PCSI - mathématiques

Entiers naturels - dénombrements

Die ganzen Zahlen hat der liebe Gott gemacht, alles anderes ist Menschwerk.

Leopold KRONECKER

Il revient à Giuseppe PEANO d'avoir dégagé, en 1889, le plus petit ensemble d'axiomes permettant de caractériser l'ensemble des entiers naturels. Toutefois, les cinq *axiomes de Peano* historiques sont différents de ceux que nous utilisons dans le cadre de ce cours.

1 Entiers naturels

On admet l'existence d'un ensemble, noté $\mathbb{N}$, dont les éléments sont appelés *entiers naturels*, vérifiant les propriétés suivantes :

[$\mathbb{N}0$] $\mathbb{N}$ est *non vide* et muni d'une relation d'*ordre total* notée $\leq$.

[$\mathbb{N}1$] Toute partie non vide de $\mathbb{N}$ admet un plus petit élément pour $\leq$.

[$\mathbb{N}2$] Toute partie non vide majorée de $\mathbb{N}$ admet un plus grand élément pour $\leq$.

[$\mathbb{N}3$] $\mathbb{N}$ n'admet pas de plus grand élément.

Ces propriétés imposées donnent immédiatement les conséquences suivantes :

- $\mathbb{N}$ a un plus petit élément, noté 0.

On pose également $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$. $\mathbb{N}^*$ n'est pas vide (sinon on aurait $\mathbb{N} = \{0\}$, contredisant [$\mathbb{N}3$]). Donc $\mathbb{N}^*$ admet à son tour un plus petit élément noté 1. $\mathbb{N}^* \setminus \{1\}$ est non vide, et ainsi de suite.

- Si $n \in \mathbb{N}$, la partie $\{p \in \mathbb{N} \mid p > n\}$ n'est pas vide (toujours [$\mathbb{N}3$]) donc admet un plus petit élément noté $n+1$: le *successeur* de n.
- Si $n \in \mathbb{N}^*$, la partie $\{p \in \mathbb{N} \mid p < n\}$ n'est pas vide (elle contient 0) et est majorée (par n) donc admet un plus grand élément noté $n-1$: le *prédécesseur* de n.

On vérifie facilement que $n = (n+1) - 1$ et (si $n \in \mathbb{N}^*$) $n = (n-1) + 1$.

1.1 Principe de récurrence

On peut donner plusieurs versions de cette propriété souvent indispensable pour faire des démonstrations dans $\mathbb{N}$. Pour démontrer qu'une partie A de $\mathbb{N}$ est égale à $\mathbb{N}$, il est nécessaire et suffisant de vérifier qu'elle contient 0 ainsi que le successeur de chacun de ses éléments :

Théorème 1 (principe de récurrence) *Soit A une partie de $\mathbb{N}$. Si*

1. $0 \in A$ *et*
2. $\forall n \in \mathbb{N},\ n \in A \Rightarrow n+1 \in A$

alors : $A = \mathbb{N}$.

Mais toute partie A de $\mathbb{N}$ peut être associée à une *propriété* $\mathcal{P}$ portant sur les entiers naturels — précisément, la propriété d'appartenir à A : $\mathcal{P}(n) \Leftrightarrow n \in A$.

Inversement, à une propriété $\mathcal{P}$ on peut associer la partie $A = \{n \in \mathbb{N} \mid \mathcal{P}(n)\}$ formée des entiers qui la vérifient.

Ceci permet de donner une nouvelle formulation du théorème 1 :

Théorème 2 *Soit $\mathcal{P}$ une propriété portant sur les entiers naturels. Si*

1. $\mathcal{P}(0)$ *et*
2. $\forall n \in \mathbb{N},\ \mathcal{P}(n) \Rightarrow \mathcal{P}(n+1)$

alors : $\forall n \in \mathbb{N},\ \mathcal{P}(n)$.

