ENTIERS ET DENOMBREMENT

PLAN

I : Les entiers

1– Le principe de récurrence

Peano (1858-1932) a posé les axiomes qui régissent $\mathbb{N}$. (Un axiome est une propriété servant de base à la construction d'une théorie et dont il est impossible de montrer la véracité ou la fausseté. Ils servent à poser les règles de fonctionnement de l'objet que l'on définit et sont considérés comme inhérents à la nature de l'objet considéré).

Il existe un ensemble noté $\mathbb{N}$ dont les éléments seront appelés entiers naturels et une fonction appelée *successeur* définie sur cet ensemble, et vérifiant les axiomes suivants :

i) 0 est un entier naturel
ii) tout entier naturel possède un successeur
iii) Deux entiers naturels ayant le même successeur sont égaux
iv) 0 n'est le successeur d'aucun entier naturel
v) Si une partie A de $\mathbb{N}$ contient 0 et si le successeur de tout élément de A appartient à A, alors A est égale à $\mathbb{N}$

v) est à la base du principe de récurrence. Soit P un prédicat sur $\mathbb{N}$, i.e. une fonction définie sur $\mathbb{N}$ à valeur dans {vrai, faux} (autrement dit, pour tout n, $P(n)$ prend l'une des valeurs vrai ou faux).

$$\text{si}\begin{cases} P(0) \\ \forall\, n \in \mathbb{N},\, P(n) \Rightarrow P(n+1) \end{cases} \qquad \text{alors } \forall\, n \in \mathbb{N},\, P(n)$$

On applique en effet l'axiome v) avec la partie A = $\{n \mid P(n)\}$.

EXEMPLE :

On rappelle que, pour tout entier n, $\sum_{k=0}^{n} k = \dfrac{n(n+1)}{2}$. Qu'en est-il de la somme des carrés ?

Montrons par récurrence que :

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

On note $P(n)$ le prédicat $\sum_{k=0}^{n} k^2 = \dfrac{n(n+1)(2n+1)}{6}$.

$P(0)$ est vérifié car $P(0) \Leftrightarrow 0 = 0$
Soit n quelconque. Supposons $P(n)$ vérifié. Montrons $P(n+1)$:

$$\sum_{k=0}^{n+1} k^2 = \sum_{k=0}^{n} k^2 + (n+1)^2 = \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \quad \text{car } P(n) \text{ est supposée vraie}$$

$$= \frac{(n+1)(2n^2+n+6n+6)}{6} = \frac{(n+1)(2n^2+7n+6)}{6} = \frac{(n+1)(n+2)(2n+3)}{6}$$

$$= \frac{(n+1)((n+1)+1)(2(n+1)+1)}{6}$$

ce qui est bien la propriété demandée.

On pourra de même montrer par récurrence que $\sum_{k=0}^{n} k^3 = \dfrac{n^2(n+1)^2}{4}$

Les axiomes de Peano permettent de définir sur $\mathbb{N}$ l'addition, le produit, la relation d'ordre, avec toutes leurs propriétés bien connues ... Nous ne nous étendrons pas sur ce sujet et nous admettrons (ce qui est bien connu) que :

+ est associative	$\forall\,(a, b, c),\ (a+b)+c = a+(b+c)$
+ est commutative	$\forall\,(a, b),\ a+b = b+a$
+ possède un élément neutre 0	$\forall\, a,\ a+0 = a$
$\times$ est associatif	
$\times$ est commutatif	
$\times$ possède un élément neutre, 1, successeur de 0	$\forall\, a,\ a \times 1 = a$
$\times$ est distributif par rapport à l'addition	$\forall\,(a, b, c),\ (a+b)\times c = ac+bc$

La relation d'ordre est telle que, pour tout n, il n'existe aucun entier x vérifiant $n < x < n+1$, et pour tout couple d'entiers (n, m), $n < m \Leftrightarrow n+1 \leq m$.

Début de partie réservée aux MPSI
$\mathbb{Z}$ est construit de façon que tout les éléments de $\mathbb{N}$ possède un symétrique pour +. $(\mathbb{Z}, +, \times)$ est alors un *anneau*. Cet anneau est commutatif (car le produit est commutatif), unitaire (car le produit

admet un neutre), intègre (ce qui signifie que : $ab = 0 \Rightarrow a = 0$ ou $b = 0$). $\mathbb{Q}$ est construit de façon que tout élément non nul possède un inverse pour $\times$. $(\mathbb{Q}, +, \times)$ est alors un *corps*.

Fin de partie réservée aux MPSI

2– Propriétés de $\mathbb{N}$

Les propriétés de ce paragraphe paraîtront évidentes en soi. Une démonstration est cependant donnée, car il s'agit de théorèmes se déduisant du principe de récurrence, et non d'axiomes supplémentaires.

