Partie II

Entiers naturels.

Dans ce chapitre, on aborde l'ensemble des entiers naturels dont l'importance est évidemment fondamentale.

Bien sûr, cet ensemble est bien connu et l'intuition qu'on en a est largement suffisante pour travailler avec. Cependant, si l'on veut construire un édifice mathématique parfaitement cohérent, on ne peut pas se contenter de l'intuition et il faut alors poser la question de la *construction de l'ensemble des entiers naturels*. Les mathématiciens se sont posé cette question et y ont répondu en montrant qu'on pouvait construire de façon rigoureuse un ensemble dont les propriétés sont précisément celles que l'on attend de $\mathbb{N}$ si l'on se fie à l'intuition qu'on en a.

Malheureusement, cette construction ne peut être comprise que si l'on maîtrise parfaitement la théorie des ensembles dont on a déjà dit qu'elle est d'un grand degré de difficulté. La construction de $\mathbb{N}$ dépasse donc largement les objectifs d'un cours de base.

Il s'avère en fait que l'on peut réduire toutes les propriétés de l'ensemble $\mathbb{N}$ ainsi construits a trois d'entre-elles, dites "axiomes de Peano". Dans ce chapitre, on va brièvement indiquer comment l'on peut construire les opérations usuelles de $\mathbb{N}$ ainsi que sa relation d'ordre à partir des axiomes de Peano. On rappelera également les propriétés essentielles de $\mathbb{N}$.

1 L'ensemble des entiers naturels.

Théorème 1.1 – *Il existe un ensemble, noté $\mathbb{N}$, un élément 0 de $\mathbb{N}$ et une application*

$$\begin{array}{rccc} s & : & \mathbb{N} & \longrightarrow & \mathbb{N} \\ & & n & \mapsto & s(n) \end{array}$$

satisfaisant les propriétés suivantes :
(A1) $s(\mathbb{N}) = \mathbb{N} \setminus \{0\}$;
(A2) s est injective ;
(A3) si A est un sous-ensemble de $\mathbb{N}$ contenant 0 et contenant l'image par s de chacun de ses éléments, alors $A = \mathbb{N}$.

Remarque 1.2 – Les assertions (A1), (A2) et (A3) sont appelées *axiomes de Peano*. L'assertion (A3) est appelé l'*axiome de récurrence*. Le rôle de l'application s est de permettre le passage d'un entier naturel à son successeur (au sens intuitif). D'ailleurs, on appelera s l'application *successeur*, d'où le choix de s pour la désigner. Ainsi, on peut dors-et-déjà décider d'utiliser le symbole 1 pour désigner $s(0)$.

L'axiome (A3) ci-dessus a une conséquence immédiate et de la plus grande importance dans la pratique. Elle est énoncée dans le théorème ci-dessous.

Théorème 1.3 – *Soit $\mathcal{P}$ une propriété portant sur les éléments de l'ensemble $\mathbb{N}$. On suppose que :*
1. $\mathcal{P}(0)$ est vraie ;
2. si n est un élément de $\mathbb{N}$ tel que $\mathcal{P}(n)$ soit vraie, alors $\mathcal{P}(s(n))$ est vraie.
Alors, $\mathcal{P}(n)$ est vraie pour tout élément n de $\mathbb{N}$.

Démonstration : Notons A le sous-ensemble de $\mathbb{N}$ défini par :

$$A = \{n \in \mathbb{N} \ ; \ \mathcal{P}(n) \text{ est vraie}\}.$$

La condition 1 de l'énoncé exprime que $0 \in A$ et la condition 2 que A contient l'image par s de chacun de ses éléments. L'axiome (A3) ci-dessus affirme donc que $A = \mathbb{N}$, c'est-à-dire que $\mathcal{P}(n)$ est vraie pour tout élément n de $\mathbb{N}$. ∎

Dans la pratique, le théorème 1.3 permet de traiter le problème suivant. On considère une propriété $\mathcal{P}$ portant sur les éléments de l'ensemble $\mathbb{N}$, et l'on souhaite démontrer que $\mathcal{P}(n)$ est vraie pour tout élément n de $\mathbb{N}$. On procède alors en deux étapes. Dans la première étape, dite d'*initialisation*, on démontre que $\mathcal{P}(0)$ est vraie. Dans la seconde, dite d'*itération*, on considère un élément $n \in \mathbb{N}$ quelconque et l'on démontre que, si l'on suppose $\mathcal{P}(n)$ vraie, alors $\mathcal{P}(s(n))$ est vraie. Il reste à appliquer le théorème 1.3 pour conclure que $\mathcal{P}(n)$ est vraie pour tout élément $n \in \mathbb{N}$. On dit alors qu'on a démontrée la propriété $\mathcal{P}$ *par récurrence*.

