Les Entiers Naturels

MPSI-1 Prytanée National Militaire

Pascal Delahaye : D'après le cours d'Alain Soyeur

10 janvier 2011

1 Les axiomes de Péano (1858 - 1932).

DÉFINITION 1 : **Définition de $\mathbb{N}$**
Il existe un ensemble $\mathbb{N}$ dont les éléments seront appelés *Entiers Naturels* et une fonction appelée *successeur* définie sur cet ensemble, et vérifiant les axiomes suivants :

1. 0 est un entier naturel
2. tout entier naturel possède un successeur
3. deux entiers naturels ayant le même successeur sont égaux
4. 0 n'est le successeur d'aucun entier naturel
5. si $A \in \mathcal{P}(\mathbb{N})$ contient 0 et si le successeur de tout élément de A appartient à A, alors A est égal à $\mathbb{N}$.

Remarque 1.
- Le 5ème axiome permet de justifier le principe de récurrence.
- Ces axiomes permettent de définir sur $\mathbb{N}$ l'addition, le produit, la relation d'ordre avec toutes les propriétés bien connues (associativité, commutativité ... etc ...)

DÉFINITION 2 : **Définitions de $\mathbb{Z}$ et $\mathbb{Q}$**
L'ensemble $\mathbb{Z}$ est alors construit pour que chaque élément de $\mathbb{N}$ admette un *symétrique* pour l'addition.
$(\mathbb{Z}, +, \times)$ a alors la structure d'anneau (voir cours sur les structures algébriques).

L'ensemble $\mathbb{Q}$ est alors construit pour que chaque élément non nul de $\mathbb{Z}$ admette un *symétrique* pour la multiplication. $(\mathbb{Q}, +, \times)$ a alors la structure de corps (voir cours sur les structures algébriques).

2 Le principe de récurrence.

Remarque 2. Tous les théorèmes suivants sont valables en remplaçant 0 par n_0, un entier naturel quelconque.

THÉORÈME 1 : **Récurrence simple** (un seul prédécesseur)
Soit une proposition $\mathcal{P}_n$ dépendant d'un entier n. On suppose que :

1. $\mathcal{P}_0$ est VRAI ;
2. $\forall n \geq 0$, $\mathcal{P}_n \Rightarrow \mathcal{P}_{n+1}$.

Alors la proposition $\mathcal{P}_n$ est vraie pour tout $n \geq 0$.

Preuve 1 : On applique l'axiome P5 à la partie $A = \{n \in \mathbb{N}$ vérifiant $P_n\}$.

`Exemple` 1. $(*)$ Montrer par récurrence que $\forall n \in \mathbb{N}^*$,

a) $1^2 + 2^2 + \cdots + n^2 = \displaystyle\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$ b) $1^3 + 2^3 + \cdots + n^3 = \displaystyle\sum_{k=1}^{n} k^3 = \frac{[n(n+1)]^2}{4}$

Remarque 3.

1. Si vous n'utilisez pas P_n pour démontrer P_{n+1}, c'est qu'il n'y a pas besoin de faire une récurrence.
2. Il faut démontrer "$\mathcal{P}_n \Rightarrow \mathcal{P}_{n+1}$" pour tout n à partir du rang d'initialisation (0 dans la plupart des cas).

Rédaction d'une récurrence

1. Pour tout $n \geq 0$, soit P_n : ...
2. Montrons que P_0 est vraie : ...
3. Hypothèse de Récurrence :
   Soit $n \geq 0$: supposons que P_n est vraie et prouvons la propriété P_{n+1} ...
4. Conclusion : P_n est donc vraie pour tout $n \geq 0$

Une variante du théorème précédent se présente sous la forme :

COROLLAIRE 2 : **Récurrence forte**
Soit une proposition $\mathcal{P}_n$ dépendant d'un entier n. On suppose que :

1. $\mathcal{P}_0$ est VRAI ;
2. $\forall n \geq 0$, $\mathcal{P}_0 \ldots \mathcal{P}_n \Rightarrow \mathcal{P}_{n+1}$.

Alors la proposition $\mathcal{P}_n$ est vraie pour tout $n \geq 0$.

