6. TECHNIQUES COMBINATOIRES, POLYNÔMES

1 Un peu d'arithmétique.

Bien que les propriétés des entiers, très élémentaires au demeurant, que nous allons examiner, soient en principe hors-programme, les méthodes de raisonnement qui suivent constituent une gymnastique utile; de plus, ce type d'analyse intervient très fréquemment en informatique (théorique), et il semble donc prudent de se familiariser avec elle; enfin, nous verrons à la fin de ce chapitre que ces propriétés se généralisent en partie aux polynômes.

1.1 Divisibilité.

Les premières propriétés «non évidentes» de l'arithmétique des entiers portent sur la divisibilité : on dit que a *divise* b (noté parfois $a \mid b$, et la non divisibilité se note $a \not| \ b$) si b/a est entier. Les nombres qui divisent a s'appellent les *diviseurs* de a; et les nombres «sans diviseurs» (ou plus précisément divisibles seulement par 1 et eux-mêmes) sont les nombres *premiers*; par convention, 1 n'en fait pas partie, et la liste des nombres premiers est donc $(2, 3, 5, 7, 11, 13, 17, \ldots)$; on a vu au chapitre 1 le raisonnement par l'absurde (dû à Euclide) qui prouve qu'elle est infinie. Pour étudier ce genre de questions, les méthodes algébriques sont généralement tout à fait insuffisantes; l'utilisation de la notation $b = ad$ pour dire que a divise b ne permet de prouver que des résultats très élémentaires, tels que la «transitivité» : $a \mid b$ et $b \mid c \Rightarrow a \mid c$; plus généralement, résoudre des équations dans $\mathbf{N}$ ou dans $\mathbf{Z}$ (qu'on appelle traditionnellement des équations diophantiennes) est extrémement difficile en général (qu'on pense au grand théorème de Fermat) et nécessite le plus souvent des méthodes différentes pour chaque équation !

1.2 L'algorithme d'Euclide.

Pour aller plus loin dans l'étude des question de divisibilité, on introduit d'abord la «division euclidienne» : c'est la division «avec reste», c'est-à-dire que $a = bq + r$ est la division euclidienne de a par b si r (entier positif) est $< b$ (q s'appelle le *quotient* (euclidien) et r le *reste*. (Une preuve d'existence et d'unicité sera donnée en classe, elle repose sur l'encadrement de a/b par des entiers). La recherche de diviseurs communs à a et b amène alors à remarquer qu'ils divisent aussi r (plus précisément, les diviseurs communs à a et b sont ceux communs à b et r); on en déduit une méthode (par divisions successives) de recherche du plus grand diviseur commun à a et b (le PGCD de a et b) :

Algorithme d'Euclide (on suppose $a > b$)

1) Poser $(a_0, b_0) = (a, b)$
2) Division euclidienne : $a_n = b_n q + r_n$
3) Si r_n est nul, b_n est le PGCD, Sinon
4) Poser $a_{n+1} = b_n ; b_{n+1} = r_n$ et aller à 2)

(les notations indicées utilisées ici seront précisées en **2.1**)

En fait, cette technique apporte d'autres renseignements; on verra en classe sur un exemple comment en déduire le «théorème de Bezout» : a et b premiers entre eux ($\mathrm{PGCD}(a, b) = 1$) $\iff$ (il existe p et q dans $\mathbf{Z}$ tels que $ap + bq = 1$), ce qui parmet de résoudre l'équation $ax + by = c$ (avec $x, y \in \mathbf{Z}$).

On peut alors prouver l'unicité de la décomposition en facteurs premiers, c'est-à-dire le fait que l'écriture de n comme produit de facteurs premiers est unique (à l'ordre des facteurs près); on se convaincra qu'elle n'était pas «intuitivement» évidente !

2 Suites d'objets.

2.1 Les notations.

On vient de voir un exemple où on est amené à effectuer une suite d'opérations répétitives; il arrive également qu'on veuille définir une suite d'objets (chaque objet dépendant par exemple du précédent); dans tous les cas de ce genre, la $n^{\text{ème}}$ valeur (ou le $n^{\text{ème}}$ objet) est notée par une notation indicée telle que x_n (la $n^{\text{ème}}$ valeur prise par x), $P_n(x)$ (le $n^{\text{ème}}$ polynôme), etc... On notera que n est une véritable variable (mais ne prenant que des valeurs entières); et on convient (bien qu'il puisse y avoir quelques exceptions)

a) que $n = 0$ est possible (et donc une suite «commence au zéro$^{\text{ème}}$ objet» !);

b) qu'à chaque valeur de n correspond un objet (il n'y a pas de «valeurs interdites» pour n, en d'autres termes le domaine de validité (pour n) est $\mathbf{N}$ tout entier)

c) que si on appelle S une suite, ses «valeurs» (les termes de S) sont notées $S_0, S_1, \ldots$ et on utilise une notation de mise entre parenthèses des valeurs : $S = (S_0, S_1, S_2, \ldots)$ ou encore $S = (S_n)$ (éventuellement en précisant en indice les valeurs de n dans les cas exceptionnels tels que $S = (S_n)_{n>0}$).

Ainsi, soit P la suite des nombres premiers. On a donc $P_0 = 2$; $P_5 = 13$; et on s'exercera par exemple à traduire en français la «définition» suivante : $(P_n ; P_{n+1})$ est un couple de nombres premiers *jumeaux* si $P_{n+1} - P_n = 2$.

2.2 Comment définir une suite.

Les suites les plus simples sont définies par une formule telle que $x_n = \dfrac{\cos n}{n^2 + 1}$. En effet, même si la formule est très compliquée, il n'en reste pas moins qu'on peut accéder à la valeur de n'importe quel terme sans calculer les autres : on dit qu'une telle suite est définie par une formule *explicite* (dont le domaine de définition doit être $\mathbf{N}$, ou à la rigueur $\mathbf{N}^*$); bien que ces suites «ressemblent» à des fonctions numériques,

on se gardera toutefois de croire qu'un prolongement (intéressant) à $\mathbf{R}$ existe toujours, comme on le verra plus loin pour la suite $(n!)$.

Mais le plus souvent, on rencontre des suites définies de proche en proche, c'est-à-dire que chaque terme dépend des précédents (le terme technique est «définies par récurrence»); telles que, par exemple,

— les suites «définies par *itération* d'une fonction f» : $u_{n+1} = f(u_n)$, par exemple la suite $s = (0; 1; 1,4142\ldots; 1,5537\ldots; \cdots)$ définie par $s_{n+1} = \sqrt{1+s_n}$ (c'est le type de suite le plus souvent utilisé en Analyse);

— les suites où chaque terme est obtenu en «combinant» les termes précédents, telle la suite de Fibonacci $F = (1, 1, 2, 3, 5, 8, 13, 21, \ldots)$ (c'est ce genre de suite qui rend nécessaire une notation précise, car il n'est peut-être pas toujours évident de deviner le sens des $\ldots$), définie par $F_{n+2} = F_{n+1} + F_n$;

et des suites bien plus «irrégulières» telle la suite P des nombres premiers : pour calculer P_{1000}, par exemple, il faut entre autre calculer tous les nombres premiers précédents, et aucune formule explicite évitant ce travail n'a jamais été trouvée ! Dans de tels cas, on est déjà heureux de découvrir des formules approchées; Gauss avait conjecturé que $P_n \simeq n \ln n$, ce qui ne fut démontré rigoureusement qu'un siècle plus tard !

3 Sommations.

3. 1 Notations et manipulations élémentaires.

