Cours d'algèbre générale 2 de S. Paños

FMdKdD
fmdkdd [à] free.fr

Université du Havre
Année 2008–2009

Table des matières

Chapitre 1

Groupes

Définition 1.1. Soit G un ensemble non vide et $*$ une loi de composition interne sur G. On dit que $(G,*)$ est un groupe si :

1. $*$ est associative,
2. il existe un élément neutre pour $*$ dans G,
3. tout élément de G possède un symétrique pour $*$.

Si de plus on a :

4. $*$ est commutative.

Alors on dit que $(G,*)$ est un groupe commutatif ou abélien. Lorsque le groupe est abélien, on dit aussi que c'est un groupe additif et on note sa loi $+$. Par souci de simplicité de l'écriture, on dira plutôt le groupe G, que le groupe $(G,*)$.

Remarques.

1. L'élément neutre est unique.
2. Le symétrique d'un élément est unique.
3. Pour un groupe commutatif la loi se note $+$, l'élément neutre 0, et le symétrique de x, $-x$. Si la loi est notée $\cdot$, l'élément neutre se note 1 et le symétrique de x, x^{-1}.
4. L'élément neutre est son propre symétrique.

Définition 1.2. Soient G_1 et G_2 deux groupes. Un homomorphisme de G_1 dans G_2 est une application $f : G_1 \to G_2$ telle que

$$\forall x, y \in G_1 \quad f(xy) = f(x)f(y)$$

Si f est bijectif, on le nomme isomorphisme. Si $G_1 = G_2$ on dit que l'homomorphisme f est un endomorphisme. Un isomorphisme d'un groupe dans lui-même est appelé un automorphisme.

Remarque. Si G_1 et G_2 sont deux groupes d'éléments neutres respectifs e_1 et e_2, f un homomorphisme de G_1 dans G_2, alors :

– $f(e_1) = e_2$

– $\forall x \in G_1, f(x^{-1}) = [f(x)]^{-1}$

L'ensemble des automorphismes d'un groupe G, que l'on note Aut(G), muni de la composition des applications, est un groupe.

Théorème 1.1. *Soient* $G_1, \ldots, G_n$ *des groupes et* $G = G_1 \times \cdots \times G_n$ *leur produit cartésien. Soient* x *et* y *deux éléments de* G *tels que* $x = (x_1, \ldots, x_n)$ *et* $y = (y_1, \ldots, y_n)$*. On considère la loi de composition interne définie sur* G *par*

$$xy = (x_1y_1, \ldots, x_ny_n)$$

G *muni de cette loi est un groupe. On dit que* G *est le produit direct (externe) des groupes* $G_1, \ldots, G_n$.

Démonstration. Soient

$$x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n), z = (z_1, \ldots, z_n)$$

trois éléments quelconques de G. Par définition,

$$xy = (x_1y_1, \ldots, x_ny_n) \text{ et } yz = (y_1z_1, \ldots, y_nz_n)$$

Alors

$$\begin{aligned} x(yz) &= (x_1, \ldots, x_n)(y_1z_1, \ldots, y_nz_n) \\ &= (x_1(y_1z_1), \ldots, x_n(y_nz_n)) \\ &= ((x_1y_1)z_1, \ldots, (x_ny_n)z_n) \\ &= (x_1y_1, \ldots, x_ny_n)(z_1, \ldots, z_n) \\ &= (xy)z \end{aligned}$$

Donc la loi sur G est associative.

Considérons $e = (e_1, \ldots, e_n)$ où $\forall i \in \mathbb{N}_n^*, e_i$ est l'élément neutre de G_i. Pour tout $x = (x_1, \ldots, x_n)$ de G,

$$\begin{aligned} ex &= (e_1, \ldots, e_n)(x_1, \ldots, x_n) \\ &= (e_1x_1, \ldots, e_nx_n) \\ &= (x_1, \ldots, x_n) \\ &= x \end{aligned}$$

$$\begin{aligned} xe &= (x_1, \ldots, x_n)(e_1, \ldots, e_n) \\ &= (x_1e_1, \ldots, x_ne_n) \\ &= (x_1, \ldots, x_n) \\ &= x \end{aligned}$$

Donc e est l'élément neutre de G.

Considérons $x' = (x_1^{-1}, \ldots, x_n^{-1})$:

$$\begin{aligned} xx' &= (x_1, \ldots, x_n)(x_1^{-1}, \ldots, x_n^{-1}) \\ &= (x_1 x_1^{-1}, \ldots, x_n x_n^{-1}) \\ &= (e_1, \ldots, e_n) \\ &= e \end{aligned}$$

$$\begin{aligned} x'x &= (x_1^{-1}, \ldots, x_n^{-1})(x_1, \ldots, x_n) \\ &= (x_1^{-1} x_1, \ldots, x_n^{-1} x_n) \\ &= (e_1, \ldots, e_n) \\ &= e \end{aligned}$$

Donc x admet x' comme symétrique.

Si de plus chaque groupe G_i est commutatif, alors G est commutatif. □

Remarques.

1. Dans le cas où chaque G_i est commutatif, si on note $+$ la loi de G

$$\begin{aligned} x + y &= (x_1, \ldots, x_n) + (y_1, \ldots, y_n) \\ &= (x_1 + y_1, \ldots, x_n + y_n) \end{aligned}$$

$$0_{\mathrm{G}} = (0_{\mathrm{G}_1}, \ldots, 0_{\mathrm{G}_n})$$

2. Si $\mathrm{G}_1 = \cdots = \mathrm{G}_n = \mathrm{G}$, alors $\mathrm{G}_1 \times \cdots \times \mathrm{G}_n$ se note G^n.

Définition 1.3. Soit G un groupe et H une partie non vide stable pour la loi de G. On dit que H est un sous groupe de G si H muni de la loi induite de G est un groupe.

Théorème 1.2. *Soit* G *un groupe et* H *une partie non vide de* G. *Une condition nécessaire et suffisante pour que* H *soit un sous groupe de* G *est*

$$\forall x \in \mathrm{H}, \forall y \in \mathrm{H} \quad x y^{-1} \in \mathrm{H} \tag{1.1}$$

ou

$$\forall x \in \mathrm{H}, \forall y \in \mathrm{H} \quad x^{-1} y \in \mathrm{H} \tag{1.2}$$

Démonstration. Si H est un sous groupe, $y \in H \Rightarrow y^{-1} \in H$. Comme H est une partie stable de G, que $x \in H$ et $y^{-1} \in H$, on a $xy^{-1} \in H$.

Réciproquement

$$\begin{array}{rll} \forall x \in H, & xx^{-1} \in H & \text{d'après (1.1)} \\ & e \in H & \end{array}$$

$$\begin{array}{rll} e \in H, \forall y \in H, & ey^{-1} \in H & \text{d'après (1.1)} \\ & y^{-1} \in H & \\ \forall x \in H, \forall y \in H, & y^{-1} \in H \Rightarrow x(y^{-1})^{-1} \in H \iff xy \in H & \end{array}$$

Donc H est stable pour la loi de G. La loi de G étant associative sur G, elle l'est sur toute partie de G. Donc H est un groupe pour la restriction de la loi de G : c'est un sous groupe de G. □

Exemples.

1. $(\mathbb{Z}, +)$ est un groupe commutatif. $\mathbb{N}$ est une partie stable de $\mathbb{Z}$ pour $+$, qui possède l'élément neutre mais qui n'est pas un sous groupe de $\mathbb{Z}$.
2. $(\mathbb{Z}, +)$
$$\forall n \in \mathbb{N}^*, n\mathbb{Z} = \{x \in \mathbb{Z} / \exists z \in \mathbb{Z}, x = nz\}$$
est un sous groupe de $(\mathbb{Z}, +)$.

Exercices.

1. Montrer que $n\mathbb{Z}$ est un sous groupe de $\mathbb{Z}$.
2. Montrer que tout sous groupe de $\mathbb{Z}$ est de cette forme.

Remarque. Si G est un groupe d'élément neutre e, alors G et $\{e\}$ sont des sous groupes. On les appelle sous groupes triviaux.

Si H est un sous groupe de G, autre que G, on dit que H est un sous groupe propre de G.

Théorème 1.3. *Toute intersection de sous groupes d'un groupe* G *est un sous groupe de* G.

Démonstration. Voir TD. □

Définition 1.4. Si A est une partie non vide de G, l'intersection de tous les sous groupes de G contenant A est le plus petit (au sens de l'inclusion) sous groupe de G contenant A. On l'appelle le sous groupe de G engendré par A.

Théorème 1.4. *Soit* A *une partie non vide d'un groupe* G. *Pour que* $x \in$ G *appartienne au sous groupe de* G *engendré par* A*, il faut et il suffit qu'il existe un entier* $p \geqslant 0$ *et des éléments* $x_1, \ldots, x_p$ *de* G *possédant les propriétés suivantes :*

(1) $x = x_1 \ldots x_p$

(2) $\forall i \in \mathbb{N}_p^*, x_i \in \mathrm{A}$ *ou* $x_i^{-1} \in \mathrm{A}$

Démonstration. On convient que dans un groupe, on attribue un sens à la notion de produit isolé (produit de zéro éléments) en déclarant qu'un tel produit est l'élément neutre du groupe. Le (1) s'écrit alors $x = e$.

Soit H l'ensemble des éléments de G qui vérifient (1) et (2) :

– $\mathrm{H} \neq \emptyset$ car le produit vide appartient à H ($e \in \mathrm{H}$)

– $\forall x, y \in \mathrm{H}, \exists p, q \in \mathbb{N}, x = x_1 \ldots x_p, y = y_1 \ldots y_q$ tels que $\forall i \in \mathbb{N}_q^*, x_i$ ou $x_i^{-1} \in \mathrm{A}$ et y_j ou $y_j^{-1} \in \mathrm{A}$. Alors

$$xy^{-1} = \left(x_1 \ldots x_p\right)\left(y_1 \ldots y_q\right)^{-1} = x_1 \ldots x_p y_q^{-1} \ldots y_1^{-1} \in \mathrm{H}$$

Donc H est un sous groupe de G (théorème 1.2).

Réciproquement :

– $\mathrm{A} \subseteq \mathrm{H}$ car $\forall x \in \mathrm{A}$ en prenant $p = 1$ et $x_1 = x$ on satisfait à la définition de H.

– Soit K un sous groupe de G contenant A. Tout élément de A est dans K donc par conséquent, K étant un sous groupe, tous les symétriques des éléments de A sont dans K. Grâce à la stabilité de K, on en déduit que tout produit formé d'éléments de A ou de symétrique d'éléments de A est encore dans K. Donc $\mathrm{H} \subseteq \mathrm{K}$. H est donc le plus petit sous groupe de G contenant A.

□

Définition 1.5. Lorsque le sous groupe de G engendré par A est G, on dit que A est un ensemble de générateurs de G. Si G admet un ensemble fini de générateurs, on dit que G est de type fini. Si $\mathrm{A} = \{a\}$ et que A engendre G, on dit que G est monogène.

Notation. On désigne par $\mathrm{gp}_{\mathrm{G}}(\mathrm{A})$ le sous groupe de G engendré par A. Si $\mathrm{A} = \{a_1, \ldots, a_n\}$ on peut écrire $\mathrm{gp}_{\mathrm{G}}(\{a_1, \ldots, a_n\})$. Parfois on trouve la notation $[\mathrm{A}]_{\mathrm{G}}$.

Remarque. Si G est un groupe commutatif de type fini et $\mathrm{A} = \{a_1, \ldots, a_n\}$ un ensemble fini de générateurs, tout x de G s'écrit sous la forme $x = x_1 \ldots x_p$ avec $\forall i \in \mathbb{N}_p^*$, $x_i \in \mathrm{A}$ ou $x_i^{-1} \in \mathrm{A}$. Chaque x_i est un a_j ou un a_j^{-1}. Comme G est commutatif on peut grouper tous les x_i qui pour un j donné sont des a_j

ou a_j^{-1}. Le produit de ces a_j est alors une puissance positive ou négative de a_j. Finalement, x s'écrit

$$x = a_1^{r_1} \dots a_n^{r_n}$$

où $r_1, \dots, r_n \in \mathbb{Z}$.

Réciproquement, si tout élément x de G s'écrit sous cette forme, G est de type fini et engendré par $\{a_1, \dots, a_n\}$.

Attention : ne pas confondre l'ordre et le type. $\mathbb{Z}$ est d'ordre infini mais de type fini.

Exemple. $(\mathbb{Z}^n, +)$ est de type fini et admet $\{e_1, \dots, e_n\}$ comme ensemble de générateurs.

$$e_1 = (1, 0, \dots, 0), e_2 = (0, 1, 0, \dots, 0), \dots, e_n = (0, 0, \dots, 0, 1)$$

Si $(r_1, \dots, r_n) \in \mathbb{Z}^n, (r_1, \dots, r_n) = \sum_{i=1}^n r_i e_i$.

$(\mathbb{Q}^n, +)$ n'est pas de type fini.

Définition 1.6. Soit E un ensemble non vide et $\cdot$ une loi de composition interne sur E. Soit $\sim$ une relation d'équivalence définie sur E. On dit que la relation d'équivalence $\sim$ est compatible avec la loi $\cdot$ si

$$\forall x, x', y, y' \in \mathrm{E}, \quad (x \sim x' \text{ et } y \sim y') \Rightarrow x \cdot y \sim x' \cdot y'$$

Définition 1.7. Soit E un ensemble non vide, $*$ une loi de composition interne sur E et $\sim$ une relation d'équivalence sur E, compatible avec $*$. La loi de composition interne $\dot{*}$ sur le quotient $\mathrm{E}/\sim$ est définie par

$$\forall \dot{x}, \dot{y} \in \frac{\mathrm{E}}{\sim} \quad \dot{x} \dot{*} \dot{y} = \widehat{\dot{x * y}}$$

est appelée loi quotient de la loi $*$ par la relation d'équivalence $\sim$.

Théorème 1.5. *Soit* E *un ensemble non vide, $*$ une loi de composition interne, $\sim$ une relation d'équivalence compatible avec $*$. Soit $\dot{*}$ la loi quotient définie sur* $\mathrm{E}/\sim$. *Alors :*

1. *Si $*$ est associative, alors $\dot{*}$ est associative.*
2. *Si e est élément neutre de $*$, alors $\dot{e}$ est élément neutre de $\dot{*}$.*
3. *Si x admet un symétrique pour $*$ dans* E*, alors $\dot{x}$ admet un symétrique pour la loi $\dot{*}$ dans* $\mathrm{E}/\sim$ *et on a*

$$(\dot{x})^{-1} = \widehat{\dot{(x^{-1})}}$$

4. *Si $*$ est commutative, alors $\dot{*}$ est commutative.*

En conséquence, si $(\mathrm{E}, *)$ *est un groupe (resp. groupe commutatif) alors* $(\mathrm{E}/\sim, \dot{*})$ *est un groupe (resp. groupe commutatif).*

Démonstration. Voir TD. □

Exemple. Les entiers modulo m où $m \in \mathbb{N}^*$.

1. On sait que tout sous groupe de $(\mathbb{Z}, +)$ est de la forme $m\mathbb{Z}$.
2. $x \sim y \iff x - y \in m\mathbb{Z}$ ou $y - x \in m\mathbb{Z}$. On a vu en TD que $\sim$ est compatible avec $+$. Le groupe quotient $\mathbb{Z}/\sim$ se note $\mathbb{Z}/m\mathbb{Z}$ (ou encore $\mathbb{Z}_m$).

Soit G un groupe ; nous nous proposons maintenant de déterminer toutes les relations d'équivalence sur G compatibles avec la loi de G.

Théorème 1.6. *Soit* G *un groupe et* H *un sous groupe de* G*. La relation* γ *définie sur* G *par*

$$\forall x, y \in \mathrm{G} \quad x \gamma y \iff x^{-1} y \in \mathrm{H}$$

est une relation d'équivalence sur G *compatible à gauche avec la loi de* G*. La relation* δ *définie sur* G *par*

$$\forall x, y \in \mathrm{G} \quad x \delta y \iff x y^{-1} \in \mathrm{H}$$

est une relation d'équivalence sur G *compatible à droite avec la loi de* G*.*

Si $\sim$ *est une relation d'équivalence sur* G *compatible à gauche (resp. à droite) avec la loi de* G*, si e est l'élément neutre de* G*, alors è est un sous groupe* H *de* G *et l'on a :*

$$(x \sim y) \iff \left(x^{-1} y \in \mathrm{H}\right) \quad (\textit{resp. } x y^{-1} \in \mathrm{H})$$

Démonstration.

1. $\forall x \in \mathrm{G}$, $x^{-1} x = e \in \mathrm{H}$ et $x \gamma x$ donc γ est réflexive.
2. $\forall x, y \in \mathrm{G}$, $x \gamma y \Rightarrow x^{-1} y \in \mathrm{H}$. Un sous groupe contient les symétriques de ses éléments donc $(x^{-1} y)^{-1} \in \mathrm{H} \iff y^{-1} x \in \mathrm{H} \iff y \gamma x$ et γ est symétrique.
3. $\forall x, y, z \in \mathrm{G}$, $x \gamma y$ et $y \gamma z \iff x^{-1} y \in \mathrm{H}$ et $y^{-1} z \in \mathrm{H}$. H étant un sous groupe de G, H est stable, c'est à dire que le produit de deux éléments de H est encore dans H. D'où

$$\begin{aligned} \left(x^{-1} y\right)\left(y^{-1} z\right) &\in \mathrm{H} \\ x^{-1}\left(y y^{-1}\right) z &\in \mathrm{H} \\ x^{-1} e z &\in \mathrm{H} \\ x^{-1} z &\in \mathrm{H} \end{aligned}$$

Donc $x \gamma z$ et γ est transitive, et est une relation d'équivalence sur G.

4. Soient x, y, z dans G tels que $x\gamma y$. Alors :

$$\begin{aligned} x^{-1}y &\in \mathrm{H} \\ x^{-1}ey &\in \mathrm{H} \\ x^{-1}\left(z^{-1}z\right)y &\in \mathrm{H} \\ \left(x^{-1}z^{-1}\right)(zy) &\in \mathrm{H} \\ (zx)^{-1}(zy) &\in \mathrm{H} \end{aligned}$$

   d'où $zx\gamma zy$ et γ est compatible à gauche avec la loi de G.

De même avec δ (aux étudiants).

Soit $\sim$ une relation d'équivalence compatible à droite (resp. à gauche) avec la loi de G. Notons H la classe de e par rapport à $\sim$.

1. $\mathrm{H} \neq \emptyset$ car $e \in \mathrm{H}$.
2. $\forall x, y \in \mathrm{H}$, x et y sont dans la même classe donc $x \sim y$. Comme $\sim$ est compatible à droite, $\forall z \in \mathrm{G}$, $xz \sim yz$, en particulier

$$\begin{aligned} xy^{-1} &\sim yy^{-1} \\ xy^{-1} &\sim e \\ xy^{-1} &\in \mathrm{H} \end{aligned}$$

D'après le théorème 1.2, H est un sous groupe de G. □

Remarques.

1. Dans un groupe commutatif, les trois notions « compatible à gauche », « compatible à droite » et « compatible » sont confondues.
2. Si $\sim$ est compatible à gauche avec la loi de G,

$$\dot{x} = \{y \in \mathrm{G} / x \sim y\} = \{y \in \mathrm{G} / x^{-1}y \in \mathrm{H}\} \quad \text{où } \mathrm{H} = \dot{e}$$

   $$\begin{aligned} x^{-1}y &= h \in \mathrm{H} \\ x(x^{-1}y) &= xh \\ y &= xh \in x\mathrm{H} \end{aligned}$$

   Réciproquement, si $y \in x\mathrm{H}$, $\exists h \in \mathrm{H}$ tel que $y = xh$. Alors $x^{-1}y = x^{-1}(xh) = h \in \mathrm{H}$ donc $x \sim y$.

   D'où $\dot{x} = x\mathrm{H}$ on l'appelle classe à gauche de x par rapport à H.

   Si $\sim$ est une relation d'équivalence sur G compatible à droite avec la loi de G, et si $\mathrm{H} = \dot{e}$, $\dot{x} = \mathrm{H}x$.

Tout sous groupe H de G définit donc deux relations d'équivalence sur G :

$$x\gamma y \iff y \in x\mathrm{H} \quad \text{compatible à gauche avec la loi de G}$$
$$x\delta y \iff y \in \mathrm{H}x \quad \text{compatible à droite avec la loi de G}$$

Les ensembles $x\mathrm{H}$ et $\mathrm{H}x$ sont respectivement appelés classe à gauche de x par rapport à H et classe à droite de x par rapport à H.

Théorème 1.7. *Soit* G *un groupe et* H *un sous groupe de* G. *Les neuf propriétés suivantes sont équivalentes :*

1. $\forall x \in \mathrm{G} \quad x\mathrm{H} = \mathrm{H}x$
2. $\forall x \in \mathrm{G} \quad x\mathrm{H} \subseteq \mathrm{H}x$
3. $\forall x \in \mathrm{G} \quad \mathrm{H}x \subseteq x\mathrm{H}$
4. $\forall x \in \mathrm{G} \quad \mathrm{H} = x^{-1}\mathrm{H}x$
5. $\forall x \in \mathrm{G} \quad \mathrm{H} = x\mathrm{H}x^{-1}$
6. $\forall x \in \mathrm{G} \quad \mathrm{H} \subseteq x^{-1}\mathrm{H}x$
7. $\forall x \in \mathrm{G} \quad \mathrm{H} \subseteq x\mathrm{H}x^{-1}$
8. $\forall x \in \mathrm{G} \quad x\mathrm{H}x^{-1} \subseteq \mathrm{H}$
9. $\forall x \in \mathrm{G} \quad x^{-1}\mathrm{H}x \subseteq \mathrm{H}$

Démonstration. Aux étudiants. □

Définition 1.8. Soit G un groupe et H un sous groupe de G. On dit que H est un sous groupe normal, ou distingué, ou invariant, de G s'il vérifie l'une des neufs propriétés du théorème 1.7. On note alors $\mathrm{H} \lhd \mathrm{G}$.

Remarque. Si G est un groupe commutatif tous ses sous groupes sont distingués.

Théorème 1.8. *Les relations d'équivalence compatibles avec la loi d'un groupe* G *sont les relations de la forme*

$$x\mathrm{R}y \iff y \in x\mathrm{H}$$

où H *est un sous groupe de* G.

Démonstration. Conséquence immédiate du théorème 1.6 et de la définition 1.7. □

Théorème 1.9. *Soit* G *un groupe et* $H \lhd G$. *L'ensemble quotient de* G *par la relation d'équivalence définie par le sous groupe distingué* H *est un groupe pour la loi quotient. On l'appelle « groupe quotient de* G *par le sous groupe distingué* H *». On le note* G/H.

