Lycée Henri IV
MPSI 2015/2016

Devoir surveillé
23/5/2016

DEVOIR SURVEILLÉ 9

(durée : 4 h 00)

Rédigez vos réponses dans un français correct. Terminez chaque résolution d'exercice par une conclusion encadrée ou soulignée. Laissez une marge au correcteur.

Les exercices sont indépendants et peuvent être traités dans n'importe quel ordre. Dans un exercice avec plusieurs questions, on pourra, si besoin est, admettre le résultat d'une question pour répondre aux suivantes.

La calculatrice n'est pas autorisée.

EXERCICE 1

Nombres algébriques

Dans cet exercice, le corps de base de tous les espaces vectoriel est $\mathbb{Q}$. Ainsi, toutes les combinaisons linéaires envisagées sont à coefficients rationnels.

Soit $\alpha \in \mathbb{C}$. On dit que α est *algébrique* lorsqu'il existe un polynôme non nul P à coefficients rationnels tel que α est racine de P. Le sous-ensemble de $\mathbb{C}$ constitué des nombres algébriques est noté $\overline{\mathbb{Q}}$ (ici, cette notation ne désigne pas le complémentaire).

L'objet de cet exercice est de démontrer que $\overline{\mathbb{Q}}$ est un sous-corps dénombrable de $\mathbb{C}$.

1. Démontrer que $\mathbb{Q} \subsetneq \overline{\mathbb{Q}}$ (où $\subsetneq$ signifie « est inclus sans être égal ») et $\overline{\mathbb{Q}} \not\subset \mathbb{R}$.
2. a) Soit $\alpha \in \mathbb{C}$. Démontrer que $\alpha \in \overline{\mathbb{Q}}$ si, et seulement si, il existe $p \in \mathbb{N}^*$ tel que la famille $(1, \alpha, \dots, \alpha^p)$ est liée.
   ▶ Lorsque $\alpha \in \overline{\mathbb{Q}}$, le plus petit entier $p \in \mathbb{N}^*$ tel que la famille $(1, \alpha, \alpha^2, \dots, \alpha^p)$ est liée est appelé le *degré* de α. On le note $\deg(\alpha)$ et on pose
   $$\mathbb{Q}[\alpha] = \text{Vect}\left(1, \alpha, \dots, \alpha^{\deg(\alpha)-1}\right).$$
   b) Soient $\alpha, \beta \in \overline{\mathbb{Q}}$. On pose
   $$\mathbb{Q}[\alpha, \beta] = \text{Vect}\left((\alpha^k \beta^\ell)_{k \in [\![0;\deg(\alpha)-1]\!],\, \ell \in [\![0;\deg(\beta)-1]\!]}\right).$$
   α] Démontrer que $\forall k \in \mathbb{N},\ \alpha^k \in \mathbb{Q}[\alpha]$ et en déduire que $\forall k, \ell \in \mathbb{N},\ \alpha^k \beta^\ell \in \mathbb{Q}[\alpha, \beta]$.
   β] À l'aide des familles $\left((\alpha\beta)^m\right)_{m \in \mathbb{N}}$ et $\left((\alpha+\beta)^m\right)_{m \in \mathbb{N}}$, démontrer que $\alpha\beta$ et $\alpha+\beta$ appartiennent à $\overline{\mathbb{Q}}$.
3. Démontrer que $\overline{\mathbb{Q}}$ est un sous-corps de $\mathbb{C}$.
4. Démontrer que $\overline{\mathbb{Q}}$ est dénombrable.

EXERCICE 2

Codimension

Soient K un corps commutatif et E un K-espace vectoriel (de dimension finie ou non).

1. Soit F un sous-espace vectoriel de E. On suppose que F admet un supplémentaire F_1' dans E qui est de dimension finie. Démontrer que si F_2' est un (autre) supplémentaire de F dans E, alors F_2' est de dimension finie et $\dim F_2' = \dim F_1'$.
   Indication : On pourra utiliser la projection sur F_1' dans la direction de F.

▶ On vient ainsi de démontrer que si un sous-espace vectoriel F de E admet un supplémentaire dans E de dimension finie, alors tous les supplémentaires de F dans E ont la même dimension finie. On dit alors que F est de *codimension finie* et la dimension commune des supplémentaires de F dans E est appelée la *codimension* de F. Elle est notée $\operatorname{codim} F$.

2. Dans cette question, on suppose E de dimension finie. Soit F un sous-espace vectoriel de E. Justifier que F est de codimension finie et exprimer $\operatorname{codim} F$ en fonction de $\dim E$ et $\dim F$.

3. Soient $E_0 = \mathbb{R}^{\mathbb{R}}$ et $F_0 = \{f \in E_0 : f(0) = f(1) = 0\}$. Démontrer que F_0 est de codimension finie (dans E_0) et préciser sa codimension.

4. Soit F un sous-espace vectoriel de E qui est de codimension finie. On considère un sous-espace vectoriel G de E tel que $F \subset G$.
   a) Démontrer que G est de codimension finie et que sa codimension est donnée par la formule $\operatorname{codim} G = \operatorname{codim} F - \dim(G \cap F')$ où F' désigne un supplémentaire de F dans E.
   Indication : On pourra déterminer un supplémentaire de F dans G.
   b) En déduire que $\operatorname{codim} G \leqslant \operatorname{codim} F$ et préciser le cas d'égalité.

5. Soient F_1 et F_2 deux sous-espaces vectoriels de E qui sont de codimension finie.
   On note S un supplémentaire de F_1 dans $F_1 + F_2$.
   On note T un supplémentaire de $F_1 \cap F_2$ dans F_2.
   a) Justifier que $F_1 + F_2$ est de codimension finie.
   b) Démontrer que S est de dimension finie et $\dim S = \operatorname{codim} F_1 - \operatorname{codim}(F_1 + F_2)$.
   c) On note $\pi \in \mathscr{L}(F_1 + F_2)$ la projection sur S dans la direction de F_1. À l'aide de la restriction de π à F_2 (au départ), démontrer que S et T sont isomorphes. En déduire que T est de dimension finie et $\dim T = \operatorname{codim} F_1 - \operatorname{codim}(F_1 + F_2)$.
   d) Démontrer que $F_1 \cap F_2$ est de codimension finie et établir la *coformule de Grassmann* :
   $$\operatorname{codim}(F_1 \cap F_2) = \operatorname{codim} F_1 + \operatorname{codim} F_2 - \operatorname{codim}(F_1 + F_2).$$

EXERCICE 3

Un cas particulier du théorème de Dirichlet

En arithmétique, le théorème de Dirichlet énonce que, dans toute progression arithmétique $(a+bn)_{n\geqslant 0}$ où a, b sont deux entiers premiers entre eux, il existe une infinité de nombres premiers.

L'objet de cet exercice est d'établir ce théorème lorsque $a = 1$ et $b = p$ où p désigne un nombre premier.

1. Que dire du cas où $p = 2$?
2. Soit q un nombre premier divisant $1 + p + p^2 + \cdots + p^{p-1}$. Déterminer l'ordre de p dans $U(\mathbb{Z}/q\mathbb{Z})$ et en déduire que q est congru à 1 modulo p.
3. Démontrer qu'il existe une infinité de nombres premiers congru à 1 modulo p.

EXERCICE 4

Théorème d'approximation de Weierstrass

Soit $f : [0;1] \longrightarrow \mathbb{R}$ une fonction continue. Pour tout $n \in \mathbb{N}^*$, on note B_n la n-ème *fonction polynomiale de Bernstein* associée à f, définie sur $[0;1]$ par

$$\forall p \in [0;1]\,, \qquad B_n(p) = \sum_{k=0}^{n} f\Big(\frac{k}{n}\Big)\binom{n}{k} p^k (1-p)^{n-k}.$$

L'objet de ce problème est de démontrer que la suite de fonctions polynomiales $(B_n)_{n\geqslant 1}$ converge uniformément vers f sur $[0;1]$, c'est-à-dire

$$\lim_{n\to+\infty} \sup_{p\in[0;1]} |f(p) - B_n(p)| = 0.$$

Dans cet exercice, la barre verticale | qui signifie « sachant que » est remplacée par le symbole [afin d'éviter les confusions avec les valeurs absolues.

1. Dans cette question (et seulement dans cette question), on suppose que f est la fonction exponentielle exp. Pour tout $n \in \mathbb{N}^*$, déterminer une expression simple de la fonction B_n sur $[0;1]$. Vérifier que, pour tout $p \in [0;1]$, la suite $\big(B_n(p)\big)_{n\geqslant 1}$ converge vers e^p.

2. Soit X une variable aléatoire réelle définie sur un espace probabilisé fini $(\Omega, \mathscr{T}, P)$. Soit $(A_k)_{1\leqslant k\leqslant m}$ un système complet d'événements (où $m \in \mathbb{N}^*$). Pour tout $k \in [\![1;m]\!]$, on note $E(X\,[\,A_k)$ l'espérance de X pour la probabilité conditionnelle P_{A_k} . Démontrer la formule de l'espérance totale :
$$E(X) = \sum_{k=1}^{m} P(A_k) E(X\,[\,A_k).$$

3. On fixe un entier $n \in \mathbb{N}^*$, un nombre réel $p \in [0;1]$ et un nombre réel $\varepsilon \in \mathbb{R}_+^*$.
   On note Z une variable aléatoire qui suit la loi binomiale $\mathscr{B}(n;p)$ sur un espace probabilisé fini $(\Omega, \mathscr{T}, P)$ quelconque.
   a) Démontrer que
   $$|f(p) - B_n(p)| \leqslant E\bigg(\Big|f(p) - f\Big(\frac{Z}{n}\Big)\Big|\bigg).$$
   b) α] Justifier l'existence d'un nombre réel $M \in \mathbb{R}_+$ tel que
   $$\forall x \in [0;1]\,, \qquad |f(x)| \leqslant M.$$
   β] Justifier l'existence d'un nombre réel $\delta \in \mathbb{R}_+^*$ tel que
   $$\forall x, y \in [0;1]\,, \qquad \big(|x-y| \leqslant \delta\big) \implies \Big(|f(x) - f(y)| \leqslant \frac{\varepsilon}{2}\Big).$$
   γ] À l'aide de la formule de l'espérance totale, démontrer que
   $$E\bigg(\Big|f(p) - f\Big(\frac{Z}{n}\Big)\Big|\bigg) \leqslant \frac{\varepsilon}{2} + 2M\,P\bigg(\Big|\frac{Z}{n} - p\Big| > \delta\bigg).$$
   c) Démontrer que
   $$P\bigg(\Big|\frac{Z}{n} - p\Big| > \delta\bigg) \leqslant \frac{1}{4n\delta^2}.$$
   d) Écrire la majoration de $|f(p) - B_n(p)|$ obtenue.

4. Démontrer que la suite de fonctions polynomiales $(B_n)_{n\geqslant 1}$ converge uniformément vers f sur $[0;1]$.

EXERCICE 5

Entropie

Dans cet exercice,

- on convient que $0 \ln 0 = 0$, ce qui revient à prolonger $x \longmapsto x \ln x$ par continuité en 0 ;
- toutes les variables aléatoires sont définies sur un espace probabilisé fini $(\Omega, \mathscr{T}, P)$ et à valeurs dans un même ensemble fini $\mathscr{E}$ dont le cardinal est noté n ;
- pour toute variable aléatoire X, on appelle *entropie* de X la quantité

$$H(X) = -\sum_{a \in \mathscr{E}} P(X = a) \ln P(X = a) ;$$

- on considère une variable aléatoire U telle que $\forall a \in \mathscr{E},\ P(U = a) \neq 0$;
- pour toute variable aléatoire X, on appelle *entropie relative* de X pour U la quantité

$$K_U(X) = \sum_{a \in \mathscr{E}} P(X = a) \ln \Big(\frac{P(X = a)}{P(U = a)} \Big).$$

A. Encadrement de l'entropie

1. a) Quel est le signe de $H(X)$?

   b) Démontrer que $H(X) = 0$ si, et seulement si, X suit une loi certaine.

2. a) Démontrer que $\forall x \geqslant 0,\ x \ln x \geqslant x - 1$ et en déduire que $K_U(X) \geqslant 0$. Quand y a-t-il égalité ?

   b) Dans cette question, on suppose que U suit la loi uniforme sur $\mathscr{E}$. Exprimer $K_U(X)$ en fonction de n et $H(X)$. En déduire une majoration de $H(X)$.

   c) Démontrer que $H(X) = \ln n$ si, et seulement si, X suit la loi uniforme sur $\mathscr{E}$.

