CALCUL MATRICIEL - ARITHMÉTIQUE

par

Christian Maire

Cursus Master en Ingénierie
Informatique 2ème année
2023/2024

Table des matières

PARTIE I
CALCUL MATRICIEL

Les coefficients des matrices sont pris dans l'ensemble des nombres réels $\mathbb{R}$, éventuellement complexes $\mathbb{C}$. Mais on peut généraliser sans peine certains des résultats si l'on change ces ensembles.

1. Introduction aux matrices

Cette section 1 est essentiellement une section dédiée aux rappels de notions vues en 1ère année. Nous omettons la plupart des preuves.

1.1. Définitions et opérations élémentaires. —

Définition 1.1. — Soient deux entiers $p, q \geqslant 1$. Une matrice A est la donnée d'un tableau à p lignes et q colonnes, composé de nombres réels (ou de nombres complexes). On note plus précisément $\mathrm{A} = (a_{i,j})$, $i = 1, \cdots, p$ et $j = 1, \cdots, q$, une telle matrice. Ainsi $a_{i,j}$ désigne le coefficient se trouvant à l'intersection de la i-ème ligne et j-ème colonne. On dit que A est d'ordre (ou de taille) $p \times q$. L'ensemble des matrices à p lignes et q colonnes est noté $\mathrm{M}_{p,q}$ $(= \mathrm{M}_{p,q}(\mathbb{R}))$.

1.1.1. Addition et transposée. — Il est assez immédiat de voir que l'ensemble $\mathrm{M}_{p,q}$ peut être muni d'une loi + résultant de l'addition entre les nombres réels. Plus précisément, pour $A = (a_{i,j})$ et $B = (b_{i,j})$ deux matrices de $\mathrm{M}_{p,q}$, on définit une troisième matrice $C = (c_{i,j}) \in \mathrm{M}_{p,q}$ par $c_{i,j} = a_{i,j} + b_{i,j}$. En d'autres termes la matrice C est obtenue en additionnant les matrices A et B "case par case". Observons que $A + B = B + A$.
La matrice nulle de $\mathrm{M}_{p,q}$, notée $O = (o_{i,j})$, est la matrice pour laquelle $o_{i,j} = 0$ pour tout i, j. Notons par $-A$ la matrice ayant pour coefficients $-a_{i,j}$ si $A = (a_{i,j})$. Alors de façon immédiate on a $A + O = O + A = A$, puis $A - A = O$.
Ces propriétés font que $\mathrm{M}_{p,q}$ muni de la loi + est un *groupe abélien* (voir la section Appendice 8).

L'ensemble $\mathrm{M}_{p,q}$ peut être également muni d'une loi externe $\cdot$ de la façon suivante. Pour $\lambda \in \mathbb{R}$ et $A = (a_{i,j}) \in \mathrm{M}_{p,q}$, on définit une nouvelle matrice $\lambda \cdot A = (a'_{i,j}) \in \mathrm{M}_{p,q}$ par $a'_{i,j} = \lambda a_{i,j}$. En d'autres termes, les coefficients de la matrice A sont multipliés par λ. On note aussi $\lambda \cdot A = \lambda A$. Il est alors assez immédiat de voir les résultats suivants :

Proposition 1.2. — *Soient $A, B \in \mathrm{M}_{p,q}$ et $\lambda, \lambda' \in \mathbb{R}$. On a les propriétés suivantes*

(*i*) $0 \cdot A = 0$, $1 \cdot A = A$,

(*ii*) $\lambda(A + B) = \lambda A + \lambda B$,

(*iii*) $(\lambda + \lambda')A = \lambda A + \lambda' A$.

Exemple 1.3. — Soient $A = \begin{pmatrix} 1 & 2 & 0 \\ 3 & -1 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 1 & 1 \\ -1 & 0 & 2 \end{pmatrix}$ deux matrices de $\mathrm{M}_{2,3}$. Alors $A + B = \begin{pmatrix} 1 & 3 & 1 \\ 2 & -1 & 3 \end{pmatrix}$ et plus généralement

$$\lambda A + \lambda' B = \begin{pmatrix} \lambda & 2\lambda + \lambda' & \lambda' \\ 3\lambda - \lambda' & -\lambda & \lambda + 2\lambda' \end{pmatrix}.$$

L'ensemble des matrices $\mathrm{M}_{p,q}$ muni de la loi externe $\cdot$ est un espace vectoriel sur $\mathbb{R}$. Il est alors assez immédiat de voir que toute matrice A de $\mathrm{M}_{p,q}$ s'écrit de façon unique comme combinaison linéaire des matrices élémentaires $E_{k,l} = (e_{i,j})$ définies par

$$e_{k,l} = \begin{cases} 1 & \text{si } (i,j) = (k,l) \\ 0 & \text{sinon} \end{cases}$$

où ici $k \in \{1, \cdots, p\}$ et $l \in \{1, \cdots, q\}$. De cette observation, on en déduit que $\mathrm{M}_{p,q}$ est un $\mathbb{R}$-espace vectoriel de dimension pq.

Exemple 1.4. — Soit $A = \begin{pmatrix} 1 & 2 & 0 \\ 3 & -1 & 1 \end{pmatrix} \in \mathrm{M}_{2,3}$. On a

$$A = E_{1,1} + 2E_{1,2} + 0E_{1,3} + 3E_{2,1} - E_{2,2} + E_{2,3},$$

où $E_{1,1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \cdots, E_{2,3} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

Il y a une autre opération élémentaire et assez naturelle, c'est l'opération qui consiste à transformer les colonnes en lignes (et *vice versa*) : c'est la notion de transposée.

Définition 1.5. — Soit $A \in \mathrm{M}_{p,q}$. La transposée de $A = (a_{i,j})$ est la matrice de $\mathrm{M}_{q,p}$, notée $A^t = (b_{i,j})$, définie par $b_{i,j} = a_{j,i}$, pour $i \in \{1, \cdots, q\}$ et $j \in \{1, \cdots, p\}$.

Exemple 1.6. — On a $\begin{pmatrix} 1 & 2 & 0 \\ 3 & -1 & 1 \end{pmatrix}^t = \begin{pmatrix} 1 & 3 \\ 2 & -1 \\ 0 & 1 \end{pmatrix}$.

Il est alors assez facile de voir les propriétés suivantes :

Proposition 1.7. — *Pour $A, B \in \mathrm{M}_{p,q}$ et $\lambda \in \mathbb{R}$, on a*

(i) $(A + B)^t = A^t + B^t$,

(ii) $(\lambda A)^t = \lambda A^t$.

1.1.2. Multiplication. — Prenons deux matrices $A \in \mathrm{M}_{p,q}$ et $B \in \mathrm{M}_{r,s}$. Ces matrices sont donc a priori de taille différente (sauf si $p = r$ et $q = s$), il n'est donc pas possible de les additionner. Mais lorsque $q = r$ il est possible de les multiplier !

Définition 1.8. — Soient $A = (a_{i,j}) \in \mathrm{M}_{p,q}$ et $B = (b_{i,j}) \in \mathrm{M}_{q,s}$, on pose $A \cdot B$ (ou encore AB) la matrice $C = (c_{i,j}) \in \mathrm{M}_{p,s}$ définie par

$$b_{i,j} = a_{i,1}b_{1,j} + a_{i,2}b_{2,j} + \cdots + a_{i,q}b_{q,j} = \sum_{k=1}^{q} a_{i,k}b_{k,j}.$$

Ici $i \in \{1, \cdots, p\}$ et $j \in \{1, \cdots, s\}$.

Remarque 1.9. — Observons que le produit AB peut avoir un sens mais pas BA (ou réciproquement).

Exemple 1.10. —

Soient $A = \begin{pmatrix} 1 & 2 & 0 \\ 3 & -1 & 1 \end{pmatrix} \in \mathrm{M}_{2,3}$ et $B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \\ 1 & 1 \end{pmatrix} \in \mathrm{M}_{3,2}$.

Alors $AB = \begin{pmatrix} -2 & 1 \\ 2 & 4 \end{pmatrix} \in \mathrm{M}_{2,2}$ et $BA = \begin{pmatrix} 3 & -1 & 1 \\ - & -2 & 0 \\ 4 & 1 & 1 \end{pmatrix} \in \mathrm{M}_{3,3}$.

Il est assez facile de voir les résultats suivants :

Proposition 1.11. — *Soient $A, B \in \mathrm{M}_{p,q}$, $C \in \mathrm{M}_{q,s}$, $D \in \mathrm{M}_{s,t}$, et $\lambda \in \mathbb{R}$. On a les propriétés suivantes :*

(*i*) $(A + B)C = AC + BC$,

(*ii*) $A(CD) = (AC)D$,

(*iii*) $\lambda A(B) = A(\lambda B)$.

(*iv*) $(A + \lambda B)^t = A^t + \lambda B^t$,

(*v*) $(AC)^t = C^t A^t$,

Le point (*ii*) indique que le produit est associatif. Par abus, on notera souvent ABC le produit $(AB)C$. Le point (*iii*) indique que le scalaire λ "glisse" dans un produit de matrices.

1.2. L'algèbre des matrices carrées. — Soit maintenant un entier $n \geqslant 1$. On note par $\mathrm{M}_n = \mathrm{M}_{n,n}$ l'ensemble des matrices carrées $n \times n$: c'est donc l'ensemble des matrices à n lignes et n colonnes. On dit par abus que A est d'ordre (ou de taille) n. Dans la section précédente, nous avons vu que M_n peut être muni d'une loi $+$ qui en fait un groupe, d'une loi externe, mais aussi d'une seconde loi interne $\cdot$ correspondant à la multiplication. Observons que pour $A, B \in \mathrm{M}_n$, les produits AB et BA sont bien définis et donnent lieu à de nouvelles matrices de M_n.
Notons par $I_n = (a_{i,j}) \in \mathrm{M}_n$ la matrice carrée de taille $n \times n$ ayant des 1 sur la diagonale et des zéros ailleurs (ou encore $a_{i,i} = 1$ et $a_{i,j} = 0$ pour $i \neq j$).
Il est alors immédiat de voir

Proposition 1.12. — *Pour toute matrice* $\mathrm{A} \in \mathrm{M}_n$*, il vient*

$$AI_n = I_n A = A.$$

La matrice I_n est appelée *matrice identité* (de M_n).
L'ensemble M_n muni des deux lois internes et de la loi externe est une *algèbre* (sur $\mathbb{R}$; sur $\mathbb{C}$ si les coefficients sont pris dans $\mathbb{C}$). A l'exception de $n = 1$, l'algèbre M_n n'est pas commutative : pour $n \geqslant 2$, on peut trouver deux matrices $A, B \in \mathrm{M}_n$ telles que $AB \neq BA$.

Remarque 1.13. — On peut montrer que si une matrice $A \in \mathrm{M}_n$ commute avec toutes les matrices de M_n, alors $A = \lambda I_n$ pour un certain nombre réel λ.

1.2.1. Inverse d'une matrice. — Soit A une matrice de M_n. Supposons qu'il existe une matrice B de M_n telle que $AB = I_n$. De cette égalité, on en déduit alors que B est injective donc surjective (résultat qui se déduit du théorème du rang). Ainsi, il existe une matrice $C \in \mathrm{M}_n$ telle que $BC = I_n$. Par conséquent il vient $C = I_n C = (AB)C = A(BC) = AI_n = A$, et donc $BA = I_n$. Nous venons donc d'observer que $AB = I_n$ implique que $BA = I_n$. A noter que la matrice B est alors unique : en effet si C est une autre matrice de M_n telle que $AC = CA = I_n$ alors

$$B = BI_n = B(AC) = (BA)C = I_n C = C.$$

Définition 1.14. — Une matrice $A \in \mathrm{M}_n$ est dite inversible s'il existe une (unique) matrice $B \in \mathrm{M}_n$ telle que $AB = BA = I_n$. On note alors par A^{-1} une telle matrice B. La matrice A^{-1} est appelée l'inverse de A.
L'ensemble des matrices inversibles de M_n est noté Gl_n $(= \mathrm{Gl}_n(\mathbb{R})$.

Remarque 1.15. — Pour $n = 1$, l'ensemble M_1 des matrices de taille 1×1 s'identifie aux nombres réels et Gl_1 aux nombres réels non nul.

On a les propriétés suivantes :

Proposition 1.16. — *Soient $A, B \in \mathrm{Gl}_n$ et $\lambda \in \mathbb{R}\backslash\{0\}$. Alors*

(i) $AB \in \mathrm{Gl}_n$ *et* $(AB)^{-1} = B^{-1}A^{-1}$,

(ii) $\lambda A \in \mathrm{Gl}_n$ *et* $(\lambda A)^{-1} = \frac{1}{\lambda}A^{-1}$,

(iii) $A^t \in \mathrm{Gl}_n$ *et* $(A^t)^{-1} = (A^{-1})^t$.

Démonstration. — Pour le premier point, il suffit de remarquer le calcul suivant

$$(AB)(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = AI_nA^{-1} = AA^{-1} = I_n.$$

Le second point se vérifie de la même façon.
Pour le troisième point, là aussi on effectue le calcul suivant

$$A^t(A^{-1})^t = (A^{-1}A)^t = I_n^t = I_n,$$

ce qui prouve que l'inverse de A^t est bien la matrice $(A^{-1})^t$. □

Le point (i) de la proposition 1.16 montre que l'ensemble Gl_n est stable par multiplication, et que la loi $\cdot$ admet I_n comme élément neutre : ainsi, Gl_n muni de la multiplication forme un groupe (non commutatif pour $n \geqslant 2$).

1.2.2. Quelques familles de matrices. —

Définition 1.17. — Une matrice $A \in \mathrm{M}_n$ telle que $A = A^t$ est appelée matrice symétrique. On note par S_n l'ensemble des matrices symétrique des M_n.
Lorsque $A \in \mathrm{M}_n$ vérifie $A = -A^t$, on dit que A est antisymétrique. On note par A_n l'ensemble des matrices antisymétriques de M_n.

On vérifie très facilement que S_n et A_n sont des sous-espaces vectoriels de M_n.

Définition 1.18. — Une matrice A est dite triangulaire supérieure (respectivement triangulaire inférieure) si les coefficients sous (resp. au-dessus de) la diagonale sont nuls. On note par T_n^+ (resp. T_n^-) l'ensemble des matrices triangulaires supérieures (resp. inférieures). Les matrices diagonales D_n sont les éléments du sous-espace vectoriel $\mathrm{T}_n^+ \cap \mathrm{T}_n^-$: ce sont donc les matrices ayant des coefficients nuls en dehors de la diagonale.

Là aussi on vérifie très facilement que T_n^+, T_n^- et D_n sont des sous-espaces vectoriels de M_n. On a même mieux :

Proposition 1.19. — *Les ensembles* T_n^+, T_n^- *et* D_n *sont stables par somme, produit et par multiplication par un scalaire (loi externe). De plus lorsqu'une matrice* A *appartient à l'un de ces ensembles et que* A *est inversible, alors* A^{-1} *appartient au même ensemble.*

Démonstration. — La stabilité par somme, produit, et loi externe, se vérifie facilement en utilisant la définition.
Nous donnerons un peu plus tard une preuve pour l'inverse d'une matrice triangulaire (lorsqu'il existe), mais pour une matrice diagonale, c'est facile. Observons tout d'abord qu'une matrice diagonale D est inversible si et seulement si les éléments de la diagonale sont non nuls (sinon le rang est strictement plus petit que n). Soit alors D une matrice diagonale dont les éléments d_i de la diagonale sont non nuls ; on note $D = \mathrm{Diag}(d_1, \cdots, d_n) = \begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & d_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & d_n \end{pmatrix}$ une telle matrice. Soit $D' = \mathrm{Diag}(1/d_1, \cdots, 1/d_n)$. Alors on vérifie que $DD' = I_n$. □

Proposition 1.20. — *Soit* $D, D' \in \mathrm{D}_n$ *deux matrices diagonales. Alors* $DD' = D'D$.

Démonstration. — C'est assez facile. Soient $D = (d_{i,j})$ et $D' = (d'_{i,j})$. Alors si $DD' = (c_{i,j})$, la formule du produit indique que $c_{i,i} = d_{i,i}d'_{i,i} = d'_{i,i}d_{i,i}$, ce dernier produit correspond aux coefficient diagonaux du produit $D'D$. □

1.2.3. Polynômes de matrices. —

Définition 1.21. — Soit $k \in \mathbb{N}$ et soit $A \in \mathrm{M}_n$. On pose

$$A^k = \overbrace{AA\cdots A}^{k \text{ fois}}.$$

Si de plus A est inversible, on pose $A^{-k} = (A^{-1})^k$. (Avec la convention $A^0 = I_n$.)

Soit maintenant $\mathbb{R}[X]$ l'algèbre des polynômes à coefficients réels. Etant donnée $A \in \mathrm{M}_n$, on construit une application de $\mathbb{R}[X]$ vers M_n de la façon suivante :

$$\varphi_A : \begin{array}{ccc} \mathbb{R}[X] & \to & \mathrm{M}_n \\ P & \mapsto & P(A) \end{array}$$

Détaillons cette application. Si $P = a_kX^k + \cdots + a_1X + a_0 \in \mathbb{R}[X]$, la matrice $\varphi_A(P) = P(A)$ est définie par

$$P(A) = a_kA^k + \cdots + a_1A + a_0I_n,$$

avec la convention que $\varphi_A(O) = O$ (l'image du polynôme nul est la matrice nulle).
On peut vérifier que l'application φ_A respecte les sommes, produits et loi externe, et ainsi φ_A est un *morphisme* d'algèbres. C'est donc aussi une application du $\mathbb{R}$-espace vectoriel $\mathbb{R}[X]$ vers M_n. Cette observation implique le résultat suivant

Proposition 1.22. — *Etant donnée une matrice $A \in \mathrm{M}_n$, il existe un polynôme non nul $P \in \mathbb{R}[X]$ tel que $P(A) = 0$.*

Démonstration. — Partons de l'application linéaire φ_A. Comme l'espace de départ a une dimension supérieure à l'espace d'arrivée (en fait l'espace de départ est de dimension infinie et l'espace d'arrivée de dimension n^2), l'application linéaire φ_A n'est pas injective, ce qui signifie qu'il existe un polynôme $P \neq 0$ avec $P \in \ker(\varphi_A)$, ou encore que $P(A) = \varphi_A(P) = 0$. □

Donnons une première conséquence de la proposition 1.22.

Proposition 1.23. — *Soit $A \in \mathrm{M}_n$ et soit $P = a_k X^k + \cdots + a_1 X + a_0 \in \mathbb{R}[X]$ tel que $P(A) = 0$. Si le coefficient constant a_0 de P est non nul alors A est inversible. De plus*

$$A^{-1} = -\frac{a_k}{a_0}A^{k-1} - \frac{a_{k-1}}{a_0}A^{k-2} - \cdots - \frac{a_1}{a_0}I_n.$$

Démonstration. — On a la relation $a_k A^k + \cdots + a_1 A + a_0 I_n = 0$. On isole I_n et on divise par a_0 pour avoir l'identité matricielle

$$I_n = -\frac{a_k}{a_0}A^k - \frac{a_{k-1}}{a_0}A^{k-1} - \cdots - \frac{a_1}{a_0}A.$$

Dans le terme de droite on peut mettre A en facteur (à gauche ou à droite), pour obtenir

$$I_n = A\left(-\frac{a_k}{a_0}A^{k-1} - \frac{a_{k-1}}{a_0}A^{k-2} - \cdots - \frac{a_1}{a_0}I_n\right).$$

En posant $B = -\frac{a_k}{a_0}A^{k-1} - \frac{a_{k-1}}{a_0}A^{k-2} - \cdots - \frac{a_1}{a_0}I_n$, on a donc $AB = I_n$, ce qui prouve le résultat annoncé. □

Exemple 1.24. — Soit la matrice $A = \begin{pmatrix} 1 & 1 & 0 \\ -1 & 1 & 1 \\ 2 & 0 & 1 \end{pmatrix}$. Alors $A^2 = \begin{pmatrix} 0 & 2 & 1 \\ 0 & 0 & 2 \\ 4 & 2 & 1 \end{pmatrix}$ puis $A^3 = \begin{pmatrix} 0 & 2 & 3 \\ 4 & 0 & 2 \\ 4 & 6 & 3 \end{pmatrix}$. On remarque ensuite que $A^3 - 3A^2 + 4A - 4I_3 = 0$. Ainsi le polynôme $P = X^3 - 3X^2 + 4X - 4$ "s'annule en A". Comme le coefficient constant de P est non nul, on en déduit que A est inversible d'inverse

$$A^{-1} = \frac{1}{4}A^2 - \frac{3}{4}A + 4I_3 = \frac{1}{4}\begin{pmatrix} 1 & -1 & 1 \\ 3 & 1 & -1 \\ -2 & 2 & 2 \end{pmatrix}.$$

Nous préciserons un peu plus tard ce résultat, en particulier comment trouver une matrice comme dans l'exemple 1.24.

1.3. Exercices. —

Exercice 1. — *Résoudre les systèmes suivants :*

$$\left\{\begin{array}{rcl} x+y-z &=& 1 \\ 2y+z &=& 1 \\ x-y+3z &=& 0 \end{array}\right. \qquad \left\{\begin{array}{rcl} x+y+z &=& 0 \\ x-y-2z &=& 1 \\ x+3y+6z &=& 0 \end{array}\right.$$

Exercice 2. — *Soient les matrices* $A = \begin{pmatrix} 1 & 2 & 0 \\ 3 & -1 & 4 \end{pmatrix}$ *et* $B = \begin{pmatrix} 2 & 1 & -3 \\ 3 & 0 & 4 \\ 0 & -1 & -1 \end{pmatrix}$.

1. *Lorsque c'est possible, effectuer les calculs* AB, BA, A^2 *et* B^2.
2. *Calculer* A^t, AA^t *et* A^tA.

Exercice 3. — *Soit la matrice* $A = \begin{pmatrix} 1 & 1 \\ 0 & -1 \\ 1 & 0 \end{pmatrix}$.
Existe-t-il des matrices B *telles que* $BA = I_n$, n *à déterminer ? Si oui, calculer* AB.

Exercice 4. — *Soit* $n \geqslant 2$. *Donner deux matrices carrées* A *et* B *de* $\mathrm{M}_n(\mathbb{R})$ *telles que* $AB \neq BA$.

Exercice 5. — *Déterminer toutes les matrices* A *de* $\mathrm{M}_2(\mathbb{R})$ *vérifiant* $A^2 = A$. *Pour ces matrices, déterminer* A^n *pour tout entier* $n \geqslant 0$. *Déterminer une telle matrice* A *lorsqu'elle est inversible.*

Exercice 6. — *On considère la matrice* $M = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}$. *On souhaite calculer les puissances de* M. *Pour cela on note, pour* $n \geqslant 1$, $M^n = \begin{pmatrix} a_n & x_n \\ b_n & c_n \end{pmatrix}$.

1. *Déterminer les valeurs de* a_n, b_n *et* c_n *pour tout entier* $n \geqslant 1$.
2. *Montrer que* $x_{n+1} = 1 + 2x_n$ *pour tout entier* n.
3. *On note* $y_n = x_n + 1$. *Déterminer l'expression de* y_{n+1} *en fonction de* y_n.
4. *En déduire l'expression de* y_n *puis de* x_n *en fonction de* n, *et enfin l'expression de* M^n.

Exercice 7. — *Calculer la puissance* n*-ème des matrices suivantes* ($n \geqslant 1$) :

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},\ B = \begin{pmatrix} 2 & 3 \\ 0 & 0 \end{pmatrix},\ C = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix},\ D = \begin{pmatrix} -2 & 1 & 1 \\ 1 & -2 & 1 \\ 1 & 1 & -2 \end{pmatrix}.$$

Exercice 8. — *On considère la matrice* $A = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & -1 \end{pmatrix}$.

1. *Montrer que* $A^3 - 6A + 4I_4 = 0$.
2. *Montrer que* A *est inversible et calculer* A^{-1}.

Exercice 9. — *Soit la matrice à coefficients réels* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

Montrer l'existence de deux réels x *et* y *tels que* $A^2 + xA + yI_2 = 0$. *Montrer que* A *est inversible si et seulement si* $ad - bc \neq 0$. *En déduire* A^{-1} *lorsque* A *est inversible.*

Exercice 10. — *Soient les matrices* $A = \begin{pmatrix} 4 & -2 \\ 3 & -1 \end{pmatrix}$ *et* $P = \begin{pmatrix} 2 & 1 \\ 3 & 1 \end{pmatrix}$.

1. *Montrer que* P *est inversible et calculer* P^{-1}.
2. *Calculer* $P^{-1}AP$.
3. *En déduire* A^n, $n \geqslant 1$. *Quel sens peut-on donner à* A^n *pour* $n \leqslant 0$ *?*

Exercice 11. — *Soit* $A \in \mathrm{M}_n(\mathbb{R})$ *vérifiant* $A^2 - 5A + 6I_n = 0$.

1. *Donner un exemple d'une telle matrice.*
2. *Montrer que* A *est inversible et exprimer* A^{-1} *en fonction de* A.
3. *Exprimer* A^n, $n \geqslant 0$, *en fonction de* A.
4. *Exprimer* A^{-n}, $n \geqslant 0$, *en fonction de* A.

Exercice 12. —

1. *Soit la matrice* $A = \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & -1 & 1 \end{pmatrix}$. *Calculer* $(A - I_3)^n$, $n \geqslant 1$ *;* *en déduire* A^n.
2. *Soit le système récurrent* ($n \geqslant 0$)

$$\begin{cases} x_{n+1} &= x_n \\ y_{n+1} &= y_n - x_n \\ z_{n+1} &= z_n - y_n \end{cases}$$

Ecrire ce système sous forme matricielle puis exprimer (x_n, y_n, z_n) *en fonction de* (x_0, y_0, z_0).

Exercice 13. — *Déterminer les dimensions des espaces vectoriels* T_n^+, T_n^- *et* D_n.

Exercice 14. — *On note par* S_n *le sous-espace vectoriel des matrices symétriques de* $\mathrm{M}_n(\mathbb{R})$ *et par* A_n *celui des matrices anti-symétriques.*

1. *Déterminer les dimensions de* S_n *et de* A_n.
2. *Montrer que* $\mathrm{M}_n(\mathbb{R}) = \mathrm{S}_n \oplus \mathrm{A}_n$.

Exercice 15. — *On note par* $\mathscr{O}_2$ *l'ensemble des matrices* A *de* $\mathrm{M}_2(\mathbb{R})$ *vérifiant* $A^tA = I$. *Les matrices de* $\mathscr{O}_2$ *sont appelées matrices orthogonales.*

1. *Montrer que* $\mathscr{O}_2$ *n'est pas vide.*
2. *Montrer que toute matrice de* $\mathscr{O}_2$ *est inversible, et que l'ensemble* $\mathscr{O}_2$ *est stable par multiplication.*
3. *Déterminer toutes les matrices orthogonales de* $\mathscr{O}_2$.
4. *Montrer qu'une matrice orthogonale est soit une matrice de rotation soit le produit d'une matrice de rotation par une matrice d'une symétrie orthogonale.*

2. Déterminant

On fixe $n \geqslant 1$ et dans toute cette section les matrices sont des matrices de M_n (à coefficients réels par exemple).

2.1. Formes multilinéaires alternées. — Soit le $\mathbb{R}$-espace vecotriel $E = \mathbb{R}^n$. Nous notons par $\{e_1, \cdots, e_n\}$ la base canonique E.
Soit $p \geqslant 1$. Une application $F : E^p \to \mathbb{R}$ est appelée forme p-linéaire si elle est linéaire en chacune des variables. C'est à dire étant donné $i \in \{1, \cdots, p\}$ et $(X_1, \cdots, X_{i_1}, X_{i+1}, \cdots, X_p) \in E^{p-1}$, l'application $F_i : \mathbb{R} \to \mathbb{R}$ définie par $F_i(X) = F(X_1, \cdots, X_{i_1}, X, X_{i+1}, \cdots, X_p)$ est linéaire.

Remarque 2.1. — Quand $p = 1$, cela signifie simplement que F est linéaire. Quand $p = 2$, les applications 2-linéaires sont les formes bilinéaires sur E.

Une forme p-linéaire est dite *alternée* si $F(X_1, \cdots, X_p) = 0$ dès qu'il existe $i \neq j$ tels que $X_i = X_j$. Une forme alternée est *anti-symétrique* : pour tout $i < j$ il vient $F(X_1, \cdots, X_i, \cdots, X_j, \cdots, X_p) = -F(X_1, \cdots, X_j, \cdots, X_i, \cdots, X_p)$. En effet, il suffit de partir de $0 = F(X_1, \cdots, X_i + X_j, \cdots, X_j + X_i, \cdots, X_p)$ puis d'utiliser la linéarité de F. De cette façon, on montre aussi qu'une forme anti-symétrique est alternée.
L'ensemble des formes p-linéaires alternées forme un espace vectoriel sur $\mathbb{R}$, noté $\mathrm{Alt}_p(E)$.

Exemple 2.2. — Soit $E = \mathbb{R}e_1 \simeq \mathbb{R}$. Prenons $p = 2$. Alors pour $v, w \in E$, il existe $a, b \in \mathbb{R}$ tel que $v = ae_1$ et $w = be_1$. Soit alors $F \in \mathrm{Alt}_p(E)$, il vient $F(v, w) = abF(e_1, e_1) = 0$. La 2-forme est donc nulle.

L'observation de l'exemple 2.2 s'étend facilement pour montrer que $\mathrm{Alt}_p(E) = \{0\}$ pour $p > n$.
Intéressons nous maintenant au cas où $p = n$.

