THÉORIE DE GALOIS INFINIE ET COHOMOLOGIE

Martin Debaisieux

Table des matières

1 Prérequis : les extensions normales

1.1 Les corps de décomposition

Soit K un corps et P un polynôme de $K[X]$ de degré au moins 1. Le *corps de décomposition* L de P est une extension de K telle que P se décompose en facteurs linéaires dans L, *i.e.* telle que

$$P(X) = c(X - \alpha_i) \cdots (X - \alpha_n) \in L[X]$$

où chaque $\alpha_i \in L$ et telle que $L = K(\alpha_1, \ldots, \alpha_n)$ est engendrée par toutes les racines de P.

Théorème 1.1. *Soit L un corps de décomposition du polynôme P à coefficients dans K. Si M est un autre corps de décomposition de P, alors il existe un isomorphisme $\sigma\colon M \xrightarrow{\sim} L$ qui fixe K. Si $K \subseteq L \subseteq K^{\mathrm{alg}}$, alors tout K-plongement de M dans K^{alg} doit être un isomorphisme de M dans L.*

Démonstration. Considérons L^{alg} une clôture algébrique de L. Dans ce cas, L^{alg} est algébrique sur K et est donc une clôture algébrique de K. Par conséquent il existe un K-plongement $\sigma\colon M \hookrightarrow L^{\mathrm{alg}}$. De la factorisation

$$P(X) = c(X - \beta_1) \cdots (X - \beta_n) \in M[X]$$

où, pour chaque i, β_i est dans M et où le coefficient c est dans K, on obtient

$$P(X) = P^{\sigma}(X) = c(X - \sigma\beta_1) \cdots (X - \sigma\beta_n) \in L^{\mathrm{alg}}[X].$$

Il y a une unique factorisation dans $L^{\mathrm{alg}}[X]$. Vu que P se factorise en

$$P(X) = c(X - \alpha_i) \cdots (X - \alpha_n) \in L[X],$$

il s'en suit que $(\sigma\beta_1, \ldots, \sigma\beta_n)$ et $(\alpha_1, \ldots, \alpha_n)$ sont égaux à permutation près. On peut alors conclure que $\sigma\beta_i$ est un élément de L pour tout i et donc $\sigma M \subseteq L$. Cependant,

$$L = K(\alpha_1, \ldots, \alpha_n) = K(\sigma\beta_1, \ldots, \sigma\beta_n)$$

et donc $\sigma M = L$ car $M = K(\beta_1, \ldots, \beta_n)$. □

Un corps de décomposition de $P(X) \in K[X]$ existe toujours, en l'occurrence le corps dans lequel on adjoint toutes les racines de P dans une clôture algébrique K^{alg} de K. Soit I un ensemble d'indices, potentiellement infini, et soit $(P_i)_{i \in I}$ une famille de polynômes de $K[X]$ de degré au moins 1, on entend par *corps de décomposition* de cette famille, une extension L de K tel que tout P_i se décompose en facteurs linéaires dans $L[X]$, et L est généré par toutes les racines de tous les polynômes P_i, pour $i \in I$.

Définition 1.2. Soient E et F des extensions d'un corps K. Si E et F sont contenues dans un même corps L, on dénote par EF le plus petit sous-corps de L qui contient à la fois E et à la fois F et on l'appelle le *compositum* de E et F.

Remarque 1.3. Si E et F ne sont pas contenus dans un même corps, alors la notion de compositum ne peut pas être définie.

Soit K^{alg} une clôture algébrique de K et soit L_i un corps de décomposition de P_i dans K^{alg}. Le compositum des L_i est un corps de décomposition pour la famille $(P_i)_{i \in I}$ vu que les deux conditions définissant un corps de décomposition sont automatiquement vérifiées. Le théorème précédent s'étend ainsi au cas infini :

Corollaire 1.4. *Soit L un corps de décomposition d'une famille $(P_i)_{i \in I}$ et soit M un autre corps de décomposition. Tout K-plongement de M dans L^{alg} donne lieu à un isomorphisme de M dans L.*

Démonstration. Remarquons que M contient un unique corps de décomposition M_i de P_i et L doit contenir un unique corps de décomposition L_i de P_i. Tout plongement $\sigma\colon M \hookrightarrow L^{\mathrm{alg}}$ doit associer M_i à L_i par le théorème précédent et donc doit associer M à L. Vu que L est le compositum des corps L_i, l'application σ doit envoyer M sur L et donc induire un isomorphisme de M dans L. □

Remarque 1.5. Si I est fini et que les polynômes sont $P_1, \ldots, P_n$, alors leur corps de décomposition est le corps de décomposition du seul polynôme

$$P(X) = P_1(X) \cdots P_n(X)$$

obtenu en prenant leur produit. Cependant, même dans le cas fini, il est pratique de travailler sur un ensemble de polynômes plutôt qu'un seul.

1.2 La normalité

Lemme 1.6. *Soit E une extension algébrique d'un corps K et soit $\sigma\colon E \hookrightarrow E$ un K-plongement. Alors σ est un automorphisme.*

Démonstration. Vu que σ est injective, il suffit de montrer la surjectivité. Soit α un élément de E et considérons $P_{\alpha,K}$ son polynôme minimal sur K. Soit E' le sous-corps de E généré par toutes les racines de $P_{\alpha,K}$ dans E. Alors E' est de type fini et est donc une extension finie de K. De plus, σ doit envoyer une racine de $P_{\alpha,K}$ sur une racine de $P_{\alpha,K}$, cela permet d'affirmer que σ envoie E' sur lui-même. On peut voir σ comme un K-morphisme d'espaces vectoriels car σ fixe K. Vu que σ est une injection, son image $\sigma E'$ est un sous-espace de E' ayant la même dimension $\dim_K E'$. Par conséquent $\sigma E' = E'$. Vu que α est un élément de E', il s'en suit que α est dans l'image de σ. □

Théorème 1.7. *Soit L une extension algébrique d'un corps K, contenue dans une clôture algébrique K^{alg} de K. Les assertions suivantes sont équivalentes :*

(1) Chaque K-plongement de L dans K^{alg} induit un automorphisme de L.

(2) L est le corps de décomposition d'une famille de polynômes de $K[X]$.

(3) Chaque polynôme irréductible de $K[X]$ qui possède une racine dans L se décompose en facteurs linéaires dans L.

Démonstration. Supposons (1). Soit α un élément de L et soit $P_{\alpha,K}$ son polynôme minimal sur K. Soit β une racine de $P_{\alpha,K}$ dans K^{alg}. Il existe un isomorphisme $K(\alpha) \xrightarrow{\simeq} K(\beta)$ qui fixe K et qui envoie α sur β. On étend cet isomorphisme en un plongement $L \hookrightarrow K^{\mathrm{alg}}$. Cette extension est un automorphisme σ de L, par hypothèse. Donc $\sigma\alpha = \beta \in L$ et ainsi chaque racine de $P_{\alpha,K}$ est dans L. Donc $P_{\alpha,K}$ se décompose en facteurs linéaires dans $L[X]$. Ainsi, L est le corps de décomposition de la famille $(P_{\alpha,K})_{\alpha\in L}$ et donc (2) est satisfait.

Supposons (2) et soit $(P_i)_{i\in I}$ une famille de polynômes dont L est le corps de décomposition. Si α est racine de l'un d'entre-eux dans L, disons P_i, alors pour tout K-plongement $L \hookrightarrow K^{\mathrm{alg}}$, on sait que $\sigma\alpha$ est encore racine de P_i. Vu que L est généré par toutes les racines de tous les polynômes P_j, il en découle que $\sigma\colon L \hookrightarrow L$. On applique le lemme précédent pour conclure que σ est un automorphisme.

La preuve que (1) implique (2) montre également (3). Réciproquement, supposons (3) et soit σ un K-plongement de $L \hookrightarrow K^{\mathrm{alg}}$. Soit $\alpha \in L$ et considérons $P_{\alpha,K}$ le polynôme minimal de α sur K. Alors σ envoie α sur β, une racine de $P_{\alpha,K}$ et, par hypothèse, β est dans L. Donc $\sigma\alpha$ est un élément de L et ainsi $\sigma\colon L \hookrightarrow L$. On utilise une nouvelle fois le lemme précédent pour conclure que σ est un automorphisme. □

Définition 1.8. Une extension L d'un corps K satisfaisant l'une des assertions du théorème précédent est qualifiée de *normale*.

Remarque 1.9. Une tour d'extensions normales n'est pas nécessairement normale. Il est facile de montrer qu'une extension quadratique est normale, cependant, si on considère $\mathbf{Q}(\sqrt[4]{2})$, elle n'est pas normale puisque les racines complexes de $X^4 - 2$ ne s'y trouvent pas. Pourtant, cette extension est obtenue par une succession d'extensions quadratiques :

$$\mathbf{Q}(\sqrt[4]{2}) \text{ —}2\text{— } \mathbf{Q}(\sqrt{2}) \text{ —}2\text{— } \mathbf{Q}.$$

Proposition 1.10. *Les extensions normales restent normales sous relèvement. Si $K \subseteq L \subseteq M$ est une tour d'extensions et M est normale sur K, alors M est normale sur L.*

Démonstration. Soit F une extension de M et supposons que M et F soient contenus dans un corps commun. Soit σ un F-plongement de MF dans F^{alg}. Alors σ fixe F et donc K. Par hypothèse, sa restriction à M envoie M sur lui-même. Ainsi,

$$\sigma(MF) = \sigma(M)\sigma(F) = MF$$

et donc MF est normale sur F. Supposons que $K \subseteq L \subseteq M$ et que M est normale sur K. Soit σ un L-plongement de M dans K^{alg}, alors σ est également un K-plongement de M dans K^{alg} et la conclusion s'obtient par définition. □

Proposition 1.11. *Si E et F sont des extensions normales sur K et sont contenues dans un corps commun, alors EF est normale sur K et il en est de même pour $E \cap F$.*

Démonstration. Si E et F sont des extensions normales sur K, alors pour tout K-plongement de EF dans K^{alg}, on a

$$\sigma(EF) = \sigma(E)\sigma(F)$$

et la conclusion s'obtient à nouveau de l'hypothèse. Pour ce qui est de l'intersection, cela découle du fait que

$$\sigma(E \cap F) = \sigma(E) \cap \sigma(F).$$ □

On constate que si L est une extension normale de type fini sur K, disons

$$L = K(\alpha_1, \ldots, \alpha_n),$$

et $P_{\alpha_1,K}, \ldots, P_{\alpha_n,K}$ sont les polynômes minimaux respectifs de $\alpha_1, \ldots, \alpha_n$ sur K, alors L est déjà le corps de décomposition d'une famille finie $(P_{\alpha_i,K})_{i=1}^n$.

2 Prérequis : les extensions séparables

2.1 Le degré séparable

Soit L une extension algébrique d'un corps K et soit $\sigma\colon K \hookrightarrow \Omega$ un plongement dans un corps algébriquement clos Ω. Par l'étude des extensions de plongements, toute extension de σ à L associe L à un sous-corps de Ω qui est algébrique sur σK. On suppose donc que Ω est algébrique sur σK et est donc une clôture algébrique de σK.

On désigne par S_σ l'ensemble des extensions de σ en un plongement de L dans Ω. Soit Ω' un autre corps algébriquement clos, et soit $\tau\colon K \hookrightarrow \Omega'$ un plongement. On suppose également que Ω' est une clôture algébrique de τK. Ces clôtures sont donc isomorphes par $\lambda\colon \Omega \xrightarrow{\sim} \Omega'$ qui étend $\tau\circ\sigma^{-1}$ appliqué au corps σK. Ceci est expliqué sur le diagramme suivant :

$$\begin{array}{ccccc}
\Omega' & \xleftarrow{\qquad\lambda\qquad} & & & \Omega \\
| & & & & | \\
\tau^*L & \xleftarrow{\tau^*} & L & \xrightarrow{\sigma^*} & \sigma^*L \\
| & & | & & | \\
\tau K & \xleftarrow{\tau} & K & \xrightarrow{\sigma} & \sigma K
\end{array}$$

On pose S_τ l'ensemble des plongements de L dans Ω' qui étendent τ. Si $\sigma^* \in S_\sigma$ est une extension du plongement σ de L dans Ω, alors $\lambda \circ \sigma^*$ est une extension du plongement τ de L dans Ω' car, en se restreignant à K, on a

$$\lambda \circ \sigma^* = \tau \circ \sigma^{-1} \circ \sigma = \tau.$$

Donc λ induit une application de S_σ dans S_τ. Il est clair que l'application inverse est induite par λ^{-1}. Donc S_σ et S_τ sont en bijection sous l'application

$$\sigma^* \mapsto \lambda \circ \sigma^*.$$

En particulier, la cardinalité de S_σ et S_τ est la même. Cette cardinalité ne dépend donc que de l'extension L/K et sera notée

$$[L : K]_{\mathrm{s}}.$$

Nous l'appelons le *degré séparable* de L sur K. Cette notion est (bien entendu) surtout intéressante en dimension finie.

Théorème 2.1. *Soit $K \subseteq L \subseteq M$ une tour d'extensions de corps. Alors le degré séparable est multiplicatif,*

$$[M : K]_s = [M : L]_s \, [L : K]_s.$$

De plus, si M est une extension finie de K, alors $[M : K]_s$ est fini et

$$[M : K]_s \leq [M : K].$$

Le degré séparable est au plus égal au degré de l'extension.

Démonstration. Soit $\sigma\colon K \hookrightarrow \Omega$ un plongement de K dans un corps algébriquement clos Ω. Soit $(\sigma_i)_{i\in I}$ la famille d'extensions de plongements distincts de σ à L et, pour tout i, soit $(\tau_{ij})_{j\in J}$ la famille d'extensions de plongements distincts de σ_i à M. Chaque σ_i possède $[M : L]_{\mathrm{s}}$ extensions distinctes de M dans Ω. L'ensemble formé des τ_{ij}, pour $i \in I$ et $j \in J$, contient donc précisément

$$[M : L]_{\mathrm{s}} \, [L : K]_{\mathrm{s}}$$

éléments. Tout plongement de M dans Ω doit être l'un des τ_{ij} et donc on a bien la multiplicativité des degrés séparables.

Pour la deuxième assertion, supposons que M/K soit finie. On peut obtenir M via une tour d'extensions, à chaque étape générée par un élément :

$$K \subseteq K(\alpha_1) \subseteq \cdots \subseteq K(\alpha_1, \ldots, \alpha_n) = M.$$

Si on défini récursivement $L_{i+1} = L_i(\alpha_{i+1})$, une proposition implique alors que

$$[L_i(\alpha_{i+1}) : L_i]_{\mathrm{s}} \leq [L_i(\alpha_{i+1}) : L_i].$$

Vu que cette inégalité est vérifiée à chaque étape de la tour, par multiplicativité on conclut qu'elle est valable pour M/K. □

Corollaire 2.2. *Soit $K \subseteq L \subseteq M$ une tour d'extensions de corps avec M/K finie. L'égalité*

$$[M : K]_s = [M : K]$$

est vérifiée si et seulement si l'égalité est vérifiée à chaque étape de la tour, i.e. pour M/L et L/K.

