

COURS D'ALGÈBRE I – ÉTÉ 2006 – EXERCICES

Série XV distribuée le 16 mars 2006

Rendre d'ici au 21 mars les exercices 2, 3, 4 et 6.

L'exercice 1 est à faire *oralement*.

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

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

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

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

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

Est-ce que f_m et f_n sont premiers entre eux pour toute paire d'entiers m, n telle que $m > n \geq 0$?

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

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

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

(5) Soit $N \geq 3$ un entier premier à 10. Montrer que N divise un entier de la forme $u_m = \sum_{j=0}^m 10^j$, c'est-à-dire un entier d'écriture décimale $111 \cdots 1$ (avec $m+1$ chiffres 1).

[Exemples : $3 \mid 111$, $7 \mid 111\,111$, $9 \mid 111\,111\,111$, $11 \mid 11$, $13 \mid 111\,111$. Il faut un peu de patience pour vérifier que le plus petit des u_k qui est un multiple de 17 est u_{16} .

Indication¹. Notons r_k le reste de la division de u_k par N . Il existe k, ℓ tels que $\ell > k \geq 1$ et $r_\ell = r_k$. Alors N divise $10^{-k}(r_\ell - r_k)$.]

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

Pour tout entier $n \geq 0$, vérifier l'alternative suivante :

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

[Indication : traiter d'abord le cas $n = 2$.]

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

[Indication² : $N = (n+2)! + 2$ convient.]

¹Cette indication est en fait une solution !

²Idem

La séance d'exercices du 17 mars sera consacrée aux exercices des examens du 3 mars. Voici à nouveau les énoncés.

!!! Vérifier vos solutions !!!

(1) Pour quelles valeurs des paramètres α et β le système linéaire en les inconnues x, y, z

$$\begin{array}{rcccccc} x & + & y & + & z & = & 1 \\ x & + & \alpha y & + & \alpha^2 z & = & 1 \\ \alpha x & + & y & + & z & = & \beta \end{array}$$

possède-t-il une unique solution ? zéro solution ? une famille à un paramètre de solutions ? une famille à deux paramètres de solutions ? Ecrire toutes les solutions dans chaque cas.

(2) Soit $\text{Sym}(7)$ le groupe des permutations de l'ensemble $\{1, 2, 3, 4, 5, 6, 7\}$ et soit $\sigma \in \text{Sym}(7)$ la permutation définie par

$$\sigma(1) = 3, \quad \sigma(2) = 7, \quad \sigma(3) = 6, \quad \sigma(4) = 2, \quad \sigma(5) = 4, \quad \sigma(6) = 1, \quad \sigma(7) = 5.$$

(o) Si $\alpha = (1\ 3\ 6)$ et $\beta = (1\ 3)(3\ 6)(6\ 1)$, vérifier que $\alpha \neq \beta$ en exhibant un entier $k \in \{1, 2, 3, 4, 5, 6, 7\}$ tel que $\alpha(k) \neq \beta(k)$.

(i) Ecrire la permutation σ comme un produit de cycles à supports disjoint deux à deux.

(ii) Ecrire σ comme un produit de transpositions.

(iii) Calculer l'ordre de σ .

(3) Soit E l'espace vectoriel des fonctions polynomiales de \mathbf{R} dans \mathbf{R} de degré plus petit ou égal à 2, muni du produit scalaire défini par

$$\langle f | g \rangle = \frac{1}{2} \int_{-1}^1 f(t)g(t)t^2 dt.$$

Soient f_0, f_1 et f_2 les fonctions polynomiales définies par

$$f_0(t) = 1, \quad f_1(t) = t, \quad f_2(t) = t^2,$$

(i) Vérifier que $\{f_0, f_1, f_2\}$ est une base de E .

(ii) Montrer que cette base n'est pas orthonormale.

(iii) Appliquer le procédé de Gram-Schmidt à cette base pour obtenir une base orthonormale.

$$(4) \text{ Soit } a = \begin{pmatrix} \frac{3}{2} & -\frac{1}{2} \\ -\frac{1}{2} & \frac{3}{2} \end{pmatrix} \in M_2(\mathbf{R}).$$

(i) Déterminer les espaces propres de la matrice a .

[Sous-entendu : pas seulement un nombre fini de vecteurs propres !]

(ii) Trouver une matrice $s \in GL_2(\mathbf{R})$ telle que la matrice sas^{-2} soit diagonale.

[L'une des difficultés : ne pas confondre s et s^{-1} .]

Série XVI distribuée le 23 mars 2006

Rédiger les exercices 1 à 3.

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

Ex. 2. Soient $(p_n)_{n \geq 0}$, $(q_n)_{n \geq 0}$ les deux suites d'entiers définies par

$$\begin{pmatrix} p_{n+1} \\ q_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} p_n \\ q_n \end{pmatrix}, \quad n \neq 0 \quad \text{et} \quad \begin{matrix} p_0 = 1 \\ q_0 = 1 \end{matrix}.$$

- (i) Vérifier que $p_n^2 = 2q_n^2 + (-1)^{n+1}$ pour tout $n \geq 0$.
- (ii) Calculer numériquement les différences $p_n/q_n - \sqrt{2}$ pour n "petit".
- (iii) Dessiner les axes propres de la matrice $\begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}$ et les points p_n/q_n pour n "petit".

Rappel (exercice XV.6) : le nombre $\sqrt{2}$ est irrationnel.

Ex. 3. On considère des entiers $a \geq 2$ et $m \geq 2$.

(i) Montrer que, si $M = a^m - 1$ est premier, alors $a = 2$ et m est premier [de sorte que M est un nombre de Mersenne].

Pour tout nombre premier p , on définit le *nombre de Mersenne* $M_p = 2^p - 1$.

(ii) Pour $p = 2, 3, 5, 7, 11$, décider si $M_p = 2^p - 1$ est premier.

[N.B. : on ignore s'il existe une infinité de nombres premiers p tels que M_p soit premier, et aussi s'il existe une infinité de nombres premiers p tels que M_p soit composé.]

(iii) Montrer que, si $n = a^m + 1$ est premier, alors a est pair et m est une puissance de 2 [de sorte que, si $a = 2$, alors n est un nombre de Fermat].

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

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

Ex. 4. Un nombre entier n est *parfait* s'il est égal à la somme de ses diviseurs stricts (c'est-à-dire à la somme des entiers d tels que $1 \leq d < n$ et $d \mid n$).

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

(ii) Montrer que, si p est un nombre premier tel que $2^p - 1$ est premier, alors $2^{p-1}(2^p - 1)$ est parfait.

Euclide connaissait une preuve de ce fait. Une vingtaine de siècles plus tard, Euler a montré que, réciproquement, tout nombre parfait *pair* est de cette forme. On ignore s'il existe une infinité de nombres parfaits, mais on conjecture que c'est le cas. On ignore s'il existe des nombres parfaits impairs ; s'il existe un nombre parfait impair, on sait qu'il doit être plus grand que 10^{200} .

Ex. 5. Consulter quelques pages de votre encyclopédie favorite sur les sujets du semestre d'été.

Par exemple, consulter *Wikipedia* sur la toile aux rubriques *natural number*, *prime number*, *cryptography*, *finite field*, ...

Correction d'une remarque des notes [no 2.4.d]. Un nombre *impair* $n > 1$ est composé, $n = ab$ avec $a, b < n$, si et seulement s'il est de la forme $n = c^2 - d^2$ avec $c, d \in \mathbb{N}$ et $c - d \geq 2$.

Il ne faut pas oublier la condition $c - d \geq 2$! par exemple : $5 = 3^2 - 2^2$ et $7 = 4^2 - 3^2$.

Série XVII à rendre jusqu'au mardi 4 avril 2006

Rédiger les exercices 2, 3.iii & iv, et 4.

Exercice 1. Vérifier que $365 \equiv 1 \pmod{7}$. Sachant que le 30 mars 2006 est un jeudi, en déduire quel jour de la semaine (lundi, mardi, ..., dimanche) était le 30 mars 2005, et quels jours seront les 30 mars 2007 et 2008 [pour ce dernier, prendre garde au fait que l'année 2008 sera bissextile].

Ex. 2. Montrer les congruences suivantes :

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

pour tout $n \geq 0$.

Ex. 3. Voici d'abord une variante du théorème concernant la division euclidienne : Soient $n, d \in \mathbf{Z}$ avec $d \neq 0$. Il existe des entiers $q', r' \in \mathbf{Z}$ tels que

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

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

- (i) Constater que, pour tout $x \in \mathbf{Q}$, il existe $q' \in \mathbf{Z}$ tel que $|x - q'| \leq \frac{1}{2}$.
- (ii) Particulariser à $x = n/d$.