L'axiome de récurrence ne permet pas seulement de démontrer des propriétés, mais aussi de *construire* des suites. C'est ce qu'illustre le théorème suivant qui va être d'une importance considérable dans la suite.

Théorème 1.4 –
Soient X un ensemble, a un élément de X et $f : X \longrightarrow X$ une application de X vers X. Il existe une unique application $u : \mathbb{N} \longrightarrow X$ de $\mathbb{N}$ vers X satisfaisant les propriétés suivantes :
1. $u(0) = a$;
2. pour tout $n \in \mathbb{N}$, $u(s(n)) = f(u(n))$.

Démonstration : On commence par montrer l'existence de u.

Considérons l'ensemble de tous les sous-ensembles S de $\mathbb{N}\times X$ vérifiant la propriété $\mathcal{P}$ suivante :

$$(0, a) \in S \qquad \text{et} \qquad \forall (n, x) \in \mathbb{N} \times X,\ ((n, x) \in S) \Longrightarrow ((s(n), f(x)) \in S)\,.$$

Notons que $\mathbb{N} \times X$ lui-même vérifie $\mathcal{P}$. On note G le sous-ensemble de $\mathbb{N} \times X$ défini comme intersection de tous les sous-ensembles de $\mathbb{N} \times X$ vérifiant la propriété $\mathcal{P}$. Montrons que G est un graphe. Pour ce faire, considérons alors le sous-ensemble A de $\mathbb{N}$ des éléments n pour lesquels il existe un unique x dans X tels que $(n, x) \in G$:

$$A = \{n \in \mathbb{N}\ ;\ \text{il existe un unique } x \in X \text{ tel que } (n, x) \in G\}.$$

Par définition, montrer que G est un graphe revient à montrer que $A = \mathbb{N}$. C'est ce que l'on fait maintenant, à l'aide de l'axiome de récurrence. On remarque d'abord que G lui-même vérifie la propriété $\mathcal{P}$; c'est facile à établir. En outre, par définition de G, G ne peut pas contenir strictement un sous-ensemble de $\mathbb{N}\times X$ satisfaisant $\mathcal{P}$ et ce fait sera utile dans la suite. Montrons que $0 \in A$. Comme G vérifie $\mathcal{P}$, $(0, a) \in G$. Supposons, en outre, qu'il existe $b \in X$, avec $b \neq a$, tel que $(0, b) \in G$. Il est alors facile de voir que $G \setminus \{(0, b)\}$ vérifir la propriété $\mathcal{P}$ et est strictement contenu dans G. Ceci est une contradiction. Ainsi, $0 \in A$. Soit à présent $n \in \mathbb{N}$. Supposons que $n \in A$. On va montrer que $s(n) \in A$. Par hypothèse, il existe un unique $x \in X$ tel que $(n, x) \in G$. Comme G vérifie $\mathcal{P}$, $(s(n), f(x)) \in G$. Supposons maintenant qu'il existe $y \in X$, $y \neq f(x)$, tel que $(s(n), y) \in G$. Là encore, il est facile de voir que $G \setminus \{(s(n), y)\}$ vérifie la propriété $\mathcal{P}$ et on conclut à une contradiction comme ci-dessus. Ainsi, on a établi que $s(n) \in A$. On a donc montré, compte tenu de l'axiome (A3), que $A = \mathbb{N}$.

Posons alors $u = (\mathbb{N}, X, G)$. On a bien $u : \mathbb{N} \longrightarrow X$ telle que $u(0) = a$ et, pour tout $n \in \mathbb{N}$, $u(s(n)) = f(u(n))$.
Il reste à montrer l'unicité de u. Pour cela, supposns qu'il existe une application $v : \mathbb{N} \longrightarrow X$

telle que $v(0) = a$ et, pour tout $n \in \mathbb{N}$, $v(s(n)) = f(v(n))$. Il est facile de montrer, à l'aide d'une récurrence, que pour tout $n \in \mathbb{N}$, $u(n) = v(n)$. Les détails sont laissés au lecteur. ∎

La première conséquence du Théorème 1.4 est l'unicité de $\mathbb{N}$. On détaille ce point dans la remarque suivante.

