Fiche résumée du cours d'algèbre 1

1 Rappel sur les anneaux commutatifs unitaires

1.1 Rappel sur les anneaux : généralités

Rq : les morphismes d'anneau préservent 1. Rq : Soit A un anneau, $(I_n)_{n\in\mathbb{N}}$ une famille d'idéaux.

$$\sum_k I_k = \{\sum_k q_k \in I_k \text{ famille presque nulle.}\}$$

Rq : Soient I, J deux idéaux, on note IJ l'idéal engendré par IJ. Rq : Un idéal I est premier si A/I est intègre. Rq : Un idéal I est maximal si A/I est un corps.

Théorème 1.1 (Krull) *Tout idéal est contenu dans un idéal maximal. Un idéal est dit propre s'il est différent de A.*

Définition 1.1 (Anneau noétherien) *Un anneau est dit* ***noetherien*** *si l'une des propriétés équivalentes suivantes est vérifiée :*

i) Tout idéal est de type fini.

ii) Toute suite croissante d'idéaux est stationnaire.

iii) Tout ensemble non vide d'idéaux a un élément maximal pour l'inclusion.

Théorème 1.2 (Hilbert) *A noetherien $\Rightarrow$ A[X] noetherien*

Corollaire 1.1 *Si A est noetherien, alors toute A-algèbre de type fini est aussi un anneau noetherien.*

Définition 1.2 (élément irréductible) *$p \in A$ est* ***irréductible*** *si*

i) $p \notin A^*$

ii) $p = ab \Rightarrow p \mid a$ ou $p \mid b$

On définit de même la notion d'éléments premiers entre eux

Définition 1.3 (Anneau factoriel) *A anneau est dit* ***factoriel*** *si :*

i) (FAC 2) $\forall a \in A$, $a \neq 0$, $\exists p_1 ... p_r \in A$, irréductibles, $\exists u \in A^*$, tels que $a = up_1...p_n$

ii) (FAC 3) Cette décomposition est unique à unités près.

Proposition 1.1 *Si A vérifie (FAC 2), alors, les propriétés suivantes sont équivalentes :*

i) (FAC 3)

ii) (Lemme d'Euclide) $\forall p$ irréductible, $p \mid ab \Rightarrow p \mid a$ ou $p \mid b$.

iii) p irréductible $\Leftrightarrow$ (p) idéal premier.

iv) (Théorème de Gauss) Si $a \mid bc$, et $a \wedge b = 1$, alors $a \mid c$.

Définition 1.4 (Anneau principal) *un anneau est dit* ***principal*** *si tous ses idéaux le sont.*

Proposition 1.2 *A principal $\Rightarrow$ A factoriel*

Théorème 1.3 (Gauss) *A factoriel $\Rightarrow$ A[X] factoriel*

Définition 1.5 (PGCD, PPCM) *Dans un anneau factoriel, PGCD et PPCM sont définis :*

i) $a \wedge b = \prod p^{\min(v_p(a), v_p(b))}$

ii) $a \vee b = \prod p^{\max(v_p(a), v_p(b))}$

Rq : Si A est principal, on a Bézout.

Définition 1.6 (Anneau euclidien) *On dit qu'un anneau A est* ***euclidien****, s'il existe $v : A - \{0\} \to \mathbb{N}$ telle que $\forall a \in A, \forall b \in A - \{0\}$, $\exists q, r \in A$, $a = bq + r$ avec $v(r) < v(b)$*

Théorème 1.4 *Tout anneau euclidien est principal.*

1.2 Factorisation de polynômes

A anneau factoriel $\mathbb{K} = Frac(A)$.

Définition 1.7 (Contenu) *On appelle* ***contenu*** *d'un polynôme non nul le PGCD de ses coefficients, défini modulo A^*. Un polynôme est primitif si son contenu est dans A^**

Proposition 1.3 *i) $c(PQ) = c(P)c(Q)$*

ii) Les $P \in A[X]$ irréductibles sont, soit les constantes irréductibles de A, et les polynômes de degré strictement positifs, primitifs, irréductibles dans $\mathbb{K}[X]$

Théorème 1.5 (Critère d'Eisenstein) *$P = a_nX^n + ... + a_0 \in A[X]$, $p \in A$ irréductible. Supposons :*

i) $p \nmid a_n$

ii) $\forall i \in \{0...n-1\}$, $p \mid a_i$

iii) $p^2 \nmid a_0$

Alors P est irréductible dans $\mathbb{K}[X]$ (et donc dans $A[X]$, si P est primitif.

Théorème 1.6 (Réduction) *Soit I un idéal premier. Soit $B = A/I$, $L = Frac(B)$, $P = a_nX^n + ... + a_0 \in A[X]$, $\overline{P} = \overline{a_n}X^n + ... + \overline{a_0} \in B[X]$ (réduction des coefficient). Alors, si $\overline{a_n} \neq 0$, $\overline{P}$ irréductible sur B ou L, alors P est irréductible sur $\mathbb{K}$*

1.3 Extension de corps

Définition 1.8 (Extension de corps) *Une* ***extension de corps*** *est un morphisme de corps $i : \mathbb{K} \to \mathbb{L}$. Etant donné une telle extension, $\mathbb{K}$ est vu comme sous corps de $\mathbb{L}$, et $\mathbb{L}$ admet une structure de $\mathbb{K}-$espace vectoriel. Cette extension est dite* ***finie*** *si la dimension de $\mathbb{L}$ en tant que $\mathbb{K}-$espace vectorielest finie, et on note $[\mathbb{L} : \mathbb{K}] = dim_{\mathbb{K}}(\mathbb{L})$, appellé* ***degré de l'extension****.*

Théorème 1.7 (De la base téléscopique) *si $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$ sont des extensions de corps, $(e_i)_i$ une $\mathbb{K}-$base de $\mathbb{L}$, et $(f_j)_j$ une $\mathbb{L}$-base de $\mathbb{M}$, alors $(e_if_j)_{i,j}$ est une $\mathbb{K}-$base de $\mathbb{L}$. le degré d'extensions est donc multiplicatif, et on a :*

$$[\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}] = [\mathbb{M} : \mathbb{K}].$$

Définition 1.9 (Extension engendrée) *Soit $\mathbb{K} \subset \mathbb{L}$ extension, $S \subset \mathbb{L}$ sous ensemble. L'extension est* ***engendrée*** *par S si $\mathbb{L}$ est le plus petit sous corps de $\mathbb{L}$ contenant $\mathbb{K}$ et S, on note $\mathbb{L} = \mathbb{K}(S)$, ou $\mathbb{L}(x_1...x_n)$, si $S = \{x_1...x_n\}$. L'extension est dite* ***simple*** *si elle est engendrée par un singleton.*

Définition 1.10 (Morphisme d'extensions) *Un* ***morphisme d'extension*** *$(\mathbb{K} \xrightarrow{i} \mathbb{L}) \to (\mathbb{K}' \xrightarrow{i'} \mathbb{L}')$ est un diagramme commutatif :*

$$\begin{array}{ccc} \mathbb{K} & \xrightarrow{i} & \mathbb{L} \\ f \downarrow & & \downarrow g \\ \mathbb{K}' & \xrightarrow{i'} & \mathbb{L}' \end{array}.$$

Définition 1.11 (Elements transcendants, algébriques) *$\mathbb{K} \subset \mathbb{L}$ une extension, $\alpha \in \mathbb{L}$, soit $\begin{array}{rccc} \phi & : & \mathbb{K}[X] & \to & \mathbb{L} \\ & & P(X) & \mapsto & P(\alpha) \end{array}$ un morphisme d'anneaux.*

i) On dit que α est ***transcendant*** *si $Ker\phi = \{0\}$.*

ii) On dit que $\mathbb{K}$ est ***algébrique*** *sinon.*

On note $\mathbb{K}[\alpha] = Im\phi$

Proposition 1.4 *Si α est algébrique, $\mathbb{K}$ est un corps $\Rightarrow \mathbb{K}[X]$ principal. Il existe un unique polynôme $P \in \mathbb{K}[X]$ tel que $Ker\phi = (P)$. P s'appelle le polynôme minimal de α.*

Théorème 1.8 *$\mathbb{K} \subset \mathbb{L}$ extension, $\alpha \in \mathbb{L}$, les propriétés suivantes sont équivalentes :*

i) α est algébrique sur $\mathbb{K}$

ii) $\mathbb{K}[\alpha] = \mathbb{K}(\alpha)$

iii) $Dim_{\mathbb{K}}\mathbb{K}[\alpha] < \infty$

Définition 1.12 (Extension algébrique) *Une extension de corps est dite algébrique si tous ses éléments le sont.*

Proposition 1.5 *L'ensemble des éléments algébriques d'une extension est un sous corps de cette extension.*

1.4 Corps de Rupture, Corps de décomposition

Théorème 1.9 *i) Si $P \in \mathbb{K}[X]$ est un polynôme unitaire irréductible, il existe une extension simple algébrique $\mathbb{K} \subset \mathbb{K}(\alpha)$ telle que le polynôme minimal de α soit P.*

ii) Si $\mathbb{K} \subset \mathbb{K}(\alpha)$, $\mathbb{K} \subset \mathbb{K}(\beta)$ extensions simples algébriques, et si α et β ont même polynôme minimal (sur $\mathbb{K}$), alors les extensions sont isomorphes, par un isomorphisme qui à α associe β.

iii) Si $\mathbb{K} \overset{i}{\tilde{\to}} \mathbb{L}$ est un isomorphisme de corps et si $\mathbb{K}(\alpha)$ et $\mathbb{L}(\beta)$ sont des extensions algébriques simples, si $i(P_\alpha) = P_\beta$, alors, on a un isomorphisme d'extensions :

$$\begin{array}{ccc} \mathbb{K} & \overset{i}{\to} & \mathbb{L} \\ \downarrow & & \downarrow \\ \mathbb{K}(\alpha) & \overset{i'}{\to} & \mathbb{L}(\beta) \\ {\scriptstyle\alpha}\uparrow & & \uparrow{\scriptstyle\beta} \end{array} .$$

Définition 1.13 (Corps de rupture) *$P \in \mathbb{K}[X]$, P irréductible, $\mathbb{K} \subset \mathbb{L}$ une extension, est un **corps de rupture** de P si $\mathbb{L} = \mathbb{K}(\alpha)$ et $P(\alpha) = 0$*

Théorème 1.10 *Soit P un polynôme irréductible sur $\mathbb{K}$, il existe un unique, à $\mathbb{K}-$isomorphisme près, corps de rupture de P*

Définition 1.14 (Corps de décomposition) *$P \in \mathbb{K}[X]$, de degré n, on appelle **corps de décomposition** de P sur $\mathbb{K}$ une extension $\mathbb{K} \subset \mathbb{L}$ tel que :*

i) Dans $\mathbb{L}[X]$, P est un produit de polynômes de degré 1, $P = \prod(X - \alpha_i)$.

ii) $\mathbb{L}$ est minimal, i.e. $\mathbb{L} = \mathbb{K}(\alpha_1 ... \alpha_n)$.

