CHAPITRE I

THÉORIE ÉLÉMENTAIRE

Dans tout ce cours, un anneau est toujours commutatif à élément unité. Si A et A' sont deux anneaux et si $\varphi: A \to A'$ est un homomorphisme d'anneaux, on suppose que $\varphi(1)=1'$. Soient A' un anneau, A un sous-anneau de A' et $x_1, \ldots, x_n$ des éléments de A'. On désigne par $A[x_1, \ldots, x_n]$ le plus petit sous-anneau de A' contenant A et les x_i.

§1. DIVISIBILITÉ

Soient K un corps, A un sous-anneau de K, K^* le groupe multiplicatif des éléments non nuls de K et $A^* = A-(0)$. Étant donnés x, y dans K^*, on dira que x *divise* y (*par rapport à* A) et l'on écrit $x|y$, s'il existe un élément a dans A tel que $y=ax$. On voit immediatement que les propriétés suivantes sont vérifiées:

(1) $x|x$ pour tout x dans K^*;

(2) si x, y, z sont dans K^* et si $x|y$ et $y|z$, alors $x|z$;

On a ainsi une *relation de préordre* sur l'ensemble K^*. On a encore les propriétés suivantes:

(3) soient z dans K^* et $x,y \in K^*$. Alors
$$x|y \Leftrightarrow xz|yz;$$

(4) soient x,y dans K^*. Alors $x|y \Leftrightarrow y^{-1}|x^{-1}$;

(5) si x,y,y' sont dans K^* et si a,a' sont dans A, alors $x|y$ et $x|y' \Rightarrow x|ay+a'y'$.

Toutes ces propriétés peuvent êtres démontrées très facilement. A partir d'une relation de préordre sur un ensemble, on peut construire une relation d'ordre. On considère la relation $R(x,y)$ sur K^* définie par $x|y$ et $y|x$, et l'on a ainsi une relation d'équivalence sur K^*. Deux éléments x,y dans K^* tels que $R(x,y)$ soit vraie, sont appelés *éléments associés*. On voit que si x et y sont associés, alors $x|z \Leftrightarrow$ $\Leftrightarrow y|z$. Ceci nous montre que deux éléments associés ont les mêmes multiples. Un raisonnement analogue nous montre que deux éléments associés ont les mêmes diviseurs. On remarque encore que

(6) si x,y sont dans K^*, alors $x|y \Leftrightarrow yx^{-1} \in A$.

De là on en déduit que

(7) si x,y sont dans K^*, alors x et y sont associés $\Leftrightarrow yx^{-1}$ est un élément inversible dans l'anneau A.

L'ensemble U des éléments inversibles de A est un groupe pour la multiplication et donc, U est un sous-groupe de K^*. La relation d'association est la relation de congruence modulo le sous-groupe U. La multiplication de K est compatible avec la relation de préordre ci-dessus (cf. propriété (3)) et ceci en fait de U un *groupe préordonné*. Par passage au quotient, la relation de préordre dans K^* va donner une relation de préordre sur K^*/U. En effet, si $\bar{x}$ et $\bar{y}$ sont dans K^*/U, on posera $\bar{y} \leq \bar{x} \Leftrightarrow x|y$. Cette définition est indépendante des representants, car si x' et y' sont deux autres representants, alors x et x' sont associés et y et y' sont aussi associés. Donc, $x'|x$, $x|y$ et $y|y'$ nous donne $x'|y'$. Il est très facile de voir qu'on obtient ainsi une vraie relation d'ordre sur K^*/U qui en fait de K^*/U un groupe ordonné. La théorie de la divisibilité se présente ainsi comme un cas particulier de la théorie des groupes ordonnés.

EXEMPLES DE LA RELATION D'ASSOCIATION - Ceci équivaut à la determination du groupe U des unités.

(1) Soit $A=\mathbf{Z}$ l'anneau des entiers rationnels. Alors $U=\{-1,+1\}$; autrement dit deux éléments associés sont égaux ou opposés.

(2) Soient k un corps et $A=k[X]$ l'anneau des polynômes en X à coefficients dans k. Un polynôme est inversible dans A si et seulement si il se réduit à une constante $\neq 0$ et donc, $U=k^*$. Deux polynômes associés sont deux polynômes proportionnels. Plus généralement, soient A un anneau intègre, $B=A[X_1,\dots,X_n]$ et $U(B)$ le groupe des éléments inversibles de B. Alors on a $U(B)=U(A)$.

(3) Soient A un anneau intègre et $C=A[[X_1,\dots,X_n]]$. On voit que $U(C)$ est l'ensemble des séries formelles dont le terme constant est inversible dans A. En effet, si f est dans C, on peut écrire $f=a_0+a_1(X)+\dots+a_q(X)+\dots$ où $a_q(X)$ est un polynôme homogène de degré q en les indeterminées $X_1,\dots,X_n$. Si $g=b_0+b_1(X)+\dots$ est l'inverse de f, alors $fg=1 \Rightarrow a_0b_0=1$ et donc, a_0 est inversible dans A. Réciproquement, si a_0 est inversible dans A, la série formelle $t(X)=$ $=a_0^{-1}(f(X)-a_0)=a_0^{-1}f(X)-1$ est sans terme constant et donc, $1+t(X)$ est inversible dans C (elle admet $1-t+t^2-t^3+\dots$ comme inverse). Alors, il en est de même de $f(X)=a_0(1+t(X))$.

