COTE : BKI 01-2.6

LIVRE I
THEORIE DES ENSEMBLES
CHAPITRE III (ETAT 3)
PUISSANCES. ENSEMBLES FINIS. ENSEMBLES DENOMBRABLES

Rédaction n° 062

Nombre de pages : 56

Nombre de feuilles : 56

Université Henri Poincaré - Nancy I
INSTITUT ÉLIE CARTAN - UMR 7502
Bibliothèque de mathématiques
B.P. 239
54506 Vandoeuvre-Lès-Nancy

Livre I Th des Ensembles
Chap III. Etat 3
Puissances

62

LIVRE I

THEORIE DES ENSEMBLES

CHAPITRE III (Etat 1).

PUISSANCES. ENSEMBLES FINIS. ENSEMBLES DENOMBRABLES.

Sommaire

§ 1. Ensembles équipotents. Puissances : 1. Ensembles équipotents. 2. Ensemble des puissances des parties d'un ensemble. 3. Comparaison des puissances. 4. Puissance de l'ensemble des parties d'un ensemble. 5. Puissance de l'image d'un ensemble par une application. 6. Puissance d'une réunion. Puissance d'une somme. 7. Calcul sur les puissances.

§ 2. Ensembles finis : 1. Ensembles énumérés. 2. Ensembles finis. 3. Puissances de parties finies. Le raisonnement par récurrence. 4. Réunion et produit de familles finies. 5. Les définitions par récurrence. 6. Applications : Itérées d'une fonction. Récurrence limitée.

§ 3. Entiers naturels. Ensembles dénombrables : 1. Puissances des parties finies d'un ensemble infini. 2. Entiers naturels. 3. Division euclidienne. Numération. 4. Analyse combinatoire. 5. Ensembles dénombrables. 6. Suites.

Commentaires.

Le rédacteur estime qu'il y aura lieu de discuter de nouveau de la place respective de ce chapitre et du chapitre sur les ensembles ordonnés (actuellement chap. IV). L'ordre actuel a l'inconvénient de couper en deux la théorie des puissances, et d'obliger à introduire une partie de la terminologie et des notations relatives aux ensembles ordonnés avant d'avoir défini de façon générale ces derniers.

Le n°1 du § 2, consacré aux ensembles "énumérés" n'est pas à sa place ici ; il doit être reporté au chap. II, de manière à permettre de relier tout de suite les notions de réunion et intersection de plusieurs ensembles aux notions de réunion et d'intersection d'une famille quelconque ; la notion étant indépendante de celle d'entier naturel peut sans inconvénient être introduite au chap. II ; bien entendu la liaison entre les deux notions reste dans la théorie des entiers naturels.

CHAPITRE III (Etat 3)

PUISSANCES. ENSEMBLES FINIS. ENSEMBLES DÉNOMBRABLES.

§ 1. Ensembles équipotents. Puissances.

1. Ensembles équipotents. Définition 1. Etant donnés deux ensembles E, F, on dit qu'une partie X de E et une partie Y de F sont des ensembles équipotents s'il existe une application biunivoque de X sur Y (et par suite une application biunivoque de Y sur X).

On dit aussi que X est équipotent à Y, et Y équipotent à X. En d'autres termes, cela signifie que l'ensemble I(X,Y) des applications biunivoques de X sur Y (chap.II, § 4, n°3) n'est pas vide. En particulier, si on sait définir une application biunivoque explicitée de X sur Y, X et Y sont équipotents.

Cette définition montre en particulier que les parties vides $\emptyset_E$ et $\emptyset_F$ sont équipotentes, puisque l'application vide est une application biunivoque de l'une sur l'autre ; on voit en outre que la partie vide de E n'est équipotente à aucune partie non vide de F.

Dans la plupart des démonstrations qui suivent, on suppose implicitement que les ensembles considérés sont non vides ; le lecteur complètera aisément les démonstrations dans les autres cas.

Toute partie X de E est équipotente à elle-même, puisque l'application identique de E sur lui-même restreinte à X est une application biunivoque de X sur lui-même.

Proposition 1. Si X est équipotent à Y, et Y équipotent à Z, X est équipotent à Z.

En effet, si u est une application biunivoque de X sur Y, v une application biunivoque de Y sur Z, $v \circ u$ est une application biunivoque de X sur Z (chap. II, §4, cor. de la prop. 14).

Proposition 2. *Si* E *et* F *sont équipotents,* $\mathfrak{P}(E)$ *et* $\mathfrak{P}(F)$ *sont équipotents.*

En effet, si u est une application biunivoque de E sur F, l'extension de u aux ensembles de parties est une application biunivoque de $\mathfrak{P}(E)$ sur $\mathfrak{P}(F)$ (chap. II, §4, cor. 2 de la prop. 11).

Proposition 3. *Si* E *est équipotent à* E', F *équipotent à* F', $E \times F$ *est équipotent à* $E' \times F'$.

En effet, si u est une application biunivoque de E sur E', v une application biunivoque de F sur F', l'èxtension (u,v) est une application biunivoque de $E \times F$ sur $E' \times F'$.

Proposition 4. *Soit* $(X_\lambda)_{\lambda \in L}$ *une famille de parties de* E, $(Y_\mu)_{\mu \in M}$ *une famille de parties de* F *; s'il existe une application biunivoque* φ *de* L *sur* M *telle que, pour tout* $\lambda \in L$, $Y_{\varphi(\lambda)}$ *soit équipotent à* X_λ, *alors* $\prod_{\lambda \in L} X_\lambda$ *est équipotent à* $\prod_{\mu \in M} Y_\mu$.

En effet, la proposition est évidente si un des X_λ est vide ; dans le cas contraire, il existe, d'après l'axiome de choix, une famille $(u_\lambda)_{\lambda \in L}$ d'applications de parties de E dans F, telle que, pour tout λ, u_λ soit une application biunivoque de X_λ sur $Y_{\varphi(\lambda)}$. L'application (u_λ), est une application biunivoque de $\prod_{\lambda \in L} X_\lambda$ sur $\prod_{\mu \in M} Y_\mu$, comme on le vérifie immédiatement.

Corollaire 1. *Si* E *est équipotent à* E', F *équipotent à* F', E^F *est équipotent à* $E'^{F'}$.

On peut donner de ce corollaire une seconde démonstration (indépendante de l'axiome de choix) : soit φ une application biunivoque de F' sur F, ψ une application biunivoque de E sur E' ; si f est une application de F dans E, $f' = \psi \circ f \circ \varphi$ est une application de F' dans E', et on vérifie aussitôt que si φ' et ψ' sont les applications réciproques de φ et ψ respectivement, on a $f = \psi'\circ f'\circ\varphi'$; l'application $f \rightarrow \psi\circ f\circ\varphi$ est donc une application biunivoque de E^F sur $E'^{F'}$; ce raisonnement prouve en outre que :

Corollaire 2. Si E est ~~réciproq~~ équipotent à E', et F équipotent à F', l'ensemble $S(E,F)$ des applications de E sur F (resp. l'ensemble $B(E,F)$ des applications biunivoques de E dans F, l'ensemble $I(E,F)$ des applications biunivoques de E sur F) est équipotent à $S(E',F')$ (resp. $B(E',F')$, $I(E',F')$).

Proposition 5. Soient E et F deux ensembles, $(F_\iota)_{\iota\in I}$ une partition de F. L'ensemble E^F est équipotent à $\prod_{\iota\in I} E^{F_\iota}$.

C'est une conséquence de la prop. 14 du chap. II, § 5.

Proposition 6. Soient E, F, G trois ensembles. L'ensemble $G^{E\times F}$ est équipotent à $(G^E)^F$.

En effet, on a défini au chap. II, § 4, n°7 une application biunivoque explicitée de l'un de ces ensembles sur l'autre.

Proposition 7. Soient E et F deux ensembles, $(X_\iota)_{\iota\in I}$ une famille de parties de E. L'ensemble $(\prod_{\iota\in I} X_\iota)^F$ est équipotent à $\prod_{\iota\in I} X_\iota^F$.

En effet, on a défini au chap. II, 5; prop. 19, une ~~xxxx~~ application biunivoque de l'un de ces ensembles sur l'autre.

2. Ensemble des puissances des parties d'un ensemble. Si X et Y sont deux parties arbitraires d'un ensemble E, la relation "X et Y sont équipotents" est une relation d'équivalence (chap. II, § 6) dans $\mathfrak{P}(E)$, en vertu de la prop. 1. Nous désignerons par $\bar{\omega}(E)$, et nous appellerons ensemble des puissances des parties de E l'ensemble quotient de $\mathfrak{P}(E)$ par cette relation d'équivalence ; nous désignerons par $p(X)$ la classe d'équivalence d'une partie quelconque X de E, que nous appellerons la puissance de X.

nous désignerons généralement les puissances par des lettres gothiques.

Si E et F sont deux ensembles quelconques, X une partie arbitraire de E , Y une partie arbitraire de F , il résulte de la prop.1 que la relation "X est équipotent à Y" est <u>compatible</u> (en X) avec la relation "X et X' sont équipotents" entre deux parties de E , et <u>compatible</u> (en Y) avec la relation "Y et Y' sont équipotents" entre deux parties de F . En <u>passant aux quotients</u> (chap.II, § 6, n°4) pour X et Y , on obtient une relation que nous exprimerons sous la forme " $\mathfrak{a}$ et $\mathfrak{b}$ sont équivalentes" entre un élément $\mathfrak{a}$ de $\varpi(E)$ et un élément $\mathfrak{b}$ de $\varpi(F)$; la relation "X et Y sont équipotents" est équivalente à "p(X) et p(Y) sont équivalentes" ; on en déduit aussitôt que la relation " $\mathfrak{a}$ est équivalente à $\mathfrak{b}$ et $\mathfrak{a}'$ est équivalente à $\mathfrak{b}$ " entraîne $\mathfrak{a} = \mathfrak{a}'$, et la relation " $\mathfrak{a}$ est équivalente à $\mathfrak{b}$ et $\mathfrak{a}$ est équivalente à $\mathfrak{b}'$ " entraîne $\mathfrak{b} = \mathfrak{b}'$. Soit S l'ensemble des éléments $\mathfrak{a}$ de $\varpi(E)$ tels qu'il existe un $\mathfrak{b} \in \varpi(F)$ équivalent à $\mathfrak{a}$, T l'ensemble des éléments $\mathfrak{b}$ de $\varpi(F)$ tels qu'il existe un $\mathfrak{a} \in \varpi(E)$ équivalent à $\mathfrak{b}$; la relation " $\mathfrak{a}$ est équivalente à $\mathfrak{b}$ " entre un élément $\mathfrak{a} \in S$ et un élément $\mathfrak{b} \in T$ est alors une <u>relation fonctionnelle biunivoque</u> (chap.II, § 1, n°4) ; elle définit donc deux applications biunivoques et réciproques explicitées de S sur T et vice-versa, que nous appellerons applications <u>canoniques de</u> $\varpi(E)$ <u>à</u> $\varpi(F)$ et <u>de</u> $\varpi(F)$ <u>à</u> $\varpi(E)$ respectivement.

On observera que S et T ne sont pas vides, puisqu'ils contiennent respectivement $p(\emptyset_E)$ et $p(\emptyset_F)$.

3. <u>Comparaison des puissances</u>. Soient E et F deux ensembles ; s'il existe une application biunivoque f d'une partie X de E <u>dans</u> une partie Y de F , il existe aussi une application biunivoque de toute partie X' de E équipotente à X dans toute partie Y' de F équipotente à Y , savoir $\psi \circ f \circ \varphi$, où φ est une application biunivoque de X' sur X et ψ une application biunivoque de Y sur Y' . On peut donc poser la définition suivante :

<u>Définition 2</u>. <u>On dit qu'un élément</u> $\mathfrak{a}$ <u>de</u> $\overline{\omega}(E)$ <u>est inférieur à un élément</u> $\mathfrak{b}$ <u>de</u> $\overline{\omega}(F)$ <u>s'il existe une application biunivoque d'une partie de</u> E <u>de puissance</u> $\mathfrak{a}$ <u>dans une partie de</u> F <u>de puissance</u> $\mathfrak{b}$.

On dit aussi dans ce cas que $\mathfrak{b}$ est <u>supérieur</u> à $\mathfrak{a}$.

Si la puissance de E est <u>inférieure</u> à celle de F , pour tout élément $\mathfrak{a} \in \overline{\omega}(E)$, il existe un élément de $\overline{\omega}(F)$ équivalent à $\mathfrak{a}$, donc l'application canonique de $\overline{\omega}(E)$ à $\overline{\omega}(F)$ (n°2) est une application <u>de</u> $\overline{\omega}(E)$ <u>dans</u> $\overline{\omega}(F)$.

<u>Définition 3</u>. <u>On dit qu'un élément</u> $\mathfrak{a}$ <u>de</u> $\overline{\omega}(E)$ <u>est strictement inférieur à un élément</u> $\mathfrak{b}$ <u>de</u> $\overline{\omega}(F)$ <u>si</u> $\mathfrak{a}$ <u>est inférieur à</u> $\mathfrak{b}$ <u>et si</u> $\mathfrak{b}$ <u>n'est pas inférieur à</u> $\mathfrak{a}$ (autrement dit, s'il n'existe aucune application biunivoque d'un ensemble de puissance $\mathfrak{b}$ dans un ensemble de puissance $\mathfrak{a}$).

On dit encore alors que $\mathfrak{b}$ est <u>strictement supérieur</u> à $\mathfrak{a}$.

Comme l'application vide est une application biunivoque de $\emptyset_E$ dans F , et que $\emptyset_E$ n'est équipotente à aucune partie non vide de F , on voit que $p(\emptyset_E)$ est <u>strictement inférieure</u> à tout élément de $\overline{\omega}(F)$ distinct de $p(\emptyset_F)$.

8

Il est clair que si X et Y sont équipotents, la puissance de X est <u>à la fois</u> supérieure et inférieure à celle de Y . Nous allons démontrer l'importante <u>réciproque</u> de cette proposition ; elle résultera du théorème plus précis suivant :

<u>Théorème 1 (Dedekind). Soient</u> E <u>et</u> F <u>deux ensembles</u>, f <u>une application biunivoque de</u> E <u>dans</u> F , g une application biunivoque de F <u>dans</u> E . <u>Il existe alors deux parties</u> A,B <u>de</u> E <u>et deux parties</u> A',B' <u>de</u> F <u>telles que</u> $E=A\cup B$, $F=A'\cup B'$, $A\cap B=\emptyset$, $A'\cap B'=\emptyset$, <u>et</u> $A'=f(A)$, $B=g(B')$.

On notera que l'un des ensembles A,B (resp. A',B') de cet énoncé peut être <u>vide</u>.

Supposons le problème résolu ; si $R=\complement g(F)$, on a $R\subset\complement g(B')=\complement B=A$; d'autre part, comme g est biunivoque, on a $g(A')\subset\complement g(B')=A$; autrement dit, si on pose $h=g\circ f$, on a $h(A)\subset A$; on a donc $A\supset R\cup h(A)$.

Inversement, considérons l'ensemble $\mathfrak{F}$ des parties M de E telles que $M\supset R\cup h(M)$; nous allons montrer que si on prend pour A l'<u>intersection</u> $\bigcap_{M\in\mathfrak{F}} M$ des ensembles $M\in\mathfrak{F}$, et si on pose $A'=f(A)$, $B'=\complement A'$, $B=g(B')$, les quatre ensembles ainsi définis satisfont aux conditions de l'énoncé.

Comme $R\subset M$ pour tout $M\in\mathfrak{F}$, ona aussi $R\subset A$; d'autre part, on a $h(A)\subset h(M)\subset M$ pour tout $M\in\mathfrak{F}$, donc $h(A)\subset A$; on a donc $A\supset R\cup h(A)=Q$. Prouvons qu'on a $A=Q$; il suffira de voir que l'on a $A\subset Q$, et pour cela, que $Q\in\mathfrak{F}$. Or, on a $R\subset Q$ par définition ; d'autre part $h(Q)\subset h(A)\subset Q$, donc $Q\in\mathfrak{F}$ et $A=Q$.

Cela étant, comme $R\cap g(F)=\emptyset$, on a a fortiori $R\cap B=R\cap g(B')=\emptyset$; d'autre part, comme g est biunivoque, $g(A')\cap g(B')=h(A)\cap B=\emptyset$, d'où $A\cap B=(R\cap B)\cup(h(A)\cap B)=\emptyset$; d'ailleurs $E=R\cup g(F)=R\cup g(A')\cup g(B')=$ $=(R\cup h(A))\cup B=A\cup B$, ce qui achève la démonstration.

Corollaire 1. Si la puissance de E est à la fois supérieure et inférieure à celle de F, E et F sont équipotents.

En effet, soit f une application biunivoque de E dans F, g une application biunivoque de F dans E ; si A,B,A',B' satisfont aux conditions du th.1, l'application de E dans F égale à f dans A, à l'application réciproque de g dans B, est une application biunivoque de E sur F.

Corollaire 2. Pour que la puissance de E soit strictement inférieure à celle de F, il faut et il suffit qu'elle soit inférieure et non équivalente à la puissance de F.

La condition est évidemment nécessaire ; elle est suffisante d'après le th.1, puisque, s'il existait une application biunivoque de F dans E, E et F seraient équipotents contrairement à l'hypothèse.

Remarques.- 1) On notera que la démonstration du th.1 ne fait pas intervenir l'axiome de choix.

