DOMAINE : Algèbre
NIVEAU : Débutants
CONTENU : Cours et exercices

AUTEUR : Guillaume CONCHON-KERJAN
STAGE : Montpellier 2013

Suites et polynômes

- Suites -

Définition 1. On appelle $u_0, \cdots, u_n \cdots$, où $u_k \in \mathbb{K}$ pour tout $k \in \mathbb{N}$ une suite à valeurs dans $\mathbb{K}$, notée (u_n) ou $(u_n)_{n\in\mathbb{N}}$. On peut en fait définir une suite $(u_n)_{n\in I}$ où I est inclus dans $\mathbb{N}$, éventuellement fini, mais c'est plus rare.

La méthode de résolution d'un exercice portant sur les suites est en général assez junglesque, mais il y a quelques idées à connaître. Il importe de chercher si :
• la suite étudiée est croissante ou décroissante,
• la suite à une **limite** : u_n se rapproche a d'une valeur l, éventuellement infinie, lorsque n tend vers l'infini (si $l \in \mathbb{R}$, on dit alors que (u_n) converge vers l),
• la suite est **périodique** : il existe $p \in \mathbb{N}$ tel que pour tout entier naturel n, $u_{n+p} = u_n$. Parfois, cette propriété n'est vraie qu'à partir d'un certain rang, et la suite est alors dite ultimement périodique. Une suite (ultimement) périodique de période 1 est dite **stationnaire**.
On dispose de quelques propriétés :

Proposition 2. Toute suite croissante majorée est convergente.
Toute suite décroissante minorée est convergente.
Toute suite périodique convergente est stationnaire.

Il existe de plus quelques types de suites assez particuliers :

Définition 3. Une suite de la forme $u_n = an + b$ avec $a, b \in \mathbb{R}$ est dite **arithmétique** de raison a.
Une suite de la forme $u_n = b \times a^n$ avec $a, b \in \mathbb{R}$ est dite **géométrique** de raison a.

Et il convient de noter quelques propriétés sommatoires :

Proposition 4. Soit $u_n := an + b$ pour tout $n \in \mathbb{N}$. On a $\sum_{n=0}^{N-1} u_n = a\frac{N(N-1)}{2} + Nb$.

Soit $u_n := ba^n$ pour tout $n \in \mathbb{N}$. On a $\sum_{n=0}^{N-1} u_n = b\frac{1-a^N}{1-a}$.

La démonstration, purement calculatoire, est laissée au bon plasir du lecteur.

On peut même envisager une sorte de mélange entre ces deux types de suites, abordé dans la rubrique suivante.

Suites et récurrence

On peut souvent démontrer une propriété voulue sur une suite, voire même trouver l'expression du terme général, en utilisant une récurrence. Cette récurrence s'exprime la plupart du temps sous forme de deux types d'équations. Le premier est une équation de la forme

$$u_{n+1} = f(u_n).$$

f est presque toujours continue, auquel cas

Proposition 5. si l est la limite de la suite (u_n) (qui n'en a pas forcément !), alors

$$f(l) = l$$

Exercice 1 Étudier la suite définie par $u_0 = 0$ et $u_{n+1} = \sqrt{12 + u_n}$ pour tout $n \in \mathbb{N}$.

Concernant le second type d'équations :

Définition 6. Soit (u_n) une suite réelle, on dit qu'elle satisfait une **équation de récurrence d'ordre k** (linéaire) lorsqu'il existe $k \in \mathbb{N}^*$ et des réels $a_0, \cdots, a_{k-1}$ tels que pour tout entier naturel n,

$$u_{n+k} + a_{k-1}u_{n+k-1} + \cdots + a_0 u_n = 0$$

Définition 7. L'équation $X^k + a_{k-1}X^{k-1} + \cdots + a_0 = 0$ est appelée **équation caractéristique**.

Exemple 8. Pour une suite arithmétique de raison a, $u_{n+1}-u_n = u_{n+2}-u_{n+1} = a$, donc $u_{n+2} - 2u_{n+1} + u_n = 0$ est une équation de récurrence vérifiée par u_n.
Pour une suite géométrique de raison a, $u_{n+1} - au_n = 0$.
Une suite **arithmético-géométrique** vérifie une relation de la forme : $u_{n+1} = au_n + b$, et on obtient l'équation de récurrence $u_{n+2} - (a+1)u_{n+1} + au_n = 0$

La résolution générale d'une telle équation de récurrence (dont la démonstration est inutile et fastidieuse dans notre cadre) utilise la notion de polynôme, abordée dans la section suivante. Contentons-nous des ordres 1 et 2 ici.

