

Notions de Base

§1. Anneaux factoriels.

(R. CHIBLON
F. S. Tekmè)

1. Préliminaires.

1.1. Soit $(A, +, \cdot)$ un anneau. Un ensemble I est dit un idéal à gauche (resp. à droite) de A si I est un s/g de $(A, +)$ et si $\forall n \in I, \forall a \in A : an \in I$ (resp. $na \in I$), I sera dit un idéal bilatère de A si I est à la fois idéal à gauche et idéal à droite de A . Lorsque A est unitaire, I est un idéal bilatère de A si et seulement si I est un s/g de $(A, +)$ et $\forall n \in I, \forall (a, b) \in A^2 : anb \in I$.

1.2. Soit $(A, +, \cdot)$ un anneau commutatif. L'intersection d'une famille quelq. d'idéaux est un idéal de A ; si B est une partie de A , l'intersection de tous les idéaux de A qui contiennent B est un idéal dit "l'idéal engendré par B ", c'est le plus petit élément de l'ensemble, ordonné par l'inclusion, des idéaux de A qui contiennent B , si $B = \{u\}$, l'idéal engendré par B est $(u) = \{au / a \in A\}$ qui est dit l'idéal principal engendré par u .

1.3. Un anneau $(A, +, \cdot)$ est dit intègre s'il est commutatif, unitaire et sans diviseur de 0 (i.e.) $\forall (a, b) \in A^2: ab = 0 \Rightarrow a = 0$ ou $b = 0$).

1.4. Définition.

Soit $(A, +, \cdot)$ un anneau commutatif unitaire. Un élément π de A est dit premier (resp. irréductible) si π est non nul et non inversible et si l'idéal engendré par π , (π) , est premier (i.e.) $(\pi) \neq A$ et $\forall (a, b) \in A^2: ab \in (\pi) \Rightarrow a \in (\pi)$ ou $b \in (\pi)$.

(resp. si $\pi = ab$ alors $a \in U(A)$ ou $b \in U(A)$, où $U(A)$ désigne l'ensemble des éléments inversibles de A).

1.5. Exemple.

Dans $\mathbb{Z}$, les notions d'éléments premiers et d'éléments irréductibles coïncident. Les éléments irréductibles de $\mathbb{Z}$ sont ~~juste~~ les éléments $\pm p$ où p est un nombre premier au sens usuel.

1.6. Proposition.

Soit $(A, +, \cdot)$ intègre. Tout élément π premier est irréductible.

Preuve:

Si $n = a \cdot b$, l'idéal (n) étant premier, donc $a \in (n)$ ou $b \in (n)$, si $a \in (n)$ alors $\exists a_1 \in A$ tel que $a = a_1 n$, donc $n = (a_1 b) n$ (i.e. $n(1 - a_1 b) = 0$), comme $n \neq 0$ et A intègre alors $a_1 b = 1$ (i.e. $b \in U(A)$), et alors n irréductible.

CQFD

1.7. Proposition

$(A, +, \cdot)$ intègre. Soit $n \in A$, il y a équivalence entre:

- 1°) n est irréductible.
- 2°) l'idéal (n) est maximal dans l'ensemble, ordonné par l'inclusion, des idéaux principaux non nuls et distincts de A .
- 3°) l'idéal (n) est maximal, distinct de A , et $\forall y \in A$:
 $(n) \subseteq (y) \implies (y) = (n)$ ou $(y) = A$.

$\ll 2^\circ \stackrel{\text{Def}}{\iff} 3^\circ \gg$

Preuve:

1°) $\implies$ 2°).

Si (y) idéal maximal et $\neq A$ avec $(n) \subseteq (y)$, $\exists y_1 \in A$ tel que $n = y_1 y_2$, or n irréductible, donc $y_1 \in U(A)$ ou $y_2 \in U(A)$, et comme $(y) \neq A$ alors

$y_1 \in U(A)$, donc $y = y_1^{-1}x \in (u) \text{ (ie) } (y) \subseteq (u)$
donc $(u) = (y)$.

2°) $\Rightarrow$ 1°)

Si $u = ab$ et $a \notin U(A)$, on a $(u) \subsetneq (b)$,
donc $(b) = A$ (ie) $b \in U(A)$, comme $(u) \neq (a)$ et
 $(u) \neq A$, u est irréductible.