Exemple 2.3. — Soit $E = \mathbb{R}e_1 \oplus \mathbb{R}e_2 \simeq \mathbb{R}^2$ et soit $F \in \mathrm{Alt}_2(E)$. Soit $v = ae_1 + be_2$ et $w = ce_1 + de_2$ des vecteurs de E avec $a, b, c, d \in \mathbb{R}$. Il vient alors

$$\begin{aligned} F(v,w) &= F(ae_1 + be_2, ce_1 + de_2) \\ &= acF(e_1,e_1) + adF(e_1,e_2) + bcF(e_2,e_1) + bdF(e_2,e_2) \\ &= adF(e_1,e_2) - bcF(e_1,e_2) \\ &= (ad - bc)F(e_1,e_2) \end{aligned}$$

Soit alors l'application Δ_2 de $\mathbb{R}^2 \to \mathbb{R}$ définie par

$$\Delta_2\Big(\begin{pmatrix} a \\ b \end{pmatrix}, \begin{pmatrix} c \\ d \end{pmatrix}\Big) = ad - bc.$$

Il est assez immédiat de voir que Δ_2 est une 2-forme linéaire alternée sur $\mathbb{R}^2$, et que Δ_2 est non nulle (en effet $\Delta_2\Big(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}\Big) = 1$). Le calcul précédent montre que $F = F(e_1, e_2)\Delta_2$, et ainsi $\mathrm{Alt}_2 = \langle \Delta_2 \rangle$, c'est à dire que Alt_2 est un $\mathbb{R}$-espace vectoriel de dimension 1 engendré par la 2-forme Δ_2.

Exemple 2.4. — Soit $E = \mathbb{R}e_1 \oplus \mathbb{R}e_2 \oplus \mathbb{R}e_3 \simeq \mathbb{R}^3$ et soit $f \in \mathrm{Alt}_3(E)$. Soit $u = ae_1 + be_2 + ce_3$, $v = de_1 + fe_2 + ge_3$, $w = he_1 + ie_2 + je_3$ des vecteurs de E avec $a, b, \cdots, i, j \in \mathbb{R}$. Avec un calcul similaire au calcul de l'exemple précédent il vient

$$F(u,v,w) = a(fj - gi) - b(dj - hg) + c(di - fh)F(e_1, e_2, e_3).$$

Soit l'application Δ_3 de $\mathbb{R}^3 \to \mathbb{R}$ définie par

$$\Delta_3\Big(\begin{pmatrix} a \\ b \\ c \end{pmatrix}, \begin{pmatrix} d \\ f \\ g \end{pmatrix}, \begin{pmatrix} h \\ i \\ j \end{pmatrix}\Big) = a(fj - gi) - b(dj - hg) + c(di - fh).$$

Il est assez immédiat de voir que Δ_3 est une 3-forme linéaire alternée sur $\mathbb{R}^3$, également non nulle (car $\Delta_3\Big(\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}\Big) = 1$). Ainsi $\mathrm{Alt}_3 = \langle \Delta_3 \rangle$.

Plus généralement, on peut montrer que Alt_n est un espace vectoriel de dimension 1 engendré par une n-forme Δ_n, avec $\Delta_n(e_1, \cdots, e_n) = 1$, où $\{e_1, \cdots, e_n\}$ est la base canonique de $\mathbb{R}^n$. En particulier pour toute forme n-linéaire alternée F sur $E = \mathbb{R}^n$, on a

(1) $$F = F(e_1, \cdots, e_n)\Delta_n.$$

2.2. Définition et propriétés. — Soit $A \in \mathrm{M}_n$. Ecrivons alors A en fonction de ses colonnes $C_{A,i} \in \mathbb{R}^n$, ou encore $A = \big[C_{A,1} | \cdots | C_{A,n}\big]$, écriture de A par blocs (ici $C_{A,i}$ désigne la i-ème colonne de A). Soit alors Δ_n la n-forme alternée sur $\mathbb{R}^n$ valant 1 sur la base canonique $\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \cdots \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$.

Définition 2.5. — Soit la matrice $A = \big[C_{A,1}|\cdots|C_{A,n}\big]$. La quantité $\Delta_n\big(C_{A,1},\cdots,C_{A,n}\big)$ est le déterminant de la matrice A. On la note $\det A$ ou encore $|A|$. Par abus on notera aussi : $\det A = \det[C_{A,1}|\cdots|C_{A,n}]$.

Exemple 2.6. — On a $\det(a) = a\det(1) = a$, $\det\begin{pmatrix} a & c \\ b & d \end{pmatrix} = ad - bc$ et $\det\begin{pmatrix} a & d & h \\ b & f & i \\ c & g & j \end{pmatrix} = a(fj - gi) - b(dj - hg) + c(di - fh)$.

Exemple 2.7. — On a $\det I_n = \Delta_n(e_1,\cdots,e_n) = 1$.

Commençons par donner des propriétés immédiates se déduisant du fait que Δ_n est une n-forme alternée.

Proposition 2.8. — *Soit une matrice $A = \big[C_1|\cdots|C_n\big] \in \mathrm{M}_n$, où l'on note $C_i = C_{A,i}$.*

(i) La linéarité de Δ_n implique que pour tout vecteur $U \in \mathbb{R}^n$,

$$\det\big[C_1|\cdots|C_i + U|\cdots|C_n\big] = \det\big[C_1|\cdots|C_i|\cdots|C_n\big] + \det\big[C_1|\cdots|U|\cdots|C_n\big].$$

(ii) Si l'on ajoute à une colonne une combinaison linéaire des autres colonnes alors le déterminant reste constant. En particulier lorsque l'on ajoute à C_i un multiple de C_j, pour $i \neq j$

$$\det\big[C_1|\cdots|C_i + \lambda C_j|\cdots|C_j|\cdots|C_n\big] = \det\big[C_1|\cdots|C_i|\cdots|C_j|\cdots C_n\big].$$

(iii) Si l'on multiplie une colonne par un scalaire λ, alors le déterminant est multiplié par λ :

$$\det\big[C_1|\cdots|\lambda C_i|\cdots|C_n\big] = \lambda\det\big[C_1|\cdots|C_i|\cdots|C_n\big].$$

Ainsi il vient : $\det(\lambda A) = \lambda^n \det A$.

(iv) Si l'on permute deux colonnes le déterminant change de signe

$$\det\big[C_1|\cdots|C_i|\cdots|C_j|\cdots|C_n\big] = -\det\big[C_1|\cdots|C_j|\cdots|C_i|\cdots|C_n\big].$$

Il se pose alors naturellement la question de savoir ce qui se passe si dans la proposition 2.8 l'on regarde les lignes plutôt que les colonnes : les résultats sont identiques, cela repose sur le résultat suivant

Proposition 2.9. — *Soit $A \in \mathrm{M}_n$. Alors* $\det A = \det A^t$.

Démonstration. — Etant donnée une matrice $A \in \mathrm{M}_n$, on écrit A sous la forme "lignes" $A = \begin{bmatrix} \frac{L_{A,1}}{\vdots} \\ \hline L_{A,n} \end{bmatrix}$. Ainsi $A^t = \big[L^t_{A,1}|\cdots|L^t_{A,n}\big]$. Soit alors l'application $G : \mathrm{M}_n \to \mathbb{R}$ définie comme suit :

$$\begin{array}{rcl} G : \mathrm{M}_n & \longrightarrow & \mathbb{R} \\ \left[\begin{array}{c} L_{A,1} \\ \hline \vdots \\ \hline L_{A,n} \end{array}\right] & \mapsto & \det\big[L^t_{A,1}|\cdots|L^t_{A,n}\big]. \end{array}$$

Il est facile de voir que G est une n-forme alternée sur $\mathbb{R}^n$, ainsi G est proportionnelle à la forme Δ_n. Il existe $\lambda \in \mathbb{R}$ tel que $G = \lambda\Delta_n$. Or pour $A = I_n$, il vient $G(I_n) = 1$ et $\det I_n = 1$. On en déduit donc que $\lambda = 1$. Ainsi $G = \Delta_n$, ou encore $G = \det$. On conclut en observant que $G(A) = \det A^t$. □

Dans la preuve de la proposition 2.9 nous avons utilisé le fait que Alt_n est un espace vectoriel de dimension 1, engendré par la forme Δ_n (ou encore par abus det). Cette propriété nous permet également de montrer les deux théorèmes à venir.

Théorème 2.10. — *On a* $\det A = 0$ *si et seulement si la matrice* A *est inversible.*

Démonstration. — Supposons la matrice non inversible. Cela signifie donc qu'il existe une relation linéaire entre les colonnes de A, et comme det est une forme alternée (en les colonnes des matrices de M_n), on en déduit que $\det A = 0$.
Réciproquement. Si A est inversible, cela signifie que les colonnes C_i $(= C_{A,i})$ de A forment une base B' de $\mathbb{R}^n$. Soit alors $\Delta_{\mathrm{B}'}$ la forme n-linéaire alternée relativement à cette base : $\Delta_{\mathrm{B}'}$ est une (en fait "la") n-forme linéaire sur les vecteurs de $\mathbb{R}^n$ dans exprimés dans la base B' (qui vaut 1 en $(C_1, \cdots, C_n)$). Alors comme pour Δ_n (voir l'égalité (1)), on a que pour tout $F \in \mathrm{Alt}_n$:

$$F = F\big(C_1, \cdots, C_n\big)\Delta_{\mathrm{B}'}.$$

Si l'on prend $F = \Delta_n$, il vient $\Delta_n = \Delta_n(C_1, \cdots, C_n)\Delta_{\mathrm{B}'}$ et comme Δ_n est une forme non nulle, on en déduit que $\Delta_n\big(C_1, \cdots, C_n\big) \neq 0$, et donc $\det A \neq 0$. □

Théorème 2.11. — *Pour toutes matrices* $A, B \in \mathrm{M}_n$, *il vient*

$$\det(AB) = \det A \times \det B.$$

Démonstration. — Cela va reposer sur le lemme suivant

Lemme 2.12. — *Soit* $A = \big[C_{A,1}|\cdots|C_{A,n}\big] \in \mathrm{M}_n$ *et soit* $F \in \mathrm{Alt}_n$.
Alors $G : (X_1, \cdots, X_n) \mapsto F(AX_1, \cdots, AX_n)$ *est une* n*-forme alternée sur* $\mathbb{R}^n$, *et* $G = F(C_{A,1}, \cdots, C_{A,n}) \cdot \Delta_n$.

Démonstration. — Le fait que G soit une forme alternée est immédiat. Ainsi, comme Alt_n est de dimension 1 engendré par Δ_n, il existe $\lambda \in \mathbb{R}$ tel que $G = \lambda\Delta_n$. On évalue ensuite cette égalité en la base canonique $\{e_1, \cdots, e_n\}$, et on conclut en notant que $Ae_i = A_i$. □

Donnons la preuve du théorème 2.11. Par définition, $\det(AB) = \Delta_n(AC_{B,1}, \cdots, AC_{B,n})$, où $B = \big[C_{B,1}|\cdots|C_{B,n}\big]$. Par le lemme 2.12, il vient ainsi (en prenant $F = \Delta_n$)

$$\det(AB) = \Delta_n(C_{A,1}, \cdots, C_{A,n})\Delta_n(C_{B,1}, \cdots, C_{B,n}) = \det A \times \det B.$$

□

Corollaire 2.13. — *Soit* $A, B \in \mathrm{M}_n$. *Alors* $\det(AB) = \det(BA)$.

Démonstration. — En effet $\det(AB) = \det A \cdot \det B = \det B \cdot \det A = \det(BA)$. □

Corollaire 2.14. — *Soit* $A \in \mathrm{Gl}_n$. *Alors* $\det A^{-1} = \dfrac{1}{\det A}$.

Démonstration. — Comme $AA^{-1} = I_n$, par le théorème 2.11, il vient

$$\det A \det(A^{-1}) = \det I_n = 1,$$

d'où le résultat. □

2.3. Développement d'un déterminant. — Le fait que Alt_n soit de dimension 1 va permettre de donner également une règle de calcul du déterminant. Commençons par le cas d'une matrice par blocs.

Théorème 2.15. — *Soit une matrice par blocs* $A = \left[\begin{array}{c|c} R & S \\ \hline O & T \end{array}\right]$, *où* $R \in \mathrm{M}_r$ *et* $T \in \mathrm{M}_t$ *sont deux matrices carrées (non nécessairement de même taille), et* O *est une matrice composée uniquement de* 0. *Alors* $\det A = \det R \times \det T$.

Démonstration. — Soit S et T fixées, alors l'application $F : X \in \mathrm{M}_r \mapsto \det \left[\begin{array}{c|c} X & S \\ \hline O & T \end{array}\right]$ est une r-forme alternée sur $\mathbb{R}^r$ (par rapport aux colonnes de X). Ainsi, $F(X) = \lambda \Delta_r$, et en prenant $X = I_r$, on obtient que $\lambda = F(I_r)$ puis que $F(R) = F(I_r) \times \det R$.
Ensuite fixons S. Alors l'application $G : Y \in \mathrm{M}_s \mapsto \det \left[\begin{array}{c|c} I_r & S \\ \hline O & Y \end{array}\right]$ est une t-forme alternée sur $\mathbb{R}^t$, par rapport aux lignes de Y. Ainsi, $G(Y) = \beta \Delta_t$, et en prenant $Y = I_t$, on obtient $\beta = G(I_t)$.
Au final, on a donc

$$\det A = F(R) = \det R \times F(I_r) = \det R \times G(T) = \det R \times G(I_t) \times \det T.$$

Or $G(I_t) = \det \left[\begin{array}{c|c} I_r & S \\ \hline O & I_t \end{array}\right]$. Une simple manipulation sur les colonnes de S en fonction des premières colonnes montre que $G(I_t)$ est égal à $\det \left[\begin{array}{c|c} I_r & O \\ \hline O & I_t \end{array}\right]$ (en utilisant la proposition 2.8 (ii)), c'est à dire au déterminant de la matrice identité qui vaut 1. □

Par induction, on en déduit immédiatement le corollaire suivant :

Corollaire 2.16. — *Soit* $A = (a_{i,j}) \in \mathrm{T}_n^+$ *une matrice triangulaire supérieure (ou inférieure, ou diagonale). Alors* $\det A = a_{1,1}a_{2,2}\cdots a_{n,n}$. *En d'autres termes, le déterminant de* A *est égal au produit des éléments de la diagonale. En particulier une matrice triangulaire supérieure (ou inférieure, ou diagonale) est inversible si et seulement si tous les éléments de la diagonale sont non nuls.*

Définition 2.17. — Soit $A = (a_{i,j}) \in \mathrm{M}_n$. Etant donnés $i, j \in \{1, \cdots, n\}$, notons par $A_{i,j}$ la matrice carrée de taille $(n-1) \times (n-1)$ obtenue à partir de A en retirant la i-ème ligne et j-ème colonne. On note par $\Delta_{i,j}$ le déterminant de $A_{i,j}$: c'est le mineur de $a_{i,j}$. La quantité $(-1)^{i+j}\Delta_{i,j}$ est appelé cofacteur.

Théorème 2.18. — *Soit $A = (a_{i,j}) \in \mathrm{M}_n$. Soit $i \in \{1, \cdots, n\}$ fixé. Alors (développement par rapport à la i-ème ligne)*

$$\det A = \sum_{j=1}^{n} (-1)^{i+j} a_{i,j} \Delta_{i,j},$$

et (développement par rapport à la i-ème colonne)

$$\det A = \sum_{j=1}^{n} (-1)^{i+j} a_{j,i} \Delta_{j,i}.$$

Démonstration. — On passe du développement par rapport à une ligne au développement par rapport à une colonne en utilisant la proposition 2.9. Donnons la preuve pour le développement par rapport à la i-ème colonne. Par le point (iv) de la proposition 2.8, il vient

$$\begin{aligned} \det A &= \det\left[C_{A,1}|\cdots|C_{A,i}|\cdots|C_{A,n}\right] \\ &= (-1)^{i-1} \det\left[C_{A,i}|C_{A,1}|\cdots|C_{A,i-1}|C_{A,i+1}|\cdots|C_{A,n}\right] \\ &= (-1)^{i-1} \begin{vmatrix} a_{1,i} & a_{1,1} & \cdots & a_{1,n} \\ a_{2,i} & a_{2,1} & \cdots & a_{n,1} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n,i} & a_{n,1} & \cdots & a_{n,n} \end{vmatrix} \end{aligned}$$

On utilise ensuite la linéraité par rapport à la première colonne (voir la proposition 2.9 (i)), pour arriver à

$$\det A = (-1)^{i-1} \left(\begin{vmatrix} a_{1,i} & a_{1,1} & \cdots & a_{1,n} \\ 0 & a_{2,1} & \cdots & a_{n,1} \\ 0 & \vdots & \vdots & \vdots \\ 0 & a_{n,1} & \cdots & a_{n,n} \end{vmatrix} + \begin{vmatrix} 0 & a_{1,1} & \cdots & a_{1,n} \\ a_{2,i} & a_{2,1} & \cdots & a_{n,1} \\ 0 & \vdots & \vdots & \vdots \\ 0 & a_{n,1} & \cdots & a_{n,n} \end{vmatrix} + \cdots + \begin{vmatrix} 0 & a_{1,1} & \cdots & a_{1,n} \\ \vdots & a_{2,1} & \cdots & a_{n,1} \\ 0 & \vdots & \vdots & \vdots \\ a_{n,i} & a_{n,1} & \cdots & a_{n,n} \end{vmatrix} \right).$$

Soit $j \in \{1, \cdots, n\}$ fixé. On a

$$\begin{vmatrix} 0 & a_{1,1} & \cdots & a_{1,n} \\ \vdots & a_{2,1} & \cdots & a_{n,1} \\ a_{j,i} & \vdots & \vdots & \vdots \\ 0 & a_{n,1} & \cdots & a_{n,n} \end{vmatrix} = (-1)^{j-1} \begin{vmatrix} a_{j,i} & a_{j,1} & \cdots & a_{j,n} \\ 0 & a_{1,1} & \cdots & a_{1,n} \\ \vdots & \vdots & \vdots & \vdots \\ 0 & a_{n,1} & \cdots & a_{n,n} \end{vmatrix}$$

après avoir ramené la j-ème ligne en première ligne. Or d'après le théorème 2.15, il vient

$$\begin{vmatrix} a_{j,i} & a_{j,1} & \cdots & a_{j,n} \\ 0 & a_{1,1} & \cdots & a_{1,n} \\ \vdots & \vdots & \vdots & \vdots \\ 0 & a_{n,1} & \cdots & a_{n,n} \end{vmatrix} = a_{k,i} \begin{vmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \vdots & \vdots \\ a_{n,1} & \cdots & a_{n,n} \end{vmatrix} = a_{j,i} \Delta_{j,i},$$

car en effet la dernière matrice s'obtient à partir de A en retirant la i-ème colonne et j-ème ligne. Il vient ainsi

$$\det A = \sum_{j=1}^{n} (-1)^{i-1+j-1} a_{j,i} \Delta_{j,i} = \sum_{j=1}^{n} (-1)^{i+j} a_{j,i} \Delta_{j,i}.$$

□

Exemple 2.19. — Soit $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$. En développant par rapport à la première ligne, on obtient

$$\det A = a\Delta_{1,1} - c\Delta_{1,2},$$

où ici $\Delta_{1,1} = \det(d)$ et $\Delta_{1,2} = \det(b)$. Or le déterminant d'une matrice $B = (\lambda)$ est égal à $\lambda \det(1) = \lambda$. D'où $\det A = ad - bc$. On retrouve le calcul bien connu du déterminant d'une matrice 2×2 (voir exemple 2.6).

Exemple 2.20. — Dans l'exemple 2.6 la formule pour $n = 3$ s'obtient en faisant un développement par rapport à la première colonne (et en utilisant la formule pour $n = 2$.)

A l'image de ces exemples, la formule du théorème 2.18 permet donc de calculer le déterminant d'une matrice de taille $n \times n$.

Exemple 2.21. — Soit $A = \begin{pmatrix} 1 & 1 & -1 & 1 \\ 1 & 0 & 2 & 1 \\ -1 & 2 & 2 & 0 \\ 2 & 1 & 0 & -1 \end{pmatrix} = \big[C_1 | \cdots | C_n\big]$. On veut calculer $\det A$.

Faisons une première opération qui consiste à mettre le plus de zéros possible sur la première ligne. Pour cela on remplace la colonne C_2 par $C_2 - C_1$, C_3 par $C_3 + C_1$ et C_4 par $C_4 - C_1$. Avec ces opérations le déterminant ne change pas (par la proposition 2.8 (ii)). Ainsi

$$\det A = \begin{vmatrix} 1 & 0 & 0 & 0 \\ 1 & -1 & 3 & 0 \\ -1 & 3 & 1 & 1 \\ 2 & 1 & 1 & -2 \end{vmatrix}.$$

Puis on développe par rapport à la première ligne pour obtenir

$$\det A = \begin{vmatrix} -1 & 3 & 0 \\ 3 & 1 & 1 \\ 1 & 1 & -2 \end{vmatrix}.$$

On développe à nouveau par rapport à la première ligne pour arriver à

$$\det A = (-1)\begin{vmatrix} 1 & 1 \\ 1 & -2 \end{vmatrix} - 3\begin{vmatrix} 3 & 1 \\ 1 & -2 \end{vmatrix} = -(-2-1) - 3(-6-1) = 24.$$

2.4. Applications. —

2.4.1. Calul du rang d'une matrice. — Commençons par rappeler la notion du rang d'une matrice.

Définition 2.22. — Soit $A \in \mathrm{M}_{p,q}$. Le rang de A est la dimension de l'espace vectoriel engendré par les vecteurs colonnes. On note par $\mathrm{rg}A$ cette quantité.

On rappelle que le théorème du rang indique que $q = \dim \ker A + \mathrm{rg}A$. La technique de réduction d'une matrice en une forme échelonnée réduite permet de montrer le théorème suivant

Théorème 2.23. — *Soit $A \in \mathrm{M}_{p,q}$. Il existe $P \in \mathrm{Gl}_p$ et $Q \in \mathrm{Gl}_q$ telles que*

$$A = P \left[\begin{array}{c|c} I_r & O_{r,q-r} \\ \hline O_{p-r,r} & O_{p-r,q-r} \end{array}\right] Q,$$

où I_r désigne la matrice identité de taille $r \times r$, et où $O_{i,j} \in \mathrm{M}_{i,j}$ est la matrice composée uniquement de 0. Un tel entier r est unique, il est égal au rang de A.

Comme conséquence, il vient

Corollaire 2.24. — *Soit $A \in \mathrm{M}_{p,q}$. Alors $\mathrm{rg}A = \mathrm{rg}A^t$. En particulier $\mathrm{rg}A \leqslant \min\{p, q\}$.*

Démonstration. — Passer à la transposée la décomposition de A du théorème 2.23, puis utiliser l'unicité de l'entier r $(= \mathrm{rg}A)$. □

Définition 2.25. — Soit $A \in \mathrm{M}_{p,q}$. Une matrice extraite B de A est une matrice obtenue à partir de A après suppression de lignes et de colonnes. On appelle déterminant extrait de A le déterminant $\det B$ d'une matrice extraite B de A.

On a le théorème suivant

Théorème 2.26. — *Soit $A \in \mathrm{M}_{p,q}$. Alors le rang de A est le plus grand entier k tel qu'il existe une matrice carrée extraite B de A de taille $k \times k$, avec $\det B \neq 0$.*

Démonstration. — Soit k_0 le maximum des entiers k pour lesquels il existe un déterminant extrait non nul de taille k.
• Soit une matrice extraite B de taille $k \times k$ de déterminant non nul. Alors les colonnes de B ne sont pas liées, ce qui implique que les colonnes de A "correspondantes" aux colonnes de B ne sont pas liées et ainsi $\mathrm{rg}A \geqslant k$. Ainsi $\mathrm{rg}A$ est plus grand que k_0.
• Soit $r = \mathrm{rg}A$. Alors il existe r colonnes $C_{i_1}, \cdots, C_{i_r}$ de $A = \left[C_1 | \cdots | C_n\right]$ qui sont linéairement indépendantes. Ainsi la matrice extraite $B = \left[C_{i_1} | \cdots | C_{i_r}\right]$ est de rang r. La matrice B^t est de même rang r, ce qui signifie que l'on peut alors extraire r lignes de B indépendantes. La matrice finale obtenue est une matrice extraite B' de taille $r \times r$ et de rang r, donc de déterminant non nul. Ainsi $k_0 \geqslant \mathrm{rg}A$, d'où l'égalité recherchée. □

Exemple 2.27. — Soit la matrice $A = \begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & 1 & 3 & 2 \end{pmatrix}$. Le rang de A est plus petit que 3 (le nombre de lignes de A). On calcule le déterminant extrait correspondant à la matrice 3×3 obtenue à partir de A après suppression de la dernière colonne : $\begin{vmatrix} 2 & 3 & 1 \\ 1 & 1 & -1 \\ 1 & 1 & 3 \end{vmatrix} = -4 \neq 0$. Ainsi $\mathrm{rg}A = 3$.

2.4.2. Inverse d'une matrice. —

Définition 2.28. — Soit $A \in \mathrm{M}_n$ et soient $(-1)^{i+j}\Delta_{i,j}$ ses cofacteurs (voir la définition 2.17). La matrice carrée d'ordre n dont le (i, j) ème coefficient est $(-1)^{i+j}\Delta_{i,j}$ est appelée comatrice de A (ou matrice des cofacteurs) et est notée $\mathrm{com}A$.

On a alors le théorème suivant

Théorème 2.29. — *Soit $A \in \mathrm{M}_n$. Alors $(\mathrm{com}A)^t A = A(\mathrm{com}A)^t = (\det A) I_n$. En particulier si A est inversible alors*

$$A^{-1} = \frac{1}{\det A}(\mathrm{com}A)^t.$$

Démonstration. — Ecrivons $A = (a_{i,j})$ et $(\mathrm{com}A)^t = (b_{i,j})$. Ainsi, $b_{i,j} = (-1)^{i+j}\Delta_{j,i}$. Soit $i, j \in \{1, \cdots, n\}$, alors

$$\left[(\mathrm{com}A)^t A\right]_{i,j} = \sum_{k=1}^{n} b_{i,k} a_{k,j} = \sum_{k=1}^{n} a_{k,j}(-1)^{i+k}\Delta_{k,i}.$$

Quand $i = j$, il vient

$$\left[(\mathrm{com}A)^t A\right]_{i,i} = \sum_{k=1}^{n} a_{k,i}(-1)^{i+k}\Delta_{k,i}.$$

Observons alors que $\sum_{k=1}^{n} a_{k,i}(-1)^{i+k}\Delta_{k,i}$ correspond au calcul de $\det A$ par rapport à la i-ème colonne. Ainsi $\left[(\mathrm{com}A)^t A\right]_{i,i} = \det A$.
Quand $i \neq j$. Dans la matrice A, remplaçons la i-ème colonne par la j-ème colonne pour obtenir une matrice A' qui a donc deux colonnes identiques (et ainsi $\det A' = 0$). Si l'on calcule $\det A'$ en effectuant le développement par rapport à la i-ème colonne, il vient exactement $\det A' = \sum_{k=1}^{n} a_{k,j}(-1)^{i+k}\Delta_{k,i}$.
Au final, on obtient bien $(\mathrm{com}A)^t A = (\det A) I_n$. Le second calcul s'obtient de la même façon. □

Exemple 2.30. — Soit $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$. Alors $\mathrm{com}A = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ et si A est inversible il vient

$$A^{-1} = \frac{1}{ad - bc}\begin{pmatrix} d & -c \\ -b & a \end{pmatrix}.$$

2.4.3. Formules de Cramer. — Soit un système linéaire de taille $n \times n$

$$AX = Y,$$

avec $Y \in \mathbb{R}^n$ donné. Notons $X = (x_1, \cdots, x_n)$ le vecteur inconnu.
On suppose $\det A \neq 0$. Le système a donc une unique solution. Ecrivons $A = \left[C_1 | \cdots | C_n\right]$. Alors

$$Y = x_1 C_1 + \cdots + x_n C_n.$$

Par conséquent, par linéarité de la forme déterminant, il vient

$$\det\left[Y | C_2 | \cdots | C_n\right] = \sum_{i=1}^{n} x_i \det\left[C_i | C_2 | \cdots | C_n\right] = x_1 \det A,$$

car pour $i > 1$, on a $\det\left[C_i | C_2 | \cdots | C_n\right] = 0$ (on retrouve deux fois la même colonne). Ainsi

$$x_1 = \frac{\det\left[Y | C_2 | \cdots | C_n\right]}{\det A}.$$

En réitérant cette démarche pour les autres x_i, nous venons de montrer le résultat suivant

Théorème 2.31. — *Soit* $A = \left[C_1|\cdots|C_n\right] \in \mathrm{Gl}_n$. *Alors la solution* $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ *du système* $AX = Y$ *s'écrit*

$$x_i = \frac{\det\left[C_1|\cdots|C_{i-1}|Y|C_{i+1}|\cdots|C_n\right]}{\det A},$$

$i = 1, \cdots, n$.

Exemple 2.32. — Soient $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$, $Y = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ et le système $AX = Y$, avec $X = \begin{pmatrix} x \\ y \end{pmatrix}$. Supposons $ad - bc \neq 0$. Alors

$$x = \frac{\alpha d - \beta c}{ad - bc}, \quad y = \frac{\alpha b - a\beta}{ad - bc}.$$

Remarque 2.33. — Remarquons que la seconde partie du théorème 2.29 peut se déduire des formules de Cramer du théorème 2.31.