Démonstration. Voir TD. □

Théorème 1.10. *Si* f *est un homomorphisme du groupe* G, *d'élément neutre* e, *dans le groupe* G′, *d'élément neutre* e', *on a les résultats suivants :*

1. $e' = f(e)$
2. $\forall x \in G \quad f(x^{-1}) = \left[f(x)\right]^{-1}$
3. $\widehat{f}(G)$ *est un sous groupe de* G′, *appelé image de* f *et noté* $\operatorname{Im} f$.
4. $N = \widetilde{f}(\{e'\})$ *est un sous groupe distingué de* G. *On l'appelle noyau de l'homomorphisme* f *et on le note* $\operatorname{Ker} f$.
5. f *est injectif si et seulement si* $\operatorname{Ker} f = \{e\}$.

Démonstration. $f : G \to G'$ homomorphisme.

1. $\forall x \in G$,

$$\begin{gathered} xe = x \\ f(xe) = f(x) \\ f(x)f(e) = f(x) \cdot e' \end{gathered}$$

   Tout élément de G′ étant régulier à gauche, $f(e) = e'$.

2. $\forall x \in G$, $e = xx^{-1}$

$$\left.\begin{aligned} e' = f(e) = f(xx^{-1}) = f(x)f(x^{-1}) \\ e' = f(e) = f(x^{-1}x) = f(x^{-1})f(x) \end{aligned}\right\} \Rightarrow f(x^{-1}) = \left[f(x)\right]^{-1}$$

3. $\widehat{f}(G) = \operatorname{Im} f = \{z \in G' / \exists x \in G \quad z = f(x)\}$
   – $e \in G$ et $f(e) = e'$ donc $\operatorname{Im} f \neq \emptyset$
   – $\forall x', y' \in \operatorname{Im} f$ il existe $x, y \in G$ tels que $f(x) = x'$ et $f(y) = y'$. Alors

$$x'y'^{-1} = f(x)\left[f(y)\right]^{-1} = f(x)f(y^{-1}) = f(xy^{-1}) \in \operatorname{Im} f$$

   Donc $\operatorname{Im} f$ est un sous groupe de G′ d'après le théorème 1.2.

4. D'après 1, $e \in \operatorname{Ker} f$. Soient x et y deux éléments quelconques de $\operatorname{Ker} f$.

$$f(xy^{-1}) = f(x)f(y^{-1}) = f(x)\left[f(y)\right]^{-1} = e'e'^{-1} = e'e' = e'$$

   D'où $xy^{-1} \in \operatorname{Ker} f$ et $\operatorname{Ker} f$ est un sous groupe de G (théorème 1.2).

$\forall x \in \mathrm{G}$, $\forall z \in x\,\mathrm{Ker}(f)x^{-1}$, $\exists n \in \mathrm{Ker}\, f$ tel que $z = xnx^{-1}$. Alors

$$\begin{aligned} f(z) &= f(xnx^{-1}) = f(x)f(n)f(x^{-1}) = f(x)f(n)\left[f(x)\right]^{-1} \\ &= f(x)e'\left[f(x)\right]^{-1} = f(x)\left[f(x)\right]^{-1} = e' \end{aligned}$$

Donc $z \in \mathrm{Ker}\, f$ et $x\,\mathrm{Ker}(f)x^{-1} \subseteq \mathrm{Ker}\, f$. D'après le théorème 1.7, $\mathrm{Ker}\, f \lhd \mathrm{G}$.

5. Supposons $\mathrm{Ker}\, f = \{e\}$. Si x et y dans G sont tels que $f(x) = f(y)$ alors :

$$f(xy^{-1}) = f(x)\left[f(y)\right]^{-1} = f(y)\left[f(y)\right]^{-1} = e'$$

donc $xy^{-1} \in \mathrm{Ker}\, f$ et $xy^{-1} = e$ d'où $x = y$.
Réciproquement, supposons f injective. Si $x \in \mathrm{Ker}\, f$:

$$f(x) = e' = f(e) \Rightarrow x = e$$

Donc $\mathrm{Ker}\, f = \{e\}$.

□

Définition 1.9. Soient $\mathrm{G}_1, \ldots, \mathrm{G}_n$ des sous groupes d'un groupe commutatif $(\mathrm{G}, +)$. Soit $f : \mathrm{G}_1 \times \cdots \times \mathrm{G}_n \to \mathrm{G}$ définie par $(x_1, \ldots, x_n) \mapsto x_1 + \cdots + x_n$. Alors f est un homomorphisme et $\mathrm{Im}\, f = \mathrm{G}_1 + \cdots + \mathrm{G}_n$. Si f est injectif, on dit que $\mathrm{G}_1, \ldots, \mathrm{G}_n$ sont linéairement indépendants.

Remarque. Au lieu de dire f est injectif, on peut dire $\mathrm{Ker}\, f = \{(0, 0, \ldots, 0)\}$, c'est à dire :

$$x_1 + \cdots + x_n = 0_{\mathrm{G}} \Rightarrow x_1 = 0 = x_2 = \cdots = x_n$$

Théorème 1.11. *Pour que deux sous groupes* H *et* K *d'un groupe commutatif* G *soient linéairement indépendants, il faut et il suffit que* $\mathrm{H} \cap \mathrm{K} = \{0_{\mathrm{G}}\}$.

Démonstration. Si $x \in \mathrm{H} \cap \mathrm{K}$ on a $x + (-x) = 0$ avec $x \in \mathrm{H}$ et $-x \in \mathrm{K}$. Donc si H et K sont linéairement indépendants, $x = -x = 0$.

Réciproquement, si $\mathrm{H} \cap \mathrm{K} = \{0\}$ et si $x \in \mathrm{H}, y \in \mathrm{K}$ et $x + y = 0$ alors $x = -y$; donc $-y \in \mathrm{H}$ car $x \in \mathrm{H}$. Comme H est un sous groupe, $-(-y) = y \in \mathrm{H}$. D'où $y \in \mathrm{H} \cap \mathrm{K} = \{0\}$. Donc $y = x = 0$. H et K sont donc linéairement indépendants. □

Remarque. $x \mapsto (x, -x)$ est un isomorphisme de $\mathrm{H} \cap \mathrm{K}$ sur $\mathrm{Ker}\, f$.

Définition 1.10. Lorsque les sous groupes $G_1, \ldots, G_n$ d'un groupe commutatif G sont linéairement indépendants, on dit que $G_1 + \cdots + G_n$ est la somme directe des sous groupes $G_1, \ldots, G_n$ et on la note $G_1 \oplus \cdots \oplus G_n$.

Si $f : G_1 \times \cdots \times G_n \to G$ qui associe $(x_1, \ldots, x_n)$ à $\sum_{i=1}^{n} x_i$ est surjective, on dit que G est la somme directe de ses sous groupes $G_1, \ldots, G_n$ et on écrit $G = \bigoplus_{i=1}^{n} G_i$, ou $G = G_1 \oplus \cdots \oplus G_n$.

Théorème 1.12. *Tout homomorphisme f d'un groupe* G *dans un groupe* K *se décompose sous la forme*

$$f = i \circ b \circ s$$

où :

1. *s est l'homomorphisme surjectif (épimorphisme) canonique de* G *sur* $G/\operatorname{Ker} f$.
2. *b est l'isomorphisme canonique de* $G/\operatorname{Ker} f$ *sur* $\operatorname{Im} f$.
3. *i est l'homomorphisme injectif (monomorphisme) canonique de* $\operatorname{Im} f$ *dans* K.

$$\begin{array}{ccc} G & \xrightarrow{f} & K \\ \downarrow{\scriptstyle s} & & \uparrow{\scriptstyle i} \\ \dfrac{G}{\operatorname{Ker} f} & \xrightarrow{b} & \operatorname{Im} f \end{array}$$

Démonstration. Soit $\sim$ la relation d'équivalence associée à f :

$$x \sim y \iff f(x) = f(y)$$

alors :

$$\begin{aligned} f(x) = f(y) &\iff f(xy^{-1}) = e' \quad \text{l'élément neutre de K} \\ &\iff xy^{-1} \in \operatorname{Ker} f \end{aligned}$$

Donc $\sim$ est la relation associée au sous groupe distingué $\operatorname{Ker} f$ de G. Donc $G/\operatorname{Ker} f$ est un groupe pour la loi quotient.

Soit

$$\begin{aligned} s : G &\to \frac{G}{\operatorname{Ker} f} \\ x &\mapsto \dot{x} \end{aligned}$$

On a

$$\forall x, y \in G, \quad s(xy) = \widehat{\dot{x}\dot{y}} = \dot{x}\dot{y} = s(x)s(y)$$

Donc s est un homomorphisme surjectif.

Soit

$$b : \frac{\mathrm{G}}{\mathrm{Ker}\, f} \to \mathrm{Im}\, f$$
$$\dot{x} \mapsto f(x)$$

On a

$$\forall \dot{x}, \dot{y} \in \mathrm{G}/\mathrm{Ker}\, f, \quad b(\dot{x}\dot{y}) = b(\widehat{\dot{x}\dot{y}}) = f(xy) = f(x)f(y) = b(\dot{x})b(\dot{y})$$

Donc b qui est bijective est un isomorphisme.

i étant une restriction de l'identité, i est injectif.

f et $i \circ b \circ s$ sont toutes deux de G dans K, il reste à prouver qu'elles ont même graphe. Soit x dans G

$$(i \circ b \circ s)(x) = (i \circ b)(s(x)) = (i \circ b)(\dot{x}) = i(b(\dot{x})) = i(f(x)) = f(x)$$

Donc $f = i \circ b \circ s$. □

Théorème 1.13. *Soit* G *un groupe et* H *un sous groupe de* G. *Soit* φ *la bijection de* G *dans* G *définie par* $x \mapsto x^{-1}$ *(ce n'est pas un homomorphisme sauf si* G *est commutatif). Alors*

$$\forall x \in \mathrm{G}, \quad \widehat{\varphi}(x\mathrm{H}) = \mathrm{H}\varphi(x) \quad et \quad \widehat{\varphi}(\mathrm{H}x) = \varphi(x)\mathrm{H}$$

Démonstration. Remarquons que pour tout $h \in \mathrm{H}$ on a $\varphi(xh) = (xh)^{-1} = h^{-1}x^{-1} = h^{-1}\varphi(x)$ et

$$\forall k \in \mathrm{H} \quad k\varphi(x) = kx^{-1} = (k^{-1})^{-1}x^{-1} = (xk^{-1})^{-1} = \varphi(xk^{-1})$$

Donc $\widehat{\varphi}(x\mathrm{H}) \subseteq \mathrm{H}\varphi(x)$ et $\mathrm{H}\varphi(x) \subseteq \widehat{\varphi}(x\mathrm{H})$. D'où $\widehat{\varphi}(x\mathrm{H}) = \mathrm{H}\varphi(x)$. L'autre résultat se montre de la même façon. □

Théorème 1.14. *L'application* $\widehat{\varphi} : x\mathrm{H} \to \mathrm{H}\varphi(x)$ *est une bijection de l'ensemble des classes à gauche modulo* H *sur l'ensemble des classes à droite modulo* H, *dont l'application réciproque* $\widehat{\varphi}^{-1}$ *est*

$$\mathrm{H}x \mapsto \varphi(x)\mathrm{H}$$

Démonstration.

– Supposons $\widehat{\varphi}(x\mathrm{H}) = \widehat{\varphi}(y\mathrm{H})$, $\mathrm{H}\varphi(x) = \mathrm{H}\varphi(y)$. On a :

$$\forall u \in \mathrm{H}, \exists v \in \mathrm{H} \quad ux^{-1} = vy^{-1}$$
$$x = yv^{-1}u$$
$$y = xu^{-1}v$$

D'où $\forall t \in \mathrm{H} \quad xt = y\overbrace{(v^{-1}ut)}^{\in \mathrm{H}} \in y\mathrm{H}$ et $x\mathrm{H} \subseteq y\mathrm{H}$. Donc $x\mathrm{H} = y\mathrm{H}$ car deux classes d'équivalences sont disjointes où confondues. Ici l'une est incluse dans l'autre, donc elles sont confondues. Donc $\widehat{\varphi}$ est injective.

– Soit $\mathrm{H}x$ une classe à droite quelconque. Alors on a $\mathrm{H}x = \mathrm{H}\varphi(x^{-1}) = \widehat{\varphi}(x^{-1}\mathrm{H})$. Or $x^{-1}\mathrm{H}$ est une classe à gauche. Donc $\widehat{\varphi}$ est surjective.

Donc $\widehat{\varphi}$ est une bijection de l'ensemble des classes à gauche dans l'ensemble des classes à droite par rapport à H. □

Définition 1.11. Soit G un groupe, et H un sous groupe de G. Lorsque le nombre de classes à gauche modulo H (ou à droite) est fini, on l'appelle indice du sous groupe H par rapport à G, et on le note $[\mathrm{G} : \mathrm{H}]$. S'il existe une infinité de classes à gauche (donc une infinité de classes à droite) modulo H, on dit que H est un sous groupe d'indice infini de G.

Définition 1.12. Soit G un groupe ayant un nombre fini d'éléments. On dit que G est un groupe fini, et on appelle ordre de G le nombre de ses éléments.

Remarque. Ne pas confondre « groupe fini » et « groupe de type fini ». $\mathbb{Z}$ n'est pas un groupe fini, mais est bien de type fini.

Théorème 1.15. *Dans tout groupe* G*, les classes à gauche* $x\mathrm{H}$ *et les classes à droite* $\mathrm{H}x$ *par rapport à un sous groupe* H *ont toutes pour cardinal le cardinal de* H*.*

Démonstration. Soit x un élément quelconque de G et soient $\delta : \mathrm{H} \to \mathrm{H}x$ définie par $h \mapsto hx$ et $\gamma : \mathrm{H} \to x\mathrm{H}$ par $h \mapsto xh$ les translations à droite et à gauche définies par x.

δ est injective, car si $\delta(z) = \delta(z')$, $zx = z'x$ et $z = z'$ car dans un groupe tout élément est simplifiable à droite.

δ est surjective car $\forall y \in \mathrm{H}x$ il existe $z \in \mathrm{H}$ tel que $y = zx = \delta(z)$. Donc y a bien un antécédent.

D'où δ est bijective. De même pour γ. □

Théorème 1.16 (Lagrange)**.** *Dans tout groupe fini* G*, l'ordre de tout sous groupe* H *de* G *divise l'ordre du groupe.*

Démonstration. H étant une partie de G, et G étant fini, H est une partie finie. Soit m l'ordre de H. H détermine une relation d'équivalence compatible à gauche avec la loi de G. H est donc à l'origine d'une partition de G en classes de cardinal tous égaux au cardinal de H. Donc :

$$\begin{aligned} \operatorname{card} \mathrm{G} &= \operatorname{card} \mathrm{H} \times \text{ nombre de classes} \\ &= \operatorname{card} \mathrm{H} \times [\mathrm{G} : \mathrm{H}] \end{aligned}$$

□

Remarque. Si G est un groupe d'ordre n et H un sous groupe de G d'ordre m, l'indice $[\mathrm{G} : \mathrm{H}]$ de H dans G est égal à

$$\frac{n}{m} = \frac{\operatorname{card} \mathrm{G}}{\operatorname{card} \mathrm{H}}$$

Théorème 1.17. *Soit* G *un groupe et a un élément de* G*. On note* $\mathrm{H} = \mathrm{gp}(a)$ *le sous groupe monogène de* G *engendré par a. Alors* H *est commutatif.*

- *Si* H *est infini, alors* H *est isomorphe à* $(\mathbb{Z}, +)$*.*
- *Si* H *est fini et de cardinal n, il est isomorphe à* $(\mathbb{Z}/n\mathbb{Z}, +)$*.*

Démonstration. Il résulte du théorème 1.4 que tout élément x de H s'écrit a^m où $m \in \mathbb{Z}$:

$$a^0 = e, a^1 = a, a^m = \begin{cases} \overbrace{a \dots a}^{m \text{ fois}} & \text{si } m > 0 \\ (a^{-1})^{-m} & \text{si } m < 0 \end{cases}$$

Nous allons prouver que $\forall p \in \mathbb{Z}, \forall q \in \mathbb{Z}$, $a^p a^q = a^{p+q}$.

Supposons $p \leqslant q$. Remarquons tout d'abord que :

$$\forall k \in \mathbb{N}^* \quad (a^{-1})^k (a^k) = a^k (a^{-1})^k = e$$

Trois cas se présentent :

1. $0 \leqslant p \leqslant q$
2. $p \leqslant 0 \leqslant q$
3. $p \leqslant q \leqslant 0$

On a :

1. $a^p a^q = \underbrace{aa \dots a}_{p \text{ fois}} \cdot \underbrace{aa \dots a}_{q \text{ fois}} = a^{p+q}$
2. (a) $0 \leqslant -p \leqslant q$

$$a^p a^q = (a^{-1})^{-p} a^q = (a^{-1})^{-p} a^{-p} a^{q-(-p)} = a^{p+q}$$

   (b) $0 \leqslant q \leqslant -p$

$$a^p a^q = (a^{-1})^{-p} a^q = (a^{-1})^{-p-q} (a^{-1})^q a^q = (a^{-1})^{-(p+q)} = a^{p+q}$$

3. $a^p a^q = (a^{-1})^{-p} (a^{-1})^{-q} = (a^{-1})^{-p-q} = (a^{-1})^{-(p+q)} = a^{p+q}$

Le cas $q \leqslant p$ découle de la commutativité de $+$ dans $\mathbb{Z}$. Donc $\forall p \in \mathbb{Z}, \forall q \in \mathbb{Z}$, $a^p a^q = a^{p+q} = a^q a^p$. Donc tout groupe monogène est commutatif.

Soit $\varphi : \mathbb{Z} \to \mathrm{H}$ définie par $m \mapsto a^m$. D'après ce qui précède, φ est un homomorphisme surjectif de $(\mathbb{Z}, +)$ sur $(\mathrm{H}, \cdot)$. Si φ est injectif, alors H et $\mathbb{Z}$ sont isomorphes. Sinon son noyau $\mathrm{Ker}\,\varphi$ est un sous groupe de $(\mathbb{Z}, +)$, autre que $\{0\}$. Il est donc de la forme $n\mathbb{Z}$ pour un certain n de $\mathbb{N}^*$. Le théorème 1.12 nous dit alors que H et $\mathbb{Z}/n\mathbb{Z}$ sont isomorphes, donc H est fini et d'ordre n. □

Définition 1.13. Un groupe monogène fini s'appelle un groupe cyclique (chez les anglophones tout groupe monogène est qualifié de cyclique).

Un élément a d'un groupe G est dit d'ordre infini si le sous groupe monogène qu'il engendre est infini, ou de manière équivalente si l'application $\varphi : \mathbb{Z} \to \mathrm{G}$ définie par $m \mapsto a^m$ est injective. Dans le cas contraire, on dit que a est d'ordre fini. Dans ce cas, l'ordre du groupe cyclique engendré par a s'appelle l'ordre de a (e est d'ordre 1).

Remarque. Si a est d'ordre fini n, l'entier n est le plus petit des entiers $k \geqslant 1$ tels que $a^k = e$. Plus précisément, si $a^k = e$ alors n divise k : si $a^k = e = \varphi(k)$ alors $k \in \mathrm{Ker}\,\varphi = n\mathbb{Z}$ donc k est un multiple de n.

Théorème 1.18 (Bézout)**.** *Pour que les entiers relatifs $x_1, \ldots, x_n$ soient premiers entre eux (on dit aussi premiers dans leur ensemble) il faut et il suffit qu'il existe des entiers relatifs $u_1, \ldots, u_n$ tels que $u_1 x_1 + \cdots + u_n x_n = 1$. On note alors $(x_1, \ldots, x_n) = 1$. Pour deux entiers u et v on note $(u, v) = 1$.*

Démonstration. Supposons $(x_1, \ldots, x_n) = 1$ et soit $\mathrm{H} = \mathrm{gp}_{\mathbb{Z}}(\{x_1, \ldots, x_n\})$.

$$\mathrm{H} = \{x \in \mathbb{Z} / \exists m_1, \ldots, m_n \in \mathbb{Z} \quad x = m_1 x_1 + \cdots + m_n x_n\}$$

d'après le théorème 1.4 et la remarque de la définition 1.5. Or H est un sous groupe de $\mathbb{Z}$, donc il existe $p \in \mathbb{N}$ tel que $\mathrm{H} = p\mathbb{Z}$. Donc $x = pk = m_1 x_1 + \cdots + m_n x_n$. Or, pour tout i de 1 à n, $x_i \in \mathrm{H}$ donc x_i est divisible par p. D'où p est un diviseur commun à $x_1, \ldots, x_n$. Or $(x_1, \ldots, x_n) = 1$ donc $p = 1$ et $\mathrm{H} = p\mathbb{Z} = \mathbb{Z}$. Donc tout élément de $\mathbb{Z}$, en particulier 1 appartient à H. Alors il existe $m_1, \ldots, m_n$ dans $\mathbb{Z}$ tels que $1 = m_1 x_1 + \cdots + m_n x_n$.

Réciproquement, supposons qu'il existe dans $\mathbb{Z}$ des entiers $m_1, \ldots, m_n$ tels que $m_1 x_1 + \cdots + m_n x_n = 1$. Posons $(x_1, \ldots, x_n) = d \in \mathbb{Z}$. Alors d divise chacun des x_i : $\exists v_i \in \mathbb{Z}$, $x_i = d v_i$ d'où

$$1 = m_1 d v_1 + m_2 d v_2 + \cdots + m_n d v_n = d(m_1 v_1 + \cdots + m_n v_n)$$

Donc d est un diviseur de 1, d'où $(x_1, \ldots, x_n) = 1$. □

Remarque. On ne confondra pas « premiers entre eux » et « premiers entre eux deux à deux ».

Théorème 1.19. *Soient* G *un groupe et x un élément de* G *d'ordre fini n. Soit $r \geqslant 2$, supposons que $n = n_1 \dots n_r$ tels que $(n_i, n_j) = 1$ si $i \neq j$ pour tous $i, j \in \mathbb{N}_r^*$.*

Alors x a une écriture unique sous la forme $x = x_1 \dots x_r$ où pour tous $i, j \in \mathbb{N}_r^*$, $x_i x_j = x_j x_i$, et pour tout $i \in \mathbb{N}_r^*$, x_i est d'ordre n_i.

