

ARITHMÉTIQUE

PIERRE DE LA HARPE

Le début de ce chapitre a pour but de justifier des résultats avec la majorité desquels le lecteur est sensé être déjà *familier*.

1. DIVISION EUCLIDIENNE ET PGCD

Dans ce cours, $\mathbb{N} = \{0, 1, 2, \dots\}$ désigne l'ensemble des *entiers naturels* et

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

celui des *entiers rationnels*. Ces ensembles sont donnés avec l'*addition* ($3 + 5 = 8$), la *multiplication* ($3 \cdot 5 = 15$) 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 : $56 = 8 \cdot 7 = 8 \times 7 \neq 87 = 80 + 7$.

(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 $\{1, 2, 3, \dots\}$, sans le zéro.

1. Théorème : division euclidienne. Soient $n, d \in \mathbb{Z}$ avec $d > 0$. Il existe deux entiers $q, r \in \mathbb{Z}$ tels que

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

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 $r' \geq 0$ et $n - (q + 1)d = r' \in S$, contrairement à la définition de r .

Unicité. Supposons qu'on a

$$n = q_1d + r_1 = q_2d + r_2 \quad \text{et} \quad 0 \leq r_1, r_2 < d.$$

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 $r_1 = r_2$. \square

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

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

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

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

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

Exemples. On a $\text{pgcd}(8, 12) = 4$. Les trois entiers 6, 10, 15 sont premiers entre eux.

Remarques. Avec les notations ci-dessus, si $n \geq 3$, on a

$$\text{pgcd}(a_1, \dots, a_n) = \text{pgcd}(\text{pgcd}(a_1, \dots, a_{n-1}), a_n).$$

Par ailleurs, si $\epsilon_1, \dots, \epsilon_n \in \{1, -1\}$, on a $\text{pgcd}(\epsilon_1 a_1, \dots, \epsilon_n a_n) = \text{pgcd}(a_1, \dots, a_n)$.

5. Lemme. Soient $n, d \in \mathbb{Z}$ avec $d \neq 0$ et soient q, r comme au théorème 1 : $n = qd + r$ et $0 \leq r < d$. On a

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

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. \square

6. Proposition : algorithme d'Euclide pour le calcul du pgcd de deux entiers d_1, d_2 tels que $d_1 \geq d_2 > 0$.

Première étape : par division euclidienne, on obtient $d_1 = a_1 d_2 + d_3$ avec $a_1 \in \mathbb{Z}$ et $0 \leq d_3 < d_2$. Si $d_3 = 0$ alors $d_2 = \text{pgcd}(d_1, d_2)$. Si $d_3 > 0$ on passe à l'étape suivante.

Deuxième étape : par division euclidienne, on obtient $d_2 = a_2 d_3 + d_4$ avec $a_2 \in \mathbb{Z}$ et $0 \leq d_4 < d_3$. Si $d_4 = 0$ alors $d_3 = \text{pgcd}(d_1, d_2)$. Si $d_4 > 0$, on recommence ...

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

Si k désigne le plus grand entier tel que $d_k > 0$, alors $d_k = \text{pgcd}(d_1, d_2)$.

Preuve : c'est une conséquence immédiate du théorème 1 et du lemme précédent. \square

7. Le plus grand commun diviseur comme combinaison entière. L'algorithme d'Euclide fournit également deux entiers x_1, x_2 tels que

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

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

$$d_1 = a_1 d_2 + d_3 \quad \text{ou} \quad 22 = 3 \cdot 6 + 4 \quad (a_1 = 3, \quad d_3 = 4)$$

$$d_2 = a_2 d_3 + d_4 \quad \text{ou} \quad 6 = 1 \cdot 4 + 2 \quad (a_2 = 1, \quad d_4 = 2)$$

$$d_3 = a_3 d_4 + d_5 \quad \text{ou} \quad 4 = 2 \cdot 2 + 0 \quad (a_3 = 2, \quad d_5 = 0)$$

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

$$\begin{aligned} \text{pgcd}(22, 6) = d_4 &= d_2 - a_2 d_3 = d_2 - a_2(d_1 - a_1 d_2) = -a_2 d_1 + (1 + a_1 a_2) d_2 \\ &= -22 + 4 \times 6. \end{aligned}$$

\square

8. Corollaire. Soient $a, b \in \mathbb{Z}$, non tous les deux nuls, et $d = \text{pgcd}(a, b)$. Soit $k \in \mathbb{Z}$. L'équation

$$ax + by = k$$

a une solution $x, y \in \mathbb{Z}$ si et seulement si $k \in d\mathbb{Z}$.

En particulier, il existe $x, y \in \mathbb{Z}$ tels que $ax + by = d$. [Voir aussi le corollaire 11.]

De plus, tout diviseur commun de a et b divise d .

Plus généralement, il résulte du corollaire 8 et d'une des remarques du numéro 4 que, pour $a_1, \dots, a_n \in \mathbb{Z}$ non tous nuls et $d = \text{pgcd}(a_1, \dots, a_n)$, l'équation

$$a_1x_1 + \dots + a_nx_n = k$$

possède une solution $x_2, \dots, x_n \in \mathbb{Z}$ si et seulement si $k \in d\mathbb{Z}$. On obtient en particulier l'énoncé suivant.

9. Théorème (Bézout). Des entiers non tous nuls a_1, \dots, a_n sont premiers entre eux si et seulement s'il existe des entiers x_1, \dots, x_n tels que

$$a_1x_1 + \dots + a_nx_n = 1.$$

Remarque. 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.

10. Proposition (Euclide). Soient $a, b \in \mathbb{Z}$ deux entiers premiers entre eux, et $c \in \mathbb{Z}$.

Si $a \mid bc$, alors $a \mid c$.

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

Si $a \mid bc$, alors $a \mid (acx + bcy)$, c'est-à-dire $a \mid c$. \square

Exemple : $7 \mid 4200 \implies 7 \mid 42$, car $\text{pgcd}(7, 100) = 1$.

11. Corollaire. Soient $a, b \in \mathbb{Z} \setminus \{0\}$; on pose $d = \text{pgcd}(a, b)$, $a_1 = \frac{a}{d}$ et $b_1 = \frac{b}{d}$. Soient de plus $x, y \in \mathbb{Z}$, et $c = ax + by \in \mathbb{Z}$.

Alors toute combinaison linéaire entière de a et b égale à c est de la forme

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

avec $k \in \mathbb{Z}$.

Preuve. Soient $m, n \in \mathbb{Z}$ tels que $c = a(x + m) + b(y - n)$. On a $ma = nb$, donc aussi $ma_1 = nb_1$ en divisant par d . Vu que a_1, b_1 sont premiers entre eux¹, il résulte de la proposition 10 que $l = n/a_1$ et $k = m/b_1$ sont des entiers. En divisant chaque terme de l'égalité $ma_1 = nb_1$ par a_1b_1 , on obtient $k = l$. Par suite $m = kb_1$ et $n = la_1 = ka_1$. \square

¹A justifier !

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 $x, y \in \mathbb{Z}$, on a $ax + by \in I$.

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 $d\mathbb{Z}$.)

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. \square

14. Proposition. *Soient a_1, \dots, a_n des entiers rationnels non tous nuls. On pose*

$$d = \text{pgcd}(a_1, \dots, a_n) \quad \text{et}$$

$$I = \{k \in \mathbb{Z} \mid \text{il existe } x_1, \dots, x_n \in \mathbb{Z} \text{ tels que } k = x_1 a_1 + \dots + x_n a_n\}$$

Alors I est un idéal de \mathbb{Z} et

$$I = d\mathbb{Z}.$$

Preuve. On vérifie immédiatement sur la définition de "idéal" que I est un idéal de \mathbb{Z} . Il résulte du corollaire 8 que $d \in I$, et de la proposition 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 $d = e$. \square

EXERCICES DU N° 1

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

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

(17) On rappelle que les *nombre 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 $m < n$?

(18) 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 $x6 + y10 + z15 = 1$.

Soient $a, b, c \in \mathbb{Z}$ des entiers tels que $\text{pgcd}(a, b) = \text{pgcd}(a, c) = 1$. Montrer que $\text{pgcd}(a, b, c) = 1$.

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

(20) Combien y a-t-il de solutions de l'équation

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

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

2. NOMBRES PREMIERS

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 $\text{pgcd}(p_1, p_2) = 1$.

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 premiers par l'hypothèse de récurrence, il en est de même de n . \square

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 $\text{pgcd}(p, b) = 1$ ou bien $\text{pgcd}(p, b) = p$. Dans le premier cas, p divise a en vertu de la proposition 1.10 ; dans le second cas, p divise b . \square

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

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

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 $j \in \{1, \dots, l\}$ 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. \square

4. Remarques. (a) 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 4.15.

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

(c) 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 cryptographie. D'après le journal "Le Monde" daté du 8 novembre 1999, les limites des possibilités actuelles ont évolué de nombres de 140 chiffres (en écriture décimale), vers février 1999, à des nombres de 150 chiffres, avec une réussite le 22 août 2000 !

5. Théorème (Euclide). *Il existe une infinité de nombres premiers.*

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

$$n = 1 + \prod_{1 \leq i \leq k} p_i.$$

En vertu du 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. \square

Autres preuves : voir l'exercice 10 et le numéro 6.

Remarque. Si p_1, p_2, \dots désigne la suite croissante des nombres premiers, le nombre $1 + \prod_{i=1}^k p_i$ est premier pour $k \in \{1, 2, 3, 4, 5\}$ et pour précisément cinq autres valeurs de k telles que $k \leq 10^5$. En particulier le nombre

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

n'est pas premier.

6. Une preuve d'Euler. Il existe de nombreuses autres preuves de l'infinité des nombres premiers. Voir par exemple "Proofs from THE BOOK"², pages 3 à 6. Ci-dessous, nous

²M. Aigner et G.M. Ziegler, *Proofs from THE BOOK*, Springer 1988,

esquissons très brièvement la *preuve analytique* d'Euler ; ce sera la première et presque la seule (voir néanmoins le complément 15) allusion de ce cours aux rapports très riches entre l'analyse classique et l'arithmétique.

Sur la preuve d'Euler. Si \mathbb{P} désigne l'ensemble des nombres premiers, nous allons esquisser un argument montrant que le produit sur \mathbb{P} des facteurs $(1 - \frac{1}{p})^{-1}$ diverge, au sens où $\lim_{x \rightarrow \infty} \prod_{p \leq x} (1 - \frac{1}{p})^{-1} = \infty$ (avec $\prod_{p \leq x}$ désignant le produit sur tous les nombres premiers $p \in \mathbb{P}$ tels que $p \leq x$).

