Outils Algébriques pour la Théorie des Modèles des Corps

1ère Partie :

Théorème de Coleman

Extension séparable

On considère une extension E/F algébrique. On s'intéresse ici à, étant donné un plongement $\tau : F \to L$ un corps L algébriquement clos, le nombre d'extensions de τ de F à E. En utilisant le fait que :

" $$\begin{array}{c} E'=E'^{alg} \\ | \\ F \end{array} \xrightarrow{\tau} L \quad \& \quad \begin{array}{c} L \\ | \\ \tau F \end{array} \text{ est algébrique} \Longrightarrow \tau \text{ s'étend en un isomorphisme de } L'=L$$ "

(une cté de la clôture algébrique) on a alors si on suppose quitte à restreindre L pour que $L-\tau F$ soit algébrique que

Fait : Le nombre d'extensions de $\tau : F \to L$ à $\tilde{\tau} : E \to L$ ne dépend que de l'extension E/F et on le note $[E:F]_s$ le degré séparable.

Exemple : Pour une extension monogène algébrique $k(x)/k$ et $\tau : k \to L = L^{alg}$, si $P = \mathrm{irr}(x,k,X)$ on voit que le nombre d'extensions de τ à $k(x)$ est égal au nombre de racines distinctes de P^τ dans L, car si β est un zéro dans L de P^τ, l'appli qui à $x = f(x) \in k(x)$ associe $f^\tau(\beta)$ ne dépend pas du f choisi et définit un plongement $\tilde{\tau} : k(x) \to L$.
On voit ici que si $\mathrm{irr}(x,k,X)$ n'a que des racines simples alors le nombre de τ à $k(x)$ est égal au degré de P^τ ie est égale au degré de $\mathrm{irr}(x,k,X)$,
ie $$[k(x):k]_s = [k(x):k]$$
Sinon $[k(x):k]_s \leq [k(x):k]$

En fait on peut aisément généraliser le résultat précédent pour les extensions algébriques :

Théorème: Si $E \supseteq F \supseteq k$ est une tour d'extensions algébriques alors

- $[E:k]_s = [E:F]_s \, [F:k]_s$

De plus si E est finie sur k alors
$$[E:k]_s \leq [E:k]$$
Le degré séparable est au plus égal au degré

On a que $[E:F] = [E:F]_s$ ssi cette égalité est vraie pour tout $[E:K]$, $[K:F]$ avec $\begin{matrix} E \\ | \\ K \\ | \\ F \end{matrix}$.

On peut montrer que $[E:F]_s$ divise $[E:F]$ et on note $[E:F]_i$ tel que $[E:F]_s \cdot [E:F]_i = [E:F]$

On a alors que $[E:F]_i$ est multiplicatif.

- Une extension $\begin{matrix} E \\ | \\ F \end{matrix}$ finie est dite __séparable__ si $[E:F]_s = [E:F]$.
- Un élément $\alpha \in F^{alg}$ est __séparable sur F__ si $F(\alpha):F$ __est séparable__.
- Un polynôme $\in F[X]$ est dit __séparable__ ~~(sur F)~~ s'il n'a pas de __racine multiple__.

__Exemple:__ Avec l'exemple précédent, si $Irr(\alpha, k, X)$ n'a que des racines simples, ie est séparable alors $[k(\alpha):k]_s$ est égal à $[k(\alpha):k]$ donc $k(\alpha) - k$ est séparable et l'élément α est séparable donc

α séparable (sur k) ssi $irr(\alpha, k, X)$ est séparable ssi $k(\alpha):k$ est séparable.

__Remarque:__ La notion dépend de k.

Pour être un peu plus précis :

<u>Proposition</u> : Si $\alpha \in k^{alg}$ est algébrique sur k, et soit $f(X) = \min(\alpha, k, X)$. Alors

si $\underline{\operatorname{car} k = 0}$: alors f est séparable.

si $\underline{\operatorname{car} k = p > 0}$: il existe $\mu \geq 0$ tel que toutes les racines de f ont multiplicité p^μ, de plus

$$[k(\alpha) : k] = p^\mu [k(\alpha) : k]_s$$

et α^{p^μ} est séparable sur k.

On a donc en caractéristique 0 que toute extension finie est séparable, toute extension monogène algébrique est séparable.

$[E:F]_i = \dfrac{[E:F]}{[E:F]_s}$ est <u>le degré d'inséparabilité</u>.

On a $$[E:F] = [E:F]_i \cdot [E:F]_s$$

et une extension est séparable ssi $[E:F]_i = 1$.

On a enfin un théorème important, généralisation de l'exemple précédent :

<u>Théorème</u> : Si $E-F$ est une <u>extension finie</u> alors E est une extension séparable ssi tout élément de E est séparable sur F.

<u>Preuve</u> : La séparabilité d'un $\alpha \in E$ se vérifie par $[F(\alpha):F]_s$ ou par $[F(\alpha):F]_i$: $[E:F]_i = [E:F(\alpha)]_i \cdot [F(\alpha):F]_i$ comme $[E:F]_i = 1$ on a $[F(\alpha):F]_i = 1$.

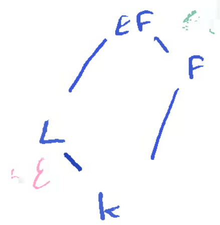
On le montre par induction ensuite réciproquement $\boxtimes$

On définit une extension <u>séparable</u> E/F <u>algébrique</u> si $\forall \alpha_1 \ldots \alpha_n \in E$, $F(\alpha_1 \ldots \alpha_n) : F$ est séparable.

• Classe distinguée : Une classe $\mathcal{E}$ d'extensions $L:k$ est dite distinguée si elle vérifie les 3 propriétés :

(i) $\begin{array}{c} L \\ | \\ F \\ | \\ k \end{array}$ alors $\begin{array}{c} L \\ | \\ k \end{array} \in \mathcal{E}$ ssi $\begin{array}{c} F \\ | \\ k \end{array}$ et $\begin{array}{c} L \\ | \\ F \end{array} \in \mathcal{E}$

(ii) $L - k \in \mathcal{E}$ et $F - k$ $\Rightarrow$ $\begin{array}{c} LF \\ | \\ F \end{array} \in \mathcal{E}$



(iii) $k \subseteq F$ et $k \subseteq L \in \mathcal{E}$ alors $k \subseteq FL \in \mathcal{E}$

On a que les extensions algébriques d'un corps, et les extensions finies d'un corps sont deux classes distinguées d'extensions.

Enfin les extensions séparables forment une classe distinguée.

• Théorème de l'élément primitif : Si $E - k$ est une extension finie alors

$\exists\, x \in E,\ E = k(x)$ ssi il n'existe qu'un nombre fini de un F où $\begin{array}{c} E \\ | \\ F \\ | \\ k \end{array}$

Si $E - k$ est séparable, alors les deux conditions sont vraies :

(1) Toute extension finie séparable est monogène

(2) le nombre de corps intermédiaires est fini ($[E:k]$ fini).

• Clôture séparable :

Soit L/k une extension. On appelle clôture séparable de k dans L le corps $\{ a \in L,\ a \text{ est séparable sur } k \}$.
C'est bien un corps, on le note $k^{sep L}$ et on a que $k^{sep L}/k$ est une extension séparable. On pourrait poser $k^{sep} = k^{sep(k^{alg})}$ et ce serait bien une extension séparable maximale. Enfin $[k^{sep L} : k] = [L:k]_s$.

• Notion d'élément, extension purement inséparable

Comme dans le cadre de la caractéristique 0, toutes les extensions sont séparables. Un élément peut ne pas être séparable si son irréductible n'a qu'une seule racine. On dit alors ce cas que l'élément est purement inséparable. Les exemples de tels éléments sont en caractéristique $p > 0$, par exemple on prend un corps F, et $\alpha \in F^{alg}$ tel que $\alpha^p = a \in F$ et $\alpha \notin F$, il est irréductible donc une racine du polynôme $X^p - a = 0$, qui est irréductible dans F si a n'est pas une racine p-ième.
On a alors $\operatorname{irr}(\alpha, F, X) = X^p - a = X^p - \alpha^p = (X-\alpha)^p$
et alors $\operatorname{irr}(\alpha, F, X)$ est irréductible sur F mais a une racine multiple dans $F(\alpha)$. L'élément α est donc purement inséparable.
Notez que $\sigma : F \to L^{= F^{alg}}$ n'a qu'une seule extension à $F(\alpha)$, exactement parce que le polynôme n'a qu'une racine, et donc $[F(\alpha) : F]_s = 1$.
Notez que $\alpha \in F$ est séparable et purement inséparable sur F et si α est séparable et purement inséparable sur F alors $\alpha \in F$.

Noter qu'un élément séparable ou inséparable α sur F est une notion ne concernant qu'un élément algébrique sur F.

Proposition : LASSE E/k extension algébrique.

- $[E:k]_s = 1$
- Tout élément $\alpha \in E$ est purement inséparable sur k.
- $\forall \alpha \in E$ on a $\mathrm{irr}(\alpha, k, X) = X^{p^n} - a$ avec $a \in k$
- $E = k(\{x_i\}_{i \in I})$ $\{x_i\}$ une base d'élément inséparables.

Noter que les extensions vérifiant les conditions sont appelées des <u>extensions purement inséparables</u>, elles forment une classe distinguée au sens de Lang.

On a déjà vu précédemment que <u>α est purement inséparable sur F</u> ssi <u>$\exists n$ tq $\alpha^{p^n} \in F$</u> ssi $X^{p^m} - \alpha^{p^m} \in F[X]$ est $\mathrm{irr}(\alpha, F, X)$ (car $X^p - x^{p^n}$ est irréductible par récurrence)

Proposition :
- Si K/F est purement inséparable, alors $\mathrm{Gal}(K/F) = \{1\}$ de plus, K/F est normale.
- Si $F \subseteq K \subseteq L$ alors L/K et K/F pur. insép. ssi L/F pur. insép.

On appelle <u>clôture inséparable</u> de K/F (ou de F dans K) l'ensemble $\{a \in K,\ a$ est pur. insép. sur $F\}$. C'est un corps et c'est une extension purement inséparable de F. On la note F^i.

On considère donc $F \subseteq K$ et on a :

$$\begin{tikzcd}
 & K \arrow[dl, dash, "\text{insep}"'] \arrow[dr, dash, "?"] & \\
F^s \arrow[dr, dash, "\text{sep}"'] & & F^i \arrow[dl, dash, "\text{insep.}"] \\
 & F &
\end{tikzcd}$$

La propriété suivante nous dit que (lorsque K/F est algébrique) alors $K - F^s$ est inséparable.

Proposition : On suppose que k/F est une extension.

$\boxed{\begin{array}{l} \text{Alors } F^i \cap F^s = F \quad (F^i \text{ et } F^s \text{ sont les clôtures inséparable et séparable}) \\ \text{et si } k/F \text{ est algébrique, alors } k/F^s \text{ est purement inséparable} \end{array}}$

Cela signifie que si l'on prend d'une part la clôture séparable, puis la clôture inséparable, on retombe sur k, i.e.

$$\begin{tikzcd} k \arrow[d, dash, "\text{inséparable}"] \\ F^s \arrow[d, dash, "\text{séparable}"] \\ F \end{tikzcd}$$

En particulier $(F^s)^i = k$.

En revanche on ne sait pas pour $\begin{array}{c} k \\ | \\ F^i \end{array}$. On retiendra ce que l'on sait par

$$\begin{tikzcd} & k \arrow[dl, dash, "\text{insép}"'] \arrow[dr, dash, "?"] & \\ F^s \arrow[dr, dash, "\text{sép}"'] & & F^i \arrow[dl, dash, "\text{insép}"] \\ & F & \end{tikzcd}$$

Exemple : (Extension ni séparable ni purement inséparable).

$\boxed{\begin{array}{l} \text{Si } F = \mathbb{F}_2(x) \text{ et } k = F(x^{1/6}) = F(\sqrt{x}, \sqrt[3]{x}) \\ \text{Mais : } \bullet \ \sqrt{x} \text{ est purement inséparable sur } F \text{ car } \sqrt{x} \text{ annule } X^2 - x \text{ et } X^2 - x \text{ irréd sur } F \\ \quad \bullet \ \sqrt[3]{x} \text{ est séparable sur } F : \text{c'est la racine de } X^3 - x \text{ et on vérifie que } \sqrt[3]{x} \text{ n'est pas racine de } \frac{X^3 - x}{X - \sqrt[3]{x}}. \\ \text{Donc } k \text{ contient des éléments séparables et inséparables} \end{array}}$

Remarquons que $k^{1/p^\infty} = \bigcup \{x \in k^{alg} \mid \exists n, x^{p^n} \in k\} = \bigcap_{n \geq 0} k^{p^n}$ est une extension maximale contenant tous les éléments purement inséparables sur k, on rejette tous les cas pathologiques. Les éléments algébriques sur k^{1/p^∞} sont par définition séparables sur k^{1/p^∞}. $k^{1/p^\infty}/k$ est la plus grande extension purement inséparable de k, c'est un corps parfait.

Enfin un théorème en lien avec la théorie de Galois

Théorème : Si K est une extension normale de F

Alors
- F^s / F est Galois
- $F^i = F^{Gal(K/F)}$
- $Gal(F^s/F) \cong Gal(K/F^i)$
- K/F^i est Galois

De plus $K = (F^s)(F^i)$

Autrement dit :

$$\begin{tikzcd}
 & K = F^s F^i \arrow[dl, dash, "\text{insep}"'] \arrow[dr, dash, "\text{sep}", "Gal"'] & \\
F^s \arrow[dr, dash, "\text{sep}"', "Gal"] & & F^i \arrow[dl, dash, "\text{insep}"] \\
 & F &
\end{tikzcd}$$

En particulier on a que K/F^i est séparable dans ce cas.

Important : Notez que dans le cadre de 2 ext formes F_1/K séparable et F_2/K purement inséparable, on a

$$\begin{tikzcd}
 & F_1F_2 \arrow[dl, dash, "\text{insep}"'] \arrow[dr, dash, "\text{sep}"] & \\
F_1 \arrow[dr, dash, "\text{sep}"'] & & F_2 \arrow[dl, dash, "\text{insep}"] \\
 & K &
\end{tikzcd}$$

par les propriétés sur les degrés :

$[F_1F_2 : F_2]_i \cdot [F_2 : K]_i = [F_1F_2 : K]_i$.

Théorie de Galois

On introduit ici des rappels de théorie de Galois. On se réfère à la feuille extension séparable.

• Extension normale

On considère ici principalement des extensions de corps qui sont algébriques. (i.e tout élément du gros corps est algébrique sur le petit, en particulier des extensions finies).

Une extension $\mathbb{K} \overset{alg}{-} k$ est dite <u>normale</u> si l'une des conditions équivalentes suivantes est vérifiée :

(i) Tout polynôme irréductible $p \in k[X]$ est scindé dans $\mathbb{K}$ (s'il a une racine dans $\mathbb{K}$).

(ii) Tout k-plongement $\sigma : \mathbb{K} \longrightarrow \bar{k}^{alg}$ est un automorphisme de $\mathbb{K}$ (i.e $\sigma\mathbb{K} = \mathbb{K}$).

(iii) $\mathbb{K}$ est le corps de décomposition d'une famille de polynômes de $k[X]$.

Exemple : • L'extension $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ est normale car $-\sqrt{2} \in \mathbb{Q}(\sqrt{2})$.

• Toute extension de degré 2 est normale pour la même raison.

• L'extension $\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}$ n'est pas normale car $X^4 - 2 = (X^2 - \sqrt{2})(X^2 + \sqrt{2})$ a des racines complexes qui ne sont donc pas dans $\mathbb{Q}(\sqrt[4]{2})$.

La classe des extensions normales n'est pas distinguée, mais :

Théorème : • $\begin{array}{c} K \\ | \\ E \\ | \\ k \end{array}$ si $K : k$ est normale alors $K : E$ est normale.

• si $K_1 : k$, $K_2 : k$ sont normales, alors aussi :

$\begin{array}{c} K_1 \cap K_2 \\ | \\ k \end{array}$ et $\begin{array}{c} K_1 K_2 \\ | \\ k \end{array}$

Étant donné un corps $L-k$, extension finie, on peut construire $\tilde{L}-L-k$ tel que $\tilde{L}-k$ est normale (remarque que $\tilde{L}-k$ est aussi normale) et $[\tilde{L}:k]$ fini. On appelle $\tilde{L}$ la clôture normale de $L-k$. (On la définit comme l'intersection de toutes les extensions normales de k qui contiennent L, sachant que cette famille est non vide, (contient k^{alg}))

⚠ remarque qu'un corps est normal sur lui-même (réductibilité si pas de racines).

- Si $L-k$ est une extension finie, et L^{nor} est la clôture normale, et $\sigma_1, \dots, \sigma_n$ sont les ~~...~~ plongements de L dans L^{alg} (fini car $L-k$ fini), On a alors que

$$L^{nor} = (\sigma_1 L) \dots (\sigma_n L) \quad (\text{composition}$$

De plus si $L-k$ est séparable alors $L^{nor}-k$ l'est aussi.
Remarque que ceci est vrai pour les extensions algébriques de degré infini, en prenant la composition infinie.

En particulier si x est algébrique sur k et si $\sigma_1 \dots \sigma_n$ sont les plongements $\underset{k}{k(x)} \xrightarrow{\sigma_i} k^{alg}$ alors

$$(k(x))^{nor} = (k(\sigma_i x))^{nor} = k(\sigma_1 x, \dots \sigma_n x)$$

- Corps parfait :

Un corps k est dit parfait si tout polynôme irréductible est séparable, i.e. n'a que des racines simples dans des extensions.

- Tout corps de caractéristique 0 est parfait.
- Un corps k de caractéristique $p>0$ est parfait ssi $k^p = k$ i.e. $k \vDash \forall x \exists y\ y^p = x$ (en particulier les $\mathbb{F}_p$ sont parfaits) car $\forall x \in \mathbb{F}_p\ x^p = x$.

Théorème : • Si k est parfait alors toute extension algébrique est séparable
• Si k est parfait, toute extension algébrique est aussi un corps parfait.

• **Extension de Galois**

Si G est un groupe d'automorphisme de K, alors K^G est le corps invariant par G, ie $K^G = \{x \in K,\ \sigma x = x\ \forall \sigma \in G\}$

C'est un corps et contient le sous corps premier.

Définition : Une extension $L - k$ est dite de Galois si elle est normale et séparable.

• Le groupe de Galois de $L - k$, $\mathrm{Gal}(L/k)$ est le groupe des automorphismes de L qui laissent k invariant.

• La clôture séparable de toute extension est une extension de Galois

Exemple : • La clôture normale d'une extension finie $L - k$, si k est parfait est normale et séparable donc de Galois,

• Toute extension normale d'un corps parfait est séparable donc de Galois

• Le corps $\mathbb{F}_3$ est parfait, $X^2 + 2$ est irréductible dans $\mathbb{F}_3$ par réduction, donc $\frac{\mathbb{F}_3[X]}{(X^2+2)} = \mathbb{F}_9$ est séparable et normale (car quadratique sur $\mathbb{F}_3$) et donc $\mathbb{F}_9 : \mathbb{F}_3$ est de Galois.

• Tout corps premier est parfait (si car $> 0 = p$, alors $\mathbb{F}_p$ vérifie $X^p - X = 0$ ie $x = x^p$).

Théorème de Correspondance de Galois

Soit $L - k$ une extension finie de Galois.

• Alors il existe une bijection entre

$$\left\{ K \text{ tels que } \begin{matrix} L \\ | \\ K \\ | \\ k \end{matrix} \right\} \longleftrightarrow \left\{ H \text{ tq } H \leq \mathrm{Gal}(L/k) \right\}$$

donnée par $K = L^H$. $\quad \begin{matrix} L \\ |\, m \\ K \\ | \\ k \end{matrix} \quad |H| = m$.

• $K = L^H$ est de Galois sur k ssi $H \trianglelefteq G$, et alors $[L:K] = |H|$

et dans ce cas $$\mathrm{Gal}(L/k)/H \simeq \mathrm{Gal}(K/k)$$

ie $$\frac{\mathrm{Gal}(L/k)}{\mathrm{Gal}(L/K)} \simeq \mathrm{Gal}(K/k)$$

Si $L - k$ est une extension de Galois alors

$$k = L^{Gal(L/k)}$$

De plus, tout corps intermédiaire : $L : K : k$, on a $L : K$ est séparable.

Enfin si $L - k$ est de Galois alors

$$[L : k] = Card\left(Gal(L/k)\right).$$

Une extension est cyclique si son groupe de Galois l'est.

Exemple : Soit $f \in k[X]$ tel que $f = (X - \alpha_1) \cdots (X - \alpha_n)$ dans une clôture algébrique.

On note $Gal(f/k)$ le groupe $Gal(k(\alpha_1 \ldots \alpha_n)/k)$ sachant que $k(\alpha_1, \ldots, \alpha_n)$ est normale, l'extension est de Galois si par exemple k est parfait.

Tout élément de $Gal(f/k)$ induit une permutation des racines mais toute permutation n'induit pas nécessairement un élément de $Gal(f/k)$ on a donc

$$Gal(f/k) \longrightarrow \mathfrak{S}_n$$

Remarquons que si $k(\alpha_1) : k$ est de galois,

$$[k(\alpha_1) : k] = n = \deg f = |Gal(f/k)|$$

pour f irréductible, ainsi si $n \neq n!$ le plongement précédent est strict.

Remarque : Si l'extension n'est pas de Galois on peut tout à fait avoir $Gal(f/k) \simeq \mathfrak{S}_n$. [cf exemple 2 p 139 LANG]

Exemple (Le polynôme $X^4 - 2$)

$f = X^4 - 2$ est irréductible sur $\mathbb{Q}$ (Eisenstein). Si α est une racine, alors $\pm\alpha$ et $\pm i\alpha$ sont les racines de f. On a de plus

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4 = \deg(\mathrm{irr}(\alpha, \mathbb{Q}, X) = f)$$

et si $K = \mathbb{Q}(\alpha, i)$, le corps de décomposition de f on a que

$$[\overset{K}{\overset{\shortparallel}{\mathbb{Q}(\alpha, i)}} : \mathbb{Q}] = 8 \quad \text{car} \quad \begin{tikzcd}[column sep=small] & \mathbb{Q}(i,\alpha) \arrow[dl, dash, "4"'] \arrow[dr, dash, "2"] & \\ \mathbb{Q}(i) \arrow[dr, dash, "2"'] & & \mathbb{Q}(\alpha) \arrow[dl, dash, "4"] \\ & \mathbb{Q} & \end{tikzcd}$$

Or $\mathbb{Q}$ est de car 0 donc parfait donc $K - \mathbb{Q}$ est séparable, de plus comme K est un corps de décomposition, $K - \mathbb{Q}$ est normale donc $K - \mathbb{Q}$ est de Galois, et on a

$$|\mathrm{Gal}(K/\mathbb{Q})| = 8$$

On a que $K - \mathbb{Q}(\alpha)$ est de degré 2 et de Galois donc il existe $\tau \in \mathrm{Gal}(K/\mathbb{Q}(\alpha))$ non trivial d'ordre 2 puisque $|\mathrm{Gal}(K/\mathbb{Q}(\alpha))| = 2$ donc $\tau(i) = -i$. On a donc $\mathrm{Gal}(K, \mathbb{Q}(\alpha)) = \langle 1, \tau \rangle$ $\tau^2 = 1$.

On détermine $\mathrm{Gal}(K/\mathbb{Q}(i))$: $K - \mathbb{Q}(i)$ est de Galois donc c'est un groupe d'ordre 4, par la classification des groupes d'ordre 4 il est soit d'exposant 2 soit cyclique. On a vérifié que $\alpha \overset{\sigma}{\longmapsto} i\alpha$ induit un élément de $\mathrm{Gal}(K/\mathbb{Q}(i))$ et $1, \sigma, \sigma^2, \sigma^3$ sont distincts donc $\mathrm{Gal}(K/\mathbb{Q}(i)) = \langle \sigma \rangle$ cyclique d'ordre 4, de plus $\sigma \neq \tau$ donc on a $|\langle \tau, \sigma \rangle| = 8$ et $\langle \tau, \sigma \rangle \subseteq \mathrm{Gal}(K/\mathbb{Q})$ donc on a égalité.

Remarquer que par le théorème de l'élément primitif, le théorème de Galois concerne que les extensions algébriques <u>monogènes</u>. (car Fini + séparable $\Rightarrow$ monogène).

Remarque sur l'intérêt des extensions séparables : Une extension séparable a un intérêt quant à la non dégénérescence de son groupe de Galois. En effet, en parlant d'une extension finie séparable, elle est monogène, donc par α et on peut décrire facilement les automorphismes car comme les éléments sont des $P(\alpha)$ il suffit de remplacer α par une autre racine de l'irréductible et si la racine est distincte on obtient un automorphisme distinct. L'intérêt est donc que si l'extension est séparable et que le corps est suffisamment gros pour contenir toutes les racines de l'irréductible (extension normale) alors le nombre d'autos différents est exactement le nombre de racines distinctes et dans le cas séparable le degré du minimal est donc le degré de l'extension.

Les éléments (algébriques) séparables sont donc les éléments non dégénérés et ce qui sont purement inséparables sont dégénérés mais n'apparaissent qu'en caractéristique positive et leur poly minimal est $Q(X^p)$.

Un polynôme irréductible quelconque P se décompose dans une extension algébrique $\Pi(X-\alpha_i)\Pi(X-\beta_i)$ où les α_i sont séparables, les β_i purement inséparables et donc le degré des racines de β_i est p^{n_i} il admet donc une écriture $P_1 \dots P_r (X^{p^{n_1}} - b_1) \dots (X^{p^{n_s}} - b_s)$ où les P_i sont séparables.

Les extensions L/K ~~dégén~~ Galoisiennes se reconnaissent donc :

- en car 0 : ce sont les extensions normales, i.e. closes par racines i.e. si $x \in L$ est racine d'un irréd P de $K[X]$ alors toutes les autres racines de P sont dans L.
- en car > 0 : elles doivent être normales et ne pas contenir de racine d'1 polynôme dégénéré : $X^{p^i} - a$. À moins que les racines de ces poly soient dans K i.e. que K soit clos par racines p-ièmes i.e. $K^p = K = \cap K^{p^i}$; dans ce cas les polys du type dégénéré $X^{p^i} - a$ sont en fait scindés sur K et donc non irréductibles sur K.

Théorie de Kummer

On étudie dans cette section les extensions dites de Kummer qui sont des extensions à première vue très particulières avec des hypothèses très restrictives mais on va voir qu'il s'y passe des choses très heureuses.

Une extension de Galois K/k est dite abélienne (respectivement d'exposant m) si son groupe de Galois G est abélien, respectivement d'exposant m.

On suppose que m est premier avec la caractéristique de k. On note μ_m le groupe multiplicatif des racines m-ièmes de l'unité. On a que si k contient une racine primitive m-ième de 1 (= générateur du groupe cyclique μ_m) alors $\mu_m \subseteq k$.

Remarquons que si $\operatorname{car} k \mid m$, μ_m n'est pas de cardinal m, il est dégénéré, si par exemple $\operatorname{car} k = p = m$, $\mu_m = \{1\}$ (unique solution du polynôme inséparable $X^p - 1$).

On considère à présent que k contient une racine primitive m-ième de l'unité avec $\operatorname{pgcd}(\operatorname{car} k, m) = 1$.

Alors si $a \in k$, on note $\alpha = a^{1/m}$ un choix d'une racine m-ième de a, or $k(\alpha)$ va contenir toutes les racines de a car $\beta = \sqrt[m]{a}$ ssi $\exists \zeta \in \mu_m,\ \beta = \zeta\alpha$.

et on a $X^m - a = \prod_{\zeta \in \mu_m} (X - \zeta\alpha)$

On peut donc sans ambiguïté parler de $k(\sqrt[m]{a})$.

Exemple : Ce n'est pas le cas si l'on n'a pas de racine primitive m-ième :

$X^3 - 2 = (X - \underbrace{\sqrt[3]{2}}_{\in \mathbb{R}})(X - j\sqrt[3]{2})(X - j^2\sqrt[3]{2})$ et

$\mathbb{Q}(\sqrt[3]{2}) \cap \mathbb{Q}(j\sqrt[3]{2}) = \mathbb{Q}$

On considère à présent le groupe multiplicatif $k^\times$ ainsi que $k^{\times m} \subseteq k^\times$ le sous groupe des puissances m-ième.

$$k^\times \trianglerighteq B \trianglerighteq k^{\times m}$$

On a $\forall\, a \in k^{\times m}$, $k(\sqrt[m]{a}) = k$.

On considère un groupe intermédiaire : B.

On a que si $a \in B \setminus k^{\times m}$, $k(\sqrt[m]{a}) \supsetneq k$: on note
$$k(B^{1/m}) = k(a^{1/m},\ a \in B).$$

En ayant choisi k avec m racines prim de 1, si $a \in B$
$X^m - a = \prod_{\xi \in \mu_m} (X - \xi\sqrt[m]{a})$ et donc $X^m - a$ est scindé sur $k(B^{1/m})$ et ce pour tout $a \in B$. De plus chacun des polynôme $X^m - a$ est séparable par l'équation précédente et parce que, comme $p \nmid m$, $|\mu_m| = m$, ie μ_m n'est pas dégénéré. On conclut que l'extension $k(B^{1/m})/k$ est galoisienne.

- $\mathrm{Gal}(k(B^{1/m})/k)$

La forme de $G = \mathrm{Gal}(k(B^{1/m})/k)$ est très particulière. Soient donc $\sigma \in G$ et $\alpha \in k(B^{1/m})$. Si $\alpha \in k^\times$ (ou $k^{\times m}$) on a $\sigma\alpha = \alpha$. Sinon, σ induit une permutation de racines, ie $\sigma\alpha$ est une racine de $X^m - \alpha^m = 0$ donc $\sigma\alpha = \xi_{\alpha,\sigma} \cdot \alpha$. Montrons que $\xi_{\alpha,\sigma} = \xi_\sigma$ ie que ξ ne dépend pas de α : on note $\xi_\sigma = \frac{\sigma\alpha}{\alpha}$. Alors si $\beta = \xi\alpha$, $\xi_\sigma = \frac{\sigma\beta}{\beta} = \frac{\sigma(\xi\cdot\alpha)}{\xi\cdot\alpha} = \frac{\sigma\alpha}{\alpha}$.

On a donc qu'à $\sigma \in G$ et $\alpha \in k(B^{1/m})$ correspond un unique $\xi \in \mu_m$ tel que $\sigma\alpha = \xi_\sigma \cdot \alpha$. Cela dépend bien sûr du α choisi, en fait cela ne dépend pas de α mais de a.

On note
$$\langle \sigma, a \rangle = \frac{\sigma\alpha}{\alpha} \quad \text{pour } a = \alpha^m.$$

Si donc a est toujours fixé, on définit un homomorphisme

$$G \longrightarrow \mu_m$$
$$\sigma \longmapsto \langle \sigma, a \rangle$$

et si $\sigma, \tau \in G$, $\langle \sigma \circ \tau, a \rangle = \dfrac{\sigma(\tau(\alpha))}{\alpha} = \dfrac{\sigma(\zeta_\tau \cdot \alpha)}{\alpha}$

$$= \zeta_\tau \cdot \zeta_\sigma$$
$$= \langle \sigma, a \rangle \cdot \langle \tau, a \rangle .$$

On voit donc que $\forall \alpha$, $\sigma \cdot \tau(\alpha) = \tau . \sigma(\alpha)$ et donc G est un groupe abélien, $k(B^{1/m})/k$ est abélienne.