Proposition 9. Si pour tout $n \in \mathbb{N}$, $u_{n+1} - au_n = 0$, alors $u_n = u_0 a^n$.

Proposition 10. Si pour tout $n \in \mathbb{N}$, $u_{n+2} + a_1u_{n+1} + a_0u_n = 0$, on résout l'équation caractéristique du second degré $X^2 + a_1X + a_0 = 0$.
• Si elle a deux solutions distinctes r_1 et r_2, alors : $u_n = c_1r_1^n + c_2r_2^n$, où c_1 et c_2 sont déterminées avec, par exemple, les valeurs de u_0 et u_1.
• Si elle a une racine double r, alors : $u_n = (an+b)r^n$, et encore une fois u_0 et u_1 permettent de déterminer a et b.

Sauriez-vous retrouver dans la propriété précédente les suites arithmétiques, géométriques, et arithmético-géométriques ?

Exemple 11. Une suite géométrique correspond à une équation de récurrence d'ordre 1.
Une suite arithmétique correspond à une équation de récurrence d'ordre 2 ayant 1 pour racine double.
Une suite arithmético-géométrique de raison a correspond à une équation de récurrence d'ordre 2 dont les solutions sont 1 et a.

Tant de théorie prometteuse n'en appelle qu'avec plus de force des exercices permettant d'appliquer victorieusement ces nouvelles connaissances.
Exercice 2 Évariste doit monter un escalier de $n \geqslant 1$ marches. Pour ne pas trop se fatiguer, il décide à chaque pas de monter une ou deux marches à la fois, pas plus. De combien de manières différentes peut-il monter l'escalier ?

Les exercices suivants ne se rapportent pas nécessairement à un paragraphe précis du cours.
Exercice 3 Existe-t-il une suite d'entiers $(u_n)_{n\in\mathbb{N}^*}$ strictement croissante telle que pour tous entiers naturels n, m, on ait $u_{nm} = u_n + u_m$? Et simplement croissante ?

Exercice 4 On définit la suite (a_n) par $a_0 > 0$ et $a_{n+1} = \sqrt{a_n + 1}$ pour tout $n \in \mathbb{N}^*$. Montrer que la suite a au moins un terme irrationnel.

Et un petit classique pour la route :
Exercice 5 Soit (u_n) la suite définie par $u_0 = 5$ et $u_{n+1} = u_n + \frac{1}{u_n}$ pour $n \in \mathbb{N}$. Montrer que $u_{1000} > 45$.

- Polynômes -

Définition 12. • Soit $n \in \mathbb{N}$, et $a_0, \cdots, a_n \in \mathbb{K}$, l'expression $P(X) = a_0 + \cdots + a_n X^n$ est un polynôme à coefficients dans $\mathbb{K}$. Si $a_n \neq 0$, condition presque systématiquement supposée réalisée dans la suite du cours, on dit que le polynôme est de degré n, ce qui s'écrit souvent $deg P = n$.
• On note $\mathbb{K}[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{K}$.
• Le coefficient a_n est appelé **coefficient dominant**. Si $a_n = 1$, le polynôme est dit **unitaire**.
• Le coefficient a_0 est souvent appelé "terme constant".
• Le terme $a_k X^k$ est appelé **monôme de degré k**.

Remarque 13. Une fonction polynôme associe à x (généralement un **réel** , on ne s'étendra pas ici au cas complexe) l'expression $P(x)$. Par la suite, on confondra classiquement et sans scrupules "polynôme" et "fonction polynôme".

Remarque 14. On a $P(0) = a_0$, petite relation très souvent utile. A noter aussi qu'en l'infini, le terme de coefficient dominant "écrase" tous les autres, d'où son nom (?) : le monôme $a_n x^n$ est arbitrairement plus grand que les autres.

Le fait que le terme dominant "écrase" les autres à l'infini et qu'un polynôme non constant diverge en $+\infty$ ou $-\infty$ permet d'établir le théorème essentiel suivant :

Théorème 15. L'écriture d'un polynôme est unique ! Si on a deux expressions pour un même polynôme, alors on peut identifier coefficient par coefficient.

