Anneaux et arithmétique

Pierron Théo

ENS Ker Lann

Table des matières

Chapitre 1

Généralités sur les groupes

1.1 Groupes

Définition 1.1 Soit G un ensemble non vide. On dit que G est un groupe pour la loi $*$ ssi il existe $* : G^2 \to G$ que l'on appelle loi de composition interne qui vérifie :

- $\forall x, y, z \in G^3$, $x * (y * z) = (x * y) * z = x * y * z$.
- $\exists e \in G, \forall x \in G$, $e * x = x * e = x$.
- $\forall x \in G, \exists x^{-1} \in G$, $x * x^{-1} = x^{-1} * x = e$.

Remarque 1.1

- *e est unique (sinon $e = e * e' = e'$)*
- *x^{-1} est unique (sinon, $(x^{-1})' = (x^{-1})' * e = (x^{-1})' * (x * x^{-1}) = ((x^{-1})' * x) * x^{-1} = x^{-1}$).*

Définition 1.2 Si $(G, *)$ est un groupe.

On dit que G est l'ensemble sous-jacent à $(G, *)$ et que $*$ munit G d'une structure de groupe.

G est dit abélien ssi $\forall x, y \in G^2$, $x * y = y * x$.

Exemples :

- $(\mathbb{Z}, +)$
- $(\mathbb{N}, +)$ n'en est pas un.
- $\{e\}$ est un groupe abélien.
- $(\mathbb{Z}/n\mathbb{Z})$ est un groupe abélien.
- Pour $\mathbb{K} \in \{\mathbb{C}, \mathbb{R}, \mathbb{Q}\}$, $(\mathbb{K}^*, \times)$ est un groupe abélien.
- $(\mathfrak{M}_n(\mathbb{K}), +)$ est un groupe abélien.
- $(GL_n(\mathbb{K}), \times)$ est un groupe non abélien.
- $(\mathfrak{S}_n, \circ)$ est un groupe.

1.2 Sous-groupes

Définition 1.3 Soit $(G, *)$ un groupe et $H \subset G$ un sous-ensemble non vide de G. H est un sous-groupe de $(G, *)$ ssi la restriction de $*$ à H induit une loi de composition interne sur H.

Remarque 1.2

- *Un sous-groupe $(H, *)$ de $(G, *)$ est un groupe.*
- *Si G est abélien, H aussi.*

Exemples :

- $(\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{Q}, +)$ qui est un sous-groupe de $(\mathbb{R}, +)$.
- G et $\{e_G\}$ sont des sous-groupes de G.
- $(\{z \in \mathbb{C}, z^n = 1\}, \times)$ est un sous-groupe de $(\mathbb{C}^*, \times)$.
- $n\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$.
- $\{M \in GL_n(\mathbb{C}), \det(M) = \pm 1\}$ est un sous-groupe de $(GL_n(\mathbb{C}), \cdot)$.

Proposition 1.1 Soit $(G, *)$ un groupe et $\varnothing \neq H \subset G$.
H est un sous-groupe de G ssi $\forall x, y \in H^2, x * y^{-1} \in H$.

Démonstration.

- $\Rightarrow$ Supposons H sous-groupe de G. Soit $(x, y) \in H^2$. y^{-1} est dans H et $*$ est interne donc $x * y^{-1} \in H$.
- $\Leftarrow$ Pour tout $x \in H$, $xx^{-1} \in H$ donc H admet un neutre e_G.
  On a de plus $(e_G, x) \in H^2$ donc $x^{-1} \in H$.
  Enfin, $(x, y^{-1}) \in H^2$ donc $xy \in H$.
  Donc H est un sous groupe de G. ∎

THÉORÈME 1.1 *Les sous-groupes de $(\mathbb{Z}, +)$ sont les $n\mathbb{Z}$, $n \in \mathbb{N}$.*

Démonstration.

- Les $n\mathbb{Z}$ sont clairement des sous-groupes de $\mathbb{Z}$.
- Soit H un sous-groupe de $\mathbb{Z}$. Si $H = \{0\}$, alors $H = 0\mathbb{Z}$.
  Sinon, $H \setminus \{0\} \neq \varnothing$ donc il existe $n \neq 0 \in H$.
  H est un groupe donc $|n| \in H$ donc on peut supposer $n \geqslant 0$. On pose ensuite $n_0 = \min\{n \in H, n > 0\}$.
  Tout élément de $n_0\mathbb{Z}$ est dans H.
  Réciproquement, si $x \in H$, $x = n_0 q + r$ avec $r < n_0$.
  On a alors $r \in H$ donc $r = 0$ donc $x \in n_0\mathbb{Z}$.
  Donc $H = n_0\mathbb{Z}$. ∎

1.3 Morphismes de groupes

Définition 1.4 Soient $(G, *)$ et $(G', *')$ deux groupes. On appelle morphisme de groupes toute application $f : G \to G'$ telle que $\forall x, y \in G \times G'$, $f(x * y) = f(x) *' f(y)$.

Si $(G', *') = (G, *)$, f est un endomorphisme de groupes.

Si f est bijective, c'est un isomorphisme de groupe.

Si f est bijective et $(G, *) = (G', *')$, f est un automorphisme de groupes.

Remarque 1.3 Soit $f : G \to G'$ un morphisme de groupes. On a $f(e_G) = e_{G'}$ et pour tout $x \in G$, $f(x^{-1}) = f(x)^{-1}$.

Exemples :

- Pour tout $k \in \mathbb{N}$, l'application :

$$f_k : \begin{cases} \mathbb{Z} & \to & \mathbb{Z} \\ x & \mapsto & kx \end{cases}$$

  est un morphisme injectif de $(\mathbb{Z}, +)$ dans lui-même.
- det : $GL_n(\mathbb{R}) \to \mathbb{R}^*$ est un morphisme de groupes de $(GL_n(\mathbb{R}), \times)$ dans $(\mathbb{R}^*, \times)$.
  Ce morphisme est surjectif et non injectif.
- $e^{i\cdot}$ est un morphisme de $(\mathbb{R}, +)$ dans $(\mathbb{C}^*, \times)$ ni surjectif ni injectif.

Proposition 1.2 Soient G, G' et G'' trois groupes, $f : G \to G'$ et $g : G' \to G''$ deux morphismes de groupes.

- $g \circ f$ est un morphisme de groupes.
- Si f est un isomorphisme, f^{-1} aussi.
- L'image directe par f d'un sous-groupe de G est un sous-groupe de G'.
- L'image réciproque par f d'un sous-groupe de G' est un sous-groupe de G.

Démonstration.

- Clair
- Considérer $f \circ f^{-1}$ et conclure par injectivité de f.
- Il suffit de dérouler les définitions. ∎

Définition 1.5 Soit $(G, *)$ et $(G', *')$ deux groupes, $f : G \to G'$ un morphisme de groupes.

On appelle noyau de f et on note $\mathrm{Ker}(f)$ le sous-groupe de $(G, *)$ défini comme $f^{-1}(\{e_{G'}\})$.

On appelle image de f et on note $\mathrm{Im}(f)$ le sous-groupe $f(G)$ de $(G', *')$.

THÉORÈME 1.2 *Avec les notations précédentes, f est injective ssi* $\mathrm{Ker}(f) = \{e_G\}$ *et f est surjective ssi* $\mathrm{Im}(f) = G'$.

Démonstration.

$$\begin{aligned}
&\forall x, x' \in G^2, (f(x) = f(x')) \Rightarrow (x = x') \\
\text{ssi}\quad &\forall x, x' \in G^2, (f(x * x'^{-1}) = e_{G'} \Rightarrow x * x'^{-1} = e_G) \\
\text{ssi}\quad &\forall x, x' \in G^2, (x * x'^{-1} \in \mathrm{Ker}(f) \Rightarrow x * x'^{-1} = e_G) \\
\text{ssi}\quad &\forall z \in G, (z \in \mathrm{Ker}(f) \Rightarrow z = e_G) \\
\text{ssi}\quad &\mathrm{Ker}(f) = \{e_G\}
\end{aligned}$$

THÉORÈME 1.3 (FACTORISATION DES MORPHISMES DE GROUPES) *Soient G, G' et G'' trois groupes et $f : G \to G'$ et $g : G \to G''$ deux morphismes de groupes.*

$$\begin{aligned}
\mathrm{Ker}(f) \subset \mathrm{Ker}(g) \quad &\text{ssi} \quad \forall x, y \in G^2, f(x) = f(y) \Rightarrow g(x) = g(y) \\
&\text{ssi} \quad \exists! \textit{ morphisme } h : \mathrm{Im}(f) \to \mathrm{Im}(g) \textit{ surjectif }, g = h \circ f
\end{aligned}$$

Démonstration.

$1 \Rightarrow 2$ Soient $x, y \in G^2$ tel que $f(x) = f(y)$.
$f(x * y^{-1}) = e_{G'}$ donc $x * y^{-1} \in \mathrm{Ker}(f) \subset \mathrm{Ker}(g)$ donc $g(x) = g(y)$.

$2 \Rightarrow 1$ Soit $x \in \mathrm{Ker}(f)$.
$f(x) = e_{G'} = f(e_G)$ donc $g(x) = g(e_G) = e_{G''}$ donc $x \in \mathrm{Ker}(g)$.

$3 \Rightarrow 2$ Soit $(x, y) \in G^2$ tel que $f(x) = f(y)$.
On a $g(x) = h(f(x)) = h(f(y)) = g(y)$.

$2 \Rightarrow 3$ Soit $y \in \mathrm{Im}(f)$. Il existe $x \in G$ tel que $y = f(x)$. On pose alors $h(y) = g(x)$.
A priori, h dépend du choix de x mais (2) nous montre l'indépendance de h vis à vis de ce choix. h est donc bien définie.
Par construction h vérifie $g = h \circ f$ et l'unicité est induite. h est de plus bien un morphisme de groupes (définitions...) ■

COROLLAIRE 1.1 $\mathrm{Ker}(f) = \mathrm{Ker}(g)$ *ssi il existe un unique isomorphisme de groupes $h :$* $\mathrm{Im}(f) \to \mathrm{Im}(g)$ *tel que $g = h \circ f$.*

Démonstration.

$\Leftarrow$ Clair

$\Rightarrow$ On a déjà un morphisme surjectif h vérifiant $h \circ f = g$. Reste à montrer qu'il est injectif.
Soit $y \in \mathrm{Im}(f)$.
$h(y) = e_G \quad \text{ssi} \quad \exists x \in G, y = f(x), h(f(x)) = g(x) = e_{G''}$
Donc $x \in \mathrm{Ker}(g) \subset \mathrm{Ker}(f)$ donc $y = f(x) = e_{G'}$.
Donc h est un isomorphisme de groupes. ■

COROLLAIRE 1.2 *Si f est surjective,* $\mathrm{Ker}(f) \subset \mathrm{Ker}(g)$ *ssi il existe un unique morphisme $h : G' \to G''$ tel que $g = h \circ f$.*

Démonstration.

$\Rightarrow$ On a un unique morphisme surjectif $h : \mathrm{Im}(f) \to \mathrm{Im}(g)$ qui marche. $\mathrm{Im}(f) = G'$ donc h induit $h' : G' \to G''$ et $h' \circ f = g$.

$\Leftarrow$ S'il existe $h : G' \to G''$ tel que $h \circ f = g$, h prend ses valeurs dans $\mathrm{Im}(g)$. h se factorise alors en $h' : \mathrm{Im}(f) \to \mathrm{Im}(g)$ et devient surjectif. Le théorème précédent assure $\mathrm{Ker}(f) \subset \mathrm{Ker}(g)$. ■

Remarque 1.4 Si on suppose f et g surjectifs, alors $h : G' \to G''$ l'est aussi.

THÉORÈME 1.4 (PRODUIT DIRECT DE GROUPES) *Soient G_1 et G_2 des groupes (resp. groupes abéliens). La loi :*

$$* : \begin{cases} (G_1 \times G_2)^2 & \to & G_1 \times G_2 \\ (x_1, x_2), (y_1, y_2) & \mapsto & (x_1 *_1 y_1, x_2 *_2 y_2) \end{cases}$$

fait de $G_1 \times G_2$ un groupe (resp. groupe abélien). Les applications :

$$p_1 : \begin{cases} G_1 \times G_2 & \to & G_1 \\ (x, y) & \mapsto & x \end{cases}$$

et

$$p_2 : \begin{cases} G_1 \times G_2 & \to & G_2 \\ (x, y) & \mapsto & y \end{cases}$$

sont des morphismes de groupes.

Démonstration. La démonstration se fait coordonnée par coordonnée. ■

Remarque 1.5 Il est donc possible de construire récursivement une structure de groupe sur un produit cartésien de $(G_1, \cdots, G_n)$.

Proposition 1.3 $(G_1 \times G_2, *)$ vérifie la propriété fondamentale : pour tout $(T, \cdot)$ groupe muni de deux morphismes $f_1 : T \to G_1$ et $f_2 : T \to G_2$, il existe un unique morphisme $f : T \to G_1 \times G_2$ tel que $f_i = p_i \circ f$.

Démonstration.

$$f : \begin{cases} T & \to & G_1 \times G_2 \\ x & \mapsto & (f_1(x), f_2(x)) \end{cases}$$

convient et c'est le seul. ■

Remarque 1.6 Une telle propriété définit $(G_1 \times G_2, *)$ à isomorphisme près.

Chapitre 2

Généralités sur les anneaux

2.1 Définitions et premières propriétés

2.1.1 Anneaux

Définition 2.1 Soit A un ensemble non vide. On dit que $(A, +, \times)$ est un anneau ssi :

- $+$ et $\times$ sont internes
- $(A, +)$ est un groupe abélien d'élément neutre noté 0
- $\times$ est associative et distributive par rapport à $+$

A est appelé ensemble sous-jacent à $(A, +, \times)$. $(A, +)$ est appelé groupe sous-jacent à $(A, +, \times)$.

Définition 2.2 (Définition équivalente) $A \neq \varnothing$ est un anneau ssi il existe deux lois de composition interne $+$ et $\times$ vérifiant :

- $\forall (x, y, z) \in A^3, (x + y) + z = x + (y + z) = x + y + z$
- $\exists 0 \in A, \forall x \in A, x + 0 = 0 + x = x$
- $\forall x \in A, \exists (-x) \in A, x + (-x) = (-x) + x = 0$
- $\forall (x, y) \in A^2, x + y = y + x$
- $\forall (x, y, z) \in A^3, (xy)z = x(yz) = xyz$
- $\forall (x, y, z) \in A^3, (x + y)z = xz + yz$ et $x(y + z) = xy + xz$

Proposition 2.1 Pour tout $x \in A$, $0x = x0 = 0$.

Démonstration. $0x = (0 + 0)x = 0x + 0x$ donc $0x = 0$. De même, $x0 = 0$. ∎

Exemples :

- $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$ sont des anneaux.
- $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau pour tout $n \in \mathbb{N}$.
- $(\mathfrak{M}_n(\mathbb{K}), +, \times)$ est un anneau avec $\mathbb{K} \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$.
- Si $(G, *)$ est un groupe abélien, $(\hom(G, G), *, \circ)$ est un anneau.

Définition 2.3 On dit que $(A, +, \times)$ est unitaire ssi il existe $x \neq y \in A^2$ et si $\times$ possède un neutre noté 1.

Définition 2.4 On dit que $(A, +, \times)$ est abélien si $\times$ est commutative.

Proposition 2.2 Si $(A, +, \times)$ est un anneau unitaire, alors, pour tout $x \in A$, $-x = (-1)x$.

Démonstration. $(-1)x + x = (-1)x + 1x = (-1+1)x = 0x = 0$. Par unicité de l'inverse, $-x = (-1)x$. ∎

Exemples :
- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/n\mathbb{Z}$, $\mathfrak{M}_p(\mathbb{K})$ et $\hom(G, G)$ sont unitaires pour $n \neq 1$.
- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ et $\mathbb{Z}/n\mathbb{Z}$ sont abéliens pour tout $n \in \mathbb{N}$.
- $(2\mathbb{Z}, +, \times)$ est un anneau commutatif non unitaire.
- $\{f \in \mathbb{R}^{\mathbb{R}}, \text{supp}(f) \text{ compact}\}$ [1] muni de $+$ et $\times$ est un anneau commutatif non unitaire.