En effet, pour tout $p \in \mathbb{P}$, on a

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

(somme d'une série géométrique). On en déduit que

$$\prod_{p \in \mathbb{P}} \left(1 - \frac{1}{p}\right)^{-1} = \prod_{p \in \mathbb{P}} \sum_{k=0}^{\infty} \frac{1}{p^k} \stackrel{*}{=} \sum_{n=1}^{\infty} \frac{1}{n}$$

où $\stackrel{*}{=}$ résulte du théorème fondamental de l'arithmétique. C'est un exercice *difficile* que de justifier soigneusement cette égalité ! voici de quoi l'éclairer :

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

où les ... de la première ligne indiquent les termes du produit correspondant aux premiers plus grand ou égaux à 7, et où les ... 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 on sait que la série harmonique $\sum_{n=1}^{\infty} \frac{1}{n}$ 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 $\prod_{p \in \mathbb{P}} \left(1 - \frac{1}{p}\right)^{-1}$ diverge aussi, et par suite \mathbb{P} est un ensemble infini. \square

[En exploitant un peu mieux la même idée, on montre facilement que, pour la fonction π introduite ci-dessous, on a $\ln x \leq \pi(x) + 1$; voir "Proofs from THE BOOK", cité ci-dessus.]

EXERCICES DU N° 2

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

Pour tout entier $n \geq 0$, montrer qu'on a l'alternative suivante :

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

(8) On considère un entier $n \geq 1$, 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) Montrer qu'il existe une infinité de nombres premiers de la forme $4k + 3$.

[Indication. Pour tout premier p de la forme $4k + 3$, considérer le produit n de tous les nombres premiers de la même forme inférieurs ou égaux à p , et la décomposition de $4n - 1$ en nombres premiers.]

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

(10) 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) Dédurre de (ii) une autre preuve de l'infinitude des nombres premiers.

Remarque. Le lemme 5.11 ci-dessous montre que tout nombre premier impair divisant 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 $4k + 1$.

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

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

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

suisant : le n -gone régulier est constructible à la règle et au compas si et seulement si n est de la forme

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

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

Il existe une construction pour $n = 257$, mais aucun des courageux chercheurs qui a entrepris de trouver une construction du 65537-gone régulier ne semble avoir abouti. 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 des polygones réguliers à mn côtés. [Indication : utiliser le théorème de Bézout.]

(11) 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 $6^3 + 1$, $6^5 + 1$ et $6^6 + 1$ sont composés.

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

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

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

(13) 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.)

On ignore s'il existe une infinité de nombres parfaits, mais on conjecture que c'est le cas. On ignore s'il existe³ 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).

(14) Contrairement à certaines idées reçues, il existe bel et bien des "formules" qui fournissent les nombres premiers (bien qu'aucune d'entre elles ne se soit jamais révélée d'un très grand intérêt). Voir le numéro 4.21.

³S'il existe un nombre parfait impair n , on sait qu'il doit être "grand", et plus précisément que $n > 10^{200}$.

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

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

$$\begin{aligned} \lim_{x \rightarrow \infty} \pi(x) &= \infty && \text{(Euclide),} \\ \lim_{x \rightarrow \infty} \frac{\pi(x)}{x} &= 0 && \text{(Legendre, 1808),} \\ \lim_{x \rightarrow \infty} \frac{\pi(x)}{x/\ln x} &= 1 && \text{(TNP, Hadamard et de la Vallée Poussin, 1896)} \end{aligned}$$

(TNP = théorème des nombres premiers). A la fin du XIX^{ème} 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. Erdős 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 sait⁴ par ailleurs que $\lim_{x \rightarrow \infty} \frac{Li(x)}{x/\ln x} = 1$.

Les propriétés de la fonction d'une variable réelle $\pi(x)$ sont très étroitement liées à celles de la "fonction zêta 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" $\{-2, -4, -6, \dots\}$ et une infinité de zéros sur la "droite critique" $s + i\mathbb{R}$.

⁴ Preuve. Posons $C = \frac{2}{\ln 2}$, de sorte que

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

Il suffit donc de montrer que

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

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

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

et

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

La conclusion en résulte.

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

$$\pi(x) = Li(x) + O(\sqrt{x} \ln x)$$

et aurait des conséquences importantes en théorie des nombres.

(16) Euler (1707–1783) a montré que la série $\sum_{p \in \mathbb{P}} \frac{1}{p}$ diverge.

Dirichlet a montré en 1837 que, pour toute paire (a, b) d'entiers premiers entre eux, la série $\sum \frac{1}{p}$ diverge encore lorsque la somme porte sur tous les nombres premiers de la forme $ka + b$.

(17) 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

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

n'est premier.

(18) 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 Bertrand", 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 $(n + 1)^3$.

(19) 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.]

(20) 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. Ribenboim⁵ mentionne une vérification de la conjecture pour tout entier $n \leq 10^8$.

(21) 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”.

(22) 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 4.21), 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 :

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

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

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

Pour la preuve en question de $\pi(x) < 1,7 \frac{x}{\ln x}$, on vérifie⁶ d’abord l’inégalité “à la main” pour $x < 1200$, puis on procède par récurrence à l’aide de l’inégalité (*).]

(23) 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

⁵ *The book of prime number records*, second edition, Springer, 1989

⁶ J’avoue ne pas avoir effectué cette vérification.

ailleurs de nombreuses *applications* de cette théorie, notamment à la cryptographie (transmission de messages secrets, sécurité de cartes bancaires, etc.).

Pour une introduction à la cryptographie, voir :

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

Je tiens aussi à signaler le recueil d'articles suivant :

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

On y raconte par exemple comment une équipe de mathématiciens anglais menés par Alan Turing a percé un important code allemand pendant la seconde guerre mondiale, ou comment l'algorithme RSA⁷, basé sur l'arithmétique élémentaire, permet de transmettre publiquement des messages secrets (paragraphe 6 ci-dessous).

3. CONGRUENCES

Ce paragraphe a pour but d'exposer la notion de *relation d'équivalence*, et l'exemple important en arithmétique de *congruence modulo un entier*.

1. Définitions. Une *relation d'équivalence* sur un ensemble E est une partie R du 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 $(x, y) \in R$:

$$\begin{aligned} x &\sim x && \text{(symétrie),} \\ \text{si } x &\sim y && \text{alors } y \sim x && \text{(réflexivité),} \\ \text{si } x &\sim y && \text{et } y \sim z && \text{alors } x \sim z && \text{(transitivité).} \end{aligned}$$

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 $\begin{cases} E &\longrightarrow E/R \\ x &\longmapsto C_x \end{cases}$.

2. 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 de la droite réelle, 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.

(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

⁷R.L. Rivest, A. Shamir et L.M. Adleman, *A method for obtaining digital signatures and public key signatures*, Communications of the ACM **21**, No 2 (1978).

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 $\mathbb{S}^2 \rightarrow \mathbb{S}^2/R$ 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 $\mathbb{P}_{\mathbb{K}}^n$ est *l'espace projectif de dimension n sur le corps \mathbb{K}* . En particulier, $\mathbb{P}_{\mathbb{K}}^0$ est réduit à un point, $\mathbb{P}_{\mathbb{K}}^1$ est la *droite projective sur \mathbb{K}* , et $\mathbb{P}_{\mathbb{K}}^2$ le *plan projectif sur \mathbb{K}* .

(vi) Sur le plan euclidien $E \approx \mathbb{R}^2$, la relation R pour deux points d'être à distance de 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. Exemple fondamental pour l'arithmétique. Pour tout entier rationnel non nul d , on définit pour $x, y \in \mathbb{Z}$ la relation “être congru modulo d ”, ou “de congruence modulo d ”, par

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

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

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

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 $0, 1, \dots, d-1$. 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 $x \equiv 1 \pmod{2}$.

4. 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 ,

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

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 .

5. Exemple fondamental. Soit d un entier rationnel non nul, comme à l'exemple 3.

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

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

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

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

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

6. 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

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

Pour la multiplication, on a par exemple

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

(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

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

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

(iii) Pour un entier écrit en forme décimale $x = a_k 10^k + a_{k-1} 10^{k-1} + \dots + a_1 10 + a_0$, avec $a_k, \dots, a_0 \in \{0, 1, \dots, 9\}$, la classe de x modulo 9 est égale à celle de $a_k + a_{k-1} + \dots + a_0$.

Application : la preuve par neuf. Appliquons par exemple cette preuve par neuf au produit $239 \times 241 = 57599$; on trouve bien $5 \times 7 \equiv 8 \pmod{9}$. Cette "preuve" permet de déceler certaines erreurs, par exemple $239 \times 241 \neq 56599$, mais bien sûr pas toutes ($239 \times 241 \neq 57509$ 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" et une "preuve par cinq". (Voir aussi l'exercice 4.12.)

EXERCICES DU N° 3

(7) 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 d'entiers.

[Un théorème d'Euler 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".]

(8) Pour $a \in \mathbb{Z}$ et $r \in \{0, 1, \dots, 7\}$ tels que $a^2 \equiv r \pmod{8}$, montrer que $r \in \{0, 1, 4\}$. En déduire que, pour tout entier de la forme $n = a^2 + b^2 + c^2$, avec $a, b, c \in \mathbb{Z}$, on a $n \not\equiv 7 \pmod{8}$.

Faire la liste de tous les nombres premiers p tels que $p \leq 40$ et $p \not\equiv 7 \pmod{8}$, et vérifier que chacun d'eux est une somme de trois carrés.

[Un théorème de Legendre montre qu'un nombre entier positif est une somme de trois carrés si et seulement s'il n'est *pas* de la forme $4^a(8k+7)$, avec a et k entiers positifs. Un théorème de Lagrange montre que tout entier positif est une somme de quatre carrés.
Exercice : vérifier ces énoncés pour n "petit".]

(9) Montrer les congruences suivantes :

$$2^{2n} - 1 \equiv 0 \pmod{3}$$

$$2^{3n} - 1 \equiv 0 \pmod{7}$$

$$2^{4n} - 1 \equiv 0 \pmod{15}$$

$$n^3 \equiv -1, 0 \text{ ou } 1 \pmod{9}$$

pour tout $n \geq 0$.

4. GROUPES, ANNEAUX, CORPS (AIDE-MÉMOIRE)

Ce paragraphe est essentiellement terminologique. Le résultat important apparaît au théorème 15.

Auparavant, on définit successivement les notions de *groupe*, *sous-groupe*, *homomorphisme*, *anneau* et *corps*. On adopte à chaque coup le programme m-i-n-i-m-a-l définition+exemples+exercices. Le lecteur le complétera avantageusement avec des exemples du cours de Géométrie I ou grâce à l'un des nombreux livres standard, par exemple celui de S. Lang, *Undergraduate algebra*, UTM, Springer, 1987.