2) Nous verrons au chap.IV, comme conséquence de l'axiome de choix, que si E et F sont deux ensembles quelconques, ou bien la puissance de E est supérieure à celle de F, ou bien elle lui est inférieure.

Proposition 8. Soient E,F,G trois ensembles ; si la puissance de E est inférieure à celle de F, et la puissance de F inférieure à celle de G, la puissance de E est inférieure à celle de G ; si en outre la puissance de E est strictement inférieure à celle de F ou si la puissance de F est strictement inférieure à celle de G, la puissance de E est strictement inférieure à celle de G.

En effet, si f est une application biunivoque de E dans F, g une application biunivoque de F dans G, $g \circ f$ est une application biunivoque de E dans G. Si G était équipotent à E, la puissance de G serait donc inférieure à celle de F , et la puissance de F inférieure à celle de E , donc (cor. du th.1) E,F et G seraient équipotents, ce qui achève la démonstration.

Si $\mathfrak{a}$ et $\mathfrak{b}$ sont deux éléments de $\varpi(\mathrm{E})$, la relation " $\mathfrak{a}$ est inférieure à $\mathfrak{b}$ " s'écrit encore $\mathfrak{a} \leqslant \mathfrak{b}$ (ou $\mathfrak{b} \geqslant \mathfrak{a}$), la relation " $\mathfrak{a}$ est strictement inférieure à $\mathfrak{b}$ " s'écrit $\mathfrak{a} < \mathfrak{b}$ (ou $\mathfrak{b} > \mathfrak{a}$). D'après le th.1 les relations $\mathfrak{a} \leqslant \mathfrak{b}$ et $\mathfrak{b} \leqslant \mathfrak{a}$ entraînent $\mathfrak{a} = \mathfrak{b}$; d'après la prop.8, les relations $\mathfrak{a} \leqslant \mathfrak{b}$ et $\mathfrak{b} \leqslant \mathfrak{c}$ entraînent $\mathfrak{a} \leqslant \mathfrak{c}$; les relations $\mathfrak{a} < \mathfrak{b}$ et $\mathfrak{b} \leqslant \mathfrak{c}$ (ou $\mathfrak{a} \leqslant \mathfrak{b}$ et $\mathfrak{b} < \mathfrak{c}$) entraînent $\mathfrak{a} < \mathfrak{c}$. D'après le cor.2 du th.1, la relation $\mathfrak{a} < \mathfrak{b}$ est équivalente à " $\mathfrak{a} \leqslant \mathfrak{b}$ et $\mathfrak{a} \neq \mathfrak{b}$ " .

Si $\mathfrak{a}'$, $\mathfrak{b}'$ sont deux éléments de $\varpi(\mathrm{F})$, respectivement équivalents à $\mathfrak{a}$, $\mathfrak{b}$, la relation $\mathfrak{a} \leqslant \mathfrak{b}$ est équivalente à $\mathfrak{a}' \leqslant \mathfrak{b}'$.

Il est clair que toute partie A d'un ensemble E a une puissance inférieure à celle de E , puisque l'application canonique de A dans E est biunivoque.

Proposition 9. Si E a une puissance inférieure à celle de E' , $\mathfrak{P}(\mathrm{E})$ a une puissance inférieure à celle de $\mathfrak{P}(\mathrm{E}')$.

En effet, si f est une application biunivoque de E dans E', l'extension de f aux ensembles de parties est une application biunivoque de $\mathfrak{P}(\mathrm{E})$ dans $\mathfrak{P}(\mathrm{E}')$.

Proposition 10. Si E a une puissance inférieure à celle de E' , F une puissance inférieure à celle de F' , $\mathrm{E} \times \mathrm{F}$ a une puissance inférieure à celle de $\mathrm{E}' \times \mathrm{F}'$.

En effet, si f est une application biunivoque de E dans E' , g une application biunivoque de F dans F' , l'extension (f,g) est une application biunivoque de $\mathrm{E} \times \mathrm{F}$ dans $\mathrm{E}' \times \mathrm{F}'$.

Proposition 11. Soit $(X_\lambda)_{\lambda \in L}$ une famille de parties non vides de E, $(Y_\mu)_{\mu \in M}$ une famille de parties non vides de F ; s'il existe une application biunivoque φ de L dans M telle que, pour tout $\lambda \in L, X_\lambda$ ait une puissance inférieure à celle de $Y_{\varphi(\lambda)}$, alors la puissance de $\prod_{\lambda \in L} X_\lambda$ est inférieure à celle de $\prod_{\mu \in M} Y_\mu$.

En effet, d'après l'axiome de choix, il existe une famille $(u_\lambda)_{\lambda \in L}$ d'applications de parties de E dans F, telle que, pour tout $\lambda \in L$, u_λ soit une application biunivoque de X_λ dans $Y_{\varphi(\lambda)}$; on en déduit comme dans la prop.4 une application biunivoque de $\prod_{\lambda \in L} X_\lambda$ dans $\prod_{\mu \in \varphi(L)} Y_\mu$; d'après la prop.8, tout revient à prouver que, pour toute partie N de M, $\prod_{\mu \in N} Y_\mu$ a une puissance inférieure à celle de $\prod_{\mu \in M} Y_\mu$; mais, si P est le complémentaire de N dans M, on voit comme dans la prop.14 du chap.II, §5, que $\prod_{\mu \in M} Y_\mu$ est équipotent à $(\prod_{\mu \in N} Y_\mu) \times (\prod_{\mu \in P} Y_\mu)$; comme les Y_μ ne sont pas vides, $\prod_{\mu \in P} Y_\mu$ n'est pas vide d'après l'axiome de choix ; si z est un élément quelconque de $\prod_{\mu \in P} Y_\mu$, $\prod_{\mu \in N} Y_\mu$ est équipotent à $(\prod_{\mu \in N} Y_\mu) \times \{z\}$, d'où la proposition.

Corollaire. Si E a une puissance inférieure à celle de E', F une puissance inférieure à celle de F', E^F a une puissance inférieure à celle de $E'^{F'}$.

Remarque.- Un ensemble E peut être tel qu'il existe une partie A de E, différente de E, et équipotente à E ; cette propriété caractérise les ensemble infinis, que nous étudierons au §3. *Par exemple, l'ensemble des entiers pairs est équipotent à l'ensemble N de tous les entiers naturels, car $n \to 2n$ est une application biunivoque de N sur l'ensemble des entiers pairs.*

Nous verrons de même ultérieurement (chap.IV, §) que les prop.10 et 11 cessent d'être exactes lorsqu'on remplace partout dans leur énoncé, le mot "inférieure" par "strictement inférieure" ; on ignore par contre si la prop.9 ainsi modifiée est encore vraie ou non.

4. Puissance de l'ensemble des parties d'un ensemble. Théorème 2. La puissance d'un ensemble E est strictement inférieure à celle de $\mathfrak{P}(E)$.

En effet, l'application $x \rightarrow \{x\}$ est une application biunivoque de E dans $\mathfrak{P}(E)$; donc E a une puissance inférieure à celle de $\mathfrak{P}(E)$. Nous allons prouver qu'il n'existe pas d'application biunivoque de $\mathfrak{P}(E)$ dans E, d'où résultera le théorème. Raisonnons par l'absurde, et soit f une telle application ; soit $\mathfrak{M}$ l'ensemble des $X \in \mathfrak{P}(E)$ tels que $f(X) \notin X$, de sorte que $X \in \mathfrak{M}$ est équivalente à $f(X) \notin X$; soit $M=f(\mathfrak{M})$; comme f est biunivoque par hypothèse, la relation $X \in \mathfrak{M}$ est équivalente à $f(X) \in f(\mathfrak{M})=M$; donc les relations $f(X) \notin X$ et $f(X) \in M$ sont équivalentes ; on en déduit en remplaçant X par M, que les relations $f(M) \notin M$ et $f(M) \in M$ sont équivalentes, ce qui est absurde.

5. Puissance de l'image d'un ensemble par une application. Proposition 12. Pour toute application f de E dans F, et toute partie X de E, la puissance de f(X) est inférieure à celle de X.

On peut se borner au cas où $X \neq \emptyset$, la proposition étant évidente dans le cas contraire. Posons $Y=f(X)$; quel que soit $y \in Y$, il existe $x \in E$ tel que $x \in X \cap \overset{-1}{f}(y)$; donc, d'après l'axiome de choix, il existe une application g de Y dans E telle que, pour tout $y \in Y$ on ait $g(y) \in X \cap \overset{-1}{f}(y)$; g est une application biunivoque de Y dans X, car la relation $y \neq z$ entraîne $\overset{-1}{f}(y) \cap \overset{-1}{f}(z)=\emptyset$, donc $g(y) \neq g(z)$.

6. Puissance d'une réunion. Puissance d'une somme. Proposition 13. Soit $(X_\lambda)_{\lambda\in L}$ une famille de parties de E, $(Y_\mu)_{\mu\in M}$ une famille de parties non vides de F telle que $\mu \neq \mu'$ entraîne $Y_\mu \cap Y_{\mu'} = \emptyset$; s'il existe une application biunivoque φ de L dans M telle que, pour tout $\lambda\in L$, X_λ ait une puissance inférieure à celle de $Y_{\varphi(\lambda)}$, alors la puissance de $\bigcup_{\lambda\in L} X_\lambda$ est inférieure à celle de $\bigcup_{\mu\in M} Y_\mu$.

En effet, $\bigcup_{\lambda\in L} X_\lambda$ est identique à la réunion des X_λ non vides ; on peut donc se borner au cas où tous les X_λ sont non vides. D'après l'axiome de choix, il existe une famille $(u_\lambda)_{\lambda\in L}$ d'applications de parties de E dans F, telle que, pour tout λ, u_λ soit une application biunivoque de X_λ dans $Y_{\varphi(\lambda)}$; posons $Z_\lambda = u_\lambda(X_\lambda)$; la relation $\lambda \neq \lambda'$ entraîne $\varphi(\lambda)\neq\varphi(\lambda')$, donc $Y_{\varphi(\lambda)} \cap Y_{\varphi(\lambda')} = \emptyset$, et a fortiori $Z_\lambda \cap Z_{\lambda'} = \emptyset$; autrement dit, $(Z_\lambda)_{\lambda\in L}$ est une partition de l'ensemble $Z = \bigcup_{\lambda\in L} Z_\lambda$. Soit alors v_λ l'application biunivoque de Z_λ sur X_λ, réciproque de u_λ ; il existe une application et une seule v de Z sur $\bigcup_{\lambda\in L} X_\lambda$, qui coïncide avec v_λ dans Z_λ pour tout $\lambda\in L$ (chap. II, § 5, prop. 14) ; d'après la prop. 12, $\bigcup_{\lambda\in L} X_\lambda$ a donc une puissance inférieure à celle de Z ; comme Z est une partie de $\bigcup_{\mu\in M} Y_\mu$, Z a une puissance inférieure à celle de $\bigcup_{\mu\in M} Y_\mu$, d'où la proposition.

Proposition 14. Soient $(X_\iota)_{\iota\in I}$, $(Y_\iota)_{\iota\in I}$ deux familles de parties non vides de E et F respectivement, ayant même ensemble d'indices et telles que $\iota \neq \varkappa$ entraîne $X_\iota \cap X_\varkappa = \emptyset$ et $Y_\iota \cap Y_\varkappa = \emptyset$; si, pour tout $\iota\in I$, X_ι est équipotent à Y_ι, alors $\bigcup_{\iota\in I} X_\iota$ est équipotent à $\bigcup_{\iota\in I} Y_\iota$.

En effet, l'axiome de choix montre qu'il existe une famille $(u_\iota)_{\iota\in I}$ telle que, pour tout ι, u_ι soit une application biunivoque de X_ι sur Y_ι ; il existe une application et une seule u de $\bigcup_{\iota\in I} X_\iota$ sur $\bigcup_{\iota\in I} Y_\iota$ qui coïncide avec u_ι dans X_ι pour tout $\iota\in I$; u est biunivoque, car la relation $x\neq y$ entraîne, ou bien qu'il existe deux indices $\iota, \varkappa$ tels que $\iota\neq\varkappa$ et $x\in X_\iota$, $y\in X_\varkappa$, d'où $u(x)=u_\iota(x)\in Y_\iota$ et $u(y)=u_\varkappa(y)\in Y_\varkappa$, et comme $Y_\iota\cap Y_\varkappa=\emptyset$, $u(x)\neq u(y)$; ou bien qu'il existe un indice ι tel que $x\in X_\iota$ et $y\in X_\iota$, d'où $u(x)=u_\iota(x)\neq u_\iota(y)=u(y)$, puisque u_ι est biunivoque par hypothèse.

On a des propositions analogues aux prop.13 et 14 lorsqu'il s'agit de réunions de plusieurs ensembles (cf. § 2).

On observera que dans ce cas on n'utilise pas l'axiome de choix pour l'analogue de la prop.14 .

La prop.14 peut s'interprèter en disant que deux ensembles sommes d'une même famille de parties non vides d'un ensemble E (chap.II, § 5, n°3) sont équipotents ; la prop.13 montre que la réunion d'une famille de parties non vides d'un ensemble E a une puissance inférieure à celle de leur somme.

7. Calcul sur les puissances. Soit $(\mathfrak{a}_\iota)_{\iota\in I}$ une famille d'éléments de l'ensemble $\varpi(E)$ des puissances des parties d'un ensemble E . Supposons qu'il existe une famille $(X_\iota)_{\iota\in I}$ de parties de E telle que $p(X_\iota)=\mathfrak{a}_\iota$ pour tout ι, et que $\iota\neq\varkappa$ entraîne $X_\iota\cap X_\varkappa=\emptyset$. Dans ces conditions, on dit que la famille de puissances $(\mathfrak{a}_\iota)$ est addible, et on appelle somme de cette famille la puissance de l'ensemble $\bigcup_{\iota\in I} X_\iota$, qu'on note $\sum_{\iota\in I}\mathfrak{a}_\iota$; il résulte aussitôt de la prop.14 que lorsque les $\mathfrak{a}_\iota$ sont tous distincts de $p(\emptyset)$ (que nous noterons 0) , la définition de la somme des $\mathfrak{a}_\iota$ ne dépend que de la famille $(\mathfrak{a}_\iota)$, et non de la famille (X_ι) ayant les propriétés précédentes ; en outre, il résulte aussitôt de la définition que, pour que la famille $(\mathfrak{a}_\iota)$ soit addible, il faut et il suffit que la sous-famille des $\mathfrak{a}_\iota\neq 0$ le soit

et qu'alors les sommes des deux familles sont égales.

De même, s'il existe une famille $(Y_\iota)_{\iota\in I}$ de parties de E telle que $p(Y_\iota) = \mathfrak{a}_\iota$ pour tout ι, et une partie de E équipotente à $\prod_{\iota\in I} Y_\iota$, on dit que la famille de puissances $(\mathfrak{a}_\iota)$ est <u>multipliable</u> et on appelle <u>produit</u> de cette famille la puissance de toute partie de E équipotente à $\prod_{\iota\in I} Y_\iota$, qu'on note $\prod_{\iota\in I} \mathfrak{a}_\iota$; il résulte encore ici de la prop.4 que cette définition ne dépend bien que de la famille $(\mathfrak{a}_\iota)$ et non de la famille (Y_ι).

De la même manière, on définit pour plusieurs éléments de $\varpi(E)$, par exemple trois éléments $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$, d'une part la notion d'<u>addibilité</u> et la <u>somme</u>, qu'on note $\mathfrak{a}+\mathfrak{b}+\mathfrak{c}$, et d'autre part la notion de <u>multipliabilité</u> et le <u>produit</u>, qu'on note $\mathfrak{a}\mathfrak{b}\mathfrak{c}$ (cf. § 2 pour la relation entre les deux sortes de définitions).

Enfin, si $\mathfrak{a}$ et $\mathfrak{b}$ sont deux éléments de $\varpi(E)$, et s'il existe une partie Z de E équipotente à X^Y, où X est une partie de E de puissance $\mathfrak{a}$, Y une partie de E de puissance $\mathfrak{b}$, la puissance de Z se note $\mathfrak{a}^{\mathfrak{b}}$; elle ne dépend que de $\mathfrak{a}$ et $\mathfrak{b}$ d'après le cor. de la prop.4 .

D'après cette définition, on a $\mathfrak{a}^{\mathfrak{b}} = \prod_{y\in Y} \mathfrak{a}_y$, où, pour tout $y \in Y$, $\mathfrak{a}_y = \mathfrak{a}$. On peut de même ramener le produit de deux puissances à une somme de puissances ; en effet, si $\mathfrak{a}\mathfrak{b}$ est défini, il existe une partie Z de E équipotente à $X \times Y$, où X est une partie de E de puissance $\mathfrak{a}$, Y une partie de E de puissance $\mathfrak{b}$; or, les ensembles $X \times \{y\}$ forment une partition de $X\times Y$, lorsque y parcourt Y ; comme chacun d'eux est équipotent à X, on voit qu'il existe une partition $(Z_y)_{y\in Y}$ de Z telle que pour tout $y \in Y$, Z_y soit équipotent à X ; on a donc

$$\mathfrak{a}\mathfrak{b} = \sum_{y\in Y} \mathfrak{a}_y \quad \text{où} \quad \mathfrak{a}_y = \mathfrak{a} \quad \text{pour tout } y\in Y.$$

On notera que si $(\mathfrak{a}'_\iota)_{\iota \in I}$ est une famille d'éléments de $\overline{\varpi}(F)$, telle que, pour tout $\iota \in I$, $\mathfrak{a}'_\iota$ soit équivalente à $\mathfrak{a}_\iota$, et si $\sum_{\iota \in I} \mathfrak{a}_\iota$ et $\sum_{\iota \in I} \mathfrak{a}'_\iota$ (resp. $\prod_{\iota \in I} \mathfrak{a}_\iota$ et $\prod_{\iota \in I} \mathfrak{a}'_\iota$) sont toutes deux définies, ces deux puissances sont équivalentes.

