VII . −Anneau, morphisme ...

VII.1 . −Anneau

Définition VII.1.1 (Anneau) Un *anneau* est un triplet $(A, +, *)$ (le plus souvent noté $A,)$ tel que :

Ann$_1$) $(A, +)$ est un groupe abélien (cf. III.1.3 ;)
et la loi $* : A \times A \to A$ vérifie :

Ann$_2$) pour tout triplet (x, y, z) d'éléments de A,

$$x * (y * z) = (x * y) * z ,$$

(la loi $*$ est *associative*) ;

Ann$_3$) il existe un élément 1_A de A, appelé *élément neutre de* $(A, *)$, (souvent noté 1 lorsque le contexte est clair) tel que, pour tout $x \in A$,

$$1_A * x = x * 1_A = x ;$$

(on supposera toujours que $1_A \neq 0_A$ où 0_A est l'élément neutre pour la loi $+$;)

Ann$_4$) pour tout triplet (x, y, z) d'éléments de A,

$$x * (y + z) = x * y + x * z, \text{ et } (x + y) * z = x * z + y * z ,$$

(la loi $*$ est *distributive* par rapport à la loi $+$.)

On dira aussi que les lois $+$ et $*$ *donnent à l'ensemble* A *une structure d'anneau*.

La loi $+$ est usuellement appelée *addition* et la loi $*$ *multiplication*, par analogie avec l'anneau "modèle" $(\mathbb{Z}, +, *)$. Pour tout couple (x, y) d'éléments de A, on appellera $x+y$ et $x*y$ respectivement *somme* et *produit* de x et y.

On remarque que pour tout $x \in A$,

$$0_A * x = x * 0_A = 0_A .$$

On dit que 0_A est un *élément absorbant*.

Remarque VII.1.2 On aurait pu formuler les axiomes VII.1.1.Ann$_2$) et VII.1.1.Ann$_3$) en disant que $(A, *)$ est un magma associatif possédant un élément neutre (cf. I.6.)

Exemple VII.1.3 Un exemple fondamental qui entrera dans un certain nombre de constructions que nous allons envisager, est constitué par l'anneau $(\mathrm{End}_{\mathbf{Gr}}(G), +, \circ)$ où $(G, +)$ est un groupe abélien. Plus précisément :

Proposition VII.1.4 *Soit $(G, +)$ un groupe abélien (cf. III.1.3.)*

i) L'ensemble $\mathrm{End}_{\mathbf{Gr}}(G) = \mathrm{Hom}_{\mathbf{Gr}}(G, G)$ est un sous-groupe du groupe G^G (cf. III.1.6.)

ii) Le triplet $(\mathrm{End}_{\mathbf{Gr}}(G), +, \circ)$ *est un anneau.*

***Preuve** :*

VII.1.1.Ann$_1$) Le point i) assure que $(\mathrm{End}_{\mathbf{Gr}}(G), +)$ *est un groupe abélien si bien que l'axiome VII.1.1.Ann$_1$) est vérifié.*
Par ailleurs, si f *et* g *sont deux éléments de* $\mathrm{End}_{\mathbf{Gr}}(G)$, $f \circ g$ *est un élément de* $\mathrm{End}_{\mathbf{Gr}}(G)$ *si bien que* $\circ$ *définit bien une loi interne sur* $\mathrm{End}_{\mathbf{Gr}}(G)$. *Reste donc à vérifier les axiomes :*

VII.1.1.Ann$_2$) C'est un résultat connu concernant les applications que la loi $\circ$ *est associative.*

VII.1.1.Ann$_3$) L'élément $\mathrm{Id}_G \in \mathrm{End}_{\mathbf{Gr}}(G)$ *vérifie*

$$f \circ \mathrm{Id}_G \;=\; \mathrm{Id}_G \circ f \;=\; f\,,$$

pour tout $f \in \mathrm{End}_{\mathbf{Gr}}(G)$.

VII.1.1.Ann$_4$) Étant donnés trois éléments f, g, h *de* $\mathrm{End}_{\mathbf{Gr}}(G)$, *pour tout* $x \in G$,

$$\begin{aligned}
[h \circ (f +_{\mathrm{End}_{\mathbf{Gr}}(G)} g)](x) &= h[(f +_{\mathrm{End}_{\mathbf{Gr}}(G)} g)(x)] \\
&= h[f(x) +_G g(x)] \\
&= h[f(x)] +_G h[g(x)] \\
&= (h \circ f)(x) +_G (h \circ g)(x) \\
&= [(h \circ f) +_{\mathrm{End}_{\mathbf{Gr}}(G)} (h \circ g)](x)\,;
\end{aligned}$$

et

$$\begin{aligned}
[(f +_{\mathrm{End}_{\mathbf{Gr}}(G)} g) \circ h](x) &= (f +_{\mathrm{End}_{\mathbf{Gr}}(G)} g)[h(x)] \\
&= (f[h(x)] +_G f[g(x)] \\
&= (f \circ h)(x) +_G (f \circ g)(x) \\
&= [(f \circ h) +_{\mathrm{End}_{\mathbf{Gr}}(G)} (f \circ g)](x)\,.
\end{aligned}$$

Ce qui prouve que $\circ$ *est distributive sur* $+_{\mathrm{End}_{\mathbf{Gr}}(G)}$.

Définition VII.1.5 (Anneau commutatif) Étant donné un anneau $(A, +, *)$, si

$$\forall (x, y) \in A \times A,\; x * y \;=\; y * x$$

on dira que la loi $*$ est *commutative* ou encore que l'anneau $(A, +, *)$ est un *anneau commutatif.*

Exemple VII.1.6 a) L'ensemble $\mathbb{Z}$ des entiers relatifs étudié au chapitre IV, muni de ses opérations $+$ et $*$ est un anneau commutatif.

b) La relation $\sim_n$ de *congruence* modulo n (cf. TD n° IV, exercice B,) est compatible à la multiplication *i.e.* pour tout $(a, b) \in \mathbb{Z} \times \mathbb{Z}$, et $(a', b') \in \mathbb{Z} \times \mathbb{Z}$, si

$$a \sim_n a' \text{ et } b \sim_n b' ,$$

alors

$$ab \sim_n a'b' .$$

Ce qui permet de définir une multiplication $*_{\mathbb{Z}/n\mathbb{Z}}$ sur l'ensemble $\mathbb{Z}/n\mathbb{Z}$ des classes modulo n par :

$$\overline{a} *_{\mathbb{Z}/n\mathbb{Z}} \overline{b} = \overline{a * b} .$$

Le triplet $(\mathbb{Z}/n\mathbb{Z}, +_{\mathbb{Z}/n\mathbb{Z}}, *_{\mathbb{Z}/n\mathbb{Z}})$, le plus souvent noté $\mathbb{Z}/n\mathbb{Z}$, est un anneau commutatif.

$(\mathbb{Z}/n\mathbb{Z}, *)$ n'est jamais un groupe.

c) On dira qu'une fonction $f : \mathbb{R} \to \mathbb{R}$ est *à support compact*, s'il existe un intervalle $[a; b] \subset \mathbb{R}$ (*i.e.*un sous ensemble compact de $\mathbb{R}$,) tel que pour tout $x \notin [a; b]$, $f(x) = 0$. L'ensemble $\mathcal{C}$ des fonctions continues à support compact, muni de l'addition :

$$\begin{array}{rccl} + : & \mathcal{C} \times \mathcal{C} & \to & \mathcal{C} \\ & (f, g) & \mapsto & f + g \mid (f + g)(x) := f(x) + g(x)\ \forall x \in \mathbb{R}, \ ; \end{array}$$

et de la multiplication :

$$\begin{array}{rccl} * : & \mathcal{C} \times \mathcal{C} & \to & \mathcal{C} \\ & (f, g) & \mapsto & f * g \mid (f * g)(x) := f(x) * g(x)\ \forall x \in \mathbb{R}, \ ; \end{array}$$

n'est pas un anneau au sens de la définition VII.1.1. En effet, $\mathcal{C}$ ne possède pas d'élément neutre pour la multiplication $*$ et ne vérifie donc pas l'axiome VII.1.1.Ann$_3$).

Dans la suite de ce cours, nous n'aurons pas à considérer de tels objets, ce qui nous a incité à donner une définition d'anneau plus restrictive à laquelle satisferont tous les objets de notre étude. Les anneaux que nous considérerons sont parfois appelés *anneaux unifères*.

Les propositions I.6.13 et III.1.4 s'étendent encore au cas des anneaux. On peut en effet remarquer qu'un anneau est un magma à la fois pour sa loi d'addition $+$ ainsi que pour sa loi de multiplication $*$ si bien que :

Proposition VII.1.7 (Propriétés) *Soient $(A, +, *)$ un Anneau. Le couple $(A, +)$ est en particulier un groupe abélien si bien que :*

i) L'élément neutre 0_A pour la loi $+$ est unique.

ii) Tout élément de A possède un unique opposé pour la loi $+$.

iii) L'élément neutre 1_A pour la loi $*$ est unique.

iv) Un élément de A possède au plus un symétrique pour la loi $*$ qu'on appellera inverse.

Définition VII.1.8 (Élément inversible) Tous les éléments d'un anneau A différents de 0_A ne possédant pas nécessairement un inverse pour la loi $*$, on notera $A^\times$ l'ensemble des éléments de A *inversibles* pour $*$ *i.e.* ceux qui possèdent un inverse. On appelle parfois également *unité* un élément de $A^\times$.

