notation. Pour tout nombre premier p, on note $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$ à p éléments.

(On dit « le » corps, car il n'est pas difficile de montrer que tout corps à p éléments est canoniquement isomorphe à $\mathbb{F}_p$.)

4.9. Mise en garde. Pour tout premier p et pour tout entier $n \geq 2$, il existe un corps à p^n éléments (voir un chapitre suivant de ce cours). Mais l'anneau $\mathbb{Z}/p^n\mathbb{Z}$, lui aussi à p^n éléments, n'est pas un corps, puisqu'il contient p^{n-1} éléments non inversibles, et donc $p^{n-1} - 1 \geq 1$ éléments non nuls non inversibles.

Ci-dessus, étant donné un entier $d \geq 2$, on a soigneusement observé la différence de notations pour un entier $n \in \mathbb{Z}$ et sa classe $[n]_d \in \mathbb{Z}/d\mathbb{Z}$. Toutefois, comme les éléments de l'anneau quotient $\mathbb{Z}/d\mathbb{Z}$ ont des représentants entiers canoniques $0, 1, \ldots, d-1$, on écrit souvent des formules du type $3 \in \mathbb{F}_5$ ou $3 \in \mathbb{Z}/9\mathbb{Z}$. Il faut toutefois *bien distinguer* le sens du « 3 » dans des expressions $3 \in \mathbb{F}_5$, $3 \in \mathbb{Z}/9\mathbb{Z}$ et $3 \in \mathbb{Z}$!

4.10. Théorème (Wilson). *Pour tout nombre premier p, on a*

$$(p-1)! \equiv -1 \pmod{p}.$$

Indication pour la preuve (exercice).

(i) Vérifier le théorème pour $p = 2$ et $p = 3$; ceci fait, on suppose $p \geq 5$.

(ii) Soient $x, y \in \{1, \ldots, p-1\}$ tels que $xy \equiv 1 \pmod{p}$; alors $x = y$ si et seulement si $x = 1$ ou $x = p - 1$.

(iii) Montrer que $2 \times 3 \times \cdots \times (p-2) \equiv 1 \pmod{p}$. [Grouper les termes par paires.]

(iv) Constater l'égalité $1 \times (p-1) \equiv -1 \pmod{p}$. □

4.11. Remarques et exercices.

(i) Pour un entier $n \geq 2$, montrer que $(n-1)! \equiv -1 \pmod{n}$ si et *seulement si* n est premier.

Indication pour la preuve. Supposons que $n = qd$ avec $1 < q < n$. Alors q est un facteur qui intervient dans $(n-1)!$, de sorte que $(n-1)! \equiv 0 \pmod{q}$. Si on avait $(n-1)! \equiv -1 \pmod{n}$, on aurait a fortiori $(n-1)! + 1 \equiv 0 \pmod{q}$, exclu par ce qui précède.

(ii) Vu de la remarque précédente, le théorème de Wilson fournit un test pour la primalité d'un nombre entier, mais aucune indication pour les facteurs d'un nombre non premier !

(iii) Soit $n > 1$ un nombre qui n'est pas premier. Si $n \neq 4$, préciser l'affirmation de la remarque (i) en montrant que $(n-1)! \equiv 0 \pmod{n}$.

4.12. Formule pour p_n. Ce numéro a pour but d'évoquer la formule (par ailleurs parfaitement inutile pour tout calcul pratique) pour le n-ième nombre premier p_n, déjà évoquée au numéro (VII.20).

Pour tout entier $j \geq 1$, on pose

$$F(j) \;=\; \left[\cos^2\left(\pi\,\frac{(j-1)!+1}{j}\right)\right]$$

où [...] désigne une partie entière. Vérifier que $F(j) = 1$ si $j = 1$ ou si j est premier, et $F(j) = 0$ sinon. Par suite,

$$\pi(x) \;=\; \sum_{j=2}^{x} F(j)$$

où $\pi(x)$ désigne (comme au numéro 2.15) le nombre des nombres premiers inférieurs ou égaux à x. Pour tout entier $n \geq 1$, on peut montrer que

$$p_n \;=\; 1 \,+\, \sum_{m=1}^{2^n} \left[\left(\frac{n}{\sum_{j=1}^{m} F(j)}\right)^{1/n}\right].$$

définit le n-ième nombre premier. [Vérifier cette affirmation pour $n = 1$, $n = 2$, et (pour le lecteur tout à fait courageux) $n = 3$.]

Pour en savoir plus, voir le chapitre 3 du « Book of prime number records » de P. Ribenboim, déjà cité.

4.13. Points d'étymologie. L'introduction du mot « corps » , ou plutôt des mots « Körper » et « Zahlkörper » , remonte à 1870, dans le « Supplemente » (= appendice) de Dedekind à l'ouvrage « Zahlentheorie » de Dirichlet (§ 159, 3e édition). D'après le « Lehrbuch der Algebra » (volume 1, page 491) de Weber[22], le terme est censé suggérer une union d'objets fortement liés entre eux (= Körper).

Le mot « anneau » , ou plutôt les mots « Ring » et « Zahlring », apparaissent dans « Die Theorie der algebraischen Zahlkörper » de D. Hilbert (Jahresbericht der DMV, 1894–1895, § 31, page 237). Le terme est probablement censé suggérer également quelque chose de similaire au terme de corps (« Ring » = anneau). Voir également le Lehrbuch der Algebra (volume 2, page 351).

[22] H. Weber, Lehrbuch der Algebra, 3 volumes (3e éd., Chelsea). Le premier volume de la première édition a paru en 1895.

Exercices du § VII.4.

(VII.30) Ecrire les tables de multiplication des corps $\mathbb{F}_2$, $\mathbb{F}_3$, $\mathbb{F}_5$.

(VII.31) Pour tout entier $a \in \{1,2,3,4,5,6\}$, calculer $b, c \in \{1,2,3,4,5,6\}$ tels que $([b]_7)^2 = [a]_7$ et $[c]_7 = ([a]_7)^{-1}$.

(VII.32) Calculer les puissances de 2 modulo 3, de 2 modulo 5, de 3 modulo 7, de 2 modulo 11, de 2 modulo 13 et de 3 modulo 17.

Qu'en déduisez-vous sur la nature du groupe multiplicatif des éléments non nuls dans $\mathbb{F}_p$?

[On sait que, pour tout premier p, il existe un entier g_p dont les puissances $(g_p)^j$ modulo p pour $1 \leq j \leq p-1$ représentent tout les éléments non nuls de $\mathbb{F}_p$. On a quelques renseignements sur la plus petite valeur de g_p possible ; par exemple : $g_{23} = 5$, $g_{41} = 6$, ou $g_{191} = 19$. Pour en savoir plus, voir le paragraphe 2.II.A du livre de P. Ribenboim, « The book of prime number records » , déjà cité.]

(VII.33) Soit m un nombre entier, $m \geq 2$. On peut montrer [23] que le groupe $\mathcal{U}(\mathbb{Z}/m\mathbb{Z})$ des éléments inversibles de l'anneau $\mathbb{Z}/m\mathbb{Z}$ est cyclique si et seulement si m est ou bien une puissance d'un nombre premier impair, ou bien le double d'une puissance d'un nombre premier impair, ou bien l'un des nombres 2, 4.

Vérifier cet énoncé pour les nombres composés $m \leq 14$.

(VII.34) Soient p un nombre premier, n un nombre entier positif et V un espace vectoriel de dimension n sur $\mathbb{F}_p$. Combien l'ensemble V a-t-il d'éléments ?

(VII.35) Enoncer les définitions de *sous-anneau* et *sous-corps.* Vérifier que

$$\left\{ z \in \mathbb{C} \,\middle|\, \text{il existe } a, b \in \mathbb{Z} \text{ tel que } z = \frac{a + b\sqrt{5}}{2} \right\}$$

et un sous-anneau de $\mathbb{C}$ et que

$$\left\{ z \in \mathbb{C} \,\middle|\, \text{il existe } x, y \in \mathbb{Q} \text{ tel que } z = x + y\sqrt{5} \right\}$$

est un sous-corps de $\mathbb{C}$. Pour $x, y \in \mathbb{Q}$ non tous les deux nuls, trouver $x', y' \in \mathbb{Q}$ tels que $x' + y'\sqrt{5} = (x + y\sqrt{5})^{-1}$.

(VII.36) Soit $\mathcal{A}$ l'ensemble des nombres réels x pour lesquels il existe des entiers $a, b, c \in \mathbb{Z}$ (dépendant de x) tels que $x = a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2$. Soit $\mathcal{B}$ l'ensemble des nombres réels y pour lesquels il existe des entiers $d, e, f \in \mathbb{Z}$ (dépendant de y) tels que $y = d + e\pi + f\pi^2$ (où $\pi = 3,14159\cdots$).

$\mathcal{A}$ est-il un sous-anneau de $\mathbb{R}$? $\mathcal{B}$ est-il un sous-anneau de $\mathbb{R}$?

[23] Voir par exemple le théorème 6.11 du livre de Jones et Jones cité en début de chapitre.

(VII.37) Vérifier que l'élévation à une puissance définit sur les entiers positifs une opération qui n'est ni commutative ni associative.

[*Indication* : calculer 3^5, 5^3, $(((2^2)^2)^2)^2$ et $2^{(2^{(2^2)})}$.]

5. Fonction d'Euler, théorèmes de Fermat et Euler

Le résultat central de ce paragraphe est le théorème 5.7.

5.1. Définition. La *fonction d'Euler* associe à tout entier $m \geq 1$ le nombre $\varphi(m)$ des entiers k qui sont premiers à m et tels que $1 \leq k \leq m$; par définition, $\varphi(1) = 1$.

De manière équivalente (lemme 4.6), $\varphi(m)$ est l'ordre[24] du groupe abélien multiplicatif

$$\mathcal{U}(\mathbb{Z}/m\mathbb{Z}) = \{\, [k]_m \in \mathbb{Z}/m\mathbb{Z} \mid [k]_m \quad \text{est inversible} \,\}.$$

Exemples. $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$, $\varphi(7) = 6$, $\varphi(8) = 4$; pour tous nombre premier p et nombre naturel $a \geq 1$, on a $\varphi(p^a) = p^{a-1}(p-1)$.

5.2. Produits d'anneaux. Soient $A_1, \ldots, A_n$ des anneaux. L'ensemble produit

$$A_1 \times \cdots \times A_n$$

muni de l'addition et de la multiplication définies composante par composante est un anneau.

Si, pour tout $j \in \{1, \ldots, n\}$, l'anneau A_j est fini et si $|A_j|$ désigne son ordre, alors $A_1 \times \cdots \times A_n$ est fini d'ordre $|A_1| \times \cdots \times |A_n|$.

5.3. Théorème chinois. *Soient $a_1, \ldots, a_n$ des entiers ≥ 2 deux à deux premiers entre eux. Alors l'application canonique*

$$\psi : \begin{cases} \mathbb{Z}/(a_1 \cdots a_n\mathbb{Z}) & \longrightarrow & \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_n\mathbb{Z} \\ [k]_{a_1 \cdots a_n} & \longmapsto & ([k]_{a_1}, \ldots, [k]_{a_n}) \end{cases}$$

est un isomorphisme d'anneaux.

Exemples. Les applications

$$\begin{cases} \mathbb{Z}/(12\mathbb{Z}) & \longrightarrow & \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \\ [k]_{12} & \longmapsto & ([k]_3, [k]_4) \end{cases} \quad \text{et} \quad \begin{cases} \mathbb{Z}/(60\mathbb{Z}) & \longrightarrow & \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \\ [k]_{60} & \longmapsto & ([k]_3, [k]_4, [k]_5) \end{cases}$$

sont des isomorphismes d'anneaux, alors que

$$\phi : \begin{cases} \mathbb{Z}/(900\mathbb{Z}) & \longrightarrow & \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z} \\ [k]_{900} & \longmapsto & ([k]_6, [k]_{10}, [k]_{15}) \end{cases}$$

n'en est pas un, par exemple parce que $\phi([30]_{900}) = \phi([60]_{900}) = ([0]_6, [0]_{10}, [0]_{15})$.

Dans le théorème 5.3, on ne peut donc pas remplacer « deux à deux premiers entre eux » par « premiers entre eux ».

[24] Rappel : l'ordre d'un ensemble (ici d'un groupe fini) est le nombre de ses éléments. En français, il y a des mots *homographes* qui ont même forme écrite, même prononciation, mais des sens différents : le *vol* de l'aigle et celui du voleur, la *page* d'un livre et le *page* du roi, la *grève* d'un lac et celle des ouvriers, ... [Il se peut bien sûr que l'étymologie révèle une filiation de sens, comme dans le cas de « grève » .] En mathématiques également, il y a des mots qui ont plusieurs sens à ne pas confondre ; les mots « ordre » et « anneau » en fournissent deux exemples.

5.4. Lemme. *Soient $a, b, k \in \mathbb{Z}$ avec a, b premiers entre eux. Si $a \mid k$ et $b \mid k$, alors $ab \mid k$.*

De même, pour $a_1, \ldots, a_n, k \in \mathbb{Z}$ avec $a_1, \ldots, a_n$ deux à deux premiers entre eux : si $a_j \mid k$ pour tout $j \in \{1, \ldots, n\}$, alors $\prod_{j=1}^{n} a_j$ divise k.

Preuve du lemme. Montrons la seconde assertion par récurrence sur n.

Supposons d'abord $n = 2$ (il s'agit de la première assertion !). Par hypothèse, il existe $x, y \in \mathbb{Z}$ tels que $k = a_1 x = a_2 y$. Comme a_2 divise x par la proposition 1.10, il existe $z \in \mathbb{Z}$ tel que $x = a_2 z$; ainsi $k = a_1 a_2 z$.

Supposons ensuite $n \geq 3$, et le lemme montré jusqu'à $n-1$. L'hypothèse du lemme et la proposition 1.10 impliquent que $\prod_{i=1}^{n-1} a_i$ et a_n sont premiers entre eux. L'hypothèse de récurrence implique alors qu'il existe $x, y \in \mathbb{Z}$ tels que $k = \left(\prod_{i=1}^{n-1} a_i\right) x = a_n y$. Comme a_n divise x par la proposition 1.10, il existe $z \in \mathbb{Z}$ tel que $k = \left(\prod_{i=1}^{n-1} a_i\right) a_n z$. □

Preuve du théorème 5.3. Le lecteur vérifiera à titre d'exercice que l'application ψ est bien un homomorphisme d'anneaux. Il reste donc à montrer que l'application ψ est injective et surjective. Comme la source et le but de cette application sont des ensembles finis de même ordre, à savoir d'ordre $a_1 \cdots a_n$, il suffit de montrer que ψ est injective. Pour cela, il suffit [25] de vérifier que le noyau de π (= l'image inverse $\pi^{-1}(0)$ de zéro) est réduit à zéro.

Soit $k \in \mathbb{Z}$ tel que l'élément $[k]_{a_1 \cdots a_n}$ soit dans le noyau de ψ. On a donc $k \equiv 0 \pmod{a_i}$, ou encore $a_i \mid k$, pour tout $i \in \{1, \ldots, n\}$. Il résulte du lemme 4 que $a_1 \cdots a_n \mid k$, donc que $[k]_{a_1 \cdots a_n} = 0$. Le noyau de ψ est donc bien réduit à zéro. □

5.5. Reformulation de la surjectivité de ψ. *Soient $a_1, \ldots, a_n$ des entiers ≥ 2 deux à deux premiers entre eux. Pour tous $k_1, \ldots, k_n \in \mathbb{Z}$, les équations*

$$\begin{aligned} x &\equiv k_1 \pmod{a_1} \\ &\cdots\cdots \\ x &\equiv k_n \pmod{a_n} \end{aligned}$$

ont une solution commune $x \in \mathbb{Z}$.

Autre preuve de la reformulation. Bien que cet énoncé résulte *immédiatement* du théorème 5.3, offrons ici une *autre* preuve.

Cas $n = 2$. Il s'agit de résoudre le système des deux équations

$$x \equiv k_1 \pmod{a_1} \qquad \text{et} \qquad x \equiv k_2 \pmod{a_2}.$$

Or il existe $y, z \in \mathbb{Z}$ tels que $a_1 y + a_2 z = 1$ (théorème de Bézout). Posons $x = k_1 a_2 z + k_2 a_1 y$. Comme $a_2 z \equiv 1 \pmod{a_1}$, on a bien $x \equiv k_1 \pmod{a_1}$; de même, $x \equiv k_2 \pmod{a_2}$.

[25] En effet, un homomorphisme de groupes $\pi : A \longrightarrow A'$ est injectif si et seulement si $\pi^{-1}(0) = \{0\}$. La preuve est en tout point analogue à celle du résultat correspondant pour les applications linéaires entre espaces vectoriels (voir le semestre d'hiver).

Cas de n quelconque. On pose $a = a_1 a_2 \cdots a_n$ et $b_j = a/a_j$ pour $j \in \{1, \ldots, n\}$, de sorte que a_j et b_j sont premiers entre eux. Pour chaque j, il existe un entier x_j tel que

$$b_j x_j \equiv k_j \pmod{a_j}.$$

[En effet, il existe $y_j, z_j \in \mathbb{Z}$ tels que $a_j y_j + b_j z_j = 1$ par le théorème de Bézout. Donc $a_j y_j k_j + b_j z_j k_j = k_j$, et $b_j(z_j k_j) \equiv k_j \pmod{a_j}$, de sorte que $x_j = z_j k_j$ convient.] On pose alors

$$x = b_1 x_1 + \cdots + b_n x_n.$$

Pour tout $j \in \{1, \ldots, n\}$, on a $b_i \equiv 0 \pmod{a_j}$ dès que $i \neq j$, et par suite $x \equiv k_j \pmod{a_j}$. □

Remarque. Le nom de «théorème chinois» vient de ce qu'il existe des solutions d'équations comme dans la reformulation dans d'anciens textes chinois. Ces textes n'ont pas d'équivalent de la formulation du théorème 5.3 ci-dessus !

Exemple. La solution de $x \equiv 1 \pmod 2$, $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$ s'obtient comme suit, en suivant la méthode de la preuve ci-dessus.

On considère d'abord les équations

$$\begin{aligned} 15x_1 &\equiv 1 \pmod 2, \\ 10x_2 &\equiv 2 \pmod 3 \\ 6x_3 &\equiv 3 \pmod 5. \end{aligned}$$

On en trouve des solutions : $x_1 = 1$, $x_2 = 2$ et $x_3 = 3$. Puis on calcule

$$x = 15 \times 1 + 10 \times 2 + 6 \times 3 = 53.$$

On constate que la solution générale s'écrit $x = 53 + 30\,l$, avec $l \in \mathbb{Z}$. Le résultat s'écrit plus volontiers : $x = 23 + 30\,l$, avec $l \in \mathbb{Z}$.

5.6. Proposition.

(i) *Soit m, n des entiers positifs premiers entre eux. Alors*

$$\varphi(mn) = \varphi(m)\varphi(n).$$

(ii) *Pour tout entier $m \geq 2$, on a*

$$\varphi(m) = m \prod_{p \mid m} \left(1 - \frac{1}{p}\right)$$

$$m = \sum_{d \mid m} \varphi(d)$$

où le produit est pris sur tous[26] *les nombres premiers divisant m et la somme sur tous*[27] *les entiers positifs divisant m.*

[26] Y compris $p = m$ au cas où m est premier.
[27] Y compris $d = 1$ et $d = m$.

Exemples pour les formules de (ii). Si p est un nombre premier, on retrouve

$$\varphi(p) \;=\; p\left(1-\frac{1}{p}\right) = p-1, \quad \varphi(p^2) \;=\; p^2-p, \quad \text{etc.}$$

Les diviseurs premiers de 60 sont 2, 3 et 5, de sorte que

$$\varphi(60) = 60(1-\frac{1}{2})(1-\frac{1}{2})(1-\frac{1}{5}) \;=\; 16.$$

Les diviseurs de 12 sont 1, 2, 3, 4, 6, et 12, de sorte que

$$12 \;=\; \varphi(1)+\varphi(2)+\varphi(3)+\varphi(4)+\varphi(5)+\varphi(12) \;=\; 1+1+2+2+2+4.$$

Preuve. L'assertion (i) résulte du théorème chinois et du fait suivant : si A_1, A_2 sont des anneaux, le groupe des éléments inversibles du produit d'anneaux $A_1 \times A_2$ s'identifie au produit des groupes des éléments inversibles de A_1 et A_2.

Pour l'assertion (ii), on écrit la décomposition en nombres premiers $m = p_1^{a_1}\cdots p_k^{a_k}$, avec des premiers distincts $p_1, \ldots, p_k$ et des entiers $a_1, \ldots, a_k \geq 1$. On a d'abord

$$\varphi(m) \;=\; \prod_{1\leq i\leq k} \varphi(p_i^{a_i}) \;=\; \prod_{1\leq i\leq k} p_i^{a_i}\left(1-\frac{1}{p_i}\right) \;=\; m\prod_{p|m}\left(1-\frac{1}{p}\right),$$

où la première égalité résulte de (i).

Les diviseurs positifs de m sont précisément les entiers de la forme $p_1^{b_1}\cdots p_k^{b_k}$, avec $b_1 \in \{0,\ldots,a_1\}$, …, $b_k \in \{0,\ldots,a_k\}$. En utilisant (i), on a donc ensuite

$$\begin{aligned}
\sum_{d|m}\varphi(d) \;&=\; \sum_{0\leq b_i\leq a_i} \varphi\left(p_1^{b_1}\cdots p_k^{b_k}\right) \;=\; \sum_{0\leq b_i\leq a_i} \varphi\left(p_1^{b_1}\right)\cdots\varphi\left(p_k^{b_k}\right) \\
&=\; \prod_{1\leq i\leq k}\Big(1 \;+\; \varphi(p_i) \;+\; \varphi(p_i^2) \;+\; \cdots \;+\; \varphi(p_i^{a_i})\Big) \\
&=\; \prod_{1\leq i\leq k}\Big(1 \;+\; (p_i-1) \;+\; (p_i^2-p_i) \;+\; \cdots \;+\; (p_i^{a_i}-p_i^{a_i-1})\Big) \\
&=\; \prod_{1\leq i\leq k} p_i^{a_i} \;=\; m. \qquad \square
\end{aligned}$$

Autre preuve (esquisse !) de la formule.

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

Pour qu'un entier $k \in \{1,2,\ldots,m\}$ soit premier à m, il faut et il suffit qu'aucun des diviseurs premiers de m ne divise k.

Soit $p_1, \ldots, p_N$ la liste des diviseurs premiers de m. Posons

$$\mathcal{P}_a \;=\; \{k\in\mathbb{N} \;\mid\; 1\leq k\leq m \quad \text{et} \quad p_a|k\} \qquad (a=1,\ldots,N).$$

L'ensemble

$$\{1,2,\ldots,m\} \;-\; \bigcup_{1\leq a\leq N}\mathcal{P}_a,$$

des entiers $k \in \{1, 2, \dots, m\}$ premiers à m est de cardinal

$$m - \sum_{1\le a\le N} |\mathcal{P}_a| + \sum_{1\le a<b\le N} |\mathcal{P}_a \cap \mathcal{P}_b| - \sum_{1\le a<b<c\le N} |\mathcal{P}_a \cap \mathcal{P}_b \cap \mathcal{P}_c| \pm \cdots$$

où $|Q|$ désigne le cardinal d'un ensemble fini Q. Par suite

$$\begin{aligned}\varphi(m) &= m - \sum_{1\le a\le N} \frac{m}{p_a} + \sum_{1\le a<b\le N} \frac{m}{p_a p_b} - \sum_{1\le a<b<c\le N} \frac{m}{p_a p_b p_c} \pm \cdots \\ &= m \prod_{1\le a\le N} \left(1 - \frac{1}{p_a}\right).\end{aligned}$$

Cette preuve illuste le *principe d'inclusion-exclusion* : le cardinal de l'ensemble $\bigcup_{1\le a\le N} \mathcal{P}_a$, est la somme des cardinaux des $\mathcal{P}_a$, moins la somme des cardinaux des intersections de deux de ces ensembles, plus la somme des cardinaux des intersections de trois de ces ensembles, etc. □

Remarque. Il résulte de l'assertion (i) de la proposition que $\varphi(k)$ est pair pour tout $k \ge 3$. En effet, si $k \ge 3$ est divisible par un nombre premier impair p, alors $\varphi(k)$ est divisible par un nombre pair de la forme $p^a - p^{a-1}$, avec $a \ge 1$; sinon, k est divisible par un nombre pair de la forme $2^b - 2^{b-1}$, avec $b \ge 2$.

5.7. Théorème (Euler, Fermat). *Soit d un entier, $d \ge 1$. Pour tout entier $a \in \mathbb{Z}$ premier à d, on a*

$$a^{\varphi(d)} \equiv 1 \pmod{d} \qquad (Euler).$$

En particulier, pour un nombre premier p et un entier $a \in \mathbb{Z}$ qui n'est pas un multiple de p, on a

$$a^{p-1} \equiv 1 \pmod{p} \qquad (Fermat).$$

Preuve. Vu le lemme 4.6, l'énoncé à montrer est équivalent à

pour tout $[a]_d \in \mathbb{Z}/d\mathbb{Z}$ qui est inversible, $[a]_d^{\varphi(d)} = [1]_d$.

Le théorème d'Euler est donc un cas particulier du théorème suivant. □

5.8. Théorème (Lagrange). *Soit G un groupe abélien d'ordre N. Alors $g^N = 1$ pour tout $g \in G$.*

Remarque. Le théorème de Lagrange (mais pas la preuve qui suit) vaut pour tout groupe fini, abélien ou non.

Preuve. Soient $g_1, g_2, \dots, g_N$ une énumération des éléments de G. Alors $gg_1, gg_2, \dots, gg_n$ est aussi une telle énumération. Comme G est abélien, on a

$$g_1 g_2 \cdots g_N = (gg_1)(gg_2)\cdots(gg_n) = g^N g_1 g_2 \cdots g_N$$

et par suite $g^N = 1$. □

Autre preuve du théorème de Fermat (marche à suivre). Soit p un nombre premier.

(i) Pour tout $k \in \{1, \ldots, p-1\}$, vérifier que p divise le coefficient binomial $\binom{p}{k}$.

(ii) Pour tout $a \in \mathbb{Z}$, vérifier que $(a+1)^p \equiv a^p + 1 \pmod{p}$.

(iii) Pour tout $a \in \mathbb{N}$, montrer par récurrence sur a que $a^p \equiv a \pmod{p}$.

(iv) Si de plus $p \nmid a$, montrer que $a^{p-1} \equiv 1 \pmod{p}$. □

[Au dernier point, utiliser le fait que a est inversible modulo p.]

Rappel et précision. Dans un groupe G, *l'ordre* d'un élément g est le plus petit des entiers $j \geq 1$ tels que $g^j = 1$; s'il n'existe pas de tels entiers, on dit que g est d'ordre infini. Par exemple, dans le groupe $SL(2, \mathbb{Z})$, la matrice $\begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$ est d'ordre 6 et la matrice $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ est d'ordre infini. [Voir la note en bas de page à la définition 5.1.]

5.9. Autre formulation du théorème de Lagrange. *Soient G un groupe fini et g un élément de G. Alors l'ordre de g divise l'ordre de G.*

Preuve, qui vaut pour TOUT groupe fini (esquisse). Soient d'abord G un groupe et H un sous-groupe de G. On définit une relation R entre éléments x, y de G en posant $x\,R\,y$ si $x^{-1}y \in H$.

Affirmation (i) : R est une relation d'équivalence sur G. Cela résulte des définitions.

Affirmation (ii) : toutes les classes ont le même ordre que la classe de 1, qui est H. En effet : soient $x \in G$ et C_x sa classe modulo R ; alors l'application $C_x \longrightarrow H$, $y \longmapsto x^{-1}y$ est une bijection d'inverse $H \longrightarrow C_x$, $h \longmapsto xh$.

Affirmation (iii) : lorsque le groupe G est fini, l'ordre $|G|$ du groupe G est le produit de l'ordre $|H|$ du sous-groupe par l'ordre de l'ensemble quotient $|G/R|$. C'est une conséquence immédiate de l'affirmation précédente.

Considérons en particulier le cas d'un groupe fini G et du sous-groupe H engendré par un élément $g \in G$, c'est-à-dire du sous-groupe des éléments de la forme g^n avec $n \in \mathbb{Z}$. Alors H est un *groupe cyclique fini,* isomorphe à $\mathbb{Z}/d\mathbb{Z}$, où d est le plus petit entier strictement positif tel que $g^d = 1$. L'ordre d de g, qui dans ce cas est aussi l'ordre du sous-groupe H, divise l'ordre de G. □

La proposition qui suit est une conséquence du théorème de Fermat.

5.10. Lemme. *Soit p un nombre premier impair et $x \geq 2$ un entier tel que p divise $x^2 + 1$. Alors $p \equiv 1 \pmod{4}$.*

Preuve. Le premier p ne divise pas x, sinon il diviserait aussi $1 = (x^2+1) - x^2$, ce qui est absurde. Donc $x^{p-1} \equiv 1 \pmod{p}$ par le théorème de Fermat. Par hypothèse, $x^2 \equiv -1 \pmod{p}$ et $\frac{p-1}{2} \in \mathbb{N}$; par suite

$$x^{p-1} = \left(x^2\right)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

De l'égalité $(-1)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, il résulte que $\frac{p-1}{2}$ est pair, c'est-à-dire que p est de la forme $4k+1$. □

5.11. Proposition. *Il existe une infinité de nombres premiers congrus à* 1 *modulo* 4*, et une infinité de nombres premiers congrus à* 3 *modulo* 4*.*

Preuve. Comme pour le théorème 2.5, on commence par observer qu'il existe au moins un nombre premier congru à 1 modulo 4, par exemple 5.

Soit alors $\{p_1, \dots, p_k\}$ un ensemble fini de nombres premiers congrus à 1 modulo 4. On considère l'entier

$$n \;=\; 1 \,+\, \left(2 \prod_{1 \le i \le k} p_i \right)^2 .$$

Soit p un nombre premier divisant n. Alors p est nécessairement congru à 1 modulo 4 par le lemme ; par ailleurs, p n'est pas dans $\{p_1, \dots, p_k\}$ (voir la preuve du théorème 2.5). Il en résulte qu'il existe une infinité de nombres premiers congrus à 1 modulo 4. [Voir aussi l'exercice (VII.16) sur les nombres de Fermat.]

Pour les premiers congrus à 3 modulo 4, voir l'exercice (VII.15). □

Compléments au § VII.5

5.12. Importance pratique du théorème chinois. Supposons qu'on travaille sur un ordinateur qui manipule facilement des nombres ≤ 100, et qu'on veut effectuer des opérations sur des nombres $\le 10^6$. On peut réduire tous les nombres en scène modulo 99, 98, 97, et 95 (ces quatre nombres sont premiers deux à deux), faire toutes les opérations désirées, puis revenir à des nombres entiers $\le 10^6$. (Voir pages 129–130 dans le livre de K.H. Rosen, *Elementary number theory and its applications,* second edition, Addison-Wesley, 1988.)

