Chapitre 3

Géométrie Affine

Sommaire

1 Espaces et sous-espaces affines

2 Géométrie affine analytique

3 Barycentre

3.1 Définition

3.2 Associativité

3.3 Coordonnées barycentriques

Soit $\mathcal{E}$ un espace affine de dimension n et de direction E. Soit $A_0, \ldots, A_n$ des points de $\mathcal{E}$ qui ne sont pas dans un hyperplan affine de $\mathcal{E}$. Alors $(A_0, \overrightarrow{A_0A_1}, \ldots, \overrightarrow{A_0A_n})$ est un repère affine de $\mathcal{E}$. Rappelons que cela signifie que $(\overrightarrow{A_0A_1}, \ldots, \overrightarrow{A_0A_n})$ est une base de E.

Lemme III.1

oit M un point de $\mathcal{E}$ et $(x_1, \ldots, x_n)$ les coordonnées de M. Alors

$$M = \mathrm{bar}\Big((A_0, 1 - \sum_i x_i), (A_1, x_1), \ldots, (A_n, x_n)\Big)$$

Le $(n+1)$-uplet $(1 - \sum_i x_i, x_1, \ldots, x_n)$ est appelé coordonnées barycentriques de M.

Démonstration. La définition des x_i signifie que

$$\overrightarrow{A_0M} = \sum_{i=1}^{n} x_i \overrightarrow{A_0A_i}).$$

En insérant M dans les vecteurs de la somme, on obtient

$$\overrightarrow{A_0M} = \sum_{i=1}^{n} x_i \overrightarrow{A_0M} + \overrightarrow{MA_i}),$$

puis

$$(1 - \sum_i x_i)\overrightarrow{MA_0} + \sum_{i=1}^{n} x_i \overrightarrow{MA_i} = \overrightarrow{0}.$$

□

De manière plus symétrique, les coordonnées barycentriques $(\lambda_0, \ldots, \lambda_n)$ de M sont caractérisées par

$$\sum_i \lambda_i = 1 \qquad M\mathrm{bar}\Big((A_i, \lambda_i)\Big).$$

3.4 Convexité

Pour $A, B \in \mathcal{E}$, on pote

$$[A; B] = \{\bar{(}(A,t),(B,1-t) \,:\, t \in [0;1]\}.$$

Intuitivement, $[A; B]$ est le segment d'extrémités A et B.

Définition III.2: Convexe

Une partie C de $\mathcal{E}$ est dîte *convexe* si pour tout A et B dans C, on a $[A; B] \in C$.

Par associativité du barycentre, une partie convexe de $\mathcal{E}$ est stable par barycentres à coefficients positifs.

Exercice 1. *(i) Montrer que l'intersections de parties convexes est convexe.*

(ii) Trouver deux parties convexes du plan dont la réunion n'est pas convexe.

Soit A une partie quelconque. L'intersection des convexes qui contiennent A est noté $\mathrm{Conv}(A)$. C'est le plus petit ensemble convexe qui contienne A. On l'appelle l'enveloppe convexe de A.

4 Applications Affines

4.1 Définition

Les applications affines sont aux espaces affines ceux que les applications linéaires sont aux espaces vectoriels. Elles ressemblent beaucoup aux applications linéaires mais avec des termes constants en plus.

Définition III.3: Application Affine

Soit $\mathcal{E}$ et $\mathcal{F}$ deux espaces affines de direction E et F. Soit A un point de $\mathcal{E}$ (pensé comme une origine). Une application $f : \mathcal{E} \longrightarrow \mathcal{F}$ est dite *affine* s'il existe une application linéaire $\overrightarrow{f} : E \longrightarrow F$ telle que pour tout $M \in \mathcal{E}$, on a

$$f(M) = f(A) + \overrightarrow{f}(\overrightarrow{AM}). \tag{4.1}$$

L'égalité (4.1) peut aussi s'écrire

$$\overrightarrow{f(A)f(B)} = \overrightarrow{f}(\overrightarrow{AM}). \tag{4.2}$$

Remarquons qu'en fait cette définition ne dépend pas du point A choisit puisque

$$f(M) = f(A)+\overrightarrow{f}(\overrightarrow{AM}) = f(B)+\overrightarrow{f(A)f(B)}+\overrightarrow{f}(\overrightarrow{AM}) = f(B)+\overrightarrow{f}(\overrightarrow{AM})+\overrightarrow{f}(\overrightarrow{AM}) = f(B)+\overrightarrow{f}(\overrightarrow{BM}).$$

L'application $\overrightarrow{f}$ est appelé application linéaire associée à f.

Lemme III.4. *La composé de deux applications affines est une application affine. De plus, l'application linéaire associée s'obtient en composant les applications linéaires associées.*

Démonstration. Laissée en exercice. □

Lemme III.5. *L'image d'un sous-espace affine par une application affine est un sous-espace affine.*

Démonstration. En écrivant le sous-espace affine sous la forme $A+F$ (pour A dans le sous-espace affine et F sa direction), c'est une conséquence immédiate de la formule (4.2). □

4.2 Ecriture matricielle

Soit $\mathcal{E}$ et $\mathcal{F}$ deux espaces affines munis de repères. En particulier on a deux bases des directions E et F. A chaque point M de $\mathcal{E}$, on associe le vecteur $X \in \mathcal{M}_{n1}(\mathbb{R})$ de ses coordonnées. Soit $Y \in \mathcal{M}_{n1}(\mathbb{R})$ le vecteur des coordonnées de $f(M)$. Alors on a

$$Y = T + MX, \tag{4.3}$$

où $T \in \mathcal{M}_{n1}(\mathbb{R})$ est le vecteur des coordonnées de l'image par f du centre du repère de $\mathcal{E}$.
Remarquons que la formule (4.3) est la traduction matricielle de (4.1). Remarquons que la formule (4.3) est proche de la formule pour une application linéaire, avec le terme constant (indépendant de X) en plus.

On suppose ici que $\mathcal{E} = \mathcal{F}$ et que l'on a **un seul repère**. Par la formule (4.3), lorsque l'on a fixé des repères une application affine f correspond à une paire $(M,T) \in \mathcal{M}_n(\mathbb{R}) \times \mathcal{M}_{n1}(\mathbb{R})$. Soit g une seconde application affine correspondant à une paire $(N,U) \in \mathcal{M}_n(\mathbb{R}) \times \mathcal{M}_{n1}(\mathbb{R})$. Alors

$$f \circ g \qquad \text{correspond a} \qquad (MN, MU+T).$$

4.3 Barycentre

Proposition III.6

es applications affines préservent le barycentre. C'est-à-dire, on a la formule suivante :

$$f(\mathrm{bar}\Big((A_0,x_0),(A_1,x_1),\dots,(A_n,x_n)\Big)) = \mathrm{bar}\Big((f(A_0),x_0),(f(A_1),x_1),\dots,(f(A_n),x_n)\Big).$$

Démonstration. Par associativité, il suffit de montrer la proposition pour deux points, cad $n=1$. Posons $G = \mathrm{bar}\Big((A_0,x_0),(A_1,x_1)\Big)$. On a $f(A_0) = f(G) + \overrightarrow{f}\,\overrightarrow{GA_0}$ et $f(A_1) = f(G) + \overrightarrow{f}\,\overrightarrow{GA_1}$. Calculons

$$\begin{aligned} x_0\overrightarrow{f(G)f(A_0)} + x_1\overrightarrow{f(G)f(A_1)} &= x_0\overrightarrow{f}(\overrightarrow{GA_0}) + x_1\overrightarrow{f}(\overrightarrow{GA_1}) \\ &= \overrightarrow{f}(x_0\overrightarrow{GA_0} + x_1\overrightarrow{GA_1}) \\ &= \overrightarrow{f}(\overrightarrow{0}) = \overrightarrow{0}. \end{aligned}$$

□

4.4 Exemples

Soit $\mathcal{E}$ unn espace affine de direction E.
Homothéties. Soit λ un scalaire et O un point $\mathcal{E}$. L'homothétie $h_{\lambda,O}$ de centre O et de rapport λ est l'application de $\mathcal{E}$ dans lui-même définie par

$$\overrightarrow{Oh_{O,\lambda}(M)} = \lambda\overrightarrow{OM}. \tag{4.4}$$

Voici leurs propriétés.

Proposition III.7

oit λ un scalaire et O un point $\mathcal{E}$.

(i) L'application $h_{\lambda,O}$ est une application affine dont l'application linéaire est $\lambda\mathrm{Id}_E$.

(ii) Si $\lambda \neq 1$, toute application affine dont l'application linéaire est $\lambda\mathrm{Id}_E$ est une homothétie.

(iii) Si $\lambda \neq 1$, O est l'unique point fixe de $h_{\lambda,O}$.

Démonstration. D'après (4.4), on a

$$h_{O,\lambda}(M) = O + \lambda\overrightarrow{OM}.$$

La première assertion en découle.
Soit $\lambda \neq 1$. Soit $A \in \mathcal{E}$ et f une application affine dont l'application linéaire est $\lambda\mathrm{Id}_E$. Soit $O = \overline{(}(f(A),1),(A,\lambda)$. Alors $\lambda\overrightarrow{AO} = \overrightarrow{f(A)O}$, c'est-à-dire $O = f(A) + \lambda\overrightarrow{AO}$. En comparant à (4.1), on déduit que O est un point fixe. Mais alors f est l'homothétie de centre O et rapport λ.
Soit $h_{O,\lambda}$ et A un point fixe. Alors Or $f(A) = f(O) + \lambda\overrightarrow{OA} = O + \lambda\overrightarrow{OA} = A$ d'après (4.1). Donc $(\lambda-1)\overrightarrow{OA} = \overrightarrow{0}$ et $O = A$ (car $\lambda \neq 1$). □

Translations. Soit $v \in E$. La translation t_v de vecteur v est l'application de $\mathcal{E}$ dans lui-même définie par

$$\overrightarrow{t_v(M)} = M + v. \tag{4.5}$$

Voici leurs propriétés.

Proposition III.8

oit $v \in E$.

(i) L'application t_v est une application affine dont l'application linéaire est Id_E.

(ii) Réciproquement, toute application affine f telle que $\overrightarrow{f} = \mathrm{Id}_E$ est une translation.

(iii) Deux translations commutent, et même : $t_v \circ t_{v'} = t_{v+v'}$.

Fixons $O \in \mathcal{E}$.

Pour tout $M \in \mathcal{E}$, on part de $M = O + \overrightarrow{OM}$ et on lui applique t_v :

$$M + v = O + v + \overrightarrow{t_v}(\overrightarrow{OM}).$$

Donc $\overrightarrow{t_v}(\overrightarrow{OM}) = \overrightarrow{OM}$ et $\overrightarrow{t_v}$ est l'identité.

Soit f une application affine telle que $\overrightarrow{f} = \mathrm{Id}_E$. Pour tout $M \in \mathcal{E}$, on part de $M = O + \overrightarrow{OM}$ et on lui applique f :

$$f(M) = f(O) + \overrightarrow{OM} = M + \overrightarrow{Mf(O)} + \overrightarrow{OM} = M + \overrightarrow{Of(O)}.$$

Donc f est la translation de vecteur $\overrightarrow{Of(O)}$.

La dernière assertion est évidente.

Démonstration. □

Projections.

Soit $\mathcal{F}$ un sous-espace affine de direction F et G un sous-espace vectoriel de E. On suppose que

$$F \oplus G = E.$$

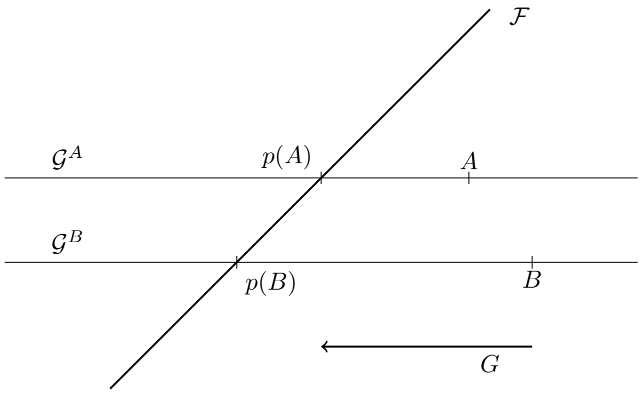
Alors, pour tout $M \in \mathcal{E}$, les sous-espaces affines $\mathcal{F}$ et $M + G$ s'intersectent en un point que l'on note $p_{\mathcal{F},G}(M)$. De plus, l'application

$$p_{\mathcal{F},G} : \begin{array}{ccc} \mathcal{E} & \longrightarrow & \mathcal{E} \\ M & \longmapsto & p_{\mathcal{F},G}(M) \end{array}$$

est une application affine dont l'application linéaire associée est la projection linéaire d'image F et de noyau G. On l'appelle *la projection sur $\mathcal{F}$ parallèlement à G*. Bien sûr, on a :

$$p_{\mathcal{F},G} \circ p_{\mathcal{F},G} = p_{\mathcal{F},G}.$$

Exercice 2. *Construire une application affine dont la partie linéaire est une projection linéaire bien qu'elle ne soit pas une projection affine.*



Symétries. Soit $\mathcal{F}$ un sous-espace affine de direction F et G un sous-espace vectoriel de E. On suppose que

$$F \oplus G = E.$$

Notons p la projection sur $\mathcal{F}$ parallèlement à G.
Alors, pour tout $M \in \mathcal{E}$. On définit un point $s_{\mathcal{F},G}(M)$ (ou $s(M)$) par la relation

$$\overrightarrow{Mp(M)} = \overrightarrow{p(M)s(M)} \qquad \text{cad} \qquad s(M) = p(M) + \overrightarrow{Mp(M)}.$$

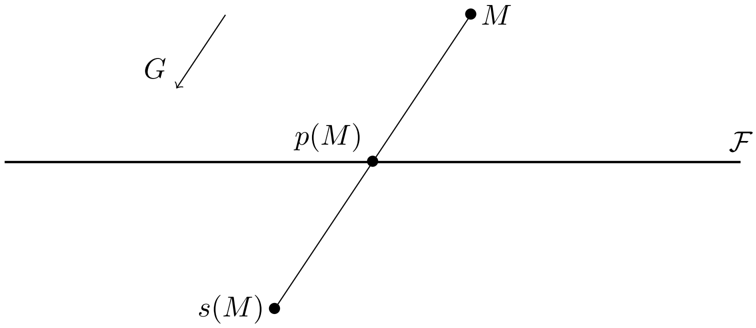
L'application

$$s_{\mathcal{F},G} : \begin{array}{ccc} \mathcal{E} & \longrightarrow & \mathcal{E} \\ M & \longmapsto & s(M) \end{array}$$

est une application affine dont l'application linéaire associée est la symétrie linéaire d'image F et de noyau G. On l'appelle *la symétrie par rapport à $\mathcal{F}$ parallèlement à G*. Bien sûr, on a :

$$s_{\mathcal{F},G} \circ s_{\mathcal{F},G} = \mathrm{Id}_{\mathcal{E}}$$

Exercice 3. *Construire une application affine dont la partie linéaire est une symétrie linéaire bien qu'elle ne soit pas une projection affine.*



5 Quelques théorèmes Classiques

5.1 Théorème de Thalès

Soit A, B et C trois points alignés de $\mathcal{E}$ tels que $A \neq C$. Alors il existe un unique scalaire λ tel que $\overrightarrow{AB} = \lambda \overrightarrow{AC}$. On définit

$$\frac{\overline{AB}}{\overline{AC}} := \lambda.$$

Théorème III.9. Thalès

Soient $\mathcal{H}_1, \mathcal{H}_2, \mathcal{H}_3$ trois hyperplans parallèles et distincts d'un espace affine $\mathcal{E}$ et D, D' deux droites dont aucune n'est faiblement parallèle à $\mathcal{H}_1$. On suppose que $\mathcal{H}_i$ coupe D au point A_i et D' au point B_i. On a alors

$$\frac{\overline{A_1A_2}}{\overline{A_1A_3}} = \frac{\overline{B_1B_2}}{\overline{B_1B_3}}. \tag{5.1}$$

Démonstration. Soit π la projection sur D' parallèlement à $\mathcal{H}_1$. Alors $\pi(A_i) = B_i$ pour tout i. Regardons la relation

$$\overrightarrow{A_1A_2} = \frac{\overline{A_1A_2}}{\overline{A_1A_3}}\overrightarrow{A_1A_3}.$$

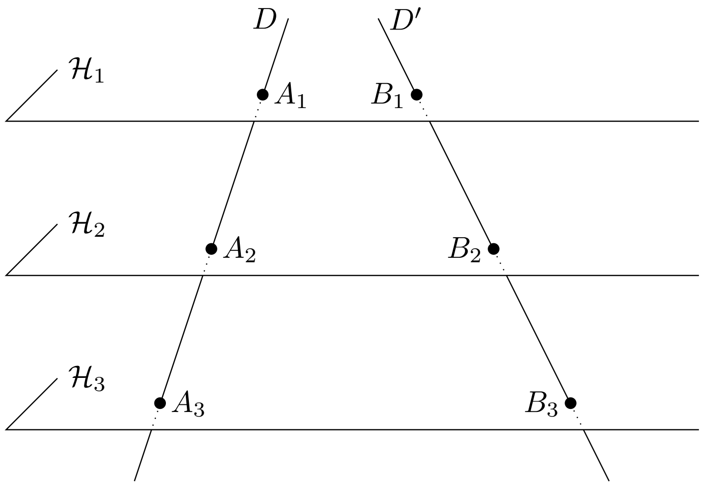
Appliquons lui $\overrightarrow{\pi}$ (qui est linéaire) :

$$\overrightarrow{\pi}(\overrightarrow{A_1A_2}) = \frac{\overline{A_1A_2}}{\overline{A_1A_3}}\overrightarrow{\pi}(\overrightarrow{A_1A_3}).$$

Mais alors

$$\overrightarrow{B_1B_2} = \frac{\overline{B_1B_2}}{\overline{B_1B_3}}\overrightarrow{B_1B_3}.$$

L'égalité du théorème en découle. □



5.2 Théorème de Pappus

Théorème III.10. Pappus

Soit D et D' deux droites distinctes du plan affine. Soit A, B et C (resp. A', B' et C') trois points distincts de D (resp. D'). On suppose qu'aucun des 6 points n'est $D \cap D'$.
Si $(AB')//(A'B)$ et $(CB')//(C'B)$ alors $(AC')//(A'C)$.

Démonstration. On distingue deux cas :

— $D \cap D' = \{O\}$. Soit h_1 l'homothétie de centre O qui envoie A sur B. Soit h_2 l'homothétie de centre O qui envoie B sur C.
Or le théorème de Thalès implique que $h_1(C') = A'$ et $h_2(C') = B'$. Mais alors

$$h_2 \circ h_1(A) = h_2(B) = C$$

et

$$h_1 \circ h_2(C') = h_1(B') = A'.$$

Comme h_1 et h_2 ont le même centre elles commutent : $h_1 \circ h_2 = h_2 \circ h_1 =: h_3$. Donc $h_3((AC')) = h_3((A'C))$.
Comme h_3 est une homothétie, les directions de $(A'C)$ et (AC') sont égales (car $\overrightarrow{h_3}$ est une homothétie linéaire et stabilise tous les sev). Donc $(A'C)//(AC')$.

— $D//D'$. Soit t_1 la translation qui envoie A sur B. Soit t_2 la translation qui envoie B sur C.
Puisque $(ABA'B')$ est un parallélogramme, $\overrightarrow{AB} = \overrightarrow{B'C'}$. De même, $\overrightarrow{BC} = \overrightarrow{C'B'}$. Donc

$$t_2 \circ t_1(A) = t_2(B) = C$$

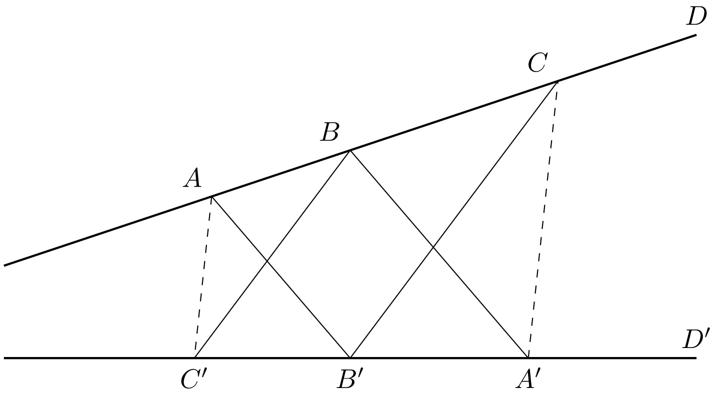
et

$$t_1 \circ t_2(C') = t_1(B') = A'.$$

Comme t_1 et t_2 commutent : $t_1 \circ t_2 = t_2 \circ t_1 =: t_3$. Donc $t_3((AC')) = t_3((A'C))$.
Comme t_3 est une homothétie, les directions de $(A'C)$ et (AC') sont égales (car $\overrightarrow{t_3}$ est une homothétie linéaire et stabilise tous les sev). Donc $(A'C)//(AC')$.