Le principe de cette preuve s'adapte à d'autres cas. Aisni, soit $\mathbf{Q}(i)$ l'ensemble des nombres complexes de la forme $x_1 + ix_2$ avec $x_1, x_2 \in \mathbf{Q}$ et $\mathbf{Z}[i]$ le sous-ensemble de ces nombres³ pour lesquels $x_1, x_2 \in \mathbf{Z}$.

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

$$n = qd + r \quad \text{et} \quad 0 \leq |r| \leq \frac{1}{\sqrt{2}}|d|$$

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

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

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

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

³ $\mathbf{Q}(i)$ est un corps pour les règles usuelles d'addition et de multiplication, et $\mathbf{Z}[i]$ est l'anneau des entiers de Gauss. Le terme "anneau" sera défini au § 4 du chapitre VII. Il suffit ici de savoir que $\mathbf{Z}[i]$ est un sous-ensemble du corps $\mathbf{Q}(i)$ contenant 0 et 1 tel que, si a et b sont dans $\mathbf{Z}[i]$, alors $-a$, $a + b$ et ab y sont aussi.

Série XVIII distribuée le 6 avril 2006

Rédiger les exercices 4 à 6.

Exercice 1. Les assertions suivantes sont-elles correctes ? Répondre soit par oui, et donner un exemple, soit par non en donnant un contre exemple.

- (i) Soient $a, b, c \in \mathbb{Z}$ tels que $\text{pgcd}(a, b) = 1$. Si $c \mid ab$, alors $c \mid a$ ou $c \mid b$.
- (ii) Soient $a, b, c \in \mathbb{Z}$ tels que $\text{pgcd}(a, b) = 1$. Si $a \mid bc$, alors $a \mid b$ ou $a \mid c$.

Quel est l'énoncé du cours auquel (i) et (ii) vous fait penser ?

Ex. 2. Soient a et b deux entiers positifs ou nuls. Montrer que $10a + b$ est divisible par 7 si et seulement si $a - 2b$ l'est, $10a + b$ est divisible par 13 si et seulement si $a + 4b$ l'est, $10a + b$ est divisible par 17 si et seulement si $a - 5b$ l'est.

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

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

Ex. 4. Pour $a \in \mathbb{Z}$, rappelons que $a^2 \equiv 0 \pmod{4}$ si a est pair et $a^2 \equiv 1 \pmod{4}$ si a est impair ; de sorte que, pour tout entier de la forme $n = a^2 + b^2$, avec $a, b \in \mathbb{Z}$, on a $n \not\equiv 3 \pmod{4}$.

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

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

(ii) Vérifier ce qui précède pour n "petit".

Ex. 5. Vérifier que le groupe des éléments inversibles de l'anneau $\mathbb{Z}/13\mathbb{Z}$ est cyclique. [Indication : calculer les puissances de 2 modulo 13.] Idem pour $\mathbb{Z}/7\mathbb{Z}$.

Vérifier que le groupe des éléments inversibles de l'anneau $\mathbb{Z}/8\mathbb{Z}$ n'est pas cyclique. Idem pour $\mathbb{Z}/12\mathbb{Z}$.

Ex. 6. Trouver un entier x tel que $x \equiv 1 \pmod{2}$, $x \equiv 3 \pmod{5}$ et $x \equiv 7 \pmod{9}$.

Ex. 7. Montrer que $55^{24} - 1$ est divisible par 72. [Indication : calculer $\varphi(72)$.]

Correction aux notes, exercice VII.37. Pour vérifier que l'élevation à une puissance définit une opération qui n'est pas associative, calculer $2^{(2^3)}$ et $(2^2)^3$.

Série XIX distribuée le 13 avril 2006

Cette série est à prendre comme un test de compréhension. **Ce n'est pas une série à rédiger.**

Exercice 1. Ecrire la liste complète des diviseurs de 60, ainsi que de votre année de naissance. Vérifier que

$$\sum_{d|60} \varphi(d) = 60.$$

.

Ex. 2. Pour $m, n \geq 1$ et deux matrices $s, t \in M_{m,n}(\mathbf{R})$, vérifier que la relation d'être *semblables* est une relation d'équivalence.

Pour $n \geq 1$ et deux matrices $s, t \in M_n(\mathbf{R})$, vérifier que la relation d'être *conjuguées* est une relation d'équivalence.

(Pour les définitions de “semblable” et “conjuguée”, voir le chapitre III du semestre d'hiver.)

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

Ex. 3. Montrer que, pour un nombre premier impair p , les conditions $p \equiv 2 \pmod{3}$ et $p \equiv 5 \pmod{6}$ sont équivalentes.

Montrer qu'il existe une infinité de nombres premiers de la forme $3k + 2$.

Ex. 4. Combien le groupe additif $\mathbf{Z}/24\mathbf{Z}$ possède-t-il de générateurs ?

(Un élément g d'un groupe abélien G , ici noté additivement, est un *générateur* du groupe si tout élément de G est de la forme ng , avec $n \in \mathbf{Z}$.)

Ex. 5. Trouver deux entiers positifs N, D tels que $\frac{N}{D} = 0, \dot{1}2345678\dot{9}$.

Ex. 6. Quel est le dernier chiffre de 7^{1000} en écriture décimale ?

Symboles de Legendre. Ce qui suit *remplace* la partie en caractères normaux de l'exercice VII.44 des notes. De plus, dans la partie en petits caractères du même exercice VII.44, il faut corriger 72 en 76.

Soient $a \in \mathbf{Z}$, $a \neq 0$, et p un nombre premier impair qui ne divise pas a . On dit que a est un *reste quadratique modulo p* , et on écrit $\left(\frac{a}{p}\right) = 1$, s'il existe $x \in \mathbf{Z}$ tel que $x^2 \equiv a \pmod{p}$; on écrit $\left(\frac{a}{p}\right) = -1$ sinon. La notation $\left(\frac{a}{p}\right)$ est un *symbole de Legendre*. La relation

$$(\#) \quad a^{\frac{p-1}{2}} \equiv 1 \pmod{p} \quad \text{si} \quad \left(\frac{a}{p}\right) = 1$$

est une conséquence immédiate du théorème de Fermat. Montrons que, d'autre part,

$$(\#\#) \quad a^{\frac{p-1}{2}} \equiv -1 \pmod{p} \quad \text{si} \quad \left(\frac{a}{p}\right) = -1.$$

Pour tout $x \in \{1, \dots, p-1\}$, il existe $y \in \{1, \dots, p-1\}$ tel que $xy \equiv a \pmod{p}$; notons que $x \neq y$, parce que $\left(\frac{a}{p}\right) = -1$. On peut donc grouper les entiers $1, 2, \dots, p-1$ par paires x, y telles que $xy \equiv a \pmod{p}$. Comme il y a $\frac{p-1}{2}$ telles paires :

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

L'égalité $(\#\#)$ résulte alors du théorème de Wilson.

Série XX distribuée le 27 avril 2006**Rédiger les exercices 2, 3, 4 et 6.**

Exercice 1. Quel est le reste de la division de $3^{24\,000}$ par 35 ?

Ex. 2. Quel est l'ordre de la matrice $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ dans le groupe $GL(2, \mathbf{R})$? Quel est l'ordre de la matrice $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ dans le groupe $GL(2, \mathbf{F}_3)$? Quel est l'ordre du groupe $GL(2, \mathbf{F}_p)$? Quel est l'ordre du groupe $SL(2, \mathbf{F}_p)$?

Ex. 3. Pour tout entier de la forme $n = a^2 + 3b^2$, avec a et b dans \mathbb{Z} , montrer que $n \not\equiv 2 \pmod{6}$ et $n \not\equiv 5 \pmod{6}$.

Faire la liste des nombres premiers p tels que $p \leq 50$ et $p \equiv 1 \pmod{6}$, et vérifier que chacun d'entre eux est de la forme $a^2 + 3b^2$.

**Complément de cours :
infinitude des nombres premiers congrus à 1 modulo 3.**

Bien que j'aie dit au cours début avril qu'il n'existe pas de "preuve élémentaire" de cette assertion, en voici une ; c'est encore un cas particulier "du" théorème de Dirichlet.

Montrons d'abord que, si n est un entier positif et p un diviseur premier de $n^2 + n + 1$ tel que $p \neq 5$, alors $p \equiv 1 \pmod{3}$.

Remarquons que $n^3 - 1 = (n - 1)(n^2 + n + 1) \equiv 0 \pmod{p}$, c'est-à-dire $n^3 \equiv 1 \pmod{p}$. Par ailleurs $n \not\equiv 1 \pmod{p}$, sinon on aurait $n^2 + n + 1 \equiv 3 \pmod{p}$, ce qui est exclu car $n^2 + n + 1 \equiv 0 \pmod{p}$ et $p \neq 3$.