Remarque 4. Dans le cas d'une récurrence forte, l'hypothèse de récurrence se rédige donc sous la forme :
"Soit $n \in \mathbb{N}$. Supposons que P_q est vrai pour tout entier q compris entre 0 et n."

`Exemple` 2. $(*)$ Démontrer que tout entier naturel $n \geq 2$ admet un diviseur premier.

Exercice : 1

$(*)$ Soit (u_n) la suite définie par $u_0 \geq 0$ et $u_{n+1} = \ln(1 + u_0.u_1 \ldots u_n)$ pour tout $n \geq 0$.
Prouver que (u_n) est définie pour tout $n \in \mathbb{N}$ et que $\forall n \in \mathbb{N}$, $u_n \geq 0$.

Parfois, la récurrence nécessite de prouver la propriété voulue pour plusieurs valeurs initiales de n.
On utilise alors le corollaire suivant du principe de récurrence :

COROLLAIRE 3 : **Récurrence avec plusieurs prédécesseurs**
On considère une proposition $\mathcal{P}_n$ dépendant d'un entier n. On suppose que :

1. $\mathcal{P}_0, \mathcal{P}_1, \ldots, \mathcal{P}_k$ sont VRAIES.
2. $\forall n \geq 0$, $\big(\mathcal{P}_n$ et $\mathcal{P}_{n+1}$ et ... et $\mathcal{P}_{n+k}\big) \Rightarrow \mathcal{P}_{n+k+1}$.

Alors $\forall n \geq 0$, la proposition $\mathcal{P}_n$ est vraie.

Remarque 5.

1. Dans le cas d'une récurrence avec k prédécesseurs, l'hypothèse de récurrence se rédige donc sous la forme :
   "Soit $n \in \mathbb{N}$. Supposons que P_q est vrai pour tout entier q compris entre n et $n + k$."
2. On détecte facilement un cas de récurrence avec plusieurs prédécesseurs lorsque la démonstration de $\mathcal{P}_{n+k+1}$ nécessite l'utilisation de $\mathcal{P}_n$ et $\mathcal{P}_{n+1}$ et ... et $\mathcal{P}_{n+k}$ avec k indépendant de n. Dans ce cas, il faut obligatoirement démontrer les k premières propriétés dans l'étape d'initialisation !!
3. Alors que l'initialisation d'une récurrence forte ne se fait que pour la première valeur de n, en revanche, celle d'une récurrence avec p prédécesseurs porte sur les p premières valeurs de n.

Exercice : 2

$(*)$ Soit (F_n) la suite de Fibonacci définie par $\begin{cases} F_0 = 0 \\ F_1 = 1 \end{cases}$ et pour tout $n \in \mathbb{N}$: $F_{n+2} = F_n + F_{n+1}$.

1. Montrer que $\forall n \in \mathbb{N}$, on a : $F_n \leq 2^n$.
2. Montrer que pour tout $n \in \mathbb{N}$ $F_n = \dfrac{\sqrt{5}}{5}(\alpha^n - \beta^n)$ où α et β sont les racines de $-x^2 + x + 1 = 0$ avec $\alpha > \beta$.

Remarque 6. On pourra envisager d'utiliser le principe de récurrence dès qu'il faut démontrer qu'une propriété est vraie pour tout entier n (ou presque).

3 Propriétés fondamentales.

La relation d'ordre sur $\mathbb{N}$ est définie de la façon suivante :

$$\forall (n, m) \in \mathbb{N}^2,\ n \leq m \Longleftrightarrow \exists k \in \mathbb{N},\ m = n + k$$

Avec cette relation d'ordre, l'ensemble des entiers naturels possède les trois propriétés données dans le théorème suivant :

Théorème 4 : **Plus petit et plus grand élément d'une partie de $\mathbb{N}$**

- (P_1) Toute partie $A \subset \mathbb{N}$ non-vide possède un plus petit élément.
- (P_2) Toute partie $A \subset \mathbb{N}$ non-vide et majorée possède un plus grand élément.
- (P_3) Toute suite d'éléments de $\mathbb{N}$ strictement décroissante est finie.

Preuve 4 : Démonstrations non exigible !