$\square$

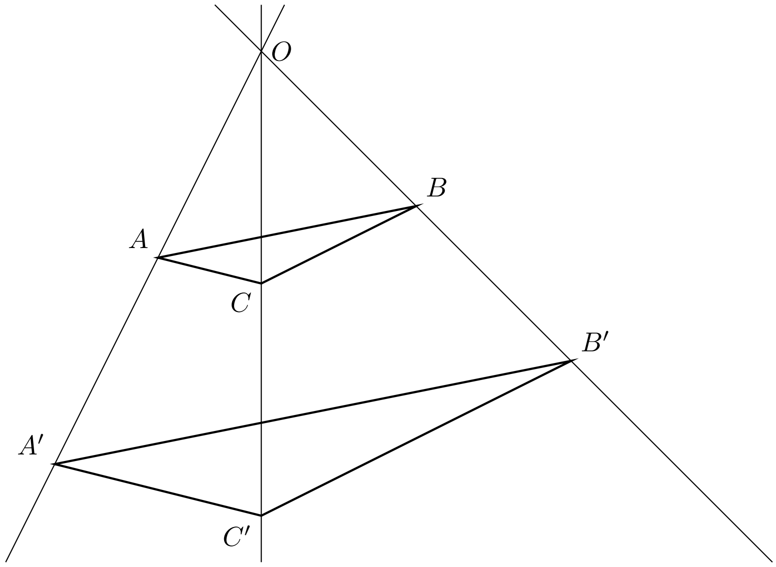
Remarque. Dans cette preuve, une translation joue le rôle d'une homothétie dont le centre serait à l'infini. Cette idée intuitive à laquelle il est difficile de donner un sens précis est pourtant assez riche.



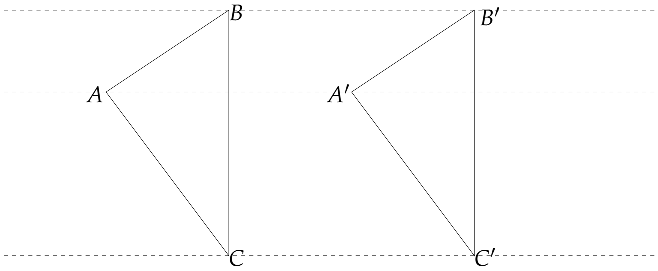
5.3 Théorème de Désargues

Théorème III.11. Désargues

Soit (ABC) et $(A'B'C')$ deux triangles non aplatis. On suppose que $(AB)//(A'B')$, $(BC)//(B'C')$ et $(AC)//(A'C')$.
Alors les trois droites (AA'), (BB') et (CC') sont concourantes ou parallèle.



Démonstration. Nous allons prouvé ce théorème seulement dans un cas particulier : **on suppose que** $(AA')//(BB')$. Dans ce cas on va montré que $(AA')//(CC')$.



Soit t la translation qui envoie A sur A'. Comme $(ABA'B')$ est un parallélogramme, $t(B) = B'$. Donc $t((AC)) = (A'C')$ et $t((BC)) = (B'C')$. Donc $t(C) = C'$ et $\overrightarrow{CC'} = \overrightarrow{AA'}$. Donc $(AA')//(CC')$. $\square$

6 Classification affine des coniques planes

6.1 Le groupe affine

Théorème III.12. Applications affines inversibles

Une application affine de $\mathcal{E}$ dans lui-même est inversible si et seulement son application linéaire associée $\overrightarrow{f}$ l'est. Dans ce cas l'application réciproque f^{-1} est affine.
L'ensemble des applications affines de $\mathcal{E}$ dans lui-même est un groupe nomé le groupe affine et se note $\mathrm{GA}(\mathcal{E})$.

Démonstration. Fixons un repère. En coordonnées, f s'écrit

$$X \longmapsto MX + T.$$

Comme T est constante, $X \mapsto (MX+T)$ est bijective si et seulement si $X \mapsto MX$ l'est. Ceci montre la première assertion.
Supposons M inversible. Posons $Y = MX + T$. Alors $MX = Y - T$ et $X = M^{-1}Y - M^{-1}T$. En particulier, $Y \mapsto X$ est affine. $\square$

6.2 Les coniques

Soit $\mathcal{P}$ un espace affine de dimension deux. On munit $\mathcal{P}$ d'un repère $(A_0, \overrightarrow{A_0A_1}, \overrightarrow{A_0A_1})$ de sorte que les coordonnées fournissent une bijection :

$$\begin{array}{rcl} \mathbb{R}^2 : & \longrightarrow & \mathcal{P} \\ \begin{pmatrix} x \\ y \end{pmatrix} & \longmapsto & A_0 + x\overrightarrow{A_0A_1} + y\overrightarrow{A_0A_1}. \end{array}$$

Définition III.13: Conique

Une *conique* de $\mathcal{P}$ est une partie de $\mathcal{P}$ définie par une équation du type

$$ax^2 + bxy + cy^2 + dx + ey + f = 0 \tag{6.1}$$

avec $(a,b,c,d,e,f) \in \mathbb{R}^6$ tels que $(a,b,c) \neq (0,0,0)$.

Classification. Soit $ax^2 + bxy + cy^2 + dx + ey + f$ l'équation d'une conique. On discute selon le rang de la forme quadratique $Q := ax^2 + bxy + cy^2$. Quitte à multiplier l'équation par -1, on dans l'un des 3 cas suivant :

(i) $\operatorname{rg} Q = 2$ et $\operatorname{sgn} Q = (2,0)$. Après changement linéaire de variable, on obtient :

$$X^2 + Y^2 + dX + eY + f = 0.$$

En changeant X en $(X + \frac{d}{2})$ et Y en $(Y + \frac{e}{2})$, on obtient une équation de la forme

$$X^2 + Y^2 + f = 0.$$

Attention f a changé. Si $f < 0$, on trouve l'ensemble vide. Si $f = 0$, on trouve un point. Si $f > 0$ on trouve une ellipse (en fait un cercle).
Avec un changement de variable $X' = \lambda X$ et $Y' = \lambda Y$, on peut supposer que $f = -1, 0$ ou 1.

(ii) $\operatorname{rg} Q = 2$ et $\operatorname{sgn} Q = (1,1)$. Après changement linéaire de variable, on obtient :

$$XY + dX + eY + f = 0.$$

En changeant X en $(X + e)$ et Y en $(Y + d)$, on obtient

$$XY + f = 0.$$

Si $f \neq 0$, on trouve une hyperbole. Si $f = 0$, on trouve la réunion de deux droites s »canntes.

(iii) $\operatorname{rg} Q = 1$ et $\operatorname{sgn} Q = (1,0)$. Après changement linéaire de variable, on obtient :

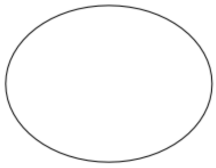
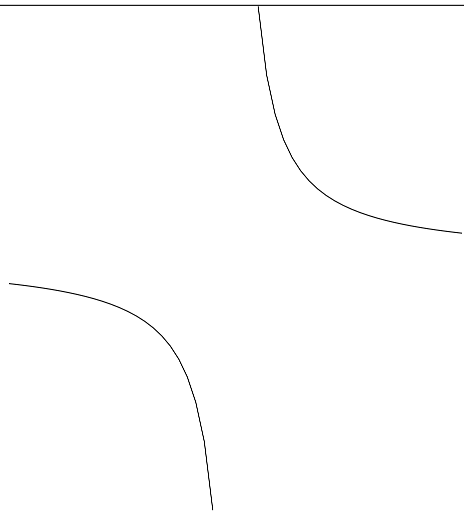
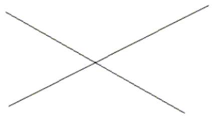
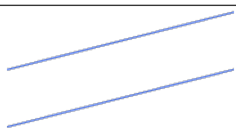
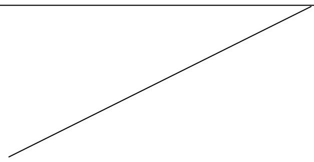
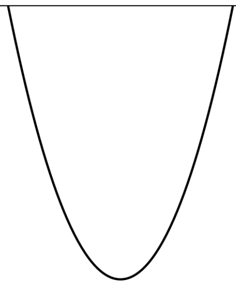
$$X^2 + dX + eY + f = 0.$$

Si $e = 0$ et $f > 0$, on obtient le vide. Si $e = 0$ et $f < 0$, on obtient deux droites parallèles. Si $e = f = 0$, on obtient une droite (double). Supposons maintenant $e \neq 0$. En changeant X en $(X + \frac{d}{2})$ et Y en $\frac{Y-f}{e}$, on obtient une équation de la forme

$$X^2 + Y = 0.$$

On obtient donc une parabole.

Résumons cela dans un tableau.

Q	Équation	Nom	Dessin
$++$ ou $--$	$X^2+Y^2=1$	ellipse	
$++$ ou $--$	$X^2+Y^2=-1$	vide	
$++$ ou $--$	$X^2+Y^2=0$	point	$\times$
$+-$	$XY=1$	hyperbole	
$+-$	XY=0	droites sécantes	
$+$ ou $-$	$X^2+1=0$	vide	
$+$ ou $-$	$X^2-1=0$	2 droites parallèles	
$+$ ou $-$	$X^2=0$	droite double	
$+$ ou $-$	$X^2-Y=0$	parabole	

Chapitre 4

Anneaux et Idéaux

Sommaire

1 Définitions

1.1 Def et Exples

Définition IV.14: Anneau

Soit A un ensemble muni de deux lois internes $+$ et $*$: $(A, +, *)$ est un *anneau* si $(A, +)$ est un groupe abélien (neutre noté 0), $*$ est commutative, associative, distributive par rapport à $+$ et possède un neutre (noté 1).
<u>*Remarque*</u> : Si $*$ est commutative, alors l'anneau est dit *commutatif*.

Remarque. Dans certains ouvrages, on ne demande pas que $*$ soit commutative. Dans ce cas, ce que nous appelons anneau s'appelle anneau commutatif.
La loi $*$ est distributive par rapport à $+$ signifie que pour tout $(x, y, z) \in A^3$, $x * (y + z) = x * y + x * z$ et $(x + y) * z = x * z + y * z$.

Exemples 1. Les ensembles suivants sont des annneaux.

(i) L'ensemble $(\mathbb{Z}, +, \times)$ des entiers relatifs.
Ceci est l'exemple principal qu'il faut toujours garder en tête.

(ii) Les ensembles $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$.
Ces exemples ont une propriété supplémenntaires : tous les éléments de A sauf 0 ont un inverse pour $\times$.

(iii) L'espace des polynômes $\mathbb{R}[X]$.
Ceci est le deuxième exemple à garder en tête.

(iv) Plus compliqué : $\mathbb{R}[X, Y]$ l'anneau des polynômes à 2 variables et coefficients réels.

Les ensembles suivants ne sont pas des annneaux. *Trouver un argument expliquant que ces esembles ne sont pas annneaux.*

Exemples 2. (i) L'ensemble $\mathbb{N}$ des entiers naturels.

(ii) L'ensemble $2\mathbb{Z}$ des entiers pairs.

(iii) L'espace des polynômes $\mathbb{R}_n[X]$ de degré inférieur à n.

(iv) L'ensemble $\mathcal{M}_n(\mathbb{R})$ des matrices.

A chaque fois, les opérations $+$ et $\times$ sont les classiques.

1.2 Premiers constructeurs

Comme pour les groupes, on a une notion de sous-anneau :

Définition IV.15: Sous-Anneau

Soit $(A, +, *)$ un anneau, $B \in \mathcal{P}(A)$: B est un *sous-anneau* de A si $0 \in B$, $1 \in B$ et B est stable pour les lois $+$ et $*$.

Exemples 3. (i) $\mathbb{Z}$ est un sous-anneau de $\mathbb{Q}$.

(ii) $\mathbb{R}$ est un sous-anneau de $\mathbb{R}[X]$.

(iii) $\{\frac{p}{2^n} : p \in \mathbb{Z}\ n \in \mathbb{N}\}$ est un sous-anneau de $\mathbb{Q}$.

(iv) L'ensemble $\mathbb{Z}[i] := \{x + iy : x, y \in \mathbb{Z}\}$ est un sous-anneau de $\mathbb{C}$. Il est appelé l'anneau des entiers de Gauss.

Comme pour les groupes, on a une notion de produit :

Définition IV.16: Produit d'Anneaux

Soit $(A, +, *)$ et $(B, +, *)$ deux anneaux. On munit $A \times B$ des lois et éléments suivants :

$0 := (0, 0)$ et $1 := (1, 1)$.
$(a, b) + (a', b') = (a + a', b + b')$ pour tout $a, a' \in A$ et $b, b' \in B$.
$(a, b) + (a', b') = (a + a', b + b')$ pour tout $a, a' \in A$ et $b, b' \in B$. On obtient ainsi un anneau $(A \times B, +, \times)$.

1.3 L'anneau $\mathbb{Z}/n\mathbb{Z}$

Fixons un entier naturel $n \geqslant 2$. On définit une relation d'équivalence sur $\mathbb{Z}$ (la congruence modulo n) :

$$a \equiv b \iff n \mid a - b.$$

La classe d'équivalence de $a \in \mathbb{Z}$ est la partie suivante

$$a + n\mathbb{Z} := \{a + kn \,:\, k \in \mathbb{Z}\}.$$

Ces classes forment une partition de $\mathbb{Z}$ en n parties deux à deux distinctes :

$$\mathbb{Z} = n\mathbb{Z} \cup (1 + n\mathbb{Z}) \cup \cdots \cup (n - 1 + n\mathbb{Z}).$$

Par définition $\mathbb{Z}/n\mathbb{Z}$ est l'ensemble de ces n parties de $\mathbb{Z}$. Attention, un élément de $\mathbb{Z}/n\mathbb{Z}$ est une partie de $\mathbb{Z}$. En particulier le cardinal de $\mathbb{Z}/n\mathbb{Z}$ est n.
On définit deux opérations $+$ et $\times$ sur $\mathbb{Z}/n\mathbb{Z}$ par les formules suivantes :

$$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) := (a + b) + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$$
$$(a + n\mathbb{Z}) \times (b + n\mathbb{Z}) := (ab) + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$$

pour tout $a, b \in \mathbb{Z}$.
Ces définitions posent une question. En effet, les membres de droite ne doit dépendre que $(a + n\mathbb{Z})$ et $(b+n\mathbb{Z})$. Or à priori, les membres de droite dépendent de a et b, utiles pour calculer $a+b$ et ab. Montrons que ceci n'est qu'apparence pour $+$:
Soit a' et b' dans $\mathbb{Z}$ tels que $a + n\mathbb{Z} = a' + n\mathbb{Z}$ et $b + n\mathbb{Z} = b' + n\mathbb{Z}$. Alors il existe k et l dans $\mathbb{Z}$ tels que $a' = a + nk$ et $b' = b + nl$. Mais alors,

$$a' + b' + n\mathbb{Z} = a + nk + b + nl + n\mathbb{Z} = a + b + n(k + l + \mathbb{Z}) = (a + b) + n\mathbb{Z}.$$

Théorème IV.17. Anneau $\mathbb{Z}/n\mathbb{Z}$

L'ensemble $\mathbb{Z}/n\mathbb{Z}$ muni de ces deux lois $+$ et $\times$ est un anneau.

Démonstration. Chaque identité est une simple vérification laissée en exercice. ☐

Exemple $n = 3$.

Les traits de la graduation représentent les entiers relaturels. Les rouges sont ceux de $3\mathbb{Z}$, les bleus ceux de $1 + 3\mathbb{Z}$ et les verts ceux de $2 + 3\mathbb{Z}$. Le fait que chaque trait est une couleur et une seule dit que ces parties forment une partition des entiers.
Les opérations $+$ et $\times$ sont définie sur ces parties. Si on représente une partie par sa couleur, on obtient

$$
\begin{array}{ccc}
{\color{red}\bullet}+{\color{red}\bullet}={\color{red}\bullet} & {\color{blue}\bullet}+{\color{blue}\bullet}={\color{green}\bullet} & {\color{green}\bullet}+{\color{green}\bullet}={\color{blue}\bullet} \\
{\color{red}\bullet}+{\color{blue}\bullet}={\color{blue}\bullet} & {\color{red}\bullet}+{\color{green}\bullet}={\color{green}\bullet} & {\color{blue}\bullet}+{\color{green}\bullet}={\color{red}\bullet}
\end{array}
$$

De même pour le produit, on obtient :

$$
\begin{array}{ccc}
{\color{red}\bullet}\times{\color{red}\bullet}={\color{red}\bullet} & {\color{blue}\bullet}\times{\color{blue}\bullet}={\color{blue}\bullet} & {\color{green}\bullet}\times{\color{green}\bullet}={\color{blue}\bullet} \\
{\color{red}\bullet}\times{\color{blue}\bullet}={\color{red}\bullet} & {\color{red}\bullet}\times{\color{green}\bullet}={\color{red}\bullet} & {\color{blue}\bullet}\times{\color{green}\bullet}={\color{green}\bullet}
\end{array}
$$

Revenons à $\mathbb{Z}/n\mathbb{Z}$. L'élément $k + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$ est noté $\bar{k}$. En particulier le n est sous-entendu bien que très important.
Les tables d'addition et de multiplication de $\mathbb{Z}/3\mathbb{Z}$ s'écrivent alors :

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

$\times$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$

Exercice 4. *Dresser de même, les tables d'addition et de multiplication de $\mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/4\mathbb{Z}$.*

1.4 Anneaux des polynômes

Soit A un anneau et X un symbole. On pose

$$A[X] := \{\sum_{n=0}^{\infty} a_n X^n \ : \ a_n \in A \quad \text{et } \exists N \quad \forall n \geqslant N a_n = 0\}.$$

La condition sur les coefficients a_n dit que tous sauf un nombre fini sont nuls. Lorsq'on écrit un polynôme, on oublie les termes de la forme $0X^n$, si bien que la somme devient finie. Il est aussi important de comprendre que la somme est formelle. Ce qui signifie que par définition $\sum_{n=0}^{\infty} a_n X^n = \sum_{n=0}^{\infty} b_n X^n$ si et seulement si $a_n = b_n$ pour tout n.
On définit les deux opérations $+$ et $\times$ sur $A[X]$ par les formules suivantes :
Pour

$$P = \sum_{n=0}^{\infty} a_n X^n \qquad Q = \sum_{n=0}^{\infty} b_n X^n,$$

on a

$$P + Q = \sum_{n=0}^{\infty} (a_n + b_n) X^n$$

et

$$PQ = \sum_{n=0}^{\infty} c_n X^n \text{ où } c_n = \sum_{k+l=n} a_k b_l.$$

La formule qui définit c_n a bien un sens car seulement un nombre fini de termes apparaissent. Combien ? Par ailleurs, PQ est bien un polynôme car les c_n sont presque tous nuls.

Proposition IV.18

L'ensemble $(A[X], +, \times)$ est un anneau.

La preuve qui est une simple vérification est laissée en exercice.

Convention. On fait le choix d'omettre $0X^k$, X^0 et de noter $1X^k$ par X^k. Ainsi $1 + X^3 + 2X^6 \in \mathbb{R}[X]$. En effet

$$a_n = \begin{cases} 1 & \text{si } n = 0 \text{ ou } 3 \\ 2 & \text{si } n = 6 \\ 0 & \text{sinon} \end{cases}$$

Fonction associée. Soit $P \in A[X]$. Alors, on obtient une fonction

$$\tilde{P} : A \longrightarrow A,$$

dont la valeur $P(a)$ s'obtient à substituer a à X dans P.
Si $A = \mathbb{R}$, on obtient les fonctions polynômiales que vous connaissez bien. Pour d'autres anneaux, les choses peuvent être plus subtiles.

Exemple 4. Prenons $A = \mathbb{Z}/2\mathbb{Z}$ dont on note les éléments 0 et 1. Alors $P = 1 + X$, $Q = 1 + X^3$ sont deux éléments distincts de $A[X]$ car ils n'ont pas les mêmes coefficients.
On calcule $\tilde{P}(0) = 1$, $\tilde{P}(1) = 1 + 1 = 0$, $\tilde{Q}(0) = 1$ et $\tilde{Q}(1) = 1 + 1 = 0$. Donc les fonctions $\tilde{P}$ et $\tilde{Q}$ sont égales.

1.5 Anneau des entiers de Gauss

L'ensemble $\mathbb{Z}[i] := \{x + iy \ : \ x, y \in \mathbb{Z}\}$ est un sous-anneau de $\mathbb{C}$. Il est appelé l'anneau des entiers de Gauss.

1.6 Petits anneaux

Dans cette section, on étudie les anneaux de petits cardinaux 2,3 et 4.

Proposition IV.19

Dans un anneau $(A, +, \times, 0, 1)$, on a, pour tout $a \in A$:

$$0 \times a = 0 \qquad -1 \times a = -a.$$

Ici, $-a$ signifie l'unique élément tel que $a + (-a) = 0$ (cad l'inverse de a pour la loi $+$).