PROPOSITION :
Toute partie non vide de $\mathbb{N}$ possède un plus petit élément

Démonstration :
Par l'absurde. Soit A une partie non vide n'admettant pas de plus petit élément. On a :

$\forall a \in A, 0 \leq a$

si n vérifie : $\forall a \in A, n \leq a$, alors n minore A, mais comme A ne possède pas de plus petit élément, n ne peut être élément de A. Donc :

$$\forall a \in A, n < a$$

Cette dernière affirmation est équivalente à :

$$\forall a \in A, n + 1 \leq a.$$

Soit $P(n)$ le prédicat $\forall a \in A, n \leq a$. On a montré que :

$$\begin{cases} P(0) \\ \forall n \in \mathbb{N}, P(n) \Rightarrow P(n+1) \end{cases}$$

Le principe de récurrence permet de conclure : $\forall n \in \mathbb{N}, P(n)$

ou encore : $\forall n \in \mathbb{N}, \forall a \in A, n \leq a$.

Or ceci est absurde. Il suffit de prendre $a \in A$ et $n = a + 1$ pour arriver à une contradiction.

COROLLAIRE :
Toute suite strictement décroissante de $\mathbb{N}$ est finie.

Démonstration :
Prendre comme partie A l'ensemble des termes de la suite. Le fait que A admette un plus petit élément x_n et que la suite soit décroissante entraîne que x_n est nécessairement le dernier élément de la suite.

Cette propriété a été utilisée par Fermat (1601-1665) sous la forme suivante : Pour montrer qu'une propriété P est vraie pour tout n, Fermat montre que si P est fausse pour un entier, alors elle est fausse pour un entier strictement plus petit. Ce qui est impossible, car en itérant le procédé, on construirait une suite strictement décroissante d'entiers. Cette méthode s'appelle principe de descente infinie de Fermat. C'est une des premières méthodes utilisées pour montrer qu'une propriété est vraie pour tout entier, à une époque où le principe de récurrence n'était pas encore clairement formulé.

COROLLAIRE :
Toute partie de $\mathbb{N}$ non vide majorée admet un plus grand élément.

Démonstration :

Soit A une partie non vide majorée. L'ensemble M de ses majorants est donc non vide. M étant non vide admet un plus petit élément m.

si $m = 0$, alors nécessairement A = {0} et 0 est le plus grand élément de A.

si $m > 0$, alors $m - 1$ n'appartient pas à M, (puisque m est le plus petit élément de M), donc $m - 1$ ne majore pas A. Il existe donc un élément a de A tel que :

$$m - 1 < a \leq m$$

Donc $a = m$, et comme m majore A, a est bien le plus grand élément de A.

3– La division euclidienne

La plupart des propriétés de $\mathbb{Z}$ reposent sur la division euclidienne :

PROPOSITION (DIVISION EUCLIDIENNE) :

Soit a et b deux entiers (relatifs) tels que b soit strictement positif. Alors il existe un couple unique (q,r) tels que :

$$a = bq + r$$
$$\text{et } 0 \leq r < b$$

q s'appelle le quotient, r s'appelle le reste.

Ceci formalise les opérations bien connues de division dans les entiers. La division de 36 par 5 donne 7 comme quotient et 1 comme reste.

Démonstration :

Prouvons l'existence. Considérons d'abord le cas où $a \geq 0$. Soit A l'ensemble des entiers naturels q tels que $a - bq \geq 0$. A est non vide car 0 appartient à A. A est majoré par a. En effet :

$$q \in \text{A} \Rightarrow a \geq bq \text{ or } bq \geq q \text{ car } b \geq 1 \text{ donc } a \geq q$$

A admet donc un plus grand élément q. $q + 1$ n'est donc pas élément de A. D'où :

$$\begin{cases} a - bq \geq 0 \\ a - b(q+1) < 0 \end{cases} \Leftrightarrow 0 \leq a - bq < b$$

La quantité $r = a - bq$ vérifie donc bien $0 \leq r < b$.

Si $a < 0$, on applique le résultat précédent à $-a$. Il existe donc q et r tels que :

$$\begin{cases} -a = bq + r \\ 0 \leq r < b \end{cases} \Rightarrow \begin{cases} a = b(-q) - r = b(-q-1) + b - r \\ 0 < b - r \leq b \end{cases}$$

Si $r = 0$, $a = b(-q)$ convient. Si $r > 0$, $-q-1$ est le quotient, $b - r$ est le reste.

Il reste à prouver l'unicité. Si l'on a :

$$\begin{cases} a = bq + r = bq' + r' \\ 0 \leq r < b \text{ et } 0 \leq r' < b \end{cases}$$

alors :

$b(q - q') = r' - r$ avec $|r' - r| < b$

donc $|b(q - q')| < b$

donc $|q - q'| < 1$ car $b \neq 0$

donc $|q - q'| = 0$ et $q = q'$

donc on a aussi $r = r'$.

Lorsque $r = 0$, on dit que b divise a, et on note $b \mid a$.