Cette extension est engendrée par les racines de P.

Théorème 1.11 *$P \in \mathbb{K}[X]$, $deg(P) = n$, il existe un corps de décomposition de P sur $\mathbb{K}$, il est unique à $\mathbb{K}-$isomorphime près.*

Rq : Cette extension est une extension finie car les α_i sont algébriques sur $\mathbb{K}$. Le degré de l'extension est borné par n !

Lemme 1.1 *$\mathbb{K}$, $\mathbb{K}'$, deux corps, $i : \mathbb{K} \overset{\sim}{\to} \mathbb{K}'$, $P \in \mathbb{K}[X]$, $P' = i(P) \in \mathbb{K}'[X]$. Soit $\mathbb{L}$ le corps de décomposition de P sur $\mathbb{K}$. Soit $\mathbb{L}'$ le corps de décomposition de P' sur $\mathbb{K}'$. Alors, il existe un isomorphisme $\mathbb{L} \to \mathbb{L}'$ tel que l'on aie le diagramme commutatif suivant.*

$$\begin{array}{ccc} \mathbb{K} & \overset{i}{\to} & \mathbb{K}' \\ \cap & & \cap \\ \mathbb{L} & \overset{\varphi}{\tilde{\to}} & \mathbb{L}' \end{array} .$$

Définition 1.15 (Corps algébriquement clos) *Un corps est **algébriquement clos** si tout polynôme de degré strcitement positif est scindé, ou encore si tout polynôme de degré strictement positif admet une racine, ou encore si toute extension algébrique est égale à $\mathbb{K}$, ou encore si les polynômes irréductibles sont les $X - \alpha$, $\alpha \in \mathbb{K}$*

Définition 1.16 (Clôture algébrique) *Une extension $\mathbb{K} \subset \overline{\mathbb{K}}$ est une **clôture algébrique** si :*

i) $\overline{\mathbb{K}}$ est algébriquement clos.

ii) L'extension $\mathbb{K} \subset \overline{\mathbb{K}}$ est algébrique.

Proposition 1.6 *Il existe une clôture algébrique, unique à isomorphisme près.*

Définition 1.17 (Sous corps premier) *On apelle sous corps premier le corps engendré par 1*

Théorème 1.12 *$\mathbb{K}$ un corps fini.*

i) $\exists p$ premier, $\exists n \geq 0$ tel que $|\mathbb{K}| = p^n$.

ii) Si $|\mathbb{K}| = p^n$, $\mathbb{K}$ est le corps de décomposition de $X^{p^n} - X$ sur $\mathbb{Z}/p\mathbb{Z}$.

iii) les corps finis sont tous de la forme ci dessus.

On note $\mathbb{F}_q$ le corps à q éléments.

Théorème 1.13 *$\mathbb{K}$ un corps*

i) Si $G \subset \mathbb{K}^*$ est un sous groupe fini, alors, G est cyclique. En particulier, $\mathbb{F}_q^* = \mathbb{Z}/(q-1)\mathbb{Z}$

ii) Tout corps fini est une extension simple de son sous corps premier

Théorème 1.14 (Structure des groupes abéliens) *Tout groupe abélien de type fini est produit direct de $\mathbb{Z}^r$, $r \geq 0$ et d'un nombre fini de $\mathbb{Z}/n\mathbb{Z}$, $n > 0$. C'est donc un produit fini de groupes cycliques.*

Lemme 1.2 (Chinois)

$$\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}/(m \wedge n)\mathbb{Z}$$

2 Groupe de Galois

Soit $\mathbb{K}$ un corps, on note $Aut_{\mathbb{K}}$ les automorphismes de corps, soit $\mathbb{K} \subset \mathbb{L}$, $\mathbb{K} \subset \mathbb{M}$ deux extensions.

On note : $Hom_{\mathbb{K}}(\mathbb{L}, \mathbb{M}) = \{\mathbb{K}-\text{isom.}\} = \{\text{isom. de corps}\} = \{\sigma : \mathbb{L} \to \mathbb{M}, \sigma_{|\mathbb{K}} = Id_{\mathbb{K}}, \sigma \text{ morphismes de corps}\}$
$Gal(\mathbb{L}_{|\mathbb{K}})$=groupe de galois de $\mathbb{L}_{|\mathbb{K}} = Hom_{\mathbb{K}}(\mathbb{L}, \mathbb{L})$ surjectifs $= \{\text{automorphismes de } \mathbb{L}_{|\mathbb{K}}\}$

Remarque : Si $\mathbb{K}$ est le sous corps premier, $Gal(\mathbb{L}_{|\mathbb{K}}) = Aut(\mathbb{L})$

Théorème 2.1 (Dedekind) *$\mathbb{K} \subset \mathbb{M}$, $\mathbb{K} \subset \mathbb{L}$ deux extensions*

i) Les éléments non nuls de $Hom_{\mathbb{K}}(\mathbb{L}, \mathbb{M})$ forment un systèmre libre du $\mathbb{M}$-espace vectoriel $Lin_{\mathbb{K}}(\mathbb{L}, \mathbb{M})$

ii) Si $[\mathbb{L} : \mathbb{K}] < \infty$, alors $\#Hom_{\mathbb{K}}(\mathbb{L}, \mathbb{M}) \leq [\mathbb{L} : \mathbb{K}]$

Lemme 2.1 *$\mathbb{K} \subset \mathbb{M}$ une extension, A une $\mathbb{K}-$algèbre unitaire, alors les éléments non nuls de $Hom_{\mathbb{K}}(A, \mathbb{M})$ forment un système libre du $\mathbb{M}$-espace vectoriel $Lin_{\mathbb{K}}(A, \mathbb{M})$.*

Lemme 2.2 *$\mathbb{K}$, $\mathbb{K}'$, $i : \mathbb{K} \xrightarrow{\sim} \mathbb{K}'$ isomorphisme de corps qui induit $i : \mathbb{K}[X] \xrightarrow{\sim} \mathbb{K}'[X]$. Soit $P \in \mathbb{K}[X]$, posons $P' = i(P) \in \mathbb{K}'[X]$. Considérons $\mathbb{L}$, $\mathbb{L}'$ les corps de décomposition de P et P' sur $\mathbb{K}$ et $\mathbb{K}'$; Soit q le nombre d'isomorphisme de corps $\mathbb{L} \to \mathbb{L}'$ qui, restreints à $\mathbb{K}$, coïncident avec i. Alors :*

i) $q \leq [\mathbb{L} : \mathbb{K}]$

ii) $q = [\mathbb{L} : \mathbb{K}]$ si P n'a que des racines simples dans $\mathbb{L}$

Corollaire 2.1 *Si $P \in \mathbb{K}[X]$, $deg(P) = n$, $\mathbb{L}$ corps de décomposition de P sur $\mathbb{K}$. Si P n'a que des racines simples dans $\mathbb{L}$, alors $\#Gal(\mathbb{L}_{|\mathbb{K}}) = [\mathbb{L}, \mathbb{K}]$*

3 Extensions normales

Définition 3.1 (Conjuguaison) *$x, y \in \overline{\mathbb{K}}$ sont dits **conjugués** s'ils ont le même polynôme minimal sur $\mathbb{K} \Leftrightarrow \exists \sigma \in Gal(\overline{\mathbb{K}}_{|\mathbb{K}}) \mid \sigma(x) = y$*

Définition 3.2 (Extension normale) *Une extension $\mathbb{K} \subset \mathbb{L}$ est dite **normale** si elle est algébrique et si tout $P \in \mathbb{K}[X]$ irréductible sur $\mathbb{K}$ qui a une racine dans $\mathbb{L}$ a toutes ses racines dans $\mathbb{L}$*

Proposition 3.1 *$\mathbb{K} \subset \mathbb{L} \subset \overline{\mathbb{K}}$, alors, les propriétés suivantes sont équivalentes :*

i) $\mathbb{K} \subset \mathbb{L}$ normale

ii) $\forall x \in \mathbb{L}$, *les conjugués de* x *dans* $\overline{\mathbb{K}}$ *sont tous dans* $\mathbb{L}$

Théorème 3.1 $\mathbb{K} \subset \mathbb{L}$ *finie, alors , les propriétés suivantes sont équivalentes :*

i) $\mathbb{L}_{|\mathbb{K}}$ *normale*

ii) $\exists P \in \mathbb{K}[X]$, $\mathbb{L}$ *est un corps de décomposition de* P *sur* $\mathbb{K}$

Définition 3.3 (CDD d'une famille de polynômes) *Soit* $(P_i)_{i\in I}$ *une famille de polynômes dans* $\mathbb{K}[X]$, *on appelle corps de décomposition de* $(P_i)_{i\in I}$ *sur* $\mathbb{K}$ *une extension* $\mathbb{L}$ *de* $\mathbb{K}$ *engendrée par les racines des* P_i *dans* $\mathbb{L}$ *et telle que chaque* P_i *est scindé sur* $\mathbb{L}$.