Ces définitions étant posées, les résultats antérieurs de ce paragraphe et certains résultats du chap. II fournissent des <u>égalités</u> et <u>inégalités</u> portant sur des puissances de parties de E. En premier lieu, on a des égalités qu'il faut entendre de la façon suivante : lorsque l'un des membres d'une telle égalité est défini, l'autre est défini et lui est égal. Tout d'abord, si $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ sont des éléments quelconques de $\overline{\varpi}(E)$, on a :

(1) $$\mathfrak{a}+\mathfrak{b} = \mathfrak{b}+\mathfrak{a} \quad , \quad \mathfrak{a}\mathfrak{b} = \mathfrak{b}\mathfrak{a}$$

("commutativité" de l'addition et de la multiplication ; cf. chap. II, § 2, prop. 11 et § 4, n°9) ;

(2) $$\mathfrak{a}+(\mathfrak{b}+\mathfrak{c}) = (\mathfrak{a}+\mathfrak{b})+\mathfrak{c} \quad , \quad \mathfrak{a}(\mathfrak{b}\mathfrak{c}) = (\mathfrak{a}\mathfrak{b})\mathfrak{c}$$

("associativité" de l'addition et de la multiplication ; cf. chap. II, § 2, prop. 15 et § 4, n°9). On a des formules d'"associativité" correspondantes pour la somme et le produit d'une famille quelconque $(\mathfrak{a}_\iota)_{\iota \in I}$ de puissances :

(3) $$\sum_{\lambda \in L}\Big(\sum_{\iota \in J_\lambda} \mathfrak{a}_\iota\Big) = \sum_{\iota \in I} \mathfrak{a}_\iota \quad , \quad \prod_{\lambda \in L}\Big(\prod_{\iota \in J_\lambda} \mathfrak{a}_\iota\Big) = \prod_{\iota \in I} \mathfrak{a}_\iota$$

où $(J_\lambda)_{\lambda \in L}$ est une <u>partition</u> de I (cela résulte sans peine, pour la somme, de la prop. 2 du chap. II, § 5, et pour le produit, de la prop. 14 du chap. II, § 5).

La relation $\sum_{\iota \in I} \mathfrak{a}_\iota = 0$ est équivalente à "quel que soit $\iota \in I$, $\mathfrak{a}_\iota = 0$" ; si $(\mathfrak{a}_\iota)_{\iota \in I}$ est une famille quelconque de puissances, J l'ensemble des $\iota \in I$ tels que $\mathfrak{a}_\iota \neq 0$, on a $\sum_{\iota \in I} \mathfrak{a}_\iota = \sum_{\iota \in J} \mathfrak{a}_\iota$. La relation $\prod_{\iota \in I} \mathfrak{a}_\iota = 0$ est équivalente (d'après l'axiome de choix) à "il existe $\iota \in I$ tel que $\mathfrak{a}_\iota = 0$". On a des résultats analogues (indépendants de l'axiome de choix) pour la somme et le produit de deux ou plusieurs puissances.

Si $(\mathfrak{a}_\iota)_{\iota\in I}$, $(\mathfrak{b}_\varkappa)_{\varkappa\in K}$ sont deux familles de puissances, on a la formule de "distributivité" :

$$(4)\qquad \Big(\sum_{\iota\in I}\mathfrak{a}_\iota\Big)\Big(\sum_{\varkappa\in K}\mathfrak{b}_\varkappa\Big) = \sum_{(\iota,\varkappa)\in I\times K}\mathfrak{a}_\iota\mathfrak{b}_\varkappa$$

qui découle aussitôt de la prop.4 du chap.II, § 5, ainsi que les formules analogues

$$(5)\qquad \mathfrak{a}\cdot\sum_{\varkappa\in K}\mathfrak{b}_\varkappa = \sum_{\varkappa\in K}\mathfrak{a}\mathfrak{b}_\varkappa$$

et

$$(6)\qquad \mathfrak{a}(\mathfrak{b}+\mathfrak{c}) = \mathfrak{a}\mathfrak{b}+\mathfrak{a}\mathfrak{c}\ .$$

De la prop.5 on déduit la formule

$$(7)\qquad \mathfrak{b}^{\sum_{\iota\in I}\mathfrak{a}_\iota} = \prod_{\iota\in I}\mathfrak{b}^{\mathfrak{a}_\iota}$$

et l'analogue

$$(8)\qquad \mathfrak{a}^{\mathfrak{b}+\mathfrak{c}} = \mathfrak{a}^{\mathfrak{b}}\mathfrak{a}^{\mathfrak{c}}$$

De la prop.6 on déduit

$$(9)\qquad (\mathfrak{a}^{\mathfrak{b}})^{\mathfrak{c}} = \mathfrak{a}^{\mathfrak{b}\mathfrak{c}}$$

Enfin la prop.7 donne la formule

$$(10)\qquad \Big(\prod_{\iota\in I}\mathfrak{a}_\iota\Big)^{\mathfrak{b}} = \prod_{\iota\in I}\mathfrak{a}_\iota^{\mathfrak{b}}$$

ainsi que l'analogue

$$(11)\qquad (\mathfrak{a}\mathfrak{b})^{\mathfrak{c}} = \mathfrak{a}^{\mathfrak{c}}\mathfrak{b}^{\mathfrak{c}}$$

Passons aux <u>inégalités</u> ; il faut encore ici entendre celles que nous écrirons de la façon suivante : lorsque le second membre est défini, le premier membre est défini et l'inégalité a lieu.

En premier lieu, pour toute famille $(\mathfrak{a}_\iota)_{\iota\in I}$ de puissances, on a

$$(12)\qquad \sum_{\iota\in J}\mathfrak{a}_\iota \leqslant \sum_{\iota\in I}\mathfrak{a}_\iota$$

pour toute partie J de I , ainsi que

$$(13)\qquad \prod_{\iota\in J}\mathfrak{a}_\iota \leqslant \prod_{\iota\in I}\mathfrak{a}_\iota$$

pourvu que tous les $\mathfrak{a}_\iota$ soient $\neq 0$ (prop.11) ; on a de même les analogues

(14) $$\mathfrak{a} \leqslant \mathfrak{a} + \mathfrak{b}$$

(15) $$\mathfrak{a} \leqslant \mathfrak{a}\mathfrak{b}$$

pourvu, dans la formule (15) que $\mathfrak{b} \neq 0$.

L'inégalité (14) admet la réciproque suivante : si $\mathfrak{a}$ et $\mathfrak{b}$ sont deux puissances telles que $\mathfrak{a} \leqslant \mathfrak{b}$, il existe $\mathfrak{c} \in \varpi(E)$ telle que $\mathfrak{a} + \mathfrak{c}$ soit définie et $\mathfrak{b} = \mathfrak{a} + \mathfrak{c}$: en effet, si M est une partie de E de puissance $\mathfrak{b}$, il existe une partie N de M de puissance $\mathfrak{a}$; il suffit de prendre pour $\mathfrak{c}$ la puissance de $M \cap \complement N$.

Si maintenant $(\mathfrak{a}_\iota)_{\iota \in I}$ et $(\mathfrak{b}_\iota)_{\iota \in I}$ sont deux familles de puissances ayant même ensemble d'indices, la relation $\mathfrak{a}_\iota \leqslant \mathfrak{b}_\iota$ pour tout $\iota \in I$ entraîne $\sum_{\iota \in I} \mathfrak{a}_\iota \leqslant \sum_{\iota \in I} \mathfrak{b}_\iota$, et $\prod_{\iota \in I} \mathfrak{a}_\iota \leqslant \prod_{\iota \in I} \mathfrak{b}_\iota$; de même, les relations $\mathfrak{a} \leqslant \mathfrak{a}'$, $\mathfrak{b} \leqslant \mathfrak{b}'$ entraînent $\mathfrak{a}+\mathfrak{b} \leqslant \mathfrak{a}'+\mathfrak{b}'$, $\mathfrak{a}\mathfrak{b} \leqslant \mathfrak{a}'\mathfrak{b}'$ et enfin $\mathfrak{a}^{\mathfrak{b}} \leqslant \mathfrak{a}'^{\mathfrak{b}'}$ (prop.10, 11 et 13).

<u>Exercice</u>. Soient $(E_\iota)_{\iota \in I}$, $(F_\iota)_{\iota \in I}$ deux familles d'ensembles non vides ayant même ensemble d'indices.

a) Si pour tout ι , E_ι est équipotent à une partie de F_ι distincte de F_ι , tout ensemble somme des E_ι a une puissance inférieure à celle de $\prod_{\iota \in I} F_\iota$.

b) Si pour tout ι E_ι a une puissance <u>strictement inférieure</u> à F_ι , tout ensemble somme des E_ι a une puissance <u>strictement inférieure</u> à $\prod_{\iota \in I} F_\iota$ (montrer qu'il ne peut exister une partition $(A_\iota)_{\iota \in I}$ de $\prod_{\iota \in I} F_\iota$ telle que A_ι soit équipotent à E_ι , en remarquant que $pr_\iota A_\iota$ ne peut être identique à F_ι).

§ 2. Ensembles finis.

Dans toutes les démonstrations de ce paragraphe, il n'est pas fait usage de l'axiome de choix.

1. Ensembles énumérés. Au chap. II, § 2, n°4, on a défini une partie d'un ensemble réduite à un seul élément. En particulier, dire qu'un ensemble E est réduit à un seul élément, ou, comme nous dirons aussi, que E est un ensemble à un élément, signifie que la relation : "il existe $a \in E$ tel que $E = \{a\}$ " est vraie. Se donner un ensemble E à un élément sera par définition considérer une théorie dans laquelle E sera un argument de base, et la relation précédente un axiome ; il revient d'ailleurs au même (chap. I, § 3, n°1) de prendre comme arguments de base E et a, avec les deux axiomes : $a \in E$, $E = \{a\}$; a est alors appelé l'élément (unique) de E.

Nous dirons maintenant qu'un ensemble E est un ensemble à deux éléments si la relation "il existe $a \in E$ et $b \in E$ tels que $a \neq b$ et $E = \{a, b\}$ " est vraie ; se donner un ensemble à deux éléments, c'est prendre pour axiome cette relation (E étant argument de base), ou encore prendre pour arguments de base E, a, b, avec les axiomes : $a \in E$, $b \in E$, $a \neq b$, $E = \{a, b\}$; a et b sont alors appelés les deux éléments de E.

On définit de la même manière un ensemble ayant un nombre quelconque d'éléments : on prend comme arguments de base E et le nombre voulu de signes (tous distincts entre eux et distincts de E) qu'on appelle les éléments énumérés de E ; on prend comme axiomes : 1° ceux obtenus en remplaçant ξ par les éléments énumérés de E dans $\xi \in E$; 2° ceux obtenus en remplaçant ξ et η par deux éléments énumérés distincts (de toutes les manières possibles) dans $\xi \neq \eta$; 3° l'axiome exprimant que E est réunion des ensembles dont chacun est réduit à un élément énuméré de E. De façon générale, un ensemble ainsi introduit sera appelé ensemble énuméré.

La notion de "nombre" qui intervient dans ces définitions est la notion expérimentale de nombre, c'est-à-dire qu'un nombre n'est considéré comme donné que lorsqu'on a écrit explicitement autant de signes distincts qu'il comporte d'unités. Il faut se garder de confondre cette notion avec celle d'entier naturel qui sera définie au §3, malgré les liens étroits qui les unissent et que nous verrons en leur lieu. En fait, nous verrons même que ces liens dispensent, dans la plupart des questions, d'avoir recours à la notion d'ensemble énuméré. Mais, du point de vue logique, l'intérêt de cette dernière est qu'elle ne dépend nullement de la théorie des entiers ; de façon plus précise on peut prouver aisément que la théorie d'un ensemble énuméré est non-contradictoire sans supposer que la théorie des entiers (ou, ce qui revient au même, la théorie des ~~xxxxxxxxxxxx~~ ensembles infinis) le soit; il suffit de supposer que la théorie des parties d'un ensemble E est non-contradictoire. En effet, si E est un ensemble quelconque $F=\{\emptyset\}$ est un ensemble à un élément (partie explicite de $\mathfrak{P}(E)$) ; si $E = \{a\}$ est un ensemble à un élément, $F=\{\emptyset, \{a\}\}$ est un ensemble à deux éléments (partie de $\mathfrak{P}(E)$) ; le procédé est évidemment applicable de proche en proche pour tout ensemble énuméré (il ne s'agit naturellement pas là d'un véritable "raisonnement par récurrence" au sens qui sera défini plus loin, mais de l'indication d'un procédé opératoire qui doit être réalisé explicitement pas à pas, dans chaque cas déterminé que l'on considère).

La notion d'ensemble énuméré permet de ramener les définitions de la <u>réunion</u> et de l'<u>intersection</u> de deux ou plusieurs ensembles (chap. II, § 2, n° 4) aux définitions de la réunion et de l'intersection d'une <u>famille</u> d'ensembles (chap. II, § 5, n°2 et n°4). En effet, soient X, Y, Z trois parties (par exemple) d'un ensemble E ; soit $I = \{\alpha, \beta, \gamma\}$ un ensemble de trois éléments, et soit $(M_\iota)_{\iota \in I}$ la famille de parties de E définie par les conditions $M_\alpha = X$, $M_\beta = Y$, $M_\gamma = Z$; on vérifie aussitôt que l'on a $\bigcup_{\iota \in I} M_\iota = X \cup Y \cup Z$, $\bigcap_{\iota \in I} M_\iota = X \cap Y \cap Z$. Les propriétés de la réunion et de l'intersection de plusieurs ensembles peuvent donc être considérées comme des cas particuliers de propriétés de la réunion et de l'intersection d'une famille d'ensembles.

2. <u>Ensembles finis</u>. La définition d'un ensemble fini que nous allons donner provient de la propriété fondamentale dont jouissent ces ensembles dans la conception "naïve" des mathématiques : on "ajoute" un élément à un ensemble fini, il reste fini. L'ensemble $\mathfrak{F}(E)$ des parties finies d'un ensemble E, que nous voulons définir, doit donc avoir la propriété que, si $X \in \mathfrak{F}(E)$, $X \cup \{y\}$ appartient aussi à $\mathfrak{F}(E)$ pour tout $y \in E$; mais cette propriété à elle seule ne suffit pas à définir (E), car il est évident que $\mathfrak{P}(E)$ la possède également. Nous sommes ainsi conduits à la définition suivante :

<u>Définition 1. Soit Φ la partie de $\mathfrak{P}(\mathfrak{P}(E))$ formée des ensembles $\mathfrak{G} \subset \mathfrak{P}(E)$ tels que : 1° $\emptyset \in \mathfrak{G}$; 2° quel que soit $X \in \mathfrak{G}$ et quel que soit $y \in E$, $X \cup \{y\} \in \mathfrak{G}$. On appelle ensemble des parties finies de E l'intersection $\mathfrak{F}(E) = \bigcap_{\mathfrak{G} \in \Phi} \mathfrak{G}$ des ensembles $\mathfrak{G} \in \Phi$; toute partie de E qui appartient à $\mathfrak{F}(E)$ est dite finie, toute partie de E qui n'appartient pas à $\mathfrak{F}(E)$ est dite infinie.</u>

Il est immédiat que $\mathfrak{F}(E)$ appartient à Φ ; en effet, comme $\emptyset \in \mathfrak{G}$ pour tout $\mathfrak{G} \in \Phi$, on a aussi $\emptyset \in \mathfrak{F}(E)$; d'autre part, si $X \in \mathfrak{F}(E)$ et $y \in E$, on a $X \in \mathfrak{S}$ pour tout $\mathfrak{S} \in \Phi$, donc $X \cup \{y\} \in \mathfrak{S}$, et par suite $X \cup \{y\} \in \mathfrak{F}(E)$.

La déf.1 donne le critère fondamental suivant :

<u>Proposition 1</u>. <u>Soit</u> $\mathfrak{S}$ <u>une partie de</u> $\mathfrak{F}(E)$ <u>telle que</u> : 1° $\emptyset \in \mathfrak{S}$; 2° <u>quel que soit</u> $X \in \mathfrak{S}$ <u>et quel que soit</u> $y \in E$, $X \cup \{y\} \in \mathfrak{S}$. <u>Dans ces conditions, on a</u> $\mathfrak{S} = \mathfrak{F}(E)$.

En effet, la définition de $\mathfrak{F}(E)$ montre que $\mathfrak{F}(E) \subset \mathfrak{S}$, et comme par hypothèse $\mathfrak{S} \subset \mathfrak{F}(E)$, on a $\mathfrak{S} = \mathfrak{F}(E)$.

Comme $\mathfrak{F}(E)$ appartient à Φ, l'ensemble vide est fini ; toute partie $\{x\}$ à un élément est finie, puisque $\{x\} = \emptyset \cup \{x\}$; on voit de même que $\{x,y\}$, $\{x,y,z\}$, etc. sont des ensembles finis quels que soient x,y,z, etc. dans E.