2.1.2 Sous-anneaux

Définition 2.5 Soit $(A, +, \times)$ un anneau et $\varnothing \neq B \subset A$. B est un sous-anneau de A ssi :
- $(B, +)$ est un sous-groupe de $(A, +)$
- $\times|_B$ est interne

Définition 2.6 (Définition équivalente) B est un sous-anneau de A ssi pour tout $(x, y) \in B^2$, $x - y \in B$ et $xy \in B$.

Remarque 2.1 Si A est unitaire, on impose $1_A \in B$. B est alors unitaire, ce qui revient à dire que $(B, +|_B, \times|_B)$ est un anneau unitaire si A l'est.

Exemples :
- A et $\{0\}$ sont des sous-anneaux de A (si A est unitaire, $\{0\}$ n'en est plus un)
- Pour tout $n \neq 1$, $n\mathbb{Z}$ n'est pas un sous-anneau de $(\mathbb{Z}, +, \times)$.
- $\mathbb{Z}$ est un sous-anneau de $\mathbb{Q}$, $\mathbb{Q}$ est un sous-anneau de $\mathbb{R}$ et $\mathbb{R}$ est un sous-anneau de $\mathbb{C}$.

2.1.3 Morphismes d'anneaux

Définition 2.7 Soient $(A, +, \times)$ et $(B, +', \times')$ deux anneaux.

Une application $f : A \to B$ est un morphisme d'anneaux ssi f est un morphisme de groupes de $(A, +) \to (B, +')$ et pour tout $(a, b) \in A^2$, $f(a \times b) = f(a) \times' f(b)$.

1. $\text{supp}(f) = \{x, f(x) \neq 0\}$

Définition 2.8 (Définition équivalente) f est un morphisme d'anneaux ssi pour tout $(a,b) \in A^2$, $f(a+b) = f(a) +' f(b)$ et $f(a \times b) = f(a) \times' f(b)$.

Remarque 2.2 Si A et B sont unitaires, on impose aussi $f(1_A) = 1_B$ pour que f soit un morphisme d'anneaux unitaires.

Si f est bijective, on parle d'isomorphisme d'anneaux. Si $A = B$, on parle d'endomorphisme d'anneaux. Si f est un endomorphisme et un isomorphisme, on parle d'automorphisme.

Exemples :

- det n'est pas un morphisme d'anneaux.
- L'application :

$$f : \begin{cases} A & \to & \hom((A,+),(A,+)) \\ a & \mapsto & f_a : \begin{cases} (A,+) & \to & (A,+) \\ x & \mapsto & ax \end{cases} \end{cases}$$

est un morphisme d'anneaux.

Définition 2.9 Soient A et B deux anneaux et $f : A \to B$ un morphisme d'anneaux.

- On appelle image de f l'image directe de A par f :

$$\mathrm{Im}(f) = \{y \in B, \exists x \in A, y = f(x)\}$$

- On appelle noyau de f l'image réciproque de $\{0_B\}$ par f :

$$\mathrm{Ker}(f) = \{x \in A, f(x) = 0\}$$

Proposition 2.3

- f est surjective ssi $\mathrm{Im}(f) = B$.
- f est injective ssi $\mathrm{Ker}(f) = \{0_A\}$.

Proposition 2.4 Soient A, B et C trois anneaux (resp. anneaux unitaires), $f : A \to B$ et $g : B \to C$ des morphismes d'anneaux (resp. d'anneaux unitaires).

- $g \circ f$ est un morphisme d'anneaux (resp. d'anneaux unitaires)
- Si f est un isomorphisme d'anneaux (resp. d'anneaux unitaires), f^{-1} est un isomorphisme d'anneaux (resp. d'anneaux unitaires)
- $\mathrm{Im}(f)$ est un sous-anneau (resp. sous-anneau unitaire) de B.

Démonstration.

- Soit $(x,y) \in A^2$.
  $g(f(x+y)) = g(f(x) +' f(y)) = g(f(x)) +'' g(f(y))$ et $g(f(x \cdot y)) = g(f(x) \cdot' f(y)) = g(f(x)) \cdot'' g(f(y))$.
  $g(f(1_A)) = g(1_B) = 1_C$.

- $f(f^{-1}(x +' y)) = x +' y = f(f^{-1}(x)) + f(f^{-1}(y))$ et $f(f^{-1}(x \cdot' y)) = x +' y = f(f^{-1}(x)) \cdot f(f^{-1}(y))$. L'injectivité de f conclut.
  De plus $f^{-1}(1_B) = f^{-1}(f(1_A)) = 1_A$.
- $1_B = f(1_A)$ donc $1_B \in \mathrm{Im}(f)$. Si x', y' appartiennent à $\mathrm{Im}(f)$, $x' = f(x)$ et $y = f(y)$ donc $x' -' y' = f(x) -' f(y) = f(x - y)$ et $x' \cdot' y' = f(x) \cdot' f(y) = f(x \cdot y)$
  Donc $\mathrm{Im}(f)$ est un sous-anneau de B. ■

Théorème 2.1 (Factorisation des morphismes d'anneaux) *Soient A, B et C trois anneaux (resp. anneaux unitaires) et $f : A \to B$ et $g : A \to C$ deux morphismes d'anneaux (resp. d'anneaux unitaires).*

$$\begin{aligned} \mathrm{Ker}(f) \subset \mathrm{Ker}(g) \quad &\text{ssi} \quad \forall x, y \in A^2, f(x) = f(y) \Rightarrow g(x) = g(y) \\ &\text{ssi} \quad \exists! \textit{ morphisme d'anneaux (resp. d'anneaux unitaires)} \\ &\quad h : \mathrm{Im}(f) \to \mathrm{Im}(g) \textit{ surjectif}, g = h \circ f \end{aligned}$$

Démonstration.

$1 \Rightarrow 2$ Soient $x, y \in A^2$ tel que $f(x) = f(y)$.
$f(x - y) = 0$ donc $x - y \in \mathrm{Ker}(f) \subset \mathrm{Ker}(g)$ donc $g(x) = g(y)$.

$2 \Rightarrow 1$ Soit $x \in \mathrm{Ker}(f)$.
$f(x) = 0 = f(0)$ donc $g(x) = g(0) = 0$ donc $x \in \mathrm{Ker}(g)$.

$3 \Rightarrow 2$ Soit $(x, y) \in A^2$ tel que $f(x) = f(y)$.
On a $g(x) = h(f(x)) = h(f(y)) = g(y)$.

$2 \Rightarrow 3$ Soit $y \in \mathrm{Im}(f)$. Il existe $x \in A$ tel que $y = f(x)$. On pose alors $h(y) = g(x)$.
A priori, h dépend du choix de x mais (2) nous montre l'indépendance de h vis à vis de ce choix. h est donc bien définie.
Par construction h vérifie $g = h \circ f$ et l'unicité est induite. h est de plus bien un morphisme d'anneaux (resp. d'anneaux unitaires) (définitions...) surjectif car l'ensemble d'arrivée est $\mathrm{Im}(g)$. ■

Corollaire 2.1 *Soient A, B et C trois anneaux (resp. anneaux unitaires) et $f : A \to B$ et $g : A \to C$ deux morphismes d'anneaux (resp. d'anneaux unitaires).*

- $\mathrm{Ker}(f) = \mathrm{Ker}(g)$ *ssi il existe un unique isomorphisme d'anneaux (resp. d'anneaux unitaires) $h : \mathrm{Im}(f) \to \mathrm{Im}(g)$ tel que $g = h \circ f$.*
- *Si f est surjectif,* $\mathrm{Ker}(f) \subset \mathrm{Ker}(g)$ *ssi il existe un unique morphisme d'anneaux (resp. d'anneaux unitaires) $h : B \to C$ tel que $g = h \circ f$.*
- *Si f et g surjectifs,* $\mathrm{Ker}(f) \subset \mathrm{Ker}(g)$ *ssi il existe un unique morphisme d'anneaux (resp. d'anneaux unitaires) surjectif $h : B \to C$ tel que $g = h \circ f$.*

- *Si f et g surjectifs,* $\mathrm{Ker}(f) = \mathrm{Ker}(g)$ *ssi il existe un unique isomorphisme d'anneaux (resp. d'anneaux unitaires) surjectif $h : B \to C$ tel que $g = h \circ f$.*

THÉORÈME 2.2 *Soient A_1 et A_2 deux anneaux (resp. anneaux unitaires). Les lois :*

$$+ : \begin{cases} (A_1 \times A_2)^2 & \to & A_1 \times A_2 \\ (x_1, x_2), (y_1, y_2) & \mapsto & (x_1 +_1 y_1, x_2 +_2 y_2) \end{cases}$$

$$\times : \begin{cases} (A_1 \times A_2)^2 & \to & A_1 \times A_2 \\ (x_1, x_2), (y_1, y_2) & \mapsto & (x_1 \times_1 y_1, x_2 \times_2 y_2) \end{cases}$$

font de $(A_1 \times A_2, +, *)$ un anneau (resp. anneau unitaire).

Les applications :

$$p_1 : \begin{cases} A_1 \times A_2 & \to & A_1 \\ (x, y) & \mapsto & x \end{cases}$$

$$p_2 : \begin{cases} A_1 \times A_2 & \to & A_2 \\ (x, y) & \mapsto & y \end{cases}$$

sont des morphismes d'anneaux (resp. d'anneaux unitaires).

Si A_1 et A_2 sont commutatifs, $A_1 \times A_2$ l'est aussi.

Démonstration. La preuve se fait coordonnée par coordonnée. ∎

Remarque 2.3 On peut alors munir récursivement $\prod_{i=1}^{n} A_i$ d'une structure d'anneau.

Proposition 2.5 $A_1 \times A_2$ vérifie aussi la ropriété fondamentale : pour tout $(T, +, \cdot)$ groupe muni de deux morphismes $f_1 : T \to A_1$ et $f_2 : T \to A_2$, il existe un unique morphisme $f : T \to A_1 \times A_2$ tel que $f_i = p_i \circ f$.

2.2 Éléments remarquables d'un anneau

Définition 2.10 Soit A un anneau. On dit que $a \in A$ est :

- diviseur de 0 ssi $\exists b \in A \setminus \{0\}$ tel que $ba = 0$ ou $ab = 0$.
- régulier à gauche (resp. à droite) ssi $\forall b, c \in A^2$, $ba = ca \Rightarrow b = c$ (resp. $ab = ac \Rightarrow b = c$)
- régulier ssi a est régulier à gauche et à droite
- idempotent ssi $a^2 = a$.
- nilpotent ssi il existe $p \in \mathbb{N}$, $a^p = 0$.

- Si A est unitaire, a est dit inversible ssi il existe $b \in A$, $ab = ba = 1$. On note $A^\times$ l'ensemble des inversibles de A.
- Si A est unitaire et commutatif, irréductible ssi $a \notin A^\times$ et $a \neq 0$ ssi $\forall b, c \in A^2$, $a = bc \Rightarrow a = b$ ou $a = c$.

Remarque 2.4

- *Si $A \neq \{0\}$, 0 n'est pas régulier.*
- *Un élément diviseur de 0 n'est pas régulier. En effet, si a est diviseur de 0, il existe $b \neq 0$ tel que $ab = 0$ ou $ba = 0$.*
  On a donc $ab = a0$ et $b \neq 0$. Donc a n'est pas régulier.
- *Un élément irréductible n'est jamais inversible ou nul.*

THÉORÈME 2.3 *Soit A un anneau et $a \in A$.*
a est régulier ssi a n'est pas diviseur de 0.

Démonstration.

$\Rightarrow$ La remarque précédente assure le résultat.

$\Leftarrow$ Supposons que a n'est pas un diviseur de 0.
Soient $b, c \in A^2$ tels que $ab = ac$ et $ba = ca$.
On a $a(b-c) = 0 = (b-c)a$. Or a n'est pas diviseur de 0 donc $b-c = 0$ et $b = c$. ∎

Exemples :

- Soit $n \geqslant 2$ non premier. Il existe $(n_1, n_2) \in [\![1, n-1]\!]$ tel que $n = n_1 n_2$. Dans $\mathbb{Z}/n\mathbb{Z}$, cette égalité donnc $\overline{n_1 n_2} = \overline{0}$ avec $\overline{n_1} \neq \overline{0} \neq \overline{n_2}$.
  $\overline{n_1}$ et $\overline{n_2}$ sont donc diviseurs de 0.
- Dans $(\mathfrak{M}_n(\mathbb{R}), +, \times)$, $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ et $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ sont diviseurs de 0.
- Soient $(G_1, +)$ et $(G_2, +)$ deux groupes abéliens. On considère :

$$\pi_1 : \begin{cases} G_1 \times G_2 & \to & G_1 \times G_2 \\ (x, y) & \mapsto & (x, 0) \end{cases}$$

et

$$\pi_2 : \begin{cases} G_1 \times G_2 & \to & G_1 \times G_2 \\ (x, y) & \mapsto & (0, y) \end{cases}$$

Dans $(\hom(G_1 \times G_2), +, \circ)$, les éléments π_i sont diviseurs de 0.

Définition 2.11 (Intégrité) Soit $(A, +, \times)$ un anneau ($\neq \{0\}$). On dit que A est intègre ssi tout $x \neq 0 \in A$ est régulier dans A.

Autrement dit, A est un anneau intègre ssi A ne contient pas de diviseurs de zéro non triviaux ssi $\forall (a, b) \in A^2$, $ab = 0 \Rightarrow a = 0$ ou $b = 0$.

2.3 Idéaux d'un anneau

Définition 2.12 (Idéal) Soit $(A, +, \times)$ un anneau et I un sous-groupe de $(A, +)$.

On dit que I est un idéal à droite (resp. à gauche) de A ssi pour tout $(a, b) \in A \times I$, $ba \in I$ (resp. $ab \in I$).

I est un idéal bilatère (ou idéal) ssi c'est un idéal à gauche et à droite.

Remarque 2.5 Si A est commutatif, les notions d'idéal à gauche, d'idéal à droite et d'idéal bilatère coïncident.

Exemples :

- A et $\{0\}$ sont des idéaux de A.
- Soit $n \in \mathbb{N} \setminus \{0, 1\}$. $n\mathbb{Z}$ est un idéal de $\mathbb{Z}$.
- $I = \left\{ \begin{pmatrix} 0 & 0 \\ p & q \end{pmatrix}, (p, q) \in \mathbb{R}^2 \right\}$ est un idéal à droite de $\mathfrak{M}_2(\mathbb{R})$.
- $I = \left\{ \begin{pmatrix} 0 & p \\ 0 & q \end{pmatrix}, (p, q) \in \mathbb{R}^2 \right\}$ est un idéal à gauche de $\mathfrak{M}_2(\mathbb{R})$.
- $aA = \{ab, b \in A\}$ est un idéal à droite de A et $Aa = \{ba, b \in A\}$ est un idéal à gauche de A. Si A est commutatif, on note $\langle A \rangle = aA = Aa$ l'idéal monogène de A engendré par A.

Proposition 2.6 Soient A et B deux anneaux, $f : A \to B$ un morphisme d'anneaux.

- Si $(I_j)_{j \in J}$ est une famille d'idéaux à droite (resp. à gauche, bilatères) de A, alors $\bigcap_{j \in J} I_j$ est un idéal à droite (resp. à gauche, bilatère)
- Si I et J sont deux idéaux à droite (resp. à gauche, bilatère) de A, $I + J = \{x + y, (x, y) \in I \times J\}$ est un idéal à droite (resp. à gauche, bilatère).
- Si J est un idéal à droite (resp. à gauche, bilatère) de B, $f^{-1}(J)$ est un idéal à droite (resp. à gauche, bilatère) de A.
- Si f est surjective et I un idéal à droite (resp. à gauche, bilatère) de A, alors $f(I)$ est un idéal à droite (resp. à gauche, bilatère) de B.
- Si I est un idéal à droite (resp. à gauche, bilatère) de A et J un idéal à droite (resp. à gauche, bilatère) de B, alors $I \times J$ est un idéal à droite (resp. à gauche, bilatère) de $A \times B$.
- Si A est commutatif, soient I et J deux idéaux de A. L'ensemble $I \cdot J$, des sommes finies de produits d'un élément de I par un élément de J. est un idéal de A.

Démonstration. On va prouver les cas des idéaux à droite. Les cas à gauche se traitent par symétrie et les cas bilatères s'en déduisent.