Remarque 1.5 – Unicité de $\mathbb{N}$.
1. Il est bien sûr légitime de se demander si il peut exister plusieurs ensembles, très différents les uns des autres, satisfaisant les axiomes de Peano. Si tel était le cas, cela signifierait que ces trois axiomes, à eux seuls, ne suffisent pas à décrire l'ensemble des entiers naturels et, par conséquent, il faudrait ajouter d'autres axiomes pour bien distinguer l'ensemble qu'on cherche à construire.
2. En fait, il s'avère que ces trois axiomes suffisent bien à caractériser $\mathbb{N}$ au sens suivant. Si l'on considère un triplet (E, e, σ) où E est un ensemble, e un élément de E et $\sigma : E \longrightarrow E \setminus \{e\}$, et si l'on suppose que ce triplet vérifie les axiomes de Peano (convenablement retranscrits pour ce triplet), alors il existe une application bijective $\alpha : \mathbb{N} \longrightarrow E$ telle que $\alpha(0) = e$ et telle que $\alpha \circ s = \sigma \circ \alpha$. Cela signifie que E muni de son élément e et de son application σ se comporte exactement comme $\mathbb{N}$ muni de son élément 0 et de son application s.
3. Les détails de la démonstration du point 2 ci-dessus son passés sous silence pour ne pas alourdir l'exposé. Cependant, le lecteur très motivé pourra le démontrer en utilisant le théorème 1.4.

2 Opérations et ordre dans $\mathbb{N}$.

Dans cette section, on va montrer comment, à partir de la présentation axiomatique de $\mathbb{N}$, on peut reconstruire les opérations élémentaires (addition et multiplication), ainsi que la relation d'ordre de $\mathbb{N}$.

En fait, on se limitera à une ?bauche dont on espère qu'elle suggèrera les idées essentielles.

2.1 Additions et multiplication.

On commence par ébaucher la construction de l'addition de deux éléments de $\mathbb{N}$.

Rappelons que l'on note 1 l'image de 0 par l'application *succéseur*.

Fixons un élément p de $\mathbb{N}$. On va définir l'opération "ajouter p" à un élément quelconque de $\mathbb{N}$. Pour cela, appliquons le Théorème 1.4 avec $X = \mathbb{N}$, $f = s$ et $a = p$. On obtient qu'il existe une unique application

$$s_p \ : \ \mathbb{N} \ \longrightarrow \ \mathbb{N}$$

telle que $s_p(0) = p$ et, pour tout $n \in \mathbb{N}$, $s_p(s(n)) = s(s_p(n))$. On remarque aussi que, lorsque $p = 1$, cette application n'est autre que s elle même : c'est-à-dire que $s_1 = s$. Ceci est bien conforme à l'idée intuitive que l'on a des entiers : *prendre le succéseur d'un entier revient à lui ajouter* 1. De même, on note que $s_0 = \mathrm{id}_{\mathbb{N}}$.

Pour deux éléments p et n de $\mathbb{N}$, on pose alors $n + p = s_p(n)$.

Ainsi, pour tout $n, p \in \mathbb{N}$, $n + 0 = n$ et $n + 1 = s(n)$, $0 + p = p$ et $(n + 1) + p = (n + p) + 1$. On a en fait la Proposition suivante.

Proposition 2.1.1 – *L'application*

$$\begin{array}{rccc} + & : & \mathbb{N}\times\mathbb{N} & \longrightarrow & \mathbb{N} \\ & & (n,p) & \mapsto & n+p \end{array}$$

vérifie les propriétés suivantes :
1. *pour tout* $p \in \mathbb{N}$, $0+p=p$ *(*0 *est neutre pour* $+$*) ;*
2. *pour tous* $n,p \in \mathbb{N}$, $n+p=p+n$ *(commutativité) ;*
3. *pour tous* $n,p,q \in \mathbb{N}$, $(n+p)+q=n+(p+q)$ *(associativité).*

Démonstration : Exercice instructif. ∎

Exercice 2.1.2 – Montrer que, pour tous $n,p,q \in \mathbb{N}$, si $n+p=n+q$, alors $p=q$.

