RÉDACTION N° 141

COTE : NBR 044

TITRE : LIVRE II ALGÈBRE
CHAPITRE VI (ÉTAT 4)
GROUPES ET CORPS ORDONNÉS

ASSOCIATION DES COLLABORATEURS DE NICOLAS BOURBAKI

NOMBRE DE PAGES : 34

NOMBRE DE FEUILLES : 34

Archives
mai 1950

N32644

141

LIVRE II

ALGÈBRE

CHAPITRE VI (Etat 4).

GROUPES ET CORPS ORDONNÉS

§1 - Groupes ordonnés ; Divisibilité.

Les notions et résultats exposés dans ce paragraphe concernent l'étude de relations d'ordre dans des monoïdes commutatifs, le cas le plus important étant celui des groupes abéliens. La loi de composition dans les groupes et monoïdes étudiés sera notée additivement, comme ce sera le cas dans les applications à la théorie de l'Intégration (cf. Livre VII). D'autre part nous exposerons, au passage, des applications algébriques de la théorie des monoïdes et groupes ordonnés ; et nous traduirons au fur et à mesure une partie des résultats obtenus dans la notation multiplicative qui est propre à ces applications.

1 - Définition des monoïdes et groupes ordonnés.

DÉFINITION 1 - Sur un ensemble M, on dit qu'une structure de monoïde commutatif (notée additivement) et une structure d'ordre (notée $\leqslant$) sont compatibles si elles satisfont à l'axiome suivant :

(MO) Quel que soit $z \in M$, la relation $x \leqslant y$ entraîne $x+z \leqslant y+z$.

Un ensemble M muni d'une structure de monoïde commutatif et d'une structure d'ordre compatibles est appelé un monoïde ordonné ; si sa structure de monoïde commutatif est une structure de groupe abélien, il est appelé groupe ordonné.

Si une structure d'ordre est compatible avec la structure d'un monoïde, il en est de même de la structure d'ordre opposée.

<u>Exemples</u> - 1) Le groupe additif des entiers rationnels, et celui des nombres rationnels sont des groupes ordonnés quand on les munit des structures d'ordres naturelles définies au chap.I, § 2,n°5 et § 9,n°5. *Il en est de même du groupe additif des nombres réels (Top.Géné, chap.III, §1,n°3)* .

2)* Le groupe additif des <u>fonctions</u> définies sur un ensemble E et à valeurs réelles est un groupe ordonné pour la structure d'ordre définie par la relation "Quel que soit $x \in E$, $f(x) \leqslant g(x)$" que l'on écrit "$f \leqslant g$". Cette relation exprime que le graphe de la fonction f est "au dessous" de celui de la fonction g ; le lecteur pourra trouver commode de se reporter quelquefois à cette interprétation graphique .*

<u>Remarque</u> - Nous verrons dans un chapitre ultérieur comment certaines structures de groupes ordonnés utilisées en Algèbre sont susceptibles d'une telle interprétation fonctionnelle.

<u>Proposition 1</u> - (Principe d'addition des inégalités) - <u>Dans un monoïde ordonné</u> M , <u>soient</u> (x_i) <u>et</u> (y_i) $(1 \leqslant i \leqslant n)$ <u>deux suites de</u> n <u>éléments, telles que, quel que soit</u> i , <u>on ait</u> $x_i \leqslant y_i$; <u>alors on a</u> $x_1+..+x_n \leqslant y_1+..+y_n$. <u>Si de plus tous les éléments</u> x_i, y_i <u>sont réguliers</u> (et, en particulier, si M est un <u>groupe</u>), <u>et s'il existe</u> i <u>tel que</u> $x_i < y_i$, <u>on a alors</u> $x_1+..+x_n < y_1+..+y_n$.

Le cas de n quelconque se ramène par récurrence au cas $n=2$, en utilisant, pour la deuxième partie, le fait qu'un produit d'éléments réguliers est régulier (Chap.I, § 2,n°2,prop.2). La première assertion résulte des relations $x_1+x_2 \leqslant y_1+y_2$ et $x_1+y_2 \leqslant y_1+y_2$, conséquences des hypothèses et de (MO). Cela étant, $x_1+x_2 = y_1+y_2$ impliquerait $x_1+x_2 = x_1+y_2 = y_1+y_2$, d'où $x_2=y_2$ et $x_1=y_1$ si x_1 et y_2 sont réguliers, ce qui démontre la seconde assertion.

<u>Proposition 2</u> - <u>Dans un groupe ordonné</u> G <u>les relations</u> $x \leqslant y$ <u>et</u> $x+z \leqslant y+z$ <u>sont équivalentes</u>.

On passe en effet de chacune de ces relations à l'autre par addition membre à membre de z , ou de $(-z)$.

On exprime ce résultat en disant que, dans un groupe ordonné G , la structure d'ordre est <u>invariante par translation</u>. En d'autres termes une translation est un <u>automorphisme</u> pour la structure <u>d'ordre</u> d'un groupe ordonné.

<u>Corollaire 1</u>.- <u>Dans un groupe ordonné</u> G , <u>les relations</u> $x \leqslant y$, $0 \leqslant y-x$, $x-y \leqslant 0$ et $(-y) \leqslant (-x)$ <u>sont équivalentes</u>.

On applique la prop.2 en prenant successivement $z=-x$, $z=-y$ et $z=-(x+y)$.

On déduit de la troisième équivalence que, si G est un groupe ordonné, l'application $x \to (-x)$ de G sur lui-même transforme sa structure d'ordre en la structure opposée.

Conformément aux définitions générales (Ens.R., § 8) une application biunivoque d'un monoïde ordonné (resp. groupe ordonné) M sur un monoïde ordonné (resp. groupe ordonné) M' est appelée un <u>isomorphisme</u> de M sur M' si la structure de M' est obtenue en transportant celle de M au moyen des extensions canoniques de f . Ceci veut dire que l'on a $f(x+y)=f(x)+f(y)$ c'est-à-dire que f est une représentation pour les structures algébriques), et que les relations "$x \leqslant y$" et "$f(x) \leqslant f(y)$" sont équivalentes.

2 - <u>Monoïdes et groupes préordonnés</u>.

Rappelons que si une relation $R(x,y)$ entre éléments génériques d'un ensemble E est réflexive et transitive, la relation "$R(x,y)$ et $R(y,x)$" est une relation d'équivalence S dans E (Ens.R, § 6) ; une telle relation R est dite relation de <u>préordre</u> (Ens., chap.III) . Sur l'ensemble quotient E/S la relation R définit une relation d'ordre, qui est dite associée à R .

<u>Définition 2</u> - <u>Sur un ensemble</u> M , <u>on dit qu'une relation de préordre</u> R(x,y) <u>et une structure de monoïde commutatif</u> (notée additivement) <u>sont compatibles si elles satisfont à l'axiome suivant</u> :

(MPO) <u>Quel que soit</u> $z \in M$, R(x,y) <u>entraîne</u> R(x+z, y+z) .

<u>Un ensemble</u> M <u>muni d'une structure de monoïde commutatif et d'une relation de préordre compatibles est appelé un monoïde préordonné</u> ; <u>si sa structure de monoïde commutatif est une structure de groupe abélien, il est appelé groupe préordonné</u>.

<u>Proposition 3</u> - <u>Soit</u> M <u>un monoïde préordonné de relation de préordre</u> R , <u>et soit</u> S <u>la relation d'équivalence associée à</u> R ; <u>alors</u> S <u>est compatible avec l'addition de</u> M (Chap.I, § 4,n°3,déf.4); <u>le quotient de l'addition par</u> S , <u>et la structure d'ordre associée à</u> S <u>définissent sur</u> M/S <u>une structure de monoïde ordonné</u>. <u>Si, de plus,</u> M <u>est un groupe préordonné</u>, M/S <u>est le groupe quotient de</u> M <u>par le sous-groupe</u> M' <u>des éléments</u> x <u>satisfaisant à</u> R(x,0) <u>et</u> R(0,x) .

Il suffit de montrer que $x \equiv x'$ (mod.S) entraîne $x+y \equiv x'+y$ (mod.S) pour tout $y \in M$. Or l'hypothèse s'écrit "R(x,x') et R(x',x)" ; d'où, d'après (MPO) "R(x+y,x'+y) et R(x'+y,x+y)", ce qui exprime que l'on a $x+y \equiv x'+y$ (mod.S). Le reste est conséquence immédiate des définitions.

3 - <u>Eléments positifs</u>.

Soit G un groupe préordonné de relation de préordre R ; de R(0,x) et R(0,y), on déduit, en vertu de (MPO), R(y,x+y), d'où R(0,x+y) par transitivité ; ceci exprime que l'ensemble P des $x \in G$ tels que R(0,x) est <u>stable</u> pour l'addition, ce qui s'écrit P+P = P. Réciproquement, étant donnée une partie P d'un groupe G, contenant 0 et telle que $P+P=P$, la relation "$y-x \in P$" est réflexive et transitive (car $z-x = (z-y)+(y-x)$) ; c'est donc une relation de préordre sur G ; elle satisfait à (MPO) car, si $x-y \in P$, on a $(x+z)-(y+z) = x-y \in P$. Nous pouvons donc énoncer le résultat suivant :

<u>Proposition 4</u> - <u>Soit</u> P <u>une partie d'un groupe</u> G, <u>contenant</u> 0 <u>et telle que</u> $P+P = P$; <u>la relation</u> "$x-y \in P$" <u>définit alors sur</u> G <u>une relation de préordre compatible avec sa structure de groupe. Et toute structure de groupe préordonné peut être définie ainsi.</u>

Pour que G soit un groupe ordonné, il faut et il suffit que le sous-groupe G' des éléments x satisfaisant à $R(x,0)$ et $R(0,x)$ se réduise à $\{0\}$. Or G' n'est autre que $P \cap (-P)$ car les relations $R(x,0)$ et $R(0,-x)$ sont équivalentes en vertu de (MPO). Donc :

<u>Corollaire 1</u> - <u>Pour que, de plus,</u> P <u>définisse sur</u> G <u>une structure de groupe ordonné, il faut et il suffit que</u> $P \cap (-P)$ <u>se réduise à</u> $\{0\}$.