2.5. Exercices. —

Exercice 16. — *Calculer les déterminants des matrices suivantes et déterminer celles qui sont inversibles :*

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix} \qquad B = \begin{pmatrix} 3 & -1 & 1 \\ 6 & 2 & 1 \\ 3 & -1 & 1 \end{pmatrix} \qquad C = \begin{pmatrix} 1 & -1 & 1 \\ -1 & 2 & 3 \\ 1 & 1 & 1 \end{pmatrix}$$

$$D = \begin{pmatrix} -5 & -6 & 12 \\ -1 & 0 & 3 \\ 1 & -3 & 1 \end{pmatrix} \qquad E = \begin{pmatrix} 6 & 0 & 0 & 5 \\ 1 & 7 & 2 & -5 \\ 2 & 0 & 0 & 0 \\ 8 & 3 & 1 & 8 \end{pmatrix} \qquad F = \begin{pmatrix} 1 & 0 & 3 & -1 \\ 1 & 2 & 2 & -3 \\ 1 & 0 & 1 & 5 \\ 6 & 3 & -3 & 4 \end{pmatrix}.$$

Exercice 17. — *Calculer* $\begin{vmatrix} 1+a & a & a \\ b & 1+b & b \\ c & c & 1+c \end{vmatrix}$.

Exercice 18. — *A quelles conditions les matrices suivantes sont-elle inversibles ?*

$$A = \begin{pmatrix} \lambda & -3 \\ 3 & -\lambda \end{pmatrix} \qquad B = \begin{pmatrix} \lambda & 0 & 2 \\ -1 & \lambda & 3 \\ 2 & 0 & \lambda \end{pmatrix} \qquad C = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & -1 \\ \lambda & 0 & 0 & 1 \end{pmatrix}$$

Exercice 19. — *1) A quelles conditions les matrices suivantes sont-elle inversibles ?*

$$A = \begin{pmatrix} 1 & 1 \\ a & b \end{pmatrix} \qquad B = \begin{pmatrix} 1 & 1 & 1 \\ a & b & c \\ a^2 & b^2 & c^2 \end{pmatrix}.$$

2) Donner une généralisation.

Exercice 20. — *Déterminer le rang des matrices suivantes*

$$A = \begin{pmatrix} 2 & 1 & 3 & 1 \\ 1 & 3 & 1 & a \\ 1 & 3 & 1 & -1 \end{pmatrix}, \quad B = \begin{pmatrix} 3 & 1 & 1 & 1 \\ 1 & -2 & 5 & a \\ 1 & 1 & -1 & 1 \end{pmatrix}.$$

Exercice 21. — *Soit la famille* $\mathrm{B} = \{\begin{pmatrix} 1 \\ 1 \\ t \end{pmatrix}, \begin{pmatrix} 1 \\ t \\ 1 \end{pmatrix}, \begin{pmatrix} t \\ 1 \\ 1 \end{pmatrix}\}$. *A quelle condition sur* $t \in \mathbb{R}$ *la famille* B *est-elle une base de* $\mathbb{R}^3$ *?*

Exercice 22. — *Calculer les inverses des matrices suivantes*

$$A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \qquad B = \begin{pmatrix} 2 & 7 & 3 \\ 3 & 9 & 4 \\ 1 & 5 & 3 \end{pmatrix} \qquad C = \begin{pmatrix} 1 & \lambda & 0 & 0 \\ 0 & 1 & \lambda & 0 \\ 0 & 0 & 1 & \lambda \\ 0 & 0 & 0 & 1 \end{pmatrix} \lambda \in \mathbb{R}.$$

Exercice 23. — *Discuter suivant les deux réels* a *et* α *la résolution du système linéaire :*

$$\begin{cases} 3x + y - z = 1 \\ x - 2y + 2z = \alpha \\ x + ay - z = 1 \end{cases}$$

3. Diagonalisation

Dans toute cette section, les matrices seront prises dans l'espace M_n (espace des matrices carrées) pour un certain entier $n \geqslant 1$.

3.1. Polynôme caractéristique. — Soit $A \in \mathrm{M}_n$. Considérons alors la matrice de M_n suivante : $XI_n - A$, où X est une indéterminée (X a les mêmes propriétés qu'un scalaire).

Si $A = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & \cdots & a_{n,n} \end{pmatrix}$ alors $A - XI_n = \begin{pmatrix} a_{1,1} - X & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} - X & \cdots & a_{2,1} \\ \vdots & \cdots & \ddots & \vdots \\ a_{n,1} & \cdots & \cdots & a_{n,n} - X \end{pmatrix}$.

Définition 3.1. — Soit $A \in \mathrm{M}_n$. On définit le polynôme caractéristique de A comme le polynôme $P_A(X) = \det(XI_n - A)$.

Exemple 3.2. — Pour $n = 1$, $A = (a)$, alors $P_A = X - A$.

Pour $n = 2$, $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$, alors

$$P_A = \begin{vmatrix} X - a & -c \\ -b & X - d \end{vmatrix} = (X - a)(X - d) - bc = X^2 - (a + d)X + ad - bc.$$

Pour une matrice $A \in \mathrm{M}_n$, la *trace* est la somme des éléments de la diagonale. On note $\mathrm{Tr}A$ cette quantité. Observons alors que pour $n = 2$, il vient $P_A = X^2 - \mathrm{Tr}A\, X + \det A$.

Proposition 3.3. — *Soient $A \in \mathrm{M}_n$ et P_A son polynôme caractéristique. Alors P_A est un polynôme unitaire de degré n et de coefficient constant $(-1)^n \det A$.*

Démonstration. — On montre par réccurence que

(i) le déterminant extrait de toute sous-matrice de $XI_n - A$ de taille $(n-1) \times (n-1)$ est un polynôme de degré plus petit que $n - 1$,

(ii) que si $A \in \mathrm{M}_n$, alors $P_A = \det(XI_n - A)$ est de degré n.

Le résultat est vrai pour $n = 1$. Supposons le résultat vrai à l'ordre $n-1$. En développant par rapport à la premièr colonne on voit que $\det(XI_n - A) = \pm(X - a_{1,1})\Delta_{1,1} + R(X)$, où R est un polynôme de degré au plus $n-1$ (par l'hypothèse de récurrence (i)) et où $\Delta_{1,1}$ est le mineur de la matrice $XI_n - A$ obtenue après retrait de la 1ère ligne et 1ère colonne. On remarque alors que $\Delta_{1,1}$ correspond au polynôme caractéristique de la matrice extraite de A (associée à $\Delta_{1,1}$), et par l'hypothèse de récurrence il vient $\deg(X - a_{1,1})\Delta_{1,1} = n$. Au final, on obtient bien $\deg P_A = n$.

Pour le second point de la proposition, il suffit de noter que $P_A(0) = \det(-A) = (-1)^n \det A$. □

Donnons une propriété importante du polynôme caractéristique, c'est le théorème de Cayley-Hamilton. Rappelons la proposition 1.22 : étant donnée $A \in \mathrm{M}_n$, il existe $P \in \mathbb{R}[X]$ non nul tel que $P(A) = 0$. Le théorème de Cayley-Hamilton indique que P_A "s'annule" en A.

Théorème 3.4. — *Soit $A \in \mathrm{M}_n$ et soit P_A son polynôme caractéristique. Alors $P_A(A) = 0$.*

Nous allons donner une preuve qui repose sur l'observation suivante : soit $P \in \mathbb{R}[X]$ et soit $a \in \mathbb{R}$. Alors $P(a) = 0$ si et seulement si $P = (X - a)R$, où $R \in \mathbb{R}[X]$. Ce résultat s'obtient par division euclidienne.
Il nous faut adapter cette observation au "monde des matrices". Nous allons donc considérer l'ensemble des polynômes dont les coefficients sont des matrices carrées de taille $n \times n$. Notons-le $\mathrm{M}_n[X]$. Il est alors immédiat de voir que $\mathrm{M}_n[X]$ est un $\mathbb{R}$ espace vectoriel de base $E_{i,j}X^k$, où les $E_{i,j}$ sont les matrices élémentaires ($i, j \in \{1, \cdots, n\}$, $k \in \mathbb{N}$). Observons à ce niveau que $\mathrm{M}_n[X]$ coincide avec l'ensemble des matrices dont les coefficients sont dans $\mathbb{R}[X]$. On peut également munir $\mathrm{M}_n[X]$ d'un produit, résultant du produit de matrices. Ici, l'indéterminée X a les mêmes propriétés qu'un scalaire, en particulier : pour $P, Q \in \mathrm{M}_n[X]$, $XPQ = PXQ = PQX$. Mais attention, pour $P, Q \in \mathrm{M}_n[X]$ il n'est pas toujours vrai que $PQ = QP$ (sauf pour $n = 1$).

Lemme 3.5. — *Soit $A \in \mathrm{M}_n$. Supposons qu'il existe $R \in \mathrm{M}_n[X]$ et $P \in \mathbb{R}[X]$ tels que*

$$(XI_n - A)R = \begin{pmatrix} P & 0 & \cdots & \cdots & 0 \\ 0 & P & 0 & \cdots & 0 \\ \vdots & 0 & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & \\ 0 & \cdots & \cdots & 0 & P \end{pmatrix},$$

c'est à dire que $(XI_n - A)R = PI_n$. Alors $P(A) = 0$.

Démonstration. — Soit k le degré de P. On observe que R est de degré $k - 1$. Ecrivons alors $R = B_{k-1}X^{k-1} + B_{k-2}X^{k-2} + \cdots + B_0$, où $B_i \in \mathrm{M}_n$ et $P = a_kX^k + \cdots + a_0$, où les $a_i \in \mathbb{R}$. Puis développons l'expression $(XI_n - A)R = PI_n$ pour obtenir dans $\mathrm{M}_n[X]$ l'identité

$$\big(B_{k-1} - a_kI_n\big)X^k + \big(B_{k-2} - AB_{k-1} - a_{k-1}I_n\big)X^{k-1} + \cdots + (-AB_0 - a_0I_n) = 0.$$

On a alors $a_kI_n = B_{k-1}$, $a_0I_n = AB_0$ et pour $i \in \{1, \cdots, k-1\}$, $a_iI_n = B_{i-1} - AB_i$. Ainsi,

$$\begin{array}{rcl} P(A) & = & \sum_{i=0}^{k} a_iA^i = -AB_0 + A(B_0 - AB_1) + A^2(B_1 - AB_2) + \cdots + A^kB_{k-1} \\ & = & -AB_0 + (AB_0 - A^2B_1) + (A^2B_1 - A^3B_2) + \cdots + A^kB_{k-1} \\ & = & 0, \end{array}$$

après avoir remarqué un téléscopage des matrices. □

Donnons alors la preuve du théorème 3.4.
La théorie des déterminant des matrices à coefficient dans $\mathbb{R}[X]$ se développe de la même façon que celle décrite pour $\mathbb{R}$. Dans ce cas la formule du théorème 2.29 reste toujours valable si les coefficients des matrices sont dans $\mathbb{R}[X]$ (c'est à dire si les matrices sont $\mathrm{M}_n(\mathbb{R}[X])$). Ainsi celle-ci appliquée à la matrice $XI_n - A$ apporte l'égalité

$$(XI_n - A)\mathrm{com}(XI_n - A)^t = P_AI_n,$$

et ainsi le lemme 3.5 indique que P_A "s'annule" en A.

3.2. Valeurs propres. — Un second intérêt du polynôme caractéristique est qu'il permet de localiser les valeurs propres de la matrice A.

Définition 3.6. — Soit $A \in \mathrm{M}_n$. Le nombre réel λ est une valeur propre de A s'il existe un vecteur non nul $X \in \mathbb{R}^n$ tel que $AX = \lambda X$. Un tel vecteur X est appelé vecteur propre associé à la veleur propre λ. L'ensemble des valeurs propres de A est appelé le spectre de A et est noté Spec$A$.

Remarque 3.7. — On a fait le choix de prendre les coefficients des matrices et vecteurs dans $\mathbb{R}$, si c'est dans $\mathbb{C}$, la définition s'adapte immédiatement.

On a alors le théorème suivant

Théorème 3.8. — *Soit $A \in \mathrm{M}_n$ et soit P_A son polynôme caractéristique. Alors λ est une valeur propre de A si et seulement si, λ est une racine de P_A (ou encore si $P_A(\lambda) = 0$).*

Démonstration. — Le nombre λ est une valeur propre de A si et seulement si la matrice $\lambda I_n - A$ n'est pas inversible et donc si et seulement si $\det(\lambda I_n - A) = 0$. On conclut en notant que $P_A(\lambda) = \det(\lambda I_n - A)$. □

Comme un polynôme de degré n admet au plus n racines (par division euclidienne), il vient (grâce à la proposition 3.3)

Corollaire 3.9. — *Une matrice $A \in \mathrm{M}_n$ admet au plus n valeurs propres distinctes.*

Soit $A \in \mathrm{M}_n$ fixée. Pour la suite, si λ désigne une valeur propre de A, on notera par E_λ le sous-espace vectoriel de $\mathbb{R}^n$ engendré par les vecteurs propres associés à la valeur propre λ. On a en fait

$$E_\lambda = \{\text{vecteurs propres de valeur propre } \lambda\} \cup \{0\}.$$

En effet si X_1 et X_2 sont deux vecteurs propres de valeur propre λ, alors pour tout $\beta \in \mathbb{R}$, il vient

$$A(X_1 + \beta X_2) = AX_1 + \beta AX_2 = \lambda(X_1 + \beta X_2),$$

prouvant que si $X_1 + \beta X_2$ est non nul c'est encore un vecteur propre de la valeur propre λ.

Remarque 3.10. — L'espace vectoriel E_λ peut être caractérisé comme le noyau de $A - \lambda I_n$.

Exemple 3.11. — Soit la matrice réelle $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Alors $P_A = X^2 + 1$. Ainsi, A n'a pas de valeur propre réelle. Par contre si l'on change l'ensemble des coefficients en considérant cette matrice à coefficients complexes, il vient que A a deux valeurs propres $\pm i$.

Proposition 3.12. — *Soit $A \in \mathrm{M}_n$ et soient $\lambda_1, \cdots, \lambda_k$ des valeurs propres distinctes de A. Alors les sous-espaces propres E_{λ_i} sont en somme directe.*

Démonstration. — Supposons $k = 2$. Soient $X_i \in E_{\lambda_i}$, $i = 1, 2$, tels que $X_1 + X_2 = 0$. On applique alors la matrice A à cette égalité pour obtenir (d'après la remarque 3.10) le système

$$\begin{cases} X_1 + X_2 &= 0 \\ \lambda_1 X_1 + \lambda_2 X_2 &= 0 \end{cases}$$

En multipliant la 1ère ligne par λ_1 puis en soustrayant les deux nouvelles lignes on obtient $(\lambda_1 - \lambda_2)X_2 = 0$ d'où $X_2 = 0$ car $\lambda_1 \neq \lambda_2$.
Pour $k \geqslant 2$ le principe est le même et la conclusion s'obtient par induction. □

3.3. Matrice diagonalisable et polynôme caractéristique. —

Définition 3.13. — Soit $A \in \mathrm{M}_n$. La matrice A est dite diagonalisable s'il existe une matrice $P \in \mathrm{Gl}_n$ telle que $P^{-1}AP = D$, avec $D \in \mathrm{D}_n$. On dit alors que A est semblable à la matrice D, et on écrit $A \sim D$.

Plus généralement, on dit que deux matrices A, B de M_n sont semblables s'il existe $P \in \mathrm{Gl}_n$ telle que $A = P^{-1}BP$. Observons que cette notion est réflexive, symétrique et transitive.

Lemme 3.14. — *Soient $A, B \in \mathrm{M}_n$ telles que $A \sim B$. Alors*

(*i*) *pour tout polynôme $R \in \mathbb{R}[X]$, il vient $R(A) \sim R(B)$. En particulier, $R(A) = 0$ si et seulement si, $R(B) = 0$.*

(*ii*) $P_A = P_B$.

Démonstration. — (*i*) On écrit $A = P^{-1}BP$ avec $P \in \mathrm{Gl}_n$. Alors notons que $A^2 = (P^{-1}BP)(P^{-1}BP) = P^{-1}B^2P$, et plus généralement, il vient pour $m \geqslant 1$, $A^m = P^{-1}B^mP$. Soit $R = a_kX^k + \cdots a_1X + a_0 \in \mathbb{R}[X]$. Alors

$$R(A) = a_kA^k + \cdots + a_1X + a_0I_n = P^{-1}R(B)P,$$

ce qui prouve le résultat souhaité.
(*ii*) On a $XI_n - A = P^{-1}(XI_n - B)P$. Par conséquent, par le corollaire 2.13 il vient $P_A = \det(P^{-1}(XI_n - B)P) = P_B$. □

Observons que pour une matrice diagonale $D = \mathrm{D}(a_1, \cdots, a_n)$, le polynôme P_D est facile à déterminer : $P_D = (X - a_1)\cdots(X - a_n)$, voir le corollaire 2.16. De ceci, on en déduit que si $A \sim D$, alors les élément sur la diagonale de D sont exactement les valeurs propres de A (au passage on a aussi que si deux matrices diagonales sont semblables, alors elles ont les mêmes éléments sur leur diagonale, comptés avec les multiplicités).
A ce niveau, faisons le lien avec les endomorphismes de $\mathbb{R}^n$. Si A désigne la matrice d'un endomorphisme f de $\mathbb{R}^n$ dans la base canonique B, dire que A est diagonalisable signifie qu'il existe une base B′ de $\mathbb{R}_n$ telle que f a pour matrice une matrice diagonale D dans la nouvelle base B′. Si l'on note alors par P la matrice de passage de la base canonique B dans la nouvelle base B′ (les colonnes de P expriment les coordonnées des vecteurs de la base B′ dans la base canonique B), alors il vient $D = P^{-1}AP$.
De cette correspondance on en déduit la proposition suivante

Proposition 3.15. — *La matrice $A \in \mathrm{M}_n$ est diagonalisable si et seulement si $\mathbb{R}^n = E_{\lambda_1} \oplus \cdots \oplus E_{\lambda_k}$, où* $\mathrm{Spec}A = \{\lambda_1, \cdots, \lambda_k\}$.

Remarque 3.16. — Un polynôme $P \in \mathbb{R}[X]$ se factorisant sous la forme $P = \prod_{i=1}^{k}(X - a_i)$, $a_i \in \mathbb{R}$, est dit scindé sur $\mathbb{R}$. Par exemple, le polynôme $X^2 + 1$ n'est pas scindé sur $\mathbb{R}$, mais il est scindé sur $\mathbb{C}$.

Théorème 3.17. — *Soit $A \in \mathrm{M}_n$. Si P_A a n racines distinctes alors A est diagonalisable.*

Remarque 3.18. — Ici les racines de P_A doivent être vues dans l'ensemble des coefficients de la matrice. Par exemple si $A \in \mathrm{M}_n(\mathbb{R})$, on veut que les racines de P_A soient dans $\mathbb{R}$.

Démonstration. — Supposons que P_A a n racines distinctes $\lambda_1, \cdots, \lambda_n$. Cela signifie donc que A a n valeurs propres distinctes. Alors $\dim(E_{\lambda_1} \oplus \cdots \oplus E_{\lambda_n}) \geqslant n$, car $\dim E_{\lambda_i} \geqslant 1$. Comme $E_{\lambda_1} \oplus \cdots \oplus E_{\lambda_n} \subset \mathbb{R}^n$, on en déduit que $\mathbb{R}^n = E_{\lambda_1} \oplus \cdots \oplus E_{\lambda_n}$. On conclut avec la proposition 3.15. Remarquons au passage que pour $i = 1, \cdots, n$, il vient $\dim E_{\lambda_i} = 1$. □

Exemple 3.19. — Soit la matrice $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \mathrm{M}_2(\mathbb{R})$. Alors $P_A = X^2 - 1 = (X - 1)(X + 1)$. La matrice A est diagonalisable, semblable à la matrice $D = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

Exemple 3.20. — Soit la matrice $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Alors $P_A = X^2 + 1$. La matrice A n'est pas diagonalisable dans $\mathbb{R}$ (le polynôme P_A n'a pas de racine réelle). Par contre dans $\mathbb{C}$ la matrice A est diagonalisable et est semblable à la matrice $D = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$.

A la lecture de la preuve du théorème 3.17 on peut donner un résultat complet mais qui nécessite un peu plus de vocabulaire.
Soit λ une valeur propre de A, notons par m_λ la dimension de E_λ. Alors $m_\lambda \geqslant 1$ par définition (nous avons vu que $m_\lambda = 1$ lorsque P_A a n racines distinctes). La quantité m_λ est appelée *multiplicité géométrique* de λ. Notons par n_λ la multiplicité de λ dans P_A : c'est sa *multiplicité algébrique*.

Proposition 3.21. — *Soit λ une valeur propre de A. Alors $1 \leqslant m_\lambda \leqslant n_\lambda$, ou encore la multiplicité géométrique est plus petite que la multiplicité algébrique.*

Démonstration. — Soit $\lambda \in \mathrm{Spec}A$ et soit $\mathrm{B}' = \{X_1, \cdots, X_r\}$ une base de E_λ ; ici $r = m_\lambda$. On complète B' en une base B'' de $\mathbb{R}^n$. Alors si l'on écrit la matrice de l'endomorphisme f associé à A dans la base B'', il vient

$$A \sim \left[\begin{array}{c|c} D_r(\lambda) & B \\ \hline O & C \end{array}\right]$$

où $D_r(\lambda) = \lambda I_r$, $B \in \mathrm{M}_{r,n-r}$, $O \in \mathrm{M}_{n,n-r}$ est composée que de 0, et $C \in \mathrm{M}_{n-r,n-r}$. De cette écriture on en déduit que $P_A = P_{D(\lambda)}P_C = (X-\lambda)^r P_C$ (c'est une application du théorème 2.15). Or $P_A = (X-\lambda)^{n_\lambda} R$ avec $R(\lambda) \neq 0$. On en déduit ainsi que $r \leqslant n_\lambda$. □

Théorème 3.22. — *Soit $A \in \mathrm{M}_n$. La matrice A est diagonalisable si et seulement si, pour toute valeur propre λ_i de A, il vient $m_{\lambda_i} = n_{\lambda_i}$ (ou encore si la multiplicité géométrique est égal à la multiplicité arithmétique). Si tel est le cas, la matrice A est semblable a une matrice diagonale avec n_{λ_i} fois la valeur propre λ_i sur la diagonale, pour chaque $\lambda_i \in \mathrm{Spec}A$.*

Démonstration. — Observons tout d'abord que $\sum_{\lambda \in \mathrm{Spec}A} n_\lambda = n$. Notons $k = \#\mathrm{Spec}A$.

• Supposons que $n_\lambda = m_\lambda$. Le principe est le même que celui de la preuve du théorème 3.17. Pour chaque $\lambda_i \in \mathrm{Spec}A$, on prend une base $\{X_{i,1}, \cdots, X_{i,m_\lambda}\}$ de E_{λ_i}. La famille $\mathrm{B}' = \{X_{1,1}, \cdots, X_{1,m_{\lambda_1}}, X_{2,1}, \cdots, X_{k,m_k}\}$ forme une famille libre de $\mathbb{R}^n$ et comme $\sum_{i=1}^{k} m_i = n$, elle forme une base de $\mathbb{R}^n$; on conclut avec la proposition 3.15. Dans cette nouvelle base, la matrice A devient semblable à la matrice diagonale

$$\begin{bmatrix} D_{m_{\lambda_1}}(\lambda_1) & & 0 \\ & \ddots & \\ 0 & & D_{m_{\lambda_k}}(\lambda_k) \end{bmatrix}$$

où $D_{m_{\lambda_i}}(\lambda_i) = \lambda_i I_{m_{\lambda_i}}$.

• La réciproque est relativement simple. Si A est semblable a une matrice diagonale, alors par la proposition 3.15, il vient $P_D = \prod_{i=1}^{k}(X-\lambda_i)^{m_{\lambda_i}}$. Mais par le lemme 3.14 $P_A = P_D$, et donc $n_{\lambda_i} = m_{\lambda_i}$. □

Exemple 3.23. — Soit la matrice $A = \begin{pmatrix} 2 & -1 & 1 \\ 1 & 0 & 1 \\ 1 & -1 & 2 \end{pmatrix}$. Alors $P_A = X^3 - 4X^2 + 5X - 2$. On observe que $P_A(1) = 0$, puis que $P_A = (X-1)(X^2-3X+2) = (X-1)^2(X-2)$. Le polynôme P_A est scindée. On recherche maintenant les multiplicités des valeurs propres $\lambda = 2$ et $\lambda = 1$.

Pour la valeur propre $\lambda = 2$, il vient $m_2 = n_2 = 1$. Pour la valeur propre $\lambda = 1$, on a $1 \leqslant m_1 \leqslant n_1 = 2$.

La recherche de $N_2 = \ker(A - 2I_3)$ montre que $N_2 = \left\langle \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \right\rangle$. Pour $N_1 = \ker(A - 2I_3)$, il vient $N_1 = \left\langle \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \right\rangle$, montrant ainsi que $m_1 = n_1 = 2$. Par le théorème 3.22, on en déduit que la matrice A est diagonalisable.

Soit la matrice de passage $P = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & -1 & 1 \end{pmatrix}$; il vient pour finir $P^{-1}AP = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

Exemple 3.24. — Soit la matrice $A = \begin{pmatrix} 0 & 2 & -1 \\ -1 & 5 & -2 \\ 0 & 4 & -1 \end{pmatrix}$.
Alors $P_A = X^3 - 4X^2 + 5X - 2 = (X-1)(X^2 - 3X + 2) = (X-1)^2(X-2)$. Or $N_1 = \ker(A - I_3) = \left\langle \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix} \right\rangle$. Ainsi $1 = m_1 \neq n_1 = 2$, la matrice A n'est diagonalisable.

3.4. Polynôme minimal. —

3.4.1. Définition. — Etant donnée $A \in \mathrm{M}_n$, rappelons la définition de φ_A vue dans la section 1.2.3 :

$$\begin{array}{rccc} \varphi_A : & \mathbb{R}[X] & \to & \mathrm{M}_n \\ & P & \mapsto & P(A) \end{array}$$

Proposition 3.25. — *Il existe un unique polynôme unitaire $\mathfrak{m}_A$ tel que $\mathfrak{m}_A$ divise tout polynôme $P \in \ker \varphi_A$.*

Démonstration. — Soit $\ker \varphi_A$. Soit $\mathfrak{m} \in \ker \varphi_A$, $\mathfrak{m} \neq 0$, de degré minimal ; on peut prendre $\mathfrak{m}$ unitaire (comme $P \in \ker \varphi_A$, on est assuré de l'existence d'un tel polynôme $\mathfrak{m}$).
Soit P un autre polynôme de $\ker \varphi_A$. Effectuons alors la divisions euclidienne de P par $\mathfrak{m}_A$: il existe deux polynômes $Q, R \in \mathbb{R}[X]$ tels que $P = Q\mathfrak{m} + R$, avec $\deg R < \deg \mathfrak{m}$. Or $R(A) = P(A) - Q(A)\mathfrak{m}(A) = 0$, car $P, \mathfrak{m} \in \ker \varphi_A$. D'où $R \in \ker \varphi_A$. Par minimalité du degré de $\mathfrak{m}$, on en déduit que $R = 0$, ou encore que $\mathfrak{m}$ divise P. □

Définition 3.26. — Le polynôme $\mathfrak{m}_A$ de la proposition 3.25 est appelé polynôme minimal de A.

Le polynôme minimal $\mathfrak{m}_A$ est le polynôme unitaire de plus petit degré s'annulant en A. Nous avons vu par le théorème de Cayley-Hamilton que $P_A \in \ker \varphi_A$, ainsi $\mathfrak{m}_A$ divise P_A. En fait, $\mathfrak{m}_A$ et P_A sont très proches comme l'indique la proposition suivante

Proposition 3.27. — *Toute valeur propre λ de A est également une racine de $\mathfrak{m}_A$ (c'est à dire $\mathfrak{m}_A(\lambda) = 0$).*

Démonstration. — Soit λ une valeur propre de A et soit X un vecteur propre. On rappelle que $X \neq 0$. Observons que $AX = \lambda X$ et donc $A^2X = A(AX) = A(\lambda X) = \lambda AX = \lambda^2 X$, et ainsi $A^r X = \lambda^r X$, pour tout entier $r \geqslant 0$ (avec la convention que $A^0 = I_n$). Par conséquent pour tout polynôme $P \in \mathbb{R}[X]$, il vient $P(A)X = P(\lambda)X$. Ainsi $0 = \mathfrak{m}_A(A)X = \mathfrak{m}_A(\lambda)X$. Comme X est un vecteur non nul, nécessairement le scalaire $\mathfrak{m}_A(\lambda)$ est nul. □

Etant donnée une matrice $A \in \mathrm{M}_n$, notons par n_λ la multiplicité arithmétique de λ, et par n'_λ la multiplicité de λ pour $\mathfrak{m}_A$. Par la proposition 3.27, on a $n'_\lambda \geqslant 1$ et par la proposition 3.25 : $n'_\lambda \leqslant n_\lambda$.

3.4.2. Le lemme des noyaux. — Le lemme suivant est un résultat mélangeant algèbre et géométrie, essentiel à la preuve du théorème principal de cette section.