Notons ν la classe de n dans le groupe $\mathcal{U}(\mathbf{Z}/p\mathbf{Z})$ des éléments inversibles de $\mathbf{Z}/p\mathbf{Z}$. Nous venons de montrer que $\nu^3 = 1$ et $\nu \neq 1$, donc en particulier que le groupe $\mathcal{U}(\mathbf{Z}/p\mathbf{Z})$ contient un élément d'ordre 3. Il résulte du théorème de Lagrange que l'ordre de ce groupe, qui est $p - 1$, est un multiple de l'ordre de ν , qui est 3 ; c'est-à-dire que $p \equiv 1 \pmod{3}$.

Soient p_1, \dots, p_k des nombres premiers tous congrus à 1 modulo 3. Posons $n = 3 \prod_{j=1}^k p_j$ et choisissons un diviseur premier p de $n^2 + n + 1$. Alors $p \notin \{3, p_1, \dots, p_k\}$ par l'argument usuel. Ce qui précède montre que $p \equiv 1 \pmod{3}$. Il en résulte qu'il existe une infinité de nombres premiers congrus à 1 modulo 3.

Il est encore bien plus élémentaire de montrer qu'il existe aussi une infinité de nombres premiers congrus à 2 modulo 3. (Voir l'exercice VII.15 des notes.)

Ex. 4. Etant donné un nombre premier $\ell \geq 3$, montrer qu'il existe une infinité de nombres premiers congrus à 1 modulo ℓ . [Indication : adapter la démonstration ci-dessus, en considérant les diviseurs premiers de $n^{\ell-1} + n^{\ell-2} + \dots + n + 1$.]

Ex. 5. Soit m un entier dont on sait qu'il est produit de deux nombres premiers impairs distincts p et q . Ecrire les valeurs de p et q en fonction de m et de $\varphi(m)$.

[Indication : écrire les solutions de l'équation $X^2 - (m + 1 - \varphi(m))X + m = 0$.]

Ex. 6 Dans l'anneau $\mathbb{Q}[X]$, pour les polynômes

$$A(X) = X^4 + X^3 - 8X^2 - 2X + 12 \quad \text{et} \quad B(X) = X^4 - X^3 - 8X^2 + 2X + 12,$$

trouver des polynômes $P(X), Q(X)$ tels que $A(X)P(X) + B(X)Q(X)$ soit un pgcd de $A(X)$ et $B(X)$.

Série XXI distribuée le 4 mai 2006

Rédiger les exercices 4 à 7.

Exercice 1. Soient V un espace vectoriel sur le corps \mathbf{F}_2 et u, v deux vecteurs non nuls de V . Vérifier que u et v sont linéairement indépendants si et seulement s'ils sont distincts.

L'assertion analogue pour un espace vectoriel sur \mathbf{F}_3 est-elle correcte ?

Ex. 2. (a) Voici une liste de groupes :

G_1 , le groupe cyclique $\mathbf{Z}/16\mathbf{Z}$ d'ordre 16 ;

G_2 , le groupe des éléments inversibles dans le corps \mathbf{F}_{17} ;

G_3 , le produit direct $(\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/8\mathbf{Z})$;

G_4 , le produit direct $(\mathbf{Z}/4\mathbf{Z}) \times (\mathbf{Z}/4\mathbf{Z})$;

G_5 , le groupe additif d'un espace vectoriel de dimension 2 sur \mathbf{F}_4 ;

G_6 , le groupe des isométries du plan euclidien laissant invariant un octogone régulier donné ;

G_7 , le groupe symétrique des permutations de 4 objets.

Décider pour quelles paires (i, j) les groupes G_i et G_j sont isomorphes.

(b) Exhiber deux groupes non isomorphes, tous les deux d'ordre 6.

Ex. 3. Vérifier que le polynôme $X^5 + X^2 + 1 \in \mathbb{F}_2[X]$ est irréductible.

[Indication. Dresser la liste des polynômes irréductibles de degrés 1 et 2 dans $\mathbb{F}_2[X]$ et vérifier

que le polynôme donné n'a pas de facteur de degré ≤ 2 en utilisant la formule $X^5 + X^2 + 1 = X^2(X + 1)(X^2 + X + 1) + 1$. Un polynôme non nul $P(X) \in \mathbb{K}[X]$ est dit *réductible* s'il existe des

polynômes $P_1(X)$ et $P_2(X)$ de degrés strictement inférieurs à celui de $P(X)$ tels que $P(X) = P_1(X)P_2(X)$, et *irréductible* sinon.]

Ex. 4. Dans l'anneau $\mathbb{F}_2[X]$, déterminer les diviseurs communs des polynômes

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

Ex. 5. Dans l'anneau $\mathbb{Q}[X]$, et pour les polynômes

$$P_1(X) = X^6 - 2X^5 + X^4 + X^3 + X^2 \quad \text{et} \quad P_2(X) = X^4,$$

trouver des polynômes $A_1(X), A_2(X)$ tels que $A_1(X)P_1(X) + A_2(X)P_2(X)$ soit un pgcd de $P_1(X)$ et $P_2(X)$.

[L'un des problèmes de l'examen du 11 juillet 2003.]

Ex. 6. Soient \mathbf{K} un corps et η un élément de \mathbf{K} . Il existe un unique homomorphisme d'anneaux $\Phi : \mathbf{K}[X] \rightarrow \mathbf{K}$ tel que $\Phi(X) = \eta$ et $\Phi(\xi) = \xi$ pour tout $\xi \in \mathbf{K}$.

Ecrire la valeur de Φ sur un polynôme $a_0 + a_1X + \dots + a_dX^d$ de $\mathbf{K}[X]$.

Ex. 7 (révision). On considère la matrice

$$a = \begin{pmatrix} 2 & 1+i \\ 1-i & 1 \end{pmatrix} \in M_2(\mathbb{C}).$$

(a) Calculer les valeurs propres de a et déterminer une base orthonormale de \mathbb{C}^2 (pour le produit scalaire canonique) formée de vecteurs propres de a .

(b) Déterminer une matrice unitaire u telle que la matrice $d = u^{-1}au$ soit diagonale, et écrire la matrice u^{-1} .

Série XXII distribuée le 11 mai 2006

Exercice 1, de révision. (i) Ecrire relativement à la base canonique l'endomorphisme de \mathbf{R}^2 qui est la composition d'un quart de tour dans le sens positif de la trigonométrie et d'une dilatation de rapport $\sqrt{2}$.

(ii) Ecrire dans le groupe symétrique $\text{Sym}(8)$ un élément d'ordre 12.

(iii) Ecrire l'inverse de 2 dans $\mathbf{Z}/11\mathbf{Z}$.

(iv) Ecrire un élément a de $\mathbf{Z}/8\mathbf{Z}$ tel que $a^2 \neq 0$ et $a^3 = 0$.

(v) Ecrire une matrice $a \in M_3(\mathbf{C})$ telle que $a^2 \neq 0$ et $a^3 = 0$. Est-ce possible dans $M_2(\mathbf{C})$?

(vi) Ecrire un élément a de l'anneau $\mathbf{F}_3[X]/((X^3+1)\mathbf{F}_3[X])$ tel que $a^2 \neq 0$ et $a^3 = 0$.

(vii) Existe-t-il des polynômes irréductibles de degré 4 dans $\mathbf{C}[X]$? dans $\mathbf{F}_2[X]$? dans $\mathbf{R}[X]$?

Ex. 2. Pour chacune des trois données ci-dessous consistant en un anneau A , un élément $a \in A$ déterminant un idéal principal (a) , et deux éléments $b, c \in A$, décider si b et c sont congrus modulo (a) ; répondre simplement "oui" ou "non".

(i)	$A = \mathbf{Z}$	$a = 11$	$b = 82225$	$c = 11$
(ii)	$A = \mathbf{F}_2[X]$	$a = X^2 + X + 1$	$b = X$	$c = X^2$
(iii)	$A = \mathbf{F}_2[X]$	$a = X^2 + X + 1$	$b = X$	$c = X^2 + 1$

Ex. 3. Soit $P \in \mathbf{F}_2[X]$ un polynôme de la liste ci-dessous, et n son degré. Déterminer dans chaque cas le plus petit entier $d \geq 1$ tel que $X^d \equiv 1 \pmod{P}$, ainsi que des polynômes R_1, \dots, R_d de degrés $< n$ tels que $X^j \equiv R_j \pmod{P}$ pour $j \in \{1, \dots, d\}$.

La réponse pour le cas (a) est donnée ci-dessous ; la vérifier.

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

(b) $P = X^4 + X^3 + 1$.

(c) $P = X^4 + X^3 + X^2 + X + 1$. [Il s'agit comme dans le cas (b) d'un corps à 16 éléments, en fait "du" corps à 16 éléments. Mais la classe ξ de X n'a pas le même ordre dans les cas (b) et (c). En particulier, dans le cas (c), ξ n'engendre pas le groupe multiplicatif \mathbf{K}^* des éléments non nuls du corps $\mathbf{F}_2[X]/(X^4 + X^3 + X^2 + X + 1)$. Par ailleurs, on vérifie facilement que, dans le cas (c), la classe de $X^2 + X$ est d'ordre 15 dans \mathbf{K}^* , qui est donc bien un groupe cyclique.]