Début de partie réservée aux MPSI

On peut remarquer que, dans $\mathbb{N}^*$, | est une relation d'ordre.
Fin de partie réservée aux MPSI

Pour n entier non nul, on définit également une relation de congruence, reliant deux entiers a et b ayant même reste dans la division euclidienne par n :

$$a \equiv b \bmod n \Leftrightarrow \exists\, q,\ a = b + nq \Leftrightarrow n \mid a - b$$

ce qu'on note encore $a \equiv b\ [n]$. Il s'agit d'une relation d'équivalence, compatible avec la somme et le produit. Autrement dit :

$$\begin{cases} a \equiv b \bmod n \\ a' \equiv b' \bmod n \end{cases} \Rightarrow \begin{cases} a + a' \equiv b + b' \bmod n \\ aa' \equiv bb' \bmod n \end{cases}$$

En effet :

$$\begin{cases} a \equiv b \bmod n \\ a' \equiv b' \bmod n \end{cases} \Rightarrow \exists\, (q, q') \text{ tel que } \begin{cases} a = b + nq \\ a' = b + nq' \end{cases}$$

$$\Rightarrow \begin{cases} a + a' = b + b' + n(q + q') \equiv b + b' \bmod n \\ aa' = bb' + n(bq' + qb' + nqq') \equiv bb' \bmod n \end{cases}$$

EXEMPLE :
On appelle sous-groupe G de $\mathbb{Z}$, une partie non vide de $\mathbb{Z}$ telle que :

$$\begin{cases} \forall\, x \in G,\ \forall\, y \in G,\ x + y \in G \\ \forall\, x \in G,\ -x \in G \end{cases}$$

On se propose de déterminer les sous-groupes de $\mathbb{Z}$.

G = {0} est un exemple trivial de sous-groupe. Soit G un sous–groupe de $\mathbb{Z}$, différent de {0}. On a :

i) $0 \in G$

prendre x dans G et calculer $x + (-x)$.

ii) si $x \in G$, alors $\forall\, n \in \mathbb{Z},\ nx \in G$

Il suffit de le montrer pour n élément de $\mathbb{N}$. La propriété $P(n)$: $nx \in G$ est vérifiée pour $n = 0$ et pour $n = 1$. Si elle est vraie pour n, elle est vraie pour $n + 1$, puisque $(n + 1)x = nx + x$, que nx et x sont tous deux dans G et que G est stable pour la somme.

iii) $\exists\, x \in G,\ x > 0$

Prendre x non nul, et si $x < 0$, prendre $-x$

iv) Soit m le plus petit élément strictement positif de G (qui existe puisque l'ensemble des éléments de G strictement positifs est non vide d'après iii). Montrons que : $\forall\, x \in G,\ \exists\, q \in \mathbb{Z}$ tel que $x = qm$. En effet, il existe q et r tels que : $x = mq + r$ avec $0 \leq r < m$. Donc $r = x - mq$. Or x est élément de G, mq aussi (d'après ii), donc r aussi. Or r est positif ou nul, et inférieur à m. m étant le plus petit élément de G strictement positif, r est nécessairement nul.

Nous avons ainsi montré que $G = \{mq \mid q \in \mathbb{Z}\}$, ensemble noté $m\mathbb{Z}$. Inversement, il n'est pas difficile de voir que tout ensemble de la forme $m\mathbb{Z}$ est un sous–groupe de $\mathbb{Z}$. Ainsi, les sous-groupes de $\mathbb{Z}$ sont de la forme $m\mathbb{Z}$.

4– Nombres premiers

On appelle nombre premier tout nombre entier supérieur ou égal à 2 qui n'est divisible que par 1 et par lui-même. Les premiers entiers premiers sont :

2 3 5 7 11 13 17 19 23 29 31 37 41 ...

Euclide a montré qu'il existait une infinité de nombres premiers. Par ailleurs, tout nombre entier peut se décomposer en un produit de nombres premiers, la décomposition étant unique à l'ordre près des facteurs.

II : Listes

1– Sans répétition

Les concepts suivants sont analogues :

- ranger dans l'ordre p objets pris parmi n.
- définir une suite $(x_1, ..., x_p)$ avec x_i éléments distincts deux à deux d'un ensemble de n éléments. x_i est l'objet rangé en i-ème position.
- définir une injection d'un ensemble à p éléments dans un ensemble à n éléments. L'injection est $i \in \{1, ..., p\} \rightarrow x_i \in \{1, ..., n\}$ et c'est une injection si et seulement si les x_i sont distincts.

On définit dans ce cas une liste (sans répétition) de p éléments parmi n. Le nombre de telles listes est :

$$n(n-1)(n-2)...(n-p+1) = \frac{n!}{(n-p)!} \quad \text{si } p \leq n$$

En effet, on choisit d'abord un objet parmi n, puis un deuxième parmi les $n - 1$ restants, puis un troisième parmi les $n - 2$ restants, etc..., les choix se multipliant (le etc... cache en fait une récurrence implicite que seuls les lecteurs avides d'une parfaite rigueur mettront en évidence).

Si $p > n$, ce nombre est nul.

EXEMPLE :

On considère 5 boules de couleurs différentes. On en prend 3 que l'on range dans un certain ordre. Il y a 60 dispositions possibles.

Dans le cas où $p = n$, on obtient une identité entre :

- ranger dans l'ordre n objets.
- définir une permutation de n objets.
- définir une bijection entre deux ensembles de n éléments.

Le nombre de permutation est $n!$

2– Avec répétition

Les concepts suivants sont analogues :

- ranger dans l'ordre p objets, chaque objet étant doté d'un attribut choisi parmi n (par exemple la couleur). Deux objets de même attributs sont indiscernables.
- définir une suite $(x_1, ..., x_p)$ avec x_i éléments distincts ou non d'un ensemble de n éléments. x_i désigne l'attribut de l'objet placé en i-ème position, le même attribut pouvant apparaître plusieurs fois.
- définir une application d'un ensemble à p éléments dans un ensemble à n éléments. L'application est $i \in \{1, ..., p\} \rightarrow x_i \in \{1, ..., n\}$ sans condition sur les x_i.