1. Définition. Un *groupe* est un ensemble G muni d'une opération $\begin{cases} G \times G \longrightarrow G \\ (a, b) \longmapsto ab \end{cases}$ satisfaisant aux conditions usuelles :

$$\text{associativité} \quad (ab)c = a(bc) \quad \forall a, b, c \in G,$$

existence d'un élément neutre $e \in G$ tel que $ea = ae = a \forall a \in G$,
 existence pour tout $a \in G$ d'un élément appelé "inverse" et noté a^{-1} ,
 tel que $aa^{-1} = a^{-1}a = e$.

[Exercice : tout élément a un *unique* inverse.]

Dans ce cours l'opération est le plus souvent notée multiplicativement : on écrit ab le produit de deux éléments $a, b \in G$. Lorsque le groupe G est *abélien* ou *commutatif*, c'est-à-dire lorsque $ab = ba \forall a, b \in G$, on utilise parfois la notation additive : $a + b$ au lieu de ab ; la commutativité s'écrit alors : $a + b = b + a \forall a, b \in G$.

L'élément neutre d'un groupe G se note souvent 1 au lieu de e , ou 1_G ou e_G s'il convient de préciser ; ou encore 0 en notation additive.

L'ordre d'un groupe fini est le nombre de ses éléments.

2. Exemples de groupes. \mathbb{Z} , \mathbb{Q} , \mathbb{R} , \mathbb{C} , un espace vectoriel, pour l'addition usuelle.

$\{1, -1\}$, \mathbb{Q}^* , \mathbb{R}_+^* , \mathbb{R}^* , \mathbb{C}^* , $\{z \in \mathbb{C} \mid |z| = 1\}$, pour la multiplication usuelle. Observer que ces groupes *abéliens* sont notés *multiplicativement* !

Le groupe $GL(n, \mathbb{R})$ des matrices n -fois- n à coefficients réels et à déterminants non nuls, pour la multiplication usuelle des matrices.

Le groupe de toutes les applications bijectives d'un ensemble dans lui-même, pour la composition. Lorsque l'ensemble a un nombre fini n d'éléments, ce groupe est le *groupe symétrique* souvent noté $Sym(n)$, et ses éléments sont appelés des *permutations* (de l'ensemble à n éléments).

3. Exercices. (a) Vérifier que, pour tout entier $d \geq 1$, l'ensemble

$$\mu(d) = \{z \in \mathbb{C} \mid z^d = 1\} = \left\{ z \in \mathbb{C} \mid \text{il existe } j \in \mathbb{Z} \text{ tel que } z = \exp\left(\frac{i2\pi}{d}j\right) \right\}$$

des racines d -ièmes de l'unité est un groupe abélien d'ordre d .

(b) Soit $Sym(5)$ le groupe des permutations de l'ensemble $\{1, 2, 3, 4, 5\}$.

(i) Calculer l'ordre de ce groupe.

(ii) Soit $\sigma \in Sym(5)$ la permutation définie par $\sigma(1) = 2$, $\sigma(2) = 1$, $\sigma(3) = 4$, $\sigma(4) = 5$ et $\sigma(5) = 3$. Quel est le plus petit entier $k \geq 1$ tel que σ^k soit la transformation identique ?

(iii)[#] Trouver tous les éléments $\tau \in Sym(5)$ tels que $\tau\sigma = \sigma\tau$.

(c) Quel est l'ordre du groupe symétrique $Sym(n)$?

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

Notation : " $H < G$ " pour " H est un sous-groupe de G ".

5. Exemples de sous-groupes. $d\mathbb{Z} < \mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}$, $\{1, -1\} < \mathbb{R}^*$,
 $\mathbb{R}_+^* < \mathbb{R}^* < \mathbb{C}^*$, $\mu(k) < \{z \in \mathbb{C} \mid |z| = 1\} < \mathbb{C}^*$.

$Sym(n) < Sym(n+1)$ (il y a plusieurs inclusions possibles ; préciser !).

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

Le sous-groupe $SL(n, \mathbb{R})$ de $GL(n, \mathbb{R})$ formé des matrices de déterminant 1 ; le sous-groupe de $GL(n, \mathbb{R})$ formé des matrices orthogonales ; celui des matrices diagonales.

Si G est un groupe, pour tout $g \in G$ 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 $G = \mathbb{C}^*$.)

Tout groupe G a deux sous-groupes "évidents" : $\{1\} < G$ et $G < G$.

6. Exercices. (a) Décrire en quelques mots et sans symbole mathématique (mots qui pourraient être transmis au téléphone) quelques-uns des groupes vus au cours de Géométrie I. Dans chaque cas, préciser si le groupe est fini ou infini, commutatif ou non.

(b) Montrer qu'il existe pour tout $n \geq 1$ un sous-groupe G de $GL(n, \mathbb{R})$ tel que les inclusions

$$SL(n, \mathbb{R}) \not\subseteq G \not\subseteq GL(n, \mathbb{R})$$

soient strictes.

7. Définition. Un *homomorphisme* d'un groupe G dans un groupe G' est une application $\phi : G \rightarrow G'$ telle que $\phi(1) = 1$ et $\phi(ab) = \phi(a)\phi(b)$ pour tous $a, b \in G$. [Exercice : il en résulte que $\phi(a^{-1}) = \phi(a)^{-1}$ pour tout $a \in G$.]

8. Exemples d'homomorphismes : $\left\{ \begin{array}{l} \mathbb{C}^* \rightarrow \mathbb{R}_+^* \\ z \mapsto |z| \end{array} \right\}, \left\{ \begin{array}{l} \mathbb{R} \rightarrow \mathbb{R}_+^* \\ t \mapsto e^t \end{array} \right\}, \left\{ \begin{array}{l} \mathbb{R}^* \rightarrow \{1, -1\} \\ t \mapsto \text{sign}(t) \end{array} \right\}$,

une application linéaire entre espaces vectoriels, l'application $\left\{ \begin{array}{l} \mathbb{Z} \rightarrow G \\ n \mapsto g^n \end{array} \right\}$ où G est un groupe (noté multiplicativement) et g l'un de ses éléments.

9. Exercices. (a) Quand $\left\{ \begin{array}{l} G \rightarrow G \\ g \mapsto g^{-1} \end{array} \right\}$ est-il un homomorphisme d'un groupe G dans

lui-même ? Même question pour $\left\{ \begin{array}{l} G \rightarrow G \\ g \mapsto g^2 \end{array} \right\}$.

(b) Pour un homomorphisme $\phi : G \rightarrow G'$, vérifier que le *noyau* $\{g \in G \mid \phi(g) = 1\}$ de ϕ est un sous-groupe de G et que l'*image* $\{g' \in G' \mid \text{il existe } g \in G \text{ tel que } \phi(g) = g'\}$ est un sous-groupe de G' .

(c) Montrer que l'application $\phi : \mathbb{Z}/d\mathbb{Z} \rightarrow \mu(d)$ définie par $\phi([k]_d) = \exp\left(\frac{2i\pi k}{d}\right)$ est un isomorphisme de groupes, où $\mu(d)$ est comme à l'exercice 3.a. [Un *isomorphisme* est un homomorphisme qui est bijectif.]

10. 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 neutre⁸ 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 $a, b \in A$.

⁸En 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 $C_0(\mathbb{R})$ des fonctions continues $f : \mathbb{R} \rightarrow \mathbb{R}$ telles que $\lim_{|t| \rightarrow \infty} f(t) = 0$ est un "anneau" SANS unité. Notons que $C_0(\mathbb{R})$ se plonge naturellement dans l'anneau (avec unité !) des fonctions continues $f : \mathbb{R} \rightarrow \mathbb{R}$ telles que $\lim_{t \rightarrow \infty} f(t)$ et $\lim_{t \rightarrow -\infty} f(t)$ existent et sont égales.

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

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

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 $1 = 1_A = 1_{A'}$.]

11.a. Exemples d'anneaux : \mathbb{Z} , \mathbb{Q} , \mathbb{R} , \mathbb{C} , l'anneau de tous les endomorphismes linéaires d'un espace vectoriel.

11.b. 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° 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 bien 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 détaillerons pas.

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

(i) Pour tout entier $d \geq 2$, l'application $\mathbb{Z} \rightarrow \mathbb{Z}/d\mathbb{Z}$ 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 (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 $\mathbb{Z}/c\mathbb{Z} \rightarrow \mathbb{Z}/d\mathbb{Z}$ qui applique la classe modulo c d'un entier sur la classe modulo d de cet entier est un homomorphisme d'anneaux, dont le noyau est formé des classes $[0]_c, [d]_c, [2d]_c, \dots, [c-d]_c$. Par exemple, si $d = 2$ et $c = 4$, l'image de $[0]_4$ (respectivement $[1]_4, [2]_4, [3]_4$) est $[0]_2$ (respectivement $[1]_2, [0]_2, [1]_2$).

12. Exercice. *Rappel.* Soit $\phi_9 : \mathbb{Z} \rightarrow \mathbb{Z}/9\mathbb{Z}$ l'homomorphisme de réduction modulo 9. Pour un entier $n = \sum_{j=0}^k a_j(10)^j \in \mathbb{Z}$, avec $a_0, \dots, a_k \in \{0, \dots, 9\}$, on vérifie que $\phi_9(n) = \phi_9\left(\sum_{j=0}^k a_j\right)$ et on en déduit le fonctionnement de la "preuve par 9" (voir le cours).

L'exercice. Soit $\phi_{11} : \mathbb{Z} \rightarrow \mathbb{Z}/(11\mathbb{Z})$ l'homomorphisme de réduction modulo 11.

(i) Montrer que $\phi_{11}(n) = \phi_{11}\left(\sum_{j=0}^k (-1)^j a_j\right)$ pour tout $n = \sum_{j=0}^k a_j(10)^j \in \mathbb{Z}$

avec $a_0, \dots, a_k \in \{0, \dots, 9\}$.

(ii) Formuler une "preuve par 11".

(iii) Démontrer cette "preuve par 11".

(iv) Vérifier *de tête* (donc sans effectuer la division !) que $99 \mid 2411046$.

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

14. 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 $[b]_d = ([a]_d)^{-1} \in \mathbb{Z}/d\mathbb{Z}$. \square

15. 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 $a \in \{1, \dots, d-1\}$, ou encore si et seulement si d est premier, vu le lemme. \square

16. 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 .)

17. Exercices. (a) Ecrire les tables de multiplication des corps \mathbb{F}_2 , \mathbb{F}_3 , \mathbb{F}_5 .

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

(c) 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.]