Ex. 4. Soit $P(X) \in \mathbf{Q}[X]$ un polynôme de la forme

$$P(X) = X^d + k_1 X^{d-1} + \dots + k_{d-1} X + k_d,$$

où les coefficients k_1, \dots, k_d sont dans \mathbf{Z} .

(i) Montrer que toute racine $c \in \mathbf{Q}$ de $P(X)$ est un entier. [Indication : écrire $c = \frac{a}{b}$ avec $a, b \in \mathbf{Z}$ premiers entre eux, et constater que, si $|b| \geq 2$, on ne peut avoir à la fois $P(c) = 0$ et $a \not\equiv 0 \pmod{b}$.]

(ii) Montrer que le polynôme $X^3 + 2X + 1$ est irréductible dans $\mathbf{Q}[X]$ en montrant qu'il n'a aucune racine dans \mathbf{Q} . [Indication : considérer $P(n)$ pour $n \in \mathbf{Z}$, d'abord lorsque $|n| \leq 1$ et ensuite lorsque $|n| \geq 2$.]

Série XXIII distribuée le 18 mai 2006

Rédiger les exercices 3 à 5.

Exercice 1, de révision. (i) Une matrice $a \in M_3(\mathbf{C})$ peut-elle avoir quatre valeurs propres distinctes ? quatre vecteurs propres distincts ?

(ii) Soit α l'endomorphisme linéaire de \mathbf{R}^{10} pour lequel chaque axe de coordonnées est invariant, tel que la restriction de α au j -ième axe est une homothétie de rapport j (pour $j = 1, 2, \dots, 10$). Quelles sont les valeurs propres de α ?

(iii) Ecrire une matrice à trois lignes et trois colonnes, non diagonalisable, de valeurs propres 2 et 5.

Ex. 2, de révision. Soit C_3 le sous-ensemble de $M_3(\mathbf{R})$ des matrices satisfaisant les trois conditions suivantes :

- (L) la somme des éléments de chaque ligne est nulle,
- (C) la somme des éléments de chaque colonne est nulle,
- (D) la somme des éléments de chacune des deux grandes diagonales est nulle.

Vérifier que C_3 est un sous-espace vectoriel de $M_3(\mathbf{R})$, appelé l'espace des *carrés magiques* d'ordre 3, et déterminer sa dimension. [Indication : montrer que $a_{2,2} = 0$ pour tout $a \in C_3$.]

Ecrire une matrice $a \in M_3(\mathbf{R})$ satisfaisant

$$\sum_{\ell=1}^3 a_{i,\ell} = \sum_{k=1}^3 a_{k,j} = \sum_{m=1}^3 a_{m,m} = \sum_{n=1}^3 a_{n,4-n} = 15 \quad \text{pour tous } i, j \in \{1, 2, 3\},$$

matrice a dont les coefficients sont précisément 1, 2, 3, 4, 5, 6, 7, 8, 9.⁴

Quelle est la dimension de l'espace C_4 défini de manière analogue à C_3 ?

Ex. 3. (i) Soit $P(X) = X^d + k_1X^{d-1} + \dots + k_d \in \mathbf{Z}[X]$ un polynôme de degré $d \geq 1$, tel que $k_d \neq 0$. Vérifier que $k_d \equiv 0 \pmod{n}$ pour toute racine $n \in \mathbf{Z}$ de $P(X)$.

[Rappel de l'exercice XXII.4 : toute racine de $P(X)$ dans \mathbf{Q} est nécessairement dans \mathbf{Z} .]

(ii) Pour tout $k \in \mathbf{Z}$, $k \neq 0, -2$, montrer que le polynôme $X^3 + kX + 1$ est irréductible dans $\mathbf{Q}[X]$.

Ex. 4. Dresser la liste des polynômes moniques irréductibles de degrés au plus trois dans $\mathbf{F}_3[X]$.

Ex. 5. Soient p un nombre premier, \mathbf{L} un corps fini d'ordre p^2 et σ l'application de \mathbf{L} dans \mathbf{L} définie par $\sigma(x) = x^p$; on identifie \mathbf{F}_p à un sous-corps de \mathbf{L} . Montrer que σ est

- (i) un homomorphisme de corps ;
- (ii) qu'il est surjectif, et donc aussi bijectif
[indication : on peut admettre ici le théorème (démontré dans les notes) qui établit que le groupe multiplicatif \mathbf{L}^* est cyclique d'ordre $p^2 - 1$;
- (iii) et que l'ensemble de ses points fixes coïncide avec \mathbf{F}_p .

L'application σ est appelée *l'automorphisme de Frobenius* de \mathbf{L} .

- (iv)[#] Etendre ce qui précède à un corps \mathbf{L} d'ordre p^a , pour tout entier $a \geq 2$.

Série XXIV distribuée le 26 mai 2006

Rédiger les exercices 2 à 5.

Exercice 1, de révision. Soit $\mathbf{R}[X]_3$ le sous-espace vectoriel de $\mathbf{R}[X]$ des polynômes de degré au plus 3. Choisir une base de $\mathbf{R}[X]_3$ et écrire la matrice relativement à cette base de l'application $f \mapsto f'' - 3xf' - f$ (où f' et f'' désignent la première et la deuxième dérivées d'une fonction⁵ f).

- (ii) Vérifier que le polynôme $X^5 + X^2 + 1 \in \mathbf{F}_2[X]$ est irréductible.

[Indication : $X^5 + X^2 + 1 = X^2(X + 1)(X^2 + X + 1) + 1$.]

- (iii) Choisir un corps \mathbf{K} et écrire dans $\mathbf{K}[X]$ un polynôme réductible sans racine.

- (iv) Montrer que $2 \cos \frac{2\pi}{5} = \frac{\sqrt{5}-1}{2}$.

[Indication : si $z = \exp(i\frac{2\pi}{5})$, alors $\sum_{k=0}^4 z^k = 0$, donc $(z + z^{-1})^2 + (z + z^{-1}) - 1 = 0$, donc $2 \cos \frac{2\pi}{5}$ est une racine du polynôme à coefficients rationnels $X^2 + X - 1$.]

Ex. 2. On considère $P(X) = X^3 + X^2 - 2X - 1 \in \mathbf{Q}[X]$.

- (i) Montrer que le polynôme P est irréductible.

- (ii) Vérifier que $P(2 \cos \frac{2j\pi}{7}) = 0$ pour $j = 1, 2, 3$. [Indication : $\sum_{k=0}^6 (\exp(i\frac{2\pi}{7}))^k = 0$.]

⁴Question pour les mordus : Quel est le nombre des matrices de cette forme ? [Indication : aucun des coefficients "des coins" $a_{1,1}, a_{1,3}, a_{3,1}, a_{3,3}$ ne peut être 1.]

⁵Le corps \mathbf{R} étant infini, on s'autorise ici l'abus de confondre un polynôme avec l'application polynomiale correspondante, qui est plus simplement dit une "fonction", et même une fonction infiniment différentiable, de \mathbf{R} dans \mathbf{R} .

(iii) En déduire que, pour tout $j \in \mathbf{Z}$ tel que $j \not\equiv 0 \pmod{7}$, le nombre $2 \cos \frac{2j\pi}{7}$ est irrationnel.

[On peut montrer que $2 \cos \frac{2\pi}{n}$ est un nombre irrationnel pour $n = 5$ et pour tout $n \geq 7$.]

Ex. 3. Soit Q le sous-ensemble de \mathbf{F}_{13}^* des carrés des éléments non nuls de \mathbf{F}_{13} .

(i) Vérifier que Q est un sous-groupe du groupe multiplicatif \mathbf{F}_{13}^* .

(ii) Enumérer les éléments de Q . Le groupe Q est-il un groupe cyclique ? Si oui, dresser la liste de ses générateurs.

Ex. 4. Soient T un tétraèdre régulier centré à l'origine de l'espace euclidien usuel \mathbf{R}^3 et G_T [respectivement SG_T] le groupe des isométries [resp. des rotations] de \mathbf{R}^3 laissant T invariant.

(i) En numérotant les quatre sommets de T de 1 à 4, on obtient un homomorphisme $G_T \rightarrow \text{Sym}(4)$. Montrer que l'image de SG_T par cet homomorphisme coïncide avec le groupe alterné $\text{Alt}(4)$.

(ii) Le groupe G_T opère aussi sur l'ensemble des droites passant par les milieux d'arêtes opposées de T , qui sont au nombre de trois. Montrer que l'homomorphisme correspondant $G_T \rightarrow \text{Sym}(3)$ est surjectif. Déterminer son noyau, ainsi que l'image de SG_T .