Exercice 2.1.3 – Soient p et q des éléments de $\mathbb{N}$. Montrer que si $p+q=0$, alors $p=q=0$. (Indication. On peut démontrer la contrapposée qui s'énonce ainsi : si p ou q est non nul, alors $p+q\neq 0$. Pour démontrer cette dernière assertion, on peut utiliser l'axiome (A1).)

Un procédé semblable (mais un peu plus délicat) permet de construire la multiplication dans $\mathbb{N}$.

STOP RELECTURE

2.2 Relation d'ordre.

Une fois définie l'addition de $\mathbb{N}$, on peut définir une relation d'ordre naturelle sur $\mathbb{N}$.

Définition 2.2.1 – *Soient* $m,n \in \mathbb{N}$. *On dira que* m est inférieur ou égal à n, *ou que* n *est* supérieur ou égal à m *ce que l'on notera* $m \leq n$, *s'il existe un élément* $p \in \mathbb{N}$ *tel que* $n=m+p$.

Il est clair, par définition, que pour tout $n \in \mathbb{N}$, $0 \leq n$.

Proposition 2.2.2 – *Avec les notations ci-dessus, on a :*
1. *pour tout* $n \in \mathbb{N}$, $n \leq n$ *(réflexivité) ;*
2. *pour tous* $m,n \in \mathbb{N}$, *si* ($m \leq n$ *et* $n \leq m$), *alors* $m=n$ *(symétrie) ;*
3. *pour tous* $m,n,p \in \mathbb{N}$, *si* ($m \leq n$ *et* $n \leq p$), *alors* $m \leq p$ *(transitivité).*

Démonstration : Exercice. ∎

Deux éléments m,n de $\mathbb{N}$ sont dits *comparables* si $m \leq n$ ou $n \leq m$. La proposition suivante montre que deux éléments de $\mathbb{N}$ sont toujours comparables.

Proposition 2.2.3 – *La relation d'ordre* $\leq$ *est totale. C'est-à-dire que, pour tous* $m,n \in \mathbb{N}$, $m \leq n$ *ou* $n \leq m$.

Idée de démonstration : on note S l'ensemble des éléments de $\mathbb{N}$ qui sont comparables avec tout élément de $\mathbb{N}$. On montre, par récurrence, que $S=\mathbb{N}$. ∎

Soit E un sous-ensemble de $\mathbb{N}$. Un élément a de $\mathbb{N}$ est un *minorant* de E s'il est inférieur ou égal à tout élément de E. Un élément a de $\mathbb{N}$ est un *plus petit élément* de E si a est dans E et est un minorant de E. Un élément a de $\mathbb{N}$ est un *majorant* de E si il est supérieur ou égal à tout élément de E. Un élément a de $\mathbb{N}$ est un *plus grand élément* de E si a est dans E et est un majorant de E.

Exercice 2.2.4 –
1. Toute partie de E admet au plus un plus petit (resp. plus grand) élément.
2. L'ensemble $\mathbb{N}$ admet un plus petit élément mais n'admet pas de plus grand élément.

Proposition 2.2.5 – *Tout sous-ensemble non-vide de $\mathbb{N}$ admet un plus petit élément.*

Démonstration : Soit E un sous-ensemble non-vide de $\mathbb{N}$. On raisonne par l'absurde, c'est-à-dire qu'on suppose que E n'admet pas de plus petit élément et on montre que cela débouche sur une absurdité. Supposons donc que E n'a pas de plus petit élément. Notons S l'ensemble des minorants de E. Bien sûr, $0 \in S$. Comme on suppose que E n'admet pas de plus petit élément, aucun élément de S n'est dans E. Soit $k \in S$. Pour tout $n \in E$, $k \leq n$. Donc, il existe $p \in \mathbb{N}$ tel que $n = k + p$. En outre, on doit avoir $p \neq 0$, sans quoi on aurait un élément dans S et dans E. Mais alors, il existe $q \in \mathbb{N}$ tel que $p = q+1$. D'où $n = (k+1)+q$. Ainsi, $k+1 \in S$. Par récurrence, on a donc montré que $S = \mathbb{N}$. Mais ceci contredit le fait que S et E n'ont pas d'élément commun. ∎

On termine par une notation pratique. Si m, n sont des éléments de $\mathbb{N}$ tels que $m \leq n$, on pose

$$[\![m, n]\!] = \{p \in \mathbb{N} \ ; \ m \leq p \leq n\}.$$

3 Ensembles finis, ensembles infinis.

Définition 3.1 – *Soit E un ensemble.*
1. On dit que E est fini si il est vide ou si il existe $p \in \mathbb{N} \setminus \{0\}$ et une bijection $[\![1, p]\!] \longrightarrow E$.
2. On dit que E est infini si E n'est pas fini.