B. Encadrement de l'entropie d'un couple

Dans cette partie et la suivante,

- on suppose que $\mathscr{E} = \mathscr{E}_1 \times \mathscr{E}_2$ avec $\operatorname{card} \mathscr{E}_1 = n_1$ et $\operatorname{card} \mathscr{E}_2 = n_2$ de sorte que $n = n_1 n_2$;
- on pose $U = (U_1, U_2)$ et $X = (X_1, X_2)$ de sorte que

$$H(X) = H(X_1, X_2) = -\sum_{\substack{a_1 \in \mathscr{E}_1 \\ a_2 \in \mathscr{E}_2}} P(X_1 = a_1\,,\, X_2 = a_2) \ln P(X_1 = a_1\,,\, X_2 = a_2),$$

$$K_U(X) = K_{(U_1,U_2)}(X_1, X_2) = \sum_{\substack{a_1 \in \mathscr{E}_1 \\ a_2 \in \mathscr{E}_2}} P(X_1 = a_1\,,\, X_2 = a_2) \ln \Big(\frac{P(X_1 = a_1\,,\, X_2 = a_2)}{P(U_1 = a_1\,,\, U_2 = a_2)} \Big) ;$$

- on suppose enfin que U_1 et U_2 sont indépendantes.

1. Majoration

Dans cette question, on suppose que U_1 suit la loi de X_1 et que U_2 suit la loi de X_2.

   a) À quelle condition nécessaire et suffisante le couple (X_1, X_2) a-t-il la même loi que le couple (U_1, U_2) ?

   b) Démontrer que

$$K_{(U_1,U_2)}(X_1, X_2) = H(X_1) + H(X_2) - H(X_1, X_2).$$

   c) En déduire que

$$H(X_1, X_2) \leqslant H(X_1) + H(X_2)$$

   et donner une condition nécessaire et suffisante pour qu'il y ait égalité.

- Dans la suite de ce sujet, on admettra que l'inégalité $H(X_1, X_2) \leqslant H(X_1) + H(X_2)$ et son cas d'égalité sont également valables pour des variables X_1 et X_2 qui vérifient $\exists a_1 \in \mathscr{E}_1,\ P(X_1 = a_1) = 0$ ou $\exists a_2 \in \mathscr{E}_2,\ P(X_2 = a_2) = 0$.

2. Minoration

a) Démontrer que
$$H(X_1, X_2) \geqslant H(X_1).$$

b) On suppose que $H(X_1, X_2) = H(X_1)$.
Démontrer que, pour tout $a_1 \in \mathscr{E}_1$ tel que $P(X_1 = a_1) \neq 0$, il existe un unique élément de $\mathscr{E}_2$, noté $r(a_1)$, tel que $P\big(X_1 = a_1\,,\, X_2 = r(a_1)\big) = P(X_1 = a_1)$.
Soit b un élément quelconque de $\mathscr{E}_2$. Lorsque $P(X_1 = a_1) = 0$, on pose $r(a_1) = b$. On a ainsi défini une application $r : \mathscr{E}_1 \longrightarrow \mathscr{E}_2$.
Démontrer que l'événement $\big(X_2 = r(X_1)\big)$ est quasi-certain.

c) Réciproquement, on suppose qu'il existe une application $r : \mathscr{E}_1 \longrightarrow \mathscr{E}_2$ telle que l'événement $\big(X_2 = r(X_1)\big)$ soit quasi-certain. Démontrer que $H(X_1, X_2) = H(X_1)$.

d) Justifier que
$$H(X_1, X_2) \geqslant \max\{H(X_1); H(X_2)\}$$
et préciser les cas d'égalité.

C. Entropie conditionnelle

Avec les notations de la partie précédente,

▶ on définit l'*entropie conditionnelle* de X_1 sachant X_2 par
$$H(X_2 \,|\, X_1) = -\sum_{\substack{a_1 \in \mathscr{E}_1 \\ a_2 \in \mathscr{E}_2}} P(X_1 = a_1\,,\, X_2 = a_2) \ln P(X_2 = a_2 \,|\, X_1 = a_1).$$

1. Démontrer que
$$H(X_2 \,|\, X_1) = H(X_1, X_2) - H(X_1).$$

2. Dans un livre de Claude Shannon sur la théorie de l'information, on trouve la description suivante de l'entropie conditionnelle :

« L'entropie conditionnelle mesure l'entropie restante provenant de la variable aléatoire X_2, si l'on connait parfaitement la variable aléatoire X_1. Plus précisément, $H(X_2 \,|\, X_1) = 0$ si, et seulement si, la variable aléatoire X_2 est complètement déterminée par la variable aléatoire X_1. Inversement $H(X_2 \,|\, X_1) = H(X_2)$ si, et seulement si, X_1 et X_2 sont des variables aléatoires indépendantes. »

Justifier cette affirmation à l'aide des résultats glanés jusqu'ici.

3. Anick et Bruno s'opposent au jeu suivant : Anick choisit un nombre au hasard dans $[\![1; 2016]\!]$. Dans le but de déterminer le nombre d'Anick, Bruno pose une série de q questions où q est un entier naturel fixé à l'avance. Ces questions sont impérativement de la forme : « le nombre choisi appartient-il à E » où E est un sous-ensemble de $[\![1; 2016]\!]$ pouvant varier à chaque question. Anick répond par l'affirmative si le nombre appartient à E et par la négative sinon. Au bout des q questions, Bruno donne sa réponse.
On désigne par N le nombre choisi par Anick et, pour $i \in [\![1; q]\!]$, on note $X_i = 1$ si la réponse d'Anick est positive à la i-ème question de Bruno et $X_i = 0$ sinon. Enfin, on pose
$$X = \sum_{i=1}^{q} X_i \, 2^{i-1}$$
la variable aléatoire qui code en binaire l'ensemble des réponses recueillies par Bruno.

a) Justifier, en langage courant, que $H(X \,|\, N) = 0$ et en déduire que
$$H(N \,|\, X) = \ln 2016 - H(X).$$

b) Démontrer que X est à valeurs dans $[\![0; 2^q - 1]\!]$ et en déduire une majoration de $H(X)$.

c) Bruno prétend pouvoir trouver à coup sûr le nombre d'Anick en au plus 10 questions. Qu'en pensez-vous ? En combien de questions au minimum êtes vous certain de pouvoir donner la valeur de N ?

Lycée Henri IV
MPSI 2015/2016

Correction

CORRECTION DU DS 9

(durée : 4 h 00)

EXERCICE 1

Dans cet exercice, le corps de base de tous les espaces vectoriel est $\mathbb{Q}$. Ainsi, toutes les combinaisons linéaires envisagées sont à coefficients rationnels. Soit $\alpha \in \mathbb{C}$. On dit que α est algébrique lorsqu'il existe un polynôme non nul P à coefficients rationnels tel que α est racine de P. Le sous-ensemble de $\mathbb{C}$ constitué des nombres algébriques est noté $\overline{\mathbb{Q}}$ (ici, cette notation ne désigne pas le complémentaire). L'objet de cet exercice est de démontrer que $\overline{\mathbb{Q}}$ est un sous-corps dénombrable de $\mathbb{C}$.

1. *Démontrer que $\mathbb{Q} \subsetneq \overline{\mathbb{Q}}$ et $\overline{\mathbb{Q}} \not\subset \mathbb{R}$.*

   Un nombre rationnel r est racine du polynôme $X - r$, qui est à coefficients rationnels, donc $r \in \overline{\mathbb{Q}}$. Cela démontre que $\mathbb{Q} \subset \overline{\mathbb{Q}}$.
   Par ailleurs, $\sqrt{2}$ est un nombre irrationnel algébrique puisqu'il est racine de $X^2 - 2$, qui est un polynôme à coefficients rationnels. Donc $\sqrt{2} \in \overline{\mathbb{Q}} \setminus \mathbb{Q}$, ce qui démontre que $\overline{\mathbb{Q}} \neq \mathbb{Q}$.
   En conclusion,

   $$\boxed{\mathbb{Q} \subsetneq \overline{\mathbb{Q}}.}$$

   Le nombre i n'est pas réel mais il est algébrique puisqu'il est racine de $X^2 + 1$, qui est un polynôme à coefficients rationnels. Donc $i \in \overline{\mathbb{Q}}$ et $i \notin \mathbb{R}$, ce qui démontre que

   $$\boxed{\overline{\mathbb{Q}} \not\subset \mathbb{R}.}$$

2. a) *Soit $\alpha \in \mathbb{C}$. Démontrer que $\alpha \in \overline{\mathbb{Q}}$ si, et seulement si, il existe $p \in \mathbb{N}^*$ tel que $(1, \alpha, \dots, \alpha^p)$ est liée. Lorsque $\alpha \in \overline{\mathbb{Q}}$, le plus petit entier $p \in \mathbb{N}^*$ tel que la famille $(1, \alpha, \alpha^2, \dots, \alpha^p)$ est liée est appelé le degré de α. On le note $\deg(\alpha)$ et on pose $\mathbb{Q}[\alpha] = \mathrm{Vect}\left(1, \alpha, \dots, \alpha^{\deg(\alpha)-1}\right)$.*

   On a

   $$\begin{aligned} \left(\alpha \in \overline{\mathbb{Q}}\right) &\iff \left(\exists P \in \mathbb{Q}[X] \setminus \{0\},\ P(\alpha) = 0\right) \\ &\iff \left(\exists p \in \mathbb{N}^*,\ \exists a_0, \dots, a_p \in \mathbb{Q},\ a_0 + a_1\alpha + \cdots + a_p\alpha^p = 0 \text{ et } a_p \neq 0\right) \\ &\iff \left(\text{il existe } p \in \mathbb{N}^* \text{ tel que } (1, \alpha, \alpha^2, \dots, \alpha^p) \text{ est liée}\right), \end{aligned}$$

   donc

   $$\boxed{\alpha \text{ est algébrique si, et seulement si, il existe } p \in \mathbb{N}^* \text{ tel que } (1, \alpha, \dots, \alpha^p) \text{ est liée.}}$$

   b) *Soient $\alpha, \beta \in \overline{\mathbb{Q}}$. On pose $\mathbb{Q}[\alpha, \beta] = \mathrm{Vect}\left((\alpha^k\beta^\ell)_{k \in [\![0;\deg(\alpha)-1]\!],\, \ell \in [\![0;\deg(\beta)-1]\!]}\right)$.*

   α] *Démontrer que $\forall k \in \mathbb{N},\ \alpha^k \in \mathbb{Q}[\alpha]$ et en déduire que $\forall k, \ell \in \mathbb{N},\ \alpha^k\beta^\ell \in \mathbb{Q}[\alpha, \beta]$.*

   Pour démontrer que $\forall k \in \mathbb{N},\ \alpha^k \in \mathbb{Q}[\alpha]$, on propose deux preuves. On pose $d = \deg(\alpha)$.

   ▶ <u>Par récurrence forte</u>

   Par définition de $\mathbb{Q}[\alpha]$, on a $1, \alpha, \dots, \alpha^{d-1} \in \mathbb{Q}[\alpha]$. Il reste donc à démontrer que l'assertion $\mathscr{P}(k) : \alpha^k \in \mathbb{Q}[\alpha]$ est vraie pour tout $k \geqslant d$.

Initialisation : Comme $(1, \alpha, \alpha^2, \dots, \alpha^d)$ est liée, il existe des nombres rationnels $a_0, \dots, a_d$ tels que $a_0 + a_1\alpha + \cdots + a_d\alpha^d = 0$. De plus, la minimalité de d (parmi les entiers $p \in \mathbb{N}^*$ tels que $(1, \alpha, \alpha^2, \dots, \alpha^p)$ est liée) nous dit que $a_d \neq 0$. On a alors

$$\alpha^d = -\frac{a_0}{a_d} - \frac{a_1}{a_d}\alpha - \cdots - \frac{a_{d-1}}{a_d}\alpha^{d-1} \qquad (*)$$

ce qui démontre que $\alpha^d \in \mathbb{Q}[\alpha]$.

Hérédité : Fixons $k \geqslant d$ tel que $\mathscr{P}(0), \mathscr{P}(1), \dots, \mathscr{P}(k)$ sont vraies et démontrons $\mathscr{P}(k+1)$. En multipliant la relation $(*)$ par α^{k+1-d}, on obtient

$$\alpha^{k+1} = -\frac{a_0}{a_d}\alpha^{k+1-d} - \frac{a_1}{a_d}\alpha^{k+2-d} - \cdots - \frac{a_{d-1}}{a_d}\alpha^k.$$

Or, d'après les hypothèses de récurrence, on sait que $\alpha^{k+1-d}, \alpha^{k+2-d}, \dots, \alpha^k$ appartiennent à $\mathbb{Q}[\alpha]$. Comme c'est un espace vectoriel, on en déduit que $\alpha^{k+1} \in \mathbb{Q}[\alpha]$. Cela démontre que $\mathscr{P}(k+1)$ est vraie.