(d) 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 ?

(e) Énoncer les définitions de *sous-anneau* et *sous-corps*. Vérifier que

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

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

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

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 $x' + y'\sqrt{5} = (x + y\sqrt{5})^{-1}$.

18. 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 $p^{n-1} - 1$ éléments non nuls qui ne sont pas 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 $0, 1, \dots, d-1$, 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 $3 \in \mathbb{Z}$!

19. 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 $x, y \in \{1, \dots, p-1\}$ tels que $xy \equiv 1 \pmod{p}$; alors $x = y$ si et seulement si $x = 1$ ou $x = p-1$.

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

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

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

21. 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, déjà évoquée au numéro 2.14.

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.

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.

5. FONCTION D'EULER, THÉORÈMES DE FERMAT ET EULER.

Le résultat central de ce paragraphe est le théorème 8.

1. Définition. La fonction d'Euler associée 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 4.14), $\varphi(m)$ est l'ordre du groupe abélien multiplicatif

$$\mathcal{U}(\mathbb{Z}/m\mathbb{Z}) = \{[a]_d \in \mathbb{Z}/m\mathbb{Z} \mid [a]_d \text{ est inversible}\}.$$

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 $\varphi(p^a) = p^{a-1}(p-1)$.

2. Produits d'anneaux. Soient A_1, \dots, A_n des anneaux. L'ensemble produit

$$A_1 \times \dots \times A_n$$

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

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

3. Théorème chinois. Soient a_1, \dots, a_n des entiers ≥ 2 deux à deux premiers entre eux. Alors l'application canonique

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

est un isomorphisme d'anneaux.

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

Preuve du lemme (première assertion). Par hypothèse, il existe $x, y \in \mathbb{Z}$ tels que $k = ax = by$. Comme $b \mid x$ par la proposition 1.10, il existe $z \in \mathbb{Z}$ tel que $x = bz$; ainsi $k = abz$.

Les détails de la preuve pour $n \geq 3$ sont laissés au lecteur. \square

Preuve du théorème 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 $a_1 \dots a_n$, il suffit de montrer que ψ est injective. Pour cela, il suffit⁹ de vérifier que le noyau (= l'image inverse de zéro) est réduit à zéro. [Voir le n^o 5 ci-dessous pour une preuve de la surjectivité.]

Soit $k \in \mathbb{Z}$ tel que l'élément $[k]_{a_1 \dots a_n}$ soit dans le noyau de ψ . On a donc $k \equiv 0 \pmod{a_i}$, ou encore $a_i \mid k$, pour tout $i \in \{1, \dots, n\}$. Il résulte du lemme 2 (appliqué $k-1$ fois !) que

⁹ 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).

$a_1 \dots a_n \mid k$, donc que $[k]_{a_1 \dots a_n} = 0$. Le noyau de ψ est donc réduit à zéro, ce qu'il fallait démontrer. \square

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

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

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

Autre preuve de la reformulation. Bien que cet énoncé résulte *immédiatement* du théorème 3, on esquisse ici une *autre* preuve.

On pose $a = a_1 a_2 \dots a_n$ et $b_j = a/a_j$ pour $j \in \{1, \dots, n\}$, 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 (théorème 1.9). Donc $a_j y_j k_j + b_j z_j k_j = k_j$, et par suite $b_j (z_j k_j) \equiv k_j \pmod{a_j}$.] On pose alors

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

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

6. 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

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

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

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

7. 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

$$\begin{aligned}\varphi(m) &= m \prod_{p|m} \left(1 - \frac{1}{p}\right) \\ m &= \sum_{d|m} \varphi(d)\end{aligned}$$

où le produit est pris sur tous les nombres premiers divisant m et la somme sur tous les entiers positifs divisant m .

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 $m = p_1^{a_1} \dots p_k^{a_k}$, avec des premiers distincts p_1, \dots, p_k et des entiers $a_1, \dots, a_k \geq 1$. 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 $p_1^{b_1} \dots p_k^{b_k}$, avec $b_1 \in \{0, \dots, a_1\}, \dots, b_k \in \{0, \dots, a_k\}$. En utilisant (i), on a donc ensuite

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

□

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

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

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

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

Preuve. Vu le lemme 4.14, l'énoncé à montrer est équivalent à

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

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

9. 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

$$g_1 g_2 \dots g_N = (gg_1)(gg_2) \dots (gg_N) = g^N g_1 g_2 \dots g_N$$

et par suite $g^N = 1$. \square

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

- (i) Pour tout $k \in \{1, \dots, p-1\}$, 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 .] \square

Autre preuve du théorème de Lagrange, qui vaut pour TOUT groupe fini (marche à suivre).

Soient 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 $x^{-1}y \in H$.

- (i) Vérifier que R est une relation d'équivalence sur G .
- (ii) Soient $x, y \in G$ et C_x, C_y leurs classes modulo R ; écrire une bijection $C_x \rightarrow C_y$.
- (iii) Lorsque le groupe G est fini, quelle est la relation entre les ordres $|G|$ et $|H|$ de G et H d'une part, et l'ordre de l'ensemble quotient d'autre part ?
- (iv) Dédire de (iii) une preuve du théorème de Lagrange

[Indication pour (iv). Appliquer (iii) au cas où G est un groupe fini et H le groupe engendré par un élément $h \in G$ (c'est-à-dire le sous-groupe des éléments de la forme h^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 $h^d = 1$.] \square

10. Exercices. (a) Vérifier naïvement le théorème d'Euler pour $d \leq 8$.

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

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

(d) 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.

[Indication : calculer leurs nombres d'éléments inversibles.] En déduire que, dans le théorème 3, on ne peut pas remplacer "deux à deux premiers entre eux" par "premiers entre eux".

11. 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, on a $x^2 \equiv -1 \pmod{p}$ et $\frac{p-1}{2} \in \mathbb{N}$; par suite

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

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 $4k + 1$. \square

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

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

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 2.10 sur les nombres de Fermat.]

Pour les premiers congrus à 3 modulo 4, voir l'exercice 2.9. \square

13. Exercice. Soit $T : X \rightarrow X$ 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

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

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

Indication : écrire $x \in [0, 1[\cap \mathbb{Q}$ sous la forme $\frac{a}{2^b c}$ avec c impair et $a, 2^b c$ premiers entre eux.

COMPLÉMENTS AU N° 5

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

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

Voici une interprétation de ce résultat. Pour tout entier $n \geq 1$, on considère les $\frac{1}{2}n(n+1) \sim \frac{1}{2}n^2$ paires d'entiers (a, b) telles que $1 \leq a \leq b \leq n$; 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. [On 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.]

15. Remarques historiques. Le théorème 8 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 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 $n \geq 3$, 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.)

16. Exercice. 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. S’il existait une solution, il en existerait aussi une telle que $\text{pgcd}(x, y, z)$ soit impair ; montrer que cela conduirait à une contradiction.]

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

6. 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 transformer 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 usuels¹⁰, 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 *chiffrement*, et la transformation inverse le *décodage*

¹⁰Choix possible : a, b, ..., z, espace blanc, point, ? \$, 0, 1, ..., 9.

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 pas 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 exception 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 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

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

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

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 se donner D , d'en déduire E d'une manière ou d'une autre, puis de transmettre E à son correspondant en gardant D secret. Ainsi B pourra-t-il encoder ses messages, grâce à E , mais seul A pourra-t-il les décoder.

Voici un exemple simple : \mathcal{M} est l'ensemble des paires de nombres premiers impairs distincts

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

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

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

L'application E est le produit, et D est la décomposition en facteurs premiers. Pour des correspondants privés de caleuettes, 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

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

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

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

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 .]

7. DESCRIPTION DU CODAGE RSA

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 calcule¹¹ $d \in \{1, 2, \dots, m - 1\}$ 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 qu'il est "très difficile" de trouver p et q , donc aussi $\varphi(m)$ (voir l'exercice du numéro précédent), donc a fortiori de calculer d à partir de e .

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 :

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

et par suite $z = x$ par la proposition suivante.

¹¹Voir l'algorithme d'Euclide et le numéro 1.7.

3. Proposition. Soient p, q deux nombres premiers distincts et $m = pq$ leur produit. On a

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

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. On peut d'abord supposer $k \geq 0$ (car il n'y a rien à montrer pour $k = 0$).

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

Exemple pour la proposition. Si $m = 15$, alors $\varphi(15) = 8$, et

$$3^9 \equiv 3(81)^2 \equiv 3(6)^2 \equiv 18 \equiv 3 \pmod{15}.$$

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

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

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

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

Lorsque A reçoit le message, il calcule

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

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 $6^{35} \equiv 11 \pmod{65}$.

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

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".)

6. Signatures.

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

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

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.

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

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

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

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

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

qu'il transmet à B .

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

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

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

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

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 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 3, donc $\tilde{s}_A = s_A$.

Dans le sens contraire, le procédé est presque 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 $s_B^{(1)} \in \{0, 1, \dots, m_A - 1\}$ tel que $s_B^{(1)} \equiv (s_B)^{e_A} \pmod{m_A}$,

(ii') puis $s_B^{(2)} \in \{0, 1, \dots, m_B - 1\}$ tel que $s_B^{(2)} \equiv (s_B^{(1)})^{d_B} \pmod{m_B}$.

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

(iv') puis $\tilde{s}_B \in \{0, 1, \dots, m_A - 1\}$ tel que $\tilde{s}_B \equiv (\tilde{s}_B^{(1)})^{d_A} \pmod{m_A}$.

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], qui est un cours de mathématiques, et [Lan], sur un sujet d'actualité.

RÉFÉRENCES POUR LES § 6 ET 7

- DiHe. W. Diffie et M.E. Hellman, *New directions in cryptography*, IEEE Transactions in Information Theory **IT-22** (1976), 644-654.
- 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 (March 2000), 341-349.
- Per. G. Perec, *La disparition*, Denoël, 1969.
- 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** (March 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]).

Les paragraphes suivants ont pour but de montrer que les propriétés et les algorithmes de la *division 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 paragraphe 4.

8. DÉFINITION DE L'ANNEAU $\mathbb{K}[X]$ – POLYNÔMES ET APPLICATIONS POLYNOMIALES

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 12. Rappelons que, pour tout entier $n \geq 0$, on désigne par \mathbb{K}^n l'ensemble des suites (a_1, \dots, 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. 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 $a_0 + a_1 X + a_2 X^2 + \dots + a_n X^n$ si $a_i = 0 \forall i > n$. Ainsi, le degré du polynôme $a_0 + a_1 X + a_2 X^2 + \dots + a_n X^n$ est n si $a_n \neq 0$.