Ainsi, les ensembles finis de référence sont $\emptyset$ les $[\![1, p]\!]$ où p est un élément non nul de $\mathbb{N}$. On va maintenant préciser le lien entre un ensemble fini et un tel ensemble de référence pour pouvoir définir la notion de *cardinal* d'un ensemble.

Les démonstrations des deux résultats suivants ne sont pas particulièrement difficiles. Cependant, on les admet pour alléger le texte.

Théorème 3.2 – *Soient p, q deux éléments non nuls de $\mathbb{N}$.*
1. Il existe une application injective de $[\![1, p]\!]$ vers $[\![1, q]\!]$ si et seulement si $p \leq q$.
2. Il existe une application surjective de $[\![1, p]\!]$ vers $[\![1, q]\!]$ si et seulement si $p \geq q$.
3. Il existe une application bijective de $[\![1, p]\!]$ vers $[\![1, q]\!]$ si et seulement si $p = q$.

Démonstration : Admis. ∎

Théorème 3.3 – *Soit $p \in \mathbb{N} \setminus \{0\}$ et $f : [\![1, p]\!] \longrightarrow [\![1, p]\!]$ une application. Les assertions suivantes sont équivalentes :*
(i) f est bijective ;
(ii) f est injective ;
(iii) f est surjective.

Démonstration : Admis. ∎

Corollaire 3.4 – *Soit E un ensemble fini et non vide. Il existe un unique élément $p \in \mathbb{N} \setminus \{0\}$ pour lequel il existe un bijection $[\![1, p]\!] \longrightarrow E$.*

Démonstration : L'existence d'un tel élément p est assurée par la définition d'ensemble fini. Supposons maintenant que p, q soient des éléments de $\mathbb{N}\backslash\{0\}$ pour lesquels il existent des bijections $f : [\![1, p]\!] \longrightarrow E$ et $g : [\![1, q]\!] \longrightarrow E$. Alors, l'application $g^{-1} \circ f$ est une bijection de $[\![1, p]\!]$ vers $[\![1, q]\!]$. Le théorème 3.2 assure donc que $p = q$. ∎

Définition 3.5 – *Soit E un ensemble fini et non vide. L'unique élément $p \in \mathbb{N} \setminus \{0\}$ pour lequel il existe un bijection $[\![1, p]\!] \longrightarrow E$ est appelé le cardinal de E. Il est noté* $\mathrm{card}(E)$. *En outre, on pose* $\mathrm{card}(\emptyset) = 0$.

Les théorèmes 3.2 et 3.3 se généralisent facilement aux ensembles fini. Les énoncés correspondants sont les suivants.

Corollaire 3.6 – *Soient E et F deux ensembles finis non-vides de cardinaux respectifs p et q.*
1. Il existe une application injective de E vers F si et seulement si $p \leq q$.
2. Il existe une application surjective de E vers F si et seulement si $p \geq q$.
3. Il existe une application bijective de E vers F si et seulement si $p = q$.

Démonstration : C'est une consequence facile du théorème 3.2. ∎

Corollaire 3.7 – *Soient E un ensemble fini non-vide et $f : E \longrightarrow E$ une application. Les assertions suivantes sont équivalentes :*
(i) f est bijective ;
(ii) f est injective ;
(iii) f est surjective.

Démonstration : C'est une consequence facile du théorème 3.3. ∎

Remarque 3.8 – Le corollaire 3.7 est faux pour les ensembles infinis. Il permet d'ailleurs de démontrer qu'un ensemble est infini. Par exemple, l'application $s : \mathbb{N} \longrightarrow \mathbb{N}$, $n \mapsto n + 1$ est injective (axiome (A2)), mais pas surjective (axiome (A1)). On en déduit que $\mathbb{N}$ est infini.