Théorème 3.2 $\mathbb{K} \subset \mathbb{L}$ *extension algébrique, alors les propriétés suivantes sont équivalentes :*

i) $\mathbb{L}_{|\mathbb{K}}$ *est normale*

ii) $\mathbb{L}$ *est corps de décomposition d'une famille* $(P_i)_{i\in I}$

Définition 3.4 (Clôture normale) $\mathbb{K} \subset \mathbb{L}$ *une extension* $\mathbb{K} \subset \mathbb{M}$ *est une clôture normale de* $\mathbb{K} \subset \mathbb{L}$ *si :*

i) $\mathbb{L} \subset \mathbb{M}$

ii) $\mathbb{K} \subset \mathbb{M}$ *normale*

iii) $\mathbb{K} \subset \mathbb{M}$ *est minimal avec i) et ii)*

i.e. si $\mathbb{L} \subset \mathbb{M}'$ *et* $\mathbb{K} \subset \mathbb{M}'$ *normale, alors si* $\mathbb{M}' \subset \mathbb{M}$, $\mathbb{M} = \mathbb{M}'$

Corollaire 3.1 $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$ *algébrique, si* $\mathbb{M}_{|\mathbb{K}}$ *normale,* $\mathbb{M}_{|\mathbb{L}}$ *aussi.*

Théorème 3.3 $\mathbb{K} \subset \mathbb{L}$ *algébrique. Cette extension :*

i) Admet une clôture normale.

ii) Cette clôture est unique à isomorphisme (entre extensions de corps) près.

4 Séparabilité

Lemme 4.1 $P \in \mathbb{K}[X]$, $\alpha \in \mathbb{K}$, *on a alors*

$$\alpha \text{ racine multiple de } P \quad \Leftrightarrow \quad P(\alpha) = P'(\alpha) = 0$$

Définition 4.1 (Séparabilité) $P \in \mathbb{K}[X]$, P *est dit séparable sur* $\mathbb{K}$ *si il vérifie l'un des énoncés équivalents suivants :*

i) $P \wedge P' = 1$ *dans* $\mathbb{K}[X]$.

ii) P n'a que des racines simples dans un corps de décomposition de P sur $\mathbb{K}$.

Proposition 4.1 $P \in \mathbb{K}[X]$ *irréductible, non constant. Alors, les propriétés suivantes sont équivalentes :*

i) P séparable

ii) $P' \neq 0$

iii) Soit $car(\mathbb{K}) = 0$, *soit* $car(\mathbb{K}) = p > 0$ *et* $P \notin \mathbb{K}[X^p]$

Définition 4.2 (Elément séparable) $\mathbb{K} \subset \mathbb{L}$, $\alpha \in \mathbb{L}$

i) α *est* ***séparable*** *sur* $\mathbb{K}$ *si* α *est algébrique et si le polynôme minimal de* α *est séparable sur* $\mathbb{K}$.

ii) $\mathbb{K} \subset \mathbb{L}$ *est* ***séparable*** *si elle est algébrique et si tout élément de* $\mathbb{L}$ *est séparable sur* $\mathbb{K}$.

Proposition 4.2 $\mathbb{K} \subset \overline{\mathbb{K}}$, $x \in \overline{\mathbb{K}}$ *séparable sur* $\mathbb{K}$. *Alors,*

$$(\forall \sigma \in Gal(\overline{\mathbb{K}}, \mathbb{K}), \sigma(x) = x) \Leftrightarrow x \in \mathbb{K}$$

Théorème 4.1 (De l'élément primitif) *Une extension finie et séparable est simple*

5 Extension normale et séparable

Proposition 5.1 $\mathbb{K} \subset \mathbb{L}$ *extension séparable finie, les propriétés suivantes sont équivalentes :*

i) $\mathbb{K} \subset \mathbb{L}$ *est normale.*

ii) $\#Gal(\mathbb{L}_{|\mathbb{K}}) = [\mathbb{L} : \mathbb{K}]$

Lemme 5.1 $\mathbb{K} \subset \mathbb{L}$ *finie, normale,* $\mathbb{K} \subset \mathbb{M} \subset \mathbb{L}$, $\tau \in Hom_{|\mathbb{K}}(\mathbb{M}, \mathbb{L})$, *alors,* $\exists \sigma \in Gal(\mathbb{L}_{|\mathbb{K}})$ *tel que* $\sigma_{|\mathbb{M}} = \tau$

Lemme 5.2 $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M} \subset \mathbb{N}$ *extensions,* $\mathbb{K} \subset \mathbb{L}$ *finie,* $\mathbb{N}$ *clôture normale de* $\mathbb{K} \subset \mathbb{L}$, *alors,* $\forall \tau \in Hom_{|\mathbb{K}}(\mathbb{L}, \mathbb{M})$, *on a* $Im(\tau) \subset \mathbb{N}$.

Lemme 5.3 $\mathbb{K} \subset \mathbb{L}$ *finie, les propriétés suivantes sont équivalentes :*

i) $\mathbb{K} \subset \mathbb{L}$ *normale*

ii) $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$, $\mathbb{K} \subset \mathbb{M}$ *normale,* $\forall \tau \in Hom_{\mathbb{K}}(\mathbb{L}, \mathbb{M})$, $\tau \in Gal(\mathbb{L}_{|\mathbb{K}})$

iii) $\exists \mathbb{K} \subset \mathbb{L} \subset \mathbb{N}$, $\mathbb{K} \subset \mathbb{N}$ *normale,* $\forall \tau \in Hom_{\mathbb{K}}(\mathbb{L}, \mathbb{N})$, $\tau \in Gal(\mathbb{L}_{|\mathbb{K}})$

Lemme 5.4 $\mathbb{K} \subset \mathbb{L}$ *finie séparable,* $n = [\mathbb{L} : \mathbb{K}]$, $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$, $\mathbb{K} \subset \mathbb{M}$ *normale,* $\#Hom_{\mathbb{K}}(\mathbb{L}, \mathbb{M}) = n$

Théorème 5.1 $\mathbb{K} \subset \mathbb{L}$ *finie séparable, les propriétés suivantes sont équivalentes :*

i) $\mathbb{K} \subset \mathbb{L}$ *normale*

ii) $\mathbb{K} = \mathbb{L}^{Gal(\mathbb{L},\mathbb{K})}$

Lemme 5.5 $G \subset Aut(\mathbb{L})$ *sous groupe fini, soit*

$$\mathbb{K} = \mathbb{L}^G = \{x \in \mathbb{L} \mid g(x) = x \ \forall g \in G\} .$$

Alors, $\mathbb{K} \subset \mathbb{L}$ *est normale séparable.*

Lemme 5.6 $G \subset Aut(\mathbb{L})$, *sous groupe fini,* $\mathbb{K} = \mathbb{L}^G$, *alors* $\mathbb{K} \subset \mathbb{L}$ *et* $[\mathbb{L} : \mathbb{K}] = \#G$

Proposition 5.2 $\mathbb{K} \subset \mathbb{L}$ *séparable normale (algébrique) , alors*

$$\mathbb{K} = \mathbb{L}^{Gal(\mathbb{L}_{|\mathbb{K}})} .$$

Définition 5.1 (Extension galoisienne) *Une extension est dite* ***galoisienne*** *si elle est normale et séparable.*

Proposition 5.3 *Une extension* $\mathbb{K} \subset \mathbb{L}$ *est galoisienne finie si et seulement si c'est le corps de décomposition d'un polynôme séparable.*

Définition 5.2 (Degré séparable) *Soit* $\mathbb{K} \subset \mathbb{L}$ *finie,* $\mathbb{K} \subset \overline{\mathbb{K}}$, *on appelle* ***degré séparable*** , *noté* $[\mathbb{L} : \mathbb{K}]_s = \#Hom_{\mathbb{K}}(\mathbb{L}_{\overline{\mathbb{K}}})$

Lemme 5.7 $\mathbb{K} \subset \mathbb{L}$, $\sigma \in Hom(\mathbb{K}, \overline{\mathbb{K}}')$, *avec* $\overline{\mathbb{K}}'$ *algébriquement clos. Alors,* $\sigma(\mathbb{K}) \subset (\overline{\mathbb{K}}')$ *est algébrique, et* $\#\{\tau \in Hom(\mathbb{L}, \overline{\mathbb{K}}'), \tau_{|\mathbb{K}} = \sigma\} = [\mathbb{L} : \mathbb{K}]_s$

Lemme 5.8

$$\mathbb{K} \subset \mathbb{L} \subset \mathbb{M} \text{ finies } \Rightarrow \ [\mathbb{M} : \mathbb{L}]_s [\mathbb{L} : \mathbb{K}]_s = [\mathbb{M} : \mathbb{K}]_s .$$

Lemme 5.9 $\mathbb{L} = \mathbb{K}(x)$ *algébrique,* $P_x \in \mathbb{K}[X]$ *le polynôme minimal de* x. *Alors,* $[\mathbb{L} : \mathbb{K}]_s$ =*nombre de racines de* P_x *dans* $\overline{\mathbb{K}}$

6 Correspondance de Galois

$\mathbb{K} \subset \mathbb{L}$, $G = Gal(\mathbb{L}_{|\mathbb{K}})$, $\mathscr{F} = \{\mathbb{M}$ corps, $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}\}$
$\mathscr{G} = \{H \subset G$ sous groupe $\}$

$$\begin{array}{rccc} \Gamma & : & \mathscr{F} & \to & \mathscr{G} \\ & & \mathbb{M} & \mapsto & Gal(\mathbb{L}_{|\mathbb{M}}) \\ \Phi & : & \mathscr{G} & \to & \mathscr{F} \\ & & H & \mapsto & \mathbb{L}^H \end{array}$$

Théorème 6.1 *Si $\mathbb{K} \subset \mathbb{L}$ galoisienne finie, $n = [\mathbb{L} : \mathbb{K}] = \#G$*

i) Γ et Φ sont bijectives décroissantes et inverses l'une de l'autre.

ii) $\forall \mathbb{M} \in \mathscr{F}$, $[\mathbb{L} : \mathbb{M}] = \#\Gamma(\mathbb{M})$, $[\mathbb{M} : \mathbb{K}] = \frac{n}{\#\Gamma(\mathbb{M})}$

iii) $\forall \mathbb{M} \in \mathscr{F}$, $\mathbb{K} \subset \mathbb{M}$ normale $\Leftrightarrow \Gamma(\mathbb{M}) \lhd G$

iv) $\forall \mathbb{M} \in \mathscr{F}$, $\mathbb{K} \subset \mathbb{M}$ normale $\Rightarrow Gal(\mathbb{M}_{|\mathbb{K}}) \simeq G/\Gamma(M)$

Lemme 6.1 *$\mathbb{K} \subset \mathbb{L}$ galoisienne finie $\mathbb{K} \subset \mathbb{M} \subset \mathbb{L}$, $\tau \in Gal(\mathbb{L}_{|\mathbb{K}})$*
$\Gamma(\tau(M)) = \tau \circ \Gamma(\mathbb{M}) \circ \tau^{-1}$

7 Produit tensoriel

M,N deux A-modules.