<u>Corollaire 2</u> - <u>Pour que, de plus,</u> P <u>détermine sur</u> G <u>une structure d'ensemble totalement ordonné, il faut et il suffit que</u> $P \cup (-P) = G$.

En effet, dire que G est totalement ordonné, équivaut à dire que, pour tout couple d'éléments (x,y) de G, $x-y$ ou $y-x$ appartient à P.

<u>Définition 3</u> - <u>Dans un groupe ordonné</u> G <u>les éléments</u> x <u>tels que</u> $0 \leqslant x$ (resp. $x \leqslant 0$) <u>sont appelés positifs</u> (resp. négatifs).

<u>Exemple</u> - Dans le groupe additif $Z \times Z$, soit P l'ensemble des éléments (x,y) satisfaisant à deux inégalités $ax+by \geqslant 0$, $cx+dy \geqslant 0$, où a,b,c,d sont des entiers (*ou des nombres réels*) tels que $ad-bc \neq 0$; le "cone" P satisfait aux conditions de la prop.4 et du cor.1. On définit ainsi sur $Z \times Z$ une infinité de structures d'ordre compatibles avec sa structure de groupe ; le groupe n'est totalement ordonné pour aucune de ces structures.

<u>Remarque</u> - La condition $P+P = P$, entraîne que le monoïde engendré par un élément $x \in P$ est contenu dans P. Si donc x est un élément d'ordre fini n d'un groupe G et si $x \in P$, le sous-groupe engendré par x est contenu dans P ; en particulier $-x=(n-1)x$ est élément de P ; en vertu de $P \cap (-P) = \{0\}$, ceci entraîne $x=0$. Ainsi 0 est le seul élément positif d'ordre fini d'un groupe ordonné. En particulier un groupe dont tous les éléments sont d'ordre fini n'est susceptible que de l'ordre trivial, pour lequel $x \leqslant y$ est équivalent à $x=y$.

4 - <u>Groupes filtrants.</u>

Rappelons (Ens.R, § 6) qu'un groupe ordonné G est <u>filtrant à droite</u> (resp. <u>à gauche</u>) si, pour tout couple (x,y) d'éléments de G, il existe $z \in G$ tel que $x \leqslant z$ et $y \leqslant z$ (resp. $z \leqslant x$ et $z \leqslant y$). Tout groupe ordonné filtrant à droite est aussi filtrant à gauche et réciproquement : en effet, comme il existe $z \in G$ tel que $-x \leqslant z$ et $-y \leqslant z$, on a (cor. de la prop.2) $-z \leqslant x$ et $-z \leqslant y$. Nous parlerons donc simplement de groupe filtrant.

<u>Proposition 5</u> - <u>Pour qu'un groupe ordonné</u> G <u>soit filtrant il faut et il suffit qu'il soit engendré par ses éléments positifs, c'est à dire que l'on ait</u> $G=P-P$, P <u>désignant l'ensemble des éléments positifs de</u> G.

En effet, si G est filtrant, il existe, pour tout $x \in G$, un élément positif z tel que $x \leqslant z$, et x est alors différence des éléments positifs z et $z-x$. Si réciproquement x et y sont différences d'éléments positifs, soit $x=u-v$, $y=w-t$, l'élément $u+w$ est supérieur à x et à y.

<u>Proposition 6</u> (lemme de translation) - <u>Si</u> (x_i) <u>est une famille finie d'éléments d'un groupe filtrant</u> G, <u>il existe</u> $z \in G$ <u>tels que</u> x_i+z <u>soit positif quel que soit</u> i.

Si $x_i=u_i-v_i$, avec u_i et v_i positifs, il suffit de prendre pour z la somme de la famille (v_i).

5 - Relations de divisibilité dans un corps.

Nous allons maintenant définir certains groupes ordonnés qui jouent un grand rôle en Algèbre. Dans ces groupes c'est la notation multiplicative qui est naturelle ; l'application à ces groupes des résultats obtenus précédemment en notation additive, suppose donc faite leur traduction en notation multiplicative ; traduction qui ne présentera aucune difficulté au lecteur. Dans tout ce §, A désignera un anneau d'intégrité (c'est-à-dire un anneau commutatif sans diviseurs de zéro ; cf.chap.I, § 8, n°3) ayant un élément unité noté 1 ; et K désignera le corps des fractions de A (Chap.I, § 9, n°4).

Dans le groupe multiplicatif K^* des éléments non nuls de K, l'ensemble $P = A^*$ des éléments non nuls de A est stable, puisque A est un anneau. Il définit donc sur K^* une relation de préordre, qui en fait un groupe préordonné (noté multiplicativement) (prop.3). Cette relation de préordre s'écrit "$x^{-1}y \in P$", c'est à dire "il existe $z \in A^*$ tel que $y=zx$". Généralisant au cas où x et y sont des éléments de K^* la terminologie relative aux éléments de A, nous dirons que x divise y, ou que x est diviseur de y, ou que y est multiple de x (relativement à l'anneau A), et nous appellerons la relation en question la relation de divisibilité dans K^* relative à l'anneau A. La relation "x divise y" se note $x|y$, et sa négation $x\nmid y$. Les éléments de A^* ne sont autres que les multiples de 1 ; on les appelle quelquefois éléments entiers.

Remarques - 1) La relation de divisibilité dans K^* dépend essentiellement de l'anneau A choisi. Pour $A=K$ on obtient la relation triviale où $x|y$ pour tout couple (x,y) d'éléments de K^*.

2) Nous étendrons parfois la relation "$x|y$" à un couple d'éléments de K (et nous plus seulement de K^*), cette relation étant synonyme de "il existe $z \in A$ tel que $y=zx$" ; on aura donc $x|0$ pour tout $x \in K$. Cette extension permet d'énoncer sans restriction les résultats suivants, qui se déduisent aussitôt de la distributivité de la multiplication par rapport à l'addition : si $x|y$ et $x|z$, alors $x|(y-z)$; si $x|y$ et $x\nmid z$, alors $x \nmid (y-z)$.

Pour déduire de la relation de divisibilité une relation d'<u>ordre</u> (prop.3), il faut passer au groupe quotient de K^* par le sous-groupe U des éléments $x \in K^*$ tels que $x|1$ et $1|x$; ces éléments sont ceux de A qui sont diviseurs de 1, c'est-à-dire les éléments de A qui sont <u>inversibles</u> dans A ; on les appelle souvent, par abus de langage, les <u>unités</u> de l'anneau A. Le groupe quotient K^*/U est alors un groupe ordonné. Deux éléments x et y de K^* qui appartiennent à la même classe mod.U sont dits <u>associés</u> ; ceci veut dire que l'on a $x|y$ et $y|x$. Lorsqu'au contraire x divise y mai[s] y ne divise pas x, on dit que x divise <u>strictement</u> y, ou que x est un diviseur strict de y, ou que y est un multiple strict de x.

On notera que K^*/U est un groupe filtrant, du fait que K est corps des fractions de A (prop.5).

Dire que deux éléments x et y de K^* sont associés, revient, en vertu de la transitivité de la relation de divisibilité, à dire que x et y ont <u>mêmes multiples</u> dans K^*. Conformément aux définitions générales (chap.I, §1,n°1) nous noterons Ax l'ensemble des multiples de x ; Ax est un sous A-module de K, que, par extension de la terminologie relative au cas où $x \in A$, nous appelerons un <u>idéal fractionnaire principal</u> (*) du corps K

(*) On notera qu'un idéal fractionnaire n'est pas un idéal de K considéré comme anneau. Nous généraliserons plus loin la notion d'idéal fractionnaire principal.

relativement à l'anneau A ; nous le noterons aussi (x) ; par opposition les idéaux de l'anneau A seront dits <u>entiers</u>. On écrira $x \equiv 0\ (y)$ pour $x \in Ay$, et $x \equiv x'$ pour $x-x' \in Ay$; si $x \equiv x'\ (y)$, on aura $zx \equiv zx'$ (zy) quel que soit $z \in K$.

On notera que $x \equiv x'\ (y)$ n'entraîne <u>pas</u> $zx \equiv zx'\ (y)$ à moins que z ne soit entier ; ainsi, dans Q, on a $4 \equiv 2\ (2)$, mais non (en prenant $z=1/2$) $2 \equiv 1\ (2)$.

La relation $x|y$ équivaut évidemment à $(x) \supset (y)$. L'application $x \longrightarrow (x)$ de K^* sur l'ensemble $\mathcal{P}^*$ des idéaux fractionnaires principaux $\neq (0)$ de K définit donc, par passage au quotient, une application <u>biunivoque</u> de K^*/U sur $\mathcal{P}^*$; en transportant à $\mathcal{P}^*$ au moyen de cette application, la structure de groupe de K^*/U, on est conduit à définir comme produit des idéaux fractionnaires principaux (x) et (y) l'idéal (xy), celui-ci ne dépendant que de (x) et (y). Muni de cette loi et de la relation d'ordre $(x) \supset (y)$, $\mathcal{P}^*$ est un groupe ordonné, isomorphe à K^*/U, et qu'on conviendra d'identifier à K^*/U au moyen de l'application ci-dessus.