Lemme 3.28. — *Soit $A \in \mathrm{M}_n$ et soit $R \in \mathbb{R}[X]$, R non nul, tel que $R(A) = 0$. Supposons que $R = R_1 \dots R_k$, où les polynômes R_i sont deux à deux premiers entre eux. Posons $N_i = \ker R_i(A)$. Alors $\mathbb{R}^n = N_1 \oplus N_2 \oplus \cdots \oplus N_k$.*

Démonstration. — Pour $i = 1, \cdots, k$, posons $\hat{R}_i = R/R_i = R_1 \cdots R_{i-1} R_{i+1} \cdots R_k$. Remarquons que les polynômes $\hat{R}_i$ n'ont pas de facteurs communs dans leur ensemble : si un polynôme irréductible U divise chaque $\hat{R}_i$, alors comme U divise $\hat{R}_1$ il divise un des R_i, et donc par exemple R_{i_0} pour un certain indice i_0. Mais alors U ne peut pas diviser $\hat{R}_{i_0}$.
Comme le polynômes les polynômes $\hat{R}_i$ sont premiers dans leurs ensemble, ils vérifient une relation de Bezout (identique à celle du théorème 4.18 de la section 4.2.2). Donnons une preuve rapide. Considérons l'ensemble $\mathscr{I}$ des polynômes de $\mathbb{R}[X]$ de la forme $T_1\hat{R}_1 + \cdots + T_2\hat{R}_2$, où les $T_i \in \mathbb{R}[X]$ sont des polynômes quelconques. L'ensemble $\mathscr{I}$ est stable par combinaison linéaire. Notons par S_0 un polynôme non nul de $\mathscr{I}$ de plus petit degré possible (on peut choisir S_0 unitaire). Soit un polynôme $S \in \mathscr{I}$ quelconque, puis effectuons la division euclidienne de S par S_0 : on observe que le reste S' de cette division est aussi dans $\mathscr{I}$. Par minimalité du degré de S_0, on en déduit que $S' = 0$ et ainsi, S est un multiple de S_0. Comme les polynômes sont dans $\mathscr{I}$, chaque $\hat{R}_i$ est un multiple de S_0, ou encore S_0 divise chaque $\hat{R}_i$. Mais si S_0 admet un facteur irréductible (c'est à dire que S_0 est divisible par un polynôme) on a vu que ce n'est pas possible ; on en déduit ainsi que S_0 est une constante égale à 1. En conclusion, $1 \in \mathscr{I}$. Il existe donc des polynômes $S_i \in \mathbb{R}[X]$ tels que

$$1 = \hat{R}_1 S_1 + \cdots + \hat{R}_k S_k. \tag{2}$$

En impliquant φ_A à l'identité (2), il vient dans M_n

$$I_n = \hat{R}_1(A)S_1(A) + \cdots + \hat{R}_k(A)S_k(A). \tag{3}$$

Observons maintenant que $R_i(A)\hat{R}_i(A)S_1(A) = R(A)S_1(A) = 0$. Ainsi pour tout vecteur de $X \in \mathbb{R}^n$, il vient $\hat{R}_i(A)S_i(A)X \in \ker(R_i(A)) = N_i$.
Si l'on applique (3) à tout vecteur $X \in \mathbb{R}^n$, on obtient

$$X = X_1 + \cdots + X_k, \tag{4}$$

avec $X_i = \hat{R}_i(A)S_i(A)X \in N_i$, d'où $\mathbb{R}^n = N_1 + \cdots + N_k$. Il nous reste à montrer que la somme est directe.

Observons alors que pour tout $X \in N_i$, il vient $X = \hat{R}_i(A)S_i(A)X$. En effet, pour $X_j \in N_j = \ker(R_j(A))$, $j \neq i$, il vient

$$\hat{R}_i(A)S_i(A)X_j = S_i(A)\hat{R}_i(A)X_j = 0, \tag{5}$$

car R_j apparaît dans $\hat{R}_i$ (et que $S_i(A)$ commute avec $\hat{R}_i(A)$, ce sont deux polynômes en la même matrice A), et l'identité (4) montre que $X = \hat{R}_i(A)S_i(A)X$.
Montrons alors la somme directe. Soient $X_i \in N_i$, $i = 1, \cdots, k$, tels que $X_1 + \cdots + X_k = 0$. On applique $\hat{R}_i(A)S_i(A)$ à cette identité pour obtenir (en utilisant (5))

$$\hat{R}_i(A)S_i(A)(X_1 + \cdots + X_k) = \hat{R}_i(A)S_i(A)X_1 + \cdots + \hat{R}_i(A)S_i(A)X_k = \hat{R}_i(A)S_i(A)X_i = X_i.$$

On conclut en observant que

$$\hat{R}_i(A)S_i(A)(X_1 + \cdots + X_k) = \hat{R}_i(A)S_i(A)0 = 0.$$

□

Pour que A soit diagonalisable, on a vu qu'il est nécessaire que $P_A = \prod_{\lambda \in \mathrm{Spec}A} (X-\lambda)^{n_\lambda}$ et $\mathfrak{m}_A = \prod_{\lambda} (X-\lambda)^{n'_\lambda}$. Nous sommes en mesure d'énoncé le théorème central de diagonalisation.

Théorème 3.29. — *Soit $A \in \mathrm{M}_n$. La matrice A est diagonalisable si et seulement si, $\mathfrak{m}_A = \prod_{\lambda \in \mathrm{Spec}A} (X-\lambda)$. Ou encore si et seulement si $n'_\lambda = 1$ pour toute valeur propre λ de A.*

Démonstration. — • Supposons A diagonalisable, alors

$$A \sim D = \begin{bmatrix} D_{m_{\lambda_1}}(\lambda_1) & & 0 \\ & \ddots & \\ 0 & & D_{m_{\lambda_1}}(\lambda_k) \end{bmatrix},$$

où $\mathrm{Spec}A = \{\lambda_1, \cdots, \lambda_k\}$ et $D_{m_{\lambda_i}}(\lambda_i) = \lambda_i I_{m_{\lambda_i}}$. Ainsi, $D_{m_{\lambda_i}}(\lambda_i) - \lambda_i I_{m_{\lambda_i}} = 0$. Il vient alors

$$D - \lambda_1 I_n = \begin{bmatrix} O & & 0 \\ & \ddots & \\ 0 & & D_{m_{\lambda_i}}(\lambda_k - \lambda_1) \end{bmatrix},$$

où $O = D_{m_{\lambda_1}}(\lambda_1) - \lambda_1 I_{m_{\lambda_i}}$ est la matrice de taille $m_{\lambda_1} \times m_{\lambda_1}$ composée uniquement de zéros. Plus généralement $D - \lambda_i I_n$ apporte un bloc de zéros à la place de $D_{m_{\lambda_i}}(\lambda_i)$. Le produit $(D - \lambda_1 I_n) \cdots (D - \lambda_k I_n)$ devient nul. Ainsi le polynôme $P = \prod_{\lambda \in \mathrm{Spec}A} (X - \lambda)$ s'annule en D. Par le lemme 3.14, P s'annule aussi en A. Par les propositions 3.25 et 3.27, on en déduit que $P = \mathfrak{m}_A$.
• La réciproque se déduit du lemme 3.28 : plus précisémment, on applique le lemme des noyaux au polynôme minimal $\mathfrak{m}_A$ de A, avec $R_i = (X - \lambda_i)$, où $\lambda_i \in \mathrm{Spec}A$. Or ici,

$$N_i = \ker(R_i(A)) = \ker(A - \lambda_i I_n) = E_{\lambda_i}.$$

On conclut avec la proposition 3.15. □

Exemple 3.30. — Le polynôme caractéristique des exemples 3.23 et 3.24 est $P_A = (X-1)^2(X-2)$. Ainsi, pour le polynôme minimal, il vient le choix entre $(X-1)(X-2)$ et $(X-1)^2(X-2)$: en effet $\mathfrak{m}_A$ et P_A ont les mêmes racines et $\mathfrak{m}_A$ divise P_A.

Soit $A = \begin{pmatrix} 2 & -1 & 1 \\ 1 & 0 & 1 \\ 1 & -1 & 2 \end{pmatrix}$ de l'exemple 3.23. Alors on vérifie que $(A - I_3)(A - 2I_3) = 0$, montrant ainsi que $\mathfrak{m}_A = (X-1)(X-2)$, et confirmant que A est diagonisable.

Soit $A = \begin{pmatrix} 0 & 2 & -1 \\ -1 & 5 & -2 \\ 0 & 4 & -1 \end{pmatrix}$ de l'exemple 3.24. On vérifie que $(A-I_3)(A-2I_3) \neq 0$, montrant ainsi que $\mathfrak{m}_A = P_A$, et confirmant que A n'est pas diagonalisable.

3.5. Récapitulatif. — Pour conclure, donnons une méthode pour tester si une matrice A est diagonalisable.

Soit donc $A \in \mathrm{M}_n$.

→ Calculer $P_A = \det(XI_n - A) \in \mathbb{R}[X]$.

→ Factoriser P_A.
Dans $\mathbb{R}[X]$, les facteurs irréductibles sont de la forme $(X-a)$ ou $X^2 + aX + b$ avec $a^2 - 4b < 0$, $a, b \in \mathbb{R}$.
Dans $\mathbb{C}[X]$, les facteurs irréductibles sont de la forme $(X-a)$, $a \in \mathbb{C}$.

→ Si le polynôme P_A n'est pas scindé, c'est à dire ne s'écrit pas sous la forme $P_A = \prod_{i=1}^{n}(X - a_i)$, la matrice A n'est pas diagonalisable.

Pour la suite, supposons P_A scindé. Alors $P_A = \prod_{\lambda \in \mathrm{Spec}A} (X-\lambda)^{n_\lambda}$.

→ **Cas particulier.** Si pour tout $\lambda \in \mathrm{Spec}A$, on a $n_\lambda = 1$, la matrice A est diagonalisable. La matrice A est semblable à une matrice diagonale avec les $\lambda \in \mathrm{Spec}A$ sur la diagonale ; ici $\#\mathrm{Spec}A = n$.

→ **1ère méthode.** On calcule $\prod_{\lambda \in \mathrm{Spec}A} (A - \lambda I_n) \in \mathrm{M}_n$.
Alors la matrice A est diagonalisable si et seulement si, $\prod_{\lambda \in \mathrm{Spec}A} (A - \lambda I_n) = 0$.
Si A est diagonalisable, alors $\mathfrak{m}_A = \prod_{\lambda \in \mathrm{Spec}A} (A - \lambda I_n)$, et A est semblable a une matrice diagonale avec n_λ fois la valeur propre λ sur la diagonale, ceci pour chaque $\lambda \in \mathrm{Spec}A$.

→ **2ème méthode.** Pour chaque valeur propre λ, on détermine m_λ, c'est à dire la dimension de $N_\lambda = \ker(A - \lambda I_n)$. On sait que $1 \leqslant m_\lambda \leqslant n_\lambda$, et ainsi le calcul de m_λ a tout son sens quand $n_\lambda \geqslant 2$.

La matrice A est diagonalisable si et seulement si, pour tout $\lambda \in \mathrm{Spec}A$, il vient $m_\lambda = n_\lambda$.

Si la matrice A est diangonalisable, alors le calcul d'une base des N_λ permet d'obtenir une matrice de passage P telle que $P^{-1}AP = D$.

3.6. Exercices. —

Exercice 24. — *Pour chacune des matrices réelles suivantes, déterminer le polynôme caractéristique, les valeurs propres et le polynôme minimal. Indiquer les matrices diagonalisables.*

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \qquad B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad C = \begin{pmatrix} 3 & 0 & 0 \\ 2 & 1 & 4 \\ 1 & 0 & 4 \end{pmatrix}$$

$$D = \begin{pmatrix} 1 & -2 & 2 \\ -2 & -1 & 2 \\ -2 & -1 & 3 \end{pmatrix} \qquad E = \begin{pmatrix} 0 & -1 & 1 \\ 0 & -1 & 0 \\ 1 & -1 & 0 \end{pmatrix} \qquad F = \begin{pmatrix} 0 & 1 & 0 \\ 3 & 2 & -4 \\ 2 & 2 & -3 \end{pmatrix}$$

$$G = \begin{pmatrix} 1 & 2 & -2 & 0 \\ 2 & 1 & -2 & 0 \\ 2 & 2 & -3 & 0 \\ 2 & 2 & -4 & 1 \end{pmatrix} \qquad H = \begin{pmatrix} 5 & 5 & -4 & -5 \\ -3 & -3 & 3 & 4 \\ -3 & -2 & 2 & 4 \\ 3 & 2 & 0 & -2 \end{pmatrix}$$

Exercice 25. — 1. *Déterminer les sous-espaces propres des matrices de l'exercice 24. Lorsque la matrice est diagonalisable, la diagonaliser.*

2. *Calculer A^n et C^n pour $n \in \mathbb{N}_{\geqslant 1}$.*
3. *Calculer B^n pour $n \in \mathbb{N}_{\geqslant 1}$.*

Exercice 26. — *On considère la matrice M suivante ($m \in \mathbb{R}$ est un paramètre)*

$$M = \begin{pmatrix} 1 & 2 & 0 \\ 1 & -1 & 0 \\ 0 & 1 & m \end{pmatrix}.$$

1. *Déterminer les valeurs propres de M.*
2. *Pour quelles valeurs de $m \in \mathbb{R}$ la matrice M est-elle diagonalisable ?*
3. *Diagonaliser M lorsque celle-ci est diagonalisable.*

Exercice 27. — *Soit la matrice à coefficients réels $A = \begin{pmatrix} 1 & 1 & 2 \\ 1 & 1 & t \\ 1 & 1 & 2 \end{pmatrix}$, où t est un paramètre.*

1. *Déterminer le polynôme caractéristique P_A de A.*
2. *Montrer que la matrice A a une unique valeur propre réelle (à déterminer) si et seulement si, $t < -2$. Dans ce cas, que peut-on dire sur la diagonalisation de A ?*
3. *Montrer qu'il existe* deux *valeurs de t, notées t_1 et t_2, pour lesquelles la matrice A a exactement deux valeurs propres distinctes que l'on déterminera.*
4. *Déterminer le polynôme minimal de A quand $t = t_1$ puis quand $t = t_2$.*

5. *En déduire l'ensemble des valeurs de t pour lesquelles la matrice A est diagonalisable. (On ne demande pas de diagonaliser A !)*

Exercice 28. — *Trianguliariser les matrices de l'exercice 24 lorsque c'est possible.*

Exercice 29. — *Soit une matrice diagonale $D \in \mathrm{M}_n$ inversible et soit $A \in \mathrm{M}_n$ quelconque.*
1) Montrer qu'il existe $t_0 > 0$ tel que pour tout réel $|t| \geqslant t_0$, la matrice $A + tD$ est inversible.
2) On suppose A inversible. Montrer qu'il existe $t_0 < 0 < t_1$ tels que la matrice $A + tD$ est inversible pour tout $t \in [t_0, t_1]$.

PARTIE II
ARITHMÉTIQUE

On notera par

- $\mathbb{N} = \{0, 1, 2, 3, \cdots\}$ l'ensemble des entiers naturels,
- $\mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2, \cdots\}$ l'ensemble des entiers (relatifs),
- $|a| = \max\{a, -a\}$ la valeur absolue du nombre réel a.

On rappelle que $(\mathbb{Z}, +, \cdot)$ est un anneau avec ± 1 comme éléments inversibles (voir la definition 8.14 de la section 8).

4. Divisibilité

4.1. Division euclidienne. —

Définition 4.1. — Soient $a, b \in \mathbb{Z}$. On dit que a divise b, ou que a est un diviseur de b, ou que b est un multiple de a, si $b = ac$ pour un certain $c \in \mathbb{Z}$. On note alors $a|b$.

Exemple 4.2. — Les entiers 1 et -1 divisent tout entier $a \in \mathbb{Z}$. En effet, $a = 1 \times a$ et $a = (-1) \times (-a)$.

Exemple 4.3. — L'entier a est dit pair quand 2 divise a. L'entier a est dit impair si il n'est pas pair.

Remarque 4.4. — Si $a|b$ alors $\pm a| \pm b$.

Remarque 4.5. — Soit un entier $b > 0$. Alors tout diviseur de b est compris entre $-b$ et b, par conséquent tout entier $b \neq 0$ a un nombre fini de diviseurs. Par contre tout entier est diviseur de l'entier $b = 0$. Enfin, $0|a$ si et seulement si, $a = 0$.

Enonçons quelques propriétés.

Proposition 4.6. — *Soient trois entiers $a, b, c \in \mathbb{Z}$. On a les propriétés suivantes :*

(*i*) *Si $a|b$ et $b|c$ alors $a|c$.*

(*ii*) *Si $a|b$ alors $ac|bc$.*

(*iii*) *Si $a|b$ et $a|c$ alors $a|(xb + yc)$ pour tout entier x, y.*

(*iv*) *Si $a|b$ et $b|a$, alors $a = \pm b$.*

Démonstration. — (*i*) Par hypothèse il existe $\alpha, \beta \in \mathbb{Z}$ tels que $b = \alpha a$ et $c = \beta b$. Ainsi $c = \alpha\beta a$ ce qui signifie que $a|c$.
(*ii*) Par hypothèse $b = \alpha a$ pour un certain $\alpha \in \mathbb{Z}$. Ainsi $bc = \alpha ac$, ce qui signifie que $ac|bc$.
(*iii*) On écrit $b = a\alpha$ et $c = a\beta$ avec $\alpha, \beta \in \mathbb{Z}$. Alors $xb + yc = a(x\alpha + y\beta)$, et ainsi $a|(xb + yc)$.
(*iv*) Par hypothèse il existe deux entiers $\alpha, \beta \in \mathbb{Z}$ tels que $b = a\alpha$ et $a = \beta b$. Par conséquent, $b = \alpha\beta b$ puis $b(1 - \alpha\beta) = 0$. Si $b = 0$, alors $a = 0$; sinon $b \neq 0$ et on en déduit que $\alpha\beta = 1$, puis que $\alpha = \pm 1$ (se rappeler que $\alpha, \beta \in \mathbb{Z}$). □

Le théorème suivant joue un rôle très important pour toute la suite.

***Théorème 4.7* (Division euclidienne).** — *Soient $a, b \in \mathbb{Z}$ avec $a \neq 0$. Il existe $q, r \in \mathbb{Z}$ tels que $b = aq + r$, avec $0 \leqslant r < |a|$. De plus, sous ces conditions, les éléments q et r sont uniques. On dit que l'entier r est le reste de la division de b par a et l'entier q est le quotient.*

Démonstration. — *Existence.* On peut noter que le principe de la division euclidienne est immédiat si $a|b$ (avec $r = 0$ alors).
• Supposons $a, b \geqslant 0$. Soit q le plus petit entier naturel tel que $qa \leqslant b < (q+1)a$. On pose alors $r = b - qa < a$.
• Si $a < 0$ et $b > 0$. D'après le premier point, on effectue le division euclidienne de b par $-a$: il existe deux entiers q et r avec $0 \leqslant r < -a$ tels que $b = q(-a) + r$, c'est à dire tels que que $b = -qa + r$; ici le quotient est $-q$ et le reste r est bien strictement plus petit que $|a|$.
• Si $a < 0$ et $b \leqslant 0$. On effectue la division euclidienne de $-b$ par $-a$: il existe deux entiers q et r avec $0 \leqslant r < -a$, tels que $-b = -qa + r$. On rappelle qu'ici $r = 0$ si et seulement si $\pm a| \pm b$ et donc en particulier si et seulement si $a|b$. Ainsi, d'après la remarque du début de la preuve, on peut supposer $r > 0$. Alors on écrit $-b = (-q-1)a + a + r$, ou encore $b = (q+1)a - a - r$. On note alors que $0 < -a - r < -a = |a|$.
• Si $a > 0$ et $b \leqslant 0$. D'après le point précédent, on effectue la division euclidienne de b par $-a$. Il existe deux entiers q et r avec $0 \leqslant r < -a$, tels que $-b = -qa + r$; ici le quotient est $-q$ et le reste r est bien strictement plus petit que $|a|$.

Unicité. Ecrivons $b = qa + r = q'a + r'$ avec $0 \leqslant r, r' < |a|$. On a alors $-|a| < a(q - q') = r' - r < |a|$: en d'autres termes l'entier $a(q - q')$ est un multiple de a compris strictement entre $-|a|$ et $|a|$, il est donc égal à 0. Comme a est non nul, on en déduit que $q = q'$, puis que $r = r'$. □

On a alors

***Corollaire 4.8*.** — *L'entier non nul a divise b si et seulement si le reste de la division euclidienne de b par a est nul.*

4.2. Relation de Bézout et algorithme d'Euclide. —

4.2.1. PGCD. —

***Définition 4.9*.** — Soient a et b deux entiers non nuls. Le Plus Grand Commun Diviseur (PGCD) de a et de b est le plus grand entier d qui divise a et b. On le note $d = \mathrm{pgcd}(a, b)$. Le plus petit commun multiple (PPCM) à a et b est le plus petit entier m multiple de a et de b. On le note $\mathrm{ppcm}(a, b)$.

***Remarque 4.10*.** — On a $\mathrm{pgcd}(\pm a, \pm b) = \mathrm{pgcd}(a, b)$.

***Remarque 4.11*.** — Il est possible d'étendre la définition du PGCD au cas où $b = 0$ par exemple. Ainsi, si $a \neq 0$, on a $\mathrm{pgcd}(a, 0) = |a|$.

Exemple 4.12. — Les diviseurs positifs de 12 sont $1, 2, 3, 4, 6, 12$ et ceux de 18 sont $1, 2, 3, 6, 9, 18$. Ainsi, $\text{pgcd}(12, 18) = 6$.

Définition 4.13. — Deux entiers non nuls a et b sont dit premiers entre eux si $\text{pgcd}(a, b) = 1$. On dit aussi que a est premier à b (ou que b est premier à a).

4.2.2. Relation de Bézout. — Si $a_1, \cdots a_n$ désignent n entiers, on note par $a_1\mathbb{Z}+\cdots+a_n\mathbb{Z}$ le sous-ensemble de $\mathbb{Z}$ suivant :

$$a_1\mathbb{Z} + \cdots + a_n\mathbb{Z} = \{a_1x_1 + \cdots + a_nx_n,\ x_1, \cdots, x_n \in \mathbb{Z}\}.$$

Remarquons que $a\mathbb{Z}$ est exactement l'ensemble des multiples de a.

Proposition 4.14. — *Soient deux entiers a et b. Alors $b\mathbb{Z} \subset a\mathbb{Z}$ si et seulement si $a|b$.*

Démonstration. — En effet, si $b\mathbb{Z} \subset a\mathbb{Z}$ alors comme $b \in b\mathbb{Z}$, on a que $b \in a\mathbb{Z}$: l'élément b est un multiple de a ou encore $a|b$. La réciproque est immédiate : si $a|b$, il existe $c \in \mathbb{Z}$ tel que $b = ac$. Ainsi $b\mathbb{Z} = ac\mathbb{Z} \subset a\mathbb{Z}$. □

On peut remarquer le lemme suivant

Lemme 4.15. — *Soient $c, c' \in a_1\mathbb{Z} + \cdots + a_n\mathbb{Z}$. Alors $\alpha c + \beta c' \in a_1\mathbb{Z} + \cdots + a_n\mathbb{Z}$, pour tout $\alpha, \beta \in \mathbb{Z}$. En particulier, $(\alpha c + \beta c')\mathbb{Z} \subset a_1\mathbb{Z} + \cdots + a_n\mathbb{Z}$.*

Démonstration. — C'est immédiat. □

On a alors une seconde proposition.

Proposition 4.16. — *Soient a et b deux entiers. Alors $a\mathbb{Z} + b\mathbb{Z} = m\mathbb{Z}$ pour un certain $m \in \mathbb{Z}$. De plus pour un tel entier m, il vient $m|a$ et $m|b$.*

Démonstration. — Si $a = b = 0$, prendre $m = 0$. Sinon, soit $m > 0$ le plus petit entier *strictement* positif appartenant à $a\mathbb{Z} + b\mathbb{Z}$. Soit alors $n \in a\mathbb{Z} + b\mathbb{Z}$. Regardons la division euclidienne de n par m : il existe q, r dans $\mathbb{Z}$ avec $0 \leqslant r < m$, tels que $n = qm + r$. Ainsi, $r = n - qm \in a\mathbb{Z} + b\mathbb{Z}$ d'après le lemme 4.15. Par minimalité de m, on en déduit $r = 0$, et ainsi $n \in m\mathbb{Z}$. Nous venons de montrer que $a\mathbb{Z} + b\mathbb{Z} \subset m\mathbb{Z}$.
Comme $m \in a\mathbb{Z} + b\mathbb{Z}$, l'inclusion inverse se déduit du lemme 4.15. Au final, on a bien $a\mathbb{Z} + b\mathbb{Z} = m\mathbb{Z}$.
Pour la seconde partie du lemme, on note que $a \in a\mathbb{Z} + b\mathbb{Z} = m\mathbb{Z}$: il existe $\alpha \in \mathbb{Z}$ tel que $a = m\alpha$, ce qui signifie que $m|a$. Idem pour b. □

Au passage, remarquons que par récurrence, on a la proposition suivante :

Proposition 4.17. — *Soient n entiers $a_1, \cdots, a_n$. Alors $a_1\mathbb{Z} + \cdots + a_n\mathbb{Z} = m\mathbb{Z}$ pour un certain entier m.*

On peut montrer le théorème suivant

Théorème 4.18. — *Soient a, b deux entiers non nuls. Alors $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$, où $d = \text{pgcd}(a, b)$.*

Démonstration. — On sait que $d|a$ et que $d|b$, ainsi d'après la proposition 4.14, il vient $a\mathbb{Z} + b\mathbb{Z} \subset d\mathbb{Z}$. De plus, d'après la proposition 4.16, il vient $a\mathbb{Z} + b\mathbb{Z} = m\mathbb{Z}$ pour un certain entier $m > 0$; par la proposition 4.14, on a alors $d|m$: ainsi il existe $\alpha \in \mathbb{Z}$ tel que $m = \alpha d$. On peut remarquer que $\alpha \geqslant 1$ car positif non nul. Mais comme $m|a$ et $m|b$ (d'après la proposition 4.16), on en déduit que $m \leqslant d$ (par définition de d). Ainsi, de $\alpha d \leqslant d$, on obtient que $\alpha = 1$ puis que $m = d$. □

Corollaire 4.19. — *Si a et b sont deux entiers non nuls et si m est tel que $m|a$ et $m|b$, alors $m|\text{pgcd}(a, b)$.*

Démonstration. — Comme $m|a$ et $m|b$, alors $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z} \subset m\mathbb{Z}$, ce qui implique que $m|d$ d'après la proposition 4.14. □

Corollaire 4.20 **(Relation de Bézout)**. — *Soient a et b deux entiers non nuls. Soit $d = \text{pgcd}(a, b)$. Alors il existe $u, v \in \mathbb{Z}$ tels que $au + bv = d$. En particulier, a et b sont premiers entre eux si et seulement si, il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$.*

Démonstration. — La première partie se déduit immédiatement du théorème 4.18.
Il reste à montrer une partie de l'équivalence. Supposons l'existence d'une relation de Bézout de la forme $au + bv = 1$. Alors, $1 \in a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ et donc $d = 1$. □

Corollaire 4.21 **(Lemme de Gauss)**. — *Soient a et b deux entiers premiers entre eux et soit $c \in \mathbb{Z}$. Si $a|bc$, alors $a|c$.*

Démonstration. — Comme $\text{pgcd}(a, b) = 1$, on a la relation de Bézout $au + bv = 1$ pour deux entiers u et v. Alors $auc + bvc = c$. Comme $a|bc$ et $a|auc$, d'après la proposition 4.6 (iii) on en déduit que $a|c$. □

Corollaire 4.22. — *Soient a et b deux entiers premiers entre eux divisant c. Alors $ab|c$.*

Démonstration. — On écrit la relation de Bézout $au + bv = 1$ avec $u, v \in \mathbb{Z}$. Alors

$$c = c \times 1 = cau + cbv.$$

Comme $a|c$ et $b|c$, on écrit également $c = a\alpha$ et $c = b\beta$, avec $\alpha, \beta \in \mathbb{Z}$. Et ainsi on trouve

$$c = b\beta au + a\alpha bv = ab(u\beta + v\alpha),$$

ce qui signifie exactement que $ab|c$. □

Corollaire 4.23. — *Soient trois entiers a, b, c tels que $\text{pgcd}(a, b) = \text{pgcd}(a, c) = 1$. Alors $\text{pgcd}(a, bc) = 1$.*

Démonstration. — On écrit les relations de Bézout $au + bv = 1$ et $au' + cv' = 1$ avec $u, u', v, v' \in \mathbb{Z}$, puis on les multiplie pour arriver à

$$a(auu' + cuv' + bu'v) + bcvv' = 1,$$

qui indique, d'après le corollaire 4.20, que $\text{pgcd}(a, bc) = 1$. □

Corollaire 4.24. — *Soient a et b deux entiers non nuls. Alors l'équation diophantienne $ax + by = k$ a des solutions entières x et y si et seulement si,* $\mathrm{pgcd}(a, b)|k$.

Démonstration. — Soit $d = \mathrm{pgcd}(a, b)$.
Supposons que x et y satisfont la relation $ax + by = k$. Alors $k \in a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ et donc $k\mathbb{Z} \subset d\mathbb{Z}$. Par la proposition 4.14, on en déduit que $d|k$.
Réciproquement, supposons que $d|k$. Alors il existe $\alpha \in \mathbb{Z}$ tel que $k = d\alpha$. En utilisant la relation de Bézout, il vient $k = d\alpha = au\alpha + bv\alpha$, et ainsi le couple $(x, y) = (u\alpha, v\alpha)$ est solution de l'équation diophantienne considérée. □

4.2.3. Algorithme d'Euclide. — L'algorithme d'Euclide va reposer sur le lemme suivant

Lemme 4.25. — *Soient a et b deux entiers non nuls. Si $b = aq + r$, alors* $\mathrm{pgcd}(a, b) = \mathrm{pgcd}(a, r)$*, avec la convention que* $\mathrm{pgcd}(a, 0) = |a|$.