Définition 7.1 (Produit tensoriel) *Le **produit tensoriel** $M \otimes_A N$ est le groupe abélien F/N tel que :*

i) F est le groupe abélien libre sur $M \times N$. (c'est à dire que F est le groupe engendré par $M \times N$, sans identification).

ii) N est le sous groupe de F engendré par les $(m_1 + m_2, n) - (m_1, n) - (m_2, n)$, les $(m, n_1 + n_2,) - (m, n_1) - (m, n_2)$ et les $(am, n) - (m, an)$

iii) On note $m \otimes n$ l'élément (m, n) de $M \otimes_A N$. $m \otimes n$ est appellé tenseur pur.

Attention : Le produit tensoriel NE CONTIENT PAS que des tenseurs purs. Il est engendré par les tenseurs purs.

Définition 7.2 (Structure) *Le groupe abélien $M \otimes_A N$ est muni d'une structure de A-module tel que :*

$$a = \sum_{i=1}^{n} am_i \otimes n_i = \sum_{i=1}^{n} m_i \otimes an_i$$

Définition 7.3 *Soient L, M, N A-modules, $f : L \times M \to N$, A-bilinéaire. Alors, $\exists ! \overline{f} : L \otimes_A M \to N$ A-linéaire tel que, si l'on pose*

$$\Pi : L \times M \to F \to F/N$$

avec $F = \{\sum \alpha_i, \alpha_i \in L \times M\}$, $\Pi(l, m) = l \otimes m$, le diagramme suivant commute :

$$\begin{array}{ccc} L \times N & \xrightarrow{f} & N \\ \Pi \downarrow & \nearrow \overline{f} & \\ L \otimes_A M & & \end{array} .$$

Cette propriété est appellée propriété universelle de produit tensoriel.

Corollaire 7.1 *Soient L, M, L', M' quatre A-modules. $f : L \to L'$, $g : M \to M'$, A-linéaires. Alors, $\exists f \otimes g : L \otimes_A M \to L' \otimes_A M'$ A-linéaire tel que :*

$$f \otimes g\,(l \otimes m) = f(l) \otimes g(m).$$

De plus, on a :

i) $Id_M \otimes Id_N = Id_{M \otimes_A N}$

ii) $f \otimes g \circ f' \otimes g' = (f \circ f') \otimes (g \circ g')$

Proposition 7.1 *On a deux bijections :*

$$Hom_A(L \otimes M, N) \simeq \{L \times M \to N, \text{ bilinéaires}\}$$

$$Hom_A(L \otimes M, N) \simeq Hom_A(L, Hom_A(M, N))$$

Définition 7.4 (Catégorie) *on appelle **Catégorie** la donnée d'un ensmble d'objets $Obj(C)$, et, $\forall X, Y \in Obj(C)$, un ensemble de morphismes $Hom_C(X, Y)$, vérifiant :*

i) $\begin{array}{ccc} Hom_C(X,Y) \times Hom_C(Y,Z) & \to & Hom_C(X,Z) \\ (f, g) & \mapsto & f \circ g \end{array}$.

ii) La composition est associative.

iii) $\forall X \in Obj(C)$, on a $Id_X \in Hom_C(X,X)$.

Proposition 7.2 *L, M, N A-Modules, on a des isomorphismes canoniques de A-modules :*

i) $\begin{array}{ccc} A \otimes_A M & \to & M \\ a \otimes m & \mapsto & am \end{array}$

ii) $\begin{array}{ccc} L \otimes_A (M \otimes_A N) & \to & (L \otimes_A M) \otimes_A N \\ l \otimes (m \otimes n) & \mapsto & (l \otimes m) \otimes n \end{array}$

iii) $\begin{array}{ccc} L \otimes_A M & \to & M \otimes_A L \\ l \otimes m & \mapsto & m \otimes l \end{array}$

iv) $(L \oplus M) \otimes_A N \simeq (L \otimes_A N) \oplus (M \otimes_A N)$

(En considérant : $L \oplus M = L \times M$, $(l,m)+(l',m') = (l+l', m+m')$, $a(l,m) = (al, am)$*)*

Corollaire 7.2 *i) Si L, M est libre, de bases $(l_1...l_p)$, et $(m_1...m_n)$, alors $L \otimes_A M$ est un A-module libre de base $(l_i \otimes m_j)_{i,j}$.*

ii) Si L est libre de base $(l_1...l_p)$, alors $\begin{array}{ccc} M \oplus M \oplus ... \oplus M & \to & L \otimes_A M \\ (m_1...m_p) & \mapsto & \sum l_i \otimes m_i \end{array}$

Proposition 7.3 *Soit $(M_i)_{i\in I}$ une famille de A-modules, $\underset{i\in I}{\oplus} M_i \subset \prod_{i\in I} M_i$. $\forall i \in I$, $f_i : M_i \to N$ des morphismes de A-modules. Alors :*

$$\exists! f : \underset{i\in I}{\oplus} M_i \to N \text{ morphisme de A-modules tel que } f_i = f \circ r_i \forall i$$

avec $r_i : M_i \hookrightarrow \underset{j\in I}{\oplus} M_j$.

Proposition 7.4 *N un A-module, on a un isomorphisme canonique de A-modules*

$$\begin{array}{ccc} \varphi : \left(\underset{i\in I}{\oplus} M_i\right) \otimes_A N & \to & \underset{i\in I}{\oplus} (M_i \otimes_A N) \\ (m_i) \otimes n & \mapsto & (m_i \otimes n) \end{array}$$

Corollaire 7.3 *L, M A-modules libres de bases $(l_i)_{i\in I}$, $(m_j)_{j\in J}$, alors $L \otimes_A M$ est libre de base $(l_i \otimes m_j)_{i,j\in I,J}$*

Lemme 7.1 *$I \subset A$ idéal, L, M A-modules tels que $IM = IL = \{0\}$. Alors, M, L peuvent être vus comme des A/I-modules, et on a l'isomorphisme de A-modules :*

$$\begin{array}{ccc} \varphi : M \otimes_A L & \to & M \underset{A/I}{\otimes} L \\ m \otimes l & \mapsto & m \otimes l \end{array}$$

Proposition 7.5 *Soient L, M deux A-modules libres de bases $(l_1...l_p)$, et $(m_1...m_q)$. Soit $\varphi \in End_A(L)$, $\psi End_A(M)$, φ, ψ sont donnés par $B \in M_p(A)$, $C \in M_q(A)$ dans les bases ci-dessus, la matrice de $\varphi \otimes \psi \in End_A(L \otimes_A M)$ dans les bases $l_1 \otimes m_1 ... l_1 \otimes m_q ... l_p \otimes m_q$ est :*

$$\begin{pmatrix} b_{11}C & ... & b_{1p}C \\ ... & & ... \\ b_{p1}C & ... & b_{pp}C \end{pmatrix}$$

On peut montrer :

$$tr(\varphi \otimes \psi) = tr(\varphi)tr(\psi) \quad det(\varphi \otimes \psi) = det(\varphi)^q det(\psi)^p$$

Proposition 7.6 $\begin{array}{ccc} \varphi : L^* \otimes_A M & \to & Hom_A(L,M) \\ f \otimes m & \mapsto & (l \to f(l).m) \end{array}$ *. Cette application est bijective si L est de type fini, ou si L est libre et M de type fini.*

Proposition 7.7 *$L \xrightarrow{u} M \xrightarrow{v} N \to 0$ suite exacte de morphismes de A-modules, i.e.* $\begin{cases} Imu = Kerv \\ Imv = N \end{cases}$ *Alors,*

$$L \otimes_A X \xrightarrow{u\otimes Id_X} M \otimes_A X \xrightarrow{v\otimes Id_X} N \otimes_A X \to 0 \text{ est une suite exacte.}$$

Corollaire 7.4 *Soient des suites exactes de A-modules*

$$L \xrightarrow{i} M \xrightarrow{p} N \to 0$$
$$X \xrightarrow{j} Y \xrightarrow{q} Z \to 0$$

Alors, on a une suite exacte :

$$(L \otimes_A Y) \oplus (M \otimes_A X) \xrightarrow{[i\otimes Id; Id\otimes j]} M \otimes_A Y \xrightarrow{p\otimes q} (N \otimes Z) \to 0$$

Corollaire 7.5 *i)* $L \subset L'$, $M \subset M'$

ii) $I, J \subset A$ *idéaux,* $A/I \otimes_A A/J = A/I + J$ *(CP :* $\mathbb{Z}/m\mathbb{Z}$*)*

iii) $A/I \otimes_A M = M/IM$

8 Restrictions et extensions de scalaires

Soient A, B deux anneaux commutatifs unitaires, $f : A \to B$ morphismes d'anneaux.On a alors une correspondance entre A-modules et B-modules.

Définition 8.1 (restriction) *Soit M un B-module, on note $M_{|A}$ ou f_M la* ***restriction de*** *M* ***à*** *A ; $M_{|A} = M$ comme groupe abélien, et $\forall a \in A$, $\forall m \in M$, on définit*

$$a \underset{M_{|A}}{.} m = f(a) \underset{A}{.} m \ .$$

Proposition 8.1
- *$M \to M_{|A}$ est un foncteur, c'est à dire que si $f \in Hom_B(M, N)$, on lui associe $f_{|A} \in Hom_A(M_{|A}, N_{|A})$*
- *Si M est un A-module, on munit $B \otimes_A M$ (où l'on considère $a.b = f(a).b$) de la structure de B-module tel que,*

$$\forall b, b' \in B, \forall m \in Mb.(b' \otimes m) = (bb') \otimes m \ .$$

- *On a un foncteur*

$$\begin{array}{ccc} \{ A\text{-modules}\} & \to & \{ B\text{-modules}\} \\ M & \mapsto & B \otimes_A M \\ f \in Hom_A(M,N) & \mapsto & Id_B \otimes f \in Hom_B(B \otimes_A M, B \otimes_A N) \end{array}$$

Lemme 8.1 *Si M est un A-module libre de base $(e_i)_{i \in I}$, alors $B \otimes_A M$ est un B-module libre de base $(1 \otimes e_i)_{i \in I}$*

Lemme 8.2 *Soit M un A-module libre de base $e_1, ..., e_p$, $\varphi \in End_A(M)$ donné par la matrice $C \in Mat\, f(A)$. Alors, $Id_B \otimes \varphi = \varphi^B \in End_B(B \otimes_A M)$ morphisme de B modules induit $B \otimes_A M$, B-libre de base $(1 \otimes e_i)$. La matrice de φ^B dans $(1 \otimes e_i)_{i=1..P}$ est $f(C) = (f(c_{ij}))_{ij}$*

Proposition 8.2 (Réciprocité de Fröbenius) *Le foncteur d'induction est adjoint à gauche du foncteur de restriction, i.e. $\forall M$ un A-module, $\forall N$ un B-module, on a :*

$$Hom_B(B \otimes_A M, N) = Hom_A(M, N_{|A}) \ .$$

9 Algèbre tensorielles, symétriques, et extérieures

Soit R un anneau unitaire.