2. Anneau factoriel.

Dans toute la suite, on suppose que A est
un anneau intègre.

2.1. Définition.

1°) L'anneau A est dit factoriel si

a) Tout élément non nul et non inversible est
produit d'éléments irréductibles.

b) Si $x_1 x_2 \dots x_n = y_1 \dots y_m$, où les x_i et les y_j
sont tous irréductibles, alors $n = m$ et $\exists \sigma \in S_n$
telle que $\forall i \in \{1, \dots, n\}$: x_i et $y_{\sigma(i)}$ sont associés
(ie) $\exists a \in U(A)$ avec $x_i = a y_{\sigma(i)}$.

2°) Un ensemble P d'éléments irréductibles de A est
appelé un ensemble de représentants de classes d'élts
irréductibles associés de A , si tout élément irréductible
de A est associé à un élément de P et si deux éléments
distincts de P ne sont pas associés.

2.2. Remarque.

1°) Soit R la relation d'équivalence sur l'ensemble des éléments irréductibles, définie par :

$$x R y \Leftrightarrow x \text{ et } y \text{ sont associés (i.e.) } \exists a \in U(A) \text{ tq } x = ay).$$

Alors, pour constituer P , on prend de chaque classe d'équivalence un représentant et un seul.

2°) Si $A = \mathbb{Z}$, $P = \{ p \in \mathbb{N} / p \text{ premier} \} = \{ 2, 3, 5, 7, 11, \dots \}$.

2.3. Théorème.

Soit P un ensemble d'éléments irréductibles. Alors il y a équivalence entre :

1°) A est factoriel et P est un ensemble de représentants de classes d'éléments irréductibles associés.

2°) Tout élément non nul x de A , s'écrit de manière unique sous la forme $x = a \cdot \prod_{p \in P} p^{M_p(x)}$ où

$a \in U(A)$ et les entiers $M_p(x)$ sont nuls, sauf pour un nombre fini de $p \in P$.

Preuve :

1°) $\Rightarrow$ 2°) évidente à partir de la définition d'un anneau factoriel et de la définition de l'ensemble P .

2° $\Rightarrow$ 1°. Soit q un élément irréductible de A , donc il existe $p \in P$ et $a_q \in U(A)$ tels que $q = a_q \cdot p$, ainsi q est associé à un élt de P .

D'autre part, si p_1 et p_2 deux éléments de P distincts, et s'ils sont associés, il existe $z \in U(A)$ tel que $p_1 = z \cdot p_2$, donc $p_1 = p_2$ et $z = 1$, absurde. Donc, deux éléments distincts de P ne sont pas associés. Ainsi P est un ensemble de représentants de classes d'éléments irréductibles associés.

• Par hypothèse, tout élément non nul et non inversible est produit d'éléments irréductibles. Soient

$q_1 \dots q_r = u_1 \dots u_s$ deux représentations d'un même élément non nul et non inversible de A comme produit d'éléments irréductibles. Il existe alors p_i (resp. p'_j) ($\forall i \in \{1, \dots, r\}$) (resp. $\forall j \in \{1, \dots, s\}$) dans P tel que $q_i = a_i p_i$ (resp. $u_j = b_j p'_j$) avec a_i (resp. b_j) dans $U(A)$. On a alors $(a_1 \dots a_r)(p_1 \dots p_r) = (b_1 \dots b_s)(p'_1 \dots p'_s)$. L'unicité entraîne alors $r = s$ et l'existence de $\sigma \in S_r$ telle que $p_i = p'_{\sigma(i)}$ (i.e) q_i et $u_{\sigma(i)}$ sont associés. Donc A est factoriel.

C.q.f.d.

2.4. Proposition.

Soit A factoriel, P un ensemble de représentants de classes d'éléments irréductibles associés de A .