De plus $\sigma^m(\alpha) = \zeta_\sigma(\zeta_\sigma \cdots (\zeta_\sigma \alpha)) = \zeta_\sigma^m \cdot \alpha = \alpha$ et ceci pour tout α donc G est d'exposant m et donc $k(B^{1/m})/k$ est d'exposant m.

- Une application bilinéaire

La notation $\langle \cdot, \cdot \rangle$ n'est pas par hasard. On montre ici que

$$\langle \cdot, \cdot \rangle : G \times B \longrightarrow \mu_m$$
$$(\sigma, a) \longmapsto \langle \sigma, a \rangle = \frac{\sigma \alpha}{\alpha}$$

où $\alpha \in \sqrt[m]{a}$.

cette application est bilinéaire et on détermine ses noyaux.

On a déjà vu que $\langle \sigma \tau, a \rangle = \langle \sigma . a \rangle . \langle \tau, a \rangle$

Soient donc $a, b \in B$, $\langle \sigma, a \cdot b \rangle = \dfrac{\sigma(\alpha \beta)}{\alpha \beta}$

$$= \frac{\sigma \alpha}{\alpha} \frac{\sigma \beta}{\beta} = \langle \sigma, a \rangle . \langle \sigma, b \rangle$$

On a donc bien affaire à une application bilinéaire.

Noyau à gauche : $\ker_g \langle \cdot, \cdot \rangle = \{ \sigma \in G, \ \forall a \in B \ \langle \sigma, a \rangle = 1 \}$

Soit donc $\sigma \in \ker_g$, on a $\forall a \in B$ $\langle \sigma, a \rangle = \dfrac{\sigma \alpha}{\alpha} = 1$

et donc $\sigma \alpha = \alpha$ $\forall \alpha \in B^{1/m}$ donc $\sigma = Id$ sur $k(B^{1/m})$.

On a donc $\ker_g = \{ Id \} \subseteq G$.

Noyau à droite : si $a \in \ker_d$, on a $\forall \sigma \in G$, $\langle \sigma, a \rangle = 1$

i.e. $\dfrac{\sigma \alpha}{\alpha} = 1$ i.e. $\sigma \alpha = \alpha$ $\forall \alpha \in \sqrt[m]{a}$.

Supposons donc que $\alpha = a^{1/m}$ ne soit pas dans k, on a donc la chaîne

$$\begin{array}{c} k(B^{1/m}) \\ | \\ k(\alpha) \\ | \\ k \end{array}$$

et $k(\alpha)/k$ est de Galois et il existe $\tau \in \mathrm{Gal}(k(\alpha)/k)$ tq $\tau\alpha \neq \alpha$ (puisque $k(\alpha)^{\mathrm{Gal}(k(\alpha)/k)} = k$).

Mais on a aussi que $\mathrm{Gal}(k(\alpha)/k) \hookrightarrow \mathrm{Gal}(k(B^{1/m})/k)$ donc τ s'étend en un k-aut de $k(B^{1/m})$ qui change donc α $\lightning$.

Donc $\ker d = k^{\times m}$ (car $\alpha \in k^{\times}$).

<u>Rappel sur le dual d'un groupe abélien</u> [F-M]

Si G est un groupe abélien et k un corps algébriquement clos alors $G^{\vee} := \mathrm{Hom}(G, k^{\times}) = \{$homomorphismes de groupes de G dans $k^{\times}\}$

$G^{\vee}$ se munit alors d'une multiplication, les éléments χ_1, χ_2 de $G^{\vee}$ sont les <u>caractères</u> de G et $\chi_1 \cdot \chi_2(g) := \chi_1(g)\cdot\chi_2(g)$.

$G^{\vee}$ est le <u>groupe dual</u> de G.

Théorème : Un groupe abélien <u>fini</u> est isomorphe à son dual.

Remarquons que si G est d'exposant m, les caractères sont à valeurs dans μ_m les racines m-ièmes de 1 et on n'a pas besoin de l'hypothèse de clôture algébrique.

Soit donc $a \in B$, on va voir que a induit un caractère de $G = \mathrm{Gal}(k(B^{1/m})/k)$, de la façon suivante :

$$\tilde{a} : G \longrightarrow \mu_m$$
$$\tau \longmapsto \langle \tau, a \rangle$$

On a donc $\begin{array}{c} B \longrightarrow G^{\vee} \\ a \longmapsto \tilde{a} \end{array}$ est un homomorphisme.

Il est surjectif : si $\chi \in G^{\vee}$, $\chi(\tau) \in \mu_m$ et on montre que $\forall \tau$, $\chi(\tau)$ est une valeur propre de τ en tant qu'application k-linéaire, on a donc $\exists \alpha$ tq $\tau(\alpha) = \chi(\tau)\cdot\alpha$ donc $\chi(\tau) = \langle \tau, a \rangle$ avec $a = \alpha^{m}$.

On équivalente alors par le morphisme en cherchant que

$\tilde{a} = \tilde{b}$ ssi $\forall \tau \in G,\ \langle \tau, a\rangle = \langle \tau, b\rangle$

ssi $\frac{\tau\alpha}{\alpha} = \frac{\tau\beta}{\beta}$ ssi $\tau(\alpha\beta^{-1}) = \alpha\beta^{-1}$

(galois) ssi $\alpha\beta^{-1} \in k^\times$ ssi $a\, b^{-1} \in k^{\times m}$

donc on a déduit l'isomorphisme :

$$\frac{B}{k^{\times m}} \simeq G^\vee$$

Si $k(B^{1/m})/k$ est finie, G aussi, alors $G \simeq G^\vee$ et on a $[k(B^{1/m}) : k] = [B : k^{\times m}]$.

On récapitule tout dans le théorème qui suit :

Théorème : Soit k un corps, m un entier premier avec car k. et on suppose que k contient une racine primitive m-ième de 1 ($\mu_m \subseteq k$). Soit B un sous groupe de $k^\times$ et $k(B^{1/m})$.

$$\begin{array}{c} k^\times \\ \cup \\ B \\ \cup \\ k^{\times m} \end{array}$$

Alors $k(B^{1/m})$ est de Galois sur k, abélienne et d'exposant m.

Si G est son groupe de Galois, on a une application bilinéaire

$$G \times B \longrightarrow \mu_m$$
$$(\sigma, a) \longmapsto \langle \tau, a\rangle = \frac{\tau\alpha}{\alpha} \quad \alpha \in \sqrt[m]{a}.$$

Le noyau à gauche est $1 = \mathrm{Id}$ et le noyau à droite est $k^{\times m} \subseteq B$.

$k(B^{1/m})/k$ est finie ssi $[B : k^{\times m}]$ est fini.

On a alors

$$B/_{k^{\times m}} \simeq G^\vee \simeq G$$

et

$$[k(B^{1/m}) : k] = [B : k^{\times m}].$$

On a en particulier donné une condition suffisante pour être une extension abélienne de Galois d'exposant fini. On a enfin une condition nécessaire : (correspondance de Kummer)

Théorème : Avec les mêmes notations, on a une bijection entre l'ensemble des sous groupes de $k^\times$ contenant $k^{\times m}$ et les extensions de Galois abéliennes d'exposant m.

Autrement dit

$$\begin{array}{ccc} k^\times & & k^{alg} \\ \rotatebox{90}{$\subseteq$} & & | \\ B & \longrightarrow & k(B^{1/m}) \\ \rotatebox{90}{$\subseteq$} & & | \\ k^{\times m} & & k \end{array}$$

. Galois
. abélienne
. d'exposant m

Preuve : On vérifie que l'application est injective avec le thm précédent.

Soit à présent L une extension abélienne de k et d'exposant m. On suppose que K est un sous extension $L \supseteq K \supseteq k$ et K/k est finie. Alors $Gal(K/k)$ est un groupe abélien fini et donc il existe $C_1, \dots, C_r$ groupes cycliques tq $Gal(K/k) = C_1 \oplus \cdots \oplus C_r$. Chaque C_i est un sous groupe de $Gal(K/k)$ et donc induit un corps $K_i = K^{C_i}$ de sorte que $K = K_1 \cdots K_r$ (d'ordre m, cf groupes). Chaque K_i/k est cyclique et on a donc par les résultats qui vont suivre que $K_i = k(\sqrt[m]{a_i})$ pour un $a_i \in k$.

$$\begin{tikzcd}[column sep=small] & & K \arrow[dll, dash] \arrow[dl, dash] \arrow[dr, dash] & \\ K_1 \arrow[drr, dash, "cycl"'] & K_2 \arrow[dr, dash] & \cdots & K_r \arrow[dl, dash, "cycl"] \\ & & k & \end{tikzcd}$$

En effet comme l'exposant de $Gal(L/k)$ est m, il en est de même pour $Gal(K/k)$ donc pour chaque C_i qui sont donc d'ordre $| m$. Enfin $K = k(\sqrt[m]{a_1}, \dots, \sqrt[m]{a_r})$ et donc comme L est le compositum de toutes ses sous extensions finies il existe $A \subseteq k^\times$ tel que $L = k(\sqrt[m]{a}, a \in A)$. Soit donc B le sous groupe multiplicatif de $k^\times$ contenant $k^{\times m}$ et A, $B = \langle k^{\times m}, A \rangle$

Alors montrons que $k(B^{1/m}) = k(A^{1/m})$. Clairement on a $\supseteq$.
Pour $\subseteq$ il suffit de le montrer pour les produits $k^{\times m}$ et A car ils engendrent B. Si donc $a \in A$, $x^m \in k^{\times m}$ on a, $b = a x^m$ et $k(b^{1/m}) = k(a^{1/m}.x) = k(a^{1/m})$ et donc $k(B^{1/m}) = k(A^{1/m})$. ■

- Extensions cycliques :

Une petite note sur les <u>extensions cycliques</u> qui sont les extensions de Galois K/k avec $Gal(K/k)$ cyclique.

<u>Lemme</u> : Si k contient une racine primitive n-ième de 1, ξ et K/k une extension cyclique, de degré n, alors, si σ est un générateur de $Gal(K/k)$, il existe $a \in K$ avec

$$\xi = \frac{\sigma(a)}{a}$$

<u>Remarque</u> : Autrement dit $\forall \xi \in \mu_n \subseteq k$, $\forall \sigma \in Gal(K/k)$ générateur, il existe $a \in K$ avec $\xi = \frac{\sigma(a)}{a}$.

<u>Preuve</u> : On veut montrer que ξ est une valeur propre de l'application k-linéaire σ. Pour cela on cherche le polynôme caractéristique de σ. On a, puisque $Gal(K/k)$ est cyclique, que $\sigma^n = Id$, on veut donc montrer que $X^n - 1$ est le polynôme minimal de σ, ce qui nous donne le lemme puisque ce polynôme n'a que des racines simples comme racines et par Cayley-Hamilton le polynôme caractéristique a les mêmes facteurs irréductibles que le minimal. L'indépendance des caractères nous assure que $X^n - 1$ est le minimal. ■

<u>Théorème</u> : Si k est un corps qui contient une racine primitive n-ième de 1 et K/k de Galois cyclique de <u>degré n</u>.
Alors $\exists\, b \in k$ tq $K = k(\sqrt[n]{b})$.

<u>Remarque</u> : "k contient une racine primitive $n^{\text{ième}}$ de 1" élimine le cas où $[K/k] = p$.

Preuve : Par le lemme il existe a avec $\sigma(a) = \zeta a$, $\zeta \in \mu_n$. Donc $\sigma^i(a) = \zeta^i a$ donc $\sigma^i(a) = a$ ssi $n \mid i$ (σ engendre Gal). Comme σ est d'ordre n, seul $\sigma^n = Id$ fixe a ce qui signifie par Galois que $a \in K \setminus k$, et que $k(a) = K^{\{Id\}}$ et donc $[K : k(a)] = |Gal(k(a)/k)| = |\{Id\}| = 1$ donc $k(a) = K$. On a enfin $\sigma(a) = \omega a$ donc $\sigma(a^n) = \sigma(a) \dots \sigma(a) = \omega^n a^n = a^n$ donc $a^n \in k$, et on conclut que pour $b = a^n$, $K = k(\sqrt[n]{b})$. $\square$

- <u>Cas des extensions abéliennes d'exposant $p = \mathrm{car}\, k$</u>

On va voir que la théorie de Kummer s'adapte très bien au cas où exposant $= \mathrm{car}\, k$, il faut juste remplacer toutes les "racines" par des "$\wp$-racines". On entre alors dans la théorie d'Artin-Schreier.

Soit donc k un corps de caractéristique $p > 0$ et

$$\wp : k \longrightarrow k$$
$$x \longmapsto x^p - x$$

C'est un homomorphisme pour l'addition k^+. On remarque que si on prend $b \in k$, $X^p - X - b$ n'est pas nécessairement scindé dans k, mais si α est une racine, comme visiblement $\alpha + n^{\in \mathbb{F}_p}$ est aussi une racine $(\alpha + n)^p - \alpha + n - b = \alpha^p - \alpha - b = 0$ car $n \in \mathbb{F}_p$ donc $\alpha + \mathbb{F}_p$ est donc les racines de $X^p - X - b = \prod_{n \in \mathbb{F}_p} (X - \alpha + n)$ et donc si l'on a une racine dans une extension, on les a toutes et cette fois on n'a pas besoin de supposer quoi que ce soit sur k. (alors que μ_n n'est pas nécessairement dans le corps premier, $\mathbb{F}_p$ l'est et les racines s'expriment en fonction du corps premier donc on les a toutes).

On démontre, de la même façon que $\sqrt[m]{a}$, $\wp^{-1}(a)$ ou $\wp^{-1}a$. On voit que $k(\wp^{-1}a)$ contient en fait toutes les "racines" de a.

On s'intéresse donc aux groupes k^+ ainsi qu'aux sous groupe $\wp k = k^p - k$. Soit donc B un sous groupe additif de k^+ contenant $k^p - k$.

La preuve est la même que précédemment, on énonce juste le théorème :

<u>Théorème :</u> k de car $p > 0$. Alors on a une bijection entre les sous groupes de k^+ contenant $\wp k$ et les extensions abéliennes de Galois cycliques de k d'exposant p.

$$\begin{array}{ccc} k^+ & & k^{ab} \\ \triangledown\!/ & & | \\ B & \longleftrightarrow & k(\wp^{-1}B) \\ \triangledown\!/ & & |\, p \\ \wp k & & k \end{array}$$

Si B est un tel sous groupe additif et $k(\wp^{-1}B)$ est l'extension de Galois cyclique associée et soit $G = Gal(k(\wp^{-1}B)/k)$. Si $\sigma \in G$, $a \in B$, on note $\langle \sigma, a\rangle = \sigma(\alpha) - \alpha$ pour un $\alpha \in \wp^{-1}a$. On a alors une application bilinéaire :

$$G \times B \longrightarrow \mathbb{F}_p$$
$$(\sigma, a) \longmapsto \langle \sigma, a\rangle$$

Le noyau à gauche est $\{1 = Id\}$, celui à droite est $\wp k$. On a $k(\wp^{-1}B)/k$ est finie ssi $[B : \wp k]$ l'est et alors $[k(\wp^{-1}B)/k] = [B : \wp k]$.

• <u>Classification des extensions cycliques</u> : On récapitule ce que l'on a dit dans le cadre des extensions de Galois cycliques, dans les 2 cas qui nous intéressent :

On suppose que K/k est une extension de <u>Galois cyclique</u>
$n = [K/k]$

• <u>Extension de Kummer</u> : Si k contient une racine primitive n-ième de 1 et <u>car $k \nmid n$</u>, Alors $\exists\, b \in k$, $K = k(\sqrt[n]{b})$.

• <u>Extension d'Artin-Schreier</u> : Si $\operatorname{car} k = p = n$, alors il existe $a \in k$ tel que $K = k(\wp^{-1} a)$.

On a bien vu les réciproques de ces 2 propriétés, et les autres infos de cette fiche.
Remarquons que dans le cas des extensions abéliennes (en particulier, cycliques), les sous extensions sont toutes de Galois car le sgp des invariants est distingué.

• <u>Un peu de théorie de galois</u> :

◦ On montre que si K/k est finie de Galois, alors $\exists\, F \subseteq K$, $F \supseteq k$ tq $[K : F] = p$. $\forall p \mid [K:k]$.
En effet si $G = \operatorname{Gal}(K/k)$, $p \mid |G|$
alors G a un sous groupe H d'ordre p $H \leq G$.
distingué
et donc $F = K^H$ est d'ordre : $[K : F] = p$.

$$\begin{array}{c} K \\ |\,p \\ F \\ | \\ k \end{array} \qquad \begin{array}{c} G \\ \vee \end{array} \leftarrow |H| = p$$

◦ La preuve du théorème de Macintyre : On montre que tout corps ω-stable n'a ni extension de Kummer, ni d'Artin-Schreier. et est parfait. Si donc k est ω-stable, et L/k est algébrique, soit $a \in L \setminus k$, $k(a)/k$ est finie, on remonte $L = k(a)$, et par précédemment, $\exists\, F$ tq L/F soit d'ordre p, donc cyclique, mais F est fini sur k donc interprétable et donc F est aussi ω-stable, et donc soit p est $=$ à car F dans ce cas $\not\downarrow$ et sinon, si il existe une racine primitive p-ième on a une extension de Kummer et $\not\downarrow$ et sinon alors comme L/F est de Galois, $L \mid L(\xi)$ donc
$$\begin{array}{c} L \\ | \\ F \end{array} \qquad \begin{array}{ccc} & L(\xi) & \\ L & & F(\xi) \\ & F & \end{array}$$
et $L(\xi)/F(\xi)$ est de Kummer.

• Utilisation de théorie de Kummer :

Si $p_1, \dots, p_r$ sont des premiers distincts. Alors

$$[\mathbb{Q}(\sqrt{p_1}, \dots \sqrt{p_r}) : \mathbb{Q}] = 2^r$$

en effet c'est une extension de Kummer et son degré est exactement : $[B : \mathbb{Q}^{\times 2}] = \left|\frac{B}{\mathbb{Q}^{\times 2}}\right|$

où $\mathbb{Q}^{\times 2} = \left\{ \frac{p^2}{q^2}, p, q \text{ premiers } \wedge 1 \right\}$ et

$$B = \langle p_1, \dots, p_r, \mathbb{Q}^{\times 2} \rangle_{multiplicatif}$$

Or les éléments de B sont de la forme

$$p_1^{x_1} \cdots p_r^{x_r} \cdot \frac{\pi_1^2 \cdots \pi_k^2}{q_1^2 \cdots q_\ell^2} \quad \text{avec } x_i = 0 \text{ ou } 1$$

et donc les seuls éléments non nuls dans le quotient seront

$$\left\{ \prod_{i \in I} p_i \quad \text{pour } I \subseteq \{1, \dots r\} \right\}$$

ces éléments sont tous distincts et il y en a 2^r ce qui est ce qu'on veut.

• Généralités :

. Si F contient une racine primitive n-ième de 1 alors pour $a \in F$: $X^n - a$ est irréd sur F ssi il n'a pas de racines sur F

En effet : $\Rightarrow$ est clair et si il n'a pas de racine alors si α est une racine, $X^n - a$ est scindé à racines simples dans $F(\alpha)$ et on a ce que $X^n - a = (X - \zeta\alpha) \cdots (X - \zeta^{n-1}\alpha)$.

si $P \in F[X]$ et $P \mid X^n - a$ on a $P(0) = \zeta^k \alpha^\ell$ où ℓ est le degré du polyn et donc $\ell < n$, de plus, $\alpha^\ell \in F$.

De même $\underbrace{\zeta^{i_1}\alpha + \dots + \zeta^{i_\ell}\alpha}_{\ell} \in F$ (coeff du deuxième)

(Si ℓ est premier avec n, $\lambda\ell + \mu n = 1$ et alors $(\alpha^\ell)^\lambda \cdot a^\mu = \alpha \in F$ ↯)

Car $\zeta^{i_1}\alpha + \dots + \zeta^{i_\ell}\alpha \in F$, $\alpha(\zeta^{i_1} + \dots + \zeta^{i_\ell}) \in F$ or comme $\mu_n \subseteq F$, alors forcé $\alpha \in F$ ↯ donc ok. ☒

Théorie de Galois infinie

On étudie ici la généralisation de la théorie de Galois des extensions finies aux extensions algébriques quelconques.

Considérons une extension algébrique L/k possiblement de degré infini (ex : $\bar{\mathbb{Q}}/\mathbb{Q}$). La notion d'extension Galoisienne se généralise tout à fait.

- L/k est <u>normale</u> : dans le même sens que si l'extension est finie, ie on demande que si un polyn irréductible de $k[x]$ admet une racine dans L alors toutes ses racines sont dans L.

- L/k est <u>séparable</u> : On demande que tout élément $\alpha \in L$ soit séparable sur k (puisque tout élément est alg. cela a bien du sens) (pas tout à fait : cf. linéairement disjonction)

Une extension algébrique L/k sera donc dite <u>Galoisienne</u> ou <u>de Galois</u> si elle est normale et séparable.

On notera alors $G = \mathrm{Gal}(L/k)$ le groupe des k-automorphismes de L que l'on appelle groupe de Galois de L/k.

• Gal (L/k) comme limite inverse.

On va identifier G comme une limite inverse de groupes finis ce qui nous permettra de le munir d'une topologie.

Soit donc $\mathcal{X}$ l'ensemble des extensions intermédiaires $\begin{array}{c} L \\ | \\ K \\ | \\ k \end{array}$ telles que K/k soit <u>de Galois</u> (finie)

À chaque $K \in \mathcal{X}$, on dispose de $G_K = \mathrm{Gal}(K/k)$ et pour $K_1, K_2 \in \mathcal{X}$ avec $K_1 \subseteq K_2$ on a l'<u>homomorphisme de groupes</u>

$$\mathrm{res}_{K_2 K_1} : G_{K_2} \longrightarrow G_{K_1}$$
$$\qquad\qquad \tau \longmapsto \mathrm{res}_{K_1}\tau = \tau_{|K_1}$$

tel que si $\tau : K_2 \longrightarrow K_2$ est un k automorphisme alors on le restreint à K_1 et cela reste un k automorphisme de K_1 cette fois-ci (car normale)

Remarquons de plus que pour tout $\tau \in G_{k_1}$, τ s'étend en un automorphisme de k_2 (non nécessairement unique bien sûr) car k_2/k est fini. donc aussi k_2/k_1 et $\tau : k_1 \to k_1$ s'étend en $\tilde{\tau} : k_2 \to k^{alg}$ et comme k_2 est normale $\tilde{\tau}$ est en fait $\tilde{\tau} : k_2 \to k_2$. Donc $res_{k_2 k_1}$ est surjective.

De plus il est clair que si $k_1 \subseteq k_2 \subseteq k_3$, et $\tau \in G_{k_3}$

$$\tau\upharpoonright_{k_1} = (\tau\upharpoonright_{k_2})\upharpoonright_{k_1}$$

(ceci est vrai pour la restriction de toute fonction). et donc on a

$$res_{k_3 k_1} = res_{k_2 k_1} \circ res_{k_3 k_2}$$

Evidemment on vérifie que $res_{k_1 k_1} = Id_{G_{k_1}}$, on a donc finalement montré que

$$\left((G_k)_{k \in \mathcal{X}}, (res_{k,k'})_{k,k' \in \mathcal{X}^2}\right)$$

est un <u>système inverse</u> de groupes finis, que l'on munit de la topologie discrète et on dispose donc du groupe topologique $\varprojlim (G_k)_{k \in \mathcal{X}}$

Rappelons quelques propriétés topologiques de $\varprojlim G_k$,

- la topologie est compacte
- la topologie est totalement déconnectée

<u>Description des éléments de $\varprojlim G_k$</u>

Si $(\tau_k)_{k \in \mathcal{X}} \in \varprojlim G_k$, chaque composante τ_k est un k-automorphisme de k pour un certain k extension galoisienne finie de k. On sait que k est en fait une extension monogène, disons $k(x)$ et donc à chaque composante est associé un élément $x \in L$ tel que τ_k soit défini en x.

De plus on a si $k_1 \subseteq k_2$ alors $\tau_{k_2}\upharpoonright_{k_1} = \tau_{k_1}$ et donc en prenant $x \in L$, on a $\tau_{k(x)}(x) = \tau_k(x)$ $\forall k \ni x$.

On comprend ainsi qu'à chaque $(\sigma_K)_{K\in\mathcal{Z}} \in \varprojlim G_K$ est associé un unique $\sigma \in Gal(L/k)$ et tel que $\forall K \in \mathcal{Z}$, $\sigma_{\restriction K} = \sigma_K$. On dispose donc d'une bijection :

$$Gal(L/k) \longrightarrow \varprojlim G_K$$

$$\sigma \longmapsto (\sigma_{\restriction K})_{K\in\mathcal{Z}}$$

qui est un isomorphisme de groupes.
On identifie donc $G = Gal(L/k)$ avec $\varprojlim G_K$ ce qui impose une topologie sur G appelée la topologie de Krull

N.B : (Retour sur l'existence de $\varprojlim G_K$)

- Il faut que $(G_K)_{K\in\mathcal{Z}}$ soit filtrante par dessus ce qui signifie que $\mathcal{Z}$ soit filtrante par dessous, (la correspondance de Galois est un foncteur contravariant entre la catégorie des extensions de Galois avec les homomorphismes de corps et les groupes (de Galois?) et les homomorphismes de Groupes). Soient donc $K_1, K_2 \in \mathcal{Z}$ il faut montrer qu'il existe K tel que $K_1 \searrow_K \swarrow K_2$ et K de Galois. Le candidat est $K_1 \cap K_2$, comme tout élément de K_1 est séparable sur k, $K_1 \cap K_2 / k$ est séparable et comme K_1 et K_2 sont normales, si $P(x) \in k[x]$ a une racine dans $K_1 \cap K_2$ alors toutes les racines sont dans K_1 et dans K_2 donc dans $K_1 \cap K_2$ et donc $K_1 \cap K_2$ est normale, on conclut que $K_1 \cap K_2$ est de Galois et donc $(G_K)_{K\in\mathcal{Z}}$ est bien un système inverse.

- On vérifie facilement que si $K_1 \subseteq K_2$, $res_{K_2 K_1}$ est un homomorphisme de groupes.

On a donc identifié $Gal(L/k)$ avec un groupe profini, un élément de $Gal(L/k)$ est représenté par l'ensemble des restrictions d'un automorphisme L/k à toute extension intermédiaire finie de Galois.

• Description de la topologie sur G : voisinages de 1

Rappelons comment s'organise la topologie sur $\varprojlim G_k = G$

On dispose pour chaque $k_0 \in \Sigma$, d'une projection (continue)

$$\pi_{k_0} : G \longrightarrow G_{k_0} = \mathrm{Gal}(k_0/k)$$
$$(\sigma_k)_{k\in\Sigma} \longmapsto \sigma_{k_0}$$

Dans un groupe topologique, la topologie est constituée de translatés des voisinages ouverts de 1 et la topologie étant celle du produit infini de type les voisinages de 1 sont donnés par les $\ker \pi_k$, i.e. les $\pi_k^{-1}(\{1_{G_k}\})$. ($= \mathrm{Id}_{\mathrm{Gal}} = \mathrm{Id}_k$)

<u>Note</u> : Pour un ouvert quelconque, la topologie étant engendrée par les translatés des $\pi_k^{-1}(\{1\})$ on peut dire qu'un ouvert de base (élément de la base d'ouvert) est donné par un élément $\sigma \in \mathrm{Aut}(L/k)$ et un $k_0 \in \Sigma$ et donc l'ouvert de base est $\pi_{k_0}^{-1}(\{\sigma\})$.

Pour être plus précis si on considère le voisinage de 1_G correspondant à $\pi_{k_0}^{-1}(1_{G_{k_0}} = \mathrm{Id}_{k_0})$ soit $(\sigma_k)_\Sigma \in \pi_{k_0}^{-1}(\mathrm{Id}_{k_0})$ on a donc que $\sigma_{k_0} = \mathrm{Id}_{k_0}$ et pour tout $k' \geq k_0$, par définition $\pi_{k'k_0}(\sigma_{k'}) = \sigma_{k_0} = \mathrm{Id}_{k_0}$ et on voit que (modulo) l'élément de $\mathrm{Aut}(L/k)$ σ tq $\sigma = (\sigma_k)_\Sigma$ vérifie $\sigma_{k_0} = \mathrm{Id}$ c'est donc un élément de <u>$\mathrm{Aut}(L/k_0)$</u>

On a donc que $\pi_{k_0}^{-1}(1_{G_{k_0}} = \mathrm{Id}_{k_0}) = \mathrm{Gal}(L/k_0)$

Un voisinage de 1_G est donc donné par un $k_0 \in \Sigma$ et $\mathrm{Gal}(L/k_0)$.

La famille $\mathcal{N} = \{\mathrm{Gal}(L/k_0),\ k_0 \in \Sigma\}$ est donc une base de voisinage pour $1 \in G$, i.e. Id_L.

Pour trouver une base de voisinage d'un élément quelconque $(\sigma^0_k)_{k\in\mathbb{Z}}$, il faut considérer les translatés dans G de la base de voisinage de $1_G = \mathrm{Id}_L$. Un $\mathcal{O}\subseteq G$ est un ouvert voisinage de $(\sigma^0_k)_{k\in\mathbb{Z}}$ si on a un $Gal(L/N)$ avec $N\supseteq k$ et tel que

$$(\tau_k)_{k\in\mathbb{Z}} \in \mathcal{O} \text{ ssi } (\tau_k)_{\mathbb{Z}} = (\sigma^0_k)_{\mathbb{Z}}\circ(\sigma_k)_{\mathbb{Z}}$$

avec $(\sigma_k)_{\mathbb{Z}} \in Gal(L/N)$.

Remarquons que l'on peut prendre aussi un translaté à droite de $Gal(L/N)$.

sg d'indice fini ⇔ ouvert fermé de G.

• Description de la topologie sur G : ouvert fermés

On sait que dans un groupe topologique si un sg $H\leq G$ fermé est d'indice fini, il est alors ouvert car complémentaire de l'union finie de ses classes à gauche propre qui est un fermé.
Si le groupe est compacte et qu'on a un groupe ouvert, la propriété de B.L nous dit qu'il est d'indice fini.

Rappelons aussi que si on prend une extension K de k dans un clos dans L on peut considérer sa clôture galoisienne dans L, notée K^{gal}, la plus petite extension de K dans L qui soit de Galois, (pour ce faire considérer la clôture normale de K dans k^{sep} et l'intersection avec L).

Si K/k est fini il vient donc $K^{gal} \in \mathcal{Z}$ fini aussi on a k et K et on a $\overbrace{k\subseteq K\subseteq K^{gal}}^{\text{fini}}\subseteq L$. On a alors par le théorème de Galois que $Gal(L/K^{gal})\leq Gal(L/K)$ et $[Gal(L/K):Gal(L/K^{gal})] = \left|\dfrac{Gal(L/K)}{Gal(L/K^{gal})}\right| = |Gal(K^{gal}/K)| < \infty$ et donc $Gal(L/K) = Gal(L/K^{gal})\cup\sigma_1 Gal(L/K^{gal})\cup\dots\cup\sigma_n Gal(L/K^{gal})$.
On voit donc que $Gal(L/K)$ est un sous groupe ouvert de G. De plus, il est clair que $[G:Gal(L/K^{gal})]$ est fini (et égale $[K^{gal}:k]$) et donc

$G = \dot{\bigcup}_{\text{fini}}$ translatés de $\mathrm{Gal}(L/k^{sol}) = \mathrm{Gal}(L/k) \cup \dot{\bigcup}_{\text{fini}}$ translatés de $\mathrm{Gal}(L/k^{sol})$

et donc $\mathrm{Gal}(L/k) = G \setminus$ ouvert et est donc fermé.