On définit dans ce cas une liste avec répétition de p éléments parmi n. Le nombre de telles listes est n^p. Pour chacun des p objets, il y a en effet n choix.

EXEMPLE 1 :
On considère des boules de 5 couleurs possibles. On en prend 3 que l'on range dans un certain ordre. Il y a 125 dispositions possibles.

EXEMPLE 2 :
Soit E un ensemble de n éléments et $\mathcal{P}$(E) l'ensemble des parties de E. Pour chaque partie A de E, on définit la fonction indicatrice de A par :

$$\begin{aligned} &\mathrm{E} \to \{0,1\} \\ &x \to \mathbf{1}_\mathrm{A}(x) = 1 \text{ si } x \in \mathrm{A} \\ &\qquad\qquad\quad\; 0 \text{ si } x \notin \mathrm{A} \end{aligned}$$

Inversement, toute fonction f de E dans $\{0,1\}$ est une fonction indicatrice. Son ensemble associé est $\mathrm{A} = \{x \mid f(x) = 1\}$. On définit ainsi une bijection entre $\mathcal{P}$(E) et l'ensemble des applications de E dans $\{0,1\}$. Il existe 2^n fonctions de E dans $\{0,1\}$. Il existe donc 2^n éléments de $\mathcal{P}$(E) ou parties de E.

III : Combinaisons

1– Sans répétition

Les concepts suivants sont analogues :

- choisir un ensemble de p objets pris parmi n, l'ordre des éléments choisis n'intervenant pas.
- définir une suite $(x_1, ..., x_p)$ avec x_i éléments d'un ensemble de $\{1, ..., n\}$, vérifiant $x_1 < x_2 < ... < x_p$. On numérote les n objets de 1 à n, et les x_i désignent les numéros des p éléments choisis. Puisque l'ordre de choix n'intervient pas, on peut classer les numéros par ordre croissant. Les inégalités sont strictes car les éléments sont distincts.

On définit dans ce cas une combinaison (sans répétition) de p éléments parmi n. Le nombre de telles combinaisons est :

$$\frac{n(n-1)(n-2)...(n-p+1)}{p!} = \frac{n!}{p!(n-p)!} = \binom{n}{p} \text{si } 0 \leq p \leq n$$

On le lit "p parmi n" ce qui correspond exactement à la situation consistant à choisir p objet parmi n. On retrouve cette quantité en probabilité dans le nombre de chemins conduisant à p succès dans la loi binomiale, puisque ce nombre de chemins revient à définir, parmi les n expériences de Bernoulli, quelles seront les p expériences qui donneront un succès, et donc à choisir p expériences parmi les n.

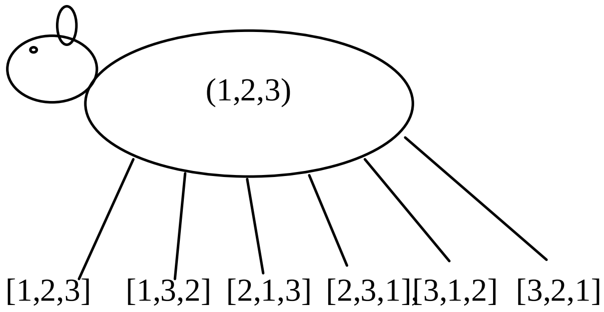
(Si $p > n$, ce nombre est nul). On note aussi (de plus en plus rarement) C_n^p le coefficient binomial.

Plus généralement, pour α réel quelconque et p entier, on note :

$$\binom{\alpha}{p} = \frac{\alpha(\alpha-1)...(\alpha-p+1)}{p!}$$

mais on prendra garde que pour α non élément de $\mathbb{N}$, il n'y a pas de définition de la factorielle de α.

Montrons donc que $\binom{n}{p} = \dfrac{n(n-1)(n-2)...(n-p+1)}{p!}$. En effet, chaque combinaison de p éléments peut être définie à partir de p! listes ordonnées différentes, obtenues en rangeant les p éléments en question selon toutes les permutations possibles de ces p éléments. Il y a donc p! fois moins de combinaisons que de telles listes. Or le nombre de listes ordonnées de p éléments distincts parmi n est $n(n-1)(n-2)...(n-p+1)$, puisqu'il y a n choix possibles pour le premier élément de la liste, $n-1$ pour le deuxième, $n-2$ pour le troisième, etc..., $n-p+1$ pour le $p^{\text{ème}}$. Cette méthode de raisonnement est connue sous le nom de principe des bergers. Pour compter ses moutons, le berger compte en effet le nombre de pattes et divise le résultat par 4.
Dans le cas présent, un mouton formant une combinaison possède p! pattes constituées de chacune des listes donnant cette combinaison.



Comme il y a au total $n(n-1)(n-2)...(n-p+1)$ listes et que chaque mouton possède p! pattes, il y a bien $\dfrac{n(n-1)(n-2)...(n-p+1)}{p!}$ moutons.