On s'aperçoit qu'en additionnant ou multipliant des polynômes, on obtient encore des polynômes. Et,

Proposition 16. Soit $P, Q \in \mathbb{K}[X]$. On a $deg(P + Q) \leqslant max(deg P, deg Q)$ et $deg(PQ) = deg P + deg Q$.

Division euclidienne

Tout comme les entiers naturels, les polynômes de $\mathbb{K}[X]$ forment un ensemble (un algébriste dirait un anneau) muni d'une division euclidienne, donc avec un reste :

Proposition 17. Si $P, Q \in \mathbb{K}[X]$, il existe $S, R \in \mathbb{K}[X]$ tels que

$$P = SQ + R$$

et $deg R < deg Q$. Et bien sûr, si $R = 0$, on dit que Q divise P.

Remarques 18. Ici, c'est donc le degré du polynôme qui joue plus ou moins le rôle de l'entier naturel de la division euclidienne habituelle.
Les polynômes de degré 0 sont les fonctions constantes, excepté $P = 0$, le polynôme nul, qui est de degré $-\infty$.

L'exercice suivant permet de se familiariser avec l'application de la division euclidienne : si $deg P < deg Q$, $S = 0$ et $R = P$, sinon, si $P = a_p X^p + \cdots + a_0$ et $Q = b_q X^q + \cdots + b_0$, le premier terme de S est $\frac{a_p}{b_q} X^{p-q}$, et on continue en divisant $P - \frac{a_p}{b_q} X^{p-q} Q$ par Q.

Exercice 6 Effectuer la division euclidienne de $2X^3+5X^2+6X+1$ par X^2-3X+2.

Racines d'un polynôme

On s'aperçoit qu'une expression factorisée de la forme $a_n(X - r_1) \cdots (X - r_n)$ constitue également un polynôme (on verra ultérieurement comment relier les r_i aux coefficients a_i dudit polynôme). Elle a **l'avantage d'être très maniable** : on identifie notamment les points où elle s'annule, qui sont alors les r_i.

Définition 19. On appelle **racine** (réelle) d'un polynôme P un réel r tel que $P(r) = 0$. Leur recherche est quasi-obsessionnelle lorsqu'on étudie un polynôme.

Remarque 20. On exclura dans les énoncés suivants le cas du polynôme nul, dont tout réel est racine.

Notons le théorème fondamental suivant :

Théorème 21. Soit P un polynôme de degré n. Il admet exactement n racines complexes (non nécessairement distinctes), donc au plus n racines réelles.

La démonstration est hors de notre propos, l'intérêt est de majorer le nombre de racines éventuelles. Parfois, on peut au contraire le minorer :
Exercice 7 Montrer qu'un polynôme de degré impair a au moins une racine réelle.

On peut voir ce théorème différement :

Proposition 22. Un polynôme de degré au plus n ayant au moins $n+1$ racines est le polynôme nul (tous ses coefficients sont nuls).

La propriété suivante est d'une grande utilité :

Proposition 23. Soit P un polynôme dont a est une racine. Il existe un polynôme Q tel que $P = (X-a)Q$.

Ceci se démontre en divisant euclidiennement P par $X-a$. Obtenir des racines d'un polynôme permet ainsi de le factoriser. Certaines racines peuvent "plus" diviser le polynôme que d'autres :

Définition 24. Soit P un polynôme, on appelle racine k-ième de P un réel a tel que $(X-a)^k$ divise P, mais pas $(X-a)^{k+1}$. On dit que la **multiplicité** de ladite racine est k.

Exemple 25. Pour le degré 2, si $P(X) = aX^2 + bX + c$, on distingue 3 cas :
-si le discriminant $\Delta := b^2 - 4ac < 0$, il n'y a pas de racine réelle.
-si $\Delta = 0$, il y a une racine réelle double.
-si $\Delta > 0$, il y a deux racines réelles simples.

Exercice 8 Soit P un polynôme de degré 2008 tel que pour tout entier $k \in \{1, \cdots 2009\}$, $P(k) = \frac{1}{k}$. Calculer $P(0)$.