Définition 9.1 (Graduation) *Une* $\mathbb{N}$***-graduation*** *sur R est une décomposition $R = \underset{i \geq 0}{\oplus} R_i$ de groupes abéliens tels que, $\forall i, j$, $R_i.R_j \subset R_{i+j}$. On dit que $x \in R - \{0\}$ est (resp.* ***homogène*****) de degré** *i si (resp. et seulement si) $x \in R_i$. On définit de même une A-algèbre graduée.*

Définition 9.2 (Idéal homogène) *Soit R un anneau gradué, $I \lhd R$ idéal bilatère, I est dit* ***homogène*** *si et seulement si $I = \underset{n \geq 0}{\oplus}$, avec $I_n = I \cap R_n$*

Définition 9.3 (Application homogène) *Si R et S sont des anneaux gradués, et $f \in Hom_{anneau}(R, S)$, alors f est* ***homogène de degré*** *0, ou encore un* ***morphisme d'anneaux gradués*** *, si $\forall n$, $f(R_n) \subset (S_n)$*

Lemme 9.1 *Soit R un anneau gradué, $I \lhd R$ homogène, $\pi : R \to R/I$ la projection (morphisme d'anneaux). Alors, $R/I = \underset{n \geq 0}{\oplus} \pi(R_n)$ est une graduation sur R/I, et π est un morphisme d'anneaux gradués.*

Définition 9.4 (Puissances tensorielles) *Soit M un A-module ; pour tout n, on note $T^0(M) = A$, et $T^n(M) = M^{\otimes n} = M \otimes M ... \otimes M$. Enfin, on note $T(M) = \oplus a \geq 0 \oplus$. Le produit tensoriel munit $T(M)$ d'une structure de A-algèbre graduée :*

$$\begin{array}{ll} T^s(M) \times T^r(M) & \to T^{s+r}(M) \\ (m_1 \otimes m_2 ... \otimes m_s) \times (m_{s+1} \otimes m_{s+2} ... \otimes m_{s+r}) & \to (m_1 \otimes m_2 ... \quad \otimes m_{s+r}) \end{array}$$

On note $i : M \to T(M)$ l'inclusion canonique.

Lemme 9.2 (Propriété universelle) *Soit M un A-module, $\forall B =$ A-algèbre, $\forall f : M \to B$ morphisme de A-modules. Alors, il existe un unique morphisme de A-algèbre*

$$\tilde{f} : T(M) \to B$$

telle que $\tilde{f} \circ i = f$, ie

$$\begin{array}{ccc} T(M) & \stackrel{\tilde{f}}{\to} & B \\ i \cup & \nearrow_{f} & \\ M & & \end{array} ,$$

c'est à dire que

$$Hom_{A-alg}(T(M), B) = Hom(A - mod(M, B) .$$

$M \to T(M)$ définit un foncteur

$$\begin{array}{ccc} \{ A\text{-modules} \} & \to & \{ A\text{-algèbres} \} \\ M & \to & T(M) \\ f & \to & \oplus_n f^{\otimes n} \end{array}$$

T est le foncteur adjoint à gauche du foncteur de restriction des A-algèbres vers les A-modules.

Définition 9.5 (Tenseurs symétriques, antisymétriques) *Soit $t = t_1 \otimes ... \otimes t_n \in M^{\otimes n}$. Pour ω dans S_n, définissons $\omega(t) = t_{\omega(1)} \otimes ... \otimes t_{\omega(n)}$*

- *t est dit **symétrique** si, $\forall \omega \in S_n$, on a $w(t) = t$*
- *t est dit **antisymétrique** si, $\forall \omega \in S_n$, on a $w(t) = \varepsilon(\omega) t$*

On note S_n (resp. A_n) l'ensemble des tenseurs symétriques (resp. antisymétriques).

Proposition 9.1 *Supposons que $1/n! \in A$. Alors, soient*

$$\begin{array}{ccccc} P_n & : & T^n(M) & \to & T^n(M) \\ & & t & \mapsto & \frac{1}{n!} \sum_\omega \omega.t \end{array} \qquad \begin{array}{ccccc} A_n & : & T^n(M) & \to & T^n(M) \\ & & t & \mapsto & \frac{1}{n!} \sum_\omega \varepsilon(\omega) \omega.t \end{array}$$

P_n et A_n sont des projecteurs d'image $S_n(M)'$ et $A_n(M)'$ respectivement.

9.1 algèbre symétrique

Définition 9.6 (Algèbre symétrique) *Pour tout n, on définit le A-sous module $I_n \subset M^{\otimes n}$ engendré par les $m_1 \otimes ... \otimes m_n - \omega(m_1 \otimes ... \otimes m_n)$, $I_0 = \{0\}$. On pose également $I = \underset{n \geq 0}{\oplus} I_n = (x \otimes y - y \otimes x)_{x,y \in M}$. On définit alors **l'algèbre symétrique** comme le quotient*

$$S(M) = T(M)/I .$$

Remarque : l'algèbre $S(M)$ est commutative et graduée, engendrée par $M = S^1(M)$:

$$T(M) \twoheadrightarrow S(M) = T(M)/I$$

avec T(M) engendrée par M

Proposition 9.2 (propriété universelle) *Pour toute A-algèbre B, commutative, et pour tout $f : M \to B$, A-linéaire, $\exists \tilde{f}$ un morphisme de A-algèbre $S(M) \to B$.*

Théorème 9.1 *Si M est un module libre de rang fini, de base $e_1, ..., e_r$, alors $S(M)$ est un module libre de base $(e_1^{n_1}, ..., e_r^{n_r})_{n_1 ... n_r}$, et l'application*

$$\begin{array}{ccc} S(M) & \to & A[X_1 ... X_r] \\ e_i & \mapsto & X_i \end{array}$$

est un isomorphime de A-algèbre.

Définition 9.7 (Produit tensoriel d'algèbres commutatives) *Soient B, C deux A-algèbres commutatives unitaires. **L'algèbre produit tensoriel** $B \otimes_A C$ est le A-module $B \otimes_A C$ muni de l'unique produit tel que $(b \otimes c).(b' \otimes c') = (b.b' \otimes c.c')$*

Proposition 9.3 *Soient M, N deux A-modules. Il existe un isomorphisme de A-algèbres graduées*

$$\begin{array}{rccc} \varphi & : & S(M\oplus N) & \to & S(M)\otimes S(N) \\ & & (m,n) & \mapsto & m\otimes 1+1\otimes n \end{array}$$

9.2 algèbre extérieure

Définition 9.8 (Algèbre extérieure) *pour tout $n\geq 2$, soit $J_n\subset T^n(M)$ le A-sous module engendré par les $m_1\otimes ...\otimes m_n$ tels que $m_i=m_j$ pour un certain couple $i\neq j$. On pose $J_0=J_1=0$, et*

$$J=\bigoplus_{n\geq 0} J_n=(x\otimes x, x\in M).$$

On définit alors ***l'algèbre extérieure*** *comme l'algèbre graduée quotient*

$$\Lambda(M)=T(M)/J=\bigoplus_{n\geq 0}\Lambda_n\ ,$$

Ou $\Lambda_n=T_n(M)/J_n$.

Proposition 9.4 *Si M est un module libre de rang fini, de base $e_1,...,e_r$, alors $\Lambda_p(M)$ est un module libre de base $(e_{i_1}\wedge,...,e_{i_p}$, où $i_1<...<i_p$. En particulier, $dim(\Lambda^p(M))=\binom{r}{p}$*

Définition 9.9 (Algèbre tensorielle graduée) *Soient B, C deux A-algèbres $\mathbb{Z}$-graduées. Alors,*

$$B\otimes_A C=\bigoplus_{n\in\mathbb{Z}}\bigoplus_{p+q=n}(B_p\otimes_A C_q)$$

est une A-algèbre graduée pour la multiplication

$$(b\otimes c).(b'\otimes c')=(-1)^{deg\, b.deg\, c}(b.b'\otimes c.c')\ ,$$

pour c, b' homogènes.

Proposition 9.5 *Soient M, N deux A-modules. Il existe un isomorphisme de A-algèbres graduées*

$$\begin{array}{rccc} \psi & : & \Lambda(M\oplus N) & \to & \Lambda(M)\otimes^g_A\Lambda(N) \\ & & (m,n) & \mapsto & m\otimes 1+1\otimes n \end{array}$$

Définition 9.10 (Déterminant) *Soit L un A-module libre de rang m, $f\in End_A(L)$. Le déterminant de f, noté $\det f$ est l'unique élément de A tel que*

$$\Lambda^n f:\Lambda^n L\to\Lambda^n L\in End_A(\Lambda^n L)$$

est le produit par $\det f$

10 Algèbres et représentations

10.1 Algèbres de Lie

Définition 10.1 (Algèbre de Lie) *Une* ***algèbre de Lie*** *$\mathcal{G}$ sur $\mathbb{K}$ est un $\mathbb{K}-$espace vectorielmuni d'un produit bilinéaire*

$$\begin{array}{ccc} \mathcal{G}\times\mathcal{G} & \to & \mathcal{G} \\ (x,y) & \mapsto & [x,y] \end{array}$$

tel que $[x,y]=-[y,x]$ et $[[x,y],z]=[[x,z],y]+[x,[y,z]]$. Pour une $\mathbb{K}-$algèbre A, on peut définir une algèbre de Lie en considérant le $\mathbb{K}-ev$ A muni du crochet de Lie $[x,y]=xy-yx$. Un morphisme d'algèbre de Lie est un morphisme de $\mathbb{K}-$espace vectorieltel que $f([x,y])=[f(x),f(y)]$

Définition 10.2 (Algèbre enveloppante) *Une* ***algèbre enveloppante (universelle)*** *de $\mathcal{G}$ algèbre de Lie est une algèbre associative unitaire $U(\mathcal{G})$ avec un morphisme d'algèbre de Lie $j:\mathcal{G}\to U(\mathcal{G})_{lie}$ dont l'image engendrée $U(\mathcal{G})_{lie}$ est telle que, pour toute algèbre unitaire associative A, pour tout morphisme d'algèbre de Lie $\varphi:\mathcal{G}\to A_{lie}$, il existe un morphisme d'algèbre $\psi:U(\mathcal{G})\to A$ tel que $\varphi=j\circ\psi$, si ψ est considéré comme un morphisme d'algèbre de Lie.*

Proposition 10.1 *Si $(U(\mathcal{G}), j)$ et $(U(\mathcal{G})', j')$ sont deux algèbres enveloppantes de $\mathcal{G}$, alors, il existe un unique isomorphisme d'algèbres $\psi : U(\mathcal{G}) \to U(\mathcal{G})'$ tel que $j' = \psi \circ j$.*

10.2 Représentations algébriques

Soit $\mathbb{K}$ un corps, A une $\mathbb{K}-$algèbre unitaire.