Démonstration. — Il suffit alors de vérifier que l'ensemble des diviseurs communs à a et b coïncide avec l'ensemble des diviseurs communs à a et r. En effet, si $d|a$ et $d|b$ alors d'après la proposition 4.6 (iii), $d|(a - bq)$, c'est à dire que $d|r$. Par contre si $d|a$ et $d|r$, alors toujours suivant la proposition 4.6, $d|(bq + r)$ et donc $d|b$. □

Ce lemme indique que si l'on part de la division euclidienne de b par a, alors $\mathrm{pgcd}(b, a) = \mathrm{pgcd}(a, r)$ avec $r < |a|$: on a remplacé b par r qui est plus petit. On propose de continuer ce processus pour aboutir au calcul du PGCD de deux entiers (c'est l'algorithme d'Euclide).
Soient deux entiers non nuls a et b. Posons $a_1 = b$, $a_2 = a$ et considérons a_3 le reste de la division euclidienne de a_1 par a_2. Alors d'après le lemme 4.25, $\mathrm{pgcd}(b, a) = \mathrm{pgcd}(a_1, a_2) = \mathrm{pgcd}(a_2, a_3)$, avec $0 \leqslant a_3 < a_2 < |a|$. On continue le processus pour obtenir une suite $(a_n)_n$, où a_{n+2} est le reste de la division euclidienne de a_n par a_{n+1} et où $0 \leqslant a_{n+1} < \cdots < |a|$. La suite d'entiers positifs $(a_n)_n$ est donc strictement décroissante et minorée par 0 : il existe n_0 tel que $a_{n_0} = 0$. Le lemme 4.29 indique alors que $\mathrm{pgcd}(b, a) = \mathrm{pgcd}(a_1, a_2) = \mathrm{pgcd}(a_2, a_3) = \cdots = \mathrm{pgcd}(a_{n_0-1}, a_{n_0}) = a_{n_0-1}$. Ainsi le PGCD de a et b est le dernier entier non nul de la suite (a_n).
Montrons alors comment l'algorithme d'Euclide donne aussi une relation de Bézout. Notons $d = \mathrm{pgcd}(a, b) = a_{n_0-1}$. Alors par définition, $a_{n_0-3} = q_{n_0-2}a_{n_0-2} + d$ pour un certain entier q_{n_0-2}, ce qui donne la relation de Bézout $a_{n_0-3} - q_{n_0-2}a_{n_0-2} = d$, ici se rappeler que $\mathrm{pgcd}(a_{n_0-3}, a_{n_0-2}) = d$. Toujours par définition, $a_{n_0-4} = q_{n_0-3}a_{n_0-3} + a_{n_0-2}$ pour un certain entier q_{n_0-3} et ainsi $a_{n_0-2} = a_{n_0-4} - q_{n_0-3}a_{n_0-3}$. On reporte dans l'égalité précédente pour arriver à

$$-a_{n_0-4}q_{n_0-2} + a_{n_0-3}(1 + q_{n_0-2}q_{n_0-2}) = d,$$

ce qui est exactement une relation de Bézout entre a_{n_0-4} et a_{n_0-3}. On continue ainsi ce processus pour arriver à une relation de Bézout entre a et b.

Exemple 4.26. — Prenons $b = 63$ et $a = 5$. La division euclidienne de 63 par 5 s'écrit

$$63 = 12 \times 5 + 3.$$

On effectue ensuite la division euclidienne de 5 par 3 pour arriver à

$$5 = 3 \times 1 + 2.$$

Puis ensuite la division euclidienne de 3 par 2

$$3 = 2 \times 1 + 1,$$

et enfin la division euclidienne de 2 par 1

$$2 = 2 \times 1 + 0.$$

Le dernier reste non nul est donc $d = 1$, c'est donc égal à $\text{pgcd}(13, 5)$.
On "remonte" maintenant les relations de Bézout en substituant les restes. On part de $1 = 3 - 2$ et on substitue le reste $r = 2$. Alors on obtient

$$1 = 3 - 2 = 3 - (5 - 3) = 3 \times 2 - 5$$

qui est une relation de Bézout entre 3 et 5. Puis on substitue le reste $r = 3$ pour obtenir

$$1 = 3 \times 2 - 5 = 2 \times (63 - 12 \times 5) - 5 = 2 \times 63 + 5(-2 \times 12 - 1) = 2 \times 63 - 25 \times 5.$$

On a donc ainsi obtenu la relation de Bézout suivante entre a et b :

$$2a - 25b = 1.$$

4.3. Nombres premiers. —

Définition 4.27. — Un entier $p > 1$ est un nombre premier si les seuls diviseurs positifs de p sont 1 et p.

Exemple 4.28. — Les entiers $2, 3, 5, 7, \cdots$ sont des nombres premiers.

Commençons par donner le lemme d'Euclide.

Lemme 4.29. — *Soient $a, b \in \mathbb{Z}$ et soit p un nombre premier. Si $p|ab$, alors $p|a$ ou $p|b$.*

Démonstration. — Comme les seuls diviseurs positifs de p sont 1 et p, on a ou bien $\text{pgcd}(a, p) = 1$ ou bien $\text{pgcd}(a, p) = p$.
Si $\text{pgcd}(a, p) = 1$, alors d'après le lemme de Gauss 4.21, $p|b$.
Si $\text{pgcd}(a, p) = p$, alors $p|a$. □

***Théorème 4.30* (fondamental de l'arithmétique)**. — *Tout entier non nul n est, au signe près, le produit de nombres premiers uniquement déterminés à l'ordre près. Ou encore l'entier n s'écrit*

$$n = \pm p_1^{n_1} \cdots p_k^{n_k},$$

où les p_i sont des nombres premiers deux à deux différents et où les n_i sont des entiers plus grand que 1. Les entiers n_i sont uniques.

Démonstration. — *Existence.* On montre la montre par récurrence sur n. Si $n = 2$, c'est vrai (2 est un nombre premier). Supposons que tout nombre plus petit que n s'écrit comme produit de nombres premiers. Regardons $n + 1$. Alors si $n + 1$ est un nombre premier, la propriété est vraie à l'ordre $n + 1$. Si $n + 1$ n'est pas premier, il existe $a, b \geqslant 2 \in \mathbb{N}$ tels que $n + 1 = ab$; en particulier $a, b \leqslant n$. On leur applique l'hypothèse de récurrence, pour obtenir que finalement $n + 1$ s'écrit bien comme produit de nombres premiers..

Unicité. Là aussi, on raisonne par récurrence. C'est vrai pour $n = 2$ et l'on suppose que c'est vrai pour tout entier plus petit que n. On écrit alors $n+1 = p_1^{n_1} \cdots p_k^{n_k} = q_1^{m_1} \cdots q_l^{m_l}$, où les p_i et q_j sont des nombres premiers, deux à deux distincts pour les p_i (de même pour les q_j), $n_i, m_j \geqslant 1$. Par le lemme d'Euclide 4.29, le nombre premier p_1 divise l'un des nombres premiers q_i ; comme q_i est un nombre premier il vient $p_1 = q_i$; quitte à reprendre la numérotation on suppose que $p_1 = q_1$. On simplifie par p_1 pour arriver à l'égalité

$$\frac{n+1}{p_1} = p_1^{n_1-1} p_2^{n_2} \cdots p_k^{n_k} = q_1^{m_1-1} q_2^{m_2} \cdots q_l^{m_l}.$$

Comme $(n+1)/p_1 < n$, l'hypothèse de récurrence s'applique et l'on en déduit l'unicité souhaitée : on a $k = l$ et quitte à reprendre la numérotation, il vient $n_i = m_i$, pour $i = 1, \cdots, k$. □

Théorème 4.31. — *L'ensemble des nombres premiers est infini.*

Démonstration. — Supposons l'ensemble des nombres premiers fini. Notons par $\{p_1, \cdots, p_k\}$ cet ensemble. Posons alors $N = p_1 \times \cdots \times p_k$ l'entier égal au produit de ces nombres, et soit $n = N + 1$. Soit $p \in \{p_1, \cdots, p_k\}$ un nombre premier divisant n. Il existe un entier b tel que $bp = n = N + 1 = p_1 \cdots p_k + 1$. On obtient alors $p(b - N/p) = 1$, où $N/p \in \mathbb{N}$ car p est l'un des p_i. On a donc obtenu que $p|1$, ce qui est absurde. □

Définition 4.32. — Soit a un entier non nul et soit p un nombre premier. La valuation p-adique de a, notée $v_p(a)$, est le plus entier $n \geqslant 0$ tel que $p^n|a$. En d'autres termes, $a = p^{v_p(a)} n_0$, avec $\mathrm{pgcd}(p, n_0) = 1$. Par convention, on pose $v_p(0) = \infty$.

On a les propriétés suivantes :

Proposition 4.33. — *Soient a et b deux entiers et soit p un nombre premier. Il vient*

(i) $v_p(ab) = v_p(a) + v_p(b)$,

(ii) $v_p(a + b) \geqslant \min(v_p(a), v_p(b)$ *avec égalité si* $v_p(a) \neq v_p(b)$.

Démonstration. — Ecrivons $a = p^{v_p(a)} a_0$ et $b = p^{v_p(b)} b_0$ avec p premier à a_0 et b_0 (ou encore $p \nmid a_0$ et $p \nmid b_0$; remarquons que par le lemme de Gauss 4.21 cela implique que $p \nmid a_0 b_0$).
(i) Alors $ab = p^{v_p(a)+v_p(b)} a_0 b_0$, et comme $p \nmid a_0 b_0$, il vient $v_p(ab) = v_p(a) + v_p(b)$.
(ii) Soit $m = \min(v_p(a), v_p(b))$; supposons que $m = v_p(a)$. Alors $a + b = p^m(a_0 + p^{v_p(b)-m} b_0)$, ce qui montre que $v_p(a + b) \geqslant m$. Si de plus $v_p(b) > m$, alors $p|(p^{v_p(b)-m} b_0)$. Mais comme $p \nmid a_0$, il vient que $p \nmid (a_0 + p^{v_p(b)-m} b_0)$ et ainsi $v_p(a + b) = m$. □

La connaissance de la factorisation d'un entier en produit de nombres premiers permet de donner la caractérisation du PGCD (et du PPCM).

Proposition 4.34. — *Soient a et b deux entiers non nuls. On a* $v_p(\mathrm{pgcd}(a, b)) = \min(v_p(a), v_p(b))$ *et* $v_p(\mathrm{ppcm}(a, b)) = \max(v_p(a), v_p(b))$.

Démonstration. — Immédiat. □

Terminons par le théorème suivant.

***Théorème 4.35* (Petit théorème de Fermat).** — *Soit p un nombre premier. Pour tout entier a, le nombre p divise $a^p - a$.*

Démonstration. — Montrons le par récurrence pour $a \geqslant 0$. C'est vrai pour $a = 0$. Regardons alors $(a+1)^p - (a+1)$. Par la formule du binôme de Newton, on a $p|\big((a+1)^p - (a^p+1)\big)$. Par l'hypothèse de récurrence, $p|(a^p - a)$, ainsi par la proposition 4.6 (iii), $p|\big((a+1)^p - (a^p+1) + a^p - a\big)$, c'est à dire $p|\big((a+1)^p - (a+1)\big)$.
Ainsi la relation de divisibilité est vraie pour $a \geqslant 0$, ce qui implique facilement qu'elle est vraie pour tout $a \in \mathbb{Z}$. □

4.4. Exercices. —

Exercice 30. — *(i) Donner la liste complète des diviseurs de* 20, 50 *et* 55.

(ii) En déduire $\mathrm{pgcd}(20, 50)$, $\mathrm{pgcd}(20, 55)$ *et* $\mathrm{pgcd}(50, 55)$.

Exercice 31. — *Déterminer* $6\mathbb{Z} + 14\mathbb{Z}$, $6\mathbb{Z} + 21\mathbb{Z}$, $14\mathbb{Z} + 21\mathbb{Z}$ *et* $6\mathbb{Z} + 14\mathbb{Z} + 21\mathbb{Z}$.

Exercice 32. — *Que vaut* $\mathrm{pgcd}(222, 344)$ *? Déterminer deux entiers $x, y \in \mathbb{Z}$ tels que* $222x + 344y = 2$.

Exercice 33. — *Résoudre les équations diophantiennes suivantes :*

- $2018x + 203y = 1$.
- $2019x + 203y = 1$.

Exercice 34. — *Trouver les entiers $a \in \mathbb{Z}$ tels que l'équation $4558x + 9546y = a$ possède une solution $x, y \in \mathbb{Z}$.*

Exercice 35. — *Etant donnés $a \in \mathbb{Z}$, $b = \pm 1$, soit la suite $(u_n)_{n\in\mathbb{N}}$ définie par*

$$u_0, u_1 \in \mathbb{Z} \text{ et, pour } n \geqslant 0,\ u_{n+2} = au_{n+1} + bu_n.$$

Montrer que pour tout entier $n \geqslant 1$, on a $\mathrm{pgcd}(u_{n+1}, u_n) = \mathrm{pgcd}(u_1, u_0)$.

Exercice 36. — *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 $1 \leqslant d < n$ et $d \mid n$). Vérifier que* 6, 28 *et* 496 *sont parfaits.*

Exercice 37. — *Donner la liste des nombres premiers plus petits que* 150.

Exercice 38. — *Les nombres de la forme $F_n = 2^{2^n} + 1$, $n \in \mathbb{N}$, sont appelés nombres de Fermat.*

1. *Calculer F_0, F_1, F_2, F_3 F_4.*
2. *Montrer que ces nombres sont des nombres premiers.*
3. *Vérifier que F_5 est divisible par* 641.
4. *Montrer que si $2^k + 1$ est un nombre premier alors k est une puissance de* 2.

Exercice 39. — *Les nombres de la forme $M_n = 2^n - 1$ sont appelés nombres de Mersenne.*

1. *Calculer M_2, M_3, M_4, M_5, M_7, M_{11}.*
2. *Factoriser ces nombres.*
3. *Montrer que si M_n est un nombre premier alors n est un nombre premier.*
4. *Montrer que si M_n est un nombre premier alors $2^{n-1}M_n$ est un nombre parfait.*

5. Congruences

5.1. L'ensemble $\mathbb{Z}/n\mathbb{Z}$. — On fixe un entier $n \geqslant 0$.

Définition 5.1. — On dit que les entiers a et b sont congrus modulo n si $n|(a-b)$, ou encore s'il existe $\alpha \in \mathbb{Z}$ tel que $a = b+\alpha n$. On note $a \equiv b\ (n)$, ou encore $a \equiv b$ (modulo n), ou encore $a \equiv_n b$.

Remarque 5.2. — Pour $n = 0$, on a $a \equiv_n b$ si et seulement si, $a = b$.

Proposition 5.3. — *Soient $a, b, c \in \mathbb{Z}$. Alors*

(i) $a \equiv_n b$ si et seulement si, $a \equiv_n b$ (la relation "modulo" est symétrique),

(ii) $a \equiv_n a$ (la relation "modulo" est réflexive),

(iii) si $a \equiv_n b$ et $b \equiv_n c$, alors $a \equiv_n c$ (la relation "modulo" est transitive).

Démonstration. — (i) C'est immédiat : on a $a = b + \alpha n$, $\alpha \in \mathbb{Z}$, si et seulement si, $b = a - \alpha n$.
(ii) On a $a = a + 0 \times n$.
(iii) Si $a = b + \alpha n$ et $b = c + \beta n$ avec $\alpha, \beta \in \mathbb{Z}$, alors $a = c + n(\alpha + \beta)$. □

Remarque 5.4. — La relation "être congru à" est une relation d'équivalence sur $\mathbb{Z}$. Cette relation est appelée relation de congruence.

Définition 5.5. — Etant donné $a \in \mathbb{Z}$, on pose $[a]_n = \{x \in \mathbb{Z}, x \equiv_n a\}$. Le sous-ensemble $[a]_n$ de $\mathbb{Z}$ est appelé classe de congruence de a modulo n. On le note également $\overline{a}$ (lorsqu'il n'y a pas d'ambiguité possible). L'ensemble des classes de congruence est noté $\mathbb{Z}/n\mathbb{Z}$. On parle aussi du quotient $\mathbb{Z}/n\mathbb{Z}$.

Remarque 5.6. — On a donc $[a]_n = a + n\mathbb{Z}$.

L'ensemble des classes $\mathbb{Z}/n\mathbb{Z}$ forme une partition de $\mathbb{Z}$: cela signifie que $\mathbb{Z}$ est réunion disjointe des classes d'équivalence. Par exemple, le lemme suivant illustre cette partition :

Lemme 5.7. — *Soient deux entiers a et b tels que $[a]_n \cap [b]_n \neq \varnothing$. Alors $[a]_n = [b]_n$.*

Démonstration. — Soit $z_0 \in [a]_n \cap [b]_n$. Alors $z_0 \equiv_n a$ et $z_0 \equiv_n b$. Il suffit de montrer une inclusion. Soit $z \in [a]_n$. Alors $z \equiv_n a$ et par transitivité, $z \equiv_n z_0$ puis $z \equiv_n b$, et ainsi $z \in [b]_n$. □

Précisons la partition de $\mathbb{Z}$ par $\mathbb{Z}/n\mathbb{Z}$.

Proposition 5.8. — *Soit $n > 1$. On a $\mathbb{Z} = [0]_n \cup [1]_n \cup \cdots \cup [n-1]_n$, et ces classes sont deux à deux disjointes. En particulier, $|\mathbb{Z}/n\mathbb{Z}| = n$.*

Démonstration. — Soit $b \in \mathbb{Z}$. Effectuons la division euclidienne de b par n : il existe q et r, avec $0 \leqslant r < n$, tels que $b = nq + r$: ce qui signifie que $b \in [r]_n$ avec $r \in \{0, 1, \cdots, n-1\}$. Il reste à montrer que ces classes d'équivalence sont disjointes. Soient donc $k, k' \in \{0, \cdots, n-1\}$ tels que $[k]_n = [k']_n$. Alors n divise $k-k'$ avec $-n < k-k' < n$, et donc $k - k' = 0$. □

Remarque 5.9. — Quand $n = 0$ il y a autant de classes que d'entiers.

Pour toute la suite, on suppose $n > 0$.

Soit donc $a \in \mathbb{Z}$. Alors il existe un unique entier $k \in \{0, \cdots, n-1\}$ tel que $a \in [k]_n$. Comme $a \in [a]_n \cap [k]_n$ d'après la proposition 5.3 (ii), il vient $[a]_n = [k]_n$ d'après le lemme 5.7.

Définition 5.10. — Si $x \in [a]_n$, on dit que x est un représentant de la classe $[a]_n$. L'entier $k \in \{0, \cdots, n-1\}$ tel que $k \in [a]_n$ est appelé représentant principal de la classe de a modulo n.

Exemple 5.11. — Soit $n = 131$ et $a = 2345$. Alors la division euclidienne de a par n s'écrit : $2345 = 17 \times 131 = 118$. Ainsi $[2345]_{131} = [118]_{131}$, et 118 est le représentant principal de la classe de 2345 modulo 131.

Proposition 5.12. — *Soient $a, b, c, d \in \mathbb{Z}$.*

(i) *Si $a \equiv_n b$ et $c \equiv_n d$, alors $a + c \equiv_n b + d$ et $ac \equiv_n bd$.*

(ii) *Si $a \equiv_n b$, alors pour tout entier $r \geqslant 1$, il vient $a^r \equiv_n b^r$.*

(iii) *Si a est premier à n, il existe $a' \in \mathbb{Z}$ tel que $aa' \equiv_n 1$.*

(iv) *Si c est premier à n et si $ac \equiv_n bc$ alors $a \equiv_n b$.*

Démonstration. — (i) Si $n|(a-b)$ et $n|(c-d)$ alors $n|(a-b)+(c-d)$ d'après la proposition 4.6 (iii). Ecrivons ensuite $a = b + \alpha n$ puis $c = d + \beta n$ avec $\alpha, \beta \in \mathbb{Z}$. Alors $ac = bd + n(d\alpha + b\beta + n\alpha\beta)$, ce qui montre que $n|(ac - bd)$.
(ii) C'est une conséquence du point précédent : en prenant $c = a$ et $b = d$, on a $a^2 \equiv_n b^2$, etc.
(iii) Comme $\text{pgcd}(a, n) = 1$, on a la relation de Bézout $au + nv = 1$ pour deux entiers u, v. Ainsi, $n|(au - 1)$ et donc $au \equiv_n 1$. Prendre par exemple $a' = u$.
(iv) Comme c est premier à n, il existe $c' \in \mathbb{Z}$ tel que $cc' \equiv_n 1$. En utilisant (i), on obtient $acc' \equiv_n bcc'$, c'est à dire $a \equiv_n b$. □

Remarque 5.13. — Attention la simplification (iv) de la proposition 5.12 n'a pas toujours lieu. En effet, prenons $n = 2$, $a = 1$ et $b = 2$. Alors $2a \equiv_2 2b$ mais $a \not\equiv_2 b$.

5.2. Congruences simultanées. — Dans ce paragraphe nous montrons

***Théorème 5.14* (des restes chinois).** — *Soient deux entiers $m, n \geqslant 1$, avec $\text{pgcd}(m, n) = 1$. Soient $a, b \in \mathbb{Z}$. Alors le système suivant d'inconnue $x \in \mathbb{Z}$*

$$(S) \quad \begin{cases} x \equiv_m a \\ x \equiv_n b \end{cases}$$

admet une solution x_0 dans l'ensemble $\{0, \cdots, mn-1\}$. De plus, les entiers de $[x_0]_{mn}$ sont exactement les solutions de (S).

Démonstration. — Nous allons deux preuves de l'existence d'une solution, la second preuve donne une façon explicite pour trouver une solution.
Première preuve. Soit l'application :

$$\begin{array}{rcl} \theta : \mathbb{Z}/mn\mathbb{Z} & \to & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ [a]_{mn} & \mapsto & \big([a]_m, [a]_n\big) \end{array}$$

L'application est bien définie : en effet, si $[a]_{mn} = [b]_{mn}$, alors $[a]_m = [b]_m$ et $[a]_n = [b]_n$. Par le corollaire 4.22, θ est injective : en effet si $[a]_{mn}$ et $[b]_{mn}$ sont tels que $[a]_m = [b]_m$ et $[a]_n = [b]_n$, alors n et m divisent $a-b$ et donc mn divise $a-b$, c'est à dire $[a]_{mn} = [b]_{mn}$. Comme $|\mathbb{Z}/mn\mathbb{Z}| = mn = |\mathbb{Z}/m\mathbb{Z}| \cdot |\mathbb{Z}/n\mathbb{Z}|$, on en déduit que l'application θ est surjective, ce qui garantit donc l'existence d'une solution à (S).

Seconde preuve. Partons d'une relation de Bézout $mu + nv = 1$ avec $u, v \in \mathbb{Z}$. Ecrivons

$$(b-a) = 1 \times (b-a) = (mu+nv)(b-a),$$

ce qui donne

$$mu(b-a) + a = b - nv(b-a).$$

Posons alors $c = mu(b-a) + a$. Alors $c \in [a]_m$ et $c \in [b]_n$, et ainsi c est une solution de (S). Soit alors x_0 le représentant principal de la classe de congruence $[c]_{mn}$ de c modulo mn. On a $x_0 \equiv_{mn} c$ et $x_0 \equiv_{mn} c$, ce qui implique $x_0 \in [c]_m = [a]_n$ et $x_0 \in [c]_n = [b]_n$.

Soit y une autre solution de (S). Alors $y \equiv_m a \equiv_m x_0$ et $y \equiv_n b \equiv_n x_0$, par conséquent $m|(y - x_0)$ et $n|(y - x_0)$. Par le corollaire 4.22, on a $mn|(y - x_0)$ et ainsi $y \in [x_0]_{mn}$. La réciproque est immédiate. □

Exemple 5.15. — On cherche à résoudre le système suivant $\begin{cases} x \equiv_5 3 \\ x \equiv_3 2 \end{cases}$. On part de la relation de Bézout $2 \times 5 - 3 \times 3 = 1$. Alors $x = 2 \times 5 \times (3-2) + 3 = 13$ est une solution particulière. Ainsi, les solutions du système étudié sont les entiers de $[13]_{15}$.

5.3. $\mathbb{Z}/n\mathbb{Z}$ et ses lois. — On se fixe un entier $n \geqslant 1$. L'objectif de ce paragraphe est de munir $\mathbb{Z}/n\mathbb{Z}$ de deux lois $+$ (addition) et $\cdot$ (multiplication) qui en font un *anneau commutatif* (voir la définition 8.14 de la section 8).

5.3.1. L'anneau $\mathbb{Z}/n\mathbb{Z}$. — Pour deux classes de congruences $[a]_n$ et $[b]_n$ de $\mathbb{Z}/n\mathbb{Z}$, on pose :

- $[a]_n + [b]_n = [a+b]_n$,
- $[a]_n \cdot [b]_n = [ab]_n$.

Remarquons immédiatement que ces lois sont bien définies. En effet, si a' est autre représentant de la classe $[a]_n$, il vient $a + b \equiv_n a' + b$ et $ab \equiv_n a'b$.

Théorème 5.16. — *L'ensemble $\mathbb{Z}/n\mathbb{Z}$ muni des lois $+$ et $\cdot$ est un anneau commutatif unitaire. De plus,*

(i) l'élément neutre pour l'addition est la classe $[0]_n$,

(ii) l'opposé de $[a]_n$ est la classe $[-a]_n$,

(iii) le neutre pour la multiplication est la classe $[1]_n$.

Démonstration. — C'est une simple vérification. □

Définition 5.17. — Lorsque $[a]_n$ admet un inverse (pour la multiplication), on le note $[a]_n^{-1}$. On note par $(\mathbb{Z}/n\mathbb{Z})^\times$ l'ensemble des classes $[a]_n$ inversibles de $\mathbb{Z}/n\mathbb{Z}$.

Pour $k \in \mathbb{N}$, on pose $[a]_n^k = \overbrace{[a]_n \cdot [a]_n \cdots [a]_n}^{k}$ et $k[a]_n = \overbrace{[a]_n + [a]_n \cdots + [a]_n}^{k}$, puis $-k[a]_n = k[-a]_n$.
Enonçons quelques propriétes de calcul.

Proposition 5.18. — *Soient $a, b \in \mathbb{Z}$, on a*

(i) pour $k \in \mathbb{Z}$, $k[a]_n = [ka]_n$,

(ii) pour $k \in \mathbb{N}$, $[a]_n^k = [a^k]_n$,

(iii) pour $k \in \mathbb{Z}$ premier à n tel $k[a]_n = k[b]_n$, alors $[a]_n = [b]_n$.

Démonstration. — (i) et (ii) sont immédiat.
(iii) est conséquence de la proposition 5.12 (iv). □

Remarque 5.19. — Observons que $k[a]_n = [ka]_n = [k]_n[a]_n$.

Notons que l'inverse (pour la multiplication) n'existe pas toujours. En effet,

Proposition 5.20. — *Soit $[a]_n \in \mathbb{Z}/n\mathbb{Z}$. Alors $[a]_n$ admet un inverse si et seulement si,* $\text{pgcd}(a, n) = 1$. *Si tel est le cas, alors pour tout $k \in \mathbb{N}$, il vient $([a]_n^{-1})^k = [a^k]_n^{-1}$.*

Démonstration. — Si $[a]_n$ admet un inverse cela signifie qu'il existe $b \in \mathbb{Z}$ tel que $[1]_n = [a]_n \cdot [b]_n = [ab]_n$, par conséquent que $n|(ab-1)$, ce qui signifie exactement qu'il existe $u \in \mathbb{Z}$ tel que $nu + ab = 1$, c'est à dire que $\text{pgcd}(n, a) = 1$ d'après le corollaire 4.20.
Réciproquement, si $\text{pgcd}(n, a) = 1$, alors d'après la proposition 5.12 (iii), il existe $a' \in \mathbb{Z}$ tel que $[a]_n[a']_n = [1]_n$.
L'égalité sur les puissances est conséquence de la proposition 5.18 (ii). □

Définition 5.21. — La fonction (ou indicatrice) d'Euler φ est la fonction définie pour $n \geqslant 2$ par $\varphi(n) = |\{k, 0 < k < n-1, \text{pgcd}(k, n) = 1\}|$. On a donc $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$, où $(\mathbb{Z}/n\mathbb{Z})^\times$ est l'ensemble des classes inversibles.

Exemple 5.22. — Considérons l'ensemble de congruence $\mathbb{Z}/14\mathbb{Z}$. Comme $\text{pgcd}(3, 14) = 1$, la classe $[3]_{14}$ admet un inverse. Il s'obtient par la relation de Bézout entre 3 et 14. En effet de la relation $5 \times 3 - 1 \times 14 = 1$, on en déduit que $[5]_{14}[3]_{14} = [1]_{14}$ et ainsi $[3]_{14}^{-1} = [5]_{14}$.

Théorème 5.23. — *Soit p un nombre premier. Alors*

(*i*) *pour tout entier $a \in \mathbb{Z}$, il vient $[a]_p^p = [a]_p$,*

(*ii*) *toute classe non nulle $[a]_p$, c'est à dire telle que $[a]_p \neq [0]_p$, admet un inverse $[a]_p^{-1}$, ou encore $\varphi(p) = p - 1$,*

(*iii*) *pour toute classe non nulle $[a]_p$, il vient $[a]_p^{-1} = [a^{p-2}]_p$,*

(*iv*) *les seules classes $[a]_p$ pour lesquelles $[a]_p = [a]_p^{-1}$ sont les classes $[1]_p$ et $[-1]_p = [p-1]_p$,*

(*v*) *si $[a]_p[b]_p = [0]_p$ alors, ou bien $[a]_p = [0]_p$, ou bien $[b]_p = [0]_p$.*

Démonstration. — (i) : c'est une conséquence du petit théorème de Fermat 4.35.
(ii) et (iii) : Comme $p|a(a^{p-1}-1)$, d'après le lemme de Gauss 4.21, ou bien $p|a$ ou bien $p|(a^{p-1}-1)$. Si $[a]_p$ est la classe non nulle, cela signifie exactement que p ne divise pas a et donc que $p|(a^{p-1}-1)$, ce qui du point de vue des classes implique que $[a]_p^{p-1} = [1]_p$. En remarquant que $[a]_p^{p-1} = [a]_p[a]_p^{p-2} = [a^{p-2}]_p$, on a donc que $[a]_p$ est inversible d'inverse $[a^{p-2}]_p$.
(iv) : soit $[a]_p$ telle que $[a]_p = [a]_p^{-1}$, alors $[a]_p^2 = [1]_p$, ce qui signifie que $[a^2-1]_p = [0]_p$. Ainsi p divise $(a-1)(a+1)$, et donc par le lemme de Gauss 4.21, ou bien $p|(a-1)$ ou bien $p|(a+1)$.
(v) Ici $p|ab$ et comme p est premier, le résultat se déduit du lemme 4.29. □

Exemple 5.24. — Dans $\mathbb{Z}/11\mathbb{Z}$, on a

$$\begin{aligned}
[5]_{11}^{-1} &= [5]_{11}^{9} \\
&= [5]_{11}^{2^3}[5]_{11} \\
&= [5^2]_{11}^{4}[5]_{11} \\
&= ([3]_{11}^{2})^2[5]_{11} \\
&= [81]_{11}[5]_{11} \\
&= [4]_{11}[5]_{11} \\
&= [9]_{11}
\end{aligned}$$

Terminons avec le :

***Théorème 5.25* (de Wilson)**. — *Soit p un nombre premier. Alors $(p-1)! \equiv_p -1$.*

Démonstration. — D'après le théorème 5.23 (iv), toute classe $[k]_p$ avec $1 < k < p-1$ a un inverse $[k']_p$ avec $1 < k' < p-1$ et $k \neq k'$. Ainsi,

$$[2]_p \cdot [3]_p \cdots [p-2]_p = [1]_p,$$

et ainsi

$$[1]_p \cdot [2]_p \cdots [p-1]_p = [1]_p \cdot [p-1]_p = [p-1]_p = [-1]_p.$$

Par conséquent, p divise $(p-1)! + 1$, ce qui est exactement le résultat recherché. □

5.4. Le groupes multiplicatif. — On se fixe un entier $n \geqslant 1$.

5.4.1. — Le groupe additif $(\mathbb{Z}/n\mathbb{Z}, +)$, noté $\mathbb{Z}/n\mathbb{Z}$, est engendré par $\overline{1}$: en effet $\overline{k} = k\overline{1}$.