5.13. Quelques propriétés de la fonction d'Euler φ. L'égalité $\varphi(p) = p - 1$ montre que $\limsup_{m\to\infty} \varphi(m) = \infty$; on peut montrer que $\lim_{m\to\infty} \varphi(m) = \infty$. Plus précisément, pour tout nombre réel $\delta > 0$, on a $\lim_{m\to\infty} m^{-1+\delta}\varphi(m) = \infty$. Par ailleurs, on peut aussi montrer que

$$\sum_{m=1}^{n} \varphi(m) \;=\; \frac{3n^2}{\pi^2} \,+\, 0(n \ln n).$$

Voici une interprétation de ce résultat. Pour tout entier $n \ge 1$, on considère les $\frac{1}{2}n(n+1) \sim \frac{1}{2}n^2$ paires d'entiers (a, b) telles que $1 \le a \le b \le n$; alors la proportion $\frac{\sum_{m=1}^{n} \varphi(m)}{\frac{1}{2}n(n+1)}$ d'entre elles pour lesquelles a et b sont premiers entre eux tend vers $6/\pi^2$ quand n tend vers l'infini. En d'autres termes, *la probabilité pour que deux entiers strictement positifs soient premiers entre eux est* $6/\pi^2 \sim 60,8\,\%$. Ce même nombre $6/\pi^2$ est aussi la probabilité pour qu'un entier positif soit « sans facteur carré » , c'est-à-dire ne soit divisible par aucun carré de nombre premier. [Ou trouve des preuves de ces résultats au chapitre XVIII de G.H. Hardy et E.M. Wright, *An introduction to the theory of numbers,* Oxford University Press ; la première édition date de 1938.]

5.14. Remarques historiques. Le théorème 5.7 est dû à Euler, qui a généralisé le cas particulier énoncé par Fermat.

Pierre de Fermat (1601-1665), conseiller au parlement de Toulouse, a énoncé sans preuve son résultat connu sous le nom de « petit théorème de Fermat » . Voici un commentaire de Legendre (1752–1833). *On a de [Fermat] un grand nombre de théorèmes intéressants, mais il les a laissés presque tous sans démonstration. C'était l'esprit du temps de se proposer des problèmes les uns aux autres. On cachait le plus souvent sa méthode, afin de se réserver des triomphes nouveaux tant pour soi que pour sa nation ; car il y avait surtout rivalité entre les géomètres français et les anglais. De là il est arrivé que la plupart des démonstrations de Fermat ont été perdues, et le peu qui nous en reste nous fait regretter d'autant plus celles qui nous manquent.*

Leonard Euler, né à Bâle en 1707 et mort à Saint-Pétersbourg en 1783, domine son siècle par l'importance et le nombre de ses travaux mathématiques.

Joseph Louis de Lagrange, né à Turin en 1736 et mort à Paris en 1813, est connu notamment pour ses travaux en théorie des nombres (tout entier est somme de quatre carrés), en mécanique, en calcul des variations (équations d'Euler-Lagrange) et sur les équations polynomiales de degré supérieur à 4 (préhistoire de la théorie des groupes).

Le « dernier théorème de Fermat » énonce que, pour tout entier $n \ge 3$, l'équation

$$x^n \,+\, y^n \;=\; z^n$$

n'a aucune solution en nombres entiers non nuls $x, y, z \in \mathbb{Z} \setminus \{0\}$. On connaît une preuve de Fermat pour $n = 4$ et une preuve d'Euler pour $n = 3$. Le problème pour n quelconque a eu une importance historique considérable pour le développement de la «théorie des nombres algébriques» et des mathématiques en général. Après de nombreuses réponses partielles, c'est à Andrew Wiles qu'est revenu le mérite et l'honneur de démontrer ce «théorème de Fermat-Wiles». (Voir *Modular elliptic curves and Fermat's last theorem,* Annals of Mathematics **141** (1995) 443–551 — article que, par ailleurs, bien peu de mathématiciens professionnels sont capables de lire, vu sa très grande difficulté technique, ainsi que l'importance des prérequis.)

Exercices du § VII.5

(VII.38) Vérifier naïvement le théorème d'Euler pour $d \leq 8$.

Calculer $\varphi(m)$ pour $m \leq 20$.

Montrer que, si $\varphi(m) \leq 2$, alors $m \in \{1, 2, 3, 4, 6\}$.

Montrer que les anneaux $\mathbb{Z}/900\mathbb{Z}$ et $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$ ne sont pas isomorphes en calculant leurs nombres d'éléments inversibles.

(VII.39) Quel est le dernier chiffre de 7^{1000} en écriture décimale ?

(VII.40) Quel est le reste de la division de $3^{24\,000}$ par 35 ?

(VII.41) Montrer que $6^{36} - 1$ est divisible par 13 et que $55^{24} - 1$ est divisible par 72.

[*Indication* : calculer les valeurs de la fonction φ d'Euler.]

(VII.42) Calculer les valeurs $\varphi(5186)$, $\varphi(5187)$ et $\varphi(5188)$ de la fonction d'Euler.

[*Indication* : les nombres 2593 et 1297 sont premiers.]

(VII.43) Trouver les entiers $x \in \mathbb{Z}$ tels que $x \equiv 9 \pmod{17}$ et $x \equiv 17 \pmod{60}$.

(VII.44) Soit p un nombre premier *impair* et soit $a \in \mathbb{Z}$ un nombre premier à p. L'exercice consiste à lire la preuve de (♯) dans (i) ci-dessous, et à rédiger une preuve (analogue) pour (♯♯).

(i) Supposons qu'il existe $x \in \mathbb{Z}$ tel que $x^2 \equiv a \pmod{p}$. Alors $(p - x)^2 \equiv a \pmod{p}$, et $p - x \not\equiv x \pmod{p}$ parce que p est impair. De plus, pour tout nombre $y \in \mathbb{Z}$ tel que $y^2 \equiv a \pmod{p}$, on a $y^2 - x^2 = (y - x)(y + x) \equiv a - a \equiv 0 \pmod{p}$ de sorte que

ou bien $y - x \equiv 0 \pmod{p}$, c'est-à-dire $y \equiv x \pmod{p}$,

ou bien $y + x \equiv 0 \pmod{p}$, c'est-à-dire $y \equiv p - x \pmod{p}$.

Il en résulte que les $p-1$ nombres $1, 2, \ldots, p-1$ peuvent être groupés comme suit : deux nombres distincts x et $p-x$ de carrés congrus à a modulo p, et des paires (s,t) d'entiers tels que $s \not\equiv t \pmod p$ et $st \equiv a \pmod p$. Il en résulte que

$$(p-1)! \;=\; x(p-x) \prod_{\text{paires } (s,t) \text{ distinctes}} st \;\equiv\; x(p-x)a^{\frac{1}{2}(p-3)} \;\equiv\; -a^{\frac{1}{2}(p-1)} \pmod p,$$

d'où

$$a^{\frac{1}{2}(p-1)} \;\equiv\; 1 \pmod p \qquad (\sharp)$$

par le théorème de Wilson.

(ii) Supposons au contraire qu'il n'existe aucun entier $x \in \mathbb{Z}$ tel que $x^2 \equiv a \pmod p$. Montrer que

$$a^{\frac{1}{2}(p-1)} \;\equiv\; -1 \pmod p. \qquad (\sharp\sharp)$$

Dans le cas (i), on dit que a est un *résidu quadratique modulo p,* et on écrit $\left(\frac{a}{p}\right) = 1$ (symbole de Legendre). Dans le cas (ii), on écrit $\left(\frac{a}{p}\right) = -1$. Ainsi, les résultats de (i) et (ii) s'écrivent

$$a^{\frac{1}{2}(p-1)} \;\equiv\; \left(\frac{a}{p}\right) \pmod p.$$

L'un des titres de gloire de Gauss est d'avoir découvert et montré, en 1795 c'est-à-dire à l'âge de 18 ans, le *théorèmede la réciprocité quadratique* :

THÉORÈME. *Soient p, q deux nombres premiers impairs distincts.*

Si $p \equiv q \equiv 3 \pmod 4$, alors $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$;

dans les autres cas, $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$.

Le théorème avait été conjecturé par Euler en 1783, et Lagrange en avait donné des « preuves » incomplètes. Legendre résumait le théorème par la formule

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) \;=\; (-1)^{\frac{p-1}{2}\frac{q-1}{2}},$$

valable pour toute paire (p,q) de nombres premiers impairs.

On peut montrer que

$$\left(\frac{ab}{q}\right) \;=\; \left(\frac{a}{q}\right)\left(\frac{b}{q}\right)$$

pour des entiers a, b premiers à q. Avec la réciprocité quadratique, cette « multiplicativité » permet des calculs rapides de symboles de Legendre. Par exemple

$$\begin{aligned}
\left(\frac{72}{97}\right) &= \left(\frac{2}{97}\right)^2\left(\frac{19}{97}\right) && \text{car } 72 = 2\times 2\times 19\\
&= \left(\frac{19}{97}\right) && \text{car le carré d'un symbole de Legendre vaut toujours 1}\\
&= \left(\frac{97}{19}\right) && \text{par réciprocité quadratique}\\
&= \left(\frac{1}{19}\right) && \text{car } 97 \equiv 1 \pmod{19}\\
&= \quad 1 && \text{car } \left(\frac{1}{p}\right) = 1 \text{ pour tout nombre premier impair } p.
\end{aligned}$$

Il n'est pas immédiat de trouver explicitement un nombre entier a tel que $a^2 \equiv 72 \pmod{97}$.

(VII.45) Soit p un nombre premier impair. Montrer que, parmi les $p-1$ entiers a tels que $1 \le a \le p-1$, il y en a $\frac{p-1}{2}$ qui sont des résidus quadratiques modulo p et $\frac{p-1}{2}$ qui n'en sont pas.

(VII.46) Vérifier que $\left(\frac{2}{p}\right) = 1$ pour $p = 7, 17, \ldots$ et $\left(\frac{2}{p}\right) = -1$ pour $p = 3, 5, 11, 13, 19, \ldots$. Plus généralement, on sait que $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$ pour tout nombre premier impair p.

(VII.47) Soient G un groupe, g un élément de G d'ordre fini et d l'ordre de g dans G.

(i) Soit $k \in \mathbb{N}$. Vérifier que $g^k = 1$ si et seulement si d divise k.

(ii) Soit $a \in \mathbb{N}$; posons $c = \operatorname{pgcd}(a, d)$ et $e = d/c$. Montrer que g^a est d'ordre e.

[*Indication* : Soit $b = a/c$, de sorte que b et e sont premiers entre eux. Soit $l \in \mathbb{N}$; alors d divise al si et seulement si e divise bl, c'est-à-dire si et seulement si e divise l.]

(iii) Parmi les puissances de g, montrer que le nombre de celles qui sont d'ordre égal à l'ordre de g est $\varphi(d)$, où φ désigne la fonction d'Euler.

(VII.48) Soit G un groupe fini ; notons n son ordre. Si G possède un élément d'ordre n, montrer que G est cyclique.

[*Rappel* : les termes « groupe cyclique » ont été définis juste après le numéro 5.8.]

[*Indication* : utiliser l'exercice précédent.]

6. A propos de la notation décimale des nombres réels

Tout nombre réel possède une écriture

$$x = \sum_{j=0}^{M} c_j 10^j + \sum_{j=1}^{\infty} a_j 10^{-j} \qquad (*)$$

où $c_j, a_j \in \{0, 1, \ldots, 9\}$. De plus, si on exclut les cas où il existe un entier $j_0 \geq 0$ tel que $a_j = 9$ pour tout $j \geq j_0$, alors l'écriture $(*)$ de x est unique. Pour la suite de ce numéro, on suppose que $0 \leq x < 1$ (sauf mention expresse du contraire).

6.1. Définition. Le développement $(*)$ de x

se termine à la μ-ième décimale, où μ est un entier positif, si $a_\mu \neq 0$ et $a_j = 0$ pour tout $j > \mu$;

est périodique s'il existe $\nu > 0$ tel que $a_{j+\nu} = a_j$ pour tout $j \geq 1$;

est ultimement périodique s'il existe $\mu \geq 0, \nu > 0$ tels que $a_{j+\nu} = a_j$ pour tout $j > \mu$.

Dans les deux derniers cas, ν s'appelle la *période* du développement ; noter qu'un développement qui se termine est un cas particulier de développement ultimement périodique (avec $\nu = 1$ et $a_1 = 0$), et qu'un développement périodique est également un cas particulier de développement ultimement périodique (avec $\mu = 0$).

On utilise un ou deux points pour indiquer les périodes, conformément aux exemples suivants :

$$\frac{1}{6} = 0,166\ 666\ 666\ \ldots = 0,1\dot{6} ;$$

$$\frac{5}{28} = 0,178\ 571\ 428\ \ldots = 0,17\dot{8}57142\dot{} ;$$

$$\frac{1}{11} = 0,090\ 909\ 090\ \ldots = 0,\dot{0}\dot{9}.$$

6.2. Nombres à développements qui se terminent.

PROPOSITION. *Pour que $x \in [0,1[$ possède un développement qui se termine, il faut et il suffit que x soit un nombre rationnel de la forme*

$$x = \frac{N}{2^\alpha 5^\beta},$$

avec $N, \alpha, \beta \in \mathbb{N}$ et

$$N \quad \textit{impair si} \quad \alpha > 0,$$
$$N \quad \textit{premier à} \quad 5 \quad \textit{si} \quad \beta > 0.$$

De plus, le développement de x se termine à la μ-ième décimale pour $\mu = \max\{\alpha, \beta\}$.

PREUVE. Si $x = N2^{-\alpha}5^{-\beta}$ et μ sont comme indiqués, alors $10^\mu x$ est entier, donc de la forme $10^\mu x = a_1 10^{\mu-1} + a_2 10^{\mu-2} + \cdots + a_\mu$; on laisse au lecteur le soin de vérifier que $a_\mu \neq 0$. Par suite le développement $x = 0, a_1 a_2 \cdots a_\mu$ se termine à la μ-ième décimale.

Réciproquement, si $x = 0, a_1 a_2 \cdots a_\mu$, alors $10^\mu x$ est entier, donc x est de la forme $N'10^{-\mu} = N2^{-\alpha}5^{-\beta}$. □

EXEMPLES. (i) $1/8 = 2^{-3} = 0,125$, le développement se termine à la 3ième décimale.

(ii) $3/400 = 3 \times 2^{-4}5^{-2} = 0,0075$, le développement se termine à la 4ième décimale, et on a bien $4 = \max\{4, 2\}$.

6.3. Nombres à développements périodiques.

PROPOSITION. *Pour que $x \in [0,1[$ possède un développement périodique, il faut et il suffit que x soit un nombre rationnel de la forme*

$$x = \frac{N}{D},$$

où N, D sont des entiers et

$$N \quad \textit{et} \quad D \quad \textit{sont premiers entre eux,}$$
$$D \quad \textit{est premier à} \quad 2 \quad \textit{et à} \quad 5 \quad [\textit{autrement dit } D \textit{ est premier à } 10].$$

De plus, la période du développement de x divise $\varphi(D)$.

PREUVE. Soit $x = N/D$ avec N, D premiers entre eux et D premier à 10. Notons ν le plus petit entier strictement positif tel que $10^\nu \equiv 1 \pmod{D}$. Remarquons d'abord que ν divise $\varphi(D)$. Ensuite il existe un entier $k \geq 1$ tel que

$$10^\nu x = \frac{10^\nu N}{D} = \frac{(kD+1)N}{D} = kN + x.$$

Si, en écriture décimale, $x = 0, a_1 a_2 \cdots a_\nu a_{\nu+1} a_{\nu+2} \cdots$, ces égalités impliquent que

$$a_1 a_2 \ldots a_\nu + 0, a_{\nu+1} a_{\nu+2} \cdots = kN + 0, a_1 a_2 \ldots$$

de sorte que $a_{\nu+j} = a_j$ pour tout $j \geq 1$.

Réciproquement, si le développement de x est périodique de période ν, alors $10^\nu x - x = N'$ est entier, de sorte que

$$x = \frac{N'}{10^\nu - 1} = \frac{N}{D}$$

où N, D sont premiers entre eux. De plus D divise $10^\nu - 1$, donc D est premier à 2 et à 5. □

EXEMPLES. (i) $1/111 = 0,\dot{0}0\dot{9}$, le développement est périodique de période 3, et on vérifie que 3 est un diviseur de $\varphi(111) = \varphi(3)\varphi(37) = 72$.

(ii) $1/81 = 0,\dot{0}12345679\dot{}$, le développement est périodique de période 9, et on vérifie que 9 est un diviseur de $\varphi(81) = \varphi(3^4) = 3^4 - 3^3 = 54$.

(iii) $1/7 = 0,\dot{1}42857\dot{}$, le développement est périodique de période $6 = \varphi(7)$.

(iv) $1/99 = 0,\dot{0}\dot{1}$, le développement est périodique de période 2, et on vérifie que 2 divise $\varphi(99) = \varphi(3^2)\varphi(11) = 6 \times 10 = 60$. En revanche, la période de

$$\left(\frac{1}{99}\right)^2 = \frac{1}{9801} = 0,\dot{0}0\,01\,02\,03\,04\,05\,06\,07\,08\,09\,10\,11\,12\,13\,14\,15\,16\,17\,18\,19\,20\,\ldots$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots 95\,96\,97\,99\dot{}$$

est bien supérieure à 2 ! (Cette période est précisément 198, dont on vérifie que c'est un diviseur de $\varphi(9801) = 5940 = 2^2 \times 3^3 \times 5 \times 11$.)

6.4. Nombres à développements ultimement périodiques.

PROPOSITION. *Pour que $x \in [0,1[$ possède un développement ultimement périodique, il faut et il suffit que $x \in \mathbb{Q}$.*

De plus, si

$$x = \frac{N}{2^\alpha 5^\beta D'},$$

où N, α, β, D' sont des entiers tels que

$$N \quad \textit{et} \quad 2^\alpha 5^\beta D' \quad \textit{sont premiers entre eux,}$$
$$D' \quad \textit{est premier à} \quad 2 \quad \textit{et} \quad 5$$

alors le développement décimal de x est de la forme $0, c_1c_2\cdots c_\mu\dot{a_1}a_2\cdots\dot{a_\nu}$ avec

$$\mu = \max\{\alpha,\beta\} \qquad \textit{et} \qquad \nu \mid \varphi(D')$$

ELÉMENTS DE PREUVE. Si $x = N/2^\alpha 5^\beta D'$ avec N, α, β, D' comme plus haut et si $a \in \mathbb{N}$ est l'entier tel que $2^\alpha 5^\beta a = 10^\mu$, alors $10^\mu x = aN/D' = q + r/D'$ avec $0 \le q < 10^\mu$ et $0 \le r < D'$. Vu le numéro 6.3 :

$$10^\mu\, x = q + 0,\dot{a_1}a_2\cdots\dot{a_\nu}$$

et par suite

$$x = 0, c_1c_2\cdots c_\mu\dot{a_1}a_2\cdots\dot{a_\nu}.$$

Resterait à voir qu'il n'y a pas d'écriture de ce type pour des valeurs de μ et ν strictement plus petites ..., ainsi qu'à montrer la réciproque. Nous renvoyons pour cela au théorème 10.4 de K.H. Rosen, *Elementary number theory and its applications,* second edition, Addison-Wesley, 1988. □

EXEMPLE. $5/28 = 5 \times 2^{-2}7^{-1} = 0,17\dot{8}5714\dot{2}$ a un développement ultimement périodique de période $6 = \varphi(7)$; on vérifie que $\mu = 2 = \max\{2,0\}$.

6.5. Conséquence. Il résulte de ce qui précède que tout nombre irrationnel, par exemple $\sqrt{2}$, π ou e, a un développement décimal qui n'est *pas* ultimement périodique.

6.6. Exercice. Voici par ailleurs un exercice fourni par G. Wanner ; soit x un nombre rationnel, $0 < x < 1$, qu'on suppose être ultimement périodique de période ν, et soit N un entier ; montrer que la période de x/N est majorée par $(N-1)\nu$.

[*Indication* : Soit $0, c_1 \cdots c_\mu \dot{a_1} \cdots \dot{a_{n\nu}}$ le développement de x en base 10. Notons A_j l'entier dont l'écriture en base 10 est $c_1 \cdots c_\mu a_1 \cdots a_\nu a_1 \cdots a_\nu \cdots\cdots a_1 \cdots a_\nu$ (avec j blocs $a_1 \cdots a_\nu$). Il existe j, k, avec $0 \le j < k \le N-1$, tels que les restes des divisions par N de A_j et A_k sont égaux. Alors x/N a un développement décimal ultimement périodique de période au plus $(k-j)\nu$.]

6.7. Curiosité. Il existe des exemples « bien connus » de paires de nombres réels distincts qui ont des développements décimaux « longtemps égaux ». Posons par exemple

$$\pi' = \left(\frac{1}{10^5} \sum_{n=-\infty}^{\infty} \exp\left(-\frac{n^2}{10^{10}}\right) \right)^2 .$$

Il n'est pas difficile de vérifier que la série converge, donc que π' est un nombre réel bien défini. Il se trouve que $3 < \pi' < 4$, donc que

$$\pi' = 3, a_1 a_2 a_3 \ldots$$

en notation décimale, avec $a_j \in \{0, 1, \ldots, 9\}$ pour tout $j \ge 1$. Ecrivons de même

$$\pi = 3, b_1 b_2 b_3 \ldots = 3, 14159 \ldots .$$

En 1992, les frères J. Borwein et P. Borwein ont montré que $a_j = b_j$ pour tout entier $j \le j_0$, où j_0 est un entier tel que $j_0 > 42 \times 10^9$, mais que néanmoins $\pi' \neq \pi$.

Pour en savoir plus, voir J.-P. Delahaye, *Le fascinant nombre* π, Belin – Pour la Science, 1997.

Les considérations de ce numéro s'étendent de la base 10 à toute autre base. Voici un exercice illustrant l'usage de la base 2.

Exercices du § VII.6

(VII.49) Soit $T : X \longrightarrow X$ une transformation d'un ensemble X. On définit par récurrence les itérés T^n de T en posant $T^2(x) = T(T(x))$, ..., $T^{n+1}(x) = T(T^n(x))$. Un point $x \in X$ est *périodique* s'il existe un entier $k > 0$ tel que $T^k(x) = x$, et *ultimement périodique* s'il existe des entiers $k, n > 0$ tels que $T^{k+n}(x) = T^n(x)$.

On considère l'intervalle $X = [0, 1[\subset \mathbb{R}$ et la transformation T de X définie par

$$T(x) = 2x \quad \text{si} \quad x < \frac{1}{2} \qquad \text{et} \qquad T(x) = 2x - 1 \quad \text{sinon.}$$

Déterminer les points périodiques et les points ultimement périodiques de T.

[*Indications* : Montrer qu'un nombre réel x tel que $0 \le x < 1$, avec un développement

$$x = \sum_{j=1}^{\infty} \epsilon_j 2^{-j} \qquad \epsilon_j \in \{0, 1\}$$

en base 2, est rationnel si et seulement si la suite $(\epsilon_j)_{j \ge 1}$ est ultimement périodique.

En particulier, le développement en base 2 d'un nombre $x \in [0, 1[$ qui est irrationnel n'est jamais ultimement périodique.

Pour $x \in [0, 1[\cap \mathbb{Q}$, écrire $x = \frac{a}{2^b c}$ avec c impair et $a, 2^b c$ premiers entre eux. Puis infliger à x les transformations T, T^2, ..., T^b, T^{b+1}, ...]

(VII.50) Soit n un entier positif et

$$n = \epsilon_k 2^k + \epsilon_{k-1} 2^{k-1} + \cdots + \epsilon_1 2 + \epsilon_0, \quad \text{où} \quad \epsilon_0, \ldots, \epsilon_k \in \{0, 1\},$$

son développement en base 2. On pose

$$\begin{aligned} m &= \epsilon_0 + 2\epsilon_1 + 4\epsilon_2 + \epsilon_3 + 2\epsilon_4 + 4\epsilon_5 + \cdots \\ &= \left(\sum_{j=0}^{[k/3]} \epsilon_{3j} \right) + 2 \left(\sum_{j=0}^{[(k-1)/3]} \epsilon_{3j+1} \right) + 4 \left(\sum_{j=0}^{[(k-2)/3]} \epsilon_{3j+2} \right). \end{aligned}$$

(i) Vérifier que n est divisible par 7 si et seulement si m l'est.

(ii) Formuler un critère de divisibilité par 17.

7. Introduction à la cryptographie à clé publique et au système RSA

La *cryptographie* est l'étude des méthodes permettant la transmission de messages qui ne soient compréhensibles que par leurs destinataires. Le problème est de transfomer un *texte en clair* en un *texte chiffré* et, une fois ce dernier transmis, de retrouver le texte original. Le texte en clair utilise un certain *alphabet,* par exemple 40 signes typographiques usuels[28], ou les deux éléments du corps $\mathbb{F}_2$, ou les 128 éléments d'un espace vectoriel de dimension 7 sur $\mathbb{F}_2$, ou les éléments d'un anneau du type $\mathbb{Z}/m\mathbb{Z}$. Le texte chiffré utilise aussi un alphabet, qui peut être différent ou non du précédent. La transformation de textes en clair en textes chiffrés s'appelle le *codage* ou le *chiffrage,* et la transformation inverse le *décodage* ou *déchiffrage.* L'espoir des interlocuteurs est que les intercepteurs éventuels du message ne pourront pas le comprendre ; l'espoir évidemment contraire de ces intercepteurs est de *percer le code.* L'histoire montre que les codes finissent souvent par être percés.

Il existe une multitude de systèmes de codage. Certains sont tout à fait naïfs, par exemple le suivant. On utilise une permutation des lettres de l'alphabet. Ainsi, avec la permutation « +1 modulo 26 » sur les lettres (avec les autres signes typographiques points fixes de la permutation), le message

« nul n entre ici s il n est geometre »

devient

« ovm o fousf jdj t jm o ftu hfpnfusf » .

Ce genre de codage est facile à percer : ci-dessus, on peut commencer par observer que la lettre qui apparaît le plus souvent est « f » , et qu'il y a donc de bonnes chances pour qu'elle corresponde à un « e » dans le texte en clair, puisque le « e » est en général la lettre la plus fréquente d'un texte français. (Il existe des exceptions célèbres, dont un ahurissant lipogramme de Georges Perec [Per].)

Les méthodes de codage classiques nécessitent la transmission préalable du procédé de décodage, et l'histoire (encore elle) montre que cette étape préliminaire est une faiblesse certaine vu qu'il est bien difficile de la garder secrète.

Les *cryptosystèmes à clé publique* datent des années 1970 [DiHe]. Avant de les décrire, commençons par formaliser le problème fondamental de la cryptographie (au

[28] Choix possible : a, b, ..., z, espace blanc, point, ?, $, 0, 1, ..., 9.

moins du point de vue des interlocuteurs souhaitant communiquer secrètement – les casseurs de code ont d'autres problèmes). On considère l'ensemble $\mathcal{M}$ de tous les messages en clair possibles, et l'ensemble $\mathcal{C}$ de tous les messages chiffrés possibles. L'encodage E et le décodage D sont des applications

$$E : \mathcal{M} \longrightarrow \mathcal{C} \qquad \text{et} \qquad D : \mathcal{C} \longrightarrow \mathcal{M}$$

qui sont bijectives et inverses l'une de l'autre : $D = E^{-1}$ et $E = D^{-1}$.

Il peut être « plus difficile » de calculer une image de D qu'une image de E, comme le montre l'exemple simple suivant : $\mathcal{M}$ est l'ensemble des paires de nombres premiers impairs distincts

$$\mathcal{M} = \{(3,5)\,,\,(3,7)\,,\,(3,11)\,,\,\ldots\,,\,(5,7)\,,\,(5,11)\,,\,\ldots\}$$

et $\mathcal{C}$ l'ensemble des entiers impairs dont la décomposition en nombres premiers est un produit d'exactement deux facteurs

$$\mathcal{C} = \{15\,,\,21\,,\,33\,,\,35\,,\,39\,,\,51\,,\,55\,,\,57\,,\,65\,,\,69\,,\,77\,,\,\ldots\}.$$

L'application E est le produit, et D est la décomposition en facteurs premiers. Pour des correspondants privés de calculettes, il est par exemple facile de calculer

$$E(881\,,\,2657) = 2\,340\,817$$

mais il est bien difficile de trouver la décomposition en facteurs premiers

$$D(2\,340\,817) = (881\,,\,2657)$$

(à moins bien sûr de disposer d'informations supplémentaires).

Supposons qu'il existe des règles faciles pour trouver l'image $E(M)$ de tout message en clair M, mais qu'il soit très difficile de trouver à partir de ces seules règles l'image $D(C)$ d'un message codé C. Si un correspondant A veut recevoir des messages d'un correspondant B avec qui il partage la connaissance des ensembles $\mathcal{M}$ et $\mathcal{C}$, il suffit à A de connaître E et D, de transmettre E à son correspondant (voir de publier E), tout en gardant D secret. Ainsi B pourra-t-il encoder ses messages, grâce à E, mais seul A pourra-t-il les décoder.

L'intérêt des cryptosystèmes à clé publique étant admis, il reste à mettre au point des algorithmes efficaces. Le système le plus utilisé est appelé RSA, en référence à [**RSA**]. L'efficacité d'un tel algorithme dépend fortement des performances des ordinateurs disponibles. Le système RSA a été efficace pendant une bonne vingtaine d'années ; mais ses détails doivent être périodiquement adaptés aux progrès de la technique.

Le système RSA transmet des entiers modulo m, où m est un entier suffisamment grand. L'usage de ce système présuppose une manière de transformer un message, par exemple un message en français d'au plus 100 lettres-et-espaces, en un nombre entier x dans le domaine $1 \leq x \leq 10^{200}$, et réciproquement. Ces étapes n'offrent pas de difficulté de principe importante, et nous n'en dirons rien de plus ici. Le but de l'exposition qui suit est donc de décrire des applications convenables

$$E : \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \qquad \text{et} \qquad D : \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$$

inverses l'une de l'autre. Pour les exemples traitables sans ordinateur, m est si petit que l'application D semble être facile à expliciter lorsque l'on connaît E. Mais pour m grand, l'expérience montre que la méthode est tout à fait utilisable en cryptographie.

EXERCICE. On se donne un entier m dont on sait qu'il est produit de deux nombres premiers distincts, et la valeur $\varphi(m)$ de la fonction d'Euler en m. Trouver les facteurs premiers de m.

[*Réponse* : ce sont les racines du polynôme $X^2-(m+1-\varphi(m))X+m$. Il en résulte que la «difficulté» de trouver $\varphi(m)$ est tout à fait comparable à la «difficulté» de trouver les deux facteurs premiers de m.]

8. Description du codage RSA

8.1. Mise en place.

(i) Le correspondant A choisit secrètement deux nombres premiers distincts p et q.

(ii) Il calcule $m=pq$ et $\varphi(m)=(p-1)(q-1)$.

(iii) Il choisit un entier $e\in\{1,2,\dots,m-1\}$ tel que e et $\varphi(m)$ sont premiers entre eux, et calcule[29] $d\in\{1,2,\dots,m-1\}$ tel que $ed\equiv 1 \pmod{\varphi(m)}$. Ainsi, il existe $k\in\mathbb{N}$ tel que $ed=k\varphi(m)+1$; la valeur numérique de k ne joue aucun rôle ci-dessous.