Proposition VII.1.9 *Si A est un anneau (resp. un anneau commutatif) $(A^\times, *)$ est un groupe (resp. un groupe abélien.)*

***Preuve** : Voir l'exercice VII.8.1.*

Exemple VII.1.10 a) Le groupe $(\mathbb{Z}^\times, *)$ des inversibles de $\mathbb{Z}$ est $(\{-1, 1\}, *)$ (cf. IV.3.14,) qui est isomorphe au groupe abélien $\mathbb{Z}/2\mathbb{Z}$.

b) Pour un $\mathbb{K}$-espace vectoriel V l'ensemble $\mathrm{End}(V)$ des endomorphismes de V est un anneau dont le groupe des inversibles $\mathrm{End}(V)^\times$ est le *groupe linéaire* $\mathrm{GL}(V)$.

Définition VII.1.11 (Anneau intègre) Si $(A, +, *)$ est un anneau tel que

$$\forall x \in A,\ \forall y \in A,\ (x * y = 0 \Rightarrow x = 0 \vee y = 0),$$

on dit que A est un anneau *intègre*.

Définition VII.1.12 (Corps) Un anneau commutatif $(A, +, *)$ est un *corps* si tous les éléments de A différents de 0_A possèdent un inverse pour la loi $*$; *i.e.* $A^\times = A \setminus \{0_A\}$.

Remarque VII.1.13 Un corps est un anneau intègre mais la réciproque est fausse. En effet l'anneau $(\mathbb{Z}, +, *)$ est intègre mais n'est pas un corps.

Exemple VII.1.14 Les ensembles $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ munis de leurs lois usuelles sont des corps commutatifs ainsi que $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ pour p premier ; en revanche le corps des *quaternions de Hamilton* n'est pas commutatif.

Les propositions I.6.20 et III.1.6 ont leur pendant pour les anneaux :

Proposition VII.1.15 *Étant donnés un anneau $(A, +, *)$ et un ensemble E, l'ensemble A^E des applications de E dans A muni des lois induites (cf. I.6.20,) est un anneau (commutatif si A l'est.)*

***Preuve** : Voir l'exercice VII.8.3.*

VII.2 . −Morphismes, isomorphismes

Définition VII.2.1 (Morphisme d'anneaux) Une application

$$f \,:\, (A, +_A, *_A) \,\to\, (B, +_B, *_B)$$

est un *morphisme (homomorphisme) d'anneaux* (ou simplement *morphisme* si le contexte ne prête pas à confusion,) si :

Ann$_5$) $f \,:\, (A, +_A) \,\to\, (B, +_B)$ est un morphisme de groupes (cf. III.2.1.)

Ann$_6$) Pour tout couple (x, y) d'éléments de A,

$$f(x *_A y) \,=\, f(x) *_B f(y)\,.$$

Ann$_7$) $f(1_A) \,=\, 1_B$.

Cela revient à dire que f est un morphisme à la fois pour les magma $(A, +)$ et $(B, +)$ (cf. Ann$_5$),) ainsi que pour les magma $(A, *)$ et $(B, *)$ (cf. Ann$_6$).) Néanmoins on ajoute la condition Ann$_7$) dont on verra l'importance dans la suite.

On a l'exact analogue des lemmes I.6.3 et III.2.3 :

Lemme VII.2.2 *i) Pour tout anneau $(A, +, *)$ l'identité Id_A est un morphisme de l'anneau A dans lui-même.*

ii) Pour A, B et C des anneaux, $f \,:\, A \,\to\, B$ et $g \,:\, B \,\to\, C$ des morphismes, le composé $g \circ f$ est un morphisme.

On peut donc donner une définition analogue aux définitions I.6.4 et III.2.4 :

Définition VII.2.3 (Isomorphisme) Étant donnés deux anneaux $(A, +, *)$ et $(B, +, *)$, un morphisme $f \,:\, A \,\to\, B$ est un *isomorphisme* s'il existe un morphisme

$$g \,:\, B \,\to\, A \text{ tel que } g \circ f \,=\, \mathrm{Id}_B \text{ et } f \circ g \,=\, \mathrm{Id}_A\,.$$

On notera $\mathrm{Isom}_{\mathbf{Ann}}(A, B)$ (ou simplement $\mathrm{Isom}(A, B)$ si le contexte est clair) l'ensemble des isomorphismes de A dans B.

On a encore, sans surprise puisqu'en fait l'axiomatique n'est pas vraiement différente, un analogue des propositions I.6.5 et III.2.5 :

Proposition VII.2.4 *Étant donnés deux anneaux A et B, une application $f \,:\, A \,\to\, B$ est un isomorphisme si et seulement si c'est un morphisme bijectif.*

Preuve : *Comme précédemment, si f est un isomorphisme c'est en particulier un morphisme bijectif.*

Réciproquement si f est un morphisme bijectif, il résulte de la proposition III.2.5 que son application réciproque $g : B \to A$ est un morphisme du groupe $(B, +)$ dans le groupe $(A, +)$ ce qui assure que g vérifie VII.2.1.Ann$_5$).

En outre il résulte de la proposition I.6.5 que g est un morphisme du magma $(B, *)$ dans le magma $(A, *)$ ce qui assure que g vérifie VII.2.1.Ann$_6$).

Enfin f vérifiant VII.2.1.Ann$_7$), $f(1_A) = 1_B$ d'où

$$1_A = g[f(1_A)] = g(1_B)$$

ce qui entraîne que g vérifie VII.2.1.Ann$_7$).

Des définitions analogues à I.6.6 et III.2.7 peuvent donc être données même si elles seront en fait moins utilisées au moins dans ce cours :

Définition VII.2.5 Soit $(A, +, *)$ un anneau.

i) (**Gndomorphismes**)
Un morphisme $f : A \to A$ de A dans lui-même est appelé *endomorphisme*. On note

$$\mathrm{End}_{\mathbf{Ann}}(A) \text{ (ou simplement } \mathrm{End}(A), \text{)}$$

l'ensemble des endomorphismes de A.

ii) (**Automorphisme**)
Un morphisme $f : A \to A$ est un *automorphisme* si c'est à la fois un isomorphisme et un endomorphisme. Il revient au même, grâce à la proposition VII.2.4, de dire que f est un endomorphisme bijectif. On note $\mathrm{Aut}_{\mathbf{Ann}}(A)$ (ou simplement $\mathrm{Aut}(A)$) l'ensemble des automorphismes de A.

Exemple VII.2.6 Pour un anneau A, l'identité Id_A est un automorphisme.

Lemme VII.2.7 *i) Pour tout morphisme d'anneaux $MorfAB$, la restriction $f^\times := f_{|A^\times}$ de f à $A^\times$ est un morphisme de groupes à valeurs dans $B^\times$.*

ii) Pour tout anneau A,

$$\mathrm{Id}_A{}^\times = \mathrm{Id}_{A^\times} .$$

iii) Pour tous morphismes d'anneaux $f : A \to B$ et $g : B \to C$,

$$(g \circ f)^\times = g^\times \circ f^\times .$$

iv) Pour tout isomorphisme d'anneaux $f : A \to B$ d'isomorphisme réciproque $g : B \to A$,

$$f^\times : (A^\times, *) \to (B^\times, *)$$

est un isomorphisme de groupes d'isomorphisme réciproque $g^\times$.

Preuve : *Voir l'exercice VII.8.5.*

Proposition VII.2.8 *Pour tout anneau $(A, +, *)$ (pas nécessairement commutatif) il existe un unique morphisme d'anneau $\mathbb{Z} \to A$ appelé morphisme structural de A.*

Preuve : *S'il existe un morphisme d'anneaux $f : \mathbb{Z} \to A$, l'axiome VII.2.1.Ann$_7$) entraîne que*

$$f(1) = 1_A .$$

Par ailleurs f étant, en particulier un morphisme de groupes de $(\mathbb{Z}, +)$ dans $(A, +)$, $f(0) = 0_A$, pour tout $n \in \mathbb{N}$,

$$f(n+1) = f(n) + f(1) = f(n) + 1_A \text{ et } f(-n) = -f(n) .$$

Il s'ensuit que f est nécessairement le morphisme de groupes ϵ_1 défini au .

L'application f est donc déjà un morphisme de groupes pour les structures additives qui, de plus, vérifie l'axiome VII.2.1.Ann$_7$). Ne reste donc qu'à montrer que f satisfait l'axiome VII.2.1.Ann$_6$).

Pour tout $q \in \mathbb{Z}$,

$$f(0 * q) = f(0) = 0_A = 0_A * f(q) = f(0) * f(q) .$$

Par ailleurs pour tout $p \in \mathbb{N}$, et tout $p \in \mathbb{Z}$, si l'on ssupose que $f(p * q) = f(p) * f(q)$, alors :

$$\begin{aligned} f((p+1) * q) &= f(p * q + q) \\ &= f(p * q) + f(q) \\ &= (f(p) + 1_A) * f(q) \\ &= f(p+1) * f(q) \end{aligned}$$

et

$$\begin{aligned} f(-(p) * q) &= f(-(p * q)) \\ &= -f(p) * f(q) \\ &= f(-p) * f(q) ; \end{aligned}$$

ce qui montre le résultat par récurrence.