Démonstration. Supposons $r = 2$: $n = n_1 n_2$ avec $(n_1, n_2) = 1$. D'après Bézout, il existe $u_1, u_2 \in \mathbb{Z}$ tels que $u_1 n_1 + u_2 n_2 = 1$. D'où

$$\begin{aligned} x = x^1 &= x^{u_1 n_1 + u_2 n_2} = x^{u_1 n_1} x^{u_2 n_2} \\ &= x^{u_2 n_2 + u_1 n_1} = x^{u_2 n_2} x^{u_1 n_1} \end{aligned}$$

Posons $x_1 = x^{u_2 n_2}$ et $x_2 = x^{u_1 n_1}$. On a $x = x_1 x_2 = x_2 x_1$. Calculons

$$\begin{aligned} x_2^{n_2} = (x^{u_1 n_1})^{n_2} = x^{u_1 n_1 n_2} = x^{u_1 n} = (x^n)^{u_1} = e^{u_1} = e \\ x_1^{n_1} = (x^{u_2 n_2})^{n_1} = x^{u_2 n_2 n_1} = x^{u_2 n} = (x^n)^{u_2} = e^{u_2} = e \end{aligned}$$

Donc l'ordre p_2 de x_2 divise n_2 et l'ordre p_1 de x_1 divise n_1. De $x = x_1 x_2 = x_2 x_1$ il résulte

$$\begin{aligned} x^{p_1 p_2} = (x_1 x_2)^{p_1 p_2} &= (x_1^{p_1})^{p_2} (x_2^{p_2})^{p_1} \quad \text{car } x_1 \text{ et } x_2 \text{ commutent} \\ &= e \end{aligned}$$

Donc n, l'ordre de x, divise $p_1 p_2$. Or $n = n_1 n_2 = k_1 p_1 k_2 p_2$. On a donc

$$\begin{aligned} k_3 n &= p_1 p_2 \\ k_3 n_1 n_2 &= p_1 p_2 \\ k_3 k_1 k_2 p_1 p_2 = p_1 p_2 &\Rightarrow k_3 k_1 k_2 = 1 \Rightarrow k_3 = k_1 = k_2 = 1 \end{aligned}$$

D'où $n_1 = p_1$ et $n_2 = p_2$. Donc x_1 est d'ordre n_1 et x_2 d'ordre n_2.

Il reste à montrer l'unicité de cette décomposition. Supposons que x admette une autre décomposition

$$x = y_1 y_2 = y_1 y_2$$

avec y_1 d'ordre n_1 et y_2 d'ordre n_2. Remarquons tout d'abord que y_1 et y_2 commutent avec x, il en est de même pour x_1 et x_2.

$$\begin{aligned} x y_1 = (y_1 y_2) y_1 = y_1 (y_2 y_1) = y_1 x \\ x y_2 = (y_2 y_1) y_2 = y_2 (y_1 y_2) = y_2 x \end{aligned}$$

Par conséquent, x^{-1} commute également avec y_1 et y_2

$$\begin{aligned} x^{-1}y_1 = x^{-1}y_1(xx^{-1}) &= x^{-1}(y_1x)x^{-1} \\ &= x^{-1}(xy_1)x^{-1} = (x^{-1}x)(y_1x^{-1}) = y_1x^{-1} \\ x^{-1}y_2 = x^{-1}y_2(xx^{-1}) &= x^{-1}(y_2x)x^{-1} \\ &= x^{-1}(xy_2)x^{-1} = (x^{-1}x)(y_2x^{-1}) = y_2x^{-1} \end{aligned}$$

On en déduit que y_1 et y_2 commutent avec $x_2 = x^{u_1n_1}$ et $x_1 = x^{u_2n_2}$.

Posons $w = y_1^{-1}x_1 = y_2x_2^{-1} \quad (x_1x_2 = y_1y_2)$. Alors

$$\begin{aligned} w^{n_1} = (y_1^{-1}x_1)^{n_1} = (y_1^{-1})^{n_1}x_1^{n_1} = ee = e \\ w^{n_2} = (y_2x_2^{-1})^{n_2} = y_2^{n_2}(x_2^{-1})^{n_2} = ee = e \end{aligned}$$

L'ordre de w divise à la fois n_1 et n_2 qui sont premiers entre eux, donc w est d'ordre 1 et $w = e$. D'où

$$\begin{aligned} y_1^{-1}x_1 = e \Rightarrow x_1 = y_1 \\ y_2x_2^{-1} = e \Rightarrow y_2 = x_2 \end{aligned}$$

Donc il y a bien unicité de la décomposition.

Supposons que l'on ait montré le théorème jusqu'au rang $(r-1)$. Posons $n = n_1n_2\dots n_r = n_1m_1$. Comme $(n_i, n_j) = 1$ pour $i \neq j$, on a $(n_1, m_1) = 1$. D'où $x = x_1y_1 = y_1x_1$ où x_1 est d'ordre n_1 et y_1 d'ordre m_1 de façon unique. On applique alors l'hypothèse de récurrence à y_1 et à m_1. □

Exemple. $G = \mathbb{Z}/12\mathbb{Z}$

$[1]_{12}$	$[2]_{12}$
ordre 12	ordre 6
$12 = 3 \times 4$	$6 = 2 \times 3$
ordre 3 : [4], [8]	ordre 3 : [4], [8]
ordre 4 : [3], [9]	ordre 2 : [6]
$[1]_{12} = [4]_{12} \dot{+} [9]_{12}$	$[2]_{12} = [8]_{12} \dot{+} [6]_{12}$

Corollaire 1.1. *Si x est d'ordre $n \geqslant 2$ et si $n = p_1^{\alpha_1}\dots p_r^{\alpha_r}$ où $\alpha_i \geqslant 1$ est sa décomposition en facteurs premiers, alors x s'écrit d'une manière unique*

$$x = x_1\dots x_r$$

où pour tout $i \in \mathbb{N}_r^*$, x_i est d'ordre $p_i^{\alpha_i}$ et $x_ix_j = x_jx_i$ si $i \neq j$.

Étudions à présent plus en détail les groupes cycliques.

Théorème 1.20. *Soit* G *un groupe cyclique d'ordre* $n \geqslant 2$*. Soient* a *un générateur de* G, $k \in \mathbb{N}^*_{n-1}$, $\mathrm{H} = \mathrm{gp}(a^k)$*. Alors* H *est aussi engendré par* a^d *où* $d = \mathrm{pgcd}(n,k)$*.*

Démonstration. $\exists l \in \mathbb{N}^*$ tel que $k = ld$. D'où $a^k = a^{ld} = (a^d)^l$. D'où $\mathrm{H} = \mathrm{gp}(a^k) \subseteq \mathrm{gp}(a^d)$.

Inversement, Bézout implique $\exists u, v \in \mathbb{Z}$, $d = nu + kv$. D'où :

$$a^d = a^{nu+kv} = (a^n)^u (a^k)^v = (a^k)^v \in \mathrm{H}$$

D'où $\mathrm{gp}(a^d) \subseteq \mathrm{H}$. D'où l'égalité. □

Exemple. $(\mathbb{Z}/12\mathbb{Z}, +) = \left\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}, \bar{10}, \bar{11}\right\}$. On peut prendre $a = \bar{1}$. Considérons :

$\bar{6} = 6 \cdot \bar{1}$	$\mathrm{pgcd}(6,12) = 6$	$\mathrm{gp}(\bar{6}) = \{\bar{0}, \bar{6}\}$
$\bar{8} = 8 \cdot \bar{1}$	$\mathrm{pgcd}(8,12) = 4$	$\mathrm{gp}(\bar{4}) = \mathrm{gp}(\bar{8}) = \{\bar{0}, \bar{8}, \bar{4}\}$
$\bar{5} = 5 \cdot \bar{1}$	$\mathrm{pgcd}(5,12) = \bar{1}$	$\mathrm{gp}(\bar{5}) = \mathrm{gp}(\bar{1})$

Remarques.

1. d divise n, donc il existe $q \in \mathbb{N}^*$, $n = qd$. Le groupe H est donc égal à $\left\{e, a^d, \ldots, a^{(q-1)d}\right\}$. L'ordre de H est donc
$$q = \frac{n}{d} = \frac{n}{\mathrm{pgcd}(n,k)}$$
2. a^k est un générateur de G si et seulement si $(n,k) = 1$.

Théorème 1.21. *Soient* G *un groupe cyclique d'ordre* n *et* a *un générateur de* G*.*

1. *Tout sous groupe* H *de* G *est cyclique. Si* d *est le plus petit entier* $\geqslant 1$ *tel que* $a^d \in \mathrm{H}$*, alors* a^d *est un générateur de* H*,* d *divise* n *et* H *est d'ordre* n/d*.*
2. *Si* q *divise* n*,* G *possède un unique sous groupe d'ordre* q*. Il est engendré par* $a^{n/q}$*.*

Démonstration.

1. Si $\mathrm{H} = \{e\}$, $d = n$ car $a^n = e$. Si $\mathrm{H} \neq \{e\}$ soit d le plus petit entier $\geqslant 1$ tel que $a^d \in \mathrm{H}$. Alors $\mathrm{gp}(a^d) \subseteq \mathrm{H}$. Réciproquement, soit $h \in \mathrm{H}$. Comme $h \in \mathrm{G}$ il existe m tel que $h = a^m$. Effectuons la division euclidienne de m par d : $m = qd + r$ avec $0 \leqslant r < d$. Alors
$$a^r = a^{m-qd} = (a^m)(a^d)^{-q} \in \mathrm{H}$$

Donc $a^r \in \mathrm{H}$, et $r < d$, d'où $r = 0$ d'après la définition de d. D'où d divise m, et $\mathrm{H} \subseteq \mathrm{gp}(a^d)$, donc $\mathrm{H} = \mathrm{gp}(a^d)$. Comme $a^n = e$, cela prouve que d divise n.

Montrons maintenant que H est d'ordre n/d. Soit k tel que $(a^d)^k = e$. k existe car $(a^d)^n = e$. On a donc $a^{dk} = e$, donc dk est un multiple de n. On a donc $dk = ln = ld(n/d)$. D'où le plus petit k tel que $(a^d)^k = e$ est $k = n/d$.

2. Si q divise n, il existe d tel que $n = qd$. Considérons le sous groupe cyclique engendré par a^d : $\mathrm{gp}(a^d) = [a^d]$. Le résultat annoncé est une conséquence du 1 : $\mathrm{H} = \mathrm{gp}(a^d)$ est d'ordre $q = n/d$. Seule l'unicité est à prouver.

   Soit K un sous groupe cyclique de G d'ordre q. Un générateur de K s'écrit alors a^p. Comme a^p est d'ordre q, $(a^p)^q = e = a^{pq}$ donc n divise pq : $pq = kn$. D'où $p = k(n/q) = kd$. D'où $a^p = (a^d)^k$ et donc $\mathrm{K} \subseteq \mathrm{H}$. Comme $\mathrm{card}\,\mathrm{H} = \mathrm{card}\,\mathrm{K} = q$ on a $\mathrm{H} = \mathrm{K}$.

□

Théorème 1.22. *Soient* H *et* K *deux groupes finis,* $\mathrm{H} \times \mathrm{K}$ *leur groupe produit. Soit* $(h,k) \in \mathrm{H} \times \mathrm{K}$. *Alors l'ordre de* (h,k) *dans* $\mathrm{H} \times \mathrm{K}$ *est le* ppcm *des ordres de* h *dans* H *et de* k *dans* K.

Démonstration. Soit q l'ordre de l'élément (h,k) dans $\mathrm{H} \times \mathrm{K}$. $(h,k)^q = (e_\mathrm{H}, e_\mathrm{K})$ c'est à dire $(h^q, k^q) = (e_\mathrm{H}, e_\mathrm{K})$. D'où $h^q = e_\mathrm{H}$ et $k^q = e_\mathrm{K}$. q est donc un multiple commun des ordres de h et de k. Si n est l'ordre de h dans H et m l'ordre de k dans K et l leur ppcm, on a $q = \alpha l$. Or, il existe m_1 et n_1 tels que $l = nn_1 = mm_1$. Donc

$$(h,k)^l = (h^l, k^l) = (h^{nn_1}, k^{mm_1}) = (e_\mathrm{H}^{n_1}, e_\mathrm{K}^{m_1}) = (e_\mathrm{H}, e_\mathrm{K})$$

Donc l est un multiple de q. D'où $l = q$. □

Théorème 1.23. *Le produit de deux groupes cycliques est cyclique si et seulement si leurs ordres sont premiers entre eux.*

Démonstration. Soient H et K deux groupes cycliques d'ordres respectifs n et m. L'ordre du groupe $\mathrm{H} \times \mathrm{K}$ est donc nm. Il sera cyclique s'il existe un élément (h,k) d'ordre nm. Soit h un générateur de H et k un générateur de K. L'ordre de (h,k) est le ppcm de n et de m. Donc si n et m sont premiers entre eux, c'est nm et alors $\mathrm{H} \times \mathrm{K}$ est cyclique.

Réciproquement, supposons $\mathrm{H} \times \mathrm{K}$ cyclique. Soit (α, β) un élément d'ordre nm. Soient n_1 l'ordre de α dans H et m_1 celui de β dans K. On a $mn =$

ppcm(n_1, m_1). Par ailleurs n_1 divise n et m_1 divise m. On a

$$n = k_1 n_1 \quad m = l_1 m_1 \quad k_1, l_1 \in \mathbb{N}^*$$
$$\text{ppcm}(m_1, n_1) = k_1 l_1 n_1 m_1 \geqslant n_1 m_1$$

Donc ppcm$(m_1, n_1) = n_1 m_1$ ce qui prouve que n_1 et m_1 sont premiers entre eux. □

Corollaire 1.2.

$$\left(\frac{\mathbb{Z}}{mn\mathbb{Z}} \approx \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{n\mathbb{Z}} \right) \iff ((m,n) = 1)$$

Corollaire 1.3.

$$\frac{\mathbb{Z}}{n\mathbb{Z}} \approx \prod_{i=1}^{r} \frac{\mathbb{Z}}{p_i^{\alpha_i}\mathbb{Z}}$$

où $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ la décomposition en facteurs premiers de n.

Remarque. Il résulte du corollaire 1.2 que $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ sont deux groupes finis commutatifs non isomorphes. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ est l'exemple du plus petit groupe commutatif non cyclique. On l'appelle groupe de Klein ou Viergruppe (V_4).

Théorème 1.24. *Soient* G *un groupe, x et y deux éléments de* G *d'ordres finis respectifs m et n, et qui commutent. Alors $z = xy$ est d'ordre mn si et seulement si m est premier avec n. Dans ce cas, x et y sont éléments de* $\text{gp}_G(z)$.

Démonstration. Si xy est d'ordre mn, soit $k = \text{ppcm}(m, n)$.

$$\begin{aligned}(xy)^k &= x^k y^k \quad \text{car } x \text{ et } y \text{ commutent} \\ &= ee = e\end{aligned}$$

Donc k est un multiple de l'ordre de xy et par conséquent un multiple de mn. D'où $k = mn$ et m est premier avec n.

Réciproquement, si $(m, n) = 1$, on a

$$(xy)^{mn} = x^{mn} y^{mn} = (x^m)^n (y^n)^m = e$$

Donc mn est un multiple de k, l'ordre de xy. De $(xy)^k = e$ on déduit que $(xy)^{km} = e = (x^m)^k y^{km} = y^{km}$. Donc km est un multiple de n. Comme $(m, n) = 1$ et que n divise km, n divise k. De même, $(xy)^{kn} = e = x^{kn} = e$ et m divise kn et donc k, car $(n, m) = 1$. D'où mn divise k. Par conséquent, $k = mn$.

Si $(m,n)=1$, $\exists u,v\in\mathbb{Z}$, $um+vn=1$. D'où

$$z^{mu}=x^{mu}y^{mu}=(x^m)^u y^{1-nv}=ey(y^n)^{-v}=y$$
$$z^{nv}=x^{nv}y^{nv}=x^{1-mu}(y^n)^v=x(x^m)^{-u}e=x$$

Donc x et y sont dans $\mathrm{gp}_{\mathrm{G}}(z)$. □

Remarques.

1. $\mathrm{gp}_{\mathrm{G}}(xy)=\mathrm{gp}_{\mathrm{G}}(x)\oplus\mathrm{gp}_{\mathrm{G}}(y)$
2. Soit $(\mathrm{G},+)$ un groupe cyclique d'ordre n avec $n=p_1^{\alpha_1}\dots p_r^{\alpha_r}$ comme décomposition en nombres premiers. Si x est un générateur de G, on a montré que $x=x_1+\cdots+x_r$ de façon unique avec pour tout $i\in\mathbb{N}_r^*$, x_i d'ordre $p_i^{\alpha_i}$; plus généralement, tout y de G s'écrit de manière unique $y=y_1+\cdots+y_r$ où $\forall i\in\mathbb{N}_r^*$, y_i d'ordre $p_i^{\beta_i}$ avec $0\leqslant\beta_i\leqslant\alpha_i$. Autrement dit, il existe k tel que $y=kx$, donc $y=kx_1+\cdots+kx_r$. Or, $\forall i\in\mathbb{N}_r^*$, $kx_i\in\mathrm{gp}_{\mathrm{G}}(x_i)$ donc l'ordre de kx_i est $p_i^{\gamma_i}$ où $0\leqslant\gamma_i\leqslant\alpha_i$. Le théorème 1.23 montre que l'ordre de y est

$$\prod_{i=1}^{r}p_i^{\gamma_i}$$

L'unicité de la décomposition impose $\gamma_i=\beta_i$ pour tout $i\in\mathbb{N}_r^*$. D'où

$$\mathrm{G}=\bigoplus_{i=1}^{r}\mathrm{gp}_{\mathrm{G}}(x_i)$$

Chapitre 2

Permutations

Définition 2.1. Soit $n \in \mathbb{N}^*$ et soit X un ensemble à n éléments. On note S_X le groupe des permutations de X, applications bijectives de X dans X, et on l'appelle le groupe symétrique de X. Sa loi est la composition des applications.

Notation. Si $X = \mathbb{N}_n^* = \{1, 2, \ldots, n\}$, S_X se notera S_n.

Remarques.

1. Si A est une partie non vide de X, S_A est canoniquement isomorphe à un sous groupe de S_X. En effet, on vérifie que l'application $\Phi : S_A \to S_X$ définie par $\forall \sigma \in S_A$, $\Phi(\sigma) = \tilde{\sigma} \in S_X$ où $\tilde{\sigma}_{|A} = \sigma$ et $\tilde{\sigma}_{|X-A} = Id_{X-A}$, est un homomorphisme injectif.
2. S_X et S_n sont isomorphes si $\operatorname{card} X = n$. En effet, si $X = \{x_1, \ldots, x_n\}$, l'application $\Psi : S_n \to S_X$ définie par $\sigma \mapsto \bar{\sigma} : x_i \mapsto x_{\sigma(i)}$ est un isomorphisme de groupe.
3. Dès que X a au moins 3 éléments, $(S_X, \circ)$ n'est pas commutatif. D'après la remarque 2, il suffit de le vérifier pour S_3.
4. Rappel : $\operatorname{card} S_n = n!$.

Notation. On utilise en général la notation à 2 rangs

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \ldots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \sigma(4) & \sigma(5) & \ldots & \sigma(n) \end{pmatrix}$$

L'ordre des colonnes n'a pas d'importance.

Définition 2.2. Soit l un entier compris entre 2 et n. On appelle cycle de longueur l (ou l-cycle) tout élément σ de S_X tel qu'il existe une partie $A = \{a_1, \ldots, a_l\} \subseteq X$ telle que

$$\begin{aligned} \forall i \in \mathbb{N}_{l-1}^* \quad & \sigma(a_i) = a_{i+1} \\ & \sigma(a_l) = a_1 \\ \forall x \in \complement_X A \quad & \sigma(x) = x \end{aligned}$$

On notera un tel cycle $\sigma = (a_1 a_2 \dots a_l)$.

Un cycle de longueur 2 s'appelle une transposition. Nous conviendrons que $e = \mathrm{Id}_X$ est un cycle de longueur 1. Nous appellerons domaine associé au cycle $\sigma = (a_1 a_2 \dots a_l)$ l'ensemble des éléments $\{a_1, a_2, \dots, a_l\}$.

Théorème 2.1. *Soit* X *un ensemble à n éléments ($n \geqslant 2$) et l un entier tel que $2 \leqslant l \leqslant n$. Tout cycle de longueur l est un élément d'ordre l dans* $(S_X, \circ)$.

Démonstration. Aux étudiants. □

Définition 2.3. Deux permutations σ_1 et σ_2 du groupe S_X sont dites disjointes si les ensembles

$$\Gamma_1 = \{x \in X / \sigma_1(x) \neq x\} \quad \text{et} \quad \Gamma_2 = \{x \in X / \sigma_2(x) \neq x\}$$

sont disjoints, c'est à dire $\Gamma_1 \cap \Gamma_2 = \emptyset$.

Remarque. Si $\sigma \in S_X$ et si $\Gamma = \{x \in X / \sigma(x) \neq x\}$ alors $\widehat{\sigma}(\Gamma) = \Gamma$. On appelle domaine associé à la permutation σ l'ensemble Γ.

Théorème 2.2. *Deux permutations disjointes σ_1 et σ_2 de S_X commutent.*

Démonstration. Soient Γ_1 le domaine associé à σ_1, $\{x \in X / \sigma_1(x) \neq x\}$ et Γ_2 le domaine associé à σ_2 et $A = \complement_X(\Gamma_1 \cup \Gamma_2)$. Il se peut que $A = \emptyset$, auquel cas on ne considère que Γ_1 et Γ_2.

$\{\Gamma_1, \Gamma_2, A\}$ réalise une partition de X. Nous allons prouver que sur chacun des éléments de la partition, $\sigma_1 \circ \sigma_2 = \sigma_2 \circ \sigma_1$.

Si $A \neq \emptyset$, soit $x \in A$. $\sigma_{1_{|A}} = \mathrm{Id}_A$ et $\sigma_{2_{|A}} = \mathrm{Id}_A$, alors

$$(\sigma_1 \circ \sigma_2)(x) = \sigma_1(\sigma_2(x)) = \sigma_1(x) = x = \sigma_2(x) = \sigma_2(\sigma_1(x)) = (\sigma_2 \circ \sigma_1)(x)$$

Si $x \in \Gamma_1$, alors $\sigma_1(x) \in \Gamma_1$ et comme $\Gamma_1 \cap \Gamma_2 = \emptyset$, $\sigma_2(x) = x$ d'où

$$(\sigma_1 \circ \sigma_2)(x) = \sigma_1(\sigma_2(x)) = \sigma_1(x)$$
$$(\sigma_2 \circ \sigma_1)(x) = \sigma_2(\sigma_1(x)) = \sigma_1(x)$$

Si $x \in \Gamma_2$, alors $\sigma_2(x) \in \Gamma_2$ et comme $\Gamma_1 \cap \Gamma_2 = \emptyset$, $\sigma_1(x) = x$. Donc

$$(\sigma_1 \circ \sigma_2)(x) = \sigma_1(\sigma_2(x)) = \sigma_2(x)$$
$$(\sigma_2 \circ \sigma_1)(x) = \sigma_2(\sigma_1(x)) = \sigma_2(x)$$

Donc $\forall x \in X$, $(\sigma_1 \circ \sigma_2)(x) = (\sigma_2 \circ \sigma_1)(x)$. D'où $\sigma_1 \circ \sigma_2 = \sigma_2 \circ \sigma_1$. □

Théorème 2.3. *Soit* X *un ensemble fini. Toute permutation σ de S_X autre que l'identité sur* X *est la composée de cycles disjoints deux à deux de longueur* 2 *au moins. Cette décomposition est unique à l'ordre près des facteurs.*

Démonstration. Soit R la relation définie sur X par

$$x\mathrm{R}y \iff \exists m \in \mathbb{Z} \quad x = \sigma^m(y)$$

On peut montrer que R est une relation d'équivalence sur X. Soit Γ le domaine associé à la permutation σ. Soit $x \in \Gamma$ ($\Gamma \neq \emptyset$ car $\sigma \neq \mathrm{Id}_X$). Soit C la classe d'équivalence de x par rapport à R,

$$\mathrm{C} = \{y \in \mathrm{X} / \exists m \in \mathbb{Z}, y = \sigma^m(x)\}$$

Soit $\{x, \sigma(x), \sigma^2(x), \ldots, \sigma^k(x), \ldots\} \subseteq \mathrm{C} \subset \mathrm{X}$.