On est souvent amené à effectuer des opérations sur tout un groupe de nombres (ou d'objets), les plus fréquentes étant la somme et le produit des éléments du groupe. Des notations particulières ont donc été développées dans ce but; si les objets s'appellent par exemple $a_0, a_1, \ldots, a_n$, leur somme $a_0+a_1+\cdots+a_n$ sera notée $\sum_{i=0}^{n} a_i$, ce qui se lit : «somme de $i = 0$ à n de a_i»; une notation analogue existe aussi pour les produits : $a_0 \times a_1 \times \cdots \times a_n$ se note $\prod_{i=0}^{n} a_i$ (et se lit «produit de $i = 0$ à n de a_i»). Plus précisément, $\sum_{k=p}^{q} f(k)$ désigne la somme $f(p)+f(p+1)+\cdots+f(q-1)+f(q)$ (si $q-p$ est assez grand), et on emploie parfois la notation encore plus générale $\sum_{k \text{ ayant la propriété } \mathcal{P}(k)} f(k)$.

On peut obtenir aisément des formules de transformation de ces expressions qui ne font que «coder» l'associativité de l'addition, par exemple; on retiendra :

$$\sum_{i=0}^{k} a_i + \sum_{i=k+1}^{n} a_i = \sum_{i=0}^{n} a_i$$

$$\sum_{i=0}^{n} a_i + \sum_{i=0}^{n} b_i = \sum_{i=0}^{n} (a_i + b_i)$$

$$\sum_{i=0}^{n} a_i = \sum_{i=0}^{n} a_{n-i}$$

(Cette dernière formule signifiant simplement qu'on peut ajouter les termes en partant du dernier !)

De manière un peu plus délicate, on examinera avec attention la façon de «décaler» une suite : le changement de variable $I = i + 1$ conduit (la technique sera précisée en cours) à

$$\sum_{i=0}^{n} a_i = \sum_{i=1}^{n+1} a_{i-1} \ ;$$

l'un des points-clés de la méthode est le fait que i n'est dans toutes ces notations qu'une variable «muette», c'est-à-dire que l'expression finale «ne contient pas i», et par conséquent qu'on a :

$$\sum_{i=0}^{n} a_i = \sum_{j=0}^{n} a_j \quad \text{(par exemple)}$$

On peut aussi traduire la formule classique de distributivité par :

$$k \sum_{i=0}^{n} a_i = \sum_{i=0}^{n} k a_i$$

mais l'expression du produit de deux sommes nécessite une notation plus générale, que l'on verra en **3. 3**.

3. 2 Progressions arithmétiques et géométriques.

Un exemple important de l'utilisation de ces notations et de ces formules est le calcul des sommes (finies) de termes d'une suite arithmétique : si $a_i = a_0 + ki$ (c'est-à-dire que a_n est une suite arithmétique (de premier terme a_0 et de raison k)), on peut écrire $\sum_{i=0}^{n} a_i = \sum_{i=0}^{n} a_{n-i} = S$, donc $2S = \sum_{i=0}^{n} (a_i + a_{n-i})$, et comme $a_i + a_{n-i} = 2a_0 + ki + k(n-i) = 2a_0 + kn$, on voit que $S = (\sum_{i=0}^{n} 2a_0 + kn)/2$; comme tous ces termes sont égaux, et qu'il y en a $n+1$, on obtient $S = (n+1)(2a_0 + kn)/2$ ou encore $S = (n+1)(a_0 + a_n)/2$.

De même, on peut obtenir «rigoureusement» la démonstration de l'identité des suites géométriques du chapitre 4 : posant $S = \sum_{i=0}^{n} x^i$, on voit que $xS = \sum_{i=0}^{n} x^{i+1} = \sum_{i=1}^{n+1} x^i$, et donc que $(x-1)S = x^{n+1} - 1$ (en remarquant que tous les termes sont nuls sauf ceux des bornes). On verra dans l'exercice-type n° 8 qu'une méthode analogue permet par exemple de calculer $\sum_{i=0}^{n} i x^i$.

3. 3 Sommes doubles.

On est parfois amené à sommer des termes dépendant de deux indices; ainsi, si on veut calculer $\sum_{i=0}^{n} a_i \times \sum_{i=0}^{n} b_i$, on voit qu'on doit sommer tous les produits $a_i.b_j$ (pour tous les indices i et j), ce qui oblige à une nouvelle notation : on écrira :

$$\sum_{i=0}^{m} a_i \times \sum_{j=0}^{n} b_j = \sum_{\substack{0 \le i \le m \\ 0 \le j \le n}} a_i b_j$$

Des variations sont possibles, ainsi dans la formule précédente, si $m = n$, on écrira simplement

$$\sum_{0\leq i,j\leq n} a_i b_j$$

et la notation

$$\sum_{0\leq i<j\leq n} a_i/b_j$$

signifie qu'il faut sommer pour tous les couples (i, j) tels que $i < j$. Un exemple (délicat) de manipulation de ces notations est la formule donnant le produit de deux polynômes, qui sera vue en **6. 1**

Ces sommations peuvent être interprétées comme des sommes de sommes, en gardant un des deux indices fixé : on a la formule presque évidente

$$\sum_{\substack{0\leq i\leq m\\ 0\leq j\leq n}} a_{ij} = \sum_{i=0}^{m}\sum_{j=0}^{n} a_{ij} = \sum_{j=0}^{n}\sum_{i=0}^{m} a_{ij}$$

Une analyse un peu plus soignée montre que

$$\sum_{0\leq i<j\leq n} a_{ij} = \sum_{j=1}^{n}\sum_{i=0}^{j-1} a_{ij}$$

Ces formules, outre les manipulations qu'elles permettent, et dont on verra des exemples lors des calculs matriciels (aux chapitres 17 et 20) sont aussi liées au calcul explicite : dans des programmes informatiques, il s'agit de ce qu'on appelle des «boucles imbriquées».

4 La formule du binôme.

4. 1 Factorielles.

On définit d'abord une notation abrégée pour le produit des n premiers entiers consécutifs : $1 \times 2 \times \cdots \times n = \prod_{i=1}^{n} i$ est noté $n!$, ce qui se lit factorielle (de) n. Dans les écritures qui l'utilisent, le calcul de la fonction «factorielle» a priorité; on s'en rappelera mieux en imaginant qu'il s'agit en fait d'une sorte d'exponentiation, et qu'on aurait donc pu l'écrire $n^!$. Ainsi, on a donc $(n + 1)! = (n + 1)n!$; en utilisant cette formule, on peut (conventionnellement) prolonger la notation à $0! = 1$ (mais il n'est pas possible de la prolonger à $\mathbf{Z}$).

La fonction «factorielle» a une croissance très rapide : on a $5! = 120$, $8! = 40320$, $20! \simeq 2.43\ 10^{18}\ldots$; une formule (due à Stirling) permet d'en connaître des valeurs approchées quand n est grand : $n! \sim n^n e^{-n}\sqrt{2\pi n}$ (le sens exact de $\sim$ sera vu au chapitre 11, et une démonstration de la formule sera donnée au chapitre 13).

D'autres produits d'entiers peuvent s'exprimer à l'aide de factorielles : on a (évidemment) $k(k+1)(k+2)\cdots(n-1)n = n!/(k-1)!$; on verra en classe (la méthode est rappelée dans l'exercice-type n° 17, où elle intervient pour simplifier l'écriture d'une

dérivée) comment transformer le produit $1 \times 3 \times 5 \times 7 \times \cdots \times (2k-1)$ pour obtenir $(2k)!/2^k k!$.

