Algèbre II

Licence, École Normale Supérieure de Lyon, 2013–2015.

François Dahmani

Université Joseph Fourier, Grenoble I. Institut Universitaire de France.

Avertissement

Ce texte constitue une tentative de rédaction de notes de cours pour 12 séances de 2h. Les notes telles qu'elles sont peuvent couvrir 14 séances, et des choix parmi les compléments peuvent être fait.

Ce cours fait suite à celui donné au premier semestre par Sandra Rozensztajn (Groupes (actions, groupes symétriques, representations de groupes finis) – Anneaux (Polynômes, Factorisations, Anneaux Noetheriens) – Modules (de type fini sur un anneau principal).)

Voici le plan grossier. (cf page suivante pour un plan détaillé.)

— 1 — Extensions de corps et d'anneaux. (5 séances)
Extensions algébriques, corps de rupture, corps finis, clotures algébriques, extensions d'anneaux.
— 2 — Groupes linéaires. (5 séances)
Groupes linéaire, génération et simplicité, exponentielle et applications, quaternions.
— 3 — Compéments autour des algèbres de polynômes. (2 séances)
Algèbre des polynômes symétriques, résultant, fractions rationelles.

Bibliographie indicative.

— D. Perrin, *Cours d'Algèbre*, Ellipse.
— S. Lang, *Algebra*, Addison Wesley.
— R. Mneimné, F. Testard *Introduction a la théorie des groupes de Lie classiques*, Hermann.
— J.-Y. Merindol *Nombres et Algèbre*, EDP Sciences, Grenoble Sciences.
— G. Birkhoff, S. Mac Lane, *A Survey of Modern Algebra*, A.K. Peters.

Merci à Emmanuel Peyre pour la mise à disposition de ses notes, à Maxime Bourrigan, pour sa large implication dans la préparation des TD lors de la première année de ce cours, à Giovanni di Matteo, Fangzhou Jin, et Matthias Moreno pour leur TD de qualité, et l'accompagnement du cours, et aux étudiants de l'ENS-Lyon promo 2012, et 2013, pour leurs commentaires et corrections. Grenoble, Avril 2014, F.D.

Table des matières

1 Extensions de corps et d'anneaux. 3

1.1 Premières notions sur les extensions de corps . . . 3
1.1.1 Extensions de corps, et éléments algébriques . . . 3
1.1.2 Le point de vue vectoriel . . . 4
1.1.3 Regle et compas . . . 6
1.1.4 Corps de rupture, corps de décomposition . . . 8
1.2 Corps finis . . . 10
1.2.1 Caracteristique et cardinal . . . 10
1.2.2 Existence et unicité des corps finis . . . 10
1.2.3 $\mathbb{F}_q^*$ . . . 11
1.2.4 Carrés . . . 11
1.3 Cloture algébrique . . . 11
1.3.1 Existence . . . 11
1.3.2 Unicité . . . 12
1.3.3 Compléments, applications aux extensions normales. . . . 13
1.4 Cyclotomie . . . 15
1.4.1 Racines de l'unité, racines primitives . . . 15
1.4.2 Irréductibilité . . . 16
1.5 Extensions d'anneaux . . . 17
1.5.1 Définitions . . . 17
1.5.2 Elements entiers . . . 17
1.5.3 Cloture integrale . . . 19
1.5.4 Exemples quadratiques . . . 19
1.6 Compléments, algèbres commutatives sur un corps . . . 21
1.6.1 Elements nilpotents . . . 21
1.6.2 Nullstellensatz . . . 23

2 Groupes linéaires 24

2.1 Groupes linéaires GL, SL . . . 24
2.1.1 Définitions . . . 24
2.1.2 Produit semi-direct . . . 25
2.1.3 Générateurs . . . 26
2.1.4 Applications . . . 26
2.1.5 Simplicité . . . 27
2.1.6 Cas exceptionnels . . . 28
2.1.7 Congruences . . . 28
2.2 Exponentielle et applications . . . 29
2.2.1 Algègres de Banach, et applications . . . 29
2.2.2 Crochet de Lie et sous-groupes de $\mathcal{A}^*$ . . . 29
2.2.3 Sous groupes compacts . . . 32
2.3 Quaternions . . . 33
2.3.1 Rappels sur O_n . . . 33
2.3.2 Le "corps" des quaternions . . . 33
2.3.3 Réalisation matricielle . . . 34
2.3.4 Applications . . . 34
2.3.5 Géométrie Euclidienne de dimension 4 . . . 35
2.3.6 Géométrie Euclidienne de dimension 3 . . . 35
2.3.7 Hopf . . . 36
2.3.8 Frobénius . . . 36
2.3.9 Cayley . . . 37

3 Compléments sur les algèbres de polynômes 37

3.0.10 Polynômes symétriques . . . 37
3.0.11 Résultant . . . 39
3.0.12 Fractions rationelles . . . 40

1 Extensions de corps et d'anneaux.

1.1 Premières notions sur les extensions de corps

Les corps sont tous supposés commutatifs.

Un polynôme P sur un corps K aura donc au plus $\deg(P)$ racines, et ses racines multiples sont données par celles de $P' \wedge P$.

1.1.1 Extensions de corps, et éléments algébriques

Définition 1.1.1. *Si L est un corps, et $\rho : K \to L$, on dit que L est une extension de K par ρ, ou encore une extension de $\rho(K)$, et on note $L\backslash\rho(K)$.*

Souvent, le contexte fera que $K \subset L$ et $\rho = id|_K$. On omet alors la mention de ρ.

Exemple 1.1.1. *:*

- $\mathbb{C}\backslash\mathbb{R}$,
- $\mathbb{R}\backslash\mathbb{Q}$,
- $\mathbb{K}(T)\backslash\mathbb{K}$, *dans lequel $\mathbb{K}(T)$ est le corps des fractions de l'anneau (integre) $\mathbb{K}[T]$.*
- $\mathbb{Q}(\sqrt{2})\backslash\mathbb{Q}$ *? à clarifier. En effet :*

La notation que l'on vient d'utiliser $K(T)$ (ou $\mathbb{Q}(\sqrt{2})$) merite que l'on clarifie ses usages futurs.

Observation 1.1.1. *l'intersection d'une famille de sous-corps est un sous-corps. Cela permet de parler de sous-corps engendré par une partie (c'est l'intersection des corps contenant cette partie).*

Notation : si $L\backslash K$ est une extension, et si $S \subset L$, $K(S)$ désigne le sous corps engendré par K et S.

Observation 1.1.2. *"$K(T)$ est bien $K(T)$."*

Exemple 1.1.2. *:* $\mathbb{R}\backslash\mathbb{Q}(\sqrt{2})\backslash\mathbb{Q}$.

$\mathbb{R}\backslash\mathbb{Q}(\pi)\backslash\mathbb{Q}$.

Spécialisation (ou évaluation). Soit $L\backslash K$. Si $\alpha \in L$, on note $K[\alpha]$ le **sous-anneau** engendré par K et α.

Oublions un instant que L et K sont des corps, et ne voyons que les anneaux.

Lemme 1.1.1. *Soit B un anneau et A un sous-anneau de B, et α dans B. Soit $A[X]$ l'anneau des polynômes à une indéterminée, à coefficients dans A. Il existe un unique morphisme $A[X] \to B$ induisant l'identité sur A et envoyant X sur α. On le note spe_α.*

Sans les notations précédentes $A[\alpha]$ est l'image de $A[X]$ par spe_α.

Démonstration. Un unique morphisme est ainsi bien défini.

Par ailleurs, $spe_\alpha(A[X]) \subset \bigcap_{\{\alpha\}\cup A\subset A'} A'$ car si $y = P(\alpha)$, y est dans tout A' de cette forme.

Aussi, $\bigcap_{\{\alpha\}\cup A\subset A'} A' \subset spe_\alpha(A[X])$, car $spe_\alpha(A[X])$ est l'un de ces anneaux A' dont il est question. □

Revenons à nos corps. Nous avions $L\backslash K$, et $\alpha \in L$.

Un tel énoncé est plus problématique pour les corps $K(X)$ a la place des anneaux $K[X]$ (il arrive que le morphisme sur $K[X]$ ne soit pas injectif, et alors il ne peut pas se prolonger en morphisme de corps).

On peut cependant décrire les éléments de $K(\alpha)$ comme ceux de la forme $x = \frac{P(\alpha)}{Q(\alpha)}$, avec P et Q des éléments de $K[X]$, et Q n'ayant pas α pour racine.

(Tout element de cette forme est dans $K(\alpha)$, et on verifie sans peine que l'ensemble de ces éléments forme un sous-corps de L.)

Définition 1.1.2. *Soit $L\backslash K$, et $\alpha \in L$. On dit que α est* **transcendant** *sur K si $spe_\alpha : K[X] \to L$ est injective.*

On dit que α est **algébrique** *sur L sinon.*

Remarque : Si α est algébrique, comme $K[X]$ est principal (K est un corps !) il existe un unique polynome unitaire $P_\alpha \in K[X]$ tel que $\ker(spe_\alpha) = (P_\alpha)$. On l'appelle le **polynôme minimal** de α sur K. Son degré est aussi appelé **degré** de α sur K.

1.1.2 Le point de vue vectoriel

Remarque clé : si $L\backslash K$, alors L est un K-ev. On dit que sa dimension est le **degré** de L sur K, et on la note $[L : K]$.

Si le degré est fini, on dit, legèrement abusivement que l'extension est finie.

Exemple 1.1.3. *si L est fini, $|L| = |K|^{[L:K]}$. On verra bientot des exemples de corps finis.*

Théorème 1.1.1. *(Base téléscopique)*

Soient $M\backslash L$ et $L\backslash K$ des extensions.

Soit $(e_i)_{i\in I}$ une base de M sur L et $(f_j)_{j\in J}$ une base de L sur K.

Alors $(e_i f_j)_{(i,j)\in I\times J}$ est une base de M sur K.

Démonstration. Liberté : Si $\sum \lambda_{i,j} e_i f_j = 0$ (avec $\lambda_{i,j} \in K$), factorisons :

$$\sum_i (\sum_j \lambda_{i,j} f_j) e_i$$

chaque coefficient $(\sum_j \lambda_{i,j} f_j)$ est dans L, et (e_i) est une base de M sur L, donc chaque coefficient

$$(\sum_j \lambda_{i,j} f_j)$$

(j fixé) est nul. Comme $\lambda_{i,j} \in K$ et (f_i) base de L sur K, chaque $\lambda_{i,j}$ est nul.

Génération : si $x \in M$ ecrivons

$$x = \sum \mu_i e_i$$

avec $\mu_i \in L$. Ecrivons pour chaque μ_i :

$$mu_i = \sum_j \nu_{i,j} f_j$$

avec $\nu_{i,j} \in K$. On a bien

$$x = \sum \sum \nu_{i,j} f_j e_i.$$

□

Corollaire 1.1.1. *Si $M\backslash L$ et $L\backslash K$ des extensions finies, alors $M\backslash K$ aussi, et $[M : L][L : K] = [M : K]$.*

Théorème 1.1.2. *Si $L\backslash K$ est une extension et si $\alpha \in L$, LASSE :*

1. *α est algébrique sur K*
2. *$K[\alpha] = K(\alpha)$*
3. *$[K[\alpha] : K]$ est fini.*

Et dans ce cas, $[K[\alpha] : K]$ vaut le degré du polynôme minimal de α sur K.

Démonstration. ($1 \implies 2$). Si P_α est le polynome minimal ; on a

$$K[X]/(P_\alpha) \xrightarrow{\simeq} K[\alpha].$$

Or à droite c'est integre,
donc à gauche aussi,
donc (P) est un ideal premier,
donc P est **irreductible** dans $K[T]$
donc (P) est aussi maximal, et donc à gauche, c'est un corps.
Donc $K[\alpha]$ aussi est un corps. Donc c'est $K(\alpha)$.

($2 \implies 1$). Si α est transcendant,

$$K[\alpha] \simeq K[X]/\ker(spe) = K[X]$$

et ce n'est pas un corps.

($3 \implies 1$). Si α est transcendant, $K[\alpha] \simeq K[X]$ est de dimension infinie sur K.

($1 \implies 3$). On affirme que $\{1, \alpha, \alpha^2, \ldots, \alpha^{deg(P_\alpha)-1}\}$ est une base de $K[\alpha]$ sur K. Cette famille est libre, sinon, on trouve un polynome de degré $< deg(P_\alpha)$ qui annule α. Elle est génératrice, car pour tout polynôme P, $P(\alpha)$ est aussi réalisé par un polynôme de bas degré (si la division Euclidienne donne $P = QP_\alpha + R$, on a $P(\alpha) = R(\alpha)$). □

Définition 1.1.3. *Une extension est* **finie** *si son degré est fini.*
Une extension est algébrique si **tous ses éléments** *sont algébriques.*

Observation 1.1.3. *le théorème précédent (en fait une partie facile de celui-ci) donne le corollaire suivant.*

Corollaire 1.1.2. *Toute extension finie de K est algébrique sur K.*

En effet, tout element β engendre un sous-K-ev $K[\beta]$ encore de dimension finie, et ($1 \implies 3$) s'applique. La réciproque est fausse comme nous allons le voir (une extension algébrique peut être non-finie.

Théorème 1.1.3. *Si $M\backslash K$ est une extension, et $L = \{x \in M, x \text{ alg. sur } K\}$, alors L est un corps (et $L\backslash K$ est une extension algébrique).*

La partie entre parenthèse est tautologique une fois que le fait que L est un corps est établi.

Démonstration. Si α, α' sont algébriques (non nuls), $\alpha^{-1}, \alpha\alpha'$ et $\alpha + \alpha'$ le sont-ils ?

Pour α^{-1} c'est clair car il est dans l'extension **finie** $K[\alpha]$ (l'observation precedente s'applique).

Les deux autres sont ailleurs. Ils sont dans $(K[\alpha])[\alpha']$ (ici $K[\alpha]$ est un corps). Comme α' est algébrique sur K, il l'est sur $K[\alpha]$, et donc, $(K[\alpha])[\alpha']$ est une extension de finie de $K[\alpha]$.

Par ailleurs, $K[\alpha]$ est une extension finie de K. Par théorème "téléscopique", $(K[\alpha])[\alpha']$ est une extension finie de K et le tour est joué, on peut à nouveau appliquer le corollaire précédent pour chacun des éléments $\alpha\alpha'$ et $\alpha + \alpha'$. □

Observation 1.1.4. *il n'est en principe pas facile (ou pas agréable ?) de trouver le polynôme minimal de $\alpha + \alpha'$ et de $\alpha\alpha'$.*

Exemple 1.1.4. *Polynôme minimal de $5^{1/7} + 7^{1/3} \times 3^{1/5}$?...*

Observation 1.1.5. *$\bar{\mathbb{Q}} = \{x \in \mathbb{C}, x$ alg. sur $\mathbb{Q}\}$ est un corps, c'est une extension algébrique de $\mathbb{Q}$, amis ce n'est pas une extension finie, car on y trouve des éléments de tout degré.*

Définition 1.1.4. *On dit qu'un corps est* **algébriquement clos** *quand sa seule extension algébrique est celle de degré* 1.

Proposition 1.1.1. *LASSE.*

- *K est alg. clos.*
- *Pour tout $P \in K[X]$ de degré ≥ 1, P a une racine dans K.*
- *Pour tout $P \in K[X]$ de degré ≥ 1, P est un produit de polynomes de $K[X]$ de degré 1.*
- *Si $P \in K[X]$ est irreductible, son degré est* 1.

(exercice)
Fait : $\mathbb{C}$ et $\bar{\mathbb{Q}}$ sont alg. clos.

1.1.3 Regle et compas

[1]

Définition 1.1.5. *Soit $\mathcal{A} \subset \mathbb{R}^2$ et $M \in \mathbb{R}^2$.*

On dit que M est **constructible à la règle et au compas** *("CALREAC", ou "constructible" dans la suite)* **en un coup** *à partir de $\mathcal{A}$ si :*

il existe $A_1, \dots A_6$ dans $\mathcal{A}$ tels que l'une des trois situations suivante est vraie :

- *$A_1 \neq A_2$, et $A_3 \neq A_4$ et $\{M\} = (A_1A_2) \cap (A_3A_4)$.*
- *$A_1 \neq A_4$ et $\{M\} \in \mathcal{C}_{A_1,d(A_2,A_3)} \cap \mathcal{C}_{A_4,d(A_5,A_6)}$.*
- *$\{M\} \in \mathcal{C}_{A_1,d(A_2,A_3)} \cap (A_4A_5)$.*

En clair : c'est quand M est à l'intersection de droites et/ou cercles distincts définis grace à $\mathcal{A}$.

Définition 1.1.6. *On dit que $M \in \mathbb{R}^2$ est CALREAC s'il existe des ensembles (finis)*

$$\{(0,0)(1,0)\} = \mathcal{A}_0 \subset \mathcal{A}_1 \subset \mathcal{A}_2 \cdots \subset \mathcal{A}_n$$

avec $M \in \mathcal{A}_n$ et $\mathcal{A}_{i+1}$ ne contient que des points CALREAC en un coup à partir de $\mathcal{A}_i$.

Exercice : l'hypothèse de finitude des ensembles est superflue : si on l'enleve, on ne change pas la classe.

Définition 1.1.7. *On dit qu'un réel x est CALREAC si $(x, 0) \in \mathbb{R}^2$ l'est.*

Proposition 1.1.2. *Sont CALREAC les points suivants :*

- *$(n, 0)$ si $n \in \mathbb{Z}$*
- *$(0, n)$ si $n \in \mathbb{Z}$*
- *$(0, x)$ si x CALREAC ‡*
- *$(x + y, 0)$ si x, y CALREAC (ex.)*

1. Utiliser une couleur pour les traits de construction, et une autre pour les points construits

— $(-x, 0)$ *si* x *CALREAC (ex.)*
— $(x, 0)$ *si* $x \in \mathbb{Q}$
— $(\frac{x}{y}, 0)$ *si* x, y *CALREAC* $y \neq 0$ ‡
— $(xy, 0)$ *si* x, y *CALREAC (ex.)*
— $(\sqrt{x}, 0)$ *si* $x > 0$ *CALREAC* ‡
— $(x, 0)$ *si* (x, y) *CALREAC.*

Démonstration. On sait tracer la mediatrice d'un segment (et donc de $[-(1,0),(1,0)]$). Donc on a (3).