On notera soigneusement que la relation "x divise y", qui, dans le cas des entiers positifs, implique que x est <u>plus petit</u> que y, correspond à l'inclusion $(x) \supset (y)$, où l'idéal (x) est "plus grand" que l'idéal (y). La situation est analogue dans les anneaux de polynomes. On se souviendra de ce "renversement d'ordre" en notant que 7 a "plus de multiples" que 91.

Comme dans les n° strictement précédents, les notions et résultats relatifs aux groupes ordonnés seront exposés en notation additive. Cependant l'introduction de la terminologie relative à la Divisibilité sera faite après l'introduction de la terminologie additive correspondante

 H

dans des alinéas précèdés du signe (DIV). Et, afin de faciliter le travail du lecteur, certains résultats importants seront traduits dans le langage de la Divisibilité, la traduction de la prop.12, par exemple, étant notée "Proposition 12 (DIV)" .

6 - Opérations élémentaires sur les groupes ordonnés.

Soit H un sous groupe d'un groupe ordonné G ; il est clair que la structure d'ordre induite sur H par celle de G est compatible avec la structure de groupe de H ; c'est toujours de celle là que H sera supposé muni, sauf mention expresse du contraire. Si P est l'ensemble des éléments positifs de G , l'ensemble des éléments positifs de H est $H \cap P$.

Soit (G_ι) une famille de groupes ordonnés ; conformément à la définition du produit d'ensembles ordonnés (Livre I, chap.III) le groupe produit $G = \prod_\iota G_\iota$ est muni d'une structure d'ordre, la relation "$(x_\iota) \leqslant (y_\iota)$" entre deux éléments de G étant, par définition, synonyme de "quel que soit ι , $x_\iota \leqslant y_\iota$ " . On voit aussitôt que cette structure d'ordre est compatible avec la structure de groupe de G ; muni de cette structure G est donc un groupe ordonné, que l'on appelle le produit des groupes ordonnés G . Les éléments positifs de G sont ceux dont toutes les composantes sont positives. Dans le cas où tous les facteurs G sont identiques à un même groupe ordonné H, G est le groupe H^I des applications d'un ensemble I dans H , la relation "$f \leqslant g$" entre deux applications de I dans H étant synonyme de "quel que soit $\iota \in I$, $f(\iota) \leqslant g(\iota)$" ; les applications positives sont celles qui ne prennent que les valeurs positives. Ceci généralise l'exemple 2) du n°1 .

Soit (G_α) $(\alpha \in I)$ une famille de groupes ordonnés dont l'ensemble d'indices I est bien ordonné par une relation d'ordre notée $\leqslant$;

rappelons que l'on définit (Livre I, chap. III) sur l'ensemble produit $G = \prod_{\alpha} G_{\alpha}$ une relation d'ordre, dite <u>lexicographique</u>, la relation "$(x_{\alpha}) \leqslant (y_{\alpha})$" entre deux éléments (x_{α}) et (y_{α}) de G étant, par définition, synonyme de "si β est le plus petit indice α tel que $x_{\alpha} \neq y_{\alpha}$, on a $x_{\beta} < y_{\beta}$". Rappelons que le produit d'une famille bien ordonnée d'ensembles <u>totalement</u> ordonnés est totalement ordonné pour l'ordre lexicographique. Dans le cas général la relation d'ordre lexicographique de G est compatible avec sa structure de groupe, comme on le voit aussitôt ; muni de cette structure G est donc un groupe ordonné, que l'on appelle le <u>produit lexicographique</u> de la famille bien ordonnée de groupes ordonnés (G_{α}).

<u>Remarques</u> - 1) Le cas le plus fréquent est celui où l'ensemble ordonné d'indices I est un intervalle <u>fini</u> $[1,n]$ de N.

2) Si tous les G_{α} sont des groupes totalement ordonnés, leur produit lexicographique est un groupe totalement ordonné.

3) L'ensemble des éléments positifs du produit lexicographique G se compose de (0) et des éléments dont la composante non nulle de plus petit indice est positive.

7 - <u>Représentations croissantes de groupes ordonnés.</u>

Soient G et G' deux groupes ordonnés ; parmi les représentations f du groupe additif sous jacent de G dans le groupe additif sous jacent de G', il y a lieu de considérer, en particulier, les applications <u>croissantes</u>, c'est-à-dire celles pour lesquelles $x \leqslant y$ entraîne $f(x) \leqslant f(y)$. En vertu de la relation $f(y-x) = f(y)-f(x)$, les représentations croissantes de G dans G' sont caractérisées par le fait que l'image par une telle représentation d'un élément positif de G est un élément positif de G' ; si P (resp. P') désigne l'ensemble des éléments positifs de G (resp. G') ceci s'écrit $f(P) \subset P'$. Il est clair que l'application canonique d'un sous groupe G dans un groupe ordonné G', et la projection d'un produit de groupes ordonnés sur un de ses facteurs sont des représentations croissantes.

En particulier un <u>isomorphisme</u> (n°1) f d'un groupe ordonné G sur un groupe ordonné G' est caractérisé par le fait que f <u>et</u> sa représentation réciproque sont toutes deux croissantes, ce qui s'écrit $f(P) = P'$.

Il peut arriver qu'un isomorphisme du groupe sous-jacent de G sur celui de G' soit croissant, sans que l'isomorphisme réciproque le soit. Il en sera ainsi, par exemple, si G=G', si f est l'application identique de G sur lui-même, et si $P \subset P'$ mais $P \neq P'$. Ainsi, sur Z, on peut prendre pour P' l'ensemble des entiers positifs (ordinaires) et pour P celui des entiers positifs pairs.

(DIV) Soit K le corps des fractions rationnelles $(Z/(2))(X)$ sur le corps à deux éléments. Les relations de divisibilité relatives aux anneaux $(Z/(2))[X] = A'$ et $(Z/(2))[X^2,X^3] = A$ définissent sur K^* deux structures de groupes ordonnés (1 étant la <u>seule</u> unité de A et la seule de A') du type précédent.

8 - <u>Bornes supérieure et inférieure dans un groupe ordonné. Groupes réticulés.</u>

Rappelons (Ens.R, §6,n°7) que, si l'ensemble des majorants d'une partie A d'un ensemble ordonné E (c'est-à-dire l'ensemble des $z \in E$ tels que $z \geqslant x$ pour tout $x \in A$) a un plus petit élément <u>a</u> , celui-ci, qui est alors unique, est appelé la <u>borne supérieure</u> de A . Si A est l'ensemble des éléments d'une famille $(x_\iota)_{\iota \in I}$ d'éléments de E , sa borne supérieure, lorsqu'elle existe, se note $\sup_{\iota \in I} x_\iota$; s'il s'agit d'une famille finie (x_i) $(1 \leqslant i \leqslant n)$, cette borne se note aussi $\sup(x_1,\dots,x_n)$. La borne inférieure se définit d'une manière analogue et se note inf .

Un ensemble ordonné dans lequel toute partie finie non vide a une borne supérieure et une borne inférieure est dit réticulé ; pour qu'un ensemble ordonné soit réticulé il suffit qu'il en soit ainsi de toute partie formée de deux éléments. Tout ensemble totalement ordonné est réticulé ; dans un tel ensemble on écrit souvent max et min au lieu de sup et inf pour noter les bornes d'une partie finie.

Rappelons (Livre I, chap. III) que si F est une partie d'un ensemble ordonné E, et (x_ι) une famille d'éléments de F, l'existence de $\sup x_\iota$ dans E (que l'on note $\sup_E x_\iota$) n'entraîne pas l'existence d'une borne supérieure des x_ι dans F (que l'on note $\sup_F x_\iota$) ; si toutes deux existent, on a seulement $\sup_E x_\iota \leqslant \sup_F x_\iota$; en revanche si $\sup_E x_\iota$ existe et est dans F, $\sup_F x_\iota$ existe et est égal à $\sup_E x_\iota$.

(DIV) On dit qu'un élément d de K^* est un plus grand commun diviseur, ou, en abrégé un pgcd, d'une famille (x_α) d'éléments de K si l'idéal principal (d) est, dans $\mathcal{P}^*$, la borne supérieure de la famille d'idéaux $((x_\alpha))$, ou, autrement dit, si pour $z \in K^*$, la relation "$z|d$" équivaut à "$z|x_\alpha$ pour tout α". On dira de même que $m \in K^*$ est un plus petit commun multiple ou un ppcm de la famille (x_α) si (m) est, dans $\mathcal{P}^*$, la borne inférieure de la famille d'idéaux $((x_\alpha))$, c'est à dire si "$m|z$" équivaut à "$x_\alpha|z$ pour tout α". Le pgcd et le ppcm, s'ils existent, sont définis modulo le sous groupe U des unités de K^*, c'est à dire que deux pgcd (ou deux ppcm) d'une famille donnée sont associés l'un à l'autre; par abus de langage on écrira souvent pgcd(x_α) et ppcm(x_α) pour l'un quelconque des pgcd ou des ppcm de la famille (x_α) lorsque de tels éléments existent.

Par abus de langage on étend parfois la notion de pgcd à une famille (x_α) d'éléments de K dont certains peuvent être nuls ; ce pgcd étant encore défini comme un élément d de K tel que "$z | d$" soit équivalent à "$z | x_\alpha$ pour tout α" , il est clair que d est 0 si tous les x_α sont nuls, et, dans le cas contraire, est un pgcd de la famille des x_α non nuls. De même le ppcm d'une famille dont certains éléments sont nuls est 0 .