VII.3 . −Sous

Définition VII.3.1 (Sous-annau) Étant donné un anneau $(A, +, *)$ un *sous-anneau* de A est une partie B de A telle que $1_A \in B$ et les restrictions respectives des lois $+$ et $*$ à B donnent à B une structure d'anneau.

En particulier $(B, +)$ est alors un sous-groupe de $(A, +)$.

Remarque VII.3.2 i) Notons que l'axiome VII.1.1.Ann$_1$) a en particulier pour conséquence que $(B, +)$ est un sous-groupe de $(A, +)$; ce qui entraîne, en particulier (cf. III.3.3,) que l'élément neutre 0_A de $(A, +)$ est aussi l'élément neutre de $(B, +)$ et que l'opposé d'un élément $x \in B$ est son opposé dans A.

ii) Notons que la condition $1_A \in B$, entraîne que 1_A est l'élément neutre pour la loi $*$ sur B (cf. I.8.16.question 1),) et que tout inversible dans B est inversible dans A et que son inverse dans B est encore son inverse dans A (cf. I.8.16.question 2).) Il s'ensuit que $(B^\times, *)$ est alors un sous-groupe de $(A^\times, *)$.

iii) La condition $1_A \in B$ est automatiquement satisfaite dans le cas où A est intègre. En revanche si l'on considère un anneau R quelconque (même intègre) et $A := R \times R$ muni des lois

$$(x, y) +_A (z, t) := (x +_R z, y +_R t) \text{ et } (x, y) *_A (z, t) := (x *_R z, y *_R t),$$

(ce qu'on appelle la structure produit,) La partie

$$B := \{(x, 0), x \in R\}$$

est une partie qui est un sous-groupe pour la loi $+_A$ un sous-magma pour la loi $*_A$. B est même un anneau isomorphe à R dont l'élément neutre est $1_B = (1_R, 0)$ différent de lélément neutre $1_A = (1_R, 1_R)$ de A. On ne dira pas dans ce cas que B est un sous-anneau de A.

La condition $1_A \in B$ est à rapprocher de la condition VII.2.1.Ann$_7$) et donne sa cohérence à un énoncé comme la proposition VII.3.3.c).

Proposition VII.3.3 (Caractérisation des sous-anneaux) *Étant donnés un anneau*

$$(A, +, *) \text{ et } B \subset A$$

une partie de A, les assertions suivantes sont équivalentes :

a) B est un sous-anneau au sens de la définition VII.3.1.

b) B est non vide, $1_A \in B$, et pour tout couple (x, y) d'éléments de B,

$$y - x \in B \text{ et } x * y \in B\,.$$

c) La restriction

$$\mathrm{Id}_{A|B} : B \to A$$

de l'identité Id_A à B est un morphisme d'anneaux. Ceci signifie implicitement que B possède une structure d'anneau.

***Preuve** : Voir l'exercice VII.8.7.*

Exemple VII.3.4 L'anneau $\mathbb{Z}$ des entiers relatifs est un sous-anneau du corps $\mathbb{Q}$ des nombres rationnels, lui-même un sous-anneau du corps $\mathbb{R}$ des nombres réels, lui-même un sous-anneau du corps des nombres complexes $\mathbb{C}$.

Proposition VII.3.5 (Image directe/réciproque) *Soit $f : A \to B$ un morphisme d'anneaux.*

*i) (**Image directe**)*
Pour tout sous-anneau A' de A, l'image directe de A'

$$f(A') = \{y \in B\,;\, \exists x \in A',\ ,\ y = f(x)\}$$

est un sous-anneau de B.

ii) ***(Image réciproque)***
Pour tout sous-anneau B' de B, l'image réciproque

$$f^{-1}(B') \;=\; \{x \in A \,;\; f(x) \;\in\; B'\}$$

est un sous-anneau de A.

Définition VII.3.6 (Noyau/image) Étant donné un morphisme d'anneaux $f \;:\; A \;\to\; B$, 0_B étant l'élément neutre du groupe $(B, +)$, on appelle

i) (**Noyau**)
noyau de f le sous-ensemble

$$\operatorname{Ker} f \;:=\; f^{-1}(\{0\}_B) \;=\; \{x \in A \,;\; f(x) \;=\; 0_B\},$$

c'est-à-dire en fait le noyau du morphisme de groupes

$$f \;:\; (A, +) \;\to\; (B, +)$$

(cf. III.3.8.i),)

ii) (**Image**)
image de f l'ensemble

$$\operatorname{Im} f \;:=\; f(A) \;=\; \{y \in B \,;\; \exists x \in A,\;\; ,\; y \;=\; f(x)\}\,.$$

Corollaire VII.3.7 *Pour un morphisme d'anneaux $f \;:\; A \;\to\; B$, l'image de f est un sous-anneau de B.*

Proposition VII.3.8 *Un morphisme d'anneaux $f \;:\; A \;\to\; B$ est injectif (resp. surjectif) (cf. I.2.7,) si et seulement si* $\operatorname{Ker} f \;=\; \{0_A\}$ *(resp.* $\operatorname{Im} f \;=\; B$.)

Remarque VII.3.9 Remarquons que le noyau d'un morphisme d'anneaux $f \;:\; A \;\to\; B$, n'est pas un sous-eanneau de A en général. En effet, si $\operatorname{Ker} f$ est un sous anneau de A, $1_A \;\in\; \operatorname{Ker} f$ si bien que $f(1_A) \;=\; 0_B$. Or, d'après l'axiome VII.2.1.Ann$_7$), $f(1_A) \;=\; 1_B$, si bien que $0_B \;=\; 1_B$, ce qui entraîne que $B \;=\; \{0\}$ qui est un cas très particulier.

Définition VII.3.10 Si $i \;:\; A \;\to\; B$ est un morphisme d'anneaux injectif, il induit un isomorphisme $A \;\cong\; \operatorname{Im} i$; si bien que A est isomorphe à un sous-anneau de B. On dira parfois même par abus de langage que A est lui-même un sous-anneau de B.

VII.4 . −Idéaux

Soit $(A, +, *)$ un anneau commutatif (cf. VII.1.5.) L'anneau $(\mathbb{Z}, +, *)$ (cf. IV,) en est un bon exemple. On notera $A^\times$ l'ensemble des éléments inversibles de A (cf. VII.1.8) et on rappelle que le couple $(A^\times, *)$ est un groupe, (resp. un groupe abélien si A est commutatif) (cf. VII.1.9.)

Définition VII.4.1 (Idéal) Étant donné un anneau commutatif $(A, +, *)$, une partie $\mathfrak{I} \subset A$ de A est un *idéal* si $\mathfrak{I}$ est un sous-groupe de $(A, +)$ tel que

$$\forall (a, x) \in A \times \mathfrak{I},\ a * x \in \mathfrak{I}\,.$$

Proposition VII.4.2 (Caractérisation des idéaux) *Une partie $\mathfrak{I}$ d'un anneau commutatif $(A, +, *)$ est un idéal de a si et seulement si $\mathfrak{I} \neq \emptyset$ et*

$$\forall (x, y) \in \mathfrak{I} \times \mathfrak{I},\ \forall (a, b) \in A \times A,\ a * x + b * y \in \mathfrak{I}\,.$$

Preuve *: Voir l'exercice VII.8.9.*

Exemple VII.4.3 a) Les sous-ensembles $\{0\}$, et A de A sont des idéaux de A. Ce sont les seuls idéaux de A si A est un corps.

b) Pour tout $a \in A$, le sous-ensemble

$$aA := \{a * b\,,\ b \in A\}$$

est un idéal de A.

c) Les idéaux de l'anneau $(\mathbb{Z}, +, *)$ sont exactement les sous-groupes du groupe $(\mathbb{Z}, +)$ c'est-à-dire les sous-ensemble de $\mathbb{Z}$ de la forme $d\mathbb{Z}$ avec $d \in \mathbb{Z}$ comme nous l'avons vu dans le corollaire IV.5.5.

Nombre des résultats établis pour les sous-groupes aux paragraphes III.3 et suivants ont leur analogue dans le cadre des idéaux. La proposition qui suit est à rapprocher de la proposition III.3.7 :

Proposition VII.4.4 *Soit*

$$f : (A, +, *) \to (B, +_B, *_B)$$

un morphisme d'anneaux (cf. VII.2.1) (où $(B, +_B, *_B)$ est un anneau commutatif.) Pour tout idéal $\mathfrak{J}$ de B, $f^{-1}(\mathfrak{J})$ est un idéal de A.

Preuve *: Puisque f est un morphisme d'anneaux, donc en particulier un morphisme de groupes $(A, +) \to (B, +_B)$, $f(0) = 0_B \in J$ si bien que $f^{-1}(J) \neq \emptyset$.*

Par ailleurs

$$\forall (x, y) \in f^{-1}(J) \times f^{-1}(J),\ \forall (a, b) \in A \times A,\ f(a*x+b*y) = f(a) *_B f(x) +_B f(b) *_B f(y) \in J$$

ce qui entraîne que $a * x + b * y \in f^{-1}(J)$ assurant que $f^{-1}(J)$ est un idéal.

Corollaire VII.4.5 *Avec les notations de la proposition VII.4.4, le noyau* $\mathrm{Ker}\, f$ *du morphisme* f *est un idéal de* A.

Preuve *: En effet,* $\mathrm{Ker}\, f \ = \ f^{-1}(\{0\})$.