Comme X est fini, les éléments de cet ensemble ne peuvent être tous distincts, et il existe des entiers m et n tels que $0 \leqslant m < n$ et tels que $\sigma^m(x) = \sigma^n(x)$, d'où $x = \sigma^{n-m}(x)$. L'ensemble $\left\{k \in \mathbb{N}^* / x = \sigma^k(x)\right\}$ n'est donc pas vide. Cette partie possède donc un plus petit élément m_0 : alors $\forall m \in \mathbb{Z}$, $\sigma^m(x) = \sigma^{m_0+m}(x)$. Donc $\mathrm{C} = \{x, \sigma(x), \ldots, \sigma^{m_0-1}(x)\}$.

Soit γ le cycle $(x\ \sigma(x)\ \sigma^2(x) \ldots \sigma^{m_0-1}(x))$, nous l'appellerons cycle associé à la classe C. On a alors

$$\begin{aligned} &\forall y \notin \mathrm{C} \quad \gamma(y) = y \\ &\forall y \in \mathrm{C} \quad \gamma(y) = \sigma(y) \end{aligned}$$

En recommençant l'opération avec $y \in \mathrm{C}$, on obtient un autre cycle. Supposons que l'on ait k classes $\mathrm{C}_1, \ldots, \mathrm{C}_k$ par rapport à R. Soient $\gamma_1, \ldots, \gamma_k$ leurs cycles associés. Ces cycles sont disjoints et si une classe est restreinte à 1 élément, le cycle associé est l'identité et on se restreint alors aux classes ayant strictement plus qu'un élément.

Montrons que $\sigma = \gamma_1 \circ \gamma_2 \circ \ldots \gamma_k$. Soit $y \in \mathrm{X}$; si $\sigma(y) = y$ alors y est dans l'une des classes à 1 élément, qui est exclue, donc y est invariant par chaque γ_i ($i \in \mathbb{N}_k^*$)

$$(\gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_k)(y) = y$$

Si $\sigma(y) \neq y$, alors y est dans l'une des classes non triviale : $\exists i \in \mathbb{N}_k^*$, $y \in \mathrm{C}_i$. Soit $z = \sigma(y)$. Alors $z = \gamma_i(y)$. Pour tout entier $j \neq i$ de $\mathbb{N}_k^*$, $\gamma_j(y) = y$. D'où

$$(\gamma_1 \circ \cdots \circ \gamma_k)(y) = (\gamma_1 \circ \cdots \circ \gamma_{k-1})(\sigma(y)) = \sigma(y)$$

Par conséquent, $\sigma = \gamma_1 \circ \ldots \gamma_k$.

Supposons que l'on ait une autre décomposition pour σ :

$$\sigma = \beta_1 \circ \beta_2 \circ \cdots \circ \beta_l$$

Pour tout $j \in \mathbb{N}_l^*$ notons Γ_j le domaine associé à β_j. Si on note A l'ensemble des points fixes de σ, c'est à dire l'ensemble contenu dans X sur lequel σ est

l'identité, la famille $\{\Gamma_1, \Gamma_2, \ldots, \Gamma_l, A\}$ est une partition de X. Pour tout j de $\mathbb{N}_l^*$, $\forall y \in C_j$, $\sigma(y) = \beta_j(y)$, alors si $x \in \Gamma_j$ on a

$$\Gamma_j = \left\{x, \beta_j(x), \beta_j^2(x), \ldots\right\} = \left\{x, \sigma(x), \sigma^2(x), \ldots\right\} = C_i$$

pour un $i \in \mathbb{N}_k^*$. D'où $\beta_j = \gamma_i$ pour un certain $i \in \mathbb{N}_k^*$.

Si on simplifie $\sigma = \gamma_1 \circ \cdots \circ \gamma_k = \beta_1 \circ \cdots \circ \beta_\ell$ en enlevant les termes communs à droite et à gauche on aboutit à une égalité de la forme $\gamma_{i_1} \circ \ldots \gamma_{i_h} = e$. Or les γ_{i_j} bougent les éléments sur des parties disjointes. Donc un élément bougé par l'un d'entre eux ne peut être remis à sa place par un autre. Donc $k = l$. Donc $\gamma_1 \circ \cdots \circ \gamma_k$ et $\beta_1 \circ \ldots \beta_k$ ne peuvent différer que par l'ordre des facteurs. □

Théorème 2.4. *L'ordre d'une permutation est le plus petit commun multiple des longeurs des cycles de sa décomposition en cycles disjoints.*

Démonstration. Les cycles $\gamma_1, \ldots, \gamma_k$ de la décomposition d'une permutation sont disjoints et d'après le théorème 2.2, $\forall i, j \in \mathbb{N}_k^*$, $\gamma_i \circ \gamma_j = \gamma_j \circ \gamma_i$.

$$\forall m \in \mathbb{N}^* \quad \sigma^m = \left(\gamma_1 \circ \cdots \circ \gamma_k\right)^m = \gamma_1^m \circ \cdots \circ \gamma_k^m$$

Comme γ_i^m et γ_j^m restent disjoints :

$$\sigma^m = \mathrm{Id}_X \Rightarrow \forall i \in \mathbb{N}_k^* \quad \gamma_i^m = \mathrm{Id}_X$$

Donc m doit être un multiple commun des ordres des $(\gamma_i)_{i \in \mathbb{N}_k^*}$. L'ordre de σ étant le plus petit entier m tel que $\sigma^m = \mathrm{Id}_X$, c'est le ppcm des ordres des $(\gamma_i)_{i \in \mathbb{N}_k^*}$. □

Théorème 2.5. *Toute permutation peut s'écrire sous forme d'un produit de transpositions.*

Démonstration. Le théorème 2.3 nous permet de dire qu'il suffit de le montrer pour les cycles. Soit $(a_1 a_2 \ldots a_l)$ un cycle. Alors :

$$(a_1 a_2 \ldots a_l) = (a_1 a_l) \circ (a_1 a_{l-1}) \circ \cdots \circ (a_1 a_3) \circ (a_1 a_2)$$

□

Définition 2.4. Soit $\sigma \in S_n$. Soient i et j distincts dans $\mathbb{N}_n^*$ tels que $i < j$. On dit que le couple (i, j) est (ou présente) une inversion pour σ quand $\sigma(j) < \sigma(i)$.

On désigne par $\mathrm{sgn}(\sigma)$ le nombre total d'inversions pour σ et par $\varepsilon(\sigma) = (-1)^{\mathrm{sgn}(\sigma)}$. $\varepsilon(\sigma)$ s'appelle la parité de la permutation σ. Si $\varepsilon(\sigma) = +1$, on dit que σ est paire. Si $\varepsilon(\sigma) = -1$, on dit que σ est impaire.

Théorème 2.6. *Toute transposition est impaire.*

Démonstration. Soient $h, k \in \mathbb{N}_n^*$ tels que $h < k$. Considérons la transposition (hk) :

$$(hk) = \begin{pmatrix} 1 & 2 & \dots & h-1 & h & h+1 & \dots & k-1 & k & k+1 & \dots n-1 & n \\ 1 & 2 & \dots & h-1 & k & h+1 & \dots & k-1 & h & k+1 & \dots n-1 & n \end{pmatrix}$$

Les inversions sont les couples (h,i) et (i,k) où $h < i < k$ et le couple (h,k). Or il y a exactement $(k-h-1)$ entiers strictement compris entre h et k, donc $(k-h-1)$ couples (h,i) et autant de couples (i,k). Au total. il y a donc $2(k-h-1)+1$ inversions : c'est un nombre impair, d'où (h,k) est impaire. □

Théorème 2.7. *L'application* $\varepsilon : (\mathrm{S}_n, \circ) \to (\{-1,+1\}, \times)$ *est un homomorphisme de groupes. La parité d'un produit de composition de permutations est le produit des parités de ces permutations.*

Démonstration. Nous dirons qu'une partie L de $\mathbb{N}_n^* \times \mathbb{N}_n^*$ est un « bon ensemble » si :

1. $\forall i \in \mathbb{N}_n^*, (i,i) \notin \mathrm{L}$
2. $\forall i \in \mathbb{N}_n^*, \forall j \in \mathbb{N}_n^*, (i \neq j) \Rightarrow$ (ou bien $(i,j) \in \mathrm{L}$ ou bien $(j,i) \in \mathrm{L}$)

On peut remarquer qu'un bon ensemble possède $n(n-1)/2$ éléments.

Si $\sigma \in \mathrm{S}_n$ et si L est un bon ensemble, $\hat{\sigma}(\mathrm{L})$ est aussi un bon ensemble.

$$\hat{\sigma}(\mathrm{L}) = \left\{(l,m) \in \mathbb{N}_n^{*^2} / \exists (i,j) \in \mathrm{L} \quad l = \sigma(i) \text{ et } m = \sigma(j)\right\} \subseteq \mathbb{N}_n^{*^2}$$

Il est clair que $\forall l \in \mathbb{N}_n^*, (l,l) \notin \hat{\sigma}(\mathrm{L})$. Soit $(l,m) \in \mathbb{N}_n^{*^2}$ tel que $l \neq m$. Comme $\sigma \in \mathrm{S}_n$ il existe $i \in \mathbb{N}_n^*$ tel que $\sigma(i) = l$ et $j \in \mathbb{N}_n^*$ tel que $\sigma(j) = m$ avec $i \neq j$. Comme L est un bon ensemble, soit (i,j) est dans L et alors (l,m) est dans $\hat{\sigma}(\mathrm{L})$, soit (j,i) est dans L et $(m,l) \in \hat{\sigma}(\mathrm{L})$. Donc $\hat{\sigma}(\mathrm{L})$ est un bon ensemble.

L'application $(i,j) \mapsto \big(\sigma(i), \sigma(j)\big)$ est une bijection de L dans $\hat{\sigma}(\mathrm{L})$, et les quantités

$$\omega(\mathrm{L}) = \prod_{(i,j)\in \mathrm{L}} (j-i) \quad \text{et} \quad \omega(\hat{\sigma}(\mathrm{L})) = \prod_{(l,m)\in \hat{\sigma}(\mathrm{L})} (m-l)$$

sont égales au signe près. En effet, si $(i,j) \in \mathrm{L}$, comme $\hat{\sigma}(\mathrm{L})$ est un bon ensemble, soit $(i,j) \in \hat{\sigma}(\mathrm{L})$, soit $(j,i) \in \hat{\sigma}(\mathrm{L})$, c'est à dire que dans $\omega(\hat{\sigma}(\mathrm{L}))$ on a soit $(j-i)$ soit $(i-j)$. Du fait de la bijection, il y a le même nombre de termes $(n(n-1)/2)$ dans $\omega(\hat{\sigma}(\mathrm{L}))$ que dans $\omega(\mathrm{L})$. D'où $\omega(\mathrm{L}) = \pm\omega(\hat{\sigma}(\mathrm{L}))$.

Les signes de $(j-i)$ et de $\sigma(j)-\sigma(i)$ ne diffèrent que si (i,j) présente une inversion pour σ. D'où :

$$\omega(\hat{\sigma}(\mathrm{L})) = \prod_{(i,j)\in \mathrm{L}} \big(\sigma(j)-\sigma(i)\big) = (-1)^{\mathrm{sgn}(\sigma)}\omega(\mathrm{L})$$

Soient σ_1 et σ_2 dans S_n, L un bon ensemble. Nous savons qu'alors $\hat{\sigma_2}(L)$ est aussi un bon ensemble. Donc

$$\omega\left(\widehat{(\sigma_1 \circ \sigma_2)}(L)\right) = (-1)^{\operatorname{sgn}\sigma_1}\omega(\widehat{\sigma_2}(L))$$

Or

$$\omega(\widehat{\sigma_2}(L)) = (-1)^{\operatorname{sgn}\sigma_2}\omega(L)$$
$$\omega\left(\widehat{(\sigma_1 \circ \sigma_2)}(L)\right) = \omega\left(\widehat{\sigma_1}(\widehat{\sigma_2}(L))\right) = (-1)^{\operatorname{sgn}(\sigma_1\circ\sigma_2)}\omega(L)$$

Alors :

$$(-1)^{\operatorname{sgn}(\sigma_1\circ\sigma_2)}\omega(L) = (-1)^{\operatorname{sgn}\sigma_1}\omega(\hat{\sigma_2}(L)) = (-1)^{\operatorname{sgn}\sigma_1}(-1)^{\operatorname{sgn}\sigma_2}\omega(L)$$

Comme les couples $(i,i) \notin L$, $\omega(L) \neq 0$ et :

$$(-1)^{\operatorname{sgn}(\sigma_1\circ\sigma_2)} = (-1)^{\sigma_1}(-1)^{\sigma_2}$$
$$\varepsilon(\sigma_1 \circ \sigma_2) = \varepsilon(\sigma_1)\varepsilon(\sigma_2)$$

□

Théorème 2.8. *Un produit de k transpositions est pair si k est pair, et impair si k est impair.*

Démonstration. Conséquence immédiate des théorèmes 2.6 et 2.7. □

Théorème 2.9. *Tout cycle de longueur k a pour parité* $(-1)^{k-1}$.

Démonstration. Application immédiate des théorèmes 2.5 et 2.8. □

Théorème 2.10. *Pour tout élément n de* $\mathbb{N}^*$*, l'ensemble* A_n *des permutations paires de* S_n *est un sous groupe distingué de* S_n *contenant* $n!/2$ *éléments. On l'appelle le groupe alterné d'ordre n.*

Démonstration. Soit $\varepsilon : S_n \to \{-1,+1\}$ définie par : $\sigma \mapsto \varepsilon(\sigma)$. Alors

$$\forall \sigma, \theta \in S_n \quad \varepsilon(\sigma \circ \theta) = \varepsilon(\sigma)\varepsilon(\theta)$$

Donc ε est un homomorphisme du groupe $(S_n, \circ)$ dans $(\{-1,+1\}, \times)$. Son noyau $\operatorname{Ker}\varepsilon$ est A_n. Donc $A_n \lhd S_n$ et le théorème de décomposition d'un homomorphisme de groupe nous dit que $S_n/\operatorname{Ker}\varepsilon$ est isomorphe à $\operatorname{Im}\varepsilon$. Or $\operatorname{Ker}\varepsilon = A_n$ et $\operatorname{Im}\varepsilon = \{-1,+1\}$. Donc $\operatorname{card} S_n/A_n = 2$ et $A_n = n!/2$. □

Chapitre 3

Anneaux

Définition 3.1. Un anneau est un ensemble non vide A muni de deux lois internes, notées $+$ et $\times$, tel que :

1. $(\mathrm{A}, +)$ est un groupe commutatif dont on note 0 (ou 0_{A}) l'élément neutre.
2. $\times$ est associative et distributive par rapport à $+$.

Si $\times$ est commutative, on dit que A est un anneau commutatif. Si $\times$ possède un élément neutre, on dit que A est un anneau unitaire (unifère). Si A n'admet pas de diviseurs de zéro ($xy = 0 \Rightarrow x = 0$ ou $y = 0$), on dit que A est intègre.

Exemples.

1. $(\mathbb{Z}/6\mathbb{Z}, \dot{+}, \dot{\times})$ est un anneau dans lequel $\dot{2}$ est un diviseur de $\dot{0}$:
$$\dot{3}\dot{\times}\dot{2} = \widehat{3 \times 2} = \dot{6} = \dot{0}$$
2. $(\mathscr{M}_2(\mathbb{R}), +, \times)$ est un anneau non commutatif qui possède des diviseurs de $\left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$: $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) \times \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$

Théorème 3.1. *Soit* $(\mathrm{A}, +, \times)$ *un anneau. Alors* $\forall a, b, c \in \mathrm{A}, \forall n \in \mathbb{Z}$ *:*

1. $a \cdot 0 = 0$
2. $a(-b) = -(ab) = -a(b)$
3. $(-a)(-b) = ab$
4. $a(b-c) = ab - ac \quad et \quad (b-c)a = ba - ca$
5. $(na)b = n(ab) = a(nb)$

Démonstration. 1. $a(0+0) = a0 + a0 = a0$, d'où
$$a0 + a0 = a0 = a0 + 0$$
$$a0 = 0$$

2. $a[b+(-b)] = a0 = 0 = ab + a(-b)$ d'où $a(-b) = -(ab)$. De même, $(-a)b = -(ab)$.
3. $(-a)(-b) = -a(-b) = -(-ab) = ab$ d'après le 2.
4. $a(b-c) = a[b+(-c)] = ab + a(-c) = ab - ac$. De même, $(b-c)a = ba - ca$.
5. Si $n > 0$:

$$(na)b = (\underbrace{a+a+\cdots+a}_{n \text{ fois}})b = \underbrace{ab+\cdots+ab}_{n \text{ fois}} = n(ab)$$

De même $a(nb) = n(ab)$.
Si $n < 0$:

$$\begin{aligned}(na)b = -(-na)b &= -(\underbrace{a+a+\cdots+a}_{-n \text{ fois}})b \\ &= -(\underbrace{ab+ab+\cdots+ab}_{-n \text{ fois}}) \\ &= -((-n)(ab)) = n(ab)\end{aligned}$$

De même pour $a(nb)$.
Si $n = 0$, c'est trivial.

□

Définition 3.2. Une partie R non vide d'un anneau A est un sous anneau de A si la restriction des lois de A à R lui confère une structure d'anneau.

Théorème 3.2. *Une partie* R *non vide d'un anneau* A *est un sous anneau de* A *si et seulement si :*

1. R *est un sous groupe de* $(A,+)$ *:* $\forall x, y \in R,\ x - y \in R$.
2. R *est stable pour la loi* $\times$ *:* $\forall x, y \in R,\ xy \in R$.

Démonstration. Si R est un sous anneau de A, alors 1 et 2 sont vérifiés. Réciproquement, supposons 1 et 2 vérifiés : alors $(R,+)$ est un groupe commutatif, car $+$ étant commutative sur tout A, elle l'est sur R. Le 2 entraîne que la restriction de $\times$ à R est une loi interne sur R. Étant distributive par rapport à l'addition sur A, elle l'est également sur R. Étant associative sur tout A, elle l'est sur toute partie stable de A, en particulier R. Donc R est un anneau. □

Remarque. Si R est un sous anneau de A et si A est commutatif (resp. intègre), alors R l'est aussi. Par contre, A peut être un anneau unitaire sans que R le soit.

Définition 3.3. Soit A un anneau unitaire et ε l'élément neutre de la seconde loi de A. Un élément s de A est appelé unité de A s'il possède un inverse pour la seconde loi (élément inversible) :

$$\exists t \in \mathrm{A} \quad st = ts = \varepsilon$$

Théorème 3.3. *Soient* A *un anneau unitaire et* $\mathrm{A}^\times$ *l'ensemble des éléments inversibles de* A. *Alors* $(\mathrm{A}^\times, \times)$ *est un groupe.*

Démonstration. Soit A un anneau unitaire, d'élément unité 1_A. Alors $1_\mathrm{A} \cdot 1_\mathrm{A} = 1_\mathrm{A}$ et $1_\mathrm{A} \in \mathrm{A}^\times$. D'où $\mathrm{A}^\times \neq \emptyset$.

Si $s, t \in \mathrm{A}^\times$ il existe s^{-1} et t^{-1} tels que $ss^{-1} = s^{-1}s = 1_\mathrm{A}$ et $tt^{-1} = t^{-1}t = 1_\mathrm{A}$. Donc $s^{-1} \in \mathrm{A}^\times$ et $t^{-1} \in \mathrm{A}^\times$. Et :

$$(st)(t^{-1}s^{-1}) = s1_\mathrm{A}s^{-1} = ss^{-1} = 1_\mathrm{A}$$

D'où $st \in \mathrm{A}^\times$. Donc $(\mathrm{A}^\times, \times)$ est un groupe. □

Remarque. $\mathbb{Z}^\times = \{+1, -1\}$.

Théorème 3.4. *Toute intersection de sous anneau de* A *est un sous anneau de* A.

Démonstration. Soit $(\mathrm{A}_i)_{i\in\mathrm{I}}$ une famille de sous anneaux de A. $\forall i \in \mathrm{I}$, A_i est un sous anneau donc un sous groupe de A. $\bigcap_{i\in\mathrm{I}} \mathrm{A}_i$ est un sous groupe de A.

$$\forall x, y \in \bigcap_{i\in\mathrm{I}} \mathrm{A}_i : \forall i \in \mathrm{I} \quad x \in \mathrm{A}_i, y \in \mathrm{A}_i$$

A_i est stable pour $\times$ donc $xy \in \mathrm{A}_i, \forall i \in \mathrm{I}$. On a donc $xy \in \bigcap_{i\in\mathrm{I}} \mathrm{A}_i$. D'où $\bigcap_{i\in\mathrm{I}} \mathrm{A}_i$ est stable pour $\times$ et $\bigcap_{i\in\mathrm{I}} \mathrm{A}_i$ est un sous anneau de A. □

Définition 3.4. Soit E une partie non vide de l'anneau A. On appelle sous anneau de A engendré par E l'intersection de tous les sous anneaux de A contenant E. C'est le plus petit (au sens de l'inclusion) sous anneau de A contenant E.

Définition 3.5. Soit $(\mathrm{A}, +, \times)$ un anneau. On appelle idéal à gauche (resp. à droite) de l'anneau A tout sous groupe I_g (resp. I_d) de $(\mathrm{A}, +)$ stable par multiplication à gauche (resp. à droite) pour chaque élément de A :

$$\forall x \in \mathrm{I}_g, \forall y \in \mathrm{I}_g \quad x - y \in \mathrm{I}_g \quad (\text{resp. } \mathrm{I}_d)$$
$$\forall a \in \mathrm{A}, \forall x \in \mathrm{I}_g \quad ax \in \mathrm{I}_g \quad (\text{resp. } xa \in \mathrm{I}_d)$$

On appelle idéal bilatère, ou idéal, de A un idéal à droite de A qui est aussi un idéal à gauche.

Exemples.

1. Dans $(\mathbb{Z}, +, \times)$ les idéaux sont de la forme $n\mathbb{Z}$ où $n \in \mathbb{N}^*$.
2. Soit A un anneau : alors aA est un idéal à droite pour tout a de A, et Aa est un idéal à gauche pour tout a de A.

Remarque. Si l'anneau est commutatif, les trois notions d'idéaux coïncident.

