UNIVERSITE D'ORLEANS **Master MEEF 2023-2024–M1**
DEPARTEMENT DE MATHEMATIQUES **S. Grellier**

CONSTRUCTION DES ENTIERS.

On rappelle les **Axiomes de Peano** .
Il existe un ensemble $\mathbf{N}$ dont les éléments sont appelés les entiers naturels, un élément $0 \in \mathbf{N}$ appelé zéro et une application $s : \mathbf{N} \to \mathbf{N}$, dite application successeur, vérifiant les propriétés suivantes :
- 0 n'est le successeur d'aucun entier (en d'autres termes 0 n'est pas dans l'image de s),
- deux nombres entiers qui ont même successeur sont égaux (autrement dit l'application s est injective),
- si une partie A de $\mathbf{N}$ contient 0 et est stable par s (i.e. $s(A) \subset A$) alors A est égale à $\mathbf{N}$.

C'est le **principe de récurrence**.

1. Montrer que tout entier $a \neq 0$ est le successeur d'un entier.
2. On considère, pour $n \in \mathbf{N}$, l'application $m \mapsto n+m$ définie en posant $n+0 = n$, $n+s(p) = s(n+p)$ pour tout $p \in \mathbf{N}$. Démontrer que l'application correspondante est définie sur $\mathbf{N}$ et identifier l'application successeur.
   On note $1 := s(0)$.
3. Etablir le théorème suivant (deuxième forme du principe de récurrence). Soit $P(n)$ une propriété de l'entier $n \in \mathbf{N}$.
   On suppose qu'on a les deux propriétés suivantes :
   – $P(0)$ est vraie (initialisation).
   – Pour tout $n \in \mathbf{N}$, $P(n)$ implique $P(n+1)(= P(s(n))$ (hérédité).
   Démontrer qu'alors $P(n)$ est vraie pour tout $n \in \mathbf{N}$.
4. Démontrer que l'addition est associative $a + (b + c) = (a + b) + c$, $a, b, c \in \mathbf{N}$ (indication : on fixera a et b et on utilisera le principe de récurrence).
5. Démontrer que $a + 0 = 0 + a$ puis que $1 + a = a + 1 = s(a)$, $a \in \mathbf{N}$ et conclure que l'addition est commutative (on pourra considérer l'ensemble des entiers b tels que $a + b = b + a$ pour $a \in \mathbf{N}$ fixé).
6. Etablir la règle de simplification : si $a + b = a + c$ alors $b = c$.
7. Etablir que si $a + b = 0$ alors $a = b = 0$.
   On définit de manière analogue la multiplication en posant $n.0 = 0$ et $n.(p+1) = (n.p)+n$, $n, p \in \mathbf{N}$.
8. Montrer que cette définition a bien un sens puis que la loi obtenue est associative, commutative, distributive par rapport à l'addition et que 1 est l'élément neutre. Quelques indications : On peut commencer par démontrer que $n.1 = n = 1.n$ et que $0.n = n.0 = 0$ puis la distributivité à droite. La commutativité puis l'associativité en découlent.
9. Montrer que si un produit est nul, c'est que l'un des facteurs est nul.
   Soient $p, q \in \mathbf{N}$. On dit que q est supérieur ou égal à p et on écrit $q \geq p$ s'il existe $n \in \mathbf{N}$ tel que $q = n + p$. On dit que q est strictement supérieur à p si on a $q \geq p$ et $q \neq p$ et on note $q > p$.
10. Montrer qu'on définit ainsi une relation d'ordre (réflexive, antisymétrique, transitive).
11. Montrer que la relation d'ordre est totale (on pourra considérer à p fixé, l'ensemble des entiers q tels que, soit $q \geq p$, soit $p \geq q$).
12. Démontrer qu'il n'existe pas d'entier $0 < n < 1$.
13. Démontrer qu'il n'existe pas d'entier supérieur à tous les autres.
14. Démontrer que toute partie non vide de $\mathbf{N}$ admet un plus petit élément : **on dit que $\mathbf{N}$ est bien ordonné** (on pourra montrer qu'une partie n'admettant pas de plus petit élément est vide).
15. Démontrer que toute partie finie non vide de $\mathbf{N}$ a un plus grand élément.

