CHAPITRE 10
ENTIERS ET DÉNOMBREMENT

PARTIE 10.1 : LES ENTIERS NATURELS

10.1.1 : L'ensemble $\mathbb{N}$, sa structure

REMARQUE 10.1 : Axiomes de PEANO *(vers 1889) : on admet l'existence d'un unique ensemble $\mathbb{N}$ (à isomorphisme près) tel qu'il existe une application $S : \mathbb{N} \to \mathbb{N}$ vérifiant les hypothèses suivantes :*

- *S est injective.*
- *Il existe un seul élément dans $\mathbb{N}$ (noté 0) qui n'admet pas d'antécédent par S.*
- $\forall A \in \mathcal{P}(\mathbb{N}),\ \Big(0 \in A \text{ et } \forall n \in A,\ S(n) \in A\Big) \Longrightarrow A = \mathbb{N}$.

REMARQUE 10.2 : Avec un peu de travail, on déduit de ces axiomes l'existence dans $\mathbb{N}$ de deux lois internes $+$ et $\times$ qui ont les propriétés suivantes :

- *$+$ est commutative et associative et possède un neutre 0.*
- *$\times$ est commutative et associative et possède un neutre $1 = S(0)$ (et on a en fait $S(n) = n + 1$).*
- *Seul 0 admet un opposé dans $\mathbb{N}$ et seul 1 admet un inverse pour $\times$.*
- *Tous les éléments de $\mathbb{N}$ sont réguliers pour la loi $+$.*
- *Tous les éléments de $\mathbb{N}$ sauf 0 (qui est absorbant) sont réguliers pour la loi $\times$.*
- *$\times$ est distributive par rapport à $+$.*

*Grâce à ces propriétés, si pour $(m, n) \in \mathbb{N}^2$, il existe un entier $k \in \mathbb{N}$ tel que $n = m + k$, alors celui-ci est unique et ceci nous permet de définir $k = n - m$ (**moins exact**).*
*De même si pour $(m, n) \in \mathbb{N}^* \times \mathbb{N}$, il existe un entier $k \in \mathbb{N}$ tel que $n = m \times k$, alors celui-ci est unique et ceci nous permet de définir $k = n/m$ (**quotient exact**).*

10.1.2 : Ordres sur $\mathbb{N}$

Définition 10.1

Grâce aux deux lois internes de $\mathbb{N}$ on définit les deux relations binaires $\leqslant$ et $|$ par les assertions suivantes : $\forall (a, b) \in \mathbb{N}^2,\ a \leqslant b \iff (\exists c \in \mathbb{N},\ b = a + c)$ *et* $a|b \iff (\exists c \in \mathbb{N},\ b = ac)$. *On dit alors que a est* **inférieur ou égal** *à b si $a \leqslant b$ ou que a est un* **diviseur** *de b (ou que b est un* **multiple** *de a) si $a|b$.*

Proposition 10.1

$\leqslant$ et $|$ sont des relations d'ordre (on admet que $\leqslant$ est totale). On dispose de plus de certaines compatibilités classiques :

- $\forall (a, b, c) \in \mathbb{N}^2 \times \mathbb{N}^*,\ a \leqslant b \iff \big(a + c \leqslant b + c$ **et** $a \times c \leqslant b \times c\big)$ **et** $a|b \iff ac|bc$**.**
- $\forall (a, b, c, d) \in \mathbb{N}^4,\ (a \leqslant b$ **et** $c \leqslant d) \Longrightarrow \big(a + c \leqslant b + d$ **et** $a \times c \leqslant b \times d\big)$**.**
- $\forall (a, b, c, d) \in \mathbb{N}^4,\ (a|b$ **et** $c|d) \Longrightarrow (a \times c)|(b \times d)$**.**

REMARQUE 10.3 : • *Bien sûr, la divisibilité n'est pas totale car $2 \not| 3$ et $3 \not| 2$.*

- *On note, pour $(a, b) \in \mathbb{N}^2$, $a \geqslant b \iff b \leqslant a$; $a < b \iff b > a \iff (a \leqslant b$ et $a \neq b)$.*

Théorème 10.1

Toute partie non vide admet un plus petit élément (un minimum) et toute partie non vide majorée admet un plus grand élément (un maximum).

DÉMONSTRATION :

• Soit $A \subset \mathbb{N}$ non vide, alors l'ensemble M de ses minorants est non vide (il contient 0) et différent de $\mathbb{N}$ donc par contre-apposée de la troisième des propriétés de PEANO, il existe $n_0 \in \mathbb{N}$ tel que $n_0 \in M$ et $n_0 + 1 \notin M$, on montre alors facilement que $n_0 = \mathrm{Min}(A)$.