On a, pour les idéaux d'un anneau A, l'exact analogue de la proposition III.3.6 pour les sous-groupes.

Proposition VII.4.6 (Propriétés des idéaux) *Étant donnés deux idéaux*

$$\mathfrak{I} \ \subset \ A \,\mathrm{et}\, \mathfrak{J} \ \subset \ A \ :$$

i) $\mathfrak{I} \cap \mathfrak{J}$ *est un idéal de* A ;

Preuve *: Comme* $\mathfrak{I}$ *et* $\mathfrak{J}$ *sont en particulier des sous-groupes de* $(A,+)$, $0 \ \in \ \mathfrak{I} \cap \mathfrak{J}$ *si bien que* $\mathfrak{I} \cap \mathfrak{J} \ \neq \ \emptyset$. *Par ailleurs,*

$$\begin{array}{ll} \forall (x,y) \in (\mathfrak{I} \cap \mathfrak{J}) \times (\mathfrak{I} \cap \mathfrak{J}), & \\ \forall (a,b) \in A \times A, & (x,y) \ \in \ \mathfrak{I} \times \mathfrak{I} \\ \Rightarrow & a*x+b*y \ \in \ \mathfrak{I} \\ \mathrm{et} & (x,y) \ \in \ \mathfrak{J} \times \mathfrak{J} \\ \Rightarrow & a*x+b*y \ \in \ \mathfrak{J} \end{array}$$

puisque $\mathfrak{I}$ *et* $\mathfrak{J}$ *sont des idéaux. Il s'ensuit que* $a*x+b*y \ \in \ \mathfrak{I} \cap \mathfrak{J}$ *ce qui assure que* $\mathfrak{I} \cap \mathfrak{J}$ *est un idéal.*

ii) Plus généralement pour $\mathcal{I}$ *un ensemble non vide d'idéaux de* A, $\bigcap_{\mathfrak{I} \in \mathcal{I}} \mathfrak{I}$ *est un idéal de* A.

iii) $\mathfrak{I} \cup \mathfrak{J}$ *est un idéal de* A *si et seulement si* $\mathfrak{I} \ \subset \ \mathfrak{J}$ *ou* $\mathfrak{J} \ \subset \ \mathfrak{I}$.

iv) Si $\left(\mathfrak{I}_n\right)_{,n\in\mathbb{N}}$ *est une suite d'idéaux de* A *telle que*

$$\forall (p,q) \in \mathbb{N} \times \mathbb{N}, \ \exists r \in \mathbb{N}, \ \mathfrak{I}_p \ \subset \ \mathfrak{I}_r \,\mathrm{et}\, \mathfrak{I}_q \ \subset \ \mathfrak{I}_r,$$

alors $\bigcup_{n\in\mathbb{N}} \mathfrak{I}$ *est un idéal de* A.

Un cas particulier est celui où $\left(\mathfrak{I}_n\right)_{,n\in\mathbb{N}}$ *est croissante, i.e.*

$$\forall p \in \mathbb{N}, \ \forall q \in \mathbb{N}, \ p \ \leq \ q \ \Rightarrow \ \mathfrak{I}_P \ \subset \ \mathfrak{I}_q$$

car alors

$$\forall p \in \mathbb{N}, \ \forall q \in \mathbb{N}, \ \mathfrak{I}_p \ \subset \ \mathfrak{I}_{\max(p,q)} \,\mathrm{et}\, \mathfrak{I}_q \ \subset \ \mathfrak{I}_{\max(p,q)} \ .$$

Le corollaire VII.4.7 qui suit est l'exact analogue du lemme III.4.1 :

Corollaire VII.4.7 *Pour $S \subset A$ une partie de A, l'ensemble $\mathcal{I}_S$ des idéaux de A contenant S possède un plus petit élément pour l'inclusion noté (S). autrement di (S) est l'unique idéal de A caractérisé par le fait que $S \subset (S)$, et pour tout idéal $\mathfrak{J}$ contenant S, $(S) \subset \mathfrak{J}$.*

***Preuve** : Il faut remarquer que $A \in \mathcal{I}_S$ entraîne que $\mathcal{I}_S \neq \emptyset$ et qu'on peut donc appliquer VII.4.6.ii) si bien que*

$$(S) := \bigcap_{\mathfrak{J} \in \mathcal{I}} \mathfrak{J}$$

répond à la question.

Définition VII.4.8 Pour toute partie $S \subset A$, l'idéal (S) construit grâce au corollaire VII.4.7 ci-dessus est appelé *idéal engendré par S*.

Exemple VII.4.9 a) $(\emptyset) = \{0\}$.

b) Pour tout idéal $\mathfrak{I}$ de A,

$$(\mathfrak{I}) = \mathfrak{I} .$$

Les résultat qui suivent sont à rapprocher de la proposition III.4.7 :

Lemme VII.4.10 *Pour tout $S \subset A$, tout $x \in A$, $x \in (S)$, si et seulement s'il existe $r \in \mathbb{N}$, $x_{i\ ,1\leq i\leq r} \in S$, et $a_{i\ ,1\leq i\leq r} \in A$ tels que*

$$x = \sum_{i=1}^{r} a_i * x_i .$$

***Preuve** : Notons $\mathfrak{I} \subset A$, l'ensemble des éléments $x \in A$ tels qu'il existe $r \in \mathbb{N}$, $x_{i\ ,1\leq i\leq r} \in S$, $a_{i\ ,1\leq i\leq r} \in A$, telque $x = \sum_{i=1}^{r} a_i * x_i$. Pour tout $(x, y) \in \mathfrak{I} \times \mathfrak{I}$, on peut, par définition,écrire $x = \sum_{i=1}^{m} a_i * x_i$ et $y = \sum_{i=1}^{n} b_i * y_i$, $a_{i\ ,1\leq i\leq m} \in A$, $b_{i\ ,1\leq i\leq n} \in A$, $x_{i\ ,1\leq i\leq m} \in S$, $y_{i\ ,1\leq i\leq n} \in S$. Pour tout $(a, b) \in A \times A$, notons*

$$\forall 1 \leq i \leq m,\ c_i := a * a_i \text{ et } z_i := x_i$$

$$\forall i \leq m 1 \leq m + n,\ c_i := b * b_{i-m} \text{ et } z_i := y_{i-m} .$$

Il s'ensuit que

$$a * x + b * y = \sum_{i=1}^{m+n} c_i * z_i \in \mathfrak{I} .$$

C'est-à-dire que $\mathfrak{I}$ est un idéal.

Il est immédiat de constater que $S \subset \mathfrak{I}$, et que pour tout idéal $\mathfrak{J}$ contenant S, $\mathfrak{I} \subset \mathfrak{J}$, si bien que

$$\mathfrak{I} = (S) .$$

Définition VII.4.11 Pour tout $S \subset A$, l'idéal (S) s'appelle l'*idéal engendré par* S.

Notation VII.4.12 Pour $\mathcal{I}$ un ensemble d'idéaux de A, on note $\sum_{\mathfrak{I}\in\mathcal{I}} \mathfrak{I}$ l'idéal engendré par l'union $\bigcup_{\mathfrak{I}\in\mathcal{I}} \mathfrak{I}$.

Corollaire VII.4.13 *Pour deux idéaux $\mathfrak{I}$ et $\mathfrak{J}$ de A, l'idéal $\mathfrak{I}+\mathfrak{J}$ engendré par $\mathfrak{I}\cup\mathfrak{J}$ est l'ensemble des $x+y$ avec $x\in\mathfrak{I}$ et $y\in\mathfrak{J}$.*

***Preuve** : Preuve tout à fait analogue à celle donnée pour les groupes au TD n° III, exercice H.*

Notation VII.4.14 Si $a \in A$, l'idéal $(\{a\})$ engendré par le singleton $\{a\}$, est usuellement noté aA ou (a), et l'on a :

$$(\{a\}) = (a) = aA = \{a*b\,,\ b\in A\}\,.$$

un tel idéal est dit *principal*.

Lemme VII.4.15 *Étant donné un idéal $\mathfrak{I}$ de A, les assertion suivantes sont équivalentes :*

a) $\mathfrak{I} = A$;

b) $\mathfrak{I}\cap A^\times \neq \emptyset$;

c) $\exists u\in A^\times,\ \mathfrak{I} = uA$.

d) $1\in\mathfrak{I}$;

***Preuve** :*

i) ***(a)*** $\Rightarrow$ ***b))***
Ceci est immédiat puisque $A^\times \subset A$.

ii) ***(b)*** $\Rightarrow$ ***c))***
Puisque $\mathfrak{I}\cap A^\times\neq\emptyset$, il existe $u\in A^\times$ tel que $u\in\mathfrak{I}$. Puisque $\mathfrak{I}$ est un idéal, pour tout $a\in A$, $u*a = u*a+u*0\in\mathfrak{I}$ c'est-à-dire que $uA\subset\mathfrak{I}$.
Réciproquement, puisque $u\in A^\times$, il existe $v\in A^\times$ tel que $u*v=1$. Ainsi pour tout $x\in\mathfrak{I}$, $x = u*v*x = u*(v*x)\in uA$ si bien que $\mathfrak{I}\subset uA$ et finalement

$$\mathfrak{I} = uA\,.$$

iii) ***(c)*** $\Rightarrow$ ***d))***
Puisque $u\in A^\times$, il existe $v\in A^\times$ tel que $u*v=1$. Donc

$$1 = u*v\in uA = \mathfrak{I}\,.$$

iv) ***(d)*** $\Rightarrow$ ***a))***
Si $1 \in \mathfrak{I}$, *pour tout* $a \in A$, $a = a*1 \in \mathfrak{I}$ *si bien que* $A \subset \mathfrak{I}$. *Comme, par définition* $\mathfrak{I} \subset A$,

$$A = \mathfrak{I} .$$

Définition VII.4.16 (Idéal stricte/propre) Un idéal $\mathfrak{I} \subset A$, est un *idéal strict* ou un *idéal propre* si $\mathfrak{I} \neq A$.