Pour (7), on considere le triangle $(0,0,(0,y),(x,0)$. Si on sait tracer la parallele au 3eme coté passant par $(0,1)$, on a fini, car Thales nous dit qu'elle intersecte l'axe des $(t,0)$ en $(x/y,0)$.

Construire la parallele a une droite D passant par un point (A) : on constuit une perpendiculaire Δ (cf avant), puis un cercle de centre A de rayon assez grand intersecte Δ en deux points. La médiatrice de ce segment est la droite cherchée (ex.).

$xy = x/(1/y)$ (ou bien 0...)

Pour $\sqrt{x}$, il s'agit de considerer le point $(0, \frac{x-1}{2})$ et le cercle centré en ce point de rayon $\frac{x+1}{2}$. Il intersecte l'axe des $(t,0)$ en $(\pm y, 0)$ (avec $y > 0$ disons). Pythagore nous dit que $y = \sqrt{x}$.

Le dernier point est une projection orthogonale, ce qu'on a déjà fait.

□

Théorème 1.1.4. *L'ensemble des* **nombres** *CALREACS est un sous-corps de* $\mathbb{R}$*, algébrique, et tout élément a pour degré une pouissance de* 2*.*

(Reciproque fausse)

Démonstration. C'est un corps d'apres la proposition.

Soit x CALREAC. Soit une famille $\mathcal{A}_0 \subset \ldots \mathcal{A}_n$ adapté à $(x,0)$. On peut supposer (quitte à rajouter des ensembles intermediaires, que chauqe $\mathcal{A}_i$ ne contient que un point de plus que $\mathcal{A}_{i-1}$.

Soit K_i le sous-corps de $\mathbb{R}$ engendré par $\mathbb{Q}$ et les coordonnées des points de $\mathcal{A}_i$.

Lemme 1.1.1. *Dans ces conditions,* $[K_i; K_{i-1}]$ *de degré* 1 *ou* 2*.*

Démonstration.

Observation 1.1.6. *(préliminaire) une equation unitaire d'une droite entre deux points de* $\mathcal{A}_{i-1}$ *est à coefficients dans* K_{i-1} *(il s'agit de* $\det(\overrightarrow{AB}, (x - x_A, y - y_A)) = 0$*). L'equation unitaire d'un cercle defini par* $\mathcal{A}_{i-1}$ *est à coefficients dans* K_{i-1} *(il s'agit de* $\|\overrightarrow{(x,y)A}\|^2 = \|\overrightarrow{BC}\|^2$*).*

Supposons pour commencer qu'il n'y a aucune construction faisant intervenir l'intersection de deux cercles. Soit $M_i = (x_i, y_i)$ le nouveau point de $\mathcal{A}_i$. Ses coordonnées sont solutions d'un systeme linéaire (si M_i est l'intersection de 2 droites) ou d'un systeme d'une equation quadratique et d'une linéaire à coefficients dans K_{i-1}. Dans ce dernier cas, l'equation linéaire permet d'éliminer au choix une inconnue de l'equation quadratique, et ainsi un polynome de degré 2 annule x_i ou y_i (et l'autre lui est linéairement liée).

Le Lemme est aussi vrai quand on obtient M_i par intersection de deux cercles : le systeme est alors

$$x^2 + ax + y^2 + by + c = 0, \quad x^2 + dx + y^2 + ey + f = 0$$

il equivaut à

$$x^2 + ax + y^2 + by + c = 0, \quad (d-a)x + (e-b)y + (f-c) = 0$$

et comme tous les coefficients sont dans K_{i-1}, on est dans le cas precedent. □

Fin de la preuve : par théorème de la base telescopique $[\mathbb{Q}[x], \mathbb{Q}]$ divise $[K_n, \mathbb{Q}]$. Par ailleurs, le Lemme montre que $[K_n, \mathbb{Q}]$ est une puissance de 2 ; on a fini.

□

Applications :
- $2^{1/3}$ n'est pas CALREAC (cf probleme du temple de Delos)
- $\cos(\pi/9)$ n'est pas CALREAC (il est annulé par $8x^3 - 6x - 1$ grace à la formule bien connue $\cos(3\theta) = 4\cos^3\theta - 3\cos\theta$. En consequence, on ne pourra pas trissecter tous les angles "constructibles".
- $\sqrt{\pi}$ n'est pas CALREAC (car π est transcendant (Lindemannn)). En consequence, on ne pourra pas "construire" un carré de même aire que le disque unité.

1.1.4 Corps de rupture, corps de décomposition

Définition 1.1.8. *Soit $P \in K[X]$ irreductible, et une extension $L\backslash K$. On dit que L est un* **corps de rupture** *pour P (sur K) si $L = K(\alpha)$ pour un certain $\alpha \in L$ annulant P.*

Théorème 1.1.5. *Etant donné $P \in K[X]$ irreductible, il existe un corps de rupture de P sur K, unique à isomorphisme (non unique) près.*

Démonstration. $\exists$: le corps $K[X]/(P)$ convient car $P(\bar{X}) = \bar{0}$ (c'est bien un corps car P est irreductible).

$\exists!$:

Lemme 1.1.2. *Soit $i : K \to K'$ un isomorphisme de corps (il induit $i : K[X] \to K'[X]$ qui envoie P sur un polynôme que l'on note P'). Prenons L un corps de rupture de P sur K ($L = K(\alpha)$, pour $P(\alpha = 0)$, et L' un corps de rupture de P' sur L' ($L' = K'(\beta')$ pour $P'(\beta') = 0$, mais en principe β' n'a encore rien à voir avec α).*

Alors il existe un unique isomorphisme $L \to L'$ induisant i sur K et envoyant α sur β'.

Observation 1.1.7. *On utilisera tres souvent le morphisme induit sur l'anneau des polynomes, sans mentionner cette induction specifiquement à chaque fois.*

Avant de montrer le lemme, remarquons qu'il donne l'unicité que l'on veut, et donnons deux exemples.

Exemple 1.1.5. *$K = K' = \mathbb{Q}, P = X^3 - 2$, et $L = \mathbb{Q}(2^{1/3})$ et $L' = \mathbb{Q}(e^{2i\pi/3}2^{1/3})$... Ce sont tous les deux des corps de ruptures de P sur $\mathbb{Q}$.*

Exemple 1.1.6. *(ou l'isomorphisme est non unique) : $K = K' = \mathbb{Q}, P = X^2 - 2$ et $L = \mathbb{Q}(\sqrt{2}) = \mathbb{Q}(-\sqrt{2}) = L'$.*

Prouvons le lemme. L'unicité est évidente, il nous faut l'existence.

Notons $\bar{\text{spe}}_\alpha : K[X]/(P) \to L$ le factorisé de spe_α. C'est un isomorphisme (surjectif par definition, et injectif car P est polynome minimal de α (ou parce qu'on est sur des corps).

On a le diagramme commutatif :

$$\begin{array}{ccc} K[X] & \xrightarrow{i} & K'[X] \\ \downarrow & & \downarrow \\ K[X]/(P) & \xrightarrow{\bar{i}} & K'[X]/(P') \\ \downarrow\simeq & & \downarrow\simeq \\ L & & L' \end{array} \quad \text{car } i(P) = P'$$

Les fleches verticales du bas sont $\overline{\text{spe}_\alpha}$ et $\overline{\text{spe}'_\alpha}$. Ce sont des isomorphismes, et donc à la ligne du bas on a un isomorphisme par composition.

□

Définition 1.1.9. *Soit $P \in K[X]$ de degré ≥ 1 (irreductible ou non), et $L\backslash K$ une extension. On dit que L est un* **corps de décomposition** *de P sur K si, dans $L[X]$, P est un produit de polynômes de degré 1, et si L est minimal pour cette propriété.*

Observation 1.1.8. *la minimalité veut dire alors que L est engendré par K et les racines de P.*

Théorème 1.1.6. *Pour tout $P \in K[X]$ de degré ≥ 1, il existe une extension $L\backslash K$ pour laqsuelle L est un corps de décomposition de P sur K. Cette extension est unique à isomorphisme (non unique) près pour cette propriété. On note $L = D_K(P)$.*

Démonstration. $\exists$. Recurrence sur le degré de P (le corps n'etant pas fixé). S'il vaut 1, il n'y a rien à dire. S'il vaut n, soit L_1 un corps de rupture d'un facteur irreductible quelconque de P. Dans $L_1[X]$, P a une racine α, et on peut ecrire par division Euclidienne $P(X) = (X-\alpha)Q(X)$ avec $Q \in L_1[X]$ de degré $n-1$. Par hypothèse de récurrence, il existe un corps de décomposition de Q sur L_1, et on verifie sans peine que c'est un corps de décomposition de P sur K.

$\exists!$. Paraphrasons.

Lemme 1.1.3. *Si $i : K \to K'$, $i(P) \in K'[X]$, et L, L' corps de decompositions respectifs, alors il existe un isomorphisme $\phi : L \xrightarrow{\sim} L'$ prolongeant i.*

La preuve est une récurrence sur le degré $[L; K]$ (ou de P directement).

Si $L = K$, cela veut dire que P est scindé sur K, donc $i(P)$ scindé sur K', donc K' est un corps de décomposition de $i(P)$ sur K', et $\phi = i$...

Si $[L; K] > 1$, soit $\alpha \in L$ une racine de P, prise hors de K (c'est possible).

Soit Q le polynôme minimal de α sur K. Enfin soit $M = K(\alpha)$ un corps de rupture de Q sur K.

En face, on a $i(Q)$ qui divise $i(P)$, et si l'on choisit α' racine de $i(Q)$ dans L', alors $K'(\alpha')$ est un corps de rupture (de $i(Q)$ sur K').

Par unicité des corps de rupture : il exite $\psi : M \xrightarrow{\sim} M'$ envoyant α sur α' et induisant i.

Dans $M[X]$: $P(X) = S(X) \times (X - \alpha)$.

Dans $M'[X]$: $i(P)(X) = \psi(P)(X) = \psi(S)(X) \times (X - \alpha')$ (premiere égalité : car P est a coefficients dans K).

Soit alors $L\backslash M$ un corps de décomposition de S sur M. Et soit $L'\backslash M'$ un corps de décomposition de $\psi(S)$ sur M'. Utilisons l'hypothese de récurrence du Lemme : $\exists \phi : L \to \xrightarrow{\sim} L'$ prolongeant ψ. Il prolonge donc i, ce qu'on voulait.

□

Exemple 1.1.7. *Sur $K = \mathbb{Q}$, si $P(X) = X^3 - 2$, on a $D_K(P) = \mathbb{Q}(2^{1/3}, j)$.*

Si $P(X) = X^4 - 2$, $D_K(P) = \mathbb{Q}(2^{1/4}, i)$.

Définition 1.1.10. *Une* **cloture algébrique** *d'un corps K est une extension algébriquement close, et algébrique.*

(Plus à ce sujet plus tard.)

1.2 Corps finis

1.2.1 Caracteristique et cardinal

Définition 1.2.1. *Soit K un corps. Le* **sous-corps premier** *de K est l'intersection de tous les sous corps.*

C'est le "sous-corps engendré par 1"

Observation 1.2.1. *Soit $\phi_{nat} : \mathbb{Z} \to K$ morphisme de groupe (d'anneau !) envoyant 1 sur 1. Son noyau est un ideal de $\mathbb{Z}$, premier car K est integre. S'il est trivial, ϕ est injective, et le corps de fractions de $\mathbb{Z}$ se plonge dans K, et est donc le sous corps premier. S'il n'est pas trivial, il est de la forme (p) avec p premier et $\Im(\mathbb{Z}) \simeq \mathbb{Z}/p\mathbb{Z}$ qui est un coprs, et c'est donc le sous corps premier de K.*

Définition 1.2.2. *La* **caracteristique** *de K est 0 si son sous-corps premier est $\simeq \mathbb{Q}$; et p si son sous-corps premier est $\simeq \mathbb{Z}/p\mathbb{Z}$.*

D'après l'observation, il n'y a pas d'autre cas possible.

Proposition 1.2.1. *Soit K de caracteristique $p > 0$. L'application : $F : K \to K$ définie par $F(x) = x^p$ est un endomorphisme de corps, qu'on appelle* **l'endomorphisme de "Frobenius"**.
Si K est fini c'est un automorphisme induisant l'identité sur le sous-corps premier.

Démonstration. Pour la première assertion, il suffit de montrer que c'est un morphisme de corps (l'injectivité est alors automatique).
Ecrivons : $F(xy) = (xy)^p = x^p y^p$ par commutativité.
$F(x+y) = (x+y)^p = \sum \overline{C_p^k} x^k y^{p-k}$, mais $p | C_p^k$ si $k \neq 0, p$.
$F(1/x) = (1/x)^p = 1/x^p = 1/F(x)$ (en fait verification inutile car $F(1) = 1$).
Si K est fini et la surjectivité se suit de l'injectivité.
Enfin si $K = \mathbb{Z}/p\mathbb{Z}$, et $x \neq 0$, son ordre (multiplicatif) divise $|\mathbb{Z}/p\mathbb{Z}^*| = p - 1$. Ainsi $x^p = x^{p-1} \times x = x$.

□

1.2.2 Existence et unicité des corps finis

Observation vectorielle : si $\mathbb{F}$ est fini, $|\mathbb{F}| = (\mathrm{car}(\mathbb{F}))^n$, car c'est un $(\mathbb{Z}/\mathrm{car}(\mathbb{F})\mathbb{Z})$-espace vectoriel.

Théorème 1.2.1. *Soit un nombre premier p et un entier $n \geq 1$. Notons $q = p^n$.*
Il existe un corps de cardinal q, unique à isomorphisme (non-unique) près. Il est de caracteristique p. On le note $\mathbb{F}_q$.

Démonstration. Soit $P(X) = X^q - X$ dans $\mathbb{Z}/p\mathbb{Z}[X]$. Considérons $D_{\mathbb{Z}/p\mathbb{Z}}(P)$.
Affirmation : L'ensemble des racines de P forme un corps. (observation : si c'est vrai, par minimalité du corps de décomposition, cela veut dire que ce corps est K).
Preuve de l'affirmation.
0 est racine ; 1 est racine.
Si x et y sont des racines, $P(xy) = x^q y^q - xy = xy - xy = 0$, donc xy aussi ; $P(x+y) = (x+y)^q - x - y = F^n(x+y) - x - y = F^n(x) - x - F^n(y) - y = x^q - x + y^q - y = 0$. Enfin, $P(1/x) = \dfrac{1}{x^q} - \dfrac{1}{x} = \dfrac{x - x^q}{x^{q+1}} = 0$.
Nous savons donc que $D_{\mathbb{Z}/p\mathbb{Z}}(P)$ est precisement l'ensemble des racines de P dans $D_{\mathbb{Z}/p\mathbb{Z}}(P)$.

2ème affirmation : P n'a pas de racine double dans $D_{\mathbb{Z}/p\mathbb{Z}}(P)$.

En effet, s'il avait une racine double, sa dérivée P' partagerait cette racine, or $P' = qX^{q-1} - 1 = -1$ dans $\mathbb{Z}/p\mathbb{Z}[X]$.

Consequence des deux affirmations : $D_{\mathbb{Z}/p\mathbb{Z}}(P)$ contient precisement $deg(P)$ elements, ce qu'on voulait pour l'existence.

Unicité. Si K possède q elements, K^* est d'ordre (multiplicatif) $q-1$ dont tout element non nul x de K verifie $x^{q-1} = 1$, et donc est racine de P. Comme 0 aussi est racine de P, le polynôme P est scindé dans K (il y trouve q racines) et K est minimal pour cela, c'est donc $D_{\mathbb{Z}/p\mathbb{Z}}(P)$. On applique l'unicité des corps de décomposition.

□

1.2.3 $\mathbb{F}_q^*$

Théorème 1.2.2. *$\mathbb{F}_q^*$ est un groupe cyclique.*

1.2.4 Carrés

Théorème 1.2.3. *Si p est un nombre premier impair, et $q = p^n$, alors -1 est un carré de $\mathbb{F}_q$ si et seulement si $q \equiv 1\,[mod\,4]$.*

cf. Partiel 2013.

1.3 Cloture algébrique

Rappel : $\bar{K}\backslash K$ est une cloture algébrique de K si c'est une extension algébrique, et si $\bar{K}$ est algébriquement clos.

Observation 1.3.1. *L est alg. clos si et seulement si tout polynôme dans $L[X]$ de degré ≥ 1 a une racine dans L.*

Dans cette partie, on admet l'axiome du choix.

Théorème 1.3.1. *Si K est un corps, il existe une cloture algébrique de K.*

Deux cloture algébriques de K sont isomorphes par un isomorphisme induisant l'identité sur K.

Lemme 1.3.1. *(Zorn) Soit un ensemble non vide, inductivement ordonné (toute partie totalement ordonnée non-vide admet un majorant).*

Alors il existe un élément maximal.

Preuve : cf. S. Lang, *Algebra*, Appendice 2 (Set theory). C'est equivalent à l'axiome du choix.

1.3.1 Existence

Lemme 1.3.2. *Il existe une extension de K dans laquelle tout polynôme de $K[X]$ de degré ≥ 1 possède une racine.*

Démonstration. Soit $S = \{X_P, P \in K[X] \setminus K\}$. (où K est vu comme les polynômes de degré 0 dans $K[X]$).

Soit $K[S]$ l'anneau des polynômes à indeterminées (commutatives) dans S.

Lemme 1.3.3. $I = (\{P(X_P), P \in K[X] \setminus K\}) \neq K[S]$.