• Soit A une partie non vide majorée de $\mathbb{N}$, l'ensemble M des majorants de A est non vide par hypothèse, et comme $M \subset \mathbb{N}$, M admet un plus petit élément $n_0 = \mathrm{Min}(M)$. On distingue ensuite les cas $n_0 = 0$ et $n_0 \neq 0$.

10.1.3 : Principes de récurrence

Théorème 10.2

Soit $n_0 \in \mathbb{N}$ et, pour $n \geqslant n_0$, une propriété $\mathcal{P}(n)$; on suppose que l'on a les informations suivantes : $\mathcal{P}(n_0)$ est vraie et $\forall p \geqslant n_0,\ \mathcal{P}(p) \Longrightarrow \mathcal{P}(p+1)$.

Alors on peut conclure que : $\forall n \geqslant n_0,\ \mathcal{P}(n)$ est vraie.

DÉMONSTRATION : Il suffit de poser $A = \{n \in \mathbb{N} \mid \mathcal{P}(n_0 + n) \text{ est vraie } \}$.

EXEMPLE 10.1 : On pose, pour $n \in \mathbb{N}$, $\mathcal{P}(n) =$ "$2^n > n$", alors $\mathcal{P}(0)$ et $\mathcal{P}(1)$ sont vraies et, pour $p \in \mathbb{N}^*$, si $\mathcal{P}(p)$ vraie : $2^{p+1} = 2 \times 2^p > 2p \geqslant p+1$. Par principe de récurrence : $\forall n \in \mathbb{N},\ 2^n > n$.

Théorème 10.3

Soit, pour $n \in \mathbb{N}$, une propriété $\mathcal{P}(n)$; on suppose cette fois-ci les renseignements : $\mathcal{P}(0)$ est vraie et $\forall p \in \mathbb{N},\ \big(\forall k \in [\![0;p]\!],\ \mathcal{P}(k)\big) \Longrightarrow \mathcal{P}(p+1)$. Alors on peut de nouveau affirmer que : $\forall n \in \mathbb{N},\ \mathcal{P}(n)$ est vraie (récurrence forte, transfinie ou avec prédécesseurs).

EXEMPLE 10.2 : Pour l'existence de la **division euclidienne** ; on se donne ici un entier $a \in \mathbb{N}^*$ et on pose, pour $n \in \mathbb{N}$, la propriété : $\mathcal{P}(n) =$ "$\exists (q,r) \in \mathbb{N} \times [\![0; a-1]\!],\ n = aq + r$". Il est clair que $\mathcal{P}(k)$ est vraie pour $k \in [\![0; a-1]\!]$ en posant $q = 0$ et $r = k$.

REMARQUE 10.4 :

• *On peut aussi procéder à des récurrences sur un intervalle d'entiers borné, ou à une récurrence descendante sur un intervalle borné ou sur des entiers relatifs, il faut juste se persuader qu'on a créé un lien entre l'initialisation de la récurrence et tous les entiers sur lesquels porte la propriété.*

• *Par exemple si on dispose d'une fonction $f : E \to E$ et d'un élément $a \in E$ alors on crée une unique suite $(u_n)_{n\in\mathbb{N}}$ d'éléments de E par $u_0 = a$ et $\forall n \in \mathbb{N},\ u_{n+1} = f(u_n)$; il s'agit d'une récurrence facile. De plus, si f est bijective, on a même une unique suite $(u_n)_{n\in\mathbb{Z}}$ telle que $u_0 = a$ et $\forall n \in \mathbb{Z},\ u_{n+1} = f(u_n)$.*

• *On définit la fonction* **factorielle** *par ce principe : $0! = 1$ et $\forall n \in \mathbb{N},\ (n+1)! = (n+1) \times (n!)$.*

PARTIE 10.2 : ENSEMBLES FINIS

10.2.1 : Définition des ensembles finis

Définition 10.2

On dit que deux ensembles non vides E et F sont **équipotents**, *noté $E \sim F$, s'il existe $f : E \to F$ bijective.*

EXEMPLE 10.3 : • Il est clair que $\mathbb{N} \sim \mathbb{N}^*$ grâce à l'application $n \mapsto n+1$; de même $\mathbb{N} \sim \mathbb{Z}$.

• $]-1;1[\sim \mathbb{R}$ par l'intermédiaire de la fonction Argth ; on sent bien que $[0;1] \sim]0;1[$ même s'il est difficile de construire une bijection explicite entre ces deux ensembles.