Démonstration. Il suffit de remarquer, en utilisant l'hypothèse et la multiplicativité que

$$[M : L] \geq [M : L]_{\mathrm{s}} = \frac{[M : K]_{\mathrm{s}}}{[L : K]_{\mathrm{s}}} = \frac{[M : K]}{[L : K]_{\mathrm{s}}} \geq \frac{[M : K]}{[L : K]} = [M : L].$$

En tenant compte de ce raisonnement, la preuve est directe. □

On peut montrer que $[M : K]_{\mathrm{s}}$ divise le degré $[M : K]$ lorsque M/K est une extension finie. On définit $[M : K]_{\mathrm{i}}$ tel que

$$[M : K]_{\mathrm{s}}\,[M : K]_{\mathrm{i}} = [M : K].$$

Par la multiplicativité du degré séparable et du degré dans les tours, on peut facilement se rendre compte que le degré $[M : K]_{\mathrm{i}}$ est également multiplicatif.

2.2 La séparabilité

Définition 2.3. Soit L une extension finie d'un corps K. On dit que L est *séparable* sur K si elle satisfait $[L : K]_{\mathrm{s}} = [L : K]$.

Définition 2.4. Un élément algébrique α sur K est qualifié de *séparable* sur K si $K(\alpha)$ est séparable sur K.

Cette condition est équivalente à ce que son polynôme minimal sur K soit à racines simples.

Définition 2.5. Un polynôme $P(X) \in K[X]$ est appelé *séparable* s'il est à racines simples.

Remarque 2.6. Si α est racine d'un polynôme séparable $P(X) \in K[X]$, alors le polynôme minimal de α sur K divise P et donc α est séparable sur K.

On peut noter que si $K \subseteq L \subseteq M$ est une tour d'extensions de corps et que $\alpha \in M$ est séparable sur K, alors il est séparable sur L. En effet, si $P(X) \in K[X]$ est un polynôme séparable tel que $P(\alpha) = 0$, alors P est aussi à coefficients dans L et donc α est séparable sur L.

Théorème 2.7. *Soit L une extension finie de K. Alors L est séparable sur K si et seulement si chaque élément de L est séparable sur K.*

Démonstration. Supposons dans un premier temps que L soit séparable sur K et soit $\alpha \in L$. On considère

$$K \subseteq K(\alpha) \subseteq L.$$

Par le corollaire précédent, $[K(\alpha) : K]_s = [K(\alpha) : K]$ et donc α est séparable sur K. Réciproquement, supposons que chaque élément de L soit séparable sur K. Étant donné que L/K est finie, il existe $\alpha_1, \ldots, \alpha_n \in L$ tel que $L = K(\alpha_1, \ldots, \alpha_n)$. En particulier, les $\alpha_1, \ldots, \alpha_n$ sont séparables sur K. On considère la tour

$$K \subseteq K(\alpha_1) \subseteq \cdots \subseteq K(\alpha_1, \ldots, \alpha_n) = L.$$

Et puisque chaque α_i est séparable sur K, chaque α_i est séparable sur le corps $K(\alpha_1, \ldots, \alpha_{i-1})$, pour $i \geq 2$, on en déduit que L est séparable sur K. □

Ce dernier argument montre que si L est généré par un nombre fini d'éléments séparables sur K alors L est séparable sur K.

Définition 2.8. Soit L une extension algébrique de K. On dit que L est *séparable* sur K si chaque extension de la forme $K(\alpha_1, \ldots, \alpha_n)$, pour $\alpha_1, \ldots, \alpha_n \in L$, est séparable sur K.

Théorème 2.9. *Soit L une extension algébrique sur K, générée par une famille d'éléments $(\alpha_i)_{i \in I}$. Si chaque α_i est séparable sur K, alors L est séparable sur K.*

Démonstration. Chaque élément de L repose dans une extension finie de la forme

$$K(\alpha_{i_1}, \ldots, \alpha_{i_n}).$$

Comme remarqué précédemment, chaque tel sous-corps est séparable sur K. Par le théorème précédent, on peut alors affirmer que chaque élément de L est séparable sur K, ce qui conclut. □

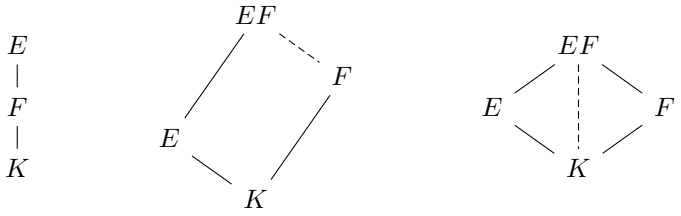
Définition 2.10. Soit C une classe d'extensions E d'un corps F. La classe C est **distinguée** si elle satisfait les conditions suivantes :

(1) Soit $K \subseteq F \subseteq E$ une tour d'extensions de corps. L'extension E/K est dans C si et seulement si F/K et E/F sont dans C.

(2) Si l'extension E/K est dans C, si F est une extension de K et E, F sont tous les deux contenus dans un corps, alors EF/F est dans C.

(3) Si les extensions F/K et E/K sont dans C et F, E sont des sous-corps d'un corps commun, alors EF/K est dans C.

Les diagrammes suivants illustrent respectivement les trois conditions de la définition.



Théorème 2.11. *Les extensions séparables forment une classe distinguée des extensions.*

Démonstration. Supposons que E soit séparable sur K et soient $K \subseteq F \subseteq E$. Chaque élément de E est séparable sur F et tout élément de F est un élément de E, donc F est séparable sur K. Donc chaque niveau de la tour est séparable. Réciproquement, supposons que $K \subseteq F \subseteq E$ est une tour d'extensions telle que E/F et F/K sont séparables. Si E est une extension finie sur K, alors on peut utiliser un corollaire précédent, à savoir le degré séparable est égal au degré à chaque étape de la tour. D'où une

égalité pour E sur K par multiplicativité. Si E est infinie, soit $\alpha \in E$. Alors, α est racine d'un polynôme séparable $P(X)$ à coefficients dans F. Soient $a_n, \ldots, a_0$ ses coefficients, posons $F_0 := K(a_n, \ldots, a_0)$. Alors F_0 est séparable sur K et α est séparable sur F_0. On peut alors se focaliser sur la tour finie

$$K \subseteq F_0 \subseteq F_0(\alpha)$$

et on peut conclure que $F_0(\alpha)$ est séparable sur K. Ainsi, α est séparable sur K. Cela prouve la condition (1) de la définition d'être distingué.

Soit E séparable sur K et soit F une autre extension de K. On suppose que E et F soient sous-corps d'un corps commun. Chaque élément de E est séparable sur K, donc séparable sur F. Étant donné que EF est généré sur F par les éléments de E, il s'en suit que EF est séparable sur F par le théorème précédent. Cela montre la condition (2) de la définition et conclut la preuve puisque la condition (3) découle des deux premières. □

Soit E une extension finie de K, l'intersection d'extensions normales L de K (dans une clôture algébrique E^{alg}) contenant E est une extension normale de K contenant E. Si $\sigma_1, \ldots, \sigma_n$ sont les plongements distincts de E dans E^{alg}, alors l'extension

$$(\sigma_1 E)(\sigma_2 E) \cdots (\sigma_n E),$$

qui est le compositum de toutes les copies de E, est une extension normale de K car, pour n'importe quel plongement τ, on peut appliquer τ à chaque $\sigma_i E$. Alors, $(\tau\sigma_1, \ldots, \tau\sigma_n)$ est une permutation de $(\sigma_1, \ldots, \sigma_n)$ et donc τ associe K à lui-même. Toute extension normale de K contenant E doit contenir $\sigma_i E$ pour chaque i, et donc, la plus petite extension normale de K contenant E est précisément le compositum

$$(\sigma_1 E)(\sigma_2 E) \cdots (\sigma_n E).$$

Si E est séparable sur K, alors par le théorème précédent et induction, on peut conclure que la plus petite extension normale de K contenant E est également séparable sur K. Des résultats similaires existent dans le cadre d'une extension algébrique infinie, en prenant un compositum infini.

Sur base du théorème précédent, le compositum de toutes les extensions séparables d'un corps K dans une clôture algébrique K^{alg} est une extension séparable, elle sera notée K^{sep} et est appelée *clôture séparable* de K. Si E est une extension algébrique de K et σ un K-plongement de E dans K^{alg}, alors on appelle σE le *conjugué* de E dans K^{alg}. On peut alors dire que la plus petite extension normale de K contenant E est le compositum de tous les conjugués de E dans E^{alg}. Soit α un élément algébrique sur K, si $\sigma_1, \ldots, \sigma_n$ sont des K-plongements distincts de $K(\alpha)$ dans K^{alg}, on appelle $\sigma_1\alpha, \ldots, \sigma_n\alpha$ les *conjugués* de α dans K^{alg}. Ces éléments sont simplement les racines du polynôme minimal de α dans K. La plus petite extension normale de K contenant l'un de ces conjugués est

$$K(\sigma_1\alpha, \ldots, \sigma_n\alpha).$$

3 La catégorie des groupes topologiques

3.1 Définitions générales et exemples

Définition 3.1. Un ensemble G muni d'une structure de groupe et d'une topologie est qualifié de *groupe topologique* si les applications

$$G \times G \to G \colon (g,h) \mapsto gh \quad \text{et} \quad G \to G \colon g \mapsto g^{-1}$$

sont continues.

Soit a un élément d'un groupe topologique G, l'application de translation à gauche par a, définie par $a_{\mathrm{G}} \colon G \to G \colon g \mapsto ag$, est continue puisqu'il s'agit de la composée

$$\begin{array}{ccccc} G & \longrightarrow & G \times G & \longrightarrow & G \\ g & \longmapsto & (a,g) & \longmapsto & ag. \end{array}$$

Il s'agit plus précisément d'un homéomorphisme avec pour inverse $(a^{-1})_{\mathrm{G}}$. Similairement, $a_{\mathrm{D}} \colon G \to G \colon g \mapsto ga$ ainsi que $G \to G \colon g \mapsto g^{-1}$ sont des homéomorphismes.

Remarque 3.2. La topologie d'un groupe topologique G est uniforme, c'est-à-dire que pour tous a, $b \in G$, il existe un homéomorphisme $f \colon G \to G$ pour lequel

$$b = f(a).$$

En effet, il suffit de considérer la translation ba_{G}^{-1}.

Exemple 3.3. Le groupe additif $(\mathbf{R}, +)$ muni de la topologie usuelle sur $\mathbf{R}$ est un groupe topologique.

Exemple 3.4. Soit $\mathrm{M}_n(\mathbf{R})$ l'ensemble des matrices carrées de degré n à coefficients réels, il peut être identifié à $\mathbf{R}^n \times \mathbf{R}^n$ et muni de la topologie usuelle sur $\mathbf{R}^n \times \mathbf{R}^n$. Alors, pour l'addition des matrices, $\mathrm{M}_n(\mathbf{R})$ est un groupe topologique.

Exemple 3.5. Soit $\mathrm{GL}_n(\mathbf{R})$, le sous-ensemble de $\mathrm{M}_n(\mathbf{R})$ des matrices inversibles. L'application qui associe à une matrice son déterminant est une fonction continue sur $\mathrm{M}_n(\mathbf{R})$ – puisque le déterminant d'une matrice est un polynôme en ses coefficients – et $\mathrm{GL}_n(\mathbf{R})$ est l'image réciproque par cette application de l'ouvert $\mathbf{R} \smallsetminus \{0\}$. Ainsi, il s'agit d'un ouvert de $\mathrm{M}_n(\mathbf{R})$ et, muni de la topologie induite, c'est un groupe topologique. On l'appelle le groupe général linéaire de degré n.

Soient A et B des sous-ensembles d'un groupe topologique G. On désigne par A^{-1} l'ensemble de tous les éléments de la forme a^{-1} où $a \in A$. On notera AB pour désigner l'ensemble de tous éléments de la forme ab où $a \in A$ et $b \in B$. Nous ferons également l'abus de noter aB pour $\{a\}B$ et Ab pour $A\{b\}$.

Proposition 3.6. *Si A (ou B) est un sous-ensemble ouvert de G, alors AB est un sous-ensemble ouvert de G.*

Démonstration. Cela provient du fait que

$$AB = \bigcup_{b \in B} b_{\mathrm{D}}(A)$$

et que chaque $b_{\mathrm{D}}(A)$ est ouvert, puisque b_{D} est un homéomorphisme de G dans G. Si B est ouvert, le résultat découle de l'égalité

$$AB = \bigcup_{a \in A} a_{\mathrm{G}}(B)$$

et du fait que $a_{\mathrm{G}}(B)$ est ouvert. □

Proposition 3.7. *Si A est un ouvert de G, alors A^{-1} est un ouvert de G.*

Démonstration. En effet, A^{-1} est l'image réciproque de A par l'application continue $g \mapsto g^{-1}$. □

Définition 3.8. Une *base de voisinages* d'un point x d'un espace topologique X est un ensemble $\mathcal{V}$ de voisinages de x tel que tout voisinage V de x contienne un élément U de $\mathcal{V}$, *i.e.* $U \subseteq V$.

Soit G un groupe topologique et posons $\mathcal{V}_e$ une base de voisinages pour l'élément neutre e de G. Les cinq propriétés suivantes sont vérifiées.