Sinon : il existe $Q_1, \dots Q_n, P_1, \dots P_n \in K[S]$ tels que

$$\sum_{i=1}^{n} Q_i P_i(X_{P_i}) = 1 \qquad (*)$$

Notons $X_{P_i} = X_i$ pour plus de commodité. Completons en $X_{n+1}, \dots, X_N$ pour obtenir la liste (finie) de toutes les indeterminées apparaissant dans les Q_i.

Prenons F un corps de rupture pour tous les $P_i, i = 1 \dots n$.

Nous avons, par telescopie, $[F; K] < \infty$.

Soit α_i une racine de P_i dans F, si $i \neq n$ et $\alpha_i = 0$ si $i > n$.

Observons $(*)$ specialié en $X_i \mapsto \alpha_i$.

$$\sum Q_i(X_1, \dots, X_N) \times P_i(X_i) = 1 \qquad (*)$$

$$\sum Q_i(\alpha_1, \dots, \alpha_N) \times P_i(\alpha_i) = 1$$

$$0 = 1,$$

une contradiction. Nous avons donc le sous-lemme.

Par Zorn, il existe un ideal maximal de $K[S]$ contenant I. Notons le $\mathfrak{m}$. Maintenant $K[S]/\mathfrak{m}$ est un corps, et il convient manifestement.

□

Lemme 1.3.4. *Il existe une extension $M \backslash K$ telle que tout polynôme* **dans** *$M[X]$ (de degré ≥ 1) ait une racine dans M.*

Démonstration. Soit L_1 le corps donné par le Lemme 1.3.2 pour K. Et soit L_{i+1} le corps donné par le Lemme 1.3.2 pour L_i. On a

$$K = L_0 \subset L_1 \subset L_2 \cdots \subset L_n \subset \dots$$

et prenons M l'union croissante des L_i. C'est un corps (car les operations se passent dans l'un des L_i). Tout polynômes à coefficients dans M a ses coefficients dans un certain L_i, donc possède une racine dans L_{i+1} donc dans M. □

Nous pouvons maintenant prouver l'existence d'une cloture algébrique. Soit $M \backslash K$ donnée par le lemme précédent, et soit $\bar{K}$ l'ensemble des éléments de M algébriques sur K.

C'est un corps (on l'a déj'a vu).

Par ailleurs, pour tout polynôme P dans $\bar{K}[X]$, si L est le corps engendré par K et ses coefficients, $[L; K] < \infty$. Prenons une racine de P dans M. Son degré sur L est fini, donc son degré sur K aussi, et donc elle est algébrique sur K, et donc dans $\bar{K}$.

1.3.2 Unicité

Lemme 1.3.5. *Si $L \backslash K$ et $L = K(\alpha)$ avec α algébrique sur K, et si $\sigma : K \to M$ avec M algebriquement clos, alors le nombre d'extensions possibles de σ à L est égal au nombre de racines distinctes de P_α dans M.*

(consequence de l'unicité des corps de ruptures.)

Lemme 1.3.6. *Si $L \backslash K$ est algébrique, et $i : K \to M$ avec M algebriquement clos, alors i s'etend à L.*

Si M algebrique sur $i(K)$, et L alg. clos, alors $\tilde{i} : L \to M$ est un isomorphisme.

Soit $\{(F,\sigma),\ L\backslash F\backslash K,\ \sigma : F \to M, \sigma|_K = i\}$.

C'est non vide, inductivement ordonné. Par Zorn, il existe un element (F_0, σ_0) maximal.

Si $F_0 \neq L$, soit $\alpha \in L \setminus F_0$. Il est algebrique sur F_0. Comme M algebriquement clos, le lemme precedent dit que σ s'etend à $F_0(\alpha)$, contradiction.

Donc $F_0 = L$.

Supposons M algebrique sur $i(K)$. C'est aussi une extension algébrique de $\sigma(L)$. Mais si L est algébriquement clos, $M = \sigma(L)$ et $\tilde{:}L \to M$ est surjective (donc un isomorphisme).

1.3.3 Compléments, applications aux extensions normales.

Théorème 1.3.2. *Soit $L\backslash K$ une extension finie (ou encore algébrique avec K dénombrable). Soit $\bar{K}\backslash L$ une cloture algébrique.*

LASSE :

1. *Pour tout $\phi : L \to \bar{K}$ induisant Id_K, on a $\phi(L) = L$.*
2. *L est un corps de* **décomposition sur** *K d'une famille de polynômes de $K[X]$.*
3. *Tout $P \in K[X]$ ayant une racine dans L y est scindé.*

Dans ce cas, on dit que l'extension $L\backslash K$ est **normale.**

Démonstration. $(1 \implies 3)$. Soit $\alpha \in L$, et P_α son polynôme minimal.

Soit $\beta \in \bar{K}$ une autre racine de P_α. Nous voulons montrer que $\beta \in L$.

On utilise l'unicité des corps de rupture : $\exists \sigma : K(\alpha) \to K(\beta)$ induisant l'identité sur K. Il nous suffit de savoir étendre σ à L, car alors le point (1) garantie que l'image de L est dans L, et donc $\beta \in L$.

Soit alors $(x_i, i = 0, 1, 2 \dots)$ engendrant L sur $K(\alpha)$ (famille finie, ou dénombrable), et P_i le polynome minimal de x_i sur $K(\alpha, x_1, ..., x_{i-1})$. Notons $\alpha = x_0$, pour unifier.

$y_0 = \beta$.

On défini **inductivement** les y_i comme suit.

y_1 est une racine (arbitraire) de $\sigma(P_1)$ dans $\bar{K}$.

On étend σ à $K(x_0, x_1)$ en envoyant x_1 sur y_1. (toujours possible par unicité des corps de rupture).

Si on a déjà défini $y_0, \dots, y_i$, et σ sur $K(x_0, \dots, x_i)$, on défini y_{i+1} comme étant une racine (arbitraire) de $\sigma(P_i)$ dans $\bar{K}$, et on étend σ à $K(x_0, \dots, x_{i+1})$ en envoyant x_{i+1} sur y_{i+1}.

Inductivement on a donc défini σ sur tout $K(x_0, x_1, \dots) = L$, à valeurs dans $\bar{K}$, ce qu'il nous fallait.

$(3 \implies 2)$. L est le corps de décomposition de la famille des $P_\alpha, \alpha \in L$.

$(2 \implies 1)$ Disons que L est le corps de décoposition d'une famille $(P_i, i = 0, 1, \dots)$ dans $K[X]$.

Soit S l'ensemble des racines de tous ces polynomes : $S = (\alpha \in \bar{K}, \exists i, P_i(\alpha) = 0)$.

On a par hypothèse $L = K(S)$.

Soit $\sigma : L \to \bar{K}$ induisant l'identité sur K, et soit $L' \subset \bar{K}$ son image. On doit montrer que $L = L'$. Montrons déjà que $\sigma(S) \subset L$. C'est facile : si $\alpha \in S$, $\sigma(\alpha)$ est une racine de $\sigma(P_i) = P_i$ (car $\sigma|_K = \mathrm{Id}_K$).

On conclut par cette observation générale.

Lemme 1.3.7. *Soit $L\backslash K$ algébrique. Si $\sigma : L \to L$ induit l'identité sur K, c'est un automorphisme de L.*

C'est un endomorphisme. Si $x \notin \sigma(L)$, soit P_x son polynôme minimal sur K. Disons qu'il a k racines dans L. On a $\sigma(P_x)$ a donc k racines dans $\sigma(L)$. Mais c'est P_x et donc P_x a k racines dans $\sigma(L)$. Comme x est l'une d'elles, $x \in \sigma(L)$.

□

Définition 1.3.1. *Dans $\bar{K}\backslash K$, α est dit* **séparable** *sur K si son polynôme minimal sur K n'a pas de racine multiple dans $\bar{K}$.*

Une extension est dite **séparable** *si tous ses elements sont séparables.*

Exemple 1.3.1. *En caracteristique 0, tout élément algébrique est séparable. En effet, P'_α est alors non nul, et si $P'_\alpha \wedge P_\alpha \neq 1$, on peut calculer le pgcd sur K, et faire la division de P_α par ce pgcd, ce qui contredit l'irreductibilité de P_α.*

Proposition 1.3.1. *Si $L\backslash K$ est séparable de degré n, il existe exactement n morphismes (differents) $\sigma_1, \ldots, \sigma_n : L \to \bar{K}$ induisant l'identité sur K.*

Si en plus l'extension est normale, il existe exactement n automorphismes de L induisant l'identité sur K. Ces automorphismes forment un groupe, qu'on appelle le groupe de Galois de $L\backslash K$.

Démonstration. Ecrivons $L = K(x_1, \ldots x_m)$, et P_i le polynôme minimal de x_i sur $K(x_1, \ldots x_{i-1}) = L_{i-1}$.

On a $[L; K] = \prod deg(P_i)$.

Par ailleurs, le lemme 1.3.5 (premier lemme de l'unicité des clotures algébriques) donne exactement $deg(P_i)$ prolongement possible de tout morphisme $L_{i-1} \to \bar{K}$ (induisant Id_K) à L_i. Cela donne ce que l'on veut.

La seconde assertion découle de la définition d'extension normale (premier point du theoreme). □

Théorème 1.3.3. *(Element primitif)*

Si $L\backslash K$ finie séparable, il existe $\alpha \in L$ tel que $L = K(\alpha)$.

Démonstration. Si L est fini, c'est parce que $L*$ est cyclique.

Supposons L infini. Soit $\bar{K}$ une cloture algébrique de K.

Soit $\sigma_i : L \to \bar{K}, i = 1, \ldots, n = [L; K]$ la collection de plongement dans $\bar{K}$.

Notons $E_{i,j} = \{x \in L, \sigma_i(x) = \sigma_j(x)\}$.

Pour $i \neq j$, ce sont des s-e.v. stricts de L (sur K), et il n'y en a qu'un nombre fini.

Lemme 1.3.8. *Si K un corps infini, et L un K-epace vectoriel (de dimension finie), et V_i une famille finie ($i = 1, \ldots, m$) de sous-espaces stricts de L, alors l'union des V_i n'est* **pas** *L tout entier.*

Démonstration. Disons que chaque V_i est un hyperplan (si ce n'est pas le cas, en complétant une base de V_i, on le plonge dans un hyperplan de L, et il suffit de montrer que l'union des hyperplans n'est pas L tout entier). Soit α_i une forme linéaire de noyau V_i. Prenons $x_1 \notin V_1$. Supposons par recurrence que x_k est construit de sorte que x_k n'est dans aucun $V_i, i \leq k$. Si $\alpha_{k+1}(x_k) \neq 0$, alors on pose $x_{k+1} = x_k$ et x_{k+1} n'est dans aucun $V_i, i \leq k+1$. Si au contraire $\alpha_{k+1}(x_k) = 0$, prenons $v \notin V_{k+1}$. Notons $X = \{\alpha_i(x_k)$, $i \leq k$ (notons que 0 n'y est pas). C'est un sous ensemble fini de K. Notons $\alpha_{i,v} : K \to K$ définie par $\alpha_{i,v}(\lambda) = \alpha_i(\lambda v)$. Ce sont des applications linéaires qui sont soit nulles soit injectives. Ainsi $\alpha_{i,v}^{-1}(X)$ est fini, pour chaque i. Aussi, il existe $\lambda \in K^*$ hors de chaque $\alpha_{i,v}^{-1}(X)$ (pour $i \leq k$). Pour ce λ, et pour chaque $i \leq k$, $\alpha_i(\lambda v) \notin X$ et donc $\alpha_i(x_k - \lambda v) \neq 0$. Par ailleurs, $\alpha_{k+1}(x_k - \lambda v) = \lambda \alpha_{k+1}(v) \neq 0$. On peut poser $x_{k+1} = x_k - \lambda v$, il verifie l'hypothèse de récurrence. Quand $k = n$, on a fini. □

Gràce au lemme, on peut choisir : $\alpha \notin \bigcup_{i \neq j} E_{i,j}$.

Soit P_α le polynôme minimal de α sur K. Chaque $\sigma_i(\alpha)$ annule $\sigma_i(P_\alpha) = P_\alpha$. Cela force le degré de P_α à être $\geq n = [L; K]$.

Ainsi $[K(\alpha); K] \geq n = [L; K]$, mais comme $K(\alpha) \subset L$, on a égalité, apr égalité des dimensions.

□

1.4 Cyclotomie

1.4.1 Racines de l'unité, racines primitives

On considère $P(X) = X^n - 1$ dans $K[X]$.

Observation 1.4.1. *Si la caracteristique $car(K)$ ne divise pas n, P n'a que des racines simples dans $D_K(P)$.*

En revanche si $car(K)$ divise n, notons $n = mp$ avec p la caracteristique $p = car(K)$. Dans ce cas, par le Frobenius sur le corps $K(X)$, on a $P(X) = (X^m - 1)^p$. Ainsi, P n'a que des racines multiples.

Dans la suite, on suppose $p \wedge n = 1$.

Notation : $\mu_n(K) = \{\zeta \in K, P(\zeta) = 0\}$.

Observation 1.4.2. *sous nos hypothèses, $|\mu_n(D_K(P)| = n$.*

On notera $K_n = D_K(P)$, car on en aura souvent besoin.

Observation 1.4.3. *$\mu_n(K) < K*$ (sous-groupe). Ainsi, il est cyclique, et isomorphe à un certain $\mathbb{Z}/d\mathbb{Z}$, pour $d|n$.*

Définition 1.4.1. *Une* **racine primitive n-ième de l'unité** *dans K_n est un générateur du groupe $\mu_n(K_n)$.*

Observation 1.4.4. *$\zeta \in K_n$ est une racine primitive n-ième de l'unité dans K si et seulement si ($\zeta^n = 1$ et $\forall d < n, d > 0, d|n, \zeta^d \neq 1$.*

Observation 1.4.5. *K_n possède $\varphi(n)$ racine primitives n-ièmes distinctes. On note $\mu_n(K)^*$ leur ensemble.*

Définition 1.4.2. $\Phi_{n,K}(X) = \prod_{\zeta \in \mu_n(K)^*} (X - \zeta) \in K_n[X]$ *est le* **n-ième polynôme cyclotomique** *"de" K. Il est de degré $\varphi(n)$.*

On n'ose pas dire "sur" K.

Observation 1.4.6. $(X^n - 1) = \prod_{d|n, 0<d<n} \Phi_{d,K}$ *simplement car $\mu_n(K) = \bigsqcup \mu_d^*(K)$. Mais le côté gauche ne dépend pas de K... Observer la relation produite au niveau des degrés des polynômes.*

Exemple 1.4.1. *Disons sur $\mathbb{Q}$.*

- $\Phi_1(X) = X - 1$.
- Φ_2 *vérifie* $\Phi_1(X)\Phi_2(X) = X^2 - 1$, *donc* $\Phi_2(X) = X + 1$.
- $\Phi_3(X)$ *vérifie* $\Phi_1(X)\Phi_3(X) = X^3 - 1$, *donc* $\Phi_3(X) = X^2 + X + 1$.
- $\Phi_4(X) = \dfrac{X^4 - 1}{\Phi_1(X)\Phi_2(X)} = \dfrac{X^4 - 1}{X^2 - 1} = X^2 + 1$

— $\Phi_5(X) = \dfrac{X^5-1}{\Phi_1(X)} = X^4+X^3+X^2+X+1$
— $\Phi_6(X) = \dfrac{X^6-1}{\Phi_1(X)\Phi_2(X)\Phi_3(X)} = X^2-X+1$
— $\Phi_7(X) = X^6+X^5+X^4+X^3+X^2+X+1$
— $\Phi_8(X) = X^4+1$
— *ad libidum...*

Proposition 1.4.1. — $\Phi_{n,\mathbb{Q}}$ *est à coefficients entiers, unitaire.*
— $\forall K$ *soit* $\sigma : \mathbb{Z} \to K$ *le morphisme d'anneau, on a* $\Phi_{n,K} = \sigma\Phi_{n,\mathbb{Q}}$.
— *En particulier,* $\Phi_{n,\mathbb{F}_p} = \overline{\Phi_{n,\mathbb{Q}}}$.

Observation 1.4.7. *Ainsi, on oubliera souvent la mention du corps de base.*

Démonstration. Comme illustré dans l'exemple précédent, $\Phi_{n,\mathbb{Q}}$ s'obtient par division Euclidienne de X^n-1 par un produit de $\Phi_{n,\mathbb{Q}}$. On obtient donc le point 1 par récurrence sur n. (la division Euclidienne dans $\mathbb{Z}[X]$ peut se faire si le dénominateur est unitaire).

Le second point est aussi une récurrence. Le cas $n=1$ est trivial. Ensuite, comme σ envoie X^n-1 sur X^n-1, on obtient que

$$X^n-1 = \sigma(\Phi_{n,\mathbb{Q}}) \times \prod \sigma(\Phi_{d,\mathbb{Q}}) = \sigma(\Phi_{n,\mathbb{Q}}) \times \prod \Phi_{d,K}.$$

Or on a aussi $X^n-1 = \Phi_{n,K} \times \prod \Phi_{d,K}$. Comme l'anneau des polynômes est integre, $BA = CA \implies B = C$, et on a ce qu'on veut.

□

1.4.2 Irréductibilité

Théorème 1.4.1. Φ_n *est irréductible sur* $\mathbb{Z}[X]$.

Conséquence immédiate :

Corollaire 1.4.1. *Si* ζ *est une racine primitive* n*-ième de l'unité dans* K *de caracteristique* 0*, alors* Φ_n *est son polynôme minimal sur* $\mathbb{Q}$ *et* $[\mathbb{Q}(\zeta),\mathbb{Q}] = \varphi(n)$.

Démonstration. Soit $K = D_{\mathbb{Q}}(\Phi_n)$, et ζ une racine primitive n-ième de l'unité dans K.

Pour tout premier p ne divisant pas n, ζ^p est une autre racine primitive n-ième de l'unité dans K.

On choisit un tel p. Soit F le polynôme minimal de ζ sur $\mathbb{Q}$ et G celui de ζ^p.