Donc, pour démontrer qu'une propriété est vraie pour tous les entiers naturels, il suffit de vérifier qu'elle est vraie pour 0 et que chaque fois qu'un entier la vérifie, il en est de même de son successeur. On peut donner une version (apparemment) affaiblie de ce résultat, parfois appelée *récurrence faible* ou *avec prédécesseurs* :

Théorème 3 *Soit $\mathcal{P}$ une propriété portant sur les entiers naturels. Si*

1. $\mathcal{P}(0)$ *et*
2. $\forall n \in \mathbb{N},\ [\forall k \in \mathbb{N},\ k < n \Rightarrow \mathcal{P}(k)] \Rightarrow \mathcal{P}(n)$

alors : $\forall n \in \mathbb{N},\ \mathcal{P}(n)$.

Ceci montre que pour effectuer l'étape de récurrence on peut supposer la propriété $\mathcal{P}$ pour *tous* les entiers $< n$.

1.2 Opérations sur $\mathbb{N}$

Les définitions "de proche en proche" de ce paragraphe reposent en fait sur le principe de définition récurrente d'une suite (th. 4).

1.2.1 Addition

La notation $n+1$ désigne le successeur de l'entier n. On définit de proche en proche (sur n) la somme $m+n$ de deux entiers m et n par

- $m+0=m$;
- $m+(n+1)=(m+n)+1$ (en supposant $m+n$ défini).

On constate que les "deux" définitions de $n+1$ (successeur de n, et somme de n et 1) sont bien en accord.

On en déduit les propriétés de l'addition de $\mathbb{N}$: $+$ est associative, commutative, admet 0 pour neutre et tout élément est régulier pour $+$.

En outre, elle est reliée à l'ordre de $\mathbb{N}$ par

$$m \leq n \Leftrightarrow \exists p,\ n = m+p \tag{1}$$

On en déduit que $+$ est compatible avec $\leq$.

Cela permet enfin de définir, si $m \leq n$, la différence $n-m$ comme l'unique entier p tel que $n = m+p$.

1.2.2 Multiplication

On définit de proche en proche le produit $m \times n$ de deux entiers m et n par

- $m \times 0 = 0$;
- $m \times (n+1) = (m \times n)+m$ (en supposant $m \times n$ défini).

On en déduit les propriétés de la multiplication de $\mathbb{N}$: $\times$ est associative, commutative, distributive par rapport à $+$, admet 1 pour élément neutre. De plus, $\times$ est compatible avec la relation d'ordre $\leq$ *sur* $\mathbb{N}^*$ *seulement*, et tout élément *non nul* est régulier pour $\times$.

Cette dernière remarque permet de définir une autre relation d'ordre sur $\mathbb{N}^*$: la relation "divise". Celle-ci est à la multiplication ce que l'ordre usuel $\leq$ est à l'addition.

Définition 1 *Si m, $n \in \mathbb{N}^*$,*

$$m \mid n \Leftrightarrow \exists p,\ n = m \times p$$

(Comparer avec la formule 1.)

L'entier p tel que $n = m \times p$ est unique ; c'est le *quotient exact* de n par m noté $\frac{n}{m}$.

1.2.3 Exponentiation

On définit de proche en proche la puissance n de l'entier m par

- $m^0 = 1$;
- $m^{n+1} = m^n \times m$ (en supposant m^n défini).

Cette opération n'a pas de propriété notable hormis l'habituelle règle des exposants.

1.3 Suites récurrentes

Le théorème suivant donne une base rigoureuse à la définition récurrente d'une suite :

Théorème 4 (principe de récursion) *Soit E un ensemble. Soient f une application de E dans E et $a \in E$.* Il existe *une* unique *application $u : \mathbb{N} \to E$ telle que $u(0) = a$ et pour tout $n \in \mathbb{N}$:*

$$u(n+1) = f(u(n)).$$

Ce résultat permet de définir une suite de réels (p. ex.) par la donnée de $u_0 = a \in \mathbb{R}$ et la relation de récurrence $u_{n+1} = f(u_n)$.

2 Ensembles finis

2.1 Intervalles de $\mathbb{N}$

Soient p, $q \in \mathbb{N}$, $p \leq q$. On note

- $[\![p,q]\!] = \{n \in \mathbb{N} \mid p \leq n \leq q\}$;
- $[\![p,q[\![= \{n \in \mathbb{N} \mid p \leq n < q\}$;
- $]\!]p,q]\!] = \{n \in \mathbb{N} \mid p < n \leq q\}$;
- $]\!]p,q[\![= \{n \in \mathbb{N} \mid p < n < q\}$.