Ex. 5. (i) Soit \mathbf{K} un corps fini à q éléments. Déterminer les ordres des groupes $GL_2(\mathbf{K})$ et $SL_2(\mathbf{K}) = \text{Ker}(\det : GL_2(\mathbf{K}) \rightarrow \mathbf{K}^*)$.

(ii) Considérer l'action naturelle du groupe $GL_2(\mathbf{F}_2)$ sur l'ensemble des droites contenant l'origine de l'espace vectoriel $(\mathbf{F}_2)^2$. En déduire un isomorphisme de $GL_2(\mathbf{F}_2)$ sur le groupe symétrique $\text{Sym}(3)$.

Série XXV distribuée le 1er juin 2006

Rédiger les exercices 1 à 5.

Exercice 1, de révision. (i) Ecrire une matrice $a \in M_2(\mathbf{C})$, $a \neq \text{id}$, qui soit à la fois unitaire et autoadjointe.

(ii) Trouver une matrice autoadjointe $b \in M_2(\mathbf{C})$ dont les valeurs propres soient des nombres positifs et qui soit telle que $b^2 = \begin{pmatrix} 1 & i \\ -i & 1 \end{pmatrix}$.

[Indication : trouver une matrice unitaire u telle que $u \begin{pmatrix} 1 & i \\ -i & 1 \end{pmatrix} u^*$ soit de la forme $\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$ et calculer $b = u^* \begin{pmatrix} \sqrt{\lambda} & 0 \\ 0 & \sqrt{\mu} \end{pmatrix} u$.]

Ex. 2. Montrer que le polynôme $X^3 + 3X^2 + 7$ est irréductible dans $\mathbf{Q}[X]$.

[Indication : revoir la série XXIII.]

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

$$(*) \quad x^2 + y^2 - 7z^2 = 0$$

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

- (i) Calculer les carrés des tous les éléments de $\mathbf{Z}/7\mathbf{Z}$.
 (ii) Montrer que la seule solution dans $\mathbf{Z}/7\mathbf{Z}$ de l'équation $a^2 + b^2 = 0$ est $a = b = 0$.
 (iii) Montrer que, s'il existe $(x, y, z) \in \mathbf{Z}^3$ tels que $x^2 + y^2 - 7z^2 = 0$, alors $(\frac{x}{7}, \frac{y}{7}, \frac{z}{7})$ est aussi dans \mathbf{Z}^3 , et solution de (*).
 (iv) Conclure.

Ex. 4. Dans l'anneau $\mathbf{Q}[X]$, et pour les polynômes

$$P_1(X) = X^6 - 2X^5 + 2X^3 + X^2 \quad \text{et} \quad P_2(X) = X^4 + X^3,$$

trouver des polynômes $A_1(X), A_2(X)$ tels que $A_1(X)P_1(X) + A_2(X)P_2(X)$ soit un pgcd de $P_1(X)$ et $P_2(X)$.

Ex. 5. On considère le polynôme $P(X) = X^3 + 3X^2 + 4X + 3 \in \mathbf{F}_5[X]$, où \mathbf{F}_5 désigne le corps à 5 éléments, l'anneau quotient $\mathbf{K} = \mathbf{F}_5[X]/(P)$, et la classe $\xi \in \mathbf{K}$ de X modulo P .

- (j) Quel est le nombre d'éléments de \mathbf{K} ? (justifier !). Est-ce un corps ?
 (jj) Ecrire ξ^{-1} comme combinaison linéaire de 1, ξ et ξ^2 .

Série XXVI distribuée le 8 juin 2006

Rédiger les exercices 2 à 5.

Exercice 1, de révision. On considère l'espace hermitien \mathbf{C}^2 muni du produit scalaire et de la base canoniques. Relativement à cette base, l'une des matrices

$$\begin{pmatrix} \frac{3}{4} & i\frac{\sqrt{3}}{4} \\ -i\frac{\sqrt{3}}{4} & \frac{1}{4} \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} \frac{\sqrt{3}}{2} & \frac{i}{2} \\ -\frac{i}{2} & -\frac{\sqrt{3}}{2} \end{pmatrix}$$

correspond à une projection orthogonale sur un sous-espace V de dimension 1 de \mathbf{C}^2 .

- (i) Laquelle de ces deux matrices ?
 (ii) Ecrire les coordonnées d'un vecteur unité de V .

Ex. 2. On note ξ la classe de X dans le corps $\mathbf{K} = \mathbf{F}_3[X]/(X^2 + 1)$, de sorte que tout élément de \mathbf{K} s'écrit $a + b\xi$, avec $a, b \in \mathbf{F}_3$. Avec cette écriture, dresser la liste des carrés dans \mathbf{K} .

Ex. 3. Déterminer pour chaque $q \in \{3, 5, 7, 9\}$ si -1 est un carré dans un corps à q éléments.

(Admettre le résultat selon lequel deux corps finis ayant le même nombre d'éléments sont isomorphes.)

La même question a-t-elle un sens pour $q \in \{2, 4, 6, 8\}$?

Ex. 4. Soit Γ_2 le graphe à 7 sommets et 6 arêtes défini comme suit. Les sommets sont indexés par les suites de 0 et de 1 de longueurs au plus deux, c'est-à-dire par la suite vide \emptyset , les deux suites de longueur un 0 et 1, et les quatre suites de longueur deux 00, 01, 10 et 11. Chaque arête a pour extrémités une suite de longueur k (où $1 \leq k \leq 2$) et la suite

de longueur $k - 1$ obtenue en effaçant la dernière lettre de la première suite ; par exemple : une arête de 0 à \emptyset , une de 1 à \emptyset , ..., une de 11 à 1.

- (i) Dessiner le graphe Γ_2 .
- (ii) Montrer que tout automorphisme de ce graphe fixe le sommet \emptyset .
- (iii) Combien ce graphe contient-il d'automorphismes fixant les sommets 0 et 1 ?
- (iv) Combien ce graphe contient-il d'automorphismes ?
- (v)[#] Définir un graphe Γ_3 à 15 sommets (suites de 0 et de 1 de longueurs au plus trois) et 14 arêtes défini de manière analogue, et répondre aux questions correspondantes ; en particulier, quel est l'ordre du groupe des automorphismes de Γ_3 ?

Ex. 5. On pose $\tau = \frac{1}{2}(1 + \sqrt{5})$, et on rappelle que $\tau^2 = \tau + 1$. L'objectif de l'exercice est de montrer (au moins partiellement !) que, dans l'espace euclidien \mathbf{R}^3 muni du produit scalaire canonique, les 12 points

$$(*) \quad (\pm\tau, \pm 1, 0), \quad (0, \pm\tau, \pm 1), \quad (\pm 1, 0, \pm\tau)$$

sont les sommets d'un icosaèdre régulier.

(i) Dessiner un croquis de trois rectangles dans les plans de coordonnées de sommets ceux de (*).

(ii) Calculer les distances séparant $(\tau, 1, 0)$ de chacun des 5 sommets $(\tau, -1, 0)$, $(0, \tau, \pm 1)$, $(1, 0, \pm\tau)$. Noter que ces cinq sommets sont dans le plan affine d'équation $\tau x + y = \tau$. [Ce sont les voisins de $(\tau, 1, 0)$ dans l'icosaèdre.]

(iii) Calculer les longueurs des côtés du pentagone de sommets

$$(0, \tau, 1), \quad (1, 0, \tau), \quad (\tau, -1, 0), \quad (1, 0, -\tau) \quad \text{et} \quad (0, \tau, -1).$$

On peut répéter ce qui précède en remplaçant $(\tau, 1, 0)$ par chacun des 11 autres sommets de (*).

Complément aux notes

A propos de la surjectivité de l'homomorphisme $SU(2) \longrightarrow SO(3)$

Rappel des notations et de la situation.