Comme F et G sont des facteurs irreductibles de Φ_n, ils sont dans $\mathbb{Z}[X]$.

Observation 1.4.8. *Ici on a utilisé le lemme de Gauss : les facteurs irreductibles de* Φ_n *dans* $\mathbb{Z}[X]$ *sont unitaires, donc (lemme de Gauss) irreductibles dans* $\mathbb{Q}[X]$*. Ainsi, la decopositions en facturs irreductibles dans* $\mathbb{Z}[X]$ *donne celle dans* $\mathbb{Q}[X]$.

Lemme 1.4.1. $F = G$.

Par l'absurde : On va montrer que si ce n'est pas le cas, $\bar{\Phi_n}$ a une racine double. On a $F(X)|G(X^p)$ car ce dernier annule ζ et est unitaire irréductible. Disons que $G(X^p) = F(X)H(X)$ dans $\mathbb{Z}[X]$.

Dans $\mathbb{Z}/p\mathbb{Z}$, on a $\bar{G}(X^p) = \bar{F}(X)\bar{H}(X) = \overline{G(X)}^p$ (par le Frobenius).

Ainsi tout facteur irréductible (disons Ψ) de $\bar{F}$ doit diviser $\bar{G}$.

Mais si $F \neq G$, on a aussi $FG|\Phi_n$, donc $\bar{F}\bar{G}|\bar{\Phi_n}$ et donc $\Psi^2|\bar{\Phi_n}$. Cela provoque une racine double pour $\Phi_{n,\mathbb{F}_p}$ dans son corps de décomposition, et cela contredit une remarque précédente (nous avons choisi p ne divisant pas n !). Le Lemme est montré.

Finalement, toute racine primitive n-ième de l'unité s'écrit

$$\zeta' = \zeta^{p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}}$$

donc en utilisant plusieurs fois le lemme precedent, on obtient qu'elles ont toutes le même polynôme minimal sur $\mathbb{Q}$, et c'est F.

Ainsi $deg(F) \geq |\mu_n^*(K_n) = deg(\Phi_n)$. Comme par ailleurs $F|\Phi_n$ et que les deux sont unitaires, on a $F = \Phi_n$.

□

Corollaire 1.4.2. *(cf partiel 2013).*

1.5 Extensions d'anneaux

Soit A un anneau commutatif, unifère (tous le seront !... ?)

1.5.1 Définitions

Définition 1.5.1. (B, ρ) *est une* A**-algèbre** *si* B *est un anneau (pas forcement commutatif) et* $\rho : A \to B$ *un morphisme d'anneau tel que* $\rho(a)b = b\rho(a)$ *pour tout* $a \in A$ *et* $b \in B$.

On appelle ρ le morphisme structural de l'algèbre B.

Observation 1.5.1. *B est alors muni d'une structure de A-module $A \times B \to B$ donnée par le produit $\rho(a)b$.*

Mais il a une loi supplementaire, $B \times B \to B$ (la multiplication dans B), qui est A-linéaire.

Observation 1.5.2. *L'observation ci-dessus est parfois prise comme définition. Dans ce cas, B n'est pas forcement associative ni unifere...*

Exemple 1.5.1. $A[X_1, \dots, X_n]$.

$\mathcal{M}_n(A)$.

Un morphisme de A-algbre est un morphisme d'anneau commutant aux morphismes structuraux.

Une sous-algbre est l'image d'un morphisme injectif.

Une **extension** de l'anneau A est une A-algèbre avec morphisme structural ρ **injectif**.

Observation 1.5.3. *Une extension de corps est bien une extension d'anneau, d'un corps, qui se trouve être un corps.*

1.5.2 Elements entiers

Comparez aux résultats sur les éléments algébriques.

Théorème 1.5.1. *Soit A un anneau commutatif, et (B, Id_A) une extension de A. Soit $\alpha \in B$. LASSE.*

- $\exists P \in A[X]$ **unitaire** *avec* $P(\alpha) = 0$.
- $A[\alpha]$ *est un* A**-module** *de type fini.*

— *Il existe un sous-$A[\alpha]$-module de B contenant 1 (donc $A[\alpha]$) et qui est de type fini* **sur** *A.*

On dit alors que α est **entier** *sur A.*

Démonstration. 1 $\implies$ 2. Par division Euclidienne dans $A[X]$ par un unitaire (en l'occurence P), la famille $1, \alpha, \ldots, \alpha^{deg(P)-1}$ engendre $A[\alpha]$ comme A-module.

2 $\implies$ 3 trivial.

3 $\implies$ 1. Soit M ce module, et $w_1, \ldots w_n$ des générateurs sur A. Ecrivons

$$\alpha w_i = \sum_{j=1}^{n} a_{i,j} w_j$$

avec $a_{i,j} \in A$ (possible car $\alpha w_i \in M$).

Observons la matrice $(a_{i,j})$ ainsi vendue.

On a

$$((a_{i,j}) - \alpha I_n) \times \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

(la matrice de gauche, disons N, etant dans $\mathcal{M}_n(A[\alpha])$).

Soit $\hat{N} = {}^tCom(N)$ de sorte que $\hat{N}N = \det(N) I_n$.

Comme $\hat{N}N \times \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$, on a

$$\forall i, \det(N) w_i = 0$$

Comme $1 \in M$ par hypothèse, cela donne $\det N = 0$.

Or on observe que $\det N$ est un polynôme unitaire en α à coefficients dans A. Cela prouve ce qu'on voulait.

□

Définition 1.5.2. *Une extension est dite* **entière** *si tous ses éléments sont entiers.*

Proposition 1.5.1. *Une extension de type fini comme A-algègre,* **entière***, est toujours de type fini* **comme A-module.**

Démonstration. Ecrivons $B = A[\alpha_1, \ldots, \alpha_n]$ avec α_i entier sur A.

Soit $k \leq n$, sur lequel on procède par récurrence. D'apres le thèorème, $A[\alpha_1, \ldots, \alpha_k]$ est de type fini comme $A[\alpha_1, \ldots, \alpha_{k-1}]$-module, ainsi en combinant (téléscopiquement) les familles génératrices, par récurrence, il est de type fini comme A-module.

□

Proposition 1.5.2. *Si C est une extension entière de B (supposé commutatif) et B est une extension entière de A, alors C est une extension entière de A.*

Démonstration. Si $\alpha \in C$, soit $b_0, \ldots b_{n-1} \in B$ tels que $(\alpha^n + b_{n-1}\alpha^{n-1} + \cdots + b_0) = 0$.

$A[b_0, \ldots, b_{n-1}]$ est de type fini comme A-module par la proposition précédente (1.5.1).

De même $A[b_0, \ldots, b_{n-1}, \alpha]$ est de type fini comme $A[b_0, \ldots, b_{n-1}]$-module (Proposition précédente (1.5.1) aussi).

Par telescopie (et commutativité), $A[b_0, \ldots, b_{n-1}, \alpha]$ est de type fini comme A module.

Le théorème 1.5.1 (la partie (3 $\implies$ 1)) implique que α est entier sur A. □

1.5.3 Cloture integrale

Proposition 1.5.3. *Soit $C \backslash A$ une extension d'anneau, et $B = \{\alpha \in C, \alpha$ entier sur $A\}$. Alors B est un anneau.*

On l'appelle **la cloture integrale** *de A dans C.*

Démonstration. Soient $\alpha, \beta \in B$ (c.à.d. entiers sur A), et $M = A[\alpha], N = A[\beta]$.

M et N sont de type fini comme A-modules.

$A([\alpha])[\beta]$ aussi (mêmes raisons téléscopiques que précédemment).

Cependant, $\alpha + \beta$ et $\alpha\beta$ sont dedans. Le théorème 1.5.1 (la partie (3 $\implies$ 1)) s'applique encore.

□

Exemple 1.5.2. *$A = \mathbb{Z}$ et K extension algébrique de $\mathbb{Q}$ (on dit que K est un "corps de nombres"). La cloture integrale de $\mathbb{Z}$ dans K est l'anneau des* **entiers algébriques** *de K (c'est une définition). On la note $\mathcal{O}_K$. On verra quelques exemples explicites dans le cas d'une extension quadratique.*

Définition 1.5.3. *A (integre) est* **integralement clos** *si c'est lui-même l'anneau des entiers de son corps de fractions.*

Proposition 1.5.4. *Si A est factoriel, il est integralement clos.*

Démonstration. Soit $\frac{a}{b}$ un entier sur A, avec $b \neq 0$, non-inversible.

Soit p premier divisant b et pas a.

Si on a

$$\left(\frac{a}{b}\right)^n + a_{n-1}\left(\frac{a}{b}\right)^{n-1} + \cdots + a_0 = 0$$

on obtient

$$a^n + ba_{n-1}a^{n-1} + \cdots + b^n a_0 = 0.$$

Or $p|b$ donc $p|a^n$, donc $p|a$ contradiction. □

1.5.4 Exemples quadratiques

Dans cette partie $A = \mathbb{Z}$, $B = K = \mathbb{Q}(\omega)$ avec $\omega^2 \in \mathbb{Z}$.

Exemple 1.5.3. *$K = \mathbb{Q}(i)$ ou encore $K = \mathbb{Q}(\sqrt{2})$ ...*

Observation 1.5.4. *Nous avons une involution de K : $^- : K \to K$ qui fixe $\mathbb{Q}$ et envoie ω sur $-\omega$. C'est un automorphisme de corps, et c'est le seul !*

Théorème 1.5.2. *Supposons $d \in \mathbb{Z}$ sans facteur carré, différent de 1.*

Soit $\omega \in \bar{Q}$ tel que $\omega^2 = d$.

Si $d \equiv 2\,[mod\,4]$, ou $d \equiv 3\,[mod\,4]$, les entiers algébriques de $\mathbb{Q}(\omega)$ sont les $a + b\omega$, pour $a, b \in \mathbb{Z}$. C'est à dire : $\mathcal{O}_{\mathbb{Q}(\omega)} = \mathbb{Z}[\omega]$.

Si $d \equiv 1\,[mod\,4]$, les entiers algébriques de $\mathbb{Q}(\omega)$ sont les $a + b(\frac{1+\omega}{2})$, pour $a, b \in \mathbb{Z}$. C'est à dire : $\mathcal{O}_{\mathbb{Q}(\omega)} = \mathbb{Z}[\frac{1+\omega}{2}]$.

Observation 1.5.5. *On pourrait avoir peur que ce deuxième cas ne contredise la proposition précédente (factoriel implique integralement clos), mais il faut se rendre compte, par exemple, que pour $d = -3$, l'anneau "naturel" $\mathbb{Z}[i\sqrt{3}]$ n'est pas factoriel (exercice : 4 y a deux décompositions en produits de premiers).*

Observation 1.5.6. $\mathbb{Z}[\frac{1+\omega}{2}]$ *contient* $\mathbb{Z}[\omega]$. *En effet,* $a+b\omega = a-b+2b(\frac{1+\omega}{2})$.

Démonstration. Soit u un element de K. Ecrivons $u = \dfrac{a+b\omega}{c}$ avec $a, b, c \in \mathbb{Z}$ sans facteur commun, et $c \neq 0$.

Supposons $b \neq 0$. Le polynôme

$$(X-u)(X-\bar{u}) = X^2 - \frac{2a}{c}X + \frac{a^2-db^2}{c^2}$$

est le polynôme minimal P_u de u (il annule u et est de degré 2, soit le plus petit possible).

Par ailleurs, si un polynôme entier unitaire irréductible (sur $\mathbb{Z}$) annule u, par Lemme de Gauss, il divise le polynôme minimal de u (sur $\mathbb{Q}$).

Ainsi u est entier si et seulement si $\frac{2a}{c} \in \mathbb{Z}$ et $\frac{a^2-db^2}{c^2} \in \mathbb{Z}$.

Supposons u entier. Montrons pour commencer que $c = 1$ou2.

Soit p un nombre premier divisant c. Nous avons 2 cas :

— si $p|a$, on a $p^2|db^2$, or il ne divise pas b^2 (cela ferait un facteur commun à a, b, c), et d est sans facteur carré. contradiction.

— si p ne divise pas a, il divise 2, donc $p = 2$. Dans ce cas, si $4|c$, $2a/c \neq \mathbb{Z}$, contradiction.

Bilan : $c = 1$ ou 2.

Si $c = 1$, notre élément u est bien dans $\mathbb{Z}[\omega]$ (et donc, au besoin, dans $\mathbb{Z}[\frac{1+\omega}{2}]$).

Si $c = 2$, nous allons montrer que $\equiv 1\,[4]$ et que a et$b$ sont impairs. Cela montrera que dans ce cas, en écrivant u sous la forme $u = \dfrac{a-b}{2} + \dfrac{b(1+\omega)}{2}$, on a bien $u \in \mathbb{Z}[\frac{1+\omega}{2}]$.)

On a $4|(a^2 - db^2)$.

Distonguons deux cas.

— b pair. Alors $b^2 \equiv 0\,[4]$, et comme $4|(a^2 - db^2)$, $a^2 \equiv 0\,[4]$, ainsi a est pair, et comme c aussi, ils ont tous trois un facteur premier commun, contradiction.

— b impair. Alors $b^2 \equiv 1\,[4]$. A nouveau, il y a en principe deux cas

— $db^2 \equiv 2$ ou $3\,[4]$. Il vient $a^2 \equiv 2$ ou $3\,[4]$. impossible pour un carré.

— $db^2 \equiv 1\,[4]$. Alors $d \equiv 1\,[4]$. Il vient $a^2 \equiv 1\,[4]$. Cela oblige a à être impair.

Comme $u = \dfrac{a-b}{2} + \dfrac{b(1+\omega)}{2}$ avec a et b impairs, on a bien $u \in \mathbb{Z}[\frac{1+\omega}{2}]$ (qui est le cas prévu, car, on l'a vu, $d \equiv 1\,[4]$.

Nous avons donc établi que l'anneau des entiers est contenu dans $\mathbb{Z}[\omega]$ si $d \equiv 2, 3\,[4]$ et dans $\mathbb{Z}[\frac{1+\omega}{2}]$ si $d \equiv 1\,[4]$.

Réciproquement, si $u \in \mathbb{Z}[\omega]$, $c = 1$, et u est clairement entier algébrique. Si $u \in \mathbb{Z}[\frac{1+\omega}{2}]$ alors $c = 2$ et $(a-b)$ est pair (ecrire $u = \frac{(a-b)+b(1+\omega)}{c}$), et même, chacun ($a$, et b) est impair car sinon a, b, c sont tous pairs. Si $d \equiv 1\,[mod\,4]$, $a^2 - db^2$ est bien divisible par 4, et u est bien entier.

□

On peut ainsi "dessiner" l'anneau $\mathcal{O}_{\mathbb{Q}(i)}$ et l'anneau $\mathcal{O}_{\mathbb{Q}(\sqrt{-3})}$.

Reprenons K un corps de nombres quadratique.

Définition 1.5.4. $N : K \to \mathbb{Q}$ *donnée par* $N(u) = u\bar{u}$ *est appelée "norme" sur* K.

On a $N(uv) = N(u)N(v)$. Attention, N peut etre négative... On n'a pas non plus d'inégalité triangulaire...

Observation 1.5.7. *Si* u *est entier sur* $\mathbb{Z}$ *alors* $N(u) \in \mathbb{Z}$.

En effet, on l'a déjà utilisé dans la preuve du théorème : si Q_u *est unitaire irréductible sur* $\mathbb{Z}$, *et annulant* u, *il est irréductible sur* $\mathbb{Q}$, *donc a degré* 2, *c'est donc* $P_u = (X-u)(X-\bar{u})$, *dont le terme constant est* $N(u)$.

Lemme 1.5.1. *Soit u entier sur $\mathbb{Z}$.*

u est inversible dans l'anneau des entiers (on dit que c'est une unité) si et seulement si $N(u) = \pm 1$.

Démonstration. $\Longrightarrow$. $1 = N(uu^{-1}) = N(u)N(u^{-1})$, et les deux sont dans $\mathbb{Z}$, donc $= \pm 1$.

Reciproque. $\bar{u}u = \pm 1$, donc $\bar{u} = \pm u^{-1}$. Or $^-$ preserve l'integralité. □

Quelques "cas exceptionnels."

Corollaire 1.5.1. *Soit $d < 0$ sans facteur carré, et $\omega^2 = d$. Si $\mathbb{Q}(\omega)$ possède des unités differentes de ± 1, alors $d = -1$ ou $d = -3$.*

Exercice (calcul explicite de $N(u)$).

Proposition 1.5.5. *Si $d < 0$ dans $\mathbb{Z}$ sans facteur carré, $\omega^2 = d$, alors l'anneau des entiers $\mathcal{O}_{\mathbb{Q}(\omega}$ est Euclidien pour la norme N si et seulement si*

$$d \in \{-1, -2, -3, -7, -11\}.$$

Observation 1.5.8. *Quand $d < 0$, N est le module complexe au carré.*

Démonstration. Soient e_1, e_2 deux entiers de $\mathbb{Q}(\omega) \subset \mathbb{C}$.

Soit $z = e_1/e_2 \in \mathbb{Q}(\omega)$.

La question est de savoir s'il existe e_3 entier tel que $z = e_3 + \xi$ avec $N(\xi) < 1$ (car alors $e_1 = e_2e_3 + e_2\xi$).

Prenons e_3 parmi les plus proches de z.

C'est maintenant **un problème métrique** et quitte à translater, on peut supposer $e_3 = 0$ (ou plus pratiquement, z dans le triangle $0, 1, \omega'$, avec $\omega' = \omega$ ou $= (1 + \omega)/2$ selon le type de reseau).

Comme $\mathcal{O}_{\mathbb{Q}(\omega)}$ est un reseau, la situation est la suivante :

(dessin du triangle $0, 1, \omega'$, des mailles adjacentes à 0, et de la couronne suivante... 2 cas, selon le type de reseau).

Il suffit de voir que pour les d donnés, tout point du triangle isocèle (selon le type du reseau) $0, 1, \omega'$ est à distance < 1 d'un sommet. (exercice).