Donc si on considère une extension finie $k/\mathbb{k}$ non nécessairement galoisienne, $\mathrm{Gal}(L/k)$ constitue un sg de G qui est ouvert et fermé. (en prolongeant par les éléments de $\mathcal{X}$).

• Description de la topologie sur G : fermés

Pour n'importe quelle extension $k \supseteq \mathbb{k}$, $k \subseteq L$, elle est algébrique issue des $\{\kappa_i\}_{i\in I}$, $k = \mathbb{k}(\{\kappa_i\}_{i\in I})$, on peut prendre $I = \omega$ ($|L| \leq |\mathbb{k}| + \aleph_0$) et on a $k = \bigcup_{n\in\omega} k((\kappa_i)_{i<n})$ et chaque extension est finie. On a donc

$$\mathrm{Gal}(L/k) = \bigcap_{n<\omega} \mathrm{Gal}(L/k((\kappa_i)_{i<n}))$$

qui est un fermé.

• Topologie de Krull

L | $\mathbb{k}$ $\quad k_0 \in \mathcal{X}$ $\quad k_0/\mathbb{k}$ fini de Galois

On a donc en récapitulant :

- base d'ouverts de 1_G : $\{\mathrm{Gal}(L/k_0),\ k_0 \in \mathcal{X}\}$ i.e. $k_0/\mathbb{k}$ de Galois finie
- ouverts-fermés : $\{\mathrm{Gal}(L/k),\ k/\mathbb{k}$ extension finie$\}$ (donc les bases sont ouvert-fermés)
- Fermés : $\{\mathrm{Gal}(L/k),\ k/\mathbb{k}$ quelconque $(k \subseteq L)\}$

• Application restriction

Si $\mathbb{k} \subseteq K \subseteq L$ $\quad K/\mathbb{k}$ est de Galois,

$$\mathrm{res}_{(K)} : G \longrightarrow \mathrm{Gal}(K/\mathbb{k}) \subseteq G$$
$$(\sigma_\ell)_{\ell\in\mathcal{X}} \longmapsto (\sigma_\ell \restriction K)_{\ell\in\mathcal{X}}$$

alors res est une application continue pour tout K

car $\mathrm{res}^{-1}(\mathrm{Gal}(K/\mathbb{k}')) = \mathrm{Gal}(L/\mathbb{k}')$ $\quad$ L | K | $\mathbb{k}'$ | $\mathbb{k}$

qui est bien un ouvert.

• Le théorème de correspondance de Galois infini

On a donc pu généraliser la notion de groupe de Galois d'une extension algébrique quelconque et on s'intéresse maintenant à savoir si, dans le cas infini il y a encore le théorème de correspondance entre les corps intermédiaires et les sous groupes du groupe de Galois. On a muni le groupe de Galois d'une topologie et ce n'est pas pour rien. Contrairement au cas fini dans le théorème de correspondance de Galois infini, à tous les sous groupes du groupe de Galois ne correspondent pas nécessairement un corps intermédiaire. Il faut spécifier que ces groupes doivent être fermés pour la topologie de Krull.

Rappelons les notations utilisées, on considère une extension L/k de Galois et $G = \mathrm{Gal}(L/k)$, un groupe profini, que l'on munit de la topologie de Krull. Pour un sous groupe $H \leq G$ on considérera

$$L^H = \{ \text{corps des éléments de } L \text{ fixés par tout élément de } H \}$$

Théorème de Correspondance de Galois. On dispose d'une

$$\boxed{\begin{array}{l} \text{bijection :} \quad \left\{ K \text{ corps intermédiaire } \begin{array}{c} L \\ | \\ K \\ | \\ k \end{array} \right\} \longrightarrow \left\{ \begin{array}{l} \text{Sous groupes fermés} \\ \text{de } G = \mathrm{Gal}(L/k) \end{array} \right\} \\ \qquad\qquad\qquad\qquad\qquad K \longmapsto \mathrm{Gal}(L/K) \\ \qquad\qquad\qquad\qquad\qquad L^H \longleftarrow\!\shortmid\; H \end{array}}$$

Preuve: Soit donc K un corps intermédiaire. On a vu que $\mathrm{Gal}(L/K)$ est un sous groupe fermé de G. Soit $H = \mathrm{Gal}(L/K)$, on a clairement $K \subseteq L^H$. Montrons la réciproque. Soit donc $x \in L^H$, on considère l'application res : $\mathrm{Gal}(L/k) \longrightarrow \mathrm{Gal}(k(x)/k(x)\cap k)$ qui est un épimorphisme continu (surjectif). Par surjectivité pour tout $\sigma \in \mathrm{Gal}(k(x)/k(x)\cap k)$ on a $\sigma = \mathrm{res}\,\tau$ et $x \in L^H$ donc $\tau x = x$ et donc $\sigma x = x$. Enfin le théorème de Galois fini permet de conclure que $x \in k(x)\cap K$ et donc $L^H \subseteq k$.

Réciproquement si H est un sous groupe fermé de $G = \mathrm{Gal}(L/k)$ et soit $k = L^H$. Montrons que $\mathrm{Gal}(L/k) = H$.

On a d'un côté que $\mathrm{Gal}(L/L^H) \geq H$ par définition.

Soit donc $\sigma \in \mathrm{Gal}(L/L^H)$, il suffit de montrer que σ est dans la clôture topologique de H ($= H$ par fermeture).

On montre donc que pour tout F voisinage fermé de σ, on a $F \cap H \neq \emptyset$. Un voisinage fermé de σ est donné par le translaté d'un voisinage fermé de $1 = \mathrm{Id}_L$ qui est lui-même donné par précédemment par un fermé de base disons $\mathrm{Gal}(L/k')$ avec k'/k fini.

Il faut montrer que $H \cap \sigma\,\mathrm{Gal}(L/k') \neq \emptyset$.

On a $k'\cap k = k'^{(\mathrm{res}_{k'} H)}$ et $k'/k'\cap k$ est fini et donc, $\mathrm{res}_{k'}\sigma \in \mathrm{Gal}(k'/k'\cap k) = \mathrm{res}_{k'} H$ par le théorème de Galois. On a donc $H \cap \sigma\,\mathrm{Gal}(N/M) \neq \emptyset$ et donc on conclut le théorème. ∎

Avant de décrire explicitement des exemples de groupes de Galois infinis, on énonce quelques propriétés de théorie de Galois infinie, qui ressemblent énormément au cas fini.

Notons que cette théorie infinie utilise la topologie pour se ramener à utiliser la théorie de Galois finie, en effet le point est qu'un fermé est le translaté d'un fermé de 1 qui est expliqué par des galois $\mathrm{Gal}(L/k)$ avec L/k finie.

- Résultats du théorème de Galois

$\mathrm{Gal}(L/k) =: G$

On considère une extension (algébrique) L/k possiblement infinie et de Galois. On a alors les théorèmes suivants :

- $k \subseteq k_1 \subseteq k_2 \subseteq L \iff \mathrm{Gal}(L/k_2) \leq \mathrm{Gal}(L/k_1)$

- $\{1\} \leq \underset{\text{fermé}}{H_1} \leq \underset{\text{fermés}}{H_2} \leq \underset{G}{\underset{\shortparallel}{\mathrm{Gal}(L/k)}} \iff L^{H_2} \leq L^{H_1}$

- $L^{H_1} \cap L^{H_2} = L^{\langle H_1 H_2 \rangle}$ $\quad$ ($\langle H_1 H_2\rangle$ est la clôture du sg engendré par H_1, H_2 (qui sont fermés))

- $L^{\sigma H \sigma^{-1}} = \sigma L^H$ $\quad$ H fermé.

- $H \trianglelefteq G$ ssi L^H/k est de Galois.

- $k \subseteq K \subseteq L$ alors
$$\mathrm{Gal}(K/k) \overset{\text{homéomorphe}}{\cong} \mathrm{Gal}(L/k)\big/\mathrm{Gal}(L/K)$$

- $k \subseteq K$ on a $[K:k] = [G : \mathrm{Gal}(K:k)]$.

Tout ceci est encore vrai dans le cadre de la clôture séparable (généralement, vu dans k^{alg}) de k. On note $G(k)$ le groupe de Galois absolu $\mathrm{Gal}(k^{sep}/k)$.

Notez que la clôture séparable d'un corps k est toujours une extension de Galois k^{sep}/k, car clairement séparable elle est aussi normale puisque si $P(x) \in k[x]$ est irréductible et a une racine dans k^{sep}, alors P est séparable et donc toutes les autres racines de P sont séparables et donc dans k^{sep}.

Si car $k = 0$ alors $k^{sep} = k^{alg}$

En caractéristique positive, la clôture séparable n'est pas la clôture algébrique car il y a des éléments algébriques purement inséparables. Ainsi $\mathbb{F}_p(t)^{alg}$ n'est pas la clôture séparable, $\mathbb{F}_p(t)^{alg}/\mathbb{F}_p(t)$ n'est pas une extension de Galois. On essayera de déterminer $G(\mathbb{F}_p) = \mathrm{Gal}(\mathbb{F}_p^{\,sep}/\mathbb{F}_p)$.

Notes sur théorème de Waterhouse :

Théorème (Waterhouse)

$\boxed{\text{Tout groupe profini est isomorphe à un groupe de Galois d'une extension externe.}}$

• **Exemple : le groupe de Galois absolu de $\mathbb{F}_q$**

On considère $q = p^n$ et $\mathbb{F}_q$ le corps à q éléments. On veut déterminer le groupe $G(\mathbb{F}_q) = Gal(\mathbb{F}_q^{sep} / \mathbb{F}_q)$, on va montrer qu'il est isomorphe à $\hat{\mathbb{Z}}$.

On commence par se rappeler que $G(\mathbb{F}_q) = \varprojlim Gal(\mathbb{F}_{q^n}/\mathbb{F}_q)$

On dispose d'une extension $\mathbb{F}_{q^n} \subseteq \mathbb{F}_{q^m}$ ssi $n \mid m$, dans ce cas on a $\pi_{m,n} : \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_{q^n}$. On a ensuite, toujours pour $n \mid m$ $\tilde{\pi}_{m,n} : Gal(\mathbb{F}_{q^m}/\mathbb{F}_q) \longrightarrow Gal(\mathbb{F}_{q^n}/\mathbb{F}_q)$

$$\sigma \longmapsto \sigma \circ \pi_{m,n}$$

On a bien une famille filtrante car si $\mathbb{F}_{q^n}, \mathbb{F}_{q^m}$ est donné, on dispose de

$$\begin{array}{ccc} & \mathbb{F}_{q^{n.m}} & \\ / & & \backslash \\ \mathbb{F}_{q^n} & & \mathbb{F}_{q^m} \end{array}$$

On le verrait déjà mais on a $G(\mathbb{F}_q) = \varprojlim \left(\mathbb{F}_{q^n}, \tilde{\pi}_{mn}\right)_{\substack{n,m\in\omega \\ n \mid m}}$

On sait que si on pose $\varphi^n(x) = x^q$ le frobenius, on a $\varphi^n \in Gal(\mathbb{F}_{q^n}/\mathbb{F}_q)$ $(\forall n \in \omega)$ et φ^n est générateur de $Gal(\mathbb{F}_{q^n}/\mathbb{F}_q)$, on conclut donc comme φ^n est d'ordre n, qu'on a un isomorphisme entre $Gal(\mathbb{F}_{q^n}/\mathbb{F}_q)$ et $\frac{\mathbb{Z}}{n\mathbb{Z}}$.

et le carré

$$\begin{array}{ccc} \frac{\mathbb{Z}}{m\mathbb{Z}} & \longrightarrow & \frac{\mathbb{Z}}{n\mathbb{Z}} \\ \wr\wr & & \wr\wr \\ Gal(\mathbb{F}_{q^m}/\mathbb{F}_q) & \longrightarrow & Gal(\mathbb{F}_{q^n}/\mathbb{F}_q) \end{array}$$

On identifie ainsi, le système

$$\left(Gal(\mathbb{F}_{q^n}/\mathbb{F}_q),\ \tilde{\pi}_{m,n} \right)_{\substack{n,m<\omega \\ n|m}} \quad \text{avec} \quad \left(\frac{\mathbb{Z}}{n\mathbb{Z}},\ \hat{\pi}_{m,n} \right)_{\substack{n,m<\omega \\ n|m}}$$

où $\hat{\pi}_{m,n} : \dfrac{\mathbb{Z}}{m\mathbb{Z}} \longrightarrow \dfrac{\mathbb{Z}}{n\mathbb{Z}}$.

$$x + m\mathbb{Z} \longmapsto x + n\mathbb{Z}$$

On a donc $G(\mathbb{F}_q) = \varprojlim \dfrac{\mathbb{Z}}{n\mathbb{Z}} = \hat{\mathbb{Z}}$.

Remarquer qu'on a le résultat suivant : tout corps fini est parfait(*). Ainsi toute extension est séparable et donc $\mathbb{F}_q^{sep} = \mathbb{F}_q^{alg}$ et on a en effet calculé $Gal(\mathbb{F}_q^{alg}/\mathbb{F}_q)$.

[(*) en effet le morphisme additif $x \mapsto x^p$ est injectif par intégrité et donc surjectif par finitude et donc $\mathbb{F}_q^{\,p} = \mathbb{F}_q$.]

<u>Récap</u> : Étant donné $G = Gal(k^{sep}/k)$ on voit que la base de la topologie est donnée par des ouverts fermés de la forme $Gal(k^{sep}/L)$ avec L/k <u>galoisienne finie</u>.
Les sg fermés de G sont les ~~[illegible]~~ $Gal(k^{sep}/L)$ avec L/k <u>quelconque</u> (ni nécessairement finie ni galoisienne). Ce qu'affirme le théorème de correspondance et que ce sont les seuls sg de G qui sont fermés, i.e. qu'à tout sg fermé de G correspond une extension. Si le sg est normal l'extension est de Galois (en fait normal mais sep aussi).

Extension linéairement disjointe

La notion d'extension linéairement disjointe est essentiel. On s'intéresse donc cette notion à la définition et montrer quelques propriétés élémentaires. Cette notion sera cruciale pour étendre la définition d'extension séparable au cas non-nécessairement algébrique.

$$\begin{tikzcd}[column sep=small] & EF \arrow[dl, dash] \arrow[dr, dash] & \\ E \arrow[dr, dash] & & F \arrow[dl, dash] \\ & k & \end{tikzcd}$$

On considère deux extensions E et F d'un corps k

LASSE (1) Toute famille de E finie k-linéairement indépendante est F-linéairement indépendante (dans EF)

(2) Toute famille finie de F k-linéairement indépendante est E-linéairement indépendante.

En effet supposons (1) et soit $f_1 \dots f_n \in F$ k-linéairement indépendante et soit $e_1 \dots e_n \in E$ tq $f_1 e_1 + \dots + f_n e_n = 0$. Réduisons alors (e_i) en une famille libre sur k et exprimons les e_i restant en fonction de la nouvelle famille, cette nouvelle famille est alors F-linéairement indépendante par hypothèse mais l'équation précédente donne une contradiction en regroupant les termes.

On dit que E et F sont <u>linéairement disjointes</u> <u>sur k</u> si elles vérifient les conditions (1) et (2). (noté $E \underset{k}{|} F$)

<u>Proposition</u> : Soit $\begin{smallmatrix} E & & F \\ & k & \end{smallmatrix}$ comme avant et supposons $[E:k]$ finie.

Alors $E \underset{k}{|} F$ ssi $[E:k] = [EF:F]$

De plus si $[E:k]$ et $[F:k]$ sont finis

$E \underset{k}{|} F$ ssi $[EF:k] = [E:k][F:k]$

<u>Preuve</u> : Si on prend $e_1 \dots e_n$ une base de k en E et que l'on regarde $e_1 \dots e_n$ dans EF. Par hypothèse $e_1 \dots e_n$ engendre E

si le corps de scalaires est k donc aussi si c'est F, de plus (e_i) est linéairement indépendante sur F. On a que le F-ev engendré par (e_i) contient E et F puisque $1 \in E$ et a fortiori 1 F ev. Donc $EF \subseteq \langle e_i \rangle_F$ et or $(e_i)_F \subseteq EF$ on conclut que (e_i) engendre EF en tant qu'espace vectoriel sur F. Comme (e_i) est linéairement indépendante sur F c'est une base et donc $[EF:F] = n = [E:k]$. Réciproquement si $[E:k]=[EF:F]$ soit $e_1 \dots e_m$ une famille k-libre (donc $m < [E:k] = \underbrace{[EF:F]}_{=n}$) on la complète en une base de E/k et comme on l'a vu dans EF cette base $e_1 \dots e_n$ engendre tout $/F$ c'est donc une famille génératrice de cardinal la dimension donc une base et en particulier $e_1 \dots e_m$ sont lin. indép. sur F donc EF ■

<u>Remarque</u> : Dans le diagramme de droite si $(e_i)_{i=1 \dots n}$ est une famille génératrice de E en tant que k-ev alors c'est aussi une famille génératrice de EF en tant que F ev.

$$\begin{tikzcd}[column sep=small] & EF \arrow[dl, dash] \arrow[dr, dash] & \\ E \arrow[dr, dash] & & F \arrow[dl, dash] \\ & k & \end{tikzcd}$$

<u>Exemples</u> : • On a $\mathbb{Q}(\sqrt{2}) \perp_{\mathbb{Q}} \mathbb{Q}(\sqrt{3})$ en effet considérons la famille $(1, \sqrt{2})$, de $\mathbb{Q}(\sqrt{2})$, c'est une base de $\mathbb{Q}(\sqrt{2})$ et clairement $(1, \sqrt{2})$ est toujours une famille libre sur $\mathbb{Q}(\sqrt{3})$ (le produit $\sqrt{2}\sqrt{3}$ ne revient pas dans $\mathbb{Q}$)

$$\begin{tikzcd}[column sep=small] & \mathbb{Q}(\sqrt{2}\sqrt{3}) \arrow[dl, dash, "2"'] \arrow[dr, dash, "2"] & \\ \mathbb{Q}(\sqrt{2}) \arrow[dr, dash, "2"'] & & \mathbb{Q}(\sqrt{3}) \arrow[dl, dash, "2"] \\ & \mathbb{Q} & \end{tikzcd}$$

On a donc d'abord que $\mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}(\sqrt{3})$ sont linéairement disjoints, le résultat étant donné par les degrés et la prop précédente. Rappelons que l'on parle de base <u>d'ev</u> et non de <u>base algébrique</u>. On a donc

$\mathbb{Q}(\sqrt{2}) / \mathbb{Q} \xleftrightarrow{\text{base}} (1, \sqrt{2})$ $\qquad$ $\mathbb{Q}(\sqrt{2}\sqrt{3}) / \mathbb{Q}(\sqrt{2}) \leftrightarrow (1, \sqrt{3})$

$\mathbb{Q}(\sqrt{3}) / \mathbb{Q} \leftrightarrow (1, \sqrt{3})$ $\qquad$ $\mathbb{Q}(\sqrt{2}\sqrt{3}) / \mathbb{Q}(\sqrt{3}) \leftrightarrow (1, \sqrt{2})$

et $\quad \mathbb{Q}(\sqrt{2}\sqrt{3}) / \mathbb{Q} \leftrightarrow 1, \sqrt{2}, \sqrt{3}, \sqrt{2}.\sqrt{3}$.

Remarque : $\begin{matrix} E \\ | \\ k \end{matrix}$ est algébrique et t transcendant sur k alors E et $k(t)$ sont linéairement disjointes sur k.

Remarque : Si $E \underset{k}{|} F$ alors $E \cap F = k$ mais ce n'est pas une condition suffisante comme le montre l'exemple suivant. (En effet si $E \cap F \supsetneq k$ par déf $[E\cap F : k] \geq 2$ donc $\exists\, x, y$ linéairement indépendants sur k et $x, y \in E \cap F$ donc $\in F$ et donc ne sont pas linéairement indépendants sur F)

Exemple : Prenons $a \neq b$ ($\sqrt[3]{2} \in \mathbb{R}$) 2 racines cubiques de 2 dans $\mathbb{C}$, on a

$$X^3 - 2 = (X-a)(X-b)\left(X - \frac{2}{ab}\right)$$

On a $\mathbb{Q}(a) \cap \mathbb{Q}(b) = \mathbb{Q}$, car $[\mathbb{Q}(a) : \mathbb{Q}] = [\mathbb{Q}(b) : \mathbb{Q}] = 3$ (extension maximale) donc si $\mathbb{Q}(a) \cap \mathbb{Q}(b) \supsetneq \mathbb{Q}$ alors $\mathbb{Q}(a) = \mathbb{Q}(b)$ or $b \in \mathbb{C} \setminus \mathbb{R}$.

On a donc
$$\begin{tikzcd}[column sep=small] \mathbb{Q}(a) & & \mathbb{Q}(b) \\ & \mathbb{Q} \arrow[ul, dash] \arrow[ur, dash] & \end{tikzcd}$$
avec $\mathbb{Q}(a) \cap \mathbb{Q}(b) = \mathbb{Q}$. Mais $\mathbb{Q}(a)$ et $\mathbb{Q}(b)$ ne sont pas linéairement disjoints sur $\mathbb{Q}$.

Par contre on a $[\mathbb{Q}(a,b) : \mathbb{Q}(b)] \leq 2 \neq [\mathbb{Q}(a) : \mathbb{Q}]$ puisque $X^3 - 2 = (X-a)(X-b)\left(X - \frac{2}{ab}\right)$, il se factorise dans $\mathbb{Q}(b)$.

Proposition : Soit les sous-extensions
$$\begin{tikzcd}[column sep=small] & EL & & F \\ E \arrow[ur, dash] & & L \arrow[ul, dash] \arrow[ur, dash] & \\ & k \arrow[ul, dash] \arrow[ur, dash] & & \end{tikzcd}$$

Alors
$$E \underset{k}{|} F \quad \text{ssi} \quad E \underset{k}{|} L \ \ \& \ \ EL \underset{L}{|} F$$

Preuve : $\boxed{\Rightarrow}$ $E \underset{k}{|} L$ est immédiat. et on suppose que $E \underset{k}{|} F$ ($EL \mid F$, $E \underset{k}{|} L$).

Soit $y_1, \dots, y_m$ des éléments de F linéairement indep sur L, alors et supposons $a_1 \dots a_m \in EL$ $a_1 y_1 + \dots + a_m y_m = 0$, on a alors on peut supposer quitte à multiplier par les dénominateurs que $a_i \in L[E]$ (valeur des polynômes à coef dans L évalués en élément de E). On a donc $a_i = \sum a_{ij} x_j$ avec $x_j \in E$ et ainsi $\sum \underset{\in L \subset F}{a_{1j}} x_j y_1 + \dots + \sum a_{mj} x_j y_m = 0$

et comme $E \underset{k}{|} F$ il est nécessaire que les a_i soient tous nuls $\boxtimes$

<u>Remarque</u> : On utilise que $EF = \mathrm{Frac}(E[F])$ ce qui permet après relèvement dans $E[F]$ par multipliant par dénominateur de voir alors ces $\sum a_i x^i$ et ou $\beta_i = x^i$ $\sum a_i \beta_i$ une combinaison linéaire.

N.B : Le sens $\Leftarrow$ est immédiat ainsi car si $x_1 \dots x_m$ est une famille libre sur k de E, elle l'est sur L par $E \underset{k}{|} L$ et comme elle est dans EL, elle est libre sur F par $EL \underset{L}{|} F$.

- <u>Cas d'une extension galoisienne</u>

<u>Proposition</u> : Si $E \diagdown_k \diagup L$ est tel que E/k est de <u>Galois</u> (finie)

$\boxed{\text{alors on a } \quad E \underset{k}{|} L \quad \text{ssi} \quad E \cap L = k.}$

<u>Preuve</u> : Rappelons un fait de théorie de Galois :

Si E/k est de Galois et si $k \subseteq L$ alors

$$\mathrm{res} : \mathrm{Gal}(EL/E) \longrightarrow \mathrm{Gal}(L/\underset{\underset{k}{\shortparallel}}{E \cap L})$$

est bijection, de plus EL/E est galoisienne. ~~tout de~~

On a donc $[EL : L] = [E/k]$ donc par le critère pour les extensions finies, $E \underset{k}{|} L$. $\boxtimes$

- <u>Degré d'imperfection d'un corps.</u>

On considère ici un corps k et p un nombre premier. On note k^p l'ensemble des puissances p-ièmes de k et on considère un corps k_0 tel que $k^p \subseteq k_0 \subseteq k$.

On a que pour $x_1 \dots x_n \in k$, $x_i^p \in k^p \subseteq k_0$ et donc $[k_0(x_i) : k_0] \leq p$. (x_i est algébrique de degré p.) et donc $[k_0(\bar{x}) : k_0] \leq p^n$

On dit alors que $x_1, \dots, x_n$ sont <u>p-indépendants</u> si $[k_0(\bar{x}) : k_0] = p^n$.

Remarque que si $[k_0(\bar{x}):k_0] = p^n$, comme on dispose de $k_0 \subseteq k_0(x_1) \subseteq k_0(x_1,x_2) \subseteq \dots \subseteq k_0(x_1 \dots x_n)$ cela force chaque extension $[k_0(x_1):k_0] = p$, $[k_0(x_1,x_2):k_0(x_1)] = p$ etc.. et donc $\forall i$ $[k_0(x_i):k_0] = p$ et $[k_0(x_i):k_0] = [k_0(x_i,x_j):k_0(x_j)]$ on a $k_0(x_i) \underset{k_0}{|} k_0(x_j)$ $\forall i, j$.

Réciproquement on suppose que $\forall i,j$ $[k_0(x_i):k_0] = p$ et $k_0(x_i) \underset{k_0}{|} k_0(x_j)$. Alors on le montre pour $n=3$ et cela suffit : $k_0(x_1) \underset{k_0}{|} k_0(x_2) \underset{k_0}{|} k_0(x_3)$. On a

$$\begin{tikzcd}[column sep=small] & k_0(x_1,x_2) & \\ k_0(x_1) \arrow[ur, dash, "p"] & & k_0(x_2) \arrow[ul, dash, "p"'] \\ & k_0 \arrow[ul, dash, "p"] \arrow[ur, dash, "p"'] & \end{tikzcd}$$

et de meme on $k_0(x_2) \underset{k_0}{|} k_0(x_3)$ on obtient

$$\begin{tikzcd}[column sep=small] & k_0(x_1,x_2) & & k_0(x_1,x_3) & \\ k_0(x_2) \arrow[ur, dash, "p"] & & k_0(x_1) \arrow[ul, dash, "p"'] \arrow[ur, dash, "p"] & & k_0(x_3) \arrow[ul, dash, "p"'] \\ & k_0 \arrow[ul, dash, "p"] \arrow[ur, dash, "p"'] & & k_0 \arrow[ul, dash, "p"] \arrow[ur, dash, "p"'] & \end{tikzcd}$$

On veut donc vérifier que $k_0(x_1,x_2) \underset{k_0(x_1)}{|} k_0(x_1,x_3)$, ceci est équivalent à $[k_0(x_1,x_2,x_3):k_0(x_1)] = p^2$ et donc $[k_0(x_1,x_2,x_3):k_0(x_2,x_3)] = p$: supposons que non, alors $x_1 \in k_0(x_2,x_3)$, $x_1 = P(x_2,x_3)$ on a donc

$$\begin{tikzcd}[column sep=small] & k_0(x_1,x_2,x_3) & \\ k_0(x_2) \arrow[ur, dash, "p"] & & k_0(x_3) \arrow[ul, dash, "p"'] \\ & k_0 \arrow[ul, dash, "p"] \arrow[ur, dash, "p"'] & \end{tikzcd}$$

et on contredit cela : On a dans $k_0(x_2)$ la famille $(1, x_2)$ qui est libre sur k_0 or dans ~~k_0~~ (x_2,x_3) les monômes en x_2, et 1 ne sont plus vu que $P(x_2,x_3) - x_1(1) = 0$ libre alors qu'ils le sont dans $k_0(x_2)$ contradiction. On a en fait contredit que si $k(x_2) \underset{k_0}{\perp} k_0(x_3)$ alors $k_0(x_2)$ est libre de $k_0(x_3)$ sur k_0.

On conclut :

Lemme : La famille $x_1 \dots x_n$ est p-indépendante, ssi

- $[k_0(x_i):k_0] = p$ $\forall i$
- $k_0(x_i) \underset{k_0}{|} k_0(x_j)$ $\forall i, j$.

Cela signifie que les polys $x_1^{i(1)} \cdots x_n^{i(n)}$ sont linéairement indépendant pour $1 \leq i(j) \leq p-1$. En particulier si $x_1, \dots, x_n$ sont indépendant sur k_0, il en est de même pour tout monôme et donc $x_1, \dots, x_n$ sont p-indépendant $\forall p$.

On dit qu'un ensemble $B \subseteq k_0$ est <u>p-indépendant</u> si toute famille finie d'élément de B est p-indépendant. Comme tout élément s'écrit comme une combinaison linéaire finie de B, c'est bien la généralisation recherchée.

Si $k_0[B] = k$ alors B est une <u>p-base</u> de k sur k_0.

<u>Remarque</u> : Une base B d'une extension L/k en tant qu'espace vectoriel vérifie toujours $k[B] = L$, cependant que dans $\mathbb{Q}(\sqrt[3]{2})$, une base d'ev est $\{1, \sqrt[3]{2}, (\sqrt[3]{2})^2\}$ alors qu'une base algébrique est $\sqrt[3]{2}$. Une base d'ev est toujours plus grosse. Étant donné une extension finie $k(x_1, \dots, x_n)$, une base algébrique est $x_1, \dots, x_n$ alors qu'une base d'espace vectorielle est donnée par l'ensemble des monômes $x_1^{i(1)} \cdots x_n^{i(n)}$ pour $i(j) \leq (\max \deg$ d'alg de $x_i) - 1$.

Exemple : On considère $\mathbb{F}_p(t)$ et $\mathbb{F}_p(t)^p = \mathbb{F}_p(t^p)$.

On a t est algébrique sur $\mathbb{F}_p(t^p)$ et on a $\mathrm{Irr}(t, \mathbb{F}_p(t^p), X) = X^p - t^p$ (tout purement inséparable sur $\mathbb{F}_p(t^p)$). Enfin $[\mathbb{F}_p(t) : \mathbb{F}_p(t^p)] = p$ et une p-base de $\mathbb{F}_p(t)$ sur $\mathbb{F}_p(t^p)$ est donnée par (t). En effet comme c'est une base d'1 élément, pas besoin de vérifier l'hypothèse de linéairement disjoint et de plus $[\mathbb{F}_p(t) : \mathbb{F}_p(t^p)] = p$.

On considère le cas où $k_0 = k^p$. On a donc que tout élément de k est algébrique de degré $\le p$ sur k et même de degré divisant p car soit $x \in k$, et x a une racine p-ième dans k donc $[k^p(x) : k^p] = 1$ et sinon x n'a pas de racine p-ième dans k et $[k^p(x) : k^p] = p$. On a donc que, si $[k : k^p]$ est fini, $[k : k^p] = p^n$ et on appelle degré d'imperfection le nombre $[k : k^p]$. n est appelé exposant d'imperfection.