Définition 10.3 (Représentation) *Une **représentation** de A, ou $A-$module, est un couple (ρ, V), où V est un $\mathbb{K}-$espace vectorielet*

$$\rho : A \to End_{\mathbb{K}}(V)$$

un morphisme d'algèbres.

Définition 10.4 (Sous module, module simple) *Si V est un $A-$module, on appelle sous module de V un sous espace vectoriel U tel que $aU \subset U \ \forall a \in A$, i.e. $\rho(a)(U) \subset U \ \forall a \in A$. On pose alors $\rho_U(a) = \rho(a)_{|U}$. Un module est dit **simple**, ou encore **représentation irréductible**, si elle n'admet pas de sous module non trivial.*

Définition 10.5 (Module quotient) *Si $U \subset V$ est un sous module, le module quotient est l'espace vectorielV/U muni de l'action*

$$\rho_{V/U}(a)(v + U) = \rho_V(a)(v) + U \ .$$

Définition 10.6 (Morphisme de $A-$modules) *Soient V, W deux A-modules,*

$$Hom_A(V, W) = \{f \in Hom(V, W), \ \forall a \in A, \ f \circ \rho_V(a) = \rho_W(a) \circ f\} \ .$$

Deux représentations V et W sont dit isomorphes si $Isom_A(V, W) \neq \emptyset$.

Définition 10.7 (Algèbre de groupe) *Soit G un groupe, $A = \mathbb{K}.G = \bigoplus_{g \in G} \mathbb{K}e_g$, on a une bijection :*

$$\begin{array}{ccc} \{rep. \ \mathbb{K} - linéaires \ de \ G\} & \Leftrightarrow & \{\mathbb{K}.G - modules\} \\ \rho_V^* \in Hom_{groupe}(G, GL(V)) & \Leftrightarrow & \rho_V \in Hom_{\mathbb{K}-ev}(\mathbb{K}.G, End(V)) \end{array}$$

Remarque : On ne peut définir dual et produit tensoriel de représentations que sur les $\mathbb{K}-$algèbres enveloppantes et de groupe. En général, ça n'a pas de sens.

Théorème 10.1 (Lemme de Schur) *Si (ρ_V, V), (ρ_W, W) sont deux représentations irréductibles de A et si $dim_{\mathbb{K}}(A) < \infty$, alors*

$$dim_{\mathbb{K}}(Hom_A(V, W)) = \begin{cases} 1 \ si \ V \simeq W \ . \\ 0 \ sinon. \end{cases}$$

Théorème 10.2 (Burnside) *$\mathbb{K} = \overline{\mathbb{K}}$. Soit (V, ρ) un $A-$module simple de dimension finie. Alors $\rho(A) = End_{\mathbb{K}}(V)$, i.e. ρ est surjective.*

Définition 10.8 (Module semi-simple) *Un $A-$module V est dit semi-simple ou complètement réductible si pour tout sous module V' il existe V'' un sous module tel que*

$$V = V' \oplus V'' \ ,$$

comme $A-$module.

Théorème 10.3 *V un $A-$module, les propriétés suivantes sont équivalentes :*

1. *V est somme directe d'une famille de $A-$modules simples.*
2. *V est somme d'une famille de $A-$modules simples.*
3. *V est semi simple.*

Proposition 10.2 *Soit V, V', V'' des représentations de A, Si $0 \to V' \to V \to V'' \to 0$ est une suite exacte de $A-$modules, alors si V est un module semi-simple, V' et V'' le sont aussi. Autrement dit, Un sous module et un quotient d'un module semi simple est semi-simple.*

Définition 10.9 (Algèbre simple) *$\mathbb{K}$ un corps commutatif algébriquement clos. Une $\mathbb{K}-$algèbre A est dite simple si tout idéal bilatère de A est trivial.*

Théorème 10.4 (Wedderburn) *Une algèbre simple de dimension finie sur $\mathbb{K}$ est isomorphe à $M_n(\mathbb{K})$, pour un certain n.*

Proposition 10.3 *Soit A une $\mathbb{K}$-algèbre de dimension finie. On définit ${}_AA$ la représentation régulière à gauche de A, i.e. le A-module $\rho(a)(b) = ab$. Alors, les propriétés suivantes sont équivalentes :*

i) ${}_AA$ *est semi-simple.*

ii) Tout $A-$module est semi-simple.

iii) A est isomorphe à une somme directe finie d'algèbres simples.

iv) $A \simeq \prod End_{\mathbb{K}}(V_i)$, V_i $\mathbb{K}-$*espace vectoriel de dimension finie.*

On dit alors que l'algèbre A est ***semi-simple****.*

Théorème 10.5 *Soit A une $\mathbb{K}-$algèbre semi-simple de dimension finie, notons ${}_AA = V_1^{m_1} \oplus ... \oplus V_r^{m_r}$, où les V_i ne sont pas isomorphes deux-à-deux. Alors,*

i) Tout $A-$module simple est isomorphe à un des V_i, tout A-module est somme des V_i

ii) Soit M un $A-$module. Alors,

$$\begin{array}{rccc} \varphi & : & \oplus Hom_A(V_i, M) \otimes_{\mathbb{K}} V_i & \to & M \\ & & \sum f_i \otimes v_i & \mapsto & \sum f_i(v_i) \end{array}$$

est un isomorphisme de A-modules.

iii) Soient $U_1 ... U_r$ des $\mathbb{K}-$espaces vectoriels de dimension finie, alors l'image du morphisme

$$\rho : A \to End_{\mathbb{K}}(\oplus U_i \otimes_{\mathbb{K}} V_i)$$

est la sous algèbre $\oplus \mathbb{K} Id_{V_1} \otimes End_{\mathbb{K}}(V_i)$.

Définition 10.10 (Composante isotypique) *Si A est semi-simple, $A = \oplus V_i$ et si M est un A-module, on appelle* ***composante isotypique*** *de type V_i l'image de*

$$\begin{array}{ccc} Hom_A(V_i, M) \otimes_{\mathbb{K}} V_i & \to & M \\ f \otimes v & \mapsto & f(v) \end{array} .$$

Proposition 10.4 *Soit A une $\mathbb{K}$-algèbre, soit V un A-module de dimension finie. Si V est semi simple, alors, l'image de A dans $End(V)$ est semi simple.*

11 Commutant et bicommutant (Dualité de Schur-Weil)

Définition 11.1 (Commutant) *Soit V un $\mathbb{K}-$espace vectoriel, et $U \subset End_{\mathbb{K}}(V)$, le* ***commutant*** *de U est*

$$Com(U) = \{f \in End_{\mathbb{K}}(V),\ f \circ v = v \circ f\ \forall v \in U\} .$$

Le bicommutant de U est $Com(Com(U))$.

Théorème 11.1 *Supposons que $dim(End_{\mathbb{K}}(V)) < \infty$. Soit $A \subset End_{\mathbb{K}}(V)$ une sous-algèbre, supposons-la semi simple. Alors, $B = Com(A)$ est encore semi-simple, et A se confond avec son bicommutant. Plus précisément, soit $Irr(A) = \{V_1, .., V_r\}$ les représentations irréductibles de A, notons $V = \oplus(U_i \otimes V_i)$, U_i un $\mathbb{K}-$ev une décomposition de $A-$modules, ie. $U_i = Hom_A(V_i, V)$. Alors :*

i) $A = \prod \mathbb{K} Id_{U_i} \otimes_{\mathbb{K}} End_{\mathbb{K}}(V_i)$

ii) $B = \prod End_{\mathbb{K}}(U_i) \otimes_{\mathbb{K}} \mathbb{K} Id_{V_i}$

Corollaire 11.1 *Si V est un $\mathbb{K}-$espace vectoriel, on pose $B = Com(A)$ et $V = \oplus U_i \otimes V_i$, comme ci-dessus, alors $Irr(B) \simeq \{U_1, ..., U_r\}$, c'est à dire que chaque $\mathbb{K}$-espace vectorielU_i est muni d'une structure de $B-$module irréductible, et tous les modules irréductibles s'obtiennent ainsi.) En particulier, on a une bijection*

$$\begin{array}{ccc} Irr(A) & \to & Irr(B) \\ V_i & \mapsto & U_i = Hom_A(V_i, V) \end{array}$$

Dualité de Schur-Weil ($\mathbb{K} = \mathbb{C}$) On considère V un $\mathbb{C}-$espace vectoriel de dimension finiel $< \infty$, $l \geq 1$, soit $\rho_k : S_k \to GL(V^{\otimes k})$ la représentation de S_k dans $V^{\otimes k}$ définie par

$$\omega.(v_1 \otimes ... \otimes v_k) = v_{\omega(1)} \otimes ... \otimes v_{\omega(k)} \ .$$

Soit également la représentation de $GL(V)$, $\varphi : GL(V) \to GL(V^{\otimes k})$ telle que

$$f.v_1 \otimes ... \otimes v_k = f(v_1) \otimes ... \otimes f(v_k) \ .$$

On note

$$A = \rho_k(\mathbb{C}S_k) \subset End_{\mathbb{C}}(V^{\otimes k})$$

et

$$B = \varphi(\mathbb{C}GL(V)) \subset End_{\mathbb{C}}(V^{\otimes k}) \ .$$

Ce sont deux sous algèbres.