<u>Proposition 2</u>. <u>Si</u> X <u>est une partie finie de</u> E, <u>toute partie</u> Y <u>de</u> X <u>est finie</u>.

Soit $\mathfrak{S}$ l'ensemble des parties X de E telles que toute partie Y de X soit finie ; en particulier, $Y=X$ doit être fini, donc $\mathfrak{S} \subset \mathfrak{F}(E)$. On a évidemment $\emptyset \in \mathfrak{S}$; d'autre part, soit X une partie appartenant à $\mathfrak{S}$, y un élément quelconque de E ; pour toute partie Z de $X \cup \{y\}$, on peut écrire $Z=Z \cap (X \cup \{y\})=(Z \cap X) \cup (Z \cap \{y\})$; comme on a $Z \cap \{y\} \subset \{y\}$, on a $Z \cap \{y\} = \emptyset$ ou $Z \cap \{y\} = \{y\}$ d'où $Z=(Z \cap X)$ ou $Z=(Z \cap X) \cup \{y\}$; comme $Z \cap X$ est finie par hypothèse, il en est de même de Z, donc $X \cup \{y\} \in \mathfrak{S}$. D'après la prop.1, on a $\mathfrak{S} = \mathfrak{F}(E)$.

<u>Proposition 3</u>. <u>Soit</u> f <u>une application de</u> E <u>dans</u> F ; <u>pour toute partie finie</u> X <u>de</u> E, $f(X)$ <u>est une partie finie de</u> F.

Soit $\mathfrak{S}$ l'ensemble des parties finies X de E telles que $f(X)$ soit finie. On a $\emptyset \in \mathfrak{S}$, puisque $f(\emptyset)=\emptyset$; d'autre part, si $X \in \mathfrak{S}$ et $y \in E$, on a $f(X \cup \{y\})=f(X) \cup f(\{y\})=f(X) \cup \{f(y)\}$, donc $X \cup \{y\} \in \mathfrak{S}$. Comme $\mathfrak{S} \subset \mathfrak{F}(E)$, on a $\mathfrak{S} = \mathfrak{F}(E)$ d'après la prop.1

Corollaire. *Toute partie de F équipotente à une partie finie de E est finie ; toute partie de F dont la puissance est inférieure à celle d'une partie finie de E est finie.*

Proposition 4. *Si X et Y sont des parties finies de E , $X \cup Y$ est fini .*

Soit $\mathfrak{G}$ l'ensemble des parties X de E telles que, pour toute partie finie Y de E , $X \cup Y$ soit fini. Comme $X \subset X \cup Y$, on voit d'abord que X doit être finie, donc $\mathfrak{G} \subset \mathfrak{F}(E)$. On a évidemment $\emptyset \in \mathfrak{G}$; d'autre part, si $X \in \mathfrak{G}$ et $y \in E$, pour toute partie finie Y de E , on a $(X \cup \{y\}) \cup Y = X \cup (Y \cup \{y\})$; comme $Y \cup \{y\}$ est finie, il en est de même de $X \cup (Y \cup \{y\})$; donc $X \cup \{y\} \in \mathfrak{G}$. D'après la prop.1, on a donc $\mathfrak{G} = \mathfrak{F}(E)$.

On déduit aussitôt de cette proposition que si X,Y,Z sont finis il en est de même de $X \cup Y \cup Z$, et de même pour la réunion d'un nombre quelconque d'ensembles finis.

Corollaire. *Tout ensemble réunion de plusieurs ensembles finis est fini.*

Proposition 5. *Si X est une partie finie de E , Y une partie finie de F , $X \times Y$ est une partie finie de $E \times F$.*

En effet, si V est vide, la proposition est évidente ; sinon, soit $\mathfrak{G}$ l'ensemble des parties X de E telles que $X \times Y$ soit une partie finie de $E \times F$. Comme X est la projection de $X \times Y$ sur E , X doit être fini (prop.3), donc $\mathfrak{G} \subset \mathfrak{F}(E)$. On a évidemment $\emptyset \in \mathfrak{G}$, puisque $\emptyset \times Y$ est vide. D'autre part, si $X \in \mathfrak{G}$ et $y \in E$, on a $(X \cup \{y\}) \times Y = (X \times Y) \cup (\{y\} \times Y)$; $X \times Y$ est fini, $\{y\} \times Y$ est équipotent à Y , donc fini, par suite (prop.4) $(X \cup \{y\}) \times Y$ est fini ; d'après la prop.1 , on a $\mathfrak{G} = \mathfrak{F}(E)$.

Proposition 6. *Si X est une partie finie de E , $\mathfrak{P}(X)$ est une partie finie de $\mathfrak{P}(E)$.*

Soit $\mathfrak{G}$ l'ensemble des parties X de E telles que $\mathfrak{P}(X)$ soit une partie finie de $\mathfrak{P}(E)$; comme X est équipotent à une partie de $\mathfrak{P}(X)$, X doit être finie (prop.2), donc $\mathfrak{G} \subset \mathfrak{F}(E)$. On a $\mathfrak{P}(\emptyset) = \{\emptyset\}$, donc $\emptyset \in \mathfrak{G}$; d'autre part, si $X \in \mathfrak{G}$ et $y \in E$, la relation $Y \subset X \cup \{y\}$ équivaut à $Y \subset X$ ou $Y = Z \cup \{y\}$, où $Z \subset X$; autrement dit $\mathfrak{P}(X \cup \{y\})$ est réunion de $\mathfrak{P}(X)$ et de l'image de $\mathfrak{P}(X)$ par l'application $Z \to Z \cup \{y\}$; ces deux ensembles étant finis (prop.3) $\mathfrak{P}(X \cup \{y\})$ est fini (prop.4) ; donc $\mathfrak{G} = \mathfrak{F}(E)$ d'après la prop.

Corollaire. Si X est une partie finie de E , Y une partie finie de F , Y^X est une partie finie de $\Phi(E,F)$.

En effet, Y^X est une partie de $\mathfrak{P}(X \times Y)$ (prop.5 et 6) .

3. Puissances de parties finies. Le raisonnement par récurrence. Nous désignerons par $\vartheta(E)$ la partie de l'ensemble $\varpi(E)$ des puissances des parties de E , formée des puissances des parties finies de E ; dire qu'une partie de E a une puissance appartenant à $\vartheta(E)$ équivaut à dire qu'elle est finie (cor. de la prop.3) ; lorsque X est une partie finie de E , sa puissance $n = p(X)$ est encore appelée le nombre d'éléments de X , et on dit que X est un ensemble à n éléments.

L'emploi du mot "nombre" dans cette définition est bien entendu purement conventionnel, et ne doit pas entraîner de confusion avec la notion expérimentale de nombre ; les relations entre les deux notions seront précisées au § 3 .

Les prop. 2,4,5,6 se traduisent en les propriétés suivantes de $\vartheta(E)$: si $n \in \vartheta(E)$ et $\mathfrak{a} \leq n$, on a $\mathfrak{a} \in \vartheta(E)$; si m et n appartiennent à $\vartheta(E)$, et si $m+n$ (resp. mn , m^n) est défini, il appartient à $\vartheta(E)$.

D'après la déf. 1, on a $0 \in \mathfrak{P}(E)$. D'autre part une partie $\{x\}$ de E et une partie $\{y\}$ de F réduites chacune à un élément, sont équipotentes, car l'application u dont le graphe dans $E \times F$ est $\{(x,y)\}$, est une application biunivoque de $\{x\}$ sur $\{y\}$. Nous désignerons par 1 la puissance des parties de E réduites à un élément ; on a évidemment $1 \in \mathfrak{P}(E)$; la relation $\mathfrak{a} \neq 0$ est équivalente à $1 \leqslant \mathfrak{a}$. Si $(\mathfrak{a}_\iota)_{\iota \in I}$ est une famille quelconque de puissances de parties de E, on a $\prod_{\iota \in \emptyset} \mathfrak{a}_\iota = 1$. Cela étant, si $n \in \mathfrak{P}(E)$ et si $n+1$ est défini, on a $n+1 \in \mathfrak{P}(E)$; lorsque $n+1$ est défini, on dit encore que c'est le <u>conséquent</u> de n ; on notera que s'il existe $n \in \mathfrak{P}(E)$ tel que $n+1$ ne soit pas défini, E est un ensemble fini de puissance n d'après la définition de la somme de deux puissances.

La prop. 1 se traduit en l'énoncé fondamental suivant, dit <u>principe d'induction totale</u> ou <u>principe de récurrence</u> :

<u>Théorème 1</u>. <u>Soit</u> H <u>une partie de</u> $\mathfrak{P}(E)$ <u>ayant les propriétés suivantes</u> : 1° $0 \in H$; 2° <u>si</u> $n \in H$ <u>et si</u> $n+1$ <u>est défini, alors</u> $n+1 \in H$. <u>Dans ces conditions, on a</u> $H = \mathfrak{P}(E)$.

En effet, soit $\mathfrak{G}$ l'ensemble des parties de E dont la puissance appartient à H ; on a par hypothèse $\mathfrak{G} \subset \mathfrak{F}(E)$, et $\emptyset \in \mathfrak{G}$. En outre, si $X \in \mathfrak{G}$ et $y \in E$, ou bien $y \in X$, d'où $X \cup \{y\} = X \in \mathfrak{G}$, ou bien $y \notin X$, et dans ce cas, si n est la puissance de X, $X \cup \{y\}$ a pour puissance $n+1 \in H$, donc $X \cup \{y\} \in \mathfrak{G}$; la prop. 1 prouve donc que $\mathfrak{G} = \mathfrak{F}(E)$, d'où $H = \mathfrak{P}(E)$.

On applique le plus souvent le principe d'induction totale sous la forme suivante : soit R une relation contenant comme argument libre un élément arbitraire n de $\mathfrak{P}(E)$; alors, si dans une théorie $\mathcal{C}$; la relation $(0|n)R$ est vraie, et si (dans la même théorie) la relation (R et $(\exists m \in \mathfrak{P}(E))(m=n+1)$) <u>entraîne</u> $(n+1|n)R$, on en conclut que, dans $\mathcal{E}$, la relation R est <u>vraie</u>. En effet, si H est l'ensemble des $n \in \mathfrak{I}(E)$ où R a lieu, H satisfait aux conditions du th.1, donc $H = \mathfrak{I}(E)$.

Lorsqu'on applique ce principe, on dit qu'on <u>raisonne par récurrence sur n</u> ; la relation $(R \text{ et } (\exists m \in \mathfrak{I}(E))(m=n+1))$ est alors appelée l'<u>hypothèse de récurrence</u>.

Le principe d'induction totale (que nous avons déjà appliqué sous une autre forme au n°2) va nous fournir d'autres propriétés de l'ensemble $\mathfrak{I}(E)$.

<u>Proposition 7</u>. <u>Soient</u> $\mathfrak{a}$, $\mathfrak{b}$ <u>deux éléments de</u> $\overline{\omega}(E)$, <u>n un élément de</u> $\mathfrak{I}(E)$; <u>si</u> $\mathfrak{a}+n$ <u>et</u> $\mathfrak{b}+n$ <u>sont définis et si</u> $\mathfrak{a}+n=\mathfrak{b}+n$, <u>on a</u> $\mathfrak{a}=\mathfrak{b}$.

Nous démontrerons la proposition par récurrence sur n ; de façon précise, la relation R à démontrer est "quels que soient $\mathfrak{a} \in \overline{\omega}(E)$ $\mathfrak{b} \in \overline{\omega}(E)$, s'il existe $\mathfrak{c} \in \overline{\omega}(E)$ tel que $\mathfrak{c} = \mathfrak{a}+n$ et $\mathfrak{c} = \mathfrak{b}+n$, $\mathfrak{a}=\mathfrak{b}$". Pour $n=0$, la relation est triviale ; montrons que l'hypothèse de récurrence entraîne que, si $\mathfrak{a}+(n+1)$ et $\mathfrak{b}+(n+1)$ sont définis et égaux, on a $\mathfrak{a}=\mathfrak{b}$. On peut se ramener au cas où $n=0$; en effet, supposons la démonstration faite dans ce cas ; la relation $\mathfrak{a}+(n+1)=\mathfrak{b}+(n+1)$ s'écrit $(\mathfrak{a}+n)+1 = (\mathfrak{b}+n)+1$; on en déduira $\mathfrak{a}+n = \mathfrak{b}+n$, et par l'hypothèse de récurrence, $\mathfrak{a}=\mathfrak{b}$.

Supposons donc que $\mathfrak{a}+1 = \mathfrak{b}+1$ (les deux puissances étant définies) Il existe donc deux parties M,N de E, de puissances respectives $\mathfrak{a}$ et $\mathfrak{b}$, un élément $a \notin M$ et un élément $b \notin N$ tels qu'il existe une application biunivoque f de $M'=M \cup \{a\}$ sur $N'=N \cup \{b\}$. Si on a $f(a)=b$, la restriction de f à M est une application biunivoque de M sur le complémentaire de $\{f(a)\}$ par rapport à N', c'est-à-dire sur N, et on a bien $\mathfrak{a}=\mathfrak{b}$. Si $b'=f(a)\neq b$, on a $b' \in N$, et si a' est l'unique élément de M' tel que $f(a')=b$, on a $a' \in M$ (puisque $f(a) \neq b$). Comme f applique $\{a,a'\}$ sur $\{b,b'\}$, il applique le complémentaire $M \cap \complement \{a'\}$ de $\{a,a'\}$ par rapport à M' sur le complémentaire $N \cap \complement \{b'\}$ de $\{b,b'\}$ par rapport à N' ; les puissances $\mathfrak{a}'$, $\mathfrak{b}'$ de ces complémentaires sont donc égales ; mais on a $\mathfrak{a} = \mathfrak{a}'+1$, $\mathfrak{b} = \mathfrak{b}'+1$, donc $\mathfrak{a} = \mathfrak{b}$.

Corollaire 1. Si m et p appartiennent à $\vartheta(E)$, la relation $m+p=m$ entraîne $p=0$ (autrement dit $p > 0$ entraîne $m < m+p$).

Corollaire 2. Si E est un ensemble fini, la seule partie de E équipotente à E est E lui-même.

En effet, si X était une partie de E distincte de E et équipotente à E , on aurait, en désignant par m et p les puissances de E et de $\complement X$ la relation $m+p=m$, ce qui contredit l'hypothèse $p > 0$.

Ce corollaire montre que si E est un ensemble fini de puissance n , $n+1$ n'est pas défini ; on peut donc dire que la condition nécessaire et suffisante pour que E soit fini est qu'il existe un $n \in \vartheta(E)$ tel que $n+1$ ne soit pas défini ; cet élément n est alors égal à la puissance de E .

Proposition 8. Soient m et n deux éléments de $\vartheta(E)$; pour que $m \leqslant n$, il faut et il suffit qu'il existe $p \in \vartheta(E)$ tel que $n=m+p$; il existe alors un seul élément $p \in \vartheta(E)$ ayant cette propriété.

La seconde partie de la proposition est une conséquence évidente de la prop.7 . La première est un cas particulier d'une proposition valable pour les puissances quelconques (§ 1,n°7), compte tenu de ce que $\mathfrak{a} \leqslant n$ entraîne que $\mathfrak{a}$ est finie.

Si $m \leqslant n$, l'unique élément $p \in \vartheta(E)$ tel que $m+p=n$ est appelé la *différence* des puissances n et m et se note $n-m$; l'application

28

$(n,m) \to n-m$ est donc définie dans la partie de $\mathfrak{I}(E) \times \mathfrak{I}(E)$ formée des couples tels que $m \leqslant n$.

En particulier, n-1 est défini pour tout $n > 0$; on dit que n-1 est l'<u>antécédent</u> de n ; deux éléments m,n de $\mathfrak{I}(E)$ tels que $m=n+1$ sont dits <u>consécutifs</u>.

<u>Remarque</u>. On applique souvent le principe d'induction totale, non pas "à partir de n=0", mais "à partir de n=h". De façon précise, soit R une relation contenant comme argument libre un élément arbitraire n de $\mathfrak{I}(E)$; si, dans une théorie $\mathcal{C}$, la relation $(h|n)R$ est vraie, ainsi que la relation $((R \text{ et } (\exists\, m \in \mathfrak{I}(E))(m=n+1)) \to (n+1|n)\, R)$ pour tout $n \in \mathfrak{I}(E)$ tel que $n \geqslant h$, alors la relation $n \geqslant h$ <u>entraîne</u> R dans la théorie $\mathcal{C}$; c'est ce que montre aussitôt le principe d'induction totale appliqué à la relation $(h+m|n)R$ et à l'argument $m \in \mathfrak{I}(E)$.

<u>Corollaire 1</u>. <u>Pour que</u> $m < n$, <u>il faut et il suffit qu'il existe</u> $p \in \mathfrak{I}(E)$ <u>tel que</u> $n=m+p$ <u>et</u> $p > 0$.

En effet, si $n=m+p$ et $p > 0$, on a $m \leqslant n$, et si on avait $m=n=m+p$, on en déduirait $p=0$ (cor. de la prop.7) contrairement à l'hypothèse ; inversement, si $m < n$, on a $n=m+p$, et la relation $p=0$ entraînerait $m=n$ contrairement à l'hypothèse.

