Algèbre Approfondie

Notes de Cours

2011

Table des matières

1 Groupes

1.1 Groupes

Définition 1.1 (*Groupe*)

Un groupe est un ensemble G muni d'une opération interne $\cdot$ vérifiant :

G1 *$\cdot$ est associative,*

G2 *Il existe un élément neutre (notation : 1 ou e),*

G3 *Tout élément est inversible (notation : x^{-1}).*

Si de plus la loi est commutative, on dit que le groupe est abélien, et on note la loi $+$, le neutre 0, et l'inverse $-x$.

Définition 1.2 (*Produit direct*)

Si $(G, \cdot)$ et $(G', *)$ sont des groupes, on définit le groupe produit direct $(G \times G', \square)$ par :

$$\begin{array}{rccc} \square : & (G \times G') \times (G \times G') & \longrightarrow & G \times G' \\ & ((g, g'), (\gamma, \gamma')) & \longmapsto & (g \cdot \gamma, g' * \gamma') \end{array}$$

Proposition 1.1

Soit G un groupe, et $g \in G$.
- *L'élément neutre est unique,*
- *L'inverse de g est unique.*

1.2 Morphisme de groupes

Définition 1.3 (*Morphisme de groupe*)

Soient $(G, \cdot)$ et $(G', *)$ deux groupes, et $\varphi : G \longrightarrow G'$. On dit que φ est un morphisme de groupe, ou un homomorphisme si :

$$\forall g, \gamma \in G,\ \varphi(g \cdot \gamma) = \varphi(g) * \varphi(\gamma)$$

Proposition 1.2

L'image du neutre de G est le neutre de G'.
L'image de l'inverse d'un élément $g \in G$ est l'inverse de l'image de g.

Définition 1.4

- *Un isomorphisme est un morphisme bijectif.*
- *Un endomorphisme est un morphisme d'un groupe dans lui-même.*
- *Un automorphisme est un endomorphisme bijectif.*

Définition 1.5 (*Ordre d'un groupe fini*)

Si G est un groupe fini, on appelle ordre du groupe et on note $\#G = |G| = \mathrm{o}(G)$ le nombre de ses éléments.

Définition 1.6 (*Puissances*)

Si G est un groupe, et $x \in G$, on définit les puissances de x pour $n \in \mathbb{N}^*$.

$$x^n := \underbrace{x \cdots x}_{n \text{ fois}} \qquad x^0 := e_G \qquad x^{-n} := \underbrace{x^{-1} \cdots x^{-1}}_{n \text{ fois}}$$

Définition 1.7 (*Ordre d'un élément*)

Soit x un élément d'un groupe G. S'il existe $k \in \mathbb{N}^*$ tel que $x^k = e$, on appelle ordre de x et on note $|x| = \mathrm{o}(x)$, le plus petit des tels k.

1.3 Sous-groupes

Définition - Proposition 1.8 (*Sous-groupe*)

Soient $(G, \cdot)$ un groupe, et H un sous-ensemble non vide G.
Si $\forall x, y \in H,\ x^{-1}y \in H$, alors on dit que H est un sous-groupe de G. On montre facilement que dans ce cas c'est un groupe pour la loi induite par celle de G. On note alors $H < G$.

Remarque : On peut remplacer les conditions précédantes sur H par :

1. $e \in H$,
2. $\forall x, y \in H,\ xy \in H$,
3. $\forall x \in H,\ x^{-1} \in H$.

Proposition 1.3 (*Intersection de sous-groupes*)

Un intersection quelconque de sous-groupes est encore un sous-groupe.

Définition - Théorème 1.9 (*Sous-groupe engendré*)

Si X est un sous-ensemble d'un groupe G, alors il existe un plus petit sous-groupe de G qui contient X. On l'appelle sous-groupe engendré par X et on le note $< X >$.
Si $X = \{g_1, \cdots, g_n\}$ est fini, on note $< X > = < g_1, \cdots, g_n >$.

Définition 1.10 (*Mot sur X*)

Si X est un sous-ensemble d'un groupe G, on définit l'ensemble des mots sur X :

$$\{e\} \cup \left\{ \omega = x_1^{e_1} \cdots x_n^{e_n} \in G \mid x_i \in X, e_i \in \{-1, 1\} \right\}$$

Théorème 1.4

Si X est un sous-ensemble d'un groupe G, alors :
– Si $X = \emptyset$, alors $< X > = \{e\}$,
– Sinon $< X >$ est l'ensemble des mots sur X.

Cas particulier : Si $X = \{a\} \subset G$ avec $a \in G$, alors $< X > = < a >$ est l'ensemble des puissances de a. On l'appelle le sous-groupe cyclique engendré par a.

Définition 1.11 (*Classes d'un sous-groupe*)

Soient $H < G$. Pour $g \in G$ on définit :
– $gH = \{gh \mid h \in H\}$ la classe à gauche de g modulo H,
– $Hg = \{hg \mid h \in H\}$ la classe à droite de g modulo H.

Remarque : En général un classe ne contient pas le neutre et n'est donc pas un sous-groupe.

Lemme 1.5

Soient $H < G$ et $a, b \in G$.
- *$aH = bH \Leftrightarrow a^{-1}b \in H$,*
- *$Ha = Hb \Leftrightarrow ab^{-1} \in H$,*
- *$aH = bH$ ou bien $aH \cap bH = \emptyset$.*

Théorème 1.6 (*Lagrange*)

Si $H < G$ avec G fini, alors l'ordre de H divise celui de G : $|H| \mid |G|$

Corollaire 1.7

Le nombre de classes à gauche est égal au nombre de classes à droite.

Définition 1.12 (*Indice d'un sous-groupe*)

L'indice $[G : H]$ d'un sous-groupe H est le nombre de classes modulo H :

$$|G| = [G : H] \cdot |H|$$

et si G est fini :

$$[G : H] = \frac{|G|}{|H|}$$

Corollaire 1.8

- *Si G est un groupe fini d'ordre premier, ses seuls sous-groupes sont le groupe trivial et lui même.*
- *Si G est un groupe fini, l'ordre de tout élément divise l'ordre du groupe.*

Remarque : Tout groupe fini d'ordre premier est cyclique et abélien (car engendré par chacun des éléments différents du neutre).

Proposition 1.9 (*Sous-groupes noyau et image*)

Si φ est un homomorphisme entre les groupes G et G', alors :
- Ker φ *est un sous-groupe de G,*
- Im φ *est un sous-groupe de G'.*

Proposition 1.10 (*Caractérisation de l'injectivité d'un morphisme*)

Si φ est un homomorphisme entre les groupes G et G', alors φ est injective si et seulement si Ker $\varphi = \{e_G\}$.

Démonstration :

Si φ est injective, assez clairement Ker $\varphi = \{e_G\}$.

Réciproquement on suppose que Ker $\varphi = \{e_G\}$ et on considère $x, y \in G, \varphi(x) = \varphi(y)$. Alors $\varphi(x)\varphi(y)^{-1} = \varphi(x)\varphi(y^{-1}) = \varphi(xy^{-1}) = e_{G'}$ donc $xy^{-1} = e_{G'}$ d'où $x = y$. ■

1.4 Le groupe symétrique $\mathcal{S}_X$

Définition 1.13 (*Groupe symétrique de X*)

Soit X un ensemble non vide. L'ensemble $\mathcal{S}_X$ des permutations de X (ie : des bijections de X dans lui même) est appelé le groupe symétrique de X.

Si $\#X = n \in \mathbb{N}^*$, on identifie $\mathcal{S}_X$ avec $\mathcal{S}_n := \mathcal{S}_{[1\cdots n]}$.

Définition 1.14 (*Fixer - déplacer*)

Si $x \in X$ et $\alpha \in \mathcal{S}_X$, on dit que α fixe, ou stabilise, x si $x = \alpha(x)$. Sinon on dit que α déplace x.

Définition 1.15 (*Cycle - Transposition*)

On dit que $\alpha \in \mathcal{S}_X$ est un r-cycle si il existe $\{i_1, \cdots, i_r\} \subset X$ tels que α fixe $X \setminus \{i_1, \cdots, i_r\}$ et $\forall j \in [1, r-1],\ \alpha(i_j) = i_{j+1}$ et $\alpha(i_r) = i_1$.
Un 2-cycle est appelé une transposition.

Définition 1.16 (*Permutations disjointes*)

Deux permutations sont dites disjointes si leurs supports sont disjoints.

Lemme 1.11

Deux cycles disjoints commutent.

Théorème 1.12 (*Décomposition en produits de cycles disjoints*)

Toute permutation se décompose en produit de cycles disjoints. Une telle factorisation est unique à permutation des cycles près.

Corollaire 1.13

Toute permutation se décompose en produit de transpositions. Cette décomposition n'est en général pas unique.

Définition - Théorème 1.17

Il existe une application $\varepsilon : \mathcal{S}_n \longrightarrow \{-1, 1\}$, appelée signature telle que :

1. *Si τ est une transposition, $\varepsilon(\tau) = -1$,*
2. *$\forall s,\ \sigma \in \mathcal{S}_n, \varepsilon(\tau \circ \sigma) = \varepsilon(s)\varepsilon(\sigma)$.*

On dit qu'une permutation est paire si sa signature est 1, et qu'elle est impaire sinon.

1.5 Conjugaison

Définition 1.18 (*Conjugué de x*)

Soient $x, y \in G$. On dit que y est un conjugué de x s'il existe $a \in G$ tel que $y = axa^{-1}$.

Proposition 1.14

La relation d'être conjugué à un élément fixé est une relation d'equivalence.

Remarque : Si x est seul dans sa classe de conjugaison, alors $\forall a \in G, axa^{-1} = x$ donc $ax = xa$, ie : x commute avec tous les éléments de G.

Définition 1.19 (*Centre d'un groupe*)

Le centre d'un groupe G, noté $\mathrm{Z}(G)$, est l'ensemble des éléments qui commutent avec tous les autres :

$$\mathrm{Z}(G) := \{g \in G \mid \forall \gamma \in G,\ g\gamma = \gamma g\}$$

Définition 1.20 (*Centralisateur d'un élément*)

Le centralisateur de $x \in G$, noté $\mathrm{C}_G(x)$, est l'ensemble des éléments qui commutent avec x.

$$\mathrm{C}_G(x) := \{\gamma \in G \mid \gamma x = x\gamma\}$$

Proposition 1.15

$\mathrm{C}_G(x)$ est un sous-groupe de G.

Théorème 1.16

Le nombre des éléments conjugués à $x \in G$ est $[G : \mathrm{C}_G(x)]$.
En particulier si G est fini, ce nombre divise $|G|$.

Démonstration : Soit x fixé. Soient $a, b \in G$, alors :

$$(axa^{-1} = bxb^{-1}) \Leftrightarrow (b^{-1}axa^{-1}b = x) \Leftrightarrow (b^{-1}a \in \mathrm{C}_G(x)) \Leftrightarrow (a\,\mathrm{C}_G(x) = b\,\mathrm{C}_G(x))$$

Il y a donc une bijection entre les classes à gauche modulo $\mathrm{C}_G(x)$ et les conjugués de x. ■

Définition 1.21 (*Equation aux classes*)

Si G est un groupe fini, son équation aux classes est :

$$|G| = |\,\mathrm{Z}(G)| + \sum_{x_i} [G : \mathrm{C}_G(x_i)]$$

où l'on choisit un représentant x_i par classe d'équivalence.

Définition 1.22 (*Sous-groupe distingué*)

On dit qu'un sous-groupe H de G est distingué (ou normal) dans G, et on note $H \lhd G$, s'il est stable par conjugaison :

$$\forall g \in G,\ gHg^{-1} \subset H$$

Proposition 1.17

Si H est un sous-groupe distingué de G, les classes à droite coïncident avec les classes à gauche, ie : $\forall g \in G,\ gH = Hg$. De plus on a l'égalité $\forall g \in G,\ gHg^{-1} = H$.

Proposition 1.18 (*Intersection de sous-groupes distingués*)

L'intersection de sous-groupes distingués de G est un groupe distingué de G.

Définition - Théorème 1.23 (*Normalisateur*)

Si H est un sous-ensemble d'un groupe G, on définit N_H le normalisateur de H :

$$\mathrm{N}_H := \{x \in G \,|\, xHx^{-1} = H\}$$

Alors N_H est un sous-groupe de G. Si de plus H est un groupe, alors N_H est distingué.
Le normalisateur est le plus grand sous-groupe tel que $H \lhd \mathrm{N}_H$.

Proposition 1.19

Si $K < \mathrm{N}_H$, alors $H \lhd KH < G$.

1.6 Les trois théorèmes d'isomorphisme

Définition 1.24 (*Groupe quotient*)

Si $H \lhd G$, on note G/H l'ensemble des classes modulo H. Alors G/H hérite d'une structure de groupe.