Ces nombres interviennent surtout dans des problèmes de «dénombrement», ainsi, on montrera en classe que le nombre de permutations (c'est-à-dire d'ordres possibles) d'un ensemble de n objets est $n!$, que le nombre de «mots» de k lettres distinctes prises parmi n est $n!/(n-k)!$, et que le nombre de sous-ensembles différents contenant k objets parmi n donnés est $n!/k!(n-k)!$, qui se note $\binom{n}{k}$ (on le notait autrefois C_n^k); ces derniers nombres, appelés coefficients du binôme, ou *coefficients binomiaux*, à cause de leur rôle dans la formule de Newton, apparaissent dans de nombreuses formules mathématiques, et il est commode de connaître quelques valeurs simples ($\binom{n}{0} = \binom{n}{n} = 1$, $\binom{n}{1} = \binom{n}{n-1} = n$, et $\binom{n}{2} = \dfrac{n(n-1)}{2}$), et d'avoir remarqué que par «symétrie» on a $\binom{n}{k} = \binom{n}{n-k}$. On verra aussi en exercice que

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}.$$

4. 2 Formule de Newton.

La dernière formule du paragraphe précédent permet de calculer «de proche en proche» les coefficients du binôme : on obtient ainsi le «triangle de Pascal». Analysant la façon dont s'obtiennent les coefficients des identités remarquables $(a+b)^2$, $(a+b)^3$, etc..., on découvre qu'ils suivent la même règle, d'où la formule de Newton (ou formule du binôme)

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i$$

dont une démonstration rigoureuse nécessite un raisonnement par récurrence, d'ailleurs assez technique; on le verra en travaux dirigés.

En pratique, si n est inférieur à 10, on a intérêt à utiliser directement le triangle de Pascal; la formule de Newton ne s'utilise sous cette forme que pour n «quelconque».

4. 3 Applications.

La formule du binôme se généralise d'abord à d'autres identités analogues :

$$(a-b)^n = \sum_{i=0}^{n} (-1)^i \binom{n}{i} a^{n-i} b^i;$$

d'autre part, en prenant des valeurs particulières pour a et b, on obtient des relations intéressantes entre les $\binom{n}{i}$, ainsi la somme des coefficients binomiaux vaut 2^n (en prenant $a = b = 1$) et leur différence alternée ($\sum_{i=0}^{n} (-1)^i \binom{n}{i}$) est nulle (en prenant $a = 1, b = -1$). Enfin, l'identité du binôme est valable **même dans C**[†]; ce qui permet (en prenant par exemple $a = 1$ et $b = i$) d'obtenir des formules moins évidentes, telles que $\binom{n}{0} - \binom{n}{2} + \binom{n}{4} - \cdots + (-1)^{n/2} \binom{n}{n} = 2^{n/2} \cos \dfrac{n\pi}{4}$.

[†] On verra aux chapitres 16 et 17 qu'on peut même la généraliser encore, par exemple aux matrices lorsqu'elles commutent.

5 Le raisonnement par récurrence.

5. 1 Cas élémentaires.

Pour de nombreuses suites d'objets, il est difficile de prouver directement une propriété générale, parce qu'on ne connait pas de formule explicite pour le $n^{\text{ème}}$ terme. Si l'on dispose d'une méthode de construction d'un terme à partir des précédents, il est toutefois possible de démontrer la propriété cherchée «de proche en proche» en la vérifiant d'abord pour les termes initiaux, et en montrant ensuite qu'elle est «héréditaire», c'est-à-dire que la méthode de construction garantit qu'elle est vraie d'un terme quand elle est vraie des précédents. On a vu au chapitre 1 qu'une telle démonstration s'appelait une démonstration *par récurrence*; cette méthode, comme on l'a dit, ne s'applique pas seulement aux suites, mais à toute propriété des entiers pour laquelle on pense avoir une relation entre la vérité pour un n donné et celle pour le suivant $(n+1)$; la formulation rigoureuse et un exemple typique (mais, volontairement, ne portant pas explicitement sur une suite, quoiqu'il serait aisé de le rédiger dans ces termes) sont donnés dans l'encadré suivant :

Pour démontrer par récurrence une propriété $\mathcal{P}(n)$

1) Annoncer le projet («on va démontrer par récurrence que ... »).

2) Vérifier que la propriété est vraie pour 0 («$\mathcal{P}(0)$ est vraie car... »).

3) Montrer que si $\mathcal{P}$ est vraie pour k, elle est encore vraie pour $k+1$: c'est en principe la partie délicate du raisonnement, et elle se présente sous la forme : «Supposons que $\mathcal{P}(k)$ soit vraie (pour un certain k fixé) (ce qu'on appelle l'hypothèse de récurrence), alors ....., ce qui prouve $\mathcal{P}(k+1)$» (ou «... ce qui équivaut à $\mathcal{P}(k+1)$»).

4) Conclure : «par récurrence, $\mathcal{P}(n)$ est donc vraie pour tout n».

Un exemple

Montrons (par récurrence) que $(1+a)^n \geq 1+na$ (a réel > -1, n entier.)

1) L'inégalité est (évidemment) vraie pour $n=0$, puisque $(1+a)^0 = 1 = 1+0.a$.

2) Supposons qu'elle soit vraie pour $n=k$, c'est-à-dire (hypothèse de récurrence) que $(1+a)^k \geq 1+ka$; on aura alors $(1+a)^{k+1} = (1+a)(1+a)^k \geq (1+a)(1+ka) = 1+(k+1)a+ka^2 \geq 1+(k+1)a$, ce qui est bien l'inégalité pour $n = k+1$.

3) Par récurrence, l'inégalité est donc vraie pour tout n.

5. 2 Applications, récurrences «généralisées».

Comme on l'a dit, la partie délicate est le passage de k à $k+1$, et en général, ce mode de démonstration ne doit être envisagé que si une démonstration directe semble impossible, ce qui correspond surtout au cas où les objets étudiés sont eux-mêmes définis par récurrence. Ainsi, par exemple, montrer qu'une suite est croissante

revient à prouver que (pour tout n) $u_n < u_{n+1}$; si u_{n+1} est fonction de u_n, on est tenté d'étudier cette fonction (pour démontrer que $f(x) > x$). Mais il sera souvent plus simple de bâtir un raisonnement par récurrence du type : « $u_0 < u_1$; f étant croissante, si $u_k < u_{k+1}$, alors $f(u_k) < f(u_{k+1})$, c'est-à-dire que $u_{k+1} < u_{k+2}$, donc... »

On doit parfois modifier un peu le modèle de raisonnement qu'on vient de voir. Tout d'abord, certaines propriétés ne sont vraies «qu'à partir d'un certain rang», c'est-à-dire pour $n \geq n_0$. On adapte alors la première étape en disant : $\mathcal{P}(n_0)$ est vraie (puisque ...), et on conclut par : donc, par récurrence à partir de n_0, $\mathcal{P}(n)$ est vraie. Dans d'autres cas, et tout particulièrement pour des suites définies par récurrence à partir de plusieurs termes (par exemple la suite de Fibonacci), on devra adopter comme «hypothèse de récurrence» : supposons que la propriété soit vraie pour tous les $i \leq k$... ; on parle alors de récurrence *cumulative*. Un exemple (un peu artificiel) est analysé dans l'exercice-type n° 9, et on trouvera un tableau-résumé des différents modèles de récurrence, accompagnés de quelques exemples plus «naturels», à la fin de la fiche d'exercice-type n° 18.