<u>Corollaire 2</u>. <u>Si</u> $\mathfrak{a}+p$ <u>et</u> $\mathfrak{b}+p$ <u>sont définis</u> ($\mathfrak{a} \in \overline{\omega}(E)$, $\mathfrak{b} \in \overline{\omega}(E)$, $p \in \mathfrak{I}(E)$) <u>la relation</u> $\mathfrak{a} \leqslant \mathfrak{b}$ (resp. $\mathfrak{a} < \mathfrak{b}$) <u>est équivalente à</u> $\mathfrak{a}+p \leqslant \mathfrak{b}+p$ (resp. $\mathfrak{a}+p < \mathfrak{b}+p$) .

Comme $\mathfrak{a} \leqslant \mathfrak{b}$ entraîne $\mathfrak{a}+p \leqslant \mathfrak{b}+p$, et que $\mathfrak{a}+p = \mathfrak{b}+p$ est équivalente à $\mathfrak{a} = \mathfrak{b}$ (prop.7), tout revient à montrer que $\mathfrak{a}+p \leqslant \mathfrak{b}+p$ entraîne $\mathfrak{a} \leqslant \mathfrak{b}$. Or, si $\mathfrak{a}+p \leqslant \mathfrak{b}+p$, il existe $\mathfrak{k} \in \overline{\omega}(E)$ tel que $(\mathfrak{a}+p)+\mathfrak{k}$ soit défini et $\mathfrak{b}+p = (\mathfrak{a}+p)+\mathfrak{k} = (\mathfrak{a}+\mathfrak{k})+p$;

on en déduit $\mathfrak{b} = \mathfrak{a} + \mathfrak{c}$ (prop.7) d'où $\mathfrak{a} \leqslant \mathfrak{b}$.

Lorsque m,n,p appartiennent à $\vartheta(E)$, que m+p et n+p sont définis et $m \leqslant n$, on a $n=m+q$, donc $n+p=(m+p)+q$ autrement dit $(n+p)-(m+p)=n-m$.

<u>Corollaire 3.- La relation</u> $n < \mathfrak{a}$ $(n \in \vartheta(E)$, $\mathfrak{a} \in \varpi(E))$ <u>est équivalente à</u> "$n+1$ <u>est défini et</u> $n+1 \leqslant \mathfrak{a}$".

En effet, si $n < \mathfrak{a}$, il existe $\mathfrak{b} \in \varpi(E)$ tel que $n+\mathfrak{b} = \mathfrak{a}$, et on a $\mathfrak{b} > 0$, donc $\mathfrak{b} \geqslant 1$, ce qui montre que n+1 est défini et $n+1 \leqslant n+\mathfrak{b} = \mathfrak{a}$; inversement, si n+1 est défini et $n+1 \leqslant \mathfrak{a}$, on a $n < n+1 \leqslant \mathfrak{a}$, donc (§1,prop.8), $n < \mathfrak{a}$.

<u>Proposition 9. Quels que soient</u> $\mathfrak{a} \in \varpi(E)$ <u>et</u> $n \in \vartheta(E)$, <u>on a</u> $\mathfrak{a}=n$ <u>ou</u> $\mathfrak{a} < n$ <u>ou</u> $n < \mathfrak{a}$.

Raisonnons par récurrence sur n ; la proposition est vraie pour n=0, puisque $0 \leqslant \mathfrak{a}$ pour tout $\mathfrak{a} \in \varpi(E)$. Si $\mathfrak{a} \leqslant n$ et si n+1 est défini, on a $\mathfrak{a} \leqslant n < n+1$ donc $\mathfrak{a} \leqslant n+1$; si au contraire $n < \mathfrak{a}$, n+1 est défini et $n+1 \leqslant \mathfrak{a}$ (cor.3 de la prop.8), d'où la proposition.

On notera que si E est fini et de puissance n, on a $m \leqslant n$ pour tout $m \in \varpi(E)$.

Etant donnés deux éléments quelconques m,n de $\vartheta(E)$ tels que $m \leqslant n$ nous désignerons désormais par $[m,n]$ (resp. $[m,n[$) l'ensemble des $p \in \vartheta(E)$ tels que $m \leqslant p \leqslant n$ (resp. $m \leqslant p < n$) (cf.chap.IV, §   ) ; si $n=m$, on a $[m,m] = \{m\}$, et $[m,m[= \emptyset$; si $m < n$, on a $[m,n[= [m,n-1]$ (cor.3 de la prop.8). Si $m \leqslant n \leqslant p$, il résulte de la prop.9 que $[m,p]$ (resp. $[m,p[$) est réunion de $[m,n]$ et $[n,p]$ (resp. de $[m,n[$ et de $[n,p[$) ; en outre, l'intersection de $[m,n]$ et $[n,p]$ se réduit à $\{n\}$, l'intersection de $[m,n[$ et $[n,p[$ est vide.

<u>Proposition 10</u>. <u>Pour tout</u> $n \in \mathfrak{I}(E)$, <u>l'ensemble</u> $[0,n[$ <u>a une puissance équivalente à n</u> .

Raisonnons par récurrence sur n , la proposition étant évidente pour $n=0$, puisque $m \geqslant 0$ pour tout $m \in \mathfrak{I}(E)$. Si $n+1$ est défini, l'ensemble $[0,n+1[$ est réunion de $[0,n[$ et de $[n,n+1[= \{n\}$; par définition, $n \notin [0,n[$, donc la puissance de $[0,n+1[$ est équivalente à $n+1$, ce qui démontre la proposition.

Si on pose $I = [0,n[$, l'application $m \to p([0,m[)$ de I dans $\overline{\omega}(I)$ est donc une application biunivoque ; elle applique en outre I <u>sur</u> $\overline{\omega}(I)$, car toute partie de I a une puissance inférieure à celle de I , donc équivalente à un élément $m \in I \subset \overline{\omega}(E)$, et par suite égale à $p([0,m[)$. Nous <u>identifierons</u> désormais $[0,n[$ à l'ensemble des puissances des parties de $[0,n[$ au moyen de cette application.

<u>Corollaire</u>. <u>Si</u> $m \leqslant n$, <u>l'ensemble</u> $[m,n[$ <u>a une puissance équivalente à</u> $n-m$.

En effet, $[0,n[$ est réunion des ensembles $[0,m[$ et $[m,n[$ sans élément commun, donc $n=m+p$, où p est la puissance de $[m,n[$.

La proposition 10 permet de donner une autre forme au principe d'induction totale :

<u>Théorème 2</u>. <u>Si</u> H <u>est une partie de</u> $\mathfrak{I}(E)$ <u>telle que la relation</u> $[0,n[\subset H$ <u>entraîne</u> $n \in H$, <u>on a</u> $H = \mathfrak{I}(E)$.

En effet, soit H' la partie de $\mathfrak{I}(E)$ formée des n tels que $[0,n[\subset H$; on a évidemment $0 \in H'$; d'autre part, si $n \in H'$ et si $n+1$ est défini, on a $[0,n[\subset H$, donc $n \in H$ d'après l'hypothèse ; comme $[0,n+1[$ est réunion de $[0,n[$ et de $\{n\}$, on a $[0,n+1[\subset H$, autrement dit $n+1 \in H'$; cela entraîne $H' = \mathfrak{I}(E)$ (th.1), donc $[0,n[\subset H$ pour tout $n \in \mathfrak{I}(E)$, ce qui entraîne $n \in H$ pour tout $n \in \mathfrak{I}(E)$, c'est-à-dire $H = \mathfrak{I}(E)$.

Cette forme du principe d'induction totale s'applique le plus souvent comme suit : soit R une relation contenant comme argument libre un élément arbitraire n de $\partial(E)$; si, dans une théorie $\mathcal{C}$ la relation $(\forall m \in \partial(E))(m < n \rightarrow (m|n)R)$ <u>entraîne</u> R , la relation R est <u>vraie</u> dans la théorie $\mathcal{C}$, car si H est l'ensemble des $n \in \partial(E)$ où R a lieu, H satisfait aux conditions du th.2 .

Nous dirons qu'une partie H de $\partial(E)$ a un <u>plus petit élément</u> (resp. un <u>plus grand élément</u>) s'il existe $a \in H$ tel que $a \leqslant x$ pour tout $x \in H$ (resp. s'il existe $b \in H$ tel que $x \leqslant b$ pour tout $x \in H$ (cf.chap.IV) ; si H a un plus petit élément (resp. un plus grand élément) il résulte aussitôt de la définition que cet élément est <u>unique</u>. Avec ces définitions :

<u>Théorème 3. Toute partie finie non vide H de $\partial(E)$ a un plus petit et un plus grand élément ; toute partie non vide K de $\partial(E)$ a un plus petit élément</u>.

Démontrons la première partie par récurrence sur la puissance p de H (dans $\partial(\partial(E))$). Si $p=1$, on a $H=\{a\}$, donc $a \leqslant n \leqslant a$ pour tout $n \in H$. Supposons $p+1$ défini, et soit H une partie de $\partial(E)$ à $p+1$ éléments, et c un élément quelconque de H ; alors $H'=H \cap \complement\{c\}$ est une partie de $\partial(E)$ à p éléments ; l'hypothèse de récurrence entraîne qu'il existe $a' \in H'$ et $b' \in H'$ tels que $a' \leqslant n \leqslant b'$ pour tout $n \in H'$. Si $c \leqslant a'$ on a donc $c \leqslant n$ pour tout $n \in H$; au contraire si $a' \leqslant c$, on a $a' \leqslant n$ pour tout $n \in H$; on montre de même qu'il existe $b \in H$ tel que $n \leqslant b$ pour tout $n \in H$; d'où la première partie du théorème.

Si maintenant K est une partie non vide quelconque de $\partial(E)$, et a un élément de K , l'ensemble $H=K \cap [0,a]$ est contenu dans $[0,a]$, donc fini ; il existe par suite $c \in H$ tel que $c \leqslant n$ pour tout $n \in H$; en particulier $a \geqslant c$; d'autre part, si $n \in K \cap \complement H$, on a $n > a$, donc $n > c$, ce qui montre que $c \leqslant n$ pour tout $n \in K$.

4. Réunion et produit de familles finies. On dit qu'une famille $(x_\iota)_{\iota \in I}$ d'éléments d'un ensemble E est finie si l'ensemble d'indices I est fini; il en résulte (prop.3) que l'ensemble des éléments de la famille est fini.

La réciproque de cette proposition est naturellement inexacte, comme le montre l'exemple où I est infini et l'application $\iota \to x_\iota$ une application constante.

Nous allons montrer que l'axiome de Zermelo (E_{VIII}) (chap.II, § 5, n°6) est une conséquence des autres axiomes de la théorie des ensembles, lorsqu'on suppose dans son énoncé que I est un ensemble fini :

Proposition 11. Si $(X_\iota)_{\iota \in I}$ est une famille finie de parties non vides d'un ensemble E, l'ensemble $\prod_{\iota \in I} X_\iota$ n'est pas vide.

Nous allons encore montrer que $\prod_{\iota \in J} X_\iota \neq \emptyset$ pour toute partie J de I, en raisonnant par récurrence sur le nombre d'éléments n de J. La proposition est vraie si $J = \emptyset$ (chap.II, § 5, n°4) ; supposons n+1 défini et soit H une partie de I à n+1 éléments, $\varkappa$ un élément de H, et $J = H \cap \complement \{\varkappa\}$; J est un ensemble à n éléments, et $\prod_{\iota \in H} X_\iota$ est équipotent à $(\prod_{\iota \in J} X_\iota) \times X_\varkappa$ (chap.II, § 5, prop.14) ; l'hypothèse de récurrence entraîne que $\prod_{\iota \in J} X_\iota$ n'est pas vide ; comme $X_\varkappa \neq \emptyset$, $\prod_{\iota \in H} X_\iota$ n'est pas vide d'après la prop.3 du chap.II, § 3.

Proposition 12. Soit $(X_\iota)_{\iota \in I}$ une famille finie de parties finies d'un ensemble E ; la réunion et le produit de cette famille sont des ensembles finis.

Nous allons montrer que pour toute partie J de I , l'ensemble $\bigcup_{\iota \in J} X_\iota$ est fini, en raisonnant par récurrence sur le nombre déléments n de J (dans $\mathfrak{I}(I)$). La proposition est évidente si n=0, puisque $\bigcup_{\iota \in \emptyset} X_\iota = \emptyset$; supposons n+1 défini et soit H une partie de I à n+1 éléments ; soit $\varkappa$ un élément de H , et soit $J = H \cap \complement\{\varkappa\}$; J est un ensemble à n éléments, et on a $\bigcup_{\iota \in H} X_\iota = (\bigcup_{\iota \in J} X_\iota) \cup X_\varkappa$; l'hypothèse de récurrence entraîne que $\bigcup_{\iota \in J} X_\iota$ est fini ; comme $X_\varkappa$ est fini, il en est de même de $\bigcup_{\iota \in H} X_\iota$ d'après la prop.4 ; la proposition est donc démontrée en ce qui concerne la réunion. On peut raisonner de même pour le produit ; on peut aussi remarquer que si $F = \bigcup_{\iota \in I} X_\iota$, le produit $\prod_{\iota \in I} X_\iota$ est contenu dans F^I ; comme F et I sont finis, il en est de même de F^I (cor. de la prop.6), donc $\prod_{\iota \in I} X_\iota$ est fini (prop.2).

<u>Corollaire</u>. <u>Soit</u> $(n_\iota)_{\iota \in I}$ <u>une famille finie d'éléments de</u> $\mathfrak{I}(E)$; <u>si</u> $\sum_{\iota \in I} n_\iota$ <u>et</u> $\prod_{\iota \in I} n_\iota$ <u>sont définis, ils appartiennent à</u> $\mathfrak{I}(E)$.

<u>5. Les définitions par récurrence</u>. Aux deux formes du principe d'induction totale correspondent deux méthodes de définition de fonctions dans un ensemble $\mathfrak{I}(E)$.

<u>Théorème 4</u>. <u>Soient</u> E <u>et</u> F <u>deux ensembles, a un élément de</u> F , φ <u>une application de</u> F <u>dans</u> F . <u>Alors il existe une application</u> f <u>de</u> $\mathfrak{I}(E)$ <u>dans</u> F <u>et une seule qui satisfasse aux conditions suivantes</u> : 1^o $f(0)=a$; 2^o <u>pour tout</u> $n \in \mathfrak{I}(E)$ <u>tel que</u> n+1 <u>soit défini</u>, $f(n+1)=\varphi(f(n))$.

En effet, soit H l'ensemble des $p \in \mathfrak{I}(E)$ ayant la propriété suivante: il existe une application f_p et une seule de $[0,p]$ dans F telle que $f_p(0)=a$ et $f_p(m+1)=\varphi(f_p(m))$ pour tout m tel que $0 \leqslant m < p$.

Montrons par récurrence sur p que $H = \vartheta(E)$; il est clair que $0 \in H$; d'autre part, supposons que $p \in H$ et que $p+1$ soit défini ; l'ensemble $[0,p+1]$ est réunion des ensembles $[0,p]$ et $\{p+1\}$ sans élément commun ; en définissant une fonction f_{p+1} par les conditions $f_{p+1}(m)=f_p(m)$ pour $0 \leqslant m \leqslant p$ et $f_{p+1}(p+1)=\varphi(f_p(p)$, l'hypothèse de récurrence montre que f_{p+1} est telle que $f_{p+1}(0)=a$ et $f_{p+1}(m+1)=\varphi(f_{p+1}(m))$ pour $0 \leqslant m < p+1$; d'autre part, si f'_{p+1} est une autre fonction satisfaisant aux mêmes conditions, on a $f'_{p+1}(m)=f_p(m)$ pour $0 \leqslant m \leqslant p$ d'après l'hypothèse de récurrence, et $f'_{p+1}(p+1)=\varphi(f'_{p+1}(p)) = \varphi(f_p(p))=f_{p+1}(p+1)$, d'où $f'_{p+1}=f_{p+1}$, et par suite $p+1 \in H$. On a donc $H = \vartheta(E)$ d'après le th.1 . Pour tout $n \in \vartheta(E)$, posons alors $f(n)=f_n(n)$; on a bien $f(0)=f_0(0)=a$; d'autre part, si $n+1$ est défini, $f_{n+1}(n)=f_n(n)$, donc $f(n+1)=f_{n+1}(n+1)=\varphi(f_{n+1}(n))=\varphi(f_n(n))=\varphi(f(n))$, la fonction f satisfait bien aux deux conditions de l'énoncé. D'autre part, si une fonction f' satisfait à ces conditions, sa restriction à $[0,n]$ pour tout $n \in \vartheta(E)$ est identique à f_n , donc $f'(n)=f_n(n)=f(n)$ pour tout n .

C.Q.F.D.

Remarque. Soit ψ une application de $\vartheta(E) \times F$ dans F ; on déduit du th.4 qu'il existe une application f et une seule de $\vartheta(E)$ dans F telle que $f(0)=a$, et pour tout n tel que $n+1$ soit défini, $f(n+1)=\psi(n,f(n))$. En effet soit φ l'application de $\vartheta(E) \times F = G$ dans lui-même telle que $\varphi(n,x)=(n+1,\psi(n,x))$ si $n+1$ est défini, $\varphi(n,x)=(n,\psi(n,x))$ dans le cas contraire. D'après le th.3, il existe une application g et une seule de $\vartheta(E)$ dans G telle que $g(0)=(0,a)$ et $g(n+1)=\varphi(g(n))$ lorsque $n+1$ est défini ; on peut écrire $g=(h,f)$, où h est une application de $\vartheta(E)$ dans lui-même et f une application de $\vartheta(E)$ dans F ; on a donc $f(0)=a$ et et $f(n+1)=\psi(n,f(n))$ lorsque $n+1$ est défini, d'où la proposition.