(iv) Le correspondant A publie la *clé de codage* (m,e) et conserve secrètement pour lui la *clé de décodage* (m,d). Rappelons que, pour qui ne connaît que m et d sans connaître p et q (c'est-à-dire sans connaître $\varphi(m)$, voir l'exercice du numéro précédent), il est «très difficile» de trouver p, q et $\varphi(m)$, donc a fortiori de calculer d à partir de e.

8.2. Codage et décodage d'un message. Quiconque souhaite envoyer secrètement à A un message $x\in\{0,1,2,\dots,m-1\}$ calcule $y\in\{0,1,2,\dots,m-1\}$ tel que $y\equiv x^e \pmod m$ et transmet y à A. Lorsque A reçoit le message codé y, il calcule $z\in\{0,1,2,\dots,m-1\}$ tel que $z\equiv y^d \pmod m$. Voici l'observation fondamentale :

$$z\equiv y^d\equiv x^{ed}\equiv x^{k\varphi(m)+1} \pmod m;$$

donc $z=x$ par la proposition suivante.

8.3. PROPOSITION. *Soient p,q deux nombres premiers distincts et $m=pq$ leur produit. Alors*

$$x^{k\varphi(m)+1}\equiv x \pmod m$$

pour tous $k\geq 0$ et $x\in\mathbb{Z}$.

REMARQUE. Si x est premier à m, la conclusion résulte du théorème d'Euler. Mais, pour un entier m de la forme indiquée, la proposition vaut pour *tout* entier x.

PREUVE. Si x est un multiple de p, on a évidemment $x^{k\varphi(m)+1}\equiv x\equiv 0 \pmod p$; si p ne divise pas x, alors $x^{k\varphi(m)}\equiv (x^{p-1})^{k(q-1)}\equiv 1 \pmod p$ par le théorème de Fermat. On a donc

$$x^{k\varphi(m)+1}\equiv x \pmod p$$

pour tout $x\in\mathbb{Z}$.

De même $x^{k\varphi(m)+1}\equiv x \pmod q$ pour tout $x\in\mathbb{Z}$. Ainsi $x^{k\varphi(m)+1}-x$, qui est à la fois un multiple de p et un multiple de q, est aussi un multiple de pq ; en d'autres termes $x^{k\varphi(m)+1}\equiv x \pmod m$. □

[29] Voir l'algorithme d'Euclide et le numéro 1.7.

Illustration de la proposition. Si $m = 15$, alors $\varphi(15) = 8$. Par exemple :

$$\begin{aligned} 3^9 &= (27)^3 \equiv (-3)^3 \equiv 3 \pmod{15};\\ 4^2 &= 16 \equiv 1 \pmod{15} \quad \text{donc} \quad 4^9 \equiv 4 \pmod{15};\\ 5^9 &= (125)^3 \equiv (5)^3 \equiv 125 \equiv 5 \pmod{15};\\ &\text{etc.} \end{aligned}$$

Exercice. Généraliser la proposition au cas d'un entier m qui est un produit de nombres premiers distincts deux à deux.

8.4. Exemples avec m petit. *Premier exemple :* A choisit les nombres premiers $p = 3$ et $q = 11$, calcule $m_A = 33$ et $\varphi(m_A) = 20$, puis choisit $e_A = 7$ et calcule $d_A = 3$, et enfin publie $(33, 7)$.

Si un correspondant connaissant la clé de codage $(33, 7)$ veut transmettre à A le nombre $x = 17$, il calcule d'abord $(17)^7 \equiv 8 \pmod{33}$, par exemple comme suit : il observe les congruences $2^5 = 32 \equiv -1 \pmod{33}$ et $17 \equiv -16 = -2^4 \pmod{33}$, puis il obtient

$$(17)^7 \equiv (-16)^7 = -2^{28} = -\left(2^5\right)^5 2^3 \equiv 2^3 \pmod{33}.$$

Ce correspondant transmet donc $y = 8$ à A.

Lorsque A reçoit le message, il calcule

$$8^3 = 8(8)^2 \equiv 8(-2) \equiv -16 \equiv 17 \pmod{33}$$

et conclut que ce nombre 17 est le message en clair que A souhaite lui transmettre, comme on le vérifie ici.

Second exemple : le correspondant B de A choisit pour sa part les premiers 5 et 13 donc l'entier $m_B = 65$, choisit $e_B = 11$, calcule $d_B = 35$, et enfin publie $(65, 11)$.

Si A, cette fois l'origine d'un message, veut transmettre le «message en clair» 11, alors A doit calculer $(11)^{11} \equiv 6 \pmod{65}$ et transmettre le résultat codé 6. Il ne reste à B qu'à déchiffrer $6^{35} \equiv 11 \pmod{65}$.

Voici une manière (parmi d'autres) de vérifier *de tête* ces calculs.

$$\begin{aligned} \varphi(65) &= \varphi(5)\varphi(13) = 48 \quad \text{et} \quad 11 \times 35 = 385 = 8 \times 48 + 1\\ 11^2 &\equiv -9 \pmod{65}, \quad 11^4 \equiv 81 \equiv 16 \pmod{65}, \quad 11^8 \equiv 256 \equiv -4 \pmod{65}\\ 11^3 &\equiv -99 \equiv 31 \pmod{65},\\ 11^{11} &\equiv -4 \times 31 \equiv -124 \equiv 6 \pmod{65}\\ 6^3 &= 216 \equiv 21 \pmod{65}, \quad 6^4 \equiv 126 \equiv -4 \pmod{65},\\ 6^{12} &\equiv (6^4)^3 \equiv (-4)^3 \equiv -64 \equiv 1 \pmod{65}\\ 6^{35} &= 6^{36} \times 6^{-1} \equiv 6^{-1} \equiv 11 \pmod{65}. \end{aligned}$$

Exercice. A choisit $m = 35$, $e = d = 5$ et $x = 4$. Calculer les nombres $y, z \in \{0, 1, \ldots, 34\}$ définis par $y \equiv x^e \pmod{35}$ et $z \equiv y^d \pmod{35}$. [Elément de réponse : $y = 9$.]

8.5. Exemples plus réalistes. A choisit deux nombres premiers p et q de l'ordre de $(10)^{100}$ avec $100 < q/p < 10000$. (La raison en est qu'il est «assez facile» de décomposer un produit de deux nombres premiers distincts proches l'un de l'autre, d'où un choix de p et q «suffisamment différents» .) La couverture du livre de Bachmann cité ci-dessous montre un exemple avec $p \approx 10^{68}$ et $q \approx 10^{78}$.

8.6. Signatures. Considérons à nouveau deux correspondants A et B, par exemple avec les données numériques ci-dessus, à savoir

$$A \quad \text{publie} \quad (m_A, e_A) = (33, 7) \quad \text{et connaît secrètement} \quad d_A = 3,$$
$$B \quad \text{publie} \quad (m_B, e_B) = (65, 11) \quad \text{et connaît secrètement} \quad d_B = 35.$$

Imaginons que A veuille envoyer à B un message signé, ou en d'autres termes un message dont B puisse être sûr qu'il provient vraiment de A. Voici un procédé naturel dans le contexte RSA (dans le cas de l'exemple, c'est-à-dire dans le cas où $m_A < m_B$).

A possède une signature numérique publique, qui est un nombre $s_A \in \{0, 1, \ldots, m_A - 1\}$.

(i) Il la transforme d'abord d'une manière connue de lui seul, en calculant

$$s_A^{(1)} \in \{0, 1, \ldots, m_A - 1\} \quad \text{tel que} \quad s_A^{(1)} \equiv (s_A)^{d_A} \pmod{m_A}.$$

(ii) Puis A utilise les données publiques de B et calcule

$$s_A^{(2)} \in \{0, 1, \ldots, m_B - 1\} \quad \text{tel que} \quad s_A^{(2)} \equiv \left(s_A^{(1)}\right)^{e_B} \pmod{m_B},$$

qu'il transmet à B.

(iii) A réception, B utilise d'abord sa connaissance secrète pour calculer

$$\tilde{s}_A^{(1)} \in \{0, 1, \ldots, m_B - 1\} \quad \text{tel que} \quad \tilde{s}_A^{(1)} \equiv \left(s_A^{(2)}\right)^{d_B} \pmod{m_B}.$$

(iv) Enfin B utilise les données publiques de A et calcule

$$\tilde{s}_A \in \{0, 1, \ldots, m_A - 1\} \quad \text{tel que} \quad \tilde{s}_A \equiv \left(\tilde{s}_A^{(1)}\right)^{e_A} \pmod{m_A}.$$

Si B retrouve la signature $s_A = \tilde{s}_A$ de A, il est convaincu que le message vient bien de A. En effet :

$$\tilde{s}_A^{(1)} \equiv \left(s_A^{(1)}\right)^{e_B d_B} \equiv s_A^{(1)} \pmod{m_B}$$

par la proposition 8.3, donc $\tilde{s}_A^{(1)} = s_A^{(1)}$, et de même

$$\tilde{s}_A \equiv \left(s_A^{(1)}\right)^{e_A} \equiv (s_A)^{d_A e_A} \equiv s_A \pmod{m_A}$$

par la même proposition 8.3, donc $\tilde{s}_A = s_A$.

Dans le sens contraire, le procédé est presqu'identique, à ceci près que $m_B > m_A$, ce qui modifie l'ordre des opérations à faire sur la signature s_B de B. On suppose que B s'est arrangé pour que sa signature numérique s_B soit un nombre inférieur à $m_A - 1$ (c'est-à-dire au *minimum* de $m_A - 1$ et $m_B - 1$).

(i′) B calcule d'abord $s_B^{(1)} \in \{0, 1, \ldots, m_A - 1\}$ tel que $s_B^{(1)} \equiv (s_B)^{e_A} \pmod{m_A}$,

(ii′) puis $s_B^{(2)} \in \{0, 1, \ldots, m_B - 1\}$ tel que $s_B^{(2)} \equiv \left(s_B^{(1)}\right)^{d_B} \pmod{m_B}$.

(iii′) A calcule d'abord $\tilde{s}_B^{(1)} \in \{0, 1, \ldots, m_B - 1\}$ tel que $\tilde{s}_B^{(1)} \equiv \left(s_B^{(2)}\right)^{e_B} \pmod{m_B}$,

(iv′) puis $\tilde{s}_B \in \{0, 1, \ldots, m_A - 1\}$ tel que $\tilde{s}_B \equiv \left(\tilde{s}_B^{(1)}\right)^{d_A} \pmod{m_A}$. Comme avant, A doit retrouver la signature $s_B = \tilde{s}_B$ de B pour être convaincu que le message contenant cette information vient bien de B.

Pour en savoir plus, voir par exemple [Sin], qui est un livre de vulgarisation, [Kob] ou [Buc], qui sont des cours de mathématiques, et [Lan], sur un sujet d'actualité.

Références pour les § VII.7 et § VII.8

[Beu] A. Beutelspacher, *Cryptology*, The Mathematical Association of America, 1994

[Buc] J.A. Buchmann, *Introduction to cryptography*, Springer, 2001

[DiHe] W. Diffie et M.E. Hellman, *New directions in cryptography*, IEEE Transactions in Information Theory **IT-22** (1976), 644–654

[Joy] D. Joyner (éditeur) *Coding theory and cryptography, from Enigma and Geheimschreiber to quantum theory*, Springer, 2000

[Kob] N. Koblitz, *A course in number theory and cryptography*, Springer, 1987

[Lan] S. Landau, *Standing the test of time : the Data Encryption Standard*, Notices of the Amer. Math. Soc. **47**[3] (2000), 341–349

[Per] G. Perec, *La disparition Denoël*, 1969. Voir aussi *Les revenentes*, Julliard, 1972

[Ree] J. Reeds, *Review of « The code book : the evolution of secrecy from Mary, Queen of Scots to quantum cryptography»*, Notices of the Amer. Math. Soc. **47-3** (2000), 369–372

[RSA] R.L. Rivest, A. Shamir et L.M. Adleman, *A method for obtaining digital signatures and public key signatures*, Communications of the ACM **21** (1978), 120-126

[Sin] S. Singh, *The code book : the evolution of secrecy from Mary, Queen of Scots to quantum cryptography*, Doubleday books, 1999 (le livre est toutefois controversé, comme l'indique [Ree])

9. Pseudopremiers

Pour savoir si un nombre entier positif n est premier ou non, un procédé naïf consiste à diviser n par les nombres premiers p tels que $2 \leq p \leq \sqrt{n}$; pour que n soit non premier, il faut et il suffit qu'au moins l'une de ces divisions fournisse un reste nul. Ce procédé prend souvent beaucoup de temps. Le but du présent paragraphe est de faire entrevoir d'autres procédés.

9.1. Calculs préliminaires.

$$2^{340} \equiv 1 \pmod{341}, \qquad 3^{340} \not\equiv 1 \pmod{341} \quad \text{et} \quad 7^{340} \not\equiv 1 \pmod{341}.$$

Il est hautement déconseillé de calculer d'abord 2^{340}, 3^{340} et 7^{340} puis de réduire modulo 341. Voici une autre méthode, utilisant la factorisation $341 = 11 \times 31$.

(i) Remarquons d'abord que

$$2^{10} \equiv 1 \pmod{11} \quad \text{donc} \quad 2^{30} \equiv 1 \pmod{11}$$
$$2^{30} \equiv 1 \pmod{31}$$

par le théorème de Fermat. Comme $2^{30}-1$ est à la fois un multiple de 11 et un multiple de 31, c'est aussi un multiple de 341 ; autrement dit $2^{30} \equiv 1 \pmod{341}$. Comme par ailleurs $340 - 10$ est un multiple de 30,

$$2^{340} \equiv 2^{10} \pmod{341}.$$

Or $2^{10} = 3 \times 341 + 1$, donc

$$2^{340} \equiv 1 \pmod{341}.$$

(ii) On montre comme ci-dessus que $3^{340} \equiv 3^{10} \pmod{341}$. Or $3^6 = 2 \times 341 + 47$ et $3^4 = 81$, de sorte que

$$3^{10} = 3^6 \times 3^4 \equiv 47 \times 81 \pmod{341}.$$

Or $47 \times 81 = 3807 = 3751 + 56 = 11 \times 341 + 56$, et donc

$$3^{340} \equiv 3^{10} \equiv 56 \not\equiv 1 \pmod{341}.$$

(iii) Enfin $7^3 = 343 \equiv 2 \pmod{341}$ et $2^{10} \equiv 1 \pmod{341}$ impliquent

$$7^{340} = (7^3)^{113} \times 7 \equiv 2^{113} \times 7 = (2^{10})^{11} \times 56 \equiv 56 \not\equiv 1 \pmod{341}.$$

9.2. Un premier test de primalité. Soit n un entier, $n \geq 3$. Si n est premier, alors

$$2^{n-1} \equiv 1 \pmod{n},$$

comme cas particulier du théorème de Fermat. Qu'en est-il de la réciproque ? Un test numérique sommaire montre que

si	$n = 3$	alors	$2^2 = 4 \equiv 1 \pmod{3}$
si	$n = 4$	alors	$2^3 = 8 \equiv 0 \pmod{4}$
si	$n = 5$	alors	$2^4 = 16 \equiv 1 \pmod{5}$
si	$n = 6$	alors	$2^5 = 32 \equiv 2 \pmod{6}$
si	$n = 7$	alors	$2^6 = 64 \equiv 1 \pmod{7}$
si	$n = 8$	alors	$2^7 = 128 \equiv 0 \pmod{8}$
si	$n = 9$	alors	$2^8 = 256 \equiv 4 \pmod{9}$
si	$n = 10$	alors	$2^9 = 512 \equiv 2 \pmod{10}$
si	$n = 11$	alors	$2^{10} = 1024 \equiv 1 \pmod{11}$
si	$n = 12$	alors	$2^{11} = 2048 \equiv 8 \pmod{12}$
. . . . .			
si	$n = 341$	alors	$2^{340} \equiv 1 \pmod{341}$.

9.3. Définition. Un nombre impair $n \geq 3$ est *pseudopremier* s'il n'est pas premier et si $2^{n-1} \equiv 1 \pmod{n}$.

Le nombre 341 est donc pseudopremier. On peut montrer que les seuls nombres pseudopremiers inférieurs à 1000 sont 341, 561 et 645, alors qu'il y a 168 nombres premiers inférieurs à 1000. De même, parmi les nombres inférieurs à 10^{10}, il y a 14 884 pseudopremiers et 455 052 512 premiers. Ainsi, le test $2^{n-1} \overset{???}{\to} \equiv 1 \pmod{n}$ détecte une grande proportion de nombres composés.

Néanmoins, il existe une infinité de nombres pseudopremiers, comme il résulte de l'exemple fourni ci-dessus (341) et de la proposition 5.

9.4. Lemme. *Soient a, b des entiers, $a, b > 1$. Alors $2^a - 1$ divise $2^{ab} - 1$.*

Preuve. Il suffit, dans l'identité $x^b - 1 = (x-1)(x^{b-1} + x^{b-2} + \cdots + 1)$, de remplacer x par 2^a. □

9.5. Proposition. *Si n est un nombre pseudopremier, alors $m = 2^n - 1$ l'est aussi.*

Preuve. Comme n est composé, m l'est aussi par le lemme précédent. Reste donc à évaluer 2^{m-1} modulo m.

Vu que $2^{n-1} \equiv 1 \pmod{n}$, il existe $k \in \mathbb{N}$ tel que $2^{n-1} - 1 = kn$. Donc

$$2^{m-1} - 1 \;=\; 2^{2^n - 2} - 1 \;=\; 2^{2kn} - 1$$

est un multiple entier de $m = 2^n - 1$, par le lemme précédent. En d'autres termes : $2^{m-1} \equiv 1 \pmod{m}$. □

Il y a d'autres tests de primalité, comme suggéré ci-dessous.

9.6. Définition. Soit b un nombre entier, $b \geq 2$. Un nombre entier $n \geq b + 1$ est *pseudopremier pour la base b* s'il n'est pas premier, si n et b sont premiers entre eux, et si $b^{n-1} \equiv 1 \pmod{n}$.

Par exemple, le nombre 341 est pseudopremier (= pseudopremier pour la base 2) et n'est pas pseudopremier pour la base 3, ni pour la base 7. En revanche, 561 est pseudopremier à la fois pour la base 2 et la base 3.

Pour toute base b, on sait montrer[30] qu'il existe une infinité de nombre pseudopremiers pour la base b. Néanmoins, chaque valeur de b fournit un test très sélectif pour savoir si un nombre est premier ou non.

Il existe des nombres $n \geq 3$ non premiers tels que

$$b^{n-1} \equiv 1 \pmod{n} \quad \text{pour tout entier} \quad b \quad \text{tel que} \quad 1 < b < n\,;$$

ce sont les *nombres de Carmichael*. Les plus petits sont $561 = 3 \times 11 \times 17$, 1105, 1729, ... ; il en existe 1547 inférieurs à 10^{10}.

Carmichael a conjecturé en 1912 et Alford-Granville-Pomerance ont montré en 1994 qu'il existe une infinité de nombres de Carmichael.

9.7. Définition. Soit b un nombre entier, $b \geq 2$. Soit n un nombre entier, $n > b$; on écrit $n - 1 = 2^s t$ avec $s \geq 0$ et t impair. On dit que n *passe le test de Miller pour la base b* si l'une des deux conditions suivantes est vérifiée :

$b^t \equiv 1 \pmod{n}$,

il existe $j \in \{0, \ldots, s-1\}$ tel que $b^{2^j t} \equiv -1 \pmod{n}$.

Exemples. (i) Montrons que le nombre $n = 341$ ne passe pas le test de Miller pour la base $b = 2$. Le nombre $n - 1$ s'écrit $340 = 4 \times 85$, de sorte que $s = 2$ et $t = 85$.

D'une part, vu que $2^{10} \equiv 1 \pmod{341}$, voir les calculs préliminaires, nous avons

$$2^t \;=\; 2^{85} \;\equiv\; 2^5 \;\equiv\; 32 \not\equiv 1 \pmod{341}.$$

D'autre part

$$2^t \;\equiv\; 32 \not\equiv -1 \pmod{341}$$
$$2^{2t} \;=\; 1024 \;=\; 3 \times 341 + 1 \;\equiv\; 1 \not\equiv -1 \pmod{341}.$$

[30] Voir par exemple le théorème 89 dans G.H. Hardy and E.M. Wright, *An introduction to the theory of numbers,* fifth edition, Oxford University Press, 1979.

Donc 341 ne passe pas le test de Miller, de sorte que 341 n'est pas un nombre premier. *Cette preuve ne fournit en aucun cas*[31] *la décomposition* $341 = 11 \times 31$ *!*

(ii) Montrons que le nombre $n = 561$ ne passe pas le test de Miller pour la base $b = 2$. Le nombre $n - 1$ s'écrit $560 = 16 \times 35$, de sorte que $s = 4$ et $t = 35$.

Nous avons d'abord

$$\begin{aligned} 2^{16} &= 65536 = 116 \times 561 + 460 \equiv 460 \pmod{561} \\ 2^{32} &\equiv (460)^2 = 377 \times 561 + 103 \equiv 103 \pmod{561} \\ 2^{35} &\equiv 8 \times 103 \equiv 263 \pmod{561} \end{aligned}$$

et en particulier $2^t = 2^{35} \not\equiv 1 \pmod{561}$. Nous avons ensuite

$$\begin{aligned} 2^t &= 2^{35} \equiv 263 \not\equiv -1 \pmod{561} \\ 2^{2t} &\equiv (263)^2 = 123 \times 561 + 166 \equiv 166 \not\equiv -1 \pmod{561} \\ 2^{2^2 t} &\equiv (166)^2 = 49 \times 561 + 67 \equiv 67 \not\equiv -1 \pmod{561} \\ 2^{2^3 t} &\equiv (67)^2 = 8 \times 561 + 1 \equiv 1 \not\equiv -1 \pmod{561}. \end{aligned}$$

Donc 561 ne passe pas le test de Miller, de sorte que 561 n'est pas un nombre premier. *Cette preuve ne fournit en aucun cas la décomposition* $561 = 3 \times 11 \times 17$ *!*

9.8. Proposition. *Soient $b \geq 2$ et $n > b$. Si n est premier, alors n passe le test de Miller pour la base b.*

Preuve. Voir par exemple le théorème 5.8 dans le livre de Rosen déjà cité. □

9.9. Test probabiliste de primalité, de Rabin. Soit n un entier. On choisit k entiers $b_1, \ldots, b_k$ inférieurs à n et on applique le test de Miller pour chacune des bases b_j. Si n est un nombre composé, la probabilité pour que n passe ces k tests est inférieure à $(\frac{1}{4})^k$. Par exemple, si $k = 100$, la probabilité pour qu'un nombre composé passe les 100 tests est inférieure à 10^{-60}.

Si la « conjecture de Riemann généralisée » est vraie, alors tout nombre composé n échoue au test de Miller pour au moins une base $b < 70(\log_2 n)^2$.

[31] Au numéro 4.10, le théorème de Wilson est déjà un exemple de test de primalité ne fournissant aucune factorisation pour les nombres composés. Au contraire du test de Miller, le « test de Wilson » n'est jamais appliqué dans la pratique à cause du temps de calcul nécessaire, rédhibitoire.

CHAPITRE VIII

Polynômes

Les paragraphes suivants ont pour but de montrer que les propriétés et les algorithmes de la *divison euclidienne* pour les entiers ont des analogues pour les polynômes en une indéterminée à coefficients dans un corps. Nous ferons aussi des allusions à la manière dont on peut obtenir *d'autres corps finis* que les corps $\mathbb{F}_p$ définis au § VII.4.

1. Définition de l'anneau $\mathbb{K}[X]$

Soit $\mathbb{K}$ un corps. Par exemple : l'un des corps bien connus $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p$ (p premier), ou un corps dont la définition apparaît au paragraphe § VIII.4. Rappelons que, pour tout entier $n \geq 0$, on désigne par $\mathbb{K}^n$ l'ensemble des suites $(a_1, \ldots, a_n)$ avec $a_i \in \mathbb{K}$ $(1 \leq i \leq n)$, et qu'on considère en général $\mathbb{K}^n$ avec une structure convenable. (Le plus souvent, il s'agit de la structure d'espace vectoriel sur $\mathbb{K}$; parfois, il s'agit seulement de sa structure de groupe additif.)

1.1. Définitions. Un *polynôme à une indéterminée à coefficients dans* $\mathbb{K}$ est une suite infinie $(a_i)_{i\in\mathbb{N}}$ d'éléments de $\mathbb{K}$ telle qu'il existe un entier $n \in \mathbb{N}$ pour lequel $a_i = 0 \ \forall\ i > n$. On désigne par $\mathbb{K}[X]$ l'ensemble de tous les polynômes de ce type.

Le *degré* d'un polynôme $a = (a_i)_{i\in\mathbb{N}}$ dont les *coefficients* a_i ne sont pas tous nuls est le plus grand entier $n = \deg(a) \in \mathbb{N}$ pour lequel $a_n \neq 0$. Le *degré* du polynôme nul, c'est-à-dire du polynôme $(a_i)_{i\in\mathbb{N}}$ pour lequel $a_i = 0 \ \forall\ i \in \mathbb{N}$, est le symbole $-\infty$.

Nous adoptons la notation suivante, tout à fait courante [voir aussi le n° 5 ci-dessous] : au lieu de $(a_i)_{i\in\mathbb{N}}$, on écrit $\sum_{i\in\mathbb{N}} a_i X^i$, ou encore $a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n$ si $a_i = 0 \ \forall\ i > n$. Ainsi, le degré du polynôme $a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n$ est n si $a_n \neq 0$.

Si $P(X) = a_d X^d + a_{d-1} X^{d-1} + \cdots + a_0$ est un polynôme non nul de degré d, son *coefficient dominant* est a_d et son *terme constant* est a_0. On dit que $P(X)$ est *unitaire* si son coefficient dominant est 1. (Certains auteurs utilisent « monique » pour « unitaire ».)

1.2. Définitions. Etant donné deux polynômes

$$a = (a_i)_{i\in\mathbb{N}} \quad \text{et} \quad b = (a_i)_{i\in\mathbb{N}}$$

dans $\mathbb{K}[X]$, on définit leur *somme* et leur *produit* par

$$a + b = (c_i)_{i\in\mathbb{N}} \quad \text{avec} \quad c_i = a_i + b_i \quad \forall\ i \in \mathbb{N}$$

$$a\,b = (d_i)_{i\in\mathbb{N}} \quad \text{avec} \quad d_i = a_0 b_i + a_1 b_{i-1} + \cdots + a_i b_0 = \sum_{\substack{j,k\in\mathbb{N} \\ j+k=i}} a_j b_k \quad \forall\, i \in \mathbb{N}.$$

On vérifie que $a+b$ et ab sont bien dans $\mathbb{K}[X]$, c'est-à-dire que $c_i = 0$ et $d_i = 0$ pour tout i assez grand. Plus précisément, on vérifie l'énoncé suivant.

1.3. Proposition. *Pour $a, b \in \mathbb{K}[X]$, on a*

$$\begin{aligned} \deg(a+b) &\leq \max\big\{\deg(a), \deg(b)\big\} \\ \deg(ab) &= \deg(a) + \deg(b). \end{aligned}$$

Preuve. Cela résulte des définitions. On adopte les conventions $\max\{-\infty, n\} = n$ et $n + (-\infty) = (-\infty) + n = -\infty$ pour tout $n \in \mathbb{N}$. □

1.4. Proposition. *L'addition et la multiplication définies ci-dessus font de $\mathbb{K}[X]$ un anneau commutatif dont l'unité est le polynôme $(1, 0, 0, \ldots)$.*

Preuve. Tout à fait élémentaire, mais fastidieuse. Explicitons par exemple une étape pour la vérification de l'associativité de la multiplication.

Soient $a = (a_i)_{i\in\mathbb{N}}$, $b = (b_i)_{i\in\mathbb{N}}$, $c = (c_i)_{i\in\mathbb{N}}$ trois polynômes dans $\mathbb{K}[X]$. Pour tout $l \in \mathbb{N}$, les l-ièmes termes de $(ab)c$ et $a(bc)$ sont respectivement

$$\sum_{\substack{i,j,k\in\mathbb{N} \\ (i+j)+k=l}} (a_i b_j) c_k \quad \text{et} \quad \sum_{\substack{i,j,k\in\mathbb{N} \\ i+(j+k)=l}} a_i (b_j c_k),$$

et sont « donc » égaux, vu l'associativité de la multiplication dans le corps $\mathbb{K}$. □

La formule de la proposition 1.3 pour le degré d'un produit montre en particulier que $ab \neq 0$ si $a \neq 0$ et $b \neq 0$. En d'autres termes, dans l'anneau $\mathbb{K}[X]$, *le produit de deux éléments non nuls est non nul.*

1.5. Retour à la notation. L'élément zéro de l'anneau $\mathbb{K}[X]$ est la suite $(0, 0, \ldots)$ dont tous les termes sont des zéros. (Distinguer $0 \in \mathbb{K}$ de $0 = (0, 0, \ldots) \in \mathbb{K}[X]$, malgré l'abus de notation. « Il faudrait » écrire $0_{\mathbb{K}}$ et $0_{\mathbb{K}[X]}$, mais personne n'est assez puriste pour s'infliger cette lourdeur de notation !) L'élément 1 de l'anneau $\mathbb{K}[X]$ est la suite $(1, 0, 0, \ldots)$.

Plus généralement, à tout $a \in \mathbb{K}$ correspond un polynôme $(a, 0, 0, \ldots)$ dont le premier terme vaut a et tous les suivants 0, et l'application $a \longmapsto (a, 0, 0, \ldots)$ est un homomorphisme injectif de l'anneau $\mathbb{K}$ dans l'anneau $\mathbb{K}[X]$; son image est l'ensemble des polynômes de degrés ≤ 0. *Désormais, on identifie $\mathbb{K}$ à un sous-ensemble de $\mathbb{K}[X]$ grâce à cette bijection.* L'ensemble des polynômes de degré 0 est ainsi identifié à $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$.

On définit le polynôme

$$X = (0, 1, 0, 0, 0, \ldots)$$

avec un seul terme non nul. La définition de la multiplication montre que

$$\begin{aligned} X^2 &= (0, 0, 1, 0, 0, 0, \ldots) \\ X^3 &= (0, 0, 0, 1, 0, 0, \ldots) \\ X^4 &= (0, 0, 0, 0, 1, 0, \ldots) \end{aligned}$$

et ainsi de suite. Pour $a_0, a_1, a_2, a_3, \ldots \in \mathbb{K}$ (avec $a_i = 0$ pour i assez grand), on a donc

$$\begin{aligned} a_0 + a_1 X + a_2 X^2 + \cdots &= (a_0, 0, 0, 0, \ldots) + (0, a_1, 0, 0, \ldots) + (0, 0, a_2, 0, \ldots) + \cdots \\ &= (a_0, a_1, a_2, \ldots), \end{aligned}$$

ce qui justifie la notation usuelle, à laquelle il a déjà été fait allusion.