Démonstration : On définit le produit suivant : $(xH)\cdot(yH) := (xy)H$. On vérifie alors facilement que les axiomes sont vérifiés. ■

Théorème 1.20 (*Noyau et groupe distingué*)

H est un sous-groupe distingué de G si et seulement si H est le noyau d'un morphisme de groupe.

Démonstration : On a déjà vu qu'un noyau est distingué. Et réciproquement, on construit :
$\varphi : G \ni x \mapsto xH \in G/H$. ■

Théorème 1.21 (*Premier théorème d'isomorphisme*)

Si $\varphi : G \longrightarrow G'$ est un homomorphisme entre les groupes G et G', alors :

$$G/\operatorname{Ker}\varphi \simeq \operatorname{Im}\varphi$$

Démonstration :

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & G' \\ \pi \downarrow & & \uparrow i \\ G/\operatorname{Ker}\varphi & \xrightarrow{\tilde{\varphi}} & \operatorname{Im}\varphi \end{array}$$

π est la projection canonique
i est l'injection canonique
$\tilde{\varphi} : G/\operatorname{Ker}\varphi \ni x\operatorname{Ker}\varphi \longmapsto \varphi(x) \in \operatorname{Im}\varphi$

On montre que $\tilde{\varphi}$ est un isomorphisme :
- $\tilde{\varphi}((x\operatorname{Ker}\varphi)(y\operatorname{Ker}\varphi)) = \tilde{\varphi}((xy)\operatorname{Ker}\varphi) = \varphi(x)\varphi(y) = \tilde{\varphi}(x\operatorname{Ker}\varphi)\tilde{\varphi}(y\operatorname{Ker}\varphi)$
- $\operatorname{Ker}\tilde{\varphi} = \operatorname{Ker}\varphi = e_{G/\operatorname{Ker}\varphi}$

■

Théorème 1.22 (*Troisième théorème d'isomorphisme*)

Soient G un groupe et $K \lhd H \lhd G$. Alors :

$$H/K \lhd G/K \quad \text{et} \quad (G/K)\big/(H/K) \simeq G/H$$

Théorème 1.23 (*Deuxième théorème d'isomorphisme*)

Soient G un groupe, $H < G$, et $K < G$. On suppose $H \subset \mathrm{N}_K$ (ce qui est en particulier le cas si $H \lhd G$). Alors :

1. $$H \cap K \lhd H \quad \text{et} \quad HK = KH < G$$
2. $$H\big/(H \cap K) \simeq (KH)\big/K$$

Définition 1.25 (*Suite exacte*)

Soient $(G_1, \cdots, G_n)$ des groupes et $(f_1, \cdots, f_{n-1})$ des morphismes tels que $f_i : G_i \longrightarrow G_{i+1}$. On dit que cette suite est exacte si pour chaque i :

$$\operatorname{Im} f_i = \operatorname{Ker} f_{i+1}$$

Définition 1.26 (*Groupe résoluble*)

Un groupe G est dit résoluble s'il existe une suite finie :

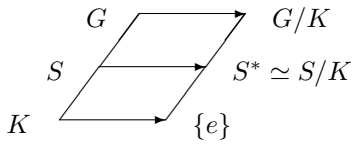
$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{e\}$$

telle que pour chaque i, G_{i-1}/G_i soit abélien. Dans ce cas une telle suite est appelée suite de résolubilité.

Théorème 1.24 (*Théorème de correspondance*)

Soient $K \lhd G$ et $\pi : G \longrightarrow G/K$. Alors π définit une correspondance entre les sous-groupes de G qui contiennent K et les sous-groupes de G/K. En notant S^* le sous-groupe de G/K correspondant au sous-groupe S de G, on a :

1. $S^* \simeq S/K \simeq \pi(S)$,
2. $T \subset S \subset K \Leftrightarrow T^* \subset S^*$,
3. $T \lhd S \Leftrightarrow T^* \lhd S^*$, *et* $S/T \simeq S^*/T^*$.



Théorème 1.25 (*Caractérisation d'un groupe résoluble*)

Si $H \lhd G$, alors G est résoluble si et seulement si H et G/H le sont.

Définition 1.27 (*Groupe simple*)

Un groupe est dit simple s'il n'est pas trivial, et qu'il ne contient aucun sous-groupe distingué propre (ie : différent de G).

Théorème 1.26

Soit G contenant deux sous-groupes distingués H et K avec $H \cap K = \emptyset$ et $HK = G$. Alors $G \simeq H \times K$.

Théorème 1.27

Soit $G = H \times K$ avec $H, K < G$. Soient $H_1 < H$ et $K_1 < K$. Alors :

1. $H_1 \times K_1 \lhd H/K$
2. $G/(H_1 \times K_1) \simeq (H/H_1) \times (K/K_1)$

Démonstration :

On définit les projections :

$$\pi_1 : \begin{array}{ccc} G & \longrightarrow & H/H_1 \\ (h,k) & \longmapsto & hH_1 =: \overline{h} \end{array} , \pi_2 : \begin{array}{ccc} G & \longrightarrow & K/K_1 \\ (h,k) & \longmapsto & kK_1 =: \overline{k} \end{array}$$

Et on considère :

$$\varphi : \begin{array}{ccc} G & \longrightarrow & (H/H_1) \times (K/K_1) \\ (h,k) & \longmapsto & (\pi_1(h,k), \pi_2(h,k)) =: (\overline{h}, \overline{k}) \end{array}$$

Comme π_1 et π_2 sont des homomorphismes, φ est aussi un homomorphisme. De plus :

$$\begin{array}{rl} \text{Im } \varphi = & (H/H_1) \times (K/K_1) \\ \text{Ker } \varphi = & H_1 \times K_1 \end{array}$$

On peut ainsi conclure par le premier théorème d'isomorphisme.

Le premier point du théorème se démontre facilement. ■

Application : Si $G = H \times K$, on a $G/(H \times \{e\}) \simeq K$.

1.7 Actions de groupes

Définition 1.28 (*Action d'un groupe G sur un ensemble X*)

On dit que G agit sur X s'il existe une fonction $\cdot$ telle que :

1. $\begin{array}{rccc} \cdot : & G \times X & \longrightarrow & X \\ & (g,x) & \longmapsto & g\cdot x \end{array}$
2. $\forall g,h \in G,\ \forall x \in X,\ g\cdot(h\cdot x) = (gh)\cdot x$
3. $\forall x \in X,\ e\cdot x = x$

Remarque : Il existe toujours une action triviale telle que $\forall g \in G,\ \forall x \in X,\ g\cdot x = x$.

Autre point de vue : Une action peut également être vue comme un homomorphisme entre G et $\mathcal{S}_X$.

$$\begin{array}{rccccccc} \varphi : & G & \longrightarrow & \mathcal{S}_X & & & & \\ & g & \longmapsto & \varphi(g) : & X & \longrightarrow & X \\ & & & & x & \longmapsto & \varphi(g)(x) = g\cdot x \end{array}$$

Définition 1.29 (*Action transitive*)

On dit que G agit transitivement sur X si :

$$\forall x,y \in X,\ \exists g \in G,\ g\cdot x = y$$

Définition 1.30 (*Action fidèle*)

On dit que G agit fidèlement sur X si :

$$\forall g \in G, [(\forall x \in X, g\cdot x = x) \Rightarrow (g = e)]$$

Remarques :

- Avec le second point de vue, une action est fidèle si et seulement si $\mathrm{Ker}\ \varphi = \{e\}$, ie : φ injective.
- Si G n'agit pas fidèlement, on peut quotienter par $\mathrm{Ker}\,(\varphi)$ pour obtenir une action fidèle.
- Si G n'agit pas transitivement, on peut introduire la relation d'équivalence suivante :

$$x\mathcal{R}y \Longleftrightarrow \exists g \in G, g\cdot x = y$$

Les classes d'équivalences sont appellée les orbites. Pour $x \in X$ on note $\omega(x) := \{g\cdot x \mid g \in G\}$ son orbite.

Exemples :

1. $\mathcal{GL}_n(\mathbb{R})$ agit transitivement sur $\mathbb{R}^n \setminus \{0\}$. En particulier, il n'y a qu'une seule orbite qui est $\mathbb{R}^n \setminus \{0\}$.
2. On rappelle que $\mathcal{O}(n) := \{M \in \mathcal{GL}_n(\mathbb{R}) \mid {}^tMM = \mathrm{Id}_n\}$. Les orbites de $\mathcal{O}(n)$ sont les sphères centrées en l'origine.

Définition 1.31 (*Stabilisateur de x dans G*)

Soient G agissant sur X et $x \in X$. On appelle stabilisateur de x dans G l'ensemble :

$$\mathrm{Stab}_G(x) := \{g \in G \mid g\cdot x = x\}$$

Proposition 1.28 (*Stabilisateur*)

Le stabilisateur de tout élément de X est un sous-groupe de G.

Démonstration : Vérifier chaque axiome. ■

Proposition 1.29 (*Stabilisateur - Orbite*)

L'application suivante est une bijection :

$$\begin{array}{rccc} \varphi : & G/(\mathrm{Stab}_G(x)) & \longrightarrow & \omega(x) \\ & \overline{g} & \longmapsto & g\cdot x \end{array}$$

Démonstration :

On commence par montrer que φ est bien définie. Soient $g, g' \in G$ tels que $g^{-1}g' \in \mathrm{Stab}_G(x)$. Alors $g\,\mathrm{Stab}_G(x) = g'\,\mathrm{Stab}_G(x)$ donc $(g^{-1}g')\cdot x = x$ et $g' \cdot x = g\cdot x$. Ainsi les éléments d'une même classe modulo le stabilisateur agissent de la même manière sur X.

La surjectivité étant évidente, il reste à montrer l'injectivité. Soient $g, g' \in G$ tels que $g\cdot x = g'\cdot x$. Alors $x = (g^{-1}g')\cdot x$ et $(g^{-1}g') \in \mathrm{Stab}_G(x)$. Ainsi si deux éléments agissent de la même manière sur X, alors ils sont dans la même classe d'équivalence. ■

Remarque : Si G est fini, on a $|\omega(x)| = |G|/|\,\mathrm{Stab}_G(x)|$.

Exemples : – Soit $H < G$ tel que H agit sur G par multiplication à gauche. Alors $\omega(x) = Hx$ et $\mathrm{Stab}_H(x) = \{e\}$.
– G agit sur G par conjugaison, ie : $g\cdot x = gxg^{-1}$. Les orbites sont alors les classes de conjugaison et $\mathrm{Stab}_G(x) = \mathrm{C}_x$ car $(gxg^{-1} = x) \Leftrightarrow (gx = xg)$. Le nombre de conjugués est $|\omega(x)| = [G : \mathrm{C}_x] = |G|/|\,\mathrm{C}_x\,|$ si G est fini.

Théorème 1.30 (*Cayley - 1878*)

Soit G un groupe. Alors :
– G s'injecte dans $\mathcal{S}_G$.
– Si G est fini, $|G| = n$, alors G est isomorphe à un sous-groupe de $\mathcal{S}_n$.

Proposition 1.31

Pour $n \geq 5$, les cycles de longueur 3 sont conjugués dans A_n.

Lemme 1.32

Le groupe A_n est $(n-2)$ transitif sur $(1, \cdots, n)$.
Cela signifie que l'on choisit $n-2$ éléments que l'on envoie transitivement sur n éléments. Si $a_1, \cdots, a_{n-2}$ sont distincts et $b_1, \cdots, b_{n-2}$ aussi, alors :

$$\exists \sigma \in A_n,\ \forall i \in [1, n-2],\ \sigma(a_i) = b_i$$

Démonstration : Si la permutation $\sigma' \in S_n$ qui envoie chaque a_i sur b_i est dans A_n il n'y a rien à montrer. Sinon on considère $\tau = (a_{n-1}, a_n)$ et ainsi $\sigma' \circ \tau =: \sigma$ convient. ■

Exemple : Soit $H < G$ et G/H les classes à gauche modulo H.
G agit sur G/H par $g\cdot(aH) = (ga)H$. Cette action est transitive mais elle n'est en général pas fidèle. Si $\varphi : G \longrightarrow \mathcal{S}_{G/H}$, alors $\mathrm{Ker}\,(\varphi) = \cup_{a\in G} aHa^{-1}$.
En particulier, $G/\,\mathrm{Stab}_G(x) \simeq \omega(x)$ par une seule bijection et donc l'action de G sur $\omega(x)$ ne peut être que l'action naturelle de G sur $G/\,\mathrm{Stab}_G(x)$.

Proposition 1.33 (*Application*)

Si G est un groupe infini, $H < G$, $H \neq G$, et $[G : H] = n < \infty$, alors G n'est pas simple.

Démonstration : G agit sur G/H d'où un homomorphisme $\varphi : G \longrightarrow \mathcal{S}_{G/H} \simeq \mathcal{S}_n$ dont le noyau est un sous-groupe distingué de G qui ne peut être $\{e\}$ car G est infini. ■

Example : Si X est l'ensemble des sous-groupes d'un groupe G, on peut faire agir G sur X par automorphisme intérieur (ie : par conjugaison).
Si $H \in X, g \in G, g\cdot H = ghg^{-1}$. Le stabilisateur de H est alors son normalisateur.