Définition VII.4.17 Un idéal $\mathfrak{p} \subset A$ est *premier* si $\mathfrak{p} \neq A$ (*i.e.* $\mathfrak{p}$ est un idéal propre) et

$$\forall (a,b) \in A \times A,\ a*b \in \mathfrak{p} \Rightarrow a \in \mathfrak{p} \vee b \in \mathfrak{p} .$$

Définition VII.4.18 (Idéaux comaximaux) On dit que deux idéaux I et J de A sont *comaximaux* ou *étrangers* (ou éventuellement *premiers entre eux*) si $I + J = A$.

VII.5 . −Divisibilité et idéaux

La relation de divisibilité peut être introduite, comme nous allons le faire dans ce paragraphe pour n'importe quel anneau commutatif et être reliée à la notion d'idéal introduite en VII.4. Nous verrons cependant qu'elle acquiert d'intéressantes propriétés (cf. VII.6,) lorsque l'anneau est intègre.

Supposons donc dans cette section (VII.5) que $(A, +, *)$ est un anneau commutatif (cf. VII.1.5.)

Définition VII.5.1 (Divisibilité) Pour tout couple $(a,b) \in A \times A$, on dit que a *divise* b ou que a est un *diviseur* de b ou encore que b est un *multiple* de a et l'on note $a|b$, s'il existe $c \in A$ tel que $a*c = b$.

Lemme VII.5.2

$$\forall (a,b) \in A \times A,\ a|b \Leftrightarrow bA \subset aA \Leftrightarrow b \in aA$$

(où aA *est l'idéal principal engendré par* a *(cf. VII.4.14.))*

Preuve *: Presqu'immédiat sur les définitions.*

Remarque VII.5.3 On sait que dans un anneau A, pour tout $a \in A$, $0*a = 0$ (cf. .) Il en résulte que pour tout $a \in A$, $a|0$.
Par ailleurs

$$\forall a \in A,\ \forall b \in A,\ \forall c \in A,\ \big(a|b \text{ et } a|c \Rightarrow a|b+c\big) .$$

Remarque VII.5.4 On remarque que la notion de divisibilité « correspond » à l'inclusion sur les idéaux laquelle est une relation d'ordre partielle. La réflexivité et la transitivité ne posent aucune difficulté pour la relation de divisibilité mais il n'est pas clair qu'elle soit antisymétrique : $a|b$ et $b|a$ n'implique pas forcément que $a = b$. Même dans $\mathbb{Z}$ $5|-5$ et $-5|5$.
On verra comment on peut affiner cette notion de manière intéressante dans le paragraphe concernant les anneaux intègres (cf. VII.6.)

Définition VII.5.5 (Élément premier) Un élément $a \in A$ est dit *premier* si l'idéal principal engendré par a (cf. VII.4.14,) aA est premier (cf. VII.4.17;) ce qui équivaut à dire que $a \notin A^\times$ (cf. VII.4.15,) et

$$\forall (b,c) \in A \times A,\ a|b*c \ \Rightarrow\ a|b \ \vee\ a|c\ .$$

Définition VII.5.6 (Élément irréductible) Un élément $a \in A$ est irréductible si $a \notin A^\times$ (a n'est pas inversible) et

$$\forall (b,c) \in A \times A,\ a = b*c \ \Rightarrow\ b \in A^\times \ \vee\ c \in A^\times\ .$$

Notation VII.5.7 On notera

$$\forall X \subset A\ ,\ \mathcal{D}(X) := \{y \in A\ ;\ \forall x \in X,\ y|x\} \text{ (resp. } \mathcal{M}(X) := \{y \in A\ ;\ \forall x \in X,\ x|y\}\ )$$

l'ensemble des diviseurs (resp. multiples) communs à tous les éléments de X.

De manière un peu abusive, on notera encore

$$\mathcal{D}(x,y) := \mathcal{D}(\{x,y\}) \text{ (resp. } \mathcal{M}(x,y) := \mathcal{M}(\{x,y\})\ .)$$

Proposition VII.5.8 *Pour tout $X \subset A$,*

$$d \in \mathcal{D}(X) \Leftrightarrow (X) \subset dA,$$

(où (X) est l'idéal engendré par X défini en (cf. VII.4.11.)

***Preuve** : Si $d \in \mathcal{D}(X)$,*

$$\forall x \in X,\ d|x\ .$$

Par conséquent, pour tout $y := \sum_{i=1}^{n} a_i * x_i \in (X)$, $d|y$ i.e.$y \in dA$ ce qui entraîne

$$(X) \subset dA\ .$$

Réciproquement si $(X) \subset dA$, pour tout $y \in (X)$, $d|y$. Comme $X \subset (X)$,

$$\forall x \in X,\ d|x$$

ce qui entraîne

$$d \in \mathcal{D}(X)\ .$$

Corollaire VII.5.9 *Pour tout $X \subset A$, $A^\times \subset \mathcal{D}(X)$.*

***Preuve** : C'est une conséquence de la proposition VII.5.8 et du lemme VII.4.15.*

Définition VII.5.10 Pour $X \subset A$, si $\mathcal{D}(X) = A^\times$ on dit que les éléments de X sont *premiers entre eux (dans leur ensemble).*

Remarque VII.5.11 Cependant la situation que nous aurons souvent à considérer par la suite est celle où deux éléments x et y de A sont premiers entre eux *i.e.*où $\mathcal{D}(\{x,y\}) = A^\times$ ou vien où $X \subset A$ est constitué d'éléments *deux à deux premiers entre eux* c'est-à-dire

$$\forall (x,y) \in X \times X,\ \mathcal{D}(\{x,y\}) = A^\times\ .$$

Bien sûr que cette situation entraîne que les éléments de X sont premiers entre eux dans leur ensemble mais le fait que les éléments de X sont deux à deux premiers entre eux est une hypothèse plus forte. Les éléments $2, 5, 6$ de $\mathbb{Z}$ sont premiers entre eux dans leur ensemble mais pas deux à deux premiers entre eux.

Définition VII.5.12 (PGCD PPCM) Étant donné un ensemble $X \subset A$, on appelle *plus grand commun diviseur* ou *PGCD* (resp. *plus petit commun multiple* ou *PPCM*)

$$\text{un plus grand élément de } \mathcal{D}(X) (\text{resp. un plus petit élément de } \mathcal{M}(X),\ )$$

au sens de la relation $|$ bien entendu, autrement dit, un élément $d \in \mathcal{D}(X)$ (resp. $m \in \mathcal{M}(X)$) tel que :

$$\forall a \in X,\ d|a \text{ et } \forall b \in \mathcal{D}(X),\ b|d \text{ (resp. } \forall a \in X,\ a|m \text{ et } \forall b \in \mathcal{M}(X),\ m|b\ .) \qquad \text{VII.5.12.1}$$

Remarque VII.5.13 La définition VII.5.12 peut sembler un peu abusive au sens où nous n'avons parlé de *plus grand élément* ou de *plus petit élément* que pour une relation d'ordre (cf. I.2.2.vii).) Nous verrons en outre que la relation $\cdot|\cdot$ n'est pas « vraiment » une relation d'ordre (cf. VII.6.6,) met en particulier en défaut le fait que de tels éléments, s'ils existent, (ce que nous n'avons pas encore établi mais qui le sera pour les anneaux principaux est unique.

Lemme VII.5.14 *Étant donné une partie $X \subset A$, tous les PGCD (resp. PPCM) de X s'ils existent engendrent un même idéal*

Preuve *: An effet si d et d' (resp. m et m') sont deux PGCD (resp. PPCM) de X, par définition on a*

$$d'|d \text{ et } d|d' \text{ (resp. } m'|m \text{ et } m|m'\ )$$

ce qui entraîne, en vertu du lemme VII.5.2

$$dA = d'A \text{ (resp. } A = m'A\ .)$$

Notation VII.5.15 Le lemme ci-dessus peux motiver les notations suivantes : Pour $X \subset A$ d (resp. m) un PGCD (resp. PPCM) de X, on notera :

$$\bigwedge X \ := \ dA \text{ et } \mathrm{PPCM}(X) \ := \ mA \, . \qquad \text{VII.5.15.1}$$

Pour tout $(x, y) \in A \times A$, on notera :

$$x \wedge y \ := \ \bigwedge \{x, y\} \text{ et } \mathrm{PPCM}(x, y) \ = \ \mathrm{PPCM}(\{x, y\}) \, . \qquad \text{VII.5.15.2}$$

VII.6 . −Éléments remarquables d'un anneau intègre

Dans cette section (VII.6,) $(A, +, *)$ est un anneau commutatif intègre (cf. VII.1.5, VII.1.11.)