2. Définitions. Etant donné deux polynômes

$$a = (a_i)_{i \in \mathbb{N}} \quad \text{et} \quad b = (b_i)_{i \in \mathbb{N}}$$

dans $\mathbb{K}[X]$, on définit leur *somme* et leur *produit* par

$$\begin{aligned} a + b &= (c_i)_{i \in \mathbb{N}} \quad \text{avec} \quad c_i = a_i + b_i \quad \forall i \in \mathbb{N} \\ ab &= (d_i)_{i \in \mathbb{N}} \quad \text{avec} \quad d_i = a_0 b_i + a_1 b_{i-1} + \dots + a_i b_0 = \sum_{\substack{j, k \in \mathbb{N} \\ j+k=i}} a_j b_k \quad \forall i \in \mathbb{N}. \end{aligned}$$

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.

3. Proposition. Pour $a, b \in \mathbb{K}[X]$, on a

$$\begin{aligned} \deg(a + b) &\leq \max\{\deg(a), \deg(b)\} \\ \deg(ab) &= \deg(a) + \deg(b). \end{aligned}$$

Preuve. Cela résulte des définitions. On adopte les conventions $\max\{-\infty, n\} = n$ et $n + (-\infty) = (-\infty) + n = -\infty$ pour tout $n \in \mathbb{N}$. \square

4. Proposition. L'addition et la multiplication définies ci-dessus font de $\mathbb{K}[X]$ un anneau commutatif dont l'unité est le polynôme $(1, 0, 0, \dots)$.

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} . \square

La formule de la proposition 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, l'anneau $\mathbb{K}[X]$ est *sans diviseur de zéro*.

5. Retour à la notation. L'élément zéro de l'anneau $\mathbb{K}[X]$ est la suite $(0, 0, 0, \dots)$ dont tous les termes sont des zéros. (Distinguer $0 \in \mathbb{K}$ de $0 = (0, 0, \dots) \in \mathbb{K}[X]$, malgré l'abus de notation. "Il faudrait" écrire $0_{\mathbb{K}}$ et $0_{\mathbb{K}[X]}$, mais personne n'est assez puriste pour s'exposer à cette lourdeur de notation !) L'élément 1 de l'anneau $\mathbb{K}[X]$ est la suite $(1, 0, 0, \dots)$.

Plus généralement, pour tout $a \in \mathbb{K}$, on a un polynôme $(a, 0, 0, \dots)$ dont le premier terme vaut a et tous les suivants 0, et l'application $a \mapsto (a, 0, 0, \dots)$ 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

$$X = (0, 1, 0, 0, 0, \dots)$$

avec un seul terme non nul. La définition de la multiplication montre qu'on a

$$X^2 = (0, 0, 1, 0, 0, 0, \dots)$$

$$X^3 = (0, 0, 0, 1, 0, 0, \dots)$$

$$X^4 = (0, 0, 0, 0, 1, 0, \dots)$$

et ainsi de suite. Pour $a_0, a_1, a_2, a_3, \dots \in \mathbb{K}$ (avec $a_i = 0$ pour i assez grand), on a donc

$$\begin{aligned} a_0 + a_1 X + a_2 X^2 + \dots &= (a_0, 0, 0, 0, \dots) + (0, a_1, 0, 0, \dots) + (0, 0, a_2, 0, \dots) + \dots \\ &= (a_0, a_1, a_2, \dots), \end{aligned}$$

ce qui justifie la notation usuelle, à laquelle il a déjà été fait allusion.

On écrit donc indifféremment

$$P = \sum_{j=0}^n a_j X^j \in \mathbb{K}[X] \quad \text{ou} \quad P(X) = \sum_{j=0}^n a_j X^j \in \mathbb{K}[X]$$

pour un polynôme de degré au plus n .

6. 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} ! par exemple de considérer d'abord le polynôme $X^2 + 1$ comme étant dans $\mathbb{R}[X]$, puis de l'évaluer en l'élément $i \in \mathbb{C}$ pour trouver $i^2 + 1 = 0 \in \mathbb{C}$.

(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” $a = (a_{i,j})_{(i,j) \in \mathbb{N}^2}$ avec $a_{i,j} = 0$ pour i et j assez grands. 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} ou $\mathbb{Z}/6\mathbb{Z}$. Exercice : voir ci-dessus ce qui n'est pas vrai lorsqu'on remplace \mathbb{K} par $\mathbb{Z}/6\mathbb{Z}$.

Exercice : imaginer d'autres variations.

(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*.

7. 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

$$\begin{aligned}(\phi + \psi)(x) &= \phi(x) + \psi(x) & \forall x \in \mathbb{K} \\ (\phi \psi)(x) &= \phi(x)\psi(x) & \forall x \in \mathbb{K}\end{aligned}$$

pour tous $\phi, \psi \in \mathcal{A}ppl(\mathbb{K})$. L'application naturelle

$$\left\{ \begin{array}{l} \mathbb{K}[X] \longrightarrow \mathcal{A}ppl(\mathbb{K}) \\ \sum a_j X^j \longmapsto \left(x \longmapsto \sum a_j x^j \right) \end{array} \right.$$

est un homomorphisme d'anneaux. (Exercice : vérifier ces affirmations.) Par définition, une *application polynomiale* est une application qui est dans l'image de cet homomorphisme.

8. Attention. Si \mathbb{K} est un corps fini, disons à q éléments, cet homomorphisme 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 naturellement un espace vectoriel sur \mathbb{K} de dimension q , et par suite un anneau fini à q^q éléments. Ce même homomorphisme est surjectif (voir l'exercice qui suit).

Si \mathbb{K} est un corps infini, il résulte de la proposition 10.4 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. Cet homomorphisme n'est alors pas surjectif, puisqu'une application de \mathbb{K} dans \mathbb{K} non nulle en exactement un point n'est pas polynomiale. En d'autres termes : *lorsque le corps \mathbb{K} est infini, les applications de $\mathcal{A}ppl(\mathbb{K})$ ne sont pas toutes polynomiales.*

9. Exercice. 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) Montrer que l'homomorphisme $\mathbb{K}[X] \longrightarrow \mathcal{A}ppl(\mathbb{K})$ est surjectif.

(v)[‡] Lorsque $\mathbb{K} = \mathbb{F}_p$, déterminer le coefficient du terme de degré $d - 1$ de $G(X)$.

(iii') Dans le cas particulier d'un corps \mathbb{F}_p , étant donné $y \in \mathbb{F}_p$, déterminer les valeurs de la fonction polynomiale définie par le polynôme $G'_y(X) = 1 - (X - y)^{p-1}$.

En particulier : *lorsque le corps \mathbb{K} est fini, toute application de $\mathcal{A}ppl(\mathbb{K})$ est polynomiale.*

9. DIVISION DES POLYNÔMES

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

$$F = PQ + R \quad \text{et} \quad \deg(R) < \deg(P).$$

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

$$\begin{aligned} F &= a_0 + a_1X + \dots + a_fX^f && \text{avec } a_f \neq 0 \\ P &= b_0 + b_1X + \dots + b_pX^p && \text{avec } b_p \neq 0. \end{aligned}$$

On distingue à nouveau deux cas. (i) Si $f < p$, on pose $Q = 0$ et $R = F$. (ii) Si $f \geq p$, alors

$$\begin{aligned} F - \frac{a_f}{b_p}X^{f-p}P &= (a_fX^f + a_{f-1}X^{f-1} + \dots) - \frac{a_f}{b_p}(b_pX^f + b_{p-1}X^{f-1} + \dots) \\ &= (a_{f-1}X^{f-1} + \dots) - \frac{a_f}{b_p}(b_{p-1}X^{f-1} + \dots) \end{aligned}$$

est de degré strictement inférieur à f ; on peut donc appliquer l'hypothèse de récurrence au couple $(F - \frac{a_f}{b_p}X^{f-p}P, P)$, 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

$$\deg(P(Q - Q')) \geq \deg(P) \quad \text{et} \quad \deg(R' - R) < \deg(P)$$

par la proposition 8.3. Donc $Q' = Q$, et par suite aussi $R' = R$. \square

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. 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 $x, y \in A$, on a $ax + by \in \mathcal{I}$.

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 .

Rappel (proposition 1.13) : tout idéal de \mathbb{Z} est principal.

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.] \square

4. Notations et définitions. Soit A un anneau commutatif. Etant donné des éléments $a_1, \dots, a_n \in A$ et des sous-ensembles $S_1, \dots, S_n \subset A$, on note

$$a_1S_1 + \dots + a_nS_n$$

le sous-ensemble de A constitué des éléments de la forme $a_1s_1 + \dots + a_ns_n$, avec $s_1 \in S_1, \dots, s_n \in S_n$. Par exemple :

$$4\mathbb{Z} + 6\mathbb{Z} = 2\mathbb{Z}$$

(sic).

On dit qu'un anneau commutatif A est *intègre* si A contient au moins deux éléments, et si $ab \neq 0$ pour toute paire (a, b) d'éléments non nuls de A . Par exemple, \mathbb{Z} est intègre, et tout corps est intègre ; il résulte de la proposition 8.3 que tout anneau de polynômes à une indéterminée 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.

Soit A un anneau commutatif intègre dans lequel tout idéal est principal. Etant donné des éléments $a_1, \dots, a_n \in A$ non tous nuls, on appelle *plus grand commun diviseur* ou *pgcd* de a_1, \dots, a_n tout élément $d \in A$ tel que

$$dA = a_1A + \dots + a_nA.$$

Si d_1, d_2 sont deux tels éléments, on a $d_1A = d_2A$, de sorte qu'il existe $a, b \in A$ tels que $d_1 = d_2a$, $d_2 = d_1b$; on a donc aussi $d_2 = d_2ab$, et $d_2(1 - ab) = 0$, et encore (intégrité) $ab = 1$. En d'autres termes, "le" plus grand commun diviseur de a_1, \dots, a_n est bien défini à multiplication près par un élément inversible de A .

On dit que des éléments non tous nuls $a_1, \dots, a_n \in A$ sont *premiers entre eux* si leurs pgcd sont les éléments inversibles de A .

Si $A = \mathbb{Z}$, il y a deux éléments inversibles qui sont 1 et -1 . Si \mathbb{K} est un corps et $A = \mathbb{K}[X]$, les éléments inversibles de A sont les polynômes constants non nuls (c'est une conséquence immédiate de la proposition 8.3).

5. Proposition. Soient \mathbb{K} un corps et $P_1, \dots, P_n, D \in \mathbb{K}[X]$ des polynômes non nuls. Les propriétés suivantes sont équivalentes :

- (i) D est un plus grand commun diviseur de P_1, \dots, P_n ,
- (ii) les diviseurs communs à P_1, \dots, P_n sont les diviseurs de D .

