Lycée Pierre-Gilles de Gennes **BCPST**
Mathématiques **2023-2024**

Révisions/Formulaire 05

Révisions/Compléments Algèbre: Polynômes, $\mathbb{R}[X]$, $\mathbb{C}[X]$

Définition, vocabulaire

Définition 1. *1. Une « expression » ou une « écriture* [1] *» d'un polynôme P en l'indéterminée X à coefficients réels, resp. complexes, est*

— *soit une expression de la forme* [2]*, dite* **normale**

$$p_0 + p_1.X + \cdots + p_d.X^d \tag{FN}$$

où la suite des **coefficients** *de P, i.e la suite de nombres réels, resp. complexes,* $(p_0, \ldots, p_d, \ldots)$ *est nulle à partir d'un certain rang.*

— *soit une expression obtenue en additionnant, multipliant de telles expressions.*

2. *Deux polynômes sont égaux si les expressions, une fois développées suivant les régles* [3] *usuelles du calcul littéral sur* $\mathbb{C}$*, –et donc mises sous forme normale* (FN)*– de chacun de ces polynômes ont mêmes coefficients.*

1. Le symbole X (l'« indéterminée ») est un polynôme particulier, ce n'est pas un nombre. Dans le programme officiel BCPST de 2020, il s'agit d'une fonction $X : \Omega \to \mathbb{C}$ où Ω est une partie infinie [4] de $\mathbb{C}$ et $\forall z \in \Omega, X(z) = z$. Le symbole X dans l'écriture d'un polynôme est destiné – lors d'une « évaluation » de ce polynôme en α – à être remplacé ou substitué par α : il faut donc que α^k ait un sens pour tout entier naturel k de même qu'une combinaison linéaire quelconque de telles puissances entières de α.
2. Le polynôme nul est le polynôme dont les coefficients de la forme normale sont tous nuls. Son **degré** est conventionnellement $-\infty$.
3. Le coefficient p_i d'indice $i \in \mathbb{N}$ est souvent appelé le coefficient du terme de degré i dans P.
4. Si P n'est pas nul, son **degré**, noté $\deg P$, est l'indice maximum au delà duquel tous les coefficients de la forme normale sont nuls. Le coefficient du terme de degré $\deg P$ est *différent de* 0. Les coefficients des termes de degré $> \deg P$ sont nuls. En particulier le polynôme X est de degré 1.
5. Un polynôme est dit *constant* s'il est nul ou de degré 0.
6. l'ensemble des polynômes à coefficients réels, resp complexes, est noté $\mathbb{R}[X]$, resp. $\mathbb{C}[X]$, l'ensemble des polynômes de degré *inférieur ou égal* à d, est noté $\mathbb{R}_d[X]$, resp. $\mathbb{C}_d[X]$.
7. Le coefficient du terme de degré $\deg P$ est appelé le **coefficient dominant** de P. Un polynôme est dit **unitaire** si son coefficient dominant vaut 1. Le polynôme X est un polynôme unitaire de degré 1.

1. On reprend ici un terme du programme officiel BCPST2 de 2020 qui est confondant de limpidité
2. On prend la convention d'écriture $X^0 = 1, X^1 = X$.
3. avec notamment la règle $X^k.X^\ell = X^{k+\ell}$.
4. par exemple $\mathbb{R}$, un intervalle de $\mathbb{R}$, le cercle unité,...on ne s'en préoccupe pas vraiment

8. La somme, le produit de deux polynômes sont des polynômes. Le coefficient du terme d'indice k dans $P+Q$ vaut p_k+q_k, le coefficient du terme d'indice k dans $P.Q$ vaut

$$\sum_{\substack{m+n=k\\ m,n\in\mathbb{N}}} p_m.q_n = \sum_{\ell=0}^{k} p_\ell.q_{k-\ell}$$

On a

$$\deg(P+Q) \leq \max(\deg P, \deg Q) \text{ et } \deg P.Q = \deg P + \deg Q.$$

9. Bien qu'on ne puisse diviser deux polynômes en général, on a la régle de simplification suivante : Si P, A, B sont des polynômes, $P \neq 0$ et $P.A = P.B$ alors $A = B$.