Si d n'est pas dans la liste donnée.

Cas $d = -5$. Dans le rectangle $(0, 1, \omega, \omega + 1)$ le centre $(1 + i\sqrt{5})/2$ est à distance $\approx 1,11$ des sommets. soit une boule B de rayon $\epsilon < 0,01$ autour de lui. Un point de cette boule est atteint comme quotient de deux entiers, car pour $e = N(1 + i\sqrt{5})$ ($N >> 1/\epsilon$), la boule eB est de rayon $>> 1$ donc contient un point du reseau.

Cas $d < -5$ et $\equiv 2, 3\,[4]$: idem.

Cas $d < -11$ et $\equiv 1\,[4]$. Premier exemple : $d = -15$. On considerel le triangle isocele $(0, 1, \omega')$, de hauteur $\sqrt{15}/2 > 1,93$. Soit $p = (\frac{1}{2} + 0,9i)$. Il est à distance > 1 des sommets du triangle. On utilise alors le même argument que ci dessus.

□

1.6 Compléments, algèbres commutatives sur un corps

1.6.1 Elements nilpotents

Soit K un corps, et $\mathcal{A}$ une algèbre **commutative** sur K **de dimension finie.**

Un élément est nilpotent, s'il est non-nul, mais une puissance est nulle.

Exemple 1.6.1. — *K^E avc E un ensemble fini. (espace des applications de E dans K). Il n'y a pas de nilpotent, mais il y a des diviseurs de 0 (si $|E| \geq 2$).*
— *$K[X]/((X-a)^2)$. L'image de $(X-a)$ est de carré nul.*
— *$K_1 \times K_2 \times \cdots \times K_n$ où $K_i \backslash K$ est une extension finie. Ici aussi, pas de nilpotent, mais des diviseurs de 0.*

Les diviseurs de zero sont frequents.

Proposition 1.6.1. *On a la dichotomie : soit $\mathcal{A}$ est un corps (extension de K), soit $\mathcal{A}$ contient des diviseurs de zero.*
Plus precisement, si un élément n'est pas inversible, il est diviseur de zero.

Démonstration. Soit $a \neq 0$ dans $\mathcal{A}$, et $\text{mult}_a : \mathcal{A} \to \mathcal{A}$ la **multiplication par** a. C'est un K-endomorphisme. Si a n'est pas un diviseur de zero, il est injectif, et donc surjectif, car $\mathcal{A}$ est de K-dimension finie. On atteint 1, donc a a un inverse. □

Proposition 1.6.2. *L'intersection des ideaux maximaux de $\mathcal{A}$ est exactement l'ensemble des elements nilpotents de $\mathcal{A}$.*

Démonstration. Soit a nilpotent, et $\mathfrak{m}$ un ideal maximal. Comme $\mathcal{A}/\mathfrak{m}$ est un corps, a y disparait, et donc $a \in \mathfrak{m}$.

Si a est dans tout ideal maximal, la suite (a^k) est une suite décroissante de s-e.v. (de dimension finie), donc stationnaire.

$\exists n, (a^n) = (a^{n+1})$. Donc

$$\exists x \in \mathcal{A},\ a^{n+1}x = a^n$$

On a donc $(1-ax)a^n = 0$. Si $a^n \neq 0$, cela signifie que $ax - 1$ est un diviseur de zero (non nul, sinon a inversible et donc dans aucun ideal maximal). L'ideal qu'il engendre ne contient pas 1.

Prenons un ideal maximal contenant $(1-ax)$ (Zorn n'est pas necessaire, car nous sommes en dimension finie, et que l'emboitement des idéaux fait croitre la dimension). Il contient aussi a car a est dans tous les ideaux maximaux. Donc il contient 1, contradiction.

□

Théorème 1.6.1. *Soit $\mathcal{A}$ une K-algèbre de dimension finie sur K. Si $\mathcal{A}$ n'a pas d'élément nilpotent, elle possède un nombre fini d'idéaux maximaux $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ tels que*

$$\mathcal{A} \simeq \prod_k \mathcal{A}/\mathfrak{m}_k.$$

Démonstration. D'apres la proposition précédente, l'intersection des idéaux maximaux est

$$\bigcap_{\max} \mathfrak{m} = \{0\}.$$

Comme c'est une intersection de sous-espaces de $\mathcal{A}$, de dimension finie, il existe une famille finie d'intersection triviale.

Prenons une telle famille **minimale** $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$.

On va montrer que $\mathcal{A} \xrightarrow{\simeq} \prod_i \mathcal{A}/\mathfrak{m}_i$, ce qui suffira, car à droite, c'est un produit de corps.

Le morphisme est bien défini (sur chaque facteur, notons $\phi_i : \mathcal{A} \to \mathcal{A}/\mathfrak{m}_i$, et notons $\oplus_i \phi_i : \mathcal{A} \to \prod_i \mathcal{A}/\mathfrak{m}_i$ la somme des ϕ_i. De plus il est injectif, car $\bigcap_i \mathfrak{m}_i = \{0\}$.

Il nous faut la surjectivité.

Nous allons montrer que pour chaque i_0, la restriction de ϕ_{i_0} à $\bigcap_{i\neq i_0} \mathfrak{m}_i$ (à valeurs dans $\mathcal{A}/\mathfrak{m}_{i_0}$) est surjective. Cela suffit à ce que $\oplus_i \phi_i$ est surjective sur chaque

$$\{0\} \times \{0\} \times \cdots \times \mathcal{A}/\mathfrak{m}_{i_0} \times \{0\} \times \cdots \times \{0\}$$

(et cela assure que $\oplus_i \phi_i$ est surjective sur $\prod_i \mathcal{A}/\mathfrak{m}_i$).

Prouvons la surjectivité de la restriction. Cette restriction est injective (car $\oplus_i \phi_i$ est injectif). Il suffit bien sur d'établir l'égalité des dimensions :

Lemme 1.6.1.

$$\dim_K(\bigcap_{i\neq i_0} \mathfrak{m}_i) = \dim_K(\mathcal{A}/\mathfrak{m}_{i_0}$$

Comme $\mathfrak{m}_{i_0}$ est en somme directe avec $\bigcap_{i\neq i_0} \mathfrak{m}_i$, il suffit de montrer que ces deux sous espaces engendrent $\mathcal{A}$. Remarquons que la somme de ces deux idéaux est encore un idéal.

($\forall a \in \mathcal{A}$, $\forall x \in \bigcap_{i\neq i_0} \mathfrak{m}_i$, $\forall y \in \mathfrak{m}_{i_0}$, $a(x+y) = ax + ay \in \mathfrak{m}_{i_0} \oplus (\bigcap_{i\neq i_0} \mathfrak{m}_i$)

Nous savons aussi que par minimalité de la famille $(\mathfrak{m}_i)$, le sous espace $\bigcap_{i\neq i_0} \mathfrak{m}_i$ n'est pas réduit à $\{0\}$.

Si $\mathfrak{m}_{i_0}$ et $\bigcap_{i\neq i_0} \mathfrak{m}_i$ n'engendrent pas $\mathcal{A}$, l'idéal $\mathfrak{m}_{i_0}$ n'est pas maximal, car il est contenu dans l'idéal $\mathfrak{m}_{i_0} \oplus (\bigcap_{i\neq i_0} \mathfrak{m}_i)$. Contradiction. Nous avons donc le lemme, et donc le résultat.

□

1.6.2 Nullstellensatz

Soit $\mathcal{A} = K[X_1, \ldots, X_n]$.

Proposition 1.6.3. *Soit K algébriquement clos, non dénombrable.*

- *Les idéaux maximaux de $K[X_1, \ldots, X_n]$ sont les $(X_1 - a_1, \ldots, X_n - a_n)$, où $a_i \in K$.*
- *Soit I un idéal de $\mathcal{A}$, et $V(I) \subset K^n$ l'ensemble des points d'annulation commun des éléments de I. Si $I \neq \mathcal{A}$, alors $V(I) \neq \emptyset$*

Démonstration. Si $I = (X_1 - a_1, \ldots, X_n - a_n)$, c'est $\ker(\mathrm{spe}_{(a_1,\ldots,a_n)}) \subset \mathrm{K}$, qui est un corps, I est donc maximal.

Reciproquement, si $\mathfrak{m}$ est un idéal maximal, $\mathcal{A}/\mathfrak{m}$ est un corps, et possède, comme $\mathcal{A}$, (en tant qu'e.v.) une base dénombrable sur K.

Observation 1.6.1. *$K(X)$ contient $\{\frac{1}{X-\alpha}, \alpha \in K\}$ qui est une famille libre (exercice), indénombrable, par hypothèse.*

Ainsi, $\mathcal{A}/\mathfrak{m}$ est algébrique sur K.

Comme K est algébriquement clos, $\mathcal{A}/\mathfrak{m} \simeq K$. Soit a_i l'image de X_i, on a donc $(X_i - a_i) \in \mathfrak{m}$. Comme on sait que $(X_1 - a_1, \ldots, X_n - a_n)$ est maximal, c'est $\mathfrak{m}$.

Enfin, pour le dernier point, par Zorn, il existe $\mathfrak{m}$ idéal maximal contenant I. Un tel idéal est donc de la forme $(X_1 - a_1, \ldots, X_n - a_n)$, et ainsi $(a_1, \ldots, a_n) \in V(I)$.

□

Soit $V \subset K^n$, on note $I(V) = \{P \in \mathcal{A},$ s'annulant sur $V\}$.

Soit I un idéal, on note $\sqrt{I} = \{a, \exists n, a^n \in I\}$.

Théorème 1.6.2. *Soit K algébriquement clos non dénombrable, et $\mathcal{A} = K[X_1, \ldots, X_n]$. Soit I un idéal de $\mathcal{A}$.*

Alors $I(V(I)) = \sqrt{I}$.

Démonstration. Le cas où $I = \mathcal{A}$ est trivial, excluons le.

On a clairement $\sqrt{I} \subset I(V(I))$.

Pour l'autre inclusion, soit $F \in I(V(I))$. Il s'annule partout où les éléments de I s'annulent. Il n'est pas inversible (sinon, $1 \in I(V(I))$ mais 1 ne s'annule pas sur $V(I) \neq \emptyset$).

Par Noetherianité, il existe $P_1, \ldots, P_r$ tels que $I = (P_1, \ldots, P_r)$.

Dans $\mathcal{A}[T]$, soit

$$J = (1 - TF, P_1, \ldots, P_r).$$

Affirmation : $J = \mathcal{A}[T]$.

Preuve de l'affirmation : il suffit de voir que $V(J) = \emptyset$. Prenons $(a_1, \ldots, a_r, t) \in V(J)$. On a $1 - tF(a_1, \ldots, a_n) = 0$ d'une part, et $(a_1, \ldots, a_n) \in V(I)$ d'autre part (car tous les P_i s'y annulent). Donc $F(a_1, \ldots, a_n) = 0$, contradiction.

Fin de la preuve du théorème.

Il existe donc $U_1, \ldots, U_r, V \in \mathcal{A}[T]$ tels que

$$1 = \sum U_i P_i \ + \ (1 - TF)V.$$

Spécialisons en $T = 1/F$, dans $\mathcal{A}[1/F] \subset \mathcal{A}(F) \subset K(X_1, \ldots, X_n)$ (corps des fractions).

$$1 = \sum U_i(X_1, \ldots X_n, \frac{1}{F} P_i(X_1, \ldots, X_n).$$

On en déduit, en mettant au même dénominateur, une extression de F^m (pour un certain entier m) comme combinaison des P_i à coefficients dans $\mathcal{A}$. Ainsi $F^m \in I$, et donc $F \in \sqrt{I}$.

□

Exemple 1.6.2. *Tracer $y^2 - x^3 + x = 0$, et $y^2 - x^3 + x - 1 = 0$...*

2 Groupes linéaires

2.1 Groupes linéaires GL, SL

2.1.1 Définitions

Soit A un anneau commutatif, et E un A-module.

On note $GL(E) = \mathrm{Aut}_A(E)$, le groupe des inversibles de la A-algèbre $\mathrm{End}_A(E)$.

On note $\mathcal{M}_n(A)$ l'algèbre des matrices carrées de taill $n \times n$ à coefficients dans A. On note $GL_n(A)$ le groupe des matrices inversibles dedans.

Proposition 2.1.1. *Si E est* **libre** *de rang n, le choix d'une base donne un isomorphisme de A-algèbre entre $\mathcal{M}_n(A)$ et $\mathrm{End}_A(E)$, et un isomorphisme de groupes $GL_n(A) \to GL(E)$.*

Standart.

Définition 2.1.1. *Le déterminant* $\det : \mathcal{M}_n(A) \to A$ *est défini par la formule usuelle.*

Observation 2.1.1. *Si E est libre de rang n,* $\det : End_A(E) \to A$ *est bien défini.*

Proposition 2.1.2. *$M \in \mathcal{M}_n(A)$ est inversible si et seulement si son determinent est inversible dans A.*

$\det : GL_n(A) \to A^*$ *est un morphisme de groupes, surjectif.*

(on utilise ${}^tCom(M)M = det(M)I_n$).

On définit $SL_n(A) = \det^{-1}(1_A)$.

2.1.2 Produit semi-direct

si G est un groupe et H un sous groupe distingué, on a une suite exacte

$$\{1\} \to H \to G \xrightarrow{\pi} G/H \to \{1\}.$$

Il arrive (mais pas toujours !) qu'il existe un morphisme $\sigma : G/H \to G$ tel que $\pi \circ \sigma = Id_{G/H}$. Quand c'est le cas on dit que σ est une section de π.

Exemples :

— $n\mathbb{Z}$ dans $\mathbb{Z}$...

— $SL_n(A)$ dans $GL_n(A)$

Notons $G/H = Q$. Lorqu'une section existe elle donne lieu à un morphisme $\tilde{\sigma} : Q \to \mathrm{Aut}(H)$ comme suit (convenons d'ecrire l'action par conjuguaison comme une action à gauche) :

$$\tilde{\sigma}(q)[h] = \sigma(q) h \sigma(q)^{-1}.$$

Proposition 2.1.3. *Si $\phi : Q \to \mathrm{Aut}(H)$ est donné, on peut définir une loi de groupe sur* **l'ensemble** $H \times Q$ *par*

$$(h_1, q_1)(h_2, q_2) = (h_1 \phi(q_1)[h_2], q_1 q_2).$$

On appelle le groupe obtenu G le **produit semi-direct de N par Q de morphisme structural** ϕ. On note $G = H \rtimes_\phi Q$.

Il faut verifier l'associativité, et l'existence d'un inverse.

On verifie que $(\phi(q^{-1}[h^{-1}], q^{-1})$ est l'inverse de (h, q).

Pour l'associativité, il suffit de l'écrire.

Proposition 2.1.4. *Soit G un groupe, H unsous groupe distingué, et $Q = G/H$. Soit $\phi : Q \to Aut(H)$.*

Alors $G \simeq H \rtimes_\phi Q$ si et seulement si $\pi : G \to G/H$ admet un section σ telle que $\tilde{\sigma} = \phi$.

Démonstration. C'est un calcul. C'est à cette occasion que l'on se rend compte si la définition de la loi convient à notre convention de faire agir les conjugaisons par la gauche. □

Application :

$$GL_n(A) \simeq SL_n(A) \rtimes A^*$$

Autre exemple classique, plus géométrique :

$$Aff(\mathbb{R}^2) \simeq \mathbb{R}^2 \rtimes GL_2(\mathbb{R})$$

ou encore

$$\mathrm{Isom}^+_{\mathrm{Aff}}(\mathbb{E}^2) \simeq \mathbb{R}^2 \rtimes SO_2$$

(les isométries affines directes du plan sont les compositions de translations et de rotations, mais bien sur lorsqu'on compose T_1, R_1, T_2, R_2, et qu'on veut exprimer cela en $T_3 R_3$, l'une des translations est "tordue" par la rotation qui precede... c'est precisement la loi du produit semi-direct).

2.1.3 Générateurs

On suppose ici que A est un anneau euclidien.

Une (matrice de) transvection est une matrice avec des 1 sur la diagonale, tous les autres coefficients nuls, sauf un.

Théorème 2.1.1. *Si A est euclidien, le groupe $SL_n(A)$ est engendré par les transvections.*

En fait on va montrer la proposition suivante :

Proposition 2.1.5. *Si A euclidien, et $M \in \mathcal{M}_{n,m}(A)$ (avec $n \geq m$), alors il existe P et Q dans $SL_n(A)$ et $SL_m(A)$ produits de transvections telles que PMQ est une matrice nulle partout hors de la "diagonale" et dont les coefficients consecutifs sur celle ci sont croissants pour la divisibilité.*

Il s'agit d'un massif pivot de Gauss.

On déduit le théorème de la proposition, car si M est dans SL, le determinant dit que touls les coefficients diagonaux doivent etre inversibles. On arrive facilement à les rendre tous égaux à 1 en manipulant les lignes et les colonnes.

Attention à l'arnaque : ou utilise-t-on que M est dans SL et pas dans GL ?!

La proposition est presque vraie pour un anneau principal : on abandonne juste que P et Q sont produits de transvections. Le théorème est en effet faux pour certains anneaux principaux non euclidiens (comme par exemple $\mathbb{Z}[i\sqrt{19}$, d'apres un théorème de P.M. Cohn).

2.1.4 Applications

La proposition de la partie préc{edente peut servir à plusieurs choses classiques.

La **résolutions des systèmes d'équations Diophantiennes linéaires**. En effet, une telle équations s'écrit

$$MX = B$$

avec M une matrice a coefficients dans $\mathbb{Z}$, X une colonne inconnue, et B une colonne dans $\mathbb{Z}^m$, et on en cherche les solutions entieres (dans $\mathbb{Z}$).

Une colonne X_0 est un vecteur solution si et seulement si $Q^{-1}X_0$ est solution de $PMQX = PB$ pour P et Q dans SL. (Ici le pont clé est que $SL_n(\mathbb{Z})$ preserve $\mathbb{Z}^n$). En choisissant P et Q comme dans la proposition, on voit que le nouveau système, diagonal, est une simple condition de divisibilité.