Exemple. Un corps parfait a un exposant d'imperfection 0 et un degré d'imperfection 1.

• Si k est un corps tel que $p^n = [k : k^p]$. Soit alors $k^{p^n} = \bigcap_{i=0}^{n-1} k^{p^i} = \{ \quad , x \in k \text{ pour } i \le n\}$ alors k^{p^n} est parfait.

Le principe de l'échange :

Soit k_0 est un sous-corps de k qui contient k^p. Si $x_1 \dots x_m, y_1 \dots y_n \in k$ tel que $x_1 \dots x_m$ sont p-indépendants sur k_0 et $x_1, \dots, x_m \in k_0[y_1, \dots, y_n]$. Alors $m \le n$ et il existe un réarrangement des $y_1, \dots, y_n$ tel que $y_1, \dots, y_m \in k_0[x_1, \dots, x_m, y_{m+1}, \dots, y_n]$.

Ainsi tout sous-ensemble de k p-indépendant sur k_0 se complète en une p-base de k sur k_0.

Exemple : $\mathbb{F}_p(t_1, \dots t_n, \dots) / \mathbb{F}_p(t_1^p, \dots t_n^p, \dots)$ (t_i alg indép / $\mathbb{F}_p$) on a alors $t_1, \dots, t_n$ est p-indépendant sur $\mathbb{F}_p(t_1^p, \dots, t_n^p, \dots)$ (en effet $[\mathbb{F}_p(t_i) / \mathbb{F}_p(t_i^p \dots t_n^p)] = p$ etc). Donc $t_1, \dots t_n$ se complète en une p-base comme $t_{n+1}, \dots$ mais aussi {monômes en t_{n+1}, t_{n+2}

Remarque : $\mathbb{F}_p$ et p base n'ont aucun rapport ⚠ bien sûr que si !

ou si car $k \neq p$, k^p n'est pas un corps...

Remarque : Soit $k \subseteq L$ et $\bar{T} = (t_1 \dots t_n)$ une famille $\boxed{\text{algébriquement indépendante sur } L}$, alors $L \underset{k}{|} k(\bar{T})$

En effet, en supposant que non il suffit de montrer que toute base du k-ev $k(\bar{T})$ reste k-linéairement indépendant. On prend comme base $M(t)$ les monômes en $t_1 \dots t_n$ et on veut que si $\exists\, l_1 \dots l_n \in L$ tq $l_1 M_1(t) + \dots + l_n M_n(t) = 0$ on a un $P(t_1 \dots t_n) = l_1 M_1(t) + \dots + l_n M_n(t)$ avec $P \in L[\bar{T}]$ et donc on a une contradiction.

N.B : Pour $L \underset{k}{|} F$ il suffit de montrer que toute base du k-ev L reste linéairement indépendante sur F.

N.B : Montrer que une $L \underset{k}{|} F$ il suffit de le montrer $\forall\, L_0 \subseteq L$, $F_0 \subseteq L$ finiment engendrés.

Extensions séparables, régulières et primaires.

On se réfère dans cette section à la notion d'extension linéairement disjointe. On généralise d'abord la notion d'extension séparable.

- Extension séparable

Tout d'abord on met en la clôture inséparable. Si $\begin{array}{c} L \\ | \\ k \end{array}$ est une extension, les éléments purement inséparables, i.e. pathologiques, vu étant l'unique racine de leur polynôme irréductible, sont les éléments algébriques sur k, vivant dans L et étant une racine p^n-ième d'un élément de k, (on peut la construire du corps, de tels éléments n'existent que dans le cadre de la caractéristique positive). Il y a 2 formes de clôture inséparable. La première est $k^{insep(L)} = \{ a \in L,\ a \text{ est purement inséparable sur } k \}$ et la seconde est $k^i = k^{insep(k^{alg})}$. Notons que l'on a en fait que $k^i = \{\text{élément algébrique inséparable sur } k\} = \bigcup_{n \in \mathbb{N}} k^{\frac{1}{p^n}} = k^{\frac{1}{p^\infty}}$ (alors que k^{p^∞} est un corps parfait contenu dans k) donc que toute extension en devient une séparable dans les 2 cas. (Notons que étant donnée une extension $\begin{array}{c} L \\ | \\ k \end{array}$ nous ne savons aussi que l'on a une décomposition $\begin{array}{c} T \\ | \ \text{sep} \\ F \\ | \ \text{insep} \\ k \end{array}$, mais ici on prend la clôture inséparable dans k^{alg}, et tout élément a dedans est nécessairement séparable).

Une extension L de k est dite séparable si $\underset{k}{L \mid k^{\frac{1}{p^\infty}}}$ si L est linéairement indépendant de k^{1/p^∞} sur k.

En particulier L ne contient pas d'élément purement inséparable sur k.

Remarquons qu'on peut montrer que

$$\underset{k}{L \mid k^{\frac{1}{p^\infty}}} \quad \text{ssi} \quad \underset{k}{L \mid k^{1/p}}$$

En utilisant les propriétés des extensions linéairement disjointes, on obtient :

Théorème : Soient $k \subseteq F \subseteq L$

(a) si L/F et F/k sont séparables alors aussi L/k

(b) Si L/k est séparable alors F/k est séparable

Preuve : (a) On a $F \underset{k}{|} k^{1/p^\infty}$ et $L \underset{F}{|} F^{1/p^\infty}$

si

$$\begin{tikzcd}[column sep=small]
 & F^{1/p^\infty} \arrow[dr, dash] & & L \arrow[dl, dash] \\
k^{1/p^\infty} \arrow[ur, phantom, "\subseteq" sloped] \arrow[dr, dash] & & F \arrow[dl, dash] & \\
 & k & &
\end{tikzcd}$$

donc $L \underset{k}{|} k^{1/p^\infty}$

(b) c'est la conséquence du théorème utilisé pour la question (a). ☒

Remarque : On a si k est parfait, i.e. si $k^p = k$ que toute extension de k est séparable car en règle générale, on a pour L/k que $L \underset{k}{|} k$ par déf de $L \underset{k}{|} k^{1/p^\infty} = k$.

$\mathbb{R}(t)/\mathbb{R}$ aussi

Exemples : • $\mathbb{F}_p(t)/\mathbb{F}_p$ pour t transcendant, est séparable.

• Si L/k est finie, séparable ou bien que tout élément est séparable, alors si $e_1 \dots e_n$ est une base de k en L, $e_1 \dots e_n$ est générateur dans $k^{1/p^\infty} \cdot L$ comme k^{1/p^∞} ~~est~~ est toujours libre car sinon on aurait $\lambda_1 e_1 + \dots + \lambda_n e_n = 0$ $\lambda_1 \neq 0$ donc $e_1 = \sum_{i=2}^{n} \tilde{\lambda}_i e_i$ et donc e_1 est inséparable donc $e_1 \in k$, on aurait aussi une contradiction.

[Notez que L/k est séparable ssi toute extension F, $L \supseteq F \supseteq k$ f.g a une base de transcendance séparante]

Remarque : Base de transcendance séparante

Soit L/k une extension finiment engendrée et $t_1 \dots t_n \in L$ est tel que $L/k(t_1, \dots, t_n)$ est algébrique de degré fini et séparable on dit que $t_1 \dots t_n$ est une base de transcendance séparante.

Supposons que $L \supseteq F \supseteq k$ et que F soit f.g et que toute extension finiment engendrée admette une base de transcendance séparable, alors L/k est séparable. La réciproque est aussi.

• <u>Extensions régulières</u>

Une extension L/k est dite <u>régulière</u> si elle satisfait l'une des conditions équivalentes suivantes :

- L/k est séparable et k est algébriquement clos dans L
- $L \underset{k}{|} k^{alg}$

Le fait que le deuxième point implique le premier vient du fait suivant : $L \underset{k}{|} k^{alg} \Rightarrow L \underset{k}{|} k^{1/p^\infty}$ par déf puisque $k^{1/p^\infty} \subseteq k^{alg}$ et de plus cela implique $L \cap k^{alg} = k$ donc k est algébriquement clos dans L.

Pour montrer que le premier point implique le deuxième, on suppose que L/k est f.g on a alors une base de transcendance $t_1, \dots, t_n$ séparable (puisque L/k est séparable) qui <u>est</u> encore une base de transcendance séparable pour Lk^{sep}/k^{sep}.

$$\begin{tikzcd}[column sep=small] Lk^{sep} \arrow[d, dash] \arrow[dr, dash] & & k^{alg} \arrow[dl, dash] \\ L \arrow[dr, dash] & k^{sep} \arrow[d, dash] & \\ & k & \end{tikzcd}$$

On a donc en supposant $x_1 \dots x_n$ une famille k^{sep}-libre de Lk^{sep}, on écrit $x_i = P_i(t_1, \dots, t_n)$ et si on avait $\alpha_i \in k^{alg}$ $\sum \alpha_i x_i = 0$ on aurait $\sum \alpha_i P_i(X_1 \dots X_n)(t_1 \dots t_n) = 0$ et donc $t_1 \dots t_n$ seraient algébriques sur k^{alg} et donc sur k ce qui est absurde, donc on a bien $\alpha_i = 0$ et (x_i) est k^{alg}-libre.

Cela donne $Lk^{sep} \underset{k^{sep}}{|} k^{alg}$.

On conclut si on montre que $L \underset{k}{|} k^{sep}$ par la <u>transitivité</u> de $|$.

Or k^{sep}/k est une extension de Galois et $L \cap k^{sep} = k$ donc on a $L \underset{k}{|} k^{sep}$ et le résultat souhaité.

De même en utilisant les propriétés de $|$, on a

<u>Théorème</u> : Soit $k \subseteq F \subset L$

$\boxed{\begin{array}{l} \text{(a) Si } L/F \text{ et } F/k \text{ sont régulières alors aussi } L/k. \\ \text{(b) Si } L/k \text{ est régulière alors aussi } F/k \end{array}}$

<u>Rem</u> : C'est la propriété

$$L \underset{k}{|} k^{alg} \quad \text{ssi} \quad k^{alg} \underset{k}{|} F, \quad F^{alg} \underset{F}{|} L$$

__Remarque :__ Si k est algébriquement clos, comme $\forall L \supseteq k$ on a $L \underset{k}{|} k = k^{alg}$ on a que toute extension est __régulière__.

• __Extension régulière – extension libre__

On dit, si $E \underset{k}{\diagdown\diagup} F$ que __E est libre de F sur k__ si tout ensemble fini de E algébriquement indépendant sur k est algébriquement indépendant sur F.

Si $E \underset{k}{|} F$ et soit $x_1 \dots x_n \in E$ algébriquement indépendant sur k (et donc linéairement indépendant sur k) alors si $P[x_1 \dots x_n]$ dans $F[\bar{X}]$ avec $P(\bar{e_i}) = 0$ alors en écrivant en composantes homogènes, et en remarquant que les monômes $e_1^{i_1} \dots e_n^{i_n}$ sont alors une famille k-libre et alors F-libre et donc contradiction.

__Exemple :__ (k libre $\not\Rightarrow$ k-linéairement disjoint)

Soient E, F deux extensions algébriques distinctes, le degré de transcendance est 0 donc E et F sont libres sur k, et ça n'est pas le cas pour ~~donc~~ les disjonctions linéaires.

Par contre un résultat d'Artin établit la place. nous dit que si $E \underset{k}{\overset{reg}{\diagdown}\diagup} F$ et E libre de F sur k alors $E \underset{k}{|} F$.

On en déduit :

__Corollaire :__ (a) Si E est une extension régulière de k, $F \supseteq k$ et E libre de F sur k alors EF est régulière sur F.

(b) si $E \underset{k}{\overset{reg}{\diagdown}\overset{reg}{\diagup}} F$ et E libre de F sur k alors EF/k est régulière.

__Preuve :__ (a) Remarque que si E libre de F sur k alors E libre de F^{alg} sur k et donc par Artin, $E \underset{k}{|} F^{alg}$ et on a donc $FE \underset{F}{|} F^{alg}$ i.e. FE/F régulière.

(b) EF/F est reg et F/k aussi donc EF/k régulière

Exemple d'extension régulière :

- $\mathbb{F}_p(t)^{alg} / \mathbb{F}_p^{alg}$: séparable car $\mathbb{F}_p^{alg}$ est parfait, et $\mathbb{F}_p^{alg} \cap \mathbb{F}_p(t)^{alg} = \mathbb{F}_p^{alg}$. On aurait pu choisir n'importe quel extension de $\mathbb{F}_p^{alg}$.

- $\mathbb{F}_q(t) / \mathbb{F}_q$: • séparable. $\mathbb{F}_q$ est parfait (tout corps fini l'est)
- $\mathbb{Q}(\pi)/\mathbb{Q}$ • $\mathbb{F}_q^{alg} \cap \mathbb{F}_q(t) = \mathbb{F}_q$: $\mathbb{F}_q$ est algébriquement clos dans $\mathbb{F}_q(t)$.

- $(\mathbb{F}_q(1))^{sep}(t) / \mathbb{F}_q(t)$: • séparable ;
  • $(\mathbb{F}_q(t))^{alg} \cap (\mathbb{F}_q(1))^{sep}(t) = \mathbb{F}_q(t)$

- Extension primaire

Une extension L/K est primaire si elle vérifie une des deux conditions équivalentes suivantes :

(a) $L \cap K^{alg} / K$ est purement inséparable

(b) $\begin{array}{c} L \quad K^{sep} \\ \diagdown \ \diagup \\ K \end{array}$ (linéairement disjointes)

C'est la notion duale d'extension séparable.

Proposition : (a) Si $L \supseteq F \supseteq K$

L/K est primaire ssi L/F & F/K sont primaires

(b) Si K est séparablement clos ($K = K^{sep}$) alors toute extension de K est primaire.

Preuve : toujours pareil

On a vu qu'une extension régulière était séparable car $K^{1/p^\infty} \subseteq K^{alg}$, mais de même $K^{sep} \subseteq K^{alg}$ et donc clair qu'une extension régulière est primaire et séparable.

De même on montre que $L \mid K^{sep}$ et $L \mid K^{1/p^\infty} \Rightarrow L \mid K^{alg}$

On en déduit :

<u>Théorème</u> : L/k est régulière ssi L/k est primaire et séparable.

Enfin on a d'autres résultats :

<u>Proposition</u> : (a) $\begin{tikzcd}[column sep=small] F \arrow[dr, dash, "\text{prim}"'] & & E \arrow[dl, dash] \\ & k & \end{tikzcd}$ et F, E libres sur k alors $\begin{tikzcd} FE \arrow[d, dash] \\ E \end{tikzcd}$ primaire.

(b) $\begin{tikzcd}[column sep=small] F \arrow[rr, phantom, "\text{lin}"] \arrow[dr, dash, "\text{prim}"'] & & E \arrow[dl, dash, "\text{prim}"] \\ & k & \end{tikzcd}$ alors $\begin{tikzcd} FE \arrow[d, dash] \\ k \end{tikzcd}$ est primaire.

<u>Preuve</u> : Même genre qu'avec régulier. ∎

2ème Partie :

Géométrie Algébrique

Fermés de Zariski et ensembles constructibles

On introduit ici les bases de la géométrie algébrique, les fermés de Zariski, et on étudie cela du point de vue modèle théorique. Soit k un corps.

Soit $S \subseteq k[X_1 \dots X_n]$ on pose $V(S) = \{a \in k^n,\ p(a)=0 \ \forall p \in S\}$

Si $A \subseteq k^n$ on note $I(A) = \{p \in k[\bar{x}] \ \ p(a)=0 \ \forall a \in A\}$

Si $A = V(S)$ on dit que l'ensemble A est un fermé de Zariski, ou un ensemble algébrique (ou (sous)-variété affine).

$I(A) = \mathfrak{a}$ est l'idéal associé à l'ensemble algébrique A. Si $S \subseteq k[\bar{x}]$, $I(V(S)) \supseteq S$ mais l'inclusion peut être stricte. (exemple : $S = \{X^2-2\}$, $I(V(S)) = \langle x^2-2 \rangle$)

On résume ce que l'on peut prouver aisément à propos de ces ensembles :

(i) $A \subseteq k^n$, $I(A)$ est un idéal radical ~~et premier~~ ($f^n \in I \Rightarrow f \in I$)

(ii) $A = V(I(A))$ si A est algébrique. et $S \subseteq I(V(S))$ | en particulier tout ensemble algébrique est de la forme $V(\mathfrak{a})$

(iii) Si A et B sont des fermés de Z, $A \subseteq B \Rightarrow I(B) \subseteq I(A)$

(iv) Si A et B __________, $\mathfrak{a} = I(A)$, $\mathfrak{b} = I(B)$

$$A \cup B = V(\mathfrak{a} \cap \mathfrak{b}) \qquad A \cap B = V(\langle \mathfrak{a}, \mathfrak{b} \rangle)$$

On remarque donc que les ensembles algébriques sont clos par union et intersection finie, pour que cela définisse les fermés d'une topologie, il faudrait que ce soit clos par intersection quelconque.

Rappel : (Théorème de la base de Hilbert)

Si k est un corps, alors $k[X_1, \dots, X_n]$ est noethérien. ie il n'y a pas de chaîne infinie ascendante d'idéaux, en particulier tout idéal est finiment engendré.

On a donc que toute intersection infinie est en fait finie ce qui nous donne que les ensembles algébriques sont clos par intersection quelconque. Comme $\emptyset = V(1)$ et $k^n = V(0)$ il suit que l'ensemble des $\{ V(\mathfrak{a})$, $\mathfrak{a}$ idéal de $k[x_1 \dots x_n] \}$ ou $\mathfrak{a} = \emptyset$ est une topologie sur k^n, on l'appelle la <u>topologie de Zariski</u>.

On a établi que si $A, B, \mathfrak{a}, \mathfrak{b}$ sont respectivement des ensembles algébriques et leurs idéaux associés ($A = V(\mathfrak{a})$, $B = V(\mathfrak{b})$) alors $A = B$ ssi $\mathfrak{a} = \mathfrak{b}$ et comme les idéaux vérifient la condition de chaîne ascendante, les ensembles algébriques vérifient la condition de chaîne descendante.

Cette correspondance
$$\left\{ A \text{ ensemble algébrique de } k^n \right\} \longrightarrow \mathrm{Spec}_R(k[\bar{x}]) \underset{\text{idéaux radicaux}}{\cong}$$
$$A \longmapsto \mathfrak{a}$$

nous permet de définir une topologie sur $\mathrm{Spec}_R(k[\bar{x}])$ par si $C \subseteq \mathrm{Spec}_R(k[\bar{x}])$, C est fermé si il existe un idéal I de $k[\bar{x}]$ tel que $C = \{ p \in \mathrm{Spec}_R(k[\bar{x}]), I \subseteq p \}$.

D'un point de vue de la théorie des modèles, on peut voir que dans ACF_0, cette topologie correspond à la topologie de Stone, les ensembles algébriques étant type-définissables par des types qui ne sont pas le type transcendant (contenant au moins une formule $f(x) = 0$) ils sont donc clos et donc définissables.

On revient à la démo. D'abord une importante remarque :

<u>Remarque</u> : Pour un corps k, les ensembles définis par une formule atomique sont exactement ceux de la forme $V(P)$ pour $P \in k[\bar{x}]$. Il suit de cela que les combinaisons booléennes de fermés de Zariski sont exactement les ensembles définis par des formules sans quantificateurs.

On appelle $A \subseteq k^n$ un <u>ensemble constructible</u> si A est une combinaison booléenne de fermés de Zariski. Le raisonnement donne

Corollaire : Si k est algébriquement clos (et car $k = 0$)

$\boxed{A \subseteq k^n \text{ est constructible ssi } A \text{ est définissable}}$.

On utilise l'élimination des quanteurs et le raisonnement précédent, ou bien le fait que les types non [illegible] sont isolés.

<u>Théorème de Chevalley</u> : Si k est algébriquement clos, alors

> l'image d'un ensemble constructible par une application polynomiale est constructible.

<u>Preuve</u> : Si $A = \varphi[k^n]$ est constructible et $P : k^n \to k^m$ est un polynôme. Alors $B = \{ y \in k^m : \exists z \; y = P(z) \wedge \varphi(z) \}$ est définissable donc constructible. ∎

• <u>Le Nullstellensatz de Hilbert</u> <u>ici k algébriquement clos</u>.

On revient sur l'application
$$\{\text{Fermés de Z. de } k^n\} \longrightarrow \mathrm{Spec}_R(k[\bar x])$$
$$A \longmapsto I(A)$$

Il n'y a aucune raison pour qu'à deux idéaux a, b radicaux ne corresponde pas qu'un seul ensemble algébrique $A = V(a) = V(b)$. (si les idéaux étaient premiers ce serait le cas). (ex : $V(\langle X^2 \rangle) = V(\langle X \rangle) = \{0\}$ mais $\langle X^2 \rangle$ pas radical)

Mais cette correspondance est en vérité bijective, i.e., si J est un idéal radical alors $J = I(V(J))$.

On utilise la modèle-complétude de ACF.

On rappelle un fait sur la décomposition primaire des idéaux radicaux :

Fait : Si $I \subseteq k[\bar x]$ est un idéal radical alors il existe des idéaux premiers $P_1 \dots P_m$ tels que $I = P_1 \cap \dots \cap P_m$ et $I \neq \bigcap_{i \in J} P_i \; \forall J \subsetneq \{1..m\}$. Cette décomposition est <u>unique</u> (à ordre près).

Donc pour tout idéal radical $I \subsetneq J$, si $a \in J \setminus I$ il existe un idéal premier P tel que $I \subseteq P$ et $a \notin P$, on prend $P_1 \dots P_m$ la décomposition de J il existe P_i tq $a \notin P_i$ et $I \subseteq J \subseteq P_i$.

Théorème des Zéros de Hilbert : Soit k un corps algébriquement clos. On suppose que $\mathfrak{a}$ et $\mathfrak{b}$ sont deux idéaux radicaux de $k[x_1 \dots x_n]$ tels que $\mathfrak{a} \subsetneq \mathfrak{b}$. Alors $V(\mathfrak{a}) \supsetneq V(\mathfrak{b})$.
On a donc que $A \longrightarrow I(A)$ est bijective dans $\mathrm{Spec}_k(k[\bar{x}])$.

Preuve : Soit donc $p \in \mathfrak{b} \setminus \mathfrak{a}$, par le fait, il existe un idéal premier $P \supseteq \mathfrak{a}$ tel que $p \notin P$. Montrons qu'il existe $x \in V(P) \subseteq V(\mathfrak{a})$ tel que $p(x) \neq 0$, on aura donc $V(I) \neq V(J)$ (on a déjà que $I \subseteq J \Rightarrow V(I) \subseteq V(J)$). Comme P est premier, $k[\bar{x}]/_{(P)}$ est un anneau intègre et donc on considère F la clôture algébrique de son corps de fractions. Comme $k[\bar{x}]$ est noethérien, soient $q_1 \dots q_m$ les générateurs de J et $a_i := X_i/_P$. Comme chaque $q_i \in P$ et $p \notin P$ on a

$$F \models \bigwedge_{i=1}^{m} q_i(\bar{a}) = 0 \wedge p(\bar{a}) \neq 0$$

donc $F \models \exists \bar{x} \bigwedge_{i=1}^{m} q_i(\bar{x}) = 0 \wedge p(\bar{x}) \neq 0$ et comme $k \subseteq F$ on a par modèle complétude que $k \preceq F$ donc il existe un témoin dans k, disons $\bar{b}$, et $\bar{b} \in V(I) \setminus V(J)$. ■

Corollaire : Si $\mathfrak{a} \subseteq k[\bar{x}]$ est un idéal radical, $\mathfrak{a} = I(V(\mathfrak{a}))$.

Preuve : L'inclusion $\subseteq$ est claire, de plus $V(\mathfrak{a}) = V(I(V(\mathfrak{a})))$ et donc par précédemment $\mathfrak{a} = I(V(\mathfrak{a}))$. ■

N.B. : • La noethérianité nous dit que si F est un fermé de Zariski, alors $\exists\, q_1 \dots q_n$ tq $F = \{\text{zéros de } q_1 \dots q_n\}$.

• Les applications rationnelles conservent le fait d'être fermé cela signifie que les applications rationnelles sont les applications continues pour la topo de Zariski.

• Les sous-variétés sont toujours définissables par le thm de Hilbert, et dans le cas ACF, par EQ, comme les formules sans quanteurs définissent des sous-variétés, les ensembles définissables sont les sous variétés

Variétés algébriques

On définit dans cette section la notion de groupe algébrique en géométrie algébrique, pour cela on introduit d'abord la notion de variété algébrique. k est algébriquement clos.

• Variété et sous-variétés.

Dans la section précédente, on appelait ensemble algébrique ou fermé de Zariski ce que l'on appellera une sous variété (affine).

Une sous variété A est dite irréductible si A n'est pas réunion de deux fermés de Zariski, ie si il n'existe pas de $B, C \neq \emptyset$ avec $B \neq A$, $C \neq A$ et $A = B \cup C$.

On a alors que tout ouvert non vide de A est dense (et réciproquement).

On a de plus le théorème : A irréductible ssi $I(A)$ est premier.

Et enfin le théorème de décomposition :

Théorème : Toute sous variété affine non vide se décompose de façon unique (à permutation près) en une réunion finie de sous variétés affines irréductibles, non contenues l'une dans l'autre.

Notons que le Nullstellensatz peut se retraduire à la forme :

• L'application $\left\{ \begin{matrix} \text{sous variétés} \\ \text{irréductibles} \end{matrix} \right\} \longrightarrow \operatorname{Spec}(k[\bar{x}]) = \left\{ \begin{matrix} \text{idéaux} \\ \text{premiers} \end{matrix} \right\}$

$$A \longmapsto I(A)$$

est bijective.

• Le nullstellensatz et le théorème précédent nous donne qu'un idéal radical est donné par une intersection d'idéaux premiers.

Définition : Une (pré)variété est un espace topologique V tel que V est recouvert par un nombre fini d'ouverts

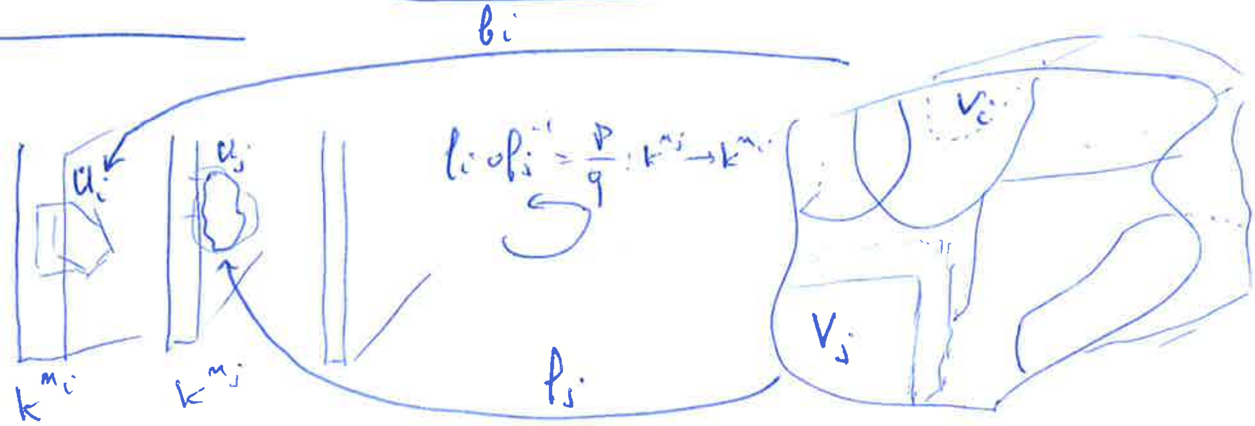
$$V = V_1 \cup \dots \cup V_n$$

tels que pour chaque i, il existe une sous variété U_i de k^{n_i} et un homéomorphisme $f_i : V_i \longrightarrow U_i$

tel que (i) $U_{ij} := f_i(V_i \cap V_j)$ est un ouvert de $U_i \subseteq k^{n_i}$

(ii) $f_{ij} := f_i \circ f_j^{-1} : \underset{\subseteq k^{n_j}}{U_{j,i}} \to \underset{\subseteq k^{n_i}}{U_{i,j}}$ est rationnelle (quotient de polys).

$f_1, \dots, f_n$ est un atlas de V.



Exemple : Soit k un corps algébriquement clos.

(i) Une sous-variété V de k^n est une variété, il suffit de voir que V est un ouvert de V, et que l'identité $V \longrightarrow V$ est un homéomorphisme dans un fermé de Zariski (= sous variété).

(ii) Si si V est une sous variété de k^n et que O est un ouvert de Zariski de k^n, $V \cap O$ est une variété.

En effet on écrit O comme F^c et F est un fermé de Zariski donc correspond aux zéros de polynômes $g_1 \dots g_n$, (type [illegible])
et donc $O = \cup O_i$ avec $O_i = \{x \in k^n, g_i(x) \neq 0\}$.

On pose $V_i = O_i \cap V$ on a alors $V \cap O = V_1 \cup \dots \cup V_n$, et V_i est un ouvert de V.

On a donc écrit $V \cap D = V_1 \cup \dots \cup V_m$ comme union d'ouvert de V. On pose

$$U_i = \{ (x,y) \in k^{n+1} : x \in V \text{ et } y g_i(x) = 1 \}$$

On a vu que U_i est un fermé de Zariski de k^{n+1} et soit

$$f_i : V_i \longrightarrow U_i, \quad x \longmapsto \left(x, \frac{1}{g_i(x)}\right)$$

f_i est rationnelle et c'est une bijection d'inverse $(x,y) \mapsto x$, et V_i et U_i sont homéomorphes. On a alors

$$U_{ij} = f_i(V_i \cap V_j) = \{ (x,y) \in U_i \,,\, g_j(x) \neq 0 \}.$$

c'est un ouvert de U_i et enfin

$$f_{ij} = f_i \circ f_j^{-1} : U_{j,i} \longrightarrow U_{i,j}$$

et on calcule, pour $(x,y) \in U_{j,i}$, $g_i(x) \neq 0$ et $f_{ij}(x,y) = \left(x, \frac{1}{g_i(x)}\right)$

- $\mathbb{P}_1(k) = \dfrac{k^2 \setminus \{(0,0)\}}{\sim}$ $\quad (x,y) \sim (x',y')$ ssi $\exists \lambda \;\; \lambda(x,y) = x',y'$ ssi $xy' = yx'$

On écrit $V_1 = \{ (x,y)/\sim \,,\, x \neq 0 \}$ $\quad V_2 = \{ (x,y)/\sim \,,\, y \neq 0 \}$ et $U_1 = U_2 = k$. On pose ensuite

$$f_1 : V_1 \longrightarrow U_1, \quad (x,y)/\sim \;\longmapsto\; y/x \qquad f_2 : V_2 \longrightarrow U_2, \quad (x,y)/\sim \;\longmapsto\; x/y$$

(ne dépend pas de la classe choisie). On a alors

$$U_{1,2} = U_{2,1} = k^\times = f_i\left(\{ (x,y)/\sim \,,\, x \neq 0 \wedge y \neq 0 \} \right)$$

et $f_{12} = f_1 \circ f_2^{-1} : k^\times \longrightarrow k^\times, \; x \longmapsto 1/x \;\; = f_{21}$.

$\mathbb{P}_1(k)$ est donc bien une variété.

Un fait important est que si k est ACF, alors les variétés sont irréductibles.

Théorème : Si V est une variété sur un corps $k \models ACF$

Alors V est interprétable dans k.