Théorème 3.9 – *Soit E un ensemble fini et F un sous-ensemble de E. Alors, F est fini et* $\mathrm{card}(F) \leq \mathrm{card}(E)$.

Démonstration : Exercice. ∎

4 Démonstrations par récurrence ; exemples et compléments.

Dans cette section, on revient plus en détail sur les démonstrations par récurrence. On a déjà vu qu'une telle démonstration s'appuie sur le théorème 1.3 qui, quant à lui, repose sur l'axiome (A3).

Pour illustrer la pratique de ce type de démonstration, on traite un exemple en détail.

Exercice 4.1 – Montrer que, pour tout n dans $\mathbb{N}$, $3^{2n} - 2^n$ est divisible par 7. (On rappelle que si a et b sont deux entiers naturels, on dit que a divise b si il existe $k \in \mathbb{N}$ tel que $b = ak$.)

Solution. Soit $\mathcal{P}$ la propriété portant sur les éléments de $\mathbb{N}$ et définie par

$$\mathcal{P}(n) \text{ est vraie lorsque 7 divise } 3^{2n} - 2^n.$$

On va procéder par récurrence.
1. *Initialisation.* Il est clair que $\mathcal{P}(0)$ est vraie puisque $3^{2.0} - 2^0 = 0$ est bien divisible par 7.
2. *Itération.* Soit $n \in \mathbb{N}$. Supposons $\mathcal{P}(n)$ vraie. Cela signifie qu'on suppose que $3^{2n} - 2^n$ est divisible par 7, c'est-à-dire qu'il existe un élément $k \in \mathbb{N}$ tel que $3^{2n} - 2^n = 7k$.

On doit démontrer qu'alors, $\mathcal{P}(n+1)$ est vraie. Or,

$$3^{2(n+1)} - 2^{n+1} = 9.3^{2n} - 2.2^n = (7+2)3^{2n} - 2.2^n = 7.3^{2n} + 2(3^{2n} - .2^n) = 7.3^{2n} + 2.7.k = 7(3^{2n} + 2k).$$

Cette dernière égalité montre que 7 divise $3^{2(n+1)} - 2^{n+1}$, c'est-à-dire que $\mathcal{P}(n+1)$ est vraie.
3. D'après le théorème 1.3, la propriété $\mathcal{P}(n)$ est vraie pour tout élément n de $\mathbb{N}$.

En conclusion, on a montré que, pour tout $n \in \mathbb{N}$, $3^{2n} - 2^n$ est divisible par 7.

Il s'avère que, dans la pratique, il est commode de disposer de quelques variantes du théorème 1.3 plus adaptées aux diverses situations que l'on rencontre. On va donc maintenant énoncer ces variantes.

Première variante. Souvent, une récurrence ne commence pas à 0 mais à 1, 2, *etc.* La première variante du théorème 1.3 prend en charge ce genre de situation.

Théorème 4.2 – *Soient n_0 un élément de $\mathbb{N}$ et $\mathcal{P}$ une propriété portant sur les éléments du sous-ensemble $\{n \in \mathbb{N} \ ; \ n \geq n_0\}$ de $\mathbb{N}$. On suppose que :*
1. $\mathcal{P}(n_0)$ est vraie ;
2. si n est un élément de $\mathbb{N}$ tel que $n \geq n_0$ et $\mathcal{P}(n)$ soit vraie, alors $\mathcal{P}(n+1)$ est vraie.
Alors, $\mathcal{P}(n)$ est vraie pour tout élément $n \geq n_0$ de $\mathbb{N}$.

Démonstration : On considère la propriété $\mathcal{Q}$ définie sur $\mathbb{N}$ par : pour n dans $\mathbb{N}$, $\mathcal{Q}(n)$ est vraie si et seulement si $\mathcal{P}(n_0+n)$ est vraie. Les hypothèses du présent théorème assurent que la propriété $\mathcal{Q}$ satisfait les hypothèses du théorème 1.3. Le théorème 1.3 assure donc que $\mathcal{Q}(n)$ est vraie pour tout $n \in \mathbb{N}$, ce qui revient à dire que $\mathcal{P}(n)$ est vraie pour tout $n \in \mathbb{N}$ tel que $n \geq n_0$. ∎

Deuxième variante. Souvent, on a besoin de supposer que la propriété considérée est vraie, non pas à un certain rang, mais pour tout les entiers inférieurs à un certain rang. La deuxième variante du théorème 1.3 prend en charge ce genre de situation.