`Exemple` 3. La propriété précédente a été, par exemple, utilisée dans le cours sur les structures algébriques pour démontrer l'existence de l'indice de nilpotence d'un élément nilpotent d'un anneau non intègre.

Définition 3 : **Ensembles dénombrables**
Tout ensemble E tel qu'il existe une bijection de $\mathbb{N}$ dans E est dit *dénombrable*.

Remarque 7. Cela revient à dire qu'il est possible de compter les éléments de E, ou encore que E et $\mathbb{N}$ ont "le même nombre d'éléments".

`Exemple` 4. $(**-***)$

1. Tout ensemble infini contenu dans $\mathbb{N}$ est dénombrable.
   En particulier, l'ensemble des nombres pairs et des nombres premiers sont dénombrables.
2. $\mathbb{Z}$ et $\mathbb{Q}$ sont dénombrables.

`Contre-Exemple` 1. $(***)$ Prouver que $[0, 1[$ (et donc, que $\mathbb{R}$ ..) n'est pas dénombrable.

Exercice : 3
$(*)$ Prouver que $\mathbb{R}$ et $]0, 1[$ ont le même nombre d'éléments.

4 Ensembles finis

On définit pour $(p, q) \in \mathbb{N}^2$ tels que $p \leq q$, l'intervalle d'entiers : $[\![p,q]\!] = \{k \in \mathbb{N} \text{ tq } p \leq k \leq q\}$.

Définition 4 : **Ensembles finis**
Soit E un ensemble non vide.
On dira que E est un ensemble *fini* lorsqu'il existe un entier $n \in \mathbb{N}^*$ et une bijection $\phi : [\![1,n]\!] \mapsto E$.
Par convention, on dira que l'ensemble vide $\emptyset$ est également un ensemble fini.

Remarque 8. Cette définition revient à dire que l'on peut compter les éléments de E.

Théorème 5 : **Unicité du cardinal**
Si E est un ensemble fini non vide, alors l'entier n de la définition précédente est unique.
Il sera appelé le *cardinal* de E et noté $|E|$ ou card(E)
On dira que $\emptyset$ a un cardinal nul : $\text{Card}(\emptyset) = 0$.

Preuve 5 : On admet que s'il existe une bijection de $[\![1,p]\!]$ dans $[\![1,q]\!]$, alors $p = q$.

Pour montrer que deux ensembles ont même cardinal, il suffira de trouver une bijection de l'un vers l'autre.

Théorème 6 : Soient deux ensembles finis E et F tels que $F \subset E$. Alors :

1. $\text{Card}(F) \leq \text{Card}(E)$
2. Si $\text{Card}(F) = \text{Card}(E)$ alors $F = E$

Preuve 6 : Théorème admis !

Pour montrer que deux ensembles E et F de même cardinal sont égaux, il suffit de prouver que $E \subset F$

Remarque 9. On verra en algèbre linéaire une propriété analogue pour démontrer l'égalité de deux espaces vectoriels.

Théorème Fondamental 7 : **Applications entre ensembles finis**
Soient deux ensembles finis E et F, et une application $f : E \mapsto F$. On a :

1. $\begin{cases} \mathrm{Card}(f(E)) \leq \mathrm{Card}(E) \\ \mathrm{Card}(f(E)) \leq \mathrm{Card}(F) \end{cases}$
2. f est injective $\iff$ $\mathrm{Card}(f(E)) = \mathrm{Card}(E)$
3. f est surjective $\iff$ $\mathrm{Card}(f(E)) = \mathrm{Card}(F)$
4. Dans le cas où $\mathrm{Card}(E) = \mathrm{Card}(F)$: (f injective) $\iff$ (f surjective) $\iff$ (f bijective)

Preuve 7 : Théorème admis !

Théorème 8 : **Parties finies de $\mathbb{N}$**

1. Une partie non vide $\mathcal{P}$ de $\mathbb{N}$ est finie si et seulement si elle est majorée.
2. Si $\mathcal{P}$ est une partie finie non vide de $\mathbb{N}$ de cadinal n, alors il existe une unique bijection strictement croissante de $[\![1,n]\!]$ sur $\mathcal{P}$.