Preuve : Soit $V = V_1 \cup \dots \cup V_n$, $f_i : V_i \to U_i$ l'atlas correspondant, quitte à augmenter à rajouter des zéros on peut supposer $U_i \subseteq k^m$.

Soient $a_1 \dots a_n \in k$, distincts. Soit ensuite

$$X = \left\{ (x, y),\ x \in \bigcup_i U_i \ \& \ y \in \{a_1 \dots a_n\} \right\}$$

$X \subseteq k^{m+1}$ et est définissable car U_i le sont et y vérifie $\prod_{i=1}^{n} (x - a_i) = 0$.

Enfin on définit une relation d'équivalence sur X par

$$(x, y) \sim (x', y') \text{ ssi } y = y'$$

Ainsi chaque classe est un des U_i et $X/_\sim$ est la variété. ☒

Remarque : • Par élimination des imaginaires, on a que la variété est définissable dans k.
• On a besoin que k soit algébriquement clos.

On considère à présent les morphismes de variétés.
Si V et W sont deux variétés, $f : V \to W$ est un morphisme si on peut trouver $V_1 \dots V_n$, $W_1 \dots W_m$ des recouvrements de V et W par des ouverts affines avec l'atlas $f_i : V_i \to U_i$ $\quad g_j : W_j \to U_j'$

et U_i, U_j' sont des ouverts d'un fermé affine et

$$g_j \circ f \circ f_i^{-1} : k^{m_i} \to k^{m_j}$$

Si V est une variété avec atlas $f_i : V_i \to U_i$ et que $X \subseteq U_i$ alors $f_i^{-1}(X) \subseteq V$ est appelé un <u>ouvert affine</u> si X est un ouvert de U_i et un <u>fermé affine</u> si X est un fermé de U_i. L'épithète <u>affine</u> veut dire que on considère des ensembles dans V et on leur enlève une topo par l'homéomorphisme f_i. (même s'il y a déjà une topo dans V).

Remarquons que dans le cas de la caractéristique $p > 0$ on ne considère plus les morphismes mais les <u>quasimorphismes</u> où l'on demande à la composante d'être une fonction quasirationnelle (i.e. compo de rationnel et $x \mapsto \sqrt[p]{x}$).

On définit ensuite le produit de deux variétés :

<u>Définition</u> : Si V et W sont deux variétés sur K.
Soient $(f_i : V_i \to U_i)_{i=1,\dots,n}$ et $(g_j : W_j \to U_j')_{j=1,\dots,m}$ deux atlas pour V et W. Le <u>produit $V \times W$</u> est une variété définie par un enrichissement de la <u>topologie</u> produit $V_i \times W_j$ de façon à ce que

$$(f_i, g_j) : V_i \times W_j \longrightarrow U_i \times U_j'$$

soit un homéomorphisme. On obtient donc un recouvrement ouvert fini de $V \times W$.

<u>N.B</u> : La topologie sur $V \times W$ est un raffinement propre de la topologie produit.

On énonce et récapitule les propriétés des variétés.

- Si V est une variété et $X \subseteq V$ est ouvert alors X est une variété.
- Il n'y a pas de chaîne infinie descendante de fermés de V.
- Tout fermé de V est une union finie de composantes irréductibles.

Si V et W sont deux variétés :

- Si $f : V \longrightarrow W$ est un morphisme, f est continue.
- Si $f : V \longrightarrow W$ et $\forall a \in V$ $\exists$ voisinage $U(a)$ et $f_{|U(a)}$ est un morphisme dans un voisinage alors f est un morphisme.
- Le produit $V \times W$ est une variété et la topologie sur $V \times W$ est un raffinement de la topologie produit.

De la topologie de Zariski aux variétés algébriques

Cette fiche contient un récapitulatif des notions de géométrie algébrique nécessaires à l'étude des groupes algébriques. Elle est issue principalement de *Linear algebraic groups* de J. Humphreys. k est un corps algébriquement clos.

• Variété affine et le nullstellensatz

On travaille toujours dans un corps k algébriquement clos. Ce que l'on appelle ici variété affine et aussi appelé sous-variété fermée de Zariski, ensemble algébrique est un ensemble de k^n donné par $V(S)$ pour $S \subseteq k[X_1 \dots X_n]$. On rappelle que ces ensembles sont les fermés d'une topologie donnée appelée topologie de Zariski, qui fonctionne grâce au théorème de la base de Hilbert, donnant la noethérianité de $k[X]$ et donc la stabilité des variétés affines par intersection quelconque ainsi que le fait que les variétés affines soient définissables en nous modèle théorique dans le corps k.

Rappelons que $A \subseteq V(I(A))$ (= clôture de Zariski de A)

si $A = V(S)$ $\quad S \subseteq I(V(S))$

A chaque variété affine est associé un idéal mais il peut y en avoir plusieurs correspondant à la même variété affine par exemple $\langle X \rangle$ et $\langle X^2 \rangle$ définissent tout deux la même variété affine. Mais on a une bijection $A \longmapsto V(A)$, à condition que l'idéal associé demandé soit radical ($f^n \in I \Rightarrow f \in I$) (et k algébriquement clos)

Le Nullstellensatz dit que pour tout idéal $\mathfrak{a}$ de $k[T]$

$$\sqrt{\mathfrak{a}} = I(V(\mathfrak{a})) \qquad \left[\begin{array}{l} \sqrt{\mathfrak{a}} = \{ f \in k[T] \\ \exists n \; f^n \in \mathfrak{a} \} \end{array} \right.$$

Et que donc $A \mapsto I(A)$ est bijection dans le spectre radical de $k[T]$.

Donc à une variété affine A est associé un unique idéal radical, $I(A)$.
Les idéaux premiers sont des cas spéciaux des idéaux radicaux et la variété affine associée est appelée irréductible.
Les idéaux maximaux aussi sont radicaux et cela implique que si m est maximal, $V(m) \ni x$ alors $m \subseteq I(\{x\})$ et par maximalité on a $V(m) = \{x\}$ donc donc en cas l'ensemble des idéaux maximaux contient par injection l'ensemble des points de k^n. $\left[\begin{array}{l} \text{ex} : \langle X^2-2, Y+1\rangle \mapsto \{(-\sqrt{2},-1),(\sqrt{2},-1)\} \\ \text{mais corps alg. clos } \langle X-\sqrt{2}, Y+1\rangle = \{(\sqrt{2},-1)\}\end{array}\right.$
Notez que lorsque l'on parle d'une variété affine A en cet lien $n < \omega$ est sous-entendu c'est celui tq $A \subseteq k^n$ et $I(A) \subseteq k[T_1, \dots T_n]$.
Ce que l'on appelle une variété linéaire affine est l'ensemble des zéros de polynômes scindés, de la forme $\sum a_i (T_i - d_i)$ c'est donc un sous espace vectoriel de $k^n + (d_1 \dots d_n)$ i.e. un sous espace affine de k^n.

- Topologie de Zariski

On a donc que l'ensemble des fermés de Zariski (i.e. les n-variétés affines) munit k^n d'une topologie que l'on appelle la topologie de Zariski.
D'une part dans cette topologie les points sont fermés, car si $a = (a_1 \dots a_n)$, alors $\{a\} = V\left(\prod_{i=1}^{n} (T_i - a_i)\right)$. En revanche la topologie n'est pas séparée car deux ensembles fermés des points ont pour voisinage des ensembles cofinis qui s'intersectent. (dès k dense si infini)
La noethérianité implique la DCC sur les fermés et donc la ACC sur les ouverts qui se traduit par la compacité de la topo de Z. (⚠ ici on appelle compact la "propriété de Borel-Lebesgue, alors qu'un espace compact est " compact et séparé").

Pour une description informelle de la topologie de Zariski, on pourrait dire que les ouverts sont gros alors que les fermés sont petits. Par exemple si $n=1$ les ouverts sont les ensembles cofinis et les fermés sont ceux finis. (ce qui n'est évidemment pas vrai si $n>1$). Il faut penser une fermé de K^2 comme des courbes et aux ouverts comme leur complémentaires.

Un fermé est déterminé par l'intersection des zéros d'un nombre fini de polynômes, par conséquent donc tout ouvert s'écrit comme l'union finie des complémentaires que l'on appelle les ouverts principaux. Ce sont les bases d'ouvert de la topologie. Si $F = F_1 \cap \dots \cap F_n$ alors $F^c = \bigcup_{i=1}^{n} (F_i^c)$, ie si $F = \{\text{zéro de } g_1 \dots g_n\}$ alors $\mathcal{O}_i = \{x,\ g_i \neq 0\}$.

- Composante irréductible

Un ensemble topologique est dit irréductible si il ne peut pas être écrit comme union de deux fermés propres et non vide. (Notez que c'est l'analogue de la connexité dans un espace non séparé).

A est irréductible ssi tout deux ouverts non vide de A s'intersectent

ssi tout ouvert non vide de A est dense dans A

Un ensemble irréductible est connexe mais la réciproque n'est pas vraie.

On peut montrer par ZL que tout espace topologique se décompose en une union d'ensemble irréductible maximaux. Dans le cas d'un espace topo vérifiant la propriété de Borel-Lebesgue cette union est finie, on a donc le théorème de décomposition qui dit que toute variété affine se décompose en un nombre fini de variété affine irréductible.

On peut de plus montrer que

A irréductible ssi $I(A)$ est premier

Toute variété affine A s'écrit de
$$A = A_1 \cup \dots \cup A_n \quad \text{avec } I(A_i) \text{ premier.}$$
On a en particulier $I(A) = \bigcap_{i=1}^{n} I(A_i)$ et les idéaux radicaux sont des intersections d'idéaux premiers, conséquence du nullstellensatz.

- Produit de variétés affines

Une variété affine est un espace topologique, si $A \subseteq k^n$ et $B \subseteq k^m$ sont deux variétés affines le produit $A \times B$ peut être vu dans k^{n+m} cela va nous permettre de définir le produit de variétés affines. $A \times B$ est fermé dans k^{n+m} car si $A = V(P_1(T_1 \dots T_n) \dots P_n(T_1 \dots T_n))$ et $B = V(Q_1(S_1 \dots S_m), \dots Q_\ell(S_1 \dots S_m))$, alors on voit les P_i et Q_i comme polys de $k[T_1 \dots T_n, T_{n+1} \dots T_{n+m}]$ et $A \times B = V(P_i(T_1 \dots T_n), Q_i(T_{n+1} \dots T_{n+m}))$.

Notez que la topologie sur $A \times B$ (dans dans k^{n+m}) n'est pas celle de la topologie produit dans de top de A × top de B.

On identifie $A \times B$ avec une et une seule variété affine incluse dans k^{n+m}. [ex : $V_1 = \{\pm 1\} = V(X^2-1)$, $V_2 = \{\pm\sqrt{2}\} = V(X^2-2)$; $V_1 \times V_2 = V(\{X^2-1, Y^2-2\}) = \{(\pm 1, \pm\sqrt{2})\}$]

On a que si $A \subseteq k^n$, $B \subseteq k^m$ sont des variétés affines irréductibles alors $A \times B \subseteq k^{n+m}$ est irréductible.

[Raffinement propre de produit : sur k : ouvert = cofini donc topo produit : ouvert = produit d'ouvert donc si topo sur k^2 = topo produit, ouvert = cofini or on sait que par exemple $V(XY=1)$ est un fermé et est infini non cofini]

- Algèbre affine :

Soit A une variété affine, $\mathfrak{a} = I(A)$ est un idéal radical. On définit l'algèbre affine $\dfrac{k[T]}{\mathfrak{a}}$ de A que l'on note $k[A]$. C'est une algèbre qui n'a pas d'éléments nilpotents. On l'appelle aussi l'algèbre des fonctions polynômes de A. (ce sont des f°t $A \to k$)

Soit $f \in k[T]$, f définit une fonction $f : A \to k$, $\bar{a} \mapsto f(\bar{a})$.

Mais si $g \in \mathfrak{a}$ alors $g(\bar{a}) = 0$ et donc $f+g$ définit la même fonction sur A on a donc $f + \mathfrak{a} \in k[A]$ est l'unique

fonction dans $k[A]$ prenant sur A la valeur de f.
On voit que le rôle de $k[A]$ pour A est le même que celui de $k[T]$ pour k^n.

- Si A est une variété affine irréductible alors $k[A]$ est un anneau intègre et on note $k(A)$ son corps de fraction appelé le corps de fonction rationnelle de la variété affine irréductible A.

C'est une extension $k(A)/k$ finiment engendrée.

On peut en fait par cette remarque expliquer une définition des variétés affines ne dépendant plus d'un corps ambiant k^n.
On donne A comme un espace topologique noethérien (vérifiant la prop de Borel-Lebesgue) dit la topo de Zariski avec comme base des ouverts principaux $A_f = \{a \in A \mid f(a) \neq 0\}$

- Les fermés de A sont en bijection avec les idéaux radicaux de $k[A]$ (une version du nullstellensatz pour $k[T]/_{I(A)}$).
- Les points de A (= éléments de A) sont en bijection avec les idéaux maximaux de $k[A]$
- Les ensembles irréductibles de A sont en bij avec les idéaux premiers de $k[A]$.

On peut donc "reconstruire" A avec la donnée de $k[A]$.
On dit qu'un anneau R est réduit si il n'y a pas d'élément nilpotent non trivial.
La discussion précédente va nous permettre d'identifier la donnée d'une k-variété affine avec la donnée d'une k-algèbre finiment engendrée réduite.

- Morphismes de variétés affines

Soient A, B deux variétés affines de k^n, k^m resp.
Un <u>morphisme</u> $\varphi : A \to B$ est la donnée de
$\varphi_1 \dots \varphi_m \in k[A]$ (classes de polys $k[T]$) tels que
$$\varphi(a_1 \dots a_n) = (\varphi_1(a_1 \dots a_n), \dots, \varphi_m(a_1 \dots a_n)).$$

Un morphisme $A \to B$ induit toujours un morphisme
$k^n \to k^m$, et un morphisme $A \to k$ est une fonction
polynomiale sur A.
On montre facilement que si $\varphi . A \to B$ est un
morphisme, alors φ est <u>continue pour la topologie de Zariski</u>

Pour la culture, notons qu'un morphisme $\varphi : A \to B$ a associé
$\varphi^* : k[B] \to k[A]$ défini par $\varphi^*(f) = f \circ \varphi$,
que l'on appelle le <u>comorphisme</u> de φ.
La correspondance $\varphi \mapsto \varphi^*$ est en fait un <u>foncteur</u>
<u>contravariant</u> allant de la catégorie des <u>variétés affines</u>
(avec pour flèches les morphismes) et celle des <u>algèbres affines</u>
(avec pour flèches les homomorphismes de k-algèbre).

- <u>Anneau locale</u>

On montre ici une étude locale d'une variété A affine.
Si $a \in A$, on peut d'abord supposer A irréductible, soit
donc $k(A)$ le corps des fractions rationnelles de polynomes (modulo
$I(A)$) défini sur A. On note $\mathcal{O}_a$ <u>l'anneau des $f \in k(A)$</u>
<u>qui sont définies en a</u> (i.e. $f = g/h$, $g, h \in k[A]$, $h(a) \neq 0$)
On a $k[A] \subseteq \mathcal{O}_a$. On appelle $\mathcal{O}_a$ l'anneau local de a
sur A. Notez que l'anneau local $\mathcal{O}_a$ est un anneau pour la
multiplication ($(f \cdot g)(a) = f(a) \cdot g(a)$.) et que c'est un anneau

locale au sens algébrique du terme, et l'idéal maximal de $\mathcal{O}_a$ est l'ensemble des $\frac{g}{h}$ où $h(a) \neq 0$, $g(a) = 0$, $g, h \in k[A]$.

On a le fait suivant, si A est une variété affine irréductible :
$$k[A] = \bigcap_{a \in A} \mathcal{O}_a$$

Preuve : $\subseteq$ est clair. Réciproquement si $f = g/h \in k(A)$ et $f \in \mathcal{O}_a$ $\forall a \in A$, donc $h(a) \neq 0$. g et h ne sont pas uniques et si on considère l'idéal I engendré par tous les h_i tq $\exists g_i$ $f = \frac{g_i}{h_i}$, si I était un idéal propre alors le Nullstellensatz impliquerait un zéro commun (un élément de $V(\sqrt{I})$ car $0 \neq \sqrt{I} \neq k[A]$) ce qui est absurde. Donc $I = k[A]$ et donc $1 = \sum l_i h_i$, $f = g_i/h_i$ donc $f = \sum g_i l_i \in k[A]$ ■

On montre de la même façon que si $U \subseteq A$ est un ouvert, on appelle cette fois le sous-anneau de $k(X)$ des fonctions régulières sur U, (ie définies partout) on le note $\mathcal{O}_A(U)$ et on a $\mathcal{O}_A(U) = \bigcap_{a \in U} \mathcal{O}_a$

On a donc $\mathcal{O}_A(A) = k[A]$; ie seuls les polynômes sont définis sur tout A.

$\mathcal{O}_A$ est ce que l'on va appeler un faisceau de fonctions sur la variété A. On montre d'abord comment on définit le faisceau sur une variété affine (non nécessairement irréductible).

Si A est une variété affine, $A = A_1 \cup \dots \cup A_l$, ses composantes irréductibles. Pour U un voisinage ouvert de $a \in A$, on dit que $f : U \longrightarrow k$ est régulière en a si il existe $g, h \in k[A]$ et un ouvert $V \subseteq U$ voisin de a tel que $\forall b \in V$ $h(b) \neq 0$ et $f(b) = \frac{g(b)}{h(b)}$. f est donc localement sur U une fonction rationnelle de $k[A]$.

On définit alors $\mathcal{O}_A(U)$ comme l'anneau des fonctions régulières en tout point de U.

On a encore $\mathcal{O}_A(A) = k[A]$.

• Faisceau de fonctions

Pour une variété affine A, $\mathcal{O}_A : \{\text{ouverts de } A\} \longrightarrow \{k\text{-algèbres}\}$ amène à chaque ouvert de A une k algèbre, celle des fonctions "localement rationnelles" définies sur l'ouvert et à valeurs dans k.

Si X est un espace topologique, et k un corps, un <u>faisceau de fonctions sur X</u> est une fonction

$$\mathcal{F} : \left\{ \begin{array}{c} \text{ouverts de } X \\ = \text{topo de } X \end{array} \right\} \longrightarrow \left\{ \begin{array}{c} k \text{ algèbre de fonctions à valeurs} \\ \text{dans } k \text{ définies sur des ouverts} \\ \text{de } X \end{array} \right\}$$

telle que si $U \subseteq X$ ouvert, $\mathcal{F}(U)$ est une k algèbre de fonctions de $U \to k$ et tq

(S1) $U \subseteq V$ deux ouverts, $f \in \mathcal{F}(V)$ alors $f_{|U} \in \mathcal{F}(U)$

(S2) si U ouvert $U = \bigcup_{i \in I} U_i$ recouvrement d'ouverts, si $f_i \in \mathcal{F}(U_i)$ et $f_i|_{U_i \cap U_j} = f_j|_{U_i \cap U_j}$ $\forall i, j \in I$, alors il existe $f \in \mathcal{F}(U)$ tel que $\forall i$ $f_{|U_i} = f_i$.

L'application $\mathcal{O}_A$ est un faisceau de fonctions sur A.

On associe donc à une variété affine un faisceau. On parle donc de $(A, \mathcal{O}_A)$.

Si A, B sont deux espaces topologiques, $\mathcal{O}_A$, $\mathcal{O}_B$ sont deux faisceaux sur A et B (et corps non précisé k).

Alors <u>$(A, \mathcal{O}_A)$ est isomorphe à $(B, \mathcal{O}_B)$</u> si

- A est homéomorphe à B, soit donc $T : A \longrightarrow B$ un homéomorphisme
- Si U est un ouvert de A, $TU = V$ est un ouvert de B et on a un isomorphisme de k-algèbres entre

$$\mathcal{O}_A(U) \text{ et } \mathcal{O}_B(V).$$

• Prévariété

On donne à présent la définition générale de prévariété abstraite, obtenue par "recollement" de variétés affines.

Une prévariété est un espace topologique noethérien A muni d'un faisceau $\mathcal{O}_A$ de fonctions à valeurs dans k. tel que $A = U_1 \cup \dots \cup U_\ell$ (U_i des ouverts de A) et pour chaque i, $(U_i, \mathcal{O}_{A|U_i})$ est isomorphe à une variété affine.

On rappelle qu'un espace topologique est noethérien si ses ouverts vérifient ACC. (ou ses fermés la DCC).

Les éléments de $\mathcal{O}_A(U)$ sont appelés les fonctions régulières de U.

Les U_i tels que $A = U_1 \cup \dots \cup U_n$ sont les ouverts affines. Plus généralement une ouvert affine d'une prévariété est un ouvert isomorphe (avec $\mathcal{O}_{A|..}$) à une variété affine.

La topologie sur une prévariété a pour base les ouverts affines (qui viennent des ouverts principaux (U_f) des variétés affines recouvrant la prévariété).

Un sous ensemble est localement clos si c'est l'intersection d'un ouvert et d'un fermé. (ex : un ouvert, un fermé)

Si U est un ensemble localement clos d'une prévariété $(A, \mathcal{O}_A)$. Alors $(U, \mathcal{O}_{A|U})$ est une sous-prévariété de A. (donc tout ouvert, tout fermé d'une prévariété)

• Prévariété irréductible

On rappelle qu'un espace topologique est irréductible si tout deux ouvert s'intersectent.

Une prévariété $(A, \mathcal{O}_A)$ irréductible. $A = U_1 \cup \dots \cup U_n$ vérifie que $U_i \cap U_j \neq \emptyset$. Remarque qu'un ouvert d'un topo irréductible est irréductible pour la topo induite donc les U_i sont des variétés affines irréductibles avec pour corps algèbre affine $k(U_i)$. On a alors $k(U_i) = k(U_j)$ et on

l'appelle le corps de fonctions $k(A)$ de A.
Noter qu'un espace topologique noethérien n'a qu'un nombre fini de composantes irréductibles, c'est donc aussi le cas pour une prévariété, on a donc que chaque prévariété se décompose en un nombre fini de prévariétés irréductibles (max), et chacune de ces prévariétés a un corps de fonctions associé.

• <u>Morphisme</u> : On note A, B deux prévariétés
Une application $\varphi : A \longrightarrow B$ est un <u>morphisme</u> si φ respecte (1) la topologie de A
(2) le faisceau de A $\mathcal{O}_A$

autrement dit

(M1) φ est continue

(M2) Si $V \overset{\text{ouvert}}{\subseteq} B$ et $U = \varphi^{-1}(V)$ alors $\forall f \in \mathcal{O}_B(V)$ (i.e. $f : V \longrightarrow k$ régulière sur V) on a $f \circ \varphi : U \longrightarrow k \in \mathcal{O}_A(U)$.

Cette définition coïncide avec la notion de morphisme de variétés affines.
La restriction d'un morphisme à une sous-prévariété est encore un morphisme.

La condition (M2) permet via $f \mapsto f \circ \varphi$ d'induire un homomorphisme de k-algèbres $\varphi^*_{(V)} \mathcal{O}_B(V) \longrightarrow \mathcal{O}_A(\varphi^{-1}(V))$
Si A et B sont irréductibles, tout ouvert est dense donc $\varphi(A)$ est dense dans B donc $\varphi^* = \varphi^*_{(B)} : k(B) \longrightarrow k(A)$
Comme φ^* est injective il suit que l'on peut considérer $k(A) / k(B)$ comme une extension de corps.

Le critère suivant, appelé <u>critère affine</u> est très utile pour vérifier qu'une application est bien un morphisme.

<u>Critère affine</u> : Soient $\varphi : A \to B$ une application entre deux préviétés. Supposons qu'il existe $U_1 \dots U_n$, $V_1 \dots V_n$ tels que

$$(a)\quad A = U_1 \cup \dots \cup U_n \qquad B = V_1 \cup \dots \cup V_n .$$

$$(b)\quad \varphi(U_i) \subset V_i \qquad i = 1 \dots n$$

$$(c)\quad f \circ \varphi \in \mathcal{O}_A(U_i) \qquad \forall f \in \mathcal{O}_B(V_i)$$

Alors φ est un morphisme.

Dans le cas d'une préviété irréductible A, une fonction régulière $f \in \mathcal{O}_A(A)$ (localement égale à une fonction rationnelle définie sur tout A, donc sans pôles) définit un morphisme

$$f : A \longrightarrow k$$

mais une fonction rationnelle n'est pas forcément régulière.

Mais si $f \in k(A)$ et si U_i, $i = 1 \dots l$ recouvre A, alors sur chaque U_i, l'ensemble où f est définie est un ouvert donc l'union de ces ensembles est un ouvert $U \subset A$ c'est l'ouvert sur lequel f est définie, f induisant un morphisme $U \longrightarrow k$.

On a traité le cas des <u>fonctions régulières</u> définies partout (sur tout U si $f \in \mathcal{O}_A(U)$, sur tout A si $f \in \mathcal{O}_A(A)$) et celui d'une fonction rationnelle $\in k(X)$ où on a prouvé l'existence d'un ouvert U sur lequel elle était définie. Ensuite, comme avant on notera A_f l'ouvert de U sur lequel $f \neq 0$.

De même $V(f) = \{a \in A,\ f(a) = 0\}$ pour $f \in \mathcal{O}_A(A)$.

• <u>Morphisme birationnel</u> :

On a vu qu'un morphisme $\varphi : A \to B$ induisait un <u>comorphisme</u> $\varphi^* : \mathcal{O}_B(B) \longrightarrow \mathcal{O}_A(A)$. Si A et B sont irréductibles, on a affaire à une injection de corps i.e un monomorphisme $\varphi^*: k(B) \longrightarrow k(A)$.

Réciproquement un monomorphisme $k(B) \longrightarrow k(A)$, si A et B sont irréductibles, induit un morphisme partiel i.e un morphisme de $U \overset{\text{ouvert}}{\subseteq} A \longrightarrow B$. En effet on remplace A et B par des ouverts affines (cela ne change pas $k(A)$, $k(B)$ comme A et B sont irréductibles), maintenant on a B défini engendré par $f_1 \dots f_n$ (i.e $B = V(f_1 \dots f_n)$) et alors on a, $k(B) = k(f_1, \dots f_n)$ et on pose $g_i = \tau(f_i)$, il existe alors un ouvert de A sur lequel les g_i sont définis et un U tq $g_i \in k[U]$ il existe alors un unique morphisme $U \longrightarrow B$ qui a $\tau: k[B] \longrightarrow k[U]$ comme comorphisme.

On dit qu'un morphisme $\varphi: A \longrightarrow B$ est <u>birationnel</u> si le comorphisme $\varphi^*: k(B) \longrightarrow k(A)$ est un isomorphisme.

Deux prévariétés irréductibles qui ont un corps de fonctions isomorphe sont dites <u>birationnellement équivalentes</u>, elles ne sont pas nécessairement isomorphes.

• <u>Produit</u>

Le produit de deux prévariétés est défini comme le produit au sens catégorique. On ne le fait pas ici en détaille. La théorie des catégories nous dit que si il existe, le produit est unique. Il faut donc montrer que le produit au sens catégorique existe.

On admet la construction du produit de deux prévariétés i.e que la catégorie des prévariétés admet un produit qui est donc unique. Notez que étant données A et B deux prévariétés, la prévariété produit $A \times B$ est une prévariété munie de la topologie produit de Zariski et c'est un raffinement propre de la topologie produit.

On a donc l'existence des projections $A \times B \xrightarrow{p_1} A$ $A \times B \xrightarrow{p_2} B$ qui sont continues et ouvertes.

- Variété

Une prévariété A est appelée une variété si la diagonale $\Delta(A) = \{(x,x) \mid x \in X\}$ est un fermé de $A \times A$ la prévariété produite. (axiome d'Hausdorff) (H)
C'est équivalent à l'axiome de séparation : (S)

$\forall B$ prévariété et des morphismes $\varphi, \psi : B \to A$
alors $\{b \in B \mid \varphi(b) = \psi(b)\}$ est un fermé de B.

En effet, si (S) est vrai alors comme ça dépend des projections $A \times A \overset{P_1}{\underset{P_2}{\rightrightarrows}} A$ on a que $\Delta(A)$ est un fermé.
Réciproquement si (H) est vraie pour A on utilise

$$\Phi : B \xrightarrow{(\varphi,\psi)} A \times A \overset{Pr_1}{\underset{Pr_2}{\rightrightarrows}} A \qquad \Phi \to A$$

alors l'image inverse de $\Delta(A)$ par Φ est un fermé car par définition du produit les projections sont continues et $\Phi^{-1}(\Delta(A))$ est $\{b \in B \mid \varphi(b) = \psi(b)\}$.

Exemples : (1) Une variété affine est une variété car pour $A \subset k^n$ la diagonale est $V(\{T_i - T_j \; ; 1 \le i, j \le n\})$ qui est fermé.
(2) Les sous-prévariétés d'une variété on a encore la diagonale fermée ce sont des variétés et on les appelle les sous-variétés.
(3) Le produit de deux variétés est une variété.

C-exemple : Soit A la prévariété $A = U \cup V$ avec $U \cong k$, $V \cong k$, et $\forall x \neq 0$ $x_U \in U$ et $x_V \in V$, $x_U = x_V$ mais si $x = 0$ $x_U \neq x_V$.
A n'est pas une variété car si $f_1 : k \to U$ id
$f_2 : V \to V$
alors $\{x \text{ tq } f_1(x) = f_2(x)\} = k \setminus \{0\}$
ce n'est pas un fermé car les fermés de Zariski de k sont les ensembles finis, k et les ouverts sont les ensembles infinis et $\emptyset$

Critères : • Si A est une pré-variété tel que pour toute paire x, y il existe un ouvert affine de A qui contient x et y alors A est une variété.

Proposition : Soit B une variété, A une pré-variété.

a) $\varphi : A \to B$ est un morphisme alors le graphe
$$\Gamma_\varphi = \{ (x, \varphi(x)) \mid x \in A \}$$
est un fermé de $A \times B$ la pré-variété produit.

b) Si $\varphi, \psi : A \to B$ sont des morphismes qui sont égaux sur un sous ensemble dense de A alors $\varphi = \psi$.

b) : En particulier si A est irréductible et que $\varphi = \psi$ sur un ouvert de A alors $\varphi = \psi$.

• Dimension d'une variété

Pour une variété irréductible A on associe un corps de fonction (= corps des fonctions rationnelles) $k(A)$. On a que $k(A)/k$ est une extension de corps finiment engendrée donc a un degré de transcendance fini sur k on l'appelle la dimension de A.

Si A n'est pas irréductible il existe des composantes irréductibles en nombre fini (car A est Noethérien) donc $A = A_1 \cup \dots \cup A_n$ et on définit $\dim A = \max_i \dim A_i$

Si A est irréductible, comme $k(A) = k(U)$ pour tout ouvert affine on a $\dim A = \dim U$ et $\dim A = \dim A_f$ $\forall f \in k(A)$

Exemple : $Gl_n(k)$: On se place dans k^{n^2} on considère le polynôme det alors si $A = k^{n^2}$ c'est une variété qui est de dimension n^2 (voir après) et $Gl_n(k)$ est un ouvert principal, défini par $\det \neq 0$, $\det \in k[T_1 \dots T_{n^2}]$ on a donc $Gl_n(k) = A_{\det}$ donc $\dim Gl_n(k) = \dim k^{n^2} = n^2$

Exemple ($k^n = A$ est une variété irréductible de dim n)

Car l'algèbre associée est $k[T_1 \dots T_n]$ qui est un anneau intègre donc $I(A)$ premier (en fait (0)) irréductible et $k(T_1 \dots T_n)/k$ est de dim n puisque $\operatorname{tr\,deg}(k(T_1 \dots T_n)/k) = n$ car $T_1 \dots T_n$ est une famille algébriquement indépendante maximale.