- Soit $(I_j)_{j\in J}$ une famille d'idéaux à droite de A. L'intersection de sous-groupes reste un sous-groupe donc $\bigcap\limits_{j\in J} I_j$ est un sous-groupe de $(A,+)$.
  Il reste à prouver simplement la stabilité par multiplication à droite.
  Soit $a\in A$ et $b\in \bigcap\limits_{j\in J} I_j$.
  Il existe j tel que $b\in I_j$. Comme I_j est un idéal à droite de A, $ba\in I_j$ donc $ba\in \bigcap\limits_{j\in J} I_j$.
- Soient I et J deux idéaux à droite de A.
  $I+J$ est un sous-groupe de $(A,+)$: Soient $x,y\in I+J$. $x=x_1+x_2$ et $y=y_1+y_2$.
  On a $x-y=\underbrace{x_1-y_1}_{\in I}+\underbrace{x_2-y_2}_{\in J}$ donc $x-y\in I+J$.
  $I+J$ est stable par multiplication à droite car si $x=x_1+x_2\in I+J$ et $a\in A$ alors $xa=\underbrace{x_1a}_{\in I}+\underbrace{x_2a}_{\in J}\in I+J$.
- Soit J un idéal à droite de B. $f^{-1}(B)$ est un sous-groupe de A (Chapitre 1).
  Soit $a\in A$, $b\in f^{-1}(J)$. On a $f(ba)=\underbrace{f(b)}_{\in J}\underbrace{f(a)}_{\in B}\in J$ car J idéal à droite.
- Soit I un idéal à droite de A. $f(A)$ est un sous-groupe de A (Chapitre 1).
  Soit $b\in f(I)$, $c\in B$. Il existe $a\in I$, $b=f(a)$. f est surjective donc $c=f(c')$ avec $c'\in A$. On a $bc=f(a)f(c')=f(\underbrace{ac'}_{\in I})\in f(I)$.
- Soit I un idéal à droite de A et J un idéal à droite de B.
  $I\times J$ est un sous-groupe de A se fait coordonnée par coordonnée.
  Soit $(a,b)\in A\times B$ et $(x_1,x_2)\in I\times J$. $(x_i,x_j)(a,b)=(\underbrace{x_ia}_{\in I},\underbrace{x_jb}_{\in J})\in I\times J$.
- Soient I et J des idéaux de A.
  Soient $x,s\in I\cdot J$. $x=\sum\limits_{i=1}^{n}x_iy_i$ et $s=\sum\limits_{i=1}^{p}u_iv_i$.
  $x-s=\sum\limits_{i=1}^{p+n}\alpha_i\beta_i$ avec $\alpha_i=x_i$ ou $\alpha_i=-u_i$ selon i et $\beta_i=y_i$ ou $\beta_i=v_i$ selon i. Donc $x-s\in I\cdot J$.
  Soit $x=\sum\limits_{i=1}^{n}x_iy_i\in I\cdot J$ et $a\in A$. $xa=\sum\limits_{i=1}^{n}x_i\underbrace{y_ia}_{\in J}\in I\cdot J$. ∎

Définition 2.13 Soit A un anneau, $S\subset A$ une partie non vide. On appelle idéal à droite (resp. à gauche, bilatère) engendré par S le plus petit idéal à

droite (resp. à gauche, bilatère) contenant S :

$$\langle S\rangle = \bigcap_{S\subset I \text{ idéal g/d/b de } A} I$$

THÉORÈME 2.4 *Soit A un anneau et $\varnothing \neq S \subset A$.*

Tout élément $x \in \langle S\rangle_d$ s'écrit sous la forme $x = \sum_{i=1}^{n} s_i a_i$ avec $s_i \in S$ et $a_i \in A$.

Tout élément $x \in \langle S\rangle_g$ s'écrit sous la forme $x = \sum_{i=1}^{n} a_i s_i$ avec $s_i \in S$ et $a_i \in A$.

Tout élément $x \in \langle S\rangle_b$ s'écrit sous la forme $x = \sum_{i=1}^{n} a_i s_i a_i'$ avec $s_i \in S$ et $a_i, a_i' \in A$.

Démonstration. Il suffit de prouver le cas à droite, en montrant que l'ensemble Γ des sommes finies de termes $s_i a_i$ est un idéal de A contenant S.

Γ est clairement un sous-groupe de $(A,+)$. Soit $a \in A$ et $\sum_{i=1}^{p} s_i a_i \in \Gamma$.

$$\left(\sum_{i=1}^{n} s_i a_i\right) a = \sum_{i=1}^{n} s_i (a_i a) \in \Gamma$$

Donc Γ est un idéal de A contenant S donc $\langle S\rangle \subset \Gamma$.

Soit I un idéal à droite de A contenant S. Soit $x = \sum_{i=1}^{n} s_i a_i \in \Gamma$.

$s_i a_i \in I$ donc $\sum_{i=1}^{n} s_i a_i \in I$ donc $\Gamma \subset I$ donc $\Gamma \subset \langle S\rangle$. ∎

THÉORÈME 2.5 *Soit A un anneau unitaire et I un idéal à droite ou à gauche de A.*

$$I = A \quad \text{ssi} \quad 1 \in I \quad \text{ssi} \quad I \cap A^\times \neq \varnothing$$

Démonstration.

- Les implications $\Rightarrow$ sont débiles.
- Supposons $I \cap A^\times \neq \varnothing$. Il existe $c \in I$ inversible. Par hypothèse, cc^{-1} ou $c^{-1}c \in I$ donc $1_A \in I$.
- Si $a \in A$, $a1_A$ ou $1_A a \in I$ donc $A \subset I$ et $A = I$. ∎

THÉORÈME 2.6 *Soit A un anneau unitaire.*

Il existe un unique morphisme d'anneaux unitaires $\varphi : \mathbb{Z} \to A$ qui, à $m \in \mathbb{Z}$, associe $m.1_A$.

Son noyau est un idéal de $\mathbb{Z}$ de la forme $n_A\mathbb{Z}$.

Définition 2.14 n_A est appelé caractéristique de l'anneau A.

Exemples :
- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont de caractéristique nulle.
- $\mathbb{Z}/p\mathbb{Z}$ est de caractéristique p.

THÉORÈME 2.7 (CORRESPONDANCE DES IDÉAUX) *Soient A et B deux anneaux commutatifs. Soit $f : A \to B$ un morphisme d'anneaux. Les applications $f^{-1} : \{$idéaux de $B\} \to \{$idéaux de A contenant $\mathrm{Ker}(f)\}$ et $f_* : \{$idéaux de A contenant $\mathrm{Ker}(f)\} \to \{$idéaux de $B\}$ sont des bijections réciproques. Ces bijections respectent les inclusions et les intersections.*

Démonstration. La seconde assertion découle des propriétés de la théorie des ensembles. Montrons la première.

Soit J un idéal de B.

$f_*(f^{-1}(J)) = f(f^{-1}(J)) = J$ car f surjective.

Soit I un idéal de A contenant $\mathrm{Ker}(f)$.

$I \subset f^{-1}(f(I))$. Supposons qu'il existe $y \in f^{-1}(f(I)) \setminus I$

$f(y) \in f(I)$ donc il existe $x \in I$, $f(y) = f(x)$. Comme f est un morphisme d'anneaux, $f(y - x) = 0$ donc $y - x \in \mathrm{Ker}(f)$.

Comme $\mathrm{Ker}(f) \subset I$, on conclut à $y \in I$, ce qui contredit $y \notin I$.

Donc $I = f^{-1}(f(I))$. ∎

2.4 Idéaux premiers et maximaux d'un anneau commutatif

Définition 2.15 Soit A un anneau commutatif et I un idéal propre de A (ie $I \neq A$). On dit que :
- I est premier ssi pour tout $(a, b) \in A$, $ab \in I \Rightarrow a \in I$ ou $b \in I$
- I est maximal ssi pour tout idéal J, $I \subset J \Rightarrow J = A$ ou $J = I$.

Remarque 2.6
- *Un idéal maximal est un élément maximal de l'ensemble des idéaux propres de A ordonné par l'inclusion.*
- *Si A est unitaire, tout idéal maximal est premier.*
  En effet, si I est maximal non premier, il existe $(a, b) \in A^2$ tel que $ab \in I$, $a \notin I$ et $b \notin I$.
  On a donc $I \subsetneq a + I$ et $I \subsetneq b + I$. Comme I est maximal, $\langle a \rangle + I = A = \langle b \rangle + I$.
  Il existe $(x, y) \in A^2$ et $(a_1, b_1) \in I^2$ tel que $1 = a_1 + ax = b_1 + by$.
  D'où $1 = a_1 b_1 + a_1 ay + ab_1 x + abxy \in I$ (car chaque terme appartient à I) donc $I = A$ donc on a contradiction.

Donc I est premier.

Définition 2.16 On dit qu'un ensemble ordonné E est inductif ssi toute partie de E totalement ordonnée possède un majorant dans E.

Exemple : $(\mathbb{R}, \geqslant)$ n'est pas inductif. Si E est un ensemble, $(\mathcal{P}(E), \subset)$ est inductif.

THÉORÈME 2.8 (LEMME DE ZORN) *Tout ensemble inductif possède un élément maximal.*

Remarque 2.7 C'est équivalent à l'axiome du choix.

THÉORÈME 2.9 *Tout anneau A commutatif et unitaire possède un idéal maximal.*

Démonstration.

- Si $\{0\}$ est un idéal maximal de A, on a le résultat.
- Sinon, on pose $J = \{\text{idéaux propres non nuls de } A\}$.
  On peut ordonner cet ensemble par l'inclusion. On montre J inductif.
  J est non vide sinon $\{0\}$ serait un idéal maximal de A.
  Soit $(I_\alpha)_{\alpha \in A}$ une famille totalement ordonnée d'idéaux propres non nuls de A. On pose $I = \bigcup_{\alpha \in A} I_\alpha$.
  — Soit $(x, y) \in I^2$. $x \in I_\alpha$ et $y \in I_\beta$.
  On peut supposer $I_\alpha \subset I_\beta$ donc $x \in I_\beta$ donc $x + y \in I_\beta \subset I$.
  — Soit $(a, x) \in A \times I$. $x \in I_\alpha$ donc $ax \in I_\alpha \subset I$.
  I est un idéal qui est non nul car $I_\alpha \neq \{0\}$. Il est propre car $I = A$ ssi $1 \in I$ ssi $1 \in \exists \alpha, I_\alpha$ ssi $\exists \alpha, I_\alpha \in A$.
  Donc $I \neq A$ et $I \in J$. J est inductif donc possède un élément maximal.
  Donc A possède un idéal maximal distinct de $\{0\}$. ■

Proposition 2.7 Soit I un idéal de $\mathbb{Z}$.
I premier ssi $I = \{0\}$ ou $I = p\mathbb{Z}$, p premier.
I est maximal ssi I premier non nul.

Démonstration.

- Si $I = \{0\}$, I est premier car $\mathbb{Z}$ est intègre.
  Si $I = p\mathbb{Z}$ avec p premier, soient $(a, b) \in p\mathbb{Z}$ On a $ab = pq$ donc $p|ab$ donc $p|a$ ou $p|b$ donc $a \in \mathbb{Z}$ ou $b \in \mathbb{Z}$.
- Soit I un idéal premier de $\mathbb{Z}$ non nul.
  I est un sous-groupe de $\mathbb{Z}$ donc il existe $n \in \mathbb{N}$, $I = n\mathbb{Z}$.
  Supposons n non premier, ie $n = n_1 n_2$ avec $1 < n_1, n_2 < n$. n_1 et n_2 n'appartiennent pas à $n\mathbb{Z}$ mais $n = n_1 n_2 \in n\mathbb{Z}$.
  Donc I n'est pas premier. Par contraposée, I est premier implique $I = p\mathbb{Z}$ avec p premier.

- $\mathbb{Z}$ est commutatif donc maximal implique premier.
  Or $I \neq \{0\}$ car, pour tout $n \geqslant 2$, $\{0\} \subsetneq n\mathbb{Z} \subsetneq \mathbb{Z}$.
- Si I est premier non nul, $I = p\mathbb{Z}$ avec p premier.
  Soit J un idéal de $\mathbb{Z}$ tel que $I \subset J$. J est un sous-groupe de $\mathbb{Z}$ donc $J = n\mathbb{Z}$.
  $p\mathbb{Z} \subset n\mathbb{Z}$ donc $n|p$. Or p est premier donc $n = 1$ ou $n = p$. Donc $J = \mathbb{Z}$ ou $J = I$.
  Donc I est maximal. ■

Exemple : Si K est un corps commutatif, on montrera que $K[X]$ vérifie le théorème.

2.5 Application à la géométrie algébrique

Soit A un anneau commutatif unitaire. On note $\mathrm{Sp}(A) = \{I \subset A, I \text{ premier}\}$.

On peut définir une topologie sur cet ensemble (topologie de Zariski) : les fermés en sont les $V(I) = \{P \in \mathrm{Sp}(A), I \subset P\}$.

Ce sont bien des fermés : $\bigcap_\alpha V(I_\alpha) = V(\langle I_\alpha \rangle_\alpha)$ et $V(I) \cup V(J) = V(I \cap J)$.

En géométrique algébrique, les objets sont sont les racines d'un polynôme de $k[X_1, \cdots, X_n]$ dans $\mathbb{K}$.

Une variété algébrique est la donnée l'un couple $(X, \mathcal{O}(X))$ où X est un espace topologique et $\mathcal{O}(X)$ un faisceau de fonctions. L'intérêt de ces monstruosités est qu'elles définissent un dictionnaire entre propriétés géométriques des espaces de solutions des équations polynômiales et algèbre commutative, et que ceci unifie la théorie des nombres et la géométrie dans un traitement moderne.

L'espace est représenté par un anneau A. Un point est représenté par un idéal premier de A, un fermé par un idéal de A, un ouvert de base par la localisation de A par un élément $f \in A$.

Comment s'interprète A intègre ?

Définition 2.17 On dit qu'un espace topologique est irréductible ssi pour tous fermés propres F et F' de X, $X = F \cup F' \Rightarrow X = F$ ou $X = F'$.

Définition 2.18 Soit A un anneau commutatif unitaire. On appelle radical de A l'idéal de A formé des éléments nilpotents de A.

Proposition 2.8 Soit A un anneau commutatif unitaire tel que $\sqrt{0} = \{0\}$. $\mathrm{Sp}(A)$ est irréductible ssi A intègre.

Démonstration.

- Si $\mathrm{Sp}(A)$ est réductible, Il existe I, I' deux idéaux de A tel que $\mathrm{Sp}(A) = V(I) \cup V(I')$ avec $V(I) \neq \mathrm{Sp}(A)$ et $V(I') \neq \mathrm{Sp}(A)$.
  On a $\mathrm{Sp}(A) = V(I \cdot I')$ donc tout $P \in \mathrm{Sp}(A)$ contient $I \cdot I'$. Autrement dit, $I \cdot I' \subset \sqrt{0}$.
  Comme $V(I) \neq \mathrm{Sp}(A)$ et $V(I') \neq \mathrm{Sp}(A)$, il existe $a \in I$ et $a \in I'$ tel que $a \neq 0$ et $a' \neq 0$. Donc il existe $(a, a') \in A^2$ tel que $aa' = 0$.
- Si A est intègre, il existe $f, g \in A^2$ non nuls tel que $fg = 0$. $\mathrm{Sp}(A) \neq V(\langle f \rangle)$ et $\mathrm{Sp}(A) \neq V(\langle g \rangle)$.
  On a $\mathrm{Sp}(A) = V(\langle f \rangle) \cup V(\langle g \rangle) = V(\langle fg \rangle) = V(0)$. ■

Chapitre 3

Généralités sur les corps

3.1 Définition

Définition 3.1 Un anneau unitaire $(A, +, \cdot)$ est un corps ssi tous les éléments non nuls de A sont inversibles ssi $(A, +)$ et $(A \setminus \{0\}, \cdot)$ sont des groupes ssi les axiomes suivants sont vérifiés :

- $\forall (x, y, z) \in A^3, (x + y) + z = x + (y + z) = x + y + z$
- $\exists 0 \in A, \forall x \in A, x + 0 = 0 + x = x$
- $\forall x \in A, \exists (-x) \in A, x + (-x) = (-x) + x = 0$
- $\forall (x, y) \in A^2, x + y = y + x$
- $\forall (x, y, z) \in A^3, (xy)z = x(yz) = xyz$
- $\exists 1 \in A, \forall x \in A, x1 = 1x = x$
- $\forall x \in A \setminus \{0\}, \exists x^{-1} \in A, xx^{-1} = x^{-1}x = 1$
- $\forall (x, y, z) \in A^3, (x + y)z = xz + yz$ et $x(y + z) = xy + xz$

Remarque 3.1 Si on veut spécifier que dans un corps A, $A \setminus \{0\}$ n'est pas commutatif, on dit que A est une algèbre à divisions. Dans le cas contraire, on dira que A est un corps commutatif.