REMARQUE 10.5 : Cette relation d'équipotence est réflexive, symétrique et transitive mais ce n'est pas une relation d'équivalence car il n'existe aucun ensemble contenant tous les ensembles.

Définition 10.3

Soit E *un ensemble, on dit que* E *est* **fini** *si* $E = \emptyset$ *ou s'il existe un entier* $n \in \mathbb{N}^*$ *tel que* $E \sim [\![1;n]\!]$. *On dit que* E *est* **infini** *dans le cas contraire.*

REMARQUE 10.6 : Soit $p \in \mathbb{N}^*$ *tel que* $p \geqslant 2$ *et soit* $c \in [\![1;p]\!]$, *alors* $[\![1;p]\!] \setminus \{c\} \sim [\![1;p-1]\!]$.

10.2.2 : Notion de cardinal

Proposition 10.2

Soit $(n,p) \in (\mathbb{N}^*)^2$**, il existe une injection de** $[\![1;n]\!]$ **dans** $[\![1;p]\!] \implies n \leqslant p$**.**
De plus, toute injection de $[\![1;n]\!]$ **dans lui-même est une bijection.**

Démonstration :

- On effectue une récurrence sur l'entier n. Cette implication est vraie pour $n = 1$. On la suppose vraie pour un entier $n \geqslant 1$ (et pour tout entier p bien sûr). Soit $f : [\![1;n+1]\!] \to [\![1;p]\!]$ injective. On pose $c = f(n+1)$ et g la corestriction de f à $[\![1;n]\!]$ au départ et $[\![1;p]\!] \setminus \{c\}$ à l'arrivée. La remarque 10.6 vient enfin à la rescousse.
- Dans la même veine, on procède à une récurrence sur n pour la seconde partie de la proposition avec 10.6.

Proposition 10.3

Soit $(n,p) \in (\mathbb{N}^*)^2$**, il existe une bijection entre** $[\![1;n]\!]$ **et** $[\![1;p]\!] \implies n = p$**.**

REMARQUE 10.7 : Grâce à cette dernière proposition, si un ensemble non vide E *est fini, il existe un unique entier* $n \geqslant 1$ *tel que* E *soit équipotent à* $[\![1;n]\!]$.

Définition 10.4

Soit E *un ensemble fini, on définit son* **cardinal**, *noté* $\operatorname{card}(E)$, *par :*
$\operatorname{card}(E) = 0$ *si* $E = \emptyset$ *;* $\texttt{card}(E) = n$ *où* n *est l'unique entier* n *tel que* $E \sim [\![1;n]\!]$ *sinon.*

Proposition 10.4

Pour deux ensembles non vides finis E **et** F **:** $(E \sim F) \iff \big(\operatorname{card}(E) = \operatorname{card}(F)\big)$**.**

10.2.3 : Parties et cardinaux

Proposition 10.5

Les parties finies de $\mathbb{N}$ **sont exactement les parties majorées.**

Démonstration :

- Pour prouver que les parties finies de $\mathbb{N}$ sont majorées, on effectue une récurrence sur le cardinal de la partie.
- Pour établir que les parties majorées sont finies, on effectue une récurrence forte sur le maximum de cette partie.

REMARQUE 10.8 : Cette proposition nous permet d'affirmer que toutes les parties d'une partie finie de $\mathbb{N}$ *sont elles-mêmes finies, toute intersection de parties finies de* $\mathbb{N}$ *est elle-même finie, toute réunion de parties finies de* $\mathbb{N}$ *est elle-même finie. Enfin, cela permet de justifier que* $\mathbb{N}$ *n'est pas fini.*

Proposition 10.6

Soit E **un ensemble fini, alors toute partie** A **de** E **est finie et on a** $\operatorname{card}(A) \leqslant \operatorname{card}(E)$**. De plus, si** $A \subset E$**, on a** $A = E \iff \operatorname{card}(A) = \operatorname{card}(E)$**.**

Démonstration :

- Notons $n = \operatorname{card}(E)$, ainsi il existe $\Phi : E \to [\![1;n]\!]$ bijective, alors $\widehat{\Phi}(A) \subset [\![1;n]\!]$ donc elle est elle-même finie. Notons $p = \operatorname{card}\big(\widehat{\Phi}(A)\big)$, il existe alors $\Psi : \widehat{\Phi}(A) \to [\![1;p]\!]$ bijective. Donc $i_{\widehat{\Phi}(A)} \circ \Psi^{-1} : [\![1;p]\!] \to [\![1;n]\!]$ est injective, on en conclut $p \leqslant n$. De plus, la corestriction $\Phi : A \to \widehat{\Phi}(A)$ est bijective donc $\texttt{card}(A) = p$.