Preuve 8 :

1. $\Rightarrow$ Comme $\mathbb{N}$ est un ensemble totalement ordonné, il admet un plus grand élément.
   $\Leftarrow$ Facile !
2. On note f la bijection cherchée. On construit f de la façon suivante :
   $f(1)$ est le plus petit élément de $\mathcal{P}$, $f(2)$ le plus petit élément de $\mathcal{P}\backslash\{f(1)\}$ ...etc ...
   Si $\exists k \in [\![1,n]\!]$ pour lequel $f(k)$ n'est pas défini de la façon précédente (on prend le plus petit k), alors f n'est plus strictement croissante. Ceci prouve l'unicité.

5 Dénombrements fondamentaux

L'objectif de cette section est de présenter les concepts et résultats fondamentaux permettant de calculer le cardinal d'ensembles finis donnés.

Lemme 9 : **Lemme des Bergers**

1. Si $\mathcal{P} = (A_1, \ldots, A_p)$ est une *partition* d'un ensemble fini E, on a : $\mathrm{Card}(E) = \mathrm{Card}(A_1) + \cdots + \mathrm{Card}(A_p)$
2. Si A et B sont deux ensembles finis, on a : $\mathrm{Card}(A \cup B) = \mathrm{Card}(A) + \mathrm{Card}(B) - \mathrm{Card}(A \cap B)$.

Lemme des bergers	Partition d'un ensemble

`Exemple` 5. Pour compter le nombre d'élève de MPSI1, on peut additionner le nombre d'élèves aux yeux bleus et le nombre d'élèves aux yeux verts avec le nombre d'élèves aux yeux marrons (plus les albinos s'il y en a !).

Théorème 10 :
Soient deux ensembles finis E et F, avec $\mathrm{Card}(E) = n$ et $\mathrm{Card}(F) = p$. Alors :

$$E \times F \text{ est fini} \quad \text{et} \quad \boxed{\mathrm{Card}(E \times F) = np}$$

Preuve 10 : Il suffit de compter ...

Remarque 10. Cette formule se généralise à $\text{Card}(E_1 \times \cdots \times E_k)$ où $E_1, \ldots, E_k$ sont k ensembles finis.

Exemple 6. $(*)$ Trouver le nombre de diviseurs de 1800.

5.1 Les arrangements sans répétition

Définition 5 :
On obtient un *arrangement de p éléments parmi n* lorsqu'on choisit p éléments différents parmi n éléments possibles en tenant compte de l'ordre dans lequel ils ont été choisis.

Remarque 11. Pour dire qu'un objet est un arrangement, on s'intéresse à l'objet lui-même mais surtout à la façon dont il a été "construit".

Remarque 12. Les objets suivants sont des arrangements :
- Un p-uplet $(x_1, \ldots, x_p)$ construit à partir de p éléments distincts 2 à 2 choisis dans un ensemble de n éléments.
- Une injection d'un ensemble à p éléments dans un ensemble à n éléments.

Définition 6 : Soit $n \in \mathbb{N}^*$. On note : $\boxed{n! = 1.2.3\ldots.n}$ et on convient que $0! = 1$

Théorème 11 :
Si $0 \leq p \leq n$, le nombre d'arrangements possibles obtenus en choisissant p éléments parmi n est :

$$\boxed{A_n^p = \frac{n!}{(n-p)!}} = n \times (n-1) \times \cdots \times (n-p+1)$$

Preuve 11 : Notons E_n un ensemble à n éléments. et $\mathcal{A}_p^n$ l'ensemble des arrangements possibles de E_n.
On a alors $\mathcal{A}_p^n = E_n \times E_{n-1} \times \cdots \times E_1$ ...

Remarque 13.
- Si $\text{Card}(E) = \text{Card}(F) = n$, le nombre d'applications bijectives de E vers F vaut $n!$
- $n!$ est aussi le nombre de permutations d'un ensemble E à n éléments

5.2 Les arrangements avec répétition (p-liste)

Définition 7 : On obtient un *arrangement "avec répétition" de p éléments parmi n* lorsqu'on choisit p éléments avec remise parmi n éléments possibles en tenant compte de l'ordre dans lequel ils ont été choisis.