La **décomposition de tout A-module de type fini en facteurs invariants**. En ecrivant qu'un tel A-module E est le quotient de A^n par un ideal N necessairement de type fini (car A^n est Noetherien), on ecrit

$$E \simeq A^n/MA^m$$

où M est la matrice representant le quotient $A^m \to N$.

On ecrit $M = PDQ$, et

$$A \simeq A^n/(PDQA^m) \simeq P^{-1}A^n/(DQA^m) \simeq A^n/DA^m$$

apres les changements de base de A^n et A^m adéquats.

Il vient que $E \simeq A^r \oplus A/(d_1A) \oplus \cdots \oplus A/(d_kA)$ avec $d_i|d_{i+1}$.

Les **invariants de similitudes** d'un endomorphisme d'un espace vectoriel. Si E est un K-ev de dimention finie, et u un endomorphisme de E, voyons E comme $K[X]$-module grace à u ainsi :

$$P \times \vec{v} := [P(u)](\vec{v}).$$

Ecrivons les facteurs invariants de ce module :

$$E \simeq K[X]/(P_1) \oplus \cdots \oplus K[X]/(P_k)$$

(il n'y a pas de facteur libre, car E est supposé de dimension finie).

Prenons $x_1, \ldots, x_k$ une base de module adaptée à cette décompositon, et completons là en $\{x_1, u(x_1), \ldots, u^{d_1-1}(x_1), x_2, u(x_2)\ldots\}$ qui est une base de l'ev E. La matrice de u dans cette base est une diagonale de matrices compagnons. Cette ecriture caracterise la classe de conjugaison de u sous l'action de $GL(E)$.

2.1.5 Simplicité

Dans cette partie, $A = K$ est un corps, et E est un K-espace vectoriel de dimension finie $= n$.

Une transvection de E est un automorphisme dont la matrice dans une base bien choisie est une matrice de transvection (non triviale).

Commentons cela tout de suite : toute transvection τ possède un hyperplan remarquable sur lequel c'est l'identité ($\ker(\tau - Id)$ est bien un hyperplan, car $\tau - Id$ est évidemment de rang 1). Elle possède aussi une direction remarquable, dans cet hyperplan : $\Im(\tau - Id)$ (c'est bien de dimension 1, dans l'hyperplan, car sinon c'est une direction propre de valeur propre differente de 1).

Une transvection est donc l'identité sur un hyperplan, et produit un décalage dans une direction choisie de cet hyperplan...

Lemme 2.1.1. *Si τ est une transvection de E, il existe $f \in E^*$, et $v \in \ker(f) \setminus \{0\}$ tels que $\tau(x) = x + f(x)v$ pour tout x.*

Si $n \geq 3$, toutes les transvections sont conjuguées entre elles dans $SL(E)$.

Démonstration. Le premier point est clair dans une base. Pour le second point, soient τ_1, τ_2 deux transvections, et f_1, f_2, v_1, v_2 les données associées. On peut trouver $\alpha \in GL(E)$ envoyant v_1 sur v_2 et $\ker f_1$ sur $\ker f_2$ (en completant v_1 et v_2 en des bases de ces deux hyperplans).

f_1 et $f_2 \circ \alpha$ sont alors colinéaires dans E^*.

Sur un supplementaire de $\ker f_1$ on peut choisir α presque arbitraire (à valeur hors de $\ker f_2$), et en particulier, telle que $f_1 = f_2 \circ \alpha$.

On a $\tau_2 \circ \alpha(x) = \alpha(x) + f_2 \circ \alpha(x)v_2 = \alpha(x) + f_1(x)v_2$. Comme α^{-1} envoie v_2 sur v_1, on a $\alpha^{-1} \circ \tau_2 \circ \alpha = \tau_1$.

Les transvections sont conjuguées dans $GL(E)$.

Prenons $\alpha_0 \in GL(E)$ comme ci dessus.

Pour trouver α comme ci-dessus, mais dans $SL(E)$, il suffit de composer α_0 avec β verifiant $\beta(v_2) = v_2$, β vaut l'identité sur un supplementaire de $\ker(f_2)$, et dans $\ker(f_2)$, sur un supplementaire de $Vect(v_2)$, choisir un automorphisme de deteminant $1/det(\alpha_0)$. C'est possible dès que $\dim(\ker f_2) \geq 2$.

□

Définition 2.1.2. *On défini le groupe $PSL(E)$ comme le quotient de $SL(E)$ par son centre :*

$$PSL(E) = SL(E)/Z(SL(E)).$$

De meme $PSL_n(K) = SL_n(K)/\{\pm I_n\}$ étant entendu que $-I_n$ n'est pas toujours dans $SL_n(K)$.

Théorème 2.1.2. *Si* $\dim(E) \geq 3$*, et si* K *est un corps arbitraire, alors* $PSL(E)$ *est un groupe simple : il n'admet aucun quotient non-trivial.*

Si $|K| \geq 7$*, alors* $PSL_2(K)$ *est aussi simple.*

Démonstration. Soit $\bar{N}$ un sous-groupe distingué de $PSL(E)$, non trivial, et N sa pré-image dans $SL(E)$.

Nous voulons montrer que N vaut tout $SL(E)$. Pour cela, il suffit de montrer que N contient une transvection : comme N est distingué, il les contiendra toutes (c'est le lemme précédent), et les transvections engendrent $SL(E)$.

Soit $\bar{\sigma} \in \bar{N}$ non trivial, et $\sigma \in N$ une préimage. C'est un élément non central. Il existe donc un vecteur v tel que $\sigma(v)(= w)$ n'est pas colinéaire à v.

Comme la dimension est ≥ 3, on peut prendre un hyperplan H contenant v et w, et une transvection τ d'hyperplan H et de vecteur v.

Soit $\rho = [\tau, \sigma] = \tau\sigma\tau^{-1}\sigma^{-1}$.

Comme produit de conjugués de σ, $\rho \in N$.

Comme produit de transvections de vecteurs non-colinéaires, $\rho \neq 1$. (Evaluer en $\sigma(z) \notin H$...)

De plus $\rho(H) \subset H$ (simple verification de l'evaluation en $h \in H$) donc $= H$ par effet des dimensions.

De plus on vérifie que $\rho(w) = w$.

Soit u une transvection d'hyperplan H et $\phi_u = [\rho, u]$. A nouveau, $\phi_u \in N$ (produit de 2 conjugués d'un élément de N). Mais aussi, ϕ_u est un produit de deux transvections de même hyperplan : c'est donc soit l'identité soit une transvection.

Dans le second cas, on a fini.

Il reste le cas où, pour toute transvection u d'hyperplan H, ϕ_u est l'identité.

Cela signifie que ρ preserve toutes les directions de H. Ainsi, ρ est scalaire sur H. Comme $\rho(w) = w$, c'est l'identité sur H.

De ce fait, en choisissant une base de E une base de H, complétée par un vecteur hors de H, la matrice de ρ vaut $\begin{pmatrix} \lambda & 0 & \dots & 0 \\ * & A & 0 & 0 \\ \vdots & 0 & \ddots & \vdots \\ * & 0 & \dots & 1 \end{pmatrix}$.

Comme elle est dans $SL_n(K)$, λ vaut 1.

Il ne nous reste plus qu'à changer un vecteur de notre base de H pour le remplacer par la colonne des étoiles, et la matrice de ρ y est une matrice de transvection.

□

2.1.6 Cas exceptionnels

Le cas $n = 2$, et $|K| \geq 7$ se traite par "force brute." Les cas $|K| \leq 5$ s'étudient en représentant $PSL_2(K)$ comme permutation dans les plans projectifs.

2.1.7 Congruences

Observation 2.1.2. *Si* $A = \mathbb{Z}$*,* $PSL_n(\mathbb{Z})$ *n'est pas simple. Les congruences dans* $PSL_n(\mathbb{Z}/p\mathbb{Z})$ *sont des exemples de quotients. Ces quotients sont en fait surjectifs.*

2.2 Exponentielle et applications

2.2.1 Algègres de Banach, et applications

Le degré de généralité de cette partie est élevée, mais ensuite on sera sur un cas bien plus précis.

Soit K un corps muni d'une valeur absolue archimédienne, et complet.

Définition 2.2.1. *Une* **algèbre de Banach** *sur K est une K-algèbre munie d'une norme d'algèbre (verifiant $\|xy\| \leq \|x\|\|y\|$ pour tout x, y) qui est complete pour la métrique induite.*

Observation 2.2.1. *En dimension finie la complétude est automatique (et consequence de celle de K).*

Exemple 2.2.1. *$\mathcal{M}_n(K)$, pour la norme d'operateur.*

Définition 2.2.2. *Si (a_n) est une suite déléments d'une algèbre de Banach $\mathcal{A}$, on dit que la série $\sum a_n$ converge absoluement si $\sum \|a_n\|$ converge. (Dans ce cas, la suite des sommes partielles converge pour la topologie de la norme).*

Ci dessous, $B_{1,1} = \{a \in \mathcal{A}, \|a - 1\| < 1\}$.

Définition 2.2.3. *Pour tout $a \in \mathcal{A}$, on pose* $\exp(a) = \sum_{\mathbb{N}} \frac{1}{n!} a^n$.
Pour tout $a \in B_{1,1}$, on pose $\log(a) = \sum_{\mathbb{N}^*} \frac{(-1)^{n+1}}{n}(a-1)^n$ *ou encore :*
Pour tout $a \in \mathcal{A}$ tel que $\|a\| < 1$, on pose $\log(a+1) = \sum_{\mathbb{N}^*} \frac{(-1)^{n+1}}{n}(a)^n$.

Proposition 2.2.1.
- $\exp(a) = 1 + a + \mathcal{O}(\|a\|^2)$.
- *Si $xy = yx$, alors* $\exp(x+y) = \exp(x)\exp(y)$.
- $\forall a \in B_{1,1}$, $\exp(\log(a)) = a$
- $\forall x, y \in B_{1,1}$, *si $xy = yx$, alors* $\log(ab) = \log(a) + \log(b)$.
- $\exp\begin{pmatrix} 0 & -2\pi \\ 2\pi & 0 \end{pmatrix} = \exp\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = I_2$
- exp *est localement injective, mais pas injective en général.*
- *Dans $\mathcal{M}_n(K)$,* $\det(\exp(M)) = \exp(\mathrm{tr}M)$.

Immediat, ou exercice...

2.2.2 Crochet de Lie et sous-groupes de $\mathcal{A}^*$

L'exponentielle est un outil important pour l'etude des sous-groupes du groupe des inversibles $\mathcal{A}^*$ d'une algèbre de Banach, par un angle topologique et différentiel.

L'exemple principal (notre seul exemple ?) est quand $\mathcal{A} = \mathcal{M}_n(K)$. Alors $\mathcal{A}^* = GL_n(K)$, qui possède de nombreux sous groupes interessants.

Lemme 2.2.1.
- $\forall x, y \in \mathcal{A}$, *on a* $\lim_{n\to\infty} \left(\exp(\frac{1}{n}x)\exp(\frac{1}{n}y)\right)^n = \exp(x+y)$.
- $\forall x, y \in \mathcal{A}$, *on a*

$$\lim_{n\to\infty} \left(\exp(\frac{1}{n}x)\exp(\frac{1}{n}y)\exp(\frac{-1}{n}x)\exp(\frac{-1}{n}y)\right)^{n^2} = \exp(xy - yx).$$

Autrement dit, infinitésimalement, le commutateur d'exponentiels (au ses du groupe) est l'exponentielle du commutateur (au sens de l'algèbre).

— *On définit* $[x,y]_{Lie} = xy - yx$ *(le "crochet de Lie"), et souvent on le notera simplement* $[x,y]$. *On a* $\forall x,y,z \in \mathcal{A}$, *l'identité suivante (l'identité de Jacobi)*

$$[x,[y,z]] + [y,[z,x]] + [z,[x,y]] = 0$$

et aussi $[x,x] = 0$.

Le premier point est donné par le produit des DL à l'ordre 1. Le second point l'est par celui des DL à l'ordre 2. Le troisième point se verifie en développant tout.

Observation 2.2.2. *Il y a un risque de confusion entre le "crochet de Lie", et le "crochet des commutateurs" dans un groupe. Il est d'autant plus fort que le second point dit que ces deux crochets sont intimement reliés l'un à l'autre.*

Observation 2.2.3. *Le troisième point sert d'axiome à la structure "d'algèbre de Lie" qui est une définition de structure d'algèbre non associative (donc hors de nos convention) dont la loi multiplicative est un crochet verifiant ce troisieme point, en plus d'être bilinéaire par rapport à la structure vectorielle sous-jacente.*

Proposition 2.2.2. *Si* G *est un sous-groupe fermé de* $\mathcal{A}^*$, *notons* $\mathfrak{G} = \{x \in \mathcal{A}, \forall t \in \mathbb{K}, \exp(tx) \in G\}$. *Alors* $\mathfrak{G}$ *est un sous-espace vectoriel de* $\mathcal{A}$ *stable par crochet de Lie.*

C'est une conséquence directe du lemme.

Exemple 2.2.2.

Si G *est discret,* $\mathfrak{G}$ *est l'espace nul.*

S'il existe un morphisme surjectif continue de $\varphi : \mathbb{R} \to G$, *on dit que* G *"est à un paramètre" (sans être necessairement fermé). Alors il existe un unique* $M \in \mathcal{A}$ *tel que* $\varphi(t) = \exp(tM)$ *pour tout* t. *En, particulier* $M = \varphi'(0)$ *caracterise le sous groupe.*

L'exponentielle réalise un homeomorphisme entre l'espace des matrices triangulaires superieures avec des 0 *sur la diagonale et le groupe des matrices triangulaires superieures avec* 1 *sur la diagonale.*

Théorème 2.2.1. *Si* G *est un sous-groupe fermé de* $\mathcal{A}^*$ *il existe un voisinage* W *de* 1 *dans* G *et un voisinage* V *de* 0 *dans* $\mathcal{A}$ *tels que* exp *réalise un homéomorphisme de* V *sur* W.

Démonstration. (de chaque affirmation de l' exemple)

Le premier point est clair.

Le second point est facile si l'on suppose φ dérivable : dans ce cas

$$\varphi'(t) = \lim \frac{1}{h}(\varphi(t+h) - \varphi(t)) = \lim \frac{1}{h}(\varphi(t)(\varphi(h) - 1)) = \varphi(t)\varphi'(0)$$

(on reconnait une sorte d'equation différentielle). Posons $F(t) = \varphi(t)\exp(-t\varphi'(0))$. Bien sûr $F(0) = 1$. On doit montrer que $F \equiv F(0)$. Mais il suffit de dériver.

Maintenant, pour verifier que φ est toujours dérivable, on utilise une astuce de lissage. Soit $\theta : \mathbb{R} \to \mathbb{R}_+$ une fonction $\mathcal{C}^\infty$ à support compact, telle que $\int \theta = 1$. On devra choisir θ de "petit" support. Soit $\psi : \mathbb{R} \to \mathcal{A}$ donné par $\psi(t) = \int_{\mathbb{R}} \theta(s-t)\varphi(s)ds$. C'est la convolée de φ et θ, donc ψ est $\mathcal{C}^\infty$.

On a

$$\theta(t) = \int_{\mathbb{R}} \theta(u)\varphi(t-u)du$$

par commutativité de la convolution. C'est à dire

$$\psi(t) = \varphi(t) \int_{\mathbb{R}} \theta(u)\varphi(-u)du$$

Posons $V = \int_{\mathbb{R}} \theta(u)\varphi(-u)du$. Alors $\|V-1\| \leq \theta(u)(\varphi(u)^{-1}-1)du$ car $\int \theta = 1$. Mais si on a choisi le support de θ assez petit autour de 0 pour que $\varphi(u)^{-1}-1$ y soit tres faible en norme, on a $\|V-1\| < 1$. Cela assure que V soit inversible (d'inverse $\exp(-\log(V))$ ou encore $\sum(-1)^k(V-1)^k$).

Finalement, on a $\varphi(t) = \psi(t)V^{-1}$ pour tout t, et donc φ est $\mathcal{C}^\infty$.

Pour le troisième point est un théorème plus profond. En réalité, tout sous groupe fermé est une sous-variét{e différentielle, mais comme je n'ai pas envie de parler de différentiabilité, je m'en tiens à l'homéomorphie.

Lemme 2.2.1. *Si $h_n \to 1$ dans G, et $h_n \neq 1$, et si $\frac{1}{\|\log h_n\|}\log h_n \to h$, alors h in$\mathfrak{G}$*

Démonstration. Soit t arbitraire. On doit montrer que $\exp(th) = \lim \exp(\frac{t\log h_n}{\|\log h_n\|})$ est dans G.

Ecrivons $\frac{t}{\|\log h_n\|)} = E_n + F_n$ avec E_n sa partie entiere.

On a $\exp(th) = \lim h_n^{E_n} \times \exp(F_n \log h_n)$ et le second facteur tend vers 1, car F_n est borné. En revanche, $h_n^{E_n} \in G$. Comme G est fermé, la limite, est aussi dans G, et on a le lemme. □

Prenons $\mathfrak{G}'$ un supplementaire de $\mathfrak{G}$ dans $\mathcal{A}$.

Lemme 2.2.2. *$\exists V'$ voisinage de 0 dans $\mathfrak{G}'$ tel que $\exp(V' \setminus \{0\}) \cap G = \emptyset$.*

Démonstration. Sinon, $\exists x'_n \in \mathfrak{G}'$, suite tendant vers 0, telle que $\forall n$, $\exp(x'_n) \in G$. Et donc, $\exp(x'_n) \to 1$.

On pose $h_n = \exp(x'_n)$, et on lui applique le lemme precedent (pour une sous suite convergente dans la sphère unité, compacte par finitude de la dimension).

La limite de $\frac{x'_n}{\|x'_n\|}$ est donc dans $\mathfrak{G}$, mais aussi dans $\mathfrak{G}'$, car ce dernier est fermé.