6 Polynômes.

6.1 Définitions et notations.

Nous avons à présent les moyens de définir rigoureusement les polynômes (à coefficients réels par exemple) : ce sont les expressions de la forme $P(X) = \sum_{i=0}^{n} a_i X^i$ (avec a_i réel). On dit que P est un *polynôme à une variable* (X est traditionnel) ; l'ensemble de tous ces polynômes se note $\mathbf{R}[X]$. De même, on note $\mathbf{C}[X]$ l'ensemble de tous les polynômes à coefficients complexes (c'est-à-dire ceux pour lesquels $a_i \in \mathbf{C}$) ; on a (bien sûr) $\mathbf{R}[X] \subset \mathbf{C}[X]$.

Des généralisations à plusieurs variables sont possibles, mais nous n'étudierons ici que le cas où il n'y a qu'une variable notée X ; la notation (par substitution) $P(y)$, par exemple, présente donc en fait certaines difficultés logiques, de peu d'importance pratique.

De même, il faudrait en toute rigueur distinguer les expressions polynomiales (qui sont en somme une liste d'instructions de calcul, applicables à n'importe quel ensemble d'objets, comme on le verra au chapitre 17) et les fonctions de la forme $x \mapsto P(x)$, appelées *fonctions polynômes* (en utilisant la définition rigoureuse du prochain chapitre). Mais il s'agit là d'une rigueur excessive à ce niveau, et la confusion est autorisée (pour ne pas dire encouragée) par les programmes officiels...

Si on écrit $P(X)$ sous la forme $\sum_{i=0}^{n} a_{n-i} X^{n-i}$ (qui est équivalente à la précédente d'après la formule d'inversion d'ordre des termes), on dit qu'on a écrit (ou ordonné) P suivant les puissances décroissantes ; on suppose naturellement que a_n est non nul (sauf si $P = 0$...) ; n s'appelle le *degré* de P et se note $\mathrm{d}^\circ(P)$ (on convient généralement que $\mathrm{d}^\circ(0)$ n'existe pas, ou vaut $-\infty$).

De façon analogue, le plus petit i pour lequel a_i n'est pas nul s'appelle la *valuation* de P, et se note $\mathrm{val}\,(P)$ (et on convient encore que $\mathrm{val}\,(0)$ n'existe pas, ou vaut $+\infty$). L'écriture $P(X) = \sum_{i=\mathrm{val}(P)}^{\mathrm{d}^\circ(P)} a_i X^i$ s'appelle rangement de P suivant les puissances croissantes.

Avec ces notations, les opérations classiques peuvent être exprimées rigoureusement : $P(X)+Q(X)=\sum_{i=0}^{p} a_iX^i+\sum_{i=0}^{q} b_iX^i=\sum_{i=0}^{n}(a_i+b_i)X^i$ où n est le plus grand (le «sup») des deux entiers p et q. Mais en réalité, cette écriture est illégale, sauf à utiliser la convention commode que $a_i=0$ pour tous les i supérieurs à $\mathrm{d}^\circ(P)$. De même, le produit PQ (on omet souvent la variable X) est donné par $P(X)Q(X)=\sum_{i=0}^{p} a_iX^i\sum_{i=0}^{q} b_iX^i$, qui vaut, comme on l'a vu,

$$\sum_{\substack{0\leq i\leq p\\0\leq j\leq q}} a_ib_jX^{i+j}$$

En réalité, cette dernière écriture n'est pas réduite : pour un k donné, plusieurs termes contribuent au coefficient de X^k, et si on pose $P(X)Q(X)=\sum_{k=0}^{p+q} c_kX^k$, une analyse soignée montre que $c_k=\sum_{i=0}^{k} a_ib_{k-i}$

On vient de voir que $\mathrm{d}^\circ(PQ)=\mathrm{d}^\circ(P)+\mathrm{d}^\circ(Q)$; il n'y a pas de formule aussi simple pour les sommes (parce que les termes de plus haut degré pourraient se compenser) ; on peut dire seulement que $\mathrm{d}^\circ(P+Q)\leq\max(\mathrm{d}^\circ(P),\mathrm{d}^\circ(Q))$.

6. 2 Divisibilité, méthode de Horner.

La division de polynômes (au sens habituel) aboutit à des «fractions rationnelles» (dont l'étude détaillée sera faite dans l'interlude suivant le chapitre 12) ; pour obtenir une division «exacte», il faut passer par un reste : on définit la *division euclidienne* de P par Q comme l'écriture (unique) $P=DQ+R$, où R est un polynôme tel que $\mathrm{d}^\circ(R)<\mathrm{d}^\circ(Q)$. Il est relativement facile (en analysant la différence (nulle) de deux telles écritures) de montrer l'unicité ; l'existence se prouve par récurrence (c'est une démonstration délicate et très technique, qui ne sera qu'esquissée en classe). D s'appelle le quotient, et R le reste ; si R est nul, on dit que P est divisible par Q.

La détermination concrète de D et R se fait en «posant» la division (comme pour une division classique d'entiers), c'est même cette méthode qui donne l'idée de la preuve mentionnée plus haut. Le cas particulier où Q est de la forme $X-a$ peut être traité de manière plus efficace : c'est ce qu'on appelle la *méthode de Horner* : écrivant en tableau les coefficients de P, un «algorithme» de décalages (qu'on verra en classe) donne les coefficients de D et la valeur de R (qui est dans ce cas une constante, égale à $P(a)$) ; et on en déduit une preuve simple du théorème classique de factorisation par les «racines évidentes» : $P(X)=(X-a)Q(X)\iff P(a)=0$.

Cette méthode permet donc de calculer $P(a)$; on constate qu'elle est en fait plus efficace que la méthode «évidente» ; ainsi, cela revient à écrire $3x^5+x^4-2x^2+x-3$ sous la forme : $((((3x+1)\times x\times x)-2)x+1)x-3$, n'effectuant que 5 multiplications au lieu de 11. C'est ce qu'on appelle le schéma de Horner de P.

On peut d'ailleurs encore améliorer ce résultat dans certains cas particuliers ; ainsi x^8 (qui est calculé en 7 multiplications par le schéma de Horner) peut être calculé comme $((x^2)^2)^2$, ce qui n'en demande que 3 ! Ce genre de recherche d'optimisation constitue une branche entière de l'informatique : la *théorie de la complexité*.

D'autres formules analogues peuvent être obtenues en redivisant le quotient, aboutissant par exemple à $P(x)=c_0+c_1(x-a)+c_2(x-a)^2+\ldots$; on les retrouvera (par une méthode complètement différente) au chapitre 11.

6. 3 Factorisation dans R et dans C.

On vient de voir que si a est *racine* de P (c'est-à-dire que $P(a) = 0$), on peut factoriser P par $(X - a)$. De plus, le degré du quotient est (évidemment) $\mathrm{d}^\circ(P) - 1$; si on a d'autres racines de P, elles seront aussi racines du quotient, et on pourra donc recommencer jusqu'à aboutir à un polynôme sans racines.

Il est temps de formuler de manière précise le

Théorème de d'Alembert-Gauss. *Tout polynôme de* $\mathbf{C}[X]$ *peut se factoriser, de manière unique à l'ordre des facteurs près, sous la forme*

$$P(X) = a_n \prod_{i=1}^{n} (X - \alpha_i)$$

où $n = d^\circ(P)$, *et où les* α_i *sont les constantes complexes (distinctes ou non) qui annulent* P *(les «racines» de* P*).*

La démonstration d'existence est une simple conséquence de l'existence de racines pour tout polynôme non constant (mais on a vu au chapitre 4 que c'est un résultat difficile); l'unicité résulte d'une récurrence (sur le degré de P).