Dans le reste de ce § les monoïdes et groupes ordonnés étudiés seront, sauf mention expresse du contraire, supposés réticulés. Le lecteur notera que les prop.7, 11, 12 s'étendent à un groupe ordonné quelconque, en ce sens que si l'un des membres de l'égalité qui y est écrite est défini, l'autre l'est aussi et l'égalité est vraie.

Il est clair que le produit (ordinaire) de groupes réticulés, et en particulier de groupes totalement ordonnés, est un groupe réticulé. Par contre un sous-groupe d'un groupe réticulé n'est pas nécessairement réticulé.

Ainsi, dans le groupe ordonné produit $Z \times Z$, la "seconde bissectrice" H (sous groupe des couples (n,n') tels que $n+n'=0$) est ordonnée par l'ordre trivial et n'est donc pas un groupe réticulé. *Un autre exemple est celui du groupe G des fonctions numériques continues d'une variable réelle, et du sous groupe des fonctions dérivables (ou des fonctions analytiques, ou des polynomes)*.

Dans un groupe ordonné (non nécessairement réticulé), il résulte aussitôt de l'invariance de l'ordre par translation que l'on a :

$$(1) \qquad \sup (z+x_\alpha) = z + \sup (x_\alpha)$$

en ce sens que, chaque fois que l'un des deux membres de l'une de ces relations existe, l'autre existe aussi et lui est égal. Il résulte de même du fait que l'application $x \rightarrow -x$ transforme l'ordre de G en l'ordre opposé (cor. de la prop.2) que l'on a

$$(2) \qquad \inf(-x_\alpha) = -(\sup(x_\alpha))$$

cette relation étant entendue dans le même sens que la précédente.

<u>Proposition 7</u> - <u>Si</u> x <u>et</u> y <u>sont éléments d'un groupe réticulé</u> G , <u>on a</u> $x+y = \inf(x,y) + \sup(x,y)$.

<u>Proposition 7 (DIV)</u> - <u>Si</u> $\mathcal{P}^*$ <u>est un groupe réticulé et si</u> x <u>et</u> y <u>sont éléments de</u> K <u>on a</u> $xy = \text{ppcm}(x,y).\text{pgcd}(x,y)$.

En effet, d'après (1) et (2) on a $\sup(a-x,a-y) = a+\sup(-x,-y) = a-\inf(x,y)$, et il suffit de prendre $a=x+y$.

<u>Proposition 8</u> - <u>Soient</u> (x_α) $(\alpha \in A)$, (y_β) $(\beta \in B)$ <u>deux familles d'éléments d'un groupe ordonné</u> G (non nécessairement réticulé), <u>ayant chacune une borne supérieure. Alors la famille</u> $(x_\alpha+y_\beta)$ $((\alpha,\beta)\in A\times B)$ <u>a une borne supérieure, et l'on a</u>

$$\sup_{(\alpha,\beta)\in A\times B}(x_\alpha+y_\beta) = \sup_{\alpha\in A}(x_\alpha) + \sup_{\beta\in B}(y_\beta)$$

Soient a et b les bornes supérieures des familles données. Dire que $x_\alpha+y_\beta \leqslant z$, β étant donné, équivaut, par translation à dire que l'on a $\sup(x_\alpha)+y_\beta \leqslant z$; donc, si l'on a $x_\alpha+y_\beta \leqslant z$ pour tout couple d'indices (α,β), ceci équivaut à $a+b \leqslant z$, ce qui montre que $a+b$ est la borne supérieure de la famille double.

<u>Proposition 9</u> - <u>Soit</u> P <u>l'ensemble des éléments positifs d'un groupe ordonné</u> G . <u>Pour que</u> G <u>soit réticulé il faut et il suffit que l'on ait</u> $G=P-P$, <u>et que de plus</u> P , <u>muni de l'ordre induit, satisfasse à l'une ou l'autre des conditions suivantes</u> :

a) <u>Tout couple d'éléments de</u> P <u>a une borne supérieure dans</u> P .

b) <u>Tout couple d'éléments de</u> P <u>a une borne inférieure dans</u> P .

La condition $G=P-P$, qui exprime que G est filtrant (prop.5) est évidemment nécessaire, et nous la supposerons satisfaite. Nous remarquerons d'abord que, si x et y sont positifs et admettent a (resp.b) pour borne supérieure (resp. inférieure) <u>dans</u> P , a (resp.b) est la borne supérieure (resp. inférieure) de x et y dans G ; ceci est évident pour sup, tout majorant de x et y étant positif ; pour inf soit $z \in G$ un minorant de x et y ; il existe alors $u \in P$ tel que $z+u \in P$ (prop.6) ; or $\inf_P(x+u,y+u)$ majore $b+u$ et est donc de la forme $b+c+u$ $(c \geqslant 0)$, et, comme $b+c$ est inférieur à x et à y , on a $c=0$; donc $\inf_P(x+u,y+u) = b+u$ ce qui implique $z+u \leqslant b+u$, donc $z \leqslant b$, et b est bien la borne inférieure de x et y dans G . Si maintenant x et y sont des éléments quelconques de G , nous les translaterons dans P : soit $v \in P$ tel que $x+v$ et $y+v$ soient positifs ; dans l'hypothèse a) (resp.b)) $x+v$ et $y+v$ admettent une borne supérieure (resp. inférieure) dans P, donc aussi dans G d'après ce qui vient d'être montré ; par translation x et y admettent donc une borne supérieure (resp. inférieure) dans G ; l'existence d'une des espèces de bornes pour tout couple (x,y) entraînant celle de l'autre en vertu de (2), ceci montre que les conditions sont suffisantes. Leur nécessité est évidente, les bornes inférieure et supérieure <u>dans</u> G de deux éléments de P étant positives, donc sont aussi leurs bornes dans P .

9 - <u>Le théorème de décomposition.</u>

<u>Théorème</u> 1 (théorème de décomposition) - <u>Soient</u> $(x_i)_{1 \leqslant i \leqslant p}$ <u>et</u> $(y_j)_{1 \leqslant j \leqslant q}$ <u>deux suites finies d'éléments positifs d'un groupe réticulé</u> G <u>telles que</u> $\sum_{i=1}^{p} x_i = \sum_{j=1}^{q} y_j$; <u>il existe alors une suite double</u> $(z_{ij})_{1 \leqslant i \leqslant p, 1 \leqslant j \leqslant q}$ <u>d'éléments positifs de</u> G <u>telle que l'on ait</u>

$x_i = \sum_{j=1}^{q} z_{ij}$ <u>pour tout</u> i , <u>et</u> $y_j = \sum_{i=1}^{p} z_{ij}$ <u>pour tout</u> j .

1° Si le théorème est vrai pour $p < m$ et $q=n$ $(m > 2,\ n \geqslant 2)$ il est vrai pour $p=m$ et $q=n$. On a en effet $x_m + \sum_{i=1}^{m-1} x_i = \sum_{j=1}^{n} y_j$; le théorème étant vrai pour $p=2$ et $q=n$, il existe 2 suites finies (z'_j), (z''_j) de n termes positifs telles que $\sum_{i=1}^{m-1} x_i = \sum_{j=1}^{n} z'_j$, $x_m = \sum_{j=1}^{n} z''_j$ et $y_j = z'_j + z''_j$ pour $1 \leqslant j \leqslant n$. D'autre part, le théorème étant vrai pour $p=m-1$ et $q=n$, il existe une suite double $(u_{ij})_{1 \leqslant i \leqslant m-1, 1 \leqslant j \leqslant n}$ telle que $x_i = \sum_{j=1}^{n} u_{ij}$ pour $1 \leqslant i \leqslant m-1$, et $z'_j = \sum_{i=1}^{m-1} u_{ij}$ pour $1 \leqslant j \leqslant n$; en posant $z_{ij} = u_{ij}$ pour $1 \leqslant i \leqslant m-1$, et $z_{mj} = z''_j$ $(1 \leqslant j \leqslant n)$, on obtient bien une suite double satisfaisant aux conditions du théorème.

2° En échangeant les rôles des (x_i) et des (y_j) on voit de même que, si le théorème est vrai pour $p=m$ et $q < n$ $(m \geqslant 2,\ n > 2)$, il est vrai pour $p=m$ et $q=n$.

3° Reste donc à démontrer le théorème pour $p=q=2$. Supposons donc que les éléments positifs x, x', y, y' soient tels que $x+x'=y+y'$. Comme $x-y'=y-x'$ est inférieur à x et y , on a $a=\sup(0, x-y') \leqslant \inf(x,y)$. Alors $b=x-a$ et $c=y-a$ sont positifs, de même que $d=a-(x-y')$. Et on a $x=a+b$, $x'=c+d$, $y=a+c$, $y'=b+d$. C.Q.F.D.

<u>Corollaire</u> - <u>Soient</u> $y, x_1, x_2, \ldots, x_n$ $n+1$ <u>éléments positifs de</u> G <u>tels que</u> $y \leqslant \sum_{i=1}^{n} x_i$; <u>il existe alors</u> n <u>éléments positifs</u> y_i $(1 \leqslant i \leqslant n)$ <u>tels que</u> $y_i \leqslant x_i$ <u>et</u> $y = \sum_{i=1}^{n} y_i$.

Il suffit d'appliquer le th. de décomposition à la suite (x_i) et à la suite formée des 2 éléments y et $z = \sum_{i=1}^{n} x_i - y$.

10 - Partie positive et partie négative.

Définition 3 - Dans un groupe réticulé G on appelle partie positive (resp. partie négative, valeur absolue) d'un élément $x \in G$, et on note x^{+} (resp. x^{-}, $|x|$) l'élément $\sup(x,0)$ (resp. $\sup(-x,0)$, $\sup(x,-x)$).