(4) Si $A=\mathbf{Z}[i]$, alors $U=\{+1,-1,i,-i\}$ est l'ensemble des $p+qi$ dans A tels que $p^2+q^2=1$. L'inverse de $p+qi$ est $p-qi$.

(5) Si $A=\mathbf{Z}[\sqrt{2}]$, alors U est l'ensemble des puissances de $1+\sqrt{2}$ et de leurs opposés.

PLUS GRAND COMMUM DIVISEUR (*pgcd*) ET PLUS PETIT COMMUM MULTIPLE (*ppcm*).

Étant donnés x et y dans K^*, on dira qu'un élé-

ment z dans K^* est *un pgcd de x et y* si $z|x$ et $z|y$ et, d'autre part, si $z'|x$ et $z'|y$ avec z' dans K^*, alors $z'|z$. On dira qu'un élément t dans K^* est *un ppcm de x et y*, si $x|t$ et $y|t$ et, d'autre part, si t' dans K^* est tel que $x|t'$ et $y|t'$, alors $t|t'$. Il en résulte que deux *pgcd* de x et y sont associés et, de même, pour deux *ppcm*. Si z est un *pgcd* de x et y, on notera $z=pgcd(x,y)$ et, de même pour le *ppcm*. Les propriétés suivantes sont vérifiées:

(8) si x et y sont dans K^*, alors

$$x|y \Leftrightarrow pgcd(x,y)=x \Leftrightarrow ppcm(x,y)=y;$$

(9) si $t=pgcd(x,y)$, alors $tz=pgcd(xz,yz)$, ou encore, $pgcd(xz,yz)=z.pgcd(x,y)$; de même, $ppcm(xz,yz)=$ $=z.ppcm(x,y)$;

(10) si x et y ont un *pgcd* z, alors z^{-1} est un *ppcm* de x^{-1} et y^{-1}, ou encore, $pgcd(x,y)^{-1}=ppcm(x^{-1},y^{-1})$; de même, $ppcm(x,y)^{-1}=pgcd(x^{-1},y^{-1})$.

COROLLAIRE 1 - *Deux éléments de K^* ont un pgcd si et seulement si, ils ont un ppcm.*

COROLLAIRE 2 - *Supposons que deux elements x,y de K^* ont un pgcd (donc, aussi un ppcm). Alors*

$$pgcd(x,y).ppcm(x,y)$$

est un élément associé à xy.

En effet, si z est un *pgcd* de x et y, alors $zx^{-1}y^{-1}=$ $=pgcd(y^{-1},x^{-1})=ppcm(x,y)^{-1}$, d'où le corollaire.

Finalement on va démontrer la propriété suivante:

(11) supposons que K soit le corps de fractions de l'anneau intègre A; alors, si deux éléments quelconques de A^* ont un *pgcd* (respectivement, un *ppcm*), alors deux éléments quelconques de K^* ont à la fois un *pgcd* et un *ppcm*.

En effet, d'après le corollaire 1, il suffit de supposer l'existence du *pgcd*. Soient x,y dans K^*, $x=a/c$, $y=b/c$ avec a,b,c dans A^* et soit d un *pgcd* de a et b. Puisque $1|a$ et $1|b$, alors $1|d$ et donc, $d\in A^*$. D'autre part, il est facile de voir que d/c est un *pgcd* de x et y. On remarque que les éléments positifs pour la relation d'ordre sur K^*/U sont les classes d'association d'éléments de A.

Soient K un corps, A un sous-anneau de K et a,b deux éléments de K^*. On dit que a et b sont *étrangers* ou *premiers entre eux* si 1 est un *pgcd* de a et b. Ceci entraîne que a,b sont dans A^*.

THÉORÈME 1 - *Soient a et b étrangers et c dans A^*. Alors $pgcd(a,c)=pgcd(a,bc)$.*

Puisque $pgcd(a,b)=1$, alors $pgcd(ac,bc)=c$ et donc, la relation $z|a$ et $z|c$ équivaut à $z|a$, $z|ac$ et $z|bc$. Comme $a|ac$, ceci équivaut à $z|a$ et $z|bc$. Le théorème est ainsi démontré.

COROLLAIRE 1 - *Soient a et b étrangers et c dans A^*. Alors $a|bc$ entraîne $a|c$.*

En effet, si $a|bc$, alors $a=pgcd(a,bc)$ et d'après le théorème 1, on a $a=pgcd(a,c)$, d'où, $a|c$.

Le corollaire 1 est connu sous le nom de *Lemme d'Euclide*.

COROLLAIRE 2 - *Si a est étranger à b et c, alors a est étranger qu produit bc.*

Comme $1=pgcd(a,b)=pgcd(a,bc)$, alors a est étranger à bc.

COROLLAIRE 3 - *Si $(a_i)_{i\in I}$ et $(b_j)_{j\in J}$ sont deux familles finies telles que pour toute couple d'indices i,j ont ait a_i étranger à b_j, alors $\prod_i a_i$ est étranger à $\prod_j b_j$.*

En effet, la démonstration se fait par double récurrence sur *Card*(I) et *Card*(J).