On écrit donc indifféremment

$$P = \sum_{j=0}^{n} a_j X^j \in \mathbb{K}[X] \qquad \text{ou} \qquad P(X) = \sum_{j=0}^{n} a_j X^j \in \mathbb{K}[X]$$

pour un polynôme de degré au plus n.

Remarques. (i) Il ne faut *surtout pas* considérer X comme représentant un « élément variable » de $\mathbb{K}$.

D'abord parce que, par exemple dans $\mathbb{F}_p[X]$, il faut soigneusement distinguer le polynôme X^p, de degré p, du polynôme X, de degré 1, même si $x^p = x$ pour tout $x \in \mathbb{F}_p$!

Ensuite parce qu'il est naturel, utile et fréquent d'évaluer un polynôme de $\mathbb{K}[X]$ sur un élément qui n'est pas dans $\mathbb{K}$!

Premier exemple. Le polynôme $X^2 + 1$, qui est dans $\mathbb{R}[X]$, peut fort bien être évalué en l'élément $i \in \mathbb{C}$, ce qui donne $i^2 + 1 = 0 \in \mathbb{C}$.

Second exemple. Le même polynôme $X^2 + 1$ peut être évalué sur une *matrice*, par exemple sur $J = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$, ce qui donne $J^2 + 1 = \begin{pmatrix} 2 & 2 & 1 \\ 0 & 2 & 2 \\ 0 & 0 & 2 \end{pmatrix}$. En revanche, si $P(X) \in \mathbb{R}[X]$ désigne le polynôme $(X-1)^3 = X^3 - 3X^2 + 3X - 1$, un calcul simple [1] montre que l'évaluation de $P(X)$ en J est la matrice nulle : $P(J) = 0$.

(ii) Une première variation sur ce qui précède consiste à définir l'anneau des suites $a = (a_i)_{i \in \mathbb{N}}$ avec $a_i \in \mathbb{K}$ pour tout $i \in \mathbb{N}$ (en permettant à une infinité de a_i d'être non nuls). On obtient ainsi l'anneau des *séries formelles à une indéterminée et à coefficients dans* $\mathbb{K}$ *;* nous ne l'étudierons pas dans ce cours.

Une seconde variation consiste à définir l'anneau des « suites doubles » $a = (a_{i,j})_{i,j \in \mathbb{N}}$ avec $a_{i,j} = 0$ pour i ou j assez grand. On obtient ainsi l'anneau des polynômes à DEUX indéterminées et à coefficients dans $\mathbb{K}$, anneau noté souvent $\mathbb{K}[X, Y]$, avec des éléments notés $\sum_{i,j \geq 0} a_{i,j} X^i Y^j$.

Une troisième variation consiste à remplacer le corps $\mathbb{K}$ par un anneau, par exemple par $\mathbb{Z}$. Nous y revenons plus bas au § VIII.5. Exercice : imaginer d'autres variations. [Une indication : séries convergentes.]

(iii) Il existe des « corps non commutatifs », par exemple le corps des quaternions de Hamilton. En revanche, dans ce chapitre (et le précédent), *tous les corps sont commutatifs.*

[1] Ceci n'est pas un hasard, mais l'illustration du *théorème de Cayley-Hamilton.* En effet $(X-1)^3$ est le polynôme caractéristique de la matrice J, et le théorème affirme que le polynôme d'une matrice carrée à coefficients dans un corps, évalué en la matrice elle-même, est la matrice nulle.

1.6. Applications polynomiales. Pour un corps $\mathbb{K}$, l'ensemble $\mathcal{A}ppl(\mathbb{K})$ des applications de $\mathbb{K}$ dans $\mathbb{K}$ est un anneau pour les opérations définies par

$$\begin{aligned}\big(\phi + \psi\big)(x) &= \phi(x) + \psi(x) \qquad \forall\, x \in \mathbb{K}\\ \big(\phi\,\psi\big)(x) &= \phi(x)\,\psi(x) \qquad \forall\, x \in \mathbb{K}\end{aligned}$$

pour tous $\phi, \psi \in \mathcal{A}ppl(\mathbb{K})$. L'application naturelle

$$\Pi : \begin{cases} \mathbb{K}[X] & \longrightarrow & \mathcal{A}ppl(\mathbb{K}) \\ \sum a_j X^j & \longmapsto & \Big(x \longmapsto \sum a_j x^j\Big) \end{cases}$$

(Π est un « pi » majuscule) est un homomorphisme d'anneaux. (Exercice : vérifier ces affirmations.) Par définition, une *application polynomiale* est une application dans l'image de l'homomorphisme Π.

1.7. Injectivité de Π. Si $\mathbb{K}$ est un corps fini, disons à q éléments, l'homomorphisme Π du 1.6 n'est pas injectif. En effet, l'anneau $\mathbb{K}[X]$ est un espace vectoriel sur $\mathbb{K}$ de dimension infinie, et en particulier un ensemble infini, alors que $\mathcal{A}ppl(\mathbb{K})$ est un anneau fini à q^q éléments. (Exercice : l'ensemble $\mathcal{A}ppl(\mathbb{K})$ a une structure naturelle d'espace vectoriel sur $\mathbb{K}$; vérifier que sa dimension est q.)

Si $\mathbb{K}$ est un corps infini, il résulte de la proposition 3.3 ci-dessous (« un polynôme de degré $d \geq 0$ a au plus d racines ») que l'homomorphisme naturel de $\mathbb{K}[X]$ dans $\mathcal{A}ppl(\mathbb{K})$ est injectif. (C'est par exemple « évident » dans le cas où $\mathbb{K}$ est le corps des nombres réels.)

1.8. Surjectivité de Π. Soit $\mathbb{K}$ un corps. Soit $N \geq 1$ un entier ; notons $\mathcal{P}_{\mathbb{K}}^N$ le sous-espace de $\mathbb{K}[X]$ des polynômes de degrés au plus N ; c'est un espace vectoriel de dimension $N+1$, avec base $\{1, X, X^2, \ldots, X^N\}$.

Supposons que $\mathbb{K}$ contienne $N+1$ éléments $x_0, x_1, \ldots, x_N$ distincts deux à deux. Pour tout $j \in \{0, 1, \ldots, N\}$, posons

$$P_j(X) = \prod_{0 \leq k \leq N, k \neq j} \frac{X - x_k}{x_j - x_k}\,,$$

qui est un élément de $\mathcal{P}_{\mathbb{K}}^N$. La définition implique que $P_j(x_k) = 1$ si $k = j$ et $P_j(x_k) = 0$ sinon. [Bien que ce soit inutile pour la suite de ce numéro, on peut noter que $P_0, P_1, \ldots, P_N$ sont linéairement indépendants, et constituent donc une base de $\mathcal{P}_{\mathbb{K}}^N$.]

On peut utiliser ces polynômes pour montrer le résultat suivant :

lorsque le corps $\mathbb{K}$ est fini, l'homomorphisme Π du 1.6 est surjectif.

En effet, soit $\psi \in Appl(\mathbb{K})$ une application de $\mathbb{K}$ dans $\mathbb{K}$. Soit N l'entier tel que $\mathbb{K}$ soit d'ordre $N+1$, soit $x_0, \ldots, x_N$ une énumération des éléments de $\mathbb{K}$, et soient $P_0, \ldots, P_N$ comme ci-dessus. Si on pose

$$P_\psi(X) = \sum_{0 \leq k \leq N} \psi(x_k) P_k(X) \in \mathcal{P}_{\mathbb{K}}^N,$$

on vérifier que $P_\psi(x_j) = \psi(x_j)$ pour tout $j \in \{0, \ldots, N\}$, c'est-à-dire que $\Pi(P(X)) = \psi$.

On sait bien que, si $\mathbb{K} = \mathbb{R}$, l'application Π n'est pas surjective (par exemple parce qu'une application non continue de $\mathbb{R}$ dans $\mathbb{R}$ n'est pas polynomiale). Plus généralement,

si $\mathbb{K}$ est un corps infini, il résulte à nouveau de la proposition 3.4 ci-dessous que l'homomorphisme naturel de $\mathbb{K}[X]$ dans $\mathcal{A}ppl(\mathbb{K})$ n'est pas surjectif, puisqu'une application de $\mathbb{K}$ dans $\mathbb{K}$ non nulle en exactement un point n'est pas dans l'image de Π.

Résumé des deux numéros précédents. Les trois assertions suivantes sont équivalentes :

(i) le corps $\mathbb{K}$ est fini,

(ii) l'application Π est surjective,

(iii) l'application Π n'est pas injective.

Exercices du § VIII.1

(VIII.1) Soit $\mathbb{K}$ un corps fini, à q éléments. On considère le polynôme

$$G(X) = \prod_{x\in\mathbb{K}}(X-x).$$

(i) Ecrire $G(X)$ lorsque $\mathbb{K}=\mathbb{F}_p$, et $p\leq 7$.

(ii) Déterminer le degré d de $G(X)$, le coefficient de son terme de degré d et son terme constant.

(iii) Pour tout $y\in\mathbb{K}$, soit $G_y(X)$ le quotient de $G(X)$ par $X-y$. Que pouvez-vous dire des valeurs de G_y aux différents points de $\mathbb{K}$?

(iv)$^\sharp$ Lorsque $\mathbb{K}=\mathbb{F}_p$, déterminer le coefficient du terme de degré $d-1$ de $G(X)$.

2. Division des polynômes

Dans tout ce paragraphe, $\mathbb{K}$ désigne un corps et $\mathbb{K}[X]$ l'anneau de polynômes défini au paragraphe précédent.

2.1. Théorème (division euclidienne). *Soient $F,P\in\mathbb{K}[X]$ tels que $P\neq 0$. Il existe alors deux polynômes $Q,R\in\mathbb{K}[X]$ tels que*

$$F = PQ+R \quad et \quad \deg(R) < \deg(P).$$

De plus Q et R sont univoquement déterminés par ces conditions.

Preuve. On pose $f=\deg(F)$ et $p=\deg(P)$. [Ne pas croire que p est ici un nombre premier !]

Existence. Montrons d'abord l'existence de Q et R lorsque $f\leq 0$. Si $F=0$, on pose $Q=R=0$. Si $f=0$, c'est-à-dire si F est un élément non nul du corps $\mathbb{K}$, on pose $Q=0$ et $R=P$ si $p>0$, et $Q=(P)^{-1}F$ et $R=0$ si $p=0$.

On procède ensuite par récurrence sur f, en supposant $f\geq 1$ et l'existence démontrée pour tous les couples de polynômes (F',P') tels que $\deg(F')<f$. On pose

$$\begin{aligned} F &= a_fX^f+\cdots+a_1X+a_0 \qquad \text{avec } a_f\neq 0\\ P &= b_pX^p+\cdots+b_1X+b_0 \qquad \text{avec } b_p\neq 0. \end{aligned}$$

On distingue à nouveau deux cas. (i) Si $f < p$, on pose $Q = 0$ et $R = F$. (ii) Si $f \geq p$, alors

$$\begin{aligned} F - \frac{a_f}{b_p} X^{f-p} P &= \left(a_f X^f + a_{f-1} X^{f-1} + \cdots\right) - \frac{a_f}{b_p}\left(b_p X^f + b_{p-1} X^{f-1} + \cdots\right) \\ &= \left(\qquad a_{f-1} X^{f-1} + \cdots\right) - \frac{a_f}{b_p}\left(\qquad b_{p-1} X^{f-1} + \cdots\right) \end{aligned}$$

est de degré strictement inférieur à f ; on peut donc appliquer l'hypothèse de récurrence au couple $\left(F - \frac{a_f}{b_p} X^{f-p} P, P\right)$, et par suite il existe des polynômes Q', R tels que

$$F - \frac{a_f}{b_p} X^{f-p}\, P = PQ' + R \quad \text{et} \quad \deg(R) < \deg(P).$$

On a donc aussi

$$F \;=\; P\left(\frac{a_f}{b_p} X^{f-p} + Q'\right) + R \quad \text{et} \quad \deg(R) < \deg(P)$$

et il suffit de poser $Q = \frac{a_f}{b_p} X^{f-p} + Q'$.

Unicité. Supposons qu'on puisse écrire

$$F \;=\; PQ + R \;=\; PQ' + R' \quad \text{avec} \quad \deg(R) < \deg(P) \quad \text{et} \quad \deg(R') < \deg(P).$$

Si on avait $Q \neq Q'$, on aurait $P(Q - Q') = R' - R$, ce qui est absurde car

$$\deg(P(Q - Q')) \;\geq\; \deg(P) \qquad \text{et} \qquad \deg(R' - R) \;<\; \deg(P)$$

par la proposition 1.3. Donc $Q' = Q$, et par suite aussi $R' = R$. □

Exercice. Identifier dans le preuve ci-dessus le passage où il est important que $\mathbb{K}$ soit un corps (et non pas, par exemple, l'anneau $\mathbb{Z}$).

Exemple. Si $\mathbb{K} = \mathbb{F}_3$, $F = X^3 + X^2 + 2$ et $P = 2X^2 + X$, alors

$$X^3 + X^2 + 2 \;=\; (2X^2 + X)\,(2X + 1) \;+\; (2X + 2)$$

de sorte que $Q = 2X + 1$ et $R = 2X + 2$.

2.2. Définition. Soit A un anneau commutatif. Un *idéal* de A est une partie non vide $\mathcal{I}$ de A telle que, pour tous $a, b \in \mathcal{I}$ et $x \in A$, on a $a + b \in \mathcal{I}$ et $ax \in \mathcal{I}$.

Un idéal $\mathcal{I}$ de A est *principal* s'il existe un élément $a \in A$ tel que $\mathcal{I} = aA$. Dans ce cas, on écrit souvent (a) au lieu de aA.

Etant donné des éléments $a_1, \ldots, a_n \in A$ et des sous-ensembles $S_1, \ldots, S_n \subset A$, on note $a_1 S_1 + \cdots + a_n S_n$ le sous-ensemble de A constitué des éléments de la forme $a_1 s_1 + \cdots + a_n s_n$, avec $s_1 \in S_1, \ldots, s_n \in S_n$. Il est *évident* qu'un sous-ensemble de A de la forme

$$I \;=\; a_1 A + \cdots + a_n A$$

est un idéal dans A.

Rappel (proposition 1.13 du chapitre précédent) : tout idéal de $\mathbb{Z}$ est principal. Ainsi, par exemple :

$$4\mathbb{Z} + 6\mathbb{Z} \;=\; 2\mathbb{Z}$$

(sic).

2.3. Proposition. *Si $\mathbb{K}$ est un corps, tout idéal de l'anneau de polynômes $\mathbb{K}[X]$ est principal.*

Preuve. Soit $\mathcal{I}$ un idéal de $\mathbb{K}[X]$. Si $\mathcal{I} = \{0\}$, il n'y a rien à montrer.

Sinon, on choisit $D \in \mathcal{I}$, $D \neq 0$, avec $\deg(D)$ minimal (c'est-à-dire $\deg(D) \leq \deg(F)$ pour tout $F \in \mathcal{I}$, $F \neq 0$). Soit alors $F \in \mathcal{I}$, $F \neq 0$. On écrit $F = DQ + R$ comme au théorème 1. Comme $R \in \mathcal{I}$ et $\deg(R) < \deg(D)$, il résulte de la définition de D que $R = 0$. On en déduit que $F \in D\mathbb{K}[X]$; en d'autres termes, $\mathcal{I}$ est contenu dans l'idéal principal défini par D, ce qu'il fallait montrer. [Comparer avec la preuve de la proposition 1.13 du chapitre précédent.] □

2.4. Définition. Un anneau commutatif A est *intègre* s'il contient au moins deux éléments et si $ab \neq 0$ pour toute paire $(a, b) \in A^2$ d'éléments non nuls.

Par exemple, $\mathbb{Z}$ est intègre, et tout corps est intègre ; il résulte de la proposition 1.3 que tout anneau de polynômes à une indéterminéee sur un corps est intègre. En revanche, $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre lorsque l'entier $n \geq 2$ n'est pas premier.

2.5. Proposition. *Soient A un anneau commutatif intègre et d_1, d_2 deux éléments non nuls de A. Pour que $d_1A = d_2A$, il faut et il suffit qu'il existe un élément inversible $u \in A$ tel que $d_2 = d_1u$.*

Preuve. Comme $d_2 \in d_2A$, on a aussi $d_2 \in d_1A$, et il existe donc $u \in A$ tel que $d_2 = d_1u$. De même il existe $v \in A$ tel que $d_1 = d_2v$. Par suite $d_2(1 - vu) = 0$. Comme $d_2 \neq 0$ et comme A est intègre, l'élément u est inversible (d'inverse v). □

Rappel. Dans l'anneau $\mathbb{Z}$, les éléments inversibles sont 1 et -1.

Remarque. Si $\mathbb{K}$ est un corps, les éléments inversibles de l'anneau de polynômes $\mathbb{K}[X]$ sont les constantes non nulles.

Preuve. Cela résulte immédiatement le la proposition 1.3. □

2.6. Idéaux principaux de $\mathbb{K}|X]$ (précision à la proposition 2.3). *Il résulte de ce qui précède que tout idéal principal $I \neq \{0\}$ de $\mathbb{K}[X]$ s'écrit d'une seule manière $I = P(X)\mathbb{K}[X]$ avec $P(X)$ un polynôme unitaire.*

2.7. Proposition. *Soient $\mathbb{K}$ un corps et $P_1(X), \ldots, P_n(X) \in \mathbb{K}[X]$ des polynômes non tous nuls ; soit $D(X) \in \mathbb{K}[X]$ un polynôme[2] tel que*

$$P_1(X)\mathbb{K}[X] + \cdots + P_n(X)\mathbb{K}[X] \;=\; D(X)\mathbb{K}[X]. \qquad (*)$$

Alors les diviseurs de $D(X)$ sont les diviseurs communs des $P_1(X), \ldots, P_n(X)$. En particulier, pour tout diviseur commun $D'(X)$ des $P_1(X), \ldots, P_n(X)$, on a

$$\deg(D') \;\leq\; \deg(D),$$

avec égalité si et seulement s'il existe $a \in \mathbb{K}^*$ tel que $D'(X) = aD(X)$.

[2] Un tel polynôme existe en vertu de la proposition 2.3.

PREUVE. L'égalité (∗), qui est une égalité entre sous-ensembles de $\mathbb{K}[X]$, implique d'une part que, pour tout $j \in \{1, \dots, n\}$, il existe $Q_j(X) \in \mathbb{K}[X|$ tel que $P_j(X) = D(X)Q_j(X)$; il en résulte que tout diviseur de $D(X)$ est un diviseur commun des $P_j(X)$.

La même égalité implique d'autre part qu'il existe des polynômes $R_1(X), \dots, R_n(X)$ tels que $D(X) = P_1(X)R_1(X) + \cdots + P_n(X)R_n(X)$; il en résulte que tout diviseur commun aux $P_j(X)$ est un diviseur de $D(X)$. □

2.8. Définitions. Soit $\mathbb{K}$ un corps. Un *plus grand commun diviseur* ou *pgcd* de polynômes non tous nuls $P_1(X), \dots, P_n(X) \in \mathbb{K}[X]$ est un polynôme $D(X)$ tel que

$$P_1(X)\mathbb{K}[X] + \cdots + P_n(X)\mathbb{K}[X] = D(X)\mathbb{K}[X]. \qquad (**)$$

Vu ce qui précède, un tel polynôme existe toujours, est déterminé à multiplication près par une constante non nulle, et son degré est le maximum des degrés des diviseurs communs aux $P_j(X)$.

Par abus de langage, on dit parfois que $D(X)$ est « le »pgcd des $P_j(X)$. Notons encore qu'il existe un unique polynôme *unitaire* satisfaisant (∗∗).

On dit que des polynômes non tous nuls $P_1(X), \dots, P_n(X) \in \mathbb{K}[X]$ sont *premiers entre eux* si leurs seuls diviseurs communs sont les constantes non nulles (c'est-à-dire les éléments de $\mathbb{K}^*$). Vu ce qui précède, des polynômes non tous nuls $P_1(X), \dots, P_n(X)$ sont premiers entre eux si et seulement si leurs pgcd sont les constantes non nulles.

Par exemple, pour $a, b \in \mathbb{K}$ tels que $a \neq b$, les polynômes $X - a$ et $X - b$ sont premiers entre eux.

2.9. Théorème de Bézout. Comme cas particulier de ce qui précède, nous avons le

THÉORÈME. *Pour que deux polynômes $P_1(X), P_2(X) \in \mathbb{K}[X]$ soient premiers entre eux (= n'aient pas d'autres diviseurs communs que les polynômes constants non nuls), il faut et il suffit qu'il existe $Q_1(X), Q_2(X) \in \mathbb{K}[X]$ tels que*

$$P_1(X)Q_1(X) + P_2(X)Q_2(X) = 1.$$

Plus généralement, pour que des polynômes $P_1, \dots, P_n \in \mathbb{K}[X]$ non tous nuls soient premiers entre eux, il faut et il suffit qu'il existe $Q_1, \dots, Q_n \in \mathbb{K}[X]$ tels que

$$P_1(X)Q_1(X) + \cdots + P_n(X)Q_n(X) = 1.$$

2.10. COROLLAIRE. *Soient $P_1(X), P_2(X), P_3(X) \in \mathbb{K}[X]$ des polynômes tels que $P_1(X)$ et $P_2(X)$ soient premiers entre eux. Si $P_1(X)$ divise $P_2(X)P_3(X)$, alors $P_1(X)$ divise $P_3(X)$.*

PREUVE (identique à celle de la proposition 1.10 du chapitre précédent). Par hypothèse, il existe $Q_1(X), Q_2(X) \in \mathbb{K}[X]$ tels que $P_1(X)Q_1(X) + P_2(X)Q_2(X) = 1$. Par suite

$$P_1(X)P_3(X)Q_1(X) + P_2(X)P_3(X)Q_2(X) = P_3(X).$$

Le polynôme $P_1(X)$ divise alors les deux produits du terme de gauche ; il divise donc aussi le terme de droite $P_3(X)$. □

2.11. Algorithme d'Euclide pour le calcul du pgcd de deux polynômes $D_1(X), D_2(X)$ tels que $\deg(D_1(X)) \geq \deg(D_2(X)) \geq 0$. L'enoncé détaillé est laissé au lecteur (parallèle en tout point à celui du § VII.1).

EXEMPLES. (i) Dans $\mathbb{R}[X]$, les polynômes X^2+1 et X^2+3X+2 sont premiers entre eux, et on a

$$\Big(X^2+1\Big)\Big(\frac{3}{10}X+\frac{8}{10}\Big) \;-\; \Big(X^2+3X+2\Big)\Big(\frac{3}{10}X-\frac{1}{10}\Big) \;=\; 1. \qquad (*)$$

(ii) Les polynômes X^3+6X^2-7 et X^8-4X+3 ne sont pas premiers entre eux car les fonctions polynomiales associées s'annulent toutes deux en $x=1$. (Ceci vaut aussi bien dans $\mathbb{Q}[X]$ que dans $\mathbb{F}_p[X]$, pour tout nombre premier p.)

(iii) Attention : les polynômes X^2+5 et X^2+4X+3 sont premiers entre eux dans $\mathbb{Q}[X]$, car

$$(X^2+5)\left(\frac{X}{21}+\frac{3}{14}\right) \;-\; (X^2+4X+3)\left(\frac{X}{21}+\frac{1}{42}\right) \;=\; 1 \qquad (**)$$

mais pas dans $\mathbb{F}_7[X|$, car

$$X^2+5 \;=\; (X+3)(X+4) \qquad \text{et} \qquad X^2+4X+3 \;=\; (X+3)(X+1).$$

Noter que le «5» de $X^2+5 \in \mathbb{Q}[X]$ n'est pas égal au «5» de $X^2+5 \in \mathbb{F}_7[X]$, ce dernier étant un abus de notation pour l'élément de $\mathbb{F}_7 = \mathbb{Z}/7\mathbb{Z}$ noté ailleurs $[5]_7$.

EXERCICE. retrouver les identités $(*)$ et $(**)$ en appliquant l'algorithme d'Euclide.

Exercices du § VIII.2

(VIII.2) On considère les polynômes $P_1(X) = (X-1)^3$ et $P_2(X) = X^2$ dans $\mathbb{Q}[X]$.

(i) Expliciter les quotients Q_2, Q_3 et les restes P_3, P_4 des divisions euclidiennes $P_1 = P_2Q_2 + P_3$ et $P_2 = P_3Q_3 + P_4$.

[*Indication* : $P_4(X) = \frac{1}{9}$.]]

(ii) En déduire la forme explicite de polynômes $T_1, T_2 \in \mathbb{Q}[X]$ tels que

$$1 \;=\; P_1(X)T_1(X) + P_2(X)T_2(X).$$

(VIII.3) Soient $\mathbb{K}$ un corps, $P(X)$, $Q(X)$ deux polynômes non nuls à coefficients dans $\mathbb{K}$, et $(P(X)), (Q(X)) \subset \mathbb{K}[X]$ les idéaux principaux correspondants.

Montrer que $(P(X)) \subset (Q(X))$ si et seulement si $Q(X)$ divise $P(X)$.

(VIII.4) Soient $\mathbb{K}$ un corps et η un élément de $\mathbb{K}$. Montrer qu'il existe un unique homomorphisme d'anneaux $\Phi : \mathbb{K}[X] \longrightarrow \mathbb{K}$ tel que $\Phi(X) = \eta$ et $\Phi(\xi) = \xi$ pour tout $\xi \in \mathbb{K}$, et que cet homomorphisme est donné par $\Phi(P(X)) = P(\eta)$.

(VIII.5) Montrer que les quatre anneaux $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathbb{F}_2[X]/(X^2+X+1)$ et $\mathbb{F}_2[X]/(X^2)$ sont non-isomorphes deux à deux.

3. Racines des polynômes à une indéterminée

Aux paragraphes § VIII.3 et § VIII.4, on désigne par $\mathbb{K}$ un corps et par $\mathbb{K}[X]$ l'anneau des polynômes à une indéterminéee à coefficients dans $\mathbb{K}$.

3.1. Définition. Soit $P(X) = \sum_{j=0}^{n} a_j X^j$ un polynôme dans $\mathbb{K}[X]$; pour $c \in \mathbb{K}$, on pose[3] $P(c) = \sum_{j=0}^{n} a_j c^j$. On dit que $c \in \mathbb{K}$ est une *racine* ou un *zéro* de P si $P(c) = 0$.

3.2. Proposition. *Soient $P(X) \in \mathbb{K}[X]$ et $c \in \mathbb{K}$. Alors c est une racine de P si et seulement si $(X - c) \mid P(X)$.*

Schéma de la preuve. Un sens est évident. Pour l'autre, écrire d'abord le résultat $P = (X-c)Q+R$ de la division euclidienne, où R est un polynôme constant ; on constate que, si c est une racine de P, alors $R = 0$. □

Exemples. (i) Lorsque $\mathbb{K} = \mathbb{C}$, le nombre complexe i est une racine du polynôme $X^2 + 1$, et

$$X^2 + 1 \;=\; (X + i)(X - i) \;\in\; \mathbb{C}[X].$$

(ii) Lorsque $\mathbb{K} = \mathbb{F}_2$, le nombre 1 est une racine du polynôme $X^3 + X^2 + X + 1$, et

$$X^3 + X^2 + X + 1 \;=\; (X + 1)^3 \;\in\; \mathbb{F}_2[X].$$

Tout polynôme de $\mathbb{R}[X]$ de degré impair possède une racine : c'est une conséquence presqu'immédiate du théorème de la valeur intermédiaire[4].

3.3. Proposition. *Un polynôme $P(X) \in \mathbb{K}[X]$ de degré $d \geq 0$ a au plus d racines dans $\mathbb{K}$.*

Preuve. La proposition étant évidente pour $d = 0$, on suppose que $d > 0$ et que la proposition est vraie jusqu'à $d - 1$. Soit $P(X) \in \mathbb{K}[X]$ un polynôme de degré d. Si $P(X)$ n'a aucune racine, il n'y a rien à montrer. Si $P(X)$ possède une racine $c \in \mathbb{K}$, il existe un polynôme $Q(X)$ de degré $d - 1$ tel que $P(X) = (X - c)Q(X)$, de sorte que l'ensemble des racines de $P(X)$ est égal à la réunion de $\{c\}$ et de l'ensemble des racines de $Q(X)$. Par suite $P(X)$ possède au plus $1 + (d - 1) = d$ racines. □

[3] Avec une notation du numéro 1.6, le nombre $P(c)$ de $\mathbb{K}$ est la valeur en c de l'application polynomiale $\Pi(P)$.

[4] Détails. Soit P un tel polynôme ; pour un nombre réel t assez grand, le signe de $P(t)$ est égal au signe du coefficient dominant de P, alors que le signe de $P(-t)$ est opposé. Il existe donc $u \in]-t, t[$ tel que $P(u) = 0$.

3.4. Théorème. *Soit $\mathbb{K}$ un corps fini.*

Le groupe multiplicatif $\mathbb{K}^*$ des éléments non nuls de $\mathbb{K}$ est cyclique. De plus, si q est l'ordre de $\mathbb{K}$, le groupe $\mathbb{K}^*$ possède $\varphi(q-1)$ générateurs

Preuve. Montrons plus généralement que, pour tout corps $\mathbb{K}$, tout sous-groupe fini G de $\mathbb{K}^*$ est cyclique ; autrement dit (voir la au numéro 5.9 la définition de « groupe cyclique fini »), pour tout sous-groupe G de $\mathbb{K}^*$ d'ordre n fini, il existe un élément $c \in G$ tel que $G = \{1 = c^0, c, c^2, \dots, c^{n-1}\}$. (Attention : pour G donné d'ordre $n \geq 3$, il y a plusieurs choix possibles de c !) Ensuite, dans le cas où $\mathbb{K}$ est fini, il suffit de particulariser à $G = \mathbb{K}^*$.

Pour tout diviseur d de n, notons $\psi(d)$ le nombre des éléments de G qui sont d'ordre d.

Soit d un diviseur de n tel que $\psi(d) > 0$, donc tel qu'il existe $a \in G$ d'ordre d. Montrons que $\psi(d) = \varphi(d)$, où φ désigne la fonction d'Euler. Par hypothèse, $a^0 = 1, a, a^2, \dots, a^{d-1}$ sont des éléments distincts de G, et sont tous des racines du polynôme $X^d - 1$. La proposition précédente montre que ce polynôme n'a pas d'autre racine. Donc tout élément $b \in \mathbb{K}^*$ tel que $b^d = 1$ est une puissance de a. Il résulte alors de l'exercice (VII.47) qu'il y a exactement $\varphi(d)$ éléments d'ordre d dans $\mathbb{K}^*$, et que ces élémenhts sont d'ailleurs tous dans G.

Montrons que $\psi(d) > 0$ pour tout diviseur d de n. Si ce n'était pas vrai, le décompte des éléments de G donnerait

$$n = \sum_{d|n} \psi(d) = \sum_{\substack{d|n \\ \psi(d)>0}} \psi(d) = \sum_{\substack{d|n \\ \psi(d)>0}} \varphi(d) < \sum_{d|n} \varphi(d) = n$$

(la dernière égalité par la proposition 5.6(ii)), ce qui est absurde.