Il est clair que l'on a $x^{-}=(-x)^{+}$, et $|-x| = |x|$.

2 Contrairement à son nom la partie négative x^{-} de x est un élément positif.

Proposition 10 - a) Tout élément x d'un groupe réticulé s'écrit, $x = x^{+}-x^{-}$ et on a $\inf(x^{+},x^{-}) = 0$.

b) Pour toute décomposition de x comme différence de deux éléments positifs, $x=u-v$, on a $u=x^{+}+w$ et $v=x^{-}+w$ avec $w=\inf(u,v)$. Si, en particulier on a $\inf(u,v)=0$, on a $u=x^{+}$ et $v=x^{-}$.

c) La relation "$x \leqslant y$" est équivalente à "$x^{+} \leqslant y^{+}$ et $x^{-} \geqslant y^{-}$" .

d) On a $|x| = x^{+} + x^{-} \geqslant 0$.

e) Quels que soient x et y de G on a l'inégalité du triangle

$$|x+y| \leqslant |x| + |y|$$

et $\big||x| - |y|\big| \leqslant |x-y|$; ainsi que $\left|\sum_{i=1}^{n} x_i\right| \leqslant \sum_{i=1}^{n} |x_i|$ pour toute famille finie (x_i) d'éléments de G .

Nous démontrerons a) et b) simultanément : si $x=u-v$ avec u et v positifs, on a $u \quad x$, donc $u \quad \sup(x,0)=x^{+}$ et $w=u-x^{+}$ est positif ; d'autre part $x^{+}-x = \sup(x,0)-x = \sup(x-x,-x)=x^{-}$, d'où résulte $x=x^{+}-x^{-}$, et donc $v-x^{-}=w$. De $z \leqslant x^{+}$ et $z \leqslant x^{-}$, on tire $z \leqslant x^{+}-x$, et $x \leqslant x^{+}-z$ avec $x^{+}-z$ positif, d'où $x^{+} \leqslant x^{+}-z$ en vertu de la définition de x^{+} ; on a donc $z \leqslant 0$, ce qui entraîne $\inf(x^{+},x^{-})=0$, d'où, par translation, $\inf(u,v)=w$.

c) "$x \leqslant y$" entraîne $\sup(y,0) \geqslant x$ et $\sup(y,0) \geqslant 0$, d'où $x^{+} \leqslant y^{+}$; de $(-y) \leqslant (-x)$ on déduit de même $x^{-} \geqslant y^{-}$. L'implication inverse se déduit aussitôt de $x=x^{+}-x^{-}$ et $y=y^{+}-y^{-}$.

d) Comme $x \leqslant x^+$ et $-x \leqslant x^-$, il est clair que $|x| = \sup(x,-x) \leqslant x^+ + x^-$: Inversement de $a \geqslant x$ et $a \geqslant -x$, on déduit, en vertu de c) $a^+ \geqslant x^+$, $a^+ \geqslant x^-$, $a^- \leqslant x^-$ et $a^- \leqslant x^+$; comme a^- est positif et que $\inf(x^+,x^-)=0$, les deux dernières inégalités entraînent $a^-=0$ et $a=a^+$; les deux premières donnent alors $a \geqslant \sup(x^+,x^-)$ élément qui est égal à $x^+ + x^-$ en vertu de la prop.7 .

e) De $x \leqslant |x|$ et $y \leqslant |y|$ on tire $x+y \leqslant |x|+|y|$; de $-x \leqslant |x|$ et $-y \leqslant |y|$ on tire $-x-y \leqslant |x|+|y|$; d'où l'inégalité du triangle. En remplaçant dans celle-ci x,y par $y,x-y$, il vient $|x|-|y| \leqslant |x-y|$; on a de même $|y|-|x| \leqslant |y-x| = |x-y|$; d'où la seconde inégalité. La troisième se déduit de l'inégalité du triangle par récurrence sur n .

Notons les formules suivantes, qui ramènent les opérations sup et inf à l'opération $x \to x^+$:

$$(3) \qquad \begin{aligned} \sup(x,y) &= x + (y-x)^+ \\ \inf(x,y) &= y - (y-x)^+ \end{aligned}$$

La première est conséquence immédiate des définitions et de l'invariance de sup par trnaslation, et la seconde s'en déduit au moyen de la prop.7.

Remarque - On déduit de c) que $|x| = 0$ entraîne $x=0$ (car x^+ et x^- sont positifs), donc $x \neq 0$ entraîne $|x| > 0$.

Proposition 10 (DIV) - Si le groupe $\mathcal{P}^*$ des idéaux fractionnaires principaux de K^* est réticulé, tout élément x de K peut être mis sous la forme $x=uv^{-1}$ où u et v sont des entiers tels que pgcd $(u,v) = 1$; pour toute autre représentation $x=u'v'^{-1}$ de x comme quotient de deux entiers, on a $u'=uw$, $v'=vw$ où w est un entier ; pgcd de u' et v' ; en particulier si pgcd$(u',v')=1$, u' et v' sont respectivement associés à u et v .

Une telle expression uv^{-1} d'un élément x de K est souvent appelée fraction irréductible ; on convient aussi de considèrer $0/1$ comme fraction irréductible.

11 - <u>Eléments étrangers.</u>

<u>Définition 4</u> - <u>Dans un groupe réticulé deux éléments</u> x <u>et</u> y <u>sont dits étrangers si l'on a</u> $\inf(x,y)=0$.

Deux éléments étrangers sont nécessairement <u>positifs</u>. Les parties positive et négative x^+ et x^- de x sont des éléments étrangers (prop.10,a). On dit que les éléments x_λ d'une famille $(x_\lambda)_{\lambda \in I}$ sont <u>étrangers dans leur ensemble</u> si l'on a $\inf_{\lambda \in I}(x_\lambda)=0$; il suffit pour cela qu'il existe une partie J de I telle que les éléments de J soient étrangers dans leur ensemble. Les éléments d'une famille (x_λ) sont dits <u>étrangers deux à deux</u> si l'on a $\inf(x_\lambda, x_\mu)=0$ pour tout couple (λ, μ) d'éléments distincts de I .

Les (x_λ) peuvent être étrangers dans leur ensemble sans être étrangers deux à deux.

Si x et y sont étrangers, on dira aussi que x est étranger à y et y à x .

(DIV) On dit que les éléments x et y de K sont <u>étrangers</u> si les idéaux principaux (x) et (y) sont étrangers dans $\mathcal{P}^*$; ceci revient à dire que $\mathrm{pgcd}(x,y)=1$, et implique que x et y sont <u>entiers</u>. Par exemple le numérateur et le dénominateur d'une fraction irréductible sont étrangers. On définit de même les notions d'entiers x_λ étrangers dans leur ensemble, et étrangers deux à deux.

(DIV) On dit souvent, quand 1 est pgcd de x et y , que x et y sont "premiers entre eux" ; il convient d'éviter cette terminologie, qui entraîne confusion avec la notion d'entier premier (v.plus loin).

<u>Proposition 11</u> - <u>Si</u> x <u>et</u> y <u>sont deux éléments étrangers et</u> z <u>un élément positif d'un groupe réticulé, on a</u> $\inf(x,z)= \inf(x,y+z)$.

On a en effet $0=\inf(x,y)$ donc $z=\inf(x+z,y+z)$. Par suite la relation "$t \leq x$ et $t \leq z$" équivaut à "$t \leq x$, $t \leq x+z$, $t \leq y+z$" , donc aussi (puisque $x \leqslant x+z$) à "$t \leqslant x$ et $t \leqslant y+z$".

<u>Corollaire 1</u> - <u>Si</u> x,y <u>sont étrangers et si</u> $x \leqslant y+z$, ($z \geqslant 0$) <u>on a</u> $x \leqslant z$.

<u>Corollaire 2</u> - <u>Si</u> x <u>est étranger à</u> y <u>et</u> z, <u>il l'est aussi à</u> $y+z$.

<u>Corollaire 3</u> - <u>Si</u> $(x_i),(y_j)$ <u>sont deux familles finies d'éléments de</u> G <u>telles que chacun des</u> x_i <u>soit étranger à chacun des</u> y_j, <u>alors</u> $x_1+\ldots+x_n$ <u>est étranger à</u> $y_1+\ldots+y_m$.

Ceci se déduit du cor.2 par récurrence sur m et n.

<u>Corollaire 4</u> - <u>Quel que soit l'entier naturel</u> n, <u>on a</u> $(nx)^+=nx^+$ $(nx)^-=nx^-$; <u>pour tout entier</u> $n \in Z$, <u>on a</u> $|nx|=|n|.|x|$.

On a en effet $nx=nx^+-nx^-$; comme x^+ et x^- sont étrangers, il en est de même de nx^+ et nx^- ; d'où la première assertion en vertu de la prop. 10,a) ; la seconde s'ensuit en vertu de la prop.10,d) dans le cas $n \geqslant 0$; on passe de là au cas $n<0$ au moyen de $|-x|=|x|$.

<u>Proposition 11</u> (DIV) - <u>Si</u> x,y,z <u>sont des entiers tels que</u> x <u>soit étranger à</u> y, <u>on a</u> pgcd(x,z) = pgcd(x,yz).

Corollaire 1 (DIV) ("Lemme d'Euclide) - <u>Soient</u> x,y,z <u>trois entiers.</u> <u>Si</u> x <u>est étranger à</u> y <u>et divise</u> yz, <u>il divise</u> z.

<u>Corollaire 2</u> (DIV) - <u>Si</u> x <u>est étranger à</u> y <u>et</u> z, <u>il l'est aussi à leur produit</u> yz.