Preuve. La propriété (i) s'écrit

$$(*) \quad D\mathbb{K}[X] = P_1\mathbb{K}[X] + \dots + P_n\mathbb{K}[X].$$

Preuve de (i) \implies (ii). L'hypothèse (i) = (*) implique d'abord que, pour tout $j \in \{1, \dots, n\}$, il existe $Q_j \in \mathbb{K}[X]$ tel que $DQ_j = P_j$. Donc tout diviseur de D divise aussi chacun des P_j . Par ailleurs, (*) implique qu'il existe $F_1, \dots, F_n \in \mathbb{K}[X]$ tels que $D = P_1F_1 + \dots + P_nF_n$. Par suite tout diviseur commun des P_j divise aussi D .

Preuve de (ii) \implies (i). L'ensemble $P_1\mathbb{K}[X] + \dots + P_n\mathbb{K}[X]$ est évidemment un idéal de $\mathbb{K}[X]$. Par la proposition 2, il existe $D' \in \mathbb{K}[X]$ tel que

$$(**) \quad D'\mathbb{K}[X] = P_1\mathbb{K}[X] + \dots + P_n\mathbb{K}[X].$$

Les diviseurs communs à P_1, \dots, P_n sont les diviseurs de D' [voir l'argument pour (i) \implies (ii)], de sorte que D et D' ont les mêmes diviseurs [puisque la propriété (ii) est vraie par hypothèse]. En particulier, D' est un diviseur de D , et D est un diviseur de D' ; il existe donc $F, G \in \mathbb{K}[X]$ tels que $D = FD'$ et $D' = GD$. Cela implique, comme juste avant la proposition 5, qu'il existe $c \in \mathbb{K}, c \neq 0$ tel que $D' = cD$; ainsi (**) implique bien (*). \square

6. Cas particulier - théorème de Bézout. Pour que deux polynômes $A, B \in \mathbb{K}[X]$ 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 $P, Q \in \mathbb{K}[X]$ tels que

$$A(X)P(X) + B(X)Q(X) = 1.$$

Plus généralement, pour que des polynômes $A_1, \dots, A_n \in \mathbb{K}[X]$ non tous nuls soient premiers entre eux, il faut et il suffit qu'il existe $P_1, \dots, P_n \in \mathbb{K}[X]$ tels que

$$A_1(X)P_1(X) + \dots + A_n(X)P_n(X) = 1.$$

7. Exemples. Dans $\mathbb{R}[X]$, les polynômes $X^2 + 1$ et $X^2 + 3X + 1$ sont premiers entre eux, et on a

$$(X^2 + 1) \left(\frac{3}{10}X + \frac{8}{10} \right) - (X^2 + 3X + 1) \left(\frac{3}{10}X - \frac{1}{10} \right) = 1.$$

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 $x = 1$.

Attention : les polynômes $X^2 + 5$ et $X^2 + 4X + 3$ sont premiers entre eux dans $\mathbb{Q}[X]$, car

$$(*) \quad (X^2 + 5) \left(\frac{X}{21} + \frac{3}{14} \right) - (X^2 + 4X + 3) \left(\frac{X}{21} + \frac{1}{42} \right) = 1$$

mais pas dans $\mathbb{F}_7[X]$, car

$$X^2 + 5 = (X + 3)(X + 4) \quad \text{et} \quad X^2 + 4X + 3 = (X + 3)(X + 1).$$

Exercice : retrouver l'identité (*) en appliquant l'algorithme d'Euclide (corollaire 1.11).

8. Exercice. On considère les polynômes $P_1(X) = (X - 1)^3$ et $P_2(X) = X^2$ dans $\mathbb{Q}[X]$.

(i) Expliciter les quotients A_2, A_3 et les restes P_3, P_4 des divisions euclidiennes $P_1 = P_2A_2 + P_3$ et $P_2 = P_3A_3 + P_4$. [Indication : $P_4(X) = \frac{1}{9}$.]

(ii) En déduire la forme explicite de polynômes $A_1, A_2 \in \mathbb{Q}[X]$ tels que

$$1 = A_1(X)P_1(X) + A_2(X)P_2(X).$$

10. RACINES DES POLYNÔMES À UNE INDÉTERMINÉE

Aux paragraphes 10 et 11, on désigne par \mathbb{K} un corps et par $\mathbb{K}[X]$ l'anneau des polynômes à une indéterminée à coefficients dans \mathbb{K} .

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 $P(c) = \sum_{j=0}^n a_j c^j$. On dit que c est une *racine* ou un *zéro* de P si $P(c) = 0$.

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 $R = 0$. \square

3. Exemples. Lorsque $\mathbb{K} = \mathbb{C}$, le nombre complexe i est une racine du polynôme $X^2 + 1$, et

$$X^2 + 1 = (X + i)(X - i) \in \mathbb{C}[X].$$

Lorsque $\mathbb{K} = \mathbb{F}_2$, le nombre 1 est une racine du polynôme $X^3 + X^2 + X + 1$, et

$$X^3 + X^2 + X + 1 = (X + 1)^3 \in \mathbb{F}_2[X].$$

4. Proposition. Un polynôme $P(X) \in \mathbb{K}[X]$ de degré $d \geq 0$ a au plus d racines dans \mathbb{K} .

Preuve. Par récurrence sur d . \square

11. POLYNÔMES IRRÉDUCTIBLES

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.

2. 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) $X^2 + X + 1 \in \mathbb{F}_2[X]$.

(iv) Un polynôme réductible P de degré $d \geq 2$ s'écrit $P = P_1 P_2$, avec P_1, P_2 de degrés $d_1, d_2 \geq 2$, 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 $n \geq 2$.

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.

3. 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 (factorisation des entiers en produit de nombres premiers).

Preuve de l'unicité. On montre d'abord que, pour $F, P_1, P_2 \in \mathbb{K}[X]$ avec F irréductible, si F divise $P_1 P_2$, alors F divise l'un au moins des polynômes P_1, P_2 . Voir le théorème 2.2 et le lemme 2.3.

On procède alors comme pour la preuve du théorème 2.2. \square

4. Définitions. 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

$$\begin{aligned} [x]_{\mathcal{I}} + [y]_{\mathcal{I}} &= [x + y]_{\mathcal{I}} \\ [x]_{\mathcal{I}} [y]_{\mathcal{I}} &= [xy]_{\mathcal{I}} \end{aligned}$$

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, 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 .

5. Exemple fondamental : l'anneau $\mathbb{K}[X]/(P)$, quotient de $\mathbb{K}[X]$ par l'idéal principal $(P) = P\mathbb{K}[X]$.

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 $E \rightarrow \mathbb{K}[X]$ et de la projection canonique $\mathbb{K}[X] \rightarrow \mathbb{K}[X]/(P)$ 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. \square

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 $P(X)$.

7. 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 :

$$(X^2 + 2)(X^2 + 5) \equiv 6X + 3 \pmod{X^3 + 1}.$$

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 presque immédiate du théorème 9.6, ou théorème de Bézout pour les polynômes. Voir la preuve du théorème 4.15 (qui dit que, pour $a \geq 1$, l'anneau $\mathbb{Z}/(a)$ est un corps si et seulement si a est premier). \square

9. 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 $\sum_{k \geq 0} a_k X^k \longmapsto \sum_{k \geq 0} a_k (-i)^k$.)

(ii) Le quotient $\mathbb{Q}[X]/(X^2 - 2)$ est isomorphe au corps $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.

(iii) Le quotient $\mathbb{F}_2[X]/(X^2 + X + 1)$ est un corps à 4 éléments.

10. Exercice. 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, \dots, R_d de degrés $< n$ tels que $X^j \equiv R_j \pmod{P}$ pour $j \in \{1, \dots, d\}$.

(a) $P = X^2 + X + 1$. [Noter que $\mathbb{F}_2[X]/(P)$ est un corps à 4 éléments. Les R_j sont $X, X + 1, 1$, ce qui montre que le groupe des éléments non nuls de ce corps est un groupe cyclique d'ordre 3.]

(b) $P = X^3 + X^2 + 1$. [Noter que $\mathbb{F}_2[X]/(P)$ est un corps à 8 éléments. Les R_j sont $X, X^2, X^2 + 1, X^1 + X + 1, X + 1, X^2 + X, 1$, ce qui montre que le groupe des éléments non nuls de ce corps est un groupe cyclique d'ordre 8.]

(c) $P = X^4 + X^3 + 1$. [On trouve un corps à 16 éléments, dont les éléments non nuls constituent un groupe multiplicatif qui est cyclique d'ordre 15.]

(d) $P = X^4 + X^3 + X^2 + X + 1$. [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.]

11. Exercice. Soit $P(X) \in \mathbb{Q}[X]$ un polynôme de la forme $P(X) = X^d + k_1 X^{d-1} + \dots + k_{d-1} X + k_d$, où les coefficients k_1, \dots, 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 le polynôme $X^3 + X + 1$ est irréductible dans $\mathbb{Q}[X]$ en montrant qu'il n'a aucune racine dans \mathbb{Q} .

12. CORPS FINIS.

Soit \mathbb{K} un corps. Considérons l'application $\varphi : \mathbb{Z} \rightarrow \mathbb{K}$ définie par $\varphi(n) = 1 + \dots + 1$, où le terme de droite contient n fois l'élément $1 \in \mathbb{K}$. Cette application peut être injective (cas de $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \dots$) ou non (cas de $\mathbb{F}_p, \mathbb{F}_2[X]/(X^2 + X + 1), \dots$). Si φ n'est pas injective, son noyau est un idéal de \mathbb{Z} ; il existe donc un entier positif p tel que $\text{Ker}(\varphi) = \mathbb{Z}/(p)$. Comme $1 \neq 0$ dans \mathbb{K} , on a $p \geq 2$. Comme tous les éléments non nuls de \mathbb{K} (et en particulier les éléments non nuls de l'image de φ) sont inversibles, p est nécessairement un nombre premier.

1. Définition. La caractéristique d'un corps \mathbb{K} est zéro si l'application φ ci-dessus est injective, et p si $\text{Ker}(\varphi) = \mathbb{Z}/(p)$.

2. Remarque. Tout corps de caractéristique zéro contient l'image de l'anneau \mathbb{Z} par l'homomorphisme injectif φ , et donc aussi 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 $\mathbb{F}_p = \mathbb{Z}/(p) = \{0, 1, \dots, p - 1\}$.

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.

3. 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) Deux corps fini de même ordre sont isomorphes.

(iv) Les éléments non nuls d'un corps fini d'ordre p^n constituent pour la multiplication un groupe cyclique d'ordre $p^n - 1$.