Remarque 14. Les objets suivants sont aussi des arrangements avec répétition :
- Une suite de p objets identiques, muni chacun d'eux d'un attribut choisi parmi n (ex : la couleur) : deux objets munis du même attribut étant indiscernables. (on choisit ici l'attribut, et non l'objet)
- Un p-uplet $(x_1, \ldots, x_p)$ construit à partir de p éléments distincts ou non choisis dans un ensemble de n éléments.
- Une application d'un ensemble à p éléments dans un ensemble à n éléments.

Théorème 12 :
Soient $p, n \in \mathbb{N}$.
Le nombre d'arrangements avec répétition obtenus à l'aide de p éléments choisis parmi n est : $\boxed{n^p}$

Preuve 12 : Notons E_n un ensemble à n éléments et $\mathcal{P}_p^n$ l'ensemble des arrangements avec répétition de E_n.
On a alors $\mathcal{P}_p^n = E_n \times E_n \times \cdots \times E_n$ ...

Exemple 7. On considère des boules de 5 couleurs possibles. On en prend 3 que l'on range dans un certain ordre. Combien peut-on obtenir de dispositions différentes ? (2 boules de même couleur étant indiscernables)

5.3 Les combinaisons

Définition 8 : On obtient une *combinaison de p éléments parmi n* lorsqu'on choisit p éléments différents parmi n éléments possibles sans tenir compte de l'ordre dans lequel ils ont été choisis.

`Exemple` 8. Les éléments suivants sont des combinaisons :
1. Un ensemble $\{x_1, \ldots, x_p\}$ construit avec p éléments distincts choisis dans un ensemble de n éléments.
2. Un p-uplet $(x_1, \ldots, x_p)$ construit avec p éléments distincts choisis dans un ensemble de n éléments, vérifiant $x_1 < x_2 < \cdots < x_p$ (cas d'une "main" de cartes).

Théorème 13 :
Si $0 \leq p \leq n$, le nombre de combinaisons possibles de p éléments parmi n est :

$$\boxed{\binom{n}{p} = \frac{n!}{(n-p)!p!}} \quad = \frac{A_n^p}{p!} \quad = \frac{n \times (n-1) \times \cdots \times (n-p+1)}{p \times (p-1) \times \cdots \times 1}$$

Preuve 13 : Si on décide de tenir compte de l'ordre, chaque combinaison génère $p!$ arrangements.

`Exemple` 9. $(*)$
1. Quel est le nombre de façons de placer k boules identiques dans n urnes pouvant contenir au plus 1 boule ?
2. Quel est le nombre de façons de placer k boules numérotées dans n urnes pouvant contenir au plus 1 boule ?

`Exemple` 10. $(*)$ Trouver le nombre d'applications strictement croissantes de l'intervalle $[\![1,p]\!]$ vers l'intervalle $[\![1,n]\!]$.

Exercice : 4

$(**)$ On trace dans un plan n droites en position générale (i.e. deux d'entre elles ne sont jamais parallèles ni trois d'entre elles concourantes). Combien forme-t-on ainsi de triangles ?

5.4 Nombre de parties d'un ensemble

Théorème 14 :
Si E est un ensemble de cardinal $n \in \mathbb{N}^*$, alors : $\boxed{\mathrm{Card}(P(E)) = 2^n}$

Preuve 14 : Simple récurrence en effectuant une partition judicieuse de $\mathcal{P}(E)$.

`Exemple` 11. $(*)$ Soit un ensemble fini E, de cardinal n, et un entier $0 \leq p \leq n$.
Le nombre de parties de E de cardinal p vaut $\binom{n}{p}$. En déduire la valeur de : $\displaystyle\sum_{k=0}^{n} \binom{n}{p}$

6 Propriétés des coefficients binômiaux

Théorème 15 : **Propriétés des coefficients binômiaux**
Soient $0 \leq p \leq n$ deux entiers. Les coefficients binômiaux vérifient les propriétés suivantes :

- ***Premiers termes*** :

  1. $\binom{n}{0} = \binom{n}{n} = 1$ 2. $\binom{n}{1} = \binom{n}{n-1} = n$ 3. $\binom{n}{2} = \binom{n}{n-2} = \frac{n(n-1)}{2}$