Démonstration. En effet, $0 \times a = (0 + 0) \times a = 0 \times a + 0 \times a$. Donc $0 \times a$ est l'élément neutre pour $+$, c'est-à-dire 0.
On a aussi $-1 \times a + a = -1 \times a + 1 \times a = (-1 + 1) \times a = 0 \times a = 0$. Donc $-1 \times a$ est bienl'inverse de a pour $+$. □

Exercice 5. *Justifier chacune des égalités de la preuve ci-dessus à l'aide de la définition d'un anneau.*

Cardinal 2. Soit A un anneau à deux éléments. Alors $A = \{0, 1\}$. Ses tables d'addition et de multiplication s'écrivent alors :

$+$	0	1
0	0	1
1	1	0

$\times$	0	1
0	0	0
1	0	1

Les valeurs noires s'obtiennent par définition des éléments neutres ou la proposition ci-dessus. La valeur rouge s'obtient en remarquant que 0 doit apparaître sur la ligne de 1 car 1 a un inverse pour $+$.
Ainsi $\mathbb{Z}/2\mathbb{Z}$ est le seul anneau à 2 éléments.

Cardinal 3. Soit A un anneau à trois éléments. Alors $A = \{0, 1, a\}$. Ses tables d'addition et de multiplication s'écrivent alors :

$+$	0	1	a
0	0	1	a
1	1	a	0
a	a	0	1

$\times$	0	1	a
0	0	0	0
1	0	1	a
a	0	a	1

Les valeurs noires s'obtiennent par définition des éléments neutres ou la proposition ci-dessus. La valeur rouge s'obtient par élimination : $1 + 1 = 1$ est impossible car $1 \neq 0$. Les valeurs vertes s'obtiennent par

symétrie (+ est commutatif) et bijection de l'application $y \mapsto x + y$ est bijective. La valeur verte se justifie ainsi : $a = 1 + 1$; donc $a \times a = (1 + 1) \times a = a + a = 1$.
Ainsi $\mathbb{Z}/3\mathbb{Z}$ est le seul anneau à 3 éléments.

Cardinal 4. A partIr de 4 les choses se compliquent. Il ya 4 possibilités, mais cela est un peu long. Si cela vous amuse vous pouvez essayer de continuer le raisonement ci-dessous, bien que cela puisse être long.
Réciproquement, les pages précédentes de ce chapitre permettent de voir que $\mathbb{Z}/2 \times \mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/4\mathbb{Z}$. Mais il y a d'autres exemples...

Soit A un anneau à quatre éléments. Alors $A = \{0, 1, a, b\}$. Ses tables d'addition et de multiplication s'écrivent alors :

$+$	0	1	a	b
0	0	1	a	b
1	1	$x?$		
a	a			
b	b			

$\times$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a		
b	0	b		

La lettre x ne peut être 1 (chaque ligne est une permutation des éléments de A). Donc, $x = 0, a$ ou b. Quitte à changer les notations (entre a et b) on peut éliminer le dernier cas.

2 Inversibilité et divisibilité

2.1 Inversibilité

Un point important des anneaux est que $-x$ existe toujours alors que x^{-1} par forcément. D'où la définition suivante :

Définition IV.20: Elément inversible

Soit $(A, +, \times, 0, 1)$ un anneau. Un élément $a \in A$ est dit *inversible* s'il existe $b \in A$ tel que $ab = 1$:

$$\exists b \in A \qquad ab = 1.$$

On note A^* l'ensemble des éléments inversibles.

Exemples 5. Voici quelques exemples.

(i) On a $\mathbb{Z}^* = \{\pm 1\}$ et $\mathbb{R}[X]^* = \mathbb{R}^* = \mathbb{R} - \{0\}$.

(ii) Plus difficile $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$.
Pour le montrer, on part de $zz' = 1$ et on s'intéresse au module $|z|$ de z.

(iii) $(\mathbb{Z}/4\mathbb{Z})^* = \{\bar{1}, \bar{3}\}$
On peut le montrer en dressant la table de multiplication de $\mathbb{Z}/4\mathbb{Z}$.

On peut vérifier que $(A^*, \times, 1)$ est un groupe abélien.

2.2 Divisibilité

Bien que b^{-1} n'est pas de sens dans un anneau, il se peut que $\frac{a}{b}$ en ait un. Penser à $\frac{6}{2}$ dans $\mathbb{Z}$.
D'où la définition suivante :

Définition IV.21: Elément inversible

Soit $(A, +, \times, 0, 1)$ un anneau et $a, b \in A$ avec $b \neq 0$. On dit que b *divise* a s'il existe $c \in A$ tel que $a = bc$ et on écrit $b \,|\, a$.

Dans $\mathbb{Z}$ on retrouve bien la divisibilité à laquelle nous sommes habitués. Voici un anneau dans lequel les choses sont plus compliquées.

Exemple 6. Posons $A = \mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\}$. On peut vérifier que A est un sous-anneau de $\mathbb{R}$. Comme $\mathbb{Z} \subset A$, on a $6 = 2 \times 3$ et 2 et 3 divisent 6. Mais on a aussi

$$6 = (1 + \sqrt{5})(1 - \sqrt{5})$$

et $1 \pm \sqrt{5}$ divisent aussi 6.
En revanche, on peut montrer que $1 + \sqrt{5}$ et 2 n'ont pas de diviseur commun. De même, $1 + \sqrt{5}$ et 3 n'ont pas de diviseur commun.

On pourra remarquer que si $b \in A*$ alors b divise a pour tout a. Ce sont les relations de divisibilité triviales. Un élément de A est dit irréductible si ces seuls diviseurs viennent de relations de divisibilité triviales. Plus précisément :

Définition IV.22: Elément irréductible

Soit $p \in A$. L'élément p est dit *irréductible*, si p n'est pas inversible et

$$p = ab \quad \Rightarrow \quad a \text{ ou } b \text{ est inversible.}$$

Dans $\mathbb{Z}$, les éléments irréductibles sont les nombres premiers et leurs opposés. De manière plus générale, dans ces questions de divisibilité un élément ou son produit avec un inversible jouent les même rôle.

3 Anneaux intègres

Vous avez appris il y a longtemps que pour qu'un produit soit nul, il faut qu'un des terme le soit. Ceci est vrai pour les nombres réels, mais pas pour les matrices (qui ne forment pas un anneau). Dans les anneaux, ça dépend. D'où la définition :

Définition IV.23: Anneau intègre

L'anneau A est dit *intègre* si

$$\forall a, b \in A \qquad (ab = 0 \quad \Rightarrow \quad a = 0 \text{ ou } b = 0).$$

Exemples 7. (i) $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}[X]$, $\mathbb{Z}[i]$ et $\mathbb{Z}[\sqrt{5}]$ sont intègres.

(ii) $\mathbb{Z}/3\mathbb{Z}$ est intègre (comment cela se lit-il sur sa table de multiplication ?).

(iii) $\mathbb{Z}/4\mathbb{Z}$ n'est pas intègre car $\bar{2}.\bar{2} = \bar{4}$.

(iv) $\mathbb{Z} \times \mathbb{Z}$ n'est pas intègre car $(1, 0)(0, 1) = 0$.

4 Corps

Définition IV.24: Corps

Un corps $(K, +, \times)$ est un anneau dont tout élément non nul est inversible :

$$\forall a \in A^* \qquad \exists b \in A \quad ab = 1.$$

Exemples 8. (i) Les corps que vous connaissiez en sont bien : $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

(ii) L'ensemble $\mathbb{R}(X)$ des fractions rationelles est un corps.

(iii) $\mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z}$ sont des corps.

(iv) Le sous-anneau $\mathbb{Q} + i\mathbb{Q}$ de $\mathbb{C}$ est un corps.
(v) $\mathbb{Z}/6\mathbb{Z}$ n'est pas un corps. *Trouver un élément non nul et non inversible.*
(vi) $\mathbb{Z}$, $\mathbb{R}[X]$, $\mathbb{Z}[i]$ ne sont pas des corps.
Trouver un élément non nul et non inversible pour chacun de ces anneaux.

5 Morphismes, idéaux et anneaux quotients

5.1 Morphismes

Définition IV.25: Morphisme

Soit A et B deux anneaux. Un *morphisme f de A vers B* est une application $f : A \longrightarrow B$ telle que

(i) $f(0) = 0$ et $f(1) = 1$;
(ii) $f(a + a') = f(a) + f(a')$ pour tout $a, a' \in A$;
(iii) $f(-a) = -f(a)$ pour tout $a \in A$,
(iv) $f(aa') = f(a)f(a')$ pour tout $a, a' \in A$.

Remarque. On pourra remarquer que f est en particulier un morphisme de groupes pour la loi $+$. En particulier, la définition ci-dessus est redondante car $f(a + a') = f(a) + f(a')$ implique $f(0) = 0$ et $f(-a) = -f(a)$.

Il est immédiat de vérifier que la composé de deux morphismes est un morphisme.
De même, la réciproque d'un morphisme bijectif f est un morphisme. On dit alors que f est un *isomorphisme*.

Voici quelques exemples de morphismes.

Exemples 9. (i) Pour $n \geqslant 2 \in \mathbb{N}$, l'application

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ k \longmapsto & \bar{k} = k + n\mathbb{Z} & \end{array}$$

est un morphisme.

(ii) Soit $a \in \mathbb{R}$. Alors, l'application

$$\mathrm{ev}_a : \begin{array}{ccc} \mathbb{R}[X] & \longrightarrow & \mathbb{R} \\ P & \longmapsto & P(a) \end{array}$$

est un morphisme.

(iii) Soit A et B deux anneaux. Alors, l'application

$$\begin{array}{ccc} A \times B & \longrightarrow & A \\ (a, b) & \longmapsto & a \end{array}$$

est un morphisme.

(iv) Soit A et B deux anneaux. Alors, l'application

$$\begin{array}{ccc} A & \longrightarrow & A \times B \\ a & \longmapsto & (a, 0) \end{array}$$

n'est pas un morphisme. Pourquoi ?

(v) L'application

$$\begin{array}{ccc} \mathbb{R} \times \mathbb{R} & \longrightarrow & \mathbb{C} \\ (x, y) & \longmapsto & x + iy \end{array}$$

n'est pas un morphisme. Pourquoi ?

(vi) Posons
$$A = \{\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in \mathcal{M}_2(\mathbb{R}) \,|\, a, b \in \mathbb{R}\}.$$
Alors $(A, 0, I_2, +, .)$ où . est le produit matriciel, I_2 la matrice identité est un anneau. De plus l'application
$$\begin{array}{ccc} \mathbb{C} & \longrightarrow & A \\ a+ib & \longmapsto & \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \end{array}$$
est un isomorphisme d'anneaux.

Le *noyau de* $f : A \longrightarrow B$ est son noyau lorsque f est pensé comme un morphisme de groupes :
$$\mathrm{Ker} f = \{a \in A \,:\, f(a) = 0\}.$$

5.2 Idéal

Définition IV.26: Idéal

Soit A un anneau commutatif, $I \subset A$. Alors, I est un *idéal* ssi $(I, +)$ est un sous-groupe de $(A, +)$ et pour tout $a \in A$, pour tout $x \in I$, $ax \in I$.

Théorème IV.27: Intersection d'idéaux

Toute intersection d'idéaux est un idéal.

La preuve est une simple vérification.

Définition IV.28: Idéal Engendré par une Partie

Soit $P \subset A$ non vide. L'intersection de tous les idéaux de A contenant P est le plus petit idéal contenant P. On l'appelle *idéal engendré par* P, noté (P).

Théorème IV.29. Idéal engendré

L'idéal engendré par P est $\{\sum_{i=1}^{r} u_i a_i \,/\, r \in \mathbb{N}, a_i \in P, u_i \in A\}$.
Remarque : Soit $a \in A$: L'idéal engendré par a est aA. On le note (a). Plus généralement, si $P = \{a_1, \ldots, a_s\}$ on note $(a_1, \ldots, a_s) = a_1 A + \cdots + a_s A$.

Démonstration. L'ensemble est bien stable par $+$, $-$ et multiplication par n'importe quel élément de A. C'est donc un idéal.
Soit I est un idéal contenant P. Comme il est stable par $+$ et multiplication par tout $a \in A$ il contient l'ensemble. □

Exemples 10. (i) L'idéal (2) engendré par 2 dans $\mathbb{Z}$ est l'ensemble des nombres pairs.

(ii) L'idéal $(6, 9)$ engendré par 6 et 9 est l'ensemble des multiples de 3.
La preuve de ce fait est laissée en exercice.

(iii) L'idéal (X) engendré par le polynôme X dans $\mathbb{R}[X]$ est l'ensemble des polynômes qui s'annulent en 0.

(iv) L'idéal $(2, X)$ engendré par les polynômes 2 et X dans $\mathbb{Z}[X]$ est l'ensemble des polynômes dont le coefficient constant est pair.
La preuve de ce fait est laissée en exercice.

(v) L'idéal engendré par deux idéaux I et J est l'ensemble

$$I + J = \{a + b \,:\, a \in I,\, b \in J\}.$$

Théorème IV.30. Noyau et Idéal

Le noyau d'un morphisme d'anneaux est un idéal.

Démonstration. Soit f un tel morphisme. Comme c'est un morphisme de groupe pour $+$, son noyau est un sous-groupe. De plus, le calcul

$$f(ab) = f(a)f(b) = f(a)0 = 0$$

montre que si $b \in \mathrm{Ker} f$ alors $ab \in \mathrm{Ker} f$. $\square$

5.3 Anneau quotient

Nous allons faire une construction qui montre la réciproque du théorème précédent : tout idéal est le noyau d'un morphisme.
Un idéal I de A est dit *strict* si $I \neq A$. Ceci équivaut à $1 \notin A$.

Théorème IV.31. Anneau quotient

Soit I un idéal strict de A. On pose

$$A/I = \{a + I \,:\, a \in A\}$$

inclus dans l'ensemble des parties de A. Il existe une unique structure d'anneau sur A/I telle que l'application

$$\begin{array}{cccc} \pi : & A & \longrightarrow & A/I \\ & a & \longmapsto & a + I \end{array}$$

soit un morphisme d'anneaux.

Les lois sont données par les formules, pour tout $a, b \in A$:

$$\begin{array}{rcl} (a + I) + (b + I) & = & (a + b) + I \\ (a + I)(b + I) & = & (ab) + I \end{array}$$

La preuve est directe et nous l'avons faite dans le cas suivant : $A = \mathbb{Z}$ et $I = n\mathbb{Z} = (n)$. Nous avions obtenu l'anneau $\mathbb{Z}/n\mathbb{Z}$. Le cas général ne posant aucune difficulté supplémentaire est omise ici.
Souvent on note $a + I =: \bar{a}$, lorsque la référence à I est claire.
Application : Construction des nombres complexes.
La relation clé dans le corps des nombres complexes est bien entendu $i^2 = -1$. L'idée est donc de partir de $\mathbb{R}[X]$ est d'imposer $X^2 = -1$ c'est-à-dire $X^2 + 1 = 0$ par quotient. On obtient l'application

$$\begin{array}{cccc} \iota : & \mathbb{C} & \longrightarrow & \mathbb{R}[X]/(X^2+1) \\ & a + ib & \longmapsto & a + bX + (X^2+1)\mathbb{R}[X] = \overline{a + bX} \end{array}$$

qui est isomorphisme d'anneaux.

Le théorème de factorisation permet d'obtenir des isomorphismes comme ι.

Théorème IV.32. Factorisation des morphismes

Soit $f : A \longrightarrow B$ un morphisme d'anneaux et I un idéal strict de A.
Si $I \subset \mathrm{Ker} f$ alors il existe un unique morphisme $\bar{f} : A/I \longrightarrow B$ tel que $\bar{f} \circ \pi = f$.

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\pi"'] & B \\ A/I \arrow[ur, "\bar{f}"'] & \end{tikzcd}$$

De plus, $\bar{f}$ est injectif si et seulement si $I = \mathrm{Ker} f$. Enfin, $\bar{f}$ est surjectif si et seulement si f l'est.

Application. Soit $I = (P)$ l'idéal de $\mathbb{R}[X]$ engendré par un polynôme P. La remarque est que si $P(x) = 0$, alors $Q(x) = 0$ pour tout $Q \in (P)$. Ainsi pour $P = X^2 - 1$ on obtient un morphisme

$$\begin{array}{rccl} f : & \mathbb{R}[X] & \longrightarrow & \mathbb{R} \times \mathbb{R} \\ & P & \longmapsto & (P(-1), P(1)) \end{array}$$

tel que $I \subset \mathrm{Ker} f$. On obtient donc $\bar{f} : \mathbb{R}[X]/(X^2 - 1) \longrightarrow \mathbb{R} \times \mathbb{R}$ qui est en fait un isomorphisme.

Exercice 6. *Montrer que $\mathbb{R}[X]/(X^2 - 4X)$ est isomorphe à $\mathbb{R} \times \mathbb{R}$.*
Plus difficile, montrer que $\mathbb{R}[X]/(X^2 - 2X + 1)$ est isomorphe à $\mathbb{R} \times \mathbb{R}$ muni d'une loi à définir.
Montrer que $\mathbb{R}[X]/(X^2 - 4X)$ et $\mathbb{R}[X]/(X^2 - 2X + 1)$ ne sont pas isomorphes.

Correction du cas $X^2 - 2X + 1 = (X - 1)^2$. Les multiples de ce polynômes sont ceux qui vérifient $P(1) = P'(1) = 0$. Donc l'application

$$\begin{array}{rccl} \theta : & \mathbb{R}[X]/(X^2 - 2X + 1) & \longrightarrow & \mathbb{R} \times \mathbb{R} \\ & P & \longmapsto & (P(1), P'(1)) \end{array}$$

est une bijection linéaire. En revanche θ n'est pas un morphisme d'anneau. En revanche, elle l'est pour la loi

$$(a, b) \star (a', b') := (aa', ab' + a'b).$$

5.4 Propriétés des idéaux

Définition IV.33: Idéal Premier

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

$$\forall a, b \in A \qquad (ab \in I \ \Rightarrow a \in I \text{ ou } b \in I).$$

Cette propriété s'interprète facilement en terme de quotients.

Théorème IV.34: Quotient par idéal premier

Soit I un idéal strict de A. Alors I est premier si et seulement si A/I est intègre.

Démonstration. Considérons $\pi : A \longrightarrow A/I$.
Supposons A/I est intègre. Soit a et b dans A. Alors $ab \in I$ si et seulement si $\pi(ab) = 0$ si et seulement si $\pi(a)\pi(b) = 0$. Alors, cette dernière égalité implique que $\pi(a) = 0$ ou $\pi(b) = 0$. C'est-à-dire $a \in I$ ou $b \in I$. Donc I est premier.
Supposons maintenant I premier. Soit deux éléments de A/I dont le produit fait zéro. On écrit ces deux éléments $\pi(a)$ et $\pi(b)$ avec a et b dans A. Alors $0 = \pi(a)\pi(b) = \pi(ab)$. Donc $ab \in I$. Comme I est premier cela implique que $a \in I$ ou $b \in I$. Donc $\pi(a) = 0$ ou $\pi(b) = 0$. $\square$

Définition IV.35: Idéal Maximal

Un idéal I d'un anneau A est dit maximal si $I \subset J \subset A$ implique $J = I$ ou $J = A$.
Les seuls idéaux contenant I sont I et A.

Cette propriété s'interprète facilement en terme de quotients.

Théorème IV.36: Quotient par idéal maximal

Soit I un idéal strict de A. Alors I est maximal si et seulement si A/I est un corps.

Démonstration. Considérons $\pi : A \longrightarrow A/I$.
Supposons A/I est un corps. Soit J un idéal contenant strictement I. Soit $b \in J$ tel que $b \notin I$. Alors $\pi(b) \neq 0$. Donc il existe $c \in A$ tel que $\pi(c)\pi(b) = 1 = \pi(bc)$. Ceci se réécrit $1 - bc \in I \subset J$. Donc $1 = (1 - bc) + bc \in J$. Mais alors $J = A$.
Supposons maintenant I maximal. Soit $a \in A$ tel que $\pi(a) \neq 0$. Cela signifie que $a \notin A$. Considérons l'idéal $J = I + aA$ engendré par I et a. Comme I est maximal, $J = A$ et $1 \in J$. Donc il existe $b \in A$ et $i \in I$ tels que $1 = i + ab$. Mais alors $1 = \pi(ab) = \pi(a)\pi(b)$. Donc $\pi(a)$ est inversible.
On a bien montré que A/I est un corps. □

Ces derniers résultats montrent que I maximal implique I premier.

Exemples 11. (i) L'idéal $(6) \subset \mathbb{Z}$ n 'est ni premier ni maximal. En revanche, (5) est maximal (donc premier).

(ii) $(X^2 + 1) \subset \mathbb{R}[X]$ est maximal.

(iii) $(X^2 - 1) \subset \mathbb{R}[X]$ n'est pas premier.

(iv) $(X) \subset \mathbb{Z}[X]$ est premier, non maximal.

(v) $(X^2 + Y^3) \subset \mathbb{C}[X, Y]$ est premier, non maximal.

(vi) $(3, X) \subset \mathbb{Z}[X]$ est maximal.

6 Anneaux euclidiens

6.1 Définition et Idéaux

Définition IV.37: Anneau euclidien

Soit A un anneau intègre. On dit que A est euclidien s'il existe une fonction $N : A - \{0\} \longrightarrow \mathbb{N}$ telle que :

(i) $N(ab) \geqslant N(b), \forall a, b \in A - \{0\}$

(ii) $\forall a, b \in A,\ b \neq 0,\ \exists!(q, r) \in A$ tq. $a = bq + r \quad (r = 0$ ou $N(r) < N(b)$

La fonction N est appelée **norme euclidienne**.