Polynômes symétriques élémentaires

On aborde ici la relation évoquée entre les coefficients et les racines d'un polynôme : on considère le polynôme

$$P(X) = a_n X^n + \cdots + a_0 = a_n(X-r_1)\cdots(X-r_n)$$

Définition 26. Le k-ème polynôme symétrique élémentaire est défini par

$$\sigma_k = \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} r_{i_1} \cdots r_{i_k}$$

Théorème 27. Formule de Viète Pour $0 \leqslant k \leqslant n$,

$$\sigma_k = (-1)^k \frac{a_{n-k}}{a_n}$$

Démonstration. On développe l'expression factorisée de P et on regroupe les termes faisant intervenir X^{n-k}. □

Remarque 28. Une fois les racines fixées, les polynômes symétriques élémentaires sont uniques. Réciproquement, une fois les polynômes symétriques fixés, les racines sont déterminées à permutations près. On a ainsi un autre moyen de manipuler les racines d'un polynôme.

Exemple 29. Pour le degré 2, si $P(X) = ax^2 + bx + c = a(x - r_1)(x - r_2)$, alors $\sigma_1 = r_1 + r_2 = -\frac{b}{a}$ et $\sigma_2 = r_1 r_2 = \frac{c}{a}$.

A présent, exerçons-nous !

Exercice 9 Exprimer $x^3+y^3+z^3-3xyz$ en fonction des polynômes symétriques élémentaires.

Exercice 10 Soit $A = \sqrt[3]{5 - 2\sqrt{13}} + \sqrt[3]{5 + 2\sqrt{13}}$. Simplifier cette expression.

Factorisation des polynômes

On a vu que pour factoriser un polynôme, on pouvait en chercher ses racines. Ce n'est pas toujours possible, et, de plus, elles ne sont pas forcément dans l'ensemble de départ considéré ($\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$, etc.). Dans certains cas, aucune factorisation (à multiplication par un terme constant près) n'est envisageable !

Définition 30. On dit que $P \in \mathbb{K}[X]$ est irréductible sur $\mathbb{K}$ lorsque toute expression de P sous la forme $Q \times R$ avec $Q, R \in \mathbb{K}[X]$ entraîne que Q ou R soit de degré 0.

Exemple 31. Le polynôme $X^2 + 1$ est irréductible sur $\mathbb{R}$: sinon, il s'écrirait $(X - a)(X - b)$ avec a, b réels or ses racines sont complexes.

Remarque 32. Si $\mathbb{K} \subset Ł$, il est clair que tout polynôme réductible sur $\mathbb{K}$ l'est sur Ł, mais la réciproque n'est pas toujours vraie, comme en atteste l'exemple suivant.

Exemple 33. Le polynôme $X^2 - 2$ est irréductible sur $\mathbb{Z}$ et $\mathbb{Q}$, mais pas sur $\mathbb{R}$, ses racines étant $\pm\sqrt{2}$.

On peut conjecturer que **pour un polynôme à coefficients entiers** la réductibilité est la même sur $\mathbb{Z}$ ou sur $\mathbb{Q}$, et en effet,

Théorème 34. Tout polynôme de $\mathbb{Z}[X]$ est réductible sur $\mathbb{Z}$ si et seulement s'il l'est sur $\mathbb{Q}$.

Démonstration. Soit $P \in \mathbb{Z}[X]$. S'il est réductible sur $\mathbb{Z}$, il l'est sur $\mathbb{Q}$. Réciproquement, supposons que l'on aie $P = RS$ avec $R, S \in \mathbb{Q}[X]$. Soit $a, b \in \mathbb{Z}$ tels que $aR, bS \in \mathbb{Z}[X]$.
Pour tout polynôme $p \in \mathbb{Z}[X]$, on note $c(p)$ le $pgcd$ de ses coefficients : le lecteur pourra vérifier que $c(pq) = c(p)c(q)$.
Alors $c(aR)c(bS) = c(abP) = ab \times c(P)$. Donc $P = R'S'$ avec $R' = c(P)\frac{aR}{c(aR)}$ et $S' = \frac{bS}{c(bS)}$, qui sont bien sûr des polynômes à coefficients entiers. □

Pour tester la réductibilité sur $\mathbb{Z}$, on dispose d'un critère incomplet :

Théorème 35. Critère d'Eisenstein : Soit $P = a_n X^n + \cdots + a_0 \in \mathbb{Z}[X]$, s'il existe un nombre premier p divisant tous les a_i sauf a_n, et tel que p^2 ne divise pas a_0, alors P est irréductible sur $\mathbb{Z}$.