1.8 Groupe abélien de type fini

Définition 1.32 (*Groupe abélien de type fini*)

Un groupe abélien est dit de type fini s'il existe une famille finie $(g_1, \cdots, g_n)$ qui l'engendre, ie : $G = < g_1, \cdots, g_n >$.

Remarque : On note $\mathbb{Z}^n := \mathbb{Z} \times \cdots \times \mathbb{Z} =: \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$ et on définit l'homomorphisme surjectif :

$$\begin{array}{rccc} \varphi : & \mathbb{Z}^n & \longrightarrow & G \\ & (z_1, \cdots, z_n) & \longmapsto & z_1 g_1 + z_2 g_2 + \cdots z_n g_n \end{array}$$

Théorème 1.34 (*Classification des groupes abéliens de type fini*)

G est un groupe abélien de type fini si et seulement si :

$$G \simeq {}^{\mathbb{Z}}/_{d_1\mathbb{Z}} \oplus \cdots \oplus {}^{\mathbb{Z}}/_{d_k\mathbb{Z}} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$$

Où pour chaque i on a $d_i > 0$ et $d_i \mid d_{i+1}$

2 Anneaux

2.1 Définitons

Définition 2.1 (*Anneau*)

Soit A un ensemble et soient $+$ et $\cdot$ deux lois internes. Le triplet $(A, +, \cdot)$ est un anneau si :

A1 *$(A, +)$ est un groupe commutatif (dont le neutre est noté 0),*

A2 *$(A, \cdot)$ est un monoïde, ie :*

1. *$\exists 1 \in A,\ \forall a \in A,\ 1 \cdot a = a = a \cdot 1$,*
2. *la loi $\cdot$ est associative.*

A3 *La loi $\cdot$ est distributive par rapport à la loi $+$, ie : $\forall a, b, c \in A$:*

1. *$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$,*
2. *$(b + c) \cdot a = (b \cdot a) + (c \cdot a)$.*

Si la loi $\cdot$ est commutative, on dit que l'anneau est commutatif.
Si $(A \setminus \{0\}, \cdot)$ est un groupe, on dit que c'est un corps.

Exemples :

1. L'anneau trivial $(\{0, 1\}, +, \cdot)$, qui est même un corps.
2. $\mathbb{Z}, \mathbb{R}, \mathbb{C}$ sont des anneaux munis des lois habituelles.
3. $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ sont des anneaux pour $n > 1$, ce sont des corps pour n premier.
4. On peut définir l'anneau des fonctions $\mathcal{A}(X, A) = \{f : X \to A\}$ où A est un anneau et X un ensemble.
5. Les suites à valeurs dans $\mathbb{R}, \mathbb{Z}$, ou $\mathbb{C}$.
6. Les fonctions de $\mathbb{R}$ à valeurs dans $\mathbb{R}, \mathbb{Z}$, ou $\mathbb{C}$.
7. Les matrices carrés de taille n à coefficients dans un anneau (ce n'est pas un anneau commutatif).
8. $$\mathcal{Q} := \left\{ \begin{pmatrix} \alpha & -\overline{\beta} \\ \beta & \overline{\alpha} \end{pmatrix} \;\middle|\; \alpha, \beta \in \mathbb{C} \right\} \text{ est le corps (non commutatif) des quaternions.}$$
9. Si A et B sont des anneaux, on peut considérer l'anneau produit direct $A \times B$.
10. Si A est un anneau, on définit $A[X]$:
    (a) comme l'ensemble des suites à valeurs dans A qui s'annulent à partir d'un certain rang,
    (b) ou bien comme l'ensemble des polynômes à une indéterminée X et à coefficients dans A.
    On identifie alors X^k avec $(\underbrace{0, \cdots, 0}_{k}, 1, 0, \cdots)$.
    La multiplication suivante garantie la distributivité : $aX^k \cdot bX^l = (ab)X^{k+l}$.
11. Si A est un anneau, on définit $A[[X]]$:
    (a) comme l'ensemble des suites à valeurs dans A,
    (b) ou bien comme l'ensemble des séries formelles à coefficients dans A,
    ie : $A[[X]] := \left\{ \sum_{k \in \mathbb{N}} a_k X^k \mid \forall k \in \mathbb{N}, a_k \in A \right\}$.

Remarques : On montre facilement que $\forall x, y \in A$:
- $x \cdot 0 = 0 = 0 \cdot x$
- $(-1) \cdot x = -x = x \cdot (-1)$
- $(-x) \cdot y = -(x \cdot y) = x \cdot (-y)$
- $(-x) \cdot (-y) = x \cdot y$

Définition 2.2 (*Inversible - Diviseur de zéro*)

- *Un élément d'un anneau sera dit inversible s'il est inversible pour la multiplication.*
- *On appelle diviseur de zéro un élément $x \neq 0$ tel qu'il existe $y \neq 0$ tel que $xy = 0 = yx$.*
- *On notera $A^\times$ l'ensemble des éléments inversibles de A.*

Remarque : $A^\times$ est un groupe pour la multiplication. Ainsi, A est un corps si et seulement si $A^\times = A \setminus \{0\}$.

Définition 2.3 (*Anneau intègre*)

Un anneau intègre est un anneau sans diviseur de zéro. Lorsqu'il est de plus commutatif, il est parfois appelé domaine d'intégrité.

Notations :

Pour $n \in \mathbb{Z}$ on définit : $$nx := \begin{cases} \underbrace{x + \cdots + x}_{n \text{ fois}} & \text{si } n > 0, \\ 0 & \text{si } n = 0, \\ \underbrace{(-x) + \cdots + (-x)}_{(-n) \text{ fois}} & \text{si } n < 0. \end{cases}$$

Et pour $n \in \mathbb{N}$ on définit : $$x^n := \begin{cases} \underbrace{x \cdots x}_{n \text{ fois}} & \text{si } n > 0, \\ 1 & \text{si } n = 0. \end{cases}$$

Si de plus x est inversible, on définit pour $n \in \mathbb{N}$: $$x^{-n} := \underbrace{x^{-1} \cdots x^{-1}}_{n \text{ fois}}$$

2.2 Sous-anneaux et idéaux

Définition 2.4 (*Sous-anneau*)

Soient A un anneau, et $B \subset A$. On dit que B est un sous-anneau de A si :

1. *$(B, +)$ est un sous-groupe de $(A, +)$,*
2. *B est stable par multiplication,*
3. *$1 \in B$.*

Définition - Proposition 2.5 (*Sous-anneau engendré*)

1. *Une intersection quelconque de sous-anneaux est un sous-anneau.*
2. *Si $X \subset A$, l'intersection de tous les sous-anneaux de A qui contiennent X est un sous-anneau de A appelé anneau engendré par X.*

Exemples : 1. Le sous-anneau engendré par $\{1, i\} \subset \mathbb{C}$ est $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$.

2. Si I est un intervalle de $\mathbb{R}$, l'ensemble des fonctions continues de $\mathcal{A}(I, \mathbb{C})$ est un sous-anneau de $\mathcal{A}(I, \mathbb{C})$.

Définition 2.6 (*Idéal*)

Une partie I d'un anneau A est appelé idéal à gauche si :

1. *C'est un sous-groupe additif de A,*
2. *$\forall a \in A, \forall x \in I, a \cdot x \in I$.*

Il est appelé idéal à droite si :

1. *C'est un sous-groupe additif de A,*
2. *$\forall a \in A, \forall x \in I, x \cdot a \in I$.*

Un idéal à droite et à gauche est dit bilatère.

Définition - Proposition 2.7 (*Idéal engendré*)

- *Un intersection d'idéaux à gauche (resp. à droite, bilatère) de A est un idéal à gauche (resp. à droite, bilatère) de A.*
- *Si $X \subset A$, l'intersection de tous les idéaux à gauche (resp. à droite, bilatères) qui contiennent X est un idéal à gauche (resp. à droite, bilatère) appelé idéal engendré par X et noté (X). Si $X = \{x\}$ on note simplement (x).*

Exemples : 1. Si $a \in \mathbb{Z}$, les multiples de a forment l'idéal (a) engendré par a.

2. Si $P \in \mathbb{K}[X]$, alors (P) est un idéal de $\mathbb{K}[X]$.

Définition 2.8 (*Idéal principal - de type fini*)

Un idéal est dit principal s'il est engendré par un seul élément.
Un idéal est dit de type fini (ou de génération finie) s'il est engendré par une partie finie.
Un anneau dont tous les idéaux sont principaux est dit principal.

Proposition 2.1 ($\mathbb{Z}$ *est principal*)

Les idéaux de $\mathbb{Z}$ sont principaux.

Démonstration : Tout sous-groupe de $(\mathbb{R}, +)$ qui n'est pas dense dans $\mathbb{R}$ est de la forme $a\mathbb{Z}$. ■

Définition 2.9 (*Idéaux somme et produit*)

Soient I et J deux idéaux. On définit :

1. *L'idéal somme $I + J := \{i + j \mid i \in I, j \in J\}$ engendré par $I \cup J$.*
2. *L'idéal produit $(IJ) := \{\sum_{k=1}^{n} i_k j_k \mid i_k \in I, j_k \in J, n \ \in \mathbb{N}^*\}$ engendré par les produits.*

Définition 2.10 (*Idéaux maximaux*)

Un idéal I d'un anneau A est dit maximal si :

1. *$I \neq A$.*
2. *Les seuls idéaux contenant I sont I et A.*

Remarque : On peut donner une définition équivalente :

1. $1 \notin I$.
2. (B idéal, $B \supset I$) $\Rightarrow$ ($B = I$ ou $B = A$).

Théorème 2.2 (*Existence d'un idéal maximal*)

Tout idéal est inclu dans un idéal maximal.

Démonstration : (C'est une "Zornette")

Soit I un idéal d'un anneau A et soit M l'ensemble des idéaux contenant I et ne contenant pas 1.

$$M = \{B \subset A \mid B \text{ idéal}, \ B \supset I, \ 1 \notin B\}$$

Soit alors (I_n) une suite croissante (pour l'inclusion) d'idéaux de M. On pose $J := \bigcup_n I_n$. On a bien J est un idéal, $1 \notin J$, $J \supset I$, donc $J \in M$.

Ansi les hypothèses du lemme de Zorn étant vérifiées, on peut conclure sur l'existence d'un idéal maximal contenant I. ■

Exemple : Dans l'anneau $\mathbb{Z}$: $7\,\mathbb{Z}$, $3\,\mathbb{Z}$, et $2\,\mathbb{Z}$ sont des idéaux maximaux de $84\,\mathbb{Z}$:

$$84\,\mathbb{Z} \subset \begin{cases} 21\,\mathbb{Z} \subset \begin{cases} 7\,\mathbb{Z} \\ 3\,\mathbb{Z} \end{cases} \\ 12\,\mathbb{Z} \subset 4\,\mathbb{Z} \subset 2\,\mathbb{Z} \end{cases}$$

Définition 2.11 (*Radical de Jacobson - Anneau local*)

Soit A un idéal commutatif. On appelle radical de Jacobson, et on note $\mathrm{Rad}(A)$ *l'intersection de tous les idéaux maximaux de A.*

Si A n'a qu'un seul idéal maximal, on dit que A est un anneau local.

2.3 Morphismes d'anneaux et quotients

Définition 2.12 (*Morphisme d'anneaux*)

Soient A et B deux anneaux. Une application $f : A \to B$ est un morphismes d'anneaux si :

1. $\forall x, y \in A,\ f(x+y) = f(x) + f(y)$
2. $\forall x, y \in A,\ f(xy) = f(x)f(y)$
3. $f(1_A) = 1_B$

En particulier, si K et L sont des corps, on parle de morphismes de corps.

Remarques :

1. Un morphisme d'anneaux est en particulier un morphisme entre les groupes $(A, +)$ et $(B, +)$.
2. Si $f : A \to B$ et $g : B \to C$ sont des morphismes d'anneaux, alors $g \circ f : A \to C$ est un morphisme d'anneaux.
3. Si $f : A \to B$ est un morphisme d'anneau bijectif, alors $f^{-1} : B \to A$ est aussi un morphisme d'anneau (bijectif).
4. En notant $A^\times$ (resp. $B^\times$) l'ensemble des inversibles de A (resp. B), et si $f : A \to B$ est un morphisme d'anneaux, alors $f(A^\times) \subset B^\times$.
   Plus précisément, f induit un morphisme de groupes $A^\times \to f(A^\times)$. En effet si $x, x^{-1} \in A^\times$ alors $f(x)f(x^{-1}) = f(xx^{-1}) = f(1_A) = 1_B$ d'où $f(x) \in B^\times$
5. Si $f : A \to B$ est un morphisme d'anneau, et si A est un corps, alors f est injectif.
   En effet, si $x, y \in 1$ tels que $f(x) = f(y)$, alors $f(x) - f(y) = f(x-y) = 0$ d'où $x - y \notin A^\times$ or $A^\times = A \setminus \{0\}$ et donc $x - y = 0 \Rightarrow x = y$.
6. Soit A un anneau et $B \subset A$ un sous-anneau. Soit $i : B \to A, x \mapsto x$. Il existe une unique structure d'anneau sur B telle que i soit un morphisme d'anneau.