Théorème 4.3 – *Soient n_0 un élément de $\mathbb{N}$ et $\mathcal{P}$ une propriété portant sur les éléments du sous-ensemble $\{n \in \mathbb{N} \ ; \ n \geq n_0\}$ de $\mathbb{N}$. On suppose que :*
1. $\mathcal{P}(n_0)$ est vraie ;
2. si n est un élément de $\{n \in \mathbb{N} \ ; \ n \geq n_0\}$ tel que $\mathcal{P}(k)$ soit vraie pour tout élément $k \in \mathbb{N}$ tel que $n_0 \leq k \leq n$, alors $\mathcal{P}(n+1)$ est vraie.
Alors, $\mathcal{P}(n)$ est vraie pour tout élément $n \geq n_0$ de $\mathbb{N}$.

Démonstration : On considère la propriété $\mathcal{Q}$ définie sur $\{n \in \mathbb{N} \ ; \ n \geq n_0\}$ par : pour n dans $\mathbb{N}$, $\mathcal{Q}(n)$ est vraie si et seulement si $\mathcal{P}(k)$ est vraie pour tout élément $k \in \mathbb{N}$ tel que $n_0 \leq k \leq n$. Les hypothèses du présent théorème assurent que la propriété $\mathcal{Q}$ satisfait les hypothèses du théorème 4.2. Le théorème 4.2 assure donc que $\mathcal{Q}(n)$ est vraie pour tout $n \in \mathbb{N}$ tel que $n \geq n_0$, ce qui entraîne bien sûr que $\mathcal{P}(n)$ est vraie pour tout $n \in \mathbb{N}$ tel que $n \geq n_0$. ∎

Exercice 4.4 – Montrer que tout entier $n \geq 2$ est produit de nombres premiers. (On rappelle qu'un élément de $\mathbb{N}$ est dit premier si il est supérieur ou égal à 2 et si ses seuls diviseurs sont 1 et lui-même.

Solution. On considère la propriété $\mathcal{P}$ portant sur les éléments de $\{n \in \mathbb{N} \ ; \ n \geq 2\}$ et définie par

$$\mathcal{P}(n) \text{ est vraie si et seulement si } n \text{ est produit de nombres premiers.}$$

On va procéder par récurrence.
1. *Initialisation.* Il est clair que $\mathcal{P}(2)$ est vraie puisque 2 est premier.
2. *Itération.* Soit $n \in \mathbb{N}$. Supposons $\mathcal{P}(k)$ vraie pour tout entier k tel que $2 \leq k \leq n$. Cela signifie qu'on suppose que tout élément k de $\mathbb{N}$ tel que $2 \leq k \leq n$ est produit de nombres premiers.

On doit démontrer qu'alors, $\mathcal{P}(n+1)$ est vraie. Or, deux cas se présentent. Ou bien $n+1$ est premier et il est bien produit de nombres premiers. Ou bien $n+1$ n'est pas premier. Dans ce second cas, il existe donc deux entiers a, b tels que $2 \leq a, b \leq n$ et $n+1 = ab$. Mais, par hypothèse de récurrence, a et b sont produits de nombres premiers, donc $n+1$ est produit de nombres premiers.
3. D'après le théorème 4.3, la propriété $\mathcal{P}(n)$ est vraie pour tout élément n de $\mathbb{N}$ supérieur ou égal à 2.

En conclusion, on a montré que tout $n \in \mathbb{N}$ supérieur ou égal à 2 est produit de nombres premiers.

Troisième variante. Il arrive qu'une propriété porte sur un sous-ensemble fini de $\mathbb{N}$. La troisième variante du théorème 1.3 prend en charge ce genre de situation. On s'y réfère en parlant de *récurrence finie*.

Théorème 4.5 – *Soient n_0, n_1 des éléments distincts de $\mathbb{N}$ et $\mathcal{P}$ une propriété portant sur les éléments du sous-ensemble $\{n \in \mathbb{N} \ ; \ n_0 \leq n \leq n_1\}$ de $\mathbb{N}$. On suppose que :*
1. $\mathcal{P}(n_0)$ est vraie ;
2. si n est un élément de $\{n \in \mathbb{N} \ ; \ n_0 \leq n \leq n_1 - 1\}$ tel que $\mathcal{P}(n)$ soit vraie, alors $\mathcal{P}(n+1)$ est vraie.
Alors, $\mathcal{P}(n)$ est vraie pour tout élément de $\{n \in \mathbb{N} \ ; \ n_0 \leq n \leq n_1\}$.