COROLLAIRE 4 - *Si a et b sont étrangers et si p et*

q sont des éléments de $\mathbf{N}$, alors a^p et b^q sont aussi étrangers.

Le corollaire 4 est un cas particulier du corollaire 3.

§2. DÉFINITION DES ANNEAUX FACTORIELS

Dans ce § et à partir de maintenant, A est un anneau intègre et K est son corps de fractions. On considère le groupe ordonné $F(A)=K^*/U$ et on aimerait que $F(A)$ soit le groupe ordonné le plus simple possible. On considère pour cela la somme directe ordonnée $\mathbf{Z}^{(I)}$, ensemble des familles d'entiers $(n(i))_{i\in I}$ où $n(i)=0$, sauf pour un nombre fini d'indices i dans I. On peut définir dans $\mathbf{Z}^{(I)}$ une structure de groupe par addition des coordonnées et on introduit dans $\mathbf{Z}^{(I)}$ une relation d'ordre (qui n'est pas une relation d'ordre totale), en posant $(p(i))_{i\in I}\leq(q(i))_{i\in I}$ si $p(i)\leq q(i)$ pour tout i dans I. Cette relation d'ordre est compatible avec la structure de groupe de $\mathbf{Z}^{(I)}$.

THÉORÈME 2 - *Soit G un groupe ordonné. Les conditions suivantes sont équivalentes:*

(1) *G, en tant que groupe ordonné, est isomorphe à $\mathbf{Z}^{(I)}$;*

(2) (a) *il existe une famille P d'éléments >0 de G telle que tout élément x dans G, $x\geq 0$, s'écrit d'une façon et d'une seule sous la forme $x=\sum_{p\in P}x(p).p$, où les $x(p)$ sont dans $\mathbf{N}$ et $x(p)=0$, sauf un nombre fini d'entr'eux*; (b) *tout élément de G est difference de deux éléments ≥ 0;*

(3) (a) *condition (M) - tout ensemble $\neq\emptyset$ d'éléments ≥ 0 de G admet un élément minimal;* (b) *deux éléments quelconques de G ont une borne inférieure (resp., supérieure);*

(4) (a) *condition (M);* (b) *si p est un élément extremal de G (voir ci-dessous la définition d'élément extremal) et si $x\geq 0$ et $y\geq 0$ sont deux éléments de G, alors $p\leq x+y$ entraîne $p\leq x$ ou $p\leq y$;* (c) *tout élément de G est difference de deux éléments ≥ 0.*

On remarque tout d'abord que le groupe G est noté additivement. On passe à la démonstration.

(1) $\Rightarrow$ (2)

Si $G=\mathbf{Z}^{(I)}$, à tout j dans I on fait correspondre l'élément $a_j=(\delta_{i,j})_{i\in I}$ où $\delta_{i,j}$ est le symbole de Kronecker (fonction caracteristique de la diagonale). Pour tout x dans G, $x\geq 0$, on a $x=\sum_{j\in I}n(j).a_j$. Il est facile à voir que tout élément de G est difference de deux éléments ≥ 0.

(2) $\Rightarrow$ (3)

Soit $F\neq\emptyset$ une famille d'éléments ≥ 0 de G et soit $x=\sum_{p\in P}n(p).p$ un élément ≥ 0 de F. Les éléments y dans G qui obéissent à la condition $0\leq y\leq x$ sont en nombre fini, ce nombre étant $\prod_{p\in P}(n(p)+1)$ et donc, cet ensemble fini admet un élément minimal qui est aussi un élément minimal de F. D'autre part, si $x=\sum_{p\in P}n(p).p$ et $y=\sum_{p\in P}m(p).p$ sont deux éléments quelconques de G, on a $inf(x,y)=\sum_{p\in P}inf(n(p),m(p)).p$ et donc, deux éléments quelconques de G ont un *inf* (resp. un *sup*).

(3) $\Rightarrow$ (4)

On dit qu'un élément p dans G est un *élément extremal de G* s'il est un élément minimal dans l'ensemble des éléments >0 de G. D'après la condition (M), il existe des éléments extremaux de G. Soit p un élément extremal de G et soient $x\geq 0$ et $y\geq 0$ des éléments de G. Supposons que $p\leq x+y$ et que $p\not\leq x$. Alors $inf(p,x)\geq 0$, $inf(p,x)\leq p$ et $inf(p,x)\neq p$ (car, sinon $p\leq x$) et donc, $inf(p,x)=0$. Comme $p\leq x+y$ et $p\leq p+y$ (car, $y\geq 0$), alors il en resulte que $p\leq inf(p+y,x+y)=y$. La partie (c) est triviale.