Ce résultat est bien entendu valable aussi si $P \in \mathbf{R}[X]$; mais la factorisation ainsi obtenue contient des constantes complexes. Toutefois, si $P(\alpha_i) = 0$, on voit aisément que $P(\overline{\alpha_i}) = 0$ (puisque les coefficients de P sont réels); si α_i n'est pas réel, on a donc les deux racines distinctes α_i et $\overline{\alpha_i}$, et en regroupant les deux facteurs $X - \alpha_i$ et $X - \overline{\alpha_i}$, on obtient $X^2 - 2\Re(\alpha_i) + |\alpha_i|^2$, qui est donc un facteur du second degré (à coefficients réels) de P; d'où le

Théorème de factorisation (dans R). *Tout polynôme de* $\mathbf{R}[X]$ *se décompose (de manière unique) en produits de facteurs du premier degré et de facteurs du second degré à discriminants négatifs.*

6. 4 Racines et coefficients.

Dans le cas complexe, on a vu qu'il y a exactement n racines α_i, mais elles ne sont pas forcément toutes distinctes. En regroupant les α_i égaux (et au besoin en changeant leur numérotation), on aboutit à la factorisation

$$P(X) = a_n (X - \alpha_1)^{k_1} (X - \alpha_2)^{k_2} \cdots (X - \alpha_m)^{k_m},$$

avec $k_1 + k_2 + \cdots k_m = n$. k_i s'appelle l'*ordre de multiplicité* de α_i, si $k_i = 1$, on dit que α_i est une racine *simple*; si $k_i = 2$, que c'est une *racine double*, etc...

Si $P = (X - a)Q$, et que a est racine multiple de P, a est aussi racine de Q. En dérivant, on voit que a est racine de P' (puisque $P' = Q + (X - a)Q'$), et il est clair d'après cette formule que la réciproque est vraie : on a donc le «critère de multiplicité» : a est racine multiple de P si et seulement si a est racine de P et de P' (qui se généralise à l'ordre de multiplicité de a, et aux dérivées successives de P, ce que la «formule de Taylor» du chapitre 11 expliquera par une toute autre approche).

En redéveloppant la factorisation de P (dans $\mathbf{C}[X]$), on obtient (par identification) des relations entre les coefficients de P (les a_i) et les racines : ainsi, on sait que

$$aX^2 + bX + c = a(X - \alpha)(X - \beta) \iff \alpha + \beta = -b/a \text{ et } \alpha\beta = c/a;$$

plus généralement, si $P = \sum_{k=0}^{n} a_k X^k = a_n \prod_{k=0}^{n} (X - \alpha_k)$, on voit (en prenant $X = 0$) que le produit des racines, $p = \prod_{k=1}^{n} \alpha_k$ s'identifie au terme constant, et donc que $p = (-1)^n a_0/a_n$; il est un peu plus délicat de montrer (par récurrence, par exemple) que la somme des racines, $s = \sum_{k=1}^{n} \alpha_k$, vaut $-a_{n-1}/a_n$.

Les autres termes du développement conduisent à des formules analogues, ainsi

$$aX^3 + bX^2 + cX + d = a(X-\alpha)(X-\beta)(X-\gamma) \iff \begin{cases} \alpha+\beta+\gamma = -b/a \\ \alpha\beta+\alpha\gamma+\beta\gamma = c/a \\ \alpha\beta\gamma = -d/a. \end{cases}$$

Le cas général sera vu en Spé.

6. 5 Familles de polynômes classiques : deux exemples.

Il existe de nombreuses suites de polynômes intéressants, qu'on appelle encore des *familles* ; en général, pour chaque valeur de n, il y a donc un polynôme de degré n, qu'on note P_n (ou plutôt B_n, T_n, ... suivant le nom de la famille). Certaines sont définies par récurrence (l'étude d'un exemple est amorcée dans l'exercice-type n° 9), d'autres par des constructions plus compliquées ; on se propose en général d'aboutir à des formules explicites pour les coefficients (ou du moins pour certains d'entre eux), ou d'obtenir des propriétés générales des polynômes ou de leurs racines, etc. On verra des exemples de telles familles tout au long de l'année : polynômes de Taylor (chapitre 11), polynômes d'Hermite (chapitre 13), polynômes d'interpolation de Lagrange (chapitre 15), etc.

Nous allons utiliser ici les techniques combinatoires comme moyen d'étude de deux familles importantes, les polynômes de Bernoulli et de Tchebychev.

— Polynômes de Bernoulli.

Le problème initial que s'est posé Bernoulli est de déterminer les valeurs de $S_k(n) = \sum_{i=0}^{n} i^k$. On a vu que $S_1(n) = n(n+1)/2$ (et bien sûr, $S_0(n) = n+1$) ; on peut deviner que $S_2(n)$ est un polynôme du troisième degré (en n), et il est alors possible de le déterminer (par identification), puis de prouver (par récurrence) que la formule obtenue est bien exacte (cet exercice classique sera fait en classe) ; on obtient $S_2(n) = \dfrac{n(n+1)(2n+1)}{6}$. Mais cette idée est impraticable pour calculer S_3, S_4, ... ; l'astuce de Bernoulli consiste d'abord à développer $(i+1)^{k+1}$ (par la formule du binôme), puis à sommer les développements ainsi obtenus (de $i = 0$ à n), et enfin à remarquer que les S_{k+1} disparaissent, et qu'on obtient une relation entre $S_k(n)$ et les $S_i(n)$, pour $i < k$.

Cette méthode sera précisée en classe ; on aboutit à la formule (qu'il est déconseillé de retenir !)

$$S_k(n) = \frac{1}{k+1}\left((n+1)^{k+1} - \binom{k+1}{2} S_{k-1}(n) - \binom{k+1}{3} S_{k-2}(n) - \cdots - \binom{k+1}{k} S_1(n) - (n+1)\right)$$

D'où il résulte que S_k est un polynôme (de degré $k+1$), appelé ($k^{\text{ème}}$) polynôme de Bernoulli (en fait, la littérature n'est pas très claire à ce sujet : les polynômes de Bernouilli «officiels» sont plutôt les B_n définis ci-dessous).

On peut retenir la valeur particulière $S_3(n) = \dfrac{n^2(n+1)^2}{4} = (S_1(n))^2$; une technique différente (et peut-être plus simple) reposant sur la recherche de polynômes

$B_n(X)$ vérifiant $B_n(X)-B_n(X-1)=X^n$ et $B_n(0)=0$ sera vue en exercice; on verra au chapitre 18 (fiche n° 35), qu'elle permet d'obtenir d'autres renseignements sur les B_n, par exemple la formule $B_n(-X)=(-1)^{n+1}B_n(X-1)$

— Polynômes de Tchebychev

Les polynômes de Tchebychev sont définis par la formule $C_n(\cos x)=\cos nx$ (il existe un analogue pour sin si n est impair); sur $[-1,1]$, on a donc $C_n(X)=\cos(n\operatorname{Arc}\cos X)$. On a vu au chapitre 3 que $C_2(X)=2X^2-1$, et $C_3(X)=4X^3-3X$. Les formules d'addition des angles donnent un calcul par récurrence si on connait les formules analogues pour $\sin nx$ (ce type de définition par récurrence est plus délicat que ceux qu'on a vu plus haut; on parle de récurrence croisée et les démonstrations nécessitent en général des hypothèses de récurrence portant à la fois sur les deux formules). Il est plus simple, pour expliciter $C_n(X)$, d'utiliser la formule de Moivre : on a d'abord $\cos nx=\Re(\cos x+i\sin x)^n=\cos^n x-\binom{n}{2}\cos^{n-2}x\sin^2 x+\binom{n}{4}\cos^{n-4}x\sin^4 x-\cdots$, puis remplaçant $\sin^{2k}x$ par $(1-\cos^2 x)^k=(1-X^2)^k$, et utilisant à nouveau la formule du binôme, on obtient un développement en puissances de X qu'il ne reste plus qu'à réduire; ce qui sera fait en exercice.