Substitution, évaluation, composition

1. Substitution de X par une valeur. Si $\alpha \in \mathbb{C}$ et $P = p_0 + p_1.X + \cdots + p_d.X^d$ on note $P(\alpha)$, la **valeur de P en α** le nombre

$$P(\alpha) = p_0 + p_1.\alpha + \cdots + p_d.\alpha^d$$

On dit qu'on a effectué la **substitution** de X par la valeur α ou que l'on a **évalué** P en α, on peut noter [5] cette opération $X \leftarrow \alpha$.

On a $(P+Q)(\alpha) = P(\alpha) + Q(\alpha)$ et $(P.Q)(\alpha) = P(\alpha).Q(\alpha)$. A un polynôme P est donc naturellement associée une fonction [6] (dite **polynomiale**) P définie sur $\mathbb{C}$ ou une partie Ω de $\mathbb{C}$. $P : z \in \Omega \mapsto P(z) \in \mathbb{C}$. On peut choisir $\Omega = \mathbb{R}$ ou un intervalle $I \subset \mathbb{R}$, ce qui est monnaie courante en Analyse.

2. Substitution de X par un polynôme Q. Si $Q \in \mathbb{C}[X]$ et $k \in \mathbb{N}$ alors $Q^k := \underbrace{Q.\ldots.Q}_{k \text{ fois}} \in \mathbb{C}[X]$.

Si maintenant $P = p_0 + p_1.X + \cdots + p_d.X^d \in \mathbb{C}[X]$, on note la **composée (à droite)** de P par Q [7]

$$P \circ Q = P(Q) := p_0 + p_1.Q + \cdots + p_d.Q^d \in \mathbb{C}[X].$$

Si P, Q, sont à coefficients réels, $P(Q)$ l'est aussi. X est un polynôme. On a donc $P(X) = P$. En général, sauf si Q est nul, $\deg P(Q) = \deg P.\deg Q$. Si p et q sont les fonctions associées à P et Q alors $p \circ q$ est la fonction associée à $P(Q) = P \circ Q$. On a $(P(Q))(\alpha) = P(Q(\alpha))$.

3. Substitution de X par une matrice carrée M. Si $n \in \mathbb{N}^*$, $M \in \mathscr{M}_n(\mathbb{C})$ et $k \in \mathbb{N}$ alors [8] $M^k := \underbrace{M.\ldots.M}_{k \text{ fois}}$.

Si maintenant $P = p_0 + p_1.X + \cdots + p_d.X^d \in \mathbb{C}[X]$, on note

$$P(M) := p_0.I_n + p_1.M + \cdots + p_d.M^d \in \mathscr{M}_n(\mathbb{C}).$$

Si P, M, sont à coefficients réels, $P(M)$ l'est aussi. Un polynôme P tel que $P(M) = 0_n$ est dit **annulateur** [9] de M. Si $Y \in \mathbb{C}^n$, on a

$$P(M).Y = p_0.Y + p_1.M.Y + \cdots + p_d.M^d.Y$$

5. et non pas $X = \alpha$, vu que X est un polynôme et donc ayant sa valeur propre–un polynôme–, on ne peut réaffecter ce symbole à une autre valeur.

6. Le programme officiel BCPST2 considère qu'un polynôme *est* la fonction polynomiale associée, la pratique des exercices d'oraux montre que ce point du programme n'est pas respecté. Pour nous un polynôme « *est* » la suite des coefficients $p_0, p_1, \ldots, p_d, \ldots$ permettant de fabriquer une « formule » polynômiale