Théorème 3.5. *Toute intersection d'idéaux à gauche (resp. à droite, bilatère) est un idéal à gauche (resp. à droite, bilatère).*

Démonstration. Nous savons depuis le premier chapitre que toute intersection de sous groupes est un sous groupe. Il reste à vérifier la deuxième propriété : soit $(\mathrm{A}_i)_{i\in\mathrm{I}}$ une famille d'idéaux à gauche. Alors :

$$\forall x \in \bigcap_{i\in\mathrm{I}} \mathrm{A}_i \quad \forall a \in \mathrm{A} \quad \text{on a} \quad \forall i \in \mathrm{I}, x \in \mathrm{A}_i$$

Or chaque A_i est un idéal à gauche donc $\forall i \in \mathrm{I}, ax \in \mathrm{A}_i$. D'où $ax \in \bigcap_{i\in\mathrm{I}} \mathrm{A}_i$. Donc $\bigcap_{i\in\mathrm{I}} \mathrm{A}_i$ est un idéal à gauche. □

Définition 3.6. On appelle idéal engendré par une partie E non vide de A l'intersection de tous les idéaux de A contenant E. C'est le plus petit idéal de A contenant E.

Théorème 3.6. *Si* A *est un anneau unitaire, l'idéal à gauche (resp. à droite) engendré par un élément a de* A *c'est* Aa *(resp.* aA*).*

Démonstration. L'idéal engendré par a contient a, donc contient également $a+a$, $a+a+a$, …, $-a$, $-a-a$, …, c'est à dire tous les éléments de la forme na où $n \in \mathbb{Z}$. Il contient aussi tous les éléments de la forme xa où $x \in$ A. Il contient donc les éléments de la forme : $na + xa$ où $n \in \mathbb{Z}$ et $x \in$ A.

Comme A est unitaire, on a

$$\begin{aligned} na &= a + \cdots + a \quad n \text{ fois si } n > 0 \\ &= -a - \cdots - a \quad -n \text{ fois si } n < 0 \\ na &= 1_\mathrm{A}a + 1_\mathrm{A}a + \cdots + 1_\mathrm{A}a = (1_\mathrm{A} + \cdots + 1_\mathrm{A})a = (n1_\mathrm{A})a \end{aligned}$$

D'où :

$$na + xa = (n \cdot 1_\mathrm{A})a + xa = (n \cdot 1_\mathrm{A} + x)a \in \mathrm{A}a$$

Inversement,

$$\forall y \in \mathrm{A}a, \exists x \in \mathrm{A} \quad y = xa$$

Or xa appartient à l'idéal engendré par a. □

Exemple. $(2\mathbb{Z}, +, \times)$ est un anneau qui n'est pas unitaire. L'idéal engendré par 4 n'est pas $4 \cdot (2\mathbb{Z}) = 8\mathbb{Z}$ car $4 \notin 8\mathbb{Z}$.

Définition 3.7. On dit qu'un idéal I d'un anneau commutatif unitaire est principal s'il peut être engendré par un seul élément.

On dit qu'un anneau commutatif unitaire est principal si et seulement si tout idéal de cet anneau est principal.

Exemples. $\mathbb{Z}, \mathrm{K}[x]$ où K est un corps commutatif.

Théorème 3.7. *Soit* A *un anneau et* I *un idéal bilatère de* A*. La relation binaire* R *définie sur* A *par :*

$$\forall x, y \in \mathrm{A} \quad x\mathrm{R}y \iff x - y \in \mathrm{I}$$

est une relation d'équivalence compatible avec la structure d'anneau de A*.*

Démonstration. $(\mathrm{A}, +)$ est un groupe commutatif donc tous ses sous groupes sont distingués donc d'après le premier chapitre, R est une relation d'équivalence compatible avec la première loi de A. Montrons qu'elle est compatible avec la deuxième loi.

$\forall x, x', y, y' \in \mathrm{A}$ supposons $x\mathrm{R}y$ et $x'\mathrm{R}y'$. On veut montrer que $xx'\mathrm{R}yy'$:

$$xx' - yy' = (x - y)x' + y(x' - y')$$

Or

$$\begin{aligned} x\mathrm{R}y \Rightarrow x - y \in \mathrm{I} \qquad & \text{I idéal et } x' \in \mathrm{A} \Rightarrow (x - y)x' \in \mathrm{I} \\ x'\mathrm{R}y' \Rightarrow x' - y' \in \mathrm{I} \qquad & \text{I idéal et } y \in \mathrm{A} \Rightarrow y(x' - y') \in \mathrm{I} \end{aligned}$$

I est stable pour $+$ donc $xx' - yy' \in \mathrm{I}$ et $xx'\mathrm{R}yy'$.

D'où R est compatible avec la structure d'anneau de A. □

Remarque. On peut donc munir A/R de deux lois quotients : la première induite par $+$ fait de A/R un groupe ; la seconde induite par $\times$ est associative et distributive par rapport à la première. A/R est donc un anneau pour les deux lois quotients. On le notera A/I.

Théorème 3.8. *Soit* A *un anneau et* R *une relation d'équivalence compatible avec la structure d'anneau de* A*. Soit* I *la classe d'équivalence de* 0_{A} *pour cette relation. Alors* I *est un idéal bilatère de* A *et* $x\mathrm{R}y \iff x - y \in \mathrm{I}$*.*

Démonstration. R étant compatible avec $+$, I est un sous groupe distingué de $(\mathrm{A},+)$. De plus

$$\begin{aligned}\forall x \in \mathrm{I}, \forall y \in \mathrm{A} \quad & x\mathrm{R}0_{\mathrm{A}} \Rightarrow xy\mathrm{R}0_{\mathrm{A}}y \\ & xy\mathrm{R}0_{\mathrm{A}} \quad \text{donc } xy \in \mathrm{I}\end{aligned}$$

De même

$$\begin{aligned}x\mathrm{R}0_{\mathrm{A}} \Rightarrow & yx\mathrm{R}y0_{\mathrm{A}} \\ & yx\mathrm{R}0_{\mathrm{A}} \quad \text{donc } yx \in \mathrm{I}\end{aligned}$$

Donc I est un idéal bilatère de A.

De plus, R est compatible avec la première loi $+$ de A, donc si $x\mathrm{R}y$

$$\begin{aligned}x+(-y)\mathrm{R}y+(-y) \\ x-y\mathrm{R}0_{\mathrm{A}} \\ x-y \in \mathrm{I}\end{aligned}$$

□

Définition 3.8. Un homomorphisme f d'un anneau A dans un anneau B est une application de A dans B telle que :

$$\begin{aligned}\forall x, y \in \mathrm{A} \quad & f(x+y) = f(x)+f(y) \\ & f(xy) = f(x)f(y)\end{aligned}$$

Théorème 3.9. *Si f est un homomorphisme de l'anneau* A *dans l'anneau* B *:*

1. $f(0_{\mathrm{A}}) = 0_{\mathrm{B}}$
2. $\forall x \in \mathrm{A}$, $f(-x) = -f(x)$
3. $\widehat{f}(\mathrm{A})$ *est un sous anneau de* B.
4. $\mathrm{Ker}\, f$ *est un idéal bilatère de* A.
5. f *est injectif si et seulement si* $\mathrm{Ker}\, f = \{0_{\mathrm{A}}\}$.

Démonstration. Les 1,2,5 découlent des propriétés des homomorphismes de groupes.

3. Nous savons que $\widehat{f}(\mathrm{A})$ est un sous groupe de B. Il reste à montrer sa stabilité dans B

$$\forall u, v \in \widehat{f}(\mathrm{A}), \exists x, y \in \mathrm{A} \quad f(x) = u \text{ et } f(y) = v$$

Alors $uv = f(x)f(y) = f(xy) \in \widehat{f}(\mathrm{A})$. Donc $\widehat{f}(\mathrm{A})$ est un sous anneau de B.

4. $\operatorname{Ker} f$ est un sous groupe distingué de A. De plus,

$$\forall x \in \operatorname{Ker} f, \forall a \in \mathrm{A} \quad f(ax) = f(a)f(x) = f(a)0_{\mathrm{B}} = 0_{\mathrm{B}}$$
$$\forall x \in \operatorname{Ker} f, \forall a \in \mathrm{A} \quad f(xa) = f(x)f(a) = 0_{\mathrm{B}}f(a) = 0_{\mathrm{B}}$$

Donc $\forall a \in \mathrm{A}$, $ax \in \operatorname{Ker} f$ et $xa \in \operatorname{Ker} f$, donc $\operatorname{Ker} f$ est un idéal de A.

□

Remarques.
- Si A est commutatif, $\widehat{f}(\mathrm{A})$ est commutatif.
- Si A est unitaire, $\widehat{f}(\mathrm{A})$ est unitaire et si 1_{A} est l'élément neutre de la seconde loi de A, $f(1_{\mathrm{A}})$ est l'élément neutre de la seconde loi de $\widehat{f}(\mathrm{A})$.
- Si $x \in \mathrm{A}^{\times}$ alors $f(x) \in \left[\widehat{f}(\mathrm{A})\right]^{\times}$ et $f(x^{-1}) = \left[f(x)\right]^{-1}$.

Cependant, A peut être intègre sans que $\widehat{f}(\mathrm{A})$ ne le soit. Par exemple :

$$\begin{aligned} \mathbb{Z} &\to \frac{\mathbb{Z}}{n\mathbb{Z}} \\ x &\mapsto \bar{x} \end{aligned}$$

où n n'est pas premier.

Théorème 3.10. *Soit f un homomorphisme d'anneau d'un anneau* A *dans un anneau* B*. Alors f peut se décomposer sous la forme $f = i \circ b \circ s$ où :*
- $s : \mathrm{A} \to \mathrm{A}/\mathrm{R}$ *homomorphisme surjectif défini par $x \mapsto \bar{x}$ où* R *est définie par $\forall x, y \in \mathrm{A}$, $x\mathrm{R}y \iff f(x) = f(y)$.*
- $b : \mathrm{A}/\mathrm{R} \to \widehat{f}(\mathrm{A})$ *homomorphisme bijectif défini par $\bar{x} \mapsto f(x)$.*
- $i : \widehat{f}(\mathrm{A}) \to \mathrm{B}$ *homomorphisme injectif défini par $f(x) \mapsto f(x)$.*

Définition 3.9. Soit A un anneau unitaire, d'élément neutre 1_{A} pour sa seconde loi. Soit A' le sous groupe monogène de $(\mathrm{A}, +)$ engendré par 1_{A}. On désigne par φ l'application de $\mathbb{Z}$ dans $(\mathrm{A}', +)$ qui à tout entier n associe $n \cdot 1_{\mathrm{A}}$: c'est un homomorphisme surjectif de $\mathbb{Z}$ sur A'.

Si φ est injective, le seul entier n tel que $n \cdot 1_{\mathrm{A}} = 0_{\mathrm{A}}$ c'est $0_{\mathbb{Z}}$. Alors $\mathrm{A}' = \widehat{\varphi}(\mathbb{Z})$ est isomorphe à $\mathbb{Z}$, et on dit que A est de caractéristique nulle.

Si φ n'est pas injective, $\operatorname{Ker}\varphi$ est un sous groupe de $\mathbb{Z}$, donc de la forme $n\mathbb{Z}$ où $n \in \mathbb{N}^*$ et $\widehat{\varphi}(\mathbb{Z}) = \mathrm{A}' \approx \mathbb{Z}/n\mathbb{Z}$. On dit que A est de caractéristique n. n est alors le plus petit entier strictement positif tel que $n \cdot 1_{\mathrm{A}} = 0_{\mathrm{A}}$.

Remarques. Si A est de caractéristique nulle, on considère $\mathbb{Z}$ comme une partie de A. On assimile $\mathbb{Z}$ et $\widehat{f}(\mathbb{Z})$ qui lui est isomorphe. On dit aussi que $\mathbb{Z}$ est plongé (*imbedded*) dans A. Dans ce cas, l'élément $n \cdot 1_{\mathrm{A}}$ est représenté par n (ou n_{A}).

La caractéristique d'un anneau ayant un nombre fini d'éléments est non nulle.

Dans un anneau de caractéristique $n > 0$, on a $n \cdot a = 0$ pour tout a de A, car

$$na = 1_A a + 1_A a + \cdots + 1_A a = (1_A + 1_A + \cdots + 1_A)a = (n1_A)a = 0_A a = 0_A$$

Théorème 3.11. *La caractéristique d'un anneau intègre unitaire est soit nulle, soit un nombre premier.*

Démonstration. Soit p la caractéristique de l'anneau unitaire intègre A. Supposons $p \neq 0$ et $p = qr$ où $q > 0$ et $r > 0$. Soit 1_A l'élément neutre de la deuxième loi de A.

$$\begin{aligned}(q1_A)(r1_A) &= \left(\overbrace{1_A + \cdots + 1_A}^{q \text{ fois}}\right)\left(\overbrace{1_A + \cdots + 1_A}^{r \text{ fois}}\right) \\ &= \left(1_A + \cdots + 1_A\right)1_A + \cdots + \left(1_A + \cdots + 1_A\right)1_A \\ &= \underbrace{1_A + \cdots + 1_A}_{(qr) \text{ fois}} = (qr)1_A = p1_A = 0_A\end{aligned}$$

A étant intègre, $q1_A = 0$ ou $r1_A = 0$. p étant le plus petit entier tel que $p1_A = 0_A$, on a soit $p = q$ et $r = 1$, soit $p = r$ et $q = 1$. Donc p est premier. □

Chapitre 4

Corps

Définition 4.1. Un corps est un anneau unitaire dans lequel tout élément non nul est inversible. Si la seconde loi est commutative, on dit que le corps est commutatif.

Définition 4.2. On dit qu'une partie non vide L de K est un sous corps de K, si les lois induites par celles de K sur cette partie donnent à cette partie une structure de corps.

Remarques.

1. L est un sous corps de $K \Rightarrow 0_K \in L$.
2. $L^* = L \setminus \{0\}$ est un sous groupe multiplicatif de K^*, donc $1_K \in L$.
3. Tout sous anneau de K contenant les inverses de tous ses éléments pour $\times$, sauf 0, est un sous corps de K.

Théorème 4.1. *Toute intersection de sous corps est un sous corps.*

Démonstration. Nous savons déjà que toute intersection de sous anneaux est un sous anneau. Il reste à montrer que 1_K appartient à l'intersection et que l'inverse de tout élément de l'intersection appartient à l'intersection.

Soit $(L_i)_{i\in I}$ une famille de sous corps de K, et $L = \bigcap_{i\in I} L_i$. Alors $\forall i \in I$, $1_K \in L_i$ donc $1_K \in L$.

$\forall x \in L, x \neq 0_K$, $\forall i \in I, x \in L_i$ donc $x^{-1} \in L_i$ et $xx^{-1} = x^{-1}x = 1_K$. Donc $x^{-1} \in L$. Donc L est un sous corps de K. □

Définition 4.3. Soit A une partie non vide d'un corps K. On appelle sous corps engendré par A le plus petit sous corps de K contenant A. C'est l'intersection de tous les sous corps de K contenant A.

Théorème 4.2. *Soit* A *un anneau commutatif unitaire. Pour que* A *soit un corps, il faut et il suffit que les deux seuls idéaux de* A *soient* $\{0_A\}$ *et* A.

Démonstration. Si A est un corps, soit I un idéal de A autre que $\{0\}$. I possède donc un élément $x \neq 0$. A étant un corps, x est inversible dans A : $\exists x^{-1} \in A$, $xx^{-1} = 1_A$. Mais $x \in I, x^{-1} \in A$ et $1_A = xx^{-1} \in I$. Alors $I = A$ car $\forall y \in A$, $y = y \cdot 1_A \in I$ et $A \subseteq I$.

Si les seuls idéaux de l'anneau commutatif unitaire A sont $\{0\}$ et A, soit a un élément quelconque de A, autre que 0. Considérons (a) l'idéal de A engendré par a. $a \in (a)$ donc $(a) \neq \{0\}$. Alors $(a) = A$. Or le théorème 3.6 nous dit que $(a) = aA$, mais $1_A \in A$ donc $1_A \in (a) = A = aA$. Il existe donc $a' \in A$ tel que $aa' = 1_A$. Donc tout élément non nul de A est inversible et A est un corps. □

Théorème 4.3. *Soient* A *un anneau commutatif unitaire et* I *un idéal de* A*. Pour que l'anneau quotient* A/I *soit un corps, il faut et il suffit que l'idéal* I *soit maximal dans l'ensemble des idéaux propres de* A *(idéaux différents de* A*) par rapport à l'inclusion.*

Démonstration. Supposons que A/I est un corps. Alors $I \neq A$ car un corps possède au moins deux éléments : $0_{A/I}$ et $1_{A/I}$. Donc I est un idéal propre de A. Soit J un idéal de A tel que $I \subseteq J \subseteq A$. Si $I \neq J$, soit $a \in \complement_J I$. Dans l'anneau quotient A/I, $[a]_I \neq [0_A]_I$ car $[0_A]_I = I$. Alors, comme A/I est un corps, $[a]_I$ est inversible. Soit $[a]_I^{-1}$ son inverse. $\forall x \in A$, soit $[x]_I$. Posons

$$\beta = [x]_I [a]_I^{-1}$$
$$\beta [a]_I = [x]_I$$

Si $b \in \beta$:

$$[b]_I [a]_I = [x]_I$$
$$[ba]_I - [x]_I = [0_A]_I = I$$
$$[ba - x]_I = I$$
$$ba - x \in I$$

Or $a \in J$ et J est un idéal donc $ba \in J$. De plus $I \subseteq J$ donc $x \in J$ et $A \subseteq J$. D'où $A = J$ et I est un idéal propre maximal de A.

Supposons que I est un idéal propre maximal de A. Soient $\gamma \in (A/I) \setminus \{[0]_I\}$ et $c \in \gamma$. Soit $C = \{b \in A / \exists x \in I, \exists a \in A \quad b = x + ca\}$. Montrons que C est un idéal de A qui contient I.

- $0_A \in C$ car $0_A = 0_A + c \cdot 0_A$, donc $C \neq \emptyset$.
- $\forall b, b' \in C, \exists x, x' \in I, \exists a, a' \in A \quad b = x + ca, b' = x' + ca'$.

$$b - b' = (x - x') + c(a - a') \in C$$

– $\forall t \in \mathrm{A},\ tb = tx + c(ta) \in \mathrm{C}$.

Donc C est un idéal de A.

$$\forall x \in \mathrm{I} \quad x = x + c \cdot 0_{\mathrm{A}} \in \mathrm{C}$$

d'où $\mathrm{I} \subseteq \mathrm{C}$. $c \in \gamma$ et $\gamma \neq \mathrm{I}$ donc $c \notin \mathrm{I}$. Or $c = 0_{\mathrm{A}} + c \cdot 1_{\mathrm{A}} \in \mathrm{C}$. D'où $\mathrm{I} \subsetneq \mathrm{C}$. I étant un idéal propre maximal de A, $\mathrm{C} = \mathrm{A}$. Par conséquent, tout élément de A a une écriture sous la forme $x + ca$. En particulier $1_{\mathrm{A}} = x + ca$ pour un x de I et un a de A. D'où :

$$\begin{aligned}
[1_{\mathrm{A}}]_{\mathrm{I}} &= [x + ca]_{\mathrm{I}} \\
&= [x]_{\mathrm{I}} + [c]_{\mathrm{I}}[a]_{\mathrm{I}} \\
&= [0]_{\mathrm{I}} + [c]_{\mathrm{I}}[a]_{\mathrm{I}} \\
&= [c]_{\mathrm{I}}[a]_{\mathrm{I}} \\
&= \gamma[a]_{\mathrm{I}}
\end{aligned}$$

D'où γ est inversible dans A/I. Alors A/I est un corps. □

Théorème 4.4. *Tout anneau fini unitaire intègre ayant au moins deux éléments est un corps.*

Démonstration. Soit $a \in \mathrm{A} \setminus \{0\}$. Soit $\gamma_a : \mathrm{A} \to \mathrm{A}$ définie par $x \mapsto ax$. γ_a est injective car si $\gamma_a(x_1) = \gamma_a(x_2)$ alors $ax_1 = ax_2 \iff a(x_1 - x_2) = 0$. Or A est intègre et $a \neq 0$ donc $x_1 = x_2$. Le cardinal étant fini, γ_a est une bijection. Il existe donc $a' \in \mathrm{A}$ tel que $\gamma_a(a') = 1_{\mathrm{A}} \iff aa' = 1_{\mathrm{A}}$. Donc a est inversible et A est un corps. □

Définition 4.4. On dit qu'un idéal I de A est premier si A/I est intègre.

On dit qu'un élément p de A est premier si l'idéal principal qu'il engendre (p) est premier, propre et non nul.

Remarques.

1. (I est premier) $\iff$ $(ab \in \mathrm{I} \Rightarrow a \in \mathrm{I}$ ou $b \in \mathrm{I})$.
   Si I est premier, supposons $[x]_{\mathrm{I}}[y]_{\mathrm{I}} = [0]_{\mathrm{I}} = \mathrm{I}$. Donc $xy \in \mathrm{I}$. Or I est premier, donc $[x]_{\mathrm{I}} = [0]_{\mathrm{I}}$ ou $[y]_{\mathrm{I}} = [0]_{\mathrm{I}} \iff x \in \mathrm{I}$ ou $y \in \mathrm{I}$.
   Réciproquement, si $xy \in \mathrm{I} \Rightarrow x \in \mathrm{I}$ ou $y \in \mathrm{I}$, soient X et Y deux classes de A/I telles que $\mathrm{XY} = [0]_{\mathrm{I}}$. Si $x \in \mathrm{X}$ et $y \in \mathrm{Y}$:

   $$\begin{aligned}
   [x]_{\mathrm{I}}[y]_{\mathrm{I}} &= [0]_{\mathrm{I}} \\
   [xy]_{\mathrm{I}} &= [0]_{\mathrm{I}} = \mathrm{I} \\
   xy &\in \mathrm{I}
   \end{aligned}$$

   Alors $x \in \mathrm{I}$, c'est à dire $[x]_{\mathrm{I}} = [0]_{\mathrm{I}}$ ou $y \in \mathrm{I}$, c'est à dire $[y]_{\mathrm{I}} = [0]_{\mathrm{I}}$. Donc A/I est intègre et I est un idéal premier de A.

2. Un élément premier p est non nul et non inversible.
   - Si $p = 0$ alors $(p) = \{0\}$ et p n'est pas premier.
   - Si p est inversible alors $(p) = \mathrm{A}$, (p) n'est pas propre et donc pas premier.
3. Si p est premier et divise ab, alors p divise a ou p divise b.