16. Démontrer que le principe de récurrence est équivalent au bon ordre (de sorte que si l'on met celui-ci dans les axiomes la récurrence devient un théorème). On pourra raisonner par l'absurde et considérer le plus petit élément de l'ensemble des contreexemples :

$$\{n \in \mathbf{N},\ P(n) \text{ n'est pas vraie.}\}.$$

: LES ENTIERS RELATIFS.

L'ensemble $\mathbf{N}$ muni de l'addition n'est pas un groupe (pourquoi ?). On veut savoir résoudre une équation du type $x + n = d$ lorsque $d < n$ (sait-on le faire lorsque $d \geq n$?).

17. Sur $E = \mathbf{N} \times \mathbf{N}$, on considère la relation $\mathcal{R}$ définie par $(a, b)\mathcal{R}(c, d)$ si $a + d = b + c$. Démontrer que la relation $\mathcal{R}$ est une relation d'équivalence ((réflexive, symétrique, transitive).
On note $\mathbf{Z}$ le quotient $E/\mathcal{R}$ et $p : E \to E/\mathcal{R}$ la projection canonique qui à un couple (a, b) associe sa classe d'équivalence.
18. Démontrer que l'addition définie sur $\mathbf{N}\times\mathbf{N}$ en posant, pour $x = (a, b)$ et $y = (c, d)$, $x+y = (a+c, b+d)$ induit une opération sur $\mathbf{Z}$ qui est commutative et associative.
19. Montrer que $p(0, 0)$ est l'élément neutre de l'addition puis que l'élément $p(b, a)$ est l'opposé de $p(a, b)$. L'ensemble $\mathbf{Z}$ muni de la loi $+$ est un groupe abélien.
20. Montrer que l'application $\varphi : \mathbf{N} \to \mathbf{Z}$ définie par $\varphi(n) = p(n, 0)$ est un homomorphisme pour les lois $+$ et envoie l'élément neutre sur l'élément neutre. Cette application permet d'identifier $\mathbf{N}$ à son image dans $\mathbf{Z}$.
21. Avec cette identification montrer que tout élément de $\mathbf{Z}$ est
– soit un élément $n \in \mathbf{N}$
– soit l'opposé d'un tel élément, noté $-n$ (attention il s'agit d'une notation pour l'opposé de n).
On définit la valeur absolue de n comme celle de $-n$ par n.

22. Démontrer que la relation binaire $\leq$ définie sur $\mathbf{N}$ possède un unique prolongement à $\mathbf{Z}$ vérifiant, pour tout $p \in \mathbf{N}$,
$$n \leq m \Rightarrow n + p \leq m + p.$$
De plus, on montrera que cet ordre est total. En déduire que toute partie non vide et minorée de $\mathbf{Z}$ admet un plus petit élément.
On définit sur $\mathbf{N} \times \mathbf{N}$ une multiplication en posant
$$(m, n).(p, q) = (mp + nq, mq + np).$$
23. Démontrer que cette loi est compatible avec la relation d'équivalence $\mathcal{R}$. On peut alors parler de multiplication sur $\mathbf{Z}$.
24. Montrer que $(\mathbf{Z}, +, .)$ est un anneau commutatif unitaire, sans diviseur de zéro et totalement ordonné. De plus, la multiplication prolonge celle de $\mathbf{N}$.
25. Montrer que, pour $a, b \in \mathbf{Z}$, $(-a).b = -(a.b)$ en déduire la règle des signes.
Remarque : Un anneau commutatif, unitaire, sans diviseur de zéro et distinct de $\{0\}$ est dit intègre. L'anneau $\mathbf{Z}$ est donc intègre. On verra qu'il est aussi euclidien et donc principal (i.e. intègre et tout idéal est principal).