Conclusion : D'après le principe de récurrence, $\mathscr{P}(k)$ est vraie pour tout $k \in \mathbb{N}$.

▶ Par division euclidienne

Comme $(1, \alpha, \alpha^2, \dots, \alpha^d)$ est liée, il existe $a_0, \dots, a_d \in \mathbb{Q}$ tels que $a_0 + a_1\alpha + \cdots + a_d\alpha^d = 0$. De plus, la minimalité de d (parmi les entiers $p \in \mathbb{N}^*$ tels que $(1, \alpha, \alpha^2, \dots, \alpha^p)$ est liée) nous dit que $a_d \neq 0$. Ainsi, $P = a_0 + a_1X + \cdots + a_dX^d$ est un polynôme non nul dont α est une racine.

Soit $k \in \mathbb{N}$. Effectuons dans $\mathbb{Q}[X]$ la division euclidienne de X^k par P. Il existe alors $Q, R \in \mathbb{Q}[X]$ tels que $X^k = PQ + R$ avec $\deg(R) < d$. En évaluant cette égalité en α, on obtient $\alpha^k = R(\alpha)$ puisque $P(\alpha) = 0$. Comme $\deg(R) < d$, cela signifie que α^k est une combinaison linéaire, à coefficients dans $\mathbb{Q}$, de $1, \alpha, \dots, \alpha^{d-1}$, autrement dit que $\alpha^k \in \mathbb{Q}[\alpha]$. On a donc démontré que $\forall k \in \mathbb{N},\ \alpha^k \in \mathbb{Q}[\alpha]$.

En définitive, on a

$$\boxed{\forall k \in \mathbb{N}, \qquad \alpha^k \in \mathbb{Q}[\alpha].}$$

On démontrerait de même que

$$\boxed{\forall \ell \in \mathbb{N}, \qquad \beta^\ell \in \mathbb{Q}[\beta].}$$

Soient $k, \ell \in \mathbb{N}$. On note p le degré de α et q celui de β. Comme $\alpha^k \in \mathbb{Q}[\alpha]$ et $\beta^\ell \in \mathbb{Q}[\beta]$, il existe $a_0, \dots, a_{p-1}, b_0, \dots, b_{q-1} \in \mathbb{Q}$ tels que l'on ait $\alpha^k = a_0 + a_1\alpha + \cdots + a_{p-1}\alpha^{p-1}$ et $\beta^\ell = a_0 + a_1\alpha + \cdots + a_{q-1}\alpha^{q-1}$. Cela donne

$$\alpha^k\beta^\ell = \sum_{i=0}^{p-1} a_i\alpha^i \sum_{j=0}^{p-1} b_j\beta^j = \sum_{\substack{0 \leqslant i \leqslant p-1 \\ 0 \leqslant j \leqslant q-1}} a_ib_j\alpha^i\beta^j,$$

donc

$$\alpha^k\beta^\ell \in \mathbb{Q}[\alpha, \beta].$$

En conclusion,

$$\boxed{\forall k, \ell \in \mathbb{N}, \qquad \alpha^k\beta^\ell \in \mathbb{Q}[\alpha, \beta].}$$

β] À l'aide des familles $\left((\alpha\beta)^m\right)_{m\in\mathbb{N}}$ et $\left((\alpha+\beta)^m\right)_{m\in\mathbb{N}}$, démontrer que $\alpha\beta \in \overline{\mathbb{Q}}$ et $\alpha+\beta \in \overline{\mathbb{Q}}$.

En faisant $k = \ell = m$ dans la propriété $\forall k, \ell \in \mathbb{N},\ \alpha^k\beta^\ell \in \mathbb{Q}[\alpha, \beta]$ (établie à la question précédente), on voit que $\forall m \in \mathbb{N},\ (\alpha\beta)^m \in \mathbb{Q}[\alpha, \beta]$. Ainsi, $\left((\alpha\beta)^m\right)_{m\in\mathbb{N}}$ est une famille infinie du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}[\alpha, \beta]$. Or celui-ci est de dimension finie (puisqu'il est engendré par une famille finie), donc la famille $\left((\alpha\beta)^m\right)_{m\in\mathbb{N}}$ est nécessairement liée. D'après la question 3, cela signifie que $\alpha\beta$ est algébrique.

Pour tout $m \in \mathbb{N}$, la fomule du binôme nous dit que $(\alpha + \beta)^m = \sum_{0 \leqslant k \leqslant m} \binom{m}{k}\alpha^k\beta^{m-k}$. Or, pour tout $m \in \mathbb{N}$ et tout $k \in [\![0; m]\!]$, on a $\alpha^k\beta^{m-k} \in \mathbb{Q}[\alpha, \beta]$, donc $(\alpha+\beta)^m \in \mathbb{Q}[\alpha, \beta]$. Ainsi, $\left((\alpha + \beta)^m\right)_{m\in\mathbb{N}}$ est une famille infinie du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}[\alpha, \beta]$. Or celui-ci est de dimension finie, donc la famille $\left((\alpha + \beta)^m\right)_{m\in\mathbb{N}}$ est nécessairement liée. D'après la question 3, cela signifie que $\alpha + \beta$ est algébrique.

En conclusion,

$$\boxed{\text{si } \alpha \text{ et } \beta \text{ sont algébriques, alors } \alpha\beta \text{ et } \alpha + \beta \text{ sont algébriques.}}$$

3. *Démontrer que $\overline{\mathbb{Q}}$ est un sous-corps de $\mathbb{C}$.*

On a $\overline{\mathbb{Q}} \subset \mathbb{C}$.

On sait que $1 \in \overline{\mathbb{Q}}$.

On sait que si $\alpha, \beta \in \overline{\mathbb{Q}}$, alors $\alpha + \beta \in \overline{\mathbb{Q}}$.

Soit $\alpha \in \overline{\mathbb{Q}}$. Il existe $P \in \mathbb{Q}[X] \setminus \{0\}$ tel que $P(\alpha) = 0$. Notons $P = a_0 + a_1 X + \cdots + a_n X^n$, avec $n \in \mathbb{N}^*$, $a_0, \ldots, a_n \in \mathbb{Q}$ et $a_n \neq 0$, de sorte que $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$. On a alors $a_0 - a_1(-\alpha) + \cdots + (-1)^n a_n(-\alpha)^n = 0$. Ainsi, $R = a_0 - a_1 X + \cdots + (-1)^n a_n X^n$ est un polynôme à coefficients rationnels, non nul qui admet $-\alpha$ comme racine, ce qui signifie que $-\alpha$ est algébrique. On a ainsi démontré que $\forall \alpha \in \overline{\mathbb{Q}},\ -\alpha \in \overline{\mathbb{Q}}$.

On sait que si $\alpha, \beta \in \overline{\mathbb{Q}}$, alors $\alpha\beta \in \overline{\mathbb{Q}}$. Notons que cette propriété donne à nouveau le fait que $-\alpha = -1 \times \alpha \in \overline{\mathbb{Q}}$.

Soit $\alpha \in \overline{\mathbb{Q}}$ tel que $\alpha \neq 0$. Il existe $P \in \mathbb{Q}[X]\setminus\{0\}$ tel que $P(\alpha) = 0$. Notons $P = a_0 + a_1 X + \cdots + a_n X^n$, avec $n \in \mathbb{N}^*$, $a_0, \ldots, a_n \in \mathbb{Q}$ et $a_n \neq 0$, de sorte que $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$. En divisant cette égalité par α^n (ce qui est licite puisque $\alpha^n \neq 0$), on obtient $a_0(\alpha^{-1})^n + a_1(\alpha^{-1})^{n-1} + \cdots + a_n = 0$. Ainsi, $R = a_0 X^n + a_1 X^{n-1} + \cdots + a_n$ est un polynôme à coefficients rationnels, non nul qui admet α^{-1} comme racine, ce qui signifie que α^{-1} est algébrique. On a ainsi démontré que $\forall \alpha \in \overline{\mathbb{Q}}\setminus\{0\},\ \alpha^{-1} \in \overline{\mathbb{Q}}$.

On en conclut que

$\boxed{\overline{\mathbb{Q}} \text{ est un sous-corps de } \mathbb{C}.}$

4. *Démontrer que $\overline{\mathbb{Q}}$ est dénombrable.*

Commençons par démontrer que l'ensemble $\mathbb{Q}[X]$ est dénombrable.
Soit $d \in \mathbb{N}$. À chaque polynôme de degré $\leqslant d$, associons la suite $(a_0, \ldots, a_d)$ de ses coefficients (en fait, cette suite est le polynôme lui-même). On obtient ainsi une injection de $\mathbb{Q}_d[X]$ (l'ensemble des polynômes à coefficients rationnels de degré $\leqslant d$) dans $\mathbb{Q}^{d+1}$, qui est dénombrable (comme produit d'ensembles dénombrables). Donc $\mathbb{Q}_d[X]$ est dénombrable.
Comme $\mathbb{Q}[X]$ est la réunion des $\mathbb{Q}_d[X]$ pour d parcourant $\mathbb{N}$, l'ensemble $\mathbb{Q}[X]$ est dénombrable en tant que réunion dénombrable d'ensembles dénombrables.

On sait que l'ensemble des nombres algébriques est la réunion des ensembles de racines des polynômes de $\mathbb{Q}[X]\setminus\{0\}$. Comme l'ensemble des racines d'un polynôme non nul est fini, l'ensemble des nombres algébriques est une réunion dénombrable d'ensembles finis, donc

$\boxed{\overline{\mathbb{Q}} \text{ est dénombrable.}}$

Remarque culturelle :

Nous venons de démontrer que l'ensemble $\overline{\mathbb{Q}}$ des nombres algébriques est un sur-corps de $\mathbb{Q}$ et un sous-corps de $\mathbb{C}$. On peut rajouter que $\overline{\mathbb{Q}}$ est algébriquement clos, c'est-à-dire qu'il contient toutes les racines des équations polynomiales à coefficients dans $\overline{\mathbb{Q}}$. C'est même le plus petit sous-corps de $\mathbb{C}$ contenant $\mathbb{Q}$ qui a cette propriété : on dit que $\overline{\mathbb{Q}}$ est la cloture algébrique de $\mathbb{Q}$.

Comme $\overline{\mathbb{Q}}$ est dénombrable alors que $\mathbb{C}$ ne l'est pas, il existe des nombres complexes non algébriques (c'est même le cas de presque tous les nombres complexes). On les appelle les nombres transcendants.

S'il est aisé (comme nous venons de le faire) de justifier l'existence de nombres transcendants, il est en revanche nettement plus difficile de démontrer qu'un nombre donné est effectivement transcendant.

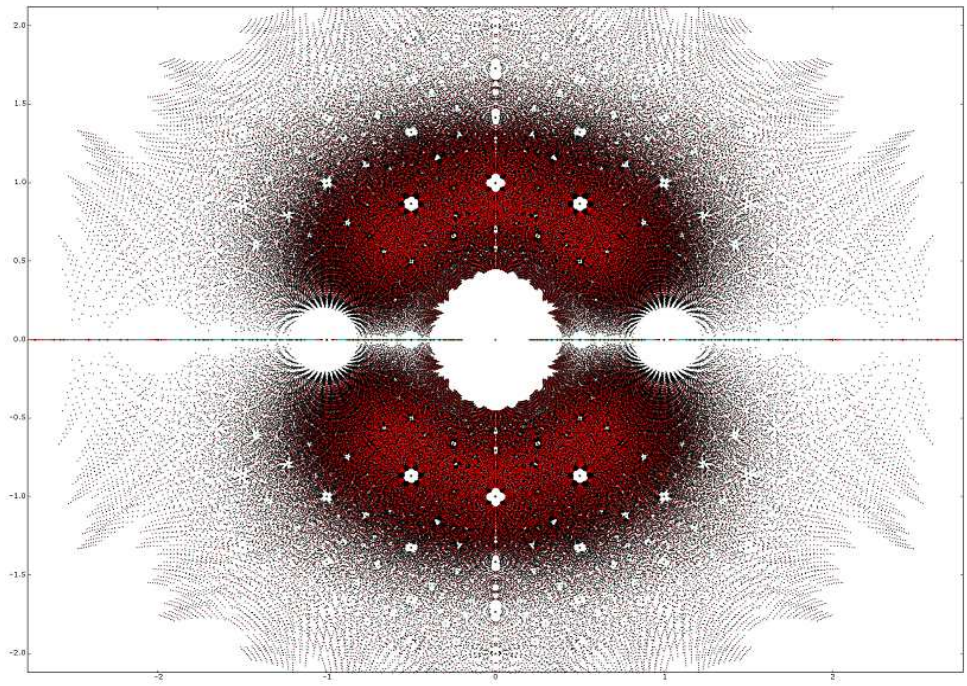
Les exemples les plus connus de transcendances sont celles de e (obtenue en 1873 par Hermite) et de π (obtenue en 1882 par von Lindemann). La transcendance de π a permis de justifier l'impossibilité de résoudre plusieurs problèmes anciens de construction géométrique avec le compas et la règle, incluant le plus célèbre d'entre eux : la quadrature du cercle.