La dimension se comporte bien sur le produit de variétés irréductibles : $\dim X \times Y = \dim X + \dim Y$

• Dimension d'une sous-variété

On a le résultat suivant :

• Si A est une variété irréductible, si Y est un fermé de A irréductible alors $\dim Y < \dim A$.

On appelle codimension de B dans A, pour B une sous variété de la variété A, notée $\operatorname{codim}_A B$ le nombre $\dim A - \dim B$.

• Si A est une variété affine irréductible, B un fermé irréductible de codimension 1 alors B est la composante (irréductible) de $V(f)$ pour un certain $f \in k[A]$.

• Hypersurfaces

Une hypersurface de k^n est un ensemble de la forme $V(f(T_1 \dots T_n))$ pour $f \in k[T_1 \dots T_n]$. Ses composantes irréductibles sont les $V(f_i)$ pour f_i les facteurs irréductibles de f.

Une hypersurface d'une variété affine A, une hypersurface est un sous ensemble de la forme $V(f)$ pour $f \in k[A]$. C'est une sous-variété affine.

Exemple : $Sl_n(k)$ est une hypersurface de $Gl_n(k)$, c'est $V(\det - 1 = 0)$.

• Les composantes irréductibles d'une hypersurface de k^n sont de codimension 1.

Exemple : $\dim Sl_n(k) = n^2 - 1$

Ce résultat est vrai pour les hypersurfaces de variétés affines :

• Si A est une variété affine irréductible, $f \in k[A] \setminus \{0\}$ et B une composante irréductible de $V(f)$, alors $\operatorname{codim}_A B = 1$.

On a la conséquence importante de ce fait :

• Si A est une variété irréductible, B un fermé irréductible de A de codimension $r \geq 1$, Alors il existe des fermés irréductibles B_i de codimension i pour $i = 1, \dots, r$ tels que

$$\begin{array}{ccccccccc} A & \supseteq & B_1 & \supseteq & B_2 & \supseteq \cdots & \supseteq & B_r = B \\ | & & | & & | & & & | \\ \dim A & & \dim A - 1 & & \dim A - 2 & \cdots & & \dim B \end{array}$$

• <u>Ensembles constructifs</u>

Un ensemble $Z \subseteq A$ une variété est dit <u>constructible</u> s'il est une combinaison booléenne d'ouverts et de fermés.

Un ensemble constructible contient un ouvert dense dans sa clôture.

Si $\varphi : A \longrightarrow B$ est un morphisme de variétés alors l'image d'un ensemble constructible est constructible, en particulier $\varphi(A) \subseteq B$ est un ensemble constructible.

Variété affine sur un non corps

On a plutôt étudié la notion de variété affine sur un corps $\mathbb{K}$ algébriquement clos, et en effet le théorème du Nullstellensatz a pour hypothèse que le corps choisi est algébriquement clos, sinon on pourrait avoir des idéaux non triviaux (et maximaux) qui nous donnent des variétés vides comme par exemple dans $\mathbb{R}$, l'idéal $< X^2+1 >$ ~~ou~~ $< X^2+Y^2+1 >$ dans $\mathbb{R}^2$ nous donne des variétés vides, mais pas dans $\mathbb{C}$.

De même l'irréductibilité d'une variété elle aussi a une dépendance au corps de base, par exemple, la variété définie par $x^2+y^2=0$ dans $\mathbb{Q}$ (ou $\mathbb{R}$) est réduite à $\{(0,0)\}$ alors que dans $\mathbb{Q}(i)$ elle est infinie, c'est l'union de 2 droites linéaires $(x-iy)(x+iy)=0$ et chacune de ces droites est irréductible de $V(x^2+y^2=0)$ est dans le cas $\mathbb{Q}$ (ou $\mathbb{R}$) irréductible (car 1 pt) et dans le cas $\mathbb{Q}(i)$ (ou $\mathbb{C}$) pas irréductible. (C'est juste dire que $x^2+y^2=0$ se scinde dans $\mathbb{Q}(i)$).

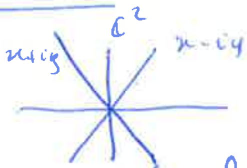
On voit donc qu'il faut prendre des précautions mais on peut se permettre de travailler dans un corps $\mathbb{K}$ algébriquement clos et parler d'une variété V <u>définie sur $F \subseteq \mathbb{K}$</u> si $I(V)$ ($\subseteq \mathbb{K}[\bar{x}]$) est engendré par $I(V) \cap F[\bar{x}]$ (autrement dit $\mathbb{K}\cdot I(V) \cap F[\bar{x}] = I(V)$)

Par exemple $x^2+y^2=0$ est définie sur $\mathbb{Q}$.

L'exemple précédent nous dit que l'on voit uniquement ce qu'est la variété sur un corps algébriquement clos.

De plus si V est défini sur $F \subseteq \mathbb{K}$ et on a $\sigma \in \mathrm{Aut}(\mathbb{K}/F)$ alors $V = V_1 \cup \cdots \cup V_n$ les composantes irréductibles

On a que σ permute les composantes V_i. Par exemple pour $x^2+y^2=0$ on a 2 droites



(qui s'intersectent en O = le point de V sur $\mathbb{Q}$) et σ permute les 2 droites, en effet si $\sigma \in \mathrm{Aut}(\mathbb{C}/\mathbb{R})$ $\sigma = \mathrm{Id}$ on a donc $\sigma(x+iy) = x-iy$.

Notons que la notion de variété ne dépend pas du corps algébriquement clos $\mathbb{K}$ avec lequel on travaille on peut mettre $\mathbb{K} = \mathbb{C}$ ou $\mathbb{K} = \overline{\mathbb{Q}}$ ou $\mathbb{K} = \mathbb{C}(X)^{alg}$ ou $\mathbb{K} = \mathbb{F}_p^{alg}$ etc.

Le théorème suivant est fondamental :

Théorème : Soit $V \subseteq \mathbb{K}^n$ une variété affine. Alors V a un plus petit corps de définition.

La démonstration est faite dans le cours de Chatzidakis, elle montre de plus

• V variété affine de $\mathbb{K}^n$, $I = I(V)$ et k_0 le corps de définition de V et $\sigma \in \mathrm{Aut}(\mathbb{K})$.

$$\sigma V = V \iff \sigma(I) = I \iff \sigma \text{ fixe } k_0.$$

• Topologie restreinte

On a donc que si $F \subseteq \mathbb{K}$, il existe une topologie de Zariski sur F, elle a les fermés sont de la forme $V(I) \cap F^n$ où $V(I) = \{\bar{x} \in \mathbb{K}^n, f(\bar{x}) = 0 \ \forall f \in I\}$ puis $I \subset F[X] \subseteq \mathbb{K}[\bar{X}]$. On pourrait croire que cette topologie dépend de $\mathbb{K}$ mais du moment que $\mathbb{K}$ est algébriquement clos, ce n'est pas le cas, on pourrait donc définir la topologie de Zariski dans n'importe quel corps F et prendre comme corps alg. F^{alg}.

· Dimension.

On rappelle que si V est une variété définie sur $\mathbb{K}$ on définit l'algèbre affine : $\mathbb{K}[V] = \dfrac{\mathbb{K}[x]}{(I(V))}$

C'est une algèbre réduite (non nilpotents) qui est intègre si V est irréductible dans ce cas on pose $\mathbb{K}(V)$ son corps de fraction, que l'on appelle le corps des fonctions rationnelles ou corps affine, on a vu que l'on peut considérer $\mathbb{K}[V]$ comme le ~~corps~~ ann. des fonctions ~~rationnelles~~ polys définies sur V.

Si V est une variété affine irréductible on appelle dimension de V $\dim V$ le degré de transcendance de $\mathbb{K}(V)$ sur $\mathbb{K}$, si V n'est pas irréductible on prend le maximum des composantes.

Noter que si V est irréductible et $f \in \mathbb{K}(V)$ alors f (qui est en fait $f = f + I(V)$) est défini sur un ouvert de V ouvert principale.

Exemple de calcul de dimension : $A^n = \mathbb{K}^n$. alors $I(A^n) = (0)$ donc $\mathbb{K}[A^n] = \mathbb{K}[X_1 \dots X_n]$ et donc $\mathbb{K}(A^n) = \mathbb{K}(X_1, \dots, X_n)$ et tr deg $(\mathbb{K}(X_1 \dots X_n)/\mathbb{K}) = n$ donc $\dim A^n = n$.

Si $f \in \mathbb{K}[\underset{X_1 \dots X_n}{\bar{X}}]$ alors $\dim V(f) = n-1$, en effet les composantes irréductibles $V_1 \dots V_k$ de $V(f)$ sont en corresp. avec les facteurs irréductibles de $f = f_1 \dots f_k$, comme pour f_i irréductible, on a $\mathbb{K}(V_i) = \dfrac{\mathbb{K}[X_1 \dots X_n]}{(f_i)}$. f_i donne une relation d'algébricité entre $X_{i1} \dots X_{il}$ et donc l'un des X_i n'est plus indépendant sur les autres d'où tr deg $(\mathbb{K}(V_i)) = n-1$ et donc $\dim V(f) = n-1$

• <u>Point générique</u> :

Soit V une variété affine irréductible définie sur $F \subseteq \mathbb{k}$

Soit $\bar{a} \in V$ est <u>un générique</u> de V sur F si

$$F(V) \longrightarrow F(\bar{a})$$

$$\bar{X}/I(V) \longmapsto \bar{a}$$

est un isomorphisme. De manière équivalente

$$\operatorname{tr\,deg}\left(F(\bar{a})/F\right) = \dim V$$

Si $\bar{a}$ et $\bar{b}$ sont des génériques de V sur F alors en composant les deux avec $F(V)$ il existe un F-automorphisme de $\mathbb{k}$ tel que $\bar{a}$ soit envoyé sur $\bar{b}$.

<u>Exemple</u> : Considérons $V = V(x^2-2)$ définie sur $\mathbb{Q}$, $V = \{\pm\sqrt{2}\}$

$I(V) = (x^2-2)$ et $\mathbb{Q}(V) = \dfrac{\mathbb{Q}[x]}{(x^2-2)} \cong \mathbb{Q}(\sqrt{2}) = \mathbb{Q}(-\sqrt{2})$ ($\operatorname{tr\,deg} = 0 = \dim$).

alors $\sqrt{2}$ et $-\sqrt{2}$ sont des génériques de V sur $\mathbb{Q}$.

Remarquer que x^2-2 est irréductible sur $\mathbb{Q}$

• <u>I idéal annulateur</u> ($= I(V)$ lorsque V est un singleton)

Soit $\bar{a} \in \mathbb{k}^n$, on pose $I(\bar{a}/F) = \{ \hat{f}(\bar{X}) \in F[\bar{X}] \mid f(\bar{a}) = 0 \}$

<u>Alors</u> : $I(\bar{a}/F)$ est un idéal premier et

$$F[\bar{a}] \cong \frac{F[\bar{X}]}{I(\bar{a}/F)}$$

Si $I = I(\bar{a}/F)$ clairement $\bar{a} \in V(I)$ mais d'autres éléments peuvent être captés. Dans tous les cas :

- $V(I)$ est irréductible
- $\bar{a}$ est un générique de $V(I)$
- $\bar{b} \in V$ ssi $I(\bar{b}/F) \supseteq I(\bar{a}/F)$.

De plus $\bar{b} \in V$ est générique de V sur F ssi $I(\bar{b}/F) = I(V) \cap F[\bar{X}]$

- Locus d'un point

Soit $\bar{a} \in \mathbb{k}^n$, $F \subseteq \mathbb{k}$. On a vu que $I(\bar{a}/F)$ est un idéal premier de $F[\bar{x}]$ et donc $V = V(I(\bar{a}/F))$ est irréductible sur F on l'appelle le locus de $\bar{a}$ sur F.
Notons que on a bien $I(V) \cap F[x] = I(a/F)$ par le Nullstellensatz. De plus $\bar{a}$ est un générique de V sur F.
On a le critère suivant :

clôture sép. dans $\mathbb{k}$

$$V \text{ est irréductible (dans } \mathbb{k}^n) \text{ ssi } F(\bar{a}) \cap F^{s} = F$$

On comprend donc que si $\bar{a} \in \mathbb{k}^n$, $F \subseteq \mathbb{k}$ et F est algébriquement clos, en particulier $F^S = F$ et donc $I(\bar{a}/F)$ a pour clôture de Zariski $(I(V(I(a/F))) \subseteq \mathbb{k}[\bar{x}])$ un idéal premier et donc le locus de $\bar{a}$ sur F est irréductible.
Si F est séparablement clos alors de même la clôture de Zariski $I(V(I(a/F)))$ est un idéal radical premier et encore le locus de $\bar{a}$ sera une variété.
Si F est de car. 0 alors $F^s = F^{alg}$ et donc $F(\bar{a})$ est transcendant.

Exemples :

- Etude de la courbe dans $A^2 = \mathbb{C}^2$ définie par $X^2 - Y$.

On pose $V = V(X^2-Y) = \{(x,y) \in \mathbb{C}^2,\ x^2-y=0\}$. Par le critère d'Eisenstein X^2-Y est irréductible donc $(X^2-Y) = I(V)$ est premier et donc V est une variété irréductible.

. dim V = 1 : En effet $\dfrac{\mathbb{C}[X,Y]}{(X^2-Y)} \simeq \mathbb{C}[X,X^2] = \mathbb{C}[X]$ et ainsi $\mathbb{C}(V) = \mathbb{C}(X)$ et $\mathrm{tr.deg}(\mathbb{C}(X)/\mathbb{C}) = 1 = \dim V$.

. Remarquons que dans $\mathbb{C}$, $x \mapsto x^2$ est surjective donc une représentation dans $\mathbb{C}^2$ de V revient une sorte de "double parabole"

- Générique sur $\mathbb{Q}$: Remarquons que V est définie sur $\mathbb{Q}$ car $X^2-Y \in \mathbb{Q}[X,Y]$ et $\langle X^2-Y\rangle_{\mathbb{Q}[X,Y]}$ est premier donc on sait que des multiples de X^2-Y et cela s'étend uniquement en $I(V)$ sur $\mathbb{C}[X,Y]$. On a que le corps de fonctions de V sur $\mathbb{C}$ est $\mathbb{C}(X)$ alors que le corps de fonctions de V sur $\mathbb{Q}$ est $\left(\frac{\mathbb{Q}[X,Y]}{(X^2-Y)}\right)^{\mathrm{Frac}}$ $\simeq \mathbb{Q}(X)$. On cherche un <u>élément générique de V sur $\mathbb{Q}$</u>.

càd un élément $(a,b) \in V \subseteq \mathbb{C}^2$ tel que

$$\mathbb{Q}(a,b) \simeq \mathbb{Q}(X) = \mathbb{Q}[V]$$ en toutes ($\mathrm{trdeg}\,\mathbb{Q}(a,b) = \dim V = 1$)

On a que si on prend $(a,b) \in V \cap \mathbb{Q}^{alg}$ alors $\mathbb{Q}(a,b)$ est une extension algébrique de $\mathbb{Q}$ donc de degré de transcendance 0, il faut donc le prendre dans $V \setminus (\mathbb{Q}^{alg})^2$, par exemple $(\sqrt{\pi},\pi)$.

Montrons que $(\sqrt{\pi},\pi)$ est un générique de V :

On a $\mathbb{Q}(\sqrt{\pi},\pi) = \mathbb{Q}(\sqrt{\pi}) \simeq \mathbb{Q}(X)$ donc π est transcendant sur $\mathbb{Q}$ et donc on a bien ce qu'il faut. En particulier $I(\sqrt{\pi},\pi/\mathbb{Q}) = (X^2-Y)$ car il ne peut pas y avoir plus de relation algébrique entre $\sqrt{\pi}$ et π et $\mathbb{Q}$ puisque π est transcendant sur $\mathbb{Q}$ et que donc la seule contrainte que l'on puisse avoir est $(\sqrt{\pi})^2 = \pi$.

• $(\sqrt{2},2)$ n'est pas un générique car évidemment $(X^2-Y) \subseteq I(\sqrt{2},2/\mathbb{Q})$ mais il y a aussi d'autres relations algébriques comme X^2-2, X^4-2Y ou autre et donc $(X^2-2, X^4-2Y) \subseteq I(\sqrt{2},2/\mathbb{Q})$ qui devient trop grand !

Un générique doit traduire, être un représentant de ce qu'il se passe sur la courbe du point de vue du corps F (= $\mathbb{Q}$ ici)

<u>Existence de générique</u> : un générique n'existe pas forcément, par exemple il n'existe pas de générique de V sur $\mathbb{C}$ puisque tout élément (a,b) de V vérifie $\mathbb{C}(a,b) = \mathbb{C}$, alors que $\mathbb{C}(V) = \mathbb{C}(X)$. Il faut que le corps $F \subsetneq \mathbb{C}$ et tel que $F^{alg} \subsetneq \mathbb{C}$. C'est pourquoi il n'y a pas de générique sur $\mathbb{R}$ non plus.

On pourrait se placer dans $\mathbb{K} = \mathbb{C}(X,Y)^{alg}$ et $(\sqrt{X}, X)$ marche.

• Locus d'un point de V : (sur $\mathbb{Q}$)

On détermine le locus de $(\sqrt{\pi}, \pi) \in V$ et $(1,1) \in V$:
On voit que les points de la courbe n'ont vraiment pas le même sens, par exemple $(1,1)$ appartient à énormément de courbes, $X=Y$, $X+Y=2$, $X^2+Y^2=2$, $X^2=Y^2$, ce n'est pas un point représentatif de la courbe contrairement à $(\sqrt{\pi}, \pi)$ qui, sur $\mathbb{Q}$, est un générique.

Le locus de $\bar{a}/F$ est la plus petite variété (irréductible) contenant $\bar{a}$ définie sur F. (c'est clair car si $V = V(I(\bar{a}/F))$ = locus de $\bar{a}/F$, si $\bar{a} \in V(J)$ alors $J(a)=0$ sur $J \subseteq I(\bar{a}/F)$ et donc $V(I(\bar{a}/F)) \subseteq V(J)$)

Comme $(\sqrt{\pi}, \pi)$ est un générique, on voit que $I(V) = I((\sqrt{\pi}, \pi)/\mathbb{Q})$ et donc $V = V(I((\sqrt{\pi}, \pi)/\mathbb{Q}))$ et V est le locus de $(\sqrt{\pi}, \pi)$.

Prenons $(1,1) \in V$, quel est son locus sur $\mathbb{Q}$?

On a à prouver que ~~$X=Y$ est irréductible~~ $(X-1)^2 + (Y-1)^2$ n'a dans $\mathbb{Q}$ que $(1,1)$ comme racine et ce polynôme est irréductible sur $\mathbb{Q}$ donc $\mathbb{Q}^2 \cap V((X-1)^2 + (Y-1)^2) = \{(1,1)\}$ et le locus de $(1,1)$ sur $\mathbb{Q}$. Sur $\mathbb{C}$, ce polynôme n'est pas irréductible car
par ~~irréductibilité~~ :
c'est $(X - iY - 1 + i)(X + iY - 1 - i)$ et donc la variété $V((X-1)^2 + (Y-1)^2)$ n'est pas irréductible, cela veut dire que le locus de $(1,1)$ sur $\mathbb{C}$ est défini autrement et a tout à fait sens différent.
Si on prend $X - iY - 1 + i$ il définit une variété irréductible qui contient $(1,1)$ et de même pour $X + iY - 1 - i$, cela veut dire que le locus a du sens que lorsque l'on parle du corps de définition de la variété.

Remarquons que le locus de $(\sqrt{\pi}, \pi)$ sur F est $V(I(\sqrt{\pi}, \pi/F))$ ie si on regarde la clôture de Zariski de $I(\sqrt{\pi}, \pi/F)$ ie

$$I(V(I(\sqrt{\pi}, \pi/F)))$$

V vit dans $\mathbb{C}^n$ mais V est irréductible sur $\mathbb{Q}$.

On discute de l'irréductibilité de V sur $\mathbb{C}$ en fonction de celle sur $\mathbb{Q}$ (on sait que V est irréductible car $X^2 - Y$ est premier autant sur $\mathbb{Q}$ que sur $\mathbb{C}$ par eisenstein mais on veut utiliser le critère) On a que $\mathbb{Q}$ est ~~séparablement~~ clos ~~dans~~ car de car 0 donc
$\mathbb{Q}^{s(\mathbb{C})} = \mathbb{Q}^{alg} \cap \mathbb{C} = \mathbb{Q}^{alg}$.

On voit donc bien que comme $(\sqrt{\pi}, \pi)$ est transcendant, $\mathbb{Q}(\sqrt{\pi}) \cap \mathbb{Q}^{alg} = \mathbb{Q}$ et ainsi on a que $\underline{V}$ (dans $\mathbb{C}$) est irréductible par le critère.

On conclut en se plaçant dans $\mathbb{K}, \supseteq F$ et le cas $A = \mathbb{K}$, i.e. dim $= 1$.

Soit $F \subseteq \mathbb{K}$ et $p(X)$ un polynôme de $F[X]$ irréductible sur F.

- Si les racines de p dans F^{alg} sont distinctes, (p séparable) alors $V \subseteq \mathbb{K}$ $V = \{$racines de $p\}$ n'est pas irréductible.
- Si F est séparablement clos, alors si α racine de p on a α inséparable donc α est la seule racine de p ($\alpha \in F^{alg} \setminus F = F^{alg} \setminus F^{s}$) et donc la variété V est aussi irréductible.
- Si F est algébriquement clos : un polynôme irréductible sur F est linéaire et donc $V = \{$seule racine de $p\}$ est irréductible.

Groupes algébriques

On est à présent en mesure de définir ce qu'est un groupe algébrique.

On appelle <u>groupe algébrique</u> une variété G telle qu'il y ait une structure de groupe sur G telle que

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ x, y & \longmapsto & x.y \end{array} \qquad\qquad \begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & x^{-1} \end{array}$$

sont des morphismes de variétés.

En général un groupe algébrique n'est pas topologique car $G \times G$ est muni de la topologie produit de Zariski qui n'est pas la topologie produit alors que un groupe topologique doit être continu pour la top produit.

Un morphisme de groupes algébriques est un morphisme de variété qui est aussi un homomorphisme pour la structure algébrique de groupe.

On s'intéresse principalement aux groupes algébriques dont la variété sous-jacente est affine. On donne quelques exemples standards.

• Le <u>groupe additif</u> G_a est la ligne affine k avec pour loi $x+y$ est un groupe algébrique <u>irréductible</u> et de <u>dimension 1</u>.
En effet il est irréductible car en dimension 1 les fermés sont exactement les ensembles finis et tout 2 ensembles cofinis s'intersectent.
Il est bien de dimension 1 car le corps de fonctions associé est $k(T)$ qui est de degré de transcendance 1 sur k.
L'addition est un morphisme car elle est donnée par des conditions polynomiales ($x+y=3$), de même pour l'inverse $a+3=10$
on a donc bien affaire à un groupe algébrique.

• Le <u>groupe multiplicatif</u> G_m est k^*, c'est bien un ouvert (principal) de la variété k donc c'est une sous-variété

et comme k est irréductible on a $\dim k = \dim k^\times = 1$
G_m est un ouvert d'un espace irréductible donc est irréductible aussi.
Notez que G_a et G_m ne sont pas nécessairement isomorphes car G_a est toujours divisible mais G_m pas nécessairement.

• L'espace $\mathbb{A}^n = k^n$ est aussi un groupe algébrique pour l'addition (donnée par des conditions polynomiales). L'algèbre locale associée en tout point est $k[T_1 \dots T_n]$, donc $\mathbb{A}^n$ est irréductible et de dimension n ($k(T_1 \dots T_n) | k$ a tr.deg $= n$). ($\mathbb{A}^n$ est irréductible car produit de Zar d'espace irréductible (k))

• Le <u>groupe additif $M_n(k)$</u> des matrices est exactement $\mathbb{A}^{n^2} = k^{n^2}$.

• Le <u>groupe général linéaire</u> $Gl_n(k)$ est un <u>ouvert principal</u> de $\mathbb{A}^{n^2} = k^{n^2}$ déterminé par $\det(T_{ij}) \neq 0$ (le déterminant est un polynôme. Comme $\mathbb{A}^{n^2}$ est irréductible cela force la variété (non-) $Gl_n(k)$ à être de dimension n^2. De plus les conditions du produit sont aussi polynomiales de même pour l'inverse donc on a bien que $Gl_n(k)$ est un groupe algébrique.

Son algèbre de fonction est l'algèbre des fonctions rationnelles définies sur toutes les coordonnées T_{ij} donc pas de restriction mais le déterminant doit être non nulle donc $\frac{1}{\det T_{ij}}$ doit être défini en tout point (T_{ij}) de k^{n^2}, cela donne donc

$$k[Gl_n(k)] = k\Big[\underbrace{T_1 \dots T_{n^2}}_{``T_{ij}"}, \frac{1}{\det(T_{ij})}\Big]$$

(notez que l'on voit bien que $\frac{1}{\det T_{ij}}$ est algébriquement lié avec T_{ij} donc la dimension est bien n^2).

N.B: Ce que l'on a fait ici se généralise : si A est une variété de dimension n et U un ouvert principal déterminé par $U = \{f \neq 0\}$ alors (si A est irréductible) on a que l'algèbre locale de U est $k[T_1 \dots T_n, \frac{1}{f(T_i)}]$ (encore de dimension n) et sur U toutes les fonctions coordonnées sont définies et la seule restriction est que $f(T_i) \neq 0$ ce qui se traduit en terme de "fonction définie" ou "fonction régulière" par le fait que $\frac{1}{f(T_i)}$ soit une fonction régulière partout sur U, i.e

$$U = \{f \neq 0\} \quad \text{ssi} \quad \frac{1}{f(T_i)} \text{ est régulière sur } U.$$

Notez que l'on a le fait suivant :

Un sous-groupe fermé d'un groupe algébrique est un groupe algébrique.

Les restrictions des morphismes multiplication et inversion sur des fermés restent des morphismes.

- Le groupe $T_n(k)$ des matrices triangulaires supérieures correspond au fermé donné par $\{T_{ij} = 0 \mid 1 \leq j < i \leq n\}$ intersecté avec $Gl_n(k)$.

On a donc
$$k[T_n(k)] = \frac{k[Gl_n(k)]}{\langle T_{ij} \; ; \; j < i \rangle}$$
$$\simeq k[T_{ij}, i \geq j, \frac{1}{\det(T_{ij})}]$$
et la dimension de l'algèbre sera $\#\{i,j \; ; \; i \geq j\} = \frac{n(n+1)}{2}$.

- Le groupe $D_n(k)$ des matrices diagonales correspond au fermé $T_{ij} = 0 \;\; \forall i \neq j$ dans $Gl_n(k)$: il est de dimension n.

- Le groupe $U_n(k)$ est le groupe des matrices de $T_n(k)$ intersecté avec $\{T_{ii} = 1, i = 1 \dots n\}$, c'est aussi une variété irréductible, de dimension $\frac{n(n-1)}{2}$.

Notez que le produit de deux groupes algébriques est un groupe algébrique (pour la topo produit de Zariski).

Par exemple $$D_n(k) \simeq \prod_n G_m$$

$$U_n(k) \simeq \prod_n G_a$$

- <u>Composante de l'identité</u>

Soit G un groupe algébrique. On va voir que dans ce cas particulier les composantes irréductibles de la variété sont en fait les <u>composantes connexes</u> et qu'une composante une en fait la classe à gauche d'un certain groupe connexe (et irréductible) appelé la <u>composante de l'identité</u> (ou composante connexe) G^0.

On montre d'abord qu'une seule des composantes irréductibles $A_1, \dots, A_n$ de G contient l'identité e de G. Si $e \in A_1 \cap \dots \cap A_m$ (quitte à réindexer) alors $A_1 \times \dots \times A_m$ est une variété irréductible et le morphisme multiplicatif nous donne que $A_1 \cdot \ldots \cdot A_m$ est un sous ensemble irréductible de G contenant e donc $A_1 \cdot \ldots \cdot A_m \subset A_i$. D'un autre côté chaque $A_i \subseteq A_1 \cdot \ldots \cdot A_m$ on a donc $A_i = A_1 \cdot \ldots \cdot A_m$ pour un certain i ce qui force $m = 1$.

On appelle G^0 la <u>composante de l'identité</u> l'unique composante irréductible de G contenant e.

<u>Proposition</u> : Pour G un groupe algébrique :

a) G^0 est un sous groupe de G caractéristique d'indice fini et dont les classes à gauche sont les composantes connexes et les composantes irréductibles de G.

b) Tout sous groupe d'indice fini de G contient G^0.

<u>Preuve:</u> a) Pour chaque $x \in G^0$, $y \mapsto x^{-1}y$ est un morphisme donc $x^{-1}G^0$ est une composante irréductible qui contient clairement $e = x^{-1}x$ donc $x^{-1}G^0 = G^0$ et donc $(G^0)^{-1} = G^0$, $G^0 \cdot G^0 = G^0$ et G^0 est un sous groupe de G. Si σ est un automorphisme de G σG^0 est encore une composante irréductible de G car σ est un morphisme et contient e donc $\sigma G^0 = G^0$.

Les translatées à gauche et droite de G^0 sont des composantes irréductibles (donc en nombre fini et en particulier $[G : G^0] = \#$ Composantes irréductibles $< \infty$ par noethérianité) qui sont de plus disjointes donc ce sont des composantes connexes.

b) Tout sous groupe fermé d'indice fini H, chacune de ses classes est un fermé et donc $\bigcup_{\text{classe de } H \neq H}$ est aussi un fermé ce qui force H à être ouvert. Donc les classes à gauche de H partitionnent G^0 en un nombre fini d'ouverts, et comme G^0 est connexe et $G^0 \cap H \neq \emptyset$ on a que $G^0 \subseteq H$. ■

<u>N.B:</u> • Rappelons qu'un ensemble d'un espace topo est irréductible ssi sa clôture l'est donc les <u>composantes maximales sont toujours fermées</u>, en particulier G^0 est un fermé.

• On a $G = \bigcup_{a_1 \ldots a_n} a_i G^0$ et donc $G^0 = G \setminus \bigcup_{a_i \neq 1} a_i G^0$ et donc G^0 est ouvert donc G^0 est un ouvert fermé.

• De même tout sous groupe fermé d'indice fini est aussi un ouvert.

<u>Définition:</u> On dit que G est <u>connexe</u> si $G = G^0$ i.e. si G est irréductible.

Notez que par exemple $GL_n(k)$ est connexe car c'est un ouvert principal d'une variété affine donc irréductible

Une conséquence terrible mais utile :

Lemme : Si U et V sont deux ouverts denses d'un groupe algébrique G, alors $G = U \cdot V$.
En particulier si G est connexe, pour tout ouvert U, V distinct on a
$$G = U \cdot V.$$

Preuve : V^{-1} est un ouvert dense à cause pr homéomorphisme.
Et de même xV^{-1} est un ouvert dense donc $xV^{-1} \cap U \neq \emptyset$
et donc $x \in U \cdot V$.
La deuxième partie vient du fait que dans un espace irréductible tout ouvert est dense. ∎

Proposition : Si $\varphi : G \longrightarrow G'$ est un morphisme de groupes algébriques, alors

(a) $\ker \varphi$ est un sous-groupe fermé de G

(b) $\operatorname{Im} \varphi$ est un sous-groupe fermé de G'

(c) $\varphi(G^\circ) = \varphi(G)^\circ$

(d) $\dim G = \dim \ker \varphi + \dim \operatorname{Im} \varphi$.