Théorème 5.26. — *Une classe $[k]_n$ engendre le groupe $\mathbb{Z}/n\mathbb{Z}$ si et seulement si,* $\text{pgcd}(k, n) = 1$.

Démonstration. — Voir le théorème 8.13. □

On a alors le théorème suivant :

Théorème 5.27. — *On a* $n = \sum_{d|n} \varphi(d)$.

Démonstration. — Soit $k \in \{0, \cdots n-1\}$. Alors $[k]_n \in \mathbb{Z}/n\mathbb{Z}$ est d'ordre un diviseur d de n (d'après la proposition 8.7) et il engendre l'unique sous-groupe H de G d'ordre d (voir le théorème 8.12). Or d'après le théorème 8.13, le groupe H (et donc $\mathbb{Z}/n\mathbb{Z}$) contient exactement $\varphi(d)$ éléments d'ordre d. D'où la formule annoncée. □

5.4.2. — Considérons maintenant le groupe multiplicatif.

Proposition 5.28. — *L'ensemble $(\mathbb{Z}/n\mathbb{Z})^\times$ muni de la loi $\cdot$ forme un groupe commutatif de cardinal $\varphi(n)$.*

Démonstration. — C'est immédiat, voir la proposition 8.17. □

On a vu que lorsque $n = p$ est un nombre premier, $(\mathbb{Z}/p\mathbb{Z})^\times = \{[1]_p, \cdots, [p-1]_p\}$ et ainsi $\varphi(p) = p - 1$. Pour le cas général, nous avons :

Théorème 5.29. — *Soit $n = p_1^{n_1} \cdots p_k^{n_k}$, où les p_i sont des nombres premiers deux à deux distincts et où les entiers n_i sont tous plus grand que 1. Alors $\varphi(n) = (p_1 - 1)p^{n_1-1} \cdots (p_k - 1)p^{n_k-1}$.*

Démonstration. — Commençons par le lemme suivant.

Lemme 5.30. — *Soit $m, n \geqslant 2$ deux entiers premiers entre eux. Alors $\varphi(nm) = \varphi(n)\varphi(m)$.*

Démonstration. — Nous avons vu dans la preuve du théorème 5.14 que l'application suivante :

$$\begin{array}{rcl} \theta : \mathbb{Z}/mn\mathbb{Z} & \to & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ [a]_{mn} & \mapsto & \big([a]_m, [a]_n\big) \end{array}$$

est bijective. Soit alors $[a]_{mn}$ inversible : cela signifie donc que $\text{pgcd}(a, mn) = 1$. L'image $\theta([a]_{mn})$ est un couple d'éléments $([a]_m, [a]_n)$ dans $(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$. Ainsi, θ induit une application θ' nécessairement injective de $(\mathbb{Z}/mn)^\times$ vers $(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n)^\times$. D'autre part on sait que θ est surjective. Donc pour $([b]_m, [c]_n) \in (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n)^\times$, il existe $a \in \mathbb{Z}$ tel que $[a]_m = [c]_m$ et $[a]_n = [c]_n$. Alors $m|(a-c)$ et $n|(a-c)$. Par le lemme 4.25, il vient $\text{pgcd}(a, m) = \text{pgcd}(b, m) = 1$ et $\text{pgcd}(a, n) = \text{pgcd}(c, n) = 1$. Par conséquent, $\text{pgcd}(a, mn) = 1$ par le corollaire 4.23. Ainsi par la proposition 5.20, $[a]_{mn} \in (\mathbb{Z}/mn\mathbb{Z})^\times$.

On vient de montrer que θ' est également une bijection. En considérant alors les cardinaux, on obtient le lemme. □

Nous avons besoin d'un second lemme

Lemme 5.31. — *Soit p un nombre premier et soit $m \geqslant 1$. Alors $\varphi(p^m) = (p-1)p^{m-1}$.*

Démonstration. — Cherchons le nombre N d'entiers a compris entre 1 et p^m et divisible par p. On aura alors $\varphi(p^k m) = p^m - N$. On écrit $a = pn_0$ avec $1 \leqslant n_0 < p^{m-1}$. Ainsi $N = p^{m-1}$. On a alors $\varphi(p^m) = p^m - p^{m-1} = (p-1)p^{m-1}$. □

Finissons la preuve du théorème 5.29 par récurrence sur k. Pour $k = 1$, c'est le cas où $n = p^m$ est la puissance d'un nombre premier p, et l'on a dans le lemme 5.31 que $|(\mathbb{Z}/p^m\mathbb{Z})^\times| = (p-1)p^{m-1}$. Partons alors de $n = p_1^{n_1} \cdots p_k^{n_k}$ et posons $n_0 = n/p_k^{n_k}$. Par hypothèse de récurrence, on suppose vrai le théorème pour n_0. On a $\operatorname{pgcd}(p_k^{n_k}, n_0) = 1$ et d'après le lemme 5.30, il vient $|(\mathbb{Z}/n\mathbb{Z})^\times| = |(\mathbb{Z}/p_k^{n_k}\mathbb{Z})^\times| \times |(\mathbb{Z}/n_0\mathbb{Z})^\times|$, le résultat s'en déduit. □

***Théorème 5.32* (d'Euler)**. — *Soit un entier a premier à $n \geqslant 2$. Alors $[a]_n^{\varphi(n)} = [1]_n$.*

Démonstration. — • Les résultats précédents permettent de montrer le théorème lorsque $n = p_1 \cdots p_k$, où les p_i sont des nombres premiers deux à deux distincts. En effet, soit a premier à n. Alors a est premier à chaque p_i. Par la théorème 5.23, il vient $[a^{(p_i-1)}]_{p_i} = [1]_{p_i}$. Ainsi, $[a_{p_1}]_{p_1-1}^{(p_2-1)\cdots(p_k-1)} = [1]_{p_1}^{(p_2-1)\cdots(p_k-1)} = [1]_{p_1}$ et, par conséquent, d'après le théorème 5.29 il vient $[a^{\varphi(n)}]_{p_1} = [1]_{p_1}$. Il en est de même pour chaque premier $p_i | n$. Ainsi, pour $i = 1, \cdots, k$, on a $p_i | (a^{\varphi(n)} - 1)$. Comme les p_i sont deux à deux distincts, on en déduit, d'après le corollaire 4.22, que le produit $p_1 \cdots p_k$ divise $a^{\varphi(n)} - 1$, ce qui signifie exactement que $[a^{\varphi(n)}]_n = [1]_n$.
• Pour le cas général où $n = p_1^{n_1} \cdots p_k^{n_k}$ nous avons besoin du corollaire 8.10 de la section Appendice 8. Partons de a premier à n, donc a est premier à chaque p_i et ainsi $[a]_{p_i^{n_i}} \in (\mathbb{Z}/p_i^{n_i})^\times$. Par le corollaire 8.10 et le lemme 5.31, il vient $[a]_{p_i^{n_i}}^{(p_i-1)p_i^{n_i-1}} = [1]_{p_i^{n_i}}$, ce qui implique, par le lemme 5.30, $[a]_{p_i^{n_i}}^{\varphi(n)} = [1]_{p_i^{n_i}}$. Ainsi $p_i^{n_i}$ divise $a^{\varphi(n)} - 1$ pour $i = 1, \cdots, k$. On conclut avec le corollaire 4.22. □

Remarque 5.33. — Le théorème 5.32 est la conséquence d'un résultat plus général, voir le corollaire 8.10 de l'Appendice §8.

5.5. Exercices. —

Exercice 40. — (*i*) *Déterminer les représentants principaux des classes de congruence suivantes :* $[223]_7$, $[354]_7$, $[1568]_7$.

(*ii*) *Parmi ces classes, a-t-on deux classes identiques ?*

Exercice 41. — *Soit $n \in \mathbb{N}$.*

(*i*) *Montrer que n est divisible par 3 si et seulement si la somme de ses chiffres est divisible par 3.*

(*ii*) *Montrer que n est divisible par 9 si et seulement si la somme de ses chiffres est divisible par 9.*

(*iii*) *Sur le modèle des deux caractérisations précédentes, donner une condition nécessaire et suffisante pour que n soit divisible par 11.*

Exercice 42. —

(*i*) *Quel est le reste de la division euclidienne de 13^{20} par 7 ?*

(*ii*) *Quel est le reste de la division euclidienne de 2017^{2018} par 5 ? par 11 ? par 15 ?*

(*iii*) *Soit $n \in \mathbb{N}$. Montrer que l'entier $5n^3 + n$ est divisible par 6.*

(*iv*) *Soit $n \in \mathbb{N}$. Montrer que l'entier $3^{2n+1} + 2^{n+2}$ est divisible par 7.*

(*v*) *Déterminer un entier $a \geqslant 0$ tel que, pour tout entier $n \in \mathbb{N}$, on ait : $3^{n+a} - 4^{4n+2} \equiv 0 \pmod{11}$.*

(*vi*) *Déterminer un entier $a \geqslant 0$ tel que, pour tout entier $n \in \mathbb{N}$, on ait : $5^{n+1} - 7^{3n+a} \equiv 0 \pmod{13}$.*

Exercice 43. —

(*i*) *Trouver les entiers $x \in \mathbb{Z}$ tels que $x \equiv 3 \pmod{7}$ et $x \equiv 5 \pmod{15}$.*

(*ii*) *Trouver les entiers $x \in \mathbb{Z}$ tels que $x \equiv 21 \pmod{37}$ et $x \equiv 130 \pmod{181}$.*

(*iii*) *Trouver le plus entier $x \in \mathbb{N}$ tels que $x \equiv 8 \pmod{14}$, $x \equiv 5 \pmod{23}$ et $x \equiv 13 \pmod{29}$.*

Exercice 44. — *Déterminer les tables d'addition et de multiplication de $\mathbb{Z}/6\mathbb{Z}$ et de $\mathbb{Z}/7\mathbb{Z}$. Préciser l'inverse de chaque classe (lorsque celle-ci existe).*

Exercice 45. —

(*i*) *Déterminer les inverses de $[11]_{23}$, $[35]_{13}$, $[13]_{35}$, et $[123]_{88}$.*

(*ii*) *Trouver les entiers $x \in \mathbb{Z}$ vérifiant $35x \equiv 2 \pmod{13}$.*

(*iii*) *Trouver les entiers $x \in \mathbb{Z}$ vérifiant $37x \equiv 2 \pmod{131}$.*

Exercice 46. —

(*i*) *Déterminer les carrés de $\mathbb{Z}/23\mathbb{Z}$.*

(*ii*) *Résoudre dans $\mathbb{Z}/23\mathbb{Z}$ l'équation $X^2 + 2X + [6]_{23} = [0]_{23}$.*

(*iii*) *Donner les entiers $x \in \mathbb{Z}$ tels que 23 divise $x^3 + 2x^2 + 6x$.*

Exercice 47. —

(*i*) *Déterminer les carrés de $\mathbb{Z}/29\mathbb{Z}$.*

(*ii*) *Donner les entiers $x \in \mathbb{Z}$ tels que 29 divise $x^2 + x - 1$.*

(*iii*) *Donner les entiers $x \in \mathbb{Z}$ tels que 29 divise $x^2 + x + 1$.*

6. Corps finis

Pour toute cette section on se fixe un nombre premier p et pour un entier k, on notera par $\overline{k}$ la classe $[k]_p$.

6.1. Structure multiplicative et logarithme discret. — Commençons par rappeler que toute classe non nulle de $\mathbb{Z}/p\mathbb{Z}$ admet un inverse, ce qui fait de $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ un corps fini de cardinal p (voir définition 8.18). On le note $\mathbb{F}_p$ (comme montré dans la section 8 théorème 8.19, tout corps ayant p éléments est isomorphe à $\mathbb{F}_p$).
Comme pour les sections précédentes, on note par $\mathbb{F}_p^\times = \{\overline{x} \in \mathbb{F}_p, \overline{x} \neq \overline{0}\}$.

Théorème 6.1. — *Soit le corps fini $\mathbb{F}_p$. Alors $\mathbb{F}_p^\times$ est un groupe cyclique d'ordre $p-1$.*

Démonstration. — On a déjà vu que $\mathbb{F}_p^\times$ est un groupe (commutatif) d'ordre $p-1$. Soit $\overline{x} \in \mathbb{F}_p^\times$, et soit d son ordre : on rappelle que c'est le plus petit entier $d > 0$ tel que $\overline{x}^d = \overline{1}$. D'après le corollaire 8.10 de la section 8, l'entier d divise $p-1$. Il vient alors que $\overline{x}$ est racine du polynôme $X^d - \overline{1}$. Ainsi, si l'on note par E_d l'ensemble des éléments de $\mathbb{F}_p^\times$ d'ordre d et par F_d les éléments de $\mathbb{F}_p$ racines de $X^d - \overline{1}$, on a $E_d \subset F_d$. Or le polynôme $X^d - \overline{1}$ a au plus d racines dans $\mathbb{F}_p$ (d'après le corollaire 6.14 à venir). Comme le sous-groupe $\langle\overline{x}\rangle$ de $\mathbb{F}_p^\times$ engendré par $\overline{x}$, de cardinal d (voir la proposition 8.8 de la section 8), est contenu dans F_d, on en déduit que $F_d = \langle\overline{x}\rangle$. Et ainsi, $E_d \subset \langle\overline{x}\rangle$. Un élément $\overline{x}^k$ est d'ordre d si et seulement si $\mathrm{pgcd}(k, d) = 1$ (d'après le théorème 8.13). Par conséquent $|E_d| = \varphi(d)$ quand E_d n'est pas vide. En conclusion, pour $d|(p-1)$, il vient $|E_d| \leqslant \varphi(d)$. On a alors

$$p - 1 = |\mathbb{F}_p^\times| = \sum_{d|(p-1)} |E_d| \leqslant \sum_{d|(p-1)} \varphi(d) = p - 1,$$

la dernière égalité résultant du théorème 5.27. Ceci implique alors que pour tout $d|(p-1)$, $|E_d| = \varphi(d)$, et en particulier que E_{p-1} est non-vide : il existe dans $\mathbb{F}_p^\times$ un élément a d'ordre $p-1$. Et ainsi $\mathbb{F}_p^\times = \langle a\rangle$. □

Définition 6.2. — Un élément a de $\mathbb{F}_p^\times$ d'ordre $p-1$ s'appelle une racine primitive de l'unité ; c'est aussi un générateur du groupe $\mathbb{F}_p^\times$.

Remarque 6.3. — Le corps $\mathbb{F}_p^\times$ contient donc $\varphi(p-1)$ racines primitives de l'unité.

On en arrive à la définition du logarithme discret.

Définition 6.4. — Soit a un générateur $\mathbb{F}_p^\times$. Pour tout $x \neq \overline{0}$, il existe un unique $k \in \{0, \cdots, p-2\}$ tel que $x = a^k$. L'entier k est par définition le logarithme de x (en base a) : on note alors $k = \log_a(x)$.

Remarque 6.5. — On a en particulier, $\log_a(a) = 1$ et $\log_a(\overline{1}) = 0$.

Remarque 6.6. — D'après le théorème 8.13, l'élément x est une racine primitive de l'unité si et seulement si, $\mathrm{pgcd}(p-1, \log_a(x)) = 1$.

Exemple 6.7. — Dans $\mathbb{F}_5^\times$, la classe $\overline{2}$ est d'ordre 4. Ainsi, $\log_{\overline{2}}(\overline{1}) = 0$, $\log_{\overline{2}}(\overline{2}) = 1$, $\log_{\overline{2}}(\overline{3}) = \log_{\overline{2}}(\overline{8}) = 3$ et $\log_{\overline{2}}(\overline{4}) = 2$.

Proposition 6.8. — *Soit a un générateur de $\mathbb{F}_p^\times$. Alors pour tout $x, y \in \mathbb{F}_p^\times$, il vient*

$$\log_a(xy) \equiv \log_a(x) + \log_a(y) \text{ (modulo } p-1).$$

Démonstration. — On écrit $x = a^k$ et $y = a^{k'}$ avec $0 \leqslant k, k' \leqslant p-2$. Si l'on note par r le reste de la division euclidienne de $k+k'$ par $p-1$, il vient $xy = a^{k+k'} = a^r$. Ainsi, $\log_a(x) + \log_a(y) = r \equiv_{p-1} k + k' = \log_a(x) + \log_a(y)$. □

Remarquons enfin le corollaire suivant :

Corollaire 6.9. — *Pour $x \in \mathbb{F}_p^\times$, on a*

$$\log a(x^{-1}) \equiv -\log_a(x) \text{ (modulo } p-1).$$

Démonstration. — C'est une conséquence de la proposition 6.8 associée au fait que $\log_a(1) = 0$.

□

6.2. Polynômes. — On se fixe le corps fini $\mathbb{F}_p$, et on considère $\mathbb{F}_p[X]$ l'ensemble des polynômes à coefficient dans $\mathbb{F}_p$. On munit $\mathbb{F}_p[X]$ des deux lois naturelles $+$, $\cdot$, issues de celles de $\mathbb{F}_p$.

Proposition 6.10. — *$(\mathbb{F}_p[X], +, \cdot)$ est un anneau (commutatif). Le groupe $\mathbb{F}_p^\times$ est exactement le groupe des inversibles de $\mathbb{F}_p[X]$.*

On définit alors le degré $\deg(P)$ d'un polynôme non nul $P = a_n X + \cdots + a_0$ comme le plus grand indice i tel que $a_i \neq 0$. On pose également $\deg(0) = \infty$. Comme pour $\mathbb{Z}$, on peut définir la notion de divisibilité et munir $\mathbb{F}_p[X]$ d'une division euclidienne

Théorème 6.11. — *Soient $Q, P \in \mathbb{F}_p[X]$ avec $P \neq 0$. Alors il existe $R, S \in \mathbb{F}_p[X]$ tels que $Q = PS + R$ et $0 \leqslant \deg(R) < \deg(P)$. De plus, sous ces conditions les polynômes R et S sont uniques.*

Cette division euclidienne est une propriété extrêmement riche : en effet comme pour $\mathbb{Z}$ (ou $\mathbb{R}[X]$), on a la notion de PGCD, d'éléments premiers entre eux, de polynômes irréductibles (l'équivalent des nombres premiers), d'algorithme d'Euclide, du théorème fondamental de factorisation (l'équivalent du théorème 4.30), du théorème des restes chinois, etc. Nous avons également les relations de Bézout (et les corollaires de la section 4.2). Typiquement

***Corollaire 6.12* (Relation de Bézout)**. — *Soient P et Q deux polynômes non nuls de $\mathbb{F}_p[X]$. Alors P et Q sont premiers entre eux si et seulement si, il existe $U, V \in \mathbb{F}_p[X]$ tels que $UP + VQ = 1$.*

Donnons également une autre conséquence de la division euclidienne.

Corollaire 6.13. — *Soit $P \in \mathbb{F}_p[X]$ non nul. Posons $r = \deg(P)$. Supposons qu'il existe $a \in \mathbb{F}_p$ tel que $P(a) = 0$. Alors il existe un polynôme Q de degré $r-1$ tel que $P = (X-a)Q$.*

Démonstration. — Grâce à la division euclidienne, on écrit $P = (X-a)Q+b$, avec $b \in \mathbb{F}_p$. Comme $P(a) = 0$, on en déduit que $b = 0$. □

On a alors

Corollaire 6.14. — *Soit $P \in \mathbb{F}_p[X]$ non nul de degré r. Alors P a au plus r racines. Plus précisément, il existe $a_1, \cdots, a_k \in \mathbb{F}_p$ tel que $P = (X-a_1)^{n_1} \cdots (X-a_k)^{n_k} Q$, avec $a_i \neq a_j$ pour $i \neq j$, avec $n_1 + \cdots + n_k \leqslant r$ et avec $Q \in \mathbb{F}_p[X]$ sans racine. De plus, si $P(b) = 0$ alors nécessairement $b = a_i$ pour un certain $i \in \{1, \cdots, k\}$.*

Démonstration. — La factorisation s'obtient à partir du corollaire 6.13. Alors pour $b \in \mathbb{F}_p$ tel que $P(b) = 0$, il vient $(b-a_1)^{n_1} \cdots (b-a_k)^{n_k} Q(b)$ et comme $\mathbb{F}_p$ est un corps, on a nécessairement l'un des $b - a_i$ qui est nul (car $Q(b) \neq 0$ par hypothèse). □

6.3. Pour aller plus loin. — Dans la section Appendice 8, remarque 8.20, on montre qu'un corps fini est de cardinal p^d pour un certain nombre premier p. Nous allons montrer ici comment construire de tel corps finis.
La démarche va être identique à celle qui permet de construire le corps $\mathbb{F}_p$ mais cette fois-ci en partant de $\mathbb{F}_p[X]$. On commence par définir une relation de congruence sur $\mathbb{F}_p[X]$ de la façon suivante :

Définition 6.15. — Soit $P \in \mathbb{F}_p[X]$ et soient $A, B \in \mathbb{F}_p[X]$. On dit que A est congru à B modulo P, si P divise $A - B$. Ou encore le reste de la division euclidienne de $A - B$ par P est le polynôme nul. On note alors $A \equiv_P B$, ou encore $A \equiv B\ (P)$, ou encore $A \equiv B$ (modulo P).

Comme dans $\mathbb{Z}$, la relation "modulo à" est une relation d'équivalence : symétrique, réflexive et transitive. On considère alors les classes d'équivalence

$$[A]_P = \{B \in \mathbb{F}_p[X], A \equiv_P B\}.$$

La classe $[A]_P$ est aussi notée $\overline{X}$.

Définition 6.16. — On note par $\mathbb{F}_p[X]/(P)$ l'ensemble des classes d'équivalences modulo P ; on parle aussi du quotient $\mathbb{F}_p[X]/(P)$.

Les classes de $\mathbb{F}_p[X]/(P)$ forment alors une partition de $\mathbb{F}_p[X]$.

Remarque 6.17. — Lorsque $P = 0$, il y a autant de classes que de polynômes.

Soit $P \in \mathbb{F}_p[X]$ non nul de degré d. Alors, comme pour $\mathbb{Z}$, on montre que toute classe d'équivalence contient un *unique* polynôme A de degré plus petit que d. Et ainsi on a $|\mathbb{F}_p[X]/(P)| = p^d$. Les deux théorèmes importants 5.16 et 5.23 deviennent ici :

Théorème 6.18. — *Soit le corps fini $\mathbb{F}_p$ et soit $P \in \mathbb{F}_p[X]$ de degré d. Alors le quotient $\mathbb{F}_p[X]/(P)$, muni des deux lois $+$ et $\cdot$ induite de $\mathbb{F}_p$, est un anneau fini de cardinal p^d, où $d = \deg(P)$. Si de plus P est un polynôme irréductible alors le quotient $\mathbb{F}_p[X]/(P)$ est un corps fini.*

Posons $\alpha = \overline{X} \in \mathbb{F}_p[X]/(P)$. Chaque classe de $\mathbb{F}_p[X]/(P)$ contient un unique polynôme A de degré plus petit que d ; écrivons $A = a_0 + a_1X + \cdots + a_dX^d$. Alors il vient $\overline{Q} = \overline{a_0 + a_1X + \cdots + a_dX^d} = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{d-1}\alpha^{d-1}$ (ici on a posé $a_0\overline{1} = a_0$). Ainsi, nous venons de montrer que tout élément $\beta \in \mathbb{F}_p[X]/(P)$ s'écrit de façon unique

$$\beta = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{d-1}\alpha^{d-1},$$

avec $\alpha_i \in \mathbb{F}_p$. On écrit alors $\mathbb{F}_p[X]/(P) := \mathbb{F}_p(\alpha)$.
En conclusion, $\mathbb{F}_p(\alpha)$ est un espace vectoriel de dimension d sur $\mathbb{F}_p$ de base $\{\overline{1}, \alpha, \cdots, \alpha^{d-1}\}$, muni d'une multiplication avec la relation $P(\alpha) = 0$.

Comme nous le rappelons dans la section 8, théorème 8.19, un corps fini à p éléments est unique à isomorphisme près. En fait, plus généralement nous avons le théorème suivant (que l'on admet)

Théorème 6.19. — *Soit un nombre premier p et soit $d \geqslant 1$. Il existe un unique corps fini de cardinal p^d (à isomorphisme près). On le note $\mathbb{F}_{p^d}$.*

Ce théorème, associé à la remarque 8.20, montre que le principe de construction d'un corps fini proposé à travers le théorème 6.18 est l'unique façon de construire un corps fini.

Le théorème 6.1 devient ici :

Théorème 6.20. — *Soit un corps fini $\mathbb{K}$ de cardinal p^d. Alors il existe $a \in \mathbb{K}$ tel que $\mathbb{K}^\times = \langle a \rangle$.*

Ainsi ce théorème montre que comme pour $\mathbb{F}_p$, il est possible de définir le logarithme discret dans un corps fini.

Exemple 6.21. — Soit le corps fini $\mathbb{F}_2$. Le polynôme $P = X^2 + X + \overline{1} \in \mathbb{F}_2[X]$ n'a pas de racine sur $\mathbb{F}_2$, il est irréductible. Ainsi le quotient $\mathbb{K} := \mathbb{F}_2[X]/(X^2 + X + 1)$ est un corps fini à 4 éléments. Tout élément de $\mathbb{K}$ s'écrit de façon unique $a_0 + b\alpha$, où α est la classe de X(modulo P) et où $a_i \in \mathbb{F}_2 = \{\overline{0}, \overline{1}\}$. On écrit alors $\mathbb{K} = \mathbb{F}_2(\alpha)$. L'élément α vérifie donc la relation $\alpha^2 + \alpha + \overline{1} = \overline{0}$.
Effectuons quelques calculs dans le corps $\mathbb{K}$. Soit $\beta = \alpha + 1$. Alors $\beta^2 = (\alpha + 1)^2 = \alpha^2 + 2\alpha + \overline{1}$. Mais ici $2\alpha = \overline{0}$ et ainsi $\beta^2 = \alpha^2 + \overline{1} = -(\alpha + \overline{1}) + \overline{1} = \alpha$, car $-\overline{1} = \overline{1}$. Puis $\beta^3 = \alpha(\alpha + 1) = \alpha^2 + \alpha = \alpha + \overline{1} + \alpha = \overline{1}$, ce qui illustre le théorème 6.20.

6.4. Exercices. —

Exercice 48. — *Soit le corps fini* $\mathbb{F}_{19}$.

(*i*) *Donner les ordres possibles d'un élément de* $\mathbb{F}_{19}^{\times}$.

(*ii*) *Quel est l'ordre de* $\overline{3}$ *?*

(*iii*) *Pour chaque ordre possible, donner un élément de* $\mathbb{F}_{19}^{\times}$ *qui a l'ordre en question.*

Exercice 49. — *Vérifier que* 107 *est un nombre premier. Soit alors le corps* $\mathbb{F}_{107}$. *Quels sont les ordres de* $\overline{2}$ *et de* $\overline{3}$ *?*

Exercice 50. — *Montrer que* $\overline{2}$ *est une racine primitive de l'unité de* $\mathbb{F}_{13}$. *Donner alors la table des logarithmes en base* $\overline{2}$ *des éléments de* $\mathbb{F}_{13}^{\times}$.

Exercice 51. — *Montrer que* $\overline{7}$ *est une racine primitive de l'unité de* $\mathbb{F}_{11}$. *Donner alors la table des logarithmes en base* $\overline{7}$ *des éléments de* $\mathbb{F}_{11}^{\times}$.

Exercice 52. — *Soit le corps* $\mathbb{F}_{29}$.

(*i*) *Montrer que* $\overline{2}$ *est une racine primitive de l'unité.*

(*ii*) *Calculer* $\log_{\overline{2}}(\overline{3})$.

(*iii*) *En déduire* $\log_{\overline{2}}(\overline{6})$ *puis* $\log_{\overline{2}}(\overline{5})$.

Exercice 53. — *Soit le corps* $\mathbb{F}_{101}$. *On admet que* $\overline{2}$ *est racine primitive de l'unité.*

(*i*) *Déterminer un représentant principal de* $\overline{2}^{50}$.

(*ii*) *En déduire* $\log_{\overline{2}}(\overline{10})$, $\log_{\overline{2}}(\overline{20})$ *puis* $\log_{\overline{2}}(\overline{40})$.