Proposition VII.6.1 *Dans un anneau commutatif intègre A, tout élément premier (cf. VII.5.5,) non nul est irréductible (cf. VII.5.6.)*

Preuve *: Soit en effet $p \in A$ et $(a, b) \in A \times A$ tels que $p = a * b$. Alors $p|a * b$ et puisque p est premier, $p|a$ ou $p|b$. Si $p|a$ il existe $c \in A$ tel que $a = p * c$. L'égalité $p = a * b$ entraîne alors $p = p * c * b$ qui entraîne encore*

$$p * (1 - c * b) \ = \ 0 \, .$$

Or $p \neq 0$ et A est intègre donc

$$c * b \ = \ 1$$

c'est-à-dire que b est inversible, ce qui assure que p est irréductible.

Définition VII.6.2 (Éléments associés) Pour $(a, b) \in A \times A$, on dit que b est *associé* à a s'il existe un élément inversible $u \in A^\times$, tel que $b = u * a$.

Lemme VII.6.3 *La relation d'association est une relation déquivalence.*

Preuve *: Voir l'exercice VII.8.11.*

Lemme VII.6.4 *Pour tout $(a, b) \in A \times A$, les assertions suivantes sont équivalentes :*

a) $a|b$ et $b|a$;

b) $aA = bA$;

c) $\exists u \in A^\times, \ b = a * u$;

d) $\exists u \in A^\times, \ a = b * u$;

e) *a et b sont associés.*

Preuve *:*

i) ***(a)*** $\Leftrightarrow$ ***b))***
L'équivalence entre a) et b) est une conséquence immédiate du lemme VII.5.2.

ii) ***(c)*** $\Rightarrow$ ***d)*** $\Leftrightarrow$ ***e))***
L'équivalence entre c) et d) signifie exactement que la relation « être associés » est symétrique. L'équivalence avec e) est tautologique.

iii) ***(c)*** $\Rightarrow$ ***a))***
Puisque d) et c) sont équivalentes, c) entraîne c) et d) qui entraînent tautologiquement a).

iv) ***(a)*** $\Rightarrow$ ***d))***

Remarque iv).1 Notons que dans cette partie seulement de la démonstration l'hypothèse que A est intègre sera utilisée.

Si $a|b$ *et* $b|a$*, il existe* $(u, v) \in A \times A$ *tels que* $a = b * u$ *et* $b = a * v$*. Il s'ensuit que* $a = a * v * u$ *ou encore que*

$$a * (1 - v * u) = 0 .$$

$a = 0$ *Si* $a = 0$, $a|b$ *entraîne* $b = 0$, *et pour tout* $w \in A^\times$, $a = b * w$.
$a \neq 0$ *Si* $a \neq 0$, *puisque* A *est intègre* $1 - v * u = 0$ *c'est-à-dire que* $v * u = 1$ *si bien que* u *et* v *sont inversibles, ce qui achève la preuve.*

Remarque VII.6.5 L'équivalence entre VII.6.4.b) et VII.6.4.e) peut se reformuler en disant qu'on a une bijection naturelle entre les classes d'équivalences pour la relation d'association et les idéaux principaux de A.

Remarque VII.6.6 Bien qu'elle soit réflexive et transitive, la relation $|$ (divise) n'est pas « vraiment » *antisymétrique* (cf. I.2.2.iii),) fait qu'on ne peut pas dire que $|$ est une relation d'ordre.

Cependant la relation d'association est une *relation d'équivalence*. On dira dans ce cas que $|$ est une relation de *pré-ordre*. Ce pré-ordre n'est pas total, en effet on ne peut pas toujours comparer deux éléments de $\mathbb{Z}$ du point de vue de la divisibilité. Par exemple, on n'a ni $3|5$ ni $5|3$.

Lemme VII.6.7 *L'élément neutre pour* $+$ 0 *est le plus grand élément pour* $|$ *tandis que tout élément* $u \in A^\times$ *est un plus petit élément pour* $|$.

Remarque VII.6.7.1 On constate d'ores et déjà que $|$ ne se comporte pas tout à fait comme une relation d'ordre puisqu'il n'y a pas unicité d'un plus petit élément.

Preuve *: On pourra rapprocher ce résultat du TD n° IV, exercice B, question 1).*

Lemme VII.6.8 *Pour tout $X \subset A$, les PGCD de X (resp. PPCM de X) forment une classe d'équivalence pour la relation d'association.*

Preuve *: C'est une conséquence du lemme VII.5.14 et de la remarque VII.6.5.*

Remarque VII.6.9 On n'a pas parlé jusqu'ici du PGCD ni du PPCM mais d'un PGCD ou d'un PPCM à cause du défaut d'unicité constaté dans le lemme ci-dessus. Ce dernier énoncé montre en outre que de toute évidence, le « bon objet » à considérer n'est pas un PGCD ou un PPCM mais la classe d'association des PGCD (resp PPCM) qui, pour le coup, et d'après le lemme VII.6.8 est unique. Cette classe d'association elle-même ne semble pourtant pas être un objet très utilisable sauf à remarquer qu'on peut la représenter par un objet tout à fait maniable à savoir un idéal. Grâce au lemme VII.6.4 on sait en effet que tous les PGCD (resp. PPCM) engendrent le même idéal.

Le défaut majeur de ces notions, dans ce cadre trop général, est de ne pas jouir d'un résultat d'existence. Un cadre confortable pour s'y intéresser est celui des anneaux principaux à moins qu'on introduise la notion d'anneau factoriel, ce qui ne sera pas fait dans le cadre de ce cours.

VII.7 . −Anneau quotient et factorisation des morphismes

Remarque VII.7.1 On a remarqué en VII.3.9, que pour un morphisme d'anneaux $f : A \to B$, le noyau $\mathrm{Ker}\, f$ de f n'est pas un sous-anneau de A. En revanche, puisque c'et le noyau du morphisme de groupes $f : (A,+) \to (B,+)$ c'est un sous-groupe de $(A,+)$ (cf. III.3.9.)

De plus pour tout couple (x,y) d'éléments de $\mathrm{Ker}\, f$ et tout couple ((a,b) d'éléments de A, puisque f est un morphisme d'anneaux,

$$f(a*x+b*y) \;=\; a*f(x)+b*f(y) \;=\; 0,$$

si bien que $a*x+b*y \in \mathrm{Ker}\, f$. On constate, comme on l'a déjà remarqué dans le corollaire VII.4.5, que le noyau d'un morphisme d'anneaux est un idéal.

Remarque VII.7.2 Pour un anneau $(A,+,*)$ puisque $(A,+)$ est un groupe abélien tout idéal $\mathfrak{I}$ de A est en particulier un sous-groupe distingué de $(A,+)$. les consttructions de la section V.5 peuvent s'appliquer mutatis mutandis. Néanmoins elles sont plus riches en générale, puisqu'on dispose d'une structure plus riche que celle de groupe.

Proposition VII.7.3 (Relations déquivalences compatibles) *Soient $(A,+,*)$ un anneau commutatif et $\mathfrak{I}$ un idéal de A la relation $\sim_{\mathfrak{I}}$ définie par*

$$\forall (x,y) \in A\times A,\; x \sim_{\mathfrak{I}} y \;\Leftrightarrow\; y-x \;\in\; \mathfrak{I}$$

est une relation d'équivalence compatible aux lois $+$ et $*$ de A. Il s'ensuit qu'il existe une unique structure d'anneau sur le quotient $A/\mathfrak{I} := A/\sim_{\mathfrak{I}}$ telle que la surjection canonique $\pi : A \to A/\mathfrak{I}$ soit un morphisme d'anneaux.

Preuve : *On a déjà remarqué mais on rappelle encore que $(A,+)$ étant un groupe abélien, et $\mathfrak{I}$ un sous-groue, il est distingué (cf. V.4.9.b).) On constate que, de plus, la relation $\sim_{\mathfrak{I}}$ définie ici est exactement celle définie dans la section V.4. Il s'ensuit que la proposition V.5.1 s'applique si bien qu'il existe une unique structure de groupe (encore notée $+$) sur $A/\mathfrak{I}$ telle que*

$$\pi \ : \ (A,+) \ \to \ (A/\mathfrak{I},+)$$

soit un morphisme de groupes.

De plus :

$$\begin{array}{lrcl}
\forall x \in A,\ \forall z \in A, & & & \\
\forall y \in A,\ \forall t \in A, & x \sim_{\mathfrak{I}} z & \text{et} & y \sim_{\mathfrak{I}} t \\
\Rightarrow & z*t - x*y & = & z*t - z*y + z*y - x*y \\
 & & = & z*(t-y) + y*(z-x) \\
 & & \in & \mathfrak{I} \\
\Rightarrow & z*t & \sim_{\mathfrak{I}} & x*y
\end{array}$$

c'est-à-dire, du fait que I est un idéal, que la relation $\sim_{\mathfrak{I}}$ est compatible à $*$ et qu'il existe donc une unique loi $*$ sur $A/\mathfrak{I}$ telle que

$$\forall x \in A,\ \forall y \in A,\ \pi(x*y) \ = \ \pi(x)*\pi(y)$$

(cf. .)

Il reste encore à vérifier que $(A/\mathfrak{I},+,*)$ satisfait aux axiomes VII.1.1.Ann$_2$) à VII.1.1.Ann$_4$) et que π vérifie bien la définition VII.2.1.