(4) $\Rightarrow$ (2)

Soit x un élément quelconque de G et soient $x^+=$

$=sup(0,x)$ et $x^- = sup(0,-x)$. On voit que x^+ et x^- sont des éléments positifs et que $x = x^+ - x^-$ et donc, il suffit de démontrer l'assertion pour des éléments positifs de G. Soit F l'ensemble des éléments ≥ 0 de G qui ne sont pas sommes d'éléments extremaux et supposons que $F \neq \emptyset$. Soit y dans F un élément minimal de F (d'après (a) - condition (M)). On peut supposer que $y \neq 0$ (car 0 est somme de la famille vide d'éléments extremaux) et on considère la famille des z dans G tels que $0 < z \leq y$. Cette famille est $\neq \emptyset$ et soit p un élément minimal de cette famille. Alors p est un élément extremal et comme $p \leq y$, alors on peut écrire $y = p + z$ avec $z > 0$ et $z \notin F$ (car $z < y$). Donc z est somme d'éléments extremaux et il en est de même de y. Ceci nous montre que $F = \emptyset$. On a ainsi démontré l'existence de la décomposition. Pour l'unicité, supposons que l'on a $x = \sum_{p \in P} x(p).p = \sum_{p \in P} x'(p).p$ et l'on va montrer que $x(p) = x'(p)$ pour tout p dans P en faisant une récurrence sur la somme $\sum_{p \in P} x(p)$. Si l'on a $\sum_{p \in P} x(p) = 0$, alors $x(p) = 0$ pour tout p dans P et donc, $x = 0$. Ceci nous montre que $x'(p) = 0$ pour tout p dans P (sinon il en existe un $x'(p) > 0$ et donc, $x > 0$). Soit q dans P tel que $x(q) > 0$. Alors $q \leq x$ et comme $x = \sum_{p \in P} x'(p).p$, alors il en existe un p dans P tel que $x'(p) > 0$ et $q \leq p$. Comme q et p sont extremaux, alors $q = p$ et donc, $x'(q) > 0$. On peut alors retrancher q dans les deux membres de $\sum_{p \in P} x(p).p = \sum_{p \in P} x'(p).p$ et on applique l'hypothèse de récurrence.

(2) $\Rightarrow$ (1)

On sait que tout x dans G s'écrit d'une façon unique $x = \sum_{p \in P} x(p).p$ et donc, on peut définir un homomorphisme $\varphi : G \longrightarrow \mathbf{Z}^{(P)}$ en posant $\varphi(x) = (x(p))_{p \in P}$ pour tout x dans G. Il est facile de voir que φ est une bijection et donc, $G \cong \mathbf{Z}^{(P)}$.

REMARQUES

(1) On peut se demander si l'homomorphisme $G \cong \mathbf{Z}^{(I)}$ est unique. Oui, avec la structure de groupe ordonné, cet homomorphisme est unique mais sans cette structure, il en n'est pas ainsi. En effet, si l'on prend $\mathbf{Z}^2$, en tant que groupe il peut être engendré par $(0,1)$ et $(1,0)$ ou encore par $(0,1)$ et $(1,1)$, par exemple. Il y a une infinité de couples qui engendrent $\mathbf{Z}^2$ en tant que groupe: si (x,y) est un tel couple, alors tout autre couple (x',y') est donnée par $x' = ax + by$ et $y' = a'x + b'y$ avec $ab' - a'b = \pm 1$ (groupe unimodulaire).

(2) Si G vérifie les conditions équivalentes du théorème 2, alors la famille P de la condition (2) est nécessairement celle de tous les éléments extremaux de G. En effet, soit P' la famille de tous les éléments extremaux de G. Alors la démonstration de (4) $\Rightarrow$ (2) nous montre que P' vérifie (2). Soit P une famille qui vérifie (2) et soit x dans P. Alors il existe un élément extremal p dans P' tel que $p \leq x$ et si l'on applique (2) relativement à la famille P, on peut écrire $p = \sum_{y \in P} n(y).y$ avec $n(y)$ dans $\mathbf{N}$ et nuls sauf un nombre fini d'entre eux. On peut encore écrire $x - p = \sum_{y \in P} m(y).y$ et donc $x = \sum_{y \in P} (n(y) + m(y)).y$. D'après l'unicité de la décomposition, il en resulte que $1 = n(x) + m(x)$ et $0 = n(y) + m(y)$ por tout $y \neq x$. Ceci nous montre que $n(y) = 0$ pour tout $y \neq x$ et comme $n(x) \neq 0$, alors $n(x) = 1$. Donc, $x = p$, c'est à dire, $P \subset P'$. Soit p dans P' et on écrit $p = \sum_{y \in P} n(y).y$; il existe un y dans P tel que $n(y) > 0$ et donc, $y \leq p$. Mais y et p étant extremaux dans P', il en resulte que $p = y \in P$, c'est à dire, $P' \subset P$. On a ainsi montré que $P = P'$.

DÉFINITION 1 - *Soient A un anneau intègre, K son corps de fractions et $F(A) = K^*/U$. On dira que A est un anneau factoriel si $F(A)$ en tant que groupe ordonné satisfait aux conditions équivalentes du théorème 2.*

La condition (c) de (4) équivaut à dire que K est le corps de fractions de A (ici on est en notation multiplicative et dans le théorème 2, en notation additive). La condition (2) se traduit par la condition suivante: (2)' il existe une famille P d'éléments non inversibles de A telle que tout x dans A s'écrit de façon unique $x = u \prod_{p \in P} p^{v_p(x)}$ avec u dans U et $v_p(x)$ dans $\mathbf{N}$ et nuls, sauf un nombre fini d'entr'eux.