Exemples 12. (i) $\mathbb{Z}$ est euclidien, avec $N(x) = |x|$. Ceci est la division euclidienne que l'on connait depuis l'école primaire.

(ii) Si $\mathbb{K}$ est un corps, $\mathbb{K}[x]$ est euclidien, avec $N(P) = deg(P)$. Ceci est la division euclidienne des polynômes.

(iii) $\mathbb{Z}[i] := \{m + in, (m, n) \in \mathbb{Z}^2\}$ est euclidien, avec $N(z = x + iy) = x^2 + y^2$.
Esquisse de démonstration. Soit $a, b \in A$, $b \neq 0$. On cherche q et r comme dans la définition. L'idée de base est que q est une approximation du quotient a/b que l'on connait dans $\mathbb{C}$. Posons donc $z = a/b \in \mathbb{C}$. Les points de $\mathbb{Z}[i]$ forme un réseau donc il existe $q \in \mathbb{Z}[i]$ tel que $|z - q| \leqslant \sqrt{2}/2$. Alors q convient.

Encore un peu de vocabulaire afin de décrire les idéaux des anneaux euclidiens. Un idéal I d'un anneau A est dit *principal* s'il est engendré par un élément. Un anneau est dit *principal* si tous ses idéaux le sont.

Théorème IV.38. Euclidien et Principal

Tout anneau euclidien est principal.

Démonstration. Soit I un idéal de A. On regarde $N(I)$. Comme partie non vide de $\mathbb{N}$ elle a un minimum. Soit $b \in I$ tel que $N(b)$ soit égal à ce minimum. Montrons que

$$I = (b).$$

Il est clair que $(b) \subset I$.
Soit $a \in I$. Ecrivons $a = bq + r$ avec $r = 0$ ou $N(r) < N(b)$. Puisque $r = a - bq$ il appartient à I. Par minimalité de $N(b)$, on en déduit que $r = 0$. Mais alors, $a \in (b)$. $\square$

On peut aussi comprendre les éléments inversibles. Regardons $\mathbb{Z}$ un élément non nul a est inversible ssi $|a| = 1$. Regardons $\mathbb{K}[X]$: un élément non nul P est inversible ssi $\deg(P) = 0$. En général, on a :

Théorème IV.39: Eléments inversibles

Soit A un anneau euclidien dont on note N la norme. Soit $a \in A$ non nul. Alors a est inversible si et seulement si $N(a) = N(1)$.

Démonstration. Si $ab = 1$ alors $N(a) \leqslant N(1)$. Or $a = a \times 1$ implique que $N(1) \leqslant N(a)$. Donc si a est inversible alors $N(a) = N(1)$.
Réciproquement supposons que $N(a) = N(1)$. On fait la division euclidienne : $1 = aq + r$ avec $N(r) < N(r)$. Ce qui est impossible. Donc $r = 0$ et a est inversible. $\square$

6.2 Pgcd et ppcm

Les pgcd et ppcm sont ceux que vous connaissez déjà sur $\mathbb{Z}$ et $\mathbb{K}[X]$. Cependant les concepts d'anneau euclidien et d'idéal permettent des définitions et démonstrations à la fois homogènes et élégantes. Soit donc A un anneau euclidien.
Une petite remarque préparatoire sous forme d'exercice.

Exercice 7. *Soit a et b non nuls dans A. Alors $(a) = (b)$ si et seulement s'il existe $c \in A$ inversible tel que $a = cb$.*

Définition IV.40: pgcd

Soit $a_1, \dots, a_s$ des éléments non tous nuls de A. Un élément $\delta \in A$ tel que $(a_1, \dots, a_s) = (\delta)$ est appelé pgcd des éléments $a_1, \dots, a_s$.
On note $\delta = a_1 \wedge \dots \wedge a_s$. On peut remarquer que δ n'est défini qu'à un inversible près. Sur $\mathbb{Z}$ (resp. $\mathbb{K}[X]$), on fixe généralement cette indétermination en demandant que le pgcd soit positif (resp. unitaire).

Le nom pgcd est justifié par l'exercice suivant.

Exercice 8. *Soit q dans A non nul. Alors q divise tous les a_i si et seulement si q divise δ.*

Le lemme de Bezout est également facile à démontrer.

Exercice 9. Lemme de Bezout version 1.
Soit a et b dans A non nuls. Alors, il existe u et v dans A tels que $au + bv = a \wedge b$.

Définition IV.41: éléments premiers entre eux

Soit $a_1, \ldots, a_s$ des éléments non nuls de A. On dit qu'ils sont premiers entre eux si $a_1 \wedge \cdots \wedge a_s = 1$ c'est-à-dire si $(a_1, \ldots, a_s) = A$.

Le lemme de Bezout est également facile à démontrer.

Exercice 10. Lemme de Bezout version 2.
Soit a et b dans A non nuls. Alors, a et b sont premiers entre eux si et seulement s'il existe u et v dans A tels que $au + bv = 1$.

Définition IV.42: ppcm

Soit $a_1, \ldots, a_s$ des éléments non nuls de A. Un élément $c \in A$ tel que $(a_1) \cap \cdots \cap (a_s) = (c)$ est appelé ppcm des éléments $a_1, \ldots, a_s$.
On note $c = a_1 \vee \cdots \vee a_s$.

6.3 Calcul des Pgcd et ppcm

On se donne a et b non nuls dans A. On veut calculer $a \wedge b$ et $a \vee b$. Un premier résultat nous dit que la connaissance de l'un détermine l'autre.

Théorème IV.43: Lien ppcm et pgcd

Il existe u inversible tel que
$$(a \wedge b)(a \vee b) = uab.$$

Démonstration. On pose $a' = a/(a \wedge b)$ et $b' = b/(a \wedge b)$. Comme $a' \wedge b' = 1$ et $a' \vee b' = (a \vee b)/(a \wedge b)$ il suffit de montrer que
$$(a' \vee b') = (a'b'),$$
sachant que $a' \wedge b' = 1$.
Autrement dit on peut supposer que $a \wedge b = 1$. Alors il existe u et v dans A tels que $au + bv = 1$.
Il est clair que $(ab) \subset (a)$. Donc $(ab) \subset (a) \cap (b) = (a \vee b)$.
Réciproquement montrons que $a \vee b \in (ab)$. Comme a divise $a \vee b$, il existe c tel que $a \vee b = ac$. Or
$$c = acu + bcv.$$
Puisque b divise bcv et $acu = u.(a \vee b)$ il divise c. Donc $c = bc'$. Ainsi $a \vee b = ac = abc'$. CQFD. $\square$

Algorithme d'Euclide. Il s'agit d'un algorithme permettant de calculer $a \wedge b$. Il est basé sur la formule suivante. On suppose b non nul et soit $a = bq + r$ la division euclidienne alors
$$\begin{cases} a \wedge b = r \wedge b \\ 0 \wedge b = b \end{cases}$$
Pour obtenir l'algorithme, on réitère le procédé en divisant b par r pour ré-exprimer $r \wedge b$.

6.4 Factorisation

Comme nous commençons à le voir, le cadre des anneaux euclidiens (en fait principal suffit souvent) est un bon cadre où étendre les propriétés des entiers. Une propriété arithmétique fondamentale des entiers est la décomposition en produit de nombres premiers. Cela s'étend à notre cadre du jour : on dit qu'un anneau principal est factoriel.

Théorème IV.44. Factoriel

Soit A un anneau euclidien et a un élément non nul de A. Alors, il existe des éléments irréductibles $p_1, \dots, p_s$ dans A, des entiers naturels non nuls $n_1, \dots, n_s$ et un élément inversible u tel que

$$a = up_1^{n_1} \dots p_s^{n_s}.$$

De plus cette écriture est unique à l'ordre près et à multiplication des p_i et de a par des inversibles.

Un ingrédient clé pour montrer cela est le

Lemme IV.45 (Lemme de Gauss)**.** *Soit a, b et c non nuls dans A. Si a divise bc et $a \wedge b = 1$ alors a divise c.*

Démonstration. On utilise encore Bezout : $au + bv = 1$. Alors $acu + bcv = c$. Donc a divise c. □

Preuve du théorème de Factorialité. Pour l'existence on fait une récurrence sur $N(a)$. Si a est irréductible, il n'y a rien à montrer. Sinon $a = bc$ avec b et c non inversibles. Alors $N(b) < N(a)$ et $N(c) < N(a)$. Par récurrence, on déduit que b et c admettent des décompositions. Donc a aussi.

Pour l'unicité supposons que

$$\prod_i p_i = u \prod_j q_j, \tag{6.1}$$

- avec p_i et q_i irréductibles et u inversible. Ici on remplace les exposant par des répétitions.
Il est clair que q_1 divisent le membre de droite. Donc il divise celui de gauche. Supposons que q_1 n'est pas conjugué à p_1. Comme ils sont irréductibles, il suit que $q_1 \wedge p_1 = 1$. Mais alors le lemme de Gauss implique que q_1 divise $\prod_{i \geqslant 2} p_i$. On recommence. On aura nécessairement à un moment q_1 divise p_i. On divise l'expression (6.1) par q_1 et on recommence (cad on fait une récurrence sur le nombre de q_i). □

Pour ceux qui auraient l'impression de ne rien avoir montré, il est intéressant de faire l'exercice suivant.

Exercice 11. *Posons $A = \{a + bi\sqrt{5} \, : \, a, b \in \mathbb{Z}\}$.*

(i) Montrer que A est un sous-anneau de $\mathbb{C}$.

(ii) Montrer que 2 et 3 sont irréductibles dans A.

(iii) Montrer que $1 \pm i\sqrt{5}$ sont irréductibles dans A.

(iv) En remarquant que $2 \times 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$, montrer que A n'est pas euclidien.

7 Anneau $\mathbb{K}[X]$

Fixons un corps $\mathbb{K}$. Vous pouvez penser à $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$ ou $\mathbb{Z}/p\mathbb{Z}$. Nous verrons d'autres exemples plus tard. Nous avons déjà vu que $\mathbb{K}[X]$ était un anneau euclidien : il vérifie donc Bezout, Gauss et il y a une unique décomposition en produit de polynômes irréductibles. Nous allons maintenant voir quelques techniques spécifiques à cet anneau.

7.1 Racines et Dérivation

Substitution. C'est l'opération la plus compliquée à comprendre. Soit

$$P = a_0 + a_1 X + \cdots + a_d X^d$$

et Q deux polynômes. On pose alors

$$P(\circ Q)(X) = a_0 + a_1 Q(X) + \cdots + a_d Q(X)^d.$$

Faisons un exemple : $P = 1 + X^3$ et $Q = 2 + X^2$:

$$\begin{aligned} P(\circ Q)(X) &= 1 + (2 + X^2)^3 \\ &= 9 + 3X^2 + 3X^4 + X^6. \end{aligned}$$

L'application $P \mapsto P \circ Q$ est linéaire mais PAS $Q \mapsto P \circ Q$.
Dérivation. L'ensemble $(1, X, X^2, \dots)$ est une base de $\mathbb{K}[X]$. On peut donc définir un endomorphisme D de $\mathbb{K}[X]$ on donnant l'image de ces monômes.

$$\begin{array}{cccc} D: & \mathbb{K}[X] & \longrightarrow & \mathbb{K}[X] \\ & X^k & \longmapsto & kX^{k-1} \quad \text{si } k \geqslant 1 \\ & 1 & \longmapsto & 0 \end{array}$$

On a définit ainsi ce que l'on appelle la dérivation. Dans le cas où le corps est celui des réels cette dérivation coïncide avec la dérivation usuelle. On note souvent P' pour $D(P)$.
On a les règles de calculs usuelles de la dérivation :

Théorème IV.46: Propriétés de la dérivation

Soit P et Q dans $\mathbb{K}[X]$. On a

$$D(PQ) = D(P)Q + PD(Q) \qquad (PQ)' = P'Q + QP'$$

et

$$D(P \circ Q) = D(Q).D(P) \circ Q \qquad (P \circ Q)' = Q' \times P' \circ Q.$$

Démonstration. Fixons Q. Les applications $P \mapsto D(PQ)$ et $P \mapsto D(P)Q + PD(Q)$ sont linéaires. Du coup il suffit de montrer l'égalité pour $P = X^k$.
Fixons maintenant $P = X^k$. Les applications $Q \mapsto D(PQ)$ et $Q \mapsto D(P)Q + PD(Q)$ sont linéaires. Du coup il suffit de montrer l'égalité pour $Q = X^l$.
Dans ce cas, on a

$$D(PQ) = D(X^{k+l}) = (k+l)X^{k+l-1}$$

et

$$D(P)Q + PD(Q) = D(X^k)X^l + X^k D(X^l) = kX^{k+l-1} + lX^{k+l-1} = (k+l)X^{k+l-1}.$$

Montrons maintenant la seconde égalité. Les applications $P \mapsto D(P \circ Q)$ et $P \mapsto D(Q) \times D(P) \circ Q$ sont linéaires. Du coup il suffit de montrer l'égalité pour $P = X^k$.
Dans ce cas, on a

$$D(P \circ Q) = D(Q^k) = kD(Q)Q^{k-1}$$

et

$$D(Q).D(P) \circ Q = D(Q).k.Q^{k-1}.$$

□

Evaluation – Racines.
Soit $a \in \mathbb{K}$. Alors on a une application évaluation

$$\begin{array}{cccc} \mathrm{ev}_a: & \mathbb{K}[X] & \longrightarrow & \mathbb{K} \\ & P & \longmapsto & P(a). \end{array}$$

On vérifie sans peine que ev_a est un morphisme d'anneaux. Son noyau est $\{P \ : \ P(a) = 0\}$. C'est un idéal maximal de $\mathbb{K}[X]$ car le quotient est isomorphe à $\mathbb{K}$. L'isomorphisme est donné par ev_a.

Théorème IV.47: Racine et division

Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. Alors a est une racine de P si et seulement si $X - a$ divise P.

Démonstration. Si $P = (X - a)Q$, il est clair que $P(a) = 0$. Réciproquement supposons que $P(a) = 0$. On écrit la division euclidienne $P = Q(X - a) + R$ avec R nul ou de degré strictement inférieur à 1. Donc R est en fait un polynôme constant. Par ailleurs, $0 = P(a) = R(a)$. Donc R est nul et $X - a$ divise P. □

Définition IV.48: Ordre d'une racine

Soit $P \in \mathbb{K}[X]$ non nul, $a \in \mathbb{K}$ et $\alpha \in \mathbb{N}$. On dit que a est *racine d'odre au moins* α si $(X-a)^\alpha$ divise P.
On dit que a est *racine d'odre exactement* α si elle est racine d'ordre au moins α mais n'est pas d'odre au moins $\alpha+1$.

Théorème IV.49: Ordre racine et dérivées

Soit $P \in \mathbb{K}[X]$ non nul, $a \in \mathbb{K}$ et $\alpha \in \mathbb{N}$. Alors

(i) Si a est racine d'odre exactement α alors

$$P(a) = P'(a) = \cdots = P^{(\alpha-1)}(a) = 0.$$

(ii) Si de plus $\mathbb{K}$ est de caractéristique nulle, la réciproque de la première assertion est vrai.

Démonstration. Supposons d'abord que $(X-a)^\alpha$ divise P. Il existe alors $Q \in \mathbb{C}[X]$ tel que $P = (X-a)^\alpha Q$. On rappelle la formule le Leibnitz :

$$(fg)^{(k)} = \sum_{i=0}^{k} \binom{k}{i} f^{(i)} g^{(k-i)}.$$

La preuve de cette formule se fait par récurrence sur k en utilisant la formule de dérivation d'un produit. On obtient pour P et $k \leqslant \alpha - 1$:

$$(P)^{(k)} = \sum_{i=0}^{k} \binom{k}{i} ((X-a)^\alpha)^{(i)} Q^{(k-i)}. \tag{7.1}$$

On remarque alors que

$$((X-a)^\alpha)^{(i)} = (\alpha.(\alpha-1)\dots(\alpha-i+1))(X-a)^{\alpha-i} \quad \text{si } i \leqslant \alpha,$$

et

$$((X-a)^\alpha)^{(i)} = 0 \quad \text{si } i > \alpha.$$

En particulier, pour tout $i \leqslant k < \alpha$, on a

$$\left(((X-z)^\alpha)^{(i)}\right)(a) = 0.$$

En injectant dans la formule (7.1), on déduit que $P^{(k)}(a) = 0$.

Réciproquement, supposons que $P(a) = \cdots = P^{(\alpha-1)}(a) = 0$. Ecrivons la division euclidienne de P par $(X-a)^\alpha$:

$$P = (X-a)^\alpha Q + R,$$

avec $\deg(R) < \alpha$. L'assertion déjà démontrée implique que

$$R(a) = \cdots = R^{(\alpha-1)}(a) = 0.$$

Considérons le polynôme auxiliaire

$$S(X) = R(z+X) \quad R(X) = S(X-a).$$

La formule de dérivation d'un polynôme composé implique que

$$S^{(k)}(X) = R^{(k)}(z+X),$$

donc

$$S(0) = \cdots = S^{(\alpha-1)}(0) = 0.$$

Ecrivons $S = a_0 + a_1 X + \cdots + a_{\alpha-1} X^{\alpha-1}$. Par une récurrence immédiate, on montre que

$$S^{(k)}(0) = k! a_k \quad \forall k = 0, \ldots, \alpha - 1.$$

On en déduit que $S = 0$, puis que $R = 0$. Ainsi $(X - a)^{\alpha}$ divise P. □

7.2 Irréductibilité

A Petits degrés

En **petit degré**, il y a un critère simple d'irréductibilité.

Théorème IV.50: Irréductibilité et racines

On a

(i) Tout polynôme de degré 1 est irréductible.

(ii) Tout polynôme irréductible de degré supérieur à 2 n'a pas de racine.

(iii) Tout polynôme de degré 2 ou 3 qui n'a pas de racine est irréductible.

Démonstration. Soit P un polynôme. Il est irréductible, si pour tout A, B dans $\mathbb{K}[X]$ tels que $P = AB$, on a $\deg(A)$ ou $\deg(B)$ nul :

$$\forall A, B \in \mathbb{K}[X] \qquad (P = AB \Rightarrow \ (\deg(A) = 0 \text{ ou } \deg(B) = 0)).$$

Les trois énoncés de la proposition découlent facilement des deux assertions suivantes :

(i) $\deg(P) = \deg(A) + \deg(B)$;

(ii) P est divisible par un polynôme de degré un si et seulement si il a une racine.

□

En appliquant la proposition, on voit que $X^2 + X + 1 \in \mathbb{Z}/2\mathbb{Z}[X]$ est irréductible. Attention, il est possible qu'un polynôme sans racine ne soit pas irréductible. $(X^2 + 1)^2$ donne un exemple dans $\mathbb{R}[X]$.

B Nombres complexes

Théorème IV.51. D'Alembert-Gauss

Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré un.

Ceci est bien une version du théorème de d'Alembert-Gauss qui dit que tout polynôme non constant sur $\mathbb{C}$ a une racine et donc est divisible par un polynôme de degré un.

C Nombres réels

Encore une façon de formuler le théorème de d'Alembert-Gauss.

Théorème IV.52. D'Alembert-Gauss

Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré un et les polynômes de degré 2 et de discriminant négatif.

D Nombres entiers et rationnels

On sort un peu du contexte en regardant les polynômes à coefficients entiers. Ce n'est pas un anneau euclidien.
Pour $P \in \mathbb{Z}[X]$ non nul on note $c(P)$ le pgcd des coefficients de P. Ce nombre est appelé le contenu de P.

Théorème IV.53. Gauss

Soit P et Q dans $\mathbb{Z}[X]$ non nuls. Alors

$$c(PQ) = c(P)c(Q).$$

Cette formule est très simple et très utile. C'est la marque des grands...théorèmes.

Démonstration. Posons $\tilde{P} = P/c(P)$ et $\tilde{Q} = Q/c(Q)$. Ceux sont des polynômes à coefficients entiers et de contenu égal à 1. Il suffit de montrer que

$$c(\tilde{P}\tilde{Q}) = 1.$$

Soit p un nombre premier. Soit $\bar{P}$ (resp. $\bar{Q}$) le polynôme de $\mathbb{Z}/p\mathbb{Z}[X]$ obtenu en considérant la classe dans $\mathbb{Z}/p\mathbb{Z}$ de chaque coefficient de $\tilde{P}$ (resp. $\tilde{Q}$). Comme $c(\tilde{P}) = 1$, $\bar{P}$ est non nul. Comme $\mathbb{Z}/p\mathbb{Z}[X]$ est intègre, on en déduit que $\bar{P}\bar{Q} \neq 0$. Donc p ne divise pas $c(\tilde{P}\tilde{Q})$. Vu l'arbitraire de p, on en déduit que $c(\tilde{P}\tilde{Q}) = 1$. □

Corollaire IV.54: Irred dans $\mathbb{Z}$ et $\mathbb{Q}$

Soit $P \in \mathbb{Z}[X]$ tel que $c(P) = 1$. Alors se valent

(i) P est irréductible dans $\mathbb{Q}[X]$;

(ii) P est irréductible dans $\mathbb{Z}[X]$.