Théorème 5. Pour tout $n \in \vartheta(E)$, soit G_n l'ensemble des applications de $[0,n]$ dans un ensemble F ; soit G la réunion des G_n, pour $n \in \vartheta(E)$. Soit a un élément de F, φ une application de G dans F. Alors il existe une application f et une seule de $\vartheta(E)$ dans F telle telle que : 1° $f(0)=a$; 2° si $f^{(n)}$ désigne la restriction de f à $[0,n]$, pour tout $n \in \vartheta(E)$ tel que $n+1$ soit défini, on a $f(n+1)=\varphi(f^{(n)})$.

Nous laissons au lecteur la démonstration, qui suit exactement la même marche que celle du th.4 .

6. Applications : Itérées d'une fonction. Récurrence limitée. Soient E et F deux ensembles, u une application arbitraire de F dans lui-même (élément arbitraire de F^F). Considérons l'application $v \to u\circ v$ de F^F dans lui-même ; le th.4 prouve qu'il existe une application et une seule f de $\vartheta(E)$ dans F^F telle que $f(0)$ soit l'application identique de F sur lui-même et $f(n+1)=u\circ f(n)$ pour tout $n \in \vartheta(E)$ tel que $n+1$ soit défini ; nous écrirons $\overset{n}{u}$ pour la valeur $f(n)$, et nous dirons que $\overset{n}{u}$ est la n-ème itérée de l'application u ; en particulier, $\overset{1}{u} = u$. On a donc d'après cette définition $\overset{n+1}{u}(x)=u(\overset{n}{u}(x))$ pour tout $x \in F$.

Il en résulte que la fonction f définie dans l'énoncé du th.4 peut s'écrire $n \to \overset{n}{\varphi}(a)$.

Nous allons maintenant étendre le th.4 au cas où la fonction φ est une application d'une partie G de F dans F. Considérons pour cela l'extension réciproque $\psi = \overset{-1}{\varphi}$ de φ ; c'est une application de $\mathfrak{P}(F)$ dans $\mathfrak{P}(G)$, donc dans $\mathfrak{P}(F)$; on peut par suite définir pour tout $n \in \vartheta(E)$, la n-ème itérée $\overset{n}{\psi}$ que nous noterons aussi $\overset{-n}{\varphi}$. On a $\overset{-0}{\varphi}(F)=F$, $\overset{-1}{\varphi}(F)=G$ par définition ; posons $R=F \cap \complement G$; on voit

36

aussitôt par récurrence sur n que, pour tout n tel que n+1 soit défini, $\overset{-(n+1)}{\varphi}(F) \subset \overset{-n}{\varphi}(F)$ et

(1) $$\overset{-n}{\varphi}(R) = \overset{-n}{\varphi}(F) \cap \complement \overset{-(n+1)}{\varphi}(F)$$

d'où on déduit aussitôt, par récurrence sur p, que si $p>0$ et si $n+p$ est défini, on a $\overset{-(n+p)}{\varphi}(R) \subset \overset{-(n+1)}{\varphi}(F)$, donc $\overset{-(n+p)}{\varphi}(R) \cap \overset{-n}{\varphi}(R) = \emptyset$; autrement dit, les ensembles $\overset{-n}{\varphi}(R)$, où n parcourt $\mathcal{V}(E)$, sont deux à deux sans élément commun. Cela étant :

<u>Proposition 13</u>. <u>Soit</u> a <u>un élément de</u> F . <u>Si</u> a <u>n'appartient à aucun des ensembles</u> $\overset{-n}{\varphi}(R)$, <u>il existe une application</u> f <u>et une seule de</u> $\mathcal{V}(E)$ <u>dans</u> F <u>telle que</u> $f(0)=a$ <u>et, pour tout</u> $n \in \mathcal{V}(E)$ <u>tel que</u> n+1 <u>soit défini,</u> $f(n) \in G$ <u>et</u> $f(n+1)=\varphi(f(n))$. <u>Si au contraire, il existe</u> $p \in \mathcal{V}(E)$ (nécessairement unique et $\geqslant 1$) <u>tel que</u> $a \in \overset{-p}{\varphi}(R)$, <u>il existe une application et une seule</u> g <u>de</u> $[0,p]$ <u>dans</u> F <u>telle que</u> $g(0)=a$, $g(n) \in G$ <u>et</u> $g(n+1)=\varphi(g(n))$ <u>pour tout</u> n <u>tel que</u> $0 \leqslant n \leqslant p$; <u>en outre, on a</u> $g(p) \in R$.

En effet, dans le premier cas, désignons par H l'ensemble des $q \in \mathcal{V}(E)$ tels qu'il existe une application f_q et une seule de $[0,q]$ dans F telle que $f_q(0)=a$, $f_q(m) \notin \overset{-(n-m)}{\varphi}(R)$ pour tout $n \in \mathcal{V}(E)$ tel que $n \geqslant m$, et tout m tel que $0 \leqslant m \leqslant q$, et enfin $f_q(m+1)=\varphi(f_q(m))$ pour tout m tel que $0 \leqslant m < q$. On voit aussitôt que $0 \in H$; si $q \in H$ et si q+1 est défini, on a $f_q(q) \notin \overset{-(n-q)}{\varphi}(R)$ pour tout n tel que $n \geqslant q$; en particulier, $f_q(q) \notin \overset{-0}{\varphi}(R) = R$, donc $\varphi(f_q(q))$ est défini ; on définit f_{q+1} en posant $f_{q+1}(m)=f_q(m)$ pour $0 \leqslant m \leqslant q$ et $f_{q+1}(q+1)=\varphi(f_q(q))$; pour tout $n \geqslant q+1$, on a $f_{q+1}(q+1) \notin \overset{-(n-(q+1))}{\varphi}(R)$, car cette relation équivaut à $f_q(q) \notin \overset{-1}{\varphi}(\overset{-(n-(q+1))}{\varphi}(R)) = \overset{-(n-q)}{\varphi}(R)$, qui est vraie par l'hypothèse de récurrence. On achève alors le raisonnement comme dans le th.4 .

Dans le second cas, il suffit d'appliquer la première partie de la proposition, en remplaçant $\mathfrak{P}(E)$ par $[0,p[$, ce qui établit l'existence de la fonction f dans $[0,p[$; on la prolonge à $[0,p]$ en posant $f(p)=\varphi(f(p-1))$; en outre, on démontre aussitôt par récurrence sur m que l'on a $f(m) \in \overset{-(p-m)}{\varphi}(R)$ pour $0 \leqslant m \leqslant p$, d'où en particulier $f(p) \in R$.

Exercices.- 1) Si $(\mathfrak{a}_\iota)_{\iota \in I}$ est une famille d'éléments $\neq 0$ de $\overline{\omega}(E)$, dont la somme est définie, montrer que $p(I)$ est inférieure à $\sum_{\iota \in I} \mathfrak{a}_\iota$.

2) Si $(\mathfrak{a}_\iota)_{\iota \in I}$ est une famille d'éléments de $\overline{\omega}(E)$ tels que $\mathfrak{a}_\iota > 1$ pour tout $\iota \in I$, montrer que

$$\sum_{\iota \in I} \mathfrak{a}_\iota \leqslant \prod_{\iota \in I} \mathfrak{a}_\iota$$

lorsque le second membre est défini.

§ 3. Entiers naturels. Ensembles dénombrables.

1. Puissances des parties finies d'un ensemble infini. Proposition 1. Soient E,F deux ensembles ; pour toute partie finie X de E, et toute partie infinie Y de F, il existe une application biunivoque de X dans Y.

En effet, soit $\mathfrak{G}$ l'ensemble des parties finies X de E telles qu'il existe une application biunivoque de X dans Y ; on a $\mathfrak{G} \subset \mathfrak{F}(E)$ et évidemment $\emptyset \in \mathfrak{G}$. Soit $X \in \mathfrak{G}$ et $y \in E$; si $y \in X$, on a $X \cup \{y\} = X \in \mathfrak{G}$; supposons donc $y \notin X$. Il existe par hypothèse une application biunivoque f de X dans Y ; $f(X)$ est fini, donc distinct de Y, autrement dit il existe $z \in Y$ tel que $z \notin f(X)$; alors l'application g de $X \cup \{y\}$ dans Y, égale à f dans X et telle que $g(y)=z$ est biunivoque. On a par suite $\mathfrak{G} = \mathfrak{F}(E)$ (§ 2,prop.1) d'où la proposition.

Corollaire 1. Soit E *un ensemble infini ; pour toute famille finie* $(n_\iota)_{\iota\in I}$ *d'éléments de* $\vartheta(E)$, $\sum_{\iota\in I} n_\iota$ *et* $\prod_{\iota\in I} n_\iota$ *sont définis.*

Il suffit de montrer que, pour deux éléments quelconques m,n de $\vartheta(E)$, $m+n$ et mn sont définis ; on raisonne ensuite par récurrence sur le nombre d'éléments de I (cf.prop.12). Or, si M est une partie de E de puissance m ; $\complement M$ est infini, sans quoi $E=M \cup \complement M$ serait fini ; il existe donc dans $\complement M$ une partie N de puissance n, ce qui montre que $m+n$ est défini ; d'autre part, comme $M \times N$ est fini, il existe une partie de E équipotente à $M\times N$, donc mn est défini.

Corollaire 2. Si E est infini, $\vartheta(E)$ *est infini*.

En effet, si $\vartheta(E)$ était fini, il existerait un élément $c \in \vartheta(E)$ tel que $n \leqslant c$ pour tout $n \in \vartheta(E)$ (§2,th.3) ; mais $c+1$ est défini (cor.1) et la relation $c+1 \leqslant c$ est absurde.

Corollaire 3. Si E *et* F *sont infinis, l'application canonique de* $\overline{\omega}(E)$ *à* $\overline{\omega}(F)$ *est définie dans une partie de* $\overline{\omega}(E)$ *contenant* $\vartheta(E)$, *et applique* $\vartheta(E)$ *sur* $\vartheta(F)$.

En effet, si $n \in \vartheta(E)$, il existe une partie de F équipotente à une partie de E de puissance n, donc il existe un élément de $\vartheta(F)$ équivalent à n.

2. *Entiers naturels*. Sauf mention expresse du contraire, dans *toutes* les théories que nous étudierons dans cet ouvrage, parmi les arguments de base de la théorie figurera l'argument I (généralement comme ensemble auxiliaire), et parmi les axiomes figurera l'axiome " I est un ensemble infini" . Nous poserons $\mathcal{N} = \vartheta(I)$; les éléments de $\mathcal{N}$ seront appelés *entiers naturels*.

Si E est un ensemble infini quelconque, nous venons de voir que l'application canonique de $\overline{\omega}(E)$ à $\overline{\omega}(I)$ est définie dans $\vartheta(E)$ et applique $\vartheta(E)$ *sur* $\mathcal{N} = \vartheta(I)$. D'autre part, si E est fini, la prop.1 montre que la puissance de E est strictement inférieure à celle de I , donc l'application canonique de $\varpi(E)$ à $\varpi(I)$ est définie dans $\mathfrak{I}(E)=\varpi(E)$, et applique $\mathfrak{I}(E)$ sur la partie $[0,n]$ de N , si la puissance de E est équivalente à n . Nous <u>identifierons</u> désormais, pour tout ensemble E , l'ensemble $\mathfrak{I}(E)$ avec son image canonique dans N ; autrement dit, la puissance d'un ensemble fini E sera identifiée à l'entier naturel n auquel elle est équivalente ; on dira encore que n est le <u>nombre d'éléments</u> de E , et que E est un <u>ensemble à n éléments</u>.

Toutes les propriétés démontrées au § 2 pour un ensemble $\mathfrak{I}(E)$ quelconque s'appliquent en particulier à N , en se simplifiant du fait que N est <u>infini</u> (cor.2 de la prop.1) ; $\sum_{\iota\in I} n_\iota$ et $\prod_{\iota\in I} n_\iota$ sont en effet définis pour toute famille finie $(n_\iota)_{\iota\in I}$ d'entiers naturels (cor.1 de la prop.1) ; en particulier, pour deux entiers naturels quelconques m,n, m+n , mn et m^n sont définis. Les résultats du § 1,n°7, sont donc applicables aux entiers naturels sans autre restriction que d'imposer aux familles qui y figurent la condition d'être <u>finies</u>.

<u>3. Division euclidienne. Numération</u>. <u>Proposition 2</u>. <u>Quels que soient les entiers naturels</u> $m\geqslant 0$ <u>et</u> $n>0$, <u>il existe un entier naturel</u> q <u>et un seul tel que</u> $qn\leqslant m<(q+1)n$.

Il suffit de démontrer l'existence de q ; son unicité est immédiate, car si $qn\leqslant m<(q+1)n$, pour tout entier $q'\neq q$, on a $q'<q$, $q+1\leqslant q'$, donc $m<(q+1)n\leqslant q'n$. Pour établir l'existence de q , raisonnons par récurrence sur m ; la proposition est évidente pour $m=0$, avec $q=0$; d'autre part, si $qn\leqslant m<(q+1)n$, on a $qn\leqslant m+1\leqslant(q+1)n$; si $m+1<(q+1)n$, on a donc $qn\leqslant m<(q+1)n$;

si au contraire $m+1=(q+1)n$, on a $(q+1)n\leqslant m<(q+2)n = (q+1)n+n$, donc la proposition est démontrée.

L'unique entier naturel q est appelé le quotient euclidien ou quotient à une unité près par défaut de m par n ; il existe un entier naturel r et un seul tel que $m=qn+r$, et on a $r<n$ (§ 2,cor.2 de la prop.8) ; on dit que r est le reste de la division de m par n ; on peut encore dire que les entiers q et r sont caractérisés par les deux relations $m=qn+r$, $r<n$.

Le quotient à une unité près par défaut de m par n se note souvent $\left[\frac{m}{n}\right]$; en particulier, on a $\left[\frac{m}{1}\right] = m$.

Corollaire. *Si* $n>0$, *la relation* $pn\leqslant qn$ (resp. $pn<qn$) *est équivalente à* $p\leqslant q$ (resp. $p<q$).

En effet, on sait que $p\leqslant q$ entraîne $pn\leqslant qn$ (§ 1,n°7) ; d'autre part $pn=qn$ entraîne $p=q$ d'après la prop.2, donc $p<q$ entraîne $pn<qn$, ce qui établit le corollaire, compte tenu de la prop.9 du § 2 .

On dit qu'un entier m est multiple d'un entier n , ou que n est diviseur de m , s'il existe un entier p tel que $m=pn$; cet entier est alors égal au quotient euclidien de m par n et se note alors $\frac{m}{n}$, le reste de la division de m par n étant nul ; si m est multiple de n, hm est multiple de hn pour tout $h\neq 0$, et le quotient de hm par hn est égal au quotient de m par n .

Proposition 3. *Quels que soient les entiers* $m>0$ *et* $n>1$, *il existe un entier* $h\geqslant 0$ *et une application* $i\rightarrow a_i$ *de* $[0,h]$ *dans* $[0,n[$, *bien déterminés et tels que* $a_0>0$ *et*

$$(1)\qquad m = \sum_{i=0}^{h} a_i n^{h-i}$$

(ce qu'on écrit encore $m=a_0n^h+a_1n^{h-1}+\ldots+a_h$).

Démontrons d'abord qu'il existe un entier h et un seul tel que

(2) $$n^h \leqslant m < n^{h+1}$$

Ici encore, l'unicité de h est immédiate, car pour $k<h$, on a $k+1 \leqslant h$ et $n^{k+1} \leqslant n^h \leqslant m$, et pour $k>h$, $h+1 \leqslant k$ et $n^k \geqslant n^{h+1} > m$. Pour établir l'existence de h, raisonnons par récurrence sur m, la proposition étant évidente pour $m=1$, avec $h=0$. Si on a $n^h \leqslant m < n^{h+1}$, on a $n^h < m+1 \leqslant n^{h+1}$; si $m+1 < n^{h+1}$, on a $n^h \leqslant m+1 < n^{h+1}$; si au contraire $m+1 = n^{h+1}$, on a $n^{h+1} \leqslant m+1 < n^{h+2}$ puisque $n>1$ par hypothèse.

Nous appellerons plus tard l'entier h ainsi déterminé la <u>partie entière du logarithme de m dans la base n</u>, et le noterons $[\log_n m]$ (cf. <u>Top. gén.</u>, chap. V, § 4).

Soit alors a_0 le quotient euclidien de m par n^h ; d'après (2), on a $1 \leqslant a_0 < n$; on pose alors $r_0 = m - a_0 n^h$, et on définit ensuite par récurrence, pour $1 \leqslant i \leqslant h$, a_i comme le quotient euclidien et r_i comme le reste de la division de r_{i-1} par n^{h-i} ; comme on a donc $a_i n^{h-i} < n^{h-i+1}$, c'est-à-dire $a_i < n$ pour $0 \leqslant i \leqslant h$; en outre, on voit par récurrence sur i que $m = \sum_{k=0}^{i} a_k n^{h-k} + r_i$, donc en particulier on a la formule (1). Reste à démontrer l'unicité de h et des a_i ; pour cela, remarquons que si $i \to b_i$ est une application quelconque d'un ensemble $[0,p]$ dans $[0,n[$, on a $\sum_{i=0}^{p} b_i n^{p-i} < n^{p+1}$, comme on le démontre aussitôt par récurrence sur p ; donc les relations $m = \sum_{i=0}^{p} b_i n^{p-i}$, $b_0 \geqslant 1$ donnent les inégalités $n^p \leqslant b_0 n^p \leqslant m < n^{p+1}$, et par suite $p=h$; en outre, on a $b_0 n^h \leqslant m < (b_0+1)n^h$, donc b_0 est le quotient euclidien de m par n^h, $b_0 = a_0$; par récurrence, on démontre de même que b_i est le quotient euclidien de r_{i-1} par n^{h-i}, autrement dit que $b_i = a_i$ pour $0 \leqslant i \leqslant h$, ce qui achève la démonstration.