Exemples :

- $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps .
- $\mathbb{Z}$ n'est pas un corps.
- $\mathbb{Z}/n\mathbb{Z}$ est un corps ssi n est premier.
  En effet n premier ssi $\forall 0 < k \leqslant n - 1, \exists (u, v) \in \mathbb{Z}^2, ku + nv = 1$ ssi $\forall 0 < k \leqslant n - 1, \exists u \in \mathbb{Z}, \overline{k}\overline{u} = \overline{1}$ ssi $\forall 0 < k \leqslant n - 1, \overline{k}$ inversible.

Proposition 3.1 Soit A un corps. A est intègre, le seul idéal propre de A est $\{0\}$ et tout morphisme d'anneaux unitaires $\varphi : A \to B$ est injectif.

Démonstration.

- Soit $a \in A$ et $b \in A \setminus \{0\}$ tel que $ab = 0$. b est inversible donc $a = 0b^{-1} = 0$. De même si $ba = 0$. Donc A est intègre.
- Si $I \neq A$ est un idéal de A. Si $a \in I$ est non nul, $aa^{-1} \in I$ ou $a^{-1}a \in I$ donc $I = A$ (contradiction) donc $I = \{0\}$.
- Soit $\varphi : A \to B$. $\mathrm{Ker}(\varphi)$ est un idéal de A propre car $1 \notin \mathrm{Ker}(A)$. Donc $\mathrm{Ker}(A) = \{0\}$. ■

Remarque 3.2 Le deuxième point admet une réciproque : si A est unitaire et si ses seuls idéaux sont A et $\{0\}$ alors A est un corps.

Démonstration. Il reste à montrer l'existence de l'inverse.

Soit $a \in A$ non nul. aA est un idéal non nul de A car $a \neq 0$ donc $aA = A$.

Il existe donc $b \in A$ tel que $ab = 1$. Dans Aa, le même raisonnement amène $ca = 1$.

$cab = b$ donc $c = b$ car $ab = 1$. Donc $ab = ba = 1$. ■

Lemme 3.0.1
Tout anneau A unitaire intègre et fini est un corps.

Remarque 3.3 La réciproque est fausse.
L'hypothèse intègre est nécessaire.

Démonstration. Soit $a \in A \setminus \{0\}$. On pose :

$$\varphi_a : \begin{cases} A & \to & A \\ b & \mapsto & ab \end{cases}$$

Par distributivité, φ_a est un endomorphisme de groupes de $(A, +)$. Par intégrité de A, $\mathrm{Ker}(\varphi_a) = \{0\}$.

Donc φ_a bijective donc il existe $a' \in A$, $aa' = 1$. Par intégrité, $a'a = 1$.

Donc $A^* = A^\times$. ■

Remarque 3.4
- *Tout corps fini est commutatif (théorème de* Wedderburn*)*
- *Si F est un corps commutatif, tout sous-groupe fini G de $F \setminus \{0\}$ est fini.*
- *Si F est un corps fini, $F \setminus \{0\}$ est cyclique.*

3.2 Extensions et caractéristique

On suppose à présent les corps commutatifs.

Définition 3.2 Soit k un corps commutatif.

Une extension de corps de k est la donnée d'une k-algèbre K qui est un corps.

Le morphisme d'anneaux (structurel) $k \to K$ définissant l'extension de corps est injectif donc bijectif sur son image que l'on identifie à k. Conventionnellement, on note $k \hookrightarrow K$ l'extension de corps.

Définition 3.3 Un sous-corps de k est un corps contenu dans k. Si F est un sous-corps de k, le morphisme d'inclusion définit une extension de corps. Si $k \hookrightarrow K$, k est un sous-corps de K.

Exemples :

- Id : $k \to k$ définit une extension de corps de k et k est un sous-corps de k.
- $\mathbb{Q}$ est un sous-corps de $\mathbb{R}$ qui est un sous-corps de $\mathbb{C}$.
- $K = \mathbb{F}_2[X]/\langle X^2 + X + 1\rangle = \{a + bX, (a, b) \in \mathbb{F}_2\} = \{0, 1, x, 1 + x\}$. K est un corps.

Lemme 3.0.2
Soit k un corps commutatif. Soit $(F_i)_{i\in I}$ une famille de sous-corps de K.

Alors $F = \bigcap\limits_{i\in I} F_i$ est un sous-corps de k.

Démonstration. Soit F_i un sous-corps. $F_i \setminus \{0\}$ est un sous-groupe de $k \setminus \{0\}$

L'intersection de sous-groupes est un sous-groupe donc $\bigcap\limits_{i\in I} F_i \setminus \{0\}$ est un sous-groupe de $k \setminus \{0\}$ et $\bigcap\limits_{i\in I} F_i$ est un sous-groupe de k. ∎

Définition 3.4 Soit k un corps commutatif.

L'intersection de tous les sous-corps de k est appelée sous-corps premier de k. C'est le plus petit sous-corps de k et il est propre.

Remarque 3.5 Plus généralement, le lemme ci-dessus permet de donner un sens à la contruction suivante. Soit $k \hookrightarrow K$ une extension de corps. Soit $(\alpha_1, \cdots, \alpha_n) \in K$. On peut alors construire le sous-corps de K engendré par k et les α_i comme :

$$k(\alpha_1, \cdots, \alpha_n) = \bigcap_{k\cup\{\alpha_1,\cdots,\alpha_n\}\subset F \text{ sous-corps de } K} F$$

ou si on se donne $S \subset K$, le lemme donne également un sens au sous-corps de K engendré par k et S.

Proposition 3.2 Soit k un corps commutatif.

Si k est de caractéristique nulle, son sous corps premier est $\mathbb{Q}$, sinon, c'est $\mathbb{F}_n$ avec n sa caractéristique.

Si $k \hookrightarrow F$ est une extension de corps de k, alors F a la même caractéristique que k et le même sous-corps premier. De même si k' est un sous-corps de k.

Démonstration.

- Notons $\varphi : n \to n.1_k$. Si $\mathrm{Ker}(\varphi) = \{0\}$, on pose :
$$\overline{\varphi} : \begin{cases} \mathbb{Q} & \to & k \\ \frac{a}{b} & \mapsto & \varphi(a)\varphi(b)^{-1} \end{cases}$$
$\overline{\varphi}$ est bien définie et est un morphisme d'anneaux. Donc $\overline{\varphi}$ est injectif et tout sous-corps contient $\mathbb{Q}$. Donc le sous-corps premier vaut $\mathbb{Q}$.
- Si $\mathrm{Ker}(\varphi) = n\mathbb{Z}$, si $n = n_1 n_2$, $\varphi(n_1)\varphi(n_2) = 0$ donc $n|n_1$ ou $n|n_2$. Contradiction.
Donc n est premier. De même, $\overline{\varphi} : \mathbb{F}_p \to k$ est un morphisme d'anneaux unitaires donc injectif et le sous-corps premier est $\mathbb{F}_p$.
- Soient $k_1 \hookrightarrow k_2$. Montrons que les caractéristiques n_1 et n_2 de k_1 et k_2 sont égales.
Notons f le morphisme structurel $k_1 \to k_2$, $\varphi_1 : n \mapsto n.1_{k_1}$ et $\varphi_2 : n \mapsto n.1_{k_2}$.
$f \circ \varphi_1 = \varphi_2$ donc $n_2\mathbb{Z} = \mathrm{Ker}(\varphi_2) = \varphi_2^{-1}(\{0\}) = \varphi_1^{-1}f^{-1}(\{0\}) = \varphi^{-1}(\{0\}) = n_1\mathbb{Z}$. car f injective (morphisme de corps).
Donc $n_1 = n_2$ car ils sont positifs. ∎

Définition 3.5 Soit K une extension de k. Le degré de l'extension K est la dimension de K en tant que k espace vectoriel. On le note $[K : k]$. On dit que l'extension est finie ssi $[K : k]$ est fini.

Remarque 3.6

- $[K : k] \geqslant 1$
- *Une extension de corps K de k ne définit pas toujours en espace vectoriel de dimension finie. Par exemple $\mathbb{Q}[X]$ et $\mathbb{F}_p[X]$.*
- $\mathbb{R} \hookrightarrow \mathbb{C}$ *et* $[\mathbb{C} : \mathbb{R}] = 2$.

Proposition 3.3 Soient $k \hookrightarrow K \hookrightarrow L$ deux extensions de corps emboîtées.

- $[K : k] < \infty$ et $[L : K] < \infty$ ssi $[L : k] < \infty$
- Dans ce cas, $[L : k] = [L : K][K : k]$.

Lemme 3.0.3
Soient $k \hookrightarrow K \hookrightarrow L$ des extensions emboîtées.

Si $(e_i)_{i\in I}$ une base du k espace vectoriel K et $(f_i)_{i\in J}$ une base du K espace vectoriel L alors $(e_i f_j)_{(i,j)\in I\times J}$ est une base du k espace vectoriel L.

Démonstration. La liberté est claire. La génératricité aussi. La proposition s'en déduit. ∎

3.3 Compléments

Définition 3.6 Soit k un corps commutatif.

- Une extension L de k est une k-algèbre dont l'anneau sous-jacent est un corps. On dit que L est un sur-corps de k.
- Un sous-corps de k est un sous-anneau de k qui est un corps.
- Soit $k \hookrightarrow L$. Si $[L : k]$ est fini, on dit que L est une extension finie de k.

Les théorèmes de Galois donne un lien entre la théorie des groupes et algèbre commutative.

Soit k un corps de caractéristique nulle.

On peut lui associer un groupe fini. $\mathrm{Gal}(L, k) = \mathrm{Aut}_k(L)$.

Théorème 3.1 (Correspondance de Galois) *Soit k un corps commutatif et $k \hookrightarrow L$ finie de degré n.*

Il existe une bijection :

$$f : \begin{cases} \{K, k \hookrightarrow K \hookrightarrow L\} & \to & \{\textit{Sous-groupes de } \mathrm{Gal}(L, k)\} \\ K & \mapsto & \mathrm{Gal}(L, k) \end{cases}$$

Chapitre 4

Les anneaux de polynômes

4.1 Définitions

On note $A^{(\mathbb{N})}$ l'ensemble des suites presque nulles d'éléments de A.

Définition 4.1 Soit $a \in A^{(\mathbb{N})}$.

- On appelle degré de a le plus grand n tel que $a_n \neq 0$. On a, par convention $\deg(0) = -\infty$.
- Pour tout k, a_k est le cœfficient de a en position k.
- Le cœfficient dominant de a est son cœfficient en psition $\deg(a)$.

Remarque 4.1 Par définition le cœfficient dominant est non nul.

THÉORÈME 4.1 *Soit A un anneau unitaire.*

$(A^{(\mathbb{N})}, +, \cdot)$ est un anneau unitaire avec la somme terme à terme et le produit de Cauchy. De plus le neutre est $1 = (\delta_{0,i})_{i\in\mathbb{N}}$ et $a \mapsto a.1$ est un morphisme d'anneaux injectif.

Démonstration. Affligeant. ■

Définition 4.2 On pose $X^0 = 1$ et X^k est le polynôme dont tous les coefficients sont nuls sauf le k-ème qui vaut 1.

Lemme 4.1.1
$X^k = X \cdot X^{k-1} = X^{k-1} \cdot X$.

Démonstration. La démonstration précédente conclut. ■

Lemme 4.1.2
Soit $P \in A^{(\mathbb{N})}$ tel que $P = (a_n)_n$.

$$P = \sum_{j=0}^{\deg(P)} \tau(a_j) X^j.$$

Définition 4.3 (Anneau polynôme) On appelle anneau de polynômes en une variable et à cœfficients dans A l'anneau :

$$A[X] = A^{(\mathbb{N})}$$

muni de la somme terme à terme et du produit de Cauchy.

Comme $a \mapsto a \cdot 1$ est injective, on notera tout polynôme sous la forme $P = \sum_{j=0}^{\deg(P)} a_j X^j$.

Remarque 4.2 $P = 0$ *ssi pour tout* n, $a_n = 0$.

Définition 4.4 (Polynômes en plusieurs variables) Soit $(A, +, \cdot)$ un anneau unitaire. On appelle anneau des polynômes en n variables l'anneau qu'on note $A[X_1, \cdots, X_n]$ défini par récurrence par :

$$A[X_1, \cdots, X_n] = A[X_1, \cdots, X_{n-1}][X_n]$$

Lemme 4.1.3
Tout élément $P \in A[X_1, \cdots, X_n]$ s'écrit $P = \sum_{i_1, \cdots, i_n} a_{i_1, \cdots, i_n} X_1^{i_1} \cdots X_n^{i_n}$.

Remarque 4.3 Comme dans le cas des polynômes en une variable, on peut définir directement les lois de composition sur $A[X_1, \cdots, X_n]$.

Par exemple, si $n = 2$, $A[X_1, X_2]$ *se définit à partir de* $A^{(\mathbb{N}\times\mathbb{N})}$ *avec l'addition de matrices et*

$$((a_{i,j})_{i,j}, (b_{i,j})) \mapsto \left(\sum_{l=0}^{j} \sum_{h=0}^{i} a_{h,l} a_{i-h,j-l} \right)_{i,j}$$

Lemme 4.1.4
Soit A un anneau unitaire. L'application deg : $A[X] \to \overline{\mathbb{N}}$ vérifie :

- $\deg(X^n) = n$
- $\deg(P + Q) \leqslant \max(\deg(P), \deg(Q))$
- $\deg(PQ) \leqslant \deg(P) + \deg(Q)$

Si le cœfficient dominant de P ou celui de Q est régulier dans A alors $\deg(PQ) = \deg(P) + \deg(Q)$.

Démonstration. Que celui qui ne sait pas faire la démo retourne en sup. ■

COROLLAIRE 4.1 *Soit* $(A, +, \cdot)$ *un anneau unitaire.*

Si A *est commutatif (resp. intègre),* $A[X]$ *est commutatif (resp. intègre).*

Démonstration. Commutativité : débile par réindiciation qui est une CS de débilité.

Intégrité : Si $PQ = 0$ avec $P \neq 0$ et $Q \neq 0$, $a_{\deg(P)} b_{\deg(Q)} = 0$ et est différent de 0. ■

Remarque 4.4 Si A unitaire, $A[X]$ n'est pas un corps car X n'a pas d'inverse : si $XP = 1$, alors $0 = \deg(X) + \deg(P) = 1 + \deg(P)$.

Définition 4.5 (Irréductibilité) Soit A commutatif unitaire. P est irréductible ssi c'est un élément irréductible de $A[X]$.

Proposition 4.1 Soient $(A, +, \cdot)$ et $(B, +, \cdot)$ deux anneaux unitaires.

Soit $\varphi : A \to B$ un morphisme d'anneaux unitaires.

Il existe un morphisme d'anneaux unitaire : $\overline{\varphi} : A[X] \to B[X]$ tel que $\overline{\varphi}|_A = \varphi$ et $\overline{\varphi}(X) = X$.

Si φ est injective (resp. surjective, bijective), $\overline{\varphi}$ est injective (resp. surjective, bijective).

Remarque 4.5 Étant donné un isomorphisme $\psi : A[X] \to B[X]$, le fait que ψ provienne d'un morphisme d'anneaux unitaires φ est faux en général (problème de simplification de Zariski*).*

Démonstration.

$$\overline{\varphi} : \begin{cases} A[X] & \to & B[X] \\ \sum_{i=0}^{n} a_i X^i & \mapsto & \sum_{i=0}^{n} \varphi(a_i) X^i \end{cases}$$

convient. ∎

4.2 Division euclidienne dans $A[X]$

Soit A un anneau unitaire et commutatif.

Définition 4.6 (Polynôme unitaire) On dit qu'un polynôme P non nul est unitaire ssi son cœfficient dominant est inversible dans A.

Remarque 4.6 Si A est un corps tout polynôme non nul de $A[X]$ est unitaire.

Théorème 4.2 (Division euclidienne) *Soit A un anneau commutatif unitaire.*

Pour tout $(F, P) \in A[X]^2$ avec F unitaire, il existe un unique couple $(Q, R) \in A[X]^2$ tel que $P = FQ + R$ avec $R = 0$ ou $0 \leqslant \deg(R) < \deg(F)$.

Démonstration.