En revanche, à ce jour, on ne sait pas démontrer que la constante d'Euler γ est trancendante (et ce n'est qu'un exemple, parmi beaucoup d'autres, de nombres dont la transcendance est conjecturée mais non démontrée).

Tous les nombres qui peuvent être obtenus à partir des entiers en utilisant un nombre fini d'additions, de soustractions, de multiplications, de divisions et d'extractions de racines n-ièmes sont algébriques. La réciproque est fausse : il existe des nombres algébriques qui ne peuvent pas être obtenus de cette manière (c'est le théorème d'Abel). D'après la théorie de Galois, tous ces nombres sont de degré supérieur ou égal à 5. C'est ce résultat qui justifie qu'il n'existe pas de méthode générale permettant de résoudre par radicaux les équations polynomiales de degré supérieur ou égal à 5.

Voici une représentation (partielle) de $\overline{\mathbb{Q}}$ dans le plan complexe. Elle rassemble les racines de tous les polynômes de degré $\leqslant 5$ à coefficients entiers compris entre -4 et $+4$. Les valeurs approchées des racines

sont obtenues par la méthode de Durand–Kerner (un homonyme !). Les nombres algébriques de degré 2 sont en gris, ceux de degré 3 sont en bleu, ceux de degré 4 sont en rouge et ceux de degré 5 sont en noir.



Mais ne vous laisser pas berner : les zones blanches ne sont pas exemptes de nombres algébriques. En effet, $\overline{\mathbb{Q}}$ est dense dans $\mathbb{C}$ (y réfléchir), ce qui signifie que les nombres algébriques sont présents dans tout ouvert de $\mathbb{C}$. En fait, les zones blanches correspondent simplement à des parties du plan complexes où les nombres algébriques ont un degré supérieur ou égal à 6. Pour plus de précisions et d'autres très jolies images, on pourra consulter le site

`http://math.ucr.edu/home/baez/roots/`

EXERCICE 2

Soient K un corps commutatif et E un K-espace vectoriel (de dimension finie ou non).

1. *Soit F un sous-espace vectoriel de E. On suppose que F admet un supplémentaire F_1' dans E qui est de dimension finie. Démontrer que si F_2' est un (autre) supplémentaire de F dans E, alors F_2' est de dimension finie et $\dim F_2' = \dim F_1'$. On aura ainsi démontré que si un sous-espace vectoriel F de E admet un supplémentaire dans E de dimension finie, alors tous les supplémentaires de F dans E ont la même dimension finie. On dit alors que F est de codimension finie et la dimension commune des supplémentaires de F dans E est appelée la codimension de F. Elle est notée $\operatorname{codim} F$.*

   Soit p la projection sur F_1' dans la direction de F. Le théorème géométrique du rang nous dit que p induit un isomorphisme entre tout supplémentaire de $\operatorname{Ker} p$ dans E et $\operatorname{Im} p$. Or on sait que $\operatorname{Ker} p = F$, que F_2' est un supplémentaire de F dans E et que $\operatorname{Im} p = F_1'$. Par conséquent, p induit un isomorphisme entre F_2' et F_1'. Dès lors, comme F_1' est de dimension finie, un résultat du cours nous dit que

   $$\boxed{F_2' \text{ est de dimension finie et } \dim F_2' = \dim F_1'.}$$

2. *Dans cette question, on suppose que E est de dimension finie. Soit F un sous-espace vectoriel de E. Justifier que F est de codimension finie dans E et exprimer $\operatorname{codim} F$ en fonction de $\dim E$ et $\dim F$.*

   Tout d'abord, on est certain que F est de codimension finie puisque tout supplémentaire de F dans E est de dimension finie comme tout sous-espace de E (qui est de dimension finie). De plus, si F' désigne l'un des supplémentaires de F dans E, on a $F \oplus F' = E$, ce qui donne, en passant aux dimensions, l'égalité $\dim F + \dim F' = \dim E$. On a donc $\operatorname{codim} F = \dim E - \dim F$. Pour résumer, on a démontré que

   $$\boxed{\begin{array}{l}\text{si } E \text{ est de dimension finie, alors tout sous-espace } F \text{ de } E\\ \text{est de codimension finie avec } \operatorname{codim} F = \dim E - \dim F.\end{array}}$$

3. *Soient $E_0 = \mathbb{R}^{\mathbb{R}}$ et $F_0 = \{f \in E_0 : f(0) = f(1) = 0\}$. Démontrer que F_0 est de codimension finie dans E_0 et préciser sa codimension.*

   Commençons par déterminer un supplémentaire de F_0 dans E_0. Procédons par analyse/synthèse.

   Analyse :
   Supposons connu un supplémentaire F_0' de F_0 dans E_0.
   Soit $u \in E_0$. Comme $E_0 = F_0 \oplus F_0'$, il existe $f \in F_0$ et $g \in F_0'$ telles que $u = f + g$.
   En évaluant en 0 et 1 cette égalité, on a $g(0) = u(0)$ et $g(1) = u(1)$. Ce sont d'ailleurs les seules conditions qui portent sur g ! On peut donc prendre pour g une fonction affine qui vaut $u(0)$ en 0 et $u(1)$ en 1.
   De là à penser que l'on peut prendre pour F_0' le sous-espace des fonctions affines, il n'y a qu'un pas...

   Synthèse :
   Notons F_0' le sous-espace de E_0 constitué des fonctions affines.
   Si u appartient à $F_0 \cap F_0'$, alors u est une fonction affine nulle en 0 et 1, donc c'est la fonction nulle.
   On a donc $F_0 \cap F_0' = \widetilde{\{0\}}$, ce qui signifie que F_0 et F_0' sont en somme directe.
   Soit $u \in E_0$. Notons g la fonction affine telle que $g(0) = u(0)$ et $g(1) = u(1)$. Dès lors, la fonction $f = u - g$ s'annule en 0 et 1, ce qui démontre que $f \in F_0$. On a donc $u = f + g$ avec $f \in F_0$ et $g \in F_0'$. Cela démontre que $E_0 = F_0 + F_0'$.
   En conclusion, on a $E_0 = F_0 \oplus F_0'$, c'est-à-dire que

   $$\boxed{\text{le sous-espace } F_0' \text{ des fonctions affines est un supplémentaire de } F_0 \text{ dans } E_0.}$$

   Le sous-espace F_0' s'identifie à $\mathbb{R}_1[X]$ (un résultat du cours dit que, sur un corps infini, on peut identifier un polynôme et sa fonction polynomiale associée). Par conséquent, F_0' est de dimension 2. On en déduit que

   $$\boxed{F_0 \text{ est de codimension 2.}}$$

4. *Soit F un sous-espace vectoriel de E qui est de codimension finie. On considère un sous-espace vectoriel G de E tel que $F \subset G$.*

   a) *Démontrer que G est de codimension finie dans E et que sa codimension est donnée par la formule $\operatorname{codim} G = \operatorname{codim} F - \dim(G \cap F')$ où F' désigne un supplémentaire de F dans E.*

   Démontrons que $G = F \oplus (G \cap F')$.

   - $\subset$ On sait que $F \subset G$ et il est clair que $G \cap F' \subset G$. Par conséquent, on a $F + (G \cap F') \subset G$.
   - $\supset$ Soit $x \in G$. Comme $F \oplus F' = E$, il existe $y \in F$ et $y' \in F'$ tels que $x = y + y'$. Comme $F \subset G$, on a $y \in G$. Il s'ensuit que $y' = x - y$ est un élément de G et donc que $y' \in G \cap F'$. On a donc $x = y + y'$ avec $y \in F$ et $y' \in G \cap F'$, ce qui démontre que $x \in F + (G \cap F')$. Par conséquent, on a $F + (G \cap F') \supset G$.
   - $\oplus$ Reste à démontrer le caractère direct de la somme. On sait que $F \cap F' = \{0_E\}$ puisque F et F' sont en somme directe. A fortiori, on a $F \cap F' \cap G = \{0_E\}$. Donc F et $G \cap F'$ sont en somme directe.

   On a ainsi démontré que

   $$\boxed{G = F \oplus (G \cap F').}$$

   Notons H un supplémentaire de G dans E. On a alors

   $$E = G \oplus H = \big(F \oplus (G \cap F')\big) \oplus H = F \oplus \big((G \cap F') \oplus H\big),$$

   où la dernière égalité découle de la propriété d'associativité des sommes directes (résultat que nous avons vu en exercice). On constate donc que $(G \cap F') \oplus H$ est un supplémentaire de F dans E. Comme F est de codimension finie, on en déduit que $(G \cap F') \oplus H$ est un sous-espace de dimension finie et que

   $$\dim\big((G \cap F') \oplus H\big) = \operatorname{codim} F.$$

   Or H est un sous-espace de $(G \cap F') \oplus H$, donc H est de dimension finie, ce qui signifie que G est de codimension finie dans E. Par ailleurs, en utilisant la formule donnant la dimension d'une somme directe, il vient

   $$\dim(G \cap F') + \dim H = \operatorname{codim} F.$$

   Comme $\dim H = \operatorname{codim} G$, on en conclut que

   $$\boxed{G \text{ est de codimension finie et } \operatorname{codim} G = \operatorname{codim} F - \dim(G \cap F')}$$

   b) *En déduire que $\operatorname{codim} G \leqslant \operatorname{codim} F$ et préciser le cas d'égalité.*

   La formule $\operatorname{codim} G = \operatorname{codim} F - \dim(G \cap F')$ associée au fait évident que $\dim(G \cap F') \geqslant 0$ nous dit que

   $$\boxed{\operatorname{codim} G \leqslant \operatorname{codim} F.}$$

   Étudions ensuite le cas d'égalité, c'est-à-dire la situation où $\operatorname{codim} G = \operatorname{codim} F$. On conjecture que cela ne peut se produire que dans le cas où $G = F$.

   Notons tout d'abord que la condition est suffisante : si $G = F$, on a bien sûr $\operatorname{codim} G = \operatorname{codim} F$.

   Supposons réciproquement que $\operatorname{codim} G = \operatorname{codim} F$. Comme $\operatorname{codim} G = \operatorname{codim} F - \dim(G \cap F')$, on a $\dim(G \cap F') = 0$, c'est-à-dire $G \cap F' = \{0_E\}$. Comme $G = F \oplus (G \cap F')$, on en déduit que $G = F \oplus \{0_E\} = F$.

   En conclusion,

   $$\boxed{\text{lorsque } F \subset G, \text{ on a } \operatorname{codim} G = \operatorname{codim} F \text{ si, et seulement si, } G = F.}$$

5. *Soient F_1 et F_2 deux sous-espaces vectoriels de E qui sont de codimension finie. On note S un supplémentaire de F_1 dans $F_1 + F_2$ et T un supplémentaire de $F_1 \cap F_2$ dans F_2.*

   a) *Justifier que $F_1 + F_2$ est de codimension finie.*

   On a $F_1 \subset F_1 + F_2$ avec F_1 qui est de codimension finie donc, d'après la question 4. a), on peut affirmer que

   $$\boxed{F_1 + F_2 \text{ est de codimension finie.}}$$

b) *Démontrer que S est de dimension finie et* $\dim S = \operatorname{codim} F_1 - \operatorname{codim}(F_1 + F_2)$.