Définition 2.13 (*Noyau et Image d'un morphisme d'anneau*)

Soit $f : A \to B$ un morphisme d'anneau. On définit :
– *L'image* $\operatorname{Im} f = \{y \in B \mid \exists x \in A,\ y = f(x)\}$
– *Le noyau* $\operatorname{Ker} f = \{x \in A \mid f(x) = 0\}$
On précise bien que le noyau est celui du morphisme de groupe $(A, +) \to (B, +)$.

Proposition 2.3

1. *L'image d'un morphisme d'anneau est un sous-anneau.*
2. *Le noyau d'un morphisme d'anneau est un idéal bilatère.*

Démonstration : On rappelle que ce sont des sous-groupes additifs.

1. $1_B = f(1_A) \in \operatorname{Im} f$, et $\forall x', y' \in \operatorname{Im} f,\ \exists x, y \in A,\ x' = f(x),\ y' = f(y)$ donc $x'y' = f(x)f(y) = f(xy) \in \operatorname{Im} f$.
2. $\forall x \in \operatorname{Ker} f,\ \forall a, b \in A,\ f(axb) = f(a)\underbrace{f(x)}_{=0}f(b) = 0.$

■

Proposition 2.4 (*Anneau quotient*)

Soit A un anneau, I un sous-groupe de $(A, +)$, et $\pi : x \mapsto x + I$. Alors A/I possède une structure d'anneau telle que π soit un morphisme si et seulement si I est un idéal bilatère.

Dans ce cas cette structure d'anneau est unique, et on dit que A/I est l'anneau quotient de A par I.

Démonstration : On a déjà vu que $(A/I, +)$ est un sous-groupe abélien, et que π est un morphisme de groupe.

($\Leftarrow$) : $\operatorname{Ker}(\pi) = I$ donc si π est un morphisme d'anneau, alors I est un idéal bilatère.

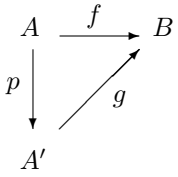
($\Rightarrow$) : Soit I un idéal bilatère. Alors on veut que π vérifie les propriétés suivantes :
– $\pi(1_A) = 1_{A/I} = 1_A + I,\ \pi(xy) = xy + I,\ \pi(x) = x + I,\ \pi(y) = y + I$

– On doit avoir la multiplication suivante : $(x+I)(y+I) = (xy+I)$
– Soient alors $i, j \in I$, on a $(x+i)(y+j) = \underbrace{xy + xj + iy + ij}_{\in I} \in (xy+I)$
c'est à dire qu'on a bien $\pi(x)\pi(y) = \pi(xy)$
– La distributivité à gauche (et de même à droite) est vérifiée car :
$(x+I)((y+I)+(z+I)) = \pi(xy+xz) = (x+I)(y+i)+(x+I)(z+I)$

Ce raisonnement conduit à construire π qui convient d'où l'existence, et ne laisse aucun choix d'où l'unicité. ■

Proposition 2.5 (*Factorisation d'un morphisme d'anneau*)

Soit $f : A \to B$ un morphisme d'anneau, et $p : A \to A'$ un morphisme d'anneau surjectif. Il existe un morphisme d'anneau $g : A' \to B$ tel que $f = g \circ p$ si et seulement si $\mathrm{Ker}\ p \subset \mathrm{Ker}\ f$.



Démonstration :

S'il existe un tel g, on vérifie que si $x \in \mathrm{Ker}\ p$ alors $f(x) = g(p(x)) = g(0) = 0$.

Réciproquement si $\mathrm{Ker}\ p \subset \mathrm{Ker}\ f$, alors $\forall a \in A',\ \exists x \in A,\ p(x) = a$ (car p surjectif). Ainsi on pose $g(a) = f(x)$ et on vérifie que g est bien définie. En effet si $p(x') = p(x) = a$, on a $p(x') - p(x) = p(x'-x) = 0$ et $x' - x \in \mathrm{Ker}\ p \subset \mathrm{Ker}\ f$. D'où $f(x'-x) = f(x') - f(x) = 0$ et $f(x') = f(x)$. ■

Proposition 2.6 (*Propriété universelle du quotient*)

Soient A est un anneau, I un idéal bilatère de A, et $\pi : A \longrightarrow A/I$ est la projection canonique. Si $f : A \longrightarrow B$ est un morphisme d'anneau tel que $I \subset \mathrm{Ker}\,(f)$, alors il existe un morphisme d'anneau $g : A/I \longrightarrow B$ tel que $g \circ \pi = f$ que l'on note généralement $\tilde{f}$.

Démonstration : C'est une conséquence de la propriété précédante en prenant $p = \pi$. ■

2.4 Algèbre

Définition 2.14 (*A-Algèbre*)

Soit A un anneau commutatif. On dit qu'un ensemble B est une A-algèbre si :

1. *B est un anneau,*
2. *$\exists \eta : A \to B$ un morphisme d'anneau tel que $\forall x \in A,\ \forall y \in B,\ \eta(x)y = y\eta(x)$.*

On dit alors que η est un morphisme structural.

Définition 2.15 (*Morphisme de A-algèbres*)

Si B et B' sont deux A-algèbres, on dit que $f : B \to B'$ est un morphisme de A-algèbres si :

1. *f est un morphisme d'anneau,*
2. *$g \circ \eta_B = \eta_{B'}$.*

Exemples : – A est une A-algèbre si A est un anneau commutatif ($\eta = \mathrm{Id}_A$).
– Tout anneau A est une $\mathbb{Z}$-algèbre ($\eta : \mathbb{Z} \ni n \longmapsto n \cdot 1_A \in A$).
– Les suites à valeurs dans un anneau A forment un anneau pour les opérations terme à terme. Si de plus A est commutatif, c'est une A-algèbre avec $\eta(a) = (a)_{n\in\mathbb{N}}$ (la suite constante).
– $\mathcal{M}_n(A)$, les matrices carrées de taille n à coefficients dans un anneaux A forment un anneau avec les opérations habituelles sur les matrices. Si de plus A est commutatif, c'est une A-algèbre avec $\eta(a) = a \cdot \mathrm{Id}$. Le lien entre ces matrices et des applications linéaires est à définir.

– $A[X]$, les polynômes à coefficients dans A est un anneau. Si de plus A est commutatif, c'est une A-algèbre avec $\eta(a) = a \cdot X^0$.

Proposition 2.7 (*Morphisme d'évaluation*)

Soient A un anneau commutatif, B une A-algèbre, et $x \in B$. Il existe un unique morphisme $e(x) : A[X] \longrightarrow B$ tel que $e(x)(X^1) = x$.
Cela donne un sens aux notions de l'évaluation et de fonction polynômiale.

Démonstration : On note $\eta : A \longrightarrow B$ le morphisme structural de B.
(unicité) Soit $e(x)$ un tel morphisme et soit $P(X) = \sum_{k=1}^{d} a_k X^k$.
En remarquant que $e(x)((a+b)X) = \eta(a+b)e(X) = (\eta(a) + \eta(b))x$. On a :

$$\begin{aligned} e(x)(P(X)) &= e(x)(\sum_{k=1}^{d} a_k X^k) &&= \sum_{k=1}^{d} e(x)(a_k X^k) \\ &= \sum_{k=1}^{d} \eta(a_k) e(x)(X^k) &&= \sum_{k=1}^{d} \eta(a_k)(e(x)(X))^k \\ &= \sum_{k=1}^{d} \eta(a_k) x^k \end{aligned}$$

(existence) On a vu qu'en fixant $e(x)(X) = x$ on fixe $e(x)(P(X))$ $(\forall P)$. Il reste à vérifier qu'on a bien un morphisme en posant $e(x)(aX^0) = \eta(a)$. ■

Remarque : En prenant $B = A$ on a l'évaluation classique.

2.5 Généralité sur les anneaux commutatifs

Dans toute cette partie les anneaux sont commutatifs.

2.5.1 Formule du binôme de Newton

Proposition 2.8 (*Binôme de Newton*)

Soit A un anneau et $x, y \in A$ deux éléments qui commutent. Alors :

$$(x+y)^n = \sum_{k=0}^{n} \mathrm{C}_n^k \; x^k y^{n-k}$$

C'est en particulier le cas si A est commutatif ou bien si $y = 1$.

Définition 2.16 (*Nilpotence*)

Un élément a d'un anneau A est dit nilpotent s'il existe $n \in \mathbb{N}$ tel que $a^n = 0$. On appelle indice de nilpotence le plus petit de ces entiers, et on note $\mathrm{Nil}\,(A)$ *l'ensemble des nilpotents.*

Remarque :
On remarque que si a est nilpotent de degrés d, alors $\forall x \in A$ on a : $(ax)^d = a^d x^d = 0$ d'où $ax \in \mathrm{Nil}\,(A)$.
De même, si a et b sont nilpotents de degrés d et d', alors $\forall n \geq d + d', (a+b) = 0$ d'où $(a+b) \in \mathrm{Nil}\,(A)$.

Proposition 2.9

$\mathrm{Nil}\,(A)$ *est un idéal de A.*

Remarque : Ce n'est pas le cas si A n'est pas commutatif.

2.5.2 Rappels

Définition 2.17 (*Diviseur de zéro - Anneau intègre*)

$a \in A$ est dit régulier si la multiplication par a est injective. Dans le cas contraire, on dit que a est un diviseur de zéro.

Si tous les éléments non nuls de A sont réguliers, alors on dit que c'est un anneau intègre.

Proposition 2.10

Si A est un anneau intègre, alors $A[X]$ est également intègre. De plus $\deg(PQ) = \deg(P)\deg(Q)$.

Démonstration : Il suffit de montrer que $\deg(PQ) = \deg(P) + \deg(Q)$. Ce qui est trivial si P ou Q est nul. Sinon on considère les coefficients (non nuls) des termes de plus haut degrès dont le produit sera non nul. ■

2.5.3 Propriétée des idéaux

Proposition 2.11

Si $X = (x_i)_{i \in I}$ est une famille quelconque d'éléments de A, alors :

$$(X) = \left\{ \sum_{i \in F} a_i x_i \mid F \in \mathcal{P}_{\text{finies}}(I), a_i \in A \right\}$$

En particulier si I est fini, il de considérer la somme sur $i \in I$.

Proposition 2.12

Soit $f : A \longrightarrow B$ un morphisme d'anneaux.

1. *Si $J \subset B$ est un idéal, alors $f^{-1}(J)$ est un idéal contenant* Ker f.
2. *Si de plus f est surjectif, l'image d'un idéal $I \subset A$ est un idéal $f(I) \subset B$. De plus l'application φ qui associe à un idéal $J \subset B$ l'idéal $f^{-1}(J)$ est une bijection :*

$$\varphi : \{\text{idéaux de } B\} \longrightarrow \{\text{idéaux de } A \text{ contenant } \text{Ker } f\}$$

Démonstration :

1. Soit J un idéal de B. Ker $f \subset f^{-1}(J)$ car $0 \in J$ et $f^{-1}(J)$ est évidemment un sous-groupe de $(A, +)$. Soit alors $x \in f^{-1}(J)$ et $a \in A$. On a $f(a) \in B$ et $f(x) \in J$ or J est un idéal de B donc $f(ax) = f(a)f(x) \in J$ d'où $ax \in f^{-1}(J)$.
2. (a) Soit I un idéal de A avec f surjective. Alors $f(I)$ est un sous-groupe de B. Il reste à vérifier que pour $\forall x \in f(I)$ et $\forall b \in B$ on a bien $bx \in f(I)$. Or il existe $y \in I,\ x = f(y)$ et comme f est surjective, il exsite $a \in A,\ b = f(a)$. Ainsi, $ay \in I$ car I est un idéal et : $bx = f(a)f(y) = f(ay) \in f(I)$.
   (b) Soit $\varphi : \{\text{idéaux de } B\} \longrightarrow \{\text{idéaux de } A \text{ contenant } \text{Ker}\,(f) \text{ telle que } \varphi(J) = f^{-1}(J)$.
   Par la théorie des ensembles, on a φ injective. Soit alors I un idéal de A contenant Ker f. On pose $J = f(I)$, on a clairement $I \subset f^{-1}(J)$. Par l'absurde, soit $x \in f^{-1}(J) \setminus I$ alors il exsite $y \in I,\ f(x) = f(y)$ donc $x - y \in \text{Ker } f \subset I$ donc $x \in I$ ce qui est absurde et conclut. ■

Exemple :

$I = A$ est un idéal de A tel que $1 \in f(A)$. Donc $f(A)$ est un idéal si et seulement si f est surjective.
Par exemple, soit $i : \mathbb{Z} \hookrightarrow \mathbb{Q}$, on a $i(\mathbb{Z}) = \mathbb{Z}$ qui n'est donc pas un idéal de $\mathbb{Q}$.