<u>Corollaire 3</u> (DIV) - <u>Si</u> $(x_i),(y_j)$ <u>sont deux familles finies d'entiers telles que chaque</u> x_i <u>soit étranger à chaque</u> y_j, <u>alors le produit des</u> x_i <u>est étranger au produit des</u> y_j.

<u>Proposition 12</u> - <u>Soient</u> x,y,z <u>trois éléments d'un groupe réticulé</u> ; <u>pour que</u> $x-z$ <u>et</u> $y-z$ <u>soient étrangers, il faut et il suffit que l'on ait</u> $z = \inf(x,y)$.

En effet "$z=\inf(x,y)$" et "$0=\inf(x-z,y-z)$" sont des relations équivalentes.

 23

<u>Proposition 12</u> (DIV) - <u>Soient</u> x, y, z <u>trois éléments de</u> K^* ($\mathcal{O}^*$ <u>étant réticulé)</u> ; <u>pour que les quotients</u> xz^{-1} <u>et</u> yz^{-1} <u>soient étrangers, il faut et il suffit que</u> z <u>soit un pgcd de</u> x <u>et</u> y .

<u>Corollaire</u> (DIV) - <u>Si</u> d <u>est un pgcd de</u> x <u>et</u> y, d^n <u>est un pgcd de</u> x^n <u>et</u> y^n <u>pour tout entier naturel</u> n .

En effet, comme xd^{-1} et yd^{-1} sont étrangers, il en est de même de $x^n d^{-n}$ et $y^n d^{-n}$ (cor.3 de la prop.11 (DIV)).

<u>Proposition 13</u> - <u>Pour que deux éléments</u> x <u>et</u> y <u>d'un groupe réticulé soient étrangers, il faut et il suffit que l'on ait</u> $x+y = \sup(x,y)$.

On a en effet $x+y = \sup(x,y)+\inf(x,y)$ (Prop.7) .

<u>Corollaire</u> - <u>Soient</u> x_i $(1 \leqslant i \leqslant n)$ n <u>éléments étrangers deux à deux d'un groupe réticulé. Alors on a</u> $\sup(x_1,\dots,x_n) = x_1+\dots+x_n$.

C'est immédiat par récurrence sur n , en tenant compte du cor.3 de la prop.11 .

<u>Corollaire</u> (DIV) - <u>Soient</u> x_i <u>des entiers en nombre fini</u> n <u>et étrangers deux à deux ; alors leur produit</u> $x_1\dots x_n$ <u>est un ppcm de</u> $x_1,\dots,x_n$.

<u>Proposition 14</u> - <u>Dans un groupe réticulé</u> G , <u>soit</u> (x_α) <u>une famille admettant une borne inférieure</u> y, <u>et soit</u> z <u>un élément quelconque de</u> G ; <u>alors la famille</u> $(\sup(z,x_\alpha))$ <u>admet une borne inférieure et on a</u>

$$\inf_\alpha(\sup(z,x_\alpha)) = \sup(z,\inf_\alpha x_\alpha)$$

On a en effet $\sup(z,x_\alpha) = z+(x_\alpha-z)^+$, et, par translation, nous sommes ramenés au cas $z=0$, c'est-à-dire à montrer que la famille (x_α^+) admet une borne supérieure qui est y^+ . Comme on a $y \leqslant x_\alpha$, on a $y^+ \leqslant x_\alpha^+$ pour tout α (prop.10,c)). Si, inversement, on a $a \leqslant x_\alpha^+$ pour tout α , on en déduit $a \leqslant x_\alpha + x_\alpha^-$ (prop.10,a)) ; or, de $y \leqslant x_\alpha$, on déduit $y^- \geqslant x_\alpha^-$; on a donc $a \leqslant x_\alpha + y^-$ pour tout α , c'est-à-dire $a \leqslant y+y^- = y^+$. C.Q.F.D.

<u>Corollaire 1</u> - <u>Si, dans un groupe réticulé</u> G, z <u>est étranger à chacun des éléments</u> x_α <u>d'une famille admettant une borne supérieure</u> y , <u>alors</u> z <u>est étranger à</u> y .

Par échange de sup et inf , la formule de la prop.14 s'écrit $\sup(\inf(z,x_\alpha)) = \inf(z,\sup x_\alpha)$, ce qui démontre le corollaire.

<u>Corollaire 2</u> - <u>Dans un groupe réticulé, chacune des lois de composition</u> <u>sup</u>, <u>inf</u> <u>est distributive par rapport à l'autre</u> : <u>autrement dit</u> :

$$\sup(z,\inf(x,y)) = \inf(\sup(z,x),\sup(z,y))$$

$$\inf(z,\sup(x,y)) = \sup(\inf(z,x),\inf(z,y))$$

Ces relations ne sont, en effet, autres que les formules de la prop.14 et du cor.1, appliquées à la famille de deux éléments (x,y) .

Z

Cette propriété de distributivité est spéciale aux <u>groupes</u> réticulés, et ne s'étend ni aux ensembles, ni même aux monoïdes réticulés. Considérons en effet l'ensemble I des idéaux d'un anneau commutatif B ; nous appellerons <u>produit</u> de deux idéaux $\mathfrak{a}$ et $\mathfrak{b}$, et nous noterons $\mathfrak{a}\mathfrak{b}$, l'idéal formé des sommes finies $\sum_i a_i b_i$, où $a_i \in \mathfrak{a}$ et $b_i \in \mathfrak{b}$; cette loi de composition est associative et est compatible avec la relation d'ordre par inclusion de I ; I est donc un monoïde ordonné ; comme la borne inférieure de deux idéaux est leur intersection, et leur borne supérieure l'idéal engendré par ces deux idéaux, I est un <u>monoïde réticulé</u> ; mais on a seulement les inclusions $\mathfrak{a}+(\mathfrak{b}\cap\mathfrak{c}) \subset (\mathfrak{a}+\mathfrak{b})\cap(\mathfrak{a}+\mathfrak{c})$ et $\mathfrak{a}\cap(\mathfrak{b}+\mathfrak{c}) \supset$ $\supset (\mathfrak{a}\cap\mathfrak{b})+(\mathfrak{a}\cap\mathfrak{c})$, et pas nécessairement l'égalité : il suffit de prendre pour B l'anneau de carré nul (chap.I, § 8) ayant pour groupe additif celui de l'espace vectoriel $Q \times Q$, et pour $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ trois sous-espaces vectoriels distincts et de dimension 1 .

Il revient au même de prendre les idéaux (X,Y^2), (X^2,Y) et $(X+Y,X^2,XY,Y^2)$ de l'anneau de polynomes $K[X,Y]$.

12 - <u>Eléments minimaux.</u>

On dira (par abus de langage) qu'élément x d'un groupe ordonné G est <u>minimal</u>, si c'est un élément minimal de l'ensemble $P \cap \complement\{0\}$ des éléments positifs non nuls de G (ensemble ordonné par l'ordre induit par celui de G, et non par celui qu'il pourrait avoir du fait qu'il pourrait être un ordinal (chap.III,Livre I)). Si y est un élément positif de G, l'élément inf(x,y), s'il existe, ne peut donc être égal qu'à x ou à 0 ; ainsi dans un groupe réticulé, tout y positif est, soit supérieur, soit étranger à l'élément minimal x ; en particulier deux éléments minimaux distincts sont étrangers.

(DIV) Un entier p est dit <u>irréductible</u> si l'idéal (p) est un élément minimal du groupe ordonné $\mathcal{P}^*$; ceci exprime que tout entier qui divise p est associé, soit à p, soit à 1. Si $\mathcal{P}^*$ est réticulé, tout entier y est, soit étranger à p, soit multiple de p.

<u>Proposition 15</u> - <u>Pour qu'un élément positif</u> x <u>d'un groupe réticulé</u> G <u>soit minimal, il faut et il suffit qu'il ne soit pas nul, et que les relations</u> "$x \leq y+z$, $0 \leq y$, $0 \leq z$" <u>entraînent</u> "$x \leq y$ <u>ou</u> $x \leq z$".

Si x est minimal, nous venons de voir que y est soit supérieur à x, soit étranger à x ; dans ce dernier cas le cor.1 de la prop.11 montre que z est supérieur à x. Réciproquement supposons la condition satisfaite : de $0 \leq y \leq x$, on déduit, en posant $x=y+z$ $(z \geqslant 0)$ que l'on a soit $x \leq y$, soit $x \leq z$; dans le premier cas on a $x=y$; dans le second on a $x \leq x-y$, donc $y \leq 0$ et $y=0$; ceci montre que x est bien minimal.

<u>Proposition 15 (DIV) - Si $\mathcal{P}^*$ est un groupe réticulé, la condition pour qu'un entier p soit minimal est qu'il ne soit pas une unité et qu'il ne puisse diviser un produit de deux entiers sans diviser l'un d'eux.</u>

Notons que nous ne nous sommes pas servis du fait que le groupe est réticulé pour démontrer que la condition est suffisante.