Démonstration. Supposons par l'absurde que $P = QR$ avec $Q = b_q X^q + \cdots + b_0$ et $R = c_r X^r + \cdots + c_0$, $q, r > 1$. Sans perte de généralité, comme p, et non pas p^2, divise $a_0 = b_0 c_0$: p divise b_0 et pas c_0. Et, $a_n = b_q c_r$ donc p ne divise pas b_q.
Soit alors i_0 le plus grand indice tel que si $i \leqslant i_0$, $p | b_i$. On a :

$$a_{i_0+1} = b_0 c_{i_0+1} + \cdots + b_{i_0+1} c_0$$

et $p | a_{i_0+1}$ donc $p | c_0$: contradiction. □

Une petite application astucieuse, qui demande de (modestes) connaissances arithmétiques : **Exercice 11** Soit p un nombre premier, montrer que le polynôme $1 + X + \cdots + X^{p-1}$ est irréductible sur $\mathbb{Z}$.

Exercice 12 Soit $n \in \mathbb{N}^*$ et $a_1, \cdots, a_n$ des entiers relatifs distincts. Montrer que le polynôme

$$P(X) = 1 + \prod_{i=1}^{n}(X - a_i)$$

est irréductible sur $\mathbb{Z}$.

- Solutions des exercices -

Suites

Solution de l'exercice 1

On constate, par une récurrence rapide, que la suite est bornée par 4. On montre de même par récurrence sur n que $u_{n+1} > u_n$: l'initialisation se vérifie avec $u_1 = \sqrt{12} > 0 = u_0$. Si on suppose $a_{n+1} > a_n$, il vient $a_{n+2} = \sqrt{12 + a_{n+1}} >= a_{n+1}$, ce qui clôt la récurrence.

La suite est croissante et majorée, elle admet donc une limite l. La fonction $x \to \sqrt{12 + x}$ est continue donc $l = \sqrt{12 + l}$, soit $l^2 - l - 12 = 0$. L'unique solution positive de cette équation est 4, qui est donc la limite de la suite.

Solution de l'exercice 2

On note u_n le nombre de manières différentes de monter un escalier de n marches. Si $n \geqslant 3$, pour la première marche, soit on la franchit seule, ce qui laisse u_{n-1} possibilités, soit on en monte 2 à la fois, ce qui laisse u_{n-2} autres possibilités. L'équation de récurrence obtenue est donc

$$u_{n+2} - u_{n+1} - u_n = 0$$

pour tout $n \in \mathbb{N}^*$. L'équation caractéristique associée $X^2 - X - 1 = 0$ a pour solutions $\Phi = \frac{1+\sqrt{5}}{2}$ et $\varphi = \frac{1-\sqrt{5}}{2}$, donc pour $n \in \mathbb{N}^*$,

$$u_n = A\Phi^n + B\varphi^n.$$

Avec $u_1 = 1$ et $u_2 = 2$, on trouve : $A = \frac{1+\sqrt{5}}{2\sqrt{5}}$ et $B = \frac{\sqrt{5}-1}{2\sqrt{5}}$.

Solution de l'exercice 3

• Si (u_n) est strictement croissante, on a pour tout $n \geqslant 1$: $u_{n+1} \geqslant u_n + 1$ donc $u_2 = u_{2n} - u_n \geqslant n$, ce qui est absurde pour $n > u_2$. Donc une telle suite n'existe pas.

• Si (u_n) est simplement croissante, c'est plus délicat. La suite nulle est clairement solution. Pour montrer que c'est la seule solution, on raisonne de nouveau par l'absurde et on suppose $u_k > 0$ pour un certain k. On sait que la suite

ne peut être strictement croissante, donc il existe $m \in \mathbb{N}^*$ tel que $u_m = u_{m+1}$. Le lecteur prouvera par récurrence sur $j \geqslant 1$ que

$$u_{n^j} = j \times u_n.$$

De ceci résulte que pour tout $j \in \mathbb{N}^*$, $u_{m^j} = u_{(m+1)^j}$.
Or $\frac{m+1}{m} > 1$ donc pour un certain $i \in \mathbb{N}^*$, $(m+1)^i \geqslant m^i \times k$ donc par croissance de la suite,