Démonstration : On laisse les détails au lecteur. Néanmoins, on lui conseille de considérer la propriété $\mathcal{Q}$ portant sur les éléments de $\{n \in \mathbb{N} \ ; \ n \geq n_0\}$ et définie ainsi. Pour $n_0 \leq n \leq n_1$, $\mathcal{Q}(n)$ est vraie si et seulement si $\mathcal{P}(n)$ est vraie. Pour $n > n_1$, $\mathcal{Q}(n)$ est toujours vraie. ∎

5 *Exercices.*

Exercice 5.1 – Soit $n \in \mathbb{N}^*$. On note p_n le nombre de sous-ensembles d'un ensemble fini à n éléments.
1. Calculez p_1, p_2, p_3, p_4.
2. Quelle formule générale cela suggère-t-il pour p_n ? Votre conjecture est-elle exacte ?

Exercice 5.2 – **Formule du binôme**. Pour tout entier $n \in \mathbb{N}^*$ et tout entier $k \in \{0, \ldots, n\}$ on définit le "coefficient" noté C_n^k par les uns, $\binom{n}{k}$ par les autres :

$$C_n^k = \binom{n}{k} = \frac{n!}{k!(n-k)} \quad \text{(avec la convention : } 0! = 1\text{)}.$$

a) Vérifiez que pour $1 \leq k \leq n$ on a : $C_{n+1}^k = C_n^k + C_n^{k-1}$.
b) Montrez que pour tout $n \in \mathbb{N}^*$ et tout $(x, y) \in \mathbb{R}^2$ on a :

$$(x+y)^n = \sum_{k=0}^{n} C_n^k . x^k . y^{n-k}.$$

Exercice 5.3 – Démontrer, par récurrence, le théorème de division euclidienne dans $\mathbb{N}$.

Exercice 5.4 – **Construction de $\mathbb{Z}$.**
On considère l'ensemble $E = \mathbb{N} \times \mathbb{N}$ et la loi de composition interne $+ : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N} \times \mathbb{N}$ définie par $(a, b) + (c, d) = (a + c, b + d)$.
1) Vérifier que la l.c.i. $+$ définie sur $\mathbb{N} \times \mathbb{N}$ est associative, commutative et possède un neutre, que l'on précisera.
2) On considère, sur E, la relation binaire $\mathcal{R}$ définie par : pour $(a, b), (c, d) \in E$, $(a, b)\mathcal{R}(c, d)$ si $a + d = c + b$. Montrer que cette relation est une relation d'équivalence, et qu'elle est compatible avec l'addition $+$ de E. On note encore $+$ la l.c.i. induite sur $E/\mathcal{R}$.
3) Montrer que la loi $+$ sur $E/\mathcal{R}$ est associative et commutative, qu'elle admet un neutre et que tout élément admet un symétrique (autrement dit $(E/\mathcal{R}, +)$ est un groupe abélien).
4) Montrer que l'ensemble $\{(n, 0),\ n \in \mathbb{N}\} \cup \{(0, n),\ n \in \mathbb{N}^*\}$ est un système complet de représentants des classes de E pour $\mathcal{R}$. On pose $\mathbb{Z} = E/\mathcal{R}$.
5) Montrer que $\iota : \mathbb{N} \longrightarrow \mathbb{Z}$, $n \mapsto (n, 0)$ est injective et compatible avec l'addition de $\mathbb{N}$ et la l.c.i. définie ci-dessus sur $\mathbb{Z}$.
6) Montrer que l'on peut également définir sur $\mathbb{Z}$ une loi $\times$ de sorte que $(\mathbb{Z}, +, \times)$ soit un anneau commutatif.

Exercice 5.5 – **Construction de $\mathbb{Q}$.**
En vous inspirant de la construction de $\mathbb{Z}$, proposer une construction de $\mathbb{Q}$ comme ensemble quotient de $\mathbb{Z} \times \mathbb{Z}^*$.