<u>Proposition 16 - Soit G' le sous-groupe d'un groupe réticulé G engendré par la famille $(p_\iota)_{\iota \in I}$ des éléments minimaux distincts de G ; tout élément x de G' peut être mis, d'une manière et d'une seule, sous la forme $x = \sum_\iota n_\iota p_\iota$, où les n sont des entiers rationnels nuls sauf un nombre fini d'entre eux ; et, pour que x soit positif, il faut et il suffit que tous les n_ι soient positifs.</u>

G' est évidemment l'ensemble des éléments de G qui sont de la forme $\sum_\iota n_\iota p_\iota$. Supposons qu'on ait une relation $\sum n_\iota p_\iota \geqslant 0$, où les n_ι ne soient pas tous positifs ; en faisant passer au second membre tous les termes de coefficient $n_\iota \leqslant 0$, on a une relation de la forme $m_1p_1+\ldots+m_rp_r \geqslant n_1q_1+\ldots+n_sq_s$, où $r \geqslant 0$, $s > 0$, où les p_i, q_j sont r+s éléments minimaux distincts, et les m_i, n_j des entiers naturels > 0. Le cor. 3 de la prop. 11 montre que les deux membres sont étrangers, donc que le second membre est nul. On en conclut donc que $\sum n_\iota p_\iota \geqslant 0$ entraîne que n_ι est positif pour tout ι. Par suite $\sum n_\iota p_\iota = 0$ entraîne à la fois $n_\iota \geqslant 0$ et $n_\iota \leqslant 0$ pour tout ι, donc $n_\iota = 0$, ce qui achève la démonstration.

On peut exprimer le résultat de la prop. 16 en disant que le groupe ordonné G' est isomorphe au groupe $Z^{(I)}$, somme directe de groupes isomorphes au groupe Z des entiers rationnels, ordonné par l'ordre naturel. Réciproquement, soit $(e_\iota)_{\iota \in I}$ la base canonique de $Z^{(I)}$

(autrement dit (chap. II, § 1; n°8) e_i est l'élément de $Z^{(I)}$ dont toutes les coordonnées sont nulles à l'exception de celle d'indice i qui est égale à 1) ; tout $x \in Z^{(I)}$ se met alors, d'une manière et d'une seule, sous la forme $x = \sum_i n_i e_i$, où les n_i sont des entiers nuls sauf un nombre fini d'entre eux ; la relation $x \geqslant 0$ est, par définition, équivalente à $n_i \geqslant 0$ pour tout i ; et, dans ces conditions, les e_i sont évidemment les éléments minimaux de $Z^{(I)}$.

Les groupes ordonnés $Z^{(I)}$ peuvent, de plus, être caractérisés, à une isomorphie près, comme suit :

<u>Théorème 2</u> - <u>Pour qu'un groupe réticulé</u> G <u>soit isomorphe à une somme directe de groupes</u> Z (ordonnés par l'ordre naturel), <u>il faut et il suffit que tout ensemble non vide d'éléments positifs de</u> G , <u>muni de la relation d'ordre induite par celle de</u> G , <u>contienne un élément minimal</u>.

Montrons d'abord que $Z^{(I)}$ satisfait à la condition énoncée : il est en effet réticulé, en tant que somme directe de groupes totalement ordonnés ; si d'autre part E est un ensemble non vide d'éléments positifs de $Z^{(I)}$, soit $x = \sum_i n_i e_i$ un élément de E ; les éléments y de $Z^{(I)}$ qui sont positifs et inférieurs à x sont en nombre fini, égal à $\prod_i (n_i + 1)$ (produit où les facteurs $\neq 1$ sont en nombre fini) ; donc l'ensemble F des éléments de E qui sont inférieurs à x est a fortiori fini ; comme il n'est pas vide, il contient un élément minimal y_0 (Livre I, chap. III), qui est évidemment élément minimal de E . Supposons réciproquement notre condition satisfaite ; par application de la prop. 16 il nous suffira de montrer que G est engendré par ses éléments minimaux ; étant donné un ~~élément~~ strictement positif x de G , il nous suffira, puisque G est filtrant, (prop. 5), de montrer que x est une somme d'éléments minimaux ;

considérons donc l'ensemble W des éléments positifs w de G qui sont de la forme $w = x-(p_1+\dots+p_n)$ où les p_i sont des éléments minimaux de G, distincts ou non ; comme x est > 0, l'ensemble des éléments de G qui sont strictement positifs et inférieurs à x n'est pas vide et contient donc, par hypothèse, un élément minimal p qui est élément minimal de G ; ainsi W n'est pas vide, et contient donc un élément minimal q ; si q était $\neq 0$, il serait supérieur à un élément minimal p' de G, et $q-p'$ appartiendrait à W contrairement à la minimalité de q dans W ; on a donc $q=0$ et $x=p_1+\dots+p_n$.

<u>Exercices sur le</u> § 1.

1) Etudier la généralisation des propriétés démontrées dans ce § aux groupes ordonnés <u>non commutatifs</u> (notés multiplicativement), un tel groupe G étant défini par le fait que $x \leq y$ entraîne $xz \leq yz$ et $zx \leq zy$ pour tout $z \in G$. On établira notamment que :

a) Si P désigne l'ensemble des éléments $x \geq e$ de G (e: élément neutre) on a $P.P=P$, $P \cap P^{-1} = \{e\}$, et $aPa^{-1}=P$ pour tout $a \in G$. Réciproque. Condition pour que G soit totalement ordonné.

b) Si l'un des éléments $\sup(x,y)$, $\inf(x,y)$ existe, l'autre existe aussi et on a $\sup(x,y)=x(\inf(x,y))^{-1}y = y(\inf(x,y))^{-1}x$.

c) Les éléments $\sup(x,e)$ et $\sup(x^{-1},e)$ sont permutables. Deux éléments étrangers sont permutables.

d) Le sous-groupe G' engendré par la famille des éléments minimaux de G est commutatif. En déduire que, si les conditions du th.2 sont satisfaites le groupe G est commutatif.

WBK OWY 29

2) Soit E un ensemble réticulé sur lequel on se donne une loi de composition $(x,y) \to xy$ (non nécessairement associative), et telle que les applications $x \to ax$ et $x \to xa$ soient des isomorphismes de l'ensemble ordonné E sur lui-même pour tout $a \in E$. On désigne par x_a (resp. $a\ {}_a x$) l'élément de E défini par $(x_a)a=x$ (resp. $a({}_a x)=x$), et on suppose que $x \to a_x$ et $x \to {}_x a$ sont des isomorphismes de l'ensemble ordonné E sur E muni de l'ordre opposé. Dans ces conditions montrer que l'on a, pour tous x,y,z : $(z_{\inf(x,y)}) = (z_y).\sup(x,y)$.

3) Soit G un groupe ordonné tel que P ne se réduise pas à 0 ; montrer que G est un groupe infini, et ne peut avoir de plus grand (ni de plus petit) élément.

4) Soit f l'application canonique d'un groupe ordonné G sur le groupe quotient G/H . Pour que f(P) détermine sur G/H une structure de groupe ordonné il faut et il suffit que $0 \leqslant y \leqslant x$ et $x \in H$ entraînent $y \in H$; on dit alors que H est un sous-groupe <u>épais</u> de G, et G/H est considéré comme un groupeordonné. Si G est, de plus, réticulé, alors, pour que G/H soit un groupe réticulé, il faut et il suffit que $|y| \leqslant |x|$ et $x \in H$ entraînent $y \in H$, montrer que ceci exprime que H est un sous-groupe épais et filtrant. Montrer qu'un groupe ordonné G qui n'a d'autres sous-groupes épais que lui-même et $\{0\}$ est totalement ordonné (considérer les sous-groupes épais engendrés par deux éléments strictement positifs de G) ; en déduire (Top.Géné.,chap.V) que G est alors un sous-groupe du groupe additif des nombres réels.

5) Montrer que P-P est le plus grand sous-groupe filtrant du groupe ordonné G , et que c'est un sous-groupe épais de G ; relation d'ordre sur le groupe quotient ?

6) Si, sur le groupe Z, on prend pour P l'ensemble composé de 0 et des entiers supérieurs à 2, le groupe ordonné obtenu est filtrant, mais non réticulé (Montrer que l'ensemble des x tels que $x \geqslant 0$ et $x \geqslant 1$ a deux éléments minimaux distincts).

7) Donner un exemple de groupe ordonné ayant des éléments $\neq 0$ d'ordre fini (prendre le quotient d'un groupe ordonné convenable G par un sous-groupe H tel que $P \cap H = \{0\}$).

8) Soit x un élément d'un groupe ordonné tel que $y = \inf(x, 0)$ soit défini ; alors, si n est un entier >0, $nx \geqslant 0$ entraîne $x \geqslant 0$ (on a $ny = \inf(nx, (n-1)x, \ldots, 0) \geqslant \inf((n-1)x, \ldots, 0) = (n-1)y$), et par suite $nx = 0$ entraîne $x = 0$.

9) Dans un groupe réticulé G, montrer que la somme d'une famille (H_α) de sous-groupes épais et filtrants est un sous-groupe épais et filtrant (utiliser le cor. du th.1).

10) Montrer que, dans un groupe réticulé G, on a, pour toute suite finie (x_i) $(1 \leqslant i \leqslant n)$ d'éléments de G,

$$\sup(x_i) = \sum_i x_i - \sum_{i<j} \inf(x_i, x_j) + \ldots + (-1)^{p+1} \sum_{i_1 < i_2 < \ldots < i_p} \inf(x_{i_1}, \ldots, x_{i_p}) + \\ + \ldots + (-1)^{n+1} \inf(x_1, \ldots, x_n).$$

(Raisonner par récurrence à partir de la prop.7 et utiliser le cor.2 de la prop.14).

11) Soit (x_i) $(1 \leqslant i \leqslant n)$ une famille de n éléments d'un groupe réticulé G ; pour tout entier k tel que $1 \leqslant k \leqslant n$ on désigne par d_k (resp. m_k) la borne inférieure (resp. supérieure) des $\binom{n}{k}$ sommes $\sum_{i \in H} x_i$, où H parcourt l'ensemble des parties de k éléments de l'intervalle $[1, n]$. Montrer que $d_k + m_{n-k} = x_1 + x_2 + \ldots + x_n$.