Démonstration. Un sens est évident. Réciproquement supposons que P est irréductible dans $\mathbb{Z}[X]$. Soit $P = AB$ dans $\mathbb{Q}[X]$. En chassant les dénominateurs de A et B, on obtient $d \in \mathbb{N}$, $\tilde{A}, \tilde{B} \in \mathbb{Z}[X]$ tels que

$$dP = \tilde{A}\tilde{B}. \tag{7.2}$$

En prenant le contenu, sachant que $c(P) = 1$, on obtient $d = c(\tilde{A})c(\tilde{B})$. Mais alors, en divisant l'équation (7.2) par d, on obtient

$$P = \frac{\tilde{A}}{c(\tilde{A})}\frac{\tilde{B}}{c(\tilde{A})}. \tag{7.3}$$

Cette équation vit dans $\mathbb{Z}[X]$. Donc l'irréductibilité de P dans $\mathbb{Z}[X]$ montre que $\deg(A)$ ou $\deg(B)$ est nul. CQFD. □

Ce corollaire est très puissant pour montrer qu'un polynôme de $\mathbb{Q}[X]$ est irréductible. Faisons un exemple.

Exemple 13. Soit $P = X^4 + X + 1$. Montrons que P est irréductible dans $\mathbb{Q}[X]$. Comme $P \in \mathbb{Z}[X]$ et $c(P) = 1$, il suffit de monter qu'il est irréductible dans $\mathbb{Z}[X]$. Ecrivons donc $P = AB$ avec A et B dans $\mathbb{Z}[X]$. Il s'agit de montrer que A ou B est constant. Quitte à permuter A et B, on peut supposer que $\deg(A) \leqslant \deg(B)$. Comme $\deg(A) + \deg(B) = \deg(P) = 4$, il y deux cas à considérer :

(i) $\deg(A) = 1$ et $\deg(B) = 3$.

Alors $A = aX + b$ avec $a, b \in \mathbb{Z}$. En regardant le coefficient dominant de AB, on déduit que a est inversible dans $\mathbb{Z}$. Donc $a = \pm 1$. On peut supposer que $a = -1$. Mais alors $b \in \mathbb{Z}$ est une racine de P. Avec des inégalité, on se convainc que cela est impossible.

(ii) $\deg(A) = 2$ et $\deg(B) = 2$.

Alors on a
$$X^4 + X + 1 = (aX^2 + bX + c)(a'X^2 + b'X + c')$$
dans $\mathbb{Z}$. En particulier $aa' = 1$. Donc on a $a = a' = \pm 1$. On peut supposer (quitte à multiplier les deux facteurs par -1) que $a = a' = 1$.
De plus, $cc' = 1$. Donc $c' = c = \pm 1$. Or
$$(X^2 + bX + c)(X^2 + b'X + c) = X^4 + (b' + b)X^3 + (2c + bb')X^2 + c(b + b')X + 1.$$
On obtient donc $b' = -b$ en regardant le coefficient en X^3. Donc le coefficient en X est nul. Contradiction.

Chapitre 5

Corps

Sommaire

1 Corps, Sous-corps, Extension

1.1 Définition et exemples

Définition V.55: Corps

Un corps $(\mathbb{K}, +, \times)$ est un anneau tel que tout élément non nul est inversible pour $\times$.

Les premiers exemples sont les corps que vous manipulez depuis longtemps : $\mathbb{R}$, $\mathbb{C}$ et $\mathbb{Q}$. Autre exemple $\mathbb{Q}(i) = \mathbb{Q} + \mathbb{Q}i$.

L'anneau $\mathbb{Z}$ n'est pas un corps car 2 n'est ni nul ni inversible.

L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier. En effet, d'après le théorème de Bezout, $\bar{k} \in \mathbb{Z}/n\mathbb{Z}$ est inversible si et seulement si k est premier avec n.

L'ensemble des fractions rationelles $\mathbb{K}(X)$ est un corps.

On montre facilement que $\mathbb{K}^* = \mathbb{K} - \{0\}$ est un groupe abélien. En particulier l'inverse de$x \in \mathbb{K}^*$ pour $\times$ est unique : on le note x^{-1} ou $\frac{1}{x}$.
Comme nous l'avons déjà vu des corps peuvent être inclus les uns dans les autres.

Définition V.56: Sous-Corps

Soit $(\mathbb{L}, +, \times)$ un corps. Une partie $\mathbb{K} \subset \mathbb{L}$ est un sous-corps si c'est un sous-anneau tel que

$$\forall x \in \mathbb{K} \qquad x^{-1} \in \mathbb{K}.$$

On dit aussi que $\mathbb{L}$ est une extension de $\mathbb{K}$.

Une remarque très importante est que si $\mathbb{K} \subset \mathbb{L}$ est une extension de corps alors $\mathbb{L}$ est un $\mathbb{K}$-espace vectoriel. La dimension de cet espace vectoriel est appelée *le degré de l'extension*. On la note $[\mathbb{L} : \mathbb{K}]$.
Par exemple $[\mathbb{C} : \mathbb{R}] = 2$, $[\mathbb{Q}(i) : \mathbb{Q}] = 2$ et $[\mathbb{C} : \mathbb{Q}] = \infty$.

1.2 Caractéristique d'un corps

Soit A un anneau. Soit n un entier naturel. On peut bien sûr le penser comme $1 + 1 + \cdots + 1$ n fois. Mais alors il prend un sens dans A. De plus, si n est négatif, $n = -(-n)$. On obtient ainsi un morphisme d'anneaux

$$\iota : \mathbb{Z} \longrightarrow A.$$

Autrement dit, $\iota(1) = 1$, $\iota(2) = 1 + 1 + 1$, $\iota(3) = 1 + 1 + 1$ etc. Et $\iota(-1) = -\iota(1)$, $\iota(-2) = -\iota(2)$, $\iota(-3) = -\iota(3)$ etc. Le noyau de ι est un idéal de A. Il s'écrit donc (n) pour un entier naturel n. L'entier n est appelé la caractéristique de A. On la note $\mathrm{car}(A)$.

Lemme V.57. *La caractéristique d'un corps est nulle ou un nombre premier p.*

Démonstration. Comme $\mathbb{Z}/n\mathbb{Z}$ s'injecte dans le corps il est intègre. Mais alors n est nul ou premier. □

Soit $\mathbb{K}$ un corps. En fait, si $\mathrm{car}(\mathbb{K}) = 0$ alors $\mathbb{K}$ contient $\mathbb{Q}$. Si $\mathrm{car}(\mathbb{K}) = p$ alors $\mathbb{K}$ contient $\mathbb{Z}/p\mathbb{Z}$.

Lemme V.58. *Le cardinal d'un corps fini est une puissance d'un nombre premier.*

Démonstration. Le morphisme ι ne peut être injectif car $\mathbb{Z}$ est infini. Il suit que le corps contient $\mathbb{Z}/p\mathbb{Z}$ avec p-premier. En particulier il est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^n$ comme espace vectoriel (pour un certain n). Donc son cardinal est p^n. □

Nous verrons dans ce chapitre que réciproquement pour tout n, il existe un unique (à iso près) corps à p^n éléments.

1.3 Double extension

Soit $\mathbb{K}_1 \subset \mathbb{K}_2 \subset \mathbb{L}$. Combien voyez-vous d'extension ? Deux ? Et non, c'est trois.

Théorème V.59. Base télescopique

Soit $\mathbb{K}_1 \subset \mathbb{K}_2 \subset \mathbb{L}$. On suppose que $\mathbb{K}_1 \subset \mathbb{L}$ est une extension finie. Alors

$$[\mathbb{L} : \mathbb{K}_1] = [\mathbb{L} : \mathbb{K}_2] \cdot [\mathbb{K}_2 : \mathbb{K}_1].$$

Démonstration. La démonstration de ce théorème explique son nom. Soit $(e_1, \dots, e_d)$ une base de $\mathbb{K}_2$ comme $\mathbb{K}_1$-espace vectoriel. Soit $(f_1, \dots, f_{d'})$ une base de $\mathbb{L}$ comme $\mathbb{K}_2$-espace vectoriel.
Chaque élément y de $\mathbb{L}$ s'écrit

$$y = \sum_i x_i f_i$$

pour $x_i \in \mathbb{K}_2$. Or chaque x_i s'écrit

$$x_i = \sum_j m_{ij} e_j,$$

pour $m_{ij} \in \mathbb{K}_1$. Mais alors,

$$y = \sum_{i,j} m_{ij}(e_j f_i)$$

. Donc la famille $(e_i f_j)$ engendre $\mathbb{L}$ comme $\mathbb{K}_1$-espace vectoriel.

Supposons maintenant que

$$\sum_{i,j} m_{ij}(e_j f_i) = 0,$$

avec $m_{ij} \in \mathbb{K}_1$. Alors

$$\sum_i (\sum_j m_{ij} e_j) f_i = 0.$$

Comme $(f_1, \dots, f_{d'})$ est libre sur $\mathbb{K}_2$, on en déduit que

$$\forall i \qquad \sum_j m_{ij} e_j = 0.$$

Comme $(e_1, \dots, e_d)$ est libre sur $\mathbb{K}_1$, on en déduit que

$$\forall i, j \qquad m_{ij} = 0.$$

Ainsi la famille $(e_i f_j)$ est libre.

Finalement la famille $(e_i f_j)$ est une base de $\mathbb{L}$ comme $\mathbb{K}_1$-espace vectoriel. La formule du théorème en découle facilement. □

2 Corps des Fractions

Une première façon de construire des corps est de faire ce que l'on a fait pour construire $\mathbb{Q}$. Nous partions de $\mathbb{Z}$ et considérions les fractions $\frac{a}{b}$ comme un objet formel. En fait cela marche dès que l'anneau de départ est intègre. Mais au fait, vous aviez déjà vu un autre exemple : le corps des fractions rationnelles.

Soit A un anneau intègre. On considère l'ensemble quotient suivant

$$\mathrm{Frac}(A) := \{\frac{a}{b} \, : \, a \in A, b \in A - \{0\}\}/ \sim$$

où la relation d'équivalence $\sim$ est définie par

$$\frac{a}{b} \sim \frac{c}{d} \quad \Leftrightarrow \quad ad - bc = 0.$$

On définit ensuite sur A les deux opérations :

$$\frac{a}{b} \times \frac{c}{d} = \frac{ac}{db} \qquad \text{et} \qquad \frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{db}.$$

On vérifie que ces opérations sont bien définies (c'est-à-dire passent au quotient par $\sim$) et dont de $\mathrm{Frac}(A)$ un corps. C'est un peu long mais sans difficulté.

L'anneau de départ A s'injecte dans K par l'application

$$\iota \,:\, A \longrightarrow \mathrm{Frac}(A),\, a \longmapsto \frac{a}{1}.$$

Le corps $\mathrm{Frac}(A)$ vérifie la propriété universelle suivante. Tout morphisme d'anneau injectif de A dans un corps se prolonge de manière unique à $\mathrm{Frac}(A)$. C'est une manière de dire que $\mathrm{Frac}(A)$ est le plus petit corps contenant A.

3 Elément algébrique – Corps de décomposition

3.1 Polynôme minimal

Soit $\mathbb{K} \subset \mathbb{L}$ une extension de corps. Pensez ici à $\mathbb{Q} \subset \mathbb{C}$. Soit $\alpha \in \mathbb{L}$ et

$$\begin{array}{rccc} \varphi_\alpha \,: & \mathbb{K}[X] & \longrightarrow & \mathbb{L} \\ & P & \longmapsto & P(\alpha). \end{array}$$

Définition V.60: Algébrique/Transcendant

Un élément $\alpha \in \mathbb{L}$ est dit *algébrique sur* $\mathbb{K}$ s'il existe un polynôme non nul $P \in \mathbb{K}[X]$ tel que $P(\alpha) = 0$. Sinon il est dit *transcendant*.

Dit autrement, α est transcendant si φ est injectif et algébrique sinon. Dans ce dernier cas, le générateur unitaire de $\mathrm{Ker}\varphi$ est appelé le *polynôme minimal de* α. On le note μ_α.

Théorème V.61: Corps engendré

oit $\alpha \in \mathbb{L}$ algébrique sur $\mathbb{K}$. Alors le polynôme minimal de α est irréductible. De plus, l'image de φ_α est un corps, noté $\mathbb{K}[\alpha]$ et isomorphe à $\mathbb{K}[X]/(\mu_\alpha)$.

Démonstration. L'anneau quotient $\mathbb{K}[X]/(\mu_\alpha)$ s'injecte dans $\mathbb{L}$, donc il est intègre. Ce qui implique que μ_α est irréductible.
Mais alors, (μ_α) est un idéal maximal donc $\mathbb{K}[X]/(\mu_\alpha)$ est un corps. □

Par exemple, $\sqrt{2}$ est algébrique sur $\mathbb{Q}$ et son polynôme minimal est $X^2 - 2$.

Théorème V.62. Corps des nombres algébriques

L'ensemble des nombres de $\mathbb{L}$ qui sont algébriques sur $\mathbb{K}$ est un sous-corps de $\mathbb{L}$ et une extension de $\mathbb{K}$.

Démonstration. La remarque essentielle de cette démonstration est la suivante : φ_α n'est pas injective si et seulement si son image est de dimension finie si et seulement si α est algébrique.
Soit maintenant α et β dans $\mathbb{L}$ qui sont algébriques sur $\mathbb{K}$. On a déjà vu que $\alpha^{-1} \in \mathbb{K}[\alpha]$.
Considérons $\mathbb{K}[\alpha,\beta] := (\mathbb{K}[\alpha])[\beta]$. Comme β est algébrique sur $\mathbb{K}$ il l'est sur $\mathbb{K}[\alpha]$. Donc la dimension de $\mathbb{K}[\alpha,\beta]$ sur $\mathbb{K}[\alpha]$ est finie et $\mathbb{K}[\alpha,\beta]$ est un corps. D'après le théorème de la base télescopique, la dimension de $\mathbb{K}[\alpha,\beta]$ sur $\mathbb{K}$ est finie.
Or $\alpha+\beta$ appartient à $\mathbb{K}[\alpha,\beta]$ qui est un corps. Donc l'image de $\varphi_{\alpha+\beta}$ est incluse dans $\mathbb{K}[\alpha,\beta]$ et donc de dimension finie. Donc $\alpha+\beta$ est algébrique sur $\mathbb{K}$. On montre de même $\alpha\beta$ est algébrique sur $\mathbb{K}$. $\square$

Le théorème précédent implique par exemple que le nombre complexe

$$\frac{\sqrt{5}+i}{\sqrt[3]{2}+i\sqrt[5]{3}}$$

est algébrique sur $\mathbb{Q}$. Il n'est pas facile du tout d'en trouver le polynôme minimal. On peut tout de même en mimant la preuve trouver une borne supérieure sur son degré.

3.2 Corps de décomposition

Soit $P \in \mathbb{K}[X]$ un polynôme irréductible. L'anneau quotient $\mathbb{K}[X]/(P)$ est un corps car l'idéal (P) est maximal. Notons $\bar{X}$ la classe de X dans $\mathbb{K}[X]/(P)$. Alors, par définition $P(\bar{X}) = 0$, si bien que $\mathbb{K}[X]/(P)$ est un corps, une extension de $\mathbb{K}$ et contenant une racine P. De plus, $\mathbb{K}[X]/(P)$ est engendré par $\bar{X}$ et $\mathbb{K}$ comme anneau et

$$[\mathbb{K}[X]/(P) : \mathbb{K}] = \deg(P).$$

Le corps $\mathbb{K}[X]/(P)$ est appelé *corps de rupture de P*. C'est l'unique (à isomorphisme près) extension de $\mathbb{K}$ contenant une racine de P et engendré par celle-ci.
Nous admettrons le résultat suivant.

Théorème V.63. Corps de décomposition

Soit P un polynôme non nul de $\mathbb{K}[X]$. Alors il existe une extension $\mathbb{L}$ de $\mathbb{K}$ telle que P est scindé sur $\mathbb{L}$ et $\mathbb{L}$ est engendré par les racines de P et $\mathbb{K}$ comme anneau.
De plus, $\mathbb{L}$ est l'unique extension de $\mathbb{K}$ vérifiant ces propriétés. $\mathbb{L}$ est appelé le *corps de décomposition de P*.

4 Corps finis

Le but de cette section est de classifier tous les corps finis. L'énoncé est le suivant :

Théorème V.64. Corps finis

(i) Soit K un corps fini. Alors il existe un nombre premier p et un entier naturel non nul n tel que $\sharp K = p^n$.
(ii) Réciproquement, soit p un nombre premier et n un entier naturel non nul. Alors, il existe un corps à p^n éléments.
(iii) De plus, deux corps finis de même cardinal sont isomorphes.

On note $\mathbb{F}_q$ l'unique corps à $q = p^n$ éléments.

4.1 Premières propriétés et exemple

Soit K un corps fini. Sa caractéristique est non nulle (car il ne peut contenir $\mathbb{Z}$), notons là p. Alors K contient $\mathbb{Z}/p\mathbb{Z}$. Posons $n = [K : \mathbb{Z}/p\mathbb{Z}]$ la dimension de K comme $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel. Alors $\sharp K = p^n$.
La première assertion du théorème V.64 est démontrée.

Si $n = 1$, à la fois l'existence et l'unicité du théorème V.64 sont claires. On pose donc $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ pensé comme un corps. Regardons le plus petit cas qui suit $p = 2$ et $n = 2$. Soit K un corps de cardinal 4. On note 0 et 1 les éléments de $\mathbb{Z}/2\mathbb{Z}$ qui est inclus dans K. Soit x dans $\mathbb{K} - \{0, 1\}$.
On peut voit que $1 + x \neq 1$ (car $x \neq 0$), $1 + x \neq 0$ (car $x \neq 1$), $1 + x \neq x$ (car $1 \neq 0$). Donc $\mathbb{K} = \{0, 1, x, 1 + x\}$. On peut dresser la table d'addition de $\mathbb{K}$:

	0	1	x	$1+x$
0	0	1	x	$1+x$
1	1	0	$1+x$	x
x	x	$1+x$	0	1
$1+x$	$1+x$	x	1	0

On s'intéresse à présent à x^2. On voit que $x^2 \neq 0$ (car $x \neq 0$), $x^2 \neq 1$ (car $x^2 - 1 = (x - 1)^2$), $x^2 \neq x$ (car $x^2 - x = x(x - 1)$). Donc $x^2 = 1 + x$. On peut dresser la table de multiplication de $\mathbb{K}$:

	0	1	x	$1+x$
0	0	0	0	0
1	0	1	x	$1+x$
x	0	x	$1+x$	1
$1+x$	0	$1+x$	1	x

Avant de se lancer dans la preuve du théorème V.64, on va montrer un lemme dans $\mathbb{C}[X]$, $\mathbb{Z}[X]$ et $\mathbb{Z}$.

Lemme V.65 (Des divisibilités). *Soit m et n deux entiers naturels non nuls.*

(i) Dans $\mathbb{C}[X]$, $X^n - 1$ divise $X^m - 1$ si et seulement si n divise m.
(ii) De plus, $X^n - 1$ divise $X^m - 1$ dans $\mathbb{C}[X]$ si et seulement si il le divise dans $\mathbb{Z}[X]$.
(iii) Soit $a \geqslant 2$ un entier naturel. Alors $a^n - 1$ divise $a^m - 1$ si et seulement si n divise m.

Démonstration. Dans $\mathbb{C}$, on écrit
$$X^n - 1 = \prod_{\zeta \in \mathbb{U}_n} X - \zeta,$$
où $\mathbb{U}_n$ désigne l'ensemble des racines n-ième de l'unité (les $e^{\frac{2ik\pi}{n}}$). Alors $X^n - 1$ divise $X^m - 1$ si et seulement si $\mathbb{U}_n$ est inclus dans $\mathbb{U}_m$ si et seulement si n divise m.

Il est clair que si $X^n - 1$ divise $X^m - 1$ dans $\mathbb{Z}[X]$ alors il le divise dans $\mathbb{C}[X]$. Réciproquement, supposons que $X^n - 1$ divise $X^m - 1$ dans $\mathbb{C}[X]$. Effectuons la division euclidienne de $X^n - 1$ par $X^m - 1$ dans $\mathbb{Q}[X]$. Comme $X^m - 1$ est unitaire, on ne divise jamais et le quotient Q et le reste R sont à coefficients entiers. Donc
$$X^n - 1 = (X^m - 1)Q + R \qquad Q, R \in \mathbb{Z}[X].$$
Effectuons la division euclidienne de $X^n - 1$ par $X^m - 1$ dans $\mathbb{C}[X]$. On fait les même calculs que lorsque nous pensions les coefficients des polynômes dans $\mathbb{Q}$. Donc les quotients et restes sont les mêmes. Mais alors comme $X^n - 1$ divise $X^m - 1$ dans $\mathbb{C}[X]$, $R = 0$. cdfd.