Le second membre de la formule (1) est appelé le <u>développement de m dans la base n</u> .

<u>Remarques</u>. On peut démontrer les propositions 2 et 3 dans un ensemble $\mathcal{N}(E)$ quelconque ; il faut seulement avoir soin d'énoncer la prop.2 sous la seconde forme que nous avons indiquée, c'est-à-dire : il existe deux éléments q,r bien déterminés de $\mathcal{N}(E)$ tels que $m=qn+r$ et $r<n$.

Voyons maintenant la liaison entre la notion d'entier naturel et celle d'ensemble énuméré, ou, ce qui revient au même, avec la notion de "nombre expérimental". Pour chaque ensemble énuméré (§ 2,n°1) on démontre aussitôt qu'il est <u>fini</u> par application répétée (autant de fois que l'ensemble a d'éléments).de la définition des ensembles finis. Il résulte en outre de l'opération expérimentale qui consiste à apparier les objets de deux collections, que deux ensembles énumérés qui ont "autant" d'éléments au sens expérimental ont <u>même puissance</u>.

Par exemple, pour montrer que les ensembles à trois éléments $E=\{a,b,c\}$, $F=\{\alpha,\beta,\gamma\}$ ont même puissance, on prouve que dans $E\times F$, l'ensemble $u=\{(a,\alpha),(b,\beta),(c,\gamma)\}$ est le graphe d'une application biunivoque de E sur F ; il est clair en effet que $u(E)=F$; d'autre part, si $x\neq a$, on a $x=b$ ou $x=c$, donc $u(x)\neq u(a)$, et on termine de même la vérification.

Inversement, si un ensemble F est équipotent à un ensemble énuméré E , on vérifie dans chaque cas que c'est un ensemble énuméré ayant "autant" d'éléments que F .

Par exemple, si F est équipotent à l'ensemble énuméré $E=\{a,b,c\}$ à trois éléments, il existe une application biunivoque u de E sur F. On a donc $u(a)\neq u(b)$, $u(b)\neq u(c)$, $u(c)\neq u(a)$, et

$F=u(E)=\{u(a),u(b),u(c)\}$, ce qui exprime par définition que F est un ensemble à trois éléments.

En particulier, les ensembles $\{1\}$, $\{1,1+1\}$, $\{1,1+1,1+1+1\}$, etc. sont respectivement des ensembles énumérés à un, deux, trois,... éléments ; on le voit en appliquant la prop.7 du § 2 et l'associativité de l'addition à chaque couple d'éléments distincts de l'un de ces ensembles. Par suite, la puissance d'un ensemble énuméré à un, deux, trois, ... éléménts est respectivement 1, 1+1, 1+1+1, etc..

A cause de ce résultat, on est amené à identifier le "nombre expérimental" des éléments d'un ensemble énuméré, et l'entier naturel qui en est la puissance ; mais il faut prendre garde de ne pas étendre cette identification à des ensembles finis <u>explicités</u>, mais <u>non énumérés</u>. C'est ainsi que l'entier $2^{2^{1000}}$ est un entier explicité, mais le considérer comme la puissance d'un ensemble énuméré reviendrait à ôter tout sens expérimental à cette dernière notion.

On simplifie la notation de certains entiers explicités de la manière suivante : on choisit un entier b identifiable à la puissance d'un ensemble énuméré, et on note chacun des entiers $< b$ par un signe distinctif (appelé <u>chiffre</u>) ; cela étant, la prop.3 montre qu'à tout entier explicité m correspond un entier explicité h et une famille explicitée $(a_i)_{0\leqslant i\leqslant h}$ d'entiers $<b$ tels que $m=\sum_{i=0}^{h} a_i b^{h-i}$; si l'entier h est identifiable à une puissance d'ensemble énuméré, et si on peut effectivement déterminer chacun des "chiffres" a_i, on dit que la combinaison de signes $a_0a_1\ldots a_h$ (dont chacun doit être explicitement écrit) est l'écriture de l'entier m dans la base b .

Le choix le plus simple de b est $b=1+1$; les seuls "chiffres" sont alors 0 et 1 . On sait qu'en pratique on prend pour b l'entier naturel puissance d'un ensemble à dix éléments, et qu'on note 2,3,4,5,6,7,8,9 les chiffres correspondant aux entiers $1+1, 1+1+1, \ldots, 1+1+1+1+1+1+1+1+1$ (écriture décimale) ; il va sans dire que nous utiliserons cette écriture dans la suite de ce Traité.

Il est immédiat que les entiers explicités ne peuvent tous être écrits dans une base donnée ; on peut même facilement donner des exemples d'entiers explicités qui ne peuvent être écrits dans aucune base : si $a=2^{2^{1000}}$, le nombre a^a est un entier de cette nature ; on remarquera pourtant que, dans le développement de cet entier dans la base 2 , on peut écrire explicitement chacun des chiffres a_i : on a en effet $a_0=1$ et $a_i=0$ pour $i>0$; ce qu'on ne peut écrire, c'est la succession des chiffres a_i .

4. Analyse combinatoire. Le calcul sur les entiers naturels permet de déterminer la puissance d'un certain nombre d'ensembles formés à partir d'ensembles finis de puissance donnée.

Définition 1. Etant donnée une partie quelconque X d'un ensemble E , on appelle fonction caractéristique de X et on note φ_X l'application de E dans l'ensemble $D=\{0,1\}$ telle que $\varphi_X(x)=1$ pour tout $x \in X$ et $\varphi_X(x)=0$ pour tout $x \in \complement X$.

L'application $X \to \varphi_X$ est évidemment une application biunivoque de $\mathfrak{P}(E)$ dans l'ensemble D^E des applications de E dans D ; mais inversement, toute application f de E dans D est de la forme φ_X , car on a $E= \overset{-1}{f}(D)= \overset{-1}{f}(0) \cup \overset{-1}{f}(1)$, et par suite si on pose $X= \overset{-1}{f}(1)$, on a $f = \varphi_X$. Donc :

Proposition 4. L'ensemble $\mathfrak{P}(E)$ est équipotent à l'ensemble D^E des applications de E dans l'ensemble $D=\{0,1\}$.

Si on identifie E à son image par l'application $x \to \{x\}$, on peut considèrer la puissance $\mathfrak{a}$ de E comme un élément de l'ensemble des puissances des parties de $\mathfrak{P}(E)$; comme la puissance de D est 2, on voit que la puissance de $\mathfrak{P}(E)$ est égale à $2^{\mathfrak{a}}$; avec ces conventions, le th.2 du §1 s'écrit

(3) $$\mathfrak{a} < 2^{\mathfrak{a}}$$

Corollaire. Pour tout ensemble fini E de n éléments, $\mathfrak{P}(E)$ est un ensemble de 2^n éléments.

Soient E et F deux ensembles finis, à m et n éléments respectivement ; par définition, l'ensemble E^F des applications de F dans E est un ensemble à m^n éléments ; nous allons déterminer la puissance de son sous-ensemble B(E,F) (ensemble des applications biunivoques de E dans F) ; on notera que l'ensemble I(E,F) des applications biunivoques de E sur F est vide sauf pour $m=n$; dans ce cas, il est identique à B(E,F) (§2, cor.2 de la prop.7).

On peut se borner au cas où $E = [0,m[$ et $F = [0,n[$ (§1, cor.2 de la prop.4).

Proposition 5. L'ensemble des applications biunivoques d'un ensemble à m éléments dans un ensemble à n éléments est vide si $m > n$; c'est un ensemble à $\prod_{0 \leqslant k < m} (n-k)$ éléments si $m \leqslant n$.

La première partie de la proposition est évidente ; pour démontrer la seconde, nous raisonnerons par récurrence sur m ($\leqslant n$) ; la proposition est triviale pour $m=0$ puisque l'application vide est la seule application de l'ensemble vide dans F.

Pour toute application biunivoque u de $E = [0,m[$ dans $F=[0,n[$, considérons la restriction u' de u à $E' = [0,m-1[$; c'est une application biunivoque de E' dans F ; nous désignerons par φ l'application $u \to u'$ de $B(E,F)$ dans $B(E',F)$. Montrons que φ est une application de $B(E,F)$ sur $B(E',F)$; en effet, si v est une application biunivoque de E' dans F , v(E') est une partie de F à m-1 éléments, donc distincte de F ; pour tout $x \in F \cap \complement(v(E'))$, il existe une application biunivoque u et une seule de E dans F telle que $u'=v$ et $u(m-1)=x$; donc φ applique $B(E,F)$ sur $B(E',F)$, et pour tout $v \in B(E',F)$, $\overset{-1}{\varphi}(v)$ est un ensemble à $n-(m-1)$ éléments. Comme $B(E,F)$ est la réunion des ensembles $\overset{-1}{\varphi}(v)$, deux à deux sans élément commun, lorsque v parcourt $B(E',F)$, la puissance de $B(E,F)$ est somme d'une famille de puissances toutes égales à $n-(m-1)$, l'ensemble d'indices étant $B(E',F)$; d'après l'hypothèse de récurrence, la puissance de $B(E,F)$ est donc $(n-(m-1)) . \prod_{0 \leqslant k < m-1} (n-k) = \prod_{0 \leqslant k < m} (n-k)$.

<u>Corollaire</u>. <u>L'ensemble des permutations d'un ensemble à n éléments est un ensemble à</u> $\prod_{0 \leqslant k < n} (n-k)$ <u>éléments</u>.

Le nombre $\prod_{0 \leqslant k < n} (n-k)$ se note le plus souvent $n!$ et s'appelle <u>factorielle</u> de n ; on l'écrit aussi $n(n-1)\ldots2.1$, ou $1.2\ldots(n-1)n$. On a en particulier $0! = 1$ et $1! = 1$.

<u>Proposition 6</u>. <u>Si</u> E <u>est un ensemble à n éléments, et p un entier</u> $\leqslant n$, <u>le nombre des parties de</u> E <u>à</u> p <u>éléments est égal à</u> $\frac{1}{p!} \prod_{0 \leqslant k < p} (n-k)$.

En effet, soit F un ensemble de p éléments ; toute application biunivoque de F dans E applique F sur une partie de E à p éléments et réciproquement, pour toute partie X de E à p éléments, il existe une application biunivoque de F sur X ; en outre, l'ensemble $I(F,X)$ des applications biunivoques de F sur X est isomorphe à $I(F,F)$, donc a $p!$ éléments ; comme $B(E,F)$ est réunion des ensembles $I(F,X)$, deux à deux sans élément commun, lorsque X parcourt l'ensemble des parties de p éléments de E, on voit que, si m est la puissance de ce dernier ensemble, la puissance de $B(E,F)$ est $p!m$, d'où la proposition.

Le nombre ~~mm~~ des parties de p éléments d'un ensemble à n éléments se note $\binom{n}{p}$ et s'appelle le <u>coefficient binomial d'indices</u> n,p (pour des raisons que nous verrons en Algèbre, cf. Alg., chap. I) ; la prop. 6 s'exprime encore par la formule

(4) $$\binom{n}{p} = \frac{n!}{p!(n-p)!}$$

Cette formule montre aussitôt que $\binom{n}{p}=\binom{n}{n-p}$ pour tout $p \leqslant n$ (ce qui résulte aussi directement du fait que l'application $X \to \complement X$ est une application biunivoque de l'ensemble des parties à p éléments de E sur celui des parties à $(n-p)$ éléments).

<u>Corollaire 1</u>. <u>On a</u>

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

En effet, si H_p est l'ensemble des parties à p éléments de E les ensembles H_p $(0 \leqslant p \leqslant n)$ forment une partition de $\mathfrak{P}(E)$.

<u>Corollaire 2</u>. <u>Soit</u> $C(p,n)$ <u>l'ensemble des applications</u> f <u>de</u> $[0,p[$ <u>dans</u> $[0,n[$ <u>telles que</u> $r<s$ <u>entraîne</u> $f(r)<f(s)$ ("fonctions strictement croissantes", cf. chap. IV) ; <u>l'ensemble</u> $C(p,n)$ <u>a</u> $\binom{n}{p}$ <u>éléments</u>.

En effet, toute application $f\in C(p,n)$ est biunivoque, donc $f([0,p[)$ est une partie de $[0,n[$ à p éléments ; inversement, montrons que pour toute partie X de $[0,n[$ à p éléments, il existe une application $f\in C(p,n)$ et une seule telle que $X=f([0,p[)$. En effet, s'il existe une telle fonction, $f(r)$ doit être tel que $x \geqslant f(r)$ pour tout $x\in X$ tel que, pour tout $s<r$, $x>f(s)$; inversement, cette condition définit par récurrence une application et une seule $f\in C(p,n)$ de de $[0,p[$ sur X ; en effet, $f(0)$ soit être tel que $x \geqslant f(0)$ pour tout $x \in X$, et il existe un élément et un seul de X ayant cette propriété (§ 2, th. 3). Si f est défini dans $[0,h[$ $(h \leqslant p)$ par la condition précédente et est telle que l'ensemble X_h des $x \in X$ tels que $x > f(s)$ pour $0 \leqslant s < h$ ait $p-h$ éléments, $f(h)$ doit être tel que $x \geqslant f(h)$ pour tout $x \in X_h$; il existe un élément et un seul de X_h ayant cette propriété, et l'ensemble X_{h+1} des éléments de X_h qui sont $> f(h)$ a $p-(h+1)$ éléments ; d'où la proposition.

Le nombre des parties de p éléments dans un ensemble E à n éléments peut encore être considéré comme le nombre des couples (X,Y) de parties de E sans élément commun, ayant respectivement p et $n-p$ éléments. La formule (4) qui donne ce nombre se généralise comme suit :

<u>Proposition 7</u>. <u>Soit E un ensemble à n éléments, et $(p_i)_{1 \leqslant i \leqslant k}$ une famille d'entiers tels que $\sum_{i=1}^{k} p_i = n$. Le nombre des familles $(X_i)_{1 \leqslant i \leqslant k}$ de parties de E , telles que $X_i \cap X_j = \emptyset$ pour $i \neq j$, et que X_i ait p_i éléments pour $1 \leqslant i \leqslant k$, est égal à $\dfrac{n!}{p_1!\,p_2!\ldots p_k!}$</u>

En effet, soit $\mathfrak{S}$ l'ensemble des familles $(X_i)_{1 \leqslant i \leqslant k}$ satisfaisant aux conditions de l'énoncé ; comme $\sum_{i=1}^{k} p_i = n$, il existe une famille $(A_i)_{1 \leqslant i \leqslant k}$ de parties de E appartenant à $\mathfrak{S}$. Pour toute permutation f de E , la famille (X_i) où $X_i = f(A_i)$ appartient à $\mathfrak{S}$; inversement, si (X_i) appartient à $\mathfrak{S}$, il existe une application biunivoque f_i de A_i sur X_i , donc une application f de E dans E dont la restriction à A_i coïncide avec f_i pour $1 \leqslant i \leqslant k$, et f est une permutation de E (§ 1, prop. 4). Soit $H((X_i))$ l'ensemble des permutations f de E telles que $f(A_i) = X_i$ pour $1 \leqslant i \leqslant k$; cet ensemble est équipotent à l'ensemble produit $\prod_{i=1}^{k} I(A_i, X_i)$, car à tout $f \in H((X_i))$ correspond la famille de ses restrictions f_i aux A_i , chaque f_i étant une application biunivoque de A_i sur X_i ; et inversement, pour toute famille

$(f_i) \in \prod_{i=1}^{k} I(A_i,X_i)$, il existe une permutation et une seule f de E dont la restriction à chaque A_i coïncide avec f_i . La puissance de $H((X_i))$ est donc $\prod_{i=1}^{k} p_i!$; comme I(E,E) est la réunion des ensembles $H((X_i))$, deux à deux sans élément commun, lorsque (X_i) parcourt $\mathfrak{G}$, on voit que si m est la puissance de $\mathfrak{G}$, on a $m.\prod_{i=1}^{k} p_i!=n!$, d'où la proposition.

<u>Proposition 8</u>. <u>Soient</u> n <u>et</u> p <u>deux entiers tels que</u> $n>0$; <u>l'ensemble des familles</u> $(m_i)_{0\leqslant i<p}$ <u>telles que</u> $\sum_{0\leqslant i<p} m_i=n$ <u>a</u> $\binom{n+p-1}{p}$ <u>éléments</u> .