Cela contredit que la somme $\mathfrak{G} \oplus \mathfrak{G}'$ est directe.

□

Finissons en remarquant que, par théorème d'inversion locale, l'application

$$\Phi : \mathfrak{G} \times \mathfrak{G}' \to \mathcal{A}^*$$

définie par

$$(x, x') \mapsto (\exp x)(\exp x')$$

réalise un diffeo local au voisinage de $(0,0)$ (sa differentielle est donné par le DL d'ordre 1 : $\Phi(x,y) = 1 + x + y + xo(\|y\|) + yo(\|x\|)$.

Restreignons Φ à $U \times U'$ sur W, sur lesquels c'est un diffeo, et $U' \subset V'$.

Alors $\Phi(x,x') \in G$ si et seulement si $x' = 0$ (car $\exp(x) \in G$ et G est un groupe). Donc $\exp(U) = W \cap G$, et exp y réalise un homéomorphisme, comme restriction d'un difféomorphisme.

□

2.2.3 Sous groupes compacts

Si G est un groupe topologique localement compact, une mesure de Haar est une mesure invariante à gauche, Borelienne, finie sur les compacts, et non nulle.

Théorème 2.2.2. *Tout sous groupe compact de $GL_n(K)$ admet une mesure de Haar.*

....
....

Proposition 2.2.3. *Si G est un groupe topologique et K est un sous-groupe compact, et si G agit de manière affine et transitive sur un convexe Ω de $\mathbb{R}^n$, dont le stabilisateur d'un point est K, alors tout sous-groupe compact de G a un conjugué dans K.*

Démonstration. Soit K' un sous groupe compact, et μ' une mesure de Haar dessus. Prenons $x_0 \in \Omega$ (fixé par K par exemple) et $z = \int_{K'} k'x_0 d\mu'(k')$.

Observons que z est limite de points dans l'enveloppe convexe de $K'x_0$, donc dans Ω car il est convexe. Comme de plus $K'x_0$ est compact (car K' est compact), son enveiloppe convexe aussi. Ainsi, z est dedans, et donc $z \in \Omega$.

Comme l'action sur Ω est affine, $K'z = z$, et comme l'action est transitive, $\exists g, gx_0 = z$, et on a $\mathrm{Stab}(z) = gKg^{-1}$. ainsi $K' \subset gKg^{-1}$. □

Corollaire 2.2.1. *Tout sous-groupe compact de $GL_n(K)$ ($K = \mathbb{R}$ ou $\mathbb{C}$) a un conjugué dans $\mathcal{O}_n$ ou U_n.*

En effet d'apres la décomposition pôlaire, $GL_n(\mathbb{R}) = \mathcal{S}^{++}\mathcal{O}_n$.

Théorème 2.2.3. *Tout sous groupe compact de $GL_n(\mathbb{R})$ est un groupe algébrique réel : c'est le lieu d'annulation d'une famille de polynômes à n^2 indeterminées dans $\mathbb{R}^{n^2} \simeq \mathcal{M}_n(\mathbb{R})$.*

Exemple 2.2.3. *Le groupe $\mathcal{O}(n)$ est clairement algébrique réel : les n^2 équations sont données en écrivant ${}^tMM = I_n$.*

Démonstration. Soit I l'idéal des polynômes nuls sur K, un sous groupe compact de $GL_n(\mathbb{R})$. Il est de type fini par Noetherianité.

Si $y \notin K$, il nous suffit de trouver $S \in I$ tel que $S(y) \neq 0$.

On a $yK \cap K = \emptyset$, et il s'agit de deux compacts. Il existe donc $f \in \mathcal{C}_c(GL_n(\mathbb{R}), \mathbb{R})$ nulle sur K et égale à 1 sur yK. (Tietze Urisohn).

Par Stone-Weierstrass, $\forall \epsilon > 0, \exists P$ polynôme, tel que

$$\forall x \in K, |P(x)| < \epsilon, \qquad \forall x' \in yK, |P(x') - 1| < \epsilon$$

Soit $Q(x) = \int_K P(gx) d\mu(g)$ pour μ une mesure de Haar sur K, que l'on choisi de masse 1 (possible car K est compact).

On a $Q|_K \equiv Q(1)$ et $Q|_{yK} \equiv Q(y)$. Par ailleurs, $|Q(1)| < \epsilon$ et $|Q(y) - 1| < \epsilon$.

Prenons $S = Q - Q(1)$, de sorte que S s'annule sur K, et pas sur y.

L'observation finale est que $Q(x)$ (donc $S(x)$) est bien un polynôme en les coefficients de x. En effet, gx est une matrice dont les coefficients sond des polynômes en les coefficients de x (mais les coefficients de ces polynômes dépendent de g). En integrant sur $d\mu(g)$ on integre en fait les coefficients de ces polynomes (à ligne et colonne fixée) et le résultat est un polynôme en les coefficients de x.

□

2.3 Quaternions

2.3.1 Rappels sur O_n

$$\mathcal{O}_n = \{M \in \mathcal{M}_n(\mathbb{R}),\ {}^tMM = I_2\} = \mathrm{Stab}_\phi I_n$$

où ϕ est l'action à droite de $GL_n(\mathbb{R})$ sur $\mathcal{M}_n(\mathbb{R})$ par $(P, M) \mapsto {}^tPMP$.

Rappelons que

$$\mathcal{O}_n = \{M \in \mathcal{M}_n(\mathbb{R}), \forall X \in \mathcal{M}_{n,1}(\mathbb{R}), \|MX\| = \|X\|\}$$

$$= \{M \in \mathcal{M}_n(\mathbb{R}), \forall X, Y \in \mathcal{M}_{n,1}(\mathbb{R}),\ {}^tXY = {}^t(MX)(MY)\}$$

Rappelons que det : $\mathcal{O}_n \to \{-1, 1\}$ est un morphisme de groupe surjectif, que son noyau est SO_n, et que ce morphisme admet une section, et que donc $\mathcal{O}_n$ est un produit semi-direct de SO_n par $\mathbb{Z}/2\mathbb{Z}$.

Par théorème spectral (sur les endomorphismes normaux (commutant avec leur adjoint),

$$\forall M \in SO_n, \exists P \in \mathcal{O}_n,\ P^{-1}MP = D_B$$

où D_B est une diagonale par bloc de rotation (2×2) ou d'identité.

En particulier (mais c'est visible à l'oeil nu), $SO_2 \simeq \mathbb{U} \simeq S^1$.

Dans le cas complexe, on a la même discussion, pour SU_n, dont tous les eléments sont diagonalisables, à valeurs propres de module 1. Aussi $SU_1 \simeq S^1$.

Peut-on aussi bien paramétrer SO_n, pour $n \geq 3$?

2.3.2 Le "corps" des quaternions

Définition 2.3.1. *On défini* **l'algèbre des quaternions de Hamilton** *comme* $\mathbb{H} = (\mathbb{R}^4, +, ., *)$ *dont on choisi une base* (e, i, j, k) *pour laquelle on définit la loi* $*$ *comme extension bilinéaire des formules suivantes :*

$$e = 1$$

$$i^2 = j^2 = k^2 = -1$$

$$ij = k\ jk = i\ ki = j$$

$$ji = -k\ kj = -i\ ik = -j.$$

Autrement dit, $\mathbb{H}$ est l'algèbre obtenue en quotientant l'algèbrre des polynômes à 4 indéterminées non-commutatives, par l'idéal bilatère engendré par ces relations.

Observation 2.3.1. 1 *est dans le centre de* $\mathbb{H}$. *Le centre de* $\mathbb{H}$ *est précisément l'espace engendré par* 1 *(ou* e*).*

$$\forall a, b, c, d,\ (a + bi + cj + dk)(a - bi - cj - dk) = a^2 + b^2 + c^2 + d^2.$$

Tout élément non nul de $\mathbb{H}$ *possède un inverse dans* $\mathbb{H}$.

$H_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ *est un sous groupe fini de* $\mathbb{H}^*$, *d'ordre* 8, *non abélien (en particulier, non cyclique).*

$i^2 = j^2 = k^2 = ijk = -1$ *définit completement la multiplication.*

Observation 2.3.2. *On pourrait remplacer* $\mathbb{R}$ *par un anneau commutatif, et conserver des propriétés interessantes (mais pas forcément l'existence d'inverses).*

Définissons $V = \text{vect}\{i, j, k\}$ le sous-espace « imaginaire pur de $\mathbb{H}$. Chaque élément s'ecrit donc avec une partie réelle et une partie imaginaire.

Si $q = \Re(q) + \Im(q)$, notons $q^* = \Re(q) - \Im(q)$.

On a déjà vu que $qq^* = q^*q \in \mathbb{R}$ et est positif, non-nul dès que $q \neq 0$.

Définition 2.3.2. *On défini* $\langle x, y\rangle = \Re(xy^*) = \frac{1}{2}(xy^* + yx^*)$.

Proposition 2.3.1. *C'est un produit scalaire. La norme au carré de x vaut $xx^* = x^*x$.*

On a immédiatement la bilinéarité, et la symétrie. La forme quadratique associée est définie positive par la remarque précédente.

2.3.3 Réalisation matricielle

Dans $\mathcal{M}_2(\mathbb{C})$ disons que $\tilde{P}$ est la comatrice de P.

Specifiquement : si $P = \begin{pmatrix} z_1 & z_2 \\ w_1 & w_2 \end{pmatrix}$, alors $\tilde{P} = \begin{pmatrix} w_2 & -w_1 \\ -z_2 & z_1 \end{pmatrix}$.

Définissons $\mathcal{H} = \{P \in \mathcal{M}_2(\mathbb{C}),\ \tilde{P} = \bar{P}\} = \{\begin{pmatrix} z_1 & z_2 \\ -\bar{z_2} & \bar{z_1} \end{pmatrix}, z_1, z_2 \in \mathbb{C}\}$.

$\mathcal{H}$ est naturellement muni d'une structure de $\mathbb{R}$- algèbre, car il est stable par multiplication (des matrices).

Proposition 2.3.2. *Une $\mathbb{R}$-base de $\mathcal{H}$ est donnée par*

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$$

Facile en considérant la dimension.

Proposition 2.3.3. *Il existe un isomorphisme d'algèbre $\mathbb{H} \to \mathcal{H}$ envoyant (e, i, j, k) sur la base précédente.*

L'involution $*$ a pour image la trans-conjugaison : $P \mapsto .^t\bar{P}$.

On verifie sans peine que les relations sont préservées, cela garantie que le morphisme d'espace vectoriel induit un morphisme d'algèbre.

En considérant les dimensions, c'est un isomorphisme.

Proposition 2.3.4. *$PP^* = \det(P)I_2$. En particulier, pour tout P, Q, la norme de PQ est le produit des normes de P et de Q.*

2.3.4 Applications

Proposition 2.3.5. *Soit A un anneau commutatif, et $a, b, c, d, \alpha, \beta, \gamma, \delta$ des éléments de A. Alors il existe $x, y, z, t \in A$ tels que*

$$(a^2 + b^2 + c^2 + d^2)(\alpha^2 + \beta^2 + \gamma^2 + \delta^2) = x^2 + y^2 + z^2 + t^2$$

Démonstration. On construit les quaternions sur A. Les sommes de carrés sont les qq^* pour q bien choisis... Prenons $q_1 = a+bi+cj+dk$ et $q_2 = \alpha+\beta i+\gamma j+\delta k$. Alors $(q_1q_2)(q_1q_2)^* = q_1q_2q_2^*q_1^*$. Comme $q_2q_2^*$ est dans A il est central, donc $(q_1q_2)(q_1q_2)^* = q_1q_1^*q_2q_2^*$. C'est ce qu'on voulait... □

Théorème 2.3.1. *La sphère unité d'un espace euclidien de dimension 4 porte une structure de groupe topologique, isomorphe à SU_2.*

Il s'agit de remarquer que dans le modèle matriciel, la sphère unité de $\mathcal{H}$ est précisément $SU_2 = \{M, M.^t\bar{M} = I_2, \det M = 1\}$.

2.3.5 Géométrie Euclidiènne de dimension 4

Soit $q \in \mathbb{H}$, de norme 1. Notons H_q le supplémentaire orthogonal de q dans $\mathbb{H}$. Notons s_q la symétrie orthogonale par rapport à H_q. On a $s_q(x) = x - 2\langle x, q\rangle q$, pour tout x.

Proposition 2.3.6. $\forall x, y \in \mathbb{H}\ yx^*y = -\langle y, y\rangle x + 2\langle x, y\rangle y$.
En particulier $s_q(x) = -qx^*q$.

Il suffit d'écrire $2\langle x, y\rangle y = (xy^* + yx^*)y$, et d'utiliser la formule précédente pour s_q.

Théorème 2.3.2. *Si p, q sont de norme 1, et $\rho_{p,q} : \mathbb{H} \to \mathbb{H}$ est défini par $\rho_{p,q}(x) = pxq^*$, alors $\rho_{p,q}$ est une isométrie.*
L'application $\rho : S^3 \times S^3 \to \mathcal{O}(\mathbb{H})$ est un morphisme de groupes continu, à valeur dans $SO(\mathbb{H})$ et surjectif sur lui. Son noyau est $\{(1,1),(-1,-1)\}$.

En résumé, on a une suite exacte de groupes

$$1 \to \mathbb{Z}/2\mathbb{Z} \to S^3 \times S^3 \to SO_4 \to 1$$

Démonstration. $\rho_{p,q}$ préserve la norme des élements de $\mathbb{H}$, c'est donc une isométrie. On vérifie immédiatement que ρ est un morphisme, continu. Comme $S^3 \times S^3$ est connexe, ρ est à valeur dans la composante connexe de l'unité de $O(\mathbb{H})$, et c'est $SO(\mathbb{H})$.
Si (p, q) est dans le noyau, alors pour tout x, $px = xq$ (en effet comme q est de norme 1, $q^{-1} = q^*$). En particulier pour $x = 1$, il vient $p = q$. De plus, p est alors central, donc dans $\mathbb{R}$. Comme il est de norme 1, c'est ± 1.
Pour la surjectivité, exprimons un élément arbitraire $R \in SO(\mathbb{H})$ comme un produit d'un nombre pair de symétries orthogonales hyperplanes. En utilisant la formule de la proposition pour chacune de ces symétries hyperplanes, on obtient (par exemple par recurrence sur leur nombre) la forme désirée.

□

2.3.6 Géométrie Euclidiènne de dimension 3

Rappel : $V = \mathrm{Vect}(i, j, k)$.

Théorème 2.3.3. *Si $q \in \mathbb{H}$ a norme 1, alors pour tout $u \in V$, posons $r_q(u) = quq^*$ et $\sigma_q(u) = qu^*q^* = -quq^*$.*
Alors r_q est une isométrie de V, $r : S^3 \to \mathcal{O}(V)$ est un morphisme à valeurs dans $SO(V)$ et surjectif dedans, et de noyau $\{\pm 1\}$.
De plus, σ_u est une isométrie indirecte, et toute isométrie indirecte s'obtient ainsi.

Démonstration. Comme r est la restriction de ρ sur la diagonale de $S^3 \times S^3$, il s'agit de voir sur chaque r_q preserve bien V, ou de manière équivalente, qu'elle preserve bien son orthogonal, c'est à dire $\mathbb{R}$.
Comme $\mathbb{R}$ est central, et comme $q^{-1} = q^*$ (il a norme 1), on a bien que r_q fixe (point par point) $\mathbb{R}$. Elle induit donc une isométrie directe de V. (en fait, réciproquement, si $\rho_{p,q}$ fixe $\mathbb{R}$ point par point, on voit que $p = q$).
Toute rotation de V s'étend à $\mathcal{H}$ en une isométrie, en choisissant de fixer $\mathbb{R}$ point par point. Donc, toute rotation est atteinte par r.
On trouve le noyau de r facilement.
Comme $\sigma_q = -r_q$, c'est une isométrie indirecte de V, et on les obtient toutes ainsi.

□

Définition 2.3.3. *Si $u, v \in V$, posons $u \wedge v = \frac{1}{2}(uv - vu) = \Im(uv)$.*

Observation 2.3.3. $\wedge$ *est antisymétrique.*

Dans V, on a :

$$uv = -\langle u, v\rangle + u \wedge w.$$

$$u \wedge (v \wedge w) = \langle u, v\rangle w - \langle u, w\rangle v.$$

Proposition 2.3.7. *Pour tout $q \in \mathbb{H}$ de norme 1, il existe $\theta \in [0, 2\pi[$, et $v \in V$ de norme 1, tels que*

$$q = \cos\theta + v \sin\theta$$

et r_q est alors la rotation d'axe v d'angle θ.

Démonstration. Le premier point est évident par Pythagore. Pour le second, il est facile d'identifier l'axe de la rotation : on a clairement $r_q(v) = v$, c'est donc l'axe.

Pour verifier l'angle, prenons u dans $v^\perp \cap V$, de norme 1. Il est dans le plan orhtogonal à l'axe de r_q.

Il s'agit de voir que $\langle u, r_q(u)\rangle = \cos 2\theta$, et que $u \wedge r_q(u) = (\sin\theta)v$.

Calculons donc $ur_q(u) = uquq^*$.

Comme $uv = -\langle u, v\rangle + u \wedge v = u \wedge v = -v \wedge u = -vu$, on a $uq = q^*u$. Utilisons cela dans l'expression de $ur_q(u)$.

$ur_q(u) = q^*u^2q^* = -(q^*)^2$, car u est de norme 1 dans V (donc de carré -1).

On ecrit alors $-(q^*)^2 = -(\cos^2\theta - \sin^2\theta - 2\cos\theta\sin\theta v) = -\cos 2\theta + v\sin 2\theta$.