2.5.4 Idéaux premiers et maximaux

Proposition 2.13 (*Caractérisation d'un idéal maximal*)

Un idéal I d'un anneau A est maximal si et seulement si A/I est un corps.

Démonstration : Soit $\pi : A \longrightarrow A/I$ le morphisme surjectif canonique. D'après la proposition précédante, les idéaux de A/I sont en bijection avec les idéaux de A contenant $I = \text{Ker } \pi$.

$$\begin{aligned} I \text{ est maximal} &\Leftrightarrow A \text{ et } I \text{ sont les seuls idéaux contenant } I \\ &\Leftrightarrow A/I \text{ contient exactement deux idéaux (qui sont donc } \{0\} \text{ et } A/I) \\ &\Leftrightarrow A/I \text{ est un corps} \\ &\quad \text{(tout idéal engendré par } x \neq 0 \text{ contient alors 1 et } x \text{ est donc inversible)} \end{aligned}$$

■

Définition 2.18 (*Idéal premier*)

Un idéal I d'un anneau A est dit premier si A/I est intègre.

Remarque : C'est en particulier le cas si I est maximal.

Proposition 2.14 (*Caractérisation d'un idéal premier*)

Un idéal I d'un anneau A est premier si et seulement si :

$$I \neq A \quad et \quad \forall x, y \in A, (xy \in I) \Longrightarrow (x \in I \text{ ou } y \in I)$$

Démonstration :

Soit I un idéal premier différent de A. Soient $x, y \in A$ tels que $xy \in I$. Alors $\pi(xy) = 0 = \pi(x)\pi(y)$ or A/I intègre donc $\pi(x) = 0$ ou $\pi(y) = 0$ (ie : $x \in I$ ou $y \in Y$).

Réciproquement, soit $\pi(x)\pi(y) = 0$ alors $xy \in I$ donc par hypothèse $x \in I$ ou $y \in I$. Ainsi $\pi(x) = 0$ ou $\pi(y) = 0$ et A/I est intègre. ■

Proposition 2.15

L'ensemble $A \setminus \{A^\times\}$ des éléments non inversibles de A est la réunion de tous les idéaux maximaux de A.

Démonstration :

Un idéal maximal ne contient pas d'inversible sinon 1 serait dans l'idéal, et il ne serait pas maximal. Donc une première inclusion est satisfaite.

Réciproquement, $x \in A^\times \iff xA = A$, donc si x n'est pas inversible, $xA \neq A$ et l'idéal xA est inclu dans un idéal maximal. ■

Proposition 2.16 (*Radical de Jacobson*)

L'intersection des idéaux maximaux de A est l'ensemble des éléments $x \in A$ tels que $\forall y \in A, 1+xy$ est inversible.

Démonstration : (exo) ■

Proposition 2.17

L'intersection de tous les idéaux premiers de A est l'ensemble $\text{Nil}(A)$ *des nilpotents de A.*

Démonstration : (exo) ■

2.5.5 Anneaux de fractions

Il s'agit ici de généraliser la construction de $\mathbb{Q}$ à partir de $\mathbb{Z}$.

Définition 2.19 (*Partie multiplicative d'un anneau*)

Une partie $S \in A$ est une partie multiplicative si : $1 \in S$ et $\forall x, y \in S, xy \in S$.
On définit une relation $\mathcal{R}$ sur $S \times A$ par :

$$(s,x)\mathcal{R}(s',x') \iff \exists \sigma \in S,\ \sigma s'x = \sigma s x'$$

Remarque : La relation $\mathcal{R}$ est une relation d'équivalence. La réflexivité est la symétrie sont évidentes. Si $(s,x)\mathcal{R}(s'x')$ et $(s',x')\mathcal{R}(s'',x'')$ alors il existe $\sigma, \rho \in S,\ \sigma s x' = \sigma s' x$ and $\rho s' x'' = \rho s'' x'$. Donc :

$$\begin{array}{rcccl} \sigma\rho s' s'' x & = & \rho s'' \sigma s' & = & \rho s'' \sigma s x' \\ & = & \sigma s \rho s'' x' & = & \sigma s \rho s' x'' \\ (\sigma\rho s') s'' x & = & (\sigma \rho s') s x'' & & \end{array}$$

Définition 2.20 (*Fractions*)

On définit les fractions à dénominateur dans une partie multiplicative S par $S^{-1}A = S \times A/\mathcal{R}$ et on note x/s une classe d'équivalence.
On définit les opétions suivantes :

$$\frac{x}{s} + \frac{x'}{s'} := \frac{s'x + sx'}{ss'} \quad et \quad \frac{x}{s} \times \frac{x'}{s'} := \frac{xx'}{ss'}$$

On pose $\eta : A \longrightarrow S^{-1}A$ tel que $\eta(a) = a/1$.

Définition - Proposition 2.21 (*Algèbre des fractions*)

L'ensemble $(S^{-1}A, +, \times)$ est un anneau commutatif et η est un morphisme d'anneau de sorte que $S^{-1}A$ soit une A-algèbre.
On l'appelle l'aglèbre des fractions de A à dénominateur dans S.

Remarque : Si $s \in S$, alors $\eta(s)$ est inversible d'inverse $1/s$.

Proposition 2.18

Soient A un anneau, S une partie multiplicative de A, B une A-algèbre de morphisme structural $\eta' : A \longrightarrow B$ telle que l'image de tout élément de S est inversible dans B.
Alors il exsite un unique isomorphisme de A-algèbres $f : S^{-1}A \longrightarrow B$.

Démonstration : On veut que $f : S^{-1}A \longrightarrow B$ soit un isomorphisme :
- $f(\eta(a)) = f(1/a) = \eta'(a)$
- $\forall s \in S,\ f(1/s) = f(\eta(s)^{-1}) = f(\eta(s))^{-1} = (\eta'(s))^{-1}$

Donc $\forall a \in A,\ \forall s \in S, f(a/s) = (f(a/1 \times 1/s)) = \eta'(a) \times (\eta'(s))^{-1}$. Ceci prouve l'unicité d'un tel morphisme s'il existe. Il reste à vérifier qu'on a bien un ismorphisme $S^{-1}A \longrightarrow B$. ■

Remarque : Si A est un anneau intègre, alors $A \setminus \{0\}$ est une partie multiplicative de A.

Définition - Proposition 2.22 (*Corps des fractions d'un anneau intègre*)

On suppose que A est un anneau intègre.

1. *L'anneau $\operatorname{Frac} A := (A \setminus \{0\})^{-1}A$ est un corps appelé corps des fractions. De plus, A s'identifie à sous-anneau de $A \setminus \{0\}A$ par $a \mapsto a/1$.*
2. *Si S est une partie multiplicative ne contenant pas 0, alors :*
   $S^{-1}A \simeq \{a/s \mid a \in A,\ s \in S\} \subset \operatorname{Frac} A$.
3. *Pour tout corps K et $f : A \hookrightarrow K$ injectif, il existe un unique morphisme d'anneau $\operatorname{Frac} A \longrightarrow K$ qui prolonge f.*

Démonstration :

1. Par construction, tous les éléments de A sont inversibles.
2. (exo, évident)
3. Par la proposition précédante avec $S = A \setminus \{0\}A$, et en remarquant que K et $\operatorname{Frac} A$ sont des A-algèbres ($f(a/b) = f(a)f(b)^{-1}$).

■

Example : Exemples $\operatorname{Frac} \mathbb{Z} = \mathbb{Q}$.
Si K est un corps (ou un anneau intègre), alors $K[X]$ est également un anneau intègre. On définit $K(X) := \operatorname{Frac} K[X]$ l'ensemble des fractions rationnelles à coefficients dans K.

2.6 Anneaux euclidiens, principaux, et factoriels

2.6.1 Divisibilité

Définition 2.23 (*Divisibilité*)

Soient $x, y \in A \setminus \{0\}$. On dit que x divise (ou est un diviseur de) y s'il exsite $z \in A \setminus \{0\}$ tel que $y = xz$. On note alors $x \mid y$.

$$x \mid y \iff (y) \subset (x)$$

Remarque : La relation de divisibilité est un préordre (réflexivité et transitivité).

Proposition 2.19

Soient $x, y \in A \setminus \{0\}$. Alors pour tout $a \in A \setminus \{0\}$:

$$ax \mid ay \iff x \mid y$$

Démonstration : ($\Rightarrow$) est évident.
($\Leftarrow$) : $\exists t \in A \setminus \{0\} ay = tax$ donc $a(y - tx) = 0$ or A est intègre et $a \neq 0$ donc $y = tx$. ■

Définition 2.24

On définit la relation d'équivalence $\sim$ par :

$$x \sim y \iff x \mid y \text{ et } y \mid x$$

Proposition 2.20

$$x \sim y \iff (x) = (y) \iff \exists u \in A^\times,\ x = uy$$

En particulier, comme pour tout $x \in A \setminus \{0\},\ 1 \mid x$, on a :

$$x \mid 1 \iff x \sim 1 \iff x \in A^\times$$

Définition 2.25 (*Irréductibilité*)

Un élément $p \in A \setminus \{0\}$ est dit irréductible si :

1. $p \notin A^\times$,
2. $\forall x, y \in A \setminus \{0\},\ (p = xy) \implies (x \in A^\times \text{ ou } y \in A^\times)$.

Example : $\mathbb{Z}$, $\mathbb{Z}^\times = \{-1, 1\}$, les irréductibles sont les premiers $\mathbb{P} \cup -\mathbb{P}$.

2.6.2 Anneaux Noethériens

Commentaire : Noether est une femme.

Définition - Proposition 2.26 (*Anneau Noethérien*)

Soit A un anneau commutatif. Les assertions suivantes sont équivalentes :

1. *Toute suite croissante d'idéaux est stationnaire.*
2. *Tout idéal de A est de type fini (ie : engendré par une partie finie).*

Dans ce cas on dira que A est Noethérien

Démonstration :

$(1 \Rightarrow 2)$: Soit I un idéal de A.
- $I_1 := (x_1)$ avec $x_1 \in I$, si $I = I_1$ on a fini, sinon :
- $I_2 := (x_1, x_2)$ avec $x_2 \in I \setminus I_1$, si $I = I_1$ on a fini, sinon :
- $\cdots$

On cosntruit ainsi une suite croissante d'idéaux $I_1 \subsetneq I_2 \subsetneq \cdots \subsetneq I_n \subset I$. Donc $(I_n)_n$ est stationnaire ainsi il existe $N \in \mathbb{N},\ \forall n \geq N,\ I_n = I_N$. On vérifie aisément que $I_N = (x_1, \cdots, x_N) = I$.

$(2 \Rightarrow 1)$: Soit $(I_n)_{n\in\mathbb{N}}$ une suite croissante d'idéaux. On pose $I := \cup_{n\in\mathbb{N}} I_n$ qui est donc un idéal de type fini par hypothèse. Donc $I = (x_1, \cdots, x_k)$ et $\forall i \in [1,k],\ \exists j_i \in \mathbb{N},\ x_i \in I_{j_i}$. On montre ainsi que la suite est stationnaire à partir du rang $N := \mathrm{Sup}\{j_i \mid i \in [1,k]\}$. ■

Définition 2.27 (*Anneau principal (rappel)*)

Un anneau est dit principal s'il est intègre et que tous ses idéaux sont principaux (ie : engendré par un seul élément). En particulier un anneau principal est Noethérien.

Définition 2.28 (*Elément décomposable*)

Un élément d'un anneau est dit décomposable s'il est associé à un produit fini d'irréductible.

Définition 2.29 (*Anneau factoriel*)

Soit A un anneau intègre. On dit que A est factoriel si :

F1 *Tout élément non nul de A est décomposable.*

F2 *$\forall m, n \in \mathbb{N},\ \forall p_1, \cdots, p_n$ et $\forall q_1,\ \cdots q_m$ irréductibles de A tels que les produits des p_i et des q_j sont associés. Alors $m = n$ et il existe σ bijective telle que : $\forall i,\ p_i \sim q_{\sigma(j)}$.*

Définition - Proposition 2.30 (*Valuation p-adique*)

Soit A un anneau factoriel.