On sait que $F_1 \oplus S = F_1 + F_2$.
Introduisons U un supplémentaire de $F_1 + F_2$ dans E, de sorte que $(F_1 + F_2) \oplus U = E$.
En combinant ces égalités, on obtient $(F_1 \oplus S) \oplus U = E$, c'est-à-dire $F_1 \oplus (S \oplus U) = E$ (d'après l'associativité des sommes directes). Ainsi $S \oplus U$ est un supplémentaire de F_1 dans E.
Or F_1 est de codimension finie, donc $S \oplus U$ est de dimension finie et $\dim(S \oplus U) = \operatorname{codim}(F_1)$.
Comme $S \subset S \oplus U$, on en déduit que S est de dimension finie. Comme $F_1 + F_2$ est de codimension finie, on sait que U est de dimension finie avec $\dim U = \operatorname{codim}(F_1 + F_2)$. On en déduit que $\dim(S \oplus U) = \dim S + \dim U = \dim S + \operatorname{codim}(F_1 + F_2)$.
En définitive, on a $\operatorname{codim}(F_1) = \dim S + \operatorname{codim}(F_1 + F_2)$.
En conclusion,

$$\boxed{S \text{ est de dimension finie et } \dim S = \operatorname{codim} F_1 - \operatorname{codim}(F_1 + F_2).}$$

c) *On note $\pi \in \mathscr{L}(F_1 + F_2)$ la projection sur S dans la direction de F_1. À l'aide de la restriction de π à F_2 (au départ), démontrer que S et T sont isomorphes. En déduire que T est de dimension finie et* $\dim T = \operatorname{codim} F_1 - \operatorname{codim}(F_1 + F_2)$.

Notons $\widehat{\pi}$ la restriction de π à F_2 (au départ) et recherchons $\operatorname{Ker}\widehat{\pi}$ et $\operatorname{Im}\widehat{\pi}$.

On a $\operatorname{Ker}\widehat{\pi} = \{x \in F_2 : \pi(x) = 0_E\} = F_2 \cap \operatorname{Ker}\pi = F_2 \cap F_1$.

Démontrons que $\operatorname{Im}\widehat{\pi} = S$. Comme $\operatorname{Im}\pi = S$, on a $\operatorname{Im}\widehat{\pi} \subset S$. Soit $y \in S$. Comme $\operatorname{Im}\pi = S$, il existe $x \in F_1 + F_2$ tel que $y = \pi(x)$. Il existe $a_1 \in F_1$ et $a_2 \in F_2$ tels que $x = a_1 + a_2$. Cela donne $y = \pi(a_1) + \pi(a_2) = \pi(a_2)$ car $a_1 \in F_1 = \operatorname{Ker}\pi$. Comme $a_2 \in F_2$, on en déduit que $y = \widehat{\pi}(a_2)$, ce qui implique que $y \in \operatorname{Im}\widehat{\pi}$. On a donc $\operatorname{Im}\widehat{\pi} \supset S$ et, par suite, $\operatorname{Im}\widehat{\pi} = S$.

Le théorème géométrique du rang nous dit alors que $\widehat{\pi}$ induit un isomorphisme entre tout supplémentaire de $\operatorname{Ker}\widehat{\pi} = F_1 \cap F_2$ dans F_2 et $\operatorname{Im}\widehat{\pi} = S$. Comme T est précisément un supplémentaire de $F_1 \cap F_2$ dans F_2, on en conclut que

$$\boxed{S \text{ et } T \text{ sont isomorphes.}}$$

Comme S est de dimension finie, notre cours nous dit alors que T est de dimension finie et $\dim T = \dim S$. Autrement dit,

$$\boxed{T \text{ est de dimension finie et } \dim T = \operatorname{codim} F_1 - \operatorname{codim}(F_1 + F_2).}$$

d) *Démontrer que le sous-espace $F_1 \cap F_2$ est de codimension finie et établir la coformule de Grassmann :* $\operatorname{codim}(F_1 \cap F_2) = \operatorname{codim} F_1 + \operatorname{codim} F_2 - \operatorname{codim}(F_1 + F_2)$.

On sait que $F_2 = (F_1 \cap F_2) \oplus T$.
Introduisons un supplémentaire F_2' de F_2 dans E, de sorte que $F_2 \oplus F_2' = E$.
En combinant ces égalités, il vient $\big((F_1 \cap F_2) \oplus T\big) \oplus F_2' = E$, c'est-à-dire $(F_1 \cap F_2) \oplus \big(T \oplus F_2'\big) = E$ où l'on a (à nouveau) utilisé la propriété d'associativité des sommes directes. Ainsi, $T \oplus F_2'$ est un supplémentaire de $F_1 \cap F_2$ dans E.
Or T est de dimension finie (d'après la question précédente) et F_2' aussi (puisque F_2 est de codimension finie), donc $T \oplus F_2'$ est de dimension finie avec

$$\dim(T \oplus F_2') = \dim T + \dim F_2' = \operatorname{codim} F_1 - \operatorname{codim}(F_1 + F_2) + \operatorname{codim} F_2.$$

On en déduit que

$$\boxed{F_1 \cap F_2 \text{ est de codimension finie et } \operatorname{codim}(F_1 \cap F_2) = \operatorname{codim} F_1 + \operatorname{codim} F_2 - \operatorname{codim}(F_1 + F_2).}$$

EXERCICE 3

En arithmétique, le théorème de Dirichlet énonce que, dans toute progression arithmétique $(a+bn)_{n\geqslant 0}$ où a, b sont deux entiers naturels premiers entre eux, il existe une infinité de nombres premiers. L'objectif de cet exercice est d'établir ce théorème lorsque $a = 1$ et $b = p$ où p désigne un nombre premier.

1. *Que dire du cas où $p = 2$?*

   Le cas $p = 2$ revient à dire qu'il existe une infinité de nombres premiers impairs. Cet énoncé est donc équivalent au théorème d'Euclide qui énonce l'existence d'une infinité de nombres premiers (et donc aussi de nombres premiers impairs puisqu'il n'existe qu'un seul nombre premier pair : 2). Par conséquent,

   $$\boxed{\text{le cas } p = 2 \text{ est connu.}}$$

2. *Soit q un nombre premier divisant $1 + p + p^2 + \cdots + p^{p-1}$. Déterminer l'ordre de p dans $U(Z/qZ)$ et en déduire que q est congru à 1 modulo p.*

   On a

   $$1 + p + p^2 + \cdots + p^{p-1} \equiv 0 \ [q]$$

   En multipliant par $p - 1$, la formule de Bernoulli nous dit que

   $$p^p - 1 \equiv 0 \ [q].$$

   Autrement dit, on a

   $$p^p \equiv 1 \ [q],$$

   ce qui signifie que l'ordre de p dans $U(\mathbb{Z}/q\mathbb{Z})$ est un diviseur de p. Comme p est premier, cet ordre vaut 1 ou p. Si l'on suppose que l'ordre vaut 1, on a $p \equiv 1 \ [q]$. En reportant dans l'égalité $1 + p + p^2 + \cdots + p^{p-1} \equiv 0 \ [q]$, on obtient $p \equiv 0 \ [q]$. C'est absurde puisque p ne peut être égal à la fois à 0 et 1 modulo q. En conclusion,

   $$\boxed{p \text{ est d'ordre } p \text{ dans } U(\mathbb{Z}/q\mathbb{Z}).}$$

   Dès lors, l'ordre de p dans $U(\mathbb{Z}/q\mathbb{Z})$ divisant nécessairement l'ordre du groupe $U(\mathbb{Z}/q\mathbb{Z})$, on a $p \mid q-1$ puisque $U(\mathbb{Z}/q\mathbb{Z})$ est d'ordre $q-1$ (car $\mathbb{Z}/q\mathbb{Z}$ est un corps, du fait que q est premier). Par conséquent, on a bien

   $$\boxed{q \equiv 1 \ [p].}$$

3. *Démontrer qu'il existe une infinité de nombres premiers congru à 1 modulo p.*

   Notons q_0 le nombre premier q déterminé à la question précédente. Considérons alors q_1 un nombre premier divisant $1+q_0p+(q_0p)^2+\cdots+(q_0p)^{p-1}$. On notera que q_1 est nécessairement différent de q_0. En multipliant l'égalité $1+q_0p+(q_0p)^2+\cdots+(q_0p)^{p-1} \equiv 0 \ [q_1]$ par q_0p-1, on obtient $(q_0p)^p \equiv 1 \ [q_1]$ ce qui signifie que l'ordre de q_0p dans $U(\mathbb{Z}/q_1\mathbb{Z})$ vaut 1 ou p. Si l'on suppose que l'ordre vaut 1, on a $q_0p \equiv 1 \ [q_1]$. En reportant dans $1 + q_0p + (q_0p)^2 + \cdots + (q_0p)^{p-1} \equiv 0 \ [q_1]$, on obtient $p \equiv 0 \ [q_1]$ puis $q_0p \equiv 0 \ [q_1]$ après multiplication par q_0. C'est absurde puisque q_0p ne peut être égal à la fois à 0 et 1 modulo q_1. Par conséquent, q_0p est d'ordre p dans $U(\mathbb{Z}/q_1\mathbb{Z})$, ce qui implique que $p \mid q_1 - 1$ ou encore $q_1 \equiv 1 \ [p]$.

   En introduisant un nombre premier q_2 divisant $1+q_1q_0p+(q_1q_0p)^2+\cdots+(q_1q_0p)^{p-1}$ et en procédant *mutatis mutandis*, on détermine un troisième nombre premier tel que $q_2 \equiv 1 \ [p]$.

   Etc.

   En conclusion,

   $$\boxed{\text{il existe une infinité de nombres premiers congru à 1 modulo } p.}$$

EXERCICE 4

Soit $f : [0;1] \to \mathbb{R}$ une fonction continue. Pour tout $n \in \mathbb{N}^*$, on note B_n la n-ème fonction polynomiale de Bernstein associée à f, définie sur $[0;1]$ par $\forall p \in [0;1]\,,\ B_n(p) = \sum_{k=0}^{n} f(k/n)\binom{n}{k}p^k(1-p)^{n-k}$. L'objet de ce problème est de démontrer que la suite de fonctions polynomiales $(B_n)_{n\geqslant 1}$ converge uniformément vers f sur $[0;1]$, c'est-à-dire $\lim\limits_{n\to+\infty} \sup\{|f(p) - B_n(p)| : p \in [0;1]\} = 0$.

1. *Dans cette question (et seulement dans cette question), on suppose que f est la fonction exponentielle* exp. *Pour tout $n \in \mathbb{N}^*$, déterminer une expression simple de la fonction B_n sur $[0;1]$. Vérifier que, pour tout $p \in [0;1]$, la suite $\big(B_n(p)\big)_{n\geqslant 1}$ converge vers e^p.*

   Pour tout $n \in \mathbb{N}^*$ et tout $p \in [0;1]$, on a

$$\begin{aligned} B_n(p) &= \sum_{k=0}^{n} \mathrm{e}^{k/n}\binom{n}{k}p^k(1-p)^{n-k} \\ &= \sum_{k=0}^{n}\binom{n}{k}(\mathrm{e}^{1/n}\,p)^k(1-p)^{n-k} \\ &= \big(\mathrm{e}^{1/n}\,p + 1 - p\big)^n \qquad \text{binôme,} \end{aligned}$$

   donc

$$\boxed{\forall n \in \mathbb{N}^*,\qquad B_n \left\{ \begin{array}{ccc} [0;1] & \longrightarrow & \mathbb{R} \\ p & \longmapsto & \big(1 + p(\mathrm{e}^{1/n} - 1)\big)^n \end{array} \right.}$$

   Pour tout $p \in [0;1]$, on a

$$\begin{aligned} B_n(p) &= \exp\big\{n \ln\big(1 + p(\mathrm{e}^{1/n} - 1)\big)\big\} \\ &= \exp\big\{n \ln\big(1 + p/n + \mathscr{O}_{n\to+\infty}(1/n)\big)\big\} \\ &= \exp\big\{n\big(p/n + \mathscr{O}_{n\to+\infty}(1/n)\big)\big\} \\ &= \exp\{p + \mathscr{O}_{n\to+\infty}(1)\}, \end{aligned}$$

   donc

$$\boxed{\forall p \in [0;1]\,,\qquad \lim_{n\to+\infty} B_n(p) = \mathrm{e}^p.}$$

2. *Soient $(\Omega, \mathscr{T}, P)$ un espace probabilisé fini, X une variable aléatoire réelle et $(A_k)_{1\leqslant k\leqslant m}$ un système complet d'événements. Pour tout $k \in [\![1;m]\!]$, on note $E(X \rfloor A_k)$ l'espérance de X pour la probabilité conditionnelle P_{A_k} . Démontrer la formule de l'espérance totale $E(X) = \sum_{k=0}^{m} P(A_k)E(X \rfloor A_k)$.*