! Soit $(Q_1, R_1), (Q_2, R_2) \in (A[X])^2$ vérifiant les propriétés de l'énoncé.
Alors $FQ_1 + R_1 = P = FQ_2 + R_2$ d'où $F(Q_1 - Q_2) = (R_2 - R_1)$.
Comme F est unitaire, son cœfficient dominant est régulier.
D'après le lemme précédent,

$$\deg(R_2 - R_1) = \deg F + \deg(Q_1 - Q_2)$$

Ou bien, $Q_1 = Q_2$, et alors $R_1 = R_2$ et c'est fini, ou bien ils sont différents, alors $\deg(Q_1 - Q_2)$ est positif et on obtient une contradiction sur $\deg(R_2 - R_1)$.

$\exists$ Soit $F \in A[X]$ unitaire de degré n.
Si $P = 0$, on peut prendre $Q = R = 0$ et tout va bien.
On le suppose donc non nul. Supposons que le degré de P soit le degré minimal pour qu'un tel couple n'existe pas. Notons $d = \deg(P)$.
Ou bien $d < n$, et dans ce cas le couple $(0, P)$ marche donc il y a comme qui dirait une contradiction.
Ou bien $d \geqslant n$. Posons $F = aX^n + F_0$.
Alors, $\deg(F_0) < n$. De même, $P = bX^k + P_0$, $\deg(P_0) < d$.
On peut écrire $P = ba^{-1}X^{d-n}F + P_1$ avec $P_1 = -ba^{-1}X^{d-n}F_0 + P_0$.
Remarquons alors que

$$\deg P_1 \leqslant \max(\deg P_0, \deg(-ba^{-1}X^{d-n}F_0)) \leqslant (d-1)$$

grâce à l'hypothèse de minimalité sur le degré de P, il existe $(Q_1, R_1) \in (A[X])^2$ comme dans l'énoncé.
D'où $P = (ba^{-1}X^{d-n} + Q_1)F + R_1$. On a prouvé l'existence d'un couple (Q, R) vérifiant l'hypothèse de l'énoncé. Contradiction ! ∎

4.3 Comparaison de $A[X]$ et $\mathbb{Z}$

On suppose que A est un corps commutatif.

Lemme 4.2.1
$A^\times = (A[X])^\times$.

Démonstration.

$\subset$ Clair

$\supset$ Soit $P \in A[X]^\times$.
Il existe Q tel que $PQ = 1$.
$\deg(P) + \deg(Q) = 0$ donc $\deg(P) = \deg(Q) = 0$ et $P \in A^\times$. ∎

Proposition 4.2 Soit A un corps commutatif et I un idéal de $A[X]$.
Il existe $P \in A[X]$ tel que $I = \langle P \rangle = P \cdot A[X]$.
De plus, I est maximal ssi I est premier non nul ssi il existe P irréductible tel que $I = \langle P \rangle$.

Démonstration.

- Soit I un idéal de $A[X]$.
  Si $I = \{0\}$, $I = 0 \cdot A[X]$.
  Sinon, il existe $P \in I$ non nul de degré minimal. On va montrer que $I = \langle P \rangle$.
  On a clairement une inclusion. Montrons la deuxième. Soit $F \in I$.
  Il existe Q, R tel que $F = PQ + R$ et $\deg(R) < \deg(P)$.
  $F \in I$ donc $R = F - PQ \in I$ donc $R \in I$ donc $\deg(R) = -\infty$ donc $R = 0$. Donc $F \in \langle P \rangle$.

$1 \Rightarrow 2$ Déjà vu : maximal implique premier et $A[X]$ pas un corps donc non nul.

$2 \Rightarrow 3$ Soit I premier non nul. Il existe $P \in A[X]$ non nul tel que $I = \langle P \rangle$.
Si $P = P_1 P_2$ avec P_1 et P_2 non inversibles. Par minimalité de $\deg(P)$, $P_1 \notin I$ et $P_2 \notin I$.
Cependant, $P_1 P_2 \in I$ donc contradiction.

$3 \Rightarrow 1$ Soit P irréductible (non nul) de degré minimal tel que $I = \langle P \rangle$.
Soit J idéal de $A[X]$ tel que $I \subset J$. On a de même $J = \langle Q \rangle$.
$I \subset J$ donc il existe $Q_0 \in A[X]$ tel que $P = QQ_0$.
Or P est irréductible donc Q ou Q_0 est inversible. Si Q inversible, $J = A$ et sinon, $I = J$. ∎

THÉORÈME 4.3 (DE BÉZOUT) *Soient P_1 et P_2 deux polynômes irréductibles tels que $P_1 \notin \langle P_2 \rangle$.*
Il existe $U, V \in A[X]$ tel que $UP_1 + VP_2 = 1$.

Démonstration. $\langle P_1 + P_2 \rangle \supsetneq \langle P_1 \rangle$ donc $\langle P_1 + P_2 \rangle = A[X]$ donc $1 \in \langle P_1 + P_2 \rangle = \langle P_1 \rangle + \langle P_2 \rangle$. ∎

Proposition 4.3 $A[X]$ est euclidien, principal, factoriel, en bref sympathique. Comme $\mathbb{Z}$.

4.4 Éléments entiers d'un anneau

On suppose les anneaux commutatifs et unitaires.

Définition 4.7 Soit B un anneau, A un sous-anneau de B et $c \in A$. On note $A[C]$ l'ensemble $\{b \in B, \exists P \in A[X], P(c) = b\}$.

Proposition 4.4 $A[c]$ est un sous-anneau de B.

Démonstration. Suis-je bien en L3 ? ∎

Proposition 4.5 Soit B un anneau commutatif unitaire, A un sous-anneau de B et $c \in B$.

$A[c]$ est un A-module de type fini ssi il existe $P \in A[X]$ unitaire non nul tel que $P(c) = 0$.

Démonstration.

$\Leftarrow$ On a $n = \deg(P) \geqslant 1$. Posons $x_i = c^i$ pour tout $i \in [\![0, n-1]\!]$.
On a clairement $Ac_0 + Ac_1 + \cdots + Ac^{n-1} \subset A[c]$.
Montrons l'autre inclusion : soit $b \in A[c]$.
Il existe $Q \in A[X]$ tel que $b = Q(c)$.
Il existe (Q_0, R) tel qe $Q = PQ_0 + R$ avec $\deg(R) < n$. Donc $b = Q(c) = P(c)Q_0(c) + R(c) = R(c)$.
Donc $b \in Ac_0 + \cdots + Ac^{n-1}$.

$\Rightarrow$ $A[c] = \sum_{i=1}^{p} x_i A$.
Par construction, $x_i \in A[c]$ donc il existe P_i tel que $P_i(c) = x_i$. Notons $q = \max_i \deg(P_i)$.
On veut trouver $S \in A[c]$ unitaire tel que $S(c) = 0$.
$A[c]$ est un sous-anneau de B donc $c^{q+1} \in A[c]$ donc il existe Q tel que $c^{q+1} = Q(c)$.
Par hypothèse, $Q(c) = \sum_{i=1}^{p} \alpha_i P_i(c)$ donc $\deg(Q) \leqslant n$.
$S = X^{q+1} - Q$ convient donc. ∎

Définition 4.8 (Élément entier) Soit B un anneau commutatif unitaire, A un sous-anneau de B et $c \in B$.

On dit que c est entier sur A ssi il existe $P \in A[X]$ unitaire tel que $P(c) = 0$.

Définition 4.9 (Élément algébrique, transcendant) Soit $k \hookrightarrow L$ une extension de corps et $c \in L$.

c est dit algébrique sur k ssi il existe $P \in k[X]$ non nul tel que $P(c) = 0$.

Si tous les éléments de L sont algébriques sur k, on dit que L est une extension agébrique de k.

Dans le cas contraire, c est dit transcendant.

Chapitre 5

Le quotient

5.1 Quotient d'un groupe par un sous-groupe distingué

cf Théorie des groupes.

Définition 5.1 Soit G un groupe.

Une relation d'équivalence $\mathcal{R}$ sur G est dite compatible avec $\cdot$ ssi on a $\forall (x, x', y, y') \in G^4$ tel que ($x\mathcal{R}x'$ et $y\mathcal{R}y'$) implique $xy\mathcal{R}x'y'$.

Théorème 5.1 (Factorisation par le quotient) *Soit $f : G \to G'$ un morphisme de groupes.*

Soit H un sous-groupe distingué de G et $\pi : G \to G/H$ le morphisme de groupes canonique. Les assertions suivantes sont équivalentes :

- *$f(H) = 1$;*
- *$H \subset \operatorname{Ker} f$;*
- *Il existe un unique morphisme de groupes $\overline{f} : G/H \to G'$ tel que $f = \overline{f} \circ \pi$. Si de plus, f est surjectif (resp. $H = \operatorname{Ker} f$), alors $\overline{f}$ est surjectif (resp. injectif)*

5.2 Quotient d'un anneau par un idéal

5.2.1 Généralités

Remarquons que, si A est un anneau, le groupe sous-jacent $(A, +)$ est commutatif. En particulier, le sous-groupe sous-jacent à un idéal I de A donné est distingué.

Théorème 5.2 (Existence du quotient) *Soit A un anneau et I un idéal de A. Alors les assertions suivantes sont équivalentes :*

- *I est un idéal bilatère de A ;*
- *Il existe sur le groupe quotient A/I une seconde loi de composition $A/I \times A/I \to A/I$ qui munit A/I d'une structure d'anneau et qui fait du morphisme de groupes canonique $A \to A/I$ un morphisme d'anneaux de A dans A/I.*
- *I est le noyau d'un morphisme d'anneaux défini sur A.*

Démonstration.

$2 \Rightarrow 3$ Découle du fait que $I = \mathrm{Ker}(\pi)$.

$3 \Rightarrow 1$ Soit $f : A \to B$ un morphisme d'anneaux de noyau I. Il s'agit de vérifier que I est un idéal bilatère de A.
Soit $x \in A$ et $i \in I$. On a $f(xi) = f(x)f(i) = 0 = f(i)f(x) = f(ix)$.
Donc I est un idéal bilatère de A.

$1 \Rightarrow 2$ Comme $(A, +)$ est commutatif, le groupe $(A/I, +)$ a bien un sens.
Soit $\overline{x}, \overline{y} \in A/I$. On pose $\overline{xy} = \overline{xy}$. Vérifions que cette définition a bien un sens.
On prend $x' \in x + I$, et $y' \in y + I$. Alors il existe $i \in I, j \in J$ tels que $x' = x + i$ et $y' = y + i$.
En développant le produit $x'y'$, on obtient une somme de xy et d'un élément de l'idéal, ce qui prouve que le produit est encore dans l'idéal.
Donc cette loi de composition est interne sur A/I.
De plus, compte tenu de la définition il est facile de vérifier :
- ▶ les axiomes de la structure d'anneau pour A,
- ▶ que le morphisme de groupes $(A, +) \to A/I$ s'étend en un morphisme d'anneaux. ■

Définition 5.2 Soient A un anneau et I un idéal bilatère de A. L'anneau A/I défini par le théorème précédent est appelé anneau quotient de A par l'idéal I.

Remarque 5.1

- *Si A est un anneau unitaire, A/I est unitaire, d'unité la classe du neutre de A.*
- *Si A est commutatif, A/I est commutatif.*

THÉORÈME 5.3 (FACTORISATION PAR LE QUOTIENT) *Soient A,B deux anneaux, $f : A \to B$ un morphisme d'anneaux.*

Soit I un idéal bilatère de A et $\pi : A \to A/I$ le morphisme d'anneaux canonique (construit par le théorème ci-dessus).

Les assertions suivantes sont équivalentes :

- $f(I) = (0)$
- $I \subset \mathrm{Ker}\, f$

- *Il existe un unique morphisme d'anneaux $\overline{f} : A/I \to B$ tel que $f = \overline{f} \circ \pi$.*
  De plus, si f est surjectif (resp. $I = \mathrm{Ker}(f)$) alors $\overline{f}$ est surjectif (resp. injectif).
  Si A, B sont unitaires et si $f : A \to B$ est un morphisme d'anneaux unitaires, alors $\overline{f}$ en est aussi un.

Démonstration.
$1 \Rightarrow 2$ Définition du noyau.
$2 \Rightarrow 3$ En vertu du résultat analogue en théorie des groupes, il existe un unique morphisme de groupes $\overline{f} : A/I \to B$ vérifiant $f = \overline{f} \circ \pi$.
Vérifions la compatibilité de cette définition pour la multiplication.
Soit $x, y \in A$. On a $\overline{f}(\overline{xy}) = \overline{f}(\pi(xy)) = f(xy) = f(x)f(y)$.
Si f est surjectif, on a vu que $\overline{f}$ en tant que morphisme de groupes est surjectif, donc $\overline{f}$ est surjectif en tant que morphisme d'anneaux.
Si $I = \mathrm{Ker}\, f$, alors $\overline{f}$ est injective, donc $\overline{f}$ est injective en tant que morphisme d'anneaux.
Si $f : A \to B$ est unitaire, $f(1) = 1$, $\overline{f}(1) = 1$.
$3 \Rightarrow 1$ Soit $x \in I = 0 + I$.
Alors $\overline{x} = 0$, donc $\overline{f}(x) = \overline{f}(0) = f(0) = 0$. ∎

Corollaire 5.1 *Soit $f : A \to B$ un morphisme d'anneaux (resp. d'anneaux unitaires) surjectif.*
Il existe un unique isomorphisme d'anneaux (resp. d'anneaux unitaires) $\overline{f} : A/\mathrm{Ker}(f) \to B$ tel que $f = \overline{f} \circ \pi$.

Démonstration. On a vu que $\mathrm{Ker}(f)$ est un idéal bilatère. On peut donc appliquer le théorème précédent avec $I = \mathrm{Ker}(f)$. ∎

5.2.2 Conséquences directes de l'existence du quotient

Proposition 5.1 Soit A un anneau, I un idéal de A.
- Si A est commutatif, I est un idéal bilatère et I est premier ssi A/I est intègre.
- Si A est commutatif et unitaire, alors I est maximal ssi A/I est un sous-corps.

Démonstration. Soit I un idéal de A.
- I est premier ssi $I \neq A$ et $ab \in I \Rightarrow (a \in I$ ou $b \in I)$
  Donc I premier ssi $A/I \neq (0)$ et $\overline{a}\overline{b} = 0 \Rightarrow \overline{a} = 0$ ou $\overline{b} = 0$ ssi A/I est intègre.

- Si $I \neq A$, I est maximal ssi pour tout idéal J de A, $J \supset I \Rightarrow (I = A$ ou $J = I)$
  Donc I est maximal ssi $\forall x \in A \setminus I, \langle x \rangle + I = A$.
  En particulier, A/I est un anneau unitaire et commutatif.

$$\begin{array}{rll} A/I \text{ est un corps} & \text{ssi} & (A/I) \setminus \{0\} \text{ est un groupe multiplicatif} \\ & \text{ssi} & \forall \overline{x} \in (A/I) \setminus \{0\}, \exists \overline{y}, \overline{xy} = 1 \\ & \text{ssi} & \forall x \in A \setminus I, \exists y \in A, xy \in 1 + I \\ & \text{ssi} & \forall x \in A \setminus I, (x) + I = A \end{array}$$

  Donc I est maximal ssi A/I est un corps. ∎

THÉORÈME 5.4 (IDÉAUX DU QUOTIENT) *Soit A un anneau commutatif et I un idéal de A.*

L'ensemble des idéaux de A contenant I est en bijection avec l'ensemble des idéaux de A/I.

Cet énoncé est une application de la correspondance des idéaux par un morphisme surjectif, appliqué à π. On le rappelle ici pour mémoire.

THÉORÈME 5.5 (CORRESPONDANCE DES IDÉAUX) *Soient A et B deux anneaux commutatifs. Soit $f : A \to B$ un morphisme d'anneaux. Les applications $f^{-1} : \{$idéaux de $B\} \to \{$idéaux de A contenant $\mathrm{Ker}(f)\}$ et $f_* : \{$idéaux de A contenant $\mathrm{Ker}(f)\} \to \{$idéaux de $B\}$ sont des bijections réciproques. Ces bijections respectent les inclusions et les intersections.*

Remarque 5.2 On peut expliciter les bijections entre ces deux ensembles grâce à :

$$\pi_* : \begin{cases} \{\text{idéaux de } A \text{ contenant } I\} & \to & \{\text{idéaux de } A/I\} \\ J \supset I & \mapsto & \pi(J) \end{cases}$$

et

$$\pi_* : \begin{cases} \{\text{idéaux de } A/I\} & \to & \{\text{idéaux de } A \text{ contenant } I\} \\ J & \mapsto & \pi^{-1}(J) \end{cases}$$

THÉORÈME 5.6 *Soit A un anneau commutatif et unitaire. Soit $I \subsetneq A$ un idéal propre de A.*

Il existe un idéal maximal $M \subset A$ tel que $M \supset I$.