Si n divise m, alors $X^n - 1$ divise $X^m - 1$ dans $\mathbb{Z}[X]$. Donc en substituant a à X, $a^n - 1$ divise $a^m - 1$. Réciproquement supposons que $a^n - 1$ divise $a^m - 1$. On écrit $m = nq + r$ avec $0 \leqslant r < n$. Comme
$$a^n - 1 = (a - 1)(a^{n-1} + a^{n-2} + \cdots + 1),$$
l'entier $(a^{n-1} + a^{n-2} + \cdots + 1)$ divise
$$\begin{aligned} 1 + \cdots + a^{m-2} + a^{m-1} = \quad & (1 + \cdots + a^{n-1}) \\ & +(1 + \cdots + a^{n-1})a^n \\ & +(1 + \cdots + a^{n-1})a^{2n} \\ & \vdots \\ & +(1 + \cdots + a^{n-1})a^{(q-1)n} \\ & +(1 + \cdots + a^{r-1})a^{qn}. \end{aligned}$$

L'entier $N := (a^{n-1} + a^{n-2} + \cdots + 1)$ est de la forme $1 + ab$ (un plus un multiple de a. Il est donc premier avec a (par Bezout si vous voulez). Par ailleurs, il divise la somme ci-dessus ainsi que tous ses premiers termes. Donc N divise le dernier terme de la somme, c'est-à-dire $(1 + \cdots + a^{r-1})a^{qn}$. Mais alors, le lemme de Gauss implique que N divise $(1 + \cdots + a^{r-1})$. Le seul moyen (inégalités) est d'avoir $r = 0$. Donc n divise m. □

4.2 Factorisation d'un polynôme dans $\mathbb{F}_p[X]$

Soit d un entier naturel non nul. On note $\mathcal{I}(d, p)$ l'ensemble des polynômes de $\mathbb{F}_p[X]$ unitaires irréductibles et de degré d.

Lemme V.66. *Si $\mathcal{I}(d, p)$ est non vide, alors il existe un corps à p^d éléments.*

Démonstration. En effet, $\mathbb{F}_p[X]/(P)$ convient pour $P \in \mathcal{I}(d, p)$. □

On veut donc montrer que $\mathcal{I}(d, p)$ est non vide.

Théorème V.67: Factorisation de $X^{p^n} - X$

Soit n un entier non nul. Dans $\mathbb{F}_p[X]$, on a

$$X^{p^n} - X = \prod_{d \mid n} \prod_{P \in \mathcal{I}(d,p)} P.$$

Démonstration. L'équation de la proposition est la décomposition de $X^{p^n} - X$ en produit de polynômes irréductibles. Il suffit donc de montrer les deux assertions suivantes, pour tout polynôme irréductible unitaire P de $\mathbb{F}_p[X]$:

(i) P^2 ne divise pas $X^{p^n} - X$;

(ii) P divise $X^{p^n} - X$ si et seulement si $\deg(P)$ divise n.

Pour la première assertion, supposons par l'absurde que $X^{p^n} - X = P^2 Q$. Alors en dérivant on obtient

$$-1 = P(2P'Q + PQ').$$

Donc P divise -1. Contradiction.

Supposons maintenant que $d = \deg(P)$ divise n. Soit $\mathbb{L} = \mathbb{F}_p[X]/(P)$ et $\alpha \in \mathbb{L}$ la classe de X. Alors $P(\alpha) = 0$.
Si $\alpha = 0$, $P = X$ et il n'y a rien à montré. Supposons donc $\alpha \neq 0$. Alors α est un élément du groupe multiplicatif $\mathbb{L} - \{0\}$ de cardinal $p^d - 1$. Le théorème de Lagrange montre donc que $\alpha^{p^d - 1} = 1$. D'après le lemme V.65, on a aussi $\alpha^{p^n - 1} = 1$ (car $p^d - 1$ divise $p^n - 1$). Mais alors α est racine de $X^{p^n} - X$.
Comme P et $X^{p^n} - X$ ont une racine commune dans $\mathbb{L}$ leur pgcd n'est pas 1. Or, grâce à l'algorithme d'Euclide, le pgcd ne dépend pas du corps contenant les coefficients des polynômes. Donc, dans $\mathbb{F}_p[X]$, le pgcd de P et $X^{p^n} - X$ n'est pas 1. Mais alors, comme P est irréductible, P divise $X^{p^n} - X$.

Supposons enfin que P divise $X^{p^n} - X$. Notons encore $d = \deg(P)$, $\mathbb{L} = \mathbb{F}_p[X]/(P)$ et $\alpha \in \mathbb{L}$ la classe de X. On peut encore supposer $\alpha \neq 0$. On fait la division euclidienne : $n = ds + r$ avec $0 \leqslant r < d$.
Comme P divise $X^{p^n} - X$, $\alpha^{p^n - 1} = 1$ et $\alpha^{p^n} = \alpha$. Donc

$$\alpha^{p^n} = (\alpha^{p^{ds}})^{p^r} = \alpha^{p^r} = \alpha.$$

On en déduit que si β est une puissance de α alors

$$\beta^{p^r} = \beta.$$

Si par l'absurde $r \neq 0$, on a

$$(x + y)^{p^r} = x^{p^r} + y^{p^r} \qquad \forall x, y \in \mathbb{L}$$

et

$$x^{p^r} = x \qquad \forall x \in \mathbb{F}_p.$$

On en déduit que

$$x^{p^r} = x \qquad \forall x \in \mathbb{L}. \tag{4.1}$$

En particulier le polynôme $X^{p^r} - X$ de degré p^r a au moins $\sharp\mathbb{L} = p^d$ racines. Contradiction. □

Exemple 14. Dans $\mathbb{F}_2[X]$, on obtient

$$X^8 - X = X(X-1)(X^3+X+1)(X^3+X^2+1).$$

Dans $\mathbb{F}_3[X]$, on obtient

$$X^9 - X = X(X-1)(X+1)(X^2+1)(X^2+X-1)(X^1-X-1).$$

4.3 Existence

L'égalité des degré dans la proposition V.67 donne

$$p^n = \sum_{d\,|\,n} \sharp\mathcal{I}(d,p)d. \tag{4.2}$$

Théorème V.68. Existence polynôme irréductible

Dans $\mathbb{F}_p[X]$ il existe des polynômes irréductibles de tout degré. En particulier, pour tout n il existe un corps à p^n éléments.

Démonstration. Il s'agit de montrer que $\mathcal{I}(d,p)$ est non vide. Or, d'après (4.2), on a

$$p^n = \sharp\mathcal{I}(n,p)n + \sum_{d\,|\,n \quad d<n} \sharp\mathcal{I}(d,p)d$$

et

$$\sharp\mathcal{I}(n,p)n \leqslant p^n.$$

Mais alors

$$p^n \leqslant \sharp\mathcal{I}(n,p)n + \sum_{d\,|\,n \quad d<n} p^d \leqslant \sharp\mathcal{I}(n,p)n + \sum_{k=0}^{n-1} p^k \leqslant \sharp\mathcal{I}(n,p)n + \frac{p^n-1}{p-1} < \sharp\mathcal{I}(n,p)n + p^n.$$

Donc $\sharp\mathcal{I}(n,p)$ est non nul.

Le lemme du début et l'existence de polynômes irréductibles impliquent l'existence de corps. □

4.4 Unicité

On peut montrer que

$$\sharp\mathcal{I}(50,2) = 22\,517\,997\,465\,744.$$

Cela fait de nombreuses manières de construire $\mathbb{F}_{2^{50}}$. Mais l'on obtient toujours la même chose !!

Démonstration. Soit $\mathbb{L}$ un corps à p^n éléments et P un polynômes irréductible unitaire de degré n dans $\mathbb{F}_p[X]$. Posons $\mathbb{K} = \mathbb{F}_p[X]/(P)$.
Tous les éléments non nuls de $\mathbb{L}$ vérifient, $\alpha^{p^n-1} = 1$, en vertu du théorème de Lagrange appliqué dans le groupe multiplicatif $\mathbb{L} - \{0\}$. Mais alors, pour tout $\alpha \in \mathbb{L}$ on a $\alpha^{p^n} = \alpha$. On en déduit que

$$X^{p^n} - X = \prod_{\alpha\in\mathbb{L}} (X - \alpha).$$

Dans $\mathbb{F}_p[X]$, on sait que P divise $X^{p^n} - X$. Donc il existe $\alpha_0 \in \mathbb{L}$ tel que $P(\alpha_0) = 0$. Comme P est irréductible sur $\mathbb{F}_p$, P est le polynôme minimal de α_0 sur $\mathbb{F}_p$. Ainsi, le morphisme

$$\mathbb{F}_p[X] \longrightarrow \mathbb{L},\ Q \longmapsto Q(\alpha_0)$$

induit un morphisme injectif

$$\mathbb{F}_p[X]/(P) \longrightarrow \mathbb{L}.$$

Par égalité des cardinaux ce morphisme injectif est en fait un isomorphisme. □

5 Corps des nombres constructibles à la règle et au compas

Dans cette dernière section nous allons voir deux sous-corps de $\mathbb{R}$ et $\mathbb{C}$ inspirés par les mathématiques de la Grece antique. On va développer des outils permettant d'étudier des problèmes comme celui de la trisection de l'angle, la quadrature du cercle ou la construction des polyèdres réguliers.
Nous identifions le corps $\mathbb{C}$ au plan euclidien $\mathbb{R}^2$. Pour $z_1 \neq z_2$ dans $\mathbb{C}$, on note (z_1z_2) la droite passant par z_1 et z_2, et $\mathscr{C}(z_1, z_2)$ le cercle de centre z_1 et passant par z_2.
Soit S une partie de $\mathbb{C}$. On dit qu'un nombre complexe est *élémentairement constructible* à partir de S s'il existe $z_1 \neq z_2 \in S$ et $z_3 \neq z_4 \in S$ tels que l'une des affirmations suivantes est vrai :

(i) les droites (z_1z_2) et (z_3z_4) sont distinctes et sécantes en z.

(ii) les cercles $\mathscr{C}(z_1, z_2)$ et $\mathscr{C}(z_3, z_4)$ sont distincts et sécants en z.

(iii) la droite (z_1z_2) et le cercle $\mathscr{C}(z_3, z_4)$ s'intersectent en z.

On dit qu'un nombre complexe z est *constructible* s'il existe une suite $0, 1, i, z_1, \ldots, z_n = z$ telles que, pour tout $1 \leqslant i \leqslant n$, z_k est élémentairement constructible à partir de $\{0, 1, i, \ldots, z_{k-1}$, pour tout $k \in \{1, \ldots, n\}$. On note $\mathscr{K}$ l'ensemble des nombres complexes constructibles. Enfin, un nombre réel x est *constructible* s'il est constructible en tant que nombre complexe.

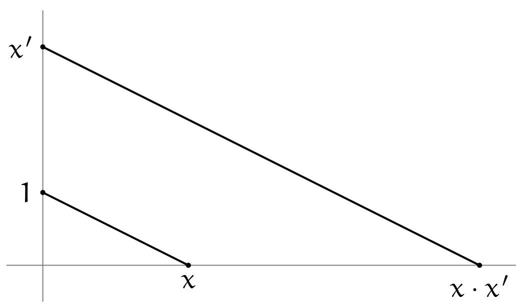
Théorème V.69. Corps des nombres constructibles

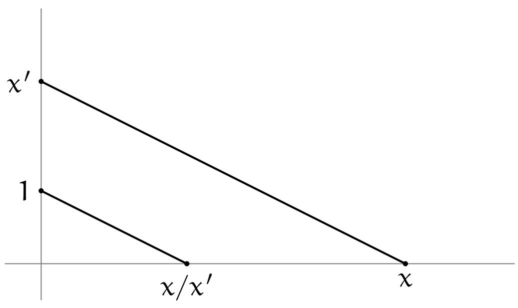
On a

(i) Les ensembles $\mathscr{K}$ et $\mathscr{K} \cap \mathbb{R}$ sont des corps.

(ii) Un élément $z \in \mathbb{C}$ appartient à $\mathscr{K}$ si et seulement si ses parties réelle et imaginaire appartiennent à $\mathscr{K} \cap \mathbb{R}$.

Démonstration. La deuxième assertion dit juste que l'on peut construire un point complexes ses coordonnées étant connues. Et que réciproquement, ses coordonnées sont constructibles à partir de z.
Comme on peut construire les paralellogrammes $\mathscr{K}$ est stable par addition. Comme on peut construire les symétries centrales $\mathscr{K}$ est stable par opposé.
On peut aussi construire la paralelle à une droite passant par un point. Mais alors en utilisant le théorème de Thalès on voit facilement que $\mathscr{K} \cap \mathbb{R}$ est stable par produit et inverse. Voir les dessins ci-dessous.





□

La théorie des corps, via le théorème suivant permet de démonter que plusieurs problèmes grecs n'ont pas de solution.

Théorème V.70. Obstruction à la constructibilité

Soit $z \in \mathscr{K}$. Alors z est algébrique sur $\mathbb{Q}$ et le degré $[\mathbb{Q}[z] : \mathbb{Q}]$ de l'extension est une puissance de 2.

Démonstration. Soit $A = x_1 + iy_2$ et $B = x_2 + iy_2$ des nombres complexes. Alors la droite (AB) a une équation de la forme :

$$\alpha x + \beta y + \gamma = 0 \tag{5.1}$$

avec α, β et γ dans $\mathbb{Q}(\alpha, \beta)$. Et le cercle $\mathscr{C}(AB)$ a une équation de la forme :

$$x^2 + y^2 + \alpha x + \beta y + \gamma = 0 \tag{5.2}$$

avec α, β et γ dans $\mathbb{Q}(\alpha, \beta)$.
Soit $\mathbb{L}$ un sous-corps de $\mathbb{R}$. Montrons que si $z = x + iy$ est élémentairement constructible à partir $\mathbb{L} + i\mathbb{L}$ alors $[\mathbb{L}(x) : \mathbb{L}]$ et $[\mathbb{L}(y) : \mathbb{L}]$ valent 1 ou 2.
Si z est l'intersection de deux droites passant par des points dont les coordonnées sont dans $\mathbb{L}$, ses coordonnées s'obtiennent en résolvant un système linéaire à coefficient dans $\mathbb{L}$ donc sont dans $\mathbb{L}$. Ainsi $\mathbb{L}(x) = \mathbb{L}(y) = \mathbb{L}$.
Si z est dans l'intersection d'une droite passant par des points dont les coordonnées sont dans $\mathbb{L}$ et d'un cercle construit à partir de tels points, ses coordonnées vérifient

$$\begin{cases} \alpha x + \beta y + \gamma = 0 \\ x^2 + y^2 + \alpha' x + \beta' y + \gamma' = 0 \end{cases}$$

avec $\alpha, \alpha', \beta, \beta', \gamma$ et γ' dans $\mathbb{L}$.
Supposons $\beta \neq 0$. Alors y s'exprime en fonction de x et $\mathbb{L} \subset \mathbb{L}(y) \subset \mathbb{L}(x)$. On tire alors y de la première équation et l'injecte dans la seconde. Le nombre x vérifie une équation de degré 2 à coefficients dans $\mathbb{L}$. Donc $[\mathbb{L}(x) : \mathbb{L}] = 1$ ou 2.
Supposons $\beta = 0$. Alors x appartient à $\mathbb{L}$. Mais alors, la deuxième équation montre que y vérifie une équation de degré 2 à coefficients dans $\mathbb{L}$. Donc $[\mathbb{L}(y) : \mathbb{L}] = 1$ ou 2.

Si z est dans l'intersection de deux cercles, ses coordonnées vérifient

$$\begin{cases} x^2 + y^2 + \alpha x + \beta y + \gamma = 0 \\ x^2 + y^2 + \alpha' x + \beta' y + \gamma' = 0 \end{cases}$$

avec $\alpha, \alpha', \beta, \beta', \gamma$ et γ' dans $\mathbb{L}$. En remplaçant la première équation par la différence des deux, on se ramène au cas précédent. □

Le problème de duplication du cube est le suivant. Etant donné un cube de côté volume V peut-on en construire un de volume $2V$. Il s'agit donc de construire $\sqrt[3]{2}$. Si cela était possible le théorème dirait que $[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}]$ serait une puissance de deux.
Or $\sqrt[3]{2}$ annule $X^3 - 2$. Ce polynôme est de degré 3 et n'a pas de racine dans $\mathbb{Q}$: il est donc irréductible dans $\mathbb{Q}[X]$. C'est donc le polynôme minimal de $\sqrt[3]{2}$ et $[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = 3$. Contradiction.

Chapitre 6

Géométrie Projective

Sommaire

1 Géométrie projective : un premier contact

1.1 Améliorer la géométrie affine plane

Deux propriétés fondamentales de la géométrie affine plane sont :

(i) Par deux points distincts du plan passe une unique droite .

(ii) L'intersection de deux droites distinctes est soit vide soit réduit à un point.

Ces deux propriétés ont une certaine symétrie qui est brisée par l'alternative dans la seconde. On se propose alors de construire une géométrie pour laquelle :

Deux droites distinctes s'intersectent en un point et un seul.

Soit $\mathcal{P}$ un plan affine (réel) et E l'espace vectoriel sous-jacent. On se propose de rajouter des points à $\mathcal{P}$ et à ses droites de manière à obtenir la propriété ci-dessus.
La question est donc quel est le point commun de deux droites parallèles. La réponse qui semble s'imposer est *leur direction.* Une direction est un vecteur non nul défini à une constante multiplicative près ou encore une droite vectorielle de E. Notons $\mathbb{P}E$ l'ensemble des droites vectorielles de E. Posons

$$\mathbb{P} = \mathcal{P} \cup \mathbb{P}E.$$

La réunion ci-dessus est formelle.
Toute partie de $\mathbb{P}$ de la forme d union sa direction est appelée une *droite de* $\mathbb{P}$. On a alors :

Deux droites distinctes de $\mathbb{P}$ *s'intersectent en exactement un point.*

En géométrie affine nous avions également la propriété :

Par deux points distincts de $\mathcal{P}$ *passent une droite et une seule.*

Cette propriété est pour l'instant fausse dans $\mathbb{P}$. En effet, par deux points distincts de $\mathbb{P}E$ ne passent aucune droite. Pour remédier à cela nous décrétons que $\mathbb{P}E$ est une droite de $\mathbb{P}$. ; Nous l'appellerons plus tard *droite à l'infini.* Nous avons maintenant les deux propriétés suivantes :

Deux droites distinctes de $\mathbb{P}$ *s'intersectent en exactement un point.*
Par deux points distincts de $\mathbb{P}$ *passent une droite et une seule.*

Ces deux propriétés énoncées de manière brève, symétrique et esthétique recouvre déjà des réalités différentes de géométrie affine :

(i) Prenons une droite d et un point A du plan affine. Alors, par A passe une unique droite parallèle à d.
En géométrie projective, A et la direction de d sont deux points par lequel passe une droite.

(ii) Deux droites se coupent en un point ou ont même direction.
En géométrie projective, deux droites se coupent. Pour distinguer les deux cas il faut regarder si le point d'intersection est dans $\mathcal{P}$ ou dans $\mathbb{P}(E)$.

1.2 L'ensemble $\mathbb{P}(E)$

Soit k un corps commutatif et E un k-espace vectoriel de dimension finie. Nous noterons $\mathbb{P}(E)$ l'ensemble des droites vectorielles de E.
Essayons de décrire ensemblistement E. Pour cela, on se donne une base $(e_0, e_1, \cdots, e_n)$ une base de E. Soit $\mathcal{H}$ le plan affine de E constitué des points dont la première coordonnée vaut 1 et H sa direction. L'application

$$\begin{array}{rccc} \eta : & \mathcal{H} & \longrightarrow & \mathbb{P}(E) \\ & v & \longmapsto & k.v \end{array}$$

est une injection.
Soit d un élément de $\mathbb{P}(E)$. Alors,
- soit d rencontre $\mathcal{H}$ en un point et un seul ; c'est-à-dire appartient à l'image de η,
- soit d est inclus dans H.

Autrement dit,
$$\mathbb{P}(E) = \eta(\mathcal{H}) \cup \mathbb{P}(H).$$
De plus, $\mathcal{H}$ s'identifie à k^n.

Exercice 12. *Dessiner H, $\mathcal{H}$ lorsque $n = 1$ et $k = \mathbb{R}$.*

Ceci décrit $\mathbb{P}(E)$ par induction sur la dimension de E :
- Si $\dim(E) = 1$, $\mathbb{P}(E)$ est réduit à un point.
- Si $\dim(E) = 2$, $\mathbb{P}(E) =: k\mathbb{P}^1$ est la réunion de k est d'un point (∞).
- Si $\dim(E) = 3$, $\mathbb{P}(E) =: k\mathbb{P}^2$ est la réunion de k^2 et de $k\mathbb{P}^1$.
- $k\mathbb{P}^n = k^n \cup k\mathbb{P}^{n-1}$.

Ainsi, $k\mathbb{P}^2$ est un candidat très raisonnable pour jouer le rôle du $\mathbb{P}$ du paragraphe 1.
L'ensemble $\mathbb{P}(E)$ est appelé *l'espace projectif* de E. Nous venons de voir que $\mathbb{P}(E)$ est la réunion d'un espace affine de dimension n ($\mathcal{H}$) et d'un espace projectif plus petit $\mathbb{P}(E)$. Ceci explique que nous appelons $n = \dim(E) - 1$ la dimension de $\mathbb{P}(E)$.

2 Quelques structures sur $\mathbb{P}(E)$

La section précédente était une introduction un peu informelle. On repart formellement à zéro.