On a bien obtenu $ur_q(u) = -\cos 2\theta + v\sin 2\theta$. Comme par ailleurs, $ur_q(u) = -\langle u, r_q(u)\rangle + u \wedge r_q(u)$, on a ce qu'on voulait. □

2.3.7 Hopf

2.3.8 Frobénius

Théorème 2.3.4. *Si $\mathcal{A}$ est une $\mathbb{R}$-algèbre (associative) de dimension finie sur $\mathbb{R}$, dont tous les éléments non-nuls sont inversibles, alors $\mathcal{A} \simeq \mathbb{R}, \mathbb{C}$, ou $\mathbb{H}$.*

Démonstration. Si $\mathcal{A}$ est commutative, c'est un corps, extension finie de $\mathbb{R}$.

Comme $\mathbb{C}$ est la clôture algébrique de $\mathbb{R}$, on a necessairement $\mathcal{A} \simeq \mathbb{R}$ ou $\mathbb{C}$.

Supposons $\mathcal{A}$ non commutative. Montrons que $\mathcal{A}$ contient une copie de $\mathcal{H}$.

Soit $\mathcal{R} \subset \mathcal{A}$ l'image de $\mathbb{R}$ par le morphisme structural. Comme $\mathcal{A}$ n'est pas commutative, $\mathcal{A}$ n'est pas réduite à $\mathcal{R}$. Soit $a \in \mathcal{A} \setminus \mathcal{R}$. On a $\mathbb{R}[a]$ sous-algèbre commutative, c'est donc une extension algébrique du corps $\mathcal{R}$, et donc $\mathbb{R}[a] \simeq \mathbb{C}$. Quite à changer a dans $\mathbb{R}[a]$, on peut supposer que $a^2 = -1$, et on notera $i = a$.

Comme $\mathcal{A}$ n'est pas commutative, $\mathcal{A}$ n'est pas réduite à $\mathbb{R}[a]$. Soit $b \in \mathcal{A} \setminus \mathbb{R}[a]$. Notons $c = bi - ib$. Si $c = 0$, alors b commute à i, et à $\mathcal{R}$ (par définition), et donc $\mathbb{R}[i, b]$ est commutative, donc extension stricte de $\mathbb{R}[i] \simeq \mathbb{C}$. Mais $\mathbb{C}$ est algébriquement clos. Contradiction.

Ainsi $c \neq 0$.

On a $ci = -ic$ (il suffit de l'ecrire) donc $c \notin \mathcal{R}$. Encore une fois, on peut considerer $\mathcal{R}[c]$, il est commutatif, non réduit à $\mathbb{R}$, donc isomorphe à $\mathbb{C}$. En particulier, de dimension 2 sur $\mathbb{R}$.

On a aussi $c^2i = -cic = ic^2$. Ainsi c^2 commute avec i et $\mathcal{R}$, donc, comme on l'a vu, il est dans $\mathbb{R}[i]$.

Par ailleurs, $c^2 \in \mathbb{R}[c]$. Comme $\mathbb{R}[i] \cap \mathbb{R}[c]$ est de dimension 1 sur $\mathbb{R}$, c'est $\mathcal{R}$, et donc $c^2 \in \mathcal{R}$, et c est donc imaginaire pur dans $\mathcal{R}[c] \simeq \mathbb{C}$.

Notons $c^2 = -t$, pour $t \in \mathcal{R}$, $t > 0$. Posons $j = \frac{1}{\sqrt{t}}c$. On a désormais $j^2 = -1$, et $ij = -ji$, et donc $(ij)^2 = -1$.

Finalement, $\mathcal{R}[i,j]$ contient $1, i, j, ij$ et c'est une partie génératrice en tant qu'espace vectoriel (en effet les produits (pour la loi d'algèbre) des 16 paires de ces éléments sont encore dans $\mathcal{R}[i,j]$).

C'est aussi une famille libre : si $a+bi+cj+dij = 0$, alors en multipliant par $a-bi-cj-dij = 0$, on obtient $a^2 + b^2 + c^2 + d^2 = 0$.

Ainsi, $\mathcal{R}[i,j]$ est de dimension 4. Comme $1, i, j, k = ij$ verifie toutes les formules définissant $\mathbb{H}$, il y a un morphisme surjectif de $\mathbb{H}$ dans $\mathcal{R}[i,j]$. Par un argument de dimension, c'est un isomorphisme.

Ainsi $\mathcal{A}$ contient une copie de $\mathbb{H}$.

Finalement, si $u \in \mathcal{A} \setminus \mathcal{H}$, on peut supposer comme avant que $(ui - iu)^2 = -1$. Posons $\ell = ui - iu$.

On a $\ell i = -i\ell$. Puis, $j\ell i = -ji\ell = ij\ell$.

Ainsi i commute avec $j\ell$, donc $j\ell \in \mathcal{R}[i]$ et donc $\ell \in \mathcal{R}[i,j]$, cela veut dire que $ui - iu$ est dans notre copie de $\mathbb{H}$. Mais $ui + iu$ aussi, car il commute avec i.

Finalement, nous avons $2ui \in \mathbb{H}$, et donc $u \in \mathbb{H}$. Contradiction.

□

2.3.9 Cayley

3 Compléments sur les algèbres de polynômes

3.0.10 Polynômes symétriques

Soit A un anneau intègre, commutatif (unifère), et $A[X_1, \dots, X_n]$ l'algèbre (associative) des polynômes à n indeterminées commutatives.

Soit $\mathfrak{S}_n$ le groupe symétrique des permutations de $\{X_1, \dots, X_n\}$ (agissant à gauche).

Ce groupe admet une action sur $A[X_1, \dots, X_n]$ par précomposition (donc à droite). Ce sont des automorphismes d'algèbre.

Notons $P^\sigma(X_1, \dots, X_n) = P(\sigma(X_1), \dots, \sigma(X_n))$.

Définition 3.0.4. *Un polynôme P est dit* **symétrique** *s'il est un point fixe de $\mathfrak{S}_n$. C'est à dire si $P^\sigma = P$ pour tout σ.*

Exemple 3.0.1. $\sum_{i=1}^n X_i = \Sigma_1^{(n)}$.

$\prod_{i=1}^n X_i = \Sigma_n^{(n)}$.

$$\sum_{1 \le j_1 \le \dots \le j_i \le n} \prod_{k=1}^{i} X_{j_k} = \Sigma_i^{(n)}.$$

$\Sigma_0^{(n)} = 1_A$.

$\sum_i X_i^k$ *(pas de nom ?)*

Observation 3.0.4. $\sigma_i^{(n)}(X_1, \dots, X_{n-1}, 0) = \Sigma_i^{(n-1)}$.

L'ensemble des polynômes symétriques forme une sous-algèbre.

Théorème 3.0.5. *Définissons $\Psi : A[Y_1, \dots, Y_n] \to A[X_1, \dots, X_n]$ par $\Psi(Y_i) = \Sigma_i^{(n)}$.*

Alors Ψ est un morphisme d'algèbre injectif, et d'image $A[X_1, \dots, X_n]^{\mathfrak{S}}$, la sous-algèbre des polynômes symétriques.

Démonstration. D'abord, notons que Ψ est un morphisme bien défini et à valeur dans la sous-algèbre $A[X_1, \ldots, X_n]^{\mathfrak{S}}$.

Ensuite, montrons que Ψ est injective. Par reccurence sur n. Si $n = 1$ il n'y a rien à dire.

Si $n > 1$, supposons par l'absurde, que $\Psi(P) = 0$ avec $P \neq 0$ et de degré (total) minimal pour cette propriété.

Ecrivons $P = P_0 + Y_n S$ avec P_0 ne dépendant que des indeterminées $Y_1, \ldots Y_{n-1}$. On a

$$0 = \Psi^{(n)}(P) = \Psi^{(n)}(P_0) + \Sigma_n^{(n)} \Psi^{(n)}(S)$$

Pris en $X_n = 0$, on a

$$0 = \Psi^{(n-1)}(P_0) + 0$$

Par hypothèse de récurrence, $P_0 = 0$. Maintenant, $0 = \Sigma_n^{(n)} \Psi^{(n)}(S)$, et donc $\Psi^{(n)}(S) = 0$. Mais le degré total de S est strictement inferieur à celui de P, contradiction.

Il faut montrer que Ψ est surective. A nouveau par recurrence, mais cette fois sur n et le degré total d de $P \in A[X_1, \ldots, X_n]^{\mathfrak{S}}$.

Si $n = 1$: rien à dire ($\Psi = Id$).

Si $n > 1$ et $d = 1$, $P = \sum a_i X_i$ mais s'il est symétrique, chaque a_i vaut a_1. Donc $P = a_1 \Sigma_1^{(n)}$. C'est bien dans l'image de Ψ.

On suppose le resultat vrai pour $n - 1$ indeterminés (tout degré) et pour n indeterminées jusqu'au degré $d - 1$.

Soit P de degré d symétrique.

Posons $P_0(X_1, \ldots, X_{n-1}) = P(X_1, \ldots, X_{n-1}, 0)$. Il est aussi symétrique car (l'image de) $\mathfrak{S}_{n-1}$ (dans le groupe de permutation de $X_1, \ldots, X_{n-1}$) est un sous-groupe de (l'image de) $\mathfrak{S}_n$ (dans le groupe de permutation de $X_1, \ldots, X_n$).

Par recurrence, $P_0 = \Psi^{(n-1)}(Q_0)$ pour $Q_0 \in A[Y_1, \ldots, Y_{n-1}]$.

Plus precisement : $P_0(X_1, \ldots X_{n-1}) = Q_0(\Sigma_1^{(n-1)}, \ldots, \Sigma_{n-1}^{(n-1)})$.

Soit $R_0(X_1, \ldots, X_n) = Q_0(\Sigma_1^{(n)}, \ldots, \Sigma_{n-1}^{(n)})$.

R_0 est symétrique (à n indeterminées) et $R_0(X_1, \ldots X_{n-1}, 0) = P_0$.

Posons $P_1 = P - R_0$.

On a $P_1(X_1, \ldots X_{n-1}, 0) = 0$.

Affirmation : $\Sigma_n^{(n)}$ divise P_1.

Si $n = 1$, c'est clair.

Sinon, voyons P_1 comme polynôme en X_n. Il possède 0 comme racine, donc X_n le divise. $P_1 = X_n S_1$

Mais par symétrie, chaque X_i le divise aussi et donc divise S_1.

Il vient que $X_1 \ldots X_n$ divise P_1. Cela montre l'affirmation.

Posons alors $P_1 = \Sigma_n^{(n)} \times P_2$.

Alors le degré de P_2 est $< d$, donc par recurrence $P_2 = \Psi(Q_2)$.

Finalement $\Psi(Y_n \times Q_2 + Q_0) = P$.

□

Proposition 3.0.8. *Si A est integre, commutatif, et $P \in A[X]$, ecrit $P(X) = \sum_{i=0}^{d} a_i X^i$. Les racines de P sont, avec multiplicité, $\alpha_1, \ldots, \alpha_d$ si et seulement si $\Sigma_i^{(d)} = (-1)^i a_{d-i}/a_d \in \mathrm{Frac}(A)$.*

En effet par recurrence sur d,

$$\prod (X - x_i) = \sum_{0 \leq k \leq d} \Sigma_k(x_1, \ldots x_d) X^{d-k}$$

Exemple d'application.

Proposition 3.0.9. *Si $P \in \mathbb{Z}[X]$ unitaire de degré d, de racines $\alpha_1, \ldots, \alpha_d$ dans $\bar{\mathbb{Q}}$ (avec multiplicité) alors pour tout polynome symétrique Q, on a $Q(\alpha_1,\ dots, \alpha_d) \in \mathbb{Z}$*

En effet $Q(\alpha_1,\ dots, \alpha_d) = \Psi(S)(\Sigma_1(\alpha_1, \ldots, \alpha_d), \ldots \Sigma_d(\alpha_1, \ldots, \alpha_d)$. Chaque $\Sigma_i(\alpha_1, \ldots, \alpha_d)$ est entier, car c'est $(-1)^i a_{d-i}/1$. Et $\Psi(S)$ est à coefficients entiers.

3.0.11 Résultant

A est toujours intègre commutatif.
Soient $P, Q \in A[X]$ ecrivons les $P(X) = \sum_0^p a_i X^i$ et $Q(X) = \sum_0^q b_i X^i$.

Définition 3.0.5. *Le* **resultant** *de P et Q est*

$$Res(P,Q) = \det \begin{pmatrix} a_p & 0\ldots0 & 0 & b_q & 0\ldots0 & 0 \\ \vdots & \ddots & 0 & \vdots & \ddots & 0 \\ a_0 & & a_p & b_0 & & b_q \\ 0 & \ddots & \vdots & 0 & \ddots & \vdots \\ 0 & 0\ldots0 & a_0 & 0 & 0\ldots0 & b_0 \\ \longleftarrow & q & \longrightarrow & \longleftarrow & p & \longrightarrow \end{pmatrix}$$

Notons $M_{P,Q}$ cette matrice et observons que c'est la matrice de l'application linéaire $\Phi_{P,Q}$ de $A_{q-1}[X] \times A_{p-1}[X]$ dans $A_{p+q-1}[X]$ donnée par $(R,S) \mapsto (PR + QS)$ dans les bases

$$(X^{q-1}, 0), \ldots, (1,0), (0, X^{p-1}), \ldots, (0,1)$$

au départ et

$$X^{p+q-1}, \ldots, X, 1$$

à l'arrivée.

Proposition 3.0.10. *Pour tout P, Q polynomes sur A de degré respectifs p et q, il existe R, S de degré respectifs $\leq q-1$ et $\leq p-1$ tels que $Res(P,Q) = PR + QS$.*

Démonstration. Prenons Ψ l'application linéaire donnée par la transposée de la comatrice de $M_{P,Q}$ dnas les bases sus-citées. Considérons $\Psi(1) = (R,S)$. On a bien $\Phi_{P,Q}(R,S) = det(M_{P,Q}) \times 1 = Res(P,Q)$. □

Dans l'application suivante, nous sommes sur un corps (évidemment commutatif).

Proposition 3.0.11. *Soit K un corps, et P, Q deux polynômes de degré ≥ 1. Les assertions suivantes sont équivalentes.*

1. $\text{pgcd}(P,Q) = 1$
2. $(P) + (Q) = K[X]$
3. $Res(P,Q) \in K^*$.

Démonstration. Le fait que 1 équivaut à 2 est simplement Bezout.

(3 $\implies$ 1) d'apres la proposition précédente.

(1 $\implies$ 3) : montrons que $\Phi_{P,Q}$ est injective. Si (R,S) est dans son noyau, $RP = -SQ$ mais comme $P \wedge Q = 1$, il vient que P divise S. Comme par ailleurs, (par définition de $\Phi_{P,Q}$ le degré de S est strictement inférieur à celui de P, cela entraine $S = 0$. On en déduit $R = 0$, et $\Phi_{P,Q}$ est bien injective.

Comme c'est une application linéaire entre deux K-espaces vectoriels de dimension $p+q$, elle est bijective, et son déterminent est non nul. Il résulte que $Res(P,Q) \in K^*$. □

Un dernier résultat d'élimination.

Proposition 3.0.12. *Soit A un anneau integre commutatif. Soit $B = A[X_1, \ldots, X_{n-1}]$. Soient $f_i, i \leq p$ et $g_j, j \leq q$ des éléments de B et supposons que $f_p g_q \neq 0$.*

Soient finalement $f(X) = \sum_{i=0}^{p} f_i X^i$ et $g(X) = \sum_{j=0}^{q} g_j X^j$ deux éléments de $B[X]$.

1. *Si $Res_X(f, g) = 0$, alors f et g ont un facteur commun non constant.*
2. *Si $(\alpha_1, \ldots, \alpha_n) \in A^n$ est un zero commun de f et g (vus dans $A[X_1, \ldots, X_{n-1}, X]$) alors $(\alpha_1, \ldots, \alpha_{n-1})$ est un zero de $Res_X(f, g)$ (vu dans $A[X_1, \ldots, X_{n-1}] = B$.*
3. *Réciproquement, si $(\alpha_1, \ldots, \alpha_{n-1})$ est un zero de $Res_X(f, g)$, et si $f_p(\alpha_1, \ldots, \alpha_{n-1}) \times g_q(\alpha_1, \ldots, \alpha_{n-1}) \neq 0$, alors il existe $\tilde{\alpha}_n \in \overline{\mathrm{Frac}(A)}$ (la cloture algébrique du corps des fractions) tel que $(\alpha_1, \ldots, \alpha_{n-1}, \tilde{\alpha}_n)$ est un zero commun de f et g dans $\overline{\mathrm{Frac}(A)}^n$.*

Démonstration. 1– On sait qu'il existe R, S tels que $PR + QS = 0$. Donc P divise QS. Comme de plus le degré de S est strictement inferieur à celui de P, un facteur irreductible de P divise Q.

2 – Spécialisons en $X_i = \alpha_i$, pour tout $i < n$. On a spe : $A[X_1, \ldots, X_{n-1}] \to A$. Notons A_0 l'image, et $\mathrm{Frac}(A_0)$ son corps des fractions. les images f_0 et g_0 de f et g s'annulent en $X = \alpha_n$. Ainsi, dans $\mathrm{Frac}(A_0)[X]$, f_0 et g_0 ne sont pas premiers entre eux, et $Res(f_0, g_0) = 0$.

Mais dans la formule du determinant, il s'agit juste de la specialisation en $X_i = \alpha_i$, pour tout $i < n$ de $Res_X(f, g)$.

3 – On reprend les notations précédentes. Par hypothèse, on a bien $deg(f_0) = p$ et $deg(g_0) = q$. Comme on suppose $Res(f_0, g_0) = 0$, d'apres la proposition précédente, f_0 et g_0 ont un facteur commun (non constant) dans $\mathrm{Frac}(A_0)[X]$. Ils ont donc une racine commune dans le corps de décomposition de ce facteur commun.

□

Exemple 3.0.2. *Si $f(X, Y) = X^4 + Y^4 - 1$ et si $g(X, Y) = X^5Y^2 - 4X^3Y^3 + X^2Y^5 - 1$, alors on peut calculer $Res_X(f, g) = 2Y^{28} - 16Y^{27}$. On a éliminé l'une des indéterminées au prix d'un accroissement du degré.*

3.0.12 Fractions rationelles

...
...
...