$$u_{(m+1)^i} \geqslant u_{m^i} + u_k > u_{m^i}$$

d'où une contradiction.
On peut donc définir u_2/u_3. Pour tout entier strictement positif n, il existe k tel que $3^k < 2^n < 3^{k+1}$, or par récurrence sur n, on a $u_{3^k} = ku_3$ et de même $u_{2^n} = nu_2$, donc $ku_3 \leqslant nu_2 \leqslant (k+1)u_3$, d'où

$$\frac{k}{n} \leqslant \frac{u_2}{u_3} \leqslant \frac{k+1}{n}$$

Si $n = u_3$, on a $u_2 \in \{k, k+1\}$, supposons $u_2 = k$. On a alors :

$$u_{3^k} = u_{2^n}$$

Donc pour tout $m \geqslant 1$, $u_{3^{km}} = u_{2^{km}}$. Or, pour un certain $m_0 \in \mathbb{N}^*$, $(2^n/3^k)^{m_0} > 3$ car $2^n/3^k > 1$. Donc $2^{nm_0} > 3^{km_0+1}$ donc :

$$u_{2^{nm_0}} \geqslant u_{3^{km_0+1}} \geqslant u_3 + u_{3^{km_0}} \geqslant u_3 + u_{2^{km_0}} > u_{2^{nm_0}}$$

car $u_3 > u_1 = 0$. On obtient la contradiction voulue.

On procède de même si $u_2 = k+1$.

Solution de l'exercice 4

Supposons par l'absurde que pour tout $n \in \mathbb{N}$, a_n est rationnel, ce que l'on écrit $a_n = \frac{p_n}{q_n}$ avec $p_n \in \mathbb{Z}$, $q_n \in \mathbb{Z}^*$ premiers entre eux. On a :

$$\frac{p_{n+1}^2}{q_{n+1}^2} = \frac{p_n + q_n}{q_n}$$

et $p_n + q_n$ et q_n sont premiers entre eux, et p_{n+1}^2 et q_{n+1}^2 aussi, donc on peut identifier le numérateur et le dénominateur des deux fractions (au signe près). Il en résulte que $|\sqrt{q_n}| = |q_{n+1}|$ et finalement : $|q_n| = \sqrt[1/2^n]{|q_0|} \in \mathbb{N}^*$ pour tout entier naturel n. On en déduit que $|q_0| = 1 = |q_n|$ autrement dit, la suite est constituée d'entiers, qui sont alors positifs (car racines carrées de réels). Or

$a_1 > 1$ donc $a_n > 1$ par récurrence, soit $a_n \geqslant 2$, auquel cas on vérifie que $a_n > \sqrt{1+a_n} = a_{n+1}$. Donc (a_n) est une suite infinie décroissante d'entiers strictement positifs, ce qui est impossible.
Conclusion : la suite admet un terme irrationnel.

Solution de l'exercice 5 La suite (u_n) étant clairement à termes positifs, il suffit de montrer que $u_{1000}^2 > 2025$. Or,

$$u_{n+1}^2 = u_n^2 + 2 + \frac{1}{u_n^2} > u_n^2 + 2$$

Donc $u_{1000}^2 > 1000 \times 2 + u_0 = 2025$.
Il est naturel d'être frustré et bluffé par une telle solution. Pour ceux qui voudraient un petit peu plus de réflexion et de calcul, on peut explorer les cas $u_0 = 4, 3$, etc.

Polynômes

Solution de l'exercice 6
Avec les notations du cours : $S = 2X + 11$ et $R = 35X - 21$.

Solution de l'exercice 7
En $+\infty$ et $-\infty$, le polynôme a des limites infinies (car non constant) et de signe opposé (car c'est le terme dominant qui l'emporte à l'infini, et c'est une puissance impaire). D'après le théorème des valeurs intermédiaire, un polynôme étant continu, le polynôme a une racine réelle.