Théorème 4.5. *Soit* A *un anneau commutatif unitaire fini et* I *un idéal propre de* A. *Les quatres propriétés suivantes sont équivalentes :*

1. I *est maximal.*
2. I *est premier.*
3. A/I *est intègre.*
4. A/I *est un corps.*

Démonstration. $1 \Rightarrow 2$. Soient a et b deux éléments de A tels que $ab \in \mathrm{I}$. Supposons $a \notin \mathrm{I}$. Alors l'idéal $\mathrm{I} + (a)$, le plus petit idéal contenant $\mathrm{I} \cup (a)$, est égal à A car I est maximal. Donc $1 \in \mathrm{I} + (a)$ et $\exists x \in \mathrm{I}$ et $\exists c \in \mathrm{A}$ tel que $1 = x + ca$ d'où $b = bx + c(ab) \in \mathrm{I}$. Donc I est premier.

$2 \Rightarrow 3$ par définition.

$3 \Rightarrow 4$. A étant fini, A/I l'est aussi et on applique le théorème 4.4.

$4 \Rightarrow 1$ d'après le théorème 4.3. □

Chapitre 5

Polynômes

Notation. Soient E et F deux ensembles non vides. On note F^E l'ensemble des applications de E dans F.

5.1 Anneau des polynômes

Définition 5.1. Soit A un anneau commutatif unitaire. On appelle polynôme à une indéterminée (on dit parfois variable) à coefficients dans A, tout élément de $A^{\mathbb{N}}$ dont l'image comporte un nombre fini d'éléments non nuls, autrement dit une suite d'éléments de A dont tous les termes sont nuls à partir d'un certain rang.

Les termes d'une telle suite sont appelés coefficients du polynôme.

Définition 5.2. Soit $P = (a_0, a_1, \dots, a_n, \dots)$. On appelle degré du polynôme P le plus grand entier p tel que $a_p \neq 0$. On le note deg(P).

$$\deg P = \max\{n \in \mathbb{N} / a_n \neq 0\}$$

Par convention, si $P = \Theta = (0, 0, \dots, 0, \dots)$ on pose $\deg P = -\infty$.

Remarque. L'égalité des polynômes est une égalité entre deux applications de $\mathbb{N}$ dans A : il faut, si $P = (a_0, a_1, \dots, a_n, \dots)$ et $Q = (b_0, b_1, \dots, b_n, \dots)$ que $a_k = b_k \ \forall k \in \mathbb{N}$.

Définition 5.3. Soit $P = (a_0, a_1, \dots, a_n, \dots)$. On appelle valuation de P et on note $\nu(P)$ le plus petit entier p tel que $a_p \neq 0$.

$$\nu(P) = \min\{n \in \mathbb{N} / a_n \neq 0\}$$

Par convention, si $P = \Theta = (0, 0, \dots, 0, \dots)$, on pose $\nu(P) = +\infty$.

Définition 5.4. Soient $P = (a_0, a_1, \dots, a_n, \dots)$ et $Q = (b_0, b_1, \dots, b_n, \dots)$ deux polynômes. On appellera somme de P et de Q le polynôme noté $P + Q$ et égal à $(a_0 + b_0, a_1 + b_1, \dots, a_n + b_n, \dots)$.

Théorème 5.1. *Muni de l'opération somme définie ci-dessus, l'ensemble des polynômes à coefficients dans un anneau commutatif unitaire* A *à une indéterminée est un groupe abélien.*

Démonstration. Aux étudiants. □

Définition 5.5. Soient $P = (a_0, \dots, a_n, \dots)$ et $Q = (b_0, \dots, b_n, \dots)$ deux polynômes. On appellera produit de P et de Q le polynôme noté PQ et égal à $(\gamma_0, \gamma_1, \dots, \gamma_n, \dots)$ où $\gamma_r = \sum_{i+j=r} a_i b_j$.

Théorème 5.2. *Muni des deux lois définies ci-dessus, l'ensemble des polynômes à coefficients dans un anneau commutatif unitaire* A *à une indéterminée est un anneau commutatif unitaire dont une partie est isomorphe à* A.

Démonstration.

1. (a) Montrons que la seconde loi est associative. Soient

$$\begin{aligned} P &= (a_0, a_1, \dots, a_n, \dots), \\ Q &= (b_0, b_1, \dots, b_n, \dots), \\ R &= (c_0, c_1, \dots, c_n, \dots) \end{aligned}$$

On a

$$QR = (\alpha_0, \dots, \alpha_n, \dots) \quad \text{où} \quad \alpha_r = \sum_{i+j=r} b_i c_j$$

$$PQ = (\beta_0, \dots, \beta_n, \dots) \quad \text{où} \quad \beta_r = \sum_{i+j=r} a_i b_j$$

P(QR) a pour coefficients les γ_r :

$$\begin{aligned} \gamma_r &= \sum_{i+j=r} a_i \alpha_j = \sum_{i+j=r} a_i \left(\sum_{m+p=j} b_m c_p \right) \\ &= \sum_{i+m+p=r} a_i b_m c_p \end{aligned}$$

(PQ)R a pour coefficients les δ_r :

$$\begin{aligned} \delta_r &= \sum_{i+j=r} \beta_i c_j = \sum_{i+j=r} \left(\sum_{m+p=i} a_m b_p \right) c_j \\ &= \sum_{m+p+j=r} a_m b_p c_j \end{aligned}$$

D'où (PQ)R = P(QR).

(b) On montre de même que $P(Q+R) = PQ+PR$ et $(P+Q)R = PR+QR$.

(c) Le polynôme $I = (1, 0, \dots, 0, \dots)$ est l'élément neutre de la seconde loi.

(d) La commutativité de la seconde loi découle de celle de la seconde loi de A.

2. Soit $\mathscr{A} = \{(a, 0, \dots, 0, \dots) / a \in A\}$. L'application $f : A \to \mathscr{A}$ définie par $a \mapsto (a, 0, \dots, 0, \dots)$ est trivialement bijective.

$$\begin{aligned} f(a+b) &= (a+b, 0, \dots, 0, \dots) = (a, 0, \dots, 0, \dots) + (b, 0, \dots, 0, \dots) \\ &= f(a) + f(b) \\ f(ab) &= (ab, 0, \dots, 0, \dots) = (a, 0, \dots, 0)(b, 0, \dots, 0) \\ &= f(a)f(b) \end{aligned}$$

Donc f est un isomorphisme de A dans $\mathscr{A}$.

Par la suite on assimilera $(a, 0, \dots, 0, \dots)$ avec a, Θ avec 0_A et I avec 1_A. □

Définition 5.6. Soient $\lambda \in A$ et P un polynôme à une indéterminée à coefficients dans A. On appellera produit de λ par P le polynôme noté λP et défini par

$$\lambda P = f(\lambda) P$$

Si $P = (a_0, \dots, a_n, \dots)$ on a $\lambda P = (\lambda a_0, \dots, \lambda a_n, \dots)$.

Théorème 5.3. *La loi définie ci-dessus a les propriétés suivantes :* $\forall \lambda, \mu \in A$, *pour tous polynômes* P *et* Q

$$\begin{gathered} \lambda(P+Q) = \lambda P + \lambda Q \\ (\lambda+\mu)P = \lambda P + \mu Q \\ \lambda(\mu P) = (\lambda\mu)P \\ 1P = P \end{gathered}$$

Démonstration. Ces propriétés sont celles des deux lois internes sur les polynômes réécrites avec nos conventions. □

Notation. On notera X le polynôme $(0, 1, 0, \dots, 0, \dots)$.

$$X = (\delta_{1i})_{i \in \mathbb{N}}$$

où δ_{ij} est la notation de Kronecker : $\delta_{ij} = 0$ si $i \neq j$ et $\delta_{ij} = 1$ si $i = j$.

Théorème 5.4.

1. *Pour tout* $n \in \mathbb{N}^*$, $X^n = (\delta_{ni})_{i \in \mathbb{N}}$.

2. $\forall p, q \in \mathbb{N}^*$, $X^{p+q} = X^p X^q$.

Démonstration.

1. Par récurrence : c'est vrai pour $n = 1$ par définition. Supposons $X^n = (\delta_{ni})_{i\in\mathbb{N}}$. Alors
$$X^{n+1} = XX^n = (\delta_{1i})(\delta_{ni}) = \sum_{i+j=k} \delta_{1i}\delta_{nj} = (c_k)$$
où $c_k = \sum_{i+j=k} \delta_{1i}\delta_{nk-i}$. Pour que $c_k \neq 0$ il faut que $\delta_{1i} \neq 0$ donc que $1 = i$, et que $n = k - i = k - 1$. Donc $k = n + 1$ et $(c_k) = (\delta_{n+1,i})$.
2. $X^p X^q = (c_0, c_1, \ldots, c_r, \ldots)$ avec $c_r = \sum_{i+j=r} \delta_{pi}\delta_{qi}$. Pour que c_r soit non nul, il faut que $i = p$ et $q = j$, donc que $r = i + j = p + q$. Donc $c_r = 0$ si $p + q \neq r$ et $c_r = 1$ si $p + q = r$. Donc $X^p X^q = X^{p+q}$.

□

Notation. Si $P = (a_0, a_1, \ldots, a_n, 0, \ldots, 0, \ldots)$ est un polynôme, on l'écrira désormais $P = a_0 + a_1 X + \cdots + a_n X^n$.

On notera A[X] l'ensemble des polynômes à une indéterminée à coefficients dans A.

Théorème 5.5. *Soit* A *un anneau commutatif unitaire. Quelque soit n dans* $\mathbb{N}$*, une relation de la forme* $\alpha_0 + \alpha_1 X + \cdots + \alpha_n X^n = 0$ *entraîne que tous les* α_i *sont nuls.*

Tout polynôme $P \in A[X]$ *s'écrit donc d'une manière unique sous la forme* $P = \alpha_0 + \alpha_1 X + \cdots + \alpha_n X^n$.

Démonstration.

$$\alpha_0 + \alpha_1 X + \cdots + \alpha_n X^n = 0$$
$$(\alpha_0, \alpha_1, \ldots, \alpha_n, 0, \ldots, 0, \ldots) = (0, 0, \ldots, 0, \ldots)$$

L'égalité des deux suites entraîne que $\alpha_0 = \alpha_1 = \cdots = \alpha_n = 0$. Donc si

$$P = \alpha_0 + \alpha_1 X + \cdots + \alpha_n X^n = \beta_0 + \beta_1 X + \cdots + \beta_m X^m$$

alors

$$(\alpha_0, \alpha_1, \ldots, \alpha_n, 0, \ldots, 0, \ldots) = (\beta_0, \beta_1, \ldots, \beta_m, 0, \ldots, 0, \ldots)$$

D'où $\alpha_0 = \beta_0$, $\alpha_1 = \beta_1$, ... L'écriture de P sous la forme ci-dessus est donc unique. □

Théorème 5.6. *Soit* A *un anneau commutatif unitaire. Si* P *et* Q *sont dans* A[X] *:*

$$\begin{aligned}\deg(PQ) &\leqslant \deg(P)+\deg(Q)\\ \nu(PQ) &\geqslant \nu(P)+\nu(Q)\\ \deg(P+Q) &\leqslant \max\big(\deg(P),\deg(Q)\big)\\ \nu(P+Q) &\geqslant \min\big(\nu(P),\nu(Q)\big)\end{aligned}$$

Si de plus A *est intègre,* $\deg(PQ)=\deg(P)+\deg(Q)$ *et* $\nu(PQ)=\nu(P)+\nu(Q)$.

Démonstration. Supposons

$$\begin{aligned}P &= \alpha_0+\alpha_1X+\cdots+\alpha_pX^p\\ Q &= \beta_0+\beta_1X+\cdots+\beta_qX^q\end{aligned}$$

On a $\deg(P)=p$ et $\deg(Q)=q$. Donc si $i+j>p+q$, $\alpha_i\beta_j=0$ d'où $\deg(PQ)\leqslant \deg(P)+\deg(Q)$. Si A est intègre, $\alpha_p\beta_q\neq 0$ donc $\deg(PQ)=\deg(P)+\deg(Q)$.

$(P+Q)=\sum_{i=0}^{\max\{p,q\}}\big(\alpha_i+\beta_i\big)X^i$ donc $\deg(P+Q)\leqslant\max\big(\deg P,\deg Q\big)$.

Soient P et Q deux polynômes tels que $\nu(P)=r$ et $\nu(Q)=s$. Si $P=(\alpha_i)_{i\in\mathbb{N}}$ et $Q=(\beta_i)_{i\in\mathbb{N}}$:

$$\forall i\in\mathbb{N},\quad i<r\Rightarrow\alpha_i=0\quad\text{et}\quad\forall j\in\mathbb{N},\quad j<s\Rightarrow\beta_j=0$$

D'où $i+j<r+s\Rightarrow\alpha_i\beta_j=0$ d'où $\nu(PQ)\geqslant\nu(P)+\nu(Q)$. Si A est intègre, $\alpha_r\beta_s\neq 0$ et alors $\nu(PQ)=\nu(P)+\nu(Q)$.

Enfin,

$$\forall i\in\mathbb{N},\quad i<\min(r,s)\Rightarrow\alpha_i=\beta_i=0$$

d'où $\alpha_i+\beta_i=0$ et $\nu(P+Q)\geqslant\min\big(\nu(P),\nu(Q)\big)$. □

Remarques.

1. D'après le théorème 5.6, si A est intègre, A[X] l'est aussi. Si $P\neq 0$, $Q\neq 0$, $\deg(P)=p$ et $\deg(Q)=q$, alors $\alpha_p\neq 0$ et $\beta_q\neq 0$. D'où $\alpha_p\beta_q\neq 0$. Or c'est le coefficient de X^{p+q} dans PQ. Donc $PQ\neq 0$.
2. On comprend mieux le choix de notre convention $\deg(0)=-\infty$ car $\deg(PQ)=\deg(P)+\deg(Q)$ même si P ou Q est nul. On aurait pu prendre $\deg(0)=+\infty$ mais $\deg(P+Q)\leqslant\sup\big(\deg(P),\deg(Q)\big)$ oblige à prendre $-\infty$.

   De même le choix de $\nu(0)=+\infty$ vient de la relation $\nu(PQ)\geqslant\nu(P)+\nu(Q)$.

Théorème 5.7. *Soit* K *un corps commutatif. Alors* K[X] *est une* K*-algèbre unitaire intègre.*

Une K*-algèbre est un ensemble* E *muni de deux lois de composition interne,* $+$ *et* $\times$*, et d'une loi externe* $\cdot$ *sur* $K\times E$ *vérifiant :*

1. $(\mathrm{E}, +, \cdot)$ *est un* K*-espace vectoriel.*
2. $(\mathrm{E}, +, \times)$ *est un anneau.*
3. $\forall x, y \in \mathrm{E},\ \forall \lambda \in \mathrm{K},\ \lambda \cdot (x \times y) = (\lambda \cdot x) \times y = x \times (\lambda \cdot y)$.

Définition 5.7. On appelle suite de polynômes de degrés échelonnés (resp. de valuations échelonnées) toute suite $(\mathrm{P}_n)_{n\in\mathbb{N}}$ de polynômes telle que $\forall n \in \mathbb{N}$, $\deg \mathrm{P}_n = n$ (resp. $\nu(\mathrm{P}_n) = n$).

Théorème 5.8. *Dans l'espace vectoriel* $\mathrm{K}[\mathrm{X}]$*, toute suite de polynômes de degrés échelonnés (resp. de valuations échelonnées) est libre. Toute suite de polynômes de degrés échelonnés est une base de* $\mathrm{K}[\mathrm{X}]$*. Toute famille* $(\mathrm{P}_0, \mathrm{P}_1, \ldots, \mathrm{P}_n)$ *de polynômes de* $\mathrm{K}_n[\mathrm{X}]$ *de valuations échelonnées est une base de* $\mathrm{K}_n[\mathrm{X}]$.

Démonstration. Soit $\sum_{i=1}^{k} \lambda_{n_i} \mathrm{P}_{n_i} = 0$ où $\deg \mathrm{P}_{n_i} = n_i$. Supposons que n_k soit le degré le plus élevé des polynômes figurant dans la combinaison linéaire avec un coefficient non nul.

$$\lambda_{n_1} \mathrm{P}_{n_1} + \cdots + \lambda_{n_k} \mathrm{P}_{n_k} = 0$$

avec $\lambda_{n_k} \neq 0$. D'où :

$$\begin{gathered}(-\lambda_{n_k})\mathrm{P}_{n_k} = \lambda_{n_1} \mathrm{P}_{n_1} + \cdots + \lambda_{n_{k-1}} \mathrm{P}_{n_{k-1}} \\ \deg\left((-\lambda_{n_k})\mathrm{P}_{n_k}\right) = n_k \\ \deg\left(\lambda_{n_1} \mathrm{P}_{n_1} + \cdots + \lambda_{n_{k-1}} \mathrm{P}_{n_{k-1}}\right) = n_{k-1} < n_k\end{gathered}$$

Absurde, Donc tous les coefficients sont nuls.

Soit (P_n) une telle suite. Elle est libre d'après ce qui précède. Pour tout entier m, $\left(\mathrm{P}_0, \mathrm{P}_1, \ldots, \mathrm{P}_m\right)$ est une famille libre à $(m+1)$ éléments de $\mathrm{K}_m[\mathrm{X}]$, qui est de dimension $(m+1)$. Donc c'est une base de $\mathrm{K}_{m+1}[\mathrm{X}]$. Soit P un polynôme quelconque de $\mathrm{K}[\mathrm{X}]$. Pour un m assez grand, $\mathrm{P} \in \mathrm{K}_m[\mathrm{X}]$ et P est une combinaison linéaire de $\left(\mathrm{P}_0, \ldots, \mathrm{P}_m\right)$. Donc $(\mathrm{P}_n)_{n\in\mathbb{N}}$ est une famille génératrice de $\mathrm{K}[\mathrm{X}]$.

Même genre d'arguments pour les valuations échelonnées. □

Remarque. Toute suite de polynômes de valuations échelonnées n'est pas forcément une base de $\mathrm{K}[\mathrm{X}]$. Soit $(\mathrm{P}_n)_{n\in\mathbb{N}}$ telle que :

$$\begin{gathered}\forall n \in \mathbb{N}, \mathrm{P}_n = (\mathrm{X}+1)\mathrm{X}^n \\ \nu(\mathrm{P}_n) = \nu(\mathrm{X}+1) + \nu(\mathrm{X}^n) = n\end{gathered}$$

Mais toute combinaison linéaire des P_n est un multiple de $(\mathrm{X}+1)$. Donc ce n'est pas une base de $\mathrm{K}[\mathrm{X}]$.

5.2 Division euclidienne

Théorème 5.9. *Soient* A *et* B *deux polynômes de* K[X] *tels que* $B \neq 0$. *Alors il existe un couple unique* (Q, R) *de polynômes de* K[X] *tels que*

$$A = BQ + R \quad \textit{avec } \deg R < \deg B$$

Q *s'appelle le quotient et* R *le reste dans la division euclidienne de* A *par* B.

Si $R = 0$, *on dit que* A *est divisible par* B, *ou que* B *divise* A *ou que* A *est un multiple de* B.

Démonstration. 1. Si $A = 0$, $0 = 0B + 0$.

2. Si $\deg A < \deg B$, $A = 0B + A$.

3. Si $\deg A \geqslant \deg B$, on pratique par récurrence sur le degré de A. Supposons que $A = a_0 + a_1X + \cdots + a_nX^n$ et $B = b_0 + b_1X + \cdots + b_qX^q$. On construit le polynôme $A_1 = A - \frac{a_n}{b_q}BX^{n-q}$. Le terme de plus haut degré de ce polynôme est strictement inférieur à n, car on a choisi le coefficient de BX^{n-q} dans ce but. Par hypothèse de récurrence, il existe Q_1 et R_1 tels que $A_1 = BQ_1 + R_1$ avec $\deg R_1 < \deg B$. D'où

$$A = \underbrace{\left(\frac{a_n}{b_q}X^{n-q} + Q_1\right)}_{Q} B + \underbrace{R_1}_{R}$$

$A = BQ + R$ ce qui montre l'existence du quotient et du reste.
Montrons l'unicité du couple (Q, R). Supposons

$$\begin{aligned} A = BQ + R = BQ_1 + R_1 \quad &\text{avec } \deg R, \deg R_1 < \deg B \\ B(Q - Q_1) &= R_1 - R \end{aligned}$$

Alors,

$$\begin{aligned} \deg\big(B(Q - Q_1)\big) &= \deg(R_1 - R) \\ \deg B + \deg(Q - Q_1) &= \deg(R_1 - R) \\ \deg(Q - Q_1) &= \deg(R_1 - R) - \deg B < 0 \end{aligned}$$

Donc $Q - Q_1 = 0$ le polynôme nul étant le seul à avoir un degré négatif. D'où $Q = Q_1$ et $R = R_1$.

□

Exemple. $A = X^3 + 2X^2 + 1$, $B = X^2 + 3$

X^3	$+2X^2$		$+1$	X^2+3
$-X^3$		$-3X$		$X+2$
	$2X^2$	$-3X$	$+1$	
	$-2X^2$		-6	
		$-3X$	-5	

$A = B(X+2) + (-3X-5)$.

Théorème 5.10. *Soit* K *un corps commutatif, alors* K[X] *est un anneau principal.*

Démonstration. Nous savons déjà que K[X] est un anneau commutatif unitaire (et même intègre). Soit I un idéal de K[X] et $H = \{n \in \mathbb{N} / \exists P \in I, P \neq 0 \text{ et } \deg P = n\}$. $H \subseteq \mathbb{N}$ donc H possède un plus petit élément n_0. Soit $P_0 \in I$ un polynôme tel que $\deg P_0 = n_0$. Alors, $\forall Q \in I$, $\exists B, R \in K[X]$ où $\deg R < \deg P_0 = n_0$ et $Q = P_0 B + R$. $P_0 \in I \Rightarrow P_0 B \in I$. D'où $Q - P_0 B \in I$, $R \in I$. Or $\deg R < n_0$ donc $R = 0$ le seul polynôme de I ayant un degré inférieur à n_0. Par conséquent, $Q = P_0 B \in (P_0)$. D'où $I \subseteq (P_0)$. Or $P_0 \in I$, donc $(P_0) \subseteq I$. D'où l'égalité $I = (P_0)$.

Tout idéal de K[X] est donc principal, par définition K[X] est un anneau principal. □

5.3 Division suivant les puissances croissantes

Théorème 5.11. *Soient* A *et* B *deux polynômes de* K[X]*,* B *étant supposé de valuation nulle, h un entier naturel. Il existe un couple unique de polynômes* (Q, R) *tels que* $A = BQ + X^{h+1}R$ *avec* $\deg Q \leqslant h$*.* Q *est appelé le quotient et* R *(ou* $X^{h+1}R$*) le reste dans la division suivant les puissances croissantes de* A *par* B *à l'ordre h.*

Démonstration. La famille $(B, XB, \ldots, X^h B, X^{h+1}, \ldots, X^{h+p})$ où $p = \deg B$ contient $h + p + 1$ polynômes de degrés inférieurs ou égaux à $(h + p)$ et de valuations échelonnées. Donc c'est une base de $K_{h+p}[X]$. On peut donc la compléter en $B, XB, \ldots, X^h B, X^{h+1}, \ldots, X^{h+p}, X^{h+p+1}, \ldots$ qui est une base de K[X].