En particulier, il existe $\varphi(n) \geq 1$ éléments de G qui sont d'ordre n, et G est un groupe cyclique. (Nous avons de plus montré que, dès que G poss'ede un élément d'un certain ordre, tout élément de $\mathbb{K}^*$ de même ordre est dans G.) □

Il existe des corps fini d'ordres arbitrairement grands, par exemple $\mathbb{Z}/p\mathbb{Z}$ pour p un « grand » nombre premier ou un corps d'ordre 2^a pour a un « grand » nombre entier. Soient $\mathbb{K}$ un tel corps et c un générateur de $\mathbb{K}^*$. L'application

$$E : \{0, 1, \dots, 2^a - 2\} \approx \mathbb{Z}/(2^a - 1)\mathbb{Z} \longrightarrow \mathbb{K}^* \qquad k \longmapsto c^k$$

est une bijection, et possède donc un inverse

$$D : \mathbb{K}^* \longrightarrow \{0, 1, \dots, 2^a - 2\}$$

qui est un « analogue discret de l'application logarithme » . Il se trouve que le calcul de $D(x)$ pour $x \in \mathbb{K}^*$ est beaucoup plus difficile (au moins avec les connaissances actuelles) que le calcul de $E(k)$ pour $k \in \{0, 1, \dots, 2^a - 2\}$ (voir le § VII.7). Cette asymétrie est l'ingrédient de base de certains codes à clé publique (voir par exemple le § 7.4 du livre de Buchmann déjà cité).

4. Polynômes irréductibles et quotients $\mathbb{K}[X]/(P)$ qui sont des corps

4.1. Définition. Un polynôme $P \in \mathbb{K}[X]$ est *irréductible* si $\deg(P) \geq 1$ et si, pour toute paire $P_1, P_2 \in \mathbb{K}[X]$ telle que $P = P_1 P_2$, l'un des polynômes P_1, P_2 est constant.

Soient $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$, $a \neq 0$. Alors P est irréductible dans $\mathbb{K}[X]$ si et seulement si aP l'est. Pour tester si P est irréductible, il est souvent pratique de se ramenr (si nécessaire) au cas du polynôme unitaire P/a_0, où a_0 est le coefficient dominant de P.

Exemples. (i) Tout polynôme de degré 1.

(ii) $X^2 + 1 \in \mathbb{R}[X]$. Plus généralement, $aX^2 + bX + c \in \mathbb{R}[X]$ est irréductible si et seulement si $b^2 - 4ac < 0$. En revanche, $X^2 + 1$ est réductible dans $\mathbb{C}[X]$! En fait, un polynôme de $\mathbb{C}[X]$ est irréductible si et seulement s'il est de degré un.

(iii) Dans $\mathbb{F}_2[X]$, le polynôme X^2+X+1 est irréductible. Une manière de le vérifier est d'écrire la liste des polynômes de degré 1 dans $\mathbb{F}_2[X]$ et la liste des produits de deux d'entre eux[5], et de constater que X^2+X+1 n'apparaît pas dans la seconde liste.

L'argument montre davantage, à savoir que, dans $\mathbb{F}_2[X]$, il existe un unique polynôme irréductible de degré 2, qui est X^2+X+1.

Il faut des moyens plus élaborés pour vérifier par exemple que $X^{12}+X^3+1$ ou $X^{100}+X^{25}+1$ sont des polynômes irréductibles dans $\mathbb{F}_2[X]$.

(iv) Dans $\mathbb{F}_2[X]$, le polynôme $X^4+X^3+X^2+X+1$ est irréductible. En effet, il n'est divisible par aucun polynôme de degré 1, car il n'a pas de racine, ni par l'unique polynôme irréductible de degré 2, car $X^4+X^3+X^2+X+1 = X^2(X^2+X+1)+(X+1)$.

(v) Un polynôme réductible P de degré $d \geq 2$ s'écrit $P = P_1P_2$, avec P_1, P_2 de degrés $d_1, d_2 \geq 1$, et $d = d_1 + d_2$. Il en résulte qu'un polynôme de degré 2 ou 3 est irréductible si et seulement s'il n'a pas de racine. En revanche, il existe des polynômes de degré ≥ 4 sans racine qui sont réductibles, par exemple $(X^2+1)^n$ dans $\mathbb{R}[X]$ pour tout $n \geq 2$.

Bien qu'il soit en général difficile de décider si un polynôme donné est irréductible[6], il existe plusieurs critères s'appliquant dans diverses situations. Dans ce cours, nous n'en utiliserons que trois :

- le critère des listes complètes, qui s'applique si l'ordre du corps $\mathbb{K}$ et le degré du polynôme sont petits (exemples (iii) et (iv) ci-dessus) ;
- le critère des racines, qui s'applique si le degré du polynôme est 2 ou 3 (exemple (v) ci-dessus) ;
- le critère d'Eisenstein du § VIII.5 pour les polynômes à coefficients dans $\mathbb{Q}$.

Exercice. Montrer que tout polynôme irréductible de $\mathbb{R}[X]$ est de degré 1 ou 2. [Utiliser le fait que tout polynôme à coefficients réels de degré au moins 1 possède des racines complexes.]

Les polynôme irréductibles jouent en un sens le même rôle dans $\mathbb{K}[X]$ que les nombres premiers dans $\mathbb{Z}$. En particulier, on a un analogue de la factorisation en nombres premiers.

4.2. Théorème (existence et unicité de la factorisation). *Tout polynôme non nul $P \in \mathbb{K}[X]$ est produit de polynômes irréductibles, uniquement déterminés à l'ordre près et à des constantes multiplicatives de $\mathbb{K}^*$ près.*

Remarque (à propos de l'énoncé). Dans le cas où P est de degré zéro, le théorème dit que P est à une constante multiplicative près «le produit vide» de polynômes irréductibles (produit vide qui vaut 1).

Preuve de l'existence. Si P est de degré un, il n'y a rien à montrer. On procède ensuite par récurrence sur le degré de P, comme pour la preuve du théorème 2.2 du chapitre précédent (factorisation des entiers en produit de nombres premiers). □

[5] Il y a exactement deux polynômes de degré 1, à savoir X et $X+1$, et par suite trois éléments dans la seconde liste, à savoir X^2, $X(X+1) = X^2+X$ et $(X+1)^2 = X^2+1$.

[6] De même qu'il est difficile de décider si un nombre entier est premier !

PREUVE DE L'UNICITÉ. On utilise le corollaire 2.10, et on procède à nouveau comme pour la preuve du théorème 2.2 (voir aussi le lemme 2.3) du chapitre précédent. □

Voici un énoncé équivalent.

4.3. THÉORÈME (existence et unicité de la factorisation). *Pour tout polynôme non nul $P \in \mathbb{K}[X]$, il existe des polynômes irréductibles $P_1, \dots, P_k$ à coefficients dominants 1 tels que $P = c\prod_{j=1}^{k} P_j$, où $c \in \mathbb{K}^*$ est le coefficient dominant de P. De plus les P_j sont univoquement déterminés pas P, à l'ordre près.*

4.4. Définitions (voir § VII.3 et § VII.4). Soit A un anneau commutatif et $\mathcal{I}$ un idéal de A. On définit une relation d'équivalence « $\equiv \pmod{\mathcal{I}}$ » sur A en posant

$$x \equiv y \pmod{\mathcal{I}} \quad \text{si} \quad x - y \in \mathcal{I}.$$

Les classes d'équivalence forment un ensemble qu'on appelle l'ensemble quotient et qu'on note $A/\mathcal{I}$. On vérifie que, pour $x, x', y, y' \in A$ avec $x \equiv x' \pmod{\mathcal{I}}$ et $y \equiv y' \pmod{\mathcal{I}}$ on a $x + y \equiv x' + y' \pmod{\mathcal{I}}$ et $xy \equiv x'y' \pmod{\mathcal{I}}$. Il en résulte d'abord qu'on peut définir une addition et une multiplication sur $A/\mathcal{I}$ en posant

$$\begin{aligned} {}_{\mathcal{I}} + [y]_{\mathcal{I}} &= [x+y]_{\mathcal{I}} \\ [x]_{\mathcal{I}}\,[y]_{\mathcal{I}} &= [xy]_{\mathcal{I}} \end{aligned}$$

pour tous $x, y \in A$, où $[x]_{\mathcal{I}}$ désigne la classe de x dans $A/\mathcal{I}$. Il en résulte ensuite que ces opérations font de $A/\mathcal{I}$ un anneau commutatif, qui est *l'anneau quotient de A par $\mathcal{I}$*.

Les définitions et les vérifications sont en tout point analogues à celles menant à un anneau du type $\mathbb{Z}/a\mathbb{Z}$, aussi noté $\mathbb{Z}/(a)$, des classes d'entiers modulo un entier a.

4.5. Exemple fondamental : l'anneau $\mathbb{K}[X]/(P)$, quotient de $\mathbb{K}[X]$ par l'idéal principal $(P) = P\mathbb{K}[X]$. En plus de sa structure d'anneau, l'ensemble $\mathbb{K}[X]/(P)$ possède une structure naturelle d'*espace vectoriel* sur $\mathbb{K}$, de dimension égale au degré de P. Plus précisément :

4.6. PROPOSITION. *Soit $P \in \mathbb{K}[X]$ un polynôme de degré $d \geq 1$, et soit E le sous-espace vectoriel de $\mathbb{K}[X]$ des polynômes de degrés strictement inférieurs à d.*

La composition de l'injection $E \longrightarrow \mathbb{K}[X]$ et de la projection canonique $\mathbb{K}[X] \longrightarrow \mathbb{K}[X]/(P)$ est un isomorphisme de $\mathbb{K}$-espaces vectoriels de E sur $\mathbb{K}[X]/(P)$.

En particulier, si $\mathbb{K}$ est fini, d'ordre q, alors $\mathbb{K}[X]/(P)$ est fini, d'ordre q^d.

PREUVE. C'est une conséquence immédiate des propriétés de la division euclidienne. □

A chaque classe modulo (P), c'est-à-dire à chaque élément de $\mathbb{K}[X]/(P)$, on associe son *représentant canonique* dans $\mathbb{K}[X]$ qui est l'unique polynôme dans cette classe de degré strictement inférieur à celui de $P(X)$.

EXEMPLE. Calculons le polynôme de degré ≤ 2 qui définit dans $\mathbb{F}_7[X]/(X^3+1)$ la même classe que $(X^2+2)(X^2+5)$. On a

$$(X^2+2)(X^2+5) \;=\; X^4+3 \;=\; X(X^3+1)+6X+3$$

de sorte que le polynôme cherché est $6X+3$. En d'autres termes :

$$(X^2+2)(X^2+5) \;\equiv\; 6X+3 \pmod{X^3+1}.$$

4.7. LEMME. *Soient $\mathbb{K}$ un corps et $P \in \mathbb{K}[X]$ un polynôme de degré au moins 1. Soit F un polynôme dans $\mathbb{K}[X]$; pour que la classe de F soit inversible dans $\mathbb{K}[X]/(P)$, il faut et il suffit que F et P soient premiers entre eux.*

PREUVE. C'est une conséquence presqu'immédiate du théorème 2.9, ou théorème de Bézout pour les polynômes. Voir la preuve du lemme 4.6 du chapitre précédent. □

4.8. THÉORÈME. *L'anneau quotient $\mathbb{K}[X]/(P)$ est un corps si et seulement si le polynôme P est irréductible.*

PREUVE. C'est une conséquence immédiate du lemme 4.7. Voir la preuve du théorème 4.7 du chapitre précédent (qui dit que, pour $d \geq 1$, l'anneau $\mathbb{Z}/(d)$ est un corps si et seulement si d est premier). □

EXEMPLES. (i) Le quotient $\mathbb{R}[X]/(X^2+1)$ est isomorphe au corps $\mathbb{C}$, avec $\pm X$ les deux racines carrées de -1. Plus précisément, le morphisme d'anneaux

$$\mathbb{R}[X] \ni \sum_{k\geq 0} a_k X^k \;\longmapsto\; \sum_{k\geq 0} a_k i^k \in \mathbb{C}$$

s'annule sur tous les polynômes de l'idéal (X^2+1) et définit un isomorphisme du quotient de $\mathbb{R}[X]$ par l'idéal (X^2+1) avec le corps $\mathbb{C}$. (Il en est de même de l'application définie par $\sum_{k\geq 0} a_k X^k \longmapsto \sum_{k\geq 0} a_k (-i)^k$.)

Attention : pour tout autre polynôme $P(X) = aX^2+bX+c \in \mathbb{R}[X]$ tel que $b^2-4ac<0$, c'est-à-dire pour tout autre polynôme irréductible de degré 2 dans $\mathbb{R}[X]$, on peut montrer que le quotient $\mathbb{R}[X]/(P(X))$ est aussi isomorphe à $\mathbb{C}$!

(ii) Le quotient $\mathbb{Q}[X]/(X^2-5)$ est isomorphe au corps $\mathbb{Q}(\sqrt{5}) = \{a+b\sqrt{5} \mid a,b \in \mathbb{Q}\}$; c'est un exemple de corps déjà évoqué à l'exercice (VII.35).

Plus précisément et comme plus haut, le morphisme d'anneaux

$$\mathbb{Q}[X] \ni \sum_{k\geq 0} a_k X^k \;\longmapsto\; \sum_{k\geq 0} a_k (\sqrt{5})^k \in \mathbb{Q}(\sqrt{5})$$

s'annule sur tous les polynômes de l'idéal (X^2-5) et définit un isomorphisme du quotient de $\mathbb{Q}[X]$ par l'idéal (X^2-5) avec le corps $\mathbb{Q}(\sqrt{5})$.

(iii) Le quotient $\mathbb{F}_2[X]/(X^2+X+1)$ est un corps à 4 éléments.

(iv) Si $P(X)$ est un polynôme de degré 1, le corps $\mathbb{K}[X]/(P(X))$ s'identifie à $\mathbb{K}$ (voir la proposition 4.6).

Exercices du § VIII.4

(VIII.6) Pour chacune des quatre données ci-dessous consistant en un anneau A, un élément $a \in A$ déterminant un idéal principal (a), et deux éléments $b, c \in A$, décider si b et c sont congrus modulo (a) ; répondre simplement « oui » ou « non ».

(i) $A = \mathbb{Z}$, $a = 11$, $b = 82224$, $c = 11$

(ii) $A = \mathbb{F}_2[X]$, $a = X^2 + X + 1$, $b = X$, $c = X^2$

(iii) $A = \mathbb{F}_2[X]$, $a = X^2 + X + 1$, $b = X$, $c = X^2 + 1$

(iv) $A = \mathbb{Q}[X]$, $a = X^2 + X + 1$, $b = X$, $c = X^2 + 1$.

(VIII.7) Soit $P \in \mathbb{F}_2[X]$ un polynôme de la liste ci-dessous, et n son degré. Déterminer dans chaque cas le plus petit entier $d \geq 1$ tel que $X^d \equiv 1 \pmod{P}$, ainsi que des polynômes $R_1, \ldots, R_d$ de degrés $< n$ tels que $X^j \equiv R_j \pmod{P}$ pour $j \in \{1, \ldots, d\}$.

(i) $P = X^2 + X + 1$. [Noter que $\mathbb{F}_2[X]/(P)$ est un corps à 4 éléments. Les R_j sont X, $X + 1$, 1, ce qui confirme que le groupe des éléments non nuls de ce corps est un groupe cyclique d'ordre 3.]

(ii) $P = X^3 + X^2 + 1$. [Noter que $\mathbb{F}_2[X]/(P)$ est un corps à 8 éléments. Les R_j sont X, X^2, $X^2 + 1$, $X^2 + X + 1$, $X + 1$, $X^2 + X$, 1, ce qui confirme que le groupe des éléments non nuls de ce corps est un groupe cyclique d'ordre 7.]

(iii) $P = X^4 + X^3 + 1$. [On trouve un corps à 16 éléments, dont les éléments non nuls constituent un groupe multiplicatif qui est cyclique d'ordre 15.]

(iv) $P = X^4 + X^3 + X^2 + X + 1$. [Il s'agit de nouveau d'un corps à 16 éléments, en fait « du » corps à 16 éléments (voir plus bas). Cette fois, la classe ξ de X vérifie $\xi^5 = 1$, et en particulier *n'engendre pas* le groupe multiplicatif des éléments non nuls ; mais on vérifie facilement que la classe de $X^2 + X$ est d'ordre 15 dans ce groupe.]

(VIII.8) Soit $P(X) \in \mathbb{Q}[X]$ un polynôme de la forme

$$P(X) \;=\; X^d + k_1 X^{d-1} + \cdots + k_{d-1} X + k_d,$$

où les coefficients $k_1, \ldots, k_d$ sont dans $\mathbb{Z}$.

(i) Montrer que toute racine $c \in \mathbb{Q}$ de $P(X)$ est un entier.

[*Indication* : écrire $c = \frac{a}{b}$ avec $a, b \in \mathbb{Z}$ premiers entre eux, et constater que, si $|b| \geq 2$, on ne peut avoir à la fois $P(c) = 0$ et $a \not\equiv 0 \pmod{b}$.]

(ii) Montrer que, pour tout entier $a \geq 2$, le polynôme $X^3 + 2X + 1$ est irréductible dans $\mathbb{Q}[X]$ en montrant qu'il n'a aucune racine dans $\mathbb{Q}$.

[*Indication* : considérer $P(n)$ pour $n \in \mathbb{Z}$, d'abord lorsque $|n| \leq 1$ et ensuite lorsque $|n| \geq 2$.]

(iii) Montrer que, dans $\mathbb{Q}[X]$, le polynôme $X^3 + 3X + 1$ est irréductible.

[*Indication* : $n^3 + 3n + 1 \not\equiv 0 \pmod{2}$ pour tout $n \in \mathbb{Z}$.]

Soient $\mathbb{K}$ un corps et $P(X) = X^d + a_1 X^{d-1} + \cdots + a_d$ un polynôme de $\mathbb{K}[X]$ de degré $d \geq 2$. Supposons P irréductible et notons $\mathbb{L}$ le corps $\mathbb{K}[X]/(P)$. Comme $\mathbb{K}$ s'identifie à un sous-corp de $\mathbb{L}$, le polynôme P peut être vu dans $\mathbb{L}[X]$.

Le polynôme P n'a aucune racine dans $\mathbb{K}$, puisqu'il est irréductible ; en revanche il y au moins une racine dans $\mathbb{L}$, à savoir la classe ξ de X dans $\mathbb{L} = [X]/(P)$, car $P(\xi) = \xi^d + a_1\xi^{d-1} + \cdots + a_0 = 0 \in \mathbb{L}$.

Pour la suite de la théorie (voir un autre cours), il est absolument essentiel de savoir *étendre* un corps (ici $\mathbb{K}$) dans lequel un polynôme donné n'a aucune racine en un corps plus grand (ici $\mathbb{L}$) dans lequel ce même polynôme possède des racines.

5. Le critère d'irréductibilité d'Eisenstein pour les polynômes à coefficients rationnels

Les *preuves* de ce paragraphe ne font pas partie du programme d'examen.

Soit A un anneau commutatif intègre (définition 2.4). Le contenu des numéros 1.1 à 1.6 s'étend sans modification à l'anneau $A[X]$ des *polynômes à une indéterminée à coefficients dans A*. L'hypothèse « A intègre » est nécessaire pour l'égalité $\deg(P_1P_2) = \deg(P_1) + \deg(P_2)$ de la proposition 1.3.

Il faut prendre garde aux modifications nécessaires dans la suite de la théorie, qui sont importantes. Par exemple, le théorème de la division euclidienne s'énonce comme suit : soient $F, P \in A[X]$ tels que $P \neq 0$ *et tel que le coefficient dominant de P soit inversible dans A*. Alors il existe deux polynômes $Q, R \in A[X]$ tels que $F = PQ + R$ et $\deg(R) < \deg(P)$; de plus, Q et R sont univoquement déterminés par ces conditions. (Si l'énoncé a changé, la preuve du § VIII.2 s'applique, elle, sans changement !)

Conformément à la définition 4.1, un polynôme $F \in A[X]$ de degré au moins 1 est *réductible* s'il existe des polynômes $G, H \in A[X]$ de degrés ≥ 1 tels que $F = GH$, et *irréductible* sinon.

Pour la suite de ce paragraphe, nous particularisons à $A = \mathbb{Z}$. Vu l'inclusion de $\mathbb{Z}$ dans le corps $\mathbb{Q}$ des nombres rationnels, l'anneau $\mathbb{Z}[X]$ s'identifie à un sous-anneau de $\mathbb{Q}[X]$.

Soit F un polynôme irréductible de $\mathbb{Z}[X]$. Comme il y a beaucoup plus de polynômes dans $\mathbb{Q}[X]$ que dans $\mathbb{Z}[X]$, il n'est pas a priori clair que F soit encore irréductible dans $\mathbb{Q}[X]$; mais c'est vrai !

5.1. Proposition. *Soit F un polynôme à une indéterminée à coefficients entiers. Si F est irréductible dans $\mathbb{Z}[X]$, alors F est irréductible dans $\mathbb{Q}[X]$.*

Remarque. L'implication réciproque est *banalement* vraie.

Preuve. Considérons un polynôme $F \in \mathbb{Z}[X]$ de degré k qui est réductible dans $\mathbb{Q}[X]$, c'est-à-dire tel qu'il existe $G, H \in \mathbb{Q}[X]$, respectivement de degrés l, m, $1 \leq l, m < k$, avec $F = GH$. Il s'agit de montrer que F est réductible dans $\mathbb{Z}[X]$. (Il ne coûte rien de supposer $k \geq 2$.)

On peut écrire

$$\begin{aligned} G(X) &= \frac{a_l}{b_l}X^l + \frac{a_{l-1}}{b_{l-1}}X^{l-1} + \cdots + \frac{a_0}{b_0} \\ H(X) &= \frac{c_m}{d_m}X^m + \frac{c_{m-1}}{d_{m-1}}X^{m-1} + \cdots + \frac{c_0}{d_0} \end{aligned}$$

avec

$$a_0, \dots, a_l, b_0, \dots, b_l, c_0, \dots, c_m, d_0, \dots, d_m \in \mathbb{Z},$$
$$b_0, \dots, b_l, d_0, \dots, d_m \geq 1,$$
$$\operatorname{pgcd}(a_0, b_0) = \cdots = \operatorname{pgcd}(a_l, b_l) = \operatorname{pgcd}(c_0, d_0) = \cdots = \operatorname{pgcd}(c_m, d_m) = 1.$$

Posons[7] $b = \prod_{1 \leq i \leq l} b_i$, $d = \prod_{1 \leq j \leq m} d_j$ et $n = bd$. Alors $nF, bG, dH \in \mathbb{Z}[X]$ et

$$nF \;=\; (bG)(dH) \qquad \text{est réductible dans} \quad \mathbb{Z}[X].$$

Si $n = 1$, il n'y a rien à montrer ; supposons désormais que $n > 1$. Ecrivons les coefficients (tous dans $\mathbb{Z}$) de bG et dH sous la forme

$$bG(X) \;=\; g_l X^l + \cdots + g_1 X + g_0$$
$$dH(X) \;=\; h_m X^m + \cdots + h_1 X + h_0.$$

Affirmation. *Soit p un diviseur premier de n. Alors l'une au moins des propriétés suivantes est vérifiée :*

(i) *p divise tous les coefficients g_i,*

(ii) *p divise tous les coefficients h_j.*

En effet, si ce n'était pas vrai, on pourrait définir le plus petit coefficient i_0 tel que p ne divise pas g_{i_0} et le plus petit coefficient j_0 tel que p ne divise pas h_{j_0}. Par hypotèse, p divise n, donc aussi le coefficient de $X^{i_0+j_0}$ dans nF, c'est-à-dire p divise

$$g_{i_0+j_0}h_0 + \cdots + g_{i_0+1}h_{j_0-1} + g_{i_0}h_{j_0} + g_{i_0-1}h_{j_0+1} + \cdots + g_0 h_{i_0+j_0}.$$

Comme p divise aussi chacun de $h_0, \dots, h_{j_0-1}, g_{i_0-1}, \dots, g_0$, il en résulte que p divise aussi $g_{i_0}h_{j_0}$, contrairement aux définitions de i_0 et j_0. L'affirmation est ainsi démontrée.

Quitte à échanger les rôles de G et de H, on peut donc supposer que p divise tous les coefficients g_i de bG. Ainsi, $\frac{b}{p}G$ est un polynôme de $\mathbb{Z}[X]$, encore de degré l, et

$$\frac{n}{p}F \;=\; \Big(\frac{b}{p}G\Big)\Big(dH\Big).$$

Si $\frac{n}{p} = 1$, il n'y a plus rien à montrer. Sinon, on choisit un facteur premier q de $\frac{n}{p}$, et on montre comme ci-dessus que $\frac{n}{pq}F$ est produit dans $\mathbb{Z}[X]$ de deux polynômes de degrés l et m. En répétant l'argument autant de fois que n possède de diviseurs premiers[8], on montre que F est produit dans $\mathbb{Z}[X]$ de deux polynômes de degrés l et m. □

5.2. Théorème (critère d'irréductibilité d'Eisenstein). *Soit*

$$F(X) \;=\; f_k X^k + \cdots + f_1 X + f_0 \qquad (f_k \neq 0)$$

un polynôme à coefficients dans $\mathbb{Z}$ de degré $k \geq 2$. On suppose qu'il existe un nombre premier p tel que

(i) *p ne divise pas f_k ,*

(ii) *p divise f_j pour $j = 0, \dots, k-1$,*

(iii) *p^2 ne divise pas f_0.*

[7] On pourrait remplacer ces produits par des plus petits communs multiples.

[8] En comptant les multiplicités : par exemple trois fois pour $n = 12 = 2^2 \times 3$.

Alors $F(X)$ est irréductible dans l'anneau $\mathbb{Q}[X]$.

PREUVE. Par la proposition précédente, il suffit de montrer que $F(X)$ est irréductible dans $\mathbb{Z}[X]$. Supposons (ab absurdo) qu'il existe

$$G(X) = g_l X^l + \cdots + g_1 X + g_0 \in \mathbb{Z}[X]$$
$$H(X) = h_m X^m + \cdots + g_1 X + h_0 \in \mathbb{Z}[X]$$

tels que $1 \leq l < k$, $1 \leq m < k$ et $F(X) = G(X)H(X)$. Nous avons en particulier $k = l + m$ et $f_0 = g_0 h_0$.

Vu que $f_0 = g_0 h_0$ est divisible par p et pas par p^2, exactement l'un de g_0, h_0 est divisible par p. Supposons les notations telles que p divise g_0 et ne divise pas h_0. Si les g_i étaient tous divisibles par p, le coefficient f_k le serait aussi, contrairement à l'hypothèse (i) ; on peut donc définir l'entier i_0 tel que p ne divise pas g_{i_0} et divise chacun de $g_0, \ldots, g_{i_0-1}$. Alors, dans l'égalité

$$f_{i_0} = g_{i_0} h_0 + g_{i_0-1} h_1 + \cdots + g_0 h_{i_0},$$

p divise $f_{i_0}, g_{i_0-1}, g_{i_0-2}, \ldots, g_0$ mais p ne divise ni g_{i_0} ni h_0, ce qui est absurde.

Donc F est irréductible dans $\mathbb{Z}[X]$. □

EXEMPLES. (i) Pour tout entier $k \geq 1$ et pour tout nombre premier p, le polynôme $X^k - p$ est irréductible dans $\mathbb{Q}[X]$ (ainsi que dans $\mathbb{Z}[X]$!).

En particulier, $\sqrt[k]{p}$, $k > 1$, n'est pas un nombre rationnel.

(ii) Le polynôme $F(X) = \frac{4}{25}X^4 + \frac{3}{5}X^2 + X + \frac{1}{5}$ est irréductible dans $\mathbb{Q}[X]$. En effet, il suffit de vérifier que le polynôme $25F(X) = 4X^5 + 15X^4 + 25X^3 + 5$ est irréductible dans $\mathbb{Z}[X]$, ce qui résulte du critère d'Eisenstein appliqué avec $p = 5$.

(iii) Pour tout nombre premier p, le polynôme à coefficients dans $\mathbb{Z}$

$$\Phi_p(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + X + 1,$$

dit *polynôme cyclotomique de degré* $p-1$, est irréductible dans $\mathbb{Q}[X]$. En effet, s'il était réductible, le polynôme

$$\Phi_p(X+1) = \frac{(X+1)^p - 1}{X} = \sum_{j=1}^{p} \binom{p}{j} X^{j-1}$$

le serait aussi ; or, pour ce polynôme,

(a) p ne divise pas le coefficient dominant $\binom{p}{p} = 1$,

(b) p divise le coefficient $\binom{p}{j} = \frac{p(p-1)\cdots(p-j+1)}{j!}$ de X^{j-1} pour $j = 1, \ldots, p-1$,

(c) p^2 ne divise pas le terme constant $\binom{p}{1} = p$,

de sorte que $\Phi_p(X+1)$ est irréductible par le critère d'Eisenstein. Ceci achève de montrer que $\Phi_p(X)$ est irréductible.

Par suite, l'anneau quotient $\mathbb{Q}[X]/(\Phi_p(X))$ est un corps pour tout nombre premier p (les cas intéressants sont $p \geq 3$) ; l'étude de ces *corps cyclotomiques* est importante en théorie des nombres.

(iv) Pour p comme ci-dessus, définissons $\Phi_{p^2}(X) \in \mathbb{Z}[X]$ par

$$\Phi_{p^2}(X) \;=\; \Phi_p(X^p) \;=\; \frac{X^{p^2}-1}{X^p-1} \;=\; X^{p(p-1)} + X^{p(p-2)} + \cdots + X^p + 1.$$

Pour tout entier j tel que $0 \le j \le p$, le coefficient de X^j dans $(X+1)^p$ est congru modulo p au coefficient de X^j dans X^p+1. Il en résulte que, pour tout polynôme $F(X) \in \mathbb{Z}[X]$ de degré $d \ge 0$ et pour tout entier k tel que $0 \le k \le dp$, le coefficient de X^k dans $F\left((X+1)^p\right)$ est congru modulo p au coefficient de X^k dans $F\left(X^p+1\right)$, ce que nous écrivons

$$F\left((X+1)^p\right) \;\equiv\; F\left(X^p+1\right) \pmod{p}.$$

En particulier

$$\Phi_{p^2}(X+1) \;=\; \Phi_p\left((X+1)^p\right) \;\equiv\; \Phi_p\left(X^p+1\right) \pmod{p}.$$

Par ailleurs (voir (iii)), nous avons

$$\Phi_p(X^p+1) \;=\; \frac{(X^p+1)^p-1}{X^p} \;=\; \sum_{j=1}^{p} \binom{p}{j} X^{p(j-1)}.$$

On peut donc appliquer le critère d'Eisenstein, de sorte que le polynôme $\Phi_{p^2}(X+1)$ est irréductible dans $\mathbb{Q}[X]$; ceci achève de montrer que le polynôme $\Phi_{p^2}(X)$ est irréductible.