12) Etant donné un groupe réticulé G, on dit qu'un sous-groupe H de G est <u>coréticulé</u> si, pour tout couple d'éléments (x,y) de H, $\sup_G(x,y)$ appartient à H (et est donc égal à $\sup_H(x,y)$).

a) Si $G = Q\times Q\times Q$ (Q : totalement ordonné par l'ordre naturel), le sous-groupe H formé des triplets (x,y,z) tels que $z=x+y$ est réticulé ; mais non coréticulé.

b) Tout sous-groupe épais (exerc.4) et filtrant H d'un groupe réticulé G est coréticulé (montrer que $x\in H$ entraîne $x^+\in H$).

c) Si G est un groupe réticulé et H un sous-groupe quelconque de G , soient H' l'ensemble des bornes inférieures des parties finies de H , et H" l'ensemble des bornes supérieures des parties finies de H' ; montrer que H" est le plus petit sous-groupe coréticulé de G contenant H (utiliser le cor.2 de la prop.14).

13) On dit qu'un monoïde M est <u>semi réticulé inférieurement</u> (ou semi réticulé pour simplifier), si c'est un monoïde ordonné, si $\inf(x,y)$ existe pour tous x,y de M , et si on a $\inf(x+z,y+z) = \inf(x,y)+z$ pour tous x,y,z de M . Démontrer que, dans un monoïde semi réticulé, on a les identités :

$$\inf(x,z)+\inf(y,z) = \inf(x+y,z+\inf(x,y,z))$$

$$\inf(x,y,z)+\inf(x+y,y+z,z+x) = \inf(x,y)+\inf(y,z)+\inf(z,x) .$$

Déduire de la première que $x \leqslant z$ et $y \leqslant z$ entraînent $x+y \leqslant z+\inf(x,y)$

14) Montrer que, dans un monoïde semi-réticulé M , on a

$$\inf(x_i+y_i) \geqslant \inf(x_i)+\inf(y_i)$$

quelles que soient les suites finies $(x_i),(y_i)$. En déduire que, dans un groupe réticulé on a les inégalités

$$(x+y)^+ \leqslant x^+ + y^+ \quad , \quad |x^+ - y^+| \leqslant |x-y| .$$

15) Déduire de la première formule de l'exer.13 que la prop.11 et ses cor. sont valables dans un monoïde semi-réticulé, ayant un élément neutre.

16) Montrer que, dans un monoïde semi-réticulé, on a

$$n.\inf(x,y)+\inf(nx,ny) = 2n.\inf(x,y)$$

En déduire que $\inf(nx,ny)=n.\inf(x,y)$ si $\inf(x,y)$ est un élément régulier

17) Soit M un monoïde semi-réticulé ayant un élément neutre 0, et soient x,y,z,t quatre éléments de M tels que $z \geqslant 0$ et $t \geqslant 0$. Démontrer l'inégalité $\inf(x+z,y+t)+\inf(x,y) \geqslant \inf(x+z,y)+\inf(x,y+t)$.

En déduire que, dans un groupe réticulé, on a

$$|\sup(x,z)-\sup(y,z)| + |\inf(x,z)-\inf(y,z)| = |x-y| .$$

18) Soit (G_ι) $(\iota \in I)$ une famille de groupes totalement ordonnés indexée par un ensemble <u>totalement ordonné</u> I ; on définit sur le groupe G' <u>somme directe</u> des G une structure de groupe ordonné en prenant comme éléments strictement positifs de G' tels que, pour le plus petit indice ι tel que $x_\iota \neq 0$, on ait $x_\iota > 0$. Montrer que, muni de cette structure, G' est un groupe totalement ordonné.

19) Soit G un groupe additif, (P_α) une famille de parties de G telles que $P_\alpha+P_\alpha = P_\alpha$ et $P_\alpha \cap (-P_\alpha) = \{0\}$; soit G_α le groupe ordonné obtenu en munissant G de la structure d'ordre pour laquelle P_α est l'ensemble des éléments positifs. On pose $P = \bigcap_\alpha P_\alpha$; montrer que l'on a $P+P = P$ et $P \cap (-P) = \{0\}$; si H est le groupe ordonné obtenu en munissant G de la structure d'ordre pour laquelle P est l'ensemble des éléments positifs, montrer que H est isomorphe à la diagonale du groupe produit $\prod_\alpha G_\alpha$.

20) Soit G un groupe additif et P une partie de G satisfaisant aux conditions : $P+P = P$, $P \cap (-P) = \{0\}$, pour tout entier $n > 0$ "$nx \in P$" entraîne "$x \in P$" (conditions (C)) .

a) Si a est un élément de G tel que $a \notin P$, montrer qu'il existe une partie P' de G, satisfaisant à (C), et telle que $P \subset P'$ et $-a \in P'$ (on prendra pour P' l'ensemble des $x \in G$ tels qu'il existe deux entiers $m > 0$, $n \geqslant 0$ et un élément $y \in P$ satisfaisant à $mx = -na + y$).

b) Déduire de a) que P est l'intersection des parties T de G telles que $T+T=T$, $T \cap (-T) = \{0\}$, $T \cup (-T) = G$ (c'est-à-dire définissant sur G une structure de groupe <u>totalement ordonné</u>), et contenant P (utiliser le th. de Zorn).

c) En particulier si G est un groupe additif dont tous les éléments non nuls sont d'ordre infini, l'intersection des parties T de G telles que $T+T=T$, $T \cap (-T) = \{0\}$, $T \cup (-T) = G$ est réduite à 0.

21) On dit qu'un groupe ordonné est <u>réticulable</u> s'il est isomorphe à un sous-groupe d'un groupe réticulé. Montrer que, pour qu'un groupe G soit réticulable, il faut et il suffit que, pour tout $n > 0$, la relation $nx \geqslant 0$ entraîne $x \geqslant 0$ (pour montrer que la condition est suffisante, utiliser l'exerc. 20,b) et l'exer. 19). Montrer que réciproquement tout groupe réticulable est isomorphe à un sous-groupe d'un produit de groupes totalement ordonnés.

22) Soit G un groupe réticulable (considéré comme Z-module) et E l'espace vectoriel $G_{(Q)}$ (chap. III, § 2) ; montrer que l'on peut définir sur le groupe additif sous-jacent de E une structure d'ordre et une seule, compatible avec la structure de groupe de E, et induisant sur G la structure donnée de groupe ordonné ; muni de cette structure E est réticulable.

23) Soit G le groupe réticulé $Z \times Z$ (Z muni de l'ordre naturel), et H le sous-groupe (épais) de G engendré par $(2,-3)$; montrer que le groupe ordonné G/H n'est pas réticulable (cf. exer. 4).

24) Soit A l'anneau extension quadratique de l'anneau Z ayant pour base $(1, e)$, e étant tel que $e^2=-5$. Montrer que A est un anneau d'intégrité ; dans cet anneau on a $9=3.3=(2+e)(2-e)$; montrer que $3, 2+e$ et $2-e$ sont irréductibles dans A, mais ne satisfont pas à la condition de la prop.15.

25) Montrer que, dans le monoïde des idéaux (n°11) de l'anneau de polynomes $K[X,Y]$ (K:corps commutatif) l'idéal (X) satisfait à la condition de la prop.15 mais n'est pas maximal.

26) Soit M le monoïde (réticulé) des idéaux d'un anneau A. Pour qu'un système de congruences en nombre fini $x \equiv a_i \ (\mathfrak{a}_i)$ ait une solution chaque fois que ces congruences sont deux à deux compatibles (c'est-à-dire que l'on a $a_i \equiv a_j \ (\mathfrak{a}_i + \mathfrak{a}_j)$ pour tous i, j), il faut et il suffit que, dans M, chacune des deux lois de composition sup, inf soit distributive par rapport à l'autre ("Théorème Chisnois"). On pourra procéder de la façon suivante :

a) Si on a $(\mathfrak{a}_1 \cap \mathfrak{a}_2)+(\mathfrak{a}_1 \cap \mathfrak{a}_3) = \mathfrak{a}_1 \cap (\mathfrak{a}_2 + \mathfrak{a}_3)$ le système de trois congruences $x \equiv a_i \ (\mathfrak{a}_i)$ admet une solution si celles-ci sont deux à deux compatibles (si x_{12} et x_{13} sont solutions des congruences d'indices 1,2 et 1,3 respectivement, montrer que les congruences $x \equiv x_{12} \ (\mathfrak{a}_1 \cap \mathfrak{a}_2)$ et $x \equiv x_{13} \ (\mathfrak{a}_1 \cap \mathfrak{a}_3)$ sont compatibles).

b) Si tout système de trois congruences deux à deux compatibles admet une solution, on a les deux formules de distributivité

$\mathfrak{a}+(\mathfrak{b} \cap \mathfrak{c}) = (\mathfrak{a}+\mathfrak{b}) \cap (\mathfrak{a}+\mathfrak{c})$ et $\mathfrak{a} \cap (\mathfrak{b}+\mathfrak{c}) = (\mathfrak{a} \cap \mathfrak{b})+(\mathfrak{a} \cap \mathfrak{c})$.

(pour la première il suffit d'écrire que tout x du second membre est dans le premier, c'est-à-dire de trouver y tel que $y \in \mathfrak{b}$, $y \in \mathfrak{c}$ et $y \equiv x \ (\mathfrak{a})$; pour la seconde montrer que tout x du premier membre est dans le second, c'est-à-d. qu'il existe y tel que $y \in \mathfrak{b}$, $y \in \mathfrak{a}$ et $y \equiv x \ (\mathfrak{c})$). On remarquera que, en vertu de a) et b) la seconde formule de distributivité entraîne la première.

c) Démontrer alors le "théorème chisnois" par récurrence sur n en utilisant une méthode analogue à celle de a).