Sous une forme abstraite, le principe des bergers s'énonce également de la façon suivante :
Etant donnés deux ensembles E et F, et une application f de E dans F tels que, pour tout élément y de F, Card $f^{-1}(\{y\}) = p$, alors Card E $= p \times$ Card F.

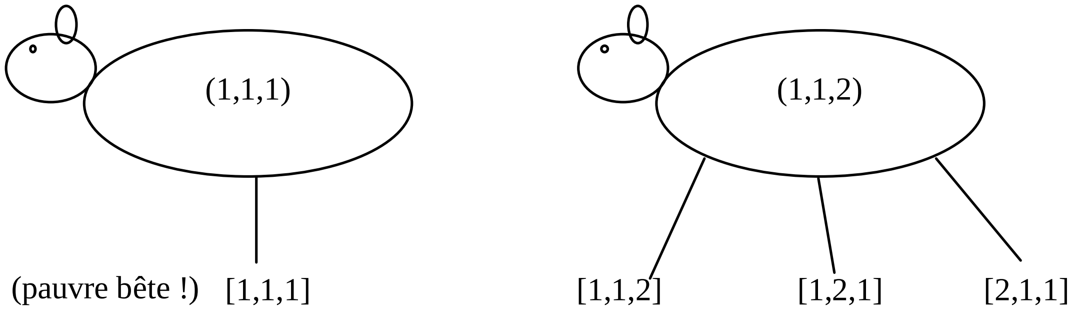
EXEMPLE :
On considère 5 boules de couleurs différentes. On en prend 3 dans un ordre arbitraire. Il y a 10 choix possibles.

2– Avec répétition

Les concepts suivants sont analogues :

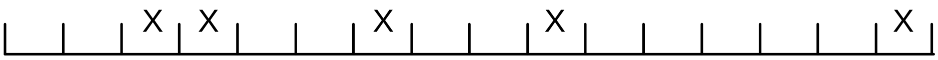
- choisir une suite non ordonnée de p objets, chaque objet étant doté d'un attribut choisi parmi n (par exemple la couleur). Deux objets de même attributs sont indiscernables.
- définir une suite $(x_1, ..., x_p)$ avec x_i éléments de $\{1, ..., n\}$ vérifiant $x_1 \leq x_2 \leq ... \leq x_p$. On numérote les n attributs possibles de 1 à n, et les x_i désignent les numéros des p attributs des éléments choisis. Puisque l'ordre de choix n'intervient pas, on peut classer les numéros par ordre croissant. Les inégalités sont larges car le même attribut peut apparaître plusieurs fois.
- définir une suite $(a_1, ..., a_n)$ avec $a_1 + ... + a_n = p$. a_i désignent le nombre de fois où l'attribut i est choisi.

On définit dans ce cas une combinaison avec répétition de p éléments parmi n. Le nombre de telles combinaisons est difficile à trouver à partir des listes. En effet, les moutons n'ont pas tous le même nombre de pattes ☹ !!



Il convient alors de coder la situation de façon à se ramener à un problème connu.

Nous disposons de n caractères distincts C_1, C_2, ..., C_n. On place, dans une suite de $n + p - 1$ cases, $n - 1$ croix qui séparent les objets de même caractère des autres. Chaque case non occupée par une croix correspond à un objet d'un caractère donné. Le nombre de cases non occupées est donc égal à p :



Dans l'exemple précédent, on a $n = 6$, $p = 11$; il y a $a_1 = 2$ objets C_1, $a_2 = 0$ objets C_2, $a_3 = 2$ objets C_3, $a_4 = 2$ objet C_4, $a_5 = 5$ objet C_5, $a_6 = 0$ objet C_6. Cette disposition correspond alors à la combinaison (1,1,3,3,4,4,5,5,5,5,5).

Il y a donc $\binom{n+p-1}{p}$ dispositions possibles. Un moyen de mémoriser ce résultat est le suivant :

$$\binom{n+p-1}{p} = \frac{(n + p - 1)(n + p)...(n + 1)n}{p!}$$

alors que $\binom{-n}{p} = \dfrac{(-n)(- n - 1)...(- n - p + 1)}{p!} = (-1)^p \binom{n+p-1}{p}$

Ainsi, le nombre de combinaisons avec répétition de p objets parmi n peut aussi s'écrire $\left|\binom{-n}{p}\right|$, à comparer au nombre de combinaisons sans répétition qui est $\binom{n}{p}$.

EXEMPLE :
On considère des boules de 5 couleurs possibles. On en prend 3. Il y a 35 choix possibles.

IV : Formules classiques des coefficients binomiaux

1– Valeurs courantes

A savoir sans hésitation

$$\binom{n}{0} = \binom{n}{n} = 1 \qquad \binom{n}{1} = \binom{n}{n-1} = n \qquad \binom{n}{2} = \binom{n}{n-2} = \frac{n(n-1)}{2}$$

2– Formules de récurrence

On prouve aisément que :

$$\binom{n}{n-p} = \binom{n}{p} \qquad \binom{n}{p} = \frac{n}{p}\binom{n-1}{p-1} \text{ pour } n \geq 1 \qquad \binom{n}{p} = \binom{n-1}{p-1} + \binom{n-1}{p}$$

La troisième formule se démontre par le calcul, ou bien en considérant que parmi les n objets, il en existe un possédant une marque particulière. Choisir p objets parmi n, c'est alors :

ou bien choisir l'objet marqué et $p-1$ objets parmi les $n-1$ restants

ou bien choisir p objets parmi les $n-1$ objets non marqués.