Propriété 3.9. *Pour tous V_1, $V_2 \in \mathcal{V}_e$, il existe un $V \in \mathcal{V}_e$ pour lequel on a que $e \in V \subseteq V_1 \cap V_2$.*

Démonstration. On peut choisir $V_1 \cap V_2$ pour V qui reste un voisinage de e car les bases de voisinages sont des filtres. □

Propriété 3.10. *Pour tout $U \in \mathcal{V}_e$, il existe un $V \in \mathcal{V}_e$ pour lequel VV est contenu dans U.*

Démonstration. Étant donné que l'application

$$\phi\colon G \times G \to G\colon (x, y) \mapsto xy$$

est continue, on en déduit que $\phi^{-1}(U)$ est un ouvert de $G \times G$ contenant (e, e) et donc il existe un voisinage V de e tel que $V \times V$ est contenu dans $\phi^{-1}(U)$. On a bien que

$$VV \subseteq U.$$ □

Propriété 3.11. *Pour tout $U \in \mathcal{V}_e$, il existe un $V \in \mathcal{V}_e$ pour lequel V est contenu dans U^{-1}.*

Démonstration. Étant donné que l'application

$$\psi\colon G \to G\colon x \mapsto x^{-1}$$

est continue, on en déduit que $\psi^{-1}(U)$ est un ouvert de G contenant e et donc il existe un voisinage V de e tel que V est contenu dans $\psi^{-1}(U)$. On a bien que

$$V^{-1} \subseteq U.$$ □

Propriété 3.12. *Pour tout $U \in \mathcal{V}_e$ et pour tout $g \in G$, il existe un $V \in \mathcal{V}_e$ pour lequel V est contenu dans gUg^{-1}.*

Démonstration. En effet, si on considère $V = gUg^{-1}$, il s'agit d'un ouvert de G. Comme il contient $geg^{-1} = e$, c'est en particulier un élément de $\mathcal{V}_e$ et $V = gUg^{-1}$ est trivialement contenu dans gUg^{-1}. □

Propriété 3.13. *Pour tout $g \in G$, l'ensemble $\{gV \mid V \in \mathcal{V}_e\}$ est une base de voisinages pour g.*

Démonstration. En effet, si V un ouvert contenant e, $gV = g_{\mathrm{G}}(V)$ est un ouvert et il contient $ge = g$. De plus, si U un ouvert contenant g, alors $g^{-1}(U)$ est un ouvert contenant e et $gg^{-1}(U) = U \subseteq U$. □

Proposition 3.14. *Réciproquement, si G est un groupe et $\mathcal{V}$ est un ensemble non-vide de sous-ensembles de G satisfaisant les propriétés 1 à 4, alors il existe une unique topologie sur G pour laquelle la propriété 5 est respectée.*

Démonstration. Soit $\mathcal{V}$ une famille de sous-ensembles de G contenant l'élément neutre e et satisfaisant les cinq propriétés précédentes. On peut remarquer que la propriété 1 implique que e se trouve dans tout $V \in \mathcal{V}$. Posons $\mathcal{U}$ l'ensemble

$$\mathcal{U} := \{U \subseteq G \mid \forall\, g \in U,\ \exists\, V \in \mathcal{V} : gV \subseteq U\}.$$

On peut clairement se persuader que l'ensemble vide et G lui-même sont des éléments de $\mathcal{U}$ ainsi que l'union d'ensembles de $\mathcal{U}$ est dans $\mathcal{U}$. Soient U_1 et $U_2 \in \mathcal{U}$ et considérons $g \in U_1 \cap U_2$. Par définition, il existe V_1, $V_2 \in \mathcal{V}$ tels que gV_1 et $gV_2 \subseteq U$. En appliquant la propriété 2, on obtient un $V \in \mathcal{V}$ tel que $gV \subseteq U_1 \cap U_2$ – ce qui montre que $U_1 \cap U_2 \in \mathcal{U}$. Il s'en suit que les éléments de $\mathcal{U}$ sont les ouverts pour une topologie sur G. On peut voir également qu'il s'agit de l'unique topologie sur G pour laquelle la propriété 5 est vérifiée.

On utilise les propriétés 2 et 4 pour montrer que l'application $(x, y) \mapsto xy$ est continue. Remarquons que les ensembles $g_1V_1 \times g_2V_2$ forment une base de voisinages pour $(g_1, g_2) \in G \times G$. Ainsi, considérons un ouvert $U \subseteq G$ et une paire (g_1, g_2) telle que $g_1g_2 \in U$. Il nous faut trouver V_1 et $V_2 \in \mathcal{V}$ tels que $g_1V_1g_2V_2 \subseteq U$. Vu que U est ouvert, il existe un $V \in \mathcal{V}$ tel que $g_1g_2V \in U$. En appliquant la propriété 2, on obtient un V' pour lequel $V'V' \subseteq V$. Alors, $g_1g_2V'V' \subseteq U$. Cependant,

$$g_1g_2V'V' = g_1(g_2V'g_2^{-1})g_2V'$$

et il reste à appliquer la propriété 4 afin d'obtenir l'existence d'un $V_1 \in \mathcal{V}$ tel que $V_1 \subseteq g_2V'g_2^{-1}$.

Finalement, on utilise les propriétés 3 et 4 pour montrer que l'application $g \mapsto g^{-1}$ est continue. Étant donné un ouvert U de G et un $g \in G$ tel que $g^{-1} \in U$, on doit trouver un $V \in \mathcal{V}$ tel que $gV \subseteq U^{-1}$. Par définition, il existe un $V \in \mathcal{V}$ tel que $g^{-1}V \subseteq U$. Ainsi, $V^{-1}g \subseteq U^{-1}$ et on utilise la propriété 3 pour obtenir l'existence d'un $V' \in \mathcal{V}$ tel que $V'g \subseteq U^{-1}$ ainsi que la propriété 4 afin d'obtenir l'existence d'un $V'' \in \mathcal{V}$ tel que

$$gV'' \subseteq g(g^{-1}Vg) \subseteq U^{-1}.$$

□

Définition 3.15. Soient G et G' deux groupes topologiques et soit f une application de G dans G'. On dit que f est un *morphisme* du groupe topologique G dans le groupe topologique G' s'il s'agit d'un morphisme de groupes $G \to G'$ continue.

Définition 3.16. Soient G et G' deux groupes topologiques et soit f une application de G dans G'. On dit que f est un *isomorphisme* de groupes topologiques de G dans G' s'il s'agit d'un isomorphisme de groupes et d'un homéomorphisme d'espaces topologiques.

3.2 Les sous-groupes d'un groupe topologique

Soit G un groupe topologique et soit H un sous-groupe de G. La topologie de G induit une topologie sur H et les applications

$$H \times H \to H : (g, h) \mapsto gh \quad \text{et} \quad H \to H : g \mapsto g^{-1}$$

sont continues sur H pour cette topologie. Ainsi H est un groupe topologique. On dira que H est un sous-groupe topologique du groupe topologique G.

Proposition 3.17. *Soient G un groupe topologique et H un sous-groupe topologique de G, alors l'adhérence de H est aussi un sous-groupe topologique de G et si H est normal,* $\mathrm{adh}(H)$ *l'est aussi.*

Démonstration. Soient g et h deux éléments de $\mathrm{adh}(H)$ et soit U un voisinage de gh^{-1}. Comme l'application $(g, h) \mapsto gh^{-1}$ est continue sur $G \times G$ – puisqu'il s'agit d'une composée d'applications continues – il existe un voisinage V de g et un voisinage W de h tels que VW^{-1} est contenu dans U. Vu que g et h sont adhérents à H, il existe $h_1 \in V \cap H$ ainsi que $h_2 \in W \cap H$ et donc $h_1h_2^{-1} \in VW^{-1}$ et par conséquent à U. De plus, $h_1h_2^{-1}$ appartient à H puisqu'il s'agit d'un sous-groupe. Donc, tout voisinage de gh^{-1} rencontre H, donc gh^{-1} est dans $\mathrm{adh}(H)$. Cela permet d'affirmer que $\mathrm{adh}(H)$ est un sous-groupe topologique. De plus, lorsque H est normal dans G, on considère pour tout $g \in G$, l'application de conjugaison

$$c = g_{\mathrm{L}} \circ g_{\mathrm{D}}^{-1}.$$

Il s'agit d'un homéomorphisme de G, donc $\mathrm{adh}(c(H)) = c(\mathrm{adh}(H))$. Par conséquent,

$$g\,\mathrm{adh}(H)g^{-1} = c(\mathrm{adh}(H)) = \mathrm{adh}(c(H)) = \mathrm{adh}(gHg^{-1}) = \mathrm{adh}(H)$$

ou encore, $\mathrm{adh}(H)$ est normal dans G. □

Proposition 3.18. *Soient G un groupe topologique et H un sous-groupe topologique de G, si H est ouvert, alors il est fermé.*

Démonstration. Si H est ouvert, les classes à gauche suivant H le sont aussi car elles sont de la forme $g_{\mathrm{G}}(H) = (g_G^{-1})^{-1}(H)$, pour $g \in G$, qui est l'image réciproque d'un ouvert par une application continue. Comme H est le complémentaire de la réunion des classes à gauche gH, pour $g \in G$, distinctes de H, H est fermé. □

Exemple 3.19. On considère le groupe $\mathrm{GL}_n(\mathbf{R})$, alors l'ensemble $\mathrm{GL}_n^+(\mathbf{R})$ des matrices de G de déterminant positif est un sous-groupe de $\mathrm{GL}_n(\mathbf{R})$, ouvert – car il s'agit de l'image réciproque de $\mathbf{R}^+$ pour l'application déterminant. Il est donc aussi fermé par la proposition précédente.

Exemple 3.20. On considère le groupe $\mathrm{GL}_n(\mathbf{R})$, alors l'ensemble $\mathrm{SL}_n(\mathbf{R})$ des matrices de G de déterminant égal à 1 est un sous-groupe fermé de $\mathrm{GL}_n(\mathbf{R})$ – car il s'agit de l'image réciproque de $\{1\}$. On l'appelle groupe linéaire spécial de degré n.

3.3 La topologie de Krull sur les groupes de Galois

Définition 3.21. Une extension Ω d'un corps K est *galoisienne* si elle est normale et séparable.

Exemple 3.22. L'extension K^{sep} est galoisienne sur K.

Proposition 3.23. *Une extension Ω/K est galoisienne si et seulement s'il s'agit d'une union d'extensions finies galoisiennes.*

Démonstration. Il est clair que si Ω est une union d'extensions finies galoisiennes, alors Ω est une extension galoisienne puisque le compositum d'extensions normales et séparables est une extension normale et séparable. Pour la réciproque, supposons que Ω/K est galoisienne et considérons L un corps intermédiaire, qui est une extension finie galoisienne sur K. Vu que L/K est séparable, le théorème de l'élément primitif fournit l'existence d'un $\alpha \in \Omega$ tel que

$$L = K(\alpha).$$

Soit $P_{\alpha,K}$ le polynôme minimal de α sur K. Alors L se plonge dans le corps de décomposition de $P_{\alpha,K}$, qui est une extension finie galoisienne sur K. Ainsi Ω est l'union de toutes ces extensions vu que les $\alpha \in \Omega$ sont contenues dans certains de ces corps intermédiaires. □

Proposition 3.24. *Si Ω est une extension galoisienne d'un corps K, alors Ω est une extension galoisienne sur tout corps intermédiaire M.*

Démonstration. Soit $P(X)$ un polynôme irréductible de $M[X]$ ayant une racine α dans Ω. Le polynôme minimal $P_{\alpha,K}(X)$ de α sur K se décompose en facteurs linéaires dans $\Omega[X]$. Comme P divise $P_{\alpha,K}$ dans $M[X]$, il doit également être décomposé en facteurs linéaires dans $M[X]$. □

Proposition 3.25. *Soit Ω une extension galoisienne sur K et soit L un sous-corps de Ω contenant K. Chaque K-plongement de L dans Ω peut s'étendre en un K-isomorphisme $\Omega \xrightarrow{\sim} \Omega$.*

Démonstration. Étant donné que chaque K-plongement $L \hookrightarrow \Omega$ peut s'étendre en un K-plongement $\Omega \hookrightarrow \Omega$ par le lemme de Zorn, il suffit de vérifier la surjectivité. Soit $\alpha \in \Omega$ et posons σ le K-plongement $\Omega \hookrightarrow \Omega$. Considérons $P_{\alpha,K}$ le polynôme minimal de α sur K. Alors, Ω possède exactement $\deg(P_{\alpha,K})$ racines de $P_{\alpha,K}$ et donc $\sigma(\Omega)$ aussi. Donc α est dans $\sigma(\Omega)$ et cela montre la surjectivité de σ. □

Corollaire 3.26. *Soit $K \subseteq L \subseteq \Omega$ comme dans la proposition. Si L est stable sous $\mathrm{Aut}_K(\Omega)$, alors L est galoisienne sur K.*

Démonstration. Soit $P(X) \in K[X]$ un polynôme irréductible ayant une racine $\alpha \in L$. Puisque Ω/K est une extension galoisienne, $P(X)$ a $n = \deg(P)$ racines dans Ω, disons $\alpha_1, \ldots, \alpha_n$. Considérons les K-isomorphismes de $K(\alpha) \xrightarrow{\sim} K(\alpha_i) \subseteq \Omega$ qui envoient α sur α_i. Ceux-ci peuvent s'étendre en un K-isomorphisme $\Omega \xrightarrow{\sim} \Omega$. Comme L est stable sous $\mathrm{Aut}_K(\Omega)$, cela permet de conclure que α_i est un élément de L. □

Soit Ω une extension galoisienne sur K et posons $G := \mathrm{Aut}_K(\Omega)$. Pour tout sous-ensemble fini S de Ω, on définit

$$G(S) \triangleq \{\sigma \in G \mid \forall\, s \in S : \sigma(s) = s\}.$$

Lemme 3.27. *Soit S un sous-ensemble fini de Ω. Alors $G(S)$ est un sous-groupe de $\mathrm{Aut}_K(\Omega)$.*

Démonstration. Il est clair que $G(S) \subseteq \mathrm{Aut}_K(\Omega)$ et que Id_Ω est un élément de $G(S)$. Soient σ et $\tau \in G(S)$ et soit $s \in S$,

$$\sigma\tau^{-1}(s) = \sigma(s) = s$$

car τ est l'identité sur S. □

Proposition 3.28. *Il existe une structure de groupe topologique sur $\mathrm{Aut}_K(\Omega)$ pour laquelle les ensembles $G(S)$ forment une base de voisinages de Id_Ω. De plus, cette structure est unique. Pour cette topologie, les ensembles $G(S)$, où S est stable sous G, forment une base de voisinages de Id_Ω composé des sous-groupes normaux ouverts.*

Démonstration. On montre que l'ensemble des ensembles de la forme $G(S)$ satisfait les propriétés 1 à 4 de l'introduction aux groupes topologiques. Puisque clairement $G(S_1) \cap G(S_2) = G(S_1 \cup S_2)$ et que $\mathrm{Id}_\Omega \in G(S)$, quel que soit le S considéré, la propriété 1 est vérifiée. Les propriétés 2 et 3 découlent du fait que chaque $G(S)$ est un groupe. Soit S un sous-ensemble fini de Ω. Dans ce cas, $K(S)$ est une extension finie de K et il y a donc un nombre fini de K-plongements $K(S) \hookrightarrow \Omega$. Vu que $\sigma S = \tau S$ dès que $\sigma_{\restriction_{K(S)}} = \tau_{\restriction_{K(S)}}$, on a que

$$\overline{S} := \bigcup_{\sigma \in G} \sigma S$$

est fini. De plus, comme G est un groupe, $\sigma\overline{S} = \overline{S}$ et ce pour tout $\sigma \in G$. Il s'en suit que $G(\overline{S})$ est normal dans G. En effet, pour $\sigma \in G$ et $\tau \in G(\overline{S})$, $\sigma^{-1}(x) = \tau\sigma^{-1}(x) \in \overline{S}$. Par conséquent, $\sigma G(\overline{S})\sigma^{-1} = G(\overline{S}) \subseteq G(S)$ et cela permet de montrer la propriété 4 et de conclure sur la deuxième assertion. □

Définition 3.29. La topologie sur $\mathrm{Aut}_K(\Omega)$ définie dans la proposition est appelée la *topologie de Krull*.