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.

Voir aussi l'exercice 11.10 pour quelques vérifications de l'assertion (iv). \square

4. Preuve de l'existence d'un corps finis 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 $P(0) = 0$) et le nombre de coefficients égaux à 1 est impair (sinon $P(1) = 0$). On obtient ainsi facilement les polynômes irréductibles de degré 2

$$X^2 + X + 1,$$

de degré 3

$$X^3 + X^2 + 1 \quad \text{et} \quad X^3 + X + 1,$$

et même de degré 4 (bien que ce ne soit pas utile pour démontrer l'existence de \mathbb{F}_{128})

$$X^4 + X^3 + X^2 + X + 1, \quad X^4 + X^3 + 1 \quad \text{et} \quad X^4 + X + 1$$

(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 polynômes de la liste $X, X + 1, X^2 + X + 1, X^3 + X^2 + 1, X^3 + X + 1$.

Assertion. 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

$$\begin{aligned} X^7 + X + 1 &= (X^2 + X + 1)(X^5 + X^4 + X^2 + X) + 1 \\ X^7 + X + 1 &= (X^3 + X + 1)(X^4 + X^2 + X + 1) + X \\ X^7 + X + 1 &= (X^3 + X^2 + 1)(X^4 + X^3 + X^2 + 1) + X. \end{aligned}$$

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 moniques¹² 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

$$\mu(d) = \begin{cases} 1 & \text{si } d = 1, \\ (-1)^k & \text{si } d = \prod_{j=1}^k p_j \text{ pour des premiers } p_1, \dots, p_k \text{ distincts,} \\ 0 & \text{s'il existe un premier } p \text{ tel que } p^2 \mid d. \end{cases}$$

Par exemple

$$\begin{aligned} N_q(6) &= \frac{1}{6} (q^6 - q^3 - q^2 + q) \\ N_q(7) &= \frac{1}{7} (q^7 - q) \\ N_q(8) &= \frac{1}{8} (q^8 - q^4), \end{aligned}$$

et, en particulier, il y a

$$N_2(7) = 18$$

polynômes irréductibles de la forme $X^7 + a_6 X^6 + a_5 X^5 + \dots + a_1 X + 1$ 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).

5. Exercice. Dresser la liste des polynômes irréductibles de degrés ≤ 4 dans $\mathbb{F}_2[X]$ et $\mathbb{F}_3[X]$.

¹²Un polynôme non nul est *monique* si le coefficient de son terme de degré maximal est 1. Par exemple, $X^2 + 2$ est monique et $2X^2 + 1$ ne l'est pas.

**GROUPES SYMÉTRIQUES ET
GROUPES DE PERMUTATION**

Les groupes symétriques auxquels les deux paragraphes suivants sont consacrés apparaissent déjà très brièvement au § 4, ainsi qu'au § 18 du semestre d'hiver.

13. GROUPES SYMÉTRIQUES

Pour tout entier $n \geq 1$, nous notons J_n l'ensemble $\{1, 2, \dots, n\}$; rappelons que le groupe $Sym(n)$ est l'ensemble de toutes les applications bijectives de J_n dans J_n , aussi appelées *permutations* de J_n , avec pour produit la composition des applications. C'est un groupe d'ordre $n!$. Le *support* d'une permutation $\sigma \in Sym(n)$ est le sous-ensemble $\{j \in J_n \mid \sigma(j) \neq j\}$ de J_n .

Le résultat principal de ce paragraphe est le théorème 7.

1. Définitions. Soit k un entier tel que $2 \leq k \leq n$, et a_1, \dots, a_k des éléments distincts de J_n . La permutation $\sigma \in Sym(n)$ définie par

$$\sigma(i) = \begin{cases} a_{j+1} & \text{si } i = a_j \text{ pour un } j \text{ tel que } 1 \leq j < k \\ a_1 & \text{si } i = a_k \\ i & \text{sinon} \end{cases}$$

est un *k-cycle*; on écrit

$$\sigma = (a_1, \dots, a_k)$$

et on note que le support d'un tel cycle est le sous-ensemble $\{a_1, \dots, a_k\}$ de J_n . Une *transposition* est un 2-cycle.

2. Remarques. (i) L'écriture d'un *k-cycle* n'est pas unique; par exemple $(2, 3, 5) = (3, 5, 2) = (5, 2, 3)$ dans $Sym(5)$, et plus généralement

$$(a_1, \dots, a_{k-1}, a_k) = (a_2, \dots, a_k, a_1).$$

(ii) Il faut toutefois noter que l'ordre d'écriture des entiers a_j n'est pas arbitraire! par exemple $(2, 3, 5) \neq (2, 5, 3)$.

(iii) L'identité est l'unique permutation de support vide. Le support d'un *k-cycle* est l'ensemble des k entiers a_j qui apparaissent dans l'écriture de ce cycle. Il faut bien observer que, avec les notations adoptées, on a $\{2, 3, 5\} = \{2, 5, 3\}$ (comparer avec la remarque précédente).

(iv) Le support d'une permutation distincte de l'identité contient au moins deux éléments.

(v) Les deux éléments de $Sym(2)$ sont l'identité et la transposition $(1, 2)$. Il y a trois transpositions dans $Sym(3)$ qui sont $(1, 2)$, $(1, 3)$ et $(2, 3)$. Plus généralement, il y a $\frac{n(n-1)}{2}$ transpositions dans $Sym(n)$.

(vi) Les éléments d'ordre¹³ 2 ne sont pas tous des transpositions! En fait, ce sont précisément les produits de transpositions à supports disjoints; par exemple, $(1, 3)(7, 8)$ et $(1, 2)(3, 4)(5, 6)$ sont des éléments d'ordre deux dans $Sym(8)$.

¹³Rappelons qu'un élément g d'un groupe G est d'ordre 2 si $g^2 = 2$ et $g \neq 1$.

(vii) Soit X un ensemble fini à n éléments. Quitte à re-nommer les éléments, on peut voir $Sym(n)$ comme le groupe de toutes les applications bijectives de X dans X .

3. Sur l'ordre des produits. Nous convenons de composer (= multiplier) les permutations comme des applications : $(\sigma\tau)(i) = \sigma(\tau(i))$. Il en résulte qu'on a par exemple

$$(1, 2)(2, 3) = (1, 2, 3) \neq (1, 3, 2) = (2, 3)(1, 2).$$

Toutefois, il faut aussi noter que des cycles à supports disjoints commutent. Par exemple

$$(1, 3)(2, 5)(4, 7) = (4, 7)(2, 5)(1, 3) = (4, 7)(1, 3)(2, 5)$$

et

$$(1, 2, 3)(4, 5) = (4, 5)(1, 2, 3).$$

Plus généralement des permutations à supports disjoints commutent.

4. Proposition. *Toute permutation de $Sym(n)$ s'écrit comme produit de cycles à supports disjoints deux à deux, et ceci de manière unique à l'ordre près des facteurs.*

Preuve. Soit $\sigma \in Sym(n)$. On définit un graphe orienté de la manière suivante : ses sommets sont les entiers $1, \dots, n$, et ses arêtes orientées sont les "flèches" $i \rightarrow \sigma(i)$, pour $i \in J_n$. Ainsi ce graphe a-t-il exactement n sommets et n arêtes orientées ; parmi ces dernières, certaines sont des *boucles* dont l'extrémité coïncide avec l'origine, et d'autres sont des arêtes dont chacune a une extrémité et une origine distinctes.

Le support de σ est le complément dans J_n des sommets correspondant aux boucles. Les autres arêtes de ce graphe orienté forment des chemins fermés de longueurs ≥ 2 qui fournissent la décomposition de la permutation en cycles. \square

Il est *essentiel* de se familiariser avec un grand nombre de cas particuliers. On laisse au lecteur le soin de dessiner le graphe orienté correspondant à la permutation $\sigma \in Sym(5)$ définie par $\sigma(1) = 3, \sigma(2) = 4, \sigma(3) = 5, \sigma(4) = 2, \sigma(5) = 1$, ainsi que les graphes correspondant à de nombreux autres exemples.

5. Exercices. (i) Ecrire la décomposition en cycles du produit $(1, 2, 3)(2, 3, 4)$ dans $Sym(4)$.

(ii) Montrer que l'ordre d'une permutation est donné par le plus petit commun multiple des ordres des cycles dans la décomposition de la proposition 4.

(iii) *Exercice pour montrer qu'il n'y a pas unicité de la décomposition en produit de transpositions* dans la proposition qui suit. Vérifier que

$$\begin{aligned} (1, 2) &= (3, 4)(1, 2)(3, 4) \\ (1, 2)(2, 3)(1, 2) &= (2, 3)(1, 2)(2, 3) = (1, 3) \\ id &= \left((1, 2)(2, 3) \dots (n-2, n-1)(n-1, n) \right)^n. \end{aligned}$$

6. Proposition. *Toute permutation $\sigma \in \text{Sym}(n)$ s'écrit au moins d'une manière comme un produit de transpositions.*

Preuve (déjà au § 18 du semestre d'hiver). On procède par récurrence sur n . Si $n \leq 2$, il n'y a rien à montrer. Sinon, on suppose la proposition vraie pour toute permutation dans $\text{Sym}(n-1)$, et on distingue deux cas.

Lorsque $\sigma(n) = n$, l'assertion pour σ résulte immédiatement de l'hypothèse de récurrence.

Lorsque $\sigma(n) = k < n$, on considère la transposition $\tau = (k, n)$ et le produit $\tau\sigma$. Comme $(\tau\sigma)(n) = n$, il résulte du premier cas que $\tau\sigma$ est un produit de transpositions τ_1, \dots, τ_p . Par suite $\sigma = \tau(\tau\sigma) = \tau \prod_{1 \leq j \leq p} \tau_j$ est encore un produit de transpositions. \square

Remarque. Si σ s'écrit comme un produit $\tau_1\tau_2 \dots \tau_k$ de transpositions, alors $\sigma^{-1} = \tau_k\tau_{k-1} \dots \tau_1$.

7. Théorème. (i) *Soient σ une permutation et $\tau_1, \dots, \tau_p, \rho_1, \dots, \rho_q$ des transpositions dans $\text{Sym}(n)$ telles que*

$$\sigma = \prod_{1 \leq j \leq p} \tau_j = \prod_{1 \leq k \leq q} \rho_k.$$

Alors $p - q$ est pair.

(ii) *L'application*

$$\text{sign} : \begin{cases} \text{Sym}(n) & \longrightarrow \{\pm 1\} \\ \sigma & \longmapsto \text{sign}(\sigma) \end{cases}$$

qui applique une permutation σ sur $+1$ si elle est produit d'un nombre pair de transpositions et sur -1 sinon est un homomorphisme de groupes.