- ***Symétrie*** : $\binom{n}{p} = \binom{n}{n-p}$

- ***Evolution*** : $\left(\binom{n}{k}\right)_{k\in[\![1,n]\!]}$ est $\begin{cases} strict^t \text{ croissante jusqu'à } k = E(\frac{n}{2}) \\ strict^t \text{ décroissante de } k = E(\frac{n}{2}) + 1 \text{ à } k = n \end{cases}$

Preuve 15 : Simples calculs ...
Pour l'*évolution*, on s'intéresse au rapport $\binom{n}{k}/\binom{n}{k-1}$ dans les cas où n est pair et où n est impair.

Structure des coefficients binômiaux (cas pair)	Structure des coefficients binômiaux (cas impair)

Remarque 15. L'élément maximal de la suite $\binom{n}{p}$ avec $0 \le p \le n$ est : $\omega(n) = \binom{n}{E(n/2)}$.

Exercice : 5

$(**)$ En utilisant le théorème des gendarmes, déterminer la limite de la suite (u_n) définie par : $u_n = \displaystyle\sum_{k=0}^{n} \frac{1}{\binom{n}{k}}$

PROPOSITION 16 : Formules

1. *Factorisation* : $\binom{n}{p} = \frac{n}{p}\binom{n-1}{p-1}$ (si $p \ge 1$) 2. *Additivité* : $\binom{n}{p} + \binom{n}{p+1} = \binom{n+1}{p+1}$

Preuve 16 : Simples calculs ...

Remarque 16.
1. Interpréter les relations de symétrie et d'additivité en termes d'ensembles.
2. Comment utiliser chacune de ces deux relations pour programmer récursivement la calcul de $\binom{n}{p}$?

`Exemple` 12. $(*)$ En appliquant la formule de factorisation, prouver que $\displaystyle\sum_{p=0}^{n} p\binom{n}{p} = n.2^{n-1}$.

Exercice : 6

$(**)$ Démontrer que pour tout $n \ge 1$: $\binom{2n}{n} \ge \dfrac{4^n}{2n+1}$

De l'additivité, on obtient le *triangle de Pascal* qui permet de calculer de proche en proche tous les coefficients binômiaux.

	0	1	2	3	p	$p+1$
0	1					
1	1	1				
2	1	2	1			
3	1	3	3	1		
n						
$n+1$						

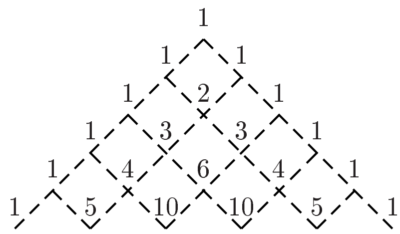

FIG. 1 – *Triangle de Pascal*

THÉORÈME 17 : Formule du binôme de Newton

Soient deux réels $a, b \in \mathbb{R}$ et un entier $n \in \mathbb{N}$. Alors

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

Preuve 17 :
1. Méthode 1 : Par récurrence (Bon entraînement au calcul sur des sommes).
2. Méthode 2 : Par dénombrement (Facile).

Remarque 17. La formule du binôme de Newton est très souvent utilisées.
Comme le montre les exemples suivants, elle permet en particulier, de calculer des sommes faisant intervenir des coefficients binômiaux.

`Exemple` 13. (∗) Calculer les sommes $S_1 = \sum_{k=0}^{n} \binom{n}{k}$ et $S_2 = \sum_{k=0}^{n} \frac{1}{3^k}\binom{n}{k}$

Exercice : 7

(∗∗) Calculer les sommes :

1. $S_1 = \sum_{\substack{0\leq k\leq n \\ k \text{ pair}}} \binom{n}{k}$
2. $S_2 = \sum_{\substack{0\leq k\leq n \\ k \text{ impair}}} \binom{n}{k}$

Exercice : 8

(∗∗) Calculer les sommes :

1. $S_1 = \sum_{k=0}^{n} k\binom{n}{k}$
2. $S_2 = \sum_{k=0}^{n} \frac{1}{k+1}\binom{n}{k}$
3. $S_3 = \sum_{k=0}^{n} k^2\binom{n}{k}$