Définition 3.30. Soit Ω une extension galoisienne d'un corps K. On désigne par $\mathrm{Gal}(\Omega/K)$ le groupe $\mathrm{Aut}_K(\Omega)$ muni de la topologie de Krull et on l'appelle le *groupe de Galois* de Ω/K.

Définition 3.31. Le groupe de Galois de K^{sep}/K est appelé *groupe de Galois absolu* de K.

Si S est un ensemble fini et stable sous $\mathrm{Aut}_K(\Omega)$, alors $K(S)$ est une extension finie de S stable sous $\mathrm{Aut}_K(\Omega)$ et est donc galoisienne sur K. Par conséquent,

$$\{\mathrm{Gal}(\Omega/L) \mid L \text{ fini et galoisien sur } K\}$$

est une base de voisinages de Id_Ω constituée de sous-groupes normaux ouverts.

Proposition 3.32. *Soit Ω une extension galoisienne sur K. Pour chaque corps intermédiaire L de degré fini et galoisien sur K, l'application*

$$\mathrm{Gal}(\Omega/K) \twoheadrightarrow \mathrm{Gal}(L/K) \colon \sigma \mapsto \sigma_{\restriction L}$$

est une surjection continue pour la topologie discrète sur $\mathrm{Gal}(L/K)$.

Démonstration. Soit $\sigma \in \mathrm{Gal}(L/K)$ et regardons le comme un K-plongement $L \hookrightarrow \Omega$. Il peut s'étendre en un K-isomorphisme $\Omega \xrightarrow{\sim} \Omega$ et cela montre que l'application est surjective. Pour tout sous-ensemble fini S de générateurs de L sur K, *i.e.* $L = K(S)$,

$$\mathrm{Gal}(\Omega/L) = G(S)$$

et cela montre que l'image réciproque de $1_{\mathrm{Gal}(L/K)}$ – qui est $G(S)$ – est un ouvert de $\mathrm{Aut}_K(\Omega)$. Le même argument est valable pour tous les autres éléments de $\mathrm{Gal}(L/K)$. □

Définition 3.33. Étant donné un point x d'un espace topologique X, l'union de toutes les parties connexes contenant x est connexe. C'est la plus grande (au sens de la relation d'inclusion) de toutes les parties connexes contenant x. On l'appelle *composante connexe* de x dans X.

Définition 3.34. Un espace topologique X est *totalement discontinu* si la composante connexe de tout point x de X est le singleton $\{x\}$.

Proposition 3.35. *Le groupe de Galois d'une extension Ω/K est de Hausdorff, compact et totalement discontinu.*

Démonstration. Montrons tout d'abord qu'il vérifie la propriété de Hausdorff. Considérons $\sigma \neq \tau$, dans ce cas, il existe un $a \in \Omega$ pour lequel $\sigma(a) \neq \tau(a)$. Soit S un ensemble comprenant a, alors $\sigma G(S)$ et $\tau G(S)$ sont disjoints car leurs éléments se comportent différemment sur a. Ainsi, σ et τ appartiennent à deux ouverts disjoints.

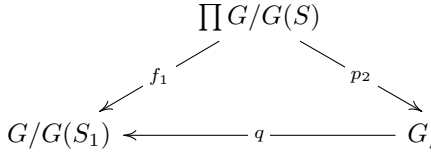
Comme remarqué précédemment, si S est fini et stable sous G, alors $G(S)$ est un sous-groupe normal de G et il est d'indice fini puisqu'il s'agit du noyau de

$$G \to \mathfrak{S}(S).$$

Vu que chaque sous-ensemble fini est contenu dans un ensemble fini et stable – la collection des racines des polynômes minimaux des éléments – alors un argument précédent permet d'affirmer que

$$f \colon G \hookrightarrow \prod_{\substack{S \text{ fini} \\ G\text{-stable}}} {}^{G}\!/_{G(S)}$$

est injective. Lorsqu'on munit $\prod G/G(S)$ de la topologie produit, la topologie induite sur G est celle pour laquelle les $G(S)$ forment une base de voisinage de e, c'est-à-dire la topologie de Krull. Cette topologie rend automatiquement f continue puisque les ouverts de G sont de la forme $f^{-1}(O)$ où O est un ouvert du produit. Par le théorème de Tikhonov, le produit $\prod G/G(S)$ est compact et donc il suffit de montrer que G est fermé dans ce produit. Soient $S_1 \subseteq S_2$, il y a deux applications continues f_1 et f_2 telles que $f_2 = q \circ p_2$ où



Soit $E(S_1, S_2)$ le sous-ensemble fermé de $\prod G/G(S)$ sur lequel f_1 et f_2 coïncident car il s'agit du noyau de $f_1 - f_2$ et est l'image réciproque du fermé $\{e\}$. Alors,

$$\bigcap_{S_1 \subseteq S_2} E(S_1, S_2) = f(G)$$

et est fermé. Ainsi G est compact.

Finalement, pour tout ensemble fini S stable sous $\mathrm{Gal}(\Omega/K)$, $G(S)$ est un sous-groupe ouvert et donc il est fermé. Vu que $\bigcap G(S) = \{\mathrm{Id}_\Omega\}$, cela montre que la composante connexe de Id_Ω est simplement $\{\mathrm{Id}_\Omega\}$. On déduit similairement le résultat pour les autres éléments de $\mathrm{Gal}(\Omega/K)$. □

Proposition 3.36. *Pour toute extension galoisienne Ω/K, $\Omega^{\mathrm{Gal}(\Omega/K)} = K$.*

Démonstration. Soit $\omega \in \Omega^{\mathrm{Gal}(\Omega/K)}$, alors ω repose dans une extension finie F de K. Les racines du polynôme minimal de ω sont les $\sigma(\alpha) = \alpha$ où σ est un élément de $\mathrm{Gal}(\Omega/K)$. Par conséquent, l'extension F est de degré 1 sur K, ce qui signifie que ω est simplement dans K. □

4 Initiation à la théorie des corps finis

On parcourt rapidement la théorie sur les corps finis dont nous aurons besoin pour les sections suivantes.

4.1 Résultats fondamentaux

Lemme 4.1. *Soit K un corps de caractéristique p, pour p premier. L'application $\sigma\colon x \mapsto x^p$ est un isomorphisme de K dans un de ses sous-corps K^p.*

Démonstration. Il est clair, par commutativité, que $\sigma(xy) = \sigma(x)\sigma(y)$. Le coefficient binomial $\binom{p}{k}$ est congru à 0 (mod p) lorsque $0 < k < p$. De cela, on déduit que

$$\sigma(x+y) = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k} = \sigma(x) + \sigma(y).$$

Ainsi, σ est un morphisme. De plus, σ est injectif puisque, par le petit théorème de Fermat, x^p est congrue à x (mod p). □

Théorème 4.2. *(1) La caractéristique d'un corps fini K est un nombre premier p. Si $n = [K : \mathbf{F}_p]$, le nombre d'éléments de K est $q = p^n$.*

(2) Soit p un nombre premier et posons, pour $n \geq 1$, $q = p^n$ une puissance de p. Soit Ω un corps algébriquement clos de caractéristique p. Il existe un unique sous-corps $\mathbf{F}_q$ de Ω qui comprend q éléments. Il s'agit de l'ensemble des racines du polynôme $X^q - X$.

(2) Tous les corps finis de $q = p^n$ éléments sont isomorphes à $\mathbf{F}_q$.

Démonstration. Pour (1), si K est un corps fini, il ne contient pas de copie de $\mathbf{Q}$. Donc sa caractéristique est un nombre premier p. Si n est le degré de l'extension $K/\mathbf{F}_p$, il est alors clair que K possède p^n éléments.

Si Ω est un corps algébriquement clos de caractéristique p, le lemme précédent montre que l'application $x \mapsto x^q$ où $q = p^n$ pour $n \geq 1$, est un automorphisme de Ω. En effet, l'application est le n-ième itéré de l'automorphisme $\sigma\colon x \mapsto x^p$ – remarquer que σ est surjectif vu que Ω est algébriquement clos. De plus, les éléments $x \in \Omega$ invariants sous $x \mapsto x^q$ forment un sous-corps $\mathbf{F}_q$ de Ω. La dérivée du polynôme $X^q - X$ est

$$qX^{q-1} - 1 = p\,p^{n-1}X^{q-1} - 1 = -1 \pmod{p}$$

et est non nulle. Cela implique, vu que Ω est algébriquement clos, que $X^q - X$ possède q racines distinctes, donc $\mathrm{card}(\mathbf{F}_q) = q$. Réciproquement, si K est un sous-corps de Ω ayant q éléments, le groupe multiplicatif $K^\times$ possède $q-1$ éléments. Alors, $x^{q-1} = 1$ si $x \in K^\times$ et $x^q = x$ si $x \in K$. Cela montre que K est contenu dans $\mathbf{F}_q$. Vu que $\mathrm{card}(K) = \mathrm{card}(\mathbf{F}_q)$, on a que $K = \mathbf{F}_q$, ce qui montre (2).

Pour (3), cela découle de (2) et du fait que tous les corps à p^n éléments peuvent être plongés dans Ω vu que Ω est algébriquement clos. □

4.2 Le groupe multiplicatif d'un corps fini

Soit p un nombre premier, soit n un naturel non nul et posons $q = p^n$.

Rappel 4.3. Si d est un naturel non nul, rappelons que $\varphi(d)$ désigne la fonction indicatrice d'Euler, *i.e.* le nombre d'entiers x, où $1 \leq x \leq d$, étant copremier à d (en d'autres termes, dont l'image dans $\mathbf{Z}/d\mathbf{Z}$ est un générateur de ce groupe). Il est clair que le nombre de générateurs d'un groupe cyclique d'ordre d est $\varphi(d)$.

Lemme 4.4. *Si n est un naturel non nul, alors $n = \sum_{d|n} \varphi(d)$.*

Démonstration. Si d divise n, soit G_d l'unique sous-groupe de $\mathbf{Z}/n\mathbf{Z}$ d'ordre d, et posons E_d l'ensemble des générateurs de G_d. Vu que chaque élément de $\mathbf{Z}/n\mathbf{Z}$ génère un des G_d, le groupe $\mathbf{Z}/n\mathbf{Z}$ est une union disjointe des E_d et on a

$$n = |\mathbf{Z}/n\mathbf{Z}| = \sum_{d|n} \mathrm{card}(E_d) = \sum_{d|n} \varphi(d). \qquad \square$$

Lemme 4.5. *Soit G un groupe fini d'ordre n. Supposons que, pour chaque diviseur d de n, l'ensemble des $x \in G$ tels que $x^d = 1$ ait au plus d éléments. Alors G est cyclique.*

Démonstration. Soit d un diviseur de n. S'il existe un $x \in G$ d'ordre d, le sous-groupe généré par x, $\langle x \rangle$, est cyclique d'ordre d. Au vu de l'hypothèse, tous les éléments $y \in G$ tel que $y^d = 1$ appartient à $\langle x \rangle$. En particulier, tous les éléments de G d'ordre d sont générateurs de $\langle x \rangle$ et sont au nombre de $\varphi(d)$. Ainsi, le nombre d'éléments de G d'ordre d est soit 0, soit $\varphi(d)$. Si c'était nul pour une valeur de d, alors $n = \sum_{d|n} \varphi(d)$ impliquerait que le nombre d'éléments dans G soit strictement inférieur à n et cela amènerait à une contradiction. En particulier, il existe un élément $x \in G$ d'ordre n et G coïncide avec le groupe cyclique $\langle x \rangle$. $\square$

Remarque 4.6. La preuve précédente montre plus généralement que tous les sous-groupes finis du groupe multiplicatif d'un corps sont cycliques.

Théorème 4.7. *Le groupe multiplicatif $\mathbf{F}_q^\times$ d'un corps fini $\mathbf{F}_q$ est cyclique d'ordre $q-1$.*

Démonstration. Ce théorème découle du précédent lemme en prenant pour G, $\mathbf{F}_q^\times$ et $n = q-1$. Il est en effet évident que l'équation $x^d = 1$, qui est de degré d, possède au plus d solutions dans $\mathbf{F}_q$. $\square$

4.3 Les automorphismes d'un corps fini

Soit $q = p^n$ et considérons $\mathbf{F}_q$ le corps fini à q éléments. On considère également l'*automorphisme de Frobenius* sur $\mathbf{F}_q$

$$\mathrm{Frob}_p \colon \mathbf{F}_q \xrightarrow{\sim} \mathbf{F}_q \colon x \mapsto x^p.$$

Alors Frob_p est un morphisme et son noyau est 0 vu que $\mathbf{F}_q$ est un corps. Ainsi, Frob_p est une injection. Comme $\mathbf{F}_q$ est fini, il s'en suit que Frob_p est également une surjection et cela fait donc de Frob_p un automorphisme. On peut remarquer qu'il fixe $\mathbf{F}_p$.

Théorème 4.8. *Le groupe des automorphismes de $\mathbf{F}_q$ est cyclique d'ordre n et généré par* Frob_p.

Démonstration. Soit G le groupe engendré par Frob_p. On remarque que Frob_p^n est l'identité sur $\mathbf{F}_q$ puisque, pour tout $x \in \mathbf{F}_q$,

$$\mathrm{Frob}_p^n(x) = x^{p^n} = x^q = x \pmod p.$$

Donc l'ordre de Frob_p divise n. Soit d l'ordre de Frob_p, ainsi $d \geq 1$. On a que $\mathrm{Frob}_p^d(x) = x^{p^d}$ pour tout $x \in \mathbf{F}_q$. Chaque élément de $\mathbf{F}_q$ est par conséquent une racine de l'équation

$$X^{p^d} - X = 0.$$

Cette équation possède au plus p^d racines. Ainsi $d \geq n$ et donc $d = n$. Il reste maintenant à montrer que G est le groupe des automorphismes de $\mathbf{F}_q$. Tout automorphisme de $\mathbf{F}_q$ doit fixer $\mathbf{F}_q$, donc il s'agit de $\mathbf{F}_q$-automorphismes. Par le premier théorème du chapitre sur la séparabilité, le nombre de tels automorphismes est inférieur (au sens large) à n. Donc $\mathbf{F}_q$ ne peut avoir d'autres automorphismes que ceux de G. $\square$

Théorème 4.9. *Soit n et m des naturels non nuls. Alors, dans toute clôture algébrique de $\mathbf{F}_p$, le sous-corps $\mathbf{F}_{p^n}$ est contenu dans $\mathbf{F}_{p^m}$ si et seulement si n divise m. Si tel est le cas, soit $q = p^n$ et posons $m = nd$, alors $\mathbf{F}_{p^m}$ est normal et séparable sur $\mathbf{F}_q$, et le groupe de $\mathbf{F}_q$-automorphismes de $\mathbf{F}_{p^m}$ est cyclique d'ordre d, généré par* Frob_p^n.