• Enfin, si $p = n$ alors $i_{\widehat{\Phi}(A)} \circ \Psi^{-1} : [\![1;n]\!] \to [\![1;n]\!]$ est injective donc bijective d'après la proposition 10.2, $i_{\widehat{\Phi}(A)}$ est bijective ce qui entraîne que $\widehat{\Phi}(A) = [\![1;n]\!]$ d'où la restriction $\Phi : A \to [\![1;n]\!]$ est bijective : $A = E$.

REMARQUE 10.9 : Ainsi, toute intersection d'ensembles finis est finie ; et même si cela ne découle pas immédiatement de ce qui précède, toute réunion finie de parties finies est elle-même finie.

10.2.4 : Fonctions et cardinaux

Théorème 10.4

Soit $f : E \to F$ une application avec E ensemble fini, alors on a :
- **$\mathrm{Im}(f)$ est fini et $\mathrm{card}(\mathrm{Im}\, f) \leqslant \mathrm{card}\, E$; de plus, $\mathrm{card}(\mathrm{Im}\, f) = \mathrm{card}(E) \iff f$ injective.**
- **si F est fini on a $\mathrm{card}(\mathrm{Im}\, f) \leqslant \mathrm{card}\, F$; de plus, $\mathrm{card}(\mathrm{Im}\, f) = \mathrm{card}(F) \iff f$ surjective.**

DÉMONSTRATION :
• Soit A une partie de E qui contient un antécédent de chaque élément de $\mathrm{Im}\, f$. Alors $f|_A^{\mathrm{Im}\, f}$ est bijective. Ainsi, $\mathrm{card}(A) = \mathrm{card}(\mathrm{Im}\, f) \leqslant \mathrm{card}(E)$. De plus, si f est injective $A = E$ donc $\mathrm{card}(E) = \mathrm{card}(\mathrm{Im}\, f)$.
• Si $\mathrm{card}(E) = \mathrm{card}(\mathrm{Im}\, f)$, on a $\mathrm{card}(A) = \mathrm{card}(E)$ donc $A = E$ car $A \subset E$ d'où f injective.

Proposition 10.7

Si $f : E \to F$ est une application entre deux ensembles finis :
f injective $\implies \mathrm{card}(E) \leqslant \mathrm{card}(F)$; f surjective $\implies \mathrm{card}(E) \geqslant \mathrm{card}(F)$; f bij. $\implies \mathrm{card}(E) = \mathrm{card}(F)$.

REMARQUE 10.10 : D'où le principe des tiroirs de DIRICHLET *(Johann Peter Gustav Lejeune* DIRICHLET *: mathématicien allemand 1805-1859) : si E et F sont finis et si $\mathrm{card}(E) > \mathrm{card}(F)$ alors il n'y a pas d'injection de E dans F (trop de chaussettes pour les tiroirs).*

Théorème 10.5

Soit $f : E \to F$ une application entre deux ensembles finis de même cardinal (en particulier si $E = F$ fini), alors on a : f injective $\iff$ f surjective $\iff$ f bijective.

REMARQUE 10.11 : Attention cela ne s'applique absolument pas aux ensembles en général comme le montre l'application injective mais non surjective $S : \mathbb{N} \to \mathbb{N}$; c'est pourquoi $\mathbb{N}$ est infini.

10.2.5 : Symboles de sommation et de produit

Définition 10.5

Dans un ensemble E muni d'une loi de composition interne T associative et commutative possédant un neutre e, si on se donne une famille $(x_i)_{i\in I}$ indexée par un ensemble fini I, on peut définir la **composée** $\underset{i\in I}{T} x_i$ *(avec la convention : cette composée est e si I est vide).*

REMARQUE 10.12 : Bien sûr si la loi est $+$, on notera $\sum_{i\in I} x_i$; si c'est la loi $\times$ (ou une loi multiplicative $*$), ce sera $\prod_{i\in I} x_i$; si l'on parle de parties $(A_i)_{i\in I}$ d'un ensemble E, on aura $\bigcap_{i\in I} A_i$ ou $\bigcup_{i\in I} A_i$; etc...

Proposition 10.8

Si I et J sont des ensembles finis disjoints et $(x_k)_{k\in I\cup J}$ une famille d'éléments de E muni d'une loi $+$ (par exemple), alors on a : $\sum_{i\in I} x_i + \sum_{j\in J} x_j = \sum_{k\in I\cup J} x_k$. Plus généralement, si $\{I_1, \cdots, I_n\}$ est une partition de I, alors on a : $\sum_{i\in I} x_i = \sum_{k=1}^{n} \Big(\sum_{i_k\in I_k} x_{i_k} \Big)$.