Certaines des propriétés de la surjection canonique $\pi \ : \ A \ \to \ A/\mathfrak{I}$ sont, pour ainsi dire, presque évidentes au vu de ce qui précède mais il n'est pas mauvais de les dégager de manière formelle :

Proposition VII.7.4 (Propriétés de la surjection canonique) *Dans la situation de la proposition VII.7.3 :*

i) Le morphisme π est surjectif.

ii) $\operatorname{Ker}\pi \ = \ \mathfrak{I}$.

Preuve :

i) Remarqons encore une fois que pour tout élément $\alpha \ \in \ A/\mathfrak{I}$, α est une classe d'équivalence qui est par conséquent non vide. Les écritures $x \ \in \ \alpha$ ou $\pi(x) \ = \ \alpha$ renvoient toute deux au même fait que $x \ \in \ A$ est un représentant de la classe α.

Les expressions « x est au-dessus de α » « x relève α » ou « x est un relèvement de α » pourraient bien échapper au rédacteur de ces lignes sans qu'elles signfient pourtant ni plus ni moins que

$$\pi(x) \ = \ \alpha \ .$$

ii) Pour tout $x \in A$, $\pi(x) = 0$, *signifie exactement* $x \sim_{\mathfrak{I}} 0$, *c'est-à-dire* $x - 0 \in \mathfrak{I}$, *i.e.*$x \in \mathfrak{I}$.

Définition VII.7.5 (Anneau quotient) L'anneau

$$A/\mathfrak{I} \text{ ou même le couple } \big(A/\mathfrak{i}, \pi : A \to A/\mathfrak{i}\big)$$

construit par la proposition VII.7.3 est appelé *anneau quotient*. On dit encore que l'ensemble $A/\sim_{\mathfrak{I}}$ est muni de la *structure quotient*.

Remarque VII.7.6 On remarque que, si on oublie la multiplication $*$ sur A, $(A, +)$ est un groupe abélien et $\mathfrak{I}$ un sous-groupe, nécessairement distingué. La structure de groupe qu'on obtient sur $A/\mathfrak{I}$ en oubliant aussi la multiplication, donne un groupe abélien qui est exactement le groupe quotient défini en V.5.2.

Exemple VII.7.7 La situation considérée dans l'exemple V.5.3 peut être complétée. En effet pour tout $d \in \mathbb{Z}$, l'ensemble $d\mathbb{Z}$ des multiples de d est non seulement un sous-groupe de $(\mathbb{Z}, +)$ mais encore un idéal de $(\mathbb{Z}, +, *)$. Il s'ensuit, hormis pour $d = 1$, que $\mathbb{Z}/d\mathbb{Z}$ a une structure d'anneau telle que $\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$ soit un morphisme d'anneaux.

Proposition VII.7.8 (Factorisation des morphismes) *Soient* $(A, +, *)$ *un anneau comutatif et* $\mathfrak{I}$ *un idéal. On note* $\pi : A \to A/\mathfrak{I}$ *la surjection canonique.*

Pour tout morphisme d'anneaux $f : A \to B$ *les assertions suivantes sont équivalentes :*

a)

$$\mathfrak{I} \subset \operatorname{Ker} f\,.$$

b) Il existe un unique morphisme d'anneaux $\overline{f} : A/\mathfrak{I} \to B$ *tel que* $\overline{f} \circ \pi = f$.

De plus, si $\mathfrak{I} = \operatorname{Ker} f$, $\overline{f}$ *est injectif et il est surjectif dès que* f *l'est.*

***Preuve** :*

i) ***(b)*** $\Rightarrow$ ***a))***

C'est un fait général et facile à vérifier que, dès qu'on a des morphismes de groupes, u, v, w

$$u = v \circ w \Rightarrow \operatorname{Ker} w \subset \operatorname{Ker} u\,.$$

Or $\operatorname{Ker}\pi = \mathfrak{I}$ *(cf. VII.7.4.ii),) si bien que*

$$\overline{f} \circ \pi = f \Rightarrow \mathfrak{I} \subset \operatorname{Ker} f\,.$$

ii) ***(a)*** $\Rightarrow$ ***b))***

$*$) ***(Unicité de*** $\overline{f}$ ***(analyse))***

Si $\overline{f}$ *existe alors nécessairement pour tout* $\alpha \in A/\mathfrak{I}$, *il existe* $x \in A$ *tel que* $\alpha = \pi(x)$ *et*

$$\overline{f}(\alpha) = \overline{f}[\pi(x)] = f(x)\,.$$

Ceci établit l'unicité de $\overline{f}$.

†) ***(Existence de $\overline{f}$ (synthèse))***
Or si $z \in A$ est tel que $\alpha = \pi(z)$ on a encore

$$\overline{f}(\alpha) = \overline{f}[\pi(z)] = f(z) .$$

Or

$$\pi(x) = \pi(z) \Rightarrow z - x \in \mathfrak{I} \subset \operatorname{Ker} f \Rightarrow f(z-x) = 0 \Rightarrow f(z) = f(x) .$$

Il s'ensuit que $\overline{f}$ existe et est bien définie par la formulle :

$$\overline{f}(\alpha) = f(x) \,\forall\, x, \alpha = \pi(x) .$$

‡) ***($\overline{f}$ est un morphisme de groupes)***

$$\forall \alpha \in A/\mathfrak{I},\ \forall \beta \in A/\mathfrak{I},\ \big(\exists x \in A,\ \exists y \in A,\ (\alpha = \pi(x) \wedge \beta = \pi(y))\big) .$$

On a alors :

$$\begin{aligned} \overline{f}(\alpha+\beta) &= \overline{f}[\pi(x)+\pi(y)] \\ &= \overline{f}[\pi(x+y)] \\ &= f(x+y) \\ &= f(x)+f(y) \\ &= \overline{f}[\pi(x)] + \overline{f}[\,\pi(y)] \\ &= \overline{f}(\alpha) + \overline{f}(\beta) . \end{aligned}$$

§) ***($\overline{f}$ est un morphisme d'anneaux)***

$$\begin{array}{lll} \forall \alpha \in A/\mathfrak{I},\ \forall \beta \in A/\mathfrak{I}, & & \\ \forall x \in A,\ \forall y \in A, & \big(\alpha = \pi(x) \text{ et } \beta = \pi(y) & \Rightarrow \ \overline{f}(\alpha * \beta) \\ & & = \ \overline{f}(\pi(x) * \pi(y)) \\ & & = \ \overline{f}(\pi(x * y)) \\ & & = \ f(x * y) \\ & & = \ f(x) * f(y) \\ & & = \ \overline{f}(\alpha) * \overline{f}(\beta)\big) \end{array}$$

De plus $\overline{f}(1) = \overline{f}[\pi(1)] = f(1) = 1$.

iii) ∗) ***($\overline{f}$ est injective)***

$$\forall \alpha \in A/\mathfrak{I},\ \exists x \in A,\ \alpha = \pi(x) .$$

$$\overline{f}(\alpha) = 0 \Leftrightarrow \overline{f}[\pi(x)] = 0 \Leftrightarrow f(x) = 0 \Leftrightarrow x \in \operatorname{Ker} f = \mathfrak{I} \Leftrightarrow \alpha = 0 .$$

†) ***(surjectivité)***
Si f est surjective, $\forall y \in B,\ \exists x \in A,\ f(x) = y$. Alors $\overline{f}[\pi(x)] = y$.

Remarque VII.7.9 Notons que dans la preuve de la proposition VII.7.8, nous avons redonné des arguments que nous avions déjà donnés dans la preuve de la proposition V.5.4 et qu'on aurait pu simplement déduire les résultats concernant la structure de groupe de l'anneau $(A, +, *)$ de cette même proposition V.5.4.

Corollaire VII.7.10 (de la proposition VII.7.8) *Étant donné un morphisme d'anneaux $f : A \to B$ il existe un unique isomorphisme d'anneaux*

$$\overline{f} : A/\mathrm{Ker}\, f \cong \mathrm{Im}\, f \text{ tel que } f = \overline{f} \circ \pi$$

où $\pi : A \to A/\mathrm{Ker}\, f$ est la surjection canonique. En particulier si f est surjectif

$$\overline{f} : A/\mathrm{Ker}\, f \cong B$$

est un isomorphisme.

Preuve : *Il suffit d'appliquer la proposition VII.7.8 à $\mathfrak{I} := \mathrm{Ker}\, f$.*

Corollaire VII.7.11 *Étant donné un morphisme surjectif d'anneaux $p : A \to B$, il existe un unique isomorphisme d'anneaux*

$$\phi : A/\mathrm{Ker}\, p \to B \text{ tel que } p = \phi \circ \pi \text{ où } \pi : A \to A/\mathrm{Ker}\, p \text{ est la surjection canonique .}$$

Preuve : *C'est une conséquence immédiate du corollaire VII.7.10 puisque $\mathrm{Im}\, p = B$.*

Remarque VII.7.12 Les constructions du début de ce paragraphe et en particulier les propositions VII.7.3 et VII.7.8 peuvent être faites, sans presque d'ajout aux preuvent, dans le cadre de structures algébriques qui sont des groupes abéliens. Ainsi on obtiendrait facilement des résultats analogues dans le cas où A est un espace vectoriel et $\mathfrak{I}$ un sous-espace vectoriel. Pour peu qu'on connaisse la définition de ces objets, le cas où A est un module et $\mathfrak{I}$ un sous-module ne présenterait aucune difficulté supplémentaire.