Démonstration. On sait que $\mathbf{F}_{p^n}$ est l'ensemble des éléments qui satisfont $x^{p^n} = x$. On a également que $x^{p^{2n}} = x^{p^n} = x$. Ainsi, lorsque n divise m, il existe un d tel que $m = dn$. En itérant, $x^{p^{dn}} = x^{p^{(d-1)n}} = \cdots = x^{p^n} = x$ et donc x est dans $\mathbf{F}_{p^m}$. Réciproquement, lorsque $\mathbf{F}_{p^n}$ est contenu dans $\mathbf{F}_{p^m}$, alors $\mathbf{F}_{p^m}$ est un espace vectoriel sur $\mathbf{F}_{p^n}$. Disons que la dimension de $\mathbf{F}_{p^m}$ sur $\mathbf{F}_{p^n}$ est d. Alors, on a $|\mathbf{F}_{p^m}| = |\mathbf{F}_{p^n}|^d$ et donc $p^m = p^{n^d} = p^{nd}$ et ainsi n divise m.

Vu qu'un corps fini est parfait, toutes ses extensions algébriques sont séparables. Également, $\mathbf{F}_{p^m}$ est le corps de décomposition du polynôme $X^{p^m} - X$, ce qui fait de $\mathbf{F}_{p^m}$ une extension normale et séparable de $\mathbf{F}_q$.

Finalement, on sait que les automorphismes de $\mathbf{F}_{p^m}$ forment un groupe cyclique, généré par Frob_p et d'ordre m. Déterminons ceux qui fixent $\mathbf{F}_{p^n}$. Soit x un élément de $\mathbf{F}_{p^n}$, alors $\mathrm{Frob}_p^k(x) = x$ si et seulement si $x^{p^k} = x$ ou encore, par un argument précédent, $k = nl$ pour $l \geq 1$. Ainsi, il s'agit des éléments de $\langle \mathrm{Frob}_p^n \rangle$ et ce groupe est d'ordre d car

$$\mathrm{ord}(\mathrm{Frob}_p^n) = \frac{\mathrm{ord}(\mathrm{Frob}_p)}{\mathrm{pgcd}(\mathrm{ord}(\mathrm{Frob}_p), n)} = \frac{nd}{\mathrm{pgcd}(nd, n)} = \frac{nd}{n} = d. \qquad \square$$

5 Groupes de Galois issus de limites projectives

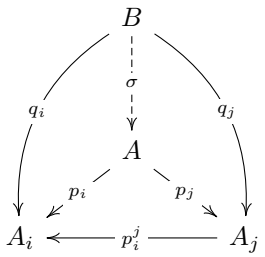
5.1 La notion de limite projective

Définition 5.1. Un ordre partiel $\leq$ sur un ensemble I est *dirigé*, et la paire $(I, \leq)$ est un *ensemble dirigé*, si pour tous i, $j \in I$, il existe un $k \in I$ tel que i, $j \leq k$.

Définition 5.2. Soit $(I, \leq)$ un ensemble dirigé, et soit C une catégorie.

(a) Un *système projectif* dans C indexé par $(I, \leq)$ est une famille $(A_i)_{i\in I}$ d'objets de C ainsi qu'une famille $(p_i^j \colon A_j \to A_i)_{i\leq j}$ de morphismes tels que $p_i^i = \mathrm{Id}_{A_i}$ et $p_i^j \circ p_j^k = p_i^k$ pour tous $i \leq j \leq k$.

(b) Un objet A de C ainsi qu'une famille $(p_j \colon A \to A_j)_{j\in I}$ de morphismes satisfaisant $p_i^j \circ p_j = p_i$ pour tous $i \leq j$ est une *limite projective* du système (a) si pour tous autre objet B et famille $(q_j \colon B \to A_j)$ de morphismes tels que $p_i^j \circ q_j = q_i$ pour tous $i \leq j$, il existe un unique morphisme $\sigma \colon B \to A$ tel que $p_j \circ \sigma = q_j$ pour tout j (propriété universelle).



Clairement, lorsqu'elle existe, la limite projective est unique à isomorphisme près. On la désigne par $\varprojlim(A_i, p_i^j)$, ou plus simplement $\varprojlim A_i$. On appelle les applications $p_j \colon A \to A_j$ les projections.

Exemple 5.3. Soit $(G_i, p_i^j \colon G_j \to G_i)$ un système projectif de groupes. On pose

$$G := \left\{ (g_i) \in \prod G_i \;\middle|\; \forall\, i \leq j : p_i^j(g_j) = g_i \right\}$$

et soient $p_i \colon G \to G_i$ les applications de projection. Alors $p_i^j \circ p_j = p_i$ nous ramène à l'équation $p_i^j(g_j) = g_i$. Soit (H, q_i) une deuxième famille telle que $p_i^j \circ q_j = q_i$. L'image du morphisme

$$H \to \prod G_i \colon h \mapsto (q_i(h))$$

est contenue dans G et il s'agit de l'unique morphisme $H \to G$ transportant les q_i sur les p_i. Ainsi, $(G, p_i) = \varprojlim(G_i, p_i^j)$.

Exemple 5.4. Soit $(G_i, p_i^j \colon G_j \to G_i)$ un système projectif de groupes topologiques et de morphismes continus. Muni de la topologie produit, $\prod G_i$ est un groupe topologique. On pose

$$G := \left\{ (g_i) \in \prod G_i \;\middle|\; \forall\, i \leq j : p_i^j(g_j) = g_i \right\}$$

qui est un sous-groupe topologique pour la topologie induite. Les applications de projections p_i sont continues. Soit (H, q_i) une deuxième famille telle que $p_i^j \circ q_j = q_i$. Le morphisme

$$H \to \prod G_i \colon h \mapsto (q_i(h))$$

est continu car il est composé des applications de projection qui sont continues. Ainsi, $H \to G$ est continue et cela montre que $(G, p_i) = \varprojlim(G_i, p_i^j)$.

Lemme 5.5. *Soit E un ensemble dans un espace topologique X. Si pour tout $x \notin E$, il existe un voisinage de x, O_x, tel que E et O_x sont disjoints, alors E est fermé dans X.*

Démonstration. Si ce n'était pas le cas, il existerait un $x \in \mathrm{adh}(E)$ tel que $x \notin E$. Puisque $x \notin E$, l'hypothèse fournit un O_x pour lequel $E \cap O_x = \varnothing$. Or cela vient directement contredire le fait que $x \in \mathrm{adh}(E)$. □

Exemple 5.6. Soit $(G_i, p_i^j : G_j \to G_i)$ un système projectif de groupes finis et regardons-le comme un système projectif de groupes topologiques en munissant chaque G_i de la topologie discrète. Un groupe topologique G résultant d'une limite projective d'un tel système est qualifié de **profini**. Si $(x_i) \notin G$, disons que $p_{i_0}^{j_0}(x_{j_0}) \neq x_{i_0}$, alors

$$G \cap \{(g_j) \mid g_{j_0} = x_{j_0},\ g_{i_0} = x_{i_0}\} = \varnothing.$$

Comme le deuxième ensemble est un voisinage de (x_i), cela montre que G est fermé dans $\prod G_i$ en utilisant le lemme précédent. Par le théorème de Tikhonov, $\prod G_i$ est compact et donc G est également compact. La projection $p_i : G \to G_i$ est continue et son noyau U_i est un sous-groupe ouvert d'indice fini dans G (et donc aussi fermé). Vu que $\bigcap U_i = \{e\}$, le composante connexe de G comprenant e est juste $\{e\}$. Par homogénéité, on peut généraliser cela à chaque point de G. Ainsi, G est totalement discontinu.

Remarque 5.7. On a montré qu'un groupe profini est compact et totalement discontinu.

Soit Ω une extension galoisienne sur K. Le compositum de deux extensions finies galoisiennes reste une extension finie galoisienne et donc les sous-extensions finies galoisiennes de Ω forment un ensemble dirigé, que nous noterons Int. Pour chaque E dans Int, on a un groupe fini $\mathrm{Gal}(E, K)$ et pour chaque $E \subseteq E'$, on a le morphisme de restriction

$$p_E^{E'} :\ \mathrm{Gal}(E'/K) \to \mathrm{Gal}(E/K).$$

Grâce à cela, on obtient un système projectif $(\mathrm{Gal}(E/K), p_E^{E'})$ de groupes finis indicé par Int. Pour chaque E, il existe un morphisme de restriction

$$p_E :\ \mathrm{Gal}(\Omega/K) \to \mathrm{Gal}(E/K)$$

et, par la propriété sur les limites projectives, ces applications définissent un morphisme

$$\mathrm{Gal}(\Omega/K) \to \varprojlim \mathrm{Gal}(E/K).$$

Cette application est un isomorphisme de groupes topologiques. Nous allons le prouver après.

Remarque 5.8. Il s'agit d'une reformulation des arguments de la preuve du théorème sur la compacité et le caractère totalement discontinu du groupe de Galois.

5.2 Caractérisation des groupes de Galois infinis

Lemme 5.9. *Soit $(X_i)_{i \in I}$ une famille d'espaces topologiques et considérons leur produit $\prod_{i \in I} X_i$. Soit B un espace topologique. Une application $f : B \to \prod_{i \in I} X_i$ est continue si et seulement si $h_i = p_i \circ f : B \to X_i$ est continue pour tout $i \in I$.*

Démonstration. On sait par définition du produit que chaque p_i est continue. La composition de deux fonctions continues est alors continue. Réciproquement, supposons que h_i soit continue pour tout $i \in I$. Soit U un sous-ensemble ouvert de $\prod_{i \in I} X_i$. Par définition du produit topologique,

$$U = \bigcup_{l \in L} \left(\left(\prod_{i \notin J_l} X_i \right) \times \left(\prod_{j \in J_l} U_{lj} \right) \right)$$

pour des ensembles d'indices finis $J_l \subseteq I$ et où $U_{lj} \subseteq X_j$ pour tout $j \in J_l$ et pour tout $l \in L$. Ainsi, nous obtenons que

$$f^{-1}(U) = \bigcup_{l \in L} \left(\bigcap_{j \in J_l} h_j^{-1}(U_{lj}) \right)$$

qui est un ouvert de B puisque chaque h_j est continue et vu que J_l est fini pour tout $l \in L$. Par conséquent, f est continue. □

Proposition 5.10. *Soit Ω une extension galoisienne de K. On désigne par Int les sous-extensions finies galoisiennes de Ω. Alors*

$$\mathrm{Gal}(\Omega/K) \simeq \varprojlim_{F\in Int} \mathrm{Gal}(F/K)$$

par l'isomorphisme de groupes topologiques $\sigma \mapsto (\sigma_{\restriction E})$.

Démonstration. On a que $p_E^{E'}(\sigma_{\restriction E'}) = \sigma_{\restriction E}$ par définition des $p_E^{E'}$. C'est un morphisme de groupe puisque

$$((\sigma\tau)_{\restriction E}) = (\sigma_{\restriction E}\tau_{\restriction E}) = (\sigma_{\restriction E})(\tau_{\restriction E})$$

pour n'importe quels σ, $\tau \in \mathrm{Gal}(\Omega/K)$. De plus, rappelons que le noyau est l'ensemble

$$\big\{\sigma \in \mathrm{Gal}(\Omega/K) \;\big|\; \sigma_{\restriction E} = \mathrm{Id}_E\big\}.$$

Vu que Ω est l'union de ses sous-extensions, *i.e.* $\Omega = \bigcup E$, le noyau est restreint à Id_Ω et donc l'application est injective. Finalement supposons que (σ_E) soit un élément de $\varprojlim \mathrm{Gal}(E/K)$ où $\sigma_E \in \mathrm{Gal}(E/K)$. On définit $\sigma\colon \Omega \to \Omega$ par $\sigma(x) = \sigma_E(x)$ pour $x \in E$. Comme $\Omega = \bigcup E$, σ est défini sur tout Ω. Il faut tout de même vérifier que cette application est bien définie. Soit $x \in E \cap E'$, il faut vérifier que $\sigma_E(x) = \sigma_{E'}(x)$. On sait que $E \cap E'$ est une extension finie galoisienne de K car une intersection d'extensions normales est normale. Étant donné que (σ_E) est un élément de $\varprojlim \mathrm{Gal}(E/K)$,

$$p^E_{E\cap E'}(\sigma_E) = \sigma_{E\cap E'} \quad \text{et} \quad p^{E'}_{E\cap E'}(\sigma_{E'}) = \sigma_{E\cap E'}.$$

Donc, σ_E et $\sigma_{E'}$ coïncident sur $E\cap E'$, qui contient x, donc σ est bien défini. Par construction, $\sigma_{\restriction E} = \sigma_E$ et donc notre application est surjective.

Finalement, cette application, que nous allons noter f, est continue et ouverte. Pour montrer que f est continue, on utilise le lemme précédent et on montre que, pour tout $E \in \mathrm{Int}$, $h_E = p_E \circ f\colon G \to \mathrm{Gal}(E, K) =: G_E$ est continue. Soit V un ouvert de G_E et soit $W = h_E^{-1}(V)$. Pour montrer que W est ouvert, on considère $\sigma \in W$, alors σG_E est un voisinage de σ contenu dans W puisque, si $\sigma' \in \sigma G_E$,

$$\sigma'_{\restriction E} = (\sigma\phi)_{\restriction E} = \sigma_{\restriction E}\phi_{\restriction E} \in V$$

où $\phi \in \mathrm{Gal}(E/K)$. Ainsi, h_E est continue, et ce, pour tout $E \in \mathrm{Int}$. Cela fait de f une application continue. Pour voir que f est ouverte, on considère U_E qu'on pose comme $\mathrm{Gal}(\Omega/E)$ pour $E \in \mathrm{Int}$, un corps intermédiaire. On peut remarquer que $\sigma \in U_E$ si et seulement si $\sigma_{\restriction E} = \mathrm{Id}_E$. Comme f est une bijection, on a que

$$f(U_E) = \varprojlim G_E \cap \big(\big(\textstyle\prod_{F\neq E} G_F\big) \times \{\mathrm{Id}_E\}\big) =: \varprojlim G_E \cap X.$$

Comme X est ouvert dans $\prod_{E\in\mathrm{Int}} G_E$, on obtient que $f(U_E)$ est ouvert dans $\varprojlim G_E$. Par conséquent, on peut conclure que f est une application ouverte et il s'en suit que f est un isomorphisme de groupes topologiques. □

Définition 5.11. Soit $(I, \leq)$ un ensemble dirigé. On dit que $J \subseteq I$ est un sous-ensemble *cofinal* de I si pour tout $i \in I$, il existe un $j \in J$ pour lequel $i \leq j$.