Ces intervalles de $\mathbb{N}$ servent de base à la définition des ensembles finis. On utilisera particulièrement l'intervalle $[\![1,q]\!]$, que l'on notera $\mathbb{N}_q$. Remarquons que $\mathbb{N}_0 = \varnothing$.

Lemme 1 *Si $n \in \mathbb{N}^*$ et $a \in \mathbb{N}_n$, il existe une bijection de $\mathbb{N}_n \setminus \{a\}$ sur $\mathbb{N}_{n-1}$.*

Corollaire 1 *Soient n, $p \in \mathbb{N}$.*

1. *S'il existe une injection de $\mathbb{N}_n$ dans $\mathbb{N}_p$ alors $n \leq p$.*
2. *S'il existe une surjection de $\mathbb{N}_n$ sur $\mathbb{N}_p$ alors $n \geq p$.*
3. *S'il existe une bijection de $\mathbb{N}_n$ sur $\mathbb{N}_p$ alors $n = p$.*

Il est facile de voir que les implications mentionnées dans ce corollaire sont en fait des équivalences.

Corollaire 2 *Soit $n \in \mathbb{N}$. Toute injection (*resp. *surjection) de $\mathbb{N}_n$ dans lui-même est bijective.*

2.2 Cardinal d'un ensemble

Nous pouvons maintenant poser

Définition 2 *Soit E un ensemble. E est* fini *s'il existe un entier naturel $n \in \mathbb{N}$ et une bijection f de $\mathbb{N}_n$ sur E.*

D'après le corollaire 1, l'entier n en question est *unique.*

Définition 3 *n est le* cardinal *de E noté* $\operatorname{card} E$.

Exemple 1

1. *$\varnothing$ est fini et* $\operatorname{card} \varnothing = 0$.
2. *Si $n \in \mathbb{N}$, $\mathbb{N}_n$ est fini et* $\operatorname{card} \mathbb{N}_n = n$.

3. *(généralisation) si* $p,\ q \in \mathbb{N}$, $p \leq q$, $[\![p,q]\!]$ *est fini et* $\operatorname{card}[\![p,q]\!] = q - p + 1$.

Il est particulièrement facile de juger si une *partie de* $\mathbb{N}$ est finie grâce au

Théorème 5 *Soit* $A \subset \mathbb{N}$, $A \neq \varnothing$. *A est finie* ssi *A est majorée dans* $\mathbb{N}$.

Un ensemble E est dit *infini* s'il n'est pas fini.

Corollaire 3 $\mathbb{N}$, $\mathbb{N}^*$ *sont infinis.*

Les corollaires 1 et 2 se généralisent aux ensembles finis quelconques :

Théorème 6 *Soient* E *et* F *des ensembles finis de cardinaux respectifs* p *et* q.

1. $p \leq q$ ssi *il existe une injection de* E *dans* F ;
2. $p \geq q$ ssi *il existe une surjection de* E *sur* F ;
3. $p = q$ ssi *il existe une bijection de* E *sur* F.

Théorème 7 *Soient* E *et* F *deux ensembles* ***finis*** *de* ***même*** *cardinal* p, *et soit* f *une application de* E *dans* F. *Il y a équivalence entre*

1. f *est injective de* E *dans* F ;
2. f *est surjective de* E *sur* F ;
3. f *est bijective de* E *sur* F.

3 Dénombrement

On étudie dans ce paragraphe l'effet des opérations ensemblistes sur les ensembles finis et leurs cardinaux.

3.1 Cardinal d'une partie

Proposition 1 *Soient* E *un ensemble fini et* F *une partie de* E.

1. F *est fini et* $\operatorname{card} F \leq \operatorname{card} E$;
2. *Si* $\operatorname{card} F = \operatorname{card} E$, $F = E$.