Démonstration. $A/I \neq (0)$ donc il existe un idéal maximal $\overline{M}$ de A/I tel que $\overline{M} \neq \langle 0 \rangle$ (par un des théorèmes précédents).

Par la correspondance des idéaux, on sait qu'il existe un idéal M contenant I tel que $\pi(M) = \overline{M}$.

Si $M = A$, $\pi(M) = A/I = \overline{M}$, ce qui est impossible (sic). Donc $M \neq A$.

Exo de TD, $(A/I)/\overline{M} \simeq A/M$, donc A/M est un corps, d'où M est maximal. ■

Définition 5.3 (Idéaux comaximaux) Soit A un anneau commutatif unitaire.

On dit que deux idéaux I et J de A, sont comaximaux si $I + J = A$.

Remarque 5.3 Soit A commutatif unitaire.

- *Deux idéaux maximaux de A distincts, sont comaximaux.*
- *Il existe des couples d'idéaux comaximaux, non maximaux.*
  Par exemple, dans $\mathbb{R}[x, y]$, $I = \langle x \rangle$, $J = \langle y, x + 1 \rangle$, et $(x + 1) - x = 1$ est la relation donnant la comaximalité.

5.2.3 Le théorème des restes chinois

THÉORÈME 5.7 DES RESTES CHINOIS *Soit A un anneau commutatif unitaire et $n \in \mathbb{N}^*$.*

Soit $I_1, \cdots, I_n$ des idéaux de A deux à deux comaximaux.

Alors :

- $I_1 \cdots I_n = \bigcap_{i=1}^{n} I_i$.
- *Le morphisme d'anneaux unitaires :*

$$f : \begin{cases} A & \to & A/I_1 \times \cdots \times A/I_n \\ x & \mapsto & (\overline{x}, \cdots, \overline{x}) \end{cases}$$

est surjectif de noyau $\bigcap_j I_j$.

En particulier, $A/\left(\bigcap_{i=1}^{n} I_i\right) \simeq A/I_1 \times \cdots \times A/I_n$.

Démonstration.

- Par définition, $\prod_{i=1}^{n} I_i \subset \bigcap_{i=1}^{n} I_i$.
  Il s'agit de prouver la réciproque. On la prouve par récurrence sur n.

$$\bigcap_{i=1}^{n+1} I_i = \left(\bigcap_{i=1}^{n} I_i\right) \cap I_{n+1} \subset \left(\prod_{i=1}^{n} I_i\right) \cap I_{n+1} \subset \prod_{i=1}^{n+1} I_i$$

si on sait prouver le résultat pour n. La deuxième inclusion est justifiée par le cas $n = 2$ ci-dessous.

Prouvons l'inclusion dans le cas où $n = 2$. Soit $x \in I_1 \cap I_2$.

Comme I_1, I_2 sont comaximaux, il existe $a_1 \in I_1, a_2 \in I_2$ tels que $1 = a_1 + a_2$, d'où $x = a_1 x + a_2 x \in I_1 I_2$.

- Soit $x \in A$. On a l'équivalence :

$$(f(x) = 0) \quad \text{ssi} \quad \forall i \in [\![1, n]\!], \overline{x} = 0 \text{ dans } A/I_i$$

qui équivaut encore à $x \in \bigcap_{i=1}^{n} I_i$.
Prouvons que f est surjective. Soit $(\overline{x}_1, \ldots, \overline{x}_n) \in A/I_1 \times \cdots \times A/I_n$.
Il s'agit de trouver x tel que $\forall i \in [\![1, n]\!]$, $\overline{x} = \overline{x}_i$ dans A/I_i.
Montrons que I_1 et $\bigcap_{j=2}^{n} I_j$ sont comaximaux.
S'ils ne l'étaient pas, il existerait un idéal maximal m de A tel que $m \supset I_1$ et $m \supset \bigcap_{j=2}^{n} I_j$.
m contient $\bigcap_{j=2}^{n} I_j$ donc il existe $j_0 \in [\![2, n]\!]$ tel que $I_{j_0} \subset m$.
Par récurrence, on voit qu'il suffit de prouver que $J_1 \cap J_2 \subset \mathcal{P}$, $\mathcal{P}$ premier, implique que $J_1 \subset \mathcal{P}$ ou $J_2 \subset \mathcal{P}$.
Si ce n'était pas le cas, il existerait $x_1 \in J_1 \setminus \mathcal{P}$, et $x_2 \in J_2 \setminus \mathcal{P}$, mais on aurait $x_1 x_2 \in J_1 J_2 \subset J_1 \cap J_2$, ce qui contredit le fait que $\mathcal{P}$ est premier.
En appliquant cette affirmation à tout $e \in [\![1, n]\!]$, on obtient :

$$I_e \text{ et } \bigcap_{j \neq e} I_j$$

sont comaximaux.
Donc $e \in [\![1, n]\!]$, il existe $\alpha_e \in I_e$ et $\beta_e \in \bigcap_{j \neq e} I_e$, tels que $1 = \alpha_e + \beta_e$.
Posons $x = \beta_1 x_1 + \cdots + \beta_n x_n$. Soit $i \in [\![1, n]\!]$.
Donc, si $j \neq i, \beta_j \in I_i$ d'où $\overline{x} = \overline{\beta}_i \overline{x}_i$.
En outre, pour tout $e \in [\![1, n]\!]$, $x_i = \alpha_e x_i + \beta_e x_i$.
Pour $e = i, \alpha_e = \alpha_i \in I_i$, donc $\overline{x}_i = \overline{\beta}_i \overline{x}_i$, ce qui achève la démonstration. ∎

Exemple :
Résoudre dans $\mathbb{Z}$ le système linéaire d'équations aux congruences suivant :

$$\begin{cases} x & \equiv 1 \mod 3 \\ x & \equiv 3 \mod 5 \\ x & \equiv 0 \mod 7 \end{cases}$$

Le théorème précédent affirme que ce système a une solution unique, modulo 105.

Proposition 5.2 Soit B un anneau intègre commutatif unitaire, A un sous-anneau de B et $c \in B$.

Si c est entier sur A notons $\delta = \min\{\deg(Q), Q \in A[X] \setminus \{0\}, Q(c) = 0\}$.

Il existe $P \in A[X] \setminus \{0\}$ unitaire de degré δ tel que $P(c) = 0$ ssi il existe $P \in A[X]$ tel que $P(c) = 0$ et $ev_c : Q \mapsto Q(c)$ induit un isomorphisme d'anneaux unitaires de $A[X]/\langle p\rangle \to A[c]$.

Dans ce cas, P est unique.

Démonstration.

$\Rightarrow$ On a déjà montré que ev_c est un morphisme d'anneaux unitaire surjectif.
Par les théorèmes d'isomorphisme, il suffit de vérifier que $\mathrm{Ker}(ev_c) = \langle P\rangle$.
Par hypothèse, $ev_c(P) = P(c) = 0$ donc $P \in \mathrm{Ker}(ev_c)$.
Or $\mathrm{Ker}(ev_c)$ est un idéal de $A[X]$ donc $\langle P\rangle \subset \mathrm{Ker}(ev_c)$.
Réciproquement, soit $Q \in \mathrm{Ker}(ev_c)$, $ev_c(Q) = 0 = Q(c)$ donc, comme P unitaire, on peut diviser Q par P.
On a donc $Q = PQ_0 + R$ et $\deg(R) < \delta$.
D'où $0 = Q(c) = P(c)Q_0(c) + R(c) = R(c)$.
Si $R \neq 0$, ça contredit la minimalité de P donc $R = 0$ donc $Q \in \langle P\rangle$.

$\Leftarrow$ Comme c est entier dans A, il existe un polynôme $\widetilde{P} \in A[X] \setminus \{0\}$ unitaire tel que $\widetilde{P}(c) = 0 = ev_c(\widetilde{P})$.
Par le lemme de factorisation, ev_c se factorise sur $A[X]/\langle P\rangle$.
Comme $\widetilde{P} \in \mathrm{Ker}(ev_c)$, on en déduit qu'il existe $Q \in A[X]$ tel que $\widetilde{P} = PQ$.
Comme B est intègre, on en déduit que le cœfficient dominant de $\widetilde{P}$ qui est inversible, est le produit de ceux de P et Q donc le cœfficient dominant de P est inversible.
Donc P est unitaire et $P(c) = 0$.
Comme $\mathrm{Ker}(ev_c) = \langle P\rangle$, on remarque que tout polynôme Q tel que $Q(c) = 0$ est bien divisible par P donc $\deg(P) = \delta$ donc est de degré minimal parmi les polynômes s'annulant en c. ∎

Remarque 5.4 (Hors programme) Soit k un corps commutatif et unitaire.

L'ensemble $\hom(\frac{k[X_1,\cdots,X_n]}{I}, k)$ *se dessine.*

Comme $k[X_1, \cdots, X_n]$ est nœtherien, il existe $f_1, \cdots, f_n \in k[X_1, \cdots, X_m]$ tel que $I = \langle f_1, \cdots, f_m\rangle$.

On peut également considérer l'ensemble $Sol(I, k) = \{x \in k^n, 0 = f_1(x) = \cdots = f_m(x)\}$.

Par exemple, si $f = x^2 + y^2 - 1$ avec $k = \mathbb{R}$ et $Sol(f, \mathbb{R})$ est le cercle de centre O et de rayon 1.

On a une bijection entre $\hom(\frac{k[X_1,\cdots,X_n]}{I}, k)$ *et* $Sol(I,k)$ *par* $\varphi \mapsto (\varphi(x_i))_i$ *avec* x_i *la classe de* X_i *dans* $k[X_1,\cdots,X_m]/I$.

Chapitre 6

Corps finis

Définition 6.1 On appelle corps fini ben un corps fini...

Remarque 6.1 Un corps fini est de caractéristique $p \neq 0$ et est muni d'une structure de $\mathbb{F}_p$-espace vectoriel.

Proposition 6.1 Soit k un corps fini de caractéristique p. Il existe $r \geqslant 1$ tel que $\mathrm{Card}(k) = p^r$.

Démonstration. $r = \dim_{\mathbb{F}_p}(k)$ qui est finie car sinon, on aurait une famille libre infinie. ∎

THÉORÈME 6.1 *Si k est un corps fini, $(k^\times, \cdot)$ est un groupe cyclique d'ordre* $\mathrm{Card}(k) - 1$.

Remarque 6.2 En particulier, il est abélien.

Démonstration. $k^\times$ est un groupe fini. Notons p^r le cardinal de k.

Donc, d'après un théorème qu'on est censé avoir vu en théorie des groupes, il existe $G_1, \cdots, G_n$ des groupes cycliques de cardinaus $r_1, \cdots, r_n$ avec $r_{i+1} | r_i$ tels que $k^\times \simeq \prod_{i=1}^{n} G_i$.

On a donc $p^r - 1 = \prod_{i=1}^{r} r_i$ donc $r_1 \leqslant p^r - 1$. Si $\alpha \in k^\times$, , $\alpha^{r_1} = 1$.

Or $X^{r_1} - 1$ a au plus r_1 racines mais on en connaît $p^r - 1$ donc $p^r - 1 \leqslant r_1$ et $r_1 = p^r - 1$.

Donc $n = 1$ et k^* est cyclique. ∎

THÉORÈME 6.2 *Tout corps fini est commutatif.*

Proposition 6.2 Soit k un corps fini de caractéristique $p > 0$.

$$\varphi : \begin{cases} k & \to & k \\ x & \mapsto & x^p \end{cases}$$

est un isomorphisme d'anneaux unitaires.

L'ensemble des éléments de k fixés par φ s'identifie à $\mathbb{F}_p$.

Démonstration. C'est le Frobénius. ∎

Définition 6.2 Un corps de caractéristique $p > 0$ où le Frobénius est surjectif est appellé corps parfait.

Exemples : Les corps finis sont parfaits. $\mathbb{F}_p(X)$ ne l'est pas

THÉORÈME 6.3 *Soit k un corps fini de caractéristique p et de cardinal p^r.*

- *Il existe $\alpha \in k^\times$ tel que $k = \mathbb{F}_p[\alpha]$.*
- *Il existe un polynôme unitaire $P \in \mathbb{F}_p[X] \setminus \{0\}$ de degré r irréductible tel que le morphisme d'anneaux ev_α induise par passage au quotient un isomorphisme $\mathbb{F}_p[X]/\langle P\rangle \to k$.*
- *De plus, si P est scindé dans k, l'ensemble de ses racines est l'ensemble des puissances de α : $\{\alpha, \alpha^p, \cdots, \alpha^{p^{r-1}}\}$ ie $P | X^{p^r} - X$ dans $\mathbb{F}_p[X]$.*

Démonstration.

- Soit α un générateur de $k^\times$.
  On va montrer qu'il existe $P \in \mathbb{F}_p[X]$ unitaire de degré minimal tek que $P(\alpha) = 0$, puis montrer que ce degré est r.
  Avec le chapitre précédent, on obtiendra l'isomorphisme.
- Soit l le plus grand entier tel que la famille $\{1, \alpha, \cdots, \alpha^{l-1}\}$ soit libre sur $\mathbb{F}_p$.
  Par maximalité de l, $\{1, \alpha, \cdots, \alpha^l\}$ est liée donc il existe $(a_0, \cdots, a_l)$ non tous nuls tels que $\sum_{i=0}^{l} a_i \alpha^i$.
  Si $a_l = 0$, par liberté de $(1, \cdots, \alpha^{l-1})$ les a_i sont tous nuls. Donc $a_p \neq 0$.
  Donc $\alpha^l + \sum_{i=0}^{l-1} \frac{a_i}{a_l} \alpha^i = 0$.
  Posons $P = X^l + \sum_{i=0}^{l-1} \frac{a_i}{a_l} X^i$. P est unitaire, de degré l et $P(\alpha) = 0$.
- Montrons que $l = r$. On a déjà $l \leqslant r$.
  De plus, si $\beta \in k$, soit $\beta = 0$ et $\beta \in \text{Vect}\left\{1, \cdots, \alpha^l\right\}$, soit $\beta \in k^\times$ et $\beta = \alpha^k$. (ce qui prouve le premier point)
  En faisant la division euclidienne de X^k par P, on a $\beta = P(\alpha)Q(\alpha) + R(\alpha) = R(\alpha)$ avec $\deg(R) < \deg(P) = l$.
  Donc $\beta \in \text{Vect}\left\{1, \cdots, \alpha^l\right\}$. Donc $(1, \cdots, \alpha^l)$ est génératrice et $r = l$.

- Soit $Q \in \mathbb{F}_p[X]$ unitaire tel que $Q(\alpha) = 0$. $Q = \sum_{i=0}^{q} b_i X^i$.
  Si $q < l$, tous les b_i sont nuls car $(1, \cdots, \alpha^{l-1})$ est libre.
  Donc $Q \neq 0 \Rightarrow q \geqslant l$.
  Donc $l = r = \min\{\deg(Q), Q \in \mathbb{F}_p \setminus \{0\}, Q(\alpha) = 0\}$. D'où le deuxième point.
- Si $P(\alpha) = 0$, $0 = \varphi^k(P(\alpha)) = P(\alpha^{p^k})$.
  Donc $(\alpha, \alpha^p, \cdots, \alpha^{p^k})$ sont des racines de P qui a au plus r racines.
  Donc P est scindé. ■

Remarque 6.3

- *En fait, on a montré que si k est un corps fini de caractéristique p et de dimension r, alors $k = \{P(\alpha) \in \mathbb{F}_p[\alpha], \deg(P) \leqslant r-1\}$ avec α générateur de $k^\times$.*
- *Le polynôme irréductible (unitaire) P et déterminé par la donnée de α. Mais, à priori, il peut exister plusieurs polynomes $Q \in \mathbb{F}_p[X]$ qui réalisent l'isomorphisme $k \simeq \mathbb{F}_p[X]/\langle Q \rangle$ il existe aussi plusieurs choix de α possiblies qui induisent différents polynômes P_α réalisant l'isomorphisme.*
- *Si k est un corps fini de cardinal p^r, alors $X^{p^r} - X$ est scindé sur k. En effet, $X^{p^r} - X = X(X^{p^r-1} - 1)$ qui a pour racines 0 et les racines de $X^{p^r-1} - 1$ qui sont les éléments de $k^\times$.*

THÉORÈME 6.4 (EXISTENCE ET UNICITÉ DES CORPS FINIS) *Soit p un nombre premier et $r \in \mathbb{N}^*$. À isomorphisme près, il existe un unique corps fini de cardinal p^r.*

Démonstration.