L'espace $M_2(\mathbf{C})$ est considéré (entre autres ...) comme un espace vectoriel *réel* de dimension 8, muni du produit scalaire défini par

$$(*) \quad \left\langle \begin{pmatrix} z_1 & z_2 \\ z_3 & z_4 \end{pmatrix} \middle| \begin{pmatrix} w_1 & w_2 \\ w_3 & w_4 \end{pmatrix} \right\rangle = \frac{1}{2} \operatorname{Re} \left(\operatorname{trace} \left(\begin{pmatrix} z_1 & z_2 \\ z_3 & z_4 \end{pmatrix}^* \begin{pmatrix} w_1 & w_2 \\ w_3 & w_4 \end{pmatrix} \right) \right) \\ = \frac{1}{2} \operatorname{Re} \left(\sum_{j=1}^4 \overline{z_j} w_j \right).$$

Il contient notamment :

— le sous-espace réel \mathbf{H} de dimension 4 des matrices de la forme $\begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix}$, avec

$z, w \in \mathbf{C}$, où la norme est donnée par $\left\| \begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix} \right\|^2 = |z|^2 + |w|^2 = \det \begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix}$
en vertu de (*); on peut identifier \mathbf{H} à l'espace euclidien \mathbf{R}^4 ;

- le groupe spécial unitaire $SU(2)$ des matrices de la forme $\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}$, avec $a, b \in \mathbf{C}$ et $|a|^2 + |b|^2 = 1$; géométriquement, c'est la sphère unité \mathbf{S}^3 de \mathbf{R}^4 ;
- le sous-espace réel \mathbf{E} de dimension 3 des matrices autoadjointes à trace nulle, c'est-à-dire des matrices de la forme $\begin{pmatrix} x_1 & x_2 + ix_3 \\ x_2 - ix_3 & -x_1 \end{pmatrix}$, avec $x = (x_1, x_2, x_3) \in \mathbf{R}^3$; nous identifions \mathbf{E} à l'espace euclidien \mathbf{R}^3 , avec le produit scalaire usuel, et de même le groupe $\mathcal{SO}(E)$ avec le groupe $\mathcal{SO}(3)$;
- la sphère unité de \mathbf{E} , que nous notons \mathbf{S}^2 , qui est le sous-ensemble de \mathbf{E} des matrices X telles que $\langle X|X \rangle = 1$ (condition qui se trouve être équivalente à $X^2 = e_0$) ;
- la matrice unité $e_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

On vérifie que

- \mathbf{H} est une sous-algèbre de $M_2(\mathbf{C})$, c'est-à-dire que le produit de deux matrices de \mathbf{H} est encore dans \mathbf{H} ;
- on a une décomposition en somme directe⁶ $\mathbf{H} = \mathbf{R}e_0 \oplus i\mathbf{E}$ qui est orthogonale.

Soit $g \in SU(2)$; pour tout $Y \in \mathbf{H}$, on vérifie d'abord que $\|gY\|^2 = \|Y\|^2 = \|Yg\|^2$, et donc que l'endomorphisme linéaire de \mathbf{H} qui applique Y sur gYg^* est orthogonal. Le vecteur e_0 étant invariant par cette endomorphisme, son orthogonal $e_0^\perp = i\mathbf{E}$ l'est aussi, de sorte qu'on obtient par restriction une transformation orthogonale $\Psi(g) : X \mapsto gXg^*$ de \mathbf{E} . On vérifie ensuite que $\det(\Psi(g)) = +1$, et que l'application

$$\Psi : SU(2) \longrightarrow \mathcal{SO}(3)$$

est un homomorphisme de groupes.

Le théorème principal de ce chapitre établit que Ψ est un homomorphisme surjectif de noyau $\pm e_0$. La partie principale de la démonstration est celle qui concerne la surjectivité de Ψ . Voici, aux 2e et 3e pas ci-dessous, une variante plus directe de l'argument rédigé dans les notes.

Démonstration de la surjectivité de Ψ .

Premier pas : les rotations autour du premier axe sont dans l'image de Ψ . En effet, pour tout $\theta \in \mathbb{R}$, on a $\begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix} \in SU(2)$ et

$$\begin{aligned} & \begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix} \begin{pmatrix} x_1 & x_2 + ix_3 \\ x_2 - ix_3 & -x_1 \end{pmatrix} \begin{pmatrix} e^{-i\theta} & 0 \\ 0 & e^{i\theta} \end{pmatrix} \\ &= \begin{pmatrix} x_1 & e^{2i\theta}(x_2 + ix_3) \\ e^{-2i\theta}(x_2 - ix_3) & -x_1 \end{pmatrix} \\ &= \begin{pmatrix} x_1 & y_2 + iy_3 \\ y_2 - iy_3 & -x_1 \end{pmatrix} \end{aligned}$$

avec

$$\begin{aligned} y_2 &= (\cos(2\theta))x_2 - (\sin(2\theta))x_3 \\ y_3 &= (\sin(2\theta))x_2 + (\cos(2\theta))x_3. \end{aligned}$$

⁶Remarque, pour tout sous-espace vectoriel réel V de $M_2(\mathbf{C})$, le sous-ensemble iV est aussi un sous-espace vectoriel réel de $M_2(\mathbf{C})$; ceci s'applique ici à E .

Il en résulte que

$$\Psi \left(\begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix} \right) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(2\theta) & -\sin(2\theta) \\ 0 & \sin(2\theta) & \cos(2\theta) \end{pmatrix}$$

est la rotation d'angle 2θ autour du premier axe. [Noter le facteur 2 !]

Deuxième pas : les rotations autour d'un axe arbitraire sont dans l'image de Ψ . Choisissons arbitrairement une matrice $X = \begin{pmatrix} x_1 & x_2 + ix_3 \\ x_2 - ix_3 & -x_1 \end{pmatrix} \in \mathbf{S}^2$, déterminant un axe de \mathbf{S}^2 passant par X et $-X$. Choisissons également un nombre $\theta \in \mathbf{R}$, et posons

$$g = (\cos \theta)e_0 + (\sin \theta)iX = \begin{pmatrix} \cos \theta + (\sin \theta)ix_1 & (\sin \theta)i(x_2 + ix_3) \\ (\sin \theta)i(x_2 - ix_3) & \cos \theta - (\sin \theta)ix_1 \end{pmatrix}.$$

C'est une matrice de la forme $\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}$, avec

$$|a|^2 + |b|^2 = (\cos \theta)^2 + (\sin \theta)^2(x_1^2 + x_2^2 + x_3^2) = 1,$$

de sorte que $g \in \mathcal{SU}(2)$.

La rotation $\Psi(g)$ fixe le point X de la sphère \mathbf{S}^2 , puisque $\Psi(g)(X) = g^*Xg = g^*gX = X$ (car X et g commutent), et de même $\Psi(g)$ fixe le point antipodal $-X$; donc $\Psi(g)$ est une rotation de \mathbf{S}^2 dont l'axe passe par X et $-X$.

Les valeurs propres de g sont $e^{i\theta}$ et $e^{-i\theta}$, car $\det(g) = 1$ et $\text{trace}(g) = 2 \cos \theta$. Le théorème spectral pour les matrices autoadjointes implique qu'il existe une matrice unitaire $h \in \mathcal{U}(2)$ telle que $g = h \text{diag}(e^{i\theta}, e^{-i\theta})h^*$; quitte à multiplier h par une racine carrée de $\det(h)^{-1}$, on peut supposer que $h \in \mathcal{SU}(2)$ [prendre toutefois garde au fait qu'il n'existe pas de choix de racine carrée qui soit cohérent pour toutes les matrices de $\mathcal{SU}(2)$ à la fois]. Par suite, la rotation

$$\Psi(g) = \Psi(h)\Psi(\text{diag}(e^{i\theta}, e^{-i\theta}))\Psi(h)^{-1}$$

est conjuguée à la rotation $\Psi(\text{diag}(e^{i\theta}, e^{-i\theta}))$ d'angle 2θ autour du premier axe (premier pas de la preuve). En faisant varier θ , on obtient toutes les rotations de \mathbf{S}^2 dont l'axe passe par X et $-X$.

Comme X est arbitraire, toute rotation de \mathbf{S}^2 est dans l'image de Ψ .

Noyau de Ψ .

Soit $g = \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \in \mathcal{SU}(2)$. Si $g \in \text{Ker}(\Psi)$, alors $gX = Xg$ pour tout $X \in \mathbf{E}$. En particulier, g commute à $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, ce qui implique $b = 0$, et g commute à $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, ce qui implique que a est réel, donc que $a = \pm 1$. Par suite $g \in \text{Ker}(\Psi)$ si et seulement si $g = \pm e_0$. \square

Série XXVII distribuée le 15 juin 2006**Rédiger les exercices 1 à 3, ainsi que 5.**

Exercice 1, de révision. (i) Indiquer un exemple d'opérateur normal, agissant sur un espace hermitien, qui ne soit ni autoadjoint ni unitaire.

(ii) Soient V un espace hermitien, $\alpha \in \mathcal{L}(V)$ et $x, y \in \mathbf{C}$ des nombres complexes tels que $|x| = |y|$. Vérifier que $x\alpha + y\alpha^*$ est normal.

(iii) Soient $P \in \mathbf{C}[X]$ un polynôme à coefficients complexes et V comme ci-dessus, avec $\dim(V) \geq 2$. Les assertions suivantes sont-elles correctes ? (répondre par “oui” ou “non”).

(b) Pour tout opérateur autoadjoint α sur V , l'opérateur $P(\alpha)$ est autoadjoint.

(#) Pour tout opérateur normal α sur V , l'opérateur $P(\alpha)$ est normal.

(iv) Exhiber deux groupes finis de même ordre, l'un abélien et l'autre pas. [Les expressions “groupe abélien” et “groupe commutatif” sont synonymes.]