Le même type d'argument permet de montrer que $\Phi_{p^{a+1}}(X) = \Phi_p(X^{p^a})$ est irréductible pour tout entier $a \ge 1$. Noter que les racines de $\Phi_{p^a}(X)$ sont les nombres complexes z tels que $z^{p^a} = 1$ et $z^{p^{a-1}} \ne 1$.

(v) Les polynômes X^4+1 et X^6+X^3+1 sont irréductibles dans $\mathbb{Z}[X]$. (On s'en assure par l'argument utilisé pour (iii), avec $p=2$ et $p=3$ respectivement.)

Noter que, au contraire, les polynômes suivants sont réductibles :

$$\frac{X^4-1}{X-1} \;=\; X^3+X^2+X+1 \;=\; (X+1)(X^2+X+1),$$

$$\frac{X^6-1}{X-1} \;=\; X^5+X^4+X^3+X^2+X+1 \;=\; (X+1)(X^2+X+1)(X^2-X+1),$$

$$\frac{X^{2n}-1}{X-1} \quad \text{est divisible par } X+1 \text{ pour tout entier pair } 2n \ge 2,$$

$$\frac{X^9-1}{X-1} \quad \text{est divisible par } X^2+X+1 \text{ (exercice).}$$

Remarque-exercice. Dans l'anneau $\mathbb{Z}[X]$, vérifier que $\{F \in \mathbb{Z}[X] \mid F(0) \text{ est pair}\}$ est un idéal qui n'est pas principal.

Contrairement à $\mathbb{Q}[X]$, l'anneau $\mathbb{Z}[X]$ possède donc des idéaux non principaux.

Généralisation des exemples (iii) *et* (iv). Pour tout entier $n \ge 1$, le *polynôme cyclotomique* $\Phi_n(X)$ est défini comme suit.

Notons C_n le sous-groupe $\{z \in \mathbb{C} \mid z^n = 1\}$ de $\mathbb{C}^*$ des *racines n-ièmes de l'unité,* qui est un groupe cyclique d'ordre n engendré par $\exp(\frac{2i\pi}{n})$. Les racines *primitives* n-ièmes de l'unité sont les générateurs de ce groupe. Il est facile de vérifier que ce sont les nombres de la forme $\exp(\frac{2i\pi k}{n})$, avec $k \in \{1, \ldots, n-1\}$ et k premier à n ; noter que, conformément à l'exercice VII.44, le nombre de générateurs du groupe C_n est la valeur $\varphi(n)$ de la fonction d'Euler.

Par définition, $\Phi_n(X) = \prod(X-\zeta)$, le produit étant pris sur toutes les racines primitives n-ièmes de l'unité. Il résulte immédiatement de cette définition que Φ_n est un polynôme de degré $\varphi(n)$. A priori, $\Phi_n(X) \in \mathbb{C}[X]$, mais on montre que $\Phi_n(X) \in \mathbb{Z}[X]$; par exemple : $\Phi_8(X) = X^4+1$, $\Phi_{12}(X) = X^4-X^2+1$. [Esquisse d'une preuve du cas général. On

montre d'abord que $X^n - 1 = \prod_{d|n} \Phi_d(X)$, puis on procède par récurrence sur n. Soit $F(X) = \prod_{d|n, d<n} \Phi_d(X)$; ainsi $F(X) \in \mathbb{Z}[X]$ par hypothèse de récurrence ; $X^n - 1$ est produit des deux polynômes unitaires $F(X)$ et $\Phi_n(X)$. Comme l'algorithme de division par un polynôme unitaire vaut dans $\mathbb{C}[X]$ ET dans $\mathbb{Z}[X]$, il en résulte que $\Phi_n(X) \in \mathbb{Z}[X]$.]

On peut montrer que $\Phi_n(X)$ est irréductible dans $\mathbb{Q}[X]$ pour tout $n \geq 1$ (et pas seulement pour n premier et puissance de premier, comme en (iii) et (iv) ci-dessus).

6. Corps finis

Soit $\mathbb{K}$ un corps. Considérons l'application $\chi : \mathbb{Z} \longrightarrow \mathbb{K}$ définie comme suit :

si $n \geq 0$, alors $\chi(n) = 1 + \cdots + 1$, où $1 \in \mathbb{K}$ apparaît n fois ;

si $n < 0$, alors $\chi(n) = -\chi(-n)$.

On vérifie que χ est un homomorphisme d'anneaux.

Cette application peut être injective (cas de $\mathbb{Q}$, de $\mathbb{Q}/(X^2 - 2)$, de $\mathbb{R}$, de $\mathbb{C}$, ...) ou non (cas de $\mathbb{F}_p$, de $\mathbb{F}_2[X]/(X^2 + X + 1)$, ...). Si χ n'est pas injective, son noyau est un idéal de $\mathbb{Z}$ et il existe un entier strictement positif p tel que $\mathrm{Ker}(\chi) = p\mathbb{Z}$. Comme $1 \neq 0$ dans $\mathbb{K}$, on a $p \geq 2$. Comme le produit de deux éléments non nuls de $\mathbb{K}$ (et en particulier de deux éléments non nuls de l'image de χ) n'est pas nul, p est nécessairement un nombre premier.

6.1. Définition. La caractéristique d'un corps $\mathbb{K}$ est zéro si l'application χ ci-dessus est injective, et p si $\mathrm{Ker}(\chi) = p\mathbb{Z}$.

Remarque. Dans tout corps de caractéristique zéro, l'image de χ est un sous-anneau isomorphe à $\mathbb{Z}$; il en résulte qu'un corps de caractéristique zéro possède un sous-corps isomorphe au corps $\mathbb{Q}$ des nombres rationnels. En particulier, un corps de caractéristique zéro est nécessairement infini.

Tout corps fini est nécessairement de caractéristique p pour un nombre premier p convenable. Il existe pour tout nombre premier p des corps infinis de caractéristique p, mais nous n'en parlerons pas davantage ici. Tout corps de caractéristique p contient un sous-corps à p éléments qu'on peut identifier à $\mathbb{F}_p = \mathbb{Z}/(p) = \{0, 1, \ldots, p-1\}$.

Soit $\mathbb{K}$ un corps fini de caractéristique p. On peut le voir comme un espace vectoriel sur $\mathbb{F}_p$, nécessairement de dimension finie. Si on note n cette dimension, $\mathbb{K}$ contient précisément p^n éléments. Ceci montre la première assertion de l'énoncé suivant.

6.2. Théorème. *Soit p un nombre premier.*

(i) *Pour tout corps fini $\mathbb{K}$ de caractéristique p, il existe un entier $n \geq 1$ tel que le corps $\mathbb{K}$ soit d'ordre p^n.*

(ii) *Pour tout entier $n \geq 1$, il existe un corps à p^n éléments.*

(iii) *Les éléments non nuls d'un corps fini d'ordre p^n constituent pour la multiplication un groupe isomorphe à $\mathbb{Z}/(p^n - 1)\mathbb{Z}$.*

(iv) *Deux corps fini de même ordre sont isomorphes.*

Sur la preuve. Pour montrer (ii), une méthode consiste à montrer que, pour tout entier $n \geq 1$, l'anneau $\mathbb{F}_p[X]$ contient au moins un polynôme irréductible P de degré n. (Voir ci-dessous pour $p = 2$ et $n \in \{2, 3, 4, 7\}$.) Alors $\mathbb{F}_p[X]/(P)$ est un corps à p^n éléments.

L'assertion (iii) est le théorème 3.4. Voir aussi l'exercice (VIII.7). □

Faute d'indiquer la preuve de l'assertion (iv), montrons au moins un exemple d'isomorphisme entre deux corps finis.

Considérons d'abord un nombre premier p, un polynôme irréductible $P(X) \in \mathbb{F}_p[X]$ de degré $d \geq 2$ et le corps $\mathbb{K} = \mathbb{F}_p[X]/(P(X))$ d'ordre $q = p^d$.

Soit $\xi \in \mathbb{K}$. Les polynômes $F(X) \in \mathbb{F}_p[X]$ tels que $F(\xi) = 0$ constituent un idéal de $\mathbb{F}_p[X]$; soit $M_\xi(X) \in \mathbb{F}_p[X]$ l'unique polynôme unitaire de degré minimum dans cet idéal ; c'est le *polynôme caractéristique* de ξ. Notons que $M_\xi(X)$ divise $X^q - X$ (car $\xi^q - \xi = 0$ pour tout $\xi \in \mathbb{K}$).

Particularisons d'abord au cas de $\mathbb{K} = \mathbb{F}_2[X]/(X^3+X+1)$. Notons α la classe de X dans $\mathbb{K}$, de sorte que les éléments de $\mathbb{K}$ s'écrivent, en plus de 0,

$$\begin{array}{rcl} \alpha & = & \text{classe de } X \\ \alpha^2 & = & \text{classe de } X^2 \\ \alpha^3 & = & \text{classe de } X+1 \\ \alpha^4 & = & \text{classe de } X^2+X \\ \alpha^5 & = & \text{classe de } X^2+X+1 \\ \alpha^6 & = & \text{classe de } X^2+1 \\ \alpha^7 & = & 1. \end{array}$$

La décomposition en facteurs irréductibles de $X^q - X$ s'écrit

$$X^8 - X = X(X+1)(X^3+X+1)(X^3+X^2+1)$$

et les polynômes minimaux des éléments de $\mathbb{K}$ sont donnés par le tableau

$$\begin{array}{lll} \xi = 0 & & M_\xi(X) = X \\ \xi = 1 & & M_\xi(X) = X+1 \\ \xi \in \{\alpha, \alpha^2, \alpha^4\} & & M_\xi(X) = X^3+X+1 \\ \xi \in \{\alpha^3, \alpha^5, \alpha^6\} & & M_\xi(X) = X^3+X^2+1. \end{array}$$

Considérons ensuite le corps $\mathbb{L} = \mathbb{F}_2[X]/(X^3+X^2+1)$ et notons β la classe de X dans $\mathbb{K}$. Un calcul simple montre que

$$M_\beta(X) = M_{\beta^2}(X) = M_{\beta^4}(X) = X^3+X^2+1 \neq M_\alpha(X)$$
$$M_{\beta^3}(X) = X^3+X+1 = M_\alpha(X).$$

Si φ est un isomorphisme de $\mathbb{K}$ sur $\mathbb{L}$, le polynôme minimal d'un élément $\xi \in \mathbb{K}$ doit coïncider avec celui de $\varphi(\xi)$. On peut poser $\varphi(\alpha) = \beta^3$ ou, avec plus de détails :

$$\varphi(0) = 0, \quad \varphi(1) = 1, \quad \varphi(\alpha^j) = \beta^{3j} \ (0 \leq j \leq 6)$$

et vérifier que φ est un isomorphisme de corps. [On pourrait aussi poser $\varphi(\alpha)$ égal à β^6 ou β^5, ce qui reviendrait à composer l'isomorphisme décrit ci-dessus avec l'automorphisme de Frobenius de $\mathbb{L}$ (voir plus bas) ou avec son carré.]

6.3. Preuve de l'existence d'un corps fini à 128 éléments. Soit $P(X) \in \mathbb{F}_2[X]$ un polynôme irréductible de degré $d \geq 2$. Le coefficient de X^d est nécessairement 1, de même que le coefficient du terme constant (sinon X divise $P(X)$) et le nombre de coefficients égaux à 1 est impair (sinon $P(1) = 0$, donc $X - 1$ divise $P(X)$). On obtient ainsi facilement les polynômes irréductibles de degré 2

$$X^2 + X + 1\,,$$

de degré 3

$$X^3 + X^2 + 1 \qquad \text{et} \qquad X^3 + X + 1\,,$$

et même de degré 4 (bien que ce ne soit pas utile pour démontrer l'existence de $\mathbb{F}_{128}$)

$$X^4 + X^3 + X^2 + X + 1\,, \qquad X^4 + X^3 + 1 \qquad \text{et} \qquad X^4 + X + 1$$

(observer que $X^4 + X^2 + 1 = (X^2 + X + 1)^2$ est réductible).

Pour qu'un polynôme $P(X)$ de degré 7 soit irréductible, il faut et il suffit qu'il ne soit pas divisible par un polynôme de degré $d \in \{1, 2, 3\}$, c'est-à-dire par l'un des poynômes de la liste $X\,,\ X+1\,,\ X^2+X+1\,,\ X^3+X^2+1\,,\ X^3+X+1$.

AFFIRMATION. *Le polynôme*

$$P(X) \,=\, X^7 + X + 1$$

est irréductible.

En effet, $P(X)$ n'a pas de diviseur de degré 1 car $P(0) \neq 0$ et $P(1) \neq 0$, et $P(X)$ n'a pas de diviseur de degré 2 ou 3 car

$$\begin{aligned} X^7 + X + 1 \,&=\, (X^2 + X + 1)(X^5 + X^4 + X^2 + X) \,+\, 1 \\ X^7 + X + 1 \,&=\, (X^3 + X + 1)(X^4 + X^2 + X + 1) \,+\, X \\ X^7 + X + 1 \,&=\, (X^3 + X^2 + 1)(X^4 + X^3 + X^2 + 1) \,+\, X \end{aligned}$$

(à choix : $X^7 + X + 1 = (X^3 + X + 1)(X^3 + X^2 + 1)(X + 1) + X$ au lieu des deux dernières égalités ci-dessus).

Par suite

$$\mathbb{F}_2[X]/(P)$$

est un corps à 128 *éléments.*

Le polynôme $X^7 + X + 1$ n'est de loin pas le seul polynôme irréductible de degré 7 dans $\mathbb{F}_2[X]$. En fait, le nombre $N_q(n)$ des polynômes unitaires irréductibles de degré n dans $\mathbb{F}_q[X]$ est donné par la formule

$$N_q(n) \,=\, \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d}$$

où la somme porte sur les diviseurs d de n (y compris 1 et n) et où

$$\mu(d) \,=\, \begin{cases} 1 & \text{si } d = 1, \\ (-1)^k & \text{si } d = \displaystyle\prod_{j=1}^{k} p_j \text{ pour des premiers } p_1, \ldots, p_k \text{ distincts}, \\ 0 & \text{s'il existe un premier } p \text{ tel que } p^2 \mid d. \end{cases}$$

Par exemple

$$\begin{aligned} N_q(1) \,&=\, q & \qquad N_q(5) \,&=\, \tfrac{1}{5}\,(q^5 - q) \\ N_q(2) \,&=\, \tfrac{1}{2}\,(q^2 - q) & \qquad N_q(6) \,&=\, \tfrac{1}{6}\,(q^6 - q^3 - q^2 + q) \\ N_q(3) \,&=\, \tfrac{1}{3}\,(q^3 - q) & \qquad N_q(7) \,&=\, \tfrac{1}{7}\,(q^7 - q) \\ N_q(4) \,&=\, \tfrac{1}{4}\,(q^4 - q^2) & \qquad N_q(8) \,&=\, \tfrac{1}{8}\,(q^8 - q^4) \end{aligned}$$

et, en particulier, il y a

$$N_2(7) \,=\, 18$$

polynômes irréductibles de la forme $X^7 + a_6X^6 + a_5X^5 + \cdots + a_1X + 1$ dans $\mathbb{F}_2[X]$.

En informatique, il est utile d'avoir un corps fini de caractéristique 2 assez grand pour que ses éléments puissent représenter 26 minuscules, 26 majuscules, et divers signes typographiques (avec une certaine marge de manoeuvre), en d'autres termes de disposer d'un corps à 128 éléments.

Plus généralement, la théorie des corps finis a de nombreuses applications, par exemple en théorie des nombres, en combinatoire, en théorie des codes et en cryptographie.

Lectures recommandées, R. Godement, *Cours d'algèbre,* Hermann 1963 (en particulier les §§ 27 et 28).

S. Lang, *Undergraduate algebra,* Springer 1987 (le chapitre IV est consacré aux polynômes à coefficients dans un corps).

Exercices du § VIII.6

(VIII.9) Dresser la liste des polynômes irréductibles de degrés ≤ 3 dans $\mathbb{F}_3[X]$.

(VIII.10) Vérifier que le polynôme $X^5 + X^2 + 1 \in \mathbb{F}_2[X]$ est irréductible.

[*Indication* : Vérifier que ce polynôme n'a pas de facteur de degré ≤ 2 en utilisant la formule $X^5 + X^2 + 1 = X^2(X + 1)(X^2 + X + 1) + 1$.]

(VIII.11$^\sharp$) Montrer qu'il existe un corps à 256 éléments en montrant que le polynôme $X^8 + X^4 + X^3 + X + 1$ est irréductible dans $\mathbb{F}_2[X]$.

[*Indication* : vérifier que ce polynôme n'est divisible par aucun des six polynômes irréductibles dans $\mathbb{F}_2[X]$ de degrés 2, 3 et 4.]

(VIII.12) Soit $\mathbb{L}$ un corps de caractéristique p. On identifie $\mathbb{F}_p$ à un sous-corps $\mathbb{K}$ de $\mathbb{L}$.

(i) Vérifier que l'application Frob : $\mathbb{L} \longrightarrow \mathbb{L}$, $\mathrm{Frob}(x) = x^p$ est un isomorphisme du corps $\mathbb{L}$ dans lui-même.

(ii) Vérifier que $\mathbb{K}$ est l'ensemble des points fixes de Frob.

[Frob est *l'isomorphime de Frobenius* de $\mathbb{L}$. Lorsque Frob est surjectif, par exemple lorsque $\mathbb{K}$ est fini, c'est donc *l'automorphisme de Frobenius*.]

(VIII.13$^{\sharp\sharp}$) Pour un entier $n \geq 2$, soit R_n l'anneau quotient de l'anneau de polynômes $\mathbb{F}_2[X]$ par l'idéal $(X^n - 1)$ et $\pi_n : \mathbb{F}_2[X] \longrightarrow R_n$ l'application canonique. Convenons d'identifier tout élément de R_n à son unique représentant de degré au plus $n - 1$ dans $\mathbb{F}_2[X]$; rappelons que R_n est naturellement un espace vectoriel de dimension n sur $\mathbb{F}_2$.

Soit $G(X) \in \mathbb{F}_2[X]$ un diviseur de $X^n - 1$; on note $n - k$ le degré de $G(X)$, de sorte que $0 \leq k \leq n$. Désignons par $\tilde{C}_G$ l'image par π_n de l'idéal principal $(G(X))$ de $\mathbb{F}_2[X]$.

(i) Observer que $\tilde{C}_G$ est un sous-espace vectoriel de R_n. Montrer que les polynômes $G(X), XG(X), \ldots, X^{k-1}G(X)$ sont dans $\tilde{C}_G$ et sont linéairement indépendants.

(ii) Observer que $\tilde{C}_G = \{0\}$ lorsque $G(X) = X^n - 1$ et que $\tilde{C}_G = R_n$ lorsque $G(X) = 1$.

(iii) Identifer $\tilde{C}_G$ et calculer sa dimension lorsque $G(X) = X - 1$. Même question lorsque $G(X) = 1 + X + \cdots + X^{n-1}$.

(iv) Soit $H(X) \in \mathbb{F}_2[X]$ le quotient de $X^n - 1$ par $G(X)$, qui est de degré k, et soit $q : R_n \longrightarrow R_n$ l'application linéaire qui associe à $P(X)$ la classe dans R_n du produit $P(X)H(X)$. Montrer que $\tilde{C}_G$ est dans le noyau de q.

(v) Constater qu'il résulte de (i) et (iv) que $n = \dim_{\mathbb{F}_2}(R_n) \geq \dim_{\mathbb{F}_2}(\tilde{C}_G) + k$ et par suite que $\dim_{\mathbb{F}_2}(\tilde{C}_G) = n - k$.

(vi) Vérifier que $X^7 - 1 = (X-1)(X^3+X^2+1)(X^3+X+1)$.

Désignons par C_G le sous-ensemble de $\mathbb{F}_2^n$ constitué des vecteurs $(c_0, c_1, \ldots, c_{n-1})$ tels que $c_0 + c_1X + \cdots + c_{n-1}X^{n-1} \in \tilde{C}_G$. Noter que C_G est *cyclique* au sens où, si $(c_0, c_1, \ldots, c_{n-1}) \in C_G$, alors la permutation circulaire $(c_{n-1}, c_0, \ldots, c_{n-2})$ est aussi dans C_G.

(vii) On définit le *code de Hamming* comme étant le sous-espace vectoriel $\mathcal{C}_G$ de $\mathbb{F}_2^7$ correspondant à $G(X) = 1 + X + X^3$. Pour $i \in \{0, 1, \ldots, 7\}$, calculer le nombre A_i des vecteurs $(c_0, \ldots, c_7) \in \mathcal{C}_G$ dont exactement i coordonnées sont égales à 1.

[*Indication* : vu ce qui précède, on sait a priori que $\sum_{i=0}^{7} A_i = 16$.]

(viii) Pour tout vecteur x dans le code de Hamming, soit B_x l'ensemble des vecteurs de $\mathbb{F}_2^7$ dont au moins 6 coordonnées sont égales à celles de x. Vérifier que $\mathbb{F}_2^7$ est la *réunion disjointe* des ensembles B_x ($x \in C_G$).

On appelle (n,k)-*code linéaire binaire* un sous-espace vectoriel de $\mathbb{F}_2^n$ de dimension k. Le présent exercice reprend quelques points de la théorie de certains de ces codes appelés les *codes cycliques*, dont le code de Hamming est un des représentants les plus intéressants en petites dimensions. Sa découverte remonte aux années 1947-48, alors que Richard W. Hamming, employé aux « Bell Telephone Laboratories » , cherchait à prévenir les arrêts intempestifs de son ordinateur suite à certains messages d'erreurs. L'idée du code de Hamming est qu'il permet de corriger automatiquement certaines erreurs : en effet, si un « message » constitué d'un vecteur $y \in \mathbb{F}_2^7$ est supposé être dans C_G mais est entaché d'une erreur au plus, le vecteur y est dans un ensemble B_x exactement, et peut être « corrigé » en x ; on dit que le code de Hamming est un *code correcteur d'erreurs*.

Voici enfin un exercice qui se réfère à la fois à la théorie des nombres et à l'algèbre linéaire.

(VIII.14) Soit $(p_i)_{1\le i\le m}$ une suite finie de nombres premiers distincts deux à deux. Soit $(s_j)_{1\le j\le n}$ une suite finie de nombres entiers distincts deux à deux, tous plus grands ou égaux à 2 ; on suppose que tous les diviseurs premiers des s_j apparaissent dans la liste des p_i. On suppose également que $n > m$.

Montrer qu'il existe une sous-suite $s_{j_1}, \ldots, s_{j_l}$ de la suite $s_1, \ldots, s_n$ telle que $\prod_{k=1}^{l} s_{j_k}$ soit un carré parfait.

Solution. Pour un nombre premier p et un entier $s \ge 1$, notons $v_p(s)$ l'exposant de la plus grande puissance de p qui divise s ; par exemple, $v_2(12) = 2$, $v_3(12) = 1$ et $v_5(12) = 0$. Notons aussi $w_p(s) \in \mathbb{F}_2$ la classe modulo 2 de $v_p(s)$; par exemple $w_2(12) = 0$, $w_3(12) = 1$ et $w_5(12) = 0$.

Soient $v \in M_{m,n}(\mathbb{N})$ et $w \in M_{m,n}(\mathbb{F}_2)$ les matrices définies par

$$v_{i,j} = v_{p_i}(s_j) \qquad \text{et} \qquad w_{i,j} = w_{p_i}(s_j) \qquad \text{pour} \qquad i \in \{1,\ldots,m\} \quad \text{et} \quad j \in \{1,\ldots,n\}.$$

Si $\epsilon \in \mathbb{N}^n$ est un vecteur de coordonnées $\epsilon_1, \ldots, \epsilon_n$ toutes égales à 0 ou 1, et si on pose $s^{(\epsilon)} = s_1^{\epsilon_1} s_2^{\epsilon_2} \cdots s_n^{\epsilon_n}$, alors

$$v_{p_i}\left(s^{(\epsilon)}\right) = \sum_{j=1}^{m} \epsilon_j v_{i,j} = (i\text{-ème coordonnée de } vs^{(\epsilon)})$$

$$w_{p_i}\left(s^{(\epsilon)}\right) = \sum_{j=1}^{m} \epsilon_j w_{i,j}$$

pour tout $j \in \{1, \ldots, n\}$.

Pour qu'un nombre $s \geq 2$ soit un carré parfait, il faut et il suffit que $v_p(s)$ soit pair, c'est-à-dire que $w_p(s) = 0$, pour tout nombre premier p. En particulier, pour que $s^{(\epsilon)}$ soit un carré parfait, il faut et il suffit que le système

$$\sum_{j=1}^{n} \epsilon_j w_{i,j} \; = \; 0 \qquad 1 \leq i \leq m \tag{$*$}$$

à coefficients $w_{i,j} \in \mathbb{F}_2$ et à inconnues $\epsilon_1, \ldots, \epsilon_n$ possède une solution autre que $(0, \ldots, 0)$.

Le système ($*$) possède une solution non nulle si et seulement si le rang de $w : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^m$ est strictement inférieur à n. Une condition suffisante pour que ($*$) possède une solution non nulle est donc que $m < n$.

CHAPITRE IX

Les groupes $\mathcal{SO}(3)$, $\mathcal{O}(3)$ et $\mathcal{SU}(2)$

Le premier but de ce chapitre est d'introduire la notion d'*action* d'un groupe sur un ensemble. Le second but est de définir un homomorphisme surjectif

$$\mathcal{SU}(2) \longrightarrow \mathcal{SO}(3)$$

qui apparaît en de nombreux contextes, notamment en physique dans l'étude des moments cinétiques et des spins. Notre preuve de sa surjectivité de fait appel à un lemme utilisant la notion d'action d'un groupe (ici $\mathcal{SO}(3)$) sur un ensemble (ici la sphère $\mathbb{S}^2$).

1. Actions de groupes

1.1. Définition. Soient G un groupe et X un ensemble. Une *action* ou *opération* de G sur X est une application

$$\alpha : G \times X \ni (g, x) \longmapsto gx \in X$$

telle que

$1x = x$ pour tout $x \in X$,

$g(hx) = (gh)x$ pour tous $g, h \in G$ et $x \in X$.

Une telle action est *fidèle* si

pour tout $g \in G$, $g \neq 1$, il existe $x \in X$ tel que $gx \neq x$.

Une action est *transitive* si

pour toute paire (x, y) d'éléments de X, il existe $g \in G$ tel que $gx = y$.

L'*orbite* d'un point $x \in X$ pour une action de G sur X est le sous-ensemble $\{y \in X \mid \text{il existe } g \in G \text{ tel que } gx = y\}$ de X.

Noter que le nombre d'éléments dans une telle orbite est toujours majoré par l'ordre du groupe G !

1.2. Observation. Si G est un groupe agissant sur l'ensemble $J_n = \{1, \ldots, n\}$, alors l'application

$$G \ni g \longmapsto (x \mapsto gx) \in \mathrm{Sym}(n)$$

est un homomorphisme de groupes. Cet homomorphisme est injectif si et seulement si l'action de G sur J_n est fidèle. Ceci vaut bien sûr aussi pour une action de G sur tout autre ensemble à n éléments.

Plus généralement, la donnée d'une action d'un groupe G sur un ensemble X (fini *ou* infini) est équivalente à la donnée d'un homomorphisme de G dans le groupe de toutes les bijections de X sur lui-même.

1.3. Exemples : les groupes diédraux finis. On considère un entier $k \geq 2$ et un polygone[1] régulier P_k centré à l'origine d'un plan euclidien E. L'ensemble G des isométries g du plan telles que $g(P_k) = P_k$ est un sous-groupe du groupe $O(E) \approx O(2)$ de toutes les isométries du plan.

Le groupe G contient d'une part les rotations d'angles les multiples entiers de $\frac{2\pi}{k}$, et d'autre part des symétries relativement à des axes passant par l'origine du plan. Si k est impair, chacun de ces axes contient un sommet et le milieu d'un côté de P_k. Si k est pair, certains de ces axes contiennent deux sommets opposés de P_k, et les autres les milieux de deux côtés opposés de P_k. Le groupe G contient donc exactement[2] $2k$ éléments. Un tel groupe s'appelle un *groupe diédral*.

Notons que G agit naturellement sur l'ensemble des sommets de P_k ; cette action est fidèle et transitive. En particulier, G s'identifie à un sous-groupe d'ordre $2k$ du groupe symétrique $\mathrm{Sym}(k)$.

Lorsque k est pair, le groupe G agit aussi sur l'ensemble des paires de sommets opposés (action transitive non fidèle), d'où un homomorphisme (non injectif) de G dans $\mathrm{Sym}(k/2)$.

1.4. Majorations pour les ordres des sous-groupes de $\mathcal{SO}(E)$ et $\mathcal{O}(E)$ définis par un polytope. Soit E un espace euclidien de dimension 3.

Nous ne détaillons pas ici les définitions relatives aux *polytopes* dans E. Pour fixer le vocabulaire, convenons toutefois qu'un polytope a un nombre fini de *sommets*, un nombre fini d'*arêtes* contenant chacune deux sommets, et un nombre fini de *faces* dont chacune est un polygone à un certain nombre (au moins 3) de sommets.

(i) Soient $S, S', S'' \in E$ trois points linéairement indépendants, $A \subset E$ l'arête d'extrémités S, S', et F une « face » de laquelle S, S' et S'' sont des sommets.

Si $g \in \mathcal{SO}(E)$ est tel que $g(S) = S$ et $g(A) = A$, alors $g = \mathrm{id}_E$; en effet, les conditions sur g impliquent que cette rotation a deux vecteurs propres linéairement indépendants de valeur propre 1, d'où l'affirmation.

Si $g \in \mathcal{O}(E)$ est tel que $g(S) = S$, $g(A) = A$ et $g(F) = F'$, alors $g = \mathrm{id}_E$, par un argument similaire.

Remarque. Lorsque $g(S) = S$, alors $g(A) = A$ si et seulement si $g(S') = S'$; lorsque $g(S) = S$ et $g(S') = S'$, alors $g(F) = F$ si et seulement si $g(S'') = S''$.

(ii) Soit P un polytope de E. On suppose que tout triple de sommets de P est linéairement indépendant.

Pour $j = 1, 2$, soient S_j, S'_j, S''_j trois sommets distincts de P ; notons A_j l'arête de P contenant S_j, S'_j et F_j une face de P de laquelle S_j, S'_j et S''_j sont des sommets.

Il existe au plus un élément $g \in \mathcal{SO}(E)$ tel que $g(S_1) = S_2$ et $g(A_1) = A_2$; en effet, si g_1 et g_2 sont deux éléments de ce type, alors $g_1^{-1} g_2 = \mathrm{id}_E$ par (i).

---

[1] Mot à prendre avec le grain de sel ad hoc si $k = 2$.

[2] On peut estimer évident que G ne contient pas d'autres éléments que ceux décrits plus haut. On peut aussi appliquer la méthode du numéro suivant.

De même, il existe au plus un élément $g \in \mathcal{O}(E)$ tel que $g(S_1) = S_2$ et $g(A_1) = A_2$ et $g(F_1) = F_2$.

(iii) Soit P comme dans (ii).