7. Il y deux notations qui coexistent.

8. avec la convention $M^0 = I_n$

9. Cette notion est officiellement hors programme BCPST mais apparait dans nombre de problèmes et d'exercices

Polynôme dérivé et dérivés successifs

Définition 2. *1. Si $P = p_0 + p_1.X + \cdots + p_d.X^d = \sum_{k=0} p_k X^k$ est un polynôme, son polynôme dérivé est*

$$P' = p_1 + 2.p_2 + \cdots + d.p_d.X^{d-1} = \sum_{k=0}^{d-1} (k+1)p_{k+1}X^k$$

2. Si $\ell \in \mathbb{N}$, le ℓ-ième polynome dérivé de P, $P^{(\ell)}$ est défini par la récurrence $P^{(0)} = P$,

$$\forall \ell \in \mathbb{N}, P^{(\ell+1)} = (P^{(\ell)})' = (P')^{(\ell)}$$

Au niveau du degré, $\deg P' = \deg P - 1$ si $\deg P \geq 1$, $-\infty$ sinon. Les dérivés d'une somme, d'un produit, d'une composition, ont les mêmes formules que pour la dérivation des fonctions d'une variable réelle.

Si $\ell > \deg P$, $P^{(\ell)} = 0$, si $d = \deg P \geq 0$, $P^{(d)} = d!p_d$. On a, pour $\ell \leq k$,

$$((X-\alpha)^k)^{(\ell)} = k.(k-1)\ldots.(k-\ell+1)(X-\alpha)^{k-\ell} = \frac{k!}{(k-\ell)!})(X-\alpha)^{k-\ell}$$

et pour $\ell > k$,

$$((X-\alpha)^k)^{(\ell)} = 0$$

Par récurrence sur le degré du polynôme P, on tire la formule [10] de TAYLOR pour les polynômes, pour $\ell > \deg P$, $\alpha \in \mathbb{C}$,

$$P = P(\alpha) + P'(\alpha)(X-\alpha) + \cdots + \frac{P^{(\ell)}(\alpha)}{\ell!}(X-\alpha)^\ell$$

Cette notion de dérivation est purement formelle : on a posé la formule du polynôme dérivé à partir de celle du polynôme, il n'y a pas de limite de taux d'accroissement en jeu. Le nom de dérivation provient de l'opération homonyme en analyse et les règles de calcul sont les mêmes [11] :

Linéarité : $\forall P, Q \in \mathbb{C}[X], \forall \lambda, \mu \in \mathbb{C}, (\lambda.P + \mu.Q)' = \lambda.P' + \mu.Q'$

LEIBNIZ : $\forall P, Q \in \mathbb{C}[X], (P.Q)' = P'.Q + P.Q'$

Composé : $\forall P, Q \in \mathbb{C}[X], (P \circ Q)' = (P' \circ Q).Q'$

Il y a évidemment compatibilité des opérations de dérivation entre algèbre et analyse. Si $P \in \mathbb{C}[X]$ et $p : I \to \mathbb{C}$ est la fonction polynomiale associée sur un certain intervalle [12] $I \subset \mathbb{R}$ non trivial définie par

$$\forall x \in I, p(x) = P(x) \text{ [substitution } X \leftarrow x \text{ dans le polynôme } P]$$

alors $\forall x \in I$,

$$\text{[dérivation analyse] } p'(x) = P'(x) \text{ [substitution } X \leftarrow x \text{ dans le polynôme } P', \text{ (dérivation algèbre)]}$$

Exercice 1.—

1. Discuter, suivant les valeurs des nombres réels a and b, du degré des polynômes P, Q, $P+Q$ et PQ si

$$P(X) = aX^3 - bX^2 + bX + a \text{ et } Q(X) = bX^2 + a^2X.$$

2. Donner leurs polynômes dérivés.

10. Hors programme BCPST

11. Il n'y a pas de règle concernant le quotient, vu qu'un quotient de deux polynôme, ce n'est pas un polynôme !

12. SVP : Ne parlez pas de fonction dérivable sur $\mathbb{C}$! ! ! !, dans la formule suivante vous ne pouvez pas remplacer I par une partie quelconque de $\mathbb{C}$ car la dérivation au sens de l'analyse d'une fonction de variable complexe est ABSOLUMENT hors de votre programme.

Exercice 2.—
1. Résoudre l'équation $Q^2 = XP^2$, où les inconnues P et Q sont des polynômes à coefficients complexes en l'indéterminée X.

Indication:Chercher les degrés possibles.