On peut facilement déterminer le degré de C_n et les premiers (et derniers) termes; d'autres propriétés (racines, encadrements) résultent de la définition (ainsi, on voit que parmi les racines de $C_5(X)$ doit figurer $\cos\frac{\pi}{10}$).

Exercices

1 Arithmétique.

1 ($\star$) Montrer que si a et b sont premiers entre eux (c'est-à-dire sans diviseurs communs), il en est de même de a et $(a+b)$

2 ($\star\star$) Montrer que pour tout $n\geq 1$, 10^n-1 est divisible par 9, et que $10^{2n+1}+1$ est divisible par 11 (penser à utiliser une factorisation des polynômes X^n-1 et $X^{2n+1}+1$)

2 Suites (notations).

3 ($\star$) Soit (u_n) une suite; décrire en français les deux suites (u_{2n}) et (u_{2n+1})

4 ($\star\star$) Les phrases suivantes définissent-elles des suites ?

«u_n est le $n^{\text{ème}}$ nombre premier»

«v_n est la $n^{\text{ème}}$ décimale de π»

«$w=(3,7,31,127,2047,\ldots)$ est la suite des nombres premiers de la forme 2^k-1»

5 (⋆⋆) Soit (u_n) la suite définie par $u_0 = 1$ et $u_{n+1} = 1 + 1/u_n$; calculer les dix premiers termes de (u_n), proposer une conjecture sur le sens de variation de u, et la noter à l'aide des suites (u_{2n}) et (u_{2n+1})

3 Sommations.

6 (⋆) Rédiger, en utilisant la notation $\sum$, le calcul de $1 + \cos x + \cos 2x + \cdots + \cos nx$

7 (⋆) Soit (u_n) une suite; v la suite définie par $v_n = u_{n+1} - u_n$; calculer $\sum_{k=0}^{n} v_k$.

Les deux exercices-types 8 et 9 (dans le prochain paragraphe) sont assez similaires ; on pourra donc, à la rigueur, n'en étudier soigneusement (c'est-à-dire en respectant le «mode d'emploi») que l'un des deux...

T 8 On veut déterminer une formule explicite pour $S = \sum_{k=1}^{n} kx^{k-1}$. Calculer (par décalage) $(x^2-2x+1)S$; en déduire la valeur de S. Que se passe-t-il dans le cas $x = 1$? Montrer qu'on pouvait obtenir (plus simplement !) ce résultat en considérant S comme un polynôme et en en cherchant une primitive.

8 (⋆⋆) Calculer (sous forme explicite) $S = \sum_{\substack{0\leq i\leq m\\ 0\leq j\leq n}} a^i b^j$; on pourra d'abord montrer que $S = \left(\sum_{i=0}^{m} a^i\right)\left(\sum_{j=0}^{n} b^j\right)$.

9 (⋆⋆⋆) Calculer (en utilisant éventuellement le résultat de l'exercice précédent)

$$\sum_{0\leq i\leq j\leq n} a^i b^j$$

10 (⋆⋆⋆⋆) Calculer $S = \sum_{0\leq i,j\leq n} ij$, puis montrer qu'en posant $T = \sum_{0\leq i<j\leq n} ij$, on obtient $S = 2T + \sum_{i=0}^{n} i^2$. Calculer directement T, et en déduire que $\sum_{i=0}^{n} i^3 = (\sum_{i=0}^{n} i)^2$.

4 Coefficients binomiaux.

11 (⋆) Que vaut $\sum_{k=0}^{n} \binom{n}{k} x^k (1-x)^{n-k}$?

12 (⋆⋆) Déterminer $\sum_{k=0}^{n} \binom{2n}{2k}$ (on pourra commencer par développer $(1-1)^{2n}$)

T 9 Montrer par récurrence que $S_n = \sum_{k=0}^{n} k\binom{n}{k} = n2^{n-1}$ (on pourra utiliser la relation entre les $\binom{n}{k}$ correspondant à la construction du triangle de Pascal). Montrer qu'on pouvait obtenir directement cette formule en utilisant la dérivée du polynôme $(1+x)^n$.

13 (★★★★) Montrer que si p est premier, p divise tous les $\binom{p}{k}$, pour k compris entre 1 et $p-1$. Étudiant l'ensemble des diviseurs de $(p-1)!$, montrer que si p ne divise pas $(p-1)!$, p est premier ou $p=4$; par un raisonnement analogue, montrer enfin que si p divise tous les $\binom{p}{k}$, pour k compris entre 1 et $p-1$, p est premier.

5 Raisonnement par récurrence.

14 (★) Montrer que (pour tout n) $3^{2n}-2^n$ est divisible par 7.

15 (★) Montrer que la suite définie par $u_0=1$ et $u_{n+1}=\ln(1+2u_n)$ est croissante. Etudier de même $v_0=1$; $v_{n+1}=\ln(1+v_n)$

T 10 Soit $(u_n)_{n\geq 1}$ la suite définie par $u_1=1$ et (pour tout $n\geq 1$) $u_{n+1}=\sum_{k=1}^{n} u_k$. Déterminer u_n en fonction de n.

16 (★★★) Soit F la suite de Fibonacci définie par $F_0=0$, $F_1=1$, et $F_{n+2}=F_{n+1}+F_n$ pour tout n. Montrer (par récurrence) les propriétés suivantes :

a) $F_n<2^n$

b) $F_n^2=F_{n-1}F_{n+1}\pm 1$ (commencer par préciser le signe en fonction de n)

c) F_{3n} est pair et F_{5n} est divisible par 5

17 (★★) Le texte suivant contient (il faut l'espérer) une erreur de raisonnement. De plus, la présentation n'en est pas tout à fait rigoureuse. Le réécrire, et diagnostiquer l'erreur :

«**Théorème.** *Pour tout réel $a>0$ et tout entier $n\geq 1$, on a $a^{n-1}=1$*

Démonstration : c'est évidemment vrai pour $n=1$. Supposons que ce le soit pour 1, 2, 3, ..., k. On aura alors

$$1=\frac{1\times 1}{1}=\frac{a^{k-1}a^{k-1}}{a^{k-2}}=\frac{a^{2k-2}}{a^{k-2}}=a^k=a^{(k+1)-1};$$

le théorème est encore vrai pour $k+1$; par récurrence, il est donc toujours vrai.»

18 (★★) Et que penser du texte suivant ?