Exemple : $\det : GL_n(k) \longrightarrow GL_1(k) = G_m$ est un morphisme de groupes algébriques, surjectif. On a $\ker \det = SL_n(k)$.
On a donc que $SL_n(k)$ est un sous groupe algébrique fermé de $GL_n(k)$ et $\dim SL_n(k) = n^2 - 1$.

Théorème (non trivial)
Soit k un corps. À isomorphisme près les seuls groupes algébriques connexes de dimension 1 sont G_a et G_m.

3ème Partie : DIVERS

Corps pseudo algébriquement clos

On introduit ici la notion de corps pseudo algébriquement clos (PAC) et on montre que la classe des corps PAC est élémentaire.

• Variété absolument irréductible

Un polynôme $f \in k[X_1 \dots X_n]$ est <u>absolument irréductible</u> si f est irréductible dans $L[X_1 \dots X_n]$ pour toute extension L du corps k.

Exemple : • Si $n = 1$ seuls les poly de deg 1 sont abs. irréductibles.

• Par le critère d'Eisenstein, $X^n - Y$ est irréductible dans $k[X, Y]$ $\forall n$, il est donc absolument irréductible (évidemment l'existence d'une racine dans le corps n'implique nullement une quelconque factorisation, pour $n \geq 2$).

Une variété affine irréductible V définie sur $k \subseteq \mathbb{K}$ qui reste irréductible sur F $\forall F$ tq $k \subseteq F \subseteq \mathbb{K}$ est dite <u>absolument irréductible</u>. (ne dépend plus du corps de définition)

Remarque : • Si $f(\bar{x})$ est absolument irréductible, alors $V(f)$ est absolument irréductible

• La réciproque <u>est fausse</u> : si car $k = p$, le polynôme $X^p - a$ irréductible sur k définit $V = V(X^p - a) \in \mathbb{K} \supseteq k^{alg}$

On a clairement $V = \{\alpha\}$ est irréductible et α pour toute extension de k, donc V est <u>absolument</u> <u>irréductible</u>, mais, $X^p - a$ se factorise dans $k(\alpha)$.

On peut montrer que si V est une variété affine avec $\bar{a}$ un point générique sur k (V déf $/k$). Alors

‖ V abs. irr. ssi $k(\bar{a})/k$ est <u>régulière</u>

Dans l'exemple précédent, α est purement inséparable sur k et donc (α racine de $P \in k[X] \Leftrightarrow \alpha$ générique de $V(f)/k$ | 1 variable) $k(\alpha)/k$ n'est pas séparable et en particulier pas singulière.

On a de plus le résultat suivant :

> Toute variété absolument irréductible V sur k admet un plus petit corps de définition L, et on a L/k est une extension finie et purement inséparable.

<u>Remarque importante</u> : Une variété (affine) $V(f_1 \dots f_n)$ où $f_1 \dots f_n \in k[\bar{X}]$ est dite <u>définie sur L</u> $(k \subseteq L \subseteq \mathbb{K})$ si

$$I_{\mathbb{K}}(V) = \langle I_{\mathbb{K}}(V) \cap L[\bar{X}] \rangle$$
$$= \mathbb{K} \cdot I_L(V)$$

Cette condition est plus forte que dire que $f_1 \dots f_n \in L[\bar{X}]$. On a toujours $k \subseteq L$ puisque $L \cdot I_k(V) \subseteq I_L(V)$.

On dit une <u>k-variété</u> V si $V = V(f_1 \dots f_n)$ $f_i \in k[\bar{X}]$ mais on réserve le terme <u>défini sur k</u> lorsque

$$I_{\mathbb{K}}(V) = \mathbb{K} \cdot I_k(V)$$

Notons que si l'on prend un corps k de car $p > 0$ non parfait, et $\alpha \in k^{alg} \setminus k$ tel que $\exists a \in k$, $\alpha^p = a$, comme d'habitude on a $V(X^p - a)$ (est absolument irréductible) et c'est une k variété affine. Mais est-elle définie sur k ? La réponse est non, car $I_k(V) = \langle X^p - a \rangle$, $I_{k(\alpha)}(V) = \langle X - \alpha \rangle$ et on a $\mathbb{K} \cdot I_k(V) = \mathbb{K}[X] \cdot (X^p - a)$ qui est strictement inclus dans $I_{k(\alpha)}(V)$. On aura en revanche que le corps de définition de V est $k(\alpha)$ car :

$$\mathbb{K} \cdot I_{k(\alpha)}(V) = \mathbb{K}[X] \cdot (X - \alpha) = I_{\mathbb{K}}(V)$$

Le corps de définition doit donc être suffisamment gros pour engendrer le même calcul que dans une clôture algébrique ce qui se traduit dans le cas d'une seule variable par le fait que le corps contienne les coefficients et soit parfait.

Remarque (Point rationnel) : En considérant une variété V définie sur k, et $\mathbb{K}$ une extension suffisamment grande de k algébriquement close, on rappelle qu'un point rationnel de V sur k est un élément de $V \cap k^n$.

- Corps pseudo algébriquement clos

Définition : On appelle un corps k pseudo algébriquement clos si toute variété affine absolument irréductible V définie sur k admet un point rationnel sur k.

Exemple : • Un corps $\mathbb{K}$ algébriquement clos est pseudo algébriquement clos, il vérifie que toute variété affine admet un point rationnel (et cette dernière condition caractérise les corps algébriquement clos évidemment)

• Si $\mathbb{F} = \prod_{p \text{ premier}} \mathcal{U} \, \mathbb{F}_p$ alors on a

  - $\mathbb{F}$ est parfait
  - $G(\mathbb{F}) \simeq \hat{\mathbb{Z}}$
  - Si $f(X,Y)$ est absolument irréductible sur $\mathbb{F}[X,Y]$

alors $V(f)$ a une infinité de point rationnel sur $\mathbb{F}$.

On va voir que $\mathbb{F}$ est alors PAC.

• Un corps séparablement clos est PAC.

On peut montrer le théorème suivant :

Soit $L \supseteq k$ extension algébrique, alors

L est PAC $\Leftrightarrow$ toute courbe plane absolument irréductible déf sur k a un point rationnel dans L

où un corps plan est une variété de la forme $V(f)$ avec $f \in k[X,Y]$.
On en déduit que

Théorème: k est PAC ssi $\forall f \in k[X,Y]$ absolument irréductible $\exists (a,b) \in k^2$ tel que $f(a,b) = 0$.

On rencontre un critère utile pour montrer que PAC est élémentaire. En attendant, quelques propriétés.

Propriété: Pour une variété V absolument irréductible ($\subseteq \mathbb{A}^n$) définie sur le corps PAC k, alors $V(k)$, l'ensemble des points rationnels de V en k est dense dans V où muni de la k-topologie de Zariski sur V.

Rappel: Rappelons qu'étant donné une variété affine $V \subseteq \mathbb{A}^n$ définie sur k, on a une topologie sur V définie par les fermés de Zariski à coefficients dans k. la k-topo de Zariski.
Pour cette preuve, on prend un fermé de Zariski sur k un complémentaire définit un ouvert pour la k-topo de Zariski et et si le complémentaire s'intersecte avec V alors cette intersection est un ouvert de V pour la k-topologie de Zariski.

Preuve: Soit donc V une variété affine absolument irréductible définie sur k et soit $\bar{x}$ un générique de V sur k.
On a que V abs. irréd ssi $k(\bar{x})/k$ est régulière.
On choisit donc un ouvert de V pour la k-topo de Zar. ie le complémentaire d'un fermé qui s'intersecte avec V donc soit $W = V(g_1 \dots g_m)$ tel que $V \cap W^{c^{/\mathbb{A}^n}} \neq \emptyset$. Cela veut dire que l'un des g_i, disons g_1 vérifie $g_1(\bar{x}) \neq 0$.

Soit alors y tel que $y \cdot g_1(\bar{x}) = 1$, et soit V' le lieu du point $(\bar{x}, y)$ sur k. ($V' \subseteq \mathbb{A}^n$ et $V' = V(I(\bar{x}y/k))$)

V' est absolument irréductible : en effet c'est le cas ssi $k(\bar{x}, y)/k$ est régulier (puisque par construction $\bar{x}y$ est un générique de V') or $k(\bar{x}, y) = k(\bar{x})$ et $k(\bar{x})/k$ est régulier donc V' est abs. irred.

On a alors, puisque k est PAC un $(\bar{x}', y') \in V' \cap k^n$ et alors $y' g_1(\bar{x}) = 1$. En particulier, $g_1'(\bar{x}') \neq 0$ or $\bar{x}'$ vérifie les mêmes équations que $\bar{x}$ et donc $\bar{x}' \in V(k)$ et donc car $g_1(\bar{x}') \neq 0$, $\bar{x}' \in V(k) \cap W^c$ ∎

Corollaire (PAC Nullstellensatz)

> Si k est PAC et si V est une variété abs. irred et si $g \in k[\bar{x}]$ s'annule sur $V(k)$ alors $g \in I_k(V)$.

Rem : Par densité - il existe un générique $\bar{x}$ de V sur k tel que $g(\bar{x}) = 0$. Donc g s'annule sur $V(\tilde{k})$. Par le Nullstellensatz, il existe n tel que g^n s'annule sur tout V donc $g^n \in I_k(V)$ et comme $I_k(V)$ est premier $g \in I_k(V)$ ∎

• **La classe des corps PAC est élémentaire**

On va maintenant montrer que la classe des corps PAC est élémentaire.

• **Polynômes** Dans le langage des anneaux, un terme est un polynôme et on peut quantifier sur les polynômes dans le sens suivant : par exemple pour un polynôme en 2 variables X, Y, on définit avec une suite $a_0, a_1, \dots$

$$P^{\bar{a}}(X,Y) = a_0 + a_1 X + a_2 Y + a_3 X^2 + a_4 XY + a_5 Y^2 + \dots$$

en composante homogène, et cela nous donne un polynôme de degré $f(|\bar{a}|)$ peu importe.

On définit aussi de suite $P^{\bar a}_{n,m}(\bar x) = P_{n,m}(\bar a, \bar x)$ un polynôme de degré n en m variables. L'énoncé tout polynôme à 3 variables de $d^\circ n < 5$ admet un zéro s'écrit

$$\bigwedge_{\substack{n\le 5\\ m\le 3}} \forall \bar x \, \exists \bar y \, P_{n,m}(\bar x, \bar y) .$$

De même k est algébriquement clos ssi $k \models \{ \forall \bar x \, \exists y \, P_{n,1}(\bar x, y) = 0 \mid n \in \mathbb{N} \}$

• Polynômes absolument irréductibles

On veut une formule $\theta^m_d(\bar a)$ telle que si $\bar a \models \theta^m_d$ alors $P_{d^m,m}(\bar a, \bar X)$ est absolument irréductible. Notez que l'on peut considérer $P_{n,m,d}(\bar a, \bar X)$ où d est une borne sur $\deg_{X_i} P$. On aura alors que k est PAC ssi il vérifie

$$\Phi_d = \text{“}\forall \bar x \; \theta^2_d(\bar x) \longrightarrow \exists y_1 y_2 \; P_{d^2,2,d}(\bar x, y_1, y_2) = 0\text{”}$$

pour tout $d \in \omega$, i.e.

$$PAC = T_{corps} \cup \{ \Phi_d \mid d < \omega \}$$

Pour montrer qu'une formule θ^n_d existe, on aura besoin du lemme suivant :

On note $S_k(n,d)$ l'ensemble des polynômes $\in k[X_1 \dots X_n]$ tels que $\deg_{X_i} f < d$ $\forall i = 1 \dots n$.

Lemme : Si $f \in S_k(n,d)$ se factorise dans une clôture algébrique k^{alg} alors il se factorise dans une extension finie de k de degré $< (d^n - 1)!$.

Preuve : On considère la transformation dite de Kronecker :

$$S_d : S_k(n,d) \longrightarrow S_k(1, d^n)$$
$$X_j \longmapsto Y^{d^{j-1}}$$

si $f = \sum a_i X_1^{i(1)} \cdots X_n^{i(n)}$ alors $S_d f = \sum a_i Y^{i(1) + i(2)d + \dots + i(n) d^{n-1}}$

On vérifie alors 3 choses :

- S_d est bijective : vue de l'écriture unique du mot $(i(1) \ldots i(n))$ en base d.

- $S_d f$ a les mêmes coefficients que f

- $f = g \cdot h$ ssi $S_d(f) = S_d(g) \cdot S_d(h)$

On a donc que si $f \in k[\bar{X}]$, f se factorise dans $L \supseteq k$ ssi $S_d(f)$ se factorise dans $L[Y]$. Si donc $f = g \cdot h$, alors $S_d f = S_d(g) \cdot S_d(h)$. De plus $\deg S_d f \leq (d-1)(1 + d + \cdots + d^{n-1}) = d^n - 1$ et donc $S_d(f)$ se factorise dans une extension de degré $\leq (d^n-1)!$ (car on a $\leq d^n - 1$ choix pour un facteur de degré 1, $(d^n-1)-1$ pour un facteur de degré 2 ... etc). Et alors $S_d g$ $S_d h$ sont à coefficients dans une ext de degré $(d^n-1)!$ et c'est donc aussi le cas pour g et h

Un polynôme $f \in S_k(n,d)$ est donc absolument irréductible ssi il ne se factorise pas dans une extension finie de degré $\leq (d^n-1)!$

Sachant que toute extension finie se décompose en séparable puis purement inséparable, i.e. si $E \supseteq k$ alors $\exists F$ tq $E \supseteq F$ p. ins, $F \supseteq k$ sép on en déduit, sachant qu'un polynôme f qui se réduit dans une ext purement inséparable se réduit en $f = (g)^p$; on a déduit :

f est absolument irréductible ssi ① f est irréductible dans toute extension séparable finie de deg $\leq (d^n-1)!$

&

② f n'est pas une puissance p-ième d'un polys $g \in k[x]$

ssi ①' f est irréductible dans toute extension monogène de deg $\leq (d^n-1)!$ (thm de l'élément primitif)

&

②' il existe un $j \in [\![1,n]\!]$ tel que $\dfrac{\partial f}{\partial X_j} \neq 0$

Le dernier du polynôme $P(\bar{a}, X)$ s'exprime en un autre terme $P'(\bar{a}, X)$ et pour vérifier que ce terme est le polynôme nul il fait donc $\forall \bar{x}\ P'(\bar{a}, \bar{x}) = 0$; appelons $\varphi_d^n(\bar{a})$ cette formule

Il reste à exprimer le $\oplus'$: Un polynôme $f(\bar{X})$ se factorise dans une extension monogène $k(\alpha)[X]$, cela veut dire que si $h(Y) = \mathrm{irr}(\alpha, k, Y)$ alors $f(\bar{x})$ se factorise dans $\left(\frac{k[Y]}{h(Y)}\right)[\bar{X}]$ (on ne perd pas on force car l'extension est monogène et α est algébrique sur k donc $k(\alpha) = k[\alpha]$)

cela veut dire que $[f(\bar{X})] = [g_1(\bar{X}, Y)\, g_2(\bar{X} Y)]$ et donc qu'il existe $g_3(\bar{X}, Y)$ tel que

$$f(\bar{X}) = g_1(\bar{X}, Y)\, g_2(\bar{X}, Y) + g_3(\bar{X}, Y) \cdot h(Y).$$

Sachant que $\deg_Y(g_i) < (d^n - 1)!$ $i = 1, 2$ et que $\deg_{X_j}(g_i) < d$ $i = 1, 2$, $j = 1..n$; que $\deg_Y(g_3) < 2((d^n-1)!)$ et $\deg_{X_j}(g_3) < d$ $j = 1..n$, on voit que tout cela s'exprime en une formule $\psi_d^n(\bar{a})$ ($\bar{a}$ définit f).

On conclut que la formule $\Theta_d^n(\bar{a})$ est la conjonction

$$\varphi_d^n(\bar{a}) \wedge \psi_d^n(\bar{a})$$

On conclut le théorème suivant

Théorème : La classe des corps PAC est élémentaire.

On a donc que tout ultraproduit de corps PAC reste PAC.

Remarque : $\bar{a}$ définit un polynôme irréductible est élémentaire, car si $|\bar{a}| = n$, il suffit de dire $\neg \exists \bar{u}_1, \bar{u}_2 \forall \bar{x} P(\bar{a}, \bar{x}) = P(\bar{u}_1, \bar{x}) . P(\bar{u}_2, \bar{x})$

Exemple : Un corps PAC est toujours infini ; si $\mathbb{F}_q$ est un corps fini alors on montre que $(X^q - X)(Y^q - Y) + 1$ est absolument irréductible (élémentaire) et n'a pas de point rationnel in $\mathbb{F}_q$.

• Corps PAC et existentiellement clos.

On a vu le résultat suivant : pour V défini sur k

V est absolument irréductible ssi $\forall x$ générique de V sur k, $k(x)/k$ est régulière.

Théorème : k est PAC ssi k est existentiellement clos dans toute extension régulière de k.

Preuve : Rappelons que $k \subseteq_{ec} L$ (k est existentiellement clos dans L) ssi $\forall \phi$ sans quantificateur $L \models \exists x\, \phi \Rightarrow k \models \exists x\, \phi$.

Le sens $\Leftarrow$ est immédiat : Soit $V = V(f_1, \dots, f_n)$ $f_i \in k[\bar{x}]$ absolument irréductible (V) et soit $\bar{x}$ un générique de V sur k. On a par définition que $\bar{x}$ vérifie les équations et donc

$$k(\bar{x}) \models \bigwedge f_i(\bar{x}) \doteq 0$$

De plus $k(\bar{x})/k$ est régulière et donc on a

$$k \models \exists \bar{x}\, f_i(\bar{x}) = 0$$

et donc V a un point rationnel dans k.

$\boxed{\Rightarrow}$ On suppose donc que k est PAC et soit donc $\phi(\bar{x})$ une formule sans quantificateur (à param. de k) tel que $L \models \exists \bar{x}\, \phi(\bar{x})$, on suppose

$$\phi(\bar{x}) \sim \left(\bigwedge_i f_i(\bar{x}) = 0\right) \vee \left(\bigwedge_i g_i(\bar{x}) \neq 0\right)$$

s'il y a bien des f_i : Soit $V = V((f_i)_i)$ et $\bar{x} \in V \cap L^n$ (existe par $L \models \exists \bar{x}\, \phi(\bar{x})$) alors soit V_0 le locus de $\bar{x}$ sur k. Comme L/k est régulière, $k(\bar{x})/k$ est aussi régulière et comme $\bar{x}$ est un générique de V_0 sur k, on a un $\bar{\beta} \in k$ point rationnel de V_0 sur k et comme $V_0 \subseteq V$ on conclut que $\bar{\beta}$ est un témoin pour $\phi(\bar{x})$ dans k.

Si il n'y a pas de f_i, on a $L \models \forall \bar{x} \neg \bigvee g_i(\bar{x}) = 0$ et cette formule est aussi vraie dans k.

Sur le produit tensoriel

On se place dans le cadre du produit tensoriel de modules et on y reviendra ensuite au cas des corps, et des algèbres.

Remarque : le point de vue des catégories

On considère fixé un anneau R et des R-modules $E_1, \dots, E_n$.
On considère la catégorie dans laquelle :

Les objets : sont des applications multilinéaires f, un R-module F est attaché et $f : E_1 \times \dots \times E_n \to F$

Les flèches : sont, lorsqu'elles existent, des applications : si $f, g : E_1 \times \dots \times E_n \to F, G$ on a h : "$f \to g$" si $h : F \to G$ et

$$\begin{tikzcd} E_1 \times \dots \times E_n \arrow[r, "f"] \arrow[d, "g"'] & F \arrow[dl, "h"] \arrow[dl, phantom, "\circlearrowleft", near start] \\ G & \end{tikzcd}$$

le diagramme est commutatif.

h est alors une flèche entre f et g.

Un objet universel (répulsif) dans une catégorie est un objet P tel que pour tout autre objet F il existe une flèche $P \to F$.

Dans cette catégorie, un objet universel est la donnée d'une application multilinéaire $\varphi : E_1 \times \dots \times E_n \to M$ et d'un ensemble M, tel que $\forall f : E_1 \times \dots \times E_n \to F$ application multilinéaire, $\exists !$ $h : M \to F$ tel que

$$\begin{tikzcd} E_1 \times \dots \times E_n \arrow[r, "\varphi"] \arrow[d, "f"'] & M \arrow[dl, "h"] \arrow[dl, phantom, "\circlearrowleft", near start] \\ F & \end{tikzcd}$$

On appelle φ le produit tensoriel de $E_1, \dots, E_n$, M est noté $E_1 \otimes \dots \otimes E_n$.

La théorie des catégories nous assure que, lorsqu'il existe, un objet universel est unique, il s'agit donc de construire formellement cet objet universel.

• <u>Produit tensoriel d'espace vectoriel</u>

Soit F un corps et U, V deux espaces vectoriels sur F, on construit le produit tensoriel $U \otimes_F V$.

On prend M le F espace vectoriel (formel) engendré par les couples $(u,v) \in U \times V$. (u,v) est une <u>base</u> de notre espace vectoriel M, un élément est de la forme $\sum_{i \leq n} \lambda_i (u_i, v_i)$. Le cardinal de la base est donc $\# U \cdot \# V$ donc c'est énorme. (Le cardinal de M est $\# F^{\# U \cdot \# V}$ (!).)

On définit alors dans M le sous espace-vectoriel engendré par

$$(a u_1 + b u_2, v) - a(u_1, v) - b(u_2, v)$$
$$(u, a v_1 + b v_2) - a(u, v_1) - b(u, v_2)$$
$$(a u, v) - a(u, v)$$
$$(u, b v) - b(u, v)$$

$\forall a \in F$, $u \in U$, $v \in V$. On le note N, et on définit

$$U \otimes_F V = \frac{M}{N} \quad \text{l'espace vectoriel quotient.}$$

On note $u \otimes v$ la classe $(u,v) + N$.

<u>Exemple</u> : $\mathbb{F}_2 \otimes_{\mathbb{F}_2} \mathbb{F}_4$. On note $\mathbb{F}_2 = \{0,1\}$ et $\mathbb{F}_4 = \{0,1,x,x^2\}$ avec $x^2 = x+1$, $x^2+x+1 = 0$, $x^{-1} = x^2$ donc $x^3 = 1$, $x^{-1} = x^2$.

On a alors $\mathbb{F}_2 \times \mathbb{F}_4 = \{(0,0),(0,1),(0,x),(0,x^2),(1,0),(1,1),(1,x),(1,x^2)\}$

et
$$M = \mathbb{F}_2 \cdot (0,0) \oplus \mathbb{F}_2 \cdot (0,1) \oplus \mathbb{F}_2 \cdot (0,x) \oplus \mathbb{F}_2 \cdot (0,x^2) \oplus \mathbb{F}_2 (1,0) \oplus \mathbb{F}_2 \cdot (1,1) \oplus \mathbb{F}_2 \cdot (1,x) \oplus \mathbb{F}_2 \cdot (1,x^2) \simeq \mathbb{F}_2^8$$

et $\# M = |\mathbb{F}_2|^{|\mathbb{F}_2 \times \mathbb{F}_4|} = 2^8 = 256$.

Notez que dans M, $(1,0) + (0,1) \neq (1,1)$ car le + dont on parle n'est pas le même, la <u>base</u> de M est $\mathbb{F}_2 \times \mathbb{F}_4$, donc il faut penser à un ev de dim 8 sur $\mathbb{F}_2$, et voir $(1,0) + (0,1)$ comme le vecteur $(0,1,0,0,1,0,0,0)$

conformément à l'écriture de $\mathbb{F}_2 \times \mathbb{F}_4$.

Pour déterminer N, on prend par exemple pour la condition

$$(a u, v) - a(u, v)$$

$u = 1$, $v = x$, $a = 0$: les deux éléments de M

$(0 \cdot 1, x) = (0, x)$ et $0 \cdot (1, x)$ se représentent

$(0, 0, 1, 0, 0, 0, 0, 0)$ et $(0, 0, 0, 0, 0, 0, 0, 0)$

la différence est un élément de N, et dans le quotient M/N

on aura donc $\overline{(0, 0, 1, 0, 0, 0, 0, 0)} = 0$

On a le théorème suivant, qui nous éclaire sur la forme de $U \otimes_F V$:

Théorème : On a $\dim_F U \otimes_F V = \dim_F U \cdot \dim_F V$

De plus, si $\{u_i\}_{i \in I}$ et $\{v_j\}_{j \in J}$ sont deux bases de U et V, alors $\{u_i \otimes v_j \; i \in I, j \in J\}$ est une base de $U \otimes_F V$.

Enfin les règles suivantes sont vérifiées pour les éléments de la base :

$$(a u + b u') \otimes v = a(u \otimes v) + b(u' \otimes v)$$

$$u \otimes (a v + b v') = a(u \otimes v) + b(u \otimes v')$$

$$(a u) \otimes v = a(u \otimes v) = u \otimes (a v)$$

On a donc que le sev N est gros, car on passe de $\# V \cdot \# U$ comme dimension pour M à $\dim V \cdot \dim U$ comme dimension pour $M/N = U \otimes_F V$. De plus, une base est donnée par le produit $\otimes$ des bases, ce qui n'est pas clair par la définition. On revient sur notre exemple

Exemple : $\mathbb{F}_2 \otimes_{\mathbb{F}_2} \mathbb{F}_4$: Une base de cet espace vectoriel est donc puisque $\mathbb{F}_2 = \mathbb{F}_2 \cdot 1$ et $\mathbb{F}_4 \overset{ev}{=} \mathbb{F}_2 \oplus \mathbb{F}_2 \cdot x$, qu'une base de $\mathbb{F}_2 \otimes_{\mathbb{F}_2} \mathbb{F}_4$ est $\{1 \otimes 1, 1 \otimes x\}$. Les élements sont des sommes finies pour $\lambda_i \in \mathbb{F}_2$ et $\mu_i \in \mathbb{F}_2$

$$\sum \lambda_i (1 \otimes 1) + \sum \mu_i \, 1 \otimes x$$

$$= 1 \otimes \sum \lambda_i + 1 \otimes \sum \mu_i x$$

$$= 1 \otimes \left(\sum \lambda_i + \left(\sum \mu_i\right) x \right)$$

On a en fait que

$$\begin{aligned} \mathbb{F}_4 &\longrightarrow \mathbb{F}_2 \otimes_{\mathbb{F}_2} \mathbb{F}_4 \\ u = \lambda + \mu x &\longmapsto 1 \otimes \lambda + 1 \otimes \mu x \\ &\qquad = \lambda (1 \otimes 1) + \mu \cdot (1 \otimes x) \end{aligned}$$

est un isomorphisme, donc dans ce cas $\mathbb{F}_4 \cong \mathbb{F}_2 \otimes_{\mathbb{F}_2} \mathbb{F}_4$.

On a plus généralement que $F \otimes_F V \cong V$ pour tout F-ev V.

Exemple : $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{R}^4$. C'est évident par les dimensions mais pour entrer un peu dans les détails ; une base est $1 \otimes 1$, $1 \otimes i$, $i \otimes 1$, $i \otimes i$, et un élément est de la forme

$$\lambda \, 1 \otimes 1 + \mu \, 1 \otimes i + \gamma \, i \otimes 1 + \delta \, i \otimes i$$

$$= 1 \otimes (\lambda + \mu i) + i \otimes (\gamma + \delta i)$$

ce qui nous donne l'isomorphisme :

$$\begin{aligned} \mathbb{R}^4 &\longrightarrow \mathbb{C}^2 \longrightarrow \mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \\ \alpha, \beta, \gamma, \delta &\longmapsto ((\alpha + i\beta), (\gamma + i\delta)) \longmapsto 1 \otimes (\alpha + i\beta) + i \otimes (\gamma + i\delta) \\ &\qquad = \lambda, 1 \otimes 1, \mu (1 \otimes i) \; \gamma \, i \otimes 1, \delta \, i \otimes i \end{aligned}$$

Exemple : $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{R}^8$ (et non $\mathbb{R}^6$). Une base est donnée par $1 \otimes 1 \otimes 1$, $1 \otimes 1 \otimes i$, $1 \otimes i \otimes 1$, $1 \otimes i \otimes i$, $i \otimes 1 \otimes 1$, $i \otimes 1 \otimes i$, $i \otimes i \otimes 1$, $i \otimes i \otimes i$.

Remarquons que l'on a défini dans le cadre des espaces vectoriels, alors que l'exacte même définition tient dans le cadre des modules. Par exemple :

Exemple : $\mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathbb{F}_3 \simeq \mathbb{F}_3 \times \mathbb{F}_3$ (en tant que $\mathbb{Z}$ module, i.e. groupe)

Une base est $\{(1,0)\otimes 1 \ , (0,1)\otimes 1\}$ et on constate que :

$$(4,7)\otimes 2 = 4\,(1,0)\otimes 2 + 7\,(0,1)\otimes 2$$
$$= (1,0)\otimes(2\cdot 4) + (0,1)\otimes(7\cdot 2)$$
$$= (1,0)\otimes 0 + (0,1)\otimes 0$$

On a donc $(a,b)\otimes c = (1,0)\otimes(\overline{a\cdot c}) + (0,1)\otimes \overline{b\cdot c}$

On définit donc

$$\mathbb{F}_3 \times \mathbb{F}_3 \longrightarrow \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathbb{F}_3$$
$$(a,b) \longmapsto a\cdot(1,0)\otimes 1 + b\,(0,1)\otimes 1$$

Clairement injectif car on part de $\mathbb{F}_3$, et si $(a,b)\otimes c$ est à droite il sera clairement l'image de $(a\cdot c, b\cdot c)$, sachant que $c \in \mathbb{F}_3$ il y a bien unicité de l'antécédent et on a un isomorphisme.

Le produit tensoriel est parfois déroutant ; lorsque l'on est sur un module, on peut par exemple avoir $\mathbb{Z}/_{n\mathbb{Z}} \otimes \mathbb{Z}/_{m\mathbb{Z}} = \{0\}$, ou encore que si $M\otimes N$ et $M_0 \subseteq M$, $N_0 \subseteq N$, $M_0 \otimes N_0$ n'est peut être pas isomorphe à un sous module de M, N engendré par $m_i \otimes n_i$ avec $m_i, n_i \in M_0, N_0$, contrairement à avec les espaces vectoriels.

- Produit tensoriel d'algèbre

Si A et B sont deux F-algèbres, on peut définir une multiplication sur $A \otimes_F B$ par

$$\left(\sum_i a_i \otimes b_i\right)\left(\sum_i a_i' \otimes b_i'\right) = \sum_{i,j} a_i a_j' \otimes b_i b_j'$$

ou encore en les définissant sur la base, i.e.

$$(a\otimes b)\cdot(c\otimes d) = ac \otimes bd$$

On peut montrer que le produit tensoriel est associatif, commutatif et (d'élément neutre F).