Il résulte évidemment de ceci qu'une *intersection* d'ensembles finis est finie. Mais la connaissance de leurs cardinaux n'est pas suffisante pour connaître celui de leur intersection (*cf.* corollaire 4).

3.2 Cardinal d'une réunion

Proposition 2 *Soient* E *et* F *deux ensemble finis disjoints. Alors* $E \cup F$ *est fini et*

$$\operatorname{card} E \cup F = \operatorname{card} E + \operatorname{card} F$$

Ce résultat s'étend facilement à une réunion d'un nombre quelconque d'ensembles *deux à deux* disjoints.

Corollaire 4 *Soient* E *et* F *deux ensembles finis. Alors* $E \cup F$ *est fini et*

$$\operatorname{card} E \cup F + \operatorname{card} E \cap F = \operatorname{card} E + \operatorname{card} F$$

Cette formule peut encore se généraliser, mais moins facilement que la proposition 2. On a cependant toujours $\operatorname{card} E \cup F \leq \operatorname{card} E + \operatorname{card} F$, que E et F soient disjoints ou non.

3.3 Cardinal d'un produit

Ici, les ensembles n'ont pas besoin d'être disjoints :

Proposition 3 *Soient* E *et* F *deux ensemble finis. Alors* $E \times F$ *est fini et*

$$\operatorname{card} E \times F = \operatorname{card} E \times \operatorname{card} F$$

La généralisation au produit d'un nombre quelconque d'ensembles est immédiate :

Corollaire 5 *Soient* E_1, ..., E_n $(n \in \mathbb{N})$ n *ensembles finis. Alors* $\prod_{k=1}^{n} E_k$ *est fini et*

$$\operatorname{card} \prod_{k=1}^{n} E_k = \prod_{k=1}^{n} \operatorname{card} E_k$$

Dans le cas particulier où tous les E_k sont égaux à un même ensemble E on obtient :

Corollaire 6 *Soient* E *un ensemble fini et* $n \in \mathbb{N}$. E^n *est fini et*

$$\operatorname{card}(E^n) = (\operatorname{card} E)^n$$

3.4 Nombre d'applications

Proposition 4 *Soient* E *et* F *des ensembles finis. Alors* $\mathcal{F}(E,F)$ *est fini et*

$$\operatorname{card} \mathcal{F}(E,F) = (\operatorname{card} F)^{\operatorname{card} E}$$

3.5 Nombre de parties

Proposition 5 *Soit* E *un ensemble fini. Alors* $\mathcal{P}(E)$ *est fini et*

$$\operatorname{card} \mathcal{P}(E) = 2^{\operatorname{card} E}$$

On se propose de préciser les deux derniers résultats en comptant le nombre d'*injections* d'un ensemble dans un autre, et le nombre de parties *de cardinal* $p \in \mathbb{N}$ *fixé* d'un ensemble.

3.6 Arrangements

Le nombre d'applications injectives d'un ensemble E dans un ensemble F ne dépend que des cardinaux de E et F.

Définition 4 *Soient* $n,\ p \in \mathbb{N}$, $0 \leq p \leq n$. *On note*

$$\mathrm{A}_n^p = \operatorname{card}(\operatorname{Inj}(E,F))$$

où E *est un ensemble de cardinal* p, F *un ensemble de cardinal* n, *et* $\operatorname{Inj}(E,F)$ *désigne l'ensemble des injections de* E *dans* F.

On effectue le calcul de A_n^p par récurrence à partir du

Lemme 2 *Si* $1 \leq p \leq n$, $\mathrm{A}_n^p = n\,\mathrm{A}_{n-1}^{p-1}$.

On en déduit

Théorème 8 *Si* $n,\ p \in \mathbb{N}$, $0 \leq p \leq n$,

$$\mathrm{A}_n^p = \prod_{k=n-p+1}^{n} k = n(n-1)\ldots(n-p+1)$$

Si l'on sait dénombrer les injections, on peut faire de même pour les bijections grâce au théorème 7 :

Définition 5 *Soit $n \in \mathbb{N}$. La* factorielle *de n est*

$$n! = \operatorname{card}(\operatorname{Bij}(E))$$

où E est un ensemble de cardinal n et $\operatorname{Bij}(E)$ l'ensemble des bijections de E sur E.