«**Théorème.** *Si un ensemble fini d'entiers contient un entier pair, tous les entiers de l'ensemble sont pairs*

Démonstration : Raisonnons par récurrence sur le nombre d'éléments n de l'ensemble. Le théorème est évidemment vrai si $n=1$. Supposons qu'il soit vrai pour tous les ensembles contenant k entiers. Soit alors E un ensemble de $k+1$ entiers, contenant un entier pair a. Retirons un entier $b\neq a$ de l'ensemble, nous obtenons un sous-ensemble S de k entiers contenant a, qui d'après l'hypothèse de récurrence est formé d'entiers tous pairs. Remplaçons alors dans cet ensemble a par b, nous obtenons un nouvel ensemble S' de k entiers contenant un entier pair (l'un des $k-1$ entiers non remplacés); tous les entiers de S' sont donc pairs, ce qui prouve que b est pair; et comme $E=S\cup\{b\}$, E ne contient que des entiers pairs; ce qui, par récurrence, achève la démonstration.»

6 Polynômes.

19 ($\star$) Montrer que si la fonction polynôme $[x \mapsto P(x)]$ est périodique, elle est constante.

20 ($\star\star$) Développer le polynôme $P(X) = \sum_{k=0}^{n} \binom{n}{k} X^{n-k}(1-X)^k$. Par identification de coefficients, en déduire la formule

$$a_{n-m} = \sum_{k=0}^{n-m} (-1)^k \binom{m+k}{k}\binom{n}{m+k} = \begin{cases} 0 & \text{si } m < n \\ 1 & \text{si } m = n \end{cases}$$

21 ($\star\star\star$) Soit $P_n(X)$ le polynôme $\sum_{k=0}^{n} \frac{X^k}{k!}$. Montrer que le polynôme Q défini par $Q(X) = (P_n(X))^2 - P_n(2X)$ est divisible par X^{n+1}

22 ($\star\star$) Factoriser dans $\mathbf{R}$ et dans $\mathbf{C}$ les polynômes suivants :

$$X^3 + X - 2\,; \qquad X^6 - 1\,; \qquad X^6 + 64\,; \qquad X^5 - 1$$

23 ($\star\star$) Pour quelles valeurs de n le polynôme $X^{n^2} - 2X^{2n} + 1$ admet-il -1 pour racine ? -1 peut-il être racine double ?

24 ($\star\star$) Pour quelles valeurs de n le polynôme $X^n + X + 1$ est-il divisible par $X^2 + X + 1$? (utiliser $j = e^{\frac{2i\pi}{3}}$)

25 ($\star\star\star$) Factoriser $X^n - A$ dans $\mathbf{C}$; en déduire la somme et le produit des racines $n^{\text{èmes}}$ de A. Ce résultat était-il prévisible ?

26 ($\star\star\star\star$) Résoudre (dans $\mathbf{C}$) le système (S) : $\begin{cases} x + y + z &= 2 \\ 1/x + 1/y + 1/z &= 5/6 \\ xyz &= -6 \end{cases}$

27 ($\star\star\star$) Soit $(x_0, x_1, x_2, \ldots, x_n)$ $n+1$ nombres distincts, montrer qu'il existe au plus un polynôme P de degré $\leq n$ tel que $P(x_k) = k$. Montrer que le polynôme

$$Q = \sum_{i=0}^{n} K_i \prod_{j \neq i} (X - x_j)$$

vérifie $Q(x_i) = K_i \prod_{j \neq i} (x_i - x_j)$ et en déduire une construction de P

28 ($\star\star$) On définit une suite (P_n) de polynômes de $\mathbf{R}[X]$ par $P_0 = 0$ et (pour tout $n \geq 0$) $P_{n+1} = P_n^2 + X$. Déterminer le degré de P_n, les racines de P_1, P_2, et celles de P_3 (à 10^{-9} près). Montrer que les racines (réelles) de P_n sont comprises entre -2 et 0. (On pourra commencer par prouver que $|x| > 2 \Rightarrow |x^2 + x| > 2$, puis montrer par récurrence que $P_n(x)$ est une suite (positive) croissante à partir de n assez grand si $x < -2$).

Attention : l'exercice-type qui suit est difficile, et nécessite, pour en comprendre vraiment l'énoncé, une démarche «expérimentale» : ne pas se décourager si vous n'avez pas su l'aborder ; penser à utiliser la TI-92 ou Maple V pour vous procurer des «données».

† **T 11** Soit P_n la suite de polynômes définis dans l'exercice précédent. Montrer qu'en écrivant $P_n = \sum_{k=0}^{\deg(P_n)} a_k(n) X^k$, les coefficients $a_k(n)$ ne dépendent pas de n si $k \leq n$.

6. TECHNIQUES COMBINATOIRES, POLYNÔMES

Plan

6. TECHNIQUES COMBINATOIRES, POLYNÔMES

(Formulaire)

1 Arithmétique.

Définition 1.1. *On dit que a est* **multiple** *de b, ou que b est un* **diviseur** *de a (a et b entiers relatifs) si $(\exists k \in \mathbf{Z})(a = kb)$, ce qu'on note $b|a$. On appelle* **plus grand diviseur commun** *à a et à b (noté $\mathrm{PGCD}(a,b)$, où a et b sont des entiers positifs) le plus grand entier k tel que $k|a$ et $k|b$. On dit que a (entier positif) est* **premier** *si $a > 1$ et si les seuls diviseurs de a sont a et 1. On dit que les entiers a et b sont* **premiers entre eux** *(ou* **étrangers***) si 1 est le seul diviseur commun à a et à b.*

Définition 1.2. *On appelle* **division euclidienne** *de a par b ($a \in \mathbf{Z}$, $b \in \mathbf{N}^*$) une écriture de la forme $a = bq + r$, avec q et r entiers, et $0 \leq r < b$. Cette écriture existe et est unique; q s'appelle le* **quotient**, *et r le* **reste** *(euclidien).*

Théorème de Bezout. *Si a et b sont premiers entre eux, il existe p et q (entiers relatifs) tels que $ap + bq = 1$*

Théorème de factorisation. *Pour tout entier n, il existe une décomposition unique (à l'ordre des facteurs près) de la forme $n = p_1^{\alpha_1} \times \cdots \times p_k^{\alpha_k}$, où les p_i sont des nombres premiers.*

Tous ces résultats se généralisent aux polynômes (voir **3**).

2 Suites; formule du binôme.

Définition 2.1. *On appelle* **suite d'objets de** *A (ou suite à valeurs dans A) une application de $\mathbf{N}$ vers A; si u est une telle suite, on note u_n (qu'on appelle le n-ème* **terme** *de la suite, ou le terme d'***indice** *n) l'image de n par u; la suite entière se note $u = (u_n)_{n \in \mathbf{N}}$.*

Définition 2.2. *On dit que la suite (u_n) est définie* **par récurrence** *si on a une relation entre chaque terme et les termes précédents. En particulier, (u_n) est définie* **par itération** *de f si (pour tout n) $u_{n+1} = f(u_n)$.*

Définition 2.3. *On note $\sum_{i=0}^{n} a_i$ le terme u_n de la suite définie par récurrence par $u_0 = a_0$ et $u_{k+1} = u_k + a_{k+1}$; on note de même $\prod_{i=0}^{n} a_i$ le terme v_n de la suite définie par récurrence par $v_0 = a_0$ et $v_{k+1} = v_k \times a_{k+1}$.*

Définition 2.4. *On note (par exemple) $\sum_{0 \leq i,j \leq n} a_{ij}$ la* **somme double** $\sum_{i=0}^{n} (\sum_{j=0}^{n} a_{ij})$.