Montrons tout d'abord que cet ensemble est équipotent à l'ensemble $C'(p,n)$ des applications f de $[0,p[$ dans $[0,n[$ telles que $r<s$ entraîne $f(r)\leqslant f(s)$ ("fonctions croissantes" ; cf.chap.IV). En effet, si f est une telle fonction, et si $X_i=\overset{-1}{f}(i)$ pour $0\leqslant i<p$ on a $[0,n[=\bigcup_{0\leqslant i<p} X_i$, et par suite, si m_i est la puissance de X_i , $\sum_{0\leqslant i<p} m_i=n$, puisque $X_i\cap X_j=\emptyset$ pour $i\neq j$; en outre, pour $i<j$, la relation "$r\in X_i$ et $s\in X_j$" entraîne $r<s$ puisque $f(r)=i$ et $f(s)=j$; on en déduit par récurrence sur i , que X_i n'est autre que l'intervalle $\left[\sum_{0\leqslant h<i} m_h , \sum_{0\leqslant h<i} m_h\right[$; en effet, si un élément r de cet intervalle n'appartenait pas à X_i , il ne pourrait appartenir aux X_j d'indice $<i$, d'après l'hypothèse de récurrence ; d'autre part, s'il appartenait à un X_j d'indice $>i$, tous les éléments $s\in X_i$ appartiendraient à l'intervalle $\left[\sum_{0\leqslant h<i} m_h, r\right[$, dont la puissance est $<m_i$, ce qui est absurde. Inversement, pour toute famille $(m_i)_{0\leqslant i<p}$ telle que $\sum_{0\leqslant i<p} m_i=n$, si on pose $f(r)=i$ dans l'intervalle $\left[\sum_{0\leqslant h<i} m_h , \sum_{0\leqslant h<i} m_h\right[$, il est clair que f appartient à $C'(p,n)$ et que $\overset{-1}{f}(i)$ est identique à $\left[\sum_{0\leqslant h<i} m_h , \sum_{0\leqslant h\leqslant i} m_h\right[$ pour $0\leqslant i<p$.

Cela étant, montrons maintenant que $C'(p,n)$ est équipotent à $C(p,n+p-1)$. En effet, pour toute application $f\in C'(p,n)$, soit $\bar{f}$ l'application $r\to r+f(r)$ de $[0,p[$ dans $\mathbb{N}$; comme $f(r)\leqslant n-1$

et $r<p$, on a $\bar{f}(r)<n+p-1$ pour tout $r\in[0,p[$; en outre, la relation $r<s$ entraîne $f(r)\leqslant f(s)$ et par suite $\bar{f}(r)<\bar{f}(s)$, $\bar{f}$ est une application appartenant à $C(p,n+p-1)$. Réciproquement, si g est une application appartenant à cet ensemble, il existe un f $C'(p,n)$ et un seul tel que $\bar{f}=g$; en effet, comme $g(r)<g(r+1)$ pour tout r , on a $g(r)+1\leqslant g(r+1)$, d'où par récurrence $g(r)\geqslant r$; d'autre part, comme $g(p-1)<n+p-1$ on voit par récurrence que $g(p-s)<n+p-s$; donc, si on pose $f(r)=g(r)-r$, f est une application de $[0,p[$ dans $[0,n[$. En outre, de $g(r)+1\leqslant g(r+1)$ on tire $f(r)\leqslant f(r+1)$, et par récurrence, $r<s$ entraîne $f(r)\leqslant f(s)$; comme on a évidemment $\bar{f}=g$, la proposition est démontrée.

5. Ensembles dénombrables. Définition 2. On dit qu'un ensemble est dénombrable s'il est équipotent à une partie de N (ou, ce qui revient au même, s'il a une puissance inférieure à celle de N).

Nous avons vu que tout ensemble fini est dénombrable, puisque si n est le nombre de ses éléments, il est équipotent à la partie $[0,n[$ de N . Toute partie, d'un ensemble dénombrable est dénombrable. L'ensemble infini N est dénombrable par définition ; en outre :

Théorème 1. Tout ensemble dénombrable infini est équipotent à N .

Il revient au même de dire que toute partie infinie X de N est équipotente à N .

Pour démontrer cet énoncé, remarquons d'abord que, pour tout $n\in N$, l'ensemble des $m\in X$ tels que $m>n$ n'est pas vide, sans quoi on aurait $m\leqslant n$ pour tout $m\in X$, et X , partie de l'ensemble fini $[0,n]$, serait un ensemble fini, contrairement à l'hypothèse. Nous pouvons alors définir par récurrence (§2,th.4) une application f de N dans X par la condition suivante : $f(0)$ est le plus petit élément de X ; $f(n+1)$ est le plus petit (§2, th.3) des éléments de X qui sont $> f(n)$.

La relation $m < n$ entraîne $f(m) < f(n)$; cela revient à dire que, pour tout n et tout $q \geqslant 1$, on a $f(n+q) > f(n)$; cette relation est vraie par définition pour $q=1$, et si elle est vraie pour q , elle l'est pour $q+1$, car $f(n+q+1) > f(n+q) > f(n)$. On en déduit aussitôt que f est une application <u>biunivoque</u> de $\mathcal{N}$ dans X , car la relation $m \neq n$ équivaut à $m < n$ ou $m > n$, donc entraîne $f(m) < f(n)$ ou $f(m) > f(n)$, et par suite $f(m) \neq f(n)$. Montrons enfin que f est une application de $\mathcal{N}$ <u>sur</u> X ; en effet, pour tout $p \in X$, l'ensemble des $m \in \mathcal{N}$ tels que $f(m) < p$ est <u>fini</u>, car f est une application biunivoque de cet ensemble sur une partie de $[0,p[$; soit n son plus grand élément ; on a donc $f(n) < p$ et $f(n+1) \geqslant p$; mais comme par définition $f(n+1)$ est le plus petit élément de X qui soit $> f(n)$ et que $p \in X$ on a $f(n+1) \leqslant p$, ce qui prouve que $f(n+1) = p$, et achève la démonstration.

<u>Théorème 2</u>. <u>Le produit de deux ensembles dénombrables est dénombrable</u>

D'après le th.1, il revient au même de prouver que <u>l'ensemble $\mathcal{N} \times \mathcal{N}$ est dénombrable</u> ; étant infini (§ 2, prop.3) il sera nécessairement équipotent à $\mathcal{N}$. Nous allons effectivement définir une application biunivoque f de $\mathcal{N} \times \mathcal{N}$ sur $\mathcal{N}$; nous poserons $f(m,n) = (m+1)^2 - n - 1$ si $m > n$, $f(m,n) = n^2 + m$ si $m \leqslant n$. Pour montrer que f est une application biunivoque de $\mathcal{N} \times \mathcal{N}$, sur $\mathcal{N}$ considérons pour chaque p $\mathcal{N}$ d'une part la partie A_p de $\mathcal{N} \times \mathcal{N}$, réunion des ensembles $\{p\} \times [0,p]$ et $[0,p] \times \{p\}$ (fig.1), d'autre part l'ensemble $B_p = [p^2, (p+1)^2[$; il est évident que $\mathcal{N} \times \mathcal{N}$ est réunion des ensembles A_p lorsque p parcourt $\mathcal{N}$, et que deux A_p d'indices distincts ne se rencontrent pas ; d'autre part, la relation $p < q$

entraîne $p^2 < q^2$, donc l'application $p \to p^2$ est biunivoque, l'ensemble K des p^2 est infini ; pour tout $r \in \mathbb{N}$, il existe donc un élément de K qui est $> r$, et par suite un plus petit élément p^2 tel que $r < p^2$; si $r=0$ on a $p=0$, $r \in B_0$; si $r > 0$, on a $p > 0$, donc par définition $(p-1)^2 \leqslant r < p^2$, $r \in B_{p-1}$; en outre si $p < q$, on a $p \leqslant q-1$, donc $r < p^2$ entraîne $r < (q-1)^2$, B_p et B_q n'ont aucun élément commun. Il nous suffira donc de prouver que la restriction de f à A_p est une application biunivoque de A_p sur B_p pour tout $p \in \mathbb{N}$. Or, la restriction de f à l'ensemble $[0,p[\times \{p\}$ est une application biunivoque de cet ensemble sur l'intervalle $[p^2,p^2+p[$; la restriction de f à l'ensemble $\{p\} \times [0,p]$ est une application biunivoque de cet ensemble sur l'intervalle $[p^2+p+1,(p+1)^2[$; comme B_p est réunion des deux ensembles sans élément commun, $[p^2,p^2+p[$ et $[p^2+p+1,(p+1)^2[$ le théorème est démontré.

Pour abréger, nous dirons qu'une famille $(x_\iota)_{\iota \in I}$ d'éléments d'un ensemble E est <u>dénombrable</u> si l'ensemble d'indices I est dénombrable ; il en résulte (§ 1, prop. 12) que l'ensemble des éléments de la famille est <u>dénombrable</u> (on peut d'ailleurs dans ce cas démontrer cette proposition sans utiliser l'axiome de choix ; cf. exerc. 5). Si $(X_\iota)_{\iota \in I}$ est une famille dénombrable de parties d'un ensemble E, nous dirons abréger que la réunion (resp. l'intersection, le produit) de cette famille est une <u>réunion dénombrable</u> (resp. intersection dénombrable, produit dénombrable) de parties de E (on dit de même réunion finie, intersection finie, produit fini lorsque I est <u>fini</u>). Avec ces conventions, on a les corollaires suivants du th. 2 :

<u>Corollaire 1. Tout produit fini d'ensembles dénombrables est dénombrable</u>

Il suffit de raisonner par récurrence sur le nombre d'éléments de la famille finie d'ensembles dénombrables considérée.

2 On notera qu'un produit dénombrable d'ensembles dénombrables n'est pas dénombrable en général ; en effet, la puissance de $\mathcal{N}^{\mathcal{N}}$ est supérieure à celle de $\mathfrak{P}(\mathcal{N})$ (égale à celle de $2^{\mathcal{N}}$), donc (§ 1, th.2) strictement supérieure à celle de $\mathcal{N}$.

Corollaire 2. Toute réunion dénombrable de parties dénombrables d'un ensemble E est une partie dénombrable de E .

En effet, soit $(X_\iota)_{\iota\in I}$ une famille dénombrable de parties de E ; par hypothèse, il existe une application biunivoque φ de I dans $\mathcal{N}$, et, en vertu de l'axiome de choix, il existe pour chaque $\iota \in I$ une application biunivoque u_ι de X_ι dans $\mathcal{N}$. Dans le produit $I \times E$, si nous considérons l'ensemble "somme" $S = \bigcup_{\iota\in I} \{\iota\} \times X_\iota$ des X_ι , l'application $(\iota, x) \to (\varphi(\iota), u_\iota(x))$ est une application biunivoque de S dans $\mathcal{N} \times \mathcal{N}$, donc S est dénombrable, et a fortiori (§1, prop.13) $\bigcup_{\iota\in I} X_\iota$ est dénombrable.

On peut démontrer sans utiliser l'axiome de choix que toute réunion finie d'ensembles dénombrables est dénombrable (exerc.6).

6. Suites. On appelle suite d'éléments d'un ensemble E une famille d'éléments de E dont l'ensemble d'indices est une partie de l'ensemble $\mathcal{N}$ des entiers naturels ; une suite ayant $I \subset \mathcal{N}$ comme ensemble d'indices se note donc $(x_n)_{n\in I}$, conformément aux notations générales ; quand il ne peut y avoir de confusion sur I , on écrit simplement (x_n) au lieu de $(x_n)_{n\in I}$; on utilise surtout cette notation abrégée lorsque $I = \mathcal{N}$, ou lorsque I est l'ensemble des entiers $\geqslant 1$; une suite dont l'ensemble des indices est un intervalle $[p,q]$ de $\mathcal{N}$ (resp. l'ensemble des $n \geqslant p$) se note encore $(x_n)_{p\leq n\leq q}$ (resp. $(x_n)_{n\geqslant p}$) . On dit que x_n est le terme général, ou terme d'indice n , de la suite $(x_n)_{n\in I}$.

Une suite est dite <u>finie</u> ou <u>infinie</u> suivant que l'ensemble des indices est une partie finie ou infinie de $\mathbb{N}$. L'ensemble des éléments d'une suite finie est fini (§ 2, prop. 3) ; l'ensemble des éléments d'une suite infinie est dénombrable (§ 1, prop. 12).

On dit que deux suites $(x_n)_{n\in I}$, $(y_n)_{n\in I}$ d'éléments d'un même ensemble E, ayant même ensemble d'indices I, <u>ne diffèrent que par l'ordre des termes</u> s'il existe une permutation σ de I telle que $y_n = x_{\sigma(n)}$ pour tout $n \in I$.

Considérons une famille $(x_\iota)_{\iota\in I}$ d'éléments de E dont l'ensemble d'indices est <u>dénombrable</u> ; si I est infini il existe donc une application biunivoque φ de $\mathbb{N}$ sur I ; si I est fini, il existe une application biunivoque φ d'un intervalle $[0,p[$ sur I ; si on pose $y_n = x_{\varphi(n)}$ pour $n \in \mathbb{N}$ (resp. $n \in [0,p[$), on dit que la suite (y_n) ainsi définie est obtenue en <u>rangeant dans un certain ordre</u> la famille $(x_\iota)_{\iota\in I}$ donnée. Si ψ est une seconde application biunivoque de $\mathbb{N}$ sur I (resp. de $[0,p[$ sur I) il est clair qu'on peut écrire $\psi = \varphi\circ\theta$, où θ est une permutation de $\mathbb{N}$ (resp. de $[0,p[$) ; donc les deux suites $(x_{\varphi(n)})$ et $(x_{\psi(n)})$ <u>ne diffèrent que par l'ordre des termes</u>.

Toute <u>sous-famille</u> $(x_n)_{n\in J}$ d'une suite $(x_n)_{n\in I}$ est encore une suite, dite <u>extraite</u> de la suite donnée $(x_n)_{n\in I}$; lorsque $I = \mathbb{N}$ et que J est infini, la démonstration du th. 1 prouve qu'il existe une application $k \to n_k$ de $\mathbb{N}$ sur J telle que $h < k$ entraîne $n_h < n_k$; la suite $(x_{n_k})_{k\in\mathbb{N}}$ est dite obtenue en rangeant les termes de la suite $(x_n)_{n\in J}$ <u>dans l'ordre des indices croissants</u> ; c'est le plus souvent de cette manière qu'on écrit une suite infinie extraite d'une suite infinie donnée. On procède de même pour les suites finies extraites d'une suite donnée.

On appelle <u>suite double</u> (ou suite <u>à deux indices</u>) une famille d'éléments d'un ensemble E dont l'ensemble d'indices I est une partie du produit $\mathbb{N}\times\mathbb{N}$; on la note donc $(x_{m,n})_{(m,n)\in I}$, ou simplement $(x_{m,n})$ et même (x_{mn}) si ces notations ne prêtent pas à confusion.
On définit de même des suites <u>multiples</u> à un nombre quelconque d'indices : une suite à p indices sera une famille dont l'ensemble d'indices est une partie de $\mathbb{N}^p$. D'après le th.2, de toute suite multiple on peut toujours déduire une suite ("simple") en rangeant ses termes dans un certain ordre.

<u>Exercices</u>.- 1) Pour $n\geqslant 1$ et $p\geqslant 1$, démontrer la relation

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

(considérer toutes les parties de p éléments de $[0,n[$ qui contiennent n-1) .

2) Démontrer la relation

$$1+2+\ldots+(n-1)=\binom{n}{2}$$

(considèrer, pour chaque élément p de $[0,n[$, l'ensemble des parties de deux éléments de $[0,n[$ dont le plus grand élément est p) .

Démontrer de même la formule générale

$$\sum_{k=q+1}^{n-p+q+1}\binom{n-k}{p-q-1}\binom{k-1}{q}=\binom{n}{p}$$

où $p\leqslant n$ et $q<p$.

3) a) Démontrer la relation

$$\binom{n}{0}-\binom{n}{1}+\binom{n}{2}-\ldots+(-1)^n\binom{n}{n}=0$$

(procèder par récurrence sur n , en utilisant l'exerc.1).

b) Déduire de a) l'identité

$$\binom{n}{0}\binom{n}{p}-\binom{n}{1}\binom{n-1}{p-1}+\binom{n}{2}\binom{n-2}{p-2}-\ldots+(-1)^p\binom{n}{p}\binom{n-p}{0}=0$$

4) a) Soit $S_{n,p}$ l'ensemble des applications de $[0,n[$ <u>sur</u> $[0,p[$ pour $p \leqslant n$; démontrer la formule

$$S_{n,p}=p^n-\binom{p}{1}(p-1)^n+\binom{p}{2}(p-2)^n-\dots+(-1)^{p-1}\binom{p}{p-1}$$

(exprimer $S_{n,p}$ à l'aide des $S_{n,k}$ où $k<p$, et utiliser l'exerc. 3b)).

b) Démontrer la formule

$$S_{n,p}=p(S_{n-1,p}+S_{n-1,p-1})$$

(même méthode que dans la prop.5).

c) Démontrer les formules

$$S_{n+1,n}=\frac{n}{2}(n+1)!$$

$$S_{n+2,n}=\frac{n(3n+1)}{24}(n+2)!$$

(considérer les éléments r de $[0,p[$ dont l'image réciproque a plus d'un élément).

d) Si $P_{n,p}$ est le nombre des partitions d'un ensemble de n éléments en p parties, montrer que $S_{n,p}=p!P_{n,p}$.

5) Démontrer, sans utiliser l'axiome de choix, que l'ensemble des éléments d'une suite est dénombrable.

6) Démontrer, sans utiliser l'axiome de choix, que toute réunion finie d'ensembles dénombrables est dénombrable.