Notons d'abord SG_P l'ensemble des rotations $g \in \mathcal{SO}(E) \approx \mathcal{SO}(3)$ telles que $g(P) = P$. Soit $\mathcal{SD}(P)$ l'ensemble[3] des paires (S, A) où S est un sommet de P et A une arête de P contenant S. Alors l'ordre de SG_P est au plus égal à l'ordre de $\mathcal{SD}(P)$; c'est une conséquence de (ii) !

Notons ensuite G_P l'ensemble des isométries $g \in \mathcal{O}(E) \approx \mathcal{O}(3)$ telles que $g(P) = P$. Soit $\mathcal{D}(P)$ l'ensemble des triples (S, A, F) où S est un sommet de P et A une arête de P contenant A et F une face de P contenant A. Alors l'ordre de G_P est au plus égal à l'ordre de $\mathcal{D}(P)$.

1.5. Exemple : les deux groupes du tétraèdre. Soit T un tétraèdre régulier centré à l'origine d'un espace euclidien E de dimension 3.

Le sous-groupe SG_T de $\mathcal{SO}(E)$ contient au plus 12 éléments par le numéro précédent. En fait, il en contient exactement 12, qui sont :

(i) l'identité,

(ii) les demi-tours d'axes passant par les milieux de deux arêtes opposées de T (il y a 3 rotations de ce type),

(iii) les tiers de tour d'axes passant par les sommets de T (il y a 8 rotations de ce type).

Par ailleurs, ce groupe agit naturellement

(a) sur l'ensemble des 4 sommets de T, d'où un homomorphisme injectif $G_T \longrightarrow \mathrm{Sym}(4)$,

(b) sur l'ensemble des 6 arêtes de T, d'où un homomorphisme injectif $G_T \longrightarrow \mathrm{Sym}(6)$,

(c) sur l'ensemble des 3 droites liant les milieux d'arêtes opposées de T, d'où un homomorphisme non injectif $G_T \longrightarrow \mathrm{Sym}(3)$.

Exercice. Montrer que l'image de SG_T dans Sym(4), voir (b), coïncide avec le groupe alterné Alt(4). Déterminer le noyau de l'homomorphisme de G_T dans Sym(3), voir (c).

Considérons ensuite le groupe G_T des isométries g de E telles que $g(T) = T$. Ce groupe agit naturellement et fidèlement[4] sur les sommets de T, d'où un homomorphisme injectif de G_T dans Sym(4). Pour toute paire (x, y) de sommets de T, la symétrie fixant le plan médiateur de l'arête joignant x à y est une isométrie de G_T qui échange x et y, et qui laisse fixes les deux autres sommets de T ; cette symétrie correspond à une transposition de Sym(4). L'image naturelle de G_T dans Sym(4) contient donc toutes les transpositions, et par suite coïncide avec Sym(4) tout entier ; en d'autres termes, *les groupes* G_T *et* Sym(4) *sont isomorphes.*

[3] La lettre $\mathcal{D}$ est l'initiale de « drapeau » , et $\mathcal{S}$ celle de « spécial ».

[4] Car une isométrie de E est complètement déterminée par les images de 3 sommets linéairement indépendants.

Exercices du § IX.1

(IX.1) **Les deux groupes du cube.** Soit C un cube centré à l'origine d'un espace euclidien E de dimension 3.

(i) Montrer que le sous-groupe SG_C de $\mathcal{SO}(E)$ a 24 éléments, et les énumérer.

(ii)$^\sharp$ En considérant l'action de SG_C sur l'ensemble des 4 diagonales de C, montrer que SG_C est isomorphe à Sym(4).

(iii) En considérant l'action de SG_C sur l'ensemble des trois droites passant par les milieux d'arêtes opposées, montrer qu'il existe un homomorphisme surjectif $SG_C \longrightarrow$ Sym(3). Quel est son noyau ?

(iv) Montrer que le groupe G_C a 48 éléments.

[*Indication* : $G_C = SG_C \sqcup (-SG_C)$.]

(IX.2) **Les deux groupes de l'icosaèdre.** Le groupe SG_I des rotations d'un espace euclidien de dimension 3 qui laissent invariant un icosaèdre régulier I est un groupe à 60 éléments. On peut montrer qu'il est isomorphe au groupe Alt(5).

Le sous-groupe correspondant G_I de $\mathcal{O}(3)$ est isomorphe au produit direct de SG_I et du groupe $\{\pm id\}$.

Remarques. (i) Le groupe du (IX.2) intervient également dans l'analyse des racines d'une équation polynomiale du cinquième degré. Galois a expliqué le fait qu'il n'existe en général pas de formule «par radicaux» pour un telle équation par la propriété du groupe Alt(5) de n'avoir aucun sous-groupe H ayant la propriété «$gHg^{-1} = H$ pour tout $g \in$ Alt(5)» , à part les sous-groupes évidents $H =$ Alt(5) et $H = \{1\}$. Au contraire, l'existence de formules «par radicaux» pour les équation de degrés 2, 3 et 4 et intimement liée à l'existence de tels sous-groupes, par exemple dans Sym(4) à un sous-groupe d'ordre 4 (voir l'exercice (IX.1)(iii)).

(ii) Soient E un espace euclidien de dimension trois, P un polytope de E dont l'intérieur contient l'origine, $\mathcal{D}_P$ et G_P l'ensemble des drapeaux et le groupe introduits au numéro 1.4. En général, $|G_P| < |\mathcal{D}_P|$. Pour un polytope «général» , on a d'ailleurs $G_P = \mathrm{id}_E$.

En fait, il existe à similitude près exactement 5 polytopes pour lesquels $|G_P| = |\mathcal{D}_P|$, qui sont le tétraèdre, le cube, l'octaèdre, le dodécaèdre et l'icosaèdre. Il y a une classification analogue en toutes dimensions, due au mathématicien bernois Ludwig Schläfli (1814–1895), et obtenue avant 1853. Pour quelques éléments biographiques sur ce mathématicien tout à fait atypique mais certainement génial et très en avance sur son temps, voir les pages 141–144 du livre *Regular polytopes* de H.S.M. Coxeter (Dover, 1973).

(IX.3) **Théorème de Cayley, 1878).** Pour tout groupe fini G, montrer qu'il existe un entier n et un sous-groupe du groupe symétrique Sym(n) isomorphe à G.

[*Indication* : considérer l'action du groupe G sur lui-même par multiplication à gauche, c'est-à-dire l'action donnée par $G \times G \longrightarrow G$, $(g, x) \longmapsto gx$.]

(IX.4) Soient K un corps et $n \geq 2$ un entier. Soit S le sous-groupe de $GL(n, \mathbb{K})$ des matrices dont tous les coefficients sont 0 ou 1, matrices qui ont de plus exactement un coefficient non nul par ligne et un coefficient non nul par colonne. Vérifier que H est isomorphe au groupe symétrique de n lettres.

(IX.5) Soient G un groupe fini et $\mathbb{K}$ un corps. Montrer qu'il existe un entier n et un sous-groupe du groupe linéaire général $GL(n, \mathbb{K})$ isomorphe à G.

Très brève évocation de résultats plus récents. Pour un groupe G agissant sur un ensemble X, nous avons déja défini la notion de *transitivité*. Plus généralement, pour un entier k, le groupe G est dit *k-transitif* si, chaque fois qu'on se donne un premier k-uple $(x_1, \ldots, x_k)$ d'éléments de X distincts deux à deux et un second k-uple $(y_1, \ldots, y_k)$ de la même espèce, il existe $\sigma \in G$ tel que $\sigma(x_1) = y_1$, …, $\sigma(x_k) = y_k$.

Par exemple, il est évident que $\mathrm{Sym}(n)$ est n-transitif sur J_n, et il est facile de vérifier que $\mathrm{Alt}(n)$ est $(n-2)$-transitif.

L'étude des groupes k-transitifs pour $k \geq 2$ a suscité dès le XIXème siècle un très grand intérêt. Pour un sous-groupe G de $\mathrm{Sym}(n)$ qui n'est ni $\mathrm{Sym}(n)$ lui-même ni $\mathrm{Alt}(n)$ et pour $k \geq 6$, il se trouve que G n'est *jamais* k-transitif. Les constructions de groupes 2-transitifs sont abondantes, et celles de groupes k-transitifs pour $k \in \{3, 4, 5\}$ constituent un beau chapitre de mathématiques, illustré notamment dès 1860 par E. Matthieu.

Les progrès récents de la théorie des groupes finis, et en particulier la « classification des groupes finis simples » (vers 1980), ont montré comment on peut classer les groupes k-transitifs pour $k \geq 2$.

2. Les groupes $\mathcal{SU}(2)$ et $\mathcal{SO}(3)$

On désigne par $M_2(\mathbb{C})$ l'algèbre des matrices 2-fois-2 à coefficients complexes ; ici, « algèbre » signifie que $M_2(\mathbb{C})$ est

(i) un espace vectoriel complexe,

(ii) un anneau avec unité pour l'addition et la multiplication des matrices,

(iii) et que ces deux structures satisfont des relations de compatibilité que nous n'explicitons pas[5].

L'ensemble de ses éléments inversibles de cette algèbre constitue un groupe (pour la multiplication) noté $GL_2(\mathbb{C})$.

On considère l'espace hermitien standard $\mathbb{C}^2$, et on note $\langle \xi \mid \eta \rangle$ le produit scalaire de deux vecteurs ξ, η de $\mathbb{C}^2$. Rappelons que le *groupe unitaire* $\mathcal{U}(2)$ est le groupe des matrices $g \in M_2(\mathbb{C})$ telles que

$$\langle g\xi \mid g\eta \rangle = \langle \xi \mid \eta \rangle \quad \text{pour tous} \quad \xi, \eta \in \mathbb{C}^2,$$

ou de manière équivalente le groupe des matrices dont les colonnes constituent une base orthonormale de l'espace $\mathbb{C}^2$. C'est un sous-groupe de $GL_2(\mathbb{C})$. Rappelons de plus que le déterminant fournit un homomorphisme surjectif du groupe $\mathcal{U}(2)$ sur le groupe des nombres complexes de module 1.

[5] Elles sont toute « évidentes » ! En voici une : $\lambda(ab) = (\lambda a)b = a(\lambda b)$ pour tous $\lambda \in \mathbb{C}$ et $a, b \in M_2(\mathbb{C})$.

Le *groupe unitaire spécial* $\mathcal{SU}(2)$ est le sous-groupe des matrices de déterminant 1 dans $\mathcal{U}(2)$.

2.1. Proposition. *Avec les notations ci-dessus :*

$$\mathcal{SU}(2) \;=\; \left\{ \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \in M_2(\mathbb{C}) \;\middle|\; |a|^2 + |b|^2 = 1 \right\}.$$

Preuve. Soit $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{C})$. Si $g \in \mathcal{SU}(2)$, alors

$$\begin{aligned} |a|^2 + |c|^2 \;&=\; |b|^2 + |d|^2 \;=\; 1 \\ \bar{a}b + \bar{c}d \;&=\; ad - bc - 1 \;=\; 0. \end{aligned}$$

Si $b = 0$, ces équations impliquent successivement

$$|d| \;=\; 1 \qquad c \;=\; 0 \qquad |a| \;=\; 1 \qquad ad \;=\; 1$$

de sorte que g a bien la forme décrite dans l'énoncé.

Si $b \neq 0$, alors

$$\begin{aligned} \bar{a}b + \bar{c}d \;&=\; 0 \quad \text{implique} \quad a = -\frac{c\bar{d}}{\bar{b}}, \\ ad - bc = 1 \quad &\text{implique} \quad -\frac{c|d|^2 + |b|^2 c}{\bar{b}} \;=\; -\frac{c}{\bar{b}} \;=\; 1 \end{aligned}$$

donc $c = -\bar{b}$ et $a = \bar{d}$.

Réciproquement, toute matrice de la forme $\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}$, avec $|a|^2 + |b|^2 = 1$, est unitaire (colonnes orthonormales) de déterminant 1, donc dans $\mathcal{SU}(2)$. □

2.2. Lemme. *Pour tout $g \in \mathcal{SU}(2)$, il existe une application continue de l'intervalle unité dans $\mathcal{SU}(2)$ qui applique 0 sur la matrice unité et 1 sur la matrice g.*

Preuve. Tout point de la sphère unité

$$\mathbb{S}^3 \;=\; \left\{ (a, b) \in \mathbb{C}^2 \mid |a|^2 + |b|^2 = 1 \right\}$$

peut s'écrire

$$(a, b) \;=\; \left(\sqrt{1 - r^2}\, e^{i\phi}, r e^{i\psi} \right)$$

avec $r \in [0, 1]$ et $\phi, \psi \in \,]-\pi, \pi]$. (Note : une telle écriture est unique si $a \neq 0$ et $b \neq 0$.) La fonction continue

$$\gamma \;:\; \begin{cases} \quad \longrightarrow & \mathbb{S}^3 \\ t \;\longmapsto & \left(\sqrt{1 - t^2 r^2}\, e^{it\phi}, tr e^{it\psi} \right) \end{cases}$$

définit un « chemin continu dans $\mathbb{S}^3$ » d'origine $\gamma(0) = (1, 0)$ et d'extrémité $\gamma(1) = (a, b)$.

Comme $\mathcal{SU}(2)$ s'identifie à $\mathbb{S}^3$, ceci prouve le lemme. □

(En topologie, le résultat du lemme 2.2 s'exprime par : « le groupe $\mathcal{SU}(2)$ est connexe par arcs, et en particulier connexe ».)

2.3. Définition. On désigne par $\mathbb{H}$ l'ensemble des matrices de $M_2(\mathbb{C})$ de la forme

$$\begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix} \qquad z, w \in \mathbb{C}.$$

L'ensemble $M_2(\mathbb{C})$, qui est naturellement un espace vectoriel (et une algèbre) *complexe* de dimension 4, est aussi un espace vectoriel (et une algèbre) *réel* de dimension 8 ; l'espace $\mathbb{H}$ est un sous-espace *réel* de dimension 4 de cet espace réel de dimension 8.

Attention : $\mathbb{H}$ *n'est pas* un sous-espace vectoriel de l'espace vectoriel complexe $M_2(\mathbb{C})$, par exemple parce que, pour tout nombre réel $t \neq 0$, nous avons $\begin{pmatrix} t & 0 \\ 0 & t \end{pmatrix} \in \mathbb{H}$ et $i\begin{pmatrix} t & 0 \\ 0 & t \end{pmatrix} \notin \mathbb{H}$.

Remarque. Il résulte des définitions que $\mathcal{SU}(2) \subset \mathbb{H}$. Plus précisément et en anticipant sur le numéro 2.6, le groupe $\mathcal{SU}(2)$ est le sous-ensemble des éléments de norme 1 dans $\mathbb{H}$.

Exercice. Ecrire une base de l'espace $M_2(\mathbb{C})$ vu comme espace vectoriel réel de dimension 8.

2.4. Base. Les éléments

$$e_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad e_1 = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \qquad e_2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad e_3 = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

forment une base de l'espace vectoriel *réel* $\mathbb{H}$.

Remarque. En physique, les matrices

$$\sigma_x = -ie_3 \qquad \sigma_y = -ie_2 \qquad \sigma_z = -ie_1$$

s'appellent les *matrices de Pauli.* (!!! On trouve aussi d'autres normalisations !!!)

2.5. Remarque et définition. Le produit de deux matrices de $\mathbb{H}$ est encore dans $\mathbb{H}$:

$$\begin{pmatrix} z_1 & w_1 \\ -\overline{w}_1 & \overline{z}_1 \end{pmatrix}\begin{pmatrix} z_2 & w_2 \\ -\overline{w}_2 & \overline{z}_2 \end{pmatrix} = \begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix}$$

où

$$z = z_1z_2 - w_1\overline{w_2} \qquad w = z_1w_2 + w_1\overline{z_2}.$$

Avec le produit des matrices, $\mathbb{H}$ est connu sous le nom *d'algèbre des quaternions,* ou plus précisément d'algèbre des quaternions *de Hamilton.*

Exercice. Écrire la table de multiplication de la base du numéro 2.4.

2.6. Produit scalaire euclidien. On définit un produit scalaire sur l'espace réel $\mathbb{H}$ en posant

$$\left\langle \begin{pmatrix} z_1 & w_1 \\ -\overline{w}_1 & \overline{z}_1 \end{pmatrix} \;\middle|\; \begin{pmatrix} z_2 & w_2 \\ -\overline{w}_2 & \overline{z}_2 \end{pmatrix} \right\rangle = \mathrm{Re}\,(\overline{z_1}z_2 + \overline{w_1}w_2)\,.$$

La norme associée est donnée par

$$\left\| \begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix} \right\|^2 = |z|^2 + |w|^2 = \det \begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix}.$$

La base $\{e_0, e_1, e_2, e_3\}$ est orthonormale pour ce produit scalaire, et le groupe $\mathcal{SU}(2)$ s'identifie à la sphère unité de l'espace euclidien $\mathbb{H}$ de dimension 4.

Attention : Comme déjà noté au N^o 3, il faut bien prendre garde au fait qu'on considère $\mathbb{H}$ comme un espace vectoriel *réel,* et que ce produit scalaire en fait un espace *euclidien*, même si z et w désignent ci-dessus des nombres complexes ! (De même qu'on peut - et que parfois on doit - considérer $\mathbb{C}^2$ comme un espace vectoriel *réel* de dimension 4.)

Exercice. (i) Vérifier que le produit scalaire défini au N^o 2.6 s'écrit aussi $\langle X \mid Y\rangle = \frac{1}{2}\,\mathrm{trace}(X^*Y)$ pour $X, Y \in \mathbb{H}$.

(ii) Soit $\langle\,|\,\rangle$ le produit scalaire canonique sur $\mathbb{C}^2$. Pour toute paire (v, w) de vecteurs dans l'espace $\mathbb{C}^2$ considéré comme espace vectoriel *réel* de dimension 4, espace noté V plus bas, on pose

$$\langle v \mid w\rangle_{\mathbb{R}} = \mathrm{Re}\,(\langle v \mid w\rangle)\,.$$

Vérifier que $\langle v \mid w\rangle_{\mathbb{R}}$ est un produit scalaire euclidien sur l'espace V. En déduire qu'il existe un homomorphisme de groupes $\mathcal{U}(2) \longrightarrow \mathcal{O}(4)$.

En utilisant le lemme 2.2, on montre facilement que l'image de cet homomorphisme est en fait dans $\mathcal{SO}(4)$.

(iii) Plus généralement, il existe un homomorphisme de groupes naturel $\mathcal{U}(n) \longrightarrow \mathcal{SO}(2n)$ pour tout $n \geq 1$.

2.7. Lemme. *Soit $g \in \mathcal{SU}(2)$. Les applications linéaires*

$$\begin{cases} \mathbb{H} \longrightarrow \mathbb{H} \\ X \longmapsto gX \end{cases} \qquad \textit{et} \qquad \begin{cases} \mathbb{H} \longrightarrow \mathbb{H} \\ X \longmapsto Xg \end{cases}$$

sont orthogonales.

Preuve. Comme $\det(g) = 1$,

$$\|gX\|^2 = \det(gX) = \det(X) = \|X\|^2$$

et l'application $X \longmapsto gX$ est orthogonale. De même, l'application $X \longmapsto Xg$ est orthogonale. □

2.8. L'orthogonal $i\mathbb{E} \approx \mathbb{R}^3$ de e_0 dans $\mathbb{H}$. On désigne par $\mathbb{E}$ l'espace des matrices hermitiennes 2-fois-2 de trace nulle, c'est-à-dire l'espace des matrices de la forme

$$\begin{pmatrix} x_1 & x_2 + ix_3 \\ x_2 - ix_3 & -x_1 \end{pmatrix} \qquad \text{avec } x_1, x_2, x_3 \in \mathbb{R}.$$

Cet espace a un produit scalaire naturel avec norme associée définie par

$$\left\| \begin{pmatrix} x_1 & x_2 + ix_3 \\ x_2 - ix_3 & -x_1 \end{pmatrix} \right\|^2 = x_1^2 + x_2^2 + x_3^2 \quad \text{c'est-à-dire } \|X\|^2 = -\det(X) = \det(iX).$$

D'une part, on observe que $i\mathbb{E}$ s'identifie à l'orthogonal de e_0 dans $\mathbb{H}$; d'autre part, on peut identifier $\mathbb{E}$ à l'espace euclidien usuel $\mathbb{R}^3$ (avec coordonnées x_1, x_2, x_3), et donc le groupe orthogonal de $\mathbb{E}$ à $\mathcal{O}(3)$ [respectivement le groupe orthogonal spécial de $\mathbb{E}$ à $\mathcal{SO}(3)$].

2.9. L'homomorphisme surjectif de $\mathcal{SU}(2)$ sur $\mathcal{SO}(3)$.

THÉORÈME. (i) *Pour tout $g \in \mathcal{SU}(2)$ et pour tout $X \in \mathbb{E}$, on a*

$$gXg^* \in \mathbb{E}.$$

De plus $\|gXg^*\| = \|X\|$; en d'autres termes, l'opérateur linéaire $\Psi(g) : \mathbb{E} \longrightarrow \mathbb{E}$ défini par

$$\Psi(g) : X \longmapsto gXg^*$$

est orthogonal.

(ii) *L'application*

$$\Psi : \begin{cases} \mathcal{SU}(2) & \longrightarrow & \mathcal{O}(3) \\ g & \longmapsto & \Psi(g) \end{cases}$$

est un homomorphisme de groupes.

(iii) *L'image de Ψ est dans le sous-groupe $\mathcal{SO}(3)$ de $\mathcal{O}(3)$.*

(iv) *L'homomorphisme $\Psi : \mathcal{SU}(2) \longrightarrow \mathcal{SO}(3)$ est surjectif.*

(v) *Le noyau de Ψ est le sous-groupe à deux éléments $\{e_0, -e_0\}$ de $\mathcal{SU}(2)$.*

PREUVE. (i) Le lemme 2.7 montre que l'application $\begin{cases} \mathbb{H} \longrightarrow \mathbb{H} \\ Y \longmapsto gYg^* \end{cases}$ est orthogonale. Comme elle préserve e_0, elle préserve aussi l'orthogonal $i\mathbb{E}$ de e_0 dans $\mathbb{H}$.

Par suite, pour tout $X \in \mathbb{E}$, on a $g(iX)g^* \in i\mathbb{E}$ et $\|g(iX)g^*\| = \|iX\|$, c'est-à-dire $gXg^* \in \mathbb{E}$ et $\|gXg^*\| = \|X\|$.

(ii) Cela résulte du calcul

$$\Psi(g)\big(\Psi(h)(X)\big) = \Psi(g)\big(hXh^*\big) = ghXh^*g^* = (gh)X(gh)^* = \Psi(gh)(X)$$

où $g, h \in \mathcal{SU}(2)$ et $X \in \mathbb{H}$.

(iii) Soit $g \in \mathcal{SU}(2)$. Si $\gamma : [0,1] \longrightarrow \mathcal{SU}(2)$ est comme dans le preuve du lemme 2.2, l'application

$$\delta : \begin{cases} \longrightarrow \{1, -1\} \\ t \longmapsto det\big(\Psi(\gamma(t))\big) \end{cases}$$

est continue. Comme $\delta(0) = \det(\Psi(e_0)) = \det(I_3) = +1$, on a aussi par continuité $\delta(1) = \det(\Psi(g)) = +1$, de sorte que g est bien dans $\mathcal{SO}(3)$. (On a noté e_0, comme au n^o 4, la matrice unité à deux lignes et deux colonnes, qui est l'élément neutre de $\mathcal{SU}(2)$, et I_3 la matrice unité à trois lignes et colonnes, qui est l'élément neutre de $\mathcal{SO}(3)$.)

(iv) La preuve se décompose en plusieurs pas.

Premier pas. Toute rotation autour du premier axe est dans l'image de Ψ. En effet, pour tout $\phi \in \mathbb{R}$, on a $\begin{pmatrix} e^{i\phi} & 0 \\ 0 & e^{-i\phi} \end{pmatrix} \in \mathcal{SU}(2)$ et

$$\begin{aligned} \begin{pmatrix} e^{i\phi} & 0 \\ 0 & e^{-i\phi} \end{pmatrix} \begin{pmatrix} x_1 & x_2+ix_3 \\ x_2-ix_3 & -x_1 \end{pmatrix} \begin{pmatrix} e^{-i\phi} & 0 \\ 0 & e^{i\phi} \end{pmatrix} \\ = \begin{pmatrix} x_1 & e^{2i\phi}(x_2+ix_3) \\ e^{-2i\phi}(x_2-ix_3) & -x_1 \end{pmatrix} \\ = \begin{pmatrix} x_1 & y_2+iy_3 \\ y_2-iy_3 & -x_1 \end{pmatrix} \end{aligned}$$

avec

$$\begin{aligned} y_2 &= (\cos(2\phi))x_2 - (\sin(2\phi))x_3 \\ y_3 &= (\sin(2\phi))x_2 + (\cos(2\phi))x_3. \end{aligned}$$

Il en résulte que

$$\Psi\left(\begin{pmatrix} e^{i\phi} & 0 \\ 0 & e^{-i\phi} \end{pmatrix}\right) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(2\phi) & -\sin(2\phi) \\ 0 & \sin(2\phi) & \cos(2\phi) \end{pmatrix}$$

est la rotation d'angle 2ϕ autour du premier axe. (Noter le facteur 2 !)

Deuxième pas. Pour tout $X = \begin{pmatrix} x_1 & x_2+ix_3 \\ x_2-ix_3 & -x_1 \end{pmatrix} \in \mathbb{E}$, il existe $g \in \mathcal{SU}(2)$ tel que $gXg^* = \begin{pmatrix} r & 0 \\ 0 & -r \end{pmatrix}$, où $r = \sqrt{x_1^2+x_2^2+x_3^2}$.

En effet, comme $tr(X) = 0$ et $\det(X) = -r^2$, les valeurs propres de X sont r et $-r$. Comme X est une matrice autoadjointe, on sait qu'il existe une matrice $h \in \mathcal{U}(2)$ telle que $hXh^* = \begin{pmatrix} r & 0 \\ 0 & -r \end{pmatrix}$. Choisissons une racine carrée β de $\det(h)$; comme h est unitaire, $|\det(h)| = 1$ et $|\beta| = 1$. (Remarque importante : il n'y a pas de choix canonique pour la racine β qui dépende continûment de la matrice h.) Posons $g = \beta^{-1}h$; on a $g \in \mathcal{U}(2)$ et $\det(g) = \beta^{-2}\det(h) = 1$, c'est-à-dire $g \in \mathcal{SU}(2)$, et on a encore $gXg^* = \begin{pmatrix} r & 0 \\ 0 & -r \end{pmatrix}$.

Conséquence du deuxième pas. Considérons la sphère unité

$$\mathbb{S}^2 = \left\{ \begin{pmatrix} x_1 & x_2+ix_3 \\ x_2-ix_3 & -x_1 \end{pmatrix} \in \mathbb{E} \;\middle|\; x_1^2+x_2^2+x_3^2 = 1 \right\}$$

de $\mathbb{E}$, et remarquons que

$$-ie_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

s'identifie au point d'intersection de $\mathbb{S}^2$ et de la partie positive du premier axe. Si $X \in \mathbb{S}^2$, il existe donc $g \in \mathcal{SU}(2)$ tel que $\Psi(g)(X) = gXg^* = -ie_1$. Par suite

l'action naturelle de $\Psi(\mathcal{SU}(2))$ sur $\mathbb{S}^2$ est transitive.

[Il y a une action naturelle du groupe des rotations sur la sphère unité $\mathbb{S}^2$, et donc aussi de tout sous-groupe du groupe des rotations – par exemple l'image de Ψ ci-dessus – sur cette même sphère. C'est de cette action-là qu'il s'agit dans la conséquence énoncée ici.]

Troisième pas. Les deux premiers pas achèvent la preuve du point (iv) en vertu du lemme ci-dessous.

(v) Il est évident que $\Psi(-e_0) = I_3$. Réciproquement, soit $g \in \mathcal{SU}(2)$ tel que $\Psi(g) = I_3$, c'est-à-dire tel que $gXg^* = X$ pour tout $X \in \mathbb{E}$. Alors

$$g \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} g,$$

d'où il résulte que la matrice g est diagonale. Le calcul du premier pas de la preuve de (iv) montre que $\Psi(g) = I_3$ implique $g = e_0$ ou $g = -e_0$. □

2.10. Lemme. *Soit H un sous-groupe de $\mathcal{SO}(3)$ possédant les deux propriétés suivantes :*

(i) *H contient toutes les rotations autour du premier axe,*

(ii) *H agit transitivement sur la sphère unité $\mathbb{S}^2$ de $\mathbb{R}^3$.*

Alors $H = \mathcal{SO}(3)$.

Preuve. Notons M le premier vecteur de coordonnées, vu comme un point de $\mathbb{S}^2$. Soit $g \in \mathcal{SO}(3)$. Par (ii), il existe $h \in H$ tel que $h(M) = g(M)$. Par suite $h^{-1}g(M) = M$, de sorte que $h^{-1}g$ est une rotation autour du premier axe. Par (i), $h^{-1}g \in H$; il en résulte que $g = h(h^{-1}g) \in H$. □

Exercice. Soient $X \in \mathbb{E}$ tel que $\|X\| = 1$ et $\phi \in \mathbb{R}$. Vérifier que la matrice

$$g \;=\; (\cos\theta)e_0 + (\sin\theta)iX$$

de $\mathbb{H}$ est dans $\mathcal{SU}(2)$ et que $\Psi(g)$ est une rotation d'angle 2θ fixant les points $X, -X$ de la sphère unité de $\mathbb{E}$.

2.11. Exemples de sous-groupes finis de $\mathcal{SO}(3)$.

(i) Pour toute droite d passant par l'origine de $\mathbb{R}^3$ et pour tout entier $k \geq 1$, la rotation d'angle $\frac{2\pi}{k}$ et ses itérés constituent un sous-groupe à k éléments $C_k^{(d)}$ de $\mathcal{SO}(3)$ qui est un *groupe cyclique d'ordre k,* isomorphe à $\mathbb{Z}/k\mathbb{Z}$.

Pour deux telles droites d, d', il existe une rotation $g \in \mathcal{SO}(3)$ telle que $g(d') = d$, et donc telle que $gC_k^{(d')}g^{-1} = C_k^{(d)}$. On dit que les sous-groupes de $\mathcal{SO}(3)$ du type $C_k^{(d)}$ sont *conjugués deux à deux.*

(ii) On considère une droite d comme ci-dessus, un entier $k \geq 2$, un plan $\mathbb{E}^2$ de $\mathbb{R}^3$ contenant l'origine et orthogonal à d, ainsi qu'un polygone régulier $\mathbb{P}$ à k sommets dans $\mathbb{E}^2$.

A toute droite e de $\mathbb{E}^2$ contenant l'origine et un sommet ou un milieu d'un côté de $\mathbb{P}$ on associe le demi-tour g_e d'axe e. Les k demi-tours ainsi définis et le groupe de (i)

constituent un sous-groupe à $2k$ éléments $D_{2k}^{d,P}$ de $\mathcal{SO}(3)$ qui est un *group diédral d'ordre* $2k$.

Lorsque d et $\mathbb{P}$ varient (toujours avec $\mathbb{P}$ orthogonal à d, et à k sommets), on obtient une famille de sous-groupes finis de $\mathcal{SO}(3)$ dont les éléments sont à nouveau *conjugués deux à deux*.