Définition 2.5. *On dit que (u_n) est une* **suite arithmétique** *(de* **raison** *a) si elle vérifie (pour tout n) $u_{n+1} = u_n + a$, ce qui équivaut à $u_n = u_0 + n.a$; on dit que*

(u_n) est une **suite géométrique** *(de* **raison** *k) si elle vérifie (pour tout n) $u_{n+1} = k.u_n$, ce qui équivaut à $u_n = u_0.k^n$.*

Outre les formules de manipulation données dans le cours, on retiendra

$$\sum_{k=0}^{n} u_k = (n+1)\frac{u_0+u_n}{2} = (n+1)u_0 + a\frac{n(n+1)}{2}$$

si u est arithmétique ($u_n = u_0 + an$)

$$\sum_{k=0}^{n} x^k = \frac{x^{n+1}-1}{x-1} \text{ (si } x \neq 1)$$

"formule des suites géométriques"

$$\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$$

$$\sum_{k=0}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$$

$$\sum_{k=0}^{n} k^3 = \frac{n^2(n+1)^2}{4}$$

(Formules de Bernouilli)

Définition 2.6. *On appelle* **factorielle de** *n (et on note $n!$) le nombre $\prod_{k=1}^{n} k$; on pose par convention $0! = 1$. On appelle* **coefficients du binôme**, *et on note $\binom{n}{k}$, les nombres donnés par $\binom{n}{k} = \frac{n!}{k!(n-k)!}$.*

On a donc

$$\binom{n}{k} = \frac{n(n-1)\cdots(n-k+2)(n-k+1)}{k(k-1)\cdots 2\times 1}$$

et on retiendra que

$$\binom{n}{0} = \binom{n}{n} = 1 \; ; \; \binom{n}{1} = \binom{n}{n-1} = n \text{ et } \binom{n}{2} = \binom{n}{n-2} = \frac{n(n-1)}{2}$$

On établit par récurence la

Formule du binôme (Newton) :

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

d'où on déduit, par exemple, que

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n; \quad \sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0$$

(prendre $x = 1$, $y = \pm 1$).

3 Schémas de raisonnement par récurrence.

Attention : les schémas suivants sont, volontairement, «trop abstraits» ; les utiliser comme aide-mémoire, mais penser à rédiger en revenant aux modèles du cours...

Définition 3. 1. **Récurrence simple** *: on veut montrer $\mathcal{A}(n)$ pour tout $n \in \mathbf{N}$. On montre que $\mathcal{A}(0)$ et que $\forall k \in \mathbf{N}$, $\mathcal{A}(k) \Rightarrow \mathcal{A}(k+1)$.*
On peut aussi montrer que $\mathcal{A}(0)$ et que $\forall n \in \mathbf{N}^*$, $\mathcal{A}(n-1) \Rightarrow \mathcal{A}(n)$.

Définition 3. 2. **Récurrence simple à partir de** n_0 *: on veut montrer $\mathcal{A}(n)$ pour tout pour tout $n \geq n_0$. On montre que $\mathcal{A}(n_0)$ et que $\forall k \in \mathbf{N}$, $k \geq n_0$ et $\mathcal{A}(k) \Rightarrow \mathcal{A}(k+1)$.*

Définition 3. 3. **Récurrence à deux termes** *: on veut montrer $\mathcal{A}(n)$ pour tout $n \in \mathbf{N}$. On montre que $\mathcal{A}(0)$, que $\mathcal{A}(1)$, et que$\forall k \in \mathbf{N}$, $\mathcal{A}(k)$ et $\mathcal{A}(k+1) \Rightarrow \mathcal{A}(k+2)$.*

Définition 3. 4. **Récurrence cumulative** *: on veut montrer $\mathcal{A}(n)$ pour tout $n \in \mathbf{N}$. On montre que $\mathcal{A}(0)$, et que si, pour tout $k \in \mathbf{N}$ et pour tout $j \leq k$, $\mathcal{A}(j)$, alors $\mathcal{A}(k+1)$.*

Définition 3. 5. **Récurrence finie** *: on veut montrer $\mathcal{A}(n)$ pour tout n tel que $n_1 \leq n \leq n_2$. On montre que $\mathcal{A}(n_1)$ et que $\forall k \in \mathbf{N}$, $n_1 \leq k < n_2$ et $\mathcal{A}(k) \Rightarrow \mathcal{A}(k+1)$.*

4 Polynômes.

Définition 4. 1. *On appelle* **polynôme à une variable** *(notée X), à coefficients dans K, toute expression de la forme $\sum_{k=0}^{n} a_k X^k$, où les a_k appartiennent à K. K doit être un «anneau» de nombres (voir chapitre 17), par exemple $\mathbf{R}$, $\mathbf{C}$ ou $\mathbf{Z}$. L'ensemble de tous les polynômes à coefficients dans K se note $K[X]$. Une fonction de la forme $f : x \mapsto P(x)$, où $P \in K[X]$, s'appelle une* **fonction polynômiale**, *et (par abus de langage) on ne fera pas en général de distinction entre f et P.*

Définition 4. 2. *Si $P(X) = \sum_{k=0}^{n} a_k X^k$ (écriture de P en* **puissances croissantes**) *et si $a_n \neq 0$, on dit que n est le* **degré** *de P (noté $\deg(P)$, ou $d^\circ(P)$), que a_n est le* **coefficient dominant**, *et que $a_n X^n$ est le* **terme dominant** *de P.*

Définition 4. 3. *On appelle* **division euclidienne** *de P par Q l'écriture $P = DQ + R$, où $\deg(R) < \deg(Q)$; on démontre que cette décomposition existe et est unique; D s'appelle le* **quotient** *(euclidien) et R le* **reste** *(euclidien). On dit que P est* **divisible** *par Q (ou que Q est un* **facteur** *de P) si $R = 0$.*

Définition 4. 4. *On dit que a (élément de K) est* **racine** *de P si $P(a) = 0$, ce qui équivaut à dire que P est divisible par $(X-a)$. Si P est divisible par $(X-a)^k$, et non divisible par $(X-a)^{k+1}$ ($k > 1$), on dit que a est* **racine multiple** *de P, et que k est son* **ordre de multiplicité**.

Caractérisation des racines multiples. *a est racine multiple de P si et seulement si $P(a) = P'(a) = 0$. Plus précisément, a est d'ordre de multiplicité k si et seulement si $P(a) = P'(a) = P''(a) = \cdots = P^{(k)}(a) = 0 \neq P^{(k+1)}(a)$*

Théorème de d'Alembert-Gauss. *Tout polynôme de* $\mathbf{C}[X]$ *peut se factoriser, de manière unique à l'ordre des facteurs près, sous la forme*

$$P(X) = a_n \prod_{i=1}^{p} (X - \alpha_i)^{k_i}$$

où $n = \deg(P) = \sum_{i=1}^{p} k_i$, *et où les* α_i *sont les racines de* P *(avec pour ordres de multiplicité les* k_i*).*

Théorème de factorisation (dans R). *Tout polynôme de* $\mathbf{R}[X]$ *se décompose (de manière unique) en produits de facteurs du premier degré et de facteurs du second degré à discriminants négatifs.*

Relations entre coefficients et racines.

Si $P(X) = aX^2 + bX + c$ a pour racines x_1 et x_2, on a

$$x_1 + x_2 = -\frac{b}{a}, \quad x_1 x_2 = \frac{c}{a}.$$

Plus généralement, si $P(X) = \sum_{k=0}^{n} a_k X^k$ a pour racines x_i $(1 \leq i \leq n)$, on a

$$\sum_{i=1}^{n} x_i = -\frac{a_{n-1}}{a_n}, \quad \prod_{i=1}^{n} x_i = (-1)^n \frac{a_0}{a_n}.$$