Proposition 5.12. *Soient I un ensemble dirigé et J un sous-ensemble cofinal de I. Alors les systèmes projectifs $(A_i, p_i^j)_{i\in I}$ et $(A_i, p_i^j)_{i\in J}$ ont des limites projectives isomorphes.*

Démonstration. Soit A_I (resp. A_J) la limite projective issue du système $(A_i, p_i^j)_{i\in I}$ (resp. $(A_i, p_i^j)_{i\in J}$). On notera, pour tout $i \in I$, $p_i\colon A_I \to A_i$ et, pour tout $j \in J$, $q_j\colon A_J \to A_j$ les projections associées. Une première utilisation de la propriété universelle fournit l'existence d'un unique morphisme

$$\sigma\colon A_I \to A_J$$

vérifiant pour tout $j \in J$ que $q_j \circ \sigma = p_j$. Étant donné que J est cofinal dans I, pour tout $i \in I$, il existe un $j \in J$ pour lequel $i \leq j$. Par conséquent, pour tout $i \in I$, on peut associer une application de la forme $p_i^j \circ q_j$. Cette application ne dépend pas du choix du $j \geq i$. En effet, comme J est dirigé, pour tout $k \geq i$, il existe un $n \in J$ pour lequel $j, k \leq n$ et donc

$$p_i^k \circ q_k = p_i^k \circ p_k^n \circ q_n = p_i^n \circ q_n = p_i^j \circ p_j^n \circ q_n = p_i^j \circ q_j.$$

On va considérer comme application réciproque $r_i \colon A_J \to A_i$ définie quel que soit $i \in I$ par $r_i = p_i^j \circ q_j$ pour un $j \geq i$. En utilisant une seconde fois la propriété universelle, on obtient un unique morphisme

$$\tau \colon A_J \to A_I$$

tel que $p_i \circ \tau = r_i$ pour tout $i \in I$. Au vu de l'unicité, ces deux applications sont inverses l'une de l'autre et on obtient ainsi un isomorphisme. □

5.3 Le groupe de Galois absolu de $\mathbf{F}_p$

Nous allons utiliser les résultats précédents afin de déterminer le groupe de Galois absolu d'un corps fini à p éléments. Soit p un nombre premier et considérons $\mathbf{F}_p$ le corps fini à p éléments. Soit Ω une clôture algébrique de $\mathbf{F}_p$, donc $\Omega/\mathbf{F}_p$ est une extension galoisienne vu que $\mathbf{F}_p$ est un corps parfait. On sait que les extensions finies galoisiennes $\mathbf{F}_p \subseteq E \subseteq \Omega$ sont exactement les corps finis $\mathbf{F}_{p^n}$, pour n un naturel non nul, et $\mathbf{F}_{p^m}$ est contenu dans $\mathbf{F}_{p^n}$ si et seulement si m divise n. On en déduit un ordre partiel

$$\mathbf{F}_p \subseteq \mathbf{F}_{p^n} \subseteq \cdots \subseteq \Omega.$$

De plus, nous savons précisément ce que sont ces groupes de Galois finis. Le groupe de Galois $\mathrm{Gal}(\mathbf{F}_{p^n}/\mathbf{F}_p)$ est cyclique d'ordre n, engendré par l'automorphisme de Frobenius $x \mapsto x^p$. Pour m un diviseur de n, l'application de restriction

$$\mathrm{Gal}(\mathbf{F}_{p^n}/\mathbf{F}_p) \to \mathrm{Gal}(\mathbf{F}_{p^m}/\mathbf{F}_p)$$

envoie le Frobenius sur lui-même, donc il s'agit juste de l'application

$$\phi_m^n \colon \mathbf{Z}/n\mathbf{Z} \to \mathbf{Z}/m\mathbf{Z} \colon x \mapsto x \bmod m.$$

La limite projective de ce système est notée $\widehat{\mathbf{Z}}$ et porte le nom de complété profini des entiers. Plus précisément,

$$\widehat{\mathbf{Z}} = \left\{ (a_n)_{n\geq 1} \in \textstyle\prod_{n\geq 1} \mathbf{Z}/n\mathbf{Z} \;\middle|\; \forall\, m \mid n : \phi_m^n(a_n) = a_m \right\}.$$

On peut également remarquer que la condition $\phi_m^n(a_n) = a_m$ est équivalente à $a_n \bmod m = a_m$ ou encore à a_n est congrue à $a_m \pmod m$. Il y a une copie de $\mathbf{Z}$ dans $\widehat{\mathbf{Z}}$, en considérant les suites constantes $a \mapsto (a \bmod n)$. Il y a également d'autres éléments dans $\widehat{\mathbf{Z}}$. Soit p un nombre premier, et posons $a_n = 1$ si n est une puissance de p et $a_n = 0$ sinon. Pour $p = 2$, on a

$$(a_n)_{n\geq 1} = (0, 1, 0, 1, 0, 0, 0, 1, 0, \ldots).$$

Vu que $1 = 0$ dans $\mathbf{Z}/1\mathbf{Z}$, cela n'a pas d'importance de comment on écrit a_1.

Proposition 5.13. *Soit p un nombre premier et considérons $q = p^n$ où $n \geq 1$. Le groupe de Galois absolu $\mathrm{Gal}(\mathbf{F}_q^{\mathrm{sep}}/\mathbf{F}_q)$ de $\mathbf{F}_q$ est isomorphe en tant que groupe topologique à $\widehat{\mathbf{Z}}$.*

Démonstration. On sait que pour tout $m \geq 1$, il existe une unique extension de $\mathbf{F}_q$ de degré m, notée $\mathbf{F}_{q^m}$. On sait également que $\mathrm{Gal}(\mathbf{F}_{q^m}/\mathbf{F}_q)$ est cyclique d'ordre m, donc

$$\mathrm{Gal}(\mathbf{F}_{q^m}/\mathbf{F}_q) \simeq \mathbf{Z}/m\mathbf{Z}. \tag{1}$$

Si on note Int l'ensemble des corps intermédiaires à $\mathbf{F}_q^{\text{sep}}$ et $\mathbf{F}_q$ de degré fini sur $\mathbf{F}_q$, alors cet ensemble est uniquement constitué des $\mathbf{F}_{q^m}$ pour tout $m \geq 1$. Par un théorème précédent,

$$\text{Gal}(\mathbf{F}_q^{\text{sep}}/\mathbf{F}_q) \simeq \varprojlim_{\mathbf{F}_{q^m} \in \text{Int}} \text{Gal}(\mathbf{F}_{q^m}/\mathbf{F}_q) \tag{2}$$

en tant que groupes topologiques. D'un autre coté, $\widehat{\mathbf{Z}}$ est la limite projective du système $(\mathbf{Z}/m\mathbf{Z}, \phi_k^m)$ où $\phi_k^m \colon \mathbf{Z}/m\mathbf{Z} \to \mathbf{Z}/k\mathbf{Z} \colon x \mapsto x \bmod k$ lorsque k divise m. Ainsi, au vu des isomorphismes (1) et (2), on déduit l'isomorphisme

$$\text{Gal}(\mathbf{F}_q^{\text{sep}}/\mathbf{F}_q) \simeq \widehat{\mathbf{Z}}. \qquad \square$$

5.4 Le groupe de Galois d'extensions cyclotomiques infinies

Soit p un nombre premier et posons Ω le sous-corps de $\mathbf{C}$ généré sur $\mathbf{Q}$ par les racines p^n-ième de l'unité, pour tout naturel n. Nous allons montrer que l'extension $\Omega/\mathbf{Q}$ est galoisienne et dont le groupe de Galois est $\mathbf{Z}_p^\times$, le groupe des inversibles des entiers p-adiques, c'est-à-dire la limite projective des quotients $(\mathbf{Z}/p^n\mathbf{Z})^\times$.

Étant donné que Ω est le corps de décomposition d'une famille de polynômes et que $\mathbf{Q}$ est un corps parfait, l'extension $\Omega/\mathbf{Q}$ est galoisienne. De même, chaque extension $\mathbf{Q}(\zeta_n)/\mathbf{Q}$ l'est car $\mathbf{Q}(\zeta_n)$ est le corps de décomposition de $X^n - 1$.

Théorème 5.14. *Soit n un naturel non nul, l'application*

$$\begin{array}{ccc} \text{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q}) & \xrightarrow{\sim} & (\mathbf{Z}/n\mathbf{Z})^\times \\ \sigma & \longmapsto & a_\sigma \bmod n, \end{array}$$

où $\sigma(\zeta_n) = \zeta_n^{a_\sigma}$, est un isomorphisme de groupes.

Démonstration. Soient σ et τ deux éléments de $\text{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q})$. Alors,

$$\zeta_n^{a_{\sigma\tau}} = (\sigma\tau)(\zeta_n) = \sigma(\zeta_n^{a_\tau}) = \sigma(\zeta_n)^{a_\tau} = \zeta_n^{a_\sigma a_\tau}$$

et, vu que ζ_n est d'ordre n, on en déduit que $a_{\sigma\tau} \equiv a_\sigma a_\tau \pmod n$. Par conséquent, il s'agit bien d'un morphisme. En ce qui concerne l'injectivité, soit σ un élément du noyau, alors $a_\sigma \equiv 1 \pmod n$ et donc $\sigma \colon \zeta_n \mapsto \zeta_n$. De plus, σ fixe $\mathbf{Q}$ donc σ est l'identité sur $\mathbf{Q}(\zeta_n)$, c'est-à-dire que σ est le neutre de $\text{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q})$. On peut finalement conclure car

$$|\,\text{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q})| = [\mathbf{Q}(\zeta_n) : \mathbf{Q}] = \deg(\Phi_n) = \varphi(n) = |(\mathbf{Z}/n\mathbf{Z})^\times|.$$

Les détails sont prouvés dans l'annexe sur les polynômes cyclotomiques. $\square$

Contrairement à ce que nous avons déjà pu rencontrer, il n'est plus possible d'affirmer que chaque extension finie et intermédiaire à Ω et $\mathbf{Q}$ est d'une forme précise – comme par exemple $\mathbf{Q}(\zeta_{p^n})$ pour $n \in \mathbf{N}$. Cependant, on peut remarquer que chaque telle extension est nécessairement incluse à un certain $\mathbf{Q}(\zeta_{p^n})$. En effet, si F est une extension finie comprise entre Ω et $\mathbf{Q}$, alors il existe un élément primitif $\alpha \in F$ pour lequel $F = \mathbf{Q}(\alpha)$. Cet élément primitif est en particulier un élément de $\Omega = \bigcup_{n\in\mathbf{N}} \mathbf{Q}(\zeta_{p^n})$. Il existe par conséquent un naturel n pour lequel $\alpha \in \mathbf{Q}(\zeta_{p^n})$ et donc

$$F = \mathbf{Q}(\alpha) \subseteq \mathbf{Q}(\zeta_{p^n}).$$

L'ensemble formé des extensions $\mathbf{Q}(\zeta_{p^n})$ est un sous-ensemble cofinal de l'ensemble des extensions finies comprises entre Ω et $\mathbf{Q}$. Étant donné que la limite projective sur un ensemble dirigé, qu'on note ici Int, est isomorphe à la limite projective sur un sous-ensemble cofinal, on déduit que

$$\text{Gal}(\Omega/\mathbf{Q}) \simeq \varprojlim_{F \in \text{Int}} \text{Gal}(F/\mathbf{Q}) \simeq \varprojlim_{n\in\mathbf{N}} \text{Gal}(\mathbf{Q}(\zeta_{p^n})/\mathbf{Q}).$$

Maintenant, en utilisant le théorème précédent et notre dernière constatation, on obtient que

$$\mathrm{Gal}(\Omega/\mathbf{Q}) \simeq \varprojlim_{n\in\mathbf{N}} (\mathbf{Z}/p^n\mathbf{Z})^\times = \mathbf{Z}_p^\times.$$

Nous allons raisonner similairement afin de déterminer le groupe de Galois du sous-corps de $\mathbf{C}$ engendré sur $\mathbf{Q}$ par les racines n-ième de l'unité, pour tout naturel n non nul. Notons ce corps Ω. Cela a bien un sens puisque $\Omega/\mathbf{Q}$ et chaque $\mathbf{Q}(\zeta_n)/\mathbf{Q}$ sont des extensions galoisiennes.

Comme précédemment, on peut montrer que les extensions $\mathbf{Q}(\zeta_n)$, où $n \geq 1$, forment un sous-ensemble cofinal des extensions finies intermédiaires à Ω et $\mathbf{Q}$. En effet, soit F une extension finie comprise entre Ω et $\mathbf{Q}$, il existe un élément primitif $\alpha \in F$ pour lequel $F = \mathbf{Q}(\alpha)$. En particulier, α est dans $\Omega = \bigcup_{n\geq 1} \mathbf{Q}(\zeta_n)$ et ainsi, il existe un $n \geq 1$ tel que $\alpha \in \mathbf{Q}(\zeta_n)$. Par conséquent,

$$F = \mathbf{Q}(\alpha) \subseteq \mathbf{Q}(\zeta_n).$$

Étant donné que la limite projective sur un ensemble dirigé, qu'on note ici Int, est isomorphe à la limite projective sur un sous-ensemble cofinal, on en déduit que

$$\mathrm{Gal}(\Omega/\mathbf{Q}) \simeq \varprojlim_{F\in\mathrm{Int}} \mathrm{Gal}(F/\mathbf{Q}) \simeq \varprojlim_{n\geq 1} \mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q}).$$

En utilisant des résultats précédents ainsi que notre dernière constatation, on obtient que

$$\mathrm{Gal}(\Omega/\mathbf{Q}) \simeq \varprojlim_{n\geq 1} (\mathbf{Z}/n\mathbf{Z})^\times = \widehat{\mathbf{Z}}^\times.$$

Proposition 5.15. *Soit K un corps dont toutes les extensions finies sont cycliques et ayant une seule extension de degré n, pour tout naturel n. Alors $\mathrm{Gal}(K^{\mathrm{alg}}/K)$ est la limite projective des $\mathbf{Z}/n\mathbf{Z}$. De plus, cette limite est isomorphe au produit des entiers p-adiques.*

Démonstration. Soit Int l'ensemble des extensions intermédiaires à K^{alg} et K de degré fini. Par un théorème précédent et vu que chaque extension finie est cyclique et est unique pour son degré, on a que

$$\mathrm{Gal}(K^{\mathrm{alg}}/K) \simeq \varprojlim_{F\in\mathrm{Int}} \mathrm{Gal}(F/K) \simeq \varprojlim_{n\geq 1} \mathbf{Z}/n\mathbf{Z} = \widehat{\mathbf{Z}}.$$

En utilisant le théorème des restes chinois et en remarquant qu'il n'y a aucune relation de compatibilité entre p^n et $\mathfrak{q}^m$ si $p \neq \mathfrak{q} \in \mathfrak{P}$ pour n, m des naturels non nuls, on obtient que

$$\widehat{\mathbf{Z}} = \varprojlim_{n\geq 1} \mathbf{Z}/n\mathbf{Z} \simeq \prod_{p\in\mathfrak{P}} \varprojlim_{n\geq 1} \mathbf{Z}/p^n\mathbf{Z} = \prod_{p\in\mathfrak{P}} \mathbf{Z}_p. \qquad \square$$

En particulier $\widehat{\mathbf{Z}}$ n'est pas intègre, il ne peut donc pas être isomorphe à $\mathbf{Z}$. On peut cependant montrer que $\mathbf{Z}_p$ est intègre. En effet, soit $a = (a_n) \in \mathbf{Z}_p$ non nul, alors il existe un plus petit naturel N tel que $a_N \not\equiv 0 \pmod{p^N}$ et donc, vu que N est minimal, $p^{N-1} < a_N < p^N$. On peut remarquer par les relations de compatibilité des limites projectives que cela implique que pour tout $n \geq N$, $a_n \not\equiv 0 \pmod{p^n}$. De plus, par le choix des applications,

$$a_n = a_N + k_1 p^{N+1} + \cdots + k_n p^n$$

où $k_i < p$. De même, pour $b = (b_n)$, il existe un M minimal pour lequel $b_M \not\equiv 0 \pmod{p^M}$ et donc $p^{M-1} < b_M < p^M$. On a aussi une décomposition en somme pour tout b_m pour $m \geq M$. Posons $K = N + M$, alors, si $c = (c_n)$ que l'on pose comme ab, $c_K \neq 0$. En effet, on a que

$$c_K = (a_N + k_1 p^{N+1} + \cdots + k_K p^K)\,(a_M + k'_1 p^{M+1} + \cdots + k'_K p^K).$$

En réduisant modulo p^K, on obtient que $c_K \equiv a_N b_M \pmod{p^K}$. Or, $0 < a_N < p^N$ et $0 < b_M < p^M$, donc $a_N b_M \not\equiv 0 \pmod{p^K}$. Par conséquent, $c_K \not\equiv 0 \pmod{p^K}$ et ainsi $c = ab$ est non nul.