DÉFINITION 2 - *On dit qu'un élément p de A est extremal ou irreductible si $x \in A$ et $x | p$, entrainent que ou*

bien x est associé à 1 ou bien x est associé à p. On dira alors que P est un système représentatif d'éléments extremaux de A.

EXEMPLES

(1) L'ensemble P des nombres premiers >0 est un système représentatif d'éléments extremaux de l'anneau $\mathbf{Z}$.

(2) Soient k un corps et $A=k[X]$ l'anneau de polynômes en X à coefficients dans k. L'ensemble P des polynômes unitaires irreductibles est un système représentatif d'éléments extremaux de A.

La condition (3) se traduit en la condition suivante: (3)′ (a) *condition* (M) - toute famille $F\neq\emptyset$ d'éléments de A admet un élément minimal (par la relation de divisibilité), c'est à dire, il existe $a\in F$ tel que pour tout x dans A tel que $x|a$, alors x est associé à a; (b) deux éléments quelconques ont un *pgcd* (resp. un *ppcm*). Quant à la condition (4), elle se traduit par la condition suivante: (4)′(a) condition (M) comme ci-dessus; (b) si p est un élément extremal de A et si x,y sont dans A, alors $p|xy \Rightarrow p|x$ ou $p|y$. Un tel élément p de A sera dit un élément premier de l'anneau A. Précisement, un élément p de A est dit un *élément premier* si toutes les fois que p divise un produit de deux éléments de A, alors p divise un des facteurs. Il est clair que tout élément premier est extremal, mais dans un anneau intègre quelconque, un élément peut-être extremal sans être premier.

EXEMPLES D'ANNEAUX FACTORIELS ET NON FACTORIELS

(1) Tout corps est un anneau factoriel, comme il est trivial de vérifier.

(2) L'anneau $\mathbf{Z}$ des entiers rationnels est un anneau factoriel (cf. théorème 3 ci-dessous).

(3) Si A est un anneau factoriel, alors $A[X]$ est aussi un anneau factoriel (cf. Théorème de Gauss, Chap. II).

(4) Tout anneau local régulier est factoriel (cf. M. Auslander and D. A. Buchsbaum, Unique factorization in regular local rings, Proc. Nat. Ac. Sc. USA 45 (1959), 733-734).

(5) Si A est un anneau factoriel, alors $A[[X]]$ n'est pas nécessairement factoriel (cf. P. Samuel, On unique factorization domains, Illinois J. Math. 5 (1961), 3-17 et Pierre Samuel, Sur les anneaux factoriels, Bull. Soc. Math. France 89 (1961), 155-173).

(6) Soit A l'ensemble des nombres réels de la forme $a+b\sqrt{10}$ avec (a,b) parcourant $\mathbf{Z}\times\mathbf{Z}$. On va montrer que A n'est pas factoriel. En effet, $(4+\sqrt{10})(4-\sqrt{10})=2.3$ et si l'on démontre que 2 est un élément extremal de A, alors 2 divise un des facteurs, car 2 divise leur produit. Supposons que $2|(4+\sqrt{10})$ (par rapport à A). On peut écrire que $4+\sqrt{10}=2(a+b\sqrt{10})$ et donc, $2a=4$ et $2b=1$, absurde. Ceci nous montre que A n'est pas factoriel. Étant donné $a+b\sqrt{10}$ dans A, on définit la norme comme étant $N(a+b\sqrt{10})=a^2-10b^2$ et il est facile de voir que $N(xy)=N(x).N(y)$ quel que soient x et y dans A. Si 2 n'est pas extremal dans A, alors on peut écrire $2=xy$ avec x,y dans A et donc, $4=N(2)=N(x).N(y)$ et comme $N(x)$ et $N(y)$ ne sont pas triviales, alors on a $N(x)=N(y)=\pm 2$. Il suffit donc de montrer que l'équation $a^2-10b^2=\pm 2$ n'est pas possible. On a immediatement $a^2\equiv\pm 2 \pmod{10}$ et donc, a^2 est un carré dont les chiffres des unités est 2 ou 8, ce qui n'est pas possible. On a ainsi montré que 2 est un élément extremal.

(7) Soit A l'ensemble des nombres complexes de la forme $a+b\sqrt{-5}$ où (a,b) parcourt $\mathbf{Z}\times\mathbf{Z}$. On montre que 3 est un élément extremal de A et comme $3.3=(2+\sqrt{-5})(2-\sqrt{-5})$, alors A n'est pas factoriel.