8. Définitions. On dit qu'une permutation est *paire* si elle s'écrit comme un produit d'un nombre pair de transpositions, et *impaire* sinon.

Le nombre $\text{sign}(\sigma) \in \{\pm 1\}$ s'appelle la *signature* de la permutation σ .

Les permutations paires de $\text{Sym}(n)$ constituent un sous-groupe appelé le *groupe alterné* $\text{Alt}(n)$.

Preuve du théorème 7 (variante d'une preuve du § 18 du semestre d'hiver). Étant donné une permutation $\sigma \in \text{Sym}(n)$ et une fonction $F : \mathbb{R}^n \longrightarrow \mathbb{R}$, on définit une nouvelle fonction $F^\sigma : \mathbb{R}^n \longrightarrow \mathbb{R}$ en posant

$$F^\sigma(x_1, \dots, x_n) = F(x_{\sigma(1)}, \dots, x_{\sigma(n)}).$$

Pour $\sigma, \sigma' \in \text{Sym}(n)$, on a

$$\begin{aligned} (F^\sigma)^{\sigma'}(x_1, \dots, x_n) &= (F^\sigma)(x_{\sigma'(1)}, \dots, x_{\sigma'(n)}) \\ &= F(x_{\sigma\sigma'(1)}, \dots, x_{\sigma\sigma'(n)}) \\ &= F^{(\sigma\sigma')}(x_1, \dots, x_n) \end{aligned}$$

pour tous $(x_1, \dots, x_n) \in \mathbb{R}^n$, c'est-à-dire

$$(F^\sigma)^{\sigma'} = F^{(\sigma\sigma')}.$$

Considérons alors la fonction $\Delta : \mathbb{R}^n \rightarrow \mathbb{R}$ définie par

$$\Delta(x_1, \dots, x_n) = \prod_{i < j} (x_i - x_j)$$

où le produit porte sur les $\frac{n(n-1)}{2}$ couples (i, j) tels que $1 \leq i < j \leq n$. Observons que $\Delta \neq 0$, puisque $\Delta(x_1, \dots, x_n) \neq 0$ chaque fois que les nombres x_1, \dots, x_n sont distincts deux à deux.

Affirmation. Si $\tau = (r, s)$ est une transposition, alors $\Delta^\tau = -\Delta$. En effet, dans le produit définissant Δ , les termes ne contenant ni x_r ni x_s ne sont pas modifiés par l'action de τ . Si on suppose $r < s$, les autres s'écrivent

$$(x_r - x_s) \prod_{i=1}^{r-1} \left((x_i - x_r)(x_i - x_s) \right) \prod_{i=r+1}^{s-1} \left((x_r - x_i)(x_i - x_s) \right) \prod_{i=s+1}^n \left((x_r - x_i)(x_s - x_i) \right).$$

Le premier terme change de signe lorsqu'on échange x_r et x_s , et chaque autre paire de termes ne change visiblement pas. Ainsi, l'effet global de τ sur Δ est bien un changement de signe.

Par suite, si $\sigma = \prod_{1 \leq j \leq p} \tau_j$ est un produit de transpositions, on a

$$\Delta^\sigma = (\dots (\Delta^{\tau_1})^{\tau_2} \dots)^{\tau_p} = (-1)^p \Delta$$

et la parité de p dépend que de σ , non du produit $\sigma = \prod_{1 \leq j \leq p} \tau_j$ lui-même.

La preuve de l'assertion (i) est ainsi achevée, et celle de (ii) est laissée au lecteur. \square

Exemple. La signature d'un k -cycle est $(-1)^{k-1}$, car

$$(a_1, a_2, \dots, a_k) = (a_1, a_2)(a_2, a_3) \dots (a_{k-1}, a_k).$$

9. Exercice. Ecrire les décompositions en cycles des permutations du groupe $Alt(4)$.

10. Théorème. Soit $A = (A_{j,k})_{1 \leq j, k \leq n}$ une matrice carrée d'ordre n , réelle ou complexe.

$$\det(A) = \sum_{\sigma \in Sym(n)} \text{sign}(\sigma) A_{1,\sigma(1)} A_{2,\sigma(2)} \dots A_{n,\sigma(n)}.$$

Sur la preuve. Pour $n = 2$, le théorème n'est qu'une re-écriture de l'identité

$$\det \begin{pmatrix} A_{1,1} & A_{1,2} \\ A_{2,1} & A_{2,2} \end{pmatrix} = A_{1,1}A_{2,2} - A_{1,2}A_{2,1}.$$

Pour n quelconque, voir le dernier théorème du § 18 du semestre d'hiver. \square

14. GROUPES DE PERMUTATIONS

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

$$\begin{aligned} 1x &= x \text{ pour tout } x \in X, \\ g(hx) &= (gh)x \text{ pour tous } g, h \in G \text{ et } x \in X. \end{aligned}$$

Une telle action est *fidèle* si

$$\text{pour tout } g \in G, \text{ il existe } x \in X \text{ tel que } gx \neq x.$$

2. Observation. Si G est un groupe agissant sur l'ensemble $J_n = \{1, \dots, n\}$, alors l'application

$$G \ni g \longmapsto (x \mapsto gx) \in \text{Sym}(n)$$

est un homomorphisme de groupes. De plus, 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 (voir la remarque 13.2.vii).

3. Exemples : les groupes diédraux. On considère un entier $k \geq 3$ et un polygone 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 $2k$ éléments.

Un tel groupe s'appelle un *groupe diédral*. Notons que G agit naturellement sur l'ensemble des sommets de P_k , et que cette action est fidèle. Par suite, G s'identifie à un sous-groupe d'ordre $2k$ du groupe symétrique $\text{Sym}(k)$.

4. Exemple : les deux groupes du tétraèdre. Soit T un tétraèdre régulier centré à l'origine d'un espace euclidien E de dimension 3.

Considérons d'abord l'ensemble SG_T des rotations $g \in SO(E) \approx SO(3)$ telles que $g(T) = T$, qui est un sous-groupe de $SO(E)$. Le groupe SG_T contient

- (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),

de sorte que SG_T est d'ordre 12. Par ailleurs, ce groupe agit naturellement

- (i) sur l'ensemble des 4 sommets de T , d'où un homomorphisme injectif $G_T \longrightarrow \text{Sym}(4)$,
- (ii) sur l'ensemble des 6 arêtes de T , d'où un homomorphisme injectif $G_T \longrightarrow \text{Sym}(6)$.

Exercice. Montrer que l'image de SG_T dans $Sym(4)$ coïncide avec le groupe alterné $Alt(4)$.

Considérons ensuite le groupe G_T des isométries g de E telles que $g(T) = T$. Ce groupe agit naturellement et fidèlement¹⁴ sur les sommets de T , d'où un homomorphisme injectif de G_T dans $Sym(4)$. Par ailleurs, 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 transpose x et y , et qui laisse fixes les deux autres sommets de T ; cette symétrie correspond donc à une transposition de $Sym(4)$. Comme l'image naturelle de G_T dans $Sym(4)$ contient toutes les transpositions, elle coïncide avec $Sym(4)$ tout entier; en d'autres termes, *les groupes G_T et $Sym(4)$ sont isomorphes.*

5. Exercice. Soit C un cube centré à l'origine d'un espace euclidien E de dimension 3.

(i) Décrire quelques éléments du sous-groupe SG_C des rotations g de E telles que $g(C) = C$.

(ii)[#] Montrer que SG_C est un groupe à 24 éléments.

(iii)[#] En considérant l'action de SG_C sur l'ensemble des 4 diagonales de C , montrer que SG_C est isomorphe à $Sym(4)$.

(iv) Montrer qu'il existe une isométrie $g \in O(E)$, $g \notin SO(E)$, telle que $g(C) = C$.

6. Remarque. On peut montrer de même que le groupe des rotations d'un espace euclidien de dimension 3 qui laissent invariant un icosaèdre régulier est un groupe à 60 éléments, et qu'il est isomorphe au groupe $Alt(5)$.

Ce même groupe 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 formules "par radicaux" pour une 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 équations de degrés 2, 3 et 4 est intimement liée à l'existence de tels sous-groupes, par exemple à un sous-groupe d'ordre 4 dans $Sym(4)$.

7. Très brève évocation de résultats plus récents. Un groupe G agissant sur un ensemble X agit *transitivement* si, pour tous $x, y \in X$, il existe $g \in G$ tel que $gx = y$. Pour un entier k tel que $2 \leq k \leq n$, le groupe G est dit *k -transitif* si, chaque fois qu'on se donne un premier k -uplet $\{x_1, \dots, x_k\}$ d'éléments de X distincts deux à deux et un second k -uplet $\{y_1, \dots, y_k\}$ de la même espèce, il existe $\sigma \in G$ tel que $\sigma(x_1) = y_1, \dots, \sigma(x_k) = y_k$.

Par exemple, il est évident que $Sym(n)$ est n -transitif sur J_n , et il est facile de vérifier que $Alt(n)$ est $(n-2)$ -transitif.

L'étude des groupes k -transitifs pour $k \geq 2$ a suscité dès le XIX^{ème} siècle un très grand intérêt. Pour un sous-groupe G de $Sym(n)$ qui n'est ni $Sym(n)$ lui-même ni $Alt(n)$ 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 par E. Mathieu dès 1860.

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 $k \geq 2$. [Il s'agit en fait d'une classification contestable, puisqu'il n'existe à ce jour aucune rédaction complète de la preuve. Mais la plupart des spécialistes de la théorie des groupes finis travaillent comme si cette lacune n'était pas gênante.]

¹⁴Car une isométrie de E est complètement déterminée par les images des 4 sommets de T

Sans pouvoir les expliquer ici, je trouve tout à fait remarquable qu'il y ait des liens très étroits entre

- (a) le sous-groupe 5-transitif de $Sym(24)$ découvert par E. Mathieu au siècle dernier,
- (b) le "code de Golay" découvert en 1949,
- (c) les travaux de Leech (années 1960) si importants dans le processus de découverte et classification des groupes finis simples.

Marcel Golay, ingénieur électricien de l'ETHZ, ne s'intéressait a priori pas aux mathématiques fondamentales et aux groupes finis, mais plutôt aux manières de transmettre des messages à travers un environnement à grand bruit de fond. Les mathématiques fondamentales et les mathématiques appliquées sont décidément inséparables.

PIERRE DE LA HARPE, SECTION DE MATHÉMATIQUES, UNIVERSITÉ DE GENÈVE, C.P. 240, CH-1211 GENÈVE 24, SUISSE. MEL : PIERRE.DELAHARPE@MATH.UNIGE.CH