Alors :

1°) Si $(x, y) \in A^* \times A^*$ et $p \in P$, on a

$$m_p(xy) = m_p(x) + m_p(y)$$

2°) $(x, y) \in A^* \times A^*$, on a l'équivalence entre :

i) y divise x

ii) $\forall p \in P, m_p(y) \leq m_p(x)$

3°) $\forall (x, y) \in A^* \times A^*$,

x et y ont un pgcd et un ppcm et on a

$$\text{pgcd}(x, y) = \prod_{p \in P} p^{\inf(m_p(x), m_p(y))}$$

$$\text{ppcm}(x, y) = \prod_{p \in P} p^{\sup(m_p(x), m_p(y))}$$

Preuve :

1°) on a $x = a_x \prod_{p \in P} p^{m_p(x)}$ et $y = a_y \prod_{p \in P} p^{m_p(y)}$

$$\text{donc } xy = a_x \cdot a_y \cdot \prod_{p \in P} p^{m_p(x) + m_p(y)}$$

$$\text{et } m_p(xy) = m_p(x) + m_p(y).$$

2°) facile

3°) utiliser 2°) (exercice).

2.5. Lemme de Gauss.

On suppose A factoriel. Si x, y et z sont des éléments non nuls de A . Alors

Si x et y sont premiers entre eux et x divise yz alors x divise z .

Preuve:

Soit $d \in A$ tel que $yz = x \cdot d$, donc
 $yz = a_y \cdot a_z \prod_{p \in P} p^{m_p(y) + m_p(z)} = a_x \cdot d \prod_{p \in P} p^{m_p(x) + m_p(d)}$

d'où $\forall p \in P: m_p(y) + m_p(z) = m_p(x) + m_p(d)$
Comme x et y sont premiers entre eux alors $\forall p \in P:$

$\inf(m_p(x), m_p(y)) = 0$ (i.e) $\forall p \in P:$

$m_p(x) = 0$ ou $m_p(y) = 0$, donc

$\forall p \in P: m_p(z) \geq m_p(x)$ et x divise z .

C.Q.F.D.

2.6. Proposition.

Il y a équivalence entre:

1° A factoriel.

2° Tout élément non nul et non inversible s'écrit comme produit d'éléments irréductibles et le lemme de Gauss est valable dans A .

Preuve:

1°) $\Rightarrow$ 2°) Définition d'un anneau factoriel et (e.5)

2°) $\Rightarrow$ 1°)

Si $x_1, \dots, x_n = y_1 \dots y_m$ où les x_i et les y_j sont tous irréductibles.

Supposons que $\forall j \in \{1, \dots, m\}$, x_1 n'est pas associé à y_j , donc x_1 et $\prod_{j=1}^{m-1} y_j$ sont premiers entre eux, le lemme de Gauss implique que x_1 divise y_m , or x_1 et y_m sont irréductibles, donc x_1 et y_m sont associés, absurde. Donc $\forall i, \exists j$ tels que x_i et y_j sont associés et par suite $n=m$, A est donc factoriel.

C.Q.F.D.

2.2 Théorème.

Il y a équivalence entre:

1°) A est factoriel

2°) i) Toute suite croissante d'idéaux principaux de A est stationnaire.

ii) Tout élément irréductible est premier.

Preuve:

1°) $\Rightarrow$ 2°) i)

Soit $n \in A \setminus \{0\}$, n est de la forme

$n = a_n \cdot \prod_{p \in P} p^{M_p(n)}$, chaque diviseur de n

est associé à un élément de l'ensemble fini
 $\left\{ \prod_{p \in P} p^{\alpha_p} / \forall p \in P : 0 \leq \alpha_p \leq n_p(n) \right\}$,

Or $\forall y \in A$, on a: y divise $n \Leftrightarrow (n) \subseteq (y)$,
donc il n'existe qu'un nombre fini d'idéaux principaux
de A contenant (n) ; ainsi toute suite $\uparrow$ d'idéaux
principaux est stationnaire.

1°) $\Rightarrow$ 2°) ii)

Soit n un élément irréductible de A , donc
 $\exists p_1 \in P$ tel que n soit associé à p_1 , soit
 $(y, z) \in A^2$ avec $yz \in (n) = (p_1)$, donc n
divise yz (ie) $\forall p \in P : n_p(yz) \geq n_p(n)$, or
 $\forall p \in P - \{p_1\} : n_p(n) = 0$ et $n_{p_1}(n) = 1$,
d'où $n_{p_1}(yz) = n_{p_1}(y) + n_{p_1}(z) \geq 1$ et
par suite $n_{p_1}(y) \geq 1$ ou $n_{p_1}(z) \geq 1$ et
 $\forall p \in P : n_p(y) \geq n_p(n)$ ou $n_p(z) \geq n_p(n)$
(ie) n divise y ou n divise z , d'où (n) est
premier.