THÉORÈME 3 - *L'anneau $\mathbf{Z}$ est factoriel.*

Il s'agit de démontrer que tout nombre $n>1$ est, de façon unique, produit de puissances de nombres premiers, un nombre premier p et $\mathbf{Z}$ étant celui qui n'a pas d'autres associés que 1 et p. La démonstration se fait par récurrance sur n, le cas $n=2$ étant trivial. Supposons donc que $n>2$ et que $n=pp_2\dots p_r=qq_2\dots q_s$ où les p,q,p_i et q_j sont premiers. Si $p=q$ on simplifie par p et d'après l'hypothèse de récurrence, on a l'unicité de la décomposition. Si $p\neq q$, par exemple $p<q$ (on peut toujours se borner à ce cas) alors $n=pa=qb$ et comme $p<q$, alors $b<a$. Donc, $(q-p)b=p(a-b)$ et d'après l'hypothèse de récurrence p figure dans l'unique décomposi-

tion de $(q-p)b$ en facteurs premiers (car, $(q-p)b<n$). Ceci nous montre que $p|(q-p)$ ou bien $p|b$. Si $p|(q-p)$ comme $p|p$, alors $p|((q-p)+p)=q$, impossible, car q est premier. Donc, $p|b=q_2\dots q_s<n$. D'après l'hypothèse de récurrence, p est l'un des q_j et nous sommes ainsi dans le 1er cas. Cette démonstration est dûe à Zermelo.

Formulaire des anneaux factoriels

Soient A un anneau factoriel, K son corps de fractions et P un système représentatif d'éléments extremaux de A. Tout élément x dans K^* s'écrit d'une seule façon sous la forme $x=u\prod_{p\in P} p^{v_p(x)}$ où les $v_p(x)$ sont dans $\mathbf{Z}$ pour tout $p\in P$ et nuls sauf un nombre fini d'entr'eux et où $u\in U$ est un élément inversible. Les fonctions $v_p: K^*\longrightarrow \mathbf{Z}$ ont les propriétés suivantes:

(1) $v_p(xy)=v_p(x)+v_p(y)$ pour tout $p\in P$.

Cette propriété se démontre très facilement.

(2) $v_p(x+y)\geq min\,(v_p(x),v_p(y))$ pour tout p dans P.

En effet, on sait qu'on peut écrire

$$x=u\prod_{p\in P} p^{v_p(x)} \quad \text{et} \quad y=v\prod_{p\in P} p^{v_p(y)}$$

et pour chaque p, on pose $n_p=min\,(v_p(x),v_p(y))$. On remarque que $u,v\in U$ sont des éléments inversibles. On peut donc écrire $v_p(x)=n_p+a_p$ et $v_p(y)=n_p+b_p$ et donc,

$$x+y=(\prod_{p\in P} p^{n_p})(u\prod_{p\in P} p^{a_p}+v\prod_{p\in P} p^{b_p}).$$

On voit que $z=u\prod_{p\in P} p^{a_p}+v\prod_{p\in P} p^{b_p}$ est tel que $v_p(z)\geq 0$ pour tout $p\in P$, car $z\in A$ et donc, $v_p(x+y)\geq n_p$ pour tout $p\in P$. Une telle fonction $v_p: K^*\longrightarrow \mathbf{Z}$ avec les propriétés (1) et (2) s'appele une *valuation* (discrète) *de* K, si l'on pose $v_p(0)=+\infty$ pour tout p dans P. La valuation v_p s'appele encore la *valuation p-adique*. On voit encore que

$$x\in A \Leftrightarrow v_p(x)\geq 0$$

pour tout p dans P et de là on déduit que

$$x|y \Leftrightarrow v_p(x)\leq v_p(y)$$

pour tout $p\in P$.

Il en resulte que

$$v_p(pgcd(x,y))=min(v_p(x),v_p(y))$$

et que $v_p(ppcm(x,y))=max(v_p(x),v_p(y))$ pour tout p dans P.

§3. ANNEAUX PRINCIPAUX

1. Idéaux et divisibilité

Étant donné un anneau commutatif à élément unité, on appele *idéal de* A à toute partie $\mathfrak{a}$ de A telle que $\mathfrak{a}$ est un sous-groupe additif de A et pour tout x dans A et t dans $\mathfrak{a}$, $tx\in\mathfrak{a}$. Ceci étant, si A est un anneau intègre et K est son corps de fractions, on peut généraliser la notion d'idéal de la façon suivante: on dit qu'une partie I de K est un *idéal fractionnaire de* A si I est un sous-groupe additif de K et si pour tout x dans I et a dans A, on a $ax\in I$. Dans ce cas, les idéaux définis ci-dessus sont appelés *idéaux entiers*. Pour tout x dans K, l'idéal fractionaire $Ax=\{ax\in K\,|\,a\in A\}$ est appelé *idéal principal fractionnaire* de l'anneau A. On remarque que toute intersection finie d'idéaux fractionnaire est encore un idéal fractionnaire. Étant donnés $x,y\in K$, pour que x et y aient un *ppcm* $\Leftrightarrow$ que $Ax\cap Ay$ soit un idéal principal. Il est facile de voir que

$$x|y \Leftrightarrow Ax\supset Ay.$$

La condition (M) est équivalente à la condition suivante: tout ensemble $\neq\emptyset$ d'idéaux principaux entiers de A admet un élément maximal (pour la relation d'inclusion).