Le théorème 8 donne alors :

Corollaire 7 *Si $n \in \mathbb{N}$, $n! = \prod_{k=1}^{n} k = n(n-1)...2.1$.*

Inversement, A_n^p peut s'exprimer à l'aide de factorielles :

Proposition 6 *Si n, $p \in \mathbb{N}$, $0 \leq p \leq n$, $n!$ est divisible par $(n-p)!$ et :*

$$\mathrm{A}_n^p = \frac{n!}{(n-p)!}.$$

3.7 Combinaisons

Le nombre de parties à p éléments d'un ensemble E ne dépend que de p et du cardinal n de E.

Définition 6 *Soient n, $p \in \mathbb{N}$, $0 \leq p \leq n$. On note*

$$\binom{n}{p} = \operatorname{card}(\mathcal{P}_p(E))$$

où E est un ensemble de cardinal n, et $\mathcal{P}_p(E)$ désigne l'ensemble des parties de E de cardinal p.

On peut obtenir la valeur de $\binom{n}{p}$ en la reliant à A_n^p :

Théorème 9 *Si n, $p \in \mathbb{N}$, $0 \leq p \leq n$, $p!$ divise A_n^p et*

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

Les nombres $\binom{n}{p}$ sont appelés *coefficients binomiaux* (car ils figurent dans la *formule du binôme* de Newton). Ils vérifient plusieurs relations importantes qui s'interprètent en termes d'algèbre aussi bien que de dénombrement.

Proposition 7 *Si n, $p \in \mathbb{N}$, $0 \leq p \leq n$,*

$$\binom{n}{p} = \binom{n}{n-p}.$$

Proposition 8 *Si $n \in \mathbb{N}$,*

$$\sum_{p=0}^{n} \binom{n}{p} = 2^n.$$

Proposition 9 *Si n, $p \in \mathbb{N}$, $1 \leq p \leq n$,*

$$\binom{n}{p} = \frac{n}{p}\binom{n-1}{p-1}.$$

Théorème 10 (formule du triangle de Pascal) *Si n, $p \in \mathbb{N}$, $1 \leq p \leq n$,*

$$\binom{n}{p} = \binom{n-1}{p} + \binom{n-1}{p-1}.$$

Ce théorème permet de calculer les valeurs de $\binom{n}{p}$ pour n et p "petits", plus rapidement que la formule du th. 9. On complète le tableau suivant :

$p=$	0	1	2	3	4	5	6	$\cdots$
$n=0$	1							
1	1	1						
2	1	2	1					
3	1	3	3	1				
4	1	4	6	4	1			
5	1	5	10	10	5	1		
6	1	6	15	20	15	6	1	
$\vdots$	$\vdots$							$\ddots$

en appliquant de façon répétée le motif :

$$\begin{array}{|ccc|} \hline \binom{n-1}{p-1} & \xrightarrow{+} & \binom{n-1}{p} \\ & & \downarrow = \\ & & \binom{n}{p} \\ \hline \end{array}$$

(pour calculer un terme de la ligne n, on ajoute les termes situés au-dessus et au-dessus à gauche.)

3.8 Tirage de p objets parmi n

Les calculs précédents permettent de remplir partiellement le tableau suivant. On récapitule le nombre de manières de "tirer au sort p objets parmi n"

- en prenant l'ordre en compte ou non ;
- en admettant les répétitions ou pas :

nombre de tirages	avec ordre	sans ordre
avec répétitions	n^p	Γ_n^p $(= \ ?)$
sans répétitions	A_n^p	$\binom{n}{p}$

4 Appendice : formule du binôme

Donnons à titre d'application des coefficients binomiaux et du principe de récurrence le

Théorème 11 (formule du binôme de Newton) *Soient x, $y \in \mathbb{C}$ et $n \in \mathbb{N}$. Alors*

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

Sous certaines conditions, il est possible d'étendre ce théorème à des objets plus généraux que les complexes (*cf.* le chapitre sur les structures algébriques).