1. *Soit p un irréductible de A et $a \in A\setminus\{0\}$, alors il existe un unique entier n tel que $a = \alpha p^n$ avec $\alpha \in A\setminus(p)$. On l'appelle la valuation p-adique de a et on le note $\nu_p(a)$ (on pose $\nu_p(0) := -\infty$).*
2. *Soit p irréductible, $a, b \in A$, alors $\nu_p(ab) = \nu_p(a) + \nu_p(b)$.*
3. *Soit $\mathcal{P}$ un système de représentants d'irréductibles de A (ie : tout irréductible de A est associé à un élément de $\mathcal{P}$).*
   Alors pour tout $a \in A\setminus\{0\}$, la famille $(\nu_p(a))_{p\in\mathcal{P}}$ est presque nulle (ie : sauf sur un nombre fini d'éléments). De plus a s'écrit :

$$a = u \prod_{p\in\mathcal{P}} p^{\nu_p(a)} \text{ (pour } u \in A^\times \text{)}$$

Démonstration :

1. Supposons que $a = \alpha p^n = \beta p^m$ avec $\alpha, \beta \in A\setminus(p)$ et $n < m$. Alors :

$$\alpha p^n - \beta p^m = 0 \Longleftrightarrow (\alpha + \beta p^{m-n}) \Longleftrightarrow \alpha \in (p) \text{ par intégrité de } A$$

2. Soient $a = \alpha p^n$ et $b = \beta p^m$ avec $\alpha, \beta \in A \setminus (p)$. Alors $ab = \alpha\beta p^{m+n}$ et on a toujours $\alpha\beta \in A \setminus (p)$.
3. Soit a un élément non nul de l'anneau factoriel A. On sait que a est associé à un produit fini d'iiréductibles de A. Ainsi il existe $p_1, \cdots, p_r$ irréductibles et u inversible tels que :

$$a = u\prod_{i=1}^{r} p_i^{n_i} \quad \text{on pose alors } x_r = u\prod_{i=1}^{r-1} p_i^{n_i} \quad (\text{ie : } a = xp_r^{n_r})$$

Comme $\nu_{p_r}(p_r^{n_r}) = p^{n_r}$ et $\nu_{p_r}(x) = 0$ d'après la propriété précédante on a $\nu_{p_r}(a) = n_r$. On obtient le résultat souhaité par récurrence. ■

Définition - Proposition 2.31 (*Elément premier*)

Soit A un anneau intègre et p un élément non nul. On dit que p est premier si l'idéal engendré par p est premier (ie : $A/(p)$ est intègre).

Cette définition est équivalente aux deux conditions suivantes :

1. *p n'est pas inversible.*
2. *Pour tous éléments $a, b \in A$, si p divise le produit alors p divise a ou b :*

$$p \mid ab \Longrightarrow p \mid a \text{ ou } p \mid b$$

Proposition 2.21

Dans un anneau A intègre, tout élément premier est irréductible.

Démonstration : Soit p premier. En particulier $(p) \neq A$ donc $p \notin A^\times$.

Supposons $p = xy$. Par la caractérisation des idéeaux premiers, on en déduit que $x \in (p)$ ou $y \in (p)$. Par exemple $x \in (p)$ donc $p \mid x$ et $x \mid p$ d'où $x = up$ avec $u \in A^\times$. Donc y inversible. ■

Proposition 2.22 (*Définition équivalente d'un anneau factoriel*)

F'1 *Toute suite croissante d'idéaux principaux est stationnaire.*

F'2 *Tout élément irréductible est premier.*

Démonstration :

(F'1 ⇒ F1) Soit p_0 un élément non décomposable (ie : n'est pas associé à un produits fini d'éléments irréductibles). $p_0 = xy$ avec x et y non inversibles et x ou y non décomposable. Supposons que x n'est pas décomposable alors : $I_0 := (p_0) \subsetneq (x) =: I_1 \subsetneq \cdots$ (récurrence)

(F'2 ⇒ F2) Soit $\Pi_{i=1}^n p_i \sim \Pi_{j=1}^m q_j$ deux produits d'irréductibles associé. Par hypothèse tous les irréductibles sont premiers. On va montrer par récurrence sur n que $n = m$ et $p_i \sim q_{\sigma(j)}$:

($n = 0$) Tous les q_j sont inversibles donc $m = 0$.

(hérédité) On suppose la propriété vraie pour $k = n - 1 \geq 0$. Si $\Pi_{i=1}^n p_i \sim \Pi_{j=1}^m q_j$, comme p_n est premier il divise l'un des q_j, par exemple q_m et $p_n \mid q_m \Rightarrow p_n \sim q_m$. On a encore $\Pi_{i=1}^{n-1} p_i \sim \Pi_{j=1}^{m-1} q_j$ et par hypothèse de récurrence $m - 1 = n - 1$ et il existe σ tel que $\forall (1 \leq i \leq n-1),\ p_i \sim q_{\sigma(j)}$. Il suffit alors de poser $\sigma(n) = m$ pour obtenir le résultat souhaité.

(Factoriel ⇒ F'1) Soit $\mathcal{P}$ un système de représentants d'irréductibles de A et a, b deux éléments non nuls de A. On a toujours : $b \mid a \Rightarrow \forall p \in \mathcal{P},\ \nu_p(b) \leq \nu_p(a)$ avec les $\nu_p(a)$ presque tous nuls.

Donc en particulier il exsite un nombre fini de diviseurs de a, pour tout a non nul.

Ainsi a appartient à un nombre fini d'idéaux principaux et toute suite croissante d'idéaux principaux contenant a est stationnaire.

(Factoriel ⇒ F'2) Soit p un irréductible et $x, y \in A \setminus 0$. Alors si $p \nmid x$ et $p \nmid y$ on a $\nu_p(x) = \nu_p(y) = 0$ et donc $\nu_p(xy) = 0$ ainsi $p \nmid xy$.

On a montré par contraposition la caractérisation d'un éléments premier. ■

Corollaire 2.23

Tout anneau principal est factoriel.

Démonstration :

(F'1) Principal ⇒ Noethérien ⇒ F'1.

(F'2) Soient p un irréductible et $x, y \in A$ tels que $p \mid xy$. On a $(p) \neq A$.
On pose $I := \{u \in A \,|\, p \mid uy\}$ et on vérifie que c'est un idéal de A donc il est principal par hypothèse et il existe $a \in A$ tel que $I = (a)$. Mais $p \in I$ donc $p \mid a$ or p irréductible. Deux cas sont possibles :
$(a \sim 1)$ $I = A$ et $p \mid y$.
$(a \sim p)$ $I = (p)$ or $x \in I$ donc $p \mid x$. ■

Corollaire 2.24

Soit A un anneau principal.

1. *Les idéaux de A sont l'idéal nul et ceux engendrés par les irréductibles de A.*
2. *Si A n'est pas un corps, les idéaux maximaux de A sont ceux engendrés par les éléments irréductibles.*

2.6.3 Pgcd, ppcm, élements premiers entre eux

Définition 2.32 (*Eléments premiers entre eux*)

Soient $x_1, \cdots, x_n \in A$. On dit que les x_i sont premiers entre eux si A est le plus petit idéal qui les contient tous.

Définition 2.33 (*pgcd - ppcm*)

On appelle pgcd *de $x, y \in A$ tout élément $c \in A$ tel que c soit le plus petit idéal principal contenant $(x) + (y) = (x, y)$. On note $c = \mathrm{pgcd}(x, y)$ ou $c = x \vee y$.*
On appelle ppcm *de $x, y \in A$ tout élément $d \in A$ tel que $(d) = (x) \cap (y)$. On note $d = \mathrm{ppcm}(x, y)$ ou $d = x \wedge y$.*

Remarques : Il n'y a pas toujours existence, mais dans ce cas il y a unicité à association près.
On a : $1 = x \vee y \Leftrightarrow x$ et y sont premiers entre eux.

Théorème 2.25 (*Bézout*)

Soient A un anneau principal et $x, y \in A$. Alors il existe $u, v \in A$ tels que : $ux + vy = x \vee y$.
En particulier si x et y sont premiers entre eux il existe $u, v \in A$ tels que : $ux + vy = 1$.

Démonstration : $(x) + (y) = (x, y)$ est principal donc engendré par l'élément $(x \vee y)$.
Par définition $x \vee y \in (x, y) \Rightarrow \exists u, v \in A,\ ux + vy = x \vee y$. ■

Proposition 2.26

Soit A un anneau factoriel.

1. pgcd *et* ppcm *existent toujours.*
2. *Soient $x, y \in A \setminus \{0\}$ et $\delta = x \vee y$ alors :*
   $x = \delta x_0,\ y = \delta y_0$ avec $x_0 \vee y_0 = 1$. De plus $x \wedge y = \delta x_0 y_0$.
3. *Soient $x, y, z \in A \setminus \{0\}$ tels que $x \mid yz$ et $x \wedge z = 1$ alors $x \mid y$.*

Lemme 2.27 (*Lemme chinois*)

Soit A un anneau et soient I, J deux idéaux de A tels que $I + J = A$. Alors :

$$A/(I \cap J) \simeq A/I \times A/J$$

En particulier si A est principal, $p, q \in A$ premiers entre eux, alors :

$$A/(pq) \simeq A/(p) \times A/(q)$$

Démonstration : On considère les projections canoniques $\pi : A \to A/I$ et $\pi' : A \to A/J$, et on pose :

$$\begin{array}{rccc} \varphi : & A & \longrightarrow & A/I \times A/J \\ & x & \longmapsto & (\pi(x), \pi'(x)) \end{array}$$

En remarquant que Ker $\varphi = I \cap J$, on applique le premier théorème d'isomorphisme :

$$A/(I \cap J) \simeq \text{Im } \varphi$$

Il reste à montrer que Im $\varphi = A/I \times A/J$. Or $I + J = A$ donc il existe $u \in I$ et $v \in J$ tels que $u + v = 1$. Soit alors $x, y \in A$ et $z = ux + vy$ on a $ux \in I$ et $vy \in J$

$$u + v = 1 \Rightarrow \left\{ \begin{array}{rcl} u \equiv 1(J) & \Rightarrow & \pi(z) = \pi(vy) = \pi(y) \\ v \equiv 1(I) & \Rightarrow & \pi'(z) = \pi'(ux) = \pi'(x) \end{array} \right.$$

Ainsi $(\pi(y), \pi(x)) = \varphi(z) \in \text{Im } \varphi$ d'où Im $\varphi \simeq A/I \times A/J$. ■

Définition 2.34 (*Anneau euclidien*)

On dit qu'un anneau intègre A est euclidien s'il existe une application $N : A \to \mathbb{N}$ telle que :

E1 $\forall x \in A,\ (N(x) = 0 \Leftrightarrow x = 0)$,

E2 $\forall x \in A,\ \forall y \in A \setminus \{0\},\ \exists q, r \in A,\ x = qy + r$ *avec* $N(r) < N(y)$.

Exemples :

1. Soit $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$ et $N : (a + ib) \mapsto |a + ib|^2 = a^2 + b^2$.
   (E1) Assez clair,
   (E2) Soit $\xi = x + iy \in \mathbb{C}$, alors il existe $z = a + ib \in \mathbb{Z}[i]$ tel que $N(\xi - z) < \frac{1}{2}$. En effet, il suffit de prendre $a = E(x - \frac{1}{2})$ et $b = E(y - \frac{1}{2})$.
   Soient alors $x, y \in \mathbb{Z}[i]$ avec $y \neq 0$. Soit $\xi = \frac{x}{y}$ et q tel que $N(\xi - q) < \frac{1}{2}$. On a $x = qy + r$ avec : $N(r) = |x - qy|^2 = |y|^2 |\xi - q|^2 < \frac{1}{2}|y|^2 < N(y)$.
2. Soit K un corps et $N : K[X] \to \mathbb{N}$ définit comme suit :

$$N(P) = \left\{ \begin{array}{ll} \deg P & \text{si } P \neq 0 \\ 0 & \text{si } P = 0 \end{array} \right.$$

   (E1) Assez clair,
   (E2) On vérifie que la division des polynômes convient.

Proposition 2.28

Soit A un anneau non nul et soient $P, T \in K[X]$ avec $T \neq 0$ et tels que leurs coefficients directeurs soient inversibles.

Alors il existe un unique couple $(Q, R) \in K[X] \times K[X]$ tel que $P = QT + R$ avec $N(R) < N(T$.

Théorème 2.29

Tout anneau eclidien est principal.

Remarque : Ainsi $K[X]$ est principal mais en général $A[X]$ ne l'est pas.

Démonstration : Soit I un idéal non nul de A. Il existe $y \in I \setminus \{0\}$ qui minimise N.
$\forall x \in I,\ x = qy + r \Rightarrow N(r) < N(y) \Rightarrow r = 0$. Ainsi $x \in (y)$ donc $I = (y)$. ■

3 Modules

Dans toute cette partie les anneaux sont commutatifs.

3.1 Définitions

3.1.1 Modules

Définition 3.1 (*Module*)

Soit A un anneau. Un ensemble M est un A-module s'il est muni d'une loi de composition interne "$+$" et d'une loi externe "$\cdot$" telles que :

M1 $(M,+)$ *est un groupe abélien,*

M2 $\forall a \in A,\ \forall x,y \in M,\ a(x+y) = (ax)+(ay)$,

M2' $\forall x \in M,\ \forall a,b \in A,\ (a+b)x = (ax)+(bx)$,

M3 $\forall x \in M,\ \forall a,b \in A,\ (ab)x = a(bx)$,

M3' $\forall x \in M,\ 1_A x = x$.