2. Anneaux noethériens

On dira qu'un anneau A commutatif à élément unité (pas nécessairement intègre) est un *anneau noethérien* si tout ensemble $\neq\emptyset$ d'idéaux de A admet un élément maxi-

mal (pour la relation d'inclusion). On voit que cette condition est plus forte que la condition (M), c'est à dire, condition noethérienne $\Rightarrow$ condition (M). La réciproque n'est pas vraie. En effet, il suffit de prendre $A = K \times V$ muni de

$$(a,x)(b,y) = (ab, ax+by),$$

où V est un K-espace vectoriel (K est un corps) de dimension infinie (donc, en tant que K-module, V n'est pas noethérien). Les idéaux principaux de A distincts de A sont les sous-espaces vectoriels de V de dimension 1 et donc, la condition (M) est vérifiée.

THÉORÈME 4 - *Soit A un anneau commutatif. Alors, les conditions suivantes sont équivalentes:*

(1) *A est un anneau noethérien;*

(2) *toute suite croissante d'idéaux de A est stationnaire, c'est à dire, si $\mathfrak{a}_1 \subset \ldots \subset \mathfrak{a}_n \subset \ldots$ est une suite croissante d'idéaux de A, alors il existe un entier q tel que $\mathfrak{a}_q = \mathfrak{a}_{q+1} = \ldots$;*

(3) *tout idéal de A admet système fini de générateurs, c'est à dire, si $\mathfrak{a}$ est un idéal de A alors il existe des éléments $a_1, \ldots, a_n$ dans A tels que $\mathfrak{a} = Aa_1 + \ldots + Aa_n$.*

(1) $\Leftrightarrow$ (2)

L'équivalence entre (1) et (2) vient du lemme suivant:

LEMME - *Soit E un ensemble ordonné. Les conditions suivantes sont équivalentes:* (a) *toute partie non $\emptyset$ de E admet un élément maximal;* (b) *toute suite croissante d'éléments de E est stationnaire.*

(a) $\Rightarrow$ (b)

Soit $a_1 \leq a_2 \leq \ldots \leq a_n \leq \ldots$ une suite croissante d'éléments de E et soit a_q un élément maximal (d'après (a)) de l'ensemble de tels éléments a_i. A cause de la croissance, pour tout $n \geq q$, on a $a_n \geq a_q$, et donc $a_n = a_q$ pour tout $n \geq q$, d'après la maximalité de a_q.

(b) $\Rightarrow$ (a)

Pour cela, on va démontrer que "non (a)" entraîne "non (b)". Supposons donc qu'il existe une partie F de E, $F \neq \emptyset$ telle que F n'a pas d'élément maximal. Étant donné a_1 dans F, il existe a_2 dans F tel que $a_1 < a_2$ et ce processus peut continuer aussi longtemps qu'on veut, car F n'a pas d'élément maximal.

(1) $\Rightarrow$ (3)

Soit $\mathfrak{a}$ un idéal de A et pour toute partie finie F de $\mathfrak{a}$, soit $\mathfrak{a}_F$ l'idéal de A engendré par F; $\mathfrak{a}_F$ est l'ensemble des combinaisons linéaires d'éléments de F et donc, $\mathfrak{a}_F \subset \mathfrak{a}$. D'après (1), la famille de tous ces $\mathfrak{a}_F$ admet un élément maximal $\mathfrak{a}_G \subset \mathfrak{a}$ et si l'on suppose que $\mathfrak{a}_G \neq \mathfrak{a}$, alors il existe un $a \in \mathfrak{a}$ tel que $a \notin \mathfrak{a}_G$. L'idéal $\mathfrak{b} = \mathfrak{a}_G + Aa = \mathfrak{a}_{G \cup \{a\}}$ contient strictement $\mathfrak{a}_G$, car a est dans $\mathfrak{b}$ et a n'est pas dans $\mathfrak{a}_G$ et ceci contredit la maximalité de $\mathfrak{a}_G$.

(3) $\Rightarrow$ (2)

Soit

$$\mathfrak{a}_1 \subset \ldots \subset \mathfrak{a}_n \subset \ldots (*)$$

une suite croissante d'idéaux de A et soit $\mathfrak{a} = \bigcup_{n=1}^{\infty} \mathfrak{a}_n$. Puisque la suite $(*)$ est croissante, il en resulte que $\mathfrak{a}$ est un idéal de A (en général une réunion d'idéaux n'est pas un idéal: on n'a que prendre dans l'anneau $k[X_1, X_2]$, où k est un corps, les idéaux (X_1) et (X_2) et vérifier que $(X_1) \cup (X_2)$ n'est pas un idéal de $k[X_1, X_2]$ ce qui est facile à voir). D'après (3), l'idéal $\mathfrak{a}$ admet un système fini de générateurs $x_1, \ldots, x_q$ et chaque x_i est dans un $\mathfrak{a}_{n(i)}$. Si l'on pose $n = max(n(1), \ldots, n(q))$, alors $x_i \in \mathfrak{a}_n$ $(i = 1, \ldots, q)$ et donc, $\mathfrak{a} \subset \mathfrak{a}_n$. D'autre part, $\mathfrak{a}_n \subset \mathfrak{a}$ et donc, $\mathfrak{a}_n = \mathfrak{a}$. Pour tout $p \geq n$, on a $\mathfrak{a} = \mathfrak{a}_n \subset \mathfrak{a}_p \subset \mathfrak{a}$ et ceci nous montre que $\mathfrak{a}_n = \mathfrak{a}_p$ pour tout $p \geq n$.