A possède donc une écriture unique par rapport à cette base :

$$\begin{aligned} A &= \alpha_0 B + \alpha_1 XB + \alpha_2 X^2 B + \cdots + \alpha_h X^h B + \alpha_{h+1} X^{h+1} + \ldots \\ &= \underbrace{\left(\alpha_0 + \alpha_1 X + \cdots + \alpha_h X^h\right)}_{Q} B + X^{h+1} \underbrace{\left(\alpha_{h+1} + \ldots\right)}_{R} \end{aligned}$$

□

5.4 Théorème de d'Alembert-Gauss

Définition 5.8. Soit $P = \sum_{i=0}^{n} a_i X^i$ un polynôme de $K[X]$. L'application $\widetilde{P} \in K^K$ définie par :

$$\forall x \in K \quad \widetilde{P}(x) = \sum_{i=0}^{n} a_i x^i$$

est appelée fonction polynôme associée à P.

Plus généralement, si L est une K-algèbre, on peut définir sur L la fonction $\widetilde{P}_L$ par $\forall x \in L$, $\widetilde{P}_L(x) = \sum_{i=0}^{n} a_i x^i$. Ceci permet de substituer à X des matrices, des endomorphismes, *etc*.

Théorème 5.12. *L'application* $K[X] \to K^K$ *définie par* $P \mapsto \widetilde{P}$ *est un morphisme de* K*-algèbre.*

Démonstration. On vérifie facilement que $\widetilde{P+Q} = \widetilde{P} + \widetilde{Q}$, $\widetilde{\lambda P} = \lambda \widetilde{P}$ ($\lambda \in K$), $\widetilde{PQ} = \widetilde{P}\widetilde{Q}$ et $\widetilde{1} = 1$. □

Remarques.

1. Si $\deg P \leqslant 0$ alors $\widetilde{P}$ est une application constante. En général la réciproque est fausse si $\operatorname{card} K$ est fini.
2. $\widetilde{X} = \mathrm{Id}_K$.
3. Si L est une K-algèbre, l'application $P \mapsto \widetilde{P}_L$ est un morphisme de K-algèbre.

Définition 5.9. Soit $P \in K[X]$.

1. On dit que l'élément α de K est une racine (ou un zéro) de P dans K si $\widetilde{P}(\alpha) = 0$.
2. On dit que l'élément α de K est une racine de P d'ordre de multiplicité k, $k \in \mathbb{N}^*$, si P est divisible par $(X-\alpha)^k$ sans l'être par $(X-\alpha)^{k+1}$.

Remarque. Il y a bien coïncidence entre les deux définitions à l'ordre 1 : si on divise P par $(X-\alpha)$, on obtient un reste de degré strictement inférieur à $\deg(X-\alpha) = 1$.

$$\begin{aligned} P &= (X-\alpha)Q + R \\ \widetilde{P} &= \widetilde{(X-\alpha)}\widetilde{Q} + \widetilde{R} \\ \widetilde{P}(\alpha) &= (\alpha-\alpha)\widetilde{Q}(\alpha) + \widetilde{R}(\alpha) \\ &= \widetilde{R}(\alpha) \end{aligned}$$

Or $R = r_0$, $r_0 \in K$, donc $\widetilde{R} = r_0 = \widetilde{R}(\alpha)$ et $\widetilde{R}(\alpha) = \widetilde{P}(\alpha) = R$. D'où

$$P = (X - \alpha)Q + \widetilde{P}(\alpha)$$

Si α est racine, $\widetilde{P}(\alpha) = 0$ donc $P = (X - \alpha)Q$. Réciproquement si $(X - \alpha)$ divise P, le reste $\widetilde{P}(\alpha) = 0$.

Définition 5.10. On dit qu'un polynôme P de K[X] est scindé sur K s'il admet des racines $\alpha_1, \ldots, \alpha_k$ distinctes, d'ordres de multiplicité respectifs $m_1, \ldots, m_k$ telles que $\sum_{i=1}^{k} m_i = \deg P$.

Théorème 5.13 (D'Alembert)**.** *Soit* P *un polynôme de* $\mathbb{C}[X]$ *tel que* $\deg P \geqslant 1$. *Alors* P *admet au moins une racine complexe.*

Démonstration. U.E. variables complexes. □

Théorème 5.14. *Tout polynôme de* $\mathbb{C}[X]$ *est scindé. On dit aussi que* $\mathbb{C}$ *est algébriquement clos.*

Démonstration. Par récurrence sur $n = \deg P$: Si $n = 1$ c'est trivial. Si $n > 1$ et le résultat vrai pour tout polynôme de degré n, soit P un polynôme de degré $(n + 1)$. D'après le théorème 5.13, P admet au moins un zéro complexe, α, et $P(X) = (X - \alpha)Q(X)$ avec $Q(X) \in \mathbb{C}[X]$ et $\deg Q = n$. Par hypothèse de récurrence, Q(X) est scindé, et par conséquent P(X) aussi. □

Corollaire 5.1. *Tout polynôme de* $\mathbb{C}[X]$ *de degré n possède exactement n racines.*

5.5 Dérivation

Ici K sera de caractéristique nulle.

Définition 5.11. Soit $P = a_0 + a_1X + \cdots + a_nX^n$ un polynôme de K[X]. On appelle polynôme dérivé de P et on note P′ (ou D(P)) le polynôme $a_1 + 2a_2X + \cdots + na_nX^{n-1}$.

On appelle polynôme dérivé d'ordre k (ou dérivée k^{e}) de P le polynôme $P^{(k)} = \underbrace{(D \circ D \circ \cdots \circ D)}_{k \text{ fois}}(P)$. Par convention on pose $P^{(0)} = P$.

Remarques. 1. Une récurrence élémentaire montre que :

$$P^{(k)} = \sum_{i=0}^{n-k} (i + k)(i + k - 1)\ldots(i + 1)a_{i+k}X^i$$

2. Si $\deg P = n$, $P^{(n)} = n! a_n$.

Théorème 5.15.

1. D *est un endomorphisme de* $K[X]$ *en tant qu'espace vectoriel.*
2. $\forall P, Q \in K[X]$, $\forall \lambda \in K$, $\forall n \in \mathbb{N}^*$
$$\begin{aligned}(P+Q)' &= P' + Q' \\ (\lambda P)' &= \lambda P' \\ (PQ)' &= P'Q + PQ' \\ (P^n)' &= nP^{n-1}P'\end{aligned}$$
3. *Si* $k \leqslant \deg P$, $\deg P^{(k)} = \deg P - k$. *Si* $k > \deg P$, $P^{(k)} = 0$.

Démonstration.

1. Trivial.
2. Les deux premières propriétés sont celles de l'homomorphisme, et la quatrième est une conséquence de la troisième.
   Par linéarité il suffit de montrer cette formule lorsque $P = X^n$ puisque :
$$\left[\left(\sum_n a_n X^n\right) Q\right]' = \left(\sum_n a_n X^n Q\right)' = \sum_n a_n (X^n Q)'$$
   Pour montrer que $(X^n Q)' = (X^n)'Q + X^n Q$, il suffit de nouveau par linéarité de l'établir pour $Q = X^p$. Or :
$$\begin{aligned}(X^n X^p)' = \left(X^{n+p}\right)' &= (n+p)X^{n+p-1} \\ (X^n)'X^p + X^n(X^p)' &= nX^{n-1}X^p + X^n pX^{p-1} \\ &= nX^{n+p-1} + pX^{n+p-1} \\ &= (n+p)X^{n+p-1} \\ &= (X^n X^p)'\end{aligned}$$
3. Si $\deg P \leqslant 0$ alors $P' = 0$. Si $\deg P > 0$ alors $\deg P' = \deg P - 1$. Le reste suit par récurrence.

□

Théorème 5.16 (Formule de Taylor)**.** *Soit* $P \in K[X]$, $a \in K$. *Alors on a*
$$P = \sum_{k=0}^{\infty} \frac{\widetilde{P^{(k)}}(a)}{k!}(X-a)^k$$
ou encore :
$$P(X+a) = \sum_{k=0}^{\infty} \frac{\widetilde{P^{(k)}}(a)}{k!}X^k$$

Démonstration. Les polynômes $1, (X-a)(X-a)^2, \ldots, (X-a)^k, \ldots$, étant de degrés échelonnés, forment une base de $K[X]$. P se décompose donc par rapport à cette base de façon unique.

$$P = \sum_{k=0}^{\infty} \lambda_k (X-a)^k$$

d'où :

$$P' = \sum_{k=0}^{\infty} k\lambda_k (X-a)^{k-1}$$

Par récurrence, on obtient :

$$P^{(j)} = \sum_{k=j}^{\infty} k(k-1)\ldots(k-j+1)\lambda_k (X-a)^{k-j}$$

En prenant la valeur en a pour $\widetilde{P^{(j)}}$, seul le terme correspondant à $k = j$ subsiste : il vaut $j!\lambda_j$ d'où

$$\lambda_j = \frac{\widetilde{P^{(j)}}(a)}{j!}$$

□

Théorème 5.17. *Si $P \in K[X]$ et a une racine de P dans K, alors a est d'ordre de multiplicité k si et seulement si pour tout $i < k$, $\widetilde{P^{(i)}}(a) = 0$ et $\widetilde{P^{(k)}}(a) \neq 0$.*

Démonstration. D'après Taylor :

$$\begin{aligned} P &= \sum_{i=0}^{k-1} \frac{\widetilde{P^{(i)}}(a)}{i!}(X-a)^i + (X-a)^k \sum_{i=k}^{\infty} \frac{\widetilde{P^{(i)}}(a)}{i!}(X-a)^{i-k} \\ &= R + (X-a)^k Q \end{aligned}$$

Donc par unicité dans la division euclidienne, Q est le quotient et R le reste dans la division euclidienne de P par $(X-a)^k$. Donc

$$Q(a) = \frac{\widetilde{P^{(k)}}(a)}{k!}$$

P est divisible par $(X-a)^k$ si et seulement si $R = 0$ et n'est pas divisible par $(X-a)^{k+1}$ si et seulement si $Q(a) \neq 0$. Or $R = 0$ s'écrit $\forall i < k$, $\frac{\widetilde{P^{(i)}}(a)}{i!} = 0$. D'où le résultat. □

5.6 Factorisation d'un polynôme

Théorème 5.18. *Tout polynôme* P *de* $\mathbb{C}[X]$ *de degré* $n > 0$ *peut se mettre de façon unique sous la forme*

$$P(x) = a_0 \left(X - x_1\right)^{\alpha_1} \dots \left(X - x_p\right)^{\alpha_p}$$

avec $a_0 \in \mathbb{C}$, $x_1, \dots, x_p \in \mathbb{C}$, $\alpha_1, \dots, \alpha_p \in \mathbb{N}^*$, *les* $(x_i)_{i \in \mathbb{N}_p^*}$ *étant tous distincts et* $\sum_{i=1}^{p} \alpha_i = n$.

Démonstration. L'existence d'une telle décomposition vient du théorème 5.14. Reste à prouver son unicité. Procédons par récurrence sur n, le degré de P. Si $n = 1$, c'est trivial. Supposons le résultat établi pour tous les polynômes jusqu'au degré $(n-1)$. Soit P un polynôme de degré n. Supposons que

$$P = a_0 \left(X - x_1\right)^{\alpha_1} \dots \left(X - x_p\right)^{\alpha_p} = a_0 \left(X - x_1'\right)^{\alpha_1'} \dots \left(X - x_q'\right)^{\alpha_q'}$$

Le a_0 est le même dans les deux écritures car c'est le coefficient du terme en X^n et d'après l'unicité de l'écriture d'un polynôme dans la base $1, X, \dots, X^p$, c'est le même de chaque côté de l'égalité. Alors $\widetilde{P}(x_1) = 0$. Donc la seconde écriture s'annule. Donc x_1 est l'un des x_i'. On peut donc simplifier les deux membres par $(X - x_1)$. On obtient alors une égalité entre deux polynômes de degrés $(n-1)$ auxquels on applique l'hypothèse de récurrence. Il en découle l'unicité de l'écriture pour P sous cette forme. □

Théorème 5.19. *Soit* $P \in \mathbb{R}[X]$. $\forall z \in \mathbb{C}$, $\widetilde{P}(\overline{z}) = \overline{\widetilde{P}(z)}$.

Démonstration. Soit $P = a_0 + a_1 X + \dots + a_n X^n$ où $\forall i \in \mathbb{N}_n$, $a_i \in \mathbb{R}$.

$$\begin{aligned}
\widetilde{P}(z) &= a_0 + a_1 z + \dots + a_n z^n \\
\overline{\widetilde{P}(z)} &= \overline{a_0 + a_1 z + \dots + a_n z^n} = \overline{a_0} + \overline{a_1 z} + \dots + \overline{a_n z^n} \\
&= \overline{a_0} + \overline{a_1}\,\overline{z} + \dots + \overline{a_n}\,\overline{z^n} = a_0 + a_1 \overline{z} + \dots + a_n \overline{z^n} \\
&= \widetilde{P}(\overline{z})
\end{aligned}$$

□

Théorème 5.20. *Soit* $P \in \mathbb{R}[X]$. *Si* z *est une racine de* P *d'ordre* α *dans* $\mathbb{C}$, $\bar{z}$ *est une racine d'ordre* α *de* P *dans* $\mathbb{C}$.

Démonstration. Si z est une racine d'ordre α de P dans $\mathbb{C}$, d'après le théorème 5.17,

$$\widetilde{P}(z) = 0, \widetilde{P}'(z) = 0, \dots, \widetilde{P^{(\alpha-1)}}(z) = 0, \widetilde{P^{(\alpha)}}(z) \neq 0$$

Donc, d'après le théorème 5.19,

$$\widetilde{\mathrm{P}}(\bar{z}) = 0, \widetilde{\mathrm{P}'}(\bar{z}) = 0, \ldots, \widetilde{\mathrm{P}^{(\alpha-1)}}(\bar{z}) = 0, \widetilde{\mathrm{P}^{(\alpha)}}(\bar{z}) \neq 0$$

□

Théorème 5.21. *Tout polynôme* $\mathrm{P} \in \mathbb{R}[\mathrm{X}]$ *de degré* $n > 0$ *s'écrit d'une manière unique sous la forme :*

$$\mathrm{P} = a_0 \left(\mathrm{X} - x_1\right)^{\alpha_1} \ldots \left(\mathrm{X} - x_h\right)^{\alpha_h} \left(\mathrm{X}^2 + p_1\mathrm{X} + q_1\right)^{\beta_1} \ldots \left(\mathrm{X}^2 + p_k\mathrm{X} + q_k\right)^{\beta_k}$$

avec $\forall j \in \mathbb{N}_k^*$, $p_j^2 - 4q_j < 0$, $\alpha_1 + \cdots + \alpha_h + 2\beta_1 + \cdots + 2\beta_k = n$, *les* x_i *étant des réels tous distincts, les trinômes* $\mathrm{X}^2 + p_j\mathrm{X} + q_j$ *étant tous distincts et à coefficients réels.*

Démonstration. Décomposons P(X) dans $\mathbb{C}[\mathrm{X}]$: il y a des racines réelles que nous noterons $x_1, \ldots, x_h$ et si z est une racine complexe alors $\bar{z}$ est aussi une racine de P.

$$\mathrm{P}(\mathrm{X}) = a_0(\mathrm{X} - x_1)^{\alpha_1} \ldots (\mathrm{X} - x_h)^{\alpha_h}(\mathrm{X} - z_1)^{\beta_1}(\mathrm{X} - \bar{z_1})^{\beta_1} \ldots (\mathrm{X} - z_k)^{\beta_k}(\mathrm{X} - \bar{z_k})^{\beta_k}$$

$$\forall i \in \mathbb{N}_k^*, \quad (\mathrm{X} - z_i)(\mathrm{X} - \bar{z_i}) = \mathrm{X}^2 - (z + \bar{z_i})\mathrm{X} + z_i\bar{z_i}$$

Or $z_i + \bar{z_i} = 2\Re(z_i) \in \mathbb{R}$, et $z_i\bar{z_i} = \left|z_i\right|^2 \in \mathbb{R}$. On pose $p_i = -(z_i + \bar{z_i})$ et $q_i = \left|z_i\right|^2$ et $p_i^2 - 4q_i < 0$. L'unicité découle de l'unicité de la décomposition de P(X) dans $\mathbb{C}[\mathrm{X}]$. □

5.7 Relations entre coefficients et racines

Théorème 5.22. *Soit* $\mathrm{P} = \sum_{j=0}^{n} a_j\mathrm{X}^j = a_n \prod_{i=1}^{n}(\mathrm{X} - x_i)$ *un polynôme scindé sur un corps commutatif* K. $x_1, \ldots, x_n$ *représentent toutes les racines, chacune apparaissant un nombre de fois égal à son ordre de multiplicité. Si on pose :*

$$\begin{aligned}\sigma_k &= \sum_{i_1 < i_2 < \cdots < i_k} x_{i_1} x_{i_2} \ldots x_{i_k} \\ &= (-1)^k \frac{a_{n-k}}{a_n}\end{aligned}$$

En particulier : $\sigma_1 = -\frac{a_{n-1}}{a_n}$, $\sigma_2 = \frac{a_{n-2}}{a_n}$, …, $\sigma_n = \prod_{i=1}^{n} x_i = (-1)^n \frac{a_0}{a_n}$.

Démonstration.

$$a_0 + a_1 X + \cdots + a_n X^n = a_n (X - x_1)(X - x_2) \ldots (X - x_n)$$

On développe le second membre et on identifie

$$a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n = a_n \left(X^n + \frac{1}{a_n} \sum_{k=1}^{n} \left[(-1)^k \sum_{i_1 < i_2 < \cdots < i_k} x_{i_1} x_{i_2} \ldots x_{i_k} \right] X^{n-k} \right)$$

□

Définition 5.12. On appelle fonction polynômiale de n variables $x_1, \ldots, x_n$ toute application f de K^n dans K telle que $f(x_1, \ldots, x_n)$ s'exprime à partir de x_1, …, x_n par sommes, produits, et produits par des éléments de K.

Une fonction rationnelle est un quotient de fonctions polynômiales. Une telle fonction n'est pas forcément définie sur tout K^n.

Une fonction rationnelle est dite symétrique si :

$$\forall \sigma \in S_n \quad f(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$$

Théorème 5.23. *1. Toute fonction rationnelle symétrique est le quotient de deux fonctions polynômiales symétriques.*

2. Toute fonction rationnelle symétrique de n variables $x_1, \ldots, x_n$ s'exprime rationnellement en fonction des expressions $\sigma_1, \ldots, \sigma_n$.

Démonstration. Hors programme. □

Chapitre 6

Fractions rationnelles

Voir polycopié distribué en cours.

6.3 Corps des fractions rationnelles

Théorème 6.3.

1. *Soient* K *un corps commutatif,* $E = K[X] \times K[X]^*$ *où* $K[X]^* = K[X] \setminus \{0\}$. *La relation binaire définie sur* E *par*

$$(P(X), Q(X))R(P_1(X), Q_1(X)) \iff P(X)Q_1(X) = P_1(X)Q(X)$$

est une relation d'équivalence sur E. *On notera* $(P(X), Q(X))$ *la classe de l'élément* $(P(X), Q(X))$ *de* E. E/R *sera noté* $K(X)$.

2. *Muni des deux lois suivantes :*

$$\overline{(P(X), Q(X))} + \overline{(P_1(X), Q_1(X))} = \overline{(P(X)Q_1(X) + P_1(X)Q(X), Q(X)Q_1(X))}$$
$$\overline{(P(X), Q(X))} \cdot \overline{(P_1(X), Q_1(X))} = \overline{(P(X)P_1(X), Q(X)Q_1(X))}$$

$K(X)$ *est un corps commutatif dont les éléments neutres sont* $\overline{(0, Q(X))}$ *et* $\overline{(1, 1)}$. *Le symétrique de* $\overline{(P(X), Q(X))}$ *pour* $+$ *est* $\overline{(-P(X), Q(X))}$, *et pour* $\cdot$ *est* $\overline{(Q(X), P(X))}$ *(*$P(X) \neq 0$*).*

3. *L'application* $\omega : K[X] \to K(X)$ *définie par* $P(X) \mapsto \overline{(P(X), 1)}$ *est un homomorphisme d'anneaux injectif et on a*

$$\begin{aligned}
\overline{(P(X), Q(X))} &= \overline{(P(X), 1)}\,\overline{(1, Q(X))} \\
&= \overline{(P(X), 1)}\,\overline{(Q(X), 1)}^{-1} \\
&= \omega\left(P(X)\omega(Q(X))\right)^{-1} \\
&= \frac{\omega(P(X))}{\omega(Q(X))}
\end{aligned}$$

On identifie alors $\omega(P(X))$ *et* $P(X)$ *en disant qu'on « plonge »* $K[X]$ *dans* $K(X)$ *et toute fraction rationnelle* $F(X)$ *s'écrit alors*

$$F(X) = \overline{(P(X), Q(X))} = \frac{P(X)}{Q(X)}$$

Démonstration. Trivial. □

Théorème 6.4. *Soit* $F \in K(X)$*,* $F \neq 0$*. Il existe un couple unique de polynômes* (P_1, Q_1) *tel que* $F = P_1(X)/Q_1(X)$ *avec* $\operatorname{pgcd}(P_1, Q_1) = 1$ *et* Q_1 *unitaire.*

Un tel couple est appelé représentant irréductible de F.

Démonstration. Soient $F = P/Q$, $D = \operatorname{pgcd}(P, Q)$ et λ le coefficient du terme de plus haut degré de Q. On a alors $P = \lambda D P_1$, $Q = \lambda D Q_1$, et $PQ_1 = QP_1$, d'où

$$\frac{P}{Q} = \frac{P_1}{Q_1}$$

avec $\operatorname{pgcd}(P_1, Q_1) = 1$ et Q_1 unitaire. Il reste à prouver l'unicité.

Supposons $F = P_1/Q_1 = P_2/Q_2$ alors $P_1Q_2 = P_2Q_1$. Comme Q_2 est premier avec P_2, il divise Q_1. Comme Q_1 est premier avec P_1, il divise Q_2. Donc Q_1 et Q_2 sont unitaires et associés, c'est à dire qu'ils ne différent que par multiplication d'une constante. Donc, étant associés et unitaires, ils sont égaux. D'où $Q_1 = Q_2$ et $P_1 = P_2$. □

Définition 6.2. Si $F \in K(X)$, $F = P/Q$, le degré de F est

$$\deg F = \deg P - \deg Q$$

En particulier $\deg 0 = -\infty$.

Théorème 6.5. *Soient* $F(X), G(X) \in K(X)$*. Alors*

1. $\deg(FG) = \deg F + \deg G$
2. $\deg(F + G) \leqslant \max(\deg F, \deg G)$

Démonstration.