PARTIE 10.3 : DÉNOMBREMENT

10.3.1 : Cardinal des applications, permutations et injections

Proposition 10.9

Soit $n \in \mathbb{N}^*$ et $E_1, \cdots, E_n$ ensembles finis disjoints deux à deux : $\operatorname{card}\left(\bigcup_{k=1}^{n} E_k\right) = \sum_{k=1}^{n} \operatorname{card}(E_k)$**.**

DÉMONSTRATION : On commence par $n = 2$ grâce aux bijections et on effectue ensuite une récurrence.

Proposition 10.10

Soit $p \in \mathbb{N}^*$, E et F deux ensembles finis et $f : E \to F$ qui vérifie : $\forall y \in F$, y possède exactement p antécédent(s). Alors $\operatorname{card}(E) = p \operatorname{card}(F)$ **(lemme des bergers).**

DÉMONSTRATION : Il suffit de constater que $\left(f^{<-1>}(\{y\})\right)_{y \in F}$ constitue une partition de E.

Proposition 10.11

Soit $m \in \mathbb{N}^*$, E et F deux ensembles finis de cardinaux respectifs n et p, alors $E \times F$ est fini et $\operatorname{card}(E \times F) = np$ **; de plus, E^m est fini et** $\operatorname{card}(E^m) = n^m$**.**

DÉMONSTRATION : On peut écrire $E = \{x_1, \cdots, x_n\}$ et on a la partition $E \times F = \bigcup_{k=1}^{n} \{x_k\} \times F$.

Proposition 10.12

Soit E et F deux ensembles finis de cardinaux respectifs n et p, alors $\operatorname{card}(\mathcal{F}(E, F)) = p^n$**.**

DÉMONSTRATION : On écrit une nouvelle fois $E = \{x_1, \cdots, x_n\}$ et on met en bijection $\mathcal{F}(E, F)$ et F^n.

REMARQUE 10.13 : Cela justifie la notation F^E pour les familles d'éléments de F indexées par E.

Proposition 10.13

Soit E et F deux ensembles finis de cardinaux respectifs n et p avec $n \leqslant p$. Il y a exactement $A_p^n = \dfrac{p!}{(p-n)!}$ injections de E dans F.

DÉMONSTRATION : C'est vrai si $n = 1$ et pour tout entier p car toute application est alors une injection et $A_p^1 = p = p^1$. Si on suppose le résultat vrai pour les ensembles à $n \geqslant 1$ éléments, soit $E = \{x_1, \cdots, x_{n+1}\}$ un ensemble de cardinal $n+1$, alors toute injection de E dans F est entièrement caractérisée par l'image y de x_{n+1} et par la corestriction g de f à $E' = \{x_1, \cdots, x_n\}$ et $F \setminus \{y\}$.

Proposition 10.14

Soit E un ensemble fini de cardinal n, alors il y a exactement $n!$ permutations de E.

REMARQUE 10.14 : Le nombre de surjections entre ensembles finis est plus difficile à établir.

10.3.2 : Cardinal des parties d'un ensemble

Proposition 10.15

Soit E un ensemble fini de cardinal n, $\mathcal{P}(E)$ est fini et $\operatorname{card}\left(\mathcal{P}(E)\right) = 2^n$**.**

Proposition 10.16

Soit E un ensemble fini de cardinal n et $p \in [\![0;n]\!]$, alors en notant $\mathcal{P}_p(E)$ l'ensemble des parties de E à p éléments, on a $\mathcal{P}_p(E)$ fini et $\operatorname{card}\left(\mathcal{P}_p(E)\right) = \binom{n}{p} = \dfrac{n!}{p!(n-p)!}$.

DÉMONSTRATION : C'est tout d'abord évident si $p = 0$, on supposera dans la suite que $p \geqslant 1$. Notons alors $I_p(E)$ l'ensemble des injections de $[\![1;p]\!]$ dans E, on sait que $\operatorname{card}\left(I_p(E)\right) = \dfrac{n!}{(n-p)!}$ d'après 10.13. Considérons alors $\varphi : I_p(E) \to \mathcal{P}_p(E)$ définie par : $\forall f \in I_p(E),\ \varphi(f) = \operatorname{Im} f$. On montre que φ est surjective et que chaque partie $A \in \mathcal{P}_p(E)$ admet exactement $p!$ antécédents ; on conclut grâce au lemme des bergers.

Proposition 10.17

Soit A et B deux parties d'un ensemble fini E, alors : $\operatorname{card}(A \cup B) = \operatorname{card}(A) + \operatorname{card}(B) - \operatorname{card}(A \cap B)$.