2°) $\Leftarrow$ 1°)

Supposons qu'il existe x non nul et non inversible de
 A tel qu'il n'est pas produit d'éléments irréductibles,
soit $\mathcal{H} = \{ (y) / y \text{ est un élément de } A \text{ qui n'est pas} \\ \text{produit d'élts irréductibles} \}$

$\mathcal{I}R$ est non vide car $(x) \in \mathcal{I}R$, d'après i) il existe (x_1) élément maximal de $\mathcal{I}R$ qui est ordonné par l'inclusion, l'élément x_1 n'est donc pas un produit d'éléments irréductibles, donc non irréductible, il existe $(y, z) \in A^2$ avec $x_1 = yz$, ainsi $(x_1) \subsetneq (y)$ et $(x_1) \subsetneq (z)$, vu la maximalité de (x_1) dans $\mathcal{I}R$, (y) et (z) ne sont pas dans $\mathcal{I}R$, donc y (resp. z) est produit d'éléments irréductibles, d'où $x_1 = yz$ est produit d'éléments irréductibles, ce qui est absurde, et tout élément non nul et non inversible de A est produit d'éléments irréductibles.

Pour l'unicité, on va la montrer par récurrence sur le nombre minimal de facteurs irréductibles dans une décomposition en éléments irréductibles pour un élément x non nul et non inversible.

Si $m=1$

$x = x_1 = y_1 y_2 \dots y_m$ où x_1 irréductible et
 $\forall i: y_i$ irréductible, x_1 est donc premier et
 $\exists i$ tel $y_i \in (x_1)$, d'où x_1 et y_i sont associés
 et $\prod_{j \neq i} y_j \in U(A)$, donc forcément $m=1$;

On suppose comme hypothèse de récurrence que l'unicité

est vérifié pour $n-1$, Soit alors $x_1 x_2 \dots x_n =$
 $= y_1 y_2 \dots y_m = n$ où les x_i et les y_j sont irréductibles,
donc $x_1 \dots x_n \in (y_1 \dots y_m) \subseteq (y_1)$ qui est premier, donc
 $\exists i$ tel que $x_i \in (y_1)$, or x_i est irréductible et
par suite x_i et y_1 sont associés, en simplifiant par
 x_i on aura $x_1 \dots x_{i-1} x_{i+1} \dots x_n = z_2 y_3 \dots y_m$ avec
 z_2 associé à y_2 , l'H.R. implique que $n-1 = m-1$
(i.e) $n = m$, et de la même façon qu'on a montré que
 x_i et y_i sont associés, on montre l'existence de
 $\sigma \in S_n$ telle que $\forall 1 \leq j \leq n : x_j$ et $y_{\sigma(j)}$ sont
associés, A est donc factoriel.

C.Q.F.D.

2.8. Corollaire.

Tout anneau principal est factoriel.

Preuve:

Soit x irréductible de A , donc (x) est maximal
dans l'ensemble des idéaux principaux de A , distincts
de A ; or tous les idéaux de A sont principaux, donc
 (x) est un idéal maximal de A et par suite (x) est
premier (i.e) x est premier.

D'autre part, si $(x_1) \subseteq (x_2) \subseteq \dots$ est une suite $\nearrow$
d'idéaux principaux de A tous distincts de A , alors

$\bigcup_{i \geq 2} (n_i)$ est un idéal de A , distinct de A ,
 $i \geq 2$ donc il existe $n \in A$ tel que $\bigcup_{i \geq 2} (n_i) = (n)$,
 il existe $m_0 \in \mathbb{N}^*$ avec $n \in (n_{m_0})$ (i.e) $(n) = (n_{m_0})$
 et $\forall m \geq m_0 : (n_m) = (n_{m_0})$.

C.Q.F.D