La proposition suivante VII.7.13 étend au cas des anneaux les constructions donées dans les propositions II.5.4 et V.5.8.

Proposition VII.7.13 *Étant donnés un entier $n \in \mathbb{N}^*$, $(A_k, +_k, *_k)_{,1\leq k\leq n}$ des anneaux*

$$\forall 1 \leq k \leq n,\ p_k : \prod_{i=1}^{n} A_i \to A_k \text{ les projections}$$

(cf. II.5.1.ii).) Alors :

i) Il existe un unique couple de lois de composition $(+,*)$ *sur* $\prod_{k=1}^{n} A_k$ *tel que pour tout* $1 \leq k \leq n$, p_k *soit un morphisme d'anneaux ; les loi* $+$ *et* $*$ *sont données par*

$$\forall\big((x_1,\dots,x_n),(y_1,\dots,x_n)\big) \in \prod_{k=1}^{n} A_k \times \prod_{k=1}^{n} A_K,$$
$$(x_1,\dots,x_n) \;+\; (y_1,\dots,y_n) \;=\; (x_1 +_1 y_1,\dots,x_n +_n y_n)\,,$$
$$(x_1,\dots,x_n) \;*\; (y_1,\dots,y_n) \;=\; (x_1 *_1 y_1,\dots,x_n *_n y_n)\,.$$

ii) Les lois $+$ *et* $*$ *étant définies sur* P *comme ci-dessus, si*

a) pour tout $1 \leq k \leq n$, 0_k *est l'élément neutre de* $(A_k,+_k)$, $(0_1,\dots,0_n)$ *est l'élément neutre pour* $+$;

b) pour tout $1 \leq k \leq n$, 1_k *est l'élément neutre de* $(A_k,*_k)$, $(1_1,\dots,1_n)$ *est l'élément neutre pour* $*$;

c) $x \in \prod_{k=1}^{n} A_k$ *est tel que pour tout* $1 \leq k \leq n$, $y_k \in A_k$ *est l'opposé de* $p_k(x)$, *alors* $(y_1,\dots,y_n)$ *est l'opposé de* x *dans* $\big(\prod_{k=1}^{n} A_k,+\big)$;

d) $x \in \prod_{k=1}^{n} A_k$ *est tel que pour tout* $1 \leq k \leq n$, $y_k \in A_k$ *est l'inverse de* $p_k(x)$, *alors* $(y_1,\dots,y_n)$ *est l'inverse de* x *dans* $\big(\prod_{k=1}^{n} A_k,*\big)$;

iii) Si pour tout $1 \leq k \leq n$, $(A_k,+_k,*_k)$ *est un anneau commutatif,* $\big(\prod_{k=1}^{n} A_k,+,*\big)$ *est un anneau commutatif.*

iv) Pour tout n*-uplet de morphismes d'anneaux*

$$f_k \;:\; B \;\to\; A_k\,,1\leq k\leq n\,,$$

il existe un unique morphisme d'anneaux

$$f \;:\; B \;\to\; \prod_{k=1}^{n} A_k \text{ tel que } \forall 1 \leq k \leq n,\; f_k \;=\; p_k \;\circ\; f\,.$$

v) Dans le cas où il existe A tel que $\forall 1 \leq k \leq n,\ A_k = A$, la bijection $\phi : A^{[1;n]} \cong \prod_{k=1}^{n} A$ définie par la proposition II.5.1.iv) est un isomorphisme, pour peu que $A^{[1;n]}$ soit muni de la structure définie par la proposition I.6.20.

Définition VII.7.14 (Anneau produit) Avec les notations de la proposition VII.7.13, les lois $+$ et $*$ définies sur $\prod_{k=1}^{n} A_k$ comme en VII.7.13.i) sont appelées *lois produits* et le triplet

$$(\prod_{k=1}^{n} G_k, +, *)$$

anneau produit.

Remarque VII.7.15 On constatera que, contrairement aux points V.5.8.i) à V.5.8.v), le point V.5.8.vi) ne peut se formuler de manière identique dans le cas des anneaux. En effet, en reprenant les notations de V.5.8.vi), l'application

$$i_1 : A_1 \to A_1 \times A_2 \text{ , (resp. } i_2 : A_2 \to A_1 \times A_2 \text{)}$$

n'est pas un morphisme d'anneaux ; et son image n'est donc pas un sous-anneau de $A_1 \times A_2$ (voir la remarque VII.3.2.iii).) On pourrait néanmoins vérifier (et c'est un bon exercice) que $\operatorname{Im} i_1$ et $\operatorname{Im} i_2$ sont des idéaux de $A_1 \times A_2$ et qu'on a toujours

$$\operatorname{Ker} p_1 = \operatorname{Im} i_2 \text{ et } \operatorname{Ker} p_2 = \operatorname{Im} i_1 \text{ (cf. V.5.8.vi).c),)}$$

ainsi que

$$p_1 \circ i_1 = \operatorname{Id}_{A_1} \text{ et } p_2 \circ i_2 = \operatorname{Id}_{A_2} \text{ (cf. V.5.8.vi).b).)}$$

VII.8 . −Exercices

Exercice VII.8.1 Faire la preuve de la proposition VII.1.9.

Exercice VII.8.2 Donner la preuve de VII.1.4.i). Ce résultat reste-t-il vrai si G n'est plus supposé abélien ?

Exercice VII.8.3 Faire la preuve de la proposition VII.1.15.

Exercice VII.8.4 Pour un anneau A, le fait que A soit intègre (respectivement un corps) entraîne-t-il que l'anneau A^E considéré à la proposition VII.1.15 soit intègre (resp. un corps ?)

Exercice VII.8.5 Faire la preuve du lemme VII.2.7.

Exercice VII.8.6 Donner les détails de l'argument dans la remarque VII.3.2.iii).

Exercice VII.8.7 Faire la preuve de la proposition VII.3.3. À noter qu'une bonne partie de cette preuve a déjà été faite pour prouver la proposition III.3.4.

Exercice VII.8.8 Expliquer pourquoi le noyau d'un morphisme d'anneaux n'est pas en général un sous-anneau de l'ensemble de départ.

Exercice VII.8.9 Faire la preuve de la proposition VII.4.2.

Exercice VII.8.10 Faire la preuve de la proposition VII.4.6.

Exercice VII.8.11 Faire la preuve du lemme VII.6.3.

Exercice VII.8.12 Que devient l'énoncé de la proposition VII.7.3 si $\mathfrak{I} = A$?

Exercice VII.8.13 Soit $X \subset A$.

1) Montrer que (X) est le plus petit idéal contenant X au sens de l'inclusion ; c'est-à-dire que, (X) est un idéal contenant X et pour tout idéal $\mathfrak{I}$ contenant X, $(X) \subset \mathfrak{I}$.

2) Montrer que si $Y \subset A$ est une autre partie de A,

$$(X \cup Y) = (X) + (Y) .$$

Exercice VII.8.14 Étant donné un morphisme d'anneau $f : A \to B$, montrer que :

1) si f est surjectif, pour tout idéal $\mathfrak{I}$ de A, $f(\mathfrak{I})$ est un idéal de B ;

2) pour tout idéal premier $\mathfrak{p}$ de B, $f^{-1}(\mathfrak{p})$ est un idéal premier de A.

Exercice VII.8.15 Soient A un anneau commutatif, $\mathfrak{I}$ et $\mathfrak{J}$ des idéaux de A. On note

$$\pi_{\mathfrak{I}} : A \to A/\mathfrak{I} \text{ et } \pi_{\mathfrak{J}} : A \to A/\mathfrak{J}$$

les surjections canoniques (cf. VII.7.5,) et

$$\pi : A \to A/\mathfrak{I} \times A/\mathfrak{J}$$

le morphisme qui s'en déduit grâce à VII.7.13.iv) autrement dit,

$$\forall x \in A,\ \pi(x) = \big(\pi_{\mathfrak{I}}(x), \pi_{\mathfrak{J}}(x)\big) .$$

1) Montrer que $\operatorname{Ker} \pi = \mathfrak{I} \cap \mathfrak{J}$.

2) En déduire qu'il existe un unique morphisme injectif d'anneaux

$$\gamma \, : \, A/(\mathfrak{I} \cap \mathfrak{J}) \, \to \, A/\mathfrak{I} \times A/\mathfrak{J}$$

vérifiant

$$\gamma \, \circ \, \pi_{\mathfrak{I}\cap\mathfrak{J}} \, = \, \pi$$

où

$$\pi_{\mathfrak{I}\cap\mathfrak{J}} \, : \, A \, \to \, A/(\mathfrak{I} \cap \mathfrak{J})$$

est la surjection canonique.

3) Le morphisme γ étant construit comme à la question 2), montrer que si $\mathfrak{I}$ et $\mathfrak{J}$ sont comaximaux (cf. VII.4.18,) γ est surjective et donc un isomorphisme.

Exercice VII.8.16 1) Montrer que

$$\forall X \, \subset \, A, \forall Y \, \subset \, A, \mathcal{D}(X \cup Y) \, = \, \mathcal{D}(X) \, \cap \, \mathcal{D}(Y) \, .$$

2) En déduire que s'il existe $(x, y) \in X \times X$ premiers entre eux, les éléments de X sont premiers entre eux dans leur ensemble.