6 Description de la clôture algébrique par limite inductive

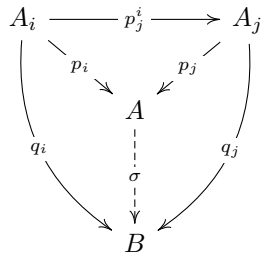
Cette brève section vise à définir une notion duale à la limite projective : la limite inductive, et de s'en servir afin de donner une caractérisation d'une clôture algébrique d'un corps.

6.1 La notion de limite inductive

Définition 6.1. Soit $(I, \leq)$ un ensemble dirigé et soit C une catégorie.

(a) Un *système inductif* dans C indexé par $(I, \leq)$ est une famille $(A_i)_{i\in I}$ d'objets de C ainsi qu'une famille $(p^i_j \colon A_i \to A_j)_{i\leq j}$ de morphismes tels que $p^i_i = \mathrm{Id}_{A_i}$ et $p^j_k \circ p^i_j = p^i_k$ pour tous $i \leq j \leq k$.

(b) Un objet A de C ainsi qu'une famille $(p_j \colon A_j \to A)_{j\in I}$ de morphismes satisfaisant $p_j \circ p^i_j = p_i$ pour tous $i \leq j$ est une *limite inductive* du système (a) si pour tous autre objet B et famille $(q_j \colon A_j \to B)$ de morphismes tels que $q_j \circ p^i_j = q_i$ pour tous $i \leq j$, il existe un unique morphisme $\sigma \colon A \to B$ tel que $\sigma \circ p_j = q_j$ pour tout j (propriété universelle).



Lorsqu'elle existe, la limite inductive est unique à isomorphisme près. On la désigne par $\varinjlim(A_i, p^i_j)$, ou plus simplement $\varinjlim A_i$.

6.2 Caractérisation d'une clôture algébrique

Soit K un corps, on considère comme ensemble dirigé $(K[X], |)$. Il s'agit bien d'un tel ensemble puisque si P et Q sont des polynômes à coefficients dans K, on peut considérer leur produit $PQ(X) \in K[X]$ et à la fois P et à la fois Q divise PQ.

Soit $P(X) \in K[X]$, on note K_P son corps de décomposition sur K dans une clôture algébrique fixée de K. On fera la convention que si P est nul, son corps de décomposition est K. On remarque que si P divise Q, alors $\mathrm{Rac}(P) \subseteq \mathrm{Rac}(Q)$ et donc $K_P \subseteq K_Q$. On note $\iota^P_Q \colon K_P \to K_Q$ le morphisme d'inclusion. L'ensemble $(K_P, \iota^P_Q)_{P\in K[X]}$ forme naturellement un système inductif.

La limite inductive de ce système est $\bigcup_{P\in I} K_P$. Pour cela, il faut vérifier la propriété universelle. Soit L un corps et $f_P \colon K_P \to L$ des morphismes compatibles, on doit montrer l'unique existence d'un morphisme $f \colon \bigcup_{P\in I} K_P \to L$. Considérons $\alpha \in \bigcup_{P\in I} K_P$, on définit

$$f(\alpha) = f_P(\alpha)$$

où $\alpha \in K_P$. C'est indépendant de P puisque si $\alpha \in K_Q$, alors $\alpha \in K_{PQ}$ et K_P, $K_Q \subseteq K_{PQ}$. L'application f est compatible et est un morphisme puisque chaque f_P l'est. Cette construction fournit également l'unicité.

On constate que la limite inductive de ce système n'est rien d'autre que K^{alg}. En effet, si α est algébrique sur K, il est racine de son polynôme minimal sur K, notons-le P, et donc $\alpha \in K_P$. Réciproquement, si $\alpha \in \bigcup_{P\in I} K_P$, il existe un P tel que α est un élément du corps de décomposition de P. Ainsi, $K(\alpha) \subseteq K_P$ qui est une extension finie de K donc $K(\alpha)$ est une extension algébrique et en particulier α est algébrique sur K. Ainsi,

$$\varinjlim_{P\in K[X]} K_P = K^{\mathrm{alg}}.$$

6.3 Un lien avec les limites projectives

Nous allons à présent prouver un résultat analogue à celui sur les limites projectives.

Proposition 6.2. *Soient I un ensemble dirigé et J un sous-ensemble cofinal de I. Alors les systèmes inductifs $(A_i, p_j^i)_{i\in I}$ et $(A_i, p_j^i)_{i\in J}$ ont des limites inductives isomorphes.*

Démonstration. Soit A_I (resp. A_J) la limite inductive issue du système $(A_i, p_j^i)_{i\in I}$ (resp. $(A_i, p_j^i)_{i\in J}$). On notera, pour tout $i \in I$, $p_i \colon A_i \to A_I$ et, pour tout $j \in J$, $q_j \colon A_j \to A_J$ les morphismes associés. Une première utilisation de la propriété universelle fournit l'existence d'un unique morphisme

$$\sigma \colon A_I \to A_J$$

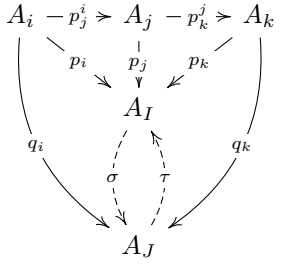
vérifiant pour tout $j \in J$ que $\sigma \circ p_j = q_j$. Étant donné que J est cofinal dans I, pour tout $i \in I$, il existe un $j \in J$ pour lequel $i \leq j$. Par conséquent, pour tout $i \in I$, on peut associer une application de la forme $q_j \circ p_j^i$. Cette application ne dépend pas du choix du $j \geq i$. En effet, comme J est dirigé, pour tout $k \geq i$, il existe un $n \in J$ pour lequel j, $k \leq n$ et donc

$$q_k \circ p_k^i = q_n \circ p_n^k \circ p_k^i = q_n \circ p_n^i = q_n \circ p_n^j \circ p_j^i = q_j \circ p_j^i.$$

On va considérer comme application réciproque $r_i \colon A_i \to A_J$ définie quel que soit $i \in I$ par $r_i = q_j \circ p_j^i$ pour un $j \geq i$. En utilisant une seconde fois la propriété universelle, on obtient un unique morphisme

$$\tau \colon A_J \to A_I$$

tel que $p_i = \tau \circ r_i$ pour tout $i \in I$. Au vu de l'unicité, ces deux applications sont inverses l'une de l'autre et on obtient ainsi un isomorphisme.



□

Corollaire 6.3. *Soit K un corps, on pose Int l'ensemble des extensions finies et intermédiaires à K^{alg} et K. Alors*

$$\mathrm{Gal}(\varinjlim_{F\in Int} F/K) \simeq \varprojlim_{F\in Int} \mathrm{Gal}(F/K).$$

Démonstration. Soit F une extension finie et comprise entre K^{alg} et K. Il existe un élément primitif $\alpha \in F$ pour lequel $F = K(\alpha)$. Soit P_α le polynôme minimal de α sur K, alors

$$F = K(\alpha) \subseteq K_{P_\alpha}$$

où K_P désigne le corps de décomposition de P sur K. Ainsi, l'ensemble des extensions du type K_P où $P \in K[X]$ est cofinal dans celui des extensions finies, Int. Par ce qui a été fait précédemment,

$$\varinjlim_{F\in \mathrm{Int}} F \simeq \varinjlim_{P\in K[X]} K_P = K^{\mathrm{alg}}.$$

Cela permet de conclure puisque, par des résultats vu dans le chapitre sur les limites projectives, on sait que

$$\mathrm{Gal}(K^{\mathrm{alg}}/K) \simeq \varprojlim_{F\in \mathrm{Int}} \mathrm{Gal}(F/K).$$ □

7 Le théorème fondamental de la théorie de Galois

7.1 Motivation

Dans le cadre des extensions infinies, la théorie de Galois classique n'est plus valable en l'état. Il faut tenir compte d'une topologie sur les groupes de Galois, la topologie de Krull.

Il est en effet possible de trouver deux groupes qui fixent le même corps mais qui pourtant sont différents. C'est le cas par exemple du groupe de Galois absolu $\mathrm{Gal}(\mathbf{F}_q^{\mathrm{sep}}/\mathbf{F}_q)$ de $\mathbf{F}_q$ et de $\langle \mathrm{Frob}_q \rangle$ où q est une puissance d'un nombre premier. Ces deux groupes fixent le même corps, à savoir $\mathbf{F}_q$. Si x est un élément de $\mathbf{F}_q$, alors $x^q = x$ et donc x est fixe par Frob_q. Réciproquement, si x est fixe par Frob_q, alors $x^q = x$ et donc x est racine du polynôme $X^q - X$. Il s'agit donc d'un élément de $\mathbf{F}_q$, qui pour rappel, est le corps formé des racines de $X^q - X$. Ainsi,

$$\mathbf{F}_q^{\mathrm{sep}\,\langle \mathrm{Frob}_q \rangle} = \mathbf{F}_q.$$

Si on note G le groupe de Galois absolu $\mathrm{Gal}(\mathbf{F}_q^{\mathrm{sep}}/\mathbf{F}_q)$ de $\mathbf{F}_q$, alors, comme $\langle \mathrm{Frob}_q \rangle$ est un sous-ensemble de G, le corps fixé par G est inclus à celui fixé par $\langle \mathrm{Frob}_q \rangle$. Réciproquement, soit $x \in \mathbf{F}_q$ et considérons σ un élément de G. Il s'agit d'un $\mathbf{F}_q$-automorphisme $\mathbf{F}_q^{\mathrm{sep}} \xrightarrow{\sim} \mathbf{F}_q^{\mathrm{sep}}$ et donc $\sigma(x) = x$. Ainsi on obtient que

$$\mathbf{F}_q^{\mathrm{sep}\,\mathrm{Gal}(\mathbf{F}_q^{\mathrm{sep}}/\mathbf{F}_q)} = \mathbf{F}_q.$$

Cependant, ces deux groupes diffèrent. Il est clair, vu que Frob_q est un $\mathbf{F}_q$-automorphisme $\mathbf{F}_q^{\mathrm{sep}} \xrightarrow{\sim} \mathbf{F}_q^{\mathrm{sep}}$, que $\langle \mathrm{Frob}_q \rangle$ soit inclus à G. Cette inclusion est néanmoins stricte. Vu que G est isomorphe, en tant que groupe, au complété profini des entiers $\widehat{\mathbf{Z}}$ et que $\langle \mathrm{Frob}_q \rangle$ est isomorphe au groupe $\mathbf{Z}$ par $n \mapsto \mathrm{Frob}_q^n$, cela revient à montrer l'existence d'un entier profini qui n'est pas un entier. L'application $\mathbf{Z} \to \widehat{\mathbf{Z}} \colon a \mapsto (a \bmod n)$ est injective. En effet, pour a, b deux entiers différents, si on considère $n > \max(a, b)$, alors l'image de a diffère de l'image de b à la composante n puisque

$$a \bmod n = a \neq b = b \bmod n.$$

Cette application n'est pas surjective. Si on considère $(a_n)_{n \geq 1}$ définie par $a_n = 1$ si n est une puissance de 2 et $a_n = 0$ sinon,

$$(a_n)_{n \geq 1} = (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, \dots),$$

alors il n'existe aucun entier a qui atteint cet élément de $\widehat{\mathbf{Z}}$. Étant donné que $a \bmod 2 = 1$, a doit être impair mais $a = a \bmod a + 2 = 0$ vu que $a + 2$ est impair et n'est donc pas une puissance de 2. Ainsi, cela permet de conclure sur le fait que G est distinct de $\langle \mathrm{Frob}_q \rangle$. Un autre argument est le suivant. Étant donné que $\widehat{\mathbf{Z}}$ et $\mathbf{Z}$ ne sont pas isomorphes, notre morphisme injectif ne peut être surjectif. Bien que ces deux groupes diffèrent, on peut en réalité montrer que

$$\mathrm{Gal}(\mathbf{F}_q^{\mathrm{sep}}/\mathbf{F}_q) = \mathrm{adh}(\langle \mathrm{Frob}_q \rangle).$$

Étant donné que G est compact, il est fermé. Vu que $\langle \mathrm{Frob}_q \rangle$ est inclus à G, ce dernier contient la fermeture de $\langle \mathrm{Frob}_q \rangle$. Réciproquement, soit σ un élément de G. Si σ n'est pas dans la fermeture de $\langle \mathrm{Frob}_q \rangle$, alors on peut trouver un ouvert O_σ qui comprend σ pour lequel

$$O_\sigma \cap \langle \mathrm{Frob}_q \rangle = \varnothing. \tag{3}$$

En se rappelant des bases de voisinage et de la particularité des extensions de $\mathbf{F}_q$, il existe un naturel non nul n pour lequel $\mathrm{Gal}(\mathbf{F}_q^{\mathrm{sep}}/\mathbf{F}_{q^n})$ est inclus à O_σ. Mais ce groupe comprend un itéré du Frobenius, à savoir $x \mapsto x^{q^n}$. Cela vient directement contredire (3).