(v) Exhiber deux groupes finis abéliens de même ordre, l'un cyclique et l'autre pas.

Ex. 2. Le but de cet exercice est d'indiquer qu'il y a une relation étroite entre la factorisation en nombres premiers et certains calculs de racines carrées. Pour un entier n , notons ici \mathcal{Q}_n le sous-ensemble des carrés dans $\mathbf{Z}/n\mathbf{Z}$.

(i) Soit p un nombre premier tel que $p \equiv 3 \pmod{4}$. Vérifier que $-1 \notin \mathcal{Q}_p$. [Indication : ramenez-vous à un lemme du cours.]

(ii) Soit p comme en (i) et soit $c \in \mathcal{Q}_p$, $c \neq 0$; on pose $x = c^{(p+1)/4}$. Montrer que $x^2 = c$. [Indication : $c^{(p-1)/2} = 1$.]

Remarque. Si p est un nombre premier tel que $p \equiv 1 \pmod{4}$, il existe des algorithmes rapides pour calculer les racines carrées d'éléments dans \mathcal{Q}_p ; voir par exemple l'exercice 1.4 dans G. Zémor, *Cours de cryptographie*, Cassini, 2000. En revanche, si n est composé, il est équivalent (dans un sens qu'on peut préciser) de savoir calculer des racines carrées d'éléments de \mathcal{Q}_n et de savoir factoriser n ; voir le numéro 4.4.1 dans le même livre. Voir aussi la question (iii) qui suit.

(iii) Soient $x, y \in \mathbf{Z}$ tels que

$$x + y \not\equiv 0 \pmod{n}, \quad x - y \not\equiv 0 \pmod{n}, \quad x^2 \equiv y^2 \pmod{n}.$$

Montrer que les nombres $\text{pgcd}(n, x + y)$ et $\text{pgcd}(n, x - y)$ sont des diviseurs stricts de n . [Indication : n divise $(x + y)(x - y)$ sans diviser $x + y$ ni $x - y$.]

Ex. 3. (i) Existe-t-il une solution en entiers positifs de l'équation à trois inconnues

$$28x + 30y + 31z = 365 ?$$

(ii) Trouver toutes les solutions en entiers positifs de l'équation à deux inconnues

$$35x + 45y = 600.$$

Ex. 4#. Rédiger un protocole permettant à Alice et Bob de jouer à pile ou face par téléphone.

Indication. Alice et Bob maîtrisent tous deux le système RSA.

Ex. 5. Soit $V = \mathcal{C}_{\mathbb{R}}([-1, 1])$ l'espace vectoriel réel des fonctions continues à valeurs réelles⁷ sur l'intervalle $[-1, 1]$, muni du produit scalaire défini par

$$\langle f | g \rangle = \int_{-1}^1 f(t)g(t)dt,$$

et soit (v_0, v_1, \dots) la suite des fonctions définies par $v_n(t) = t^n$. Soit (e_0, e_1, \dots) la suite de polynômes définis par le procédé de Gram-Schmidt. Par ailleurs, on pose

$$(*) \quad P_n(t) = \frac{1}{2^n n!} \frac{d^n}{dt^n} ((t^2 - 1)^n)$$

pour tout $n \geq 0$. Le but de l'exercice est de montrer les relations

$$(**) \quad P_n(t) = \frac{e_n(t)}{e_n(1)}.$$

(i) Calculer e_n et P_n , et vérifier $(**)$ pour $n = 0, 1, 2$.

(ii) Vérifier que $P_n(t)$ est un polynôme de degré n et que $P_n(1) = 1$.

(iii) Vérifier que $\frac{d^j}{dt^j} ((t^2 - 1)^n)$ s'annule en $t = \pm 1$ si $j < n$.

(iv) Montrer que $\int_{-1}^1 P_n(t)t^m dt = 0$ si $m < n$.

[Indication : intégrer m fois par parties, en utilisant (iii).]

(v) En déduire que $\int_{-1}^1 P_n(t)P_m(t)dt = 0$ si $n \neq m$.

(vi) Achever la preuve des relations $(**)$.

(vii) On peut montrer que $\int_{-1}^1 (P_n(t))^2 dt = \frac{2}{2n+1}$ pour tout $n \geq 0$. Vérifier cette égalité pour $n \leq 2$.

Les polynômes P_n sont les *polynômes de Legendre*.

INDICATION DÉTAILLÉE POUR L'EXERCICE 4

Alice a publié un nombre n , produit de deux nombres premiers qu'elle est seule à connaître ; elle a aussi publié un nombre $e \in \{1, \dots, n\}$ premier à $\varphi(n)$, mais elle est seule à connaître la valeur de $\varphi(n)$ et l'inverse d de e modulo $\varphi(n)$. Au lieu de choisir "pile" ou "face", Alice choisit un nombre pair ou impair $x \in \{1, \dots, n\}$; elle annonce qu'elle a fait son choix et publie un nombre $y \in \{1, \dots, n\}$ tel que $y \equiv x^e \pmod{n}$.

Bob choisit le gagnant parmi "pair" ou "impair". Il connaît y mais, à ce stade, il n'a aucun moyen de deviner la parité de x .

Alice déclare qu'elle a gagné ou perdu selon que la parité de x est celle choisie par Bob ou non. Alice prouve sa bonne foi en révélant x .

Bob s'assure de la bonne foi d'Alice en vérifiant que $y \equiv x^e \pmod{n}$.

⁷Pour rester dans les limites des hypothèses du cours, il faudrait remplacer V par l'espace des fonctions à valeurs réelles qui sont polynomiales de degré au plus N , où N est un entier fixé (y penser comme un entier assez grand), et considérer dans la suite des entiers n tels que $0 \leq n \leq N$.

Série XXVIII — réserve

Exercice 1. Identifions \mathbf{Z}^2 à l'ensemble des points à coordonnées entières dans le plan \mathbf{R}^2 . Soit S le plus petit sous-ensemble de \mathbf{Z}^2 tel que

$$(0, 0), (0, 1), (1, 0) \in S$$

et

$$\text{si } (a, b) \in S \text{ et } (c, d) \in S, \text{ alors } (2c - a, 2d - b) \in S.$$

Montrer que $(1, 1) \notin S$.

[Solution : $xy \equiv 0 \pmod{2}$ pour tout $(x, y) \in S$.]

Ex. 2. Soient $a, b \in \mathbf{Z}$. Montrer que $10a + b$ est un multiple de 7 si et seulement si $a - 2b$ l'est.

Ex. 3. Soient $\lambda_0, \lambda_1, \dots, \lambda_n$ des nombres complexes distincts deux à deux. Pour tout $k \in \{0, 1, \dots, n\}$, on définit un polynôme ℓ_k de degré n en posant

$$\ell_k(z) = \frac{\prod_{0 \leq j \leq n, j \neq k} (z - \lambda_j)}{\prod_{0 \leq j \leq n, j \neq k} (\lambda_k - \lambda_j)}.$$

(i) Vérifier que $\sum_{k=0}^n \ell_k(z) = 1$ pour tout $z \in \mathbf{C}$.

[Indication : calculer $\ell_k(\lambda_i)$ pour $k, i \in \{0, 1, \dots, n\}$.]

(ii) Montrer de même que

$$\sum_{k=0}^n \lambda_k^\alpha \ell_k(z) = z^\alpha$$

pour tous $\alpha \in \{0, 1, \dots, n\}$ et $z \in \mathbf{C}$.

(iii) Vérifier la propriété suivante, en raison de quoi les polynômes ℓ_k sont appelés des *polynômes d'interpolation* : pour $\lambda_0, \lambda_1, \dots, \lambda_n \in \mathbf{C}$ comme ci-dessus et $w_0, \dots, w_n \in \mathbf{C}$, l'unique polynôme de degré au plus n prenant en chaque λ_j la valeur w_j est le polynôme $\sum_{k=0}^n w_k \ell_k$.

Ex. 4. Pour tout entier $n \geq 1$, notons $f(n)$ le maximum des ordres des éléments du groupe symétrique de n lettres. Tabuler la fonction $f(n)$ pour $n \leq 12$.

[Indication par un exemple. Soit $\sigma \in \text{Sym}(7)$ une permutation dont les cycles sont de longueurs n_1, \dots, n_k , où chaque point fixe est compté comme un cycle de longueur 1 ; en particulier, $n = n_1 + \dots + n_k$. Alors l'ordre de σ est le plus grand commun diviseur des entiers n_1, \dots, n_k .

Pour $n = 7$, les possibilités pour (n_1, \dots, n_k) , avec $n_1 \geq \dots \geq n_k$, sont

$$(7), (6, 1), (5, 2), (5, 1, 1), (4, 3), (4, 2, 1), (4, 1, 1, 1), \text{ et des } k\text{-uplets où } n_1 \leq 3.$$

Il en résulte que $f(7) = \text{pgcd}(4, 3) = 12$.]