Théorème 11.2 (Schur-Weil) *A, B sont semi-simples et $A = Com(B)$, $B = Com(A)$.*

12 Compléments

Soit $\mathbb{K}$ un corps algébriquement clos, A une $\mathbb{K}$-algèbre.

12.1 Caractères

Définition 12.1 (Caractère) *Soit U une représentation de A de dimension finie. Le **caractère** de U est la forme linéaire $ch_V \in A^*$ définie par $ch_V(a) = tr_V(\rho_V(a))$,*

Proposition 12.1 *i) $ch_V(ab) = ch_V(ba)$*
ii) $ch_V(1) = \dim V$
iii) Si $U \subset V$ sous module, alors $ch_V(a) = ch_U(a) + ch_{V/U}(a)$, $\forall a \in A$

Lemme 12.1 *Soient $V_1, ..., V_r$ des représentations de dimension finie non isomorphes. Alors, leurs caractères sont linéairement indépendants. Soit $V = V_1 \oplus ... \oplus V_r$ une représentation semi-simple de A. $\rho_V(A) = \oplus End_{\mathbb{K}}(V_i) \subset End_{\mathbb{K}}(V)$ (Lemme de Schur) est une algèbre semi-simple. Alors, $\forall i$, $\exists a_i \in A$, tel que $\rho_V(a_i) = (0, ..., 0, Id_{V_i}, 0..., 0)$.*

Corollaire 12.1 *Si A est semi-simple, alors deux représentations sont isomorphes si et seulement si elles ont même caractère.*

12.2 Théorème de Jordan-Hölder

Définition 12.2 (Série de composition) *Soit V un A-module de dimension finie. Une **série de composition** de V est une suite de sous $A-$modules*

$$0 = V_0 \subset V_1 \subset ... \subset V_r = V$$

telle que $\forall i$, $W_i = V_i/V_{i-1}$ est un $A-$module simple.

Définition 12.3 (Semi-simplifié) *Sous les hypothèses précédentes, on appelle **semi-simplifié** de V le $A-$module $V_{ss} = \oplus W_i$*

Théorème 12.1 (Jordan-Hölder, Krullschmidt) *Soit V un $A-$module de dimension finie, les facteurs simples d'une série de composition de V sont uniques à isomorphismes près et à ordre près.*

13 Introduction à la géométrie algébrique

13.1 Algèbre commutative

Définition 13.1 (Radical de Jacobson) *Soit A un anneau commutatif unitaire. le radical de Jacobson de A est*

$$rad(A) = \{x \in A,\ 1 + ax \text{ est inversible } \forall a \in A\}\ .$$

Lemme 13.1 *i) $Rad(A)$ est un idéal de A, et $1 + Rad(A) \subset A^*$. Par ailleurs, $Rad(A)$ est le plus grand idéal vérifiant cette propriété.*

ii) $Rad(A)$ est l'intersection de tous les idéaux maximaux.

Définition 13.2 (Definition) *Soit $I \subset A$ idéal, la racine (ou le radical) de I est $\sqrt{I} = \{a \in A \mid \exists n \geq 1, a^n \in I\}$. I est dit radical si $\sqrt{I} = I$*

Proposition 13.1 *i) $\sqrt{I}$ est un idéal, c'est le plus petit radical contenant I. Tout idéal premier est radical*

ii) $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$

iii) $\sqrt{I}$ est l'intersection de tous les idéaux premiers contenant I

13.2 Lemme de Nakayama

Théorème 13.1 (Cayleigh-Hamilton) *Soit M un $A-$module de type fini, soit $u \in End_A(M)$, il existe un polynome unitaire qui annule u.*

Corollaire 13.1 *Soit M un $A-$module de type fini.*

i) Tout endomorphisme surjectif de M est injectif.

ii) Si M est libre de rang n, toute famille génératrice de n éléments est une base.

Corollaire 13.2 *Soit M un $A-$module de type fini, $I \subset A$ idéal tel que $IM = M$, alors, $\exists x \in I,\ (1 - x)M = 0$.*

Lemme 13.2 (Nakayama) *Soit $I \subset A$ un idéal contenu dans $Rad(A)$, M un $A-$module de type fini.*

i) $IM = M \Rightarrow M = 0$

ii) Si $m_1, ..., m_n \in M$ sont tels que $m_1, ..., m_n$ engendrent M/IM comme A/I-module, alors $m_1, ..., m_n$ engendrent M comme $A-$module.

14 Normalisation

14.1 Extensions entières

Soit A un anneau commutatif unitaire, B une $A-$algèbre.

Définition 14.1 (finitude, élément entier) *a) B est **de type fini** (comme $A-$algèbre) si il existe un nombre fini d'éléments de B, $x_1...x_n$, telle que B est engendrée (comme A-algèbre), par $x_1...x_n$, i.e*

$$\exists \begin{array}{ccc} A[X_1...X_n] & \to & B \\ X_i & \mapsto & x_i \end{array}$$

surjective.

*b) B est **finie** si et seulement si B est engendrée par un nombre fini d'éléments comme $A-$module, i.e.*

$$\exists \begin{array}{ccc} A^{\oplus n} & \to & B \\ (0, ..., 0, 1, 0, ..., 0) & \mapsto & x_i \end{array}$$

*c) Un élément $x \in B$, x est dit **entier** sur A s'il est annulé par un polynôme unitaire à coefficients dans A*

d) La $A-$algèbre B est entière sur A si tout élément de B est entier sur A.

e) B est une extension entière de A si c'est une $A-$algèbre entière contenant A, i.e. $\begin{array}{ccc} A & \to & B \\ x & \mapsto & x1_B \end{array}$ est injective.

Proposition 14.1 *$A \subset B$ extension d'anneaux, $x \in B$, les propriétés suivantes sont équivalentes :*

i) x est entier sur A

ii) $A[x]$, sous algèbre de B engendrée par x, est une $A-$algèbre finie.

iii) $\exists A'$ *une* $A-$*algèbre finie tel que* $A \subset A[x] \subset A' \subset B$

Corollaire 14.1 *Toute extension finie* $A \subset B$ *est entière.*

Proposition 14.2 $A \hookrightarrow B \hookrightarrow C$ *morphismes injectifs d'anneaux.*

i) $A \subset B$, $B \subset C$ *finies* $\Rightarrow A \subset C$ *finie.*

ii) $y_1...y_n \in B$ *entiers sur* $A \Rightarrow A[y_1...y_n]$ *finie sur* A.

iii) $A \subset B$, $B \subset C$ *entières* $\Rightarrow A \subset C$ *entière.*

Définition 14.2 (Clôture entière) *Soit* $A \subset B$ *une extension d'anneaux. La clôture entière de* A *dans* B *est l'ensemble* $\widetilde{A}$ *des éléments de* B *entiers sur* A. *A est intégralement clos dans B si $A = \widetilde{A}$. Si A est intègre, on dit que A est intégralement clos (ou normal), si A est intégralement clos dans son corps des fractions.*

Lemme 14.1 *i)* $\widetilde{A} \subset B$ *est une sous* $A-$*algèbre*

ii) $A \subset \widetilde{A}$ *extension entière*

iii) $\widetilde{\widetilde{A}} = \widetilde{A}$

Proposition 14.3 *Soit* $A \subset B$ *une extension,* $P \subset A[X]$ *polynôme unitaire. Si* $P = QR$, Q, $R \in B[X]$ *unitaires, alors les coefficents de Q et R sont entiers sur A.*

Corollaire 14.2 (Lemme de Gauss) *Soit A intégralement clos (A intègre). Si* $P \in A[X]$, $P = QR$, Q *et* R *unitaires à coefficients dans* $Frac(A)$. *Alors, Q et R sont à coefficients dans A.*

Lemme 14.2 *Un anneau factoriel est intégralement clos.*

Proposition 14.4 A *normal* $\Rightarrow A[X]$ *normal.*

Définition 14.3 (Elements algébriquements liés) *i)* $a_1, ..., a_n \in A$ *sont dits* ***algébriquement liés*** *(sur* $\mathbb{K}$*) si* $\exists P \in \mathbb{K}[X_1...X_n]$ *tel que* $P(a_1...a_n) = 0$, *et* ***algébriquement indépendants*** *sinon.*

ii) A est une extension algébrique pure de $\mathbb{K}$ *si* $A = \mathbb{K}[x_1...x_n]$, *les* x_i *sont algébriqueent indépendants de A dans* $\mathbb{K}$.

Théorème 14.1 (Normalisation de Noëther) *Soit A une* $\mathbb{K}$*-algèbre de type fini. Alors, il existe* $y_1...y_n \in A$ *algébriquement indépendants sur* $\mathbb{K}$ *tels que A est une extension finie de* $\mathbb{K}[y_1...y_n]$.

Lemme 14.3 *Soit A une* $\mathbb{K}$ *algèbre de type fini engendrée par* $x_1, ..., x_n$ *algébriquement liés. Alors, il existe* $x'_1, ..., x'_{n-1} \in A$ *tels que* x_n *soit entier sur* $A[x'_1, ..., x'_{n-1}]$, *et* $A = A'[x_n]$, *où* $A' = [x'_1, ..., x'_{n-1}]$.

Lemme 14.4 *Soit* $A \subset B$ *une extension entière d'anneaux intègres. Alors*

$$A \text{ corps } \Leftrightarrow B \text{ corps } .$$

Théorème 14.2 (Hilbert) *Soit k un corps,* $k \subset \mathbb{K}$ *une* $k-$*algèbre de type fini. Supposons que* $\mathbb{K}$ *est un corps, alors* $k \subset \mathbb{K}$ *est une extension entière.*

Corollaire 14.3 *Supposons* $\mathbb{K} = \overline{\mathbb{K}}$. *Alors, les idéaux maximaux de* $\mathbb{K}[X_1, ..., X_n]$ *sont de codimension 1 et sont en bijection avec les points de* $\mathbb{K}^n$, *i.e. ils sont de la forme* $m_x = (X_1 - x_1, ..., X_n - x_n)$, *où* $x = (x_1, ..., x_n) \in \mathbb{K}^n$.