2. De même, résoudre l'équation d'inconnue $P \in \mathbb{C}[X]$

$$(P')^2 = 4P.$$

Exercice 3.—
1. Trouver un polynôme P_2 tel que $P_2(0) = 0$ et

$$P_2(X+1) - P_2(X) = X^2$$

et en déduire la valeur de $\sum_{i=1}^{n} i^2$. Indication:Commencer par déterminer le degré d'un tel polynôme P_2

2. Déterminer par la même méthode une formule fermée pour $\sum_{i=1}^{n} i^3$.

Indication:Trouver un polynôme P_3 adhoc, par exemple, en primitivant P_2.

Racines et racines multiples

Définition 3

On dit que $\alpha \in \mathbb{C}$ est **racine** de P si $P(\alpha) = 0$.

Proposition 4

α est racine de P si (et seulement si) il existe $Q \in \mathbb{C}[X]$ tel que $P = (X - \alpha).Q$.

Proposition–Définition 5

Soit $\alpha \in \mathbb{C}$, $P \in \mathbb{C}[X]$, $k \in \mathbb{N}^*$,

- Si il existe $Q \in \mathbb{C}[X]$ tel que $P = (X-\alpha)^k.Q$, on dit que α est **racine d'ordre au moins** k de P.
- Si α est racine de P, la **multiplicité**[a] **de α en tant que racine de** P est l'entier k tel que α est racine d'ordre au moins k de P **et** α n'est pas racine d'ordre au moins $k+1$ de P.
- Une racine α de P est dite :
  - simple si elle est de multiplicité 1 ;
  - double si elle est de multiplicité 2.

a. par convention α est racine de multiplicité 0 si α n'est pas racine de P, i.e $P(\alpha) \neq 0$

Théorème 6

1. Si P est un polynôme **non nul** de degré $d \in \mathbb{N}$ alors P admet au plus d racines en comptant les multiplicités.
2. Si P est un polynôme ayant plus de $d \in \mathbb{N}$ racines distinctes alors soit $\deg P > d$, soit $P = 0$.
3. Si P est un polynôme ayant une infinité de racines distinctes alors $P = 0$.

Théorème 7: D'ALEMBERT-GAUSS

Soit $P \in \mathbb{C}[X]$, non constant. P admet au moins une racine $\alpha \in \mathbb{C}$.

Exercice 4.—Soit $P \in \mathbb{C}[X]$ et $\alpha \in \mathbb{C}$. Montrer que

1. α est racine simple de P si et seulement si $P(\alpha) = 0$ et $P'(\alpha) \neq 0$;
2. α est racine de multiplicité au moins 2 si et seulement si $P(\alpha) = 0$ et $P'(\alpha) = 0$;
3. α est racine double de P si et seulement si $P(\alpha) = 0$, $P'(\alpha) = 0$ et $P''(\alpha) \neq 0$;

Exercice 5.— Pour un entier $n \geq 4$, on considère le polynôme $P = X^{2n} - nX^{n+1} + nX^{n-1} - 1$. Prouver que 1 est racine triple de P.

Exercice 6.— Soit $n \in \mathbb{N}^*$.
1. Démontrer que les racines complexes du polynôme $P_n = 1 + X + \frac{1}{2!}X^2 + \cdots + \frac{1}{n!}X^n = \sum_{k=0}^{n} \frac{1}{k!}X^k$ sont toutes simples.
2. On considère maintenant P_n comme fonction polynomiale sur $\mathbb{R}$. Démontrer par récurrence

$$\forall k \in \mathbb{N},\ P_{2k} \text{ ne s'annule pas et } P_{2k+1} \text{ s'annule exactement une fois}$$

Exercice 7.—
1. On considère, pour $p, q \in \mathbb{R}$, le polynome $P = X^3 + pX + q$.
Montrer, par une étude de fonction que ce polynôme admet trois racines réelles distinctes si et seulement si $4p^3 + 27q^2 < 0$.
Indication:Que penser du fait que les valeurs de P aux deux racines de son dérivé sont de signes opposés ?
2. Peut-on, sur cette base, déterminer une CNS sur les coefficients réels a, b, c pour que le polynôme $Q = X^3 + aX^2 + bX + c$ ait trois racines réelles distinctes ?
Indication:Ecrire Q sous le forme $P(X + \frac{1}{3}a)$ avec p et q bien choisis

Divisibilité, décomposition en facteurs irréductibles

Fixons, dans toute cette partie, $\mathbb{K}$ l'un [13] des deux ensembles $\mathbb{R}$ ou $\mathbb{C}$.