2.1 Espaces et sous-espaces projectifs

Soit E un k-espace vectoriel. *L'espace projectif* $\mathbb{P}(E)$ est l'ensemble des droites vectorielles de E. Tout vecteur non nul v de E engendre une unique droite vectoriel kv que l'on note $[v]$. On obtient ainsi une application surjective
$$\begin{array}{cccc} \pi : & E & \longrightarrow & \mathbb{P}(E) \\ & v & \longmapsto & [v] \end{array}$$
On peut donc penser à $\mathbb{P}(E)$ comme à un quotient
$$\mathbb{P}(E) = \frac{E - \{0\}}{v \sim v' \text{ ssi } \exists \lambda \in k \quad v' = \lambda v}.$$
Si F est un sous-espace vectoriel de E alors toute droite vectorielle de F est une droite vectorielle de E. On obtient une inclusion $\mathbb{P}(F) \subset \mathbb{P}(E)$. Une partie de $\mathbb{P}(E)$ de la forme $\mathbb{P}(F)$ est appelé une un *sous-espace projectif*.

Dimension. Par définition $\dim(\mathbb{P}(E)) = \dim(E) - 1$. Nous avons déjà vu une explication pour ce -1 : $\mathbb{P}(E)$ s'identifie à la d'un hyperplan affine de E et d'un espace projectif plus petit.
Un *point* de $\mathbb{P}(E)$ est un élément de $\mathbb{P}(E)$. C'est aussi un sous-espace projectif de dimension 0. Une *droite* de $\mathbb{P}(E)$ est un sous-espace projectif de $\mathbb{P}(E)$ de dimension un (donc avec E de dimension 2). Une *hyperplan* de $\mathbb{P}(E)$ est un sous-espace projectif de $\mathbb{P}(E)$ de dimension $\dim(\mathbb{P}(E)) - 1$.

2.2 Homographies

Le groupe $\mathrm{GL}(E)$ agit naturellement sur E et envoie toute droite vectorielle sur une droite vectorielle. Ce groupe agit donc sur $\mathbb{P}(E)$. De plus, le sous-groupe H des homothéties de $\mathrm{GL}(E)$ agit trivialement sur $\mathbb{P}(E)$. Ainsi, le quotient $\mathrm{PGL}(E) := \mathrm{GL}(E)/H$ agit sur $\mathbb{P}(E)$. Les éléments de $\mathrm{PGL}(E)$ sont appelées homographies.

Théorème VI.71: Homographie et sep

L'image d'un sous-espace projectif par une homographie est un sous-espace projectif de même dimension.

De plus, pour tout $0 \leqslant k \leqslant \dim(E) - 1$, l'action de $\mathrm{PGL}(E)$ sur l'ensemble des sous-espaces projectifs de dimension k est transitive.

Démonstration. Il suffit de voir que $\mathrm{GL}(E)$ agit transitivement sur l'ensemble des sous-espaces vectoriels de E de dimension $k+1$. Ce qui est un exercice facile d'algèbre linéaire (pensez au théorème de la base incomplète). □

Théorème VI.72: Points et sep

Soit $\mathbb{P}(E)$ un espace projectif de dimension n (donc $\dim(E) = n+1$) et $1 \leqslant k \leqslant n-1$. Soit $p_1, \ldots, p_{k+1}$ $k+1$ points de $\mathbb{P}(E)$.
Alors il existe un sous-espace projectif de dimension k contenant ces points.
De plus, si $k = 1$ et $p_1 \neq p_2$, il existe une unique droite projective contenant p_1 et p_2. Elle est notée $(p_1 p_2)$.

Démonstration. Il suffit de relever la situation à E. Les points p_i sont des droites vectorielles l_i de E. Soit v_i non nul sur l_i. Considérons $F = \overrightarrow{(}v_1, \ldots, v_{k+1})$. C'est un sev de E de dimension au plus égale à $k+1$. Il est donc inclus dans un sev $\tilde{F}$ de dimension $k+1$. Alors $\mathbb{P}(\tilde{F})$ convient.

Si $k = 1$ et $p_1 \neq p_2$ alors la famille (v_1, v_2) est libre. Donc F a dimension 2. Alors $\mathbb{P}(F)$ est la seule droite projective qui contienne p_1 e p_2. □

Regardons maintenant l'action de $\mathrm{PGL}(E)$ sur les uples de points distincts.

Théorème VI.73: Actions sur $n+2$-uplets

Soit $\mathbb{P}(E)$ un espace projectif de dimension n (donc $\dim(E) = n+1$). Soit $\mathcal{R}$ l'ensemble des $n+2$-uplets $(p_1 \ldots, p_{n+2})$ de points de $\mathbb{P}(E)$ tels que aucun des $n+1$-uplets (il y en a $n+2$) extraits (en enlevant un des points) n'est inclus dans un hyperplan affine.
Le groupe $\mathrm{PGL}(E)$ agit transitivement sur $\mathcal{R}$.

Démonstration. Il est clair que $\mathrm{PGL}(E)$ agit sur $\mathcal{R}$. Montrons que l'action est transitive. Soit donc (p_i) et (q_i) deux éléments de $\mathcal{R}$. On relève la situation à E. Les points p_i sont des droites vectorielles l_i de E. Soit v_i non nul sur l_i. De même on obtient les w_i. D'après l'hypothèse, $(v_1, \ldots, v_{n+1})$ et $(w_1, \ldots, w_{n+1})$ sont deux bases de E. Il existe donc $g \in \mathrm{GL}(E)$ tel que $g.v_i = w_i$ pour tout i. Quitte à composer avec g on peut donc supposer que pour tout $i = 1, \ldots, n+1$, $w_i = v_i$.
Posons $\mathcal{B} = (v_1, \ldots, v_{n+1})$. Soit $(\lambda_1, \ldots, \lambda_{n+1})$ et $(\mu_1, \ldots, \mu_{n+1})$ les coordonnées de v_{n+2} et w_{n+2} dans la base $\mathcal{B}$.
Comme $(v_1, \ldots, v_n, v_{n+2})$ est libre, λ_{n+1} est non nul. De même, tous les λ_i et tous les μ_i sont non nuls. Soit g dans $\mathrm{GL}(E)$ dont la matrice dans la base $\mathcal{B}$ est diagonale avec $(\frac{\mu_1}{\lambda_1}, \ldots, \frac{\mu_{n+1}}{\lambda_{n+1}})$ sur la diagonale. On a bien $gv_{n+2} = w_{n+2}$ et pour $i = 1, \ldots, n+1$, $g.v_i \in l_i$ donc $gp_i = p_i$. □

Exercice 13. *Montrer qu'en fait l'action de* $\mathrm{PGL}(E)$ *sur* $\mathcal{R}$ *est simplement transitive.*

2.3 Coordonnées projectives

Soit $\mathcal{B} = (e_0, \ldots, e_n)$ une base de E. Utilisant les coordonnées pour repérer les éléments de E, on obtient

$$\mathbb{P}(E) = \frac{\{(x_0, \ldots, x_n) \in k^n - \{0\}}{(x_0, \ldots, x_n) \sim (\lambda x_0, \ldots, \lambda x_n) \qquad \forall \lambda \in k^*}.$$

Un élément de ce quotient est noté

$$[x_0 : \cdots : x_n].$$

La notation : fait référence à la division puisque lorsque les coordonnées sont non nulles

$$[x_0 : \cdots : x_n] = [y_0 : \cdots : y_n]$$

si et seulement si $\frac{x_i}{x_j} = \frac{y_i}{y_j}$ pour tout $i \neq j$.

3 Lien Affine Projectif

3.1 Carte affine et droite à l'infini

Soit E de dimension $n+1$ et $\mathcal{H}$ un hyperplan affine de E ne contenant pas 0. Notons H la direction de $\mathcal{H}$. Comme nous l'avons déjà vu, $\mathcal{H}$ s'injecte dans $\mathbb{P}(E)$, c'est-à-dire s'identifie à une partie de $\mathbb{P}(E)$. Cette application associe à un point de $\mathcal{E}$ la droite vectorielle de E qu'il engendre et vue comme un point de $\mathbb{P}(E)$. Le complémentaire de l'image est $\mathbb{P}(H)$. En effet, les droites vectorielles de E qui ne rencontrent pas $\mathcal{H}$ sont exactement celles incluses dans H.

Théorème VI.74. Sous-espaces affines et projectifs

Dans la situation ci-dessus, on a :

(i) L'intersection d'un sous-espace projectif de dimension d de $\mathbb{P}(E)$ et de $\mathbb{P}(E)-\mathbb{P}(H)$ est soit vide (s'il est inclus dans $\mathbb{P}(H)$) soit un sous-espace affine de dimension d.

(ii) Réciproquement, tout sous-espace affine F de $\mathcal{H}$ est inclus dans un unique sous-espace projectif minimal de $\mathbb{P}(E)$. De plus, l'intersection de ce dernier et de $\mathcal{H}$ est F.

(iii) Toute homographie de $\mathbb{P}(E)$ qui préserve $\mathbb{P}(H)$ définit par restriction une application affine de $\mathbb{P}(E)-\mathbb{P}(H)$.

(iv) Réciproquement, toute application affine inversible de $\mathbb{P}(E)-\mathbb{P}(H)$ se prolonge de manière unique en une homographie de $\mathbb{P}(E)$.

Démonstration. Soit $\mathbb{P}(G)$ un sous-espace projectif de $\mathbb{P}(E)$ où G est un sous-espace vectoriel de E de dimension $d+1$.
Si $G\subset H$ alors G est parallèle à $\mathcal{H}$ et $\mathcal{H}\cap G=\emptyset$. Alors, $\mathbb{P}(G)\cap\mathcal{H}$ est vide aussi.
Sinon, $G\cap\mathcal{H}$ est un sous-espace affine de direction $G\cap H$. Alors $\mathbb{P}(G)\cap\mathcal{H}$ s'identifie à $G\cap\mathcal{H}$ est un sous-espace affine de dimension d.

Réciproquement, soit $F\subset\mathcal{H}$ un sous-espace affine de dimension d. Soit $\tilde{F}$ le sous-espace vectoriel engendré par F : il est de dimension $d+1$. Ainsi, $\mathbb{P}(\tilde{F})$ est le seul sous-espace projectif contenant F.

Pour la troisième assertion, on va expliciter les choses en choisissant une base. Soit $\mathcal{B}=(e_1,\dots,e_{n+1})$ une base de E telle que

$$\mathcal{H}=\{v\in E\,:\,e_{n+1}^*(v)=1\}.$$

Soit $g\in\mathrm{GL}(E)$ qui préserve H. Alors la matrice de g dans la base est de la forme

$$\mathrm{Mat}_{\mathcal{B}}(g)=\begin{pmatrix}A & w\\ 0 & \lambda\end{pmatrix}$$

Comme g est inversible λ est non nul. Comme seule la classe de g dans $\mathrm{GL}(E)$ compte, on peut supposer que $\lambda=1$. Soit v un point de $\mathcal{H}$. Ses coordonnées dans la base $\mathcal{B}$ sont de la forme

$$v=\begin{pmatrix}x_1\\ \vdots\\ x_n\\ 1\end{pmatrix}$$

Mais alors

$$gv=[AX+w:1]$$

appartient à $\mathcal{H}$. Comme $X\longmapsto AX+w$ est affine l'assertion suit.

Réciproquement soit φ une application affine de $\mathcal{H}$ dans lui même. Alors, en coordonnée $\varphi(X)=AX+B$ pour une matrice inversible A et un vecteur colonne B. Alors la matrice

$$\mathrm{Mat}_{\mathcal{B}}(g)=\begin{pmatrix}A & B\\ 0 & 1\end{pmatrix}$$

fournit unne homographie qui étend φ. □

4 La droite projective

Soit $E = k^2$ le k-espace vectoriel de dimension 2 standard. Deux points $[x : y]$ et $[x' : y']$ sonnt égaux si et seulement si $\frac{x}{y} = \frac{x'}{y'}$, au moins si y et y' sont non nuls. On obtient donc

$$\mathbb{P}(k^2) = k\mathbb{P}^1 = \{[t : 1] \ : \ t \in k\} \cup \{[1 : 0]\}.$$

Pensant à $[1 : 0]$ comme à $\frac{1}{0}$, on le note ∞. Alors

$$k\mathbb{P}^1 = k \cup \{\infty\}.$$

Exercice 14. *Montrer que toute homographie est de la forme*

$$\begin{array}{cccc} \varphi : & k\mathbb{P}^1 & \longrightarrow & k\mathbb{P}^1 \\ & [x : y] & \longmapsto & [ax + by : cx + dy] \end{array}$$

avec a, b, c et d dans k tels que $ad - bc \neq 0$. Si on prend la convention $\frac{\neq 0}{0} = \infty$, on obtient

$$\varphi(t) = \frac{at + b}{ct + d} \qquad \forall t \in k$$

et on reconnait les homographies usuelles du plan complexe lorsque $k = \mathbb{C}$.

5 Le plan projectif

Soit E un k-espace vectoriel de dimension 3. On s'intéresse à $\mathbb{P}(E) = k\mathbb{P}^2$.

Théorème VI.75: Incidences droites-points

(i) Par deux points distincts passe une unique droite.

(ii) Deux droites distinctes s'intersectent en un unique point.

Démonstration. La première propriété est générale. Pour la seconde soit $\mathbb{P}(F_1)$ et $\mathbb{P}(F_2)$ deux droites de $\mathbb{P}(E)$. Alors F_1 et F_2 sont deux hyperplans distincts de E. Donc $F_1 \cap F_2$ est un sous-espace vectoriel de codimension 2. C'est donc un point de $\mathbb{P}(E)$. □

Fixons des coordonnées (x, y, z) sur k^3. Soit $\mathbb{P}(F)$ une droite projective et $\mathbb{P}(k^3)$. Alors F est unn hyperplan de k^3. C'est donc le noyau d'une forme linéaire $\varphi = ax + by + cz = 0$ pour $a, b, c \in k$ non tous nuls.
et choisissons l'hyperplan affine $z = 1$.

Supposons un instant que k est fini, disons de cardinal q. Alors $k\mathbb{P}^2 = k^2 \cup k\mathbb{P}^1$ est de cardinal $q^2 + q + 1$.
De plus chaque droite est de cardinal $q + 1$.
Il y a autant de droites que d'hyperplans dans E, c'est-à-dire que d'éléments de $\mathbb{P}(E^*)$. Il y a donc $q^2 + q + 1$ droites. Si on dénombre les bases possibles pour les hyperplan plutôt que les équations on trouve :

$$\frac{(q^3 - 1)(q^3 - q)}{(q^2 - 1)(q^2 - q)} = q^2 + q + 1.$$

Exercice 15. *Soit $E = \mathbb{F}_2^3$. Montrer que $\mathbb{P}(E)$ contient 7 points et 7 droites. Montrer que chaque droite contient 3 points, que chaque point appartient à trois droites. En déduire qu'il existe une bijection de $\mathbb{P}(E)$ sur l'ensemble des points de la figure ci-dessous telle que les droites s'envoient sur des points sur un même segment ou le cercle de la figure.*
Vérifier qu'en enlevant une droite (disons celle dessinée comme un cercle), on retrouve $\mathbb{F}_2^2$ et ses 6 droites. Le plan projectif $\mathbb{F}_7\mathbb{P}^2$ est appelé plan de Fano. Il est représenté par la figure 6.1

Exercice 16. *Faire de même avec $E = \mathbb{F}_3^2$. On doit trouver le dessin de la figure5.*

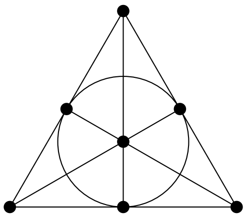


FIGURE 6.1 – Plan projectif sur $\mathbb{F}_2$

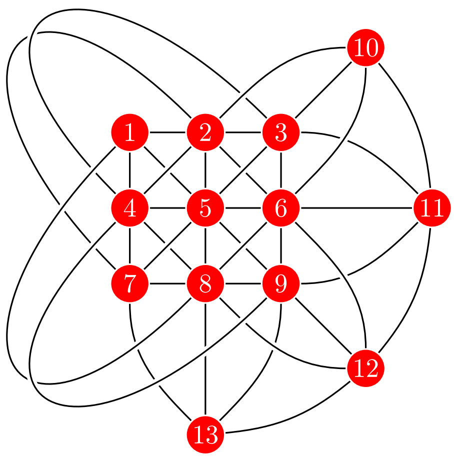


FIGURE 6.2 – Plan projectif sur $\mathbb{F}_3$

6 Dualité projective

Il s'agit d'une construction littéralement magique qui permet de transformer tout problème de géométrie affine plane faisant intervenir des points et des droites. L'idée est d'utiliser l'orthogonalité en dualité linéaire.

Soit E un k-espace vectoriel de dimension trois. Pour tout sous-espace vectoriel F de E, son orthogonal $F^{\perp}$ est un sous-espace vectoriel de E^* de dimension $3 - \dim(F)$.
Soit donc un point A de $\mathbb{P}(E)$. Alors $A = \mathbb{P}(F)$ où F est un sous-espace vectoriel de E de dimension 1. Donc $F^{\perp}$ est un sous-espace vectoriel de E^* de dimension 2. Donc $P(F^{\perp})$ est une droite de $\mathbb{P}(E^*)$, notée $p^{\perp}$.
De même, si nous étions partis d'une droite d de $\mathbb{P}(E)$, nous aurions obtenu un point $d^{\perp}$ de $\mathbb{P}(E)$.

Le point est que $F_1 \subset F_2$ si et seulement si $F_1^{\perp} \supset F_2^{\perp}$. Voici quelques exemples de conséquences :

(i) Un point A appartient à une droite d dans $\mathbb{P}(E)$ si et seulement si la droite $A^{\perp}$ contient le point $d^{\perp}$ dans $\mathbb{P}(E^*)$;

(ii) Les 3 points A, B et C de $\mathbb{P}(E)$ sont alignés si seulement si les droites $A^{\perp}$, $B^{\perp}$ et $C^{\perp}$ de $\mathbb{P}(E^*)$ sont concourantes...

Ci-dessous, nous montrons quelques exemples.

7 Application à la géométrie affine plane

Le principe ici est assez simple mais magnifiquement miraculeux.

(i) On part d'un énoncé de géométrie affine ne faisant intervenir que des droites et des points.

(ii) On le voit comme un dessin dans $\mathcal{H}$ une carte affine d'un plan projectif. Le théorème VI.74 donne un énoncé dans le plan projectif.

(iii) On change de carte affine. Le théorème VI.74 donne un **nouvel** énoncé dans le plan affine.

Onn peut même obtenir encore plus en appliquant la dualité projective.

7.1 Théorème de Pappus

Nous allons illustré le principe énoncé ci-dessus avec le théorème de Pappus. Commençons donc par rappeler l'énoncé affine que nous avions vu et son dessin (figure 7.1).

Théorème VI.76. Pappus Affine

Soit D et D' deux droites distinctes du plan affine. Soit A, B et C (resp. A', B' et C') trois points distincts de D (resp. D'). On suppose qu'aucun des 6 points n'est $D \cap D'$.
Si $(AB')//(A'B)$ et $(CB')//(C'B)$ alors $(AC')//(A'C)$.

Considérons maintenant un plan projectif $\mathbb{P}(E)$ muni d'une carte affine $\mathcal{H}$. Pensons au dessin de la figure comme à l'intersection avec $\mathcal{H}$ d'un dessin plongé dans $\mathbb{P}(E)$. Alors,

(i) A, B, C, A', B' et C' sont des points ;

(ii) D et D' sont des droites projectives (dont il manque un point le dessin)

(iii) (AB'), (AC'), (BA'), (BC'), (CA') et (CB') sont des droites projectives (dont il manque un point le dessin)

(iv) Il y a droite $\mathbb{P}(H)$ qui n'est pas visible sur le dessin mais qui est dans toutes les têtes.

Les droites projectives (BC') et (CB') se coupent (comme toute paire de droites projectives). Comme on ne voit pas le point d'intersection (que nous appellerons A''), on a $A'' \in \mathbb{P}(H)$.
De même, (AB') et (BA') se coupent (comme toute paire de droites projectives). Comme on ne voit pas le point d'intersection (que nous appellerons C''), on a $C'' \in \mathbb{P}(H)$.