DÉMONSTRATION : On écrit $A \cup B = (A \setminus B) \cup B$ et $A = (A \setminus B) \cup (A \cap B)$ et ces réunions sont disjointes.

REMARQUE 10.15 : On a une formule plus générale, si $(A_k)_{1 \leqslant k \leqslant n}$ est une famille de parties d'un ensemble fini E : $\operatorname{card}\left(\bigcup_{k=1}^{n} A_k\right) = \sum_{k=1}^{n} (-1)^{k+1} \left(\sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} \operatorname{card}\left(\bigcap_{j=1}^{k} A_{i_j}\right)\right)$ *(***formule du crible***).*

10.3.3 : Coefficients binomiaux et triangle de PASCAL

Définition 10.6

Soit $n \in \mathbb{N}$ et $p \in \mathbb{Z}$, on définit $\binom{n}{p}$ qui est le nombre de parties de cardinal p dans un ensemble de cardinal n, c'est-à-dire $\binom{n}{p} = \dfrac{n!}{p!(n-p)!}$ si $p \in [\![0;n]\!]$ et $\binom{n}{p} = 0$ sinon.

REMARQUE 10.16 : Il est souvent plus pratique d'écrire ces coefficients sous forme polynomiale : $\binom{n}{1} = n$, $\binom{n}{2} = \dfrac{n(n-1)}{2}$, $\binom{n}{3} = \dfrac{n(n-1)(n-2)}{6}$, $\binom{n}{4} = \dfrac{n(n-1)(n-2)(n-3)}{24}$, *etc...*

Proposition 10.18

On dispose sur les coefficients binomiaux de formules classiques :

$$\forall (n,p) \in \mathbb{N}^* \times \mathbb{Z},\ \binom{n}{p} = \binom{n-1}{p} + \binom{n-1}{p-1},\ \binom{n}{p} = \binom{n}{n-p},\ p\binom{n}{p} = n\binom{n-1}{p-1}.$$

DÉMONSTRATION : On peut le vérifier calculatoirement ou trouver une interprétation ensembliste.

Proposition 10.19

Soit A un anneau, $(x,y) \in A^2$, $n \in \mathbb{N}$, $xy = yx$: $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$ **(binôme de NEWTON).**

REMARQUE 10.17 : On peut une nouvelle fois généraliser cette formule pour parvenir à la **formule du multinôme** *: si $x_1, \cdots, x_p$ sont p éléments d'un anneau qui commutent deux à deux, alors :*

$$\forall n \in \mathbb{N},\ (x_1 + \cdots + x_p)^n = \sum_{\substack{(k_1,\cdots,k_p) \in \mathbb{N}^p \\ k_1 + \cdots k_p = n}} \frac{n!}{k_1! \cdots k_p!} x_1^{k_1} \cdots x_p^{k_p}.$$

PARTIE 10.4 : CARDINAUX DES INFINIS (HP)

10.4.1 : Les ensembles dénombrables

Définition 10.7

On dit qu'un ensemble est **dénombrable** *s'il est équipotent à* $\mathbb{N}$.

REMARQUE 10.18 : • $\mathbb{N}^*$, $\mathbb{Z}$, $\mathbb{N}\times\mathbb{N}$ *sont dénombrables : les bijections sont assez simples à trouver.*

• *Ces exemples fournissent en prime : une réunion de deux ensembles dénombrables l'est encore, une réunion dénombrable d'ensembles dénombrables l'est aussi, un produit de deux ensembles dénombrables l'est de nouveau, un produit fini d'ensemble dénombrables l'est toujours.*

• *Nous avons le magnifique théorème de* Cantor -Bernstein *(Georg* Cantor *(1845-1918) : mathématicien allemand fondateur de la théorie des ensembles et Félix* Bernstein *(1878-1956) : mathématicien allemand) qui affirme que si pour deux ensembles* $\mathtt{E}$ *et* $\mathtt{F}$ *on dispose d'une injection* $\mathtt{f}$ *de* $\mathtt{E}$ *dans* $\mathtt{F}$ *et d'une injection* $\mathtt{g}$ *de* $\mathtt{F}$ *dans* $\mathtt{E}$*, alors les deux ensembles sont équipotents.*

EXEMPLE 10.4 : • Les **nombres algébriques** forment donc un ensemble dénombrable.

• Par l'intermédiaire de l'analyse, on peut établir que $\mathbb{R}$ est équipotent à $\mathcal{P}(\mathbb{N})$ et à $\mathbb{N}^{\mathbb{N}}$.