Définition 8. *Soient P, Q deux polynomes dans $\mathbb{K}[X]$. On dit que P* **divise** *Q ou que Q est* **factorisable** *par P s'il existe un polynôme $R \in \mathbb{K}[X]$ tel que $Q = P.R$.*

Exemples : Un polynôme quelconque divise le polynôme nul. Un polynôme constant non nul divise tout polynôme. Le polynôme nul ne divise que lui-même. $\alpha \in \mathbb{K}$ est racine de P d'ordre au moins k si et seulement si $(X - \alpha)^k$ divise P.

Définition 9. *On dit qu'un polynôme $P \in \mathbb{K}[X]$, de degré > 0, est* **irréductible** *dans $\mathbb{K}[X]$ si pour tous $Q, R \in \mathbb{K}[X]$ tels que $P = Q.R$, soit Q, soit R est constant.*

Un polynôme de degré 1 est toujours irréductible. Par une quasi-tautologie et une récurrence sur le degré (un polynôme de degré ≥ 2 est soit irréductible, soit produit de deux polynômes de degrés strictement inférieurs) :

Proposition 10. *Si $P \in \mathbb{K}[X]$, $\deg(P) > 0$, il existe $P_1, \ldots, P_r$, irréductibles, tels que $P = P_1 \ldots . P_r$.*

Théorème 11: D'ALEMBERT-GAUSS **revisité**

Les polynômes irréductibles dans $\mathbb{C}[X]$ sont exactement les polynômes de degré 1.

13. Dans le programme officiel de BCPST, seul le cas $\mathbb{K} = \mathbb{C}$ est au programme.

Une conséquence [14] en est l'énoncé suivant : les polynômes irréductibles dans $\mathbb{R}[X]$ sont exactement

1. les polynômes de degré 1.
2. les polynômes de degré 2 sans racines réelles

Dans la preuve de la deuxième partie de ce résultat apparait l'énoncé suivant qu'il convient de singulariser, il est au programme.

Proposition 12

Si $P \in \mathbb{R}[X]$, $\alpha \in \mathbb{C}$ est racine de P de multiplicité m alors $\overline{\alpha}$ est racine de P de multiplicité m.

Démonstration. — Soit $P = \sum_{k=0}^{d} p_k.X^k$ où les p_k sont réels. Si $P(\alpha) = 0$ alors en utilisant les règles algébriques satisfaites par la conjugaison et le fait que $\overline{p_k} = p_k$:

$$\overline{P(\alpha)} = \overline{\sum_{k=0}^{n} p_k.\alpha^k} = \sum_{k=0}^{n} p_k.\overline{\alpha}^k = P(\overline{\alpha})$$

Cela montre que si α est racine de P, $\overline{\alpha}$ l'est aussi. Si α est complexe non réel et si α est racine de P : $P = (X-\alpha).Q_1(X)$ pour un certain $Q_1 \in \mathbb{C}[X]$ vérifiant $Q_1(\overline{\alpha}) = 0$ (car $(\overline{\alpha} - \alpha) \neq 0$) et donc, pour un certain polynôme $Q \in \mathbb{C}[X]$,

$$P = (X-\alpha).(X-\overline{\alpha})Q = (X^2 - 2\mathrm{Re}(\alpha).X + |\alpha|^2).Q$$

Comme $(X-\alpha).(X-\overline{\alpha}) = X^2 - 2\mathrm{Re}(\alpha).X + |\alpha|^2$ est réel, le polynôme Q est à coefficients réels.

— Concernant les multiplicités, on montre le résultat par récurrence sur m en se basant sur la remarque suivante : si α (α complexe non réel) est racine de multiplicité $\geq m$ ($m \geq 2$) de P alors par le point précédent, $P = (X-\alpha).(X-\overline{\alpha}).Q$ où $Q \in \mathbb{R}[X]$ et α est racine de multiplicité $\geq m-1$ de Q.