3. ANNEAUX PRINCIPAUX

On dit qu'un anneau A est *principal*, s'il est intègre et si tout idéal entier de A est principal. On voit que

"principal" $\Rightarrow$ "noethérien" $\Rightarrow$ "condition (M)" et donc, la condition (M) est vérifiée pour les anneaux principaux. D'autre part, deux éléments quelconques $a,b \in A$ ont un *ppcm*. En effet, $Aa \cap Ab$ est principal. Il en resulte donc du théorème 2 le théorème suivant:

THÉORÈME 5 - *Tout anneau principal est factoriel.*

THÉORÈME 6 - *Soient A un anneau principal, K son corps de fractions et $x,y \in K$. Alors, tout pgcd de x et y est un générateur de l'idéal $Ax+Ay$.*

Selon la légende, ce théorème est dû à Bezout. Puisque A est principal, il existe un z dans K tel que $Ax+Ay=Az$ et comme $Ax \subset Az$ et $Ay \subset Az$, alors $z|x$ et $z|y$. Soit $t \in K$ tel que $t|x$ et $t|y$. Ceci équivaut à $Ax \subset At$ et $Ay \subset At$ et donc, $Az=Ax+Ay \subset At$, d'où, $t|z$.

COROLLAIRE - *Soient a,b dans A. Pour que a et b soient étrangers il faut et il suffit qu'il existent u,v dans A tels que $au+bv=1$ (identité de Bezout).*

EXEMPLES D'ANNEAUX PRINCIPAUX

(1) Un anneau est dit *euclidien* s'il est muni d'une application $\varphi: A^* \to \mathbf{N}$ telle que: (E_1) $\varphi(xy) \geq \varphi(y)$ quel que soient x et y dans A^*; (E_2) étant donnés $a,b \in A^*$, il existe $q,r \in A$ tels que $a=bq+r$, où $r=0$ ou $\varphi(r)<\varphi(b)$. On suppose, de plus, que l'anneau A soit intègre.

PROPOSITION - *Tout anneau euclidien est principal.*

En effet, soit $\mathfrak{a}$ un idéal de A. Ou bien $\mathfrak{a}=(0)$ et donc, $\mathfrak{a}$ est principal, ou bien $\mathfrak{a} \neq (0)$ et à ce moment là, il existe un a dans $\mathfrak{a}$ tel que $\varphi(a)$ soit minimal. Ici, minimal ça veut dire que $\varphi(a)= = min\{\varphi(y) \in \mathbf{N} | y \in \mathfrak{a}\}$. Pour tout x dans $\mathfrak{a}$, on peut écrire $x=aq+r$ avec $r=0$ ou bien $\varphi(r)<\varphi(a)$. D'après la minimalité de $\varphi(a)$, on a $r=0$ et donc, $x=aq$. (On remarque que $r=x-aq \in \mathfrak{a}$ et que $\varphi(r)<\varphi(a)$). On a ainsi montré que $\mathfrak{a}=A\mathfrak{a}$ et donc, que A est principal.

(2) L'anneau $\mathbf{Z}$ des entiers rationnels avec $\varphi(x)=|x|$ pour tout x dans $\mathbf{Z}$ est un anneau euclidien, donc principal.

(3) Soient k un corps de $A=k[X]$. Si l'on pose $\varphi(f)=d^0 f$ pour tout f dans A, alors A est un anneau euclidien, où $d^0(f)$ est le degré du polynôme f.

(4) Soit $A=\mathbf{Z}[i]$ l'anneau des *entiers de Gauss*, c'est à dire, A est l'ensemble des nombres complexes de la forme $a+bi$ avec $(a,b) \in \mathbf{Z} \times \mathbf{Z}$. On va montrer que A est un anneau principal. En effet, pour tout $a+bi$ dans A, on posera $\varphi(a+bi)=a^2+b^2$ et on va montrer que étant donnés x,y dans A^*, il existent q,r dans A tels que $x=qy+r$ avec $r=0$ ou $\varphi(r)<\varphi(y)$. En effet, étant donné x/y dans le corps $\mathbf{C}$ des complexes, il existe q dans A tel que $|(x/y)-q| \leq \sqrt{2}/2<1$ et donc, $|x-yq|<|y|$. Si l'on pose $r=x-yq$, on a ou bien $r=0$ ou alors on a $|r|<|y|$ et donc, en élevant au carré, $\varphi(r)<\varphi(y)$.

(5) L'anneau $A=\mathbf{Z}[\sqrt{2}]$, ensemble des nombres réels de la forme $a+b\sqrt{2}$ avec $(a,b) \in \mathbf{Z} \times \mathbf{Z}$, est un anneau principal, en posant $\varphi(a+b\sqrt{2})=|a^2-2b^2|$ pour tout $(a,b) \in \mathbf{Z} \times \mathbf{Z}$.

(6) Soient k un corps et $A=k[[X]]$. L'anneau A est principal et on peut montrer que les seuls idéaux de A sont (0) et les puissances $(X)^n$.

UNIVERSITÉ DE GRENOBLE I
LABORATOIRE
DE MATHÉMATIQUES PURES