Attention :

Ne pas confondre les lois additive de l'anneau et du module.
Ne pas confondre la loi multiplication de la l'anneau et la loi externe.
Ne pas inventer de loi multiplicative interne dans le module.

Remarque : Si K est un corps, tout K-module est un K-espace vectoriel.

Autre point de vue : On remarque que comme $(M,+)$ est un groupe abélien, l'ensemble $\operatorname{End} M$ est un anneau (non commutatif en général). On montre alors que la donnée d'une loi externe de module revient à se donner un morphisme d'anneau $\rho : A \to \operatorname{End} M$.
En effet, si M est un module, on définit $\rho(a)(x) = ax$ qui est bien un morphisme d'anneau.
Réciproquement, si $\rho : A \to \operatorname{End} M$ est un morphisme d'anneau alors on vérifie que M est bien un module.

Exemples :

1. Un $\mathbb{Z}$-module est simplement un groupe abélien, et tout groupe abélien peut être vu comme un $\mathbb{Z}$-module.
2. A est un A-module.
3. (0) est un A-module.
4. Tout idéal d'un anneau A est un A-module.
5. Si B est une A-algèbre, et M un A-module, alors en considérant les morphismes :
   $\eta : A \to B$ et $\rho : B \to \operatorname{End} M$ on construit $\rho' = \rho \circ \eta : A \to \operatorname{End} M$ qui est aussi un morphisme.
   Donc M est un A-module et en particulier, B et ses idéaux sont des A-modules.
6. Si I est un ensemble quelconque on note A^I l'ensemble des fonctions de I dans A que l'on appelle aussi suites indexées par I. On a déjà vu que A^I est une A-algèbre.
   On définit également $A^{(I)}$ l'ensemble des suites presque nulles. On vérifie aisément que $A^{(I)}$ est un idéal bilatère de A^I. Donc A^I et $A^{(I)}$ sont des A-modules.
   Pour $i \in I$ on définit $e_i \in A^{(I)}$ tel que $(e_i)j = \delta_{ij}$. Ainsi pour tout $a = (a_i)_{i\in I} \in A^{(I)}$ on a :

   $$a = \sum_{i\in I} a_i e_i \text{ et cette somme est finie.}$$

   On appellera $(e_i)_{i\in I}$ la base canonique.

3.2 Sous-modules et applications linéaires

Définition 3.2 (*Sous-module*)

Soient M un A-module et $N \subset M$. On dit que N est un sous-module de M si :

1. *N est un sous-groupe de $(M, +)$,*
2. *N est stable pour la loi externe $A \times N \to N \subset M$.*

Remarque : Cette notion généralise celle d'idéal. En effet A est un A-module dont les sous-modules sont ses idéaux.

Définition - Proposition 3.3 (*Sous-module engendré*)

Toute intersection de sous-modules est un sous-module. En particulier, pour toute partie $X \subset M$ il existe un plus petit sous-module de M qui contient X.

On le définit comme le sous-module engendré par X et on le note $< X >$.

Définition 3.4 (*Combinaison linéaire*)

On appelle combinaison linéaire d'éléments de $X \subset M$ à coefficients dans A tout élément x de la forme :

$$x = \sum_{i \in F} a_i x_i \text{ où } F \text{ est fini, et pour tout } i \in F \text{ et } a_i \in A,\ x_i \in X$$

Proposition 3.1 (*Description du sous-module engendré*)

$< X >$ est l'ensemble des combinaisons linéaires d'éléments de X.

Définition 3.5 (*Module de type fini et cyclique*)

On dit qu'une partie X d'un module M l'engendre si $< X > = M$.

1. *On dit qu'un module est de type fini s'il est engendré par une partie finie,*
2. *On dit qu'il est cyclique s'il est engendré par un seul élément.*

Définition 3.6 (*Application linéaire*)

Soient M et N deux A-modules. Un application $f : M \to N$ est dite A-linéaire si :

1. *f est un morphisme de groupe $(M, +) \to (N, +)$,*
2. *$\forall a \in A,\ \forall x \in M,\ f(ax) = af(x)$.*

On dit aussi que f est alors un morphisme de A-modules.

Remarque :

1. La composée de deux applications A-linéaires est encore une application A-linéaire.
2. Si f est linéaire bijective alors f^{-1} est aussi linéaire. On dit alors que f est un ismorphisme de A-modules.
3. Soient M un module et M' un sous-module. Soit $i : M' \hookrightarrow M$. Alors il existe une unique structure de A-module sur M' telle que i soit linéaire.

Proposition 3.2 (*Noyau et image d'une application linéaire*)

Soit $f : M \to N$ une application linéaire. Alors :

1. Ker f *est un sous-module de M,*
2. Im f *est un sous-module de N.*

Démonstration : Ce sont des sous-groupes car f est en particulier un morphisme de groupe.
De plus, si $x \in \text{Ker } f$ et $a \in A$ alors $f(ax) = f(a)f(x) = 0$ donc $ax \in \text{Ker } f$.
De même si $y = f(x) \in \text{Im } f$ alors $ay = af(x) = f(ax) \in \text{Im } f$. ■

3.3 Produit et somme directe de modules

Définition 3.7 (*Module produit*)

Soient A un anneau, I un ensemble, et $(M_i)_{i\in i}$ une famille de A-modules indexée par I. On définit le produit $\prod_{i\in I} M_i$ (éventuellement via l'axiome du choix) que l'on muni des lois suivantes :

1. *Pour $X = (x_i)_{i\in I},\ Y = (y_i)_{i\in I},\ \in \prod_{i\in I} M_i$ on pose $X + Y = (x_i + y_i)_{i\in I} \in \prod_{i\in I} M_i$.*
2. *Et pour $a \in a$ on pose $aX = (ax_i)_{i\in I} \in \prod_{i\in I} M_i$.*

On appelle ce A-module le A-module produit des M_i.

Définition 3.8 (*Projection canonique*)

Pour chaque $j \in I$ on définit l'application linéaire $j^{\text{ème}}$ projection canonique :

$$\begin{array}{rccc} p_j : & \displaystyle\prod_{i\in I} M_i & \longrightarrow & M_j \\ & (x_i)_{i\in I} & \longmapsto & x_j \end{array}$$

Proposition 3.3

Soit M' un module. On se donne pour tout $i \in I$ une application linéaire $f_i : M' \to M_i$.
Alors il existe une unique application linéaire $f : M' \to \prod_{i\in I} M_i$ telle que :

$$f_i = p_i \circ f \text{ pour tout } i$$

Démonstration : On prend $f(x) = (f_i(x))_{i\in I}$ qui est linéaire. Il reste à vérifier l'unicité. ■

Remarque : $A^I = \prod_{i\in I} A_i$ en prenant $A_i = A$ pour chaque i.

Définition 3.9 (*Somme directe*)

Le sous ensemble du produit constitué des familles presques nulles est un sous-module appelé somme directe des M_i et noté $\bigoplus_{i\in I} M_i$.

Définition 3.10 (*Injection canonique*)

Pour chaque $j \in I$ on définit l'application linéaire $j^{\text{ème}}$ injection canonique :

$$\begin{array}{rccc} i_j : & M_j & \longrightarrow & \displaystyle\bigoplus_{i\in I} M_i \\ & x & \longmapsto & (y_i)_{i\in I} \text{ avec } y_j = x \text{ et } y_i = 0 \text{ pour } i \neq j \end{array}$$

Proposition 3.4

Soit M' un module. On se donne pour tout $i \in I$ une application linéaire $f_i : M_i \to M'$.
Alors il existe une unique application linéaire $f : \bigoplus_{i\in I} M_i \to M'$ telle que :

$$f \circ i_j = f_j \text{ pour tout } j$$

Démonstration : Soit $(x_i)_{i\in I} \in \bigoplus_{i\in I}$ alors $f((x_i)_{i\in I}) = \sum_{i\in I} f_i(x_i)$. ■

Remarque : $A^{(I)} = \bigoplus_{i\in I} A_i$ en prenant $A_i = A$ pour chaque i.

Proposition 3.5 (*Caractérisation de la somme directe*)

Soient M un module et I un ensemble. Soit $(M_i)_{i\in I}$ une famille de sous-modules telle que :

1. $\sum_{i\in I} M_i = M$ *en tant que sous-module engendré par l'union,*
2. $\forall j \in I,\ M_j \cap \sum_{i\neq j} M_i = \{0\}$.

Alors M est isomorphe à la somme directe $\bigoplus_{i\in I} M_i$. On dit dans ce cas que M est somme directe des sous-modules M_i et on note :

$$M = \bigoplus_{i\in I} M_i$$

Définition 3.11 (*Supplémentaire*)

Soit M un module et soient M', M'' deux sous-modules. On dit que M' et M'' sont supplémentaires si $M = M' \oplus M''$.

3.4 Module quotient

Définition - Proposition 3.12 (*Module quotient*)

Soient M un module et M' un sous-groupe de $(M,+)$. M' est un sous-module de M si et seulement si il existe sur le sous-groupe quotient M/M' une structure de module telle que la projection canonique $\pi : M \to M/M'$ soit linéaire.

Dans ce cas, cette structure est unique et M/M' est alors le module quotient.

Démonstration :

(rappel) On considère la congruence modulo M' telle que $x \equiv y \Leftrightarrow (x-y) \in M'$.

M/M' sont les classes d'équivalence, et $\pi : x \mapsto \overline{x}$ associe la classe d'un élément. On sait qu'il existe sur M/M' une unique loi de composition telle que : M/M' soit un groupe abélien, π soit un morphisme de groupe et Ker $\pi = M'$.

(sous-module) On suppose l'existe de la projection canonique linéaire sur le module M/M'. Alors soient $a \in A,\ x \in M'$ on a $\pi(ax) = a\pi(x) = 0$ donc $ax \in M'$ et ainsi M' est un sous-module.

(module quotient) Réciproquement, on suppose que M' est un sous-module de M.

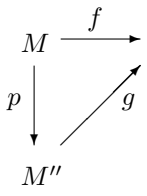
(π linéaire) Soient $\xi \in M/M'$ et $a \in A$. Il existe $x \in M$ tel que $\pi(x) = \xi$. TODO

(M1) M/M' est en particulier un groupe abélien.

(M2) TODO ... ■

Proposition 3.6 (*Factorisation*)

Soient $f : M \to N$ un morphisme de modules
et $p : M \to M'$ un morphisme de modules surjectif.



Alors les deux assertions suivantes sont équivalentes :

1. Ker $p \subset$ Ker f
2. *Il existe un morphisme de modules $g : M'' \to N$ tel que $f = g \circ p$*

Dans ce cas, un tel g est unique.

Démonstration : Soit $M' = \ker p$.

(2 $\Rightarrow$ 1) On suppose que g existe. Soit alors $x \in \ker p$. On a bien $g \circ p(x) = 0 = f(x)$ d'où l'inclusion demandée.

(1 $\Rightarrow$ 2) On suppose que Ker $p \subset$ Ker f.

(définition de g) Soit $y \in M''$ alors il existe $x \in M$ tel que $p(x) = y$ par surjectivité de p. On pose $g(y) = f(x)$ et on vérifie que pour tout $x' \in M''$ tel que $p(x) = p(x')$ on a bien $f(x) = f(x')$. En effet $p(x - x') = 0$ donc $f(x - x') = 0$.

(linéarité) Avec les mêmes notations $g(ay) = f(ax) = af(x) = ag(y)$, et si $p(x) = y$ alors $p(ax) = ap(x) = ay$.

(additivité) Soit $y' = p(y)$ et $x' = p(x)$. Alors $p(x + y) = x' + y'$ donc $g(x' + y') = f(x + y) = f(x) + f(y) = g(x') + g(y')$. ■

Théorème 3.7 (*Propriété universelle du quotient*)

Soient N un A-module, M un A-module, M' un sous module de M et $\pi : M \to M/M'$ la projection canonique. Alors il y a une équivalence entre :

1. *La donnée d'un morphisme de A-modules $g : M/M' \to N$.*
2. *La donnée d'un morphisme de A-modules $f : M \to N$ tel que $M' \subset \operatorname{Ker} f$.*

De plus, étant donné un tel morphisme f il existe une unique application A-linéaire $\tilde{f} : M/M' \to N$ tel que $\tilde{f} \circ \pi = f$ et $\operatorname{Im} \tilde{f} = \operatorname{Im} f$ et $\operatorname{Ker} \tilde{f} = \pi(\operatorname{Ker} f)$.

On dit alors qu'on obtient $\tilde{f}$ par passage au quotient.