∃ On a vu que si k est un corps de cardinal p^r, il existe un isomorphisme d'anneaux unitaires $\mathbb{F}_p[X]/P_\alpha \to k$ avec α un générateur de $k^\times$ et P_α irréductible.
Réciproquement, si $P \in \mathbb{F}_p[X]$ est irréductible et de degré r, on sait que $\mathbb{F}_p[X]/\langle P \rangle$ est un corps de cardinal p^r. Il suffit donc de prouver l'existence d'un $P \in \mathbb{F}_p[X]$ irréductible. (Voir TD)

! Soit p un nombre premier et $r \in \mathbb{N}^*$.
On veut montrer que si k et k' sont deux corps finis de cardinal p^r, il existe un isomorphisme d'anneaux unitaires de k dans k'.
Soit k un corps fini de cardinal p^r. On a $k = \mathbb{F}_p[X]/\langle P \rangle$.
Soit Q un polynôme irréductible de $\mathbb{F}_p[X]$ de degré r.
On est ramené à prouver que $k \simeq \mathbb{F}_p[X]/\langle Q \rangle$.
D'après la preuve précédente, $Q | X^{p^r} - X$ dans $\mathbb{F}_p[X]$. Or ce dernier est scindé dans k et Q le divise dans $k[X]$ donc Q est scindé dans k.

Soit β une racine de Q.

$$\varphi : \begin{cases} \mathbb{F}_p[X]/\langle Q\rangle & \to & k \\ R & \mapsto & R(\beta) \end{cases}$$

est l'isomorphisme recherché. ■

Exemple : Calculer le corps à 4 éléments.

Ce corps est de caractéristique 2, donc on le construit comme quotient de $\mathbb{F}_2[X]$ par $P = X^2 + bX + c$ irréductible. On doit avoir $c \neq 0$ et $b = 2 + b \neq 0$ donc $P = X^2 + X + 1$ est irréductible.

C'est donc $\mathbb{F}_2[X]/\langle X^2 + X + 1\rangle = \{0, 1, X, 1 + X\}$.

Chapitre 7

Localisation d'anneaux

Dans ce chapitre, A est un anneau commutatif unitaire.

Le but du chapitre est de formaliser la construction algébrique qui permet de passer de $\mathbb{Z}$ à $\mathbb{Q}$.

7.1 Définition de la localisation

Définition 7.1 (Partie multiplicative) On dit que $S \subset A$ non vide est multiplicative ssi $1 \in S$, S est stable par multiplication et $0 \notin S$.

Exemple : $\mathbb{Z}^*$ est multiplicative.

Définition 7.2 (Localisation d'un anneau par rapport à une partie multiplicative) Soit $S \subset A$ une partie multiplicative.

On note $S^{-1}A = (A \times S)/\sim$ où $\sim$ est définie par

$$(a, s) \sim (a', s') \quad \text{ssi} \quad \exists r \in S, r(as' - a's) = 0$$

Remarque 7.1 Dans le cas non intègre, il ne faut pas oublier le r dans le définition de $\sim$.

Démonstration. C'est bien une relation d'équivalence car la symétrie et la réflexivité sont évidentes et la transitivité se fait :

Si $(a, s) \sim (b, t) \sim (c, u)$, $r_0(as-bt) = 0$ et $r_1(bu-ct) = 0$, on a $atr_0 = bsr_0$ et $bur_1 = ctr_1$ donc $autr_0r_1 = bsr_0ur_1 = sr_0ctr_1$ donc $tr_0r_1(au - cs) = 0$. ■

Définition 7.3 On note $\frac{a}{s}$ la classe de (a, s) dans $S^{-1}A$.

Théorème 7.1

- *Les opérations :*

$$+ : \begin{cases} S^{-1}A \times S^{-1}A & \to & S^{-1}A \\ (\frac{a}{s}, \frac{b}{t}) & \mapsto & \frac{at+bs}{st} \end{cases}$$

$$\cdot : \begin{cases} S^{-1}A \times S^{-1}A & \to & S^{-1}A \\ (\frac{a}{s}, \frac{b}{t}) & \mapsto & \frac{ab}{st} \end{cases}$$

sont bien définies.

- *Elles font de* $(S^{-1}A, +, \cdot)$ *un anneau commutatif unitaire de neutre* $\frac{1}{1}$.
- *L'application :*

$$\varphi : \begin{cases} A & \to & S^{-1}A \\ a & \mapsto & \frac{a}{1} \end{cases}$$

est un morphisme d'anneaux unitaires.

- $\mathrm{Ker}(\varphi) = \bigcup_{s \in S} \{a \in A, as = 0\}$.

Remarque 7.2 Si A est intègre, φ est injectif.

Démonstration.

- Laissé en exo.
- Allélluia !! Il n'a pas voulu démontrer tous les axiomes !
- Je laisse tomber.
- Soit $a \in A$.
  $a \in \mathrm{Ker}(\varphi)$ ssi $\varphi(a) = \frac{0}{1}$ ssi $\frac{a}{1} = \frac{0}{1}$ ssi $\exists s \in S, sa = 0$
  Donc $\mathrm{Ker}(\varphi) = \bigcup_{s \in S} \{a \in A, sa = 0\}$. ■

Exemple : $\mathbb{Q}$ est la localisation de $\mathbb{Z}$ par rapport à $\mathbb{Z} \setminus \{0\}$.
Si $f \in A$ est nilpotent, on pose $S = \{f^i, i \in \mathbb{N}\}$. $S^{-1}A \simeq A[X]/\langle fX - 1\rangle$.

THÉORÈME 7.2 (PROPRIÉTÉ UNIVERSELLE DE LA LOCALISATION) *Soit A un anneau commutatif unitaire et S une partie multiplicative de A. Posons $\varphi : a \mapsto \frac{a}{1}$.*

- *Pour tout $s \in S$, $\varphi(s) \in (S^{-1}A)^\times$.*
- *Si $f : A \to B$ est un morphisme d'anneaux unitaires tel que pour tout $s \in S$, $f(s) \in B^\times$, il existe un unique morphisme d'anneaux unitaires $\overline{f} : S^{-1}A \to B$ tel que $f = \overline{f} \circ \varphi$.*

Remarque 7.3 Ce théorème définit la localisation à isomorphisme près.

Démonstration.

- L'inverse de $\frac{s}{1}$ est $\frac{1}{s}$.
- On pose :

$$\overline{f} : \begin{cases} S^{-1}B & \to & B \\ \frac{a}{s} & \mapsto & f(a)f^{-1}(s) \end{cases}$$

$\overline{f}$ est bien définie et on a donc l'existence.
Soit g un autre truc qui marche.

$g(\frac{a}{s}) = g(\frac{a}{1}\frac{1}{s}) = g(\frac{a}{1})g(\frac{s}{1})^{-1} = f(a)f(s)^{-1}$. Et bim. ■

Définition 7.4 (Corps des fractions) Soit A un anneau commutatif unitaire intègre.

On appelle corps des fractions de A l'anneau $S^{-1}A$ avec $S = A \setminus \{0\}$. On le note $\mathrm{Frac}(A)$.

Remarque 7.4 Si A intègre, $\mathrm{Frac}(A)$ *est un corps commutatif.*

Exemples : $\mathbb{Q} = \mathrm{Frac}(\mathbb{Z})$ et $k(X) = \mathrm{Frac}(k[X])$.

Remarque 7.5 (Hors programme) Soit X un espace topologique. On appelle chaîne de fermés de X de longueur n toute suite $Z_0 \subsetneq Z_1 \subsetneq \cdots \subsetneq Z_n$ croissante de fermés irréductibles.

On appelle dimension de X la borne supérieure dans $\overline{\mathbb{R}}$ des longueurs des chaînes de fermés.

On appelle degré de transcendance de L/K le plus grand entier n tel que L soit algébrique sur $k(x_1, \cdots, x_n) = \mathrm{Frac}(k[x_1, \cdots, x_n])$ où les x_i sont algébriquement indépendants dans k.

Théorème 7.3 (De normalisation de Nœther) *Soit k un corps et A une k-algèbre isomorphe à $k[T_1, \cdots, T_n]/I$ intègre.*

$\mathrm{Sp}(A)$ *est de dimension finie qui vaut le degré de transcendance de l'extension* $\mathrm{Frac}(A)/k$

$\mathbb{R}[X, Y]$ *correspond en géométrie au plan $\mathbb{R}^2$.*

L'idéal $\langle X^2+Y^2-1\rangle$ correspond au niveau des anneaux à $\mathbb{R}[X, Y]/\langle X^2 + Y^2 - 1\rangle$ et au niveau de la géométrie au cercle d'équation $x^2 + y^2 = 1$.

On remarque qu'on peut emboîter seulement 3 fermés (les idéaux précédents : $V(\langle X, Y - 1\rangle) \subsetneq V(\langle X^2 + Y^2 - 1\rangle) \subsetneq V(0) = \mathrm{Sp}(\mathbb{R}[X, Y])$.

Donc $\dim(\mathbb{R}[X, Y]) = 2$. *On a de même* $\dim(\mathbb{R}[X, Y]/\langle X^2+Y^2-1\rangle) = 1$.

L'idéal $\langle X, Y - 1\rangle$, correspond du point de vue des anneaux à $(\mathbb{R}/\langle X^2 + Y^2 - 1\rangle)/\langle \overline{X}, \overline{Y} - 1\rangle \simeq \mathbb{R}$ qui correspond, en géométrie à un point du cercle.

Chapitre 8

Anneaux factoriels

8.1 Divisibilité

Définition 8.1 Soit A un anneau unitaire et commutatif.

On dit que a divise b (ou que b est divisible par a) ssi il existe $c \in A$ tel que $b = ac$.

On notera $a|b$.

Remarque 8.1 $a|0$ *pour tout* $a \in A$. *Pour tout* $\alpha, a \in A^\times \times A$, $\alpha|a$.

La relation $|$ *est réflexive et transitive.*

Définition 8.2 On définit la relation binaire sur A : $a\mathcal{R}b$ ssi $\langle a\rangle = \langle b\rangle$. On dit alors que a et b sont associés.

Proposition 8.1 C'est une relation d'équivalence.

Lemme 8.0.1
Soit A un anneau commutatif unitaire intègre, $a, b \in A$.

$a\mathcal{R}b \quad$ ssi $\quad \exists c \in A^\times, a = bc$.

Démonstration. Si $a = bc$ avec $c \in A^\times$, $\langle a\rangle \subset \langle b\rangle$ et $b = c^{-1}a$ donc $\langle b\rangle \subset \langle a\rangle$.

Réciproquement, si $\langle a\rangle = \langle b\rangle$, soit $a = 0$, alors $\langle b\rangle = 0$ donc c'est bon.

Si $a \neq 0$, il existe $c, c' \in A$ tel que $a = bc$ et $b = c'a$. On a $a = c'ca$ donc $a(1 - c'c) = 0$. Par intégrité, $c'c = 1$ donc $c \in A^\times$. ∎

Remarque 8.2 *Soit* A *un anneau commutatif intègre.*

- *Pour tout* $(a, b) \in A$,

$$\begin{cases} a|b \\ b|a \end{cases} \quad \text{ssi} \quad a\mathcal{R}b$$

- *Pour tout* $a \in A$, $a \in A^\times \quad$ ssi $\quad \forall b \in A, a|b$.

Exemples :

- Les éléments irréductibles de $\mathbb{Z}$ sont les nombres premiers et leurs opposés.
- Un corps ne contient pas d'éléments irréductibles.
- Les éléments irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.

Proposition 8.2 Soit A un anneau commutatif intègre unitaire et $a \in A$.

a est irréductible dans A ssi l'idéal $\langle a \rangle = aA$ est un idéal propre non nul qui n'est contenu sans aucun autre idéal principal propre non nul de A.

Démonstration.

$\Leftarrow$ Si $aA = A$, a est inversible donc $aA \neq A$.
Si $aA = \langle 0 \rangle$, $a = 0$. Donc aA est propre non nul.
S'il existe $b \in A$ non nul et non inversible tel que $\langle a \rangle \subset \langle b \rangle$.
Il existe c tel que $a = bc$.
Donc $A^\times \cap \{b, c\} \neq \varnothing$. Comme $b \notin A^\times$, $c \in A^\times$. Donc $\langle b \rangle = \langle a \rangle$.

$\Rightarrow$ On a comme précédemment $a \neq 0$ et $a \notin A^\times$.
Soient $b, c \in A$. Si $a = bc$, $\langle a \rangle \subset \langle b \rangle$.
Si $\langle b \rangle = A$, $b \in A^\times$, sinon, $\langle a \rangle = \langle b \rangle$ donc $c \in A^\times$. ∎

Proposition 8.3 Soit A un anneau commutatif unitaire intègre, $a \in A^*$.

Si $\langle a \rangle$ est premier, a est irréductible.

Remarque 8.3 La réciproque est fausse en général.

Démonstration. $a \neq 0$ par hypothèse, $a \notin A^\times$ car aA premier.

Soient $(b, c) \in A$ tel que $a = bc$. $bc \in aA$ or aA est premier donc $b \in aA$ ou $c \in aA$.

On peut supposer $b \in aA$ donc $b = ad$ donc $a = adc$ donc, par intégrité, $dc = 1$ donc c est inversible. ∎

Définition 8.3 On note $\mathrm{Irr}(A)$ l'ensembles des éléments irréductibles de A.

Définition 8.4 (factorisation en éléments irréductibles) Soit A un anneau commutatif unitaire intègre. Soit $a \in A^*$.

On appelle factorisation de A en élément irréductibles la donnée d'un entier $n \in \mathbb{N}$ et d'une application $q : [\![0, n]\!] \to A$ tel que $q_0 \in A^\times$, $q([\![1, n]\!]) \subset \mathrm{Irr}(A)$ et $a = \prod_{i=0}^{n} q_i$.

On dit que deux factorisations p et q sont équivalentes ssi $n = m$, $q_0 p_0^{-1} \in A^\times$ et il existe $\sigma \in \mathfrak{S}_n$ tel que $(q_1, \cdots, q_n) = (r_1 p_{\sigma(1)}, \cdots, r_n p_{\sigma(n)})$ avec $(r_1, \cdots, r_n)$ inversibles.

Remarque 8.4

- *Les p_i peuvent être égaux.*

- *On a une surjection $\chi : A \to A/\mathcal{R}$.*
  Deux factorisations sont égales ssi elles sont définies sur $[\![0, n]\!]$, $\chi \circ p = \chi \circ q$ et pour tout $r \in \mathrm{Irr}(A)$, $\chi(r) \in \mathrm{Irr}(\chi \circ p) \Rightarrow \mathrm{Card}((\chi \circ p)^{-1}(\chi(r))) = \mathrm{Card}((\chi \circ q)^{-1}(\chi(r)))$.

Définition 8.5 (Système de représentants des irréductibles) Soit A un anneau commutatif unitaire intègre. On dit qu'une partie S de A est un système de représentant des irréductibles de A ssi pour tout $r \in \mathrm{Irr}(A)$, il existe un unique $(u, s) \in A^\times \times S$ tel que $r = us$.

Remarque 8.5 Un tel système existe toujours.

Définition 8.6 Soit A un anneau commutatif unitaire intègre et S un système de représentants de A.

Soit $\mathbb{N}^{(S)}$ l'ensembles des applications presques nulles de $S \to \mathbb{N}$.

Notons :

$$\phi_S : \begin{cases} A^\times \times \mathbb{N}^{(S)} & \to & A \setminus \{0\} \\ (u, f) & \mapsto & u \prod_{s \in S} s^{f(s)} \end{cases}$$

Lemme 8.0.2

Soit A un anneau commutatif unitaire intègre. LASSE[1] :

- Pour tout système de représentants S des irréductibles de A, φ_S est bijective
- Il existe un système S de représentants des irréductibles de A tel que ϕ_S est bijective.
- Tout élément $a \in A$ non nul possède une factorisation unique à permutation près en éléments irréductibles.

Démonstration.