Elle reste vraie pour $p = 0$ en convenant que $\binom{n-1}{-1} = 0$, et pour $n = p$ puisque $\binom{n-1}{n} = 0$.

Cette formule se visualise dans le triangle de Pascal de la façon suivante :

1												
1	1											
1	2	1										
1	3	3	1									
1	4	6	4	1								
1	5	10	10	5	1							
1	6	15	20	15	6	1						
1	7	21	35	35	21	7	1					
1	8	28	56	70	56	28	8	1				
1	9	36	84	126	126	84	36	9	1			
1	10	45	120	210	252	210	120	45	10	1		
1	11	55	165	330	462	462	330	165	55	11	1	
1	12	66	220	495	792	924	792	495	220	66	12	1

EXERCICE :

En itérant la troisième formule, on prouve par récurrence sur n que :

$$\binom{n}{p} = \binom{n-1}{p-1} + \binom{n-2}{p-1} + \binom{n-3}{p-1} + \ldots + \binom{p}{p-1} + \binom{p-1}{p-1}$$

Elle peut se montrer directement de la façon suivante. On considère n boules numérotées de 1 à n. On a $\binom{n}{p}$ choix d'en tirer p, et parmi ces choix, il y en a $\binom{n-1}{p-1}$ d'en choisir p dont le numéro maximum est n, $\binom{n-2}{p-1}$ choix dont le numéro maximum est $n-1$, ..., $\binom{p}{p-1}$ choix dont le numéro maximum est $p+1$ et $\binom{p-1}{p-1} = 1$ choix dont le numéro maximum est p.

Cette formule se visualise enfin dans le triangle de pascal de la façon suivante :

1												
1	1											
1	2	1										
1	3	3	1									
1	4	6	4	1								
1	5	10	10	5	1							
1	6	15	20	15	6	1						
1	7	21	35	35	21	7	1					
1	8	28	56	70	56	28	8	1				
1	9	36	84	126	126	84	36	9	1			
1	10	45	120	210	252	210	120	45	10	1		
1	11	55	165	330	462	462	330	165	55	11	1	
1	12	66	220	495	792	924	792	495	220	66	12	1

3– Formule du binôme de Newton

Dans un anneau commutatif unitaire (pour les MPSI) ou dans tout ensemble doté d'une somme et d'un produit ayant les propriétés usuelles (pour les PCSI), on a :

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

Cette formule se montre par récurrence sur n. En effet, elle est vraie pour $n = 0$ ou $n = 1$. Si elle est vraie au rang n, alors :

$$(a+b)^{n+1} = \Big(\sum_{p=0}^{n} \binom{n}{p} a^p\, b^{n-p}\Big)(a+b) =$$

$$= \sum_{p=0}^{n} \binom{n}{p} a^{p+1}\, b^{n-p} + \sum_{p=0}^{n} \binom{n}{p} a^p\, b^{n-p+1}$$

$$= \sum_{p=1}^{n+1} \binom{n}{p-1} a^p\, b^{n-p+1} + \sum_{p=0}^{n} \binom{n}{p} a^p\, b^{n-p+1}$$

en faisant le changement d'indice $p+1 \rightarrow p$ dans la première somme

$$= \sum_{p=0}^{n+1} \left(\binom{n}{p-1} + \binom{n}{p}\right) a^p\, b^{n-p+1} \quad \text{avec la convention} \binom{n}{-1} = \binom{n}{n+1} = 0$$

$$= \sum_{p=0}^{n+1} \binom{n+1}{p} a^p\, b^{n+1-p} \text{ avec la formule} \binom{n}{p-1} + \binom{n}{p} = \binom{n+1}{p}$$

Annexe I : Sur le principe de récurrence

Le principe de récurrence ne se prouve pas. Comme nous l'avons dit, c'est un axiome supposé par définition être vérifié par les entiers. Cependant, on trouve parfois dans la littérature mathématiques des tentatives de justification. En voici deux exemples :

Le premier est un extrait d'un livre paru en 1993 (Le langage CAML, Weis et Leroy, InterEditions) :

> *Le principe de récurrence s'énonce informellement ainsi ; si une certaine propriété sur les nombres entiers est vraie pour 0 et si la propriété est vraie pour le successeur d'un*

nombre dès qu'elle est vraie pour ce nombre, alors cette propriété est vraie pour tous les nombres. Formellement : soit $P(n)$ *une propriété qui dépend d'un entier* n*. Si les phrases suivantes sont vraies :*