Exemple : La table de multiplication de l'algèbre $\mathbb{F}_2 \otimes_{\mathbb{F}_2} \mathbb{F}_4$ est

	$1\otimes 1$	$1 \otimes x$
$1\otimes 1$	$1\otimes 1$	$1\otimes x$
$1\otimes x$	$1\otimes x$	$1\otimes x^2 = 1\otimes x + 1 \otimes 1$

$\simeq$

	$(1,0)$	$(0,1)$
$(1,0)$	$(1,0)$	$(0,1)$
$(0,1)$	$(0,1)$	$(1,1)$

Remarquons que le produit tensoriel de deux corps n'a pas de raison d'être un corps, en effet, si c'était le cas, comme la multiplication est commutative si les corps l'est, on aurait que $\mathbb{C}\otimes_{\mathbb{R}}\mathbb{C}$ serait un corps de dimension 4 sur $\mathbb{R}$ ce qui est absurde car le seul corps de dim 4 sur $\mathbb{R}$ n'est pas commutatif : c'est $\mathbb{H}$.

• <u>Produit tensoriel et anneaux linéairement disjoints</u>

Si l'on considère A, B deux sous anneaux d'un corps commutatif F, alors $A[B] = \{$ polys de $A[X]$ évalués en $\bar{b} \in B\}$

$= B[A]$

est le plus petit <u>sous anneau</u> de R contenant A et B.

Si $x \in A[B]$, $x = a^0 + a^1_1 b_1 + \dots + a^1_n b_n + a^2_1 b_1^{i} \dots b_n^{i} \dots$

$= P(b_1 \dots b_n) = \sum a_i M_i(\bar{b})$

où les $M(\bar{b})$ sont des monômes en $\bar{b}$, donc $M(\bar{b}) \in B$ et on montre ainsi que

$$A[B] = \left\{ \sum a_i b_i \, , \, a_i \in A, \, b_i \in B \right\}$$

On a donc que l'application $f : A \times B \longrightarrow A[B]$
$(a,b) \longmapsto a.b$

est F-linéaire en chaque variable, donc <u>F-bilinéaire</u>.

On a donc, par la propriété universelle du produit tensoriel, qu'il existe $h : A \otimes_F B \to F$ tel que

$$\begin{tikzcd} A \times B \arrow[r, "f"] \arrow[d] & A[B] \\ A \otimes_F B \arrow[ur, dashed, "\varphi"'] & \end{tikzcd}$$

le diagramme commute, i.e. $f = h \circ \varphi$.

On met cela en rapport avec le fait que les extensions soient linéairement disjointes : i.e. pour $\begin{matrix} K & & L \\ & F & \end{matrix}$

et

$$\begin{tikzcd} K \times L \arrow[r, "f"] \arrow[d] & K[L] \\ K \otimes_F L \arrow[ur, dashed, "\varphi"'] & \end{tikzcd}$$

$f(x,y) = x \cdot y$.

$(x,y) = x \otimes y$.

Théorème : Avec les notations précédentes :

$K \underset{F}{|} L$ ssi $\varphi : K \otimes_F L \longrightarrow K[L]$, $\underset{\text{générateur}}{a \otimes b} \longmapsto a.b$ est un isomorphisme de F-espaces vectoriels.

Preuve : L'application φ est surjective : en effet, soit $x = \sum a_i b_i \in K[L]$, alors $x = \varphi(\sum a_i \otimes b_i)$. L'application φ étant F-linéaire clairement.

On montre donc que

$K \underset{F}{|} L$ ssi φ est injective. On suppose d'abord que $K \underset{F}{|} L$ et soit donc $\{k_i\}_i$ une base du F-ev K. Il est clair que tout élément de $K \otimes_F L$ s'écrit, après traduction des éléments à gauche de la somme dans la base de K, $\sum k_i \otimes l_i$ avec $l_i \in L$. Donc si $\sum k_i \otimes l_i \in \ker \varphi$, alors

$\varphi(\sum k_i \otimes l_i) = 0 = \sum k_i . l_i$ mais cela contredit que $K \underset{F}{|} L$.

Réciproquement, si φ est un isomorphisme $\varphi : K \otimes_F L \to K[L]$, on se donne $\{e_i\}$ une base de K comme F-espace vectoriel et on suppose les $\{a_j\}$. On fait les remarques suivantes sur $K \otimes_F L$: tout élément s'écrit de manière unique comme

$$\sum a_j \otimes l_j \quad \text{pour certains } l_j$$

(En effet, écrire l'élément $\sum k_i \otimes l_i$ et exprimer $k_i = \sum \lambda_j^i a_j$ alors
$$\sum k_i \otimes l_i = \sum_i \Big(\sum_j \lambda_j^i a_j\Big) \otimes l_i = \sum a_j \otimes l_j' .)$$

Maintenant, si $\{a_j\}$ est libre dans L, alors $\sum a_j l_j = 0$ et par conséquent $\sum a_j \otimes l_j = 0$ mais seul l'élément 0 admet cette écriture, et le 0 est $0 \cdot \sum a_j \otimes l_i = \sum a_j \otimes 0$ comme $\sum a_j \otimes l_j = \sum a_j \otimes 0$ cela force $l_j = 0$ ■

Remarque : On utilise que l'on peut fixer une base $\{a_j\}$ du F espace-vectoriel K, l'écriture des éléments de $K \otimes_F L$ comme

$$\sum a_j \otimes l_j \quad \text{est } \underline{\text{unique}}.$$

On en déduit :

Corollaire : $K \underset{F}{|} L$ ssi $K \otimes_F L \simeq K[L] = L[K] \simeq L \otimes_F K$ ssi $L \underset{F}{|} K$, i.e. la relation de disjonction est symétrique.

Exemple : Le critère pour que $K \underset{F}{|} L$ est que $K \otimes_F L \to KL$ soit injective. Prenons donc $K = \mathbb{Q}(\sqrt[3]{2})$ et $L = \mathbb{Q}(j\sqrt[3]{2})$
$= \mathbb{Q} \oplus \sqrt[3]{2}\mathbb{Q} \oplus (\sqrt[3]{2})^2\mathbb{Q}$; $= \mathbb{Q} \oplus j\sqrt[3]{2}\mathbb{Q} \oplus j^2\sqrt[3]{2}^2\mathbb{Q}$

On a que K et L sont de dimension 3 sur $\mathbb{Q}$ et donc $K \otimes_{F = \mathbb{Q}} L$ aussi. Or $KL = K[L] = L[K] = \mathbb{Q}(\sqrt[3]{2}, j)$ est de dimension 6 sur $\mathbb{Q}$ et non 9, puisqu'une base est donnée par les monômes en $1, \sqrt[3]{2}, (\sqrt[3]{2})^2, j, j^2$ ce qui donne
$$1, \sqrt[3]{2}, (\sqrt[3]{2})^2, j, j\sqrt[3]{2}, j(\sqrt[3]{2})^2 \quad \text{car } j^2 = j+1$$

Un peu de cohomologie Galoisienne

• Introduction : Hilbert 90

La façon classique de prouver le théorème 90 de Hilbert est celle introduite ici. Elle amène naturellement à la cohomologie galoisienne.

Un homomorphisme croisé est une application

$$f : G \longrightarrow k^\times \qquad \text{où} \quad G \leq \mathrm{Aut}(k)$$

tel que pour $\sigma, \tau \in G$, $\quad f(\sigma\tau) = f(\sigma) \cdot \sigma(f(\tau))$

On rappelle le fait suivant, appelé indépendance des caractères :

Rappel : Étant donné $\chi_1, \dots, \chi_n$ des caractères de G (i.e. $\chi : G \to k^\times$ vérifie $\chi(g \cdot h) = \chi(g) \cdot \chi(h)$, ce sont les éléments du dual $G^\vee$). G est un groupe fini. Alors les caractères sont linéairement indépendants sur k. $\chi_1 + \chi_2(x) = \chi_1(x) + \chi_2(x)$, où on a i.e. en définissant

$$\sum c_i \chi_i = 0 \quad \text{ssi} \quad c_i = 0 \ \forall i$$

Preuve : Par induction, $\chi_1 \neq 0$ puisque $\chi_1 : G \to k^\times$. Comme $\chi_1 \neq \chi_2$ il existe β tel que $\chi_1(\beta) \neq \chi_2(\beta)$. Si on a $\sum \lambda_i \chi_i = 0$ $\forall g$, $\sum \lambda_i \chi_i(\beta g) = 0$ ce qui implique $\sum \lambda_i \chi_i(g) - \frac{1}{\chi_1(\beta)} \left(\sum \lambda_i \chi_i(\beta g) \right) = 0$ ($\chi_1(\beta) \neq 0$, $\chi_2(\beta) \neq 0$) et donc $\sum_{i > 1} \lambda_i \chi_i(g) = 0$ et on conclut par récurrence ■

Proposition : Si K/k est une extension (finie) de Galois de groupe de Galois G et si $f : G \to k^\times$ est un homomorphisme croisé, alors il existe $a \in k$ tel que

$$\forall \sigma \in G, \qquad f(\sigma) = \frac{\sigma(a)}{a}$$

Preuve : Un homomorphisme croisé est en particulier un caractère du groupe G. L'indépendance des caractères appliquée à $\sum_{\sigma \in G} f(\sigma).\sigma(x)$ nous donne l'existence d'un $c \in K$ tel que $\sum_{\sigma \in G} f(\sigma).\sigma(c) \neq 0$. (les constantes de la combinaison linéaire sont $\sigma(c)$). Et soit b ce nombre $\neq 0$. Alors pour $\tau \in G$

$$\begin{aligned}
\tau(b) &= \sum_{\sigma \in G} \tau(f(\sigma)).\tau\sigma(c) \\
&= \sum_{\sigma \in G} f(\tau\sigma).f(\tau)^{-1}.\tau\sigma(c) \\
&= f(\tau)^{-1}.\Big(\sum_{\sigma \in G} f(\tau\sigma).\tau\sigma(c)\Big) \\
&= f(\tau)^{-1}.b
\end{aligned}$$

avec $a = b^{-1}$ cela donne $f(\tau) = \dfrac{\tau(a)}{a}$

Rappel : (Norme d'un élément) : Si K/k est une extension de Galois finie, alors pour chaque $a \in K$, on définit $\hat{a} : K \to K$, $x \mapsto a.x$, c'est une application k-linéaire.

On associe donc la matrice $M(a)$ (de taille $[K:k]^2$) et les deux applications

$$\begin{cases} N_{K/k}(a) = \det M(a) & \text{(norme)} \\ Tr_{K/k}(a) = Tr(M(a)). & \text{(trace)} \end{cases}$$

On rappelle alors les résultats sur la norme :

- $N(a.b) = N(a).N(b)$
- $\forall \sigma \in Gal(K/k)$, $N(\sigma a) = N(a)$
- $N(a) = \prod_{\sigma \in G} \sigma(a)$

Théorème 90 de Hilbert (multiplicatif)

Soit K/k une extension de Galois cyclique.
Soit σ un générateur de $\mathrm{Gal}(K/k) = G$.
Pour $u \in K$ on a

$$N_{K/k}(u) = 1 \quad \text{ssi} \quad u = \frac{\sigma(a)}{a} \text{ pour un } a \in K$$

Preuve: $\boxed{\Leftarrow}$ Si $u = \frac{\sigma(a)}{a}$ alors $N(u) = \frac{N(\sigma a)}{N(a)} = \frac{N(a)}{N(a)} = 1$.

$\boxed{\Rightarrow}$ On définit un homomorphisme croisé $f : G \longrightarrow K^\times$ et on utilise la proposition précédente. On pose $n = |G|$. Puis $f : G \longrightarrow K^\times$ $f(\mathrm{Id}) = $, $f(\sigma) = u$ et

$$f(\sigma^i) = u . \sigma u \dots \sigma^{i-1} u$$

On a alors, pour $i + j < n$:

$$f(\sigma^i \sigma^j) = f(\sigma^{i+j}) = \underbrace{u . \sigma u . \sigma^2 u \dots \sigma^{i-1} u}_{f(\sigma^i)} \dots \sigma^{i+j-1}$$

$$= f(\sigma^i) . \sigma^i u . \sigma^{i+1} u \dots \sigma^{i+j-1} u$$

$$= f(\sigma^i) . \sigma^i (u . \sigma u \dots \sigma^{j-1} u)$$

$$= f(\sigma^i) . \sigma^i (f(\sigma^j)) .$$

A présent si $i + j \geq n$, $i + j - n < n$ et on a

$$f(\sigma^{i+j}) = f(\sigma^{i+j-n}) = u . \sigma u . \dots . \sigma^{i+j-n-1} u$$

or comme $1 = N(u) = \prod_{\tau \in G} \tau u = u . \sigma u . \dots . \sigma^{n-1} u$ et aussi $\sigma^{i+j-n}(1) = 1$ on a

$$= u . \sigma u . \dots . \sigma^{i+j-n-1} u . (\sigma^{i+j-n}(1))$$

$$= u . \sigma u . \dots . \sigma^{i+j-n-1} u . \sigma^{i+j-n} (u . \sigma u . \sigma^2 u \dots \sigma^{n-1} u)$$

$= u . \sigma u . \dots \sigma^{i+j-1} u = f(\sigma^i) . \sigma^i f(\sigma^j)$ et on conclut par la proposition précédente que si u est tel que $N(u) = 1$ alors $f = f_u$ est un homomorphisme multiplicatif donc il existe $a \in k$ tel que $\forall \tau \in G$

$$f(\tau) = \frac{\tau(a)}{a}$$

en particulier si $\tau = \sigma$, $f(\sigma) = \frac{\sigma a}{a}$ et $f(\sigma) = u$ ■

<u>Remarque</u>: Le fait que la norme est $\prod_{\sigma \in G} \sigma u$ donne directement le fait que f est un homomorphisme croisé.

<u>Remarque</u>: On a vu un lemme dans la partie théorie de Kummer qui est traditionnellement prouvé par ce théorème : il s'agit de trouver pour une racine primitive n-ième ζ d'une extension cyclique d'ordre n, un a tq $\zeta = \frac{\sigma(a)}{a}$ (pour σ le générateur). Cela est directement de H 90 puisque $N(\zeta) = 1$ (ζ est dans le corps de base donc $\sigma\zeta = \zeta$ et $N(\zeta) = \prod_{\sigma \in G} \sigma\zeta = \zeta^n = 1$).

On peut montrer la version additive du théorème 90 de Hilbert, en montrant d'une part que tout homomorphisme croisé additif ($f : G \to k$, $f(\sigma\tau) = f(\sigma) + \sigma f(\tau)$) est de la forme $f(\tau) = \tau(a) - a$, en utilisant la propriété suivante de la trace :

$$Tr(x) = \sum_{\sigma \in G} \sigma x.$$

On arrive au résultat suivant :

<u>Théorème 90 de Hilbert (additif)</u> Si K/k est une extension de Galois cyclique avec σ un générateur de $Gal(K/k)$. Soit $u \in K$ alors

$Tr(u) = 0$ ssi $\exists a \in K$ $\sigma(a) - a = u$.

<u>Preuve</u>: On considère cette fois l'homomorphisme croisé $f : G \to K$

$$f(Id) = 0 \qquad f(\sigma) = u$$

$$f(\sigma^i) = u + \cdots + \sigma^{i-1}(u).$$

et on utilise $Tr(u) = \sum_{i=1}^{n} \sigma^i u = 0$ ■

- Cohomologie

On passe à présent à la définition du groupe de cohomologie, et on traduira les résultats de la section précédente en termes de cohomologie.

On considère deux groupes G et M où M est abélien et noté additivement et G multiplicativement. On dit que M est un <u>G-module</u> si le groupe G agit sur le groupe M et si cette action est compatible avec le groupe M, autrement dit : $G \times M \longrightarrow M$

$$1 . m = m$$

$$\sigma . (\tau m) = (\sigma \tau)(m)$$

$$\sigma (m_1 + m_2) = \sigma m_1 + \sigma m_2$$

On peut penser à l'action du groupe d'homomorphismes du groupe M sur M. On peut aussi voir cette action comme M étant un $\mathbb{Z}[G]$-module.

- <u>Cochaîne</u> : Une n-cochaîne est une application

$$f : \overbrace{G \times \dots \times G}^{n} \longrightarrow M$$

On note $C^n(G, M)$ l'ensemble M^{G^n} des cochaînes.
Si $n = 0$, $C^0(G, M)$ est par convention M.
On munit $C^n(G, M)$ d'une addition qui est celle de M, par $f + g(x_1 \dots x_n) = f(x_1 \dots x_n) + g(x_1 \dots x_n)$.
$C^n(G, M)$ est donc muni d'une opération qui en fait un groupe abélien.

- <u>Application de bord</u> : On définit $\delta_n : C^n(G, M) \to C^{n+1}(G, M)$ par

$$\delta_n(f)(\sigma_1, \dots, \sigma_{n+1}) = \sigma_1 f(\sigma_2, \dots, \sigma_{n+1})$$
$$+ \sum_{i=1}^{n} (-1)^i f(\sigma_1, \dots, \sigma_i \cdot \sigma_{i+1}, \dots, \sigma_{n+1})$$
$$+ (-1)^{n+1} f(\sigma_1, \dots, \sigma_n)$$

et pour $n=0$, $\delta_0 : M = C^0(G,M) \longrightarrow C^1(G,M)$

$$m \longmapsto (\sigma \longmapsto \sigma m - m)$$

On a que $\delta_n(f+g) = \delta_n(f) + \delta_n(g)$, c'est un <u>homomorphisme additif</u>, on a de plus que

$$\delta_{n+1} \circ \delta_n : C^n(G,M) \xrightarrow{\delta_n} C^{n+1}(G,M) \xrightarrow{\delta_{n+1}} C^{n+2}(G,M)$$

est <u>l'application nulle</u>. On le fait pour $n=1$:

<u>Exemple</u> : $\delta_0 \circ \delta_1 = 0$

On a $\delta_0 : M \to C^1(G,M)$ $\quad \delta_1 : C^1(G,M) \to C^2(G,M)$

$m \mapsto (\sigma \mapsto \sigma m - m)$ $\quad f \mapsto ((\sigma_1\sigma_2) \mapsto \sigma_1 f(\sigma_2) - f(\sigma_1\sigma_2) + f(\sigma_1))$

On a alors que

$$\delta_0 \circ \delta_1(m)(\sigma_1\sigma_2) = \sigma_1(\sigma_2 m - m) - (\sigma_1\sigma_2(m) - m) + (\sigma_1(m) - m)$$

$$= 0$$

Les applications $\delta_n : C^n(G,M) \longrightarrow C^{n+1}(G,M)$ étant des morphismes de groupe, on peut considérer leur noyaux

$$Z^n(G,M) = \ker \delta_n \subseteq C^n(G,M)$$

c'est l'ensemble des <u>cocycles</u> (ou <u>n-cocycles</u>).

<u>Exemple</u> : (0-cocycles) : Un 0-cocycle est un élément de M vérifiant $\forall \sigma \in G$, $\sigma m - m = 0$ i.e. $\sigma m = m$.

(1-cocycle) : Un 1 cocycle est une applic $f : G \to M$ tel que $f(\sigma_1\sigma_2) = f(\sigma_1) + \sigma_1 f(\sigma_2)$

Enfin, puisque $\delta_n \circ \delta_{n-1} = 0$, il s'ensuit que

$$C^{n-1}(G,M) \xrightarrow{\delta_{n-1}} C^n(G,M) \xrightarrow{\delta_n} C^{n+1}(G,M)$$

$$\operatorname{Im} \delta_{n-1} \subseteq \ker \delta_n$$

On appelle $B^n(G,M) = \operatorname{Im} \delta_{n-1}$ (pour $n=0$ $B^0(G,M) = \{0\}$)

Les éléments de $B^n(G,M)$ sont appelés les <u>cobords</u>.

• Le <u>n-ième groupe de cohomologie</u> de G et M est

$$H^n(G,M) = \frac{Z^n(G,M)}{B^n(G,M)}$$

Deux n-cocycles sont cohomologues si elles sont dans la même classe modulo $B^n(G,M)$, i.e. si leur différence est un cobord.

Exemple : $H^0(G,M) = \dfrac{Z^0(G,M)}{B^0(G,M)} = Z^0(G,M)$

$= \{m \in M,\ \forall \sigma \in G,\ \sigma m = m\}$

On a à présent la définition formelle des groupes de cohomologie associés à un G-module M. On va à présent étudier le cas Galoisien.

• <u>Cohomologie Galoisienne</u> :

On considère une extension de Galois finie K/k et $G = \mathrm{Gal}(K/k)$. On a alors que le groupe K^+ est un G-module, de même pour le groupe $K^\times$.

Exemple : $H^0(G, K^+) = k^+$

En effet, on a $H^0(G, K^+) = Z^0(G, K^+) = \ker \delta_0$

avec $\delta_0 : K^+ = C^0(G, K^+) \longrightarrow C^1(G, K^+)$

$$x \longmapsto (\sigma \mapsto \sigma x - x)$$

donc si $\delta_0(x) = 0$, on a $\forall \sigma \in G$, $\sigma x - x = 0$ donc on a bien $x \in k$.

De même :

Exemple ($H^0(G, k^\times) = k^\times$)

Cette fois ci $Z^0(G, k^\times) = \{x \in k^\times \text{ tq } \forall \sigma \in G \ \sigma x . x^{-1} = 1\}$

$= \{x \in k^\times \ \sigma x = x\} = k$.

- Théorème 90 de Hilbert cohomologique

- Additif :

On décrit les éléments de $Z^1(G, k^+)$. Soit donc $f \in Z^1(G, k^+)$ un 1-cocycle, alors $f : G \to k^+$ et :

$$\delta_1(f)(\sigma_1, \sigma_2) = 0 \quad \text{i.e.}$$

$$\sigma_1 f(\sigma_2) - f(\sigma_1 . \sigma_2) + f(\sigma_1) = 0$$

et donc $f(\sigma_1 . \sigma_2) = f(\sigma_1) + \sigma_1 f(\sigma_2)$. C'est donc un homomorphisme croisé.

On décrit les éléments de $B^1(G, k^+)$. Soit donc $f \in B^1(G, k^+)$ un cobord, par définition cela veut dire qu'il existe un $\beta \in C^0(G, k^+) = k^+$ tel que $\delta_0(\beta) = f$. Autrement dit on a $f(\sigma) = \sigma\beta - \beta$.

Un cocycle est donc une application $f : G \to k^+$ tel que $f(\sigma_1 . \sigma_2) = f(\sigma_1) + \sigma_1 f(\sigma_2)$

Un cobord est donc une application $f : G \to k^+$ tel que il existe $a \in k^+$ tel que $f(\sigma) = \sigma a - a$

La discussion avant le Hilbert 90 additif nous dit alors que tout cocycle est un cobord et donc $H^1(G, k^+) = \{0\}$

• Multiplicatif

On récapitule ce que l'on voit pour la description des 1-cocycles et 1-cobords.

Proposition : Soit G le groupe de Galois d'une extension de Galois finie K/k. Alors

- Les 1-cocycles $f \in Z^1(G, K^\times)$ sont de la forme
$$f(\tau\sigma) = f(\tau) \cdot \tau f(\sigma)$$
- Les 1-cobords $f \in B^1(G, K^\times)$ vérifient qu'il existe $a \in K^\times$ tel que $f(\tau) = \frac{\tau a}{a}$

Preuve : Il s'agit juste de retraduire ce qu'on a fait précédemment. ⊠

À présent la proposition première de cette fiche nous dit que pour tout homomorphisme croisé $f : G \to K^\times$ il existe $a \in K$ tel que $f(\tau) = \frac{\tau a}{a}$. On a donc que tout 1-cocycle est un 1-cobord et donc que le groupe de cohomologie est trivial. On récapitule :

Théorème (Hilbert 90 cohomologique)

Soit K/k une extension Galoisienne finie de groupe de Galois G. Alors

- $H^1(G, K^+) = 0$
- $H^1(G, K^\times) = 1$

Notons que ce que l'on appelle ici Hilbert 90 correspond plus à la proposition servant à prouver le véritable Hilbert 90, celui qui parle de la norme et la trace. Donc nous allons en retenir que $H^1(G, K^+) = 0$ et $H^1(G, K^\times) = 1$

en construisant un homomorphisme croisé additif et multiplicatif et on utilise la cohomologie pour dire qu'il existe un a tel que ces homomorphismes sont des cobords.

<u>Exemple</u>: <u>Toute extension cyclique de Galois de degré la caractéristique du corps de base est d'Artin - Schreier</u>

En effet si K/k est de Galois de degré $p = \mathrm{car}\, k$.
On a alors que $Tr(1) = \sum_{\tau \in G} \tau(1) = p.1 = 0$. Donc par Hilbert 90 additif il existe u tel que pour τ le générateur de G, $1 = \tau u - u$ i.e. $\tau u = 1 + u$.

Alors $\tau(u^p - u) = \tau(u)^p - \tau u = (1+u)^p - 1 + u$
$= u^p - u$ donc $u^p - u \in k$

et donc $k(u)/k$ est d'Artin - Schreier, et comme $[K:k]$ est premier et $u \notin k$ $(\tau u = u+1)$ on conclut que $k(u) = K$.

Limite inductive

Il existe une notion duale à celle de limite inverse, étant donné un système inverse dans lequel on inverse les flèches, on peut définir une notion de limite. Pour cette notion sera celle de limite inductive $\varinjlim$.

On se donne donc un système inductif d'ensemble à savoir :

- un ensemble (partiellement) ordonné $(I, \leq)$ tq $\forall i, j\ \exists k\ \ i \leq k \geq j$
- une famille d'ensemble $(E_i)_{i \in I}$
- pour chaque i, j tq $i \leq j$, une fonction
$$f_{ij} : E_i \longrightarrow E_j$$
- si $i \leq j \leq k$ alors $f_{ik} = f_{jk} \circ f_{ij}$
$$f_{ik} : E_i \xrightarrow{f_{ij}} E_j \xrightarrow{f_{jk}} E_k$$
- $f_{ii} = 1\!\!1_{E_i}$

Un tel système $(E_i, f_{ij})_{i \leq j \in I}$ est appelé un système inductif d'ensemble.

Un tel ensemble ordonné $(I, \leq)$ est un ensemble filtrant supérieurement.

On considère ensuite l'union disjointe $\mathcal{E} = \coprod_{i \in I} E_i$, un élément de $\mathcal{E}$ est "taggé", i.e. de la forme (x, i) avec $x \in E_i$ et on a des injections $u_i : E_i \longrightarrow \mathcal{E}$

Sur $\mathcal{E}$ on définit une relation d'équivalence de la façon suivante,

$$(x, i) \, R \, (y, j) \quad \text{ssi} \quad \forall k \ \ i \leq k \geq j \ \text{ on a}$$
$$f_{ik}(x) = f_{jk}(y).$$

On pose ensuite $\varinjlim E_i = \mathcal{E}/R$, la limite inductive d'un système inductif $(E_i, f_{ij})_{i,j \in I}$.

On dispose de $s : \mathcal{E} \longrightarrow \mathcal{E}/_R$ la surjection canonique.

On dispose alors de
$$f_i : E_i \longrightarrow \mathcal{E}/_R$$
$$x \longmapsto s(x) \quad (= s(u_i(x)))$$

En remarquant le fait trivial que si $x \in E_i$, $i \leq j$ alors $(f_{ij}(x), j) R (x, i)$ on a que le diagramme suivant commute : $f_i = f_j \circ f_{ij}$

$$\begin{tikzcd} E_i \arrow[r, "f_i"] \arrow[d, "f_{ij}"'] & \varinjlim E_i \\ E_j \arrow[ur, "f_j"'] & \end{tikzcd}$$

<u>Exemple</u> : (Dans la catégorie des ensembles) Si $(E_i)_{i \in I}$ sont des ensembles et $f_{ij} : E_i \longrightarrow E_j$ est l'inclusion, alors $(x, i) R (y, j)$ ssi pour tout $k \geq i, k \geq j$ $f_{ik}(x) = f_{jk}(y)$ alors veut dire que x et y sont égaux dans un ensemble qui les contient tous les deux en même temps et donc on a qu'un seul représentant de ce pour tous les ensembles qui le contiennent et donc $\varinjlim E_i = \bigcup E_i$.

• <u>Propriété universelle</u>

Supposons que l'on dispose d'un système inductif $(E_i, f_{ij})_{i,j \in I, i \leq j}$ et que l'on a de plus un ensemble F et des fonctions $(g_i)_{i \in I}$ qui sont <u>compatibles avec le système inductif</u>, i.e

$$\begin{tikzcd} E_i \arrow[r, "g_i"] \arrow[d, "f_{ij}"'] & F \\ E_j \arrow[ur, "g_j"'] & \end{tikzcd} \qquad g_i = g_j \circ f_{ij} \quad \forall i \leq j.$$

Alors il existe une unique application $\underset{\displaystyle g}{\overset{\varinjlim g_i}{\shortparallel}} : \varinjlim E_i \longrightarrow F$ telle que l'on ait : $g_i = g \circ f_i$ i.e

$$\begin{tikzcd} E_i \arrow[r, "g_i"] \arrow[d, "f_i"'] & F \\ \varinjlim E_i \arrow[ur, "g"'] & \end{tikzcd}$$

et ce $\forall i \in I$.

C'est une conséquence du théorème de factorisation des applications. On note

Dans notre exemple :

Exemple : Si tous les E_i sont inclus dans un certain F, $g_i : E_i \longrightarrow F$ est l'inclusion, alors $g : \bigcup E_i \longrightarrow F$.

• Cofinalité et calcul de $\varinjlim$

Une partie $I' \subseteq I$ est cofinale si $\forall i \in I$ il existe $j \in I'$ tel que $j \geq i$.

Si l'on se donne un système inductif $(E_i, f_{ij})_{i\in I}$ et $I' \subseteq I$ cofinale, alors si $i, j \in I'$ il existe $k \in I$ avec $k \geq i,j$ et donc il existe $k' \geq k \geq i,j$ cela implique que I' est filtrante au-dessus et donc que $(E_i, f_{ij})_{i\in I'}$ est encore un système inductif que l'on appelle la restriction à I' du système $(E_i, f_{ij})_{i\in I}$.

On constate de plus que sous ces hypothèses, avec pour chaque $i \in I'$ $f_i : E_i \longrightarrow \varinjlim_I E_i$ est compatible avec le système et $(f_i)_{i\in I}$ admet donc une limite (avec $F = \varinjlim_I E_i$), et par la propriété universelle :

$$f := \varinjlim_{I'} f_i : \varinjlim_{I'} E_i \longrightarrow \varinjlim_{I} E_i$$

On vérifie ensuite que cet f est en fait une bijection.

On voit donc que pour calculer une limite inductive du système inductif $(E_i, f_{ij})_{i,j\in I}$ il suffit de la calculer pour une restriction de ce système à une partie cofinale $I' \subseteq I$.

• Limite inductive de structures

On peut rajouter des contraintes pour enrichir notre notion de limite inductive. Si l'on dispose d'une certaine famille inductive (M_i, f_{ij}) où les f_{ij} sont des homomorphismes alors la limite inductive est munie de la même structure. La propriété universelle reste vraie avec les g_i étant des homomorphismes et de même pour le résultat sur la restriction à une partie cofinale, $\varinjlim f_i$ devient un isomorphisme.

Plus précisément, il est montré dans le [Barnes-Mack An algebraic introduction to mathematical logic] que pour toute structure axiomatisée par une axiomatique $\forall \exists$, alors la limite inductive est encore un modèle de la théorie.

<u>Exemple</u>: On peut montrer que si A est un anneau et que $\mathcal{S}$ est l'ensemble des parties S multiplicativement fermées de A avec $1 \in S$ et $0 \notin S$, alors $\varinjlim (S^{-1}A)_{S \in \mathcal{S}}$ est isomorphe à l'anneau des fractions de A. [Cf. Fr Géométrie algébrique]