On peut appliquer l'hypothèse de récurrence (bien rédigée et quantifiée pour que cela « passe ») à Q pour obtenir que $\overline{\alpha}$ est racine de multiplicité $\geq m-1$ de Q et conclure que est racine de multiplicité $\geq m$ de P. Il existe $R \in \mathbb{R}[X]$ tel que

$$P = (X-\alpha).(X-\overline{\alpha}).\underbrace{(X-\alpha)^{m-1}.(X-\overline{\alpha})^{m-1}R}_{Q} = (X-\alpha)^m.(X-\overline{\alpha})^m R.$$

□

Théorème 13: Décomposition en irréductibles

Si $P \in \mathbb{C}[X]$, $P \neq 0$, $d := \deg P \geq 0$, il existe une unique famille [a] non ordonnée de polynômes unitaires irréductibles dans $\mathbb{C}[X]$, $(P_i)_{i\in\{1,\dots,d\}} = (X-\alpha_i)_{i\in\{1,\dots,d\}}$ et un unique $\lambda \in \mathbb{C}$ tels que

$$P = \lambda.\prod_i P_i = \lambda.\prod_i (X-\alpha_i)$$

a. Noter que $\lambda \neq 0$. Si $d = 0$, cette famille est vide, le produit sur une famille vide vaut conventionnellement 1

Exercice 8.—
1. Factoriser en irréductibles dans $\mathbb{C}[X]$: $P = 6X^3 + X^2 - 19X + 6$ et $Q = X^4 + 1$.
2. Et dans $\mathbb{R}[X]$?

14. Hors programme BCPST

Exercice 9.— Soit $P=(X+1)^7-X^7-1\in\mathbb{C}[X]$.
1. Donner au moins deux racines évidentes de P.
2. Montrer que si $j\in\mathbb{C}\setminus\{1\}$ vérifie $j^3=1$, alors j est racine au moins double de P.
3. Factoriser P en produit de polynômes irréductibles dans $\mathbb{C}[X]$ puis dans $\mathbb{R}[X]$.

Relations racines coefficients : exercices

Soit $P=p_0+p_1.X+\cdots+p_d.X^d=p_d(X-\alpha_1).\ldots.(X-\alpha_d)$ un polynôme de degré $d\geq 2$. On a alors

$$\frac{p_0}{p_d}=(-1)^d\prod_{j=1}^{d}\alpha_j \text{ et } \frac{p_{d-1}}{p_d}=-\sum_{j=1}^{d}\alpha_j.$$

Exercice 10.—Déterminer les solutions du système d'inconnue $(a,b)\in\mathbb{C}^2$

$$\left\{\begin{array}{rcl} a+b & = & 2\\ a.b & = & \frac{1}{2}\end{array}\right.$$

Indication:Montrer qu'un couple (a,b) est solution ssi c'est le couple des racines d'un certain polynôme de degré 2.

Exercice 11.— Soit $n\geq 2$. On pose $P=(X+1)^n-1$.
1. Déterminer toutes les racines de P dans $\mathbb{C}$, puis factoriser P.
2. Soit $Q\in\mathbb{C}[X]$, de degré supérieur ou égal à 1. Exprimer la relation existant entre le produit des racines de Q et le terme constant dans Q.
3. Déterminer un polynôme Q vérifiant $P=XQ$ puis calculer à l'aide de Q.2 : $\prod_{k=1}^{n-1}\sin\left(\frac{k\pi}{n}\right)$.

Exercice 12.— Somme et produit des racines n-ièmes de l'unité
Soit $n\in\mathbb{N}^*$. Calculer le produit et la somme des racines n-ièmes de l'unité.