15 Variétés algébriques affines

Définition 15.1 (partie algébrique, lieu d'annulation)

1. *Une partie $S \subset \mathbb{K}^n$ est algébrique s'il existe une famille de polynômes $(P_i)_{i\in I} \in \mathbb{K}[X_1, ..., X_n]^I$, telle que*

$$S = \{x \in \mathbb{K}^n \mid P_i(x_1, ..., x_n) = 0 \ \forall i \in I\}$$

2. *Si $J \in \mathbb{K}[X_1, ..., X_n]$ est un idéal, on définit son* ***lieu d'annulation*** *dans $\mathbb{K}^n$ est l'ensemble algébrique*

$$V(J) = \{x \in \mathbb{K}^n \mid P(x_1, ..., x_n) = 0 \ \forall P \in J\}$$

3. *Si $X \subset \mathbb{K}^n$, on lui associe l'idéal*

$$I(X) = \{P \in \mathbb{K}[X_1, ..., X_n] \mid P(x) = 0 \ \forall x \in X\}$$

Théorème 15.1 (Hilbert) *Soit $\overline{\mathbb{K}} = \mathbb{K}$, alors $I(V(J)) = \sqrt{J}$.*

Lemme 15.1 *Un système d'équations algébriques*

$$(J) \begin{cases} G_1(x_1, ..., x_n) = 0 \\ \vdots \\ G_r(x_1, ..., x_n) = 0 \end{cases}$$

à coefficients dans $\mathbb{K} = \overline{\mathbb{K}}$ n'a pas de solutions dans $\mathbb{K}^n$ si et seulement si $\exists M_1, ..., M_r \in \mathbb{K}[X_1, ..., X_n]$ tels que

$$\sum_{i=1}^{r} M_i G_i = 1 \ .$$

Définition 15.2 (Espace noetherien) *Un espace topologique est* ***noetherien*** *si toute suite d'ouverts $U_0 \subset U_1 \subset ...$ est stationnaire.*

Lemme 15.2 *L'espace $(\mathbb{K}^n, Zariski)$ est noetherien.*

Définition 15.3 (Composante irréductible) *Une* ***composante irréductible*** *d'un espace topologique est une partie irréductible maximale.*

Lemme 15.3 *Soit X un espace topologique.*

1. *Les composantes irréductibles de X sont fermées, X est leur réunion.*
2. *Si $X = F_1 \cup ... \cup F_n$, F_i fermée irréductible, $F_i \not\subseteq F_j$, $i \neq j$, alors les F_i sont les composantes irréductibles de X.*
3. *X noetherien $\Rightarrow$ X n'a qu'un nombre fini de composantes irréductibles.*

Corollaire 15.1 *Tout idéal radical de $\mathbb{K}[X_1, ..., X_n]$ est intersection d'un nombre fini d'idéaux premiers. (décomposition primaire)*

Définition 15.4 (Dimension) *1. La dimension d'un espace topologique Y est le sup des longueurs l des chaînes $F_l \subsetneq ... \subsetneq F_0$ de fermés irréductibles de Y.*

2. *La dimension de Krull d'un anneau A est le sup des longueurs l de chaînes d'idéaux premiers $P_l \supsetneq P_{l-1} \supsetneq ... \supsetneq P_0$.*

16 Localisation

Définition 16.1 (Localisé) *Soit A un anneau, et S une partie multiplicative de A. Sur $A \times S$, on définit la relation d'équivalence*

$$(a, s) \sim (b, t) \ \Leftrightarrow \ r(at - bs) = 0 \ .$$

On note $A_S = \{\frac{a}{s} \mid a \in A, \ s \in S\}$. A_S est appellé ***localisé*** *de A.*

Lemme 16.1 *1. $\frac{a}{s}, \frac{b}{t} \in A_S$, on a $\frac{a}{s} + \frac{b}{t} = \frac{at+bs}{st}$ et $\frac{a}{s}.\frac{b}{t} = \frac{ab}{st}$ et ces définitions sont indépendants du choix des représentants.*

2. $+, .$ *munissent* A_S *d'une structure d'anneau.*

3. $$\begin{array}{rccc} can & : & A & \to & A_S \\ & & a & \mapsto & \frac{a}{1} \end{array}$$
est un morphisme d'anneaux canonique, vérifiant $can(S) \subset A_S^*$, *et est universel pour cette propriété : pour tout* $\phi : A \to B, \phi(S) \subset B^*$, *on aie un diagramme commutatif* $\phi = can \circ f$.

4. $Ker(can) = \{a \in A \mid \exists s \in S,\ as = 0\}$.

Lemme 16.2 *1.*
$$\begin{array}{ccc} spec(A_S) & \to & spec(A) \\ p & \mapsto & can^{-1}(p) \end{array}$$
est une injection d'image $\{p \in spec(A), p \cap S = \emptyset\}$.

2. $p \subset A$ *idéal, on a* p *premier* $\Leftrightarrow S = A - p$ *partie multiplicative.*

Lemme 16.3 *1.* $\frac{m}{s}, \frac{n}{t} \in M_S$, $\frac{a}{r} \in A_S$ *on a* $\frac{m}{s} + \frac{n}{t} = \frac{mt+ns}{st}$ *et* $\frac{a}{r}.\frac{m}{s} = \frac{am}{rs}$ *et ces définitions sont indépendants du choix des représentants.*

2. $+, .$ *munissent* M_S *d'une structure de* A_S*-module.*

3. $$\begin{array}{rccc} can & : & M & \to & M_S \\ & & m & \mapsto & \frac{m}{1} \end{array}$$
est un morphisme de $A-$*modules, où l'action des éléments de* S *est inversible, et est universel pour cette propriété.*

4. $M_S \simeq A_S \otimes_A M$ *comme* A_S *module.*

5. $Ker(M \to M_S) = \{m \in M \mid \exists s \in S,\ sm = 0\}$.

Lemme 16.4 *Si* $0 \to L \to M \to N \to 0$ *une suite exacte de* A*-modules, alors* $0 \to L_S \to M_S \to N_S \to 0$ *est une suite exacte de* A_S*-modules. Le foncteur de localisation peut être vu comme un foncteur (induction de* A *à* A_S*)*
$$\begin{array}{ccc} A-modules & \to & A_S-modules \\ M & \mapsto & A_S \otimes_A M \end{array}$$
exact à droite. ($\Rightarrow L_S \to M_S \to N_S \to 0$ *exacte.)*

Théorème 16.1 (Cohen-Seidenberg) *Soit* $A \subset B$ *extension finie d'anneaux. (*$\Leftrightarrow$ B *un* $A-$*module de type fini.) Alors* $dim A = dim B$.

Théorème 16.2 *1.* $dim\mathbb{K}[X_1, ..., X_n] = n$.

2. *Si* $\mathbb{K} = \overline{\mathbb{K}}$, $dim\mathbb{K}^n = n$.

Théorème 16.3 (Cohen-Seidenberg) *Soit* $A \subset B$ *une extension finie d'anneaux (i.e.* B *est un* $A-$*module de type fini). Alors,* $dim(A) = dim(B)$

Corollaire 16.1 $\mathbb{K}$ *corps* $\Rightarrow dim(\mathbb{K}[X_1, ..., X_n]) = n$

Lemme 16.5 *Soit Soit* $A \subset B$ *une extension finie d'anneaux.*

i) $\forall p \in spec(A)$, $\exists p' \in spec(B)$, $p' \cap A = p$.

ii) $\forall p' \subset p'' \in spec(B)$ *tel que* $p' \cap A = p'' \cap B$, *on a* $p' = p''$.

iii) $p' \in spec(B)$ *maximal* $\Leftrightarrow p' \cap A$ *maximal dans* A .

Lemme 16.6 *i) Si* $p'_0 \subsetneq p'_1 \subsetneq ... \subsetneq p'_s$ *est une chaîne d'idéaux premiers de* B. *Alors, les* $p_i = p'_i \cap A$ *forment une chaîne strictement croissante d'idéaux premiers de* A.

ii) Si $p_0 \subsetneq p_1 \subsetneq ... \subsetneq p_l$ *est une chaîne d'idéaux premiers de* A. *Alors, il existe une chaîne Si* $p'_0 \subsetneq p'_1 \subsetneq ... \subsetneq p'_l$ *d'idéaux premiers de* B *telle que* $p_i = A \cap p'_i$ $\forall i$.

Définition 16.2 (Soit $\mathbb{K} \subset \mathbb{K}(B) \subset \mathbb{L}$ **une extension de corps. Alors,** $B \subset \mathbb{L}$
Les éléments de B *sont algébriquement indépendants sur* $\mathbb{K}$.

ii) $\mathbb{L}$ *est algébrique sur* $\mathbb{K}(B)$.

Lemme-Définition 16.1 (Degré de transcendance) *Soit* $\mathbb{K} \subset \mathbb{L}$ *une extension de corps telle que* $\mathbb{L} = \mathbb{K}(x_1, ..., x_n)$. *Alors :*

i) $\mathbb{L}$ *admet une base de transcendance sur* $\mathbb{K}$ *et elle est finie.*

ii) Deux bases de transcendance de $\mathbb{L}$ *ont même cardinal, fini, appellé degré de transcendance de* $\mathbb{K} \subset \mathbb{L}$.

Proposition 16.1 *Soit $\mathbb{K}$ un corps, A une $\mathbb{K}-$algèbre intègre de type fini, alors $dim(A) = degtr_{\mathbb{K}}(Frac(A))$*

Définition 16.3 (Variété algébrique) *Soit $\mathbb{K}$ un corps algébriquement clos.*

*i) Une **variété (algébrique) affine** est un sous ensemble $X \subset A_n$ (où $A_n = \mathbb{K}^n$ vu comme variété affine).*

*ii) Une **fonction (polynomiale)** sur X est la restriction d'un polynôme de $\mathbb{K}[X_1, ..., X_n]$ à X, l'algèbre des fonctions sur X est donc $A(X) = \mathbb{K}[X_1, ..., X_n]/I(X)$.*

*iii) Un **morphisme de variétés affines** est une application $f : X \to Y$, $f = f_1...f_m$, $f_i X \to A_i$, où chaque f_i est uen fonction polynomiale sur X.*

Définition 16.4 (comorphisme) *Le **comorphisme** d'un morphisme de variétés affines, $f : X \to Y$ est le morphisme de $A-$algèbres $f^* : \begin{array}{ccc} A(Y) & \to & A(X) \\ g & \mapsto & g \circ f \end{array}$. (cf : foncteur contravariant sur la catégorie des variétés affines sur $\mathbb{K}$)*