   On a

$$\begin{aligned} E(X) &= \sum_{x\in X(\Omega)} xP(X = x) \\ &= \sum_{x\in X(\Omega)} x \sum_{k=1}^{m} P(A_k)P(X = x \rfloor A_k) && \text{formule des probas totales à travers le s.c.e } (A_k)_{1\leqslant k\leqslant n} \\ &= \sum_{k=1}^{m} P(A_k) \sum_{x\in X(\Omega)} xP(X = x \rfloor A_k) \end{aligned}$$

   donc

$$\boxed{E(X) = \sum_{k=1}^{m} P(A_k)E(X \rfloor A_k).}$$

3. *On fixe un entier $n \in \mathbb{N}^*$, un nombre réel $p \in [0;1]$ et un nombre réel $\varepsilon \in \mathbb{R}_+^*$. On note Z une variable aléatoire qui suit la loi binomiale $\mathscr{B}(n;p)$ sur un espace probabilisé fini $(\Omega, \mathscr{T}, P)$ quelconque.*

a) *Démontrer que $|f(p) - B_n(p)| \leqslant E\big(|f(p) - f(Z/n)|\big)$.*

On a

$$\begin{aligned} |f(p) - B_n(p)| &= \left|f(p) - \sum_{k=0}^{n} f\Big(\frac{k}{n}\Big)\binom{n}{k}p^k(1-p)^{n-k}\right| \\ &= \left|f(p) - E\Big(f\Big(\frac{Z}{n}\Big)\Big)\right| \qquad \text{formule de transfert} \\ &= \left|E\Big(f(p) - f\Big(\frac{Z}{n}\Big)\Big)\right|. \end{aligned}$$

En utilisant l'inégalité triangulaire pour l'espérance, on en déduit que

$$\boxed{|f(p) - B_n(p)| \leqslant E\left(\left|f(p) - f\Big(\frac{Z}{n}\Big)\right|\right).}$$

b) α] *Justifier l'existence de $M \in \mathbb{R}_+$ tel que $\forall x \in [0;1]\,,\ |f(x)| \leqslant M$.*

La fonction f étant continue sur le segment $[0;1]$, le théorème des bornes nous dit qu'

$$\boxed{\text{il existe } M \in \mathbb{R}_+ \text{ tel que } \forall x, y \in [0;1]\,,\ |f(x)| \leqslant M.}$$

β] *Justifier l'existence de $\delta \in \mathbb{R}_+^*$ tel que $\forall x, y \in [0;1]\,,\ (|x-y| \leqslant \delta) \Longrightarrow (|f(x)-f(y)| \leqslant \varepsilon/2)$.*

La fonction f étant continue sur le segment $[0;1]$, le théorème de Heine nous dit que f est uniformément continue sur $[0;1]$. Par conséquent,

$$\boxed{\text{il existe } \delta \in \mathbb{R}_+^* \text{ tel que } \forall x, y \in [0;1]\,,\ (|x-y| \leqslant \delta) \Longrightarrow \Big(|f(x) - f(y)| \leqslant \frac{\varepsilon}{2}\Big).}$$

γ] *Démontrer que $E\big(|f(p) - f(Z/n)|\big) \leqslant \varepsilon/2 + 2M\,P\big(|Z/n - p| > \delta\big)$.*

Appliquons la formule de l'espérance totale à la variable aléatoire $|f(p) - f(Z/n)|$ à travers le système complet d'événements $(A, \overline{A})$ où

$$A = \left(\left|\frac{Z}{n} - p\right| \leqslant \delta\right) \qquad \text{et} \qquad \overline{A} = \left(\left|\frac{Z}{n} - p\right| > \delta\right).$$

Cela donne

$$\begin{aligned} E\left(\left|f(p) - f\Big(\frac{Z}{n}\Big)\right|\right) &= P\left(\left|\frac{Z}{n} - p\right| \leqslant \delta\right) E\left(\left|f(p) - f\Big(\frac{Z}{n}\Big)\right| \coprod \left|\frac{Z}{n} - p\right| \leqslant \delta\right) \\ &\quad + P\left(\left|\frac{Z}{n} - p\right| > \delta\right) E\left(\left|f(p) - f\Big(\frac{Z}{n}\Big)\right| \coprod \left|\frac{Z}{n} - p\right| > \delta\right). \end{aligned}$$

On a

$$P\left(\left|\frac{Z}{n} - p\right| \leqslant \delta\right) \leqslant 1.$$

Par ailleurs, si $|Z/n - p| \leqslant \delta$, la question β] nous dit que $|f(Z/n) - f(p)| \leqslant \varepsilon/2$, donc

$$E\left(\left|f(p) - f\Big(\frac{Z}{n}\Big)\right| \coprod \left|\frac{Z}{n} - p\right| \leqslant \delta\right) \leqslant E\left(\frac{\varepsilon}{2} \coprod \left|\frac{Z}{n} - p\right| \leqslant \delta\right) = \frac{\varepsilon}{2}.$$

Enfin, on a

$$\left|f(p) - f\Big(\frac{Z}{n}\Big)\right| \leqslant |f(p)| + \left|f\Big(\frac{Z}{n}\Big)\right| \leqslant M + M = 2M,$$

donc

$$E\left(\left|f(p) - f\Big(\frac{Z}{n}\Big)\right| \coprod \left|\frac{Z}{n} - p\right| > \delta\right) \leqslant E\left(2M \coprod \left|\frac{Z}{n} - p\right| > \delta\right) = 2M.$$

En rassemblant ces résultats, il vient

$$\boxed{E\left(\left|f(p) - f\Big(\frac{Z}{n}\Big)\right|\right) \leqslant \frac{\varepsilon}{2} + 2M\,P\left(\left|\frac{Z}{n} - p\right| > \delta\right).}$$

c) *Démontrer que* $P\big(|Z/n - p| > \delta\big) \leqslant 1/(4n\delta^2)$.

Comme $E(Z) = np$ puisque $Z \hookrightarrow \mathscr{B}(n;p)$, on a $E(Z/n) = p$ et donc

$$P\left(\left|\frac{Z}{n} - p\right| > \delta\right) = P\left(\left|\frac{Z}{n} - E\Big(\frac{Z}{n}\Big)\right| > \delta\right).$$

L'inégalité de Bienaymé–Tchebychev nous dit que

$$P\left(\left|\frac{Z}{n} - E\Big(\frac{Z}{n}\Big)\right| > \delta\right) \leqslant \frac{V(Z/n)}{\delta^2}$$

avec

$$V\Big(\frac{Z}{n}\Big) = \frac{1}{n^2}V(Z) = \frac{1}{n^2}np(1-p) = \frac{p(1-p)}{n} \leqslant \frac{1}{4n}$$

où l'inégalité découle du fait que $\forall t \in \mathbb{R},\ t(1-t) \leqslant 1/4$. On a donc

$$\boxed{P\left(\left|\frac{Z}{n} - p\right| > \delta\right) \leqslant \frac{1}{4n\delta^2}.}$$

d) *Écrire la majoration de* $|f(p) - B_n(p)|$ *obtenue.*

En rassemblant les résultats glanés jusqu'ici, on obtient

$$\boxed{|f(p) - B_n(p)| \leqslant \frac{\varepsilon}{2} + \frac{M}{2n\delta^2}.}$$

4. *Démontrer que la suite de fonctions polynomiales* $(B_n)_{n\geqslant 1}$ *converge uniformément vers* f *sur* $[0;1]$.

Soit $\varepsilon > 0$. Le résultat de la question précédente nous dit qu'il existe $\delta_\varepsilon \in \mathbb{R}_+^*$ tel que la fonction $p \longmapsto |f(p) - B_n(p)|$ est majorée par $\varepsilon/2 + M/(2n{\delta_\varepsilon}^2)$ sur $[0;1]$. Cela nous autorise à passer à la borne supérieure, ce qui donne

$$\sup_{p\in[0;1]} |f(p) - B_n(p)| \leqslant \frac{\varepsilon}{2} + \frac{M}{2n{\delta_\varepsilon}^2}.$$

Comme la suite $\big(M/(2n{\delta_\varepsilon}^2)\big)_{n\geqslant 1}$ tend vers 0, il existe $N_\varepsilon \in \mathbb{N}^*$ tel que

$$\forall n \geqslant N_\varepsilon, \qquad \frac{M}{2n{\delta_\varepsilon}^2} \leqslant \frac{\varepsilon}{2}.$$

Il s'ensuit que

$$\forall n \geqslant N_\varepsilon, \qquad \sup_{p\in[0;1]} |f(p) - B_n(p)| \leqslant \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

Pour résumer, on a démontré que

$$\forall \varepsilon > 0, \quad \exists N_\varepsilon \in \mathbb{N}^*, \quad \forall n \geqslant N_\varepsilon, \qquad \sup_{p\in[0;1]} |f(p) - B_n(p)| \leqslant \varepsilon,$$

ce qui signifie que

$$\lim_{n\to+\infty} \sup_{p\in[0;1]} |f(p) - B_n(p)| = 0$$

ou encore que

$$\boxed{\text{la suite de fonctions polynomiales } (B_n)_{n\geqslant 1} \text{ converge uniformément vers } f \text{ sur } [0;1].}$$

Remarque culturelle :

Nous venons de démontrer que toute fonction continue sur le segment $[0;1]$ est la limite uniforme d'une suite de polynômes. La propriété reste vraie sur tout segment (car on peut toujours se ramener à $[0;1]$ en composant par une fonction affine). Ainsi, une fonction continue sur un segment y est limite uniforme d'une suite de polynômes. C'est le théorème d'approximation polynomiale de Weierstrass.

Ce théorème est un résultat d'analyse remarquable. Il possède plusieurs autres démonstrations classiques par des arguments d'analyse et de topologie.

EXERCICE 5

On convient que $0\ln 0 = 0$; toutes les variables aléatoires sont à valeurs dans un ensemble fini $\mathscr{E}$ de cardinal n ; on appelle entropie de lavariable X la quantité $H(X) = -\sum_{a\in\mathscr{E}} P(X=a)\ln P(X=a)$; on considère une variable U telle que $\forall a \in \mathscr{E},\ P(U=a) \neq 0$; pour toute variable X, on appelle entropie relative de X pour U la quantité $K_U(X) = \sum_{a\in\mathscr{E}} P(X=a)\ln\big(P(X=a)/P(U=a)\big)$.

A. *Nous allons encadrer l'entropie.*

1. a) *Quel est le signe de $H(X)$?*

Soit $a \in \mathscr{E}$. Si $P(X=a) = 0$ alors $P(X=a)\ln\big(P(X=a)\big) = 0$. Si $P(X=a) \in]0;1]$, alors $P(X=a)\ln\big(P(X=a)\big) < 0$. La quantité $H(X)$ est donc l'opposée d'une somme de termes négatifs ou nuls, ce qui donne

$$\boxed{H(X) \geqslant 0.}$$

b) *Démontrer que $H(X) = 0$ si, et seulement si, X suit une loi certaine.*

Supposons que la variable aléatoire X suit une loi certaine, c'est-à-dire qu'il existe $a_0 \in \mathscr{E}$ tel que $P(X=a_0) = 1$. On a alors $P(X=a_0)\ln P(X=a_0) = P(X=a_0)\ln 1 = 0$ et pour les autres valeurs de a, on a $P(X=a)\ln P(X=a) = 0$ car $P(X=a) = 0$. Par suite, $H(X)$ est une somme de termes tous nuls, d'où $H(X) = 0$.
Supposons réciproquement que $H(X) = 0$. Comme $H(X)$ est une somme de termes négatifs ou nuls, tous ces termes sont nuls, i.e. $\forall a \in \mathscr{E},\ P(X=a)\ln P(X=a) = 0$. Comme $\sum_{a\in\mathscr{E}} P(X=a) = 1$, l'une des probabilités $P(X=a)$ est forcément non nulle. Considérons alors $a_0 \in \mathscr{E}$ tel que $P(X=a_0) \neq 0$. Comme $P(X=a_0)\ln P(X=a_0) = 0$, on a nécessairement $P(X=a_0) = 1$. Donc X suit une loi certaine de paramètre a_0.
En résumé,

$$\boxed{H(X) = 0 \text{ si, et seulement si, } X \text{ suit une loi certaine.}}$$

2. a) *Démontrer que $\forall x \geqslant 0,\ x\ln x \geqslant x-1$. En déduire que $K_U(X) \geqslant 0$. Quand y a-t-il égalité ?*