Exercice 13.— Un parallélépipède a pour côtés d'arêtes les trois nombres (réels positifs), a, b et c. On appelle V son volume, S la surface de ses faces et P la longueur totale de ses arêtes.
1. Exprimer P, S et V en fonction de a, b et c et montrer l'égalité polynomiale

$$(X-a)(X-b)(X-c)=X^3-\frac{P}{4}X^2+\frac{S}{2}X-V$$

2. En étudiant à quelle(s) condition(s) nécéssaires la fonction définie par le membre de droite admet trois racines réelles positives, montrer qu'il n'existe pas de parallélépipède vérifiant $P^2<24S$.
3. Montrer que si $P^2=24S$ alors le seul parallélépipède possible est un cube.

Exercice 14.— Soient n et p deux entiers naturels tels que $p\leq n$.
1. Pour $x\in\mathbb{R}^*$, calculer de deux façons différentes $\sum_{k=p}^{n}(1+x)^k$ en terme de puissances de x.
2. En déduire deux écritures différentes du polynôme $\sum_{k=p}^{n}(1+X)^k$. Grâce au coefficient de X^p, calculer :

$$\sum_{k=p}^{n}\binom{k}{p}.$$

Application des polynômes en dénombrement/probabilités (Attention, très très technique)

La technique utilisée dans l'exercice 14 est une technique commune, dûe à LAPLACE en théorie des probabilités. Il s'agit de la construction du *polynôme générateur* d'une loi de v.a. prenant un nombre fini de valeurs entières positives : Si X est une telle variable, sa loi est donnée par la suite $p = (p_k)_{k\in\mathbb{N}} = (\mathbb{P}(X = k))_{k\in\mathbb{N}}$ dont seul un nombre fini de termes est non nul. Connaitre cette suite, c'est connaitre le polynôme (la fonction polynomiale) de $\mathbb{R}[t]$:

$$P_X(t) = \sum_{k=0}^{K^*} p_k.t^k$$

où K^* est un entier à partir duquel $p_k = 0$. Ce polynôme est lié à l'espérance et la variance de X par le biais des formules

$$\mathbb{E}(X) = P_X'(1) \text{ et } \mathbb{E}(X.(X-1)) = \mathbb{V}(X) + \mathbb{E}(X)^2 - \mathbb{E}(X) = P_X''(1)$$

Ce type de technique permet de retrouver par exemple espérance et variance de nombreuses lois discrètes. On en donne une variante permettant de calculer espérances et variances des lois hypergéométriques.

On rappelle [15] que la loi hypergéométrique $\mathscr{H}(n,p,N)$ de paramètres N, n, $p = b/N$ est la loi du nombre de boules blanches obtenues en n tirages sans remise d'une urne contenant initialement N boules dont $b = p.N$ blanches.

Pour une v.a. $X \sim \mathscr{H}(n,p,N)$, à valeurs dans $\{\max(0,n-(1-p)N),\dots,\min(n,p.N)\}$, on a

$$\forall k \in \{\max(0,n-(1-p)N),\dots,\min(n,p.N)\}, \mathbb{P}(X=k) = \frac{\binom{p.N}{k}.\binom{(1-p).N}{n-k}}{\binom{N}{n}}$$

Lorsque $k \in \mathbb{N}$ n'est pas dans la gamme précisée dans la formule, on a $\mathbb{P}(X=k) = 0$ et l'on convient dans les calculs suivants de considérer les coefficients binomiaux écrits comme nuls lorsque leurs arguments sont hors de la zone de définition habituelle. Pour $t,s \in \mathbb{R}$, $N \in \mathbb{N}^*$, définissons

$$P(t,s) = \sum_{n=0}^{N} \binom{N}{n} \left(\sum_k \frac{\binom{p.N}{k}.\binom{(1-p).N}{n-k}}{\binom{N}{n}} t^k \right) s^n$$

On a

$$\begin{aligned} P(t,s) &= \sum_{n=0}^{N} \binom{N}{n} \left(\sum_{k+\ell=n} \frac{\binom{p.N}{k}.\binom{(1-p).N}{\ell}}{\binom{N}{n}} (s.t)^k.s^\ell \right) = \left(\sum_k \binom{p.N}{k} (s.t)^k \right) \left(\sum_\ell \binom{(1-p).N}{\ell} s^\ell \right) \\ &= (1+s.t)^{p.N}(1+s)^{(1-p).N} \end{aligned}$$