Ex. 5. Montrer que l'équation

$$x^2 + y^2 = 3$$

n'a pas de solution avec $x, y \in \mathbf{Q}$. [Indication : montrer que l'équation $x^2 + y^2 = 3z^2$ n'a pas de solution entières en raisonnant modulo 3.]

Ex. 6. Soient n un entier, $n \geq 2$, et $\mathcal{U}(\mathbf{Z}/n\mathbf{Z})$ le groupe multiplicatif des éléments inversibles de l'anneau $\mathbf{Z}/n\mathbf{Z}$. Notons $\lambda(n)$ le plus petit entier $\ell \geq 1$ tel que $g^\ell = 1$ pour tout $g \in \mathcal{U}(\mathbf{Z}/n\mathbf{Z})$

(i) Observer que $\lambda(n)$ est un diviseur de $\varphi(n)$, c'est-à-dire de la valeur en n de la fonction d'Euler.

(ii) Vérifier que $\lambda(24) = 2 < \varphi(24) = 8$.

Pour quelques indications supplémentaires sur la *fonction de Carmichael* λ , voir par exemple le paragraphe 5.1.1 de G. Zémor, *Cours de cryptographie*, Cassini, 2000. En particulier, si $n = 2^{\alpha_0} p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, alors $\lambda(n) = \text{ppcm}(\lambda(2^{\alpha_0}), \varphi(p_1^{\alpha_1}), \dots, \varphi(p_r^{\alpha_r}))$, où $\lambda(1) = 1$, $\lambda(2^t) = 2^{t-1}$ si $t \in \{1, 2\}$, et $\lambda(2^t) = 2^{t-2}$ si $t \geq 3$.

Ex. 7. (i) Vérifier que la matrice $\begin{pmatrix} 1 & \lambda \\ \lambda & 1 \end{pmatrix}$ est normale pour tout $\lambda \in \mathbf{C}$. Pour quelles valeurs de λ est-elle auto-adjointe ? unitaire ?

(ii) Dans la liste ci-dessous, identifier quelles sont les matrices qui sont auto-adjointes, unitaires, normales.

$$\begin{pmatrix} e^{i\alpha} & 0 & 0 \\ 0 & e^{i\beta} & 0 \\ 0 & 0 & e^{i\gamma} \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix}, \quad \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix},$$

$$\begin{pmatrix} a & b+ic \\ b-ic & d \end{pmatrix}, \quad \begin{pmatrix} a & b+ic \\ -b+ic & d \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

(les lettres $\alpha, \beta, \gamma, \theta, a, b, c$ représentent des nombres réels).

Ex. 8. Soit $a \in M_3(\mathbf{C})$ une matrice de valeurs propres 0, 1, 2. Quelles sont les valeurs propres de la matrice $I_3 + a - 2a^3$?

Correction aux notes concernant le polynôme caractéristique d'une matrice

Soient \mathbf{K} un corps, $n \geq 1$ un entier, $A = (a_{i,j})_{1 \leq i,j \leq n} \in M_n(\mathbf{K})$ une matrice et

$$\begin{aligned}
 \det(XI_n - A) &= \sum_{\sigma \in \text{Sym}(n)} \epsilon(\sigma) (X\delta_{\sigma(1),1} - a_{\sigma(1),1}) \cdots (X\delta_{\sigma(n),n} - a_{\sigma(n),n}) \\
 (*) \qquad &= X^n + c_1(A)X^{n-1} + c_2(A)X^{n-2} + \cdots + c_{n-1}(A)X + c_n(A)
 \end{aligned}$$

son polynôme caractéristique ($\delta_{i,j}$ est le symbole de Kronecker, qui vaut 1 si $i = j$ et 0 sinon).

Si S est une matrice inversible dans $M_n(\mathbf{K})$, on vérifie sans peine que A et SAS^{-1} ont même polynôme caractéristique. Lorsque $\mathbf{K} = \mathbf{C}$, il existe une matrice inversible S telle que la matrice SAS^{-1} soit triangulaire, avec termes diagonaux les valeurs propres $\lambda_1, \dots, \lambda_n$ de A . Il en résulte que

$$(**) \qquad c_p(A) = c_p(SAS^{-1}) = (-1)^p \sum_{1 \leq i_1 < \cdots < i_p \leq n} \lambda_{i_1} \cdots \lambda_{i_p}$$

pour tout $p \in \{1, \dots, n\}$. En particulier, $c_n(A) = (-1)^n \det(A)$.

En séparant dans la somme \sum_{σ} de (*) le terme pour lequel σ est l'identité des autres termes, on s'assure que $\det(XI_n - A)$ est la somme de $(X - a_{1,1}) \cdots (X - a_{n,n})$ et d'un polynôme d'ordre au plus $n - 2$. Il en résulte que

$$-c_1(A) = \sum_{i=1}^n a_{i,i} = \text{trace}(A),$$

ce qui est cohérent avec l'égalité $-c_1(A) = \lambda_1 + \cdots + \lambda_n$ établie en (**).

L'indication donnée dans les notes pour $c_2(A)$ ne vaut que lorsque les termes diagonaux $a_{i,i}$ sont nuls⁸. Supposons désormais que ce soit le cas (ça l'est lorsque A est la matrice d'adjacence d'un graphe), et reprenons ce point.

Dans (*), les termes en X^{n-2} proviennent de permutations σ ayant exactement $n - 2$ points fixes, c'est-à-dire des transpositions (i, j) , où i, j sont deux entiers *distincts* entre 1 et n . Par suite

$$c_2(A) = \sum_{1 \leq i < j \leq n} \epsilon(i, j) (-a_{j,i}) (-a_{i,j}) = - \sum_{1 \leq i < j \leq n} a_{j,i} a_{i,j}.$$

Lorsque A est la matrice d'adjacence d'un graphe $G = (V, E)$, le coefficient $-c_2(A)$ est donc bien le nombre $|E|$ des arêtes de G .

On montre de manière analogue que $-c_3(A)$ est le double du nombre des triangles de G .

⁸De même, il faut supposer que les termes diagonaux sont nuls pour que $(-1)^p c_p(A)$ soit égal à la somme des mineurs principaux de A .

QUESTIONS PRINCIPALES POUR LES EXAMENS ORAUX⁹

- (i) Définition de la dimension d'un espace vectoriel de type fini sur un corps \mathbf{K} ; rôle du lemme d'échange de Grassmann.
- (ii) Espaces vectoriels d'applications linéaires $\mathcal{L}(W, V)$ et espaces de matrices $M_{m,n}(\mathbf{K})$; changements de bases.
- (iii) Formule de la dimension pour une application linéaire $f : V \longrightarrow W$ lorsque V est un espace vectoriel de dimension finie. Rang d'une application linéaire.
- (iv) Relations d'équivalence, espaces vectoriels quotients et espaces vectoriels duaux. Pour un espace V complexe et hermitien, isomorphisme de V avec son dual.
- (v) Groupes symétriques. Décomposition en cycles d'une permutation. Exemples de groupes et homomorphismes.
- (vi) Déterminants des matrices : définition, propriétés, calculs ; cas des matrices triangulaires par blocs. Notions de déterminant et de polynôme caractéristique pour un endomorphisme linéaire.
- (vii) Espaces propres, vecteurs propres, valeurs propres, multiplicités. Trigonalisation et diagonalisation des matrices complexes.
- (viii) L'inégalité de Cauchy-Schwarz (cas réel et complexe).
- (ix) Le procédé d'orthonormalisation de Gram-Schmidt (cas réel et complexe).
- (x) Le théorème spectral pour les matrices réelles symétriques et pour les opérateurs normaux sur les espaces hermitiens.
- (xi) Algorithme d'Euclide pour le calcul du pgcd. Cas des entiers et des polynômes.
- (xii) Infinitude des nombres premiers congrus à 1 modulo 4, congrus à 3 modulo 4.
- (xiii) Théorème de Bézout. Cas des entiers et des polynômes.
- (xiv) Le théorème chinois.
- (xv) Le théorème de Fermat–Euler.
- (xvi) Cas où $\mathbf{Z}/(d)$ est un corps, cas où $\mathbf{K}[X]/(P(X))$ est un corps. Exemples de corps finis.
- (xvii) Groupes de symétrie SG_P et G_P d'un polytope P dans l'espace euclidien de dimension 3. Cas où P est un polytope régulier (tétraèdre, octaèdre, cube, icosaèdre, dodécaèdre). Isomorphismes de G_T et SG_C avec $\text{Sym}(4)$.
- (xviii) L'homomorphisme $SU(2) \longrightarrow SO(3)$.
- (xix) Spectres de graphes.

⁹La question (xix) sera posée à la session d'automne, mais pas à la session de juillet.