1. Supposons $F = P/Q$ et $G = R/S$ alors

   $$\deg F = \deg P - \deg Q$$

   et

   $$\deg G = \deg R - \deg S$$

   $FG = PR/QS$ donc

   $$\begin{aligned} \deg FG &= \deg(PR) - \deg(QS) \\ &= \deg P + \deg R - \deg Q - \deg S \\ &= (\deg P - \deg Q) + (\deg R - \deg S) \end{aligned}$$

2. Considérons un représentant de F et un représentant de G ayant même dénominateur. $F = P/Q$ et $G = R/Q$. Alors $F + G = (P + R)/Q$ donc $\deg(F + G) = \deg(P + R) - \deg Q$. Or $\deg(P + R) \leqslant \max(\deg P, \deg R)$,

$$\begin{aligned}\deg(F + Q) &\leqslant \max(\deg P, \deg R) - \deg Q \\ &\leqslant \max(\deg P - \deg Q, \deg R - \deg Q) \\ &\leqslant \max(\deg F, \deg G)\end{aligned}$$

□

Remarque. Si $\deg F = 0$, cela ne signifie pas que F est une constante, c'est à dire un polynôme constant. Par exemple,

$$F = \frac{X^2 + 1}{X^2 - 1}$$

Définition 6.3. Soit $F = P/Q \in K(X)$, K étant de caractéristique nulle. On appelle fraction dérivée et on note

$$F' = D(F) = \frac{P'Q - PQ'}{Q^2}$$

Théorème 6.6. *Pour tous* F, G *dans* $K(X)$ *et* $\lambda \in K$ *on a :*

1. $(FG)' = F'G + FG'$
2. $(F + \lambda G)' = F' + \lambda G'$
3. $(1/F)' = -F'/F$ *pour* $F \neq 0$.

Démonstration. Supposons $F = P/Q$ et $G = R/S$. Alors :

1.

$$\begin{aligned}(FG)' &= \left(\frac{PR}{QS}\right)' \\ &= \frac{(PR)'QS - (QS)'PR}{(QS)^2} \\ &= \frac{(P'R + PR')QS - (Q'S + QS')PR}{(QS)^2} \\ &= \frac{P'RQS + PR'QS - Q'SPR - QS'PR}{(QS)^2} \\ &= \frac{(P'Q - Q'P)RS}{(QS)^2} + \frac{(R'S - RS')PQ}{(QS)^2} \\ &= \frac{P'Q - Q'P}{Q^2} \cdot \frac{R}{S} + \frac{R'S - RS'}{S^2} \cdot \frac{P}{Q} \\ &= F'G + FG'\end{aligned}$$

2.

$$\begin{aligned}
(F+\lambda G)' &= \left(\frac{P}{Q}+\lambda\frac{R}{S}\right)\\
&= \left(\frac{PS+\lambda RQ}{QS}\right)'\\
&= \frac{((PS)'+(\lambda RQ)')(QS)-(PS+\lambda RQ)(QS)'}{(QS)^2}\\
&= \frac{(P'S+PS'+\lambda(R'Q+RQ'))QS-(PS+\lambda RQ)(Q'S+QS')}{(QS^2)}\\
&= \frac{P'SQS+PS'QS+\lambda R'QQS+\lambda RQ'QS}{(QS)^2}\\
&\quad - \frac{PSQ'S+\lambda RQQ'S+PSQS'+\lambda RQQS'}{(QS)^2}\\
&= \frac{P'QSS-PQ'SS}{Q^2S^2}+\lambda\frac{R'SQQ-RS'QQ}{Q^2S^2}\\
&= \frac{P'Q-PQ'}{Q^2}+\lambda\frac{R'S-RS'}{S^2}\\
&= F'+\lambda G'
\end{aligned}$$

3.

$$\begin{aligned}
\left(\frac{1}{F}\right)' = \left(\frac{Q}{P}\right)' &= \frac{Q'P-P'Q}{P^2}\\
&= -\frac{P'Q-PQ'}{Q^2}\times\frac{Q^2}{P^2}\\
&= -F'\frac{1}{F^2}\\
&= -\frac{F'}{F^2}
\end{aligned}$$

□

Définition 6.4. Soit $F = P/Q \in K(X)$ avec $\text{pgcd}(P,Q) = 1$. On appelle zéro de F toute racine de P, et pôle de F toute racine de Q. L'ordre de multiplicité de cet élément (zéro ou pôle) est égal à l'ordre de la racine du polynôme qu'il annule.

Définition 6.5. Soit $F = P/Q \in K(X)$ sous forme irréductible. La fonction rationnelle $\widetilde{F}$ associée à F est l'application de K diminuée des pôles de F dans K

définie par

$$\widetilde{F}(x) = \frac{\widetilde{P}(x)}{\widetilde{Q}(x)}$$

Remarques.

1. Il faut prendre un représentant irréductible de F, car si x est un pôle de F il n'est pas dans l'ensemble de départ de $\widetilde{F}$. Si F n'est pas sous forme irréductible, il se peut qu'il y ait un « y » dans l'ensemble de départ qui annule le numérateur et les dénominateurs de F. La valeur en « y » ne serait pas définie, alors qu'elle l'est avec la fraction réduite.
2. Si L est une K-algèbre, on peut grâce à $\widetilde{P}_L/\widetilde{Q}_L$ définir des fonctions rationnelles sur L. On peut ainsi substituer des fractions rationnelles dans d'autres, ou en composer. On peut ainsi calculer $F(-X)$ ou $F(X^2)$.

Théorème 6.7. *Soient* F, G *deux éléments de* $K(X)$ *et* $\lambda \in K$*. Si* x *n'est ni pôle de* F*, ni pôle de* G*, on a*

$$\widetilde{(F + \lambda G)}(x) = \widetilde{F}(x) + \lambda \widetilde{G}(x)$$
$$\widetilde{(FG)}(x) = \widetilde{F}(x)\widetilde{G}(x)$$

Démonstration. Trivial. □

Définition 6.6. On dit qu'une fraction rationnelle $F \in K(X)$ est paire si $F(-X) = F(X)$. On dit qu'elle est impaire si $F(-X) = -F(X)$.

6.4 Décomposition en éléments simples

6.4.1 Théorèmes généraux

Théorème 6.8. *Pour toute fraction* $F \in K(X)$*, il existe un polynôme* E *et une fraction* G *unique tels que*

$$F = E + G$$

avec $\deg G < 0$*.*

Démonstration. Posons $F = P/Q$ et effectuons la division euclidienne de P par Q. On obtient $P = EQ + R$ avec $\deg R < \deg Q$. On en déduit

$$\frac{P}{Q} = E + \frac{R}{Q}$$

avec $\deg R/Q < 0$. On pose $R/Q = G$ et c'est terminé.

Montrons l'unicité : si $E + G = E_1 + G_1$, alors $E - E_1 = G_1 - G$ donc $\deg(E - E_1) \leqslant max(\deg G_1, \deg G) < 0$. Or le seul polynôme de degré négatif est le polynôme nul. Donc $E - E_1 = 0$, $E = E_1$ et $G - G_1 = 0$, d'où $G = G_1$. □

Théorème 6.9. *Soit* $B \in K[X]$ *et* $B = P_1 \dots P_q$ *une décomposition de* B *en produit de polynômes deux à deux étrangers (leurs seuls diviseurs communs sont des polynômes constants).*

Pour toute fraction A/B *de degré strictement négatif, il existe des polynômes* $A_1, \dots, A_q$ *uniques tels que*

$$\frac{A}{B} = \sum_{i=1}^{q} \frac{A_i}{P_i}$$

et $\forall i \in \mathbb{N}_q^*$, $\deg A_i < \deg P_i$.

Démonstration. Si $q = 1$, c'est déjà fait. Si $q = 2$, soient $k = \deg P_1$, $m = \deg P_2$ et $E = K_{k+m-1}[X]$. $\deg A/B < 0$, $A \in E$. Comme P_1, P_2 sont étrangers,

$$S = \{P_1, XP_1, \dots, X^{m-1}P_1, P_2, XP_2, \dots, X^{k-1}P_2\}$$

est un système libre d'éléments de E : s'il était lié, on aurait

$$\lambda_0 P_1 + \dots + \lambda_{m-1} X^{m-1} P_1 + \lambda_m P_2 + \lambda_{m+1} X P_2 + \dots + \lambda_{m+k-1} X^{k-1} P_2 = 0$$
$$\underbrace{(\lambda_0 + \lambda_1 X + \dots + \lambda_{m-1} X^{m-1})}_{U} P_1 = \underbrace{(-\lambda_m - \lambda_{m+1} X - \dots - \lambda_{m+k-1} X^{k-1})}_{V} P_2$$

avec $\deg U < \deg P_2$ et $\deg V < \deg P_1$, ce qui contredit le fait que P_1 et P_2 sont étrangers.

Or S contient $(m + k)$ polynômes, donc S est une base de E. A s'écrit donc d'une manière unique sous la forme d'une combinaison linéaire d'éléments de la base S :

$$A = \sum_{i=0}^{m-1} \alpha_i X^i P_1 + \sum_{j=0}^{k-1} \beta_j X^j P_2 = A_2 P_1 + A_1 P_2$$

avec $\deg A_2 < m$ et $\deg A_1 < k$. D'où

$$\frac{A}{B} = \frac{A}{P_1 P_2} = \frac{A_2 P_1 + A_1 P_2}{P_1 P_2} = \frac{A}{P_1} + \frac{A_2}{P_2}$$

Supposons le théorème vrai jusqu'au rang $(q - 1)$. Soit $B = P_1 \dots P_q$ alors $B = (P_1 \dots P_{q-1}) P_q$ et on est ramené au cas $q = 2$. □

Théorème 6.10. *Soit une fraction rationnelle* $F = A/P^\alpha$ *avec* $\deg F < 0$. *Il existe des polynômes* $Q_1, \dots, Q_\alpha$ *uniques tels que*

$$F = \frac{Q_1}{P} + \frac{Q_2}{P^2} + \dots + \frac{Q_\alpha}{P^\alpha}$$

où, $\forall i \mathbb{N}_\alpha^*$, $\deg Q_i < \deg P$.

Démonstration. Pour $\alpha = 1$ c'est déjà le cas. Supposons le résultat établi à l'ordre α, et soit $G = B/P^{\alpha+1}$ où $\deg B < (\alpha+1)\deg P$. Effectuons la division euclidienne de B par P :

$$B = AP + Q_{\alpha+1}$$

comme $\deg B < (\alpha+1)\deg P$, $\deg A < \alpha \deg P$ et l'hypothèse de récurrence s'applique à A/P^{α}. Or

$$\frac{B}{P^{\alpha+1}} = \frac{AP + Q_{\alpha+1}}{P^{\alpha+1}} = \frac{A}{P^{\alpha}} + \frac{Q_{\alpha+1}}{P^{\alpha+1}}$$

On a bien $\deg Q_{\alpha+1} < \deg P$. Ceci nous fournit donc un algorithme pour trouver successivement les Q_i. □

Théorème 6.11 (Décomposition en éléments simples)**.** *Soit* $F = N/D \in K(X)$*, où* $D = P_1^{\alpha_1} \dots P_q^{\alpha_q}$ *la factorisation de* D *sous forme de puissances de polynômes irréductibles. Il existe un unique polynôme* E *et une formule unique de polynômes* A_{ij}*, où* $i \in \mathbb{N}_q^*$ *et* $j \in \mathbb{N}_{\alpha_i}^*$ *tels que*

$$F = E + \sum_{i=1}^{q} \sum_{j=1}^{\alpha_i} \frac{A_{ij}}{P_i^j}$$

avec $\forall i \in \mathbb{N}_q^*$, $\forall j \in \mathbb{N}_{\alpha_i}^*$, $\deg A_{ij} < \deg P$.

Cette décomposition s'appelle « décomposition en éléments simples de F *sur* K *».*

Démonstration. Les polynômes $P_1^{\alpha_1} \dots P_q^{\alpha_q}$ étant deux à deux étrangers, les théorèmes 6.8 et 6.9 s'appliquent :

$$F = E + \sum_{i=1}^{q} \frac{A_i}{P_i^{\alpha_i}}$$

avec $\deg A_i < \deg P_i^{\alpha_i}$. On applique alors q fois le théorème 6.10 et on obtient la forme annoncée. □

6.4.2 Décomposition dans $\mathbb{C}(X)$

Théorème 6.12. *Soit* $F = N/D \in \mathbb{C}(X)$, $D = \prod_{i=1}^{q} (X - a_i)^{p_i}$ *(sur* $\mathbb{C}$*, les seuls polynômes irréductibles sont ceux du premier degré), les* a_i *étant deux à deux distincts. Il existe un unique polynôme* E *et une unique famille de complexes* A_{ij} *pour* $1 \leqslant i \leqslant q$, $1 \leqslant q \leqslant p_i$ *tels que*

$$F = E + \sum_{i=1}^{q} \sum_{j=1}^{p_i} \frac{A_{ij}}{(X - a_i)^j}$$

Démonstration. C'est la simple formulation du théorème 6.11 dans $\mathbb{C}(X)$. □

Remarques.

1. Ce théorème signifie entre autres que l'on obtient une base du $\mathbb{C}$-espace vectoriel $\mathbb{C}(X)$ en prenant les monômes X^k pour $k \in \mathbb{K}$ et les fractions $1/(X-a)^k$ pour $a \in \mathbb{C}$ et $k \in \mathbb{N}^*$.
2. E s'appelle la partie entière de F et s'obtient par division euclidienne de N par D. Pour calculer les A_{ij}, il y a la méthode générale ou les quelques astuces suivantes.

Calcul des coefficients par division. Considérons une fraction F ayant 0 pour pôle, d'ordre de multiplicité k.

$$F = \frac{N}{X^k Q} = \underbrace{\left(\frac{A_1}{X} + \frac{A_2}{X^2} + \cdots + \frac{A_k}{X^k}\right)}_{\text{partie polaire relative au pôle 0}} + \frac{N_1}{Q}$$

avec $Q(0) \neq 0$ et $N(0) \neq 0$. On obtient

$$N = (A_k + A_{k-1}X + \cdots + A_1 X^{k-1})Q + X^k N_1$$

On voit apparaître le résultat de la division suivant les puissances croissantes de N par Q, à l'ordre $(k-1)$.

Considérons une fraction F ayant α pour pôle, d'ordre de multiplicité k. On commence par effectuer une translation en posant $Y = X - \alpha$ et en calculant $F_1 = F(\alpha + Y)$, ce qui nous ramène au cas précédent. On effectue les calculs en Y, puis on reconvertit en X à la fin. On peut ainsi calculer séparément les différentes parties polaires, ou poursuivre les calculs sur la fraction N_1/Q.

En résumé : si $F \in \mathbb{C}(X)$ admettant un pôle α d'ordre k, on considère $F_1 = F(\alpha + Y) = N/Y^\alpha Q$. F_1 admet 0 pour pôle d'ordre k, la partie polaire de F au pôle α correspond à la partie polaire de F_1 au pôle 0. Les coefficients cherchés sont ceux du quotient de la division suivant les puissances croissantes de N par Q à l'ordre $(k-1)$.

Calcul des coefficients par dérivation. En général, on appelle résidu de F au pôle α, le coefficient placé au dessus de $(X-\alpha)$ dans la décomposition.

– Dans le cas d'un pôle simple :

$$F = \frac{N}{(X-\alpha)Q} = \frac{\lambda}{X-\alpha} + \frac{N_1}{Q}$$

avec $Q(\alpha) \neq 0$. λ est le résidu de F au pôle α. $N = \lambda Q + (X-\alpha)N_1$ d'où

$$\lambda = N(\alpha)/Q(\alpha)$$

Mais $D[(X-\alpha)Q] = (X-\alpha)Q' + Q$. Si on pose $P = (X-\alpha)Q$, $P'(\alpha) = Q(\alpha)$ et

$$\lambda = \frac{N(\alpha)}{P'(\alpha)}$$

– Dans le cas d'un pôle α d'ordre de multiplicité k :

$$F = \frac{N}{P} = \frac{N}{(X-\alpha)^k Q} = \frac{A_1}{X-\alpha} + \frac{A_2}{(X-\alpha)^2} + \cdots + \frac{A_k}{(X-\alpha)^k} + \frac{N_1}{Q}$$

avec $Q(\alpha) \neq 0$.

$$N = A_k Q + A_{k-1}(X-\alpha)Q + \cdots + A_1(X-\alpha)^{k-1}Q + (X-\alpha)^k N_1$$

D'où l'on déduit

$$A_k = \frac{N(\alpha)}{Q(\alpha)}$$

La formule de Taylor au point α pour $P = (X-\alpha)^k Q$ nous dit que $P^{(k)}(\alpha) = k!Q(\alpha)$ et

$$A_k = \frac{k!N(\alpha)}{P^{(k)}(\alpha)}$$

Calcul par la méthode des coefficients indéterminés. Le principe consiste à remplacer X par différentes valeurs dans F, puis à calculer les coefficients cherchés en résolvant le système d'équations linéaires obtenu. Il faut veiller à limiter le nombre et la complexité des équations. On a donc intérêt à limiter son usage à la fin des calculs.

Somme des résidus. Si $\deg F < -1$, la somme des résidus est nulle ; si $\deg F = -1$, la somme des résidus est la partie entière de XF, c'est à dire le quotient des coefficients dominants du numérateur et du dénominateur de F.

$$F = \sum_i \frac{A_{i_1}}{X - a_i} + H$$

avec $\deg H < -1$,

$$XF = \sum_i \frac{A_{i_1} X}{X - a_i} + XH = \sum_i A_{i_1} + G$$

avec $\deg G < 0$, $\sum_i A_{i_1}$ est donc la partie entière de XF.

Parité et imparité. Si F est paire, $F = N(X^2)/D(X^2)$. Donc si F admet le pôle a à l'ordre k, elle admet aussi le pôle $-a$ à l'ordre k.

$$F = \sum_{i=1}^{k} \frac{\lambda_i}{(X-a)^i} + \sum_{i=1}^{k} \frac{\mu_i}{(X+a)^i} + G$$

où G n'a ni a, ni $-a$ pour pôle. De plus, $F(-X) = F(X)$, donc par unicité de la décomposition, les décompositions de $F(-X)$ et de $F(X)$ coïncident.

$$F(-X) = \sum_{i=1}^{k} \frac{(-1)^i \lambda_i}{(X+a)^i} + \sum_{i=1}^{k} \frac{(-1)^i \mu_i}{(X-a)^i} + G(-X)$$

D'où, $\forall i \in \mathbb{N}_k^*$, $\mu_i = (-1)^i \lambda_i$. Si F admet le pôle 0, son ordre de multiplicité est nécessairement pair, et le raisonnement ci-dessus prouve que seuls les coefficients correspondants aux puissances paires ne sont pas nuls.

$$F = E(X^2) + \sum_i \frac{\alpha_i}{X^{2i}} + \sum_j \left(\sum_i \frac{\lambda_{ji}}{(X-a_j)^i} + \sum_i \frac{(-1)^i \lambda_{ji}}{(X+a_j)^i} \right)$$

Même genre de formule pour les fractions impaires.

6.4.3 Décomposition sur $\mathbb{R}(X)$

Dans $\mathbb{R}[X]$ les seuls polynômes irréductibles sont ceux du premier degré et ceux du second degré dont les discriminants sont strictement négatifs. Le théorème 6.11 s'écrit alors :

Théorème 6.13. *Soit* $F = N/D \in \mathbb{R}(X)$, $D = \prod_i (X-a_i)^{p_i} \prod_j (\lambda^2 + 2b_j X + c_j)^{q_j}$ *avec pour tout* j, $b_j^2 < c_j$. *Il existe un polynôme unique réel* E, *et une famille de réels uniques* A_{ik}, B_{jk}, C_{jk} *tels que*

$$F = E + \underbrace{\sum_i \sum_{k=1}^{p_i} \frac{A_{ik}}{(X-a_i)^k}}_{\text{éléments simples de première espèce}} + \underbrace{\sum_j \sum_{k=1}^{a_j} \frac{B_{jk}X + C_{jk}}{(X^2 + 2b_j X + c_j)^k}}_{\text{éléments simples de deuxième espèce}}$$

Remarque. Pour obtenir les éléments simples de première espèce, on procède comme dans $\mathbb{C}$. Ceux de seconde espèce peuvent être obtenus grâce aux théorèmes 6.9, 6.10 et 6.11, avec les mêmes méthodes que celles vues précédemment, mais avec quelques adaptations.

Somme des résidus. Dans un élément simple de la forme

$$\frac{BX+C}{X^2+2bX+c}$$

le coefficient de B doit être considéré comme résidu, car c'est la partie entière de la fraction

$$X\frac{BX+C}{X^2+2bX+c}$$

Valeur au pôle Si

$$F=\frac{N}{D}=\frac{N}{(X^2+2bX+c)^qQ}$$

soit r une racine complexe de $X^2+2bX+c$. Alors

$$F=\frac{B_qX+C_q}{(X^2+2bX+c)^q}+G$$

où G est le reste de la décomposition de F.

$$\frac{N}{Q}=B_qX+C_q+(X^2+2bX+c)^qG$$

et r est un zéro de $(X^2+2bX+c)^q)G$. D'où

$$B_qr+C_q=\frac{N(r)}{Q(r)}$$

Comme B_q et C_q sont des réels, ils sont calculables.

Parité. Si F est paire, sa décomposition doit refléter cette propriété : ainsi si on a un élément simple de la forme

$$\frac{BX+C}{(X^2+2bX+c)^q}$$

on aura aussi

$$\frac{-BX+C}{(X^2+2bX+c)^q}$$

En particulier, pour $b=0$ et $c>0$, l'élément simple

$$\frac{BX+C}{(X^2+c)^q}$$

vérifie nécessairement $B=0$.

Remarque. Soit $F \in \mathbb{R}(X)$ et α un pôle non réel de F considéré comme élément de $\mathbb{C}(X)$. $\bar{\alpha}$ est aussi pôle de F avec le même ordre de multiplicité, et l'unicité de la décomposition dans $\mathbb{C}$ montre qu'à l'élément simple

$$\frac{A}{(X-\alpha)^k}$$

correspond

$$\frac{\overline{A}}{(X-\overline{\alpha})^k}$$

Il est alors tentant de décomposer dans $\mathbb{C}(X)$, puis de regrouper les termes conjugués,

$$\frac{A}{X-\alpha}+\frac{\overline{A}}{X-\overline{\alpha}}=\frac{(A+\overline{A})X-\alpha\overline{A}-\overline{\alpha}A}{X^2-(\alpha+\overline{\alpha})X+\alpha\overline{\alpha}}$$

Mais ce n'est simple que pour les résidus et compliqué pour les autres.

$$\frac{A}{(X-\alpha)^k}+\frac{\overline{A}}{(X-\overline{\alpha})^k}=\frac{\overline{A}(X-\alpha)^k+A(X-\overline{\alpha})^k}{(X^2-(\alpha+\overline{\alpha})X+\alpha\overline{\alpha})^k}$$

qui n'est pas un élément de deuxième espèce. Sa décomposition s'obtient avec le théorème 6.10.

Index