$1 \Rightarrow 2$ Clair

$2 \Rightarrow 3$ Aussi

$3 \Rightarrow 1$ De même ∎

Définition 8.7 (Anneau factoriel) Soit A commutatif unitaire intègre. On dit que A est factoriel ssi A est intègre et tout élément de A admet une unique décomposition en éléments irréductibles (à permutation près).

Remarque 8.6 On peut se dispenser d'introduire la notion de système de représentants des irréductibles de A. Mais dans ce cas, l'écriture n'est pas uniqur.

Définition 8.8 (Valuation p-adique) Soit A un anneau factoriel et S un système de représentant des irréductibles de A.

1. Les assertions suivantes sont équivalentes

Tout élément $a \in A^*$ s'écrit de manière unique sous la forme $u\prod_{s\in S} s^{v_s(a)}$.

Si $p \in \mathrm{Irr}(A)$, l'entier $v_p(a)$ est appelé valuation p-adique de a.

Remarque 8.7 *$v_s(a)$ ne dépend que de la classe de s modulo $\mathcal{R}$.*

Lemme 8.0.3 (Propriétés des valuations p-adiques)
Soit A un anneau factoriel et S un système de représentants des irréductibles de A.

Pour tout $r \in S$ et $a, b \in A^*$,
$v_r(ab) = v_r(a) + v_r(b)$ et $v_r(a+b) \geqslant \min(v_r(a), v_r(b))$.
Si $v_r(a) \neq v_r(b)$, $v_r(a+b) = \min(v_r(a), v_r(b))$.
Enfin, $r|a$ ssi $v_r(a) > 0$.

Démonstration. Écrire les décompositions et regarder. ∎

Définition 8.9 (Éléments premiers entre eux) Soit A un anneau commutatif unitaire intègre et $a, b \in A$.

On dit que a et b sont premiers entre eux ssi, pour tout $d \in A$, $d|a$ et $d|b$ implique $d \in A^\times$.

Proposition 8.4 Soit A un anneau commutatif unitaire intègre où il y a existence de la factorisation.

A est factoriel ssi $\forall p \in \mathrm{Irr}(A), \forall a, b \in A$, $p|ab \Rightarrow p|a$ ou $p|b$ (lemme d'Euclide) ssi ($\forall p \in A$, $p \in \mathrm{Irr}(A)$ ssi $\langle p\rangle \in \mathrm{Sp}(A)$) ssi $\forall a, b, c \in A$, $a|bc$ et a premier avec b implique $a|c$ (théorème de Gauss).

Démonstration. Soit $a = u\prod_{s\in S} s^{v_s(a)}$, $b = v\prod_{s\in S} s^{v_s(b)}$ et $c = w\prod_{s\in S} s^{v_s(c)}$.

$2 \Rightarrow 1$ Si $a = u'\prod_{s\in S} s^{\omega_s(a)}$.

Soit $s_0 \in S$ tel que $v_{s_0}(a) > 0$. $s_0 \left| \prod_{s\in S} s^{\omega_s(a)} \right.$. On en déduit $\omega_{s_0}(a) > 0$.

Comme A est intègre, on peut simplifier par $s_0$dans les deux écritures et on conclut par récurrence sur le nombre de facteurs.

$1 \Rightarrow 3$ Montrons que $p \in \mathrm{Irr}(A) \Rightarrow \langle p\rangle$ premier.

Soit $ab \in \langle p\rangle$. On a $v_p(ab) = v_p(a) + v_p(b) > 0$.

Comme $v_p(a) \geqslant 0$ et $v_p(b) \geqslant 0$, $v_p(a) > 0$ ou $v_p(b) > 0$. Donc $p|a$ ou $p|b$.

$3 \Rightarrow 4$ Si $a|bc$, soit $a \in A^\times$ et $a|c$, soit $a \notin A^\times$ et il existe $p \in \mathrm{Irr}(A)$ tel que $p|a$.

Soit $r \in \mathrm{Irr}(A)$ tel que $v_r(a) > 0$. Comme $a|bc$, $r|bc$ sonc $bc \in \langle r\rangle$. Par 3, $b \in \langle r\rangle$ ou $c \in \langle r\rangle$.

Donc $v_r(b) > 0$ ou $v_r(a) > 0$.

Comme A est intègre, en divisant a et bc par r, on conclut par récurrence sur le nombre de facteurs irréductibles comptés avec multiplicité.

$4 \Rightarrow 2$ Clair ∎

Définition 8.10 (PGCD,PPCM) Soit A un anneau factoriel et S un système de représentants des irréductibles de A et $a, b \in A^*$.

On définit le pgcd et le ppcm de a et b par :

$$a \wedge b = \prod_{s \in S} s^{\min(v_s(a), v_s(b))}$$

$$a \vee b = \prod_{s \in S} s^{\max(v_s(a), v_s(b))}$$

8.2 Anneaux factoriels et localisation

Lemme 8.0.4
Soit A un anneau commutatif intègre unitaire et $S \subset A$ une partie multiplicative.

- Le morphisme
$$\varphi : \begin{cases} A & \to & S^{-1}A \\ a & \mapsto & \frac{a}{1} \end{cases}$$
est injectif
- Soit $K = \mathrm{Frac}(A)$. $S^{-1}A$ s'identifie à un sous-anneau de K qui contient A.

Démonstration.

- $\mathrm{Ker}(\varphi) = \bigcup_{s \in S} \{a \in A, as = 0\}$.
Si $a \in \mathrm{Ker}(\varphi)$, il existe $s \in S$, $as = 0$. Comme A est intègre et que $s \neq 0$, $a = 0$.
- En remarquant que $\mathrm{Frac}(A) = T^{-1}A$ avec $T = A^*$, $\mathrm{Id} : S^{-1}A \to T^{-1}A$ est injectif cat sa composée avec φ est la localisation en T.
Id identifie donc $S^{-1}A$ à son image et l'image de A par $\mathrm{Id} \circ \varphi$ est contenue dans l'image par Id de $S^{-1}A$. ∎

Proposition 8.5 Soit A un anneau factoriel et $S \subset A$ une partie multiplicative.

- Les éléments irréductibles de $S^{-1}A$ sont, à un facteur $d \in (S^{-1}A)^\times$ près, les irréductibles de A qui ne divisent aucun élément de S.
- $S^{-1}A$ est factoriel.

Démonstration.

- On a déjà $\frac{a}{s} \in S^{-1}A$ est irréductible ssi $\frac{a}{1}$ l'est. En effet, si $\frac{a}{1} = \frac{b}{s}\frac{c}{t}$, $ast = bc$ donc $s|c$ et $t|b$.
  On a $c = sc'$ et $b = tc'$ donc $a = b'c'$, donc comme a est irréductible, b' ou c' l'est donc $\frac{b}{s} = \frac{b't}{s}$ l'est ou $\frac{c}{t} = \frac{c's}{t}$ l'est.
  Et l'autre sens est débile.
  Soit $a \in A$. $\frac{a}{1} \in (S^{-1}A)^\times$ ssi il existe $s \in S$ tel que a divise s.
  Si $\frac{a}{1}$ est inversible, on a $\frac{b}{t} \in S^{-1}A$ avec $b \wedge t = 1$ tel que $\frac{a}{1}\frac{b}{t} = \frac{1}{1}$. Donc $ab = t$ et $a|t$ avec $t \in S$.
  Réciproquement s'il existe s tel que $a|s$, il existe $b \in A$ tel que $s = ab$. Dans $S^{-1}A$, on a $\frac{s}{1} = \frac{ab}{1}$ donc, comme $\frac{s}{1}$ est inversible, $\frac{a}{1}\frac{b}{s} = \frac{1}{1}$. Donc $\frac{a}{1}$ est inversible.
- Soit $a \in A$ et $s \in S$. A est factoriel donc $a = u\prod_{i=1}^{n} p_i$.
  On a donc $\frac{a}{s} = \frac{1}{s}\frac{u}{1}\prod_{i=1}^{n}\frac{p_i}{1}$.
  Il y a un p_i non inversible sinon a le serait donc on a l'existence.
  Soit deux décompositions de $\frac{a}{s}$:

$$\frac{b}{t}\prod_{i=1}^{m}\frac{p_i}{1} = \frac{a}{s} = \frac{c}{u}\prod_{i=1}^{n}\frac{q_i}{1}$$

  Comme A est intègre, $bu\prod_{i=1}^{m} p_i = ct\prod_{i=1}^{n} q_i$
  Par Gauss, $p_i|c$ ou $p_i|t$. Donc $\frac{c}{1} = \frac{v}{1}\frac{p_i}{1}$ ou $\frac{t}{1} = \frac{v'}{1}\frac{v'}{1}$.
  Donc $\frac{p_i}{1} \in (S^{-1}A)^\times$ et on a une contradiction.
  Donc $p_i|q_{j_i}$. Par récurrence, on montre que les p_i divisent des q_{j_i} distincts donc par symétrie, $m = n$ et $p_i = q_{j_i}$ pour tout i.
  Donc il y a unicité. ∎

8.3 Anneaux factoriels et anneaux de polynômes

Lemme 8.0.5
Soit k un corps. $k[X]$ est factoriel.

Remarque 8.8 On n'utilise seulement le fait que tous les idéaux de $k[X]$ sont principaux.

Démonstration.

- Soit $\mathcal{A}$ l'ensembles des polynômes qui n'ont pas de déomposition en éléments irréductibles. Supposons $\mathcal{A} \neq \{0\}$.
  Notons $\mathcal{P}_r(\mathcal{A}) = \{\langle a\rangle, a \in \mathcal{A}\}$. On a par hypothèse $\mathcal{P}_r(\mathcal{A}) \neq \{\langle 0\rangle\}$.
  Vérifions que $\mathcal{P}_r(\mathcal{A})$ est inductif.
  Soit $(I_\alpha)_\alpha$ une famille totalement ordonnée d'idéaux de $\mathcal{P}_r(\mathcal{A})$.
  L'union de ces idéaux est un idéaul de $k[X]$. Donc il existe $a \in A$ tel que l'union vaille $\langle a\rangle$. Il existe donc α_0 tel que $a \in I_{\alpha_0}$.
  a et a_{α_0} sont donc associés donc si $a \notin \mathcal{A}$, a_{α_0} aussi d'où la contradiction. Donc $a \in \mathcal{A}$.
  Donc $\mathcal{P}_r(\mathcal{A})$ est inductif donc (lemme de Zorn) il admet un élément maximal $I = \langle b\rangle$.
  On sait que $b \neq 0$ et $b \notin A^\times$.
  Comme $b \in \mathcal{A}$, il existe $b_1, b_2 \in A$ non inversibles tels que $b = b_1 b_2$.
  On a $\langle b\rangle \subsetneq \langle b_1\rangle$ et $\langle b\rangle \subsetneq \langle b_2\rangle$ donc $b_1, b_2 \notin \mathcal{A}$ donc ils possèdent une factorisation, donc $b = b_1 b_2$ aussi, ce qui est une contradiction.
  Donc on a l'existence de la factorisation.
- Pour voir l'unicité, il suffit de vérifier la formule : $\forall a \in A, a \in \mathrm{Irr}(A) \Rightarrow \langle a\rangle$ est premier.
  Soit $a \in \mathrm{Irr}(A)$. Prouvons que $\langle a\rangle$ est maximal.
  $\langle a\rangle$ est un idéal non nul propre de A qui n'est contenu dans aucun idéal principal non nul propre de A. Or ne A possède que des idéaux principaux.
  $\langle a\rangle$ n'est donc contenu dans aucun idéal propre non nul de A donc $\langle a\rangle$ est maximal donc premier. ■

Définition 8.11 (Polynôme primitif) Soit A un anneau factoriel. On dit que $\sum_{i=0}^{n} a_i X^i$ est primitif ssi $n \geqslant 1$ et $\bigwedge_{i=1}^{n} a_i = 1$.

Lemme 8.0.6
Soit A un anneau factoriel et $P, Q \in A[X]$.

- Si P et Q sont primitifs, PQ aussi.
- Soit $K = \mathrm{Frac}(A)$. Si P est primitif, alors pour tout $\lambda \in K$, $\lambda \in A[X]$ ssi $\lambda \in A$.

Démonstration.

- $\deg(PQ) \geqslant 1$ car A est intègre. Supposons $PQ \in aA[X]$ pour $a \in A \setminus A^\times$.
  Comme A est factoriel, il existe $a' \in \mathrm{Irr}(A)$ tel que $a \in a'A \subset a'A[X]$.
  Donc $aA[X] \subset a'A[X]$.
  On peut donc supposer que $a \in \mathrm{Irr}(A)$ (quitte à remplacer a par a').
  Comme A est factoriel, $\langle a\rangle \in \mathrm{Sp}(A)$.

Donc $A[X]/aA[X] \simeq (A/\langle a\rangle)[X]$.
Comme $A/\langle a\rangle$ est intègre, $A[X]/aA[X]$ aussi. Donc $aA[X]$ est premier.
Donc P n'est pas primitif ou Q n'est pas primitif. Contradiction.

- Si$\lambda \in A$, alors $\lambda P \in A[X]$.
  Réciproquement, soit $\lambda \in K$ tel que $\lambda P \in A[X]$.
  Posons $P = \sum_{i=0}^{n} a_i X^i$ et $\lambda = \frac{c}{d}$.
  Pour tout i, $\frac{ca_i}{d} \in A$ donc il existe $b_i \in A$ tel que $\frac{ca_i}{d} = \frac{b_i}{1}$.
  Comme A est intègre, $ca_i = b_i d$.
  Supposons $\lambda \notin A$. Comme A est factorieln il existe $r \in \mathrm{Irr}(A)$ tel que $r|d$.
  Par le lemme d'Euclide, $r|a_i$ donc $r \left| \bigwedge_{i=1}^{n} a_i \right.$ et on a une contradiction. ■

THÉORÈME 8.1 *Soit A un anneau factoriel, de corps des fractions K.*
$P \in A[X] \setminus A$ est irréductible ssi P est primitif et irrductible dans $K[X]$.

Démonstration. Voir TD ■

THÉORÈME 8.2 *Si A est factoriel, alors $A[X]$ l'est.*

Démonstration. Soit $P \in A[X]$.

Si $P \in A$, comme A est factoriel, c'est fini.

Sinon, $P \neq 0$ et $P \notin (K[X])^\times = K^\times$ donc il existe $\lambda \in K^\times$, et des polynôme irréductibles de $K[X]$ tels que $P = \lambda P_1 \cdots P_n$.

On peut supposer les P_i primitifs quitte à changer λ. On conclut que $\lambda \in A$.

Donc, comme A est factoriel, $\lambda = u\lambda_1 \cdots \lambda_n$. On a donc la décomposition de P.

L'unicité est facile. ■

COROLLAIRE 8.1 *Si A est factoriel, pour tout $n \in \mathbb{N}$, $A[X_1, \cdots, X_n]$ l'est.*

8.4 Test d'irréductibilité

THÉORÈME 8.3 (IRRÉDUCTIBILITÉ PAR RÉDUCTION) *Soit A un anneau factoriel de corps des fractions K et $I \in \mathrm{Sp}(A)$.*
Posons $B = A/I$ et $L = \mathrm{Frac}(B)$.
Soit $P = \sum_{i=0}^{n} a_i X^i$ et $\overline{P} = \sum_{i=0}^{n} \overline{a_i} X^i$.
Si $\overline{a_n} \neq 0$ et si $P \in \mathrm{Irr}(L[X])$ alors $P \in \mathrm{Irr}(K[X])$.

THÉORÈME 8.4 (CRITÈRE D'EISENSTEIN) *Soit A un anneau factoriel de corps des fractions K.*

Soit $Q = \sum_{i=0}^{n} a_i X^i$ et $p \in \mathrm{Irr}(A)$.

Si pour tout $i < n$, $p | a_i$, $p \not| a_n$ et $p^2 \not| a_0$, alors $Q \in \mathrm{Irr}(K[X])$.

Chapitre 9

Anneaux principaux et euclidiens

Définition 9.1 Soit A un anneau commutatif unitaire.
A est principal ssi A est intègre et tous ses idéaux sont principaux.
A est euclidien ssi A est intègre et il possède une division euclidienne.

THÉORÈME 9.1 *Euclidien* $\Rightarrow$ *Principal.*

Démonstration. C'est la même que celle de $k[X]$ principal si k l'est. ■

THÉORÈME 9.2 *Principal* $\Rightarrow$ *Factoriel.*

Démonstration. C'est la même que celle de $k[X]$ factoriel si k l'est. ■

Remarque 9.1

- *Il existe des idéaux principaux non euclidiens.*
- $\mathbb{Z}[i]$ *est euclidien.*