1. $P(0)$ *est vraie,*
2. *si* $P(n)$ *est vraie, alors* $P(n+1)$ *est vraie,*

alors $P(n)$ *est vraie pour tout* n*.*

Ce principe est en fait évident : les deux propriétés demandées par le principe de récurrence permettent facilement de démontrer la propriété P pour toute valeur entière. Par exemple, supposons que P vérifie les deux propriétés et qu'on veuille démontrer que P est vraie pour 2*. Puisque P est vraie pour* 0*, elle est vraie pour son successeur* 1*. Mais puisque P est vraie pour* 1*, elle est vraie pour son successeur, donc elle est vraie pour* 2*. Il est clair que ce raisonnement se poursuit sans problème pour tout nombre entier fixé à l'avance.*

On prendra conscience que le principe de récurrence n'est pas une évidence en soi. Ainsi, Gödel (1906-1978) dans les années 1930 a présenté un prédicat[1] stupéfiant $P(n)$ tel que :

pour tout n, il existe une démonstration de $P(n)$

il n'existe pas de démonstration de $\forall\ n, P(n)$

En effet, la réunion de toutes les démonstrations de $P(n)$ n'est pas une démonstration de $\forall\ n, P(n)$, car cette réunion est infinie, or une démonstration se doit d'être finie. C'est cette objection qui rend invalide la tentative de justification de ce texte. Le principe de récurrence consiste justement à décider d'accepter comme démonstration valide une démarche qui nécessiterait une infinité de pas. C'est un élargissement de la notion de démonstration qui est ainsi proposé.

Le deuxième exemple est tiré de la revue *Tangente* de Décembre 1987 (n° 2). Il affirme démontrer le principe de récurrence. Or il n'en est rien. Il y a une faille[2] dans le raisonnement qui n'échappera pas à un esprit sagace.

Premièrement : Le principe de descente infinie de Fermat. Il ne peut exister de suite infinie strictement décroissante d'entiers naturels.

Démonstration : si (x_n) *était une telle suite, on aurait* $x_{n+1} < x_n$ *pour tout n entier naturel, donc* $x_{n+1} \leq x_n - 1$*. En appliquant ceci à* $n = 0, 1, 2, \ldots$*, on trouve successivement :* $x_1 \leq x_0 - 1$*,* $x_2 \leq x_1 - 1$*, etc. On en déduit :* $x_2 \leq x_0 - 2$*,* $x_3 \leq x_0 - 3, \ldots,$ $x_n \leq x_0 - n$*. En prenant* $n = x_0 + 1$*, on obtient* $x_n < -1$*, ce qui contredit le fait que la suite* x_n *est composée d'entiers naturels.*

Deuxièmement : Le principe du bon ordre. Tout ensemble non vide X d'entiers naturels comporte un plus petit élément.

Démonstration : Si X n'avait pas de plus petit élément, alors pour chaque élément de X, il y en aurait un autre, strictement plus petit. Partant d'un élément donné a appartenant à X, on pourrait fabriquer ainsi une suite strictement décroissante : $x_0 = a$*,* $x_1 < x_0$*,* $x_2 < x_1$*, etc, infinie, composée d'éléments de X, ce qui contredit le principe précédent.*

---

[1] Ce prédicat est par exemple exposé dans le livre grand public de Douglas Hofstader, *Gödel, Escher, Bach,* InterEditions (1985), p.507.

[2] La faille réside dans le fait que la relation $x_n \leq x_0 - n$ se montre évidemment par récurrence !! Le principe de récurrence est donc supposé valide pour pouvoir montrer le principe de descente infini de Fermat.

Troisièmement : Le principe de récurrence. Soit X un ensemble d'entiers naturels contenant 0 qui vérifie la propriété suivante : pour tout x appartenant à X, alors $x+1$ appartient à X. On peut en conclure que X est l'ensemble de tous les entiers naturels.

Démonstration : Si X n'était pas l'ensemble de tous les entiers naturels, soit Y l'ensemble des entiers naturels y non éléments de X. D'après le principe du bon–ordre, cet ensemble Y aurait un plus petit élément y_0 qui ne serait pas égal à 0, puisque 0 appartient à X. Donc $y_0 \geq 1$ et par suite $y_0 - 1$ appartient à $\mathbb{N}$. Si $y_0 - 1$ appartient à X, on a de par la propriété de X : $(y_0 - 1) + 1$ appartient à X, soit y_0 appartient à X, ce qui est impossible. Si $y_0 - 1$ n'appartient pas à X, on a $y_0 - 1$ dans Y, impossible encore car y_0 est le plus petit élément de l'ensemble Y.

En outre, il est possible de rejeter l'axiome de récurrence, débouchant ainsi sur une nouvelle théorie, celle de l'analyse non standard, évoquée ci-après.

Annexe II : Analyse non standard

Le plus généralement, on se laisse facilement convaincre de la validité du principe de récurrence. Il paraît en effet irréfutable que, si une propriété P définie sur $\mathbb{N}$ vérifie P(0) et si, pour tout n, $P(n) \Rightarrow P(n+1)$, on a nécessairement $P(n)$ vrai pour tout n. P(0) et $P(0) \Rightarrow P(1)$ étant vrais, on peut en déduire que P(1) est vrai. De même P(1) et $P(1) \Rightarrow P(2)$ vrais permettent d'en déduire que P(2) est vrai, et ainsi de suite pour les autres entiers.