Démonstration : C'est un corollaire de la proposition précédante en prenant $M'' = M/M'$ et $p = \pi$. ■

Proposition 3.8 (*Factorisation canonique d'un morphisme de A-module*)

Soit $f : M \to N$ une application linéaire. Alors il existe un unique isomorphisme de A-module $\tilde{f} : M/\operatorname{Ker} f \to \operatorname{Im} f$ tel que le diagramme suivant commute :

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ \pi \downarrow & & \uparrow i \\ M/\operatorname{Ker} f & \xrightarrow{\tilde{f}} & \operatorname{Im} f \end{array}$$

En particulier on a :

$$M/\operatorname{Ker} f \simeq \operatorname{Im} f$$

Démonstration : La propriété universelle du quotient, en prenant $M' = \operatorname{Ker} f$, nous assure l'existence d'un unique $\tilde{f} : M/\operatorname{Ker} f \to N$ tel que $\tilde{f} \circ \pi = f$. De plus on a $\operatorname{Im} \tilde{f} = \operatorname{Im} f$ et $\operatorname{Ker} \tilde{f} = \pi(\operatorname{Ker} f) = \{0\}$. Donc $\tilde{f}$ est un isomorphisme. ■

3.5 Suites exactes

Définition 3.13

Soient M, M', M'' des A-modules, $f : M' \to M$ et $g : M \to M''$ deux applications A-linéaires. On dit que la suite suivante est exacte si $\ker g = \operatorname{Im} f$:

$$M' \xrightarrow{f} M \xrightarrow{g} M''$$

Plus généralement, si I est un intervalle de $\mathbb{Z}$ et pour tout $i \in I$, M_i est un A-module et $f_i : M_i \to M_{i+1}$ est une application linéaire, on dit que la suite suivante est exacte si $\operatorname{Ker} f_{i+1} = \operatorname{Im} f_i$:

$$\dashrightarrow M_{i-1} \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \dashrightarrow$$

Exemples :

1. Les suites suivantes sont exactes si et seulement si f est surjective, g est injective, et h est bijective :
$$(0) \longrightarrow M \xrightarrow{f} N$$
$$M \xrightarrow{g} N \longrightarrow (0)$$
$$(0) \longrightarrow M \xrightarrow{h} N \longrightarrow (0)$$

2. La suite suivante est une suite exacte courte si g est surjective, f injective et $\operatorname{Ker} g = \operatorname{Im} f$:
$$(0) \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow (0)$$

3. Soient M_1 et M_2 deux A-modules. $i_1 : M_1 \to M_1 \oplus M_2$ l'injection canonique et $p_2 : M_1 \oplus M_2 \to M_2$ la projection canonique. Alors on a la suite exacte courte :
$$(0) \longrightarrow M_1 \xrightarrow{i_1} M_1 \oplus M_2 \xrightarrow{p_2} M_2 \longrightarrow (0)$$

3.6 Modules de type fini

Proposition 3.9 (*Caractérisation des modules de type fini*)

Un A-module est de type fini si et seulement si il existe $n \in \mathbb{N}$ et une application linéaire $\sigma : A^n \to M$ surjective.

Démonstration :

(⇒) Soit M un A-module de type fini. Alors il est engendré par une famille finie $\{x_1, \cdots, x_n\} \subset M$. Ainsi $M = \left\{\sum_{i=1}^n a_i x_i \mid a_i \in A\right\}$, il suffit donc de prendre $\sigma(a_1, \cdots, a_n) = \sum_{i=1}^n a_i x_i$.

(⇐) En considérant la famille des $x_i = (0, \cdots, 0, 1, 0, \cdots, 0)$ avec un 1 en $i^{\text{ème}}$ position, par linéarité et surjectivité de σ on obtient que $M = \left\{\sum_{i=1}^n a_i x_i \mid a_i \in A\right\}$ est de type fini. ■

Théorème 3.10 (*Sur les modules de type fini*)

1. *Soient M et M' deux A-modules et $f : M \to M'$ une application linéaire. Si M est de type fini, alors M' est aussi de type fini.*
2. *Soit la suite exacte :*
$$M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow (0)$$
Si M' et M'' sont de type fini alors M est de type fini.
3. *Soient M et M' deux A-modules et $f : M' \to M$ une application linéaire injective. Si de plus A est Nœthérien et M est de type fini, alors M' est de type fini.*

Démonstration :

1. On a $\sigma : A^n \to M$ et $f : M \to M'$ avec σ et f deux applications linéaires surjectives. On peut donc considérer l'application linéaire surjective $\sigma' = f \circ \sigma : A^n \to M'$ donc M' est de type fini.
2. TODO
3. TODO ■

Théorème 3.11 (*Théorème de Hilbert*)

Si A est un anneau Nœthérien, alors l'anneau $A[X]$ est Nœthérien.

Démonstration : TODO ■

3.7 Algèbre de type finie

– Dans cette partie A est un anneau et B une A-algèbre –

Définition 3.14 (*Algèbre de type finie*)

1. *Une partie $X \subset B$ engendre B comme A-algèbre si le sous-anneau de B engendré par $\eta_B(A) \cup X$ est B.*
2. *On dit que B est une A-algèbre de type finie si B est engendré comme A-algèbre par une partie finie de B.*

Remarque : Soient $x_1, \cdots, x_n \in B$ et $\phi : A[X_1, \cdots, X_n] \to B$ le morphisme de A-algèbre défini par $\phi(X_i) = x_i$. Alors l'image de ϕ est le sous-anneau engendré par $\eta_B(A) \cup \{c_1, \cdots, x_n\}$. Ainsi B est engendré comme A-algèbre par les x_i si et seulement si ϕ est surjective.

En particulier pour toute A-algèbre B de type finie, il existe $n \in \mathbb{N}$ un idéal I de $A[X_1, \cdots, x_n]$ tel que :

$$B \simeq A[X_1, \cdots, x_n]$$

Rappel : Si B est une A-algèbre alors B est naturellement muni d'une structure de A-module.

Proposition : Si B est de type fini comme A-module, alors c'est une A-algèbre de type fini. Mais il n'y a pas de réciproque.

Contre exemple : $\mathbb{Q}[X]$ est une $\mathbb{Q}$-algèbre de type finie (car engendré par X). Mais c'est un $\mathbb{Q}$-espace vectoriel de dimension infinie (donc un $\mathbb{Q}$-module qui n'est pas de type fini).

Lemme 3.12

Soit $f : A \to B$ un morphisme d'anneaux. Alors :

1. *L'application qui à un idéal J de B associe l'idéal $f^{-1}(J)$ de A est injective.*
2. *Si A est Nœthérien, alors B aussi.*

Démonstration :

– C'est un rappel du chapitre sur les anneaux.

– Soit $(J_n)_{n\in\mathbb{N}}$ une suite croissante d'idéaux de B. On pose $(I_n = f^{-1}(J_n))_{n\in\mathbb{N}}$ qui est une suite croissante d'idéaux de A donc stationnaire. Il existe donc $N \in \mathbb{N}$ tel que pour tout $n \geq N$ on a $I_n = I_N$. Par injectivité de $J \mapsto f^{-1}(J)$ on obtient également que $J_n = J_N$ ce qui montre que B est Nœthérien. ■

Proposition 3.13 (*Quotient d'anneau Nœthérien*)

Si A est un anneau Nœthérien, alors pour tout idéal I de A le quotient A/I est Nœthérien.

Démonstration : C'est une conséquence du lemme en prenant $f = \pi : A \to A/I$. ■

Proposition 3.14 (*Algèbre de type finie et anneau Nœthérien*)

Soit A un anneau Nœthérien et B une A-algèbre de type fini. Alors B est un anneau Nœthérien.

Démonstration : Le théorème de Hilbert nous assure que $A[X_1, \cdots, X_n]$ est Nœthérien et que $B \simeq A[X_1, \cdots, X_n]/I$ qui est Nœthérien d'après la propriété précédante. ■

3.8 Modules libres et modules de torsion

3.8.1 Modules libres

Définition 3.15 (*Famille libre, génératrice, et base*)

Soient A un anneau, M un A-module et $(x_i)_{i\in I}$ une famille d'éléments de M.
Soit $\phi : A^{(I)} \ni e_i \longrightarrow x_i \in M$ une application linéaire. On rappele que les e_i forment la base canonique de $A^{(I)}$.

1. *On dit que la famille des x_i est libre si ϕ est injective. On dit aussi que les x_i sont linéairement indépendants.*
2. *On dit qu'elle est génératrice si ϕ est surjective.*
3. *On dit que c'est une base si ϕ est bijective. C'est à dire qu'elle est libre et génératrice.*

Remarque :

1. Une famille est génératrice si et seulement si elle engendre M comme module.
   En particulier tout module admet une famille génératrice : $(x)_{x\in M}$.
2. Si K est un corps alors un K module est un espace vectoriel et admet une base, mais ce n'est pas le cas pour un anneau en général.

Définition 3.16 (*Module libre*)

Un A module M est dit libre s'il admet un base.
Cela revient à dire qu'il existe un ensemble I tel que $M \simeq A^{(I)}$.

Exemples : A, $A^{(I)}$, $A[X]$.

Définition 3.17 (*Annulateur d'un module*)

L'annulateur d'un module M est :

$$\operatorname{Ann} M = \{a \in A \mid \forall x \in M,\ ax = 0\}$$

Remarques :

1. En considérant le morphisme $\rho : A \to \operatorname{End}(M, +)$ définissant la structure de A-module de M on remarque que $\operatorname{Ann}(M) = \operatorname{Ker}\rho$ est un idéal de A.
2. Si I est un idéal de M contenu dans $\operatorname{Ker}\rho = \operatorname{Ann} M$ alors par passage au quotient, il existe un morphisme d'anneau $\tilde{\rho} : {}^{A}/_{I} \to \operatorname{End}(M, +)$. Donc M hérite d'une structure de ${}^{A}/_{I}$ module.
3. Si M est un A-module et I un idéal de A alors IM est un sous-module de M. On a alors $\operatorname{Ann} {}^{M}/_{IM} \subset I$ donc le A-module ${}^{M}/_{IM}$ hérite d'une structure de ${}^{A}/_{I}$ -module.

Définition - Proposition 3.18 (*Rang d'un module libre*)

Soit A un anneau non nul et soit L un A-module libre.
Alors toutes les bases de L ont le même cardinal appelé rang de L et noté $\operatorname{rg} L$.

Démonstration : Comme L est libre on a $L \simeq A^{(I)}$ pour un certain ensemble I.

Soit m un idéal maximal de A. Par définition ${}^{A}/_{m}$ est un corps donc d'après la troisième remarque ${}^{L}/_{mL}$ est un ${}^{A}/_{m}$ -module donc un K-espace vectoriel admettant une base de cardinal C (on rappelle qu'un cardinal est une classe d'équivalence sur les ensembles définie par la relation d'être en bijection).

Comme ${}^{L}/_{mL} \simeq {}^{A^{(I)}}/_{mA^{(I)}}$ on déduit que $I \in C$. ■

3.8.2 Torsion

Définition 3.19 (*Elément de torsion*)

Un élément x d'un A-module M est un élément de torsion s'il existe un $a \in A$ non nul tel que $ax = 0$.
Un module est dit de torsion si tous ses éléments sont de torsion.
Un module est dit sans torsion si le seul élément de torsion est 0.

Remarques :

1. Un module libre est sans torsion car isomorphe à $A^{(I)}$ avec A intègre.
2. Si $\operatorname{Ann} M \neq 0$ alors M est de torsion. Réciproquement, si M est de type fini et de torsion alors $\operatorname{Ann} M \neq 0$.
3. Si I est un idéal de A alors l'annulateur de ${}^{A}/_{I}$ est I. Donc mour I non nul, ${}^{A}/_{I}$ est un module de torision. Anisi si A n'est pas un corps, il existe des modules de torsion non nuls, et ils ne sont pas libres.

Définition - Proposition 3.20 (*Sous-module de torsion*)

Soit M un A-module. L'ensemble des éléments de torsion de M est un sous-module de M noté $\mathrm{T}(M)$ *ou* M_{tors}.

Remarque : On a la suite exacte courte :

$$0 \longrightarrow M_{\mathrm{tors}} \xrightarrow{i} M \xrightarrow{\pi} {}^{M}/_{M_{\mathrm{tors}}} \longrightarrow 0$$

Donc ${}^{M}/_{M_{\mathrm{tors}}}$ est sans torsion.

3.8.3 Module de fraction

Soit A un anneau et S une partie multiplicative de A. On construit, comme dans la section précédante l'algèbre $S^{-1}A$. Alors un $S^{-1}A$-module est naturellement muni d'une structure de A-module.

Réciproquement, étant donnée un A-module M on va construire un $S^{-1}A$ module noté $S^{-1}M$.

1. On muni $S \times M$ de la relation d'équivalence $\mathcal{R}$ définie par :

$$(s, x)\mathcal{R}(s', x') \Longleftrightarrow \exists \sigma \in S,\ \sigma s' x = \sigma s x'$$

2. On pose $S^{-1}M = {}^{S \times M}/_{\mathcal{R}}$ dont les éléments seront notés ${}^{x}/_{s}$.

Index