(iii) Soit $\mathbb{T}$ [respectivement $\mathbb{O}$, $\mathbb{I}$] un tétraèdre régulier [resp. un octaèdre régulier, un icosaèdre régulier] centré à l'origine de $\mathbb{R}^3$. Les sous-groupes $SG_{\mathbb{T}}$, $SG_{\mathbb{O}}$ et $SG_{\mathbb{I}}$ de $\mathcal{SO}(3)$ ont déjà étés évoqués au § 1 ; ils sont respectivement d'ordres 12, 24 et 60.

On obtient comme plus haut trois familles de sous-groupes de $\mathcal{SO}(3)$ conjugués deux à deux.

2.12. Théorème. *Tout sous-groupe fini de $\mathcal{SO}(3)$ apparaît parmi les exemples du numéro précédent.*

Faute d'indiquer la preuve de ce théorème, nous recommendons la lecture du livre de Hermann Weyl intitulé *Symmetry* (Princeton University Press, 1952). Il s'agit de la rédaction de quatre leçons données par Weyl en 1951 et destinées à un large public. Pour le théorème ci-dessus, voir la fin de la deuxième leçon ainsi que l'appendice A.

Les sous-groupes finis de $\mathcal{SO}(3)$ s'organisent donc en deux familles infinies (les groupes cycliques et les groupes diédraux) et trois cas exceptionnels (correspondant aux polytopes réguliers). On peut aussi classer les sous-groupes finis du groupe $\mathcal{O}(3)$ tout entier ; on trouve alors 5 familles infinies supplémentaires et quatre cas exceptionnels supplémentaires (voir l'appendice B du livre de Weyl).

Ces groupes finis jouent un rôle important en chimie-physique, dans la description des cirstaux et des molécules. Ils jouent bien sûr un rôle tout aussi important en géométrie ; ainsi qu'en de nombreux autres chapitres de mathématiques, comme par exemple la théorie de l'équation du cinquième degré (sujet qui n'est en général pas évoqué dans les cours de premier ou second cycle) ou les fonctions d'une variable complexe (sujet abordé en Analyse 2).

A tout sous-groupe fini G de $\mathcal{SO}(3)$ correspond un sous-groupe fini $\Psi^{-1}(G)$ de $\mathcal{SU}(2)$, d'ordre donné par $|\Psi^{-1}(G)| = 2\,|G|$.

CHAPITRE X

Spectres de graphes

1. Motivation. Soit F une fonction à valeurs réelles ou complexes, définie sur un intervalle de la droite, et suffisamment régulière. La dérivée première de F en un point x est donnée par

$$F'(x) \approx \frac{F(x+h) - F(x)}{h}$$

et la seconde dérivée par

$$F''(x) \approx \frac{F'(x) - F'(x-h)}{h} \approx \frac{F(x+h) + F(x-h) - 2F(x)}{h^2}$$

pour h assez petit. De même, si F est une fonction définie sur un domaine U de $\mathbb{R}^2$ et suffisamment régulière, le *laplacien* de F en un point (x, y) du plan est donné par

$$\begin{aligned}(\Delta F)(x,y) &= \frac{\partial^2 F}{\partial x^2}(x,y) + \frac{\partial^2 F}{\partial y^2}(x,y) \\ &\approx \frac{1}{h^2}\Big(F(x+h,y) + F(x-h,y) + F(x,y+h) + F(x,y-h) - 4F(x,y)\Big)\end{aligned}$$

pour h assez petit. « Assez petit » dépend bien sûr des unités choisies, et il est toujours possible de supposer $h = 1$.

Supposons pour simplifier que le domaine U soit un rectangle, et supposons qu'il est quadrillé par une fine grille de sommets $(x_{i,j})_{0 \le i \le k+1, 0 \le j \le l+1}$. L'étude des fonctions F sur U qui sont *harmoniques dans* U, c'est-à-dire telles que $\Delta F(x, y) = 0$ pour tout $(x, y) \in U$, motive l'étude des fonctions f définies aux seuls sommets de la grille et satisfaisant les relations

$$\frac{f(x_{i+1,j}) + f(x_{i-1,j}) + f(x_{i,j+1}) + f(x_{i,j-1})}{4} = f(x_{i,j})$$

pour tous $i \in \{1, \ldots, k\}$ et $j \in \{1, \ldots, l\}$.

D'autres situations conduisent à considérer des « grilles » de formes autres que rectangulaires, et plus généralement des « graphes », au sens suivant.

2. Définitions. Un *graphe* G est un couple (V, E) où V est un ensemble (dont les éléments sont les *sommets* du graphe) et E un sous-ensemble de l'ensemble des parties à deux éléments de E (les éléments de E sont les *arêtes* du graphe) ; les deux sommets d'une arête sont ses *extrémités.*

Un tel graphe est *connexe* si, pour toute paire $x, y \in V$ se sommets, il existe une suite $x_0 = x, x_1, \ldots, x_{n-1}, x_n = y$ de sommets telle que $\{x_{i-1}, x_i\} \in E$ pour tout $i \in \{1, \ldots, n\}$.

Dans ce chapitre, tous les graphes sont supposés *finis.*

L'ensemble $C(V)$ des fonctions de V dans $\mathbb{R}$ est naturellement un espace vectoriel réel. Il possède une *base canonique* $(\delta_x)_{x\in V}$, où pour tout $x \in V$ la fonction $\delta_x \in C(V)$ est définie par

$$\delta_x(y) = \begin{cases} 1 & \text{si} \quad y = x \\ 0 & \text{sinon.} \end{cases}$$

L'opérateur d'adjacence $A : C(V) \longrightarrow C(V)$ est défini par

$$(Af)(x) = \sum_{y\sim x} f(y)$$

où la notation indique une somme sur les sommets $y \in V$ qui sont liés à x par une arête. La *matrice d'adjacence* est la matrice de A relativement à la base canonique $(\delta_x)_{x\in V}$; par abus d'écriture, on la note également A ; c'est donc la matrice de coefficients $(A_{x,y})_{x,y\in V}$ donnés par

$$A_{x,y} = \begin{cases} 1 & \text{si} \quad \{x, y\} \in E \\ 0 & \text{sinon.} \end{cases}$$

Noter que, en général, il n'y a pas d'ordre *naturel* sur l'ensemble V des sommets du graphe G, ni par conséquent sur les lignes et colonnes de cette matrice.

Le *polynôme caractéristique* du graphe G est le polynôme caractéristique de sa matrice d'adjacence (voir le § V.2). Le *spectre* de G est le spectre de A, c'est-à-dire l'ensemble des valeurs propres de A, avec leurs multiplicités ; la matrice d'adjacence étant par définition symétrique, le spectre d'un graphe est nécessairement *réel*, de sorte que les valeurs propres du graphe sont n nombres réels (certains peuvent être répétés, voir plus bas).

L'exemple de la motivation est un graphe fini donné par un quadrillage d'un domaine du plan.

Exemples à deux et trois sommets. (i) Si G est un segment à deux sommets, $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ et le spectre de G est $(1, -1)$. Si G est un segment à trois sommets, $A = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$ et le spectre de G est $(\sqrt{2}, 0, -\sqrt{2})$. Ce sont des cas particuliers du calcul de Lagrange (§ VI.7 du semestre d'hiver).

(ii) Si G est un triangle, $A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$ et le spectre de G est $(2, -1^2)$, où l'exposant 2 indique que -1 est valeur propre de multiplicité 2.

(iii) Si G a 2 sommets et 0 arête (G est non connexe), son spectre est (0^2). Plus généralement, si G possède n sommets et 0 arête, alors A est la matrice nulle à n lignes et n colonnes, de spectre (0^n).

(iv) Si G possède 3 sommets et une seule arête (G est non connexe), sa matrice d'adjacence est $A = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ et son spectre est $(1, 0, -1)$.

Plus généralement, si $G = (V, E)$ est une réunion disjointe de deux graphes non vides, c'est-à-dire s'il existe une partition de V en deux sous-ensembles disjoints V_1, V_2 tels que toute arête $e \in E$ ait ses deux extrémités dans V_1 ou ses deux extrémités dans V_2, alors le spectre de G est la réunion des spectres des sous-graphes G_1 et G_2, déterminés respectivement par V_1 et V_2. Ceci réduit essentiellement l'étude des spectres de graphes au cas des graphes *connexes.*

3. Exemple des graphes complets. Soient $n \geq 1$ un entier et K_n le *graphe complet* à n sommets $\{1, \ldots, n\}$, c'est-à-dire le graphe pour lequel toute paire $\{x, y\} \subset \{1, \ldots, n\}$ (avec $x \neq y$) est une arête. Pour calculer le spectre de K_n, on peut procéder comme suit.

Soit J_n la matrice n-fois-n dont tous les coefficients sont $+1$, et soit I_n la matrice unité d'ordre n ; la matrice d'adjacence de K_n est $J_n - I_n$.

Un calcul immédiat montre que $J_n^2 = nJ_n$, donc que $\left(\frac{1}{n}J_n\right)^2 = \frac{1}{n}J_n$. La matrice $\frac{1}{n}J_n$, vue comme une application linéaire de l'espace euclidien $\mathbb{R}^n$ dans lui-même, est donc la projection orthogonale de $\mathbb{R}^n$ sur la droite formée des vecteurs de la forme $(t, t, \ldots, t)$ avec $t \in \mathbb{R}$. Par suite, le spectre de $\frac{1}{n}J_n$ est $(1, 0^{n-1})$. Il en résulte que le spectre de $J_n - I_n$ est $(n-1, -1^{n-1})$.

En résumé, le spectre du graphe complet à n sommets est $(n-1, -1^{n-1})$.

4. Rappel du § IV.5 et compléments sur les mineurs. Soient $\mathbb{K}$ un corps, $n \geq 1$ un entier et $A = (a_{i,j})_{1 \leq i,j \leq n} \in M_n(\mathbb{K})$ une matrice carrée à coefficients dans $\mathbb{K}$. Pour un entier $p \in \{1, \ldots, n\}$, un *mineur principal d'ordre p de A* est un déterminant de la forme

$$\det\left(a_{i,j}\right)_{i,j \in H}$$

où $H = \{i_1, \ldots, i_p\}$ est une partie de $\{1, \ldots, n\}$ à p éléments ($1 \leq i_1 < i_2 < \ldots < i_p \leq n$). ainsi la matrice A a-t-elle exactement

(1) n mineurs principaux d'ordre 1, qui sont ses éléments diagonaux $a_{i,i}$, pour $i \in \{1, \ldots, n\}$,

(2) $\frac{n(n-1)}{2}$ mineurs principaux d'ordre 2, qui sont

$$\det\begin{pmatrix} a_{i,i} & a_{i,j} \\ a_{j,i} & a_{j,j} \end{pmatrix} = a_{i,i}a_{j,j} - a_{i,j}a_{j,i},$$

pour $i, j \in \{1, \ldots, n\}$ avec $i < j$,

(3) $\frac{n(n-1)(n-2)}{6}$ mineurs principaux d'ordre 3, qui sont

$$\det\begin{pmatrix} a_{i,i} & a_{i,j} & a_{i,k} \\ a_{j,i} & a_{j,j} & a_{j,k} \\ a_{k,i} & a_{k,j} & a_{k,k} \end{pmatrix}$$

pour $i, j, k \in \{1, \ldots, n\}$ avec $i < j < k$,

(...) .....

$(n-1)$ n mineurs principaux d'ordre $n-1$, qui sont les déterminants des matrices obtenues à partir de A en effaçant la j-ème ligne et la j-ème colonne ($1 \leq j \leq n$),

(n) 1 mineur principal d'ordre n, qui est le déterminant de A.

Rappelons que le déterminant d'une matrice $B = (b_{i,j})_{1 \leq i,j \leq n} \in M_n(\mathbb{K})$ est donné par la formule

$$\det(B) = \sum_{\sigma \in Sym(n)} \epsilon(\sigma) b_{\sigma(1),1} b_{\sigma(2),2} \cdots b_{\sigma(n),n} \in \mathbb{K}. \qquad (*)$$

Pour une matrice $B(X)$ à coefficients dans l'anneau $\mathbb{K}[X]$ des polynômes à une indéterminée à coefficients dans $\mathbb{K}$, la même formule fournit

$$\det(B(X)) \in \mathbb{K}[X].$$

Soient en particulier $A \in M_n(\mathbb{K})$ et $B = XI_n - A$. Les formules ci-dessus montrent que $\det(XI_n - A)$ est un polynôme de degré n, c'est-à-dire un polynôme de la forme

$$\det(XI_n - A) = X^n + c_1(A)X^{n-1} + c_2(A)X^{n-2} + \ldots + c_{n-1}(A)X + c_n(A)$$

où $c_1(A), \ldots, c_n(A) \in \mathbb{K}$.

Pour $p \in \{1, \ldots, n\}$, le coefficient $c_p(A)$ de X^{n-p} provient de termes qui, dans l'analogue du développement $(*)$ pour $XI_n - A$, contient exactement

$$n-p \text{ termes diagonaux } X - a_{i_1,i_1}, \ldots, X - a_{i_{n-p},i_{n-p}} \text{ et } p \text{ autres termes,}$$

c'est-à-dire des termes correspondant aux permutations $\sigma \in Sym(n)$ telles que $\sigma(i_1) = i_1$, …, $\sigma(i_{n-p}) = i_{n-p}$.

Lorsque $n - p = 1$, on a simplement

$$c_1(A) \;=\; -\sum_{i=1}^{n} a_{i,i} \;=\; -\operatorname{trace}(A).$$

Lorsque $n - p = 2$,

$$c_2(A) \;=\; (-1)^2 \sum_{\substack{1 \le i,j \le n \\ i<j}} \epsilon(\sigma) a_{\sigma(i),i} a_{\sigma(j),j}.$$

Pour i, j fixés, la permutation σ, qui est a priori une permutation des entiers $\{1, \ldots, n\}$ fixant tous les entiers distincts de i et j, peut être vue comme une permutation de l'ensemble à deux éléments $\{i, j\}$; par suite

$$c_2(A) \;=\; \sum_{\substack{1 \le i,j \le n \\ i<j}} \det \begin{pmatrix} a_{i,i} & a_{i,j} \\ a_{j,i} & a_{j,j} \end{pmatrix}$$

est la somme de tous les mineurs d'ordre 2 de A.

De même $-c_3(A)$ est la somme de tous les mineurs d'ordre 3 de A, etc.

Il est évident que le terme constant du polynôme $\det(XI_n - A)$ est $(-1)^n \det A$. En résumé :

Proposition. *Le polynôme caractéristique d'une matrice $A \in M_n(\mathbb{K})$ est égal à*

$$\begin{aligned} \det(XI_n - A) \;=\; & X^n - \operatorname{trace}(A) X^{n-1} + c_2(A) X^{n-2} + \ldots \\ & + c_p(A) X^{n-p} + \ldots + c_{n-1}(A) X + (-1)^n \det(A) \end{aligned}$$

où $(-1)^p c_p(A)$ est la somme de tous le mineurs principaux d'ordre p de A, pour $p \in \{1, \ldots, n\}$.

Dans cet énoncé, on a écrit $-\operatorname{trace}(A)$ au lieu de $c_1(A)$ et $(-1)^n \det(A)$ au lieu de $c_n(A)$.

Pour toute matrice inversible $S \in GL(n, \mathbb{K})$, on a évidemment

$$\det(XI_n - A) \;=\; \det(S(XI_n - A)S^{-1}) \;=\; \det(XI_n - SAS^{-1}).$$

En particulier, s'il existe une matrice $S \in GL(n, \mathbb{K})$ telle que $SAS^{-1} = diag(\lambda_1, \ldots, \lambda_n)$, la somme des mineurs princiaux non nuls d'ordre p de A est égale à la somme des mineurs principaux non nuls d'ordre p de $diag(\lambda_1, \ldots, \lambda_n)$, c'est-à-dire à la somme des produits de p valeurs propres de A.

Corollaire. *Avec les notations de la proposition, on suppose de plus que A possède n valeurs propres $\lambda_1, \ldots, \lambda_n$ dans $\mathbb{K}$. Alors*

$$(-1)^p c_p(A) = \sum_{1 \le i_1 < \ldots < i_p \le n} \lambda_{i_1} \ldots \lambda_{i_p},$$

où la somme porte sur tous les sous-ensembles à p éléments de $\{1, \ldots, n\}$.

5. Proposition. *Soit G un graphe à n sommets et*

$$P(T) \;=\; T^n + c_1 T^{n-1} + c_2 T^{n-2} + c_3 T^{n-3} + \ldots + c_n$$

son polynôme caractéristique. Alors :

$c_1 = 0$,

$-c_2$ *est le nombre d'arêtes de G,*

$-c_3$ *est deux fois le nombre de triangles de G.*

Exercice préliminaire à la preuve : vérifier la proposition 5 lorsque G est un triangle.

Remarque. Il est possible de « continuer » ; par exemple, c_4 est le nombre de paires d'arêtes disjointes moins deux fois le nombre de cycles de longueur 4 dans G.

Rappel. Les coefficients c_j du polynôme P de la proposition 5 s'expriment facilement en termes des valeurs propres du graphe ; par exemple, $-c_1$ est la somme des valeurs propres de G.

Preuve. Pour tout $p \in \{1, \ldots, n\}$, le nombre $(-1)^p c_p$ est la somme des mineurs principaux d'ordre p de la matrice d'adjacence A du graphe G. On peut donc raisonner comme suit.

(i) Comme les termes diagonaux de A sont tous nuls, on a $c_1 = 0$.

(ii) Comme les mineurs principaux de A à 2 lignes et colonnes qui sont non identiquement nuls sont de la forme $\begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix}$ et correspondent bijectivement aux arêtes du graphe, on a bien

$$(-1)^2 c_2 \;=\; -(\text{nombre d'arêtes}).$$

(iii) Pour les mineurs principaux de A à 3 lignes et colonnes qui sont non identiquement nuls, il y a à permutation près des lignes et colonnes trois possibilités qui sont

$$\begin{vmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{vmatrix} \quad , \quad \begin{vmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{vmatrix} \quad \text{et} \quad \begin{vmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{vmatrix}.$$

Les deux premiers déterminants sont nuls, et le troisième vaut 2.

Ce troisième cas correspond à trois sommets mutuellement adjacents dans le graphe, de sorte que

$$(-1)^3 c_3 \;=\; 2(\text{nombre de triangles}). \qquad \square$$

6. Définitions. Soit $G = (V, E)$ un graphe. Le *degré* d'un sommet $x \in V$ est le nombre d'arêtes de la forme $\{x, y\}$ dans E. Le *degré maximum* de G est le maximum $d_{max}(G)$ des degrés des sommets de G. Un graphe G est *régulier* si tous ses sommets ont le même degré, et *régulier de degré k* si de plus ce degré est k.

Le *rayon spectral* de G, noté $\lambda_{max}(G)$, est la plus grande valeur absolue de valeur propre de la matrice d'adjacence de G.

7. Théorème. *Soit $G = (V, E)$ un graphe connexe.*

(i) *Le rayon spectral et le degré maximum satisfont l'inégalité $\lambda_{max}(G) \leq d_{max}(G)$.*

(ii) *Si G est régulier de degré k, alors $\lambda_{max}(G) = k$.*

(iii) *Si G est connexe, alors $\lambda_{max}(G)$ est une valeur propre simple de G.*

Preuve, dans le cas particulier d'un graphe régulier de degré k (donc tel que $\lambda_{max} = k$)

(i) Soit λ une valeur propre de G et $f \in C(V)$ une fonction propre correspondante. Soit $x_0 \in V$ un sommet tel que $|f(x_o)| \geq |f(x)|$ pour tout $x \in V$; quitte à remplacer f par $-f$, on peut supposer $f(x_0) > 0$. Alors

$$|\lambda| f(x_0) \;=\; |(Af)(x_0)| \;=\; \Big| \sum_{y \sim x} f(y) \Big| \;\leq\; \sum_{y \sim x} |f(y)| \;\leq\; k f(x_0)$$

car la somme $\sum_{y \sim x}$ contient k termes, et par suite $|\lambda| \leq k$.

(ii) La fonction constante de valeur 1 est une fonction propre de A de valeur propre k (que le graphe G soit connexe ou non).

(iii) Il s'agit de montrer que, si G est connexe, toute fonction propre de valeur propre k est constante. Soit à nouveau $x_0 \in V$ un point où une telle fonction f est maximum ; on peut de nouveau supposer $f(x_0) > 0$. Comme

$$k f(x_0) \;=\; \sum_{y \sim x} f(y)$$

on a nécessairement $f(y) = f(x_0)$ pour tout $y \in V$ entrant dans la somme, c'est-à-dire tel que $\{x, y\} \in E$. On montre ainsi de proche en proche que $f(z) = f(x_0)$ pour tout $z \in V$. □

REMARQUE. Il est facile de vérifier que, si G est un graphe k-régulier *non connexe,* alors k est une valeur propre *multiple* de G.

PREUVE DANS LE CAS GÉNÉRAL. Cela résulte d'un *théorème de Perron-Frobenius* qu'on trouve par exemple au chapitre XIII d'un livre de F.R. Gantmacher, *The theory of matrices, Volume two*, Chelsea 1959. □

8. Exercice. On considère les deux matrices

$$\begin{pmatrix} 0&1&0&0&0&0\\ 1&0&1&1&0&0\\ 0&1&0&1&1&0\\ 0&1&1&0&1&0\\ 0&0&1&1&0&1\\ 0&0&0&0&1&0 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 0&1&0&1&0&0\\ 1&0&0&1&0&0\\ 0&0&0&1&0&0\\ 1&1&1&0&1&1\\ 0&0&0&1&0&1\\ 0&0&0&1&1&0 \end{pmatrix}.$$

Dessiner les graphes correspondants, et vérifier qu'ils ne sont pas isomorphes. (Cela fait partie de l'exercice de formuler une définition raisonnable de « graphes isomorphes » .)

Vérifier ensuite que ces deux graphes ont le même polynôme caractéristique, qui est

$$T^6 - 7T^4 - 4T^3 + 7T^2 + 4T - 1,$$

et donc aussi même spectre.

9. Définition. Un graphe $G = (V, E)$ est *biparti* s'il existe une partition de V en deux sous-ensembles V_I, V_{II} disjoints non vides (penser à une coloration des sommets en deux couleurs) telle que toute arête $e \in E$ ait une extrémité dans V_I et l'autre dans V_{II}.

EXEMPLES DE GRAPHES BIPARTIS : un segment, un carré, les sommets et les arêtes d'un cube ; plus généralement, tout graphe dans lequel tous les circuits sont de longueurs paires (c'est une proposition facile à montrer).

EXEMPLES DE GRAPHES NON BIPARTIS : un triangle et plus généralement un graphe complet à $n \geq 3$ sommets, les sommets et les arêtes d'un octaèdre, un pentagone ; plus généralement, tout graphe contenant un circuit de longueur impaire.

10. THÉORÈME. *Soit G un graphe connexe.*

(i) *Si G est biparti, pour toute valeur propre λ de G, le nombre $-\lambda$ est aussi valeur propre ; en particulier, $-\lambda_{max}$ est valeur propre de G.*

(ii) *Si $-\lambda_{max}(G)$ est une valeur propre de G, alors G est biparti.*

PREUVE DE (i). Soit $f \in C(V)$, $f \neq 0$, une fonction propre de valeur propre λ :

$$\sum_{y \sim x} f(y) \;=\; \lambda f(x) \quad \text{pour tout} \quad x \in V.$$

Soit $V = V_I \coprod V_{II}$ comme dans la définition 9, et soit $g \in C(V)$ la fonction définie par $g(x) = f(x)$ pour $x \in V_I$, $g(x) = -f(x)$ pour $x \in V_{II}$. On vérifie que $Ag = -\lambda g$. [Ceci n'utilise pas l'hypothèse de connexité.]

Preuve de (ii), dans le cas particulier où G est régulier de degré k, et où par suite $\lambda_{max}(G) = k$. Soit $f : V \longrightarrow \mathbb{R}$ une fonction non nulle telle que $Af = -kf$. On choisit un sommet $x \in V$ tel que $|f(x)| \geq |f(y)|$ pour tout $y \in V$; quitte à remplacer f par $(1/f(x))f$, on peut supposer que $f(x) = 1$. Si $y_1, \ldots, y_k$ sont les sommets voisins de x, on a

$$(Af)(x) \;=\; -kf(x) \;=\; -k \;=\; \sum_{j=1}^{k} f(y_j)$$

$$|\sum_{j=1}^{k} f(y_j)| \;\leq\; \sum_{j=1}^{k} |f(y_j)| \;\leq\; k$$

et par suite $f(y_1) = \ldots = f(y_k) = -1$. On montre de proche en proche que, pour tout sommet $z \in V$, on a ou bien $f(z) = 1$ et $f(v) = -1$ pour tout voisin v de z, ou bien $f(z) = -1$ et $f(v) = 1$ pour tout voisin v de z. Le graphe G est donc biparti, avec sous-ensembles V_I et V_{II} de V respectivement définis par les équations $f(z) = 1$ et $f(z) = -1$. □

La proposition 5 et les théorèmes 7 et 10 montrent qu'il y a des liens étroits entre le spectre d'un graphe et ses propriétés géométriques. Le résultat de l'exercice 8 montre que le spectre d'un graphe ne caractérise *pas* complètement le graphe lui-même. Dans la fin de ce chapitre, nous allons présenter un autre de ces liens, découvert plus récemment et qui est encore l'objet de recherches fondamentales. *La matière qui suit ne fait pas partie du programme d'examen.*

11. Définition. Soit $G = (V, E)$ un graphe fini connexe. Pour tout sous-ensemble U de V, on définit le *bord* ∂U de U comme le sous-ensemble de E formé des arêtes de la forme $\{x, y\}$ avec $x \in U$ et $y \notin U$.

La *constante isopérimétrique* de G est le nombre

$$h(G) \;=\; \min\left\{ \frac{|\partial U|}{|U|} \;:\; U \subset V\,,\, 0 < |U| \leq \frac{|V|}{2} \right\}$$

où $|\partial U|$, $|U|$ et $|V|$ désignent respectivement les nombres d'éléments de ∂U, U et V.

Si G est vu comme un circuit de transmission, la grandeur de $h(G)$ mesure la qualité de G à transmettre de l'information.

Si $G = C_n$ est le circuit à $n \geq 4$ sommets, on vérifie que $h(C_n) = 2/\lfloor n/2 \rfloor \approx 4/n$. Exercice : évaluer $h(G)$ lorsque $G = K_n$ est le graphe complet à n sommets.

12. Problème fondamental. Construire *explicitement* des suites infinies

$$(G_m = (V_m, E_m))_{m \geq 1}$$

de graphes finis connexes, tous réguliers d'un même degré k, avec $\lim_{m\to\infty} |V_m| = \infty$ et $\liminf_{m\to\infty} h(G_m)$ strictement positif.

13. Notation. Il se trouve qu'il n'est pas facile de contrôler directement la constante $h(G)$ d'un graphe G ; on préfère introduire le nombre $\mu_1(G)$ défini ci-dessous, et tirer profit du théorème 14.

Soit $G = (V, E)$ un graphe fini connexe régulier de degré k ; on note $\mu_1(G)$ la plus grande des valeurs propres de G qui sont strictement inférieure à k. Par exemple, si G est un triangle, $\mu_1(G) = -1$. (La plupart du temps, on a néanmoins $\mu_1(G) > 0$.)

14. Théorème. *Soit $G = (V, E)$ un graphe fini connexe et régulier de degré k. Alors*

$$\frac{k - \mu_1(G)}{2} \leq h(G) \leq \sqrt{2k(k - \mu_1(G))}.$$

Preuve. Voir par exemple le chapitre 3 dans le livre de Y. Colin de Verdière, *Spectres de graphes,* Cours spécialisé N^o 4, Soc. Math. France, 1998. □

Le résultat suivant, dû à Allon et Boppana, date du milieu des années 1980.

15. Théorème. *Etant donné un entier $k \geq 3$ et une famille $(G_m = (V_m, E_m))_{m \geq 1}$ de graphes finis connexes réguliers de degré k tels que $\lim_{m \to \infty} |V_m| = \infty$, on a*

$$\liminf_{m \to \infty} \mu_1(G_m) \geq 2\sqrt{k-1}.$$

La terminologie suivante est motivée par des travaux importants de la première moitié du siècle en arithmétique.

16. Définition. Un graphe fini connexe $G = (V, E)$ régulier de degré k est un *graphe de Ramanujan* si toute valeur propre μ de G distincte de k et de $-k$ satisfait

$$|\mu| \leq 2\sqrt{k-1}.$$

Il résulte du théorème 15 que, pour un graphe de Ramanujan G de degré k, la constante isopérimétrique satisfait l'inégalité $h(G) \geq \frac{1}{2}\left(k - 2\sqrt{k-1}\right)$.

17. Reformulation du problème fondamental. Étant donné un entier $k \geq 3$, construire *explicitement* des suites infinies de graphes de Ramanujan.

A la suite de nombreux travaux, on connaît de telles suites pour des degrés de la forme $k = p^a + 1$ avec p premier et a entier (de sorte que $k - 1$ est l'ordre d'un corps fini).

18. Problème ouvert. Existe-t-il des suites infinies de graphes de Ramanujan pour d'autres degrés, par exemple pour le degré $k = 7$?

Les graphes de Ramanujan ont été l'objet de nombreuses recherches ces dernières années, à Genève et à Neuchâtel notamment. Voir par exemple

A. Lubotzky et T. Smirnov-Nagnibeda, *Not every uniform tree covers Ramanujan graphs,* Journal of Combinatorial Theory B (1999).

A. Valette, *Graphes de Ramanujan et applications*, séminaire Bourbaki **829**, mars 1997.

G. Davidoff, P. Sarnak et A. Valette, *Elementary number theory, group theory, and Ramanujan graphs*, London math. Soc. Student Texts **55**, Cambridge University Press (2003).

La théorie des graphes est un sujet de recherche très actif. Elle donne lieu chaque année à un nombre considérable d'articles et de livres, parmi lesquels il n'est pas facile de repérer les résultats les plus importants et les arguments les plus élégants. J'aimerais terminer ces notes en recommandant la lecture d'un livre récent M. Aigner et G.M. Ziegler, *Proofs from THE BOOK,* Springer 1988 dont la cinquième et dernière partie traite de théorie des graphes (après : théorie des nombres, géométrie, analyse, combinatoire). Le livre se réfère à un personnage unique des mathématiques du XXème siècle, Paul Erdös (1913-1997). La dernière liste de ses publications que j'ai vue comptait 1542 entrées ! Il aimait à parler du LIVRE, dans lequel Dieu conserve les preuves parfaites des théorèmes mathématiques (il n'y a pas de place durable pour les mathématiques laides). Erdös disait aussi qu'il n'est pas nécessaire de croire en Dieu, mais qu'un mathématicien devrait croire en le LIVRE. Paul Erdös s'était enthousiasmé pour tenter une très modeste approximation du LIVRE, et en avait suggéré de nombreuses pages. La publication de Aigner et Ziegler est, pour l'instant au moins, l'achèvement de ce projet.