10.4.2 : Cardinal par les bijections

REMARQUE 10.19 :

• *Pour deux ensembles* $\mathtt{E}$ *et* $\mathtt{F}$*, on dira que* $\operatorname{card}(\mathtt{E})\leqslant\operatorname{card}(\mathtt{F})$ *s'il existe une injection de* $\mathtt{E}$ *dans* $\mathtt{F}$ *(un exercice classique et encore une fois admis ici consiste à prouver que ceci est équivalent à l'existence d'une surjection de* $\mathtt{F}$ *dans* $\mathtt{E}$*).*

• *Cette relation sur les ensembles est sûr réflexive et transitive, non symétrique et non antisymétrique mais le théorème de* Cantor-Bernstein *prouve qu'en posant* $\operatorname{card}(\mathtt{E})=\operatorname{card}(\mathtt{F})\iff\mathtt{E}\sim\mathtt{F}$*, on a* $\operatorname{card}(\mathtt{E})\leqslant\operatorname{card}(\mathtt{F})$ *et* $\operatorname{card}(\mathtt{F})\leqslant\operatorname{card}(\mathtt{E})\iff\operatorname{card}(\mathtt{E})=\operatorname{card}(\mathtt{F})$.

• *Grâce à l'injection canonique, cette fonction* card *est croissante vis-à-vis de l'inclusion.*

• *On peut montrer qu'il n'existe pas d'injection de* $\mathcal{P}(\mathtt{E})$ *dans* $\mathtt{E}$ *quel que soit l'ensemble* $\mathtt{E}$ *: ce qui se traduit par le fait que* $\operatorname{card}(\mathtt{E})<\operatorname{card}\big(\mathcal{P}(\mathtt{E})\big)$.

• $\mathbb{R}$ *n'est pas dénombrable ; on note* $\aleph_0$ *le cardinal de* $\mathbb{N}$ *et* $\aleph_1$ *celui de* $\mathbb{R}$.

• Cantor *a émis la conjecture qui est devenue une assertion indécidable puisqu'elle est indépendante des axiomes : "il n'existe aucun cardinal strictement intermédiaire entre* $\aleph_0$ *et* $\aleph_1$*".*

PARTIE 10.5 : LES ENTIERS RELATIFS

10.5.1 : Présentation de $\mathbb{Z}$ avec sa structure

REMARQUE 10.20 :

• *L'ensemble* $\mathbb{N}$ *est le plus petit des ensembles infinis, il possède deux lois avec de bonnes propriétés mais on n'a pas de structure intéressante de* $\mathbb{N}$*, ce n'est même pas un groupe pour la loi* $+$*. C'est pourquoi on veut trouver des opposés aux entiers naturels.*

• *La plus claire des constructions se fait en notant* $\mathbb{Z}$ *l'ensemble des classes d'équivalence pour la relation d'équivalence* $\mathcal{R}$ *définie sur* $\mathbb{N}^2$ *par :* $\forall(\mathtt{a},\mathtt{b},\mathtt{a},\mathtt{b}')\in\mathbb{N}^4$, $(\mathtt{a},\mathtt{b})\mathcal{R}(\mathtt{a}',\mathtt{b}')\iff\mathtt{a}+\mathtt{b}'=\mathtt{a}'+\mathtt{b}$*. Les classes d'équivalence sont des demi-droites d'entiers naturels ; par exemple* $\overline{(0,4)}=\overline{(3,7)}$ *et* $\overline{(3,0)}=\overline{(7,4)}$.

• *On définit sur* $\mathbb{Z}$ *deux lois de composition internes par les formules :* $\overline{(\mathtt{a},\mathtt{b})}+\overline{(\mathtt{a}',\mathtt{b}')}=\overline{(\mathtt{a}+\mathtt{a}',\mathtt{b}+\mathtt{b}')}$ *et* $\overline{(\mathtt{a},\mathtt{b})}*\overline{(\mathtt{a}',\mathtt{b}')}=\overline{(\mathtt{a}\mathtt{a}'+\mathtt{b}\mathtt{b}',\mathtt{a}\mathtt{b}'+\mathtt{a}'\mathtt{b})}$*. On vérifie que ces lois sont bien définies (le résultat ne dépend pas des représentants choisis dans la classe d'équivalence) et on montre que :*

Proposition 10.20

$\mathbb{Z}$ est un anneau intègre.