Il y a cependant une difficulté qui est ici en général escamotée. Car si pour montrer P(1.000.000.000), il est possible d'écrire les 2.000.000.000 de lignes suivantes :

P(0) vrai
et $P(0) \Rightarrow P(1)$ donc P(1) vrai
P(1) vrai
et $P(1) \Rightarrow P(2)$ donc P(2) vrai
. . .
. . . (je me permets d'économiser un peu de papier)
. . .
P(999.999.999) vrai
et $P(999.999.999) \Rightarrow P(1.000.000.000)$ donc P(1.000.000.000) vrai

en revanche, pour montrer que $P(n)$ est vrai pour ***tout*** entier, il faudrait écrire une ***infinité*** de lignes. Or une démonstration se doit, par essence, d'être ***finie***.

Il est en fait vain de chercher une démonstration du principe de récurrence. Il fait partie des axiomes de Peano. Or comme tout axiome, la décision de l'adopter ne relève pas d'une évidence en soi, mais d'un choix arbitrairement fait, essentiellement pour des raisons de commodité ou d'efficacité.

De même que le rejet de l'axiome d'Euclide conduit aux géométrie non-euclidienne, que se passe-t-il si l'on décide de ***rejeter l'axiome de récurrence*** ? On obtient alors une nouvelle théorie mathématique totalement étrangère à tout ce à quoi nous sommes habitués, mais tout aussi cohérente que la théorie usuelle (si tant est que celle-ci le soit, ce qu'on ignore). Que signifie rejeter le principe de récurrence ? Cela signifie que, dans notre nouvel ensemble d'entiers, il existe un prédicat P tel que l'on ait ***simultanément*** les ***trois*** propriétés suivantes :

P(0) est vrai
$\forall n, P(n) \Rightarrow P(n+1)$
$\exists n$, non $P(n)$

Quel sens donner à un tel prédicat P ? Est-ce concevable ? Comment définir une propriété vraie pour 0, vraie pour $n + 1$ si elle est vraie pour n, et cependant fausse pour un certain entier. Voici une possibilité. Les entiers n vérifiant la propriété P seront qualifiés d'accessibles, de limités, ou de standard. Les entiers n ne vérifiant pas la propriété P seront qualifiés d'inaccessibles, d'illimités, ou de non standard. Ainsi, 0 est accessible. Si n est accessible, alors $n + 1$ l'est aussi. Cependant, il existe des entiers qui nous sont inaccessibles. Finalement, cette position n'est peut-être pas si incroyable que cela. Après tout, la propriété P ainsi définie ne correspond-elle pas à la réalité ? Cette position a été développée par Nelson dans les années 1960. Il définit l'analyse non standard de la façon suivante :

- On se place dans le cadre de la théorie des ensembles de Zermelo-Fraenkel (celle que nous pratiquons tous sans le savoir, comme M. Jourdain).
- Les objets ou les ensembles définis par cette théorie seront qualifiés d'**internes** ou **classiques**.
- On introduit un nouveau prédicat, **étranger à la théorie de Zermelo-Fraenkel**, et qui s'applique sur les ensembles internes. Un tel ensemble ou objet pourra être qualifié de **standard** ou de **non standard**. Ce prédicat est une notion primitive au même titre que la notion d'ensemble ou d'appartenance.
- On définit trois règles – que nous ne détaillerons pas ici – permettant de manipuler ce nouveau prédicat.

Pour comprendre cette démarche, faisons un parallélisme avec ce que vivent les élèves de Terminale lorsqu'ils découvrent les nombres complexes :
- Ils se placent dans le cadre des nombres rencontrés jusqu'en Première.
- De tels nombres sont qualifiés de **réels**.
- On introduit un nombre, **étranger aux réels**, baptisé ***i***.
- On définit les règles de calcul relatives à i (essentiellement $i^2 = -1$)

Une fois cette démarche adoptée, on dispose d'une théorie mathématique plus riche qu'avant. (Il faut bien sûr s'assurer que l'on a pas introduit d'incohérence). Pour en revenir à l'analyse non standard, le principe de récurrence continuera à s'appliquer aux prédicats internes. En particulier, la somme des n premiers entiers continuera à valoir $\frac{n(n+1)}{2}$. Mais le principe de récurrence **ne peut pas** s'appliquer aux entiers non standard, car le fait d'être standard ou non n'est pas une propriété interne. 0 est standard. Si n est standard, alors $n + 1$ est standard, **mais** il existe néanmoins des entiers non standard. Ceci est déroutant (mais peut-être tout autant que d'admettre qu'il existe un nombre de carré –1 ! !).

A quoi peut bien servir cette théorie ? Il y a deux types d'applications :
- Il a été établi qu'un énoncé interne, possédant une démonstration dans le cadre de l'analyse non standard, était vrai dans le cadre des mathématiques classiques. La situation est tout à fait comparable aux calculs numériques réels qui donnent un résultat réel valide, même si, transitoirement, on a utilisé les nombres complexes.
- L'analyse non-standard permet en outre de manipuler les concepts nouveaux de nombre infiniment petit ou d'infiniment grand qui ont posé tant de problèmes aux mathématiciens et qui avaient été bannis de l'analyse. Elle est donc plus générale, de même que l'analyse complexe est plus générale que l'analyse réelle.

◆