Exercice 54. — *1. Donner quelques solutions de l'équation diophantienne* $5X^2 - Y^2 = 1$, *c'est à dire avec* $X, Y \in \mathbb{Z}$.

2. Montrer que l'équation diophantienne $5X^2 - Y^2 = 3$ *n'a pas de solution dans* $\mathbb{Z}$.

Exercice 55. — *Résoudre dans* $\mathbb{F}_7$ *le système* $\begin{cases} x + y = \overline{2} \\ x + 2y = \overline{1} \end{cases}$.

Exercice 56. — *Résoudre dans* $\mathbb{F}_{11}$ *le système* $\begin{cases} -x + 2y = \overline{2} \\ 3x + 4y = \overline{1} \end{cases}$.

Exercice 57. — *A quelle condition sur le paramètre* $\lambda \in \mathbb{F}_{13}$ *la matrice* $A = \begin{pmatrix} \overline{1} & \overline{3} \\ \overline{\lambda} & \overline{4} \end{pmatrix}$ *est-elle inversible ?*

Exercice 58. — *Dans* $\mathbb{F}_7$, *inverser la matrice* $B = \begin{pmatrix} \overline{1} & \overline{2} \\ \overline{2} & \overline{1} \end{pmatrix}$.

Exercice 59. — *Dans* $\mathbb{F}_2$, *inverser la matrice* $C = \begin{pmatrix} \overline{1} & \overline{0} & \overline{1} \\ \overline{1} & \overline{1} & \overline{0} \\ \overline{1} & \overline{1} & \overline{1} \end{pmatrix}$.

Exercice 60. — *Déterminer les polynômes irréductibles (unitaires) de* $\mathbb{F}_2[X]$ *de degré* 1*, de degré* 2*, de degré* 3*, degré* 4 *et de degré* 5*.*

Exercice 61. — *Déterminer les polynômes irréductibles de degré* 2 *de* $\mathbb{F}_3$ *puis de* $\mathbb{F}_5$*.*

Exercice 62. — *Dans* $\mathbb{F}_2[X]$*, factoriser les polynômes* $P = X^4 + X^2 + X + \overline{1}$ *et* $Q = X^4 + X^3 + X + \overline{1}$*.*

Exercice 63. — *Dans* $\mathbb{F}_5[X]$*, factoriser les polynômes* $P = X^3 + X^2 + X + \overline{1}$ *puis* $Q = X^3 + X^2 + X + \overline{2}$*.*

Exercice 64. — *Sur* $\mathbb{F}_p$*, soit la matrice* $A = \begin{pmatrix} \overline{1} & \overline{2} & \overline{1} \\ \overline{1} & \overline{0} & -\overline{1} \\ \overline{0} & \overline{1} & -\overline{1} \end{pmatrix}$.

(*i*) *Calculer le polynôme caractéristique de* A*.*

(*ii*) *Etudier la diagonalisation de la matrice* A *pour* $p = 2$*, pour* $p = 3$*, pour* $p = 5$ *et pour* $p = 13$*.*

Exercice 65. — *Montrer qu'une matrice carrée* A *à coefficient dans* $\mathbb{F}_p$ *est diagonalisable si et seulement si,* $A^p = A$*.*

Exercice 66. — *Donner les tables d'addition et de multiplication du corps* $\mathbb{F}_4$*. Déterminer l'ordre de chaque élément de* $\mathbb{F}_4^\times$*.*

Exercice 67. — *Expliquer comment construire le corps à* 1024 *éléments.*

Exercice 68. — *Soit le corps fini* $\mathbb{F}_9 = \mathbb{F}_3(\alpha)$*, avec* α *vérifiant l'équation* $\alpha^2 + 1 = 0$*. Vérifier que le corps* $\mathbb{F}_9$ *contient les racines de tous les polynômes irréductibles de degré* 2 *de* $\mathbb{F}_3[X]$*.*

Exercice 69. — *Donner les tables d'addition et de multiplication du corps* $\mathbb{F}_9$*. Déterminer l'ordre de chaque élément non nul de* $\mathbb{F}_9$*. Parmi les polynomes irréductibles de degré 2 sur* $\mathbb{F}_3$*, trouver les polynomes primitifs (c'est à dire ceux dont une racine engendre* $\mathbb{F}_p^\times$*).*

Exercice 70. — *Reprendre l'exercice précédent avec* $\mathbb{F}_8$*.*

Exercice 71. — *Soit le corps fini* $\mathbb{F}_{16} = \mathbb{F}_2(\alpha)$*, avec* α *vérifiant l'équation* $\alpha^4+\alpha+1 = 0$*. Exprimer les éléments* α^{-1} *et* $(\alpha^5 + \alpha)^{-1}$*.*

Exercice 72. — *Soit* $P = X^2 + X - \overline{1} \in \mathbb{F}_3[X]$ *et soit* $\alpha = \overline{X} \in \mathbb{F}_3[X]/(P)$*. Vérifier que* $\mathbb{F}_3(\alpha) = \mathbb{F}_9$*.*
On considère l'application Z_α *définie par*

$$\begin{array}{rcl} Z_\alpha : \{1, \cdots, 7\} & \to & \{1, \cdots, 7\} \\ i & \mapsto & \log_\alpha(1 - \alpha^i) \end{array}$$

Déterminer explicitement Z_α*. En déduire :*

(*i*) *La simplification de* $(1 + \alpha + \alpha^6) + \alpha(1 - \alpha^6)^4$*.*

(*ii*) *La factorisation sur* $\mathbb{F}_9$ *du polynôme* $X^3 + 1 + \alpha^7 \in \mathbb{F}_9[X]$*.*

Exercice 73. — *Soit* $\mathbb{F}_q$ *le corps à* q *éléments. On suppose* q *impair.*

(*i*) *Montrer que tout élément de* $\mathbb{F}_q$ *est somme de deux carrés.*

(*ii*) *Montrer que* -1 *est un carré dans* $\mathbb{F}_q$ *si et seulement si* $q \equiv 1$ (modulo 4).

7. Un peu de cryptographie

Le but de cette section est de donner quelques protocoles cryptographiques pour illustrer les sections précédentes.
Nous commencerons par donner deux protocoles symétriques (le chiffrement de Vigenère, et le chiffrement de Hill), puis un protocole d'échange de clefs (Diffie-Hellman), et enfin le protocole asymétrique RSA.

Expliquons le principe général. Deux personnes, que l'on nomme traditionnellement Alice et Bob, veulent échanger un message qu'ils souhaitent garder confidentiel. Ils vont donc procéder à un chiffrement de celui-ci. Il apparaît alors au moins trois types de principes.
– *Protocole symétrique.* Alice et Bob disposent d'une clef de chiffrement et d'une clef de déchiffrement, que eux seuls possédent (enfin, c'est ce qu'ils espèrent...). Grâce à ces clefs, Alice peut envoyer un message chiffré à Bob, et Bob peut le déchiffrer ; et vice et versa. Et ainsi, les deux personnes sont en mesure de s'envoyer des messages : les échanges peuvent aller dans les deux sens.
– *Protocole d'échange de clefs.* Pour le protocole précédent, on voit aisément une première question : si Alice et Bob ne se rencontrent pas, comment partager un système de clefs avec une certaine sécurité ?
– *Protocole asymétrique.* Alice rend publique une clef permettant à toute personne de lui envoyer un message chiffré. Alice déchiffre à l'aide d'une clef privée tout message chiffré par cette clef publique. Cet échange ne va que dans un sens : de Bob vers Alice.

D'autres exigences peuvent apparaître comme l'authentification, la non-répudiation et l'authenticité. Nous ne les aborderons pas.

7.1. Chiffrement de Vigenère. — C'est un principe de chiffrement par substitution. On commence par numéroter les lettres de l'alphabet : la lettre A est numérotée 0, la lettre B numérotée 1,... , la lettre Z numérotée 25. Cette numérotation permet de voir l'alphabet dans l'ensemble $\{0, 2, \cdots, 25\}$... que l'on peut voir dans $\mathbb{Z}/26\mathbb{Z}$.
On choisit ensuite la clef de chiffrement : c'est un mot (que l'on traduit dans $\mathbb{Z}/26\mathbb{Z}$).
Expliquons maintenant le principe de ce chiffrement à partir d'un exemple. Typiquement prenons comme clef le mot EXEMPLE, et le texte à chiffrer VOICI UN EXEMPLE. L'opération va alors être la suivante : on commence par écrire le texte à chiffrer, puis en dessous en écrit le mot clef autant de fois que nécessaire pour "couvrir" le texte.

V	O	I	C	I	U	N	E	X	E	M	P	L	E
E	X	E	M	P	L	E	X	E	M	P	L	E	E

Le chiffrement va consister à faire la somme "lettre par lettre", modulo 26. Par exemple, la première colonne voit la somme de V avec E, c'est à dire de 21 et de 4, soit 25, qui correspond à la lettre Z. Pour la seconde colonne, c'est la somme de O avec X, c'est à dire de 14 et 23, soit 37 modulo 26, c'est à dire 11, qui correspond à la lettre L.

V	O	I	C	I	U	N	E	X	E	M	P	L	E
E	X	E	M	P	L	E	X	E	M	P	L	E	E
Z	L	M	O	X	F	R	I	U	I	Y	E	W	I

Le texte chiffré est donc ZLMOX FRIUI YEWI. Le déchiffrement va consister à faire la même opération avec le mot "inverse". La clef de chiffrement EXEMPLE consiste à translater les lettres successivement rencontrées par : 4, 23, 4, 12, 15, 11, 4. Pour le déchiffrement il faut donc translater par -4, -23, -4, -12, -15, -11, -4, ce qui modulo 26 correspond à 22, 3, 22, 14, 11, 15, 22, soit le mot WDWOLPW.

Observons qu'avec le chiffrement de Vegenère une même lettre peut être chiffrée différement. Ce chiffrement est protégé contre une attaque à partir de l'analyse classique des fréquences d'apparition des lettres.

Pour terminer, notons qu'il est possible d'agrandir l'alphabet en introduisant le caractère blanc, la virgule, le point, etc.

7.2. Le chiffrement de Hill. —

7.2.1. Le chiffrement affine. — C'est une extension du chiffrement par transformation affine. Commençons par rappeler celui-ci. Comme précédemment on part de l'alphabet vu dans $\mathbb{Z}/26\mathbb{Z}$. Soient ensuite $a \in (\mathbb{Z}/26\mathbb{Z})^\times$ et $b \in \mathbb{Z}/26\mathbb{Z}$. On rappelle que $a \in (\mathbb{Z}/26\mathbb{Z})^\times$ si et seulement si a est premier à 26. On considère alors l'application affine φ sur $\mathbb{Z}/26\mathbb{Z}$ définie par

$$\varphi(x) = ax + b.$$

Comme $a \in (\mathbb{Z}/26\mathbb{Z})^\times$, l'application φ est inversible d'inverse $\varphi'(y) = a^{-1}y - a^{-1}b$, où ici a^{-1} est l'inverse de a dans $\mathbb{Z}/26\mathbb{Z}$. L'application φ est la clef de chiffrement, et φ' la clef de déchiffrement.
Partons du texte à chiffrer VOICI UN EXEMPLE. Alors V est chiffrée par $\varphi(21)$, O par $\varphi(14)$, etc. Typiquement prenons $a = \overline{3}$ et $b = \overline{5}$. Il vient alors $\varphi(21) = 16$, et V est chiffrée par Q, puis $\varphi(14) = 21$, et donc O est chiffrée par V, etc. Après quelques calculs on trouve le message chiffré QVDLD NSPRH HFXR.
La relation de Bézout $9 \times 3 - 26 = 1$ montre que $(\overline{3})^{-1} = \overline{9}$, et ainsi la clef de déchiffrement est la fonction $\varphi'(y) = \overline{9}y - \overline{1}$. Le message de départ s'obtient en "appliquant" φ' au message QVDLD NSPRH HFXR.

Lorsque $a = 1$, la fonction φ correspond à une translation, c'est le principe de chiffrement de César.

7.2.2. — Le chiffrement de Hill va consister à une généralisation du chiffrement affine. On se donne un entier $n \geqslant 1$, puis une matrice carrée A, de taille $n \times n$, à coefficients dans $\mathbb{Z}/26\mathbb{Z}$. Le déterminant de la matrice A se calcule comme pour le cas où les coefficients sont réels ; les formules du théorème 2.29 restent valable et en particulier A est inversible dès lors que $\det(A) \in (\mathbb{Z}/26\mathbb{Z})^\times$; dans ce cas, il existe une matrice B à coefficients dans $\mathbb{Z}/26\mathbb{Z}$ telle que $AB = BA = I_n$, où I_n est la matrice identité (la classe $\overline{1}$ sur la diagonale et la classe $\overline{0}$ ailleurs).
On suppose A inversible. La matrice A est la clef de chiffrement.

On va appliquer des transformations sur le texte à chiffrer sur des paquets de n lettres via la matrice A.

Voyons ce principe sur l'exemple initial. Soit le texte à chiffrer VOICI UN EXEMPLE. Prenons $n = 2$, et soit la matrice $A = \begin{pmatrix} \overline{2} & \overline{3} \\ \overline{1} & \overline{1} \end{pmatrix}$ à coefficients dans $\mathbb{Z}/26\mathbb{Z}$. La matrice A a pour déterminant $-\overline{1}$, la matrice A est inversible.
Prenons le premier paquet de 2 lettres du texte à chiffre VO. On lui associe le vecteur de coordonnées $\begin{pmatrix} \overline{21} \\ \overline{14} \end{pmatrix}$. Alors, le couple VO est chiffré par le vecteur

$$A \begin{pmatrix} \overline{21} \\ \overline{14} \end{pmatrix} = \begin{pmatrix} \overline{2} & \overline{3} \\ \overline{1} & \overline{1} \end{pmatrix} \begin{pmatrix} \overline{21} \\ \overline{14} \end{pmatrix} = \begin{pmatrix} \overline{6} \\ \overline{9} \end{pmatrix};$$

le vecteur $\begin{pmatrix} \overline{6} \\ \overline{9} \end{pmatrix}$ correspond au couple de lettres GJ. Ansi VO est chiffré en GJ.
Il vient ainsi les transformations suivantes :

$$VO \longrightarrow \begin{pmatrix} \overline{21} \\ \overline{14} \end{pmatrix} \xrightarrow{\varphi} \begin{pmatrix} \overline{6} \\ \overline{9} \end{pmatrix} \longrightarrow GJ \ ; \ IC \longrightarrow \begin{pmatrix} \overline{8} \\ \overline{2} \end{pmatrix} \xrightarrow{\varphi} \begin{pmatrix} \overline{22} \\ \overline{10} \end{pmatrix} \longrightarrow WK \ ;$$

$$IU \longrightarrow \begin{pmatrix} \overline{8} \\ \overline{0} \end{pmatrix} \xrightarrow{\varphi} \begin{pmatrix} \overline{24} \\ \overline{2} \end{pmatrix} \longrightarrow YC \ ; \ NE \longrightarrow \begin{pmatrix} \overline{21} \\ \overline{14} \end{pmatrix} \xrightarrow{\varphi} \begin{pmatrix} \overline{10} \\ \overline{25} \end{pmatrix} \longrightarrow KZ \ ;$$

$$XE \longrightarrow \begin{pmatrix} \overline{0} \\ \overline{5} \end{pmatrix} \xrightarrow{\varphi} \begin{pmatrix} \overline{10} \\ \overline{22} \end{pmatrix} \longrightarrow KW \ ; \ MP \longrightarrow \begin{pmatrix} \overline{24} \\ \overline{5} \end{pmatrix} \xrightarrow{\varphi} \begin{pmatrix} \overline{10} \\ \overline{8} \end{pmatrix} \longrightarrow KS \ ;$$

$$LE \longrightarrow \begin{pmatrix} \overline{13} \\ \overline{16} \end{pmatrix} \xrightarrow{\varphi} \begin{pmatrix} \overline{24} \\ \overline{10} \end{pmatrix} \longrightarrow YK.$$

Le texte chiffré est GJWKY CKZKW KSYK.
La clef de déchiffrement est la matrice inverse de A : pour le déchiffrement, on procède comme pour le chiffrement mais avec la matrice A^{-1}.
Pour l'exemple suivi, on a $A^{-1} = \begin{pmatrix} -\overline{1} & \overline{3} \\ \overline{1} & -\overline{2} \end{pmatrix}$.

7.3. Le protocole de Diffie-Hellman. — La question ici est la suivante : comment Alice et Bob peuvent partager une clef secrète ?
Nous allons donner le protocole de Diffie-Hellman (datant de 1976).

Soit p un nombre premier et soit $g \in (\mathbb{Z}/p\mathbb{Z})^\times$ d'ordre assez grand. On sait que l'ordre d'un élément de $(\mathbb{Z}/p\mathbb{Z})^\times$ divise $p-1$, et qu'il existe des éléments d'ordre $p-1$.

Le nombre premier p et l'élément g peuvent être rendus publics.

Alice choisit alors un entier n, et Bob en entier m. Alice et Bob gardent bien pour eux ces entiers.
Alice calcule g^n ; Bob calcule g^m ; ces calculs se font dans $\mathbb{Z}/p\mathbb{Z}$. Notons par g_n la classe de g^n et par g_m la classe de g^m.

Alice envoie alors g_n à Bob, et Bob envoie g_m à Alice. Ensuite, Alice calcule $(g_m)^n$ et Bob calcule $(g_n)^m$. La clef partagée est alors le résultat obtenu, car en effet on a :

$$(g_m)^n = (g^m)^n = g^{mn} = g^{nm} = (g^n)^m = (g_n)^m.$$

Observons que si une tiers personne intercepte les messages envoyés, c'est à dire g_n et g_m, il lui faut connaître n ou m pour avoir la clef. En d'autres termes, la question est la suivante : sachant g et g_m est-il facile de déterminer m ? C'est la problèmatique du logarithme discret... et c'est quelque chose qu'on ne sait pas résoudre "efficacement".

Bien entendu dans la pratique le nombre premier p doit ètre très grand ainsi que les entiers m et n. Le calcul g^m est un calcul modulo p, qui par une approche naive nécessite m opérations (dans $\mathbb{Z}/p\mathbb{Z}$). Mais on peut optimiser celui-ci. Donnons ici le principe de l'*exponentiation rapide*. Ecrivons m en base 2 :

$$m = a_0 + 2a_1 + 4a_2 + 8a_3 + \cdots + 2^k,$$

où $a_i \in \{0, 1\}$; cela nécessite au plus k opérations (divisions et soustractions). Observons alors que $m \geqslant 2^k$ et donc $k \leqslant \log m / \log 2$. Alors

$$g^m = g^{a_0}(g^2)^{a_1}(g^4)^{a_2} \cdots (g^{2^k}).$$

Etant donnés les g^{2^i}, $i = 1, \cdots, k$, il faut au plus k opérations pour avoir g^m. Mais comme $g^{2^{i+1}} = (g^{2^i})^2$, on voit que k opérations suffisent pour avoir la famille g^{2^i}, $i = 0, \cdots, k$. Ainsi au total il faut donc de l'ordre de $k = \log m$ opérations pour avoir g^m.

Prenons un exemple. Soit le nombre premier $p = 2459$. Alors $p - 1 = 2458 = 2 \times 1229$; ici 1229 est un nombre premier. Observons alors que tout élément non nul de $\mathbb{Z}/2459\mathbb{Z}$ est d'ordre $1, 2, 1229$ ou 2458 dans $(\mathbb{Z}/2459\mathbb{Z})^\times$.
Prenons $g = \overline{2}$ (la classe de 2 dans $\mathbb{Z}/2459\mathbb{Z}$). Cherchons l'ordre de g. Pour cela calculons g^{1229} en utilisant l'exponentiation rapide. Ecrivons 1229 en base 2 :

$$1229 = 1 + 2^2 + 2^3 + 2^6 + 2^7 + 2^{10}.$$

On trouve alors

$$g^{1229} = g \cdot g^{2^2} \cdot g^{2^3} \cdot g^{2^6} \cdot g^{2^7} \cdot g^{2^{10}}.$$

Ecrivons le calcul des g^{2^k} pour $0 \leqslant k \leqslant 10$:

k	0	1	2	3	4	5	6	7	8	9	10
g^{2^k}	$\overline{2}$	$\overline{4}$	$\overline{16}$	$\overline{256}$	$\overline{1602}$	$\overline{1667}$	$\overline{219}$	$\overline{1240}$	$\overline{725}$	$\overline{1858}$	$\overline{2187}$

Alors,

$$g^{1229} = \overline{2} \cdot \overline{16} \cdot \overline{256} \cdot \overline{219} \cdot \overline{1240} \cdot \overline{2187} = -\overline{1},$$

et ainsi $(\mathbb{Z}/2459\mathbb{Z})^\times = \langle \overline{2} \rangle$: en d'autres termes $\overline{2}$ est d'ordre maximal dans $(\mathbb{Z}/2459\mathbb{Z})^\times$. Les données $p = 2459$ et $g := \overline{2} = 2$ (mod 2459) peuvent être publiques.

Supposons que Alice choisisse le nombre $n = 1300$. Comme $n = 2^2 + 2^4 + 2^8 + 2^{10}$, il vient

$$g_n = g^n = g^{2^2} g^{2^4} g^{2^8} g^{2^{10}} = \overline{16} \cdot \overline{1602} \cdot \overline{725} \cdot \overline{2187} = \overline{1476}.$$

Quant à Bob, supposons qu'il choisisse le nombre $m = 123$. Comme $m = 1 + 2 + 2^3 + 2^4 + 2^5 + 2^6 + 2^7$, il vient

$$g_m = g^m = gg^2g^{2^3}g^{2^4}g^{2^5}2^{2^6}g^{2^7} = \overline{1883}.$$

Ainsi Alice envoie à Bob la classe $\overline{1476}$ et Bob envoie la classe $\overline{1883}$ à Alice. Toujours avec l'exponentiation rapide, Alice calcule $\overline{1883}^{1300}$ et Bob calcule $\overline{1476}^{123}$: la clef partagée par Alice et Bob est le résulat de ces deux calculs, à savoir $\overline{42}$.

7.4. Le protocole RSA (Rivest-Shamir-Adelman). — C'est un protocole asymétrique datant de 1978.
Alice va générer une clef publique qui permettra à toute personne (ici Bob) de lui envoyer un message chiffré, qu'elle pourra déchiffrer avec sa clef privée. Le protocole ici va dans un sens unique : seul Bob peut envoyer un message à Alice (le protocole ne permet pas à Alice d'envoyer un message à Bob).

Alice commence par choisir deux nombres premiers p et q (dans la pratique ces nombres premiers sont très grands). Alice effectue ensuite les opérations suivantes :

(*i*) elle calcule $n = pq$,

(*ii*) elle calcule $\varphi(n) = (p-1)(q-1)$,

(*iii*) elle choisit un entier e premier à $\varphi(n)$, et elle calcule l'inverse d de e modulo $\varphi(n)$, ou encore $[d]_{\varphi(n)} = [e]^{-1}_{\varphi(n)}$.

Notons que (*i*) et (*ii*) sont de simples multiplications. Pour (*iii*), il faut déterminer une relation de Bézout entre e et $\varphi(n)$, cela se fait via l'algorithme d'Euclide, c'est une opération très rapide.

Alice rend public le couple (n, e) : c'est la *clef publique*. Par contre, elle conserve secrètement l'entier d : c'est la *clef privée*. Un message sera un élément de $(\mathbb{Z}/n\mathbb{Z})^\times$.

Bob souhaite envoyer le message $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ à Alice : le message a peut être vu comme un entier plus petit que n et premier à n.
Bob calcule $a^e \in \mathbb{Z}/n\mathbb{Z}$; notons par b le résultat. Bob envoie alors b à Alice.

Alice reçoit b puis calcule $b^d \in \mathbb{Z}/n\mathbb{Z}$... et retrouve a.
En effet, comme $[d]_{\varphi(n)} = [e]^{-1}_{\varphi(n)}$, cela signifie qu'il existe un entier k tel que

$$de = 1 + k\varphi(n).$$

Il vient alors

$$b^d = (a^e)^d = a^{ed} = a^{1+k\varphi(n)}.$$

Par le théorème d'Euler 5.29, on a que $a^{\varphi(n)} = [1]_n$. Ainsi

$$b^d = a \cdot (a^{\varphi(n)})^k = a \cdot [1]^k_n = a.$$

Ici la sureté du protocole réside sur le fait que, sachant (n, e), il est difficile de déterminer $[e]^{-1}_{\varphi(n)}$. En effet, la réelle difficulté est de déterminer $\varphi(n)$ sachant n : pour cela il faut factoriser n... ce qui est considéré comme un problème difficile.

Prenons un exemple.

Soient $p = 29$ et $q = 31$; posons $n = 29 \times 31 = 899$. On a alors $\varphi(899) = 28 \times 30 = 840$. Prenons $e = 37$. On a la relation de Bézout

$$840 \times 10 - 227 \times 37 = 1,$$

prouvant que 37 est bien premier à 840 et que

$$[37]_{840}^{-1} = [-227]_{840} = [613]_{840}.$$

La clef publique ici est le couple $(899, 37)$ et la clef privée est l'entier 613.
Bob souhaite envoyer un entier a premier à 899 (l'algorithme d'Euclide détermine rapidement si a est bien premier à 899). Par exemple Bob souhaite envoyer $a = 121$. Il calcule alors $([121]_{899})^{37}$ par l'exponentiation rapide ; détaillons ce calcul. Etablissons tout d'abord les puissances successives de $\overline{121}$ (dans $\mathbb{Z}/899\mathbb{Z}$) :
$\overline{121}^2 = \overline{257}$, $\overline{121}^{2^2} = \overline{257}^2 = \overline{422}$, $\overline{121}^{2^3} = \overline{422}^2 = \overline{82}$, $\overline{121}^{2^4} = \overline{82}^2 = \overline{431}$, $\overline{121}^{2^5} = \overline{567}$.
De $37 = 1 + 2^2 + 2^5$, il vient

$$\overline{121}^{37} = \overline{121} \cdot \overline{121}^{2^2} \cdot \overline{121}^{2^5} = \overline{121} \cdot \overline{422} \cdot \overline{567} = \overline{758}.$$

Ainsi Bob envoie $\overline{758}$ à Alice.
Alice calcule ensuite $([758]_{899})^{613}$ qui est bien égal à $[121]_{899}$.

7.5. Exercices. —

Exercice 74. — *On numérote les lettres de l'alphabet de* 1 *à* 26. *Le blanc, symbolisé par* •, *est numéroté* 0. *Les éléments de cette numérotation peuvent être vus dans* $\mathbb{Z}/27\mathbb{Z}$.
Pour le protocole de Hill (dans $\mathbb{Z}/27\mathbb{Z}$*) avec la clef* $A = \begin{pmatrix} \overline{1} & \overline{2} \\ \overline{3} & \overline{4} \end{pmatrix}$, *on reçoit le message chiffré RYCX SLTF. Déchiffrer ce message.*

Exercice 75. — *Soit le nombre premier* $p = 47$.

(*i*) *Quels sont les ordres possibles des éléments de* $(\mathbb{Z}/47\mathbb{Z})^\times$ *?*

(*ii*) *Déterminer l'ordre de* $\overline{2} \in (\mathbb{Z}/47\mathbb{Z})^\times$.

(*iii*) *Déterminer l'ordre de* $\overline{5} \in (\mathbb{Z}/47\mathbb{Z})^\times$.

(*iii*) *Alice et Bob souhaitent partager une clef via le protocope de Deffie-Hellman à partir du nombre premier* $p = 47$ *et de* $\overline{5} \in (\mathbb{Z}/p\mathbb{Z})^\times$. *Alice choisit le nombre* $m = 15$ *et Bob le nombre* $n = 24$.

- (*a*) *Quelle classe va envoyer Alice ?*
- (*b*) *Quelle classe va envoyer Bob ?*
- (*c*) *Quelle est la clef produite ?*

Exercice 76. — *Soit le nombre* $n = 2021 = 43 \times 47$.

(*i*) *Soit* $e = 59$. *Donner une relation de Bézout entre* $\varphi(n)$ *et* e.

(*ii*) *Avec la clef publique* $(2021, 59)$, *Bob envoie à Alice la classe* $[1969]_{2021}$. *Quel est le message que Bob souhaite partager avec Alice via le protocole RSA ?*

8. Appendice

8.1. Groupes. — Commençons par la notion de groupe.

Définition 8.1. — Un groupe (abélien ou commutatif) G est un ensemble muni d'une loi interne $+$ telle que

(i) pour tout $g, g' \in G$, $g + g' = g' + g \in G$ (commutativité),

(ii) pour tout $g, g', g'' \in G$, $g + (g' + g'') = (g + g') + g$" (associativité),

(iii) il existe un élément neutre, noté 0, c'est dire tel que $g + 0 = g$, pour tout $g \in G$,

(iv) pour tout $g \in G$, il existe un élément opposé dans G, noté $-g$, tel que $g + (-g) = 0$.

Si G est fini, son cardinal $|G|$ est appelé l'ordre de G. Un sous-groupe H de G est un sous-ensemble de G qui muni de la loi induite $+$ forme également un groupe.

Remarque 8.2. — Ici, on a fait le choix d'utiliser une loi additive $+$. Pour une loi multiplicative $\cdot$, on note par 1 l'élément neutre.

Proposition 8.3. — *L'ensemble $\mathbb{Z}/n\mathbb{Z}$ muni de la loi $+$ (issue de l'addition dans $\mathbb{Z}$) forme un groupe : pour $[a]_n$ et $[b]_n$ de $\mathbb{Z}/n\mathbb{Z}$, on pose :* $[a]_n + [b]_n = [a + b]_n$.

Remarquons immédiatement que cette loi est bien définie. En effet, si a' est autre représentant de la classe $[a]_n$, il vient $a + b \equiv_n a' + b$.