Si $x = 0$, on a clairement $x\ln x > x-1$ car $0\ln 0 = 0$.
Pour $x > 0$, on considère $\varphi(x) = x\ln x - x + 1$. C'est une fonction de classe $\mathscr{C}^\infty$ sur $\mathbb{R}_+^*$ et $\forall x > 0,\ \varphi'(x) = \ln x$. On a donc $\varphi'(x) \geqslant 0$ si, et seulement si, $x \geqslant 1$ (avec égalité si, et seulement si, $x = 1$), donc φ décroît strictement sur $]0;1]$ et croît strictement sur $[1;+\infty[$. Ainsi φ atteint son minimum en 1. Comme $\varphi(1) = 0$, on a $\forall x > 0,\ \varphi(x) \geqslant 0$ (avec égalité si, et seulement si, $x = 1$), c'est-à-dire $\forall x > 0,\ x\ln x \geqslant x-1$ (avec égalité si, et seulement si, $x = 1$).
Pour résumer, on a

$$\boxed{\forall x \geqslant 0,\ x\ln x \geqslant x-1 \text{ avec égalité si, et seulement si, } x = 1.}$$

On a

$$\begin{aligned}
K_U(X) &= \sum_{a\in\mathscr{E}} P(X=a)\ln\Big(\frac{P(X=a)}{P(U=a)}\Big) \\
&= \sum_{a\in\mathscr{E}} P(U=a)\frac{P(X=a)}{P(U=a)}\ln\Big(\frac{P(X=a)}{P(U=a)}\Big) \\
&\geqslant \sum_{a\in\mathscr{E}} P(U=a)\Big(\frac{P(X=a)}{P(U=a)} - 1\Big) \qquad \text{d'après l'inégalité } \forall x \geqslant 0,\ x\ln x \geqslant x-1 \\
&= \underbrace{\sum_{a\in\mathscr{E}} P(X=a)}_{=1} - \underbrace{\sum_{a\in\mathscr{E}} P(U=a)}_{=1} \\
&= 0,
\end{aligned}$$

donc

$$\boxed{K_U(X) \geqslant 0.}$$

Pour qu'il y ait égalité dans cette inégalité, il faut et suffit que l'on ait égalité dans toutes les inégalités du raisonnement ci-dessus. Or $x\ln x = x-1$ si, et seulement si, $x = 1$, donc

$$K_U(X) \geqslant 0 \iff \forall a \in \mathscr{E},\ \frac{P(X=a)}{P(U=a)} = 1 \iff \forall a \in \mathscr{E},\ P(X=a) = P(U=a).$$

Ainsi

$$\boxed{K_U(X) = 0 \text{ si, et seulement si, } X \text{ et } U \text{ ont la même loi.}}$$

b) *Dans cette question, on suppose que U suit la loi uniforme sur $\mathscr{E}$. Exprimer $K_U(X)$ en fonction de n et $H(X)$ et en déduire une majoration de $H(X)$.*

On a

$$\begin{aligned} K_U(X) &= \sum_{a\in\mathscr{E}} P(X=a)\ln\Big(\frac{P(X=a)}{1/n}\Big) \\ &= \sum_{a\in\mathscr{E}} P(X=a)\ln\big(P(X=a)\big) + \sum_{a\in\mathscr{E}} P(X=a)\ln n \\ &= -H(X)+\ln n \qquad \text{car } \sum_{a\in\mathscr{E}} P(X=a)=1, \end{aligned}$$

donc

$$\boxed{\text{si } U \text{ suit la loi uniforme sur } \mathscr{E}, \text{ alors } K_U(X)=\ln n - H(X).}$$

Comme $K_U(X)\geqslant 0$, on a $\ln n - H(X)\geqslant 0$, d'où

$$\boxed{H(X)\leqslant \ln n.}$$

c) *Démontrer que $H(X)=\ln n$ si, et seulement si, X suit la loi uniforme sur $\mathscr{E}$.*

Supposons que X suit la loi uniforme sur $\mathscr{E}$. Alors

$$H(X) = -\sum_{a\in\mathscr{E}} \frac{1}{n}\ln\Big(\frac{1}{n}\Big) = -n\times\frac{1}{n}\ln\Big(\frac{1}{n}\Big) = \ln n.$$

Supposons réciproquement que $H(X)=\ln n$. Alors, d'après la question précédente, on a $K_U(X)=0$. On sait depuis la question a) que cela implique que X et U ont la même loi et donc que X suit la loi uniforme sur $\mathscr{E}$.
En conclusion,

$$\boxed{H(X)=\ln n \text{ si, et seulement si, } X \text{ suit la loi uniforme sur } \mathscr{E}.}$$

B. *Dans cette partie et la suivante, on suppose que $\mathscr{E}=\mathscr{E}_1\times\mathscr{E}_2$ avec $\operatorname{card}\mathscr{E}_1=n_1$ et $\operatorname{card}\mathscr{E}_2=n_2$ de sorte que l'on ait $n=n_1n_2$; on pose $U=(U_1,U_2)$ et $X=(X_1,X_2)$ de sorte que l'on ait $H(X)=H(X_1,X_2)=-\sum_{a_1\in\mathscr{E}_1,a_2\in\mathscr{E}_2} P(X_1=a_1\,,\,X_2=a_2)\ln P(X_1=a_1\,,\,X_2=a_2)$ et $K_U(X)=K_{(U_1,U_2)}(X_1,X_2)=\sum_{a_1\in\mathscr{E}_1,a_2\in\mathscr{E}_2} P(X_1=a_1,X_2=a_2)\ln\big(P(X_1=a_1\,,X_2=a_2)/P(U_1=a_1,U_2=a_2)\big)$; on suppose enfin que U_1 et U_2 sont indépendantes.*

1. *Dans cette question, on suppose que U_1 suit la même loi que X_1 et que U_2 suit la même loi que X_2.*

a) *À quelle condition nécessaire et suffisante le couple (X_1,X_2) a-t-il la même loi que le couple (U_1,U_2) ?*

Les deux couples ont les mêmes lois marginales mais seules U_1 et U_2 sont a priori indépendantes. Comme l'indépendance suffit à reconstituer la loi conjointe, on en déduit donc que

$$\boxed{(X_1,X_2) \text{ et } (U_1,U_2) \text{ ont même loi si, et seulement si, } X_1 \text{ et } X_2 \text{ sont indépendantes.}}$$

b) *Démontrer que $K_{(U_1,U_2)}(X_1,X_2)=H(X_1)+H(X_2)-H(X_1,X_2)$.*

On a

$$\begin{aligned} & K_{(U_1,U_2)}(X_1,X_2) \\ = & \sum_{\substack{a_1\in\mathscr{E}_1\\ a_2\in\mathscr{E}_2}} P(X_1=a_1\,,\,X_2=a_2)\ln\Big(\frac{P(X_1=a_1\,,\,X_2=a_2)}{P(U_1=a_1\,,\,U_2=a_2)}\Big) \\ = & \sum_{\substack{a_1\in\mathscr{E}_1\\ a_2\in\mathscr{E}_2}} P(X_1=a_1\,,\,X_2=a_2)\ln\Big(\frac{P(X_1=a_1\,,\,X_2=a_2)}{P(U_1=a_1)P(U_2=a_2)}\Big) \qquad \text{car } U_1 \perp\!\!\!\perp U_2 \\ = & \sum_{\substack{a_1\in\mathscr{E}_1\\ a_2\in\mathscr{E}_2}} P(X_1=a_1\,,\,X_2=a_2)\ln P(X_1=a_1\,,\,X_2=a_2) \\ & \quad - \sum_{\substack{a_1\in\mathscr{E}_1\\ a_2\in\mathscr{E}_2}} P(X_1=a_1\,,\,X_2=a_2)\ln P(U_1=a_1) \\ & \quad\quad - \sum_{\substack{a_1\in\mathscr{E}_1\\ a_2\in\mathscr{E}_2}} P(X_1=a_1\,,\,X_2=a_2)\ln P(U_2=a_2) \end{aligned}$$

Or

$$\sum_{\substack{a_1\in\mathscr{E}_1\\ a_2\in\mathscr{E}_2}} P(X_1=a_1\,,\,X_2=a_2)\ln P(X_1=a_1\,,\,X_2=a_2)=-H(X_1,X_2),$$

$$\begin{aligned}\sum_{\substack{a_1\in\mathscr{E}_1\\ a_2\in\mathscr{E}_2}} P(X_1=a_1\,,\,X_2=a_2)\ln P(U_1=a_1) &= \sum_{a_1\in\mathscr{E}_1}\underbrace{\sum_{a_2\in\mathscr{E}_2} P(X_1=a_1\,,\,X_2=a_2)}_{=P(X_1=a_1)}\ln P(U_1=a_1)\\ &= \sum_{a_1\in\mathscr{E}_1} P(X_1=a_1)\ln P(X_1=a_1)\\ &\qquad\qquad \text{car } P(U_1=a_1)=P(X_1=a_1)\\ &= -H(X_1)\end{aligned}$$

et de même

$$\sum_{\substack{a_1\in\mathscr{E}_1\\ a_2\in\mathscr{E}_2}} P(X_1=a_1\,,\,X_2=a_2)\ln P(U_2=a_2)=-H(X_2)$$

donc

$$\boxed{K_{(U_1,U_2)}(X_1,X_2)=H(X_1)+H(X_2)-H(X_1,X_2).}$$

c) *En déduire que $H(X)\leqslant H(X_1)+H(X_2)$ et donner une condition nécessaire et suffisante pour qu'il y ait égalité.*

On a vu, à la question A. 2. a), que $K_{(U_1,U_2)}(X_1,X_2)=K_U(X)\geqslant 0$. Associée au résultat de la question précédente, cette inégalité nous dit que $H(X_1)+H(X_2)-H(X_1,X_2)\geqslant 0$, c'est-à-dire

$$\boxed{H(X_1,X_2)\leqslant H(X_1)+H(X_2).}$$

On a égalité dans cette inégalité si, et seulement si, $K_U(X)=0$, ce qui revient à dire (d'après A. 2. a)) que les couples $X=(X_1,X_2)$ et $U=(U_1,U_2)$ ont la même loi, ou encore, d'après a), que X_1 et X_2 sont indépendantes. En conclusion,

$$\boxed{H(X_1,X_2)=H(X_1)+H(X_2)\text{ si, et seulement si, }X_1\perp\!\!\!\perp X_2.}$$

2. a) *Démontrer que $H(X_1,X_2)\geqslant H(X_1)$.*

Soit $(a_1,a_2)\in\mathscr{E}_1\times\mathscr{E}_2$. Comme $(X_1=a_1\,,\,X_2=a_2)\subset(X_1=a_1)$, on a

$$P(X_1=a_1\,,\,X_2=a_2)\leqslant P(X_1=a_1).$$

La croissance du logarithme nous dit alors que

$$P(X_1=a_1\,,\,X_2=a_2)\ln P(X_1=a_1\,,\,X_2=a_2)\leqslant P(X_1=a_1\,,\,X_2=a_2)\ln P(X_1=a_1)$$

et l'on peut noter que cette inégalité est bien vraie lorsque $P(X_1=a_1\,,\,X_2=a_2)=0$ puisqu'elle est alors équivalente à $0\leqslant 0$.
En effectuant une double sommation sur $a_1\in\mathscr{E}_1$, $a_2\in\mathscr{E}_2$ dans les deux membres de cette inégalité, on obtient alors

$$-H(X_1,X_2)\leqslant \sum_{a_1\in\mathscr{E}_1}\underbrace{\sum_{a_2\in\mathscr{E}_2} P(X_1=a_1\,,\,X_2=a_2)}_{=P(X_1=a_1)}\ln\big(P(X_1=a_1)\big),$$

c'est-à-dire

$$-H(X_1,X_2)\leqslant -H(X_1),$$

ou encore

$$\boxed{H(X_1,X_2)\geqslant H(X_1).}$$

b) *On suppose que $H(X_1,X_2)=H(X_1)$. Prouver que pour tout $a_1\in\mathscr{E}_1$ tel que $P(X_1=a_1)\neq 0$, il existe un unique élément de $\mathscr{E}_2$, noté $r(a_1)$, tel que $P\big(X_1=a_1\,,\,X_2=r(a_1)\big)=P(X_1=a_1)$. Soit $b\in\mathscr{E}_2$ quelconque. Lorsque $P(X_1=a_1)=0$, on pose $r(a_1)=b$. On définit ainsi une application $r:\mathscr{E}_1\longrightarrow\mathscr{E}_2$. Démontrer que l'événement $\big(X_2=r(X_1)\big)$ est quasi-certain.*

Pour avoir $H(X_1,X_2)=H(X_1)$, il est nécessaire, d'après a), que pour tout $(a_1,a_2)\in\mathscr{E}_1\times\mathscr{E}_2$,

$$P(X_1=a_1\,,\,X_2=a_2)\ln P(X_1=a_1\,,\,X_2=a_2)=P(X_1=a_1\,,\,X_2=a_2)\ln P(X_1=a_1).$$

Soit $a_1\in\mathscr{E}_1$ tel que $P(X_1=a_1)\neq 0$. Il existe alors $a_2\in\mathscr{E}_2$ tel que $P(X_1=a_1\,,\,X_2=a_2)\neq 0$. L'égalité ci-dessus permet d'en déduire que $P(X_1=a_1\,,\,X_2=a_2)=P(X_1=a_1)$ et donc que, parmi les nombres $P(X_1=a_1\,,\,X_2=b)$ où b parcourt $\mathscr{E}_2$, $P(X_1=a_1\,,\,X_2=a_2)$ est le seul qui soit non nul. Ainsi,

> on a bien justifié l'existence et l'unicité d'un élément de $\mathscr{E}_2$, qu'il est alors licite de noter $r(a_1)$, tel que $P\big(X_1=a_1\,,\,X_2=r(a_1)\big)=P(X_1=a_1)$.