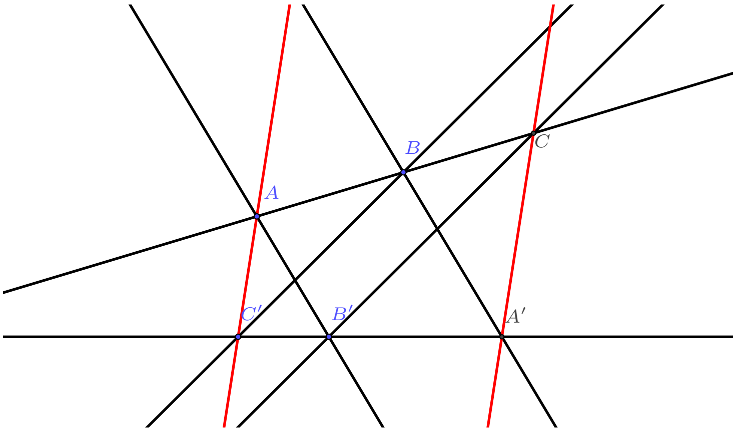


FIGURE 6.3 – Pappus Affine

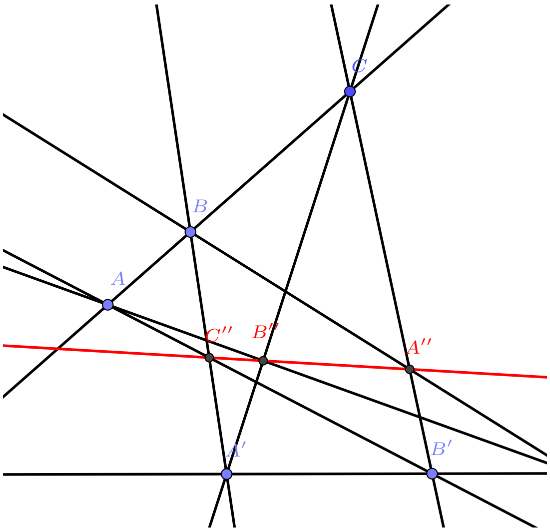


FIGURE 6.4 – Pappus projectif

De même la conclusion du théorème dit que

$$B'' := (AC') \cap (CA') \in \mathbb{P}(H).$$

Donc les trois points A'', B'' et C'' sont sur la même droite projective : ils sont alignés. On vient de montrer l'énoncé projectif du théorème VI.77 suivant illustré par la figure 7.1 :

Théorème VI.77. Pappus projectif

Soit $\mathbb{P} = \mathbb{R}P^2$. Soit (A, B, C) et (A', B', C') deux triplets de points alignés et 2 à 2 distincts de $\mathbb{P}$. Soit $A'' = (BC') \cap (B'C)$, $B'' = (AC') \cap (A'C)$ et $C'' = (BA') \cap (B'A)$.
Alors A'', B'' et C'' sont alignés.

L'énoncé précédent reste vrai en affine à la seule condition que les points existes.
Notons $0 = D \cap D'$. Si on envoie (O, B'') à l'infini, on obtient la figure 7.1.
La figure 7.1 vu comme un dessin affine donne le théorèmeVI.78 suivant.

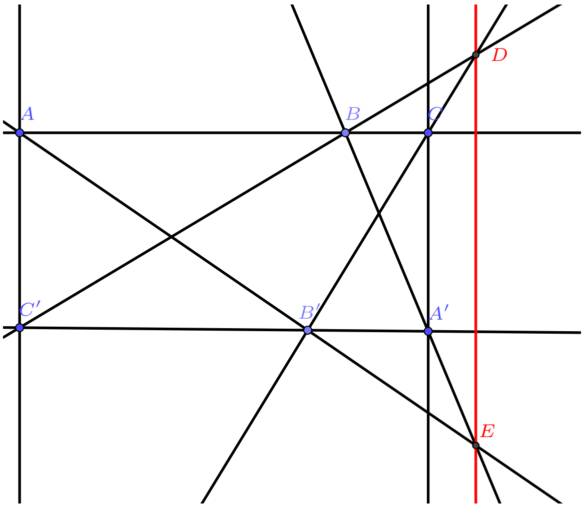


FIGURE 6.5 – Pappus Affine 2

Théorème VI.78. Pappus Affine v2

Soit D et D' deux droites distinctes du plan affine. Soit A, B et C (resp. A', B' et C') trois points distincts de D (resp. D'). On suppose qu'aucun des 6 points n'est $D \cap D'$ telle que $(AC')//(A'C)$.
Soit $C'' = (AB') \cap (A'B)$ et $A'' = (CB') \cap (C'B)$.
Alors $(C''A'')//(AC')$.

Démonstration. Le point projectif B'' appartient à la droite projective $(C''A'')$ d'après la version projective. Par ailleurs, il est à l'infini puisque $(AC')//(A'C)$. Ceci signifie que les droites projectives $(C''A'')//(AC')$ se coupent à l'infini. En affine, elles sont donc parallèles. □

A Version Duale

Théorème VI.79. Dual de Pappus projectif

Soit A et A' deux points distinct du plan projectif $k\mathbb{P}^2$. Soit d_1, d_2 et d_3 3 droites passants par A.
Soit d'_1, d'_2 et d'_3 3 droites passants par A'.
On note d''_3 la droite passant par $d_1 \cap d'_2$ et $d_2 \cap d'_1$. On note d''_2 la droite passant par $d_1 \cap d'_3$ et $d_3 \cap d'_1$. On note d''_1 la droite passant par $d_2 \cap d'_3$ et $d_3 \cap d'_2$.
Alors les trois droites d''_1, d''_2 et d''_3 sont concourantes.

Démonstration. C'est exactement le dual de Pappus projectif :

(i) A est l'orthogonal de la droite (AB) ;
(ii) d_1 est l'orthogonal du point A ;
(iii) d'_2 est l'orthogonal du point B' ;
(iv) d'''_3 est l'orthogonal de C''...

□

Considérons unne version affine de ce théorème en envoyant la droite (AA') à l'infini. Alors d_1, d_2 et d_3 sont parallèles ainsi que d'_1, d'_2 et d'_3. On obtient alors le théorème VI.80, illustré par la figure 6.6 :

Théorème VI.80. Pappus dual Affine

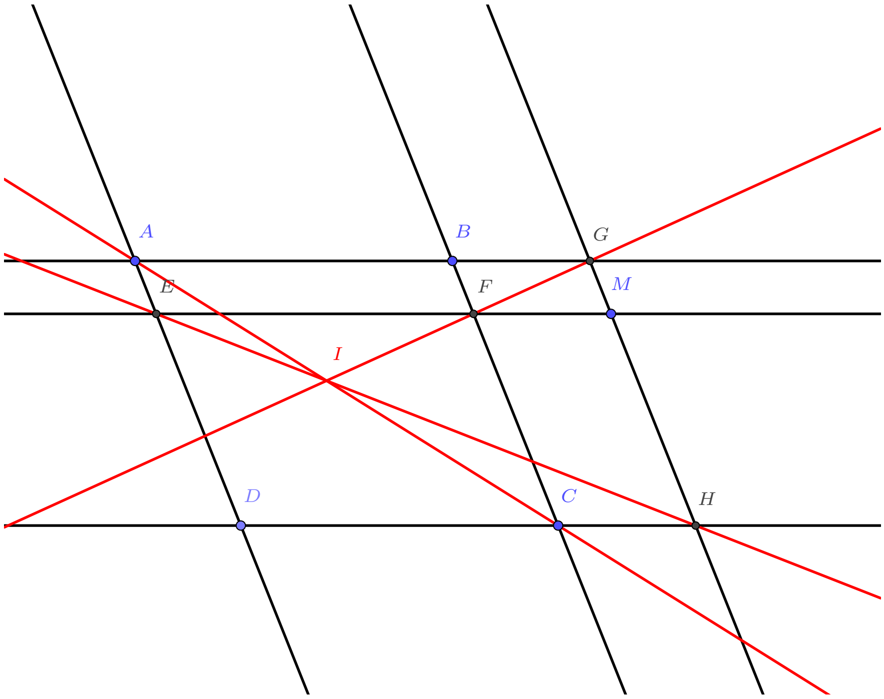


Figure 6.6 – Pappus dual Affine

Soit $(ABCD)$ un parallélogramme du plan affine et M un point en dehors des 4 droites côtés. La parallèle à (AB) qui passe par M coupe (AD) et (BC) en E et F. La parallèle à (AD) qui passe par M coupe (AB) et (DC) en G et H.
Alors les droites (AC), (EH) et (FG) sont concourantes.

7.2 Théorème de Désargues

Rappelons l'énoncé affine.

Théorème VI.81. Désargues

Soit (ABC) et $(A'B'C')$ deux triangles non aplatis. On suppose que $(AB)//(A'B')$, $(BC)//(B'C')$ et $(AC)//(A'C')$.
Alors les trois droites (AA'), (BB') et (CC') sont concourantes ou parallèle.

La figure 6.7 illustre le théorème VI.81.
Version projective de cet énoncé est le théorème VI.82, illustré par la figure 6.8 Autrement dit, c'est l'énoncé que l'on obtient en réalisant l'énoncé affine dans une carte affine d'un plan projectif.

Théorème VI.82. Désargues projectif

Soit (ABC) et $(A'B'C')$ deux triangles non aplatis d'un plan projectif. Alors les assertions suivantes sont équivalentes :

(i) Les droites (AA'), (BB') et (CC') sont concourantes.

(ii) Les points $P = (BC) \cap (B'C')$, $Q = (AC) \cap (A'C')$ et $R = (AB) \cap (A'B')$ sont alignés.

Démonstration. Supposons la deuxième assertion vrai. Envoyons la droite (PQ) à l'infini. Alors R est aussi à l'infini. Donc $(BC)//(B'C')$, $(AC)//(A'C')$ et $(AB)//(A'B')$. La version affine du théorème im-

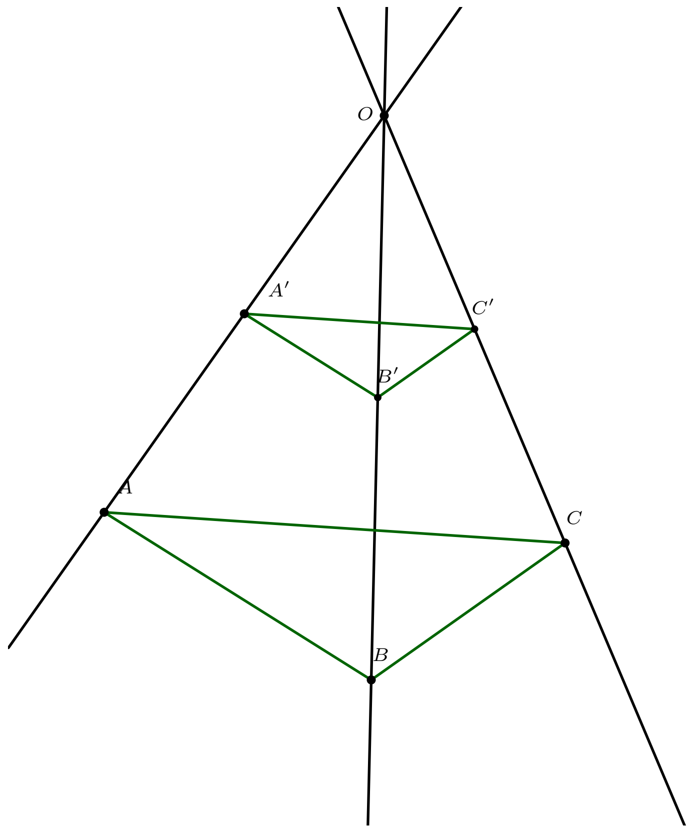


Figure 6.7 – Désargues Affine

plique alors que Les droites (AA'), (BB') et (CC') sont concourantes. On a montré la première assertion.

On regarde à présent le dual de l'implication que l'on vient de montrer. Et quelle surprise : on obtient que la première assertion implique la seconde. □

Remarque. Dans le théorème VI.81 il se peut que les trois droites (AA'), (BB') et (CC') soient parallèles. Ceci n'arrive pas dans le cas projectif car en projectif des droites ne sont jamais parallèles. En fait si les 3 droites affines sont parallèle, elles ont même direction. Cette direction est un point d'intersection des 3 droites projectives.

8 Application à l'étude des coniques

8.1 Homogénéisation

On se place dans $k\mathbb{P}^2$ et on utilise les coordonnées projectives $[x : y : z]$.

Définition VI.83: Conique projective

Une *conique projective* est une partie de $k\mathbb{P}^2$ définie par une équation du type

$$ax^2 + by^2 + cz^2 + dyz + exz + fxy = 0,$$

où $(a, b, c, d, e, f) \in k^6 - \{0\}$.

Quelques remarques s'imposent :

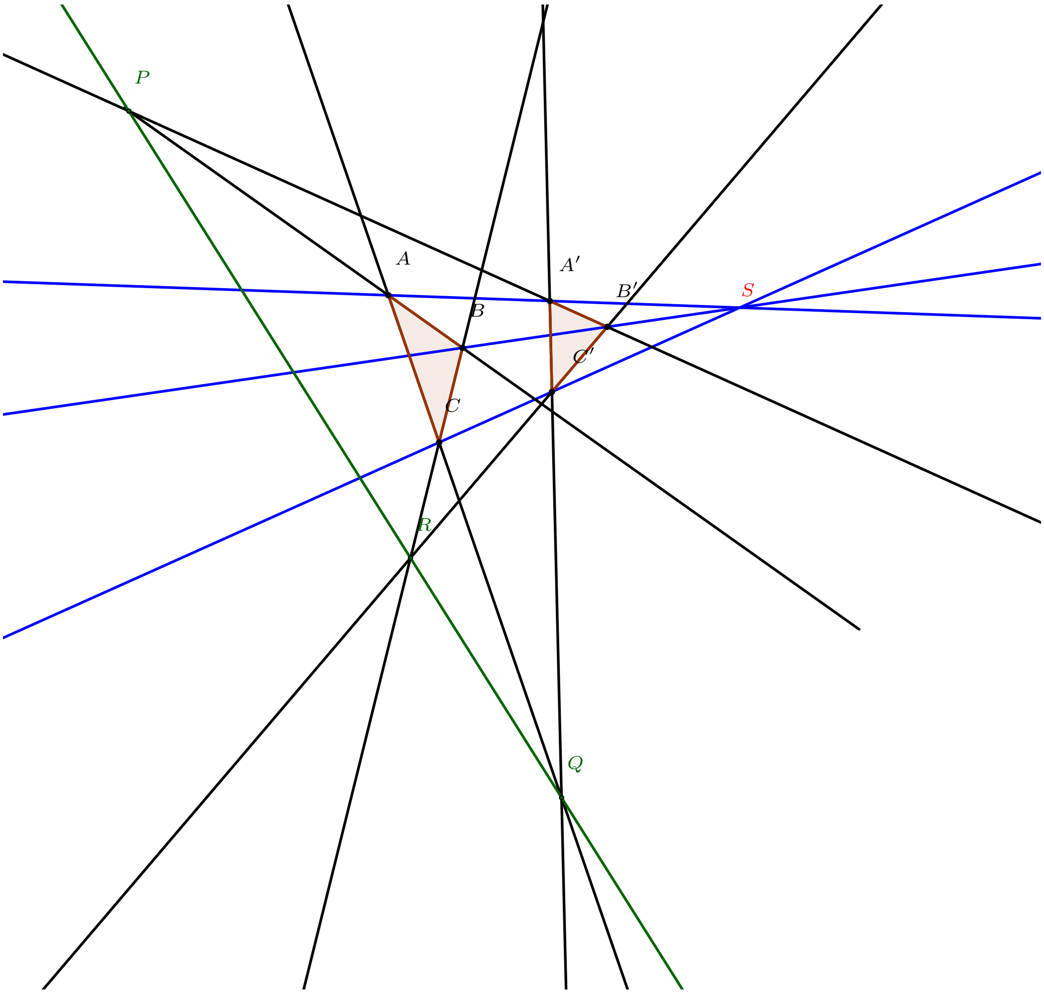


Figure 6.8 – Désargues Projectif

Remarque. (i) Attention, la quantité $ax^2+by^2+cz^2+dyz+exz+fxy$ dépend du représentant choisi pour écrire $[x:y:z]$. En effet, pour $[\lambda x:\lambda y:\lambda z]$, cette quantité est multiplié par λ^2. En revanche le fait que cette quantité soit nulle ou pas nne dépend pas du représentant choisi, si bien que la conique est bien définie.

(ii) L'application $k^3 \longrightarrow k,\ (x,y,z) \longmapsto ax^2+by^2+cz^2+dyz+exz+fxy$ est une forme quadratique. En fait n'importe quelle forme quadratique non nulle.

Regardons la trace de la conique dans la carte affine $z=1$.

Théorème VI.84. Coniques projectives et affines

Soit $(a,b,c,d,e,f) \in k^6 - \{0\}$.

(i) L'intersection de la carte affine $z=1$, et de la conique projective

$$C_p = \{[x:y:z] \ : \ ax^2+by^2+cz^2+dyz+exz+fxy=0\}$$

est

(a) la conique d'équation $ax^2+by^2+fxy+dy+ex+c=0$, si $(a,b,f) \neq (0,0,0)$;

(b) la droite d'équation $dy+ex+c=0$, si $(a,b,f)=(0,0,0)$.

(ii) Réciproquement, considérons la conique C_a plane d'équation

$$ax^2+by^2+cxy+dy+ex+f=0,$$

avec $(a,b,c) \neq (0,0,0)$ vu comme une partie de la carte affine $z=1$. Alors, la conique projective C_p d'équation $ax^2+by^2+fz^2+dyz+exz+cxy=0$ est l'unique contenant C_a.

Démonstration. La première affirme est une conséquence directe du fait qu'en remplaçant z par 1 dans $ax^2+by^2+cz^2+dyz+exz+fxy$, on trouve $ax^2+by^2+c+dy+ex+fxy$.

Réciproquement, $ax^2+by^2+fz^2+dyz+exz+cxy$ est la seule forme quadratique que donne $ax^2+by^2+cxy+dy+ex+f$ lorsque $z=1$. La seconde assertion en découle. □

Remarque. Il est possible de munir $k\mathbb{P}^2$ d'une topologie de sorte que C_p soit l'adhérence de C_a. Cela est très éclairant mais dépasse le cadre de cours.

8.2 Classification projective des coniques de $\mathbb{RP}^2$

Ici le corps est celui des nombres réels. Le groupe $\mathrm{GL}_3(\mathbb{R})$ agit par changement de variables sur l'ensemble des quadriques. Il agit donc sur l'ensemble des coniques. Par ailleurs, deux formes quadratiques opposées donnent la même conique.

Théorème VI.85. Classification projective des coniques

A action de $GL_3(\mathbb{R})$ et multiplication par -1 près, la liste complète des coniques de $\mathbb{RP}^2$ est la suivante :

(i) L'équation
$$x^2 + y^2 + z^2 = 0$$
qui donne le vide. Ceci arrive lorsque la forme quadratique est de signature $(3, 0)$ ou $(0, 3)$.

(ii) L'équation
$$x^2 + y^2 - z^2 = 0$$
qui donne une *conique non dégénérée*. Ceci arrive lorsque la forme quadratique est de signature $(2, 1)$ ou $(1, 2)$.

(iii) L'équation
$$x^2 + y^2 = 0$$

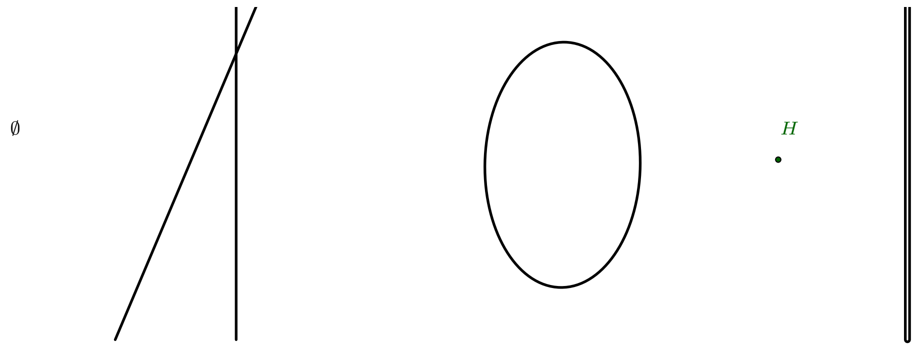


FIGURE 6.9 – Coniques projectives

qui donne un point. (On peut penser à un cercle de rayon zéro). Ceci arrive lorsque la forme quadratique est de signature $(2, 0)$ ou $(0, 2)$.

(iv) L'équation

$$xy = 0$$

qui donne la réunion de deux droites. Ceci arrive lorsque la forme quadratique est de signature $(1, 1)$.

(v) L'équation

$$x^2 = 0$$

qui donne une droite (pensée comme une droite double). Ceci arrive lorsque la forme quadratique est de signature $(1, 0)$ ou $(0, 1)$.

Démonstration. Ceci est une conséquence immédiate du fait que les formes quadratiques sont caractérisées par leur signature. □

8.3 Application à la classification affine des coniques

Lorsque l'on regarde les théorèmesVI.84 et VI.85 deux impressions opposées nous viennent. Le premier énoncé semble dire que les coniques affines et projectives sont le même objet. Le second semble dire que les coniques projectives sont plus simples et moins nombreuses que les coniques affines. Nous allons lever ce paradoxe.
En fait pour passer d'une conique projective à une conique affine, il faut choisir une carte affine ou, par passage au complémentaire, une droite à l'infini. Suivant la position de cette dernière et de la conique projective on trouve différentes coniques affines pour une même conique projective.
Voici quelques exemples sur la figure 6.10 où la droite à l'infini est rouge. A gauche, on a deux droites sécantes, à droites deux droites parallèles.
Sur la figure 6.11 où la droite à l'infini est rouge, nous avons dans l'ordre une ellipse, une hyperbole et une parabole.

Figure 6.10 – Droites sécantes et parallèles

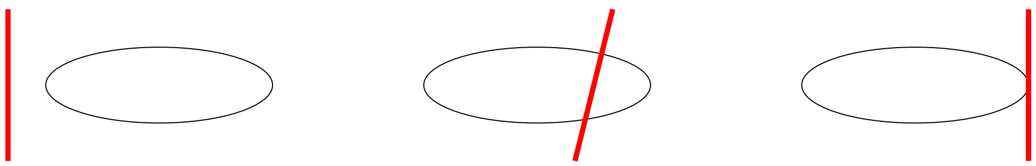


Figure 6.11 – Ellipse, hyperbole et parabole