Solution de l'exercice 8
On cherche un polynôme proche de P que l'on puisse déterminer en utilisant ses racines. Si $1 \leqslant k \leqslant 2009$, on a :

$$kP(k) - 1 = 0,$$

donc si on pose $Q(X) = XP(X) - 1$, Q est de degré 2009, donc on a trouvé toutes ses racines et il existe $A \in \mathbb{R}$ tel que

$$Q(X) = A(X-1)\cdots(X-2009).$$

En faisant $X = 0$ on trouve $-1 = A \times (-1)^{2009} \times 2009!$, donc $A = \frac{1}{2009!}$. On a donc

$$P(X) = \frac{2009! + (X-1) + \cdots (X-2009)}{2009!X}$$

(pour avoir un polynôme, on a bien pris soin par le choix de A que le dénominateur divise le numérateur !). On cherche $P(0)$ qui est le terme constant, donc on cherche le terme de degré 1 dans le numérateur. En développant, il vient : $P(0) = \frac{2009!/2009+2009!/2008+\cdots+2009!/1}{2009!}$ donc $P(0) = \sum_{k=1}^{2009} \frac{1}{k}$. *Solution de l'exercice 9*

On obtient $x^3 + y^3 + z^3 = \sigma_1(\sigma_1^2 - \sigma_2)$.

Solution de l'exercice 10

On pose $a = \sqrt[3]{5 - 2\sqrt{13}}$ et $b = \sqrt[3]{5 + 2\sqrt{13}}$. On a

$$\begin{aligned} A^3 &= a^3 + b^3 + 3ab(a + b) \\ A^3 &= 10 + 3\sqrt[3]{25 - 52}A \\ A^3 &= 10 - 9A \\ A^3 + 9A - 10 &= 0 \end{aligned}$$

On a affaire à un polynôme de degré 3 dont 1 est racine évidente. On factorise :

$$A^3 + 9A - 10 = (A - 1)(A^2 + A + 10)$$

Le polynôme de degré 2 ci-dessus n'a pas de racine réelle, on en déduit $A = 1$.

Solution de l'exercice 11

Selon la subtile suggestion de l'enchaînement du cours, l'application du critère d'Eisenstein avec le nombre premier p permet de résoudre le problème. Notons déjà que l'on peut écrire $P(X) = \frac{X^p - 1}{X - 1}$ puisqu'il s'agit d'une somme géométrique. Pour faire apparaître p, on procède (astuce suprême) à un petit changement de variable en posant $Y = X - 1$ et en développant avec le binôme de Newton :

$$P(Y) = \frac{(Y + 1)^n - 1}{Y} = \sum_{k=1}^{p} \binom{p}{k} Y^{k-1}$$

On vérifie aisément que $P(Y)$ se factorise dans $\mathbb{Z}[Y]$ si et seulement si $P(X)$ se factorise dans $\mathbb{Z}[X]$. Notons donc, pour $0 \leqslant k \leqslant p - 1$, $c_k = \binom{p}{k+1}$. On a $c_0 = p$, donc il est divisible par p, et pas par p^2. $c_{p-1} = 1$ qui n'est pas multiple de p. Il reste donc à prouver que pour $2 \leqslant k \leqslant p - 1$, $p | \binom{p}{k}$. Or,

$$p! = \binom{p}{k} \times ((p - k)!k!).$$

Or p, premier, divise $p!$ et non pas $(p-k)!k!$, donc par le lemme d'Euclide, $p|\binom{p}{k}$, ce qui (par)achève la démonstration.

Solution de l'exercice 12

Remarquons que sans perte de généralité, quitte à permuter les a_i, on peut supposer que

$$a_1 < \cdots < a_n.$$

Une fois n'est pas coutume, on raisonne par l'absurde. Supposons que $P = QR$ avec $Q, R \in \mathbb{Z}[X]$. P étant de degré n, Q et R sont de degré au plus $n-1$. Pour tout i, $Q(a_i)R(a_i) = 1$, donc $Q(a_i) = R(a_i) = \pm 1$. Autrement dit, le polynôme $R - Q$ a au moins n racines distinctes, or il est de de degré au plus $n-1$ (car c'est le cas de R et Q). Donc $R - Q = 0$, donc $P = R^2 + 1$. Il en découle que pour tout réel x :

$$P(x) - 1 = R^2(x) \geqslant 0.$$

Or $P - 1$ change de signe (sans s'annuler) entre $]-\infty, a_1[$ et $]a_1, a_2[$: contradiction. Donc P est irréductible sur $\mathbb{Z}$.

Remarque : on a supposé à la fin du raisonnement que $n \geqslant 2$, mais si $n = 1$, un polynôme de degré 1 est toujours irréductible.