Démonstration. — La proposition 8.3 est immédiate. Notons simplement que le neutre est la classe $[0]_n$ et que l'opposé de $[a]_n$ est la classe $[-a]_n$. □

Soit G un groupe. Pour $k \in \mathbb{N}$ et $g \in G$, on pose $kg = \overbrace{g + \cdots + g}^{k}$ puis $-kg = k(-g)$. Considérons le sous-ensemble $\langle g \rangle = \mathbb{Z}G$ de G constitué des kg, avec $k \in \mathbb{Z}$. Il est alors immédiat de voir que $\langle g \rangle$ muni de la loi $+$ est également un groupe : c'est le sous-groupe de G engendré par g. En fait,

Lemme 8.4. — *Soit G un groupe fini et soit $g \in G$. Alors $\mathbb{N}g = \mathbb{Z}g$.*

Démonstration. — En effet, comme G est fini, il existe deux entiers $m, k \in \mathbb{N}$, $m \neq k$, tels que $mg = kg$, ce qui implique $\lambda g = 0$ avec $\lambda \in \mathbb{N}_{>0}$. Par conséquent, $-g = (\lambda - 1)g$, avec $\lambda \in \mathbb{N}$. □

Définition 8.5. — Soit G un groupe fini. L'ordre de g est par définition le plus petit entier $k > 0$ tel que $kg = 0$. On le note $\mathrm{ord}(g)$.

Remarque 8.6. — L'élément neutre est d'ordre 1.

On a le résultat suivant bien utile

Proposition 8.7. — *Soit G un groupe et soit $g \in G$. Alors si g est d'ordre k et que $mg = 0$, on a $k|m$.*

Démonstration. — Soit m tel que $mg = 0$. Effectuons la division euclidienne de m par k : il existe deux entiers q et $0 \leqslant r < k$ tel que $m = qk + r$. Alors $rg = mg - qkg = 0$. Par minimalité de k, on en déduit que $r = 0$. □

Proposition 8.8. — *Soit G un groupe fini. Alors l'ordre de g est aussi égal à l'ordre du sous-groupe $\langle g\rangle$. Ou encore,* $\mathrm{ord}(g) = |\langle g\rangle|$.

Démonstration. — Soit r l'ordre de g. D'après le lemme 8.4, $\langle g\rangle = \{0, g, \cdots, (r-1)g\}$ et ainsi $|\langle g\rangle| \leqslant r$. Supposons que $|\langle g\rangle| < r$: il existe deux entier $0 \leqslant k < m \leqslant r-1$ tels que $(m-k)g = 0$. Or $0 < m-k < r$, ce qui contredit la minimalité de r. □

On a le théorème suivant sur le lien entre l'ordre d'un groupe et celui d'un de ses sous-groupes.

Théorème 8.9. — *Soit H un sous-groupe d'un groupe fini G. Alors $|H|$ divise $|G|$.*

Démonstration. — On définit sur G une relation d'équivalence $\sim$ par : $g \sim g'$ si et seulement si, il existe $h \in H$ tel que $g = g' + h$. Comme H est un groupe, il est immédiat de voir que c'est bien une relation d'équivalence. Une classe est de la forme $g+H$. Comme G est fini, le nombre de classes est fini ; notons le k. L'ensemble de ces classes forment une partition de G : le groupe G peut s'écrire comme une réunion disjointe d'un nombre fini k de classes. Or chaque classe est de cardinal $|H|$, et ainsi $|G| = k|H|$. □

On en déduit alors immédiatement le corollaire suivant.

Corollaire 8.10. — *Soit G un groupe fini et soit $g \in G$. Alors l'ordre de g divise $|G|$. En particulier $|G|g = 0$.*

Démonstration. — Cela provient du fait que $\mathrm{ord}(g) = |\langle g\rangle|$. □

Enfin, terminons par la notion de groupe cyclique.

Définition 8.11. — Un groupe G est dit cyclique s'il est engendré par un élément g ; ou encore si $G = \langle g\rangle$. On dit que g est un générateur de G.

On a alors

Théorème 8.12. — *Soit $G = \langle g\rangle$ un groupe cyclique d'ordre n. Alors*

(i) tout sous-groupe H de G est cyclique,

(ii) pour tout $d \geqslant 1$ diviseur de n, il existe un unique sous-groupe cyclique H de G d'ordre d.

Démonstration. — *(i)* Si $H = \langle 0\rangle$, c'est immédiat ! Soit donc $a > 0$ le plus petit entier tel que $ag \in H$. Alors $\langle ag\rangle \subset H$. Soit $g' \in H$. Comme G est cyclique et fini engendré par g, il existe un entier $b \geqslant 0$ tel que $g' = bg$. Effectuons alors la division euclidienne de b par a : il existe deux entiers q et $0 \leqslant r < a-1$ tel que $b = qa + r$ ce qui implique que $rg = g' - qag \in H$. Par minimalité de a, on en déduit que $r = 0$ et donc que $g' = qag \in \langle ag\rangle$.

(ii) Soit d un diviseur de n. Posons $n_0 = n/d$. Alors $n_0 g$ est d'ordre d et ainsi $\langle n_0 g\rangle$ est un sous-groupe d'ordre d (si l'ordre de $n_0 g$ était strictement plus petit que d cela impliquerait que l'ordre de g serait strictement plus petit que n). Montrons qu'un tel sous-groupe est unique. Soit H un sous-groupe de G d'ordre $d|n$. Nous avons vu dans *(i)* que $H = \langle ag\rangle$

pour un certain entier a. Mais comme ag doit être d'ordre d, cela signifie que $dag = 0$ et donc que da est un multiple de n (d'après la proposition 8.7) : il existe un entier λ tel que $da = \lambda n$ et ainsi $a = \lambda n_0$, ce qui implique que $H = \langle \lambda n_0 g \rangle \subset \langle n_0 g \rangle$. En comparant les ordres, on en déduit que $H = \langle n_0 g \rangle$. □

Enfin on termine par le résultat suivant

Théorème 8.13. — *Soit $G = \langle g \rangle$ un groupe cyclique d'ordre n. Soit $k \in \mathbb{Z}$. Alors kg est un générateur de G si et seulement si,* $\mathrm{pgcd}(k, n) = 1$. *En particulier, G a exactement $\varphi(n)$ générateurs.*

Démonstration. — Supposons $\mathrm{pgcd}(k, n) = 1$. Alors il existe $u, v \in \mathbb{Z}$ tel que $ku + nv = 1$, ce qui signifie que

$$g = (ku + nv)g = kug + vng = u(kg).$$

Or pour tout élément h de G, il existe un entier m tel que $h = mg$, et ainsi $h = mu(kg)$, ce qui signifie que kg est bien un générateur de G.
Réciproquement. Supposons qu'il existe un nombre premier $p | \mathrm{pgcd}(k, n)$. Posons $n_0 = n/p$ et $k_0 = k/p$. Alors

$$n_0(kg) = n_0 p k_0 g = n k_0 g = k_0(ng) = 0.$$

Par conséquent, kg est d'ordre $n_0 < n$ et ainsi kg n'engendre pas G. □

8.2. Anneaux. — Passons maintenant à la notion d'anneau.

Définition 8.14. — Un anneau (commutatif) A est un ensemble muni de deux lois $+$ (additive) et $\cdot$ (multiplicative) telles que

(*i*) l'ensemble A muni de la loi $+$ forme un groupe (commutatif),

(*ii*) la loi $\cdot$ est une loi interne associative (et commutative) munie d'un élément neutre, noté 1, qui vérife $g \cdot 1 = 1 \cdot g = g$ pour tout $g \in G$,

(*iii*) la loi $\cdot$ est distributive par rapport à la loi $+$: $(g + g') \cdot g'' = g \cdot g'' + g' \cdot g''$ et $g \cdot (g' + g'') = g \cdot g' + g \cdot g''$.

Remarque 8.15. — Pour $x, y \in A$, on note par abus $xy = x \cdot y$.

Il est important de noter à ce niveau qu'un élément non nul de l'anneau A n'admet pas forcément d'inverse pour la seconde loi $\cdot$.

Définition 8.16. — Soit A un anneau. Un élément $a \in A$ est dit inversible s'il existe $b \in A$ tel que $ab = 1$. Dans ce cas, l'inverse de a est unique et on le note a^{-1}. L'ensemble des éléments inversible de A est noté $A^\times$.

On a alors

Proposition 8.17. — *L'ensemble $A^\times$ muni de la loi $\cdot$ forme un groupe (commutatif) de neutre* 1.

Démonstration. — Il nous suffit de vérifier que si $x, y \in A^{-1}$, alors $xy \in A^\times$, ce qui est immédiat : en effet, xy est inversible d'inverse $x^{-1}y^{-1}$. □

Définition 8.18. — Lorsque pour un anneau A, tout élément g non nul (ou encore $g \neq 0$) admet un inverse alors on dit que A est un corps. Ou encore, A est un corps si $A^\times = A - \{0\}$.

Théorème 8.19. — *L'anneau $\mathbb{Z}/p\mathbb{Z}$ muni des lois $+$ et $\cdot$ est un corps. C'est l'unique corps à p éléments (à isomorphisme près). On le note $\mathbb{F}_p$.*

Démonstration. — La première partie est conséquence du théorème 5.23. Il nous reste à montrer l'unicité. Soit $\mathbb{K}$ un corps ayant p éléments. Notons par e le neutre multiplicatif de $\mathbb{K}$. Alors $\mathbb{Z}e \subset \mathbb{K}$. En fait, de cette inclusion on construit une application $\psi : \mathbb{Z} \to \mathbb{K}$ définie par $\psi(k) = ke$. Cette application est un morphisme d'anneaux, c'est à dire que ψ respecte les lois de $\mathbb{Z}$ et de $\mathbb{K}$: $\psi(k+k') = \psi(k) + \psi(k')$, $\psi(1) = e$ et $\psi(kk') = \psi(k)\psi(k')$. On cherche à déterminer le noyau $\ker(\psi)$ de ψ : c'est l'ensemble des entiers k tels que $ke = 0$. Soit $m \geqslant 1$ le plus entier non nul tel que $me = 0$. Alors $m \leqslant p$. En utilisant la division euclidienne, on vérifie que $\ker(\psi) = m\mathbb{Z}$.
Ceci permet alors de construire une application injective ψ_m définie par

$$\begin{array}{rcl} \psi_m : \mathbb{Z}/m\mathbb{Z} & \to & \mathbb{K} \\ [k]_m & \mapsto & ke \end{array}$$

Maintenant comme $\mathbb{K}$ est un corps, alors nécessairement m est un nombre premier (en effet si $ne \cdot n'e = 0$ alors ou bien $ne = 0$ ou bien $n'e = 0$). Notons par $\mathbb{F} := \psi(\mathbb{F}_m)$: c'est un sous-corps de $\mathbb{K}$, et les compatibilités des lois font que $\mathbb{K}$ est un $\mathbb{F}$-espace vectoriel. Appelons d la dimension de $\mathbb{K}$ sur $\mathbb{F}$ (comme $\mathbb{K}$ est fini, le dimension du $\mathbb{F}$-espace vecttoriel $\mathbb{K}$ est finie). Alors $|\mathbb{K}| = |\mathbb{F}|^d$ et donc $p = |\mathbb{K}| = m^d$, ce qui entraîne $m = p$ et $d = 1$. D'où $\mathbb{K} = \mathbb{F} = \psi_p(\mathbb{F}_p)$. □

Remarque 8.20. — Nous avons montré au passage qu'un corps fini $\mathbb{K}$ est en particulier un espace vectoriel de dimension d sur un corps $\mathbb{F}$ isomorphe à $\mathbb{F}_p$, et donc de cardinal p^d.

PARTIE III
SUJETS

Université de Franche-Comté / 2018-2019 Mathématiques
CMI Info 2ème année

Contrôle 1

Exercice 1. Déterminer le polynôme caractéristisque de la matrice

$$A = \begin{pmatrix} 1 & -1 & 1 \\ -1 & 0 & 1 \\ 2 & 1 & 1 \end{pmatrix}.$$

Exercice 2. Déterminer toutes les matrices A de $\mathrm{M}_2(\mathbb{R})$ vérifiant $A^2 = I_2$. Pour ces matrices, déterminer A^n pour tout entier $n > 0$. Montrer qu'une telle matrice A est inversible puis déterminer A^n pour tout entier $n < 0$.

Exercice 3. Soit A une matrice de $\mathrm{M}_n(\mathbb{R})$ vérifiant $A^2 - 3A + 2I_n = 0$.

1. Donner un exemple d'une telle matrice.
2. Montrer que A est inversible et exprimer A^{-1} en fonction de A.
3. Pour $n > 0$, exprimer A^n en fonction de A.
4. Pour $n < 0$, exprimer A^n en fonction de A.

Exercice 4. Soit la matrice $A = \begin{pmatrix} -1 & 1 & a \\ -1 & 0 & 1 \\ b & 1 & 1 \end{pmatrix}$, où a et b sont deux paramètres réels.

1. A quelle condition la matrice A est elle inversible ?
2. Lorsque A est inversible, déterminer A^{-1}.
3. Lorsque A n'est pas inversible, discuter le nombre de solutions du système $AX = Y$ d'inconnue $X = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$, et où $Y = \begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix}$.

Université de Franche-Comté / 2018-2019 Mathématiques
CMI Info 2ème année

Contrôle 2

Exercice 1. Soit la matrice à coefficients réels $A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 2 & 1 \end{pmatrix}$.

1) Calculer le polynôme caractéristique P_A de A.
2) Déterminer les valeurs propres de A. Est ce que la matrice A est diagonalisable ?
3) Déterminer une base de chaque sous-espace propre de A.
4) Calculer A^n pour $n \geqslant 1$.

Exercice 2. Soit la matrice à coefficients réels

$$B = \begin{pmatrix} -a-1 & -1 & a+2 \\ 1 & 2 & -1 \\ -a-2 & -1 & a+3 \end{pmatrix},$$

où a est un paramètre réel.

1) Calculer le polynôme caractéristique P_B de B.
2) Factoriser P_B en produit de polynômes irréductibles (on pourra vérifier que $P_B(1) = 0$).
3) Déterminer le polynôme minimal de B suivant les valeurs de a.
4) En déduire les valeurs de a pour lesquelles B est diagonalisable (on ne demande pas de diagonaliser B).

Université de Franche-Comté / 2018-2019 Mathématiques
CMI Info 2ème année

Contrôle 3

Notations. *Si $n > 0$ et x sont deux entiers, on note par $[x]_n$ la classe de x dans $\mathbb{Z}/n\mathbb{Z}$.*

Exercice 1. Résoudre dans $\mathbb{Z}/28\mathbb{Z}$ l'équation $3X = [5]_{28}$.

Exercice 2. Trouver l'ensemble des entiers n tel que 13 divise $n^2 + n + 1$.

Exercice 3. Trouver le plus petit entier positif x tel que $[x]_{89} = [60]_{89}$ et $[x]_{55} = [38]_{55}$.

Exercice 4. Soit le corps $\mathbb{F}_{29} = \mathbb{Z}/29\mathbb{Z}$. Pour $x \in \mathbb{Z}$, on note $\overline{x} = [x]_{29}$.

1. Quels sont les ordres possibles d'un élément de $\mathbb{F}_{29}^\times$?
2. Quel est l'ordre de $\overline{2}$?
3. Pour chaque ordre possible, donner un élément de $\mathbb{F}_{29}^\times$ qui a l'ordre en question.
4. Donner la table des logarithmes en base $\overline{2}$ de $\mathbb{F}_{29}^\times$.

Université de Franche-Comté / 2019-2020 Mathématiques
CMI Info 2ème année

Contrôle 1

Exercice 1. Soit la matrice $A = \begin{pmatrix} 1 & 2 & a \\ 2 & -1 & 2 \\ 1 & -1 & b \end{pmatrix}$, où a et b sont deux paramètres réels.

1. A quelle condition la matrice A est elle inversible ?
2. Lorsque A est inversible, déterminer A^{-1}.

Exercice 2. Soit la matrice à coefficients réels $A = \begin{pmatrix} 0 & -2 & -1 \\ 0 & 2 & 1 \\ -1 & -1 & 1 \end{pmatrix}$.

1. Calculer le polynôme caractéristique P_A de A.
2. Déterminer les valeurs propres de A. Est ce que la matrice A est diagonalisable ?
3. Déterminer une base de chaque sous-espace propre de A.
4. Calculer A^n pour $n \geqslant 1$.

Exercice 3. Soit la matrice à coefficients réels

$$B = \begin{pmatrix} 2 & -a+2 & 0 \\ 0 & a & 0 \\ 1 & a+1 & 1 \end{pmatrix},$$

où a est un paramètre réel.

1. Calculer le polynôme caractéristique P_B de B.
2. Déterminer le polynôme minimal de B suivant les valeurs de a.
3. En déduire les valeurs de a pour lesquelles B est diagonalisable (on ne demande pas de diagonaliser B).

Université de Franche-Comté / 2019-2020 Mathématiques
CMI Info 2ème année

Contrôle 2

Notations. *Si $n > 0$ et x sont deux entiers, on note par $[x]_n$ la classe de x dans $\mathbb{Z}/n\mathbb{Z}$.*

Exercice 1. Déterminer $\text{pgcd}(831, 7353)$.

Exercice 2. Donner une relation de Bézout entre 345 et 254. En déduire l'ensemble des solutions de l'équation diophantienne

$$345 \times u + 254 \times v = 1.$$

Exercice 3.
Trouver le plus petit entier $x \geqslant 0$ vérifiant $x \equiv 13 \pmod{17}$ et $x \equiv 5 \pmod{23}$.

Exercice 4. Soit le nombre entier $N = 27^{5n+a} - 26^{3n+b}$.

1. Déterminer les représentants principaux de $[27^5]_{31}$ et de $[26^3]_{31}$.
2. Calculer $[26^k]_{31}$ pour $k = 0, \cdots, 6$.
3. Soit $a = 10$. Donner un entier $b > 0$ tel que 31 divise N.
4. Soit $a = 1$ et soit b quelconque. Montrer que le nombre N est premier à 31.

Université de Franche-Comté / 2019-2020 Mathématiques
CMI Info 2ème année

Contrôle 3

Notations. Si p désigne un nombre premier, on note par $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$.

Exercice 1.

1. Déterminer les polynômes *irréductibles* (et unitaires) de degré 2 sur $\mathbb{F}_3$.
2. Déterminer un polynôme irréductible de degré 2 sur $\mathbb{F}_5$.

Exercice 2. Soit le corps $\mathbb{F}_{199}$. On admet que $\overline{3}$ est d'ordre 198 dans $\mathbb{F}_{199}^\times$.

1. Simplifier $\overline{3}^5$. En déduire $\log_{\overline{3}}(\overline{44})$.
2. Donner une relation de Bézout entre 44 et 199.
3. Que vaut $\log_{\overline{3}}(\overline{95})$?

Exercice 3. Soit le corps $\mathbb{F}_{29}$.

1. Quels sont les ordres possibles d'un élément de $\mathbb{F}_{29}^\times$?
2. Quel est l'ordre de $\overline{2}$?
3. Donner la table des logarithmes en base $\overline{2}$ de $\mathbb{F}_{29}^\times$.

Université de Franche-Comté / 2020-2021 Mathématiques
CMI Info 2ème année

Contrôle 1

Exercice 1. Soit la matrice $A = \begin{pmatrix} a & 0 & a-2 \\ 2 & 2a & 2 \\ a-2 & 0 & a \end{pmatrix}$, où a est un paramètre réel.

1. À quelle condition la matrice A est elle inversible ?
2. Lorsque A est inversible, déterminer A^{-1}.

Exercice 2. Soit la matrice à coefficients réels $A = \begin{pmatrix} -1 & -2 & 2 \\ 2 & 3 & -2 \\ 2 & 2 & -1 \end{pmatrix}$.

1. Calculer le polynôme caractéristique P_A de A.
2. Déterminer les valeurs propres de A.
3. Déterminer le polynôme minimal de A. Est-ce que la matrice A est diagonalisable ?
4. Déterminer une base de chaque sous-espace propre de A.
5. Calculer A^n pour $n \geqslant 1$.

Exercice 3. Soit n fixé, et soit E l'ensemble des matrices $A \in \mathrm{M}_n(\mathbb{R})$ vérifiant $A^2 = -A$.

1. Soit $A \in E$ que l'on suppose inversible. Que vaut A ?
2. Quand $n = 2$, déterminer toutes les matrices diagonales D de E. Généraliser à tout n le résultat précédent.
3. Soit A une matrice de E et soit $Q \in \mathrm{Gl}_n(\mathbb{R})$ une matrice inversible de $\mathrm{M}_n(\mathbb{R})$. Montrer que $Q^{-1}AQ \in E$.
4. Soit A une matrice de E.

   a) Donner un polynôme $P \in \mathbb{R}[X]$ tel que $P(A) = 0$.

   b) Quelles sont alors les possibilités pour le polynôme minimal de A ? Est-ce que la matrice A est diagonalisable ?

   c) Quelles sont les valeurs propres de A ? Donner la forme du polynôme caractéristique P_A de A.
5. Montrer que $E = \{QDQ^{-1};\ D \in E, D \text{ diagonale}, P \in \mathrm{Gl}_n(\mathbb{R})\}$.

Université de Franche-Comté / 2020-2021 Mathématiques
CMI Info 2ème année

Contrôle 2

Notations. *Si $n > 0$ et x sont deux entiers, on note par $[x]_n$ la classe de x dans $\mathbb{Z}/n\mathbb{Z}$. Si p désigne un nombre premier, on note par $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$.*

Exercice 1.

1. Donner une relation de Bézout entre 1023 et 761.
2. En déduire l'ensemble des solutions de l'équation diophantienne
$$1023 \times u + 761 \times v = 1.$$
3. Dans $\mathbb{Z}/1023\mathbb{Z}$ résoudre l'équation : $761x = [2]_{1023}$.
4. Trouver le plus petit entier x vérifiant $x \equiv 25 \pmod{1023}$ et $x \equiv 3 \pmod{761}$.

Exercice 2. Soit le nombre entier $N = 31^{2n} - 27^{3n+a}$.

1. Déterminer les représentants principaux de $[31^2]_{37}$ et de $[27^3]_{37}$.
2. Donner un entier a tel que 37 divise N.

Exercice 3. Soit le corps $\mathbb{F}_{23}$.

1. Quels sont les ordres possibles d'un élément de $\mathbb{F}_{23}^\times$?
2. Déterminer l'ordre des éléments suivants : $\overline{2}$, $\overline{3}$, et $\overline{5}$.
3. Donner la table des logarithmes en base $\overline{5}$ de $\mathbb{F}_{23}^\times$.

Université de Franche-Comté / 2021-2022 Mathématiques
CMI Info 2ème année

Contrôle 1

Exercice 1. Soit la matrice $A = \begin{pmatrix} a-1 & -1 & a \\ 2 & a+3 & -2 \\ 2 & 3 & a-2 \end{pmatrix}$, où a est un paramètre réel.

1. À quelles conditions la matrice A est elle inversible ?
2. Lorsque A est inversible, déterminer A^{-1}.

Exercice 2. Soit la matrice à coefficients réels $A = \begin{pmatrix} 2 & 1 & -1 \\ -1 & 0 & 1 \\ -1 & -1 & 2 \end{pmatrix}$.

1. Calculer le polynôme caractéristique P_A de A.
2. Déterminer les valeurs propres de A.
3. Déterminer le polynôme minimal de A. Est-ce que la matrice A est diagonalisable ?
4. Déterminer une base de chaque sous-espace propre de A.
5. Calculer A^n pour $n \geqslant 1$.

Exercice 3.
Soit A une matrice de $\mathrm{M}_n(\mathbb{R})$ vérifiant $A^2 + A - 2I_n = 0$.

1. Donner un exemple d'une telle matrice.
2. Montrer que A est inversible et exprimer A^{-1} en fonction de A.
3. Pour $n > 0$, exprimer A^n en fonction de A.
4. Pour $n < 0$, exprimer A^n en fonction de A.

Université de Franche-Comté / 2021-2022 Mathématiques
CMI Info 2ème année

Contrôle 2

Notations. *Si $n > 0$ et x sont deux entiers, on note par $[x]_n$ la classe de x dans $\mathbb{Z}/n\mathbb{Z}$. Si p désigne un nombre premier, on note par $\mathbb{F}_p$ le corps fini $\mathbb{Z}/p\mathbb{Z}$, et par $\overline{x}$ la classe de x dans $\mathbb{F}_p$.*

Exercice 1.

1. Donner une relation de Bézout entre 750 et 133.
2. Dans $\mathbb{Z}/750\mathbb{Z}$, résoudre l'équation : $133x = [2]_{750}$.
3. Trouver le plus petit entier x vérifiant $x \equiv 25 \pmod{133}$ et $x \equiv 3 \pmod{750}$.

Exercice 2.
Soit le nombre entier $N = 2 \times 17^{3n} + 27^{7n+a}$.

1. Déterminer les représentants principaux de $[17^3]_{31}$ et de $[27^7]_{31}$.
2. Donner un entier a tel que 31 divise N.

Exercice 3.
Soit le corps fini $\mathbb{F}_{17}$.

1. Quels sont les ordres possibles d'un élément de $\mathbb{F}_{17}^\times$?
2. Déterminer l'ordre des éléments suivants : $\overline{2}$, $\overline{3}$.
3. Donner la table des logarithmes en base $\overline{3}$ de $\mathbb{F}_{17}^\times$.

Université de Franche-Comté / 2021-2022 Mathématiques
CMI Info 2ème année

Epreuve de rattrapage

Notations. *Si $n > 0$ et x sont deux entiers, on note par $[x]_n$ la classe de x dans $\mathbb{Z}/n\mathbb{Z}$. Si p désigne un nombre premier, on note par $\mathbb{F}_p$ le corps fini $\mathbb{Z}/p\mathbb{Z}$, et par $\overline{x}$ la classe de x dans $\mathbb{F}_p$.*

Exercice 1.

1. Donner une relation de Bézout entre 245 et 131.
2. Dans $\mathbb{Z}/245\mathbb{Z}$, résoudre l'équation : $131x = [2]_{245}$.
3. Trouver le plus petit entier x vérifiant $x \equiv 2 \pmod{131}$ et $x \equiv 3 \pmod{245}$.

Exercice 2.
Soit le nombre entier $N = 2 \times 13^{2n} + 3^{8n+a}$.

1. Déterminer les représentants principaux de $[13^2]_{17}$ et de $[3^8]_{17}$.
2. Donner un entier a tel que 17 divise N.

Exercice 3.
Soit le corps fini $\mathbb{F}_{19}$.

1. Quels sont les ordres possibles d'un élément de $\mathbb{F}_{19}^{\times}$?
2. Déterminer l'ordre de $\overline{2}$.
3. Donner la table des logarithmes en base $\overline{2}$ de $\mathbb{F}_{19}^{\times}$.

Université de Franche-Comté / 2022-2023 Mathématiques
CMI Info 2ème année

Contrôle 1

Exercice 1. Soit la matrice $A = \begin{pmatrix} a-1 & -1 & -2 \\ 0 & a & 2 \\ -1 & -1 & a-2 \end{pmatrix}$, où a est un paramètre réel.

1. À quelles conditions la matrice A est elle inversible ?
2. Lorsque A est inversible, déterminer A^{-1}.

Exercice 2. Soit la matrice $A = \begin{pmatrix} 2a-1 & a & -a+1 \\ a & 0 & -a \\ 3a-1 & a & -2a+1 \end{pmatrix}$, où a est un paramètre réel.

1. Calculer le polynôme caractéristique P_A de A.
2. Déterminer les valeurs propres de A.
3. Déterminer le polynôme minimal de A.
4. Est-ce que la matrice A est diagonalisable ?

Exercice 3. Soit A une matrice de $\mathrm{M}_n(\mathbb{R})$ vérifiant $A^2 + A - 6I_n = 0$.

1. Donner un exemple d'une telle matrice.
2. Montrer que A est inversible et exprimer A^{-1} en fonction de A.
3. Pour $n > 0$, exprimer A^n en fonction de A.

Université de Franche-Comté / 2022-2023 Mathématiques
CMI Info 2ème année

Contrôle 2

Notations. *Si $n > 0$ et x sont deux entiers, on note par $[x]_n$ la classe de x dans $\mathbb{Z}/n\mathbb{Z}$. Si p désigne un nombre premier, on note par $\mathbb{F}_p$ le corps fini $\mathbb{Z}/p\mathbb{Z}$, et par $\overline{x}$ la classe de x dans $\mathbb{F}_p$.*

Exercice 1.

1. Donner une relation de Bézout entre 254 et 137.
2. Dans $\mathbb{Z}/137\mathbb{Z}$, résoudre l'équation : $254 \cdot X = [3]_{137}$.
3. Trouver le plus petit entier $x \geqslant 0$ vérifiant $x \equiv 2 \pmod{254}$ et $x \equiv 5 \pmod{137}$.

Exercice 2.
Soient deux entiers a et n, et soit le nombre entier $N = 16^{n+1} + a \cdot 27^{2n+4}$.
Donner une valeur de a pour que 31 divise N quelque soit la valeur de n.

Exercice 3.

1. Déterminer les polynômes *irréductibles* (et unitaires) de degré 2 sur $\mathbb{F}_3$.
2. Déterminer un polynôme irréductible de degré 2 sur $\mathbb{F}_5$.

Exercice 4.
Soit le corps fini $\mathbb{F}_{29}$.

1. Quel est l'ordre possible d'un élément de $\mathbb{F}_{29}^{\times}$?
2. Déterminer l'ordre de $\overline{2}$.
3. Donner la table des logarithmes en base $\overline{2}$ de $\mathbb{F}_{19}^{\times}$.

---

19 septembre 2023

Christian Maire, Institut FEMTO-ST, Université de Franche-Comté, 15B chemin des Montboucons, 25000 Besançon • *E-mail :* christian.maire@univ-fcomte.fr
Url : http://members.femto-st.fr/christian-maire/fr