REMARQUE 10.21 :

- *De plus et c'est essentiel, on interprète $\mathbb{N}$ comme une partie de $\mathbb{Z}$ en identifiant les entiers naturels n aux classes $\overline{(n,0)}$ et on se rend compte que les lois de $\mathbb{Z}$ prolongent celles de $\mathbb{N}$.*
- *On retrouve nos entiers relatifs classiques en notant comme on vient de le dire $5 = \overline{(5,0)}$ et $-3 = \overline{(0,3)}$ l'opposé de $3 = \overline{(3,0)}$. Les seuls inversibles de $\mathbb{Z}$ sont -1 et 1 et le seul sous-anneau de $\mathbb{Z}$ est $\mathbb{Z}$.*

10.5.2 : Ordre classique dans $\mathbb{Z}$

REMARQUE 10.22 : On définit $\leqslant$ dans $\mathbb{Z}$ par : $\forall (a,a',b,b') \in \mathbb{N}^4$, $\overline{(a,b)} \leqslant \overline{(a',b')} \iff a+b' \leqslant a'+b$, on vérifie encore une fois que ceci ne dépend pas du représentant choisi dans la classe, que c'est une relation d'ordre total et que cette relation prolonge le $\leqslant$ classique dans $\mathbb{N}$.

Proposition 10.21

On dispose de plus de compatibilités classiques :

- $\forall (a,b,c) \in \mathbb{Z}^3,\ a \leqslant b \iff a+c \leqslant b+c$.
- $\forall (a,b,c) \in \mathbb{Z}^2 \times \mathbb{N}^*,\ a \leqslant b \iff a \times c \leqslant b \times c$.

⊙ On dispose encore d'un théorème très puissant, qui plus est symétrique maintenant :

Théorème 10.6

Toute partie non vide minorée de $\mathbb{Z}$ admet un plus petit élément (un minimum) et toute partie non vide majorée de $\mathbb{Z}$ admet un plus grand élément (un maximum).

DÉMONSTRATION : Soit $A \neq \emptyset$ et $A \subset \mathbb{Z}$ et $m \in \mathbb{Z}$ un minorant de A : $A - m = \{a - m \mid a \in A\} \neq \emptyset$...

REMARQUE 10.23 : Les récurrences peuvent se faire sur $\mathbb{Z}$, par exemple si on a une propriété $\mathcal{P}(n)$ qui porte sur les entiers relatifs $n \in \mathbb{Z}$ alors il suffit que $\mathcal{P}(0)$ soit vrai et que : $\forall n \in \mathbb{N},\ \mathcal{P}(n) \Longrightarrow \mathcal{P}(n+1)$ et $\mathcal{P}(-n) \Longrightarrow \mathcal{P}(-n-1)$ pour qu'on puisse conclure : $\forall n \in \mathbb{Z},\ \mathcal{P}(n)$ est vrai.

Définition 10.8

On définit la **valeur absolue** *d'un entier relatif n par $|n| = \mathrm{Max}(\{n,-n\})$; c'est-à-dire $|n| = n$ si $n \geqslant 0$ et $|n| = -n$ si $n \leqslant 0$.*

REMARQUE 10.24 : On dispose sur cette "première" valeur absolue des propriétés classiques :

- $\forall n \in \mathbb{Z},\ |n| = 0 \iff n = 0$
- $\forall (n,m) \in \mathbb{Z}^2,\ |n+m| \leqslant |n| + |m|$
- $\forall (n,m) \in \mathbb{Z}^2,\ |nm| = |n|.|m|$
- $\forall (n,m) \in \mathbb{Z}^2,\ \Big||n| - |m|\Big| \leqslant |n \pm m|$

10.5.3 : Divisibilité dans $\mathbb{Z}$

Définition 10.9

Soit $(n,m) \in \mathbb{Z}^2$, on dit que $n|m \iff \exists p \in \mathbb{Z},\ m = np$ (divisibilité classique dans un anneau). On dit alors que m est un **multiple** *de n ou que n est un* **diviseur** *de m.*

REMARQUE 10.25 : • *Par les propriétés de la valeur absolue : $n|m$ dans $\mathbb{Z} \iff |n| \,\Big||m|$ dans $\mathbb{N}$.*

• *Cette relation $|$ est de nouveau réflexive et transitive mais elle n'est plus anti-symétrique donc ce n'est pas une relation d'ordre : $2|(-2)$ et $(-2)|2$ alors que $2 \neq -2$.*

Proposition 10.22

On dispose de nouveau de compatibilités et propriétés classiques :

- $\forall (a,b,c) \in \mathbb{Z}^2 \times \mathbb{Z}^*,\ a|b \iff ac|bc$.
- $\forall (a,b) \in (\mathbb{Z}^*)^2,\ a|b \implies |a| \leqslant |b|$.

REMARQUE 10.26 : Ainsi, un entier relatif non nul possède un nombre fini de diviseurs.