On peut remarquer que pour $t = 1$, on a

$$P(1,s) = \sum_{n=0}^{N} \binom{N}{n} \left(\sum_k \frac{\binom{p.N}{k}.\binom{(1-p).N}{n-k}}{\binom{N}{n}} \right) s^n = (1+s)^{p.N+(1-p).N} = (1+s)^N$$

En développant à gauche et en identifiant les coeff de s^n, on a [16]

$$\left(\sum_k \frac{\binom{p.N}{k}.\binom{(1-p).N}{n-k}}{\binom{N}{n}} \right) = 1$$

Evaluons maintenant espérance et variance de la loi hypergéométrique. On a

15. Cette loi n'est plus au programme central de mathématiques de BCPST2, elle est cependant présente dans le programme d'informatique

16. Ce qui est normal car on a une loi de v.a.

1. Pour l'espérance,

$$\begin{aligned}\frac{\partial P(t,s)}{\partial t} &= \sum_{n=0}^{N}\binom{N}{n}\left(\sum_k \frac{\binom{p.N}{k}.\binom{(1-p).N}{n-k}}{\binom{N}{n}}k.t^{k-1}\right)s^n \\ &= p.N.s.(1+t.s)^{p.N-1}.(1+s)^{(1-p).N}\end{aligned}$$

En prenant $t=1$, on obtient l'égalité de polynômes (en s),

$$\sum_{n=0}^{N}\binom{N}{n}\left(\sum_k \frac{\binom{p.N}{k}.\binom{(1-p).N}{n-k}}{\binom{N}{n}}k\right)s^n = p.N.s.(1+s)^{N-1}$$

En développant et en identifiant les coefficients de chaque monôme s^n, on a donc, pour $1 \leq n \leq N$

$$\binom{N}{n}\sum_k \frac{\binom{p.N}{k}.\binom{(1-p).N}{n-k}}{\binom{N}{n}}k = p.N.\binom{N-1}{n-1}$$

Après simplification, il vient

$$\sum_k \frac{\binom{p.N}{k}.\binom{(1-p).N}{n-k}}{\binom{N}{n}}k = p.N.\frac{n}{N} = p.n \text{ } i.e. \text{ } \mathbb{E}(X) = n.p$$

.

2. Pour la variance,

$$\begin{aligned}\frac{\partial^2 P(t,s)}{\partial t^2} &= \sum_{n=0}^{N}\binom{N}{n}\left(\sum_k \frac{\binom{p.N}{k}.\binom{(1-p).N}{n-k}}{\binom{N}{n}}k.(k-1).t^{k-2}\right)s^n \\ &= p.N(p.N-1).s^2.(1+t.s)^{p.N-2}.(1+s)^{(1-p).N}\end{aligned}$$

En prenant $t=1$, on obtient l'égalité de polynômes (en s),

$$\sum_{n=0}^{N}\binom{N}{n}\left(\sum_k \frac{\binom{p.N}{k}.\binom{(1-p).N}{n-k}}{\binom{N}{n}}k.(k-1)\right)s^n = p.N.(p.N-1)s^2.(1+s)^{N-2}$$

En développant en en identifiant les coefficients de s^n, on a donc, pour $2 \leq n \leq N$

$$\binom{N}{n}\sum_k \frac{\binom{p.N}{k}.\binom{(1-p).N}{n-k}}{\binom{N}{n}}k.(k-1) = p.N.(p.N-1)\binom{N-2}{n-2}$$

Après simplification, il vient

$$\sum_k \frac{\binom{p.N}{k}.\binom{(1-p).N}{n-k}}{\binom{N}{n}}k.(k-1) = p.N.(p.N-1)\frac{n.(n-1)}{N.(N-1)}$$

i.e. $\mathbb{E}(X.(X-1)) = p.n.(p.N-1)\frac{(n-1)}{(N-1)}$ et en utilisant $\mathbb{V}(X) = \mathbb{E}(X.(X-1)) + \mathbb{E}(X) - \mathbb{E}(X)^2$, on obtient

$$\mathbb{V}(X) = n.p(1-p).\frac{N-n}{N-1}$$