Calculons la probabilité de l'événement $\big(X_2=r(X_1)\big)$. On a

$$\begin{aligned}
P\big(X_2=r(X_1)\big) &= \sum_{a_1\in\mathscr{E}_1} P\big(X_1=a_1\,,\,X_2=r(X_1)\big) && \text{par filtration à travers le s.c.e. } (X_1=a_1)_{a_1\in\mathscr{E}_1}\\
&= \sum_{a_1\in\mathscr{E}_1} P\big(X_1=a_1\,,\,X_2=r(a_1)\big)\\
&= \sum_{a_1\in\mathscr{E}_1} P(X_1=a_1)\\
&= 1,
\end{aligned}$$

donc

> l'événement $\big(X_2=r(X_1)\big)$ est quasi-certain.

c) *Réciproquement, on suppose qu'il existe une application $r:\mathscr{E}_1\longrightarrow\mathscr{E}_2$ telle que l'événement $\big(X_2=r(X_1)\big)$ soit quasi-certain. Démontrer que $H(X_1,X_2)=H(X_1)$.*

On a

$$\begin{aligned}
H(X_1,X_2) &= H\big(X_1,g(X_1)\big)\\
&= -\underbrace{\sum_{\substack{a_1\in\mathscr{E}_1\\ a_2\in\mathscr{E}_2}} P\big(X_1=a_1\,,\,g(X_1)=a_2\big)\ln P\big(X_1=a_1\,,\,g(X_1)=a_2\big)}_{\text{dans cette somme, seuls les termes tels que } a_2=g(a_1) \text{ sont non nuls car l'événement } (X_2=r(X_1)) \text{ est quasi-certain.}}\\
&= -\sum_{a_1\in\mathscr{E}_1} P\big(X_1=a_1\,,\,g(X_1)=g(a_1)\big)\ln P\big(X_1=a_1\,,\,g(X_1)=g(a_1)\big)\\
&= -\sum_{a_1\in\mathscr{E}_1} P(X_1=a_1)\ln P(X_1=a_1) && \text{car } (X_1=a_1) \text{ implique } \big(g(X_1)=g(a_1)\big)\\
&= H(X_1),
\end{aligned}$$

donc

> s'il existe une application $r:\mathscr{E}_1\longrightarrow\mathscr{E}_2$ telle que l'événement $\big(X_2=r(X_1)\big)$ soit quasi-certain, alors $H(X_1,X_2)=H(X_1)$.

d) *Justifier que $H(X_1,X_2)\geqslant\max\{H(X_1);H(X_2)\}$ et préciser les cas d'égalité.*

Les rôles de X_1 et X_2 étant symétriques dans l'expression de $H(X_1,X_2)$, on démontrerait de même que $H(X_1,X_2)\geqslant H(X_2)$. On a donc bien

$$\boxed{H(X_1,X_2)\geqslant\max\{H(X_1),H(X_2)\}.}$$

De plus,

> $H(X_1,X_2)=H(X_1)$ si, et seulement si, X_2 est presque surement une fonction de X_1
>
> et
>
> $H(X_1,X_2)=H(X_2)$ si, et seulement si, X_1 est presque surement une fonction de X_2.

C. *Avec les notations de la partie précédente, on définit l'entropie conditionnelle de X_2 sachant X_1 par $H(X_2 \,|\, X_1) = -\sum_{a_1 \in \mathscr{E}_1 a_2 \in \mathscr{E}_2} P(X_1 = a_1\,,\, X_2 = a_2) \ln P(X_2 = a_2 \,|\, X_1 = a_1)$.*

1. *Démontrer que $H(X_2 \,|\, X_1) = H(X_1, X_2) - H(X_1)$.*

On a

$$\begin{aligned}
H(X_2 \,|\, X_1) &= -\sum_{\substack{a_1 \in \mathscr{E}_1 \\ a_2 \in \mathscr{E}_2}} P(X_1 = a_1\,,\, X_2 = a_2) \ln P(X_2 = a_2 \,|\, X_1 = a_1) \\
&= -\sum_{\substack{a_1 \in \mathscr{E}_1 \\ a_2 \in \mathscr{E}_2}} P(X_1 = a_1\,,\, X_2 = a_2) \ln \Big(\frac{P(X_2 = a_2\,,\, X_1 = a_1)}{P(X_1 = a_1)} \Big) \\
&= -\sum_{\substack{a_1 \in \mathscr{E}_1 \\ a_2 \in \mathscr{E}_2}} P(X_1 = a_1\,,\, X_2 = a_2) \ln P(X_2 = a_2\,,\, X_1 = a_1) \\
&\qquad + \sum_{\substack{a_1 \in \mathscr{E}_1 \\ a_2 \in \mathscr{E}_2}} P(X_1 = a_1\,,\, X_2 = a_2) \ln P(X_1 = a_1) \\
&= H(X_1, X_2) + \sum_{a_1 \in \mathscr{E}_1} \underbrace{\sum_{a_2 \in \mathscr{E}_2} P(X_1 = a_1\,,\, X_2 = a_2)}_{= P(X_1 = a_1)} \ln P(X_1 = a_1) \\
&= H(X_1, X_2) - H(X_1),
\end{aligned}$$

donc

$$\boxed{H(X_2 \,|\, X_1) = H(X_1, X_2) - H(X_1).}$$

2. *Dans un livre sur la théorie de l'information, Claude Shannon écrit : « L'entropie conditionnelle mesure l'entropie restante provenant de la variable X_2, si l'on connait parfaitement la variable X_1. Plus précisément, $H(X_2 \,|\, X_1) = 0$ si, et seulement si, la variable X_2 est complètement déterminée par la variable X_1. Inversement $H(X_2 \,|\, X_1) = H(X_2)$ si, et seulement si, X_1 et X_2 sont des variables indépendantes. » Justifier cette affirmation à l'aide des résultats de la partie précédente.*

Nous avons vu dans la partie B que

$$H(X_1) \leqslant H(X_1, X_2) \leqslant H(X_1) + H(X_2)$$

avec égalité à gauche lorsque X_2 est une fonction de X_1 et avec égalité à droite si, et seulement si, X_1 et X_2 sont indépendantes. En soustrayant $H(X_1)$ à cet encadrement, on obtient

$$0 \leqslant H(X_2 \,|\, X_1) \leqslant H(X_2),$$

avec les mêmes conditions d'égalité. Cela justifie bien le fait que

> l'entropie conditionnelle mesure l'entropie restante provenant de la variable X_2, si l'on connait parfaitement la première variable X_1.

3. *Anick et Bruno s'opposent au jeu suivant : Anick choisit un nombre dans $[\![1; 2016]\!]$. Pour trouver le nombre d'Anick, Bruno pose une série de q questions où $q \in \mathbb{N}$ est fixé à l'avance. Ces questions sont de la forme : « le nombre choisi appartient-il à E » où E est un sous-ensemble de $[\![1; 2016]\!]$ pouvant varier à chaque question. Anick répond « oui » si le nombre appartient à E et « non » sinon. Au bout des q questions, Bruno donne sa réponse. On note N le nombre choisi par Anick et, pour $i \in [\![1; q]\!]$, on note $X_i = 1$ si la réponse d'Anick est positive à la i-ème question et $X_i = 0$ sinon. Enfin, on pose $X = \sum_{i=1}^{q} X_i\, 2^{i-1}$ la variable aléatoire qui code en binaire les réponses d'Anick.*

a) *Justifier, en langage courant, que $H(X \,|\, N) = 0$ et en déduire que $H(N \,|\, X) = \ln 2016 - H(X)$.*

Lorsqu'on connait la variable N, on connait les réponses d'Anick, c'est-à-dire les valeurs des variables X_i et donc aussi la valeur de X. Cela signifie que X est une fonction de N et donc, d'après la question précédente,

$$\boxed{H(X \,|\, N) = 0.}$$

Comme $H(X \,|\, N) = H(N, X) - H(N)$, on a par conséquent $H(N, X) = H(N)$. Or on sait que $H(N \,|\, X) = H(N, X) - H(X)$, donc

$$H(N \,|\, X) = H(N) - H(X).$$

Or N suit la loi uniforme sur $[\![1; 2016]\!]$, donc, d'après A. 2. c), $H(N) = \ln 2016$. Il s'ensuit que

$$\boxed{H(N \,|\, X) = \ln 2016 - H(X).}$$

b) *Démontrer que X est à valeurs dans $[\![0;2^q-1]\!]$ et en déduire une majoration de $H(X)$.*

Comme $\forall i \in [\![1;q]\!]\,,\ X_i \in \{0;1\}$, on a clairement

$$0 = \sum_{i=1}^{q} 0 \times 2^{i-1} \leqslant X \leqslant \sum_{i=1}^{q} 1 \times 2^{i-1} = 2^q - 1,$$

donc

$$\boxed{X(\Omega) = [\![0;2^q-1]\!].}$$

D'après A. 2. b), on a alors

$$H(X) \leqslant \ln \operatorname{card} X(\Omega) = \ln 2^q = q \ln 2,$$

donc

$$\boxed{H(X) \leqslant q \ln 2.}$$

c) *Bruno prétend pouvoir trouver à coup sûr le nombre d'Anick en au plus 10 questions. Qu'en pensez-vous ? En combien de questions au minimum êtes vous certain de pouvoir donner la valeur de N ?*

En combinant les résultats des deux questions précédentes, il vient

$$H(N \mid X) \geqslant \ln 2016 - q \ln 2.$$

Avec $q = 10$, on obtient

$$H(N \mid X) \geqslant 0,6$$

ce qui prouve qu'il reste une incertitude sur la valeur de N connaissant celle de X. On en déduit que

$$\boxed{\text{Bruno est un gros arnaqueur !}}$$

On désire déterminer une valeur de q telle que $H(N \mid X) = 0$. Pour cela, il est nécessaire que $\ln 2016 - q \ln 2 \leqslant 0$ donc que

$$q \geqslant \frac{\ln 2016}{\ln 2} \approx 10,97 \qquad \text{c'est-à-dire} \qquad q \geqslant 11.$$

Reste à voir si la condition $q = 11$ est suffisante, c'est-à-dire si, pour $q = 11$, on a $H(N \mid X) = 0$. Pour le vérifier, il suffit de donner une tactique qui permette à Bruno de deviner le nombre d'Anick en 11 questions. Pour cela, on décompose les différents éléments de $[\![1;2016]\!]$ en base 2. Comme $2^{10} \leqslant 2016 < 2^{11}$, ces écritures dyadiques possèdent au plus 11 chiffres et sont donc de la forme $\overline{b_{10}b_9\cdots b_1b_0}$ avec $\forall j \in [\![0;10]\!]\,,\ b_j \in \{0;1\}$. On considère alors les 11 ensembles

$$E_k = \{\overline{b_{10}b_9\cdots b_1b_0} : b_k = 1\} \qquad 0 \leqslant k \leqslant 10.$$

Les 11 questions posées par Bruno permettent alors de déterminer un par un les « bits » de l'écriture dyadique de N, c'est-à-dire

$$N = \sum_{i=1}^{q} X_i\, 2^{i-1} = X.$$

On en déduit bien que l'

$$\boxed{\text{on est certain de pouvoir donner la valeur de } N \text{ en au plus 11 questions.}}$$