7.2 La correspondance de Galois

Proposition 7.1. *Soit Ω une extension galoisienne sur K, soit L un sous-corps de Ω contenant K. Alors Ω est galoisien sur L, le groupe de Galois $\mathrm{Gal}(\Omega/L)$ est fermé dans $\mathrm{Gal}(\Omega/K)$ et $\Omega^{\mathrm{Gal}(\Omega/L)} = L$.*

Démonstration. La première assertion a été prouvé précédemment. Pour chaque sous-ensemble fini S de L, $G(S)$ est un sous-groupe ouvert de $\mathrm{Gal}(\Omega/L)$ et donc il est fermé. Vu que

$$\mathrm{Gal}(\Omega/L) = \bigcap_{S \subseteq L} G(S),$$

alors $\mathrm{Gal}(\Omega/L)$ est également fermé. La dernière assertion s'obtient par un résultat précédent. □

Proposition 7.2. *Soit Ω une extension galoisienne sur K. Pour tout sous-groupe H de $\mathrm{Gal}(\Omega/K)$, $\mathrm{Gal}(\Omega/\Omega^H)$ est la fermeture de H.*

Démonstration. Vu que $\mathrm{Gal}(\Omega/\Omega^H)$ contient H et qu'il est fermé, il contient la fermeture de H. Soit $\sigma \in \mathrm{Gal}(\Omega/K) \setminus \mathrm{adh}(H)$, il faut montrer que σ n'est pas fixe sur Ω^H. Vu que σ n'est pas dans la fermeture de H,

$$\sigma \,\mathrm{Gal}(\Omega/E) \cap H = \varnothing \tag{4}$$

pour une certaine extension finie E de K dans Ω (puisque les ensembles de la forme $\mathrm{Gal}(\Omega/E)$ constituent une base de voisinage de Id_Ω). Soit ϕ l'application $\mathrm{Gal}(\Omega/K) \twoheadrightarrow \mathrm{Gal}(E/K)$ de restriction. Alors $\sigma_{\restriction_E}$ n'est pas dans ϕH. En effet, si ce n'était pas le cas, $\sigma_{\restriction_E} = \tau_{\restriction_E}$ pour $\tau \in H$ et donc $\sigma^{-1}\tau$ serait un élément de $\mathrm{Gal}(\Omega/E)$, ou encore $\tau \in \sigma\,\mathrm{Gal}(\Omega/E)$ et cela contredit (4). Par conséquent σ n'est pas fixe sur $E^{\phi H} \subseteq \Omega^H$. □

Théorème 7.3 (correspondance de Galois)**.** *Soit Ω une extension galoisienne sur K. Les applications*

$$H \mapsto \Omega^H \quad \textit{et} \quad L \mapsto \mathrm{Gal}(\Omega/L)$$

sont des bijections inverses l'une de l'autre entre l'ensemble des sous-groupes fermés de $\mathrm{Gal}(\Omega/K)$ et l'ensemble des corps intermédiaires à Ω et K. De plus,

(a) la correspondance renverse les inclusions : $H_1 \supseteq H_2$ si et seulement si $\Omega^{H_1} \subseteq \Omega^{H_2}$.

(b) un sous-groupe fermé H de $\mathrm{Gal}(\Omega/K)$ est ouvert si et seulement si Ω^H est de degré fini sur K, dans ce cas $(\mathrm{Gal}(\Omega/K) : H) = [\Omega^H : K]$.

(c) le conjugué $\sigma H \sigma^{-1}$ correspond à σL, i.e. $\Omega^{\sigma H \sigma^{-1}} = \sigma(\Omega^H)$; $\mathrm{Gal}(\Omega/\sigma L) = \sigma\,\mathrm{Gal}(\Omega/L)\sigma^{-1}$.

(d) un sous-groupe fermé H de $\mathrm{Gal}(\Omega/K)$ est normal si et seulement si Ω^H est galoisien sur K, auquel cas $\mathrm{Gal}(\Omega^H/K) \simeq \mathrm{Gal}(\Omega/K)/H$.

Démonstration. Dans un premier temps, montrons que les applications $H \mapsto \Omega^H$ et $L \mapsto \mathrm{Gal}(\Omega/L)$ sont inverses l'une de l'autre. Soit H un sous-groupe fermé de $\mathrm{Gal}(\Omega/K)$, alors Ω est galoisien sur Ω^H et, par un résultat précédent, $\mathrm{Gal}(\Omega/\Omega^H) = H$. Soit L un corps intermédiaire, alors $\mathrm{Gal}(\Omega/L)$ est un sous-groupe fermé de $\mathrm{Gal}(\Omega/K)$ et, par le même résultat, $\Omega^{\mathrm{Gal}(\Omega/L)} = L$.

Pour le point (a), il est clair que si $H_1 \supseteq H_2$, alors $\Omega^{H_1} \subseteq \Omega^{H_2}$ et donc $\mathrm{Gal}(\Omega/\Omega^{H_1}) \supseteq \mathrm{Gal}(\Omega/\Omega^{H_2})$. On peut alors conclure sur base de la proposition précédente puisque, pour $i = 1, 2$, $\mathrm{Gal}(\Omega/\Omega^{H_i}) = H_i$.

En ce qui concerne (b), on a vu qu'un sous-groupe fermé d'indice fini dans un espace topologique est toujours ouvert. Réciproquement, comme $\mathrm{Gal}(\Omega/K)$ est compact, un sous-groupe ouvert de $\mathrm{Gal}(\Omega/K)$ est toujours d'indice fini. Soit H un tel sous-groupe, l'application

$$\begin{array}{ccc} \mathrm{Gal}(\Omega/K)/H & \xrightarrow{\sim} & \mathrm{Hom}_K(\Omega^H, \Omega) \\ \sigma & \longmapsto & \sigma_{\restriction_{\Omega^H}} \end{array}$$

définie une bijection, ce qui permet de conclure.

Dans le cas de (c), soit $\tau \in \mathrm{Gal}(\Omega/K)$. Alors $\tau \in \mathrm{Gal}(\Omega/\sigma L)$ si et seulement si, pour tout $x \in L$, $\tau\sigma(x) = \sigma(x)$, ou encore, pour $x \in L$, $\sigma^{-1}\tau\sigma(x) = x$. Cela revient à dire que $\sigma^{-1}\tau\sigma \in \mathrm{Gal}(\Omega/L)$, ce qui est équivalent à ce que $\tau \in \sigma\,\mathrm{Gal}(\Omega/L)\sigma^{-1}$. Donc, à $\sigma\,\mathrm{Gal}(\Omega/L)\sigma^{-1}$ correspond σL.

Finalement, pour (d), soit $H \leftrightarrow L$. Par le point précédent, H est normal dans $\mathrm{Gal}(\Omega, K)$ si et seulement si L est stable sous l'action de $\mathrm{Gal}(\Omega, K)$. Mais L est stable sous l'action de $\mathrm{Gal}(\Omega, K)$ est équivalent à ce que L soit une union d'extensions finies galoisiennes de K stables sous $\mathrm{Gal}(\Omega, K)$, *i.e.* d'extensions galoisiennes finies de K. Nous avons déjà montré qu'une extension est galoisienne si et seulement si elle est une union d'extensions galoisiennes finies. □

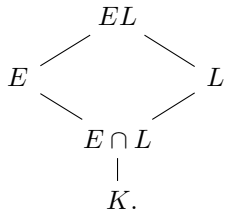
Remarque 7.4. Comme dans le cas fini, pour $(M_i)_{i\in I}$ une famille (potentiellement infinie) de corps intermédiaires, et soit H_i correspondant à M_i, on pose $\prod_{i\in I} M_i$ le plus petit corps contenant chacun des M_i. Comme $\bigcap_{i\in I} H_i$ est le plus gros sous-groupe (fermé) contenu dans chacun des H_i,

$$\mathrm{Gal}\left(\Omega/\textstyle\prod_{i\in I} M_i\right) = \bigcap_{i\in I} H_i.$$

Remarque 7.5. Soit $L \leftrightarrow H$, le plus gros sous-groupe normal (fermé) contenu dans H est

$$N := \bigcap_{\sigma\in\mathrm{Gal}(\Omega/K)} \sigma H \sigma^{-1}$$

et, donc Ω^N est le plus petite extension normale de K contenant L.



Proposition 7.6. *Soient E et L des extensions d'un corps K. Si E/K est galoisienne, alors EL/L et $E/E\cap L$ sont galoisiennes et l'application*

$$\begin{array}{ccc} \mathrm{Gal}(EL/L) & \xrightarrow{\sim} & \mathrm{Gal}(E/E\cap L) \\ \sigma & \longmapsto & \sigma_{\restriction E} \end{array}$$

est un isomorphisme de groupes topologiques.

Démonstration. Cette fonction est clairement continue, posons G_1 (resp. G_2) le groupe $\mathrm{Gal}(EL/L)$ (resp. $\mathrm{Gal}(E/E\cap L)$). Pour tout sous-ensemble fini S de E, l'image réciproque de $G_2(S)$ dans G_1 est précisément $G_1(S)$.

Il s'agit d'un isomorphisme de groupes. Comme dans le cas fini, l'application est un morphisme injectif. Soit H l'image de cette application, le corps fixe par H est $E\cap L$ et donc H est dense dans $\mathrm{Gal}(E/E\cap L)$ via l'une des propositions précédentes. Étant donné que H est fermé – il est l'image d'une application continue dans un espace compact – on en déduit que $H = \mathrm{Gal}(E/E\cap L)$.

L'application est ouverte. Un sous-groupe ouvert de $\mathrm{Gal}(EL/L)$ est fermé (et par conséquent compact) d'indice fini, donc son image dans $\mathrm{Gal}(E/E\cap L)$ est compacte (et aussi fermée) d'indice fini, et donc ouverte.

Il est clair que lorsque E/K est une extension galoisienne, $E/E\cap L$ est également galoisienne. De plus, vu que E/K est une extension normale et séparable, il s'agit du corps de décomposition d'une famille de polynômes. Alors, EF/F est le corps de décomposition de cette même famille de polynômes. □

Corollaire 7.7. *Soit Ω un corps algébriquement clos contenant K et soient E et L comme dans la proposition précédente. Si $\rho\colon E \hookrightarrow \Omega$ et $\sigma\colon L \hookrightarrow \Omega$ sont des K-plongements qui coïncident sur $E \cap L$, alors il existe un K-plongement $\tau\colon EL \hookrightarrow \Omega$ tel que $\tau_{\restriction_E} = \rho$ et $\tau_{\restriction_L} = \sigma$.*

Démonstration. Par le théorème d'extensions des plongements, σ peut s'étendre en un K-plongement $\sigma^*\colon EL \hookrightarrow \Omega$. En utilisant l'hypothèse, c'est-à-dire en supposant que σ^* et ρ coïncident sur $E \cap L$, on peut écrire ${\sigma^*}_{\restriction_E} = \rho \circ \varepsilon$ pour un certain $\varepsilon \in \mathrm{Gal}(E/E \cap L)$. Selon la proposition, il existe un unique $e \in \mathrm{Gal}(EL/L)$ tel que $e_{\restriction_E} = \varepsilon$. On prend alors $\tau = \sigma^* \circ e^{-1}$. □

7.3 Application : le théorème de résolubilité

Définition 7.8. Soit P un polynôme à coefficients dans un corps K de degré ≥ 1. L'équation $P(X) = 0$ est *résoluble* si le corps de décomposition de P sur K est contenu dans une tour d'extensions

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_{m-1} \subseteq K_m$$

telle que pour tout $0 \leq i \leq m-1$, K_{i+1}/K_i est le corps de décomposition d'un polynôme de la forme $X^{n_i} - a_i$ pour $a_i \in K_i$.

Autrement dit, les racines de P dans K^{alg} sont obtenues à partir de K en utilisant les opérations de corps et $\sqrt[n]{\ }$ pour $n \geq 1$.

Définition 7.9. Un groupe fini G est *résoluble* s'il existe une chaîne de sous-groupes

$$\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$$

telle que pour tout $0 \leq i \leq n-1$, G_{i+1}/G_i est cyclique (ou abélien).

Proposition 7.10. *Tout sous-groupe et tout groupe quotient d'un groupe résoluble est résoluble.*

Démonstration. Soit $G \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_n$ la chaîne de sous-groupes associée au groupe résoluble G. Soit H un sous-groupe de G. Le morphisme

$$H \cap G_i \to {G_i}/{G_{i+1}} : x \mapsto xG_{i+1}$$

a pour noyau $(H \cap G_i) \cap G_{i+1} = H \cap G_{i+1}$. Par conséquent, $H \cap G_{i+1}$ est normal dans $H \cap G_i$ et le quotient $H \cap G_i / H \cap G_{i+1}$ s'injecte dans G_i/G_{i+1}, qui est abélien. On a donc montré que

$$H \trianglerighteq H \cap G_1 \trianglerighteq \cdots \trianglerighteq H \cap G_n$$

est une chaîne résoluble pour H. Si on considère à présent $\overline{G}$ un groupe quotient de G, et posons $\overline{G}_i$ l'image de G_i dans $\overline{G}$, alors

$$\overline{G} \trianglerighteq \overline{G}_1 \trianglerighteq \cdots \trianglerighteq \overline{G}_n = \{1\}$$

est une chaîne résoluble pour $\overline{G}$. □

Lemme 7.11. *Soit P un polynôme séparable à coefficients dans K et soit K' un corps contenant K. Alors le groupe de Galois de P vu comme un élément de $K'[X]$ est un sous-groupe de Galois de P vu comme un élément de $K[X]$.*

Démonstration. Soit E' un corps de décomposition de P sur K' et posons $\alpha_1, \ldots, \alpha_n$ les racines de $P(X)$ dans E'. Dans ce cas, $E = K(\alpha_1, \ldots, \alpha_n)$ est un corps de décomposition de P sur K. Chaque automorphisme de $\mathrm{Gal}(E'/F')$ permute les α_i et donc envoie E sur lui-même. Ainsi, l'application de restriction $\sigma \mapsto \sigma_{\restriction_E}$ est une injection $\mathrm{Gal}(E'/K') \hookrightarrow \mathrm{Gal}(E/K)$. □

Théorème 7.12. *Soit K un corps de caractéristique nulle. Un polynôme de $K[X]$ est résoluble si et seulement si son groupe de Galois est résoluble.*

Démonstration. Intéressons-nous tout d'abord à l'implication dans le sens opposé de la lecture. Soit P un polynôme à coefficients de K dont le groupe de Galois, que nous désignerons par G_P, est résoluble. On pose $K' = K(\zeta)$ où ζ est une racine primitive n-ième de l'unité pour un n très grand – par exemple, $n = (\deg P)!$. Le lemme précédent permet d'affirmer que le groupe de Galois G de P vu comme un élément de $K'[X]$ est un sous-groupe de G_P et est donc également résoluble par la proposition précédente. Cela signifie qu'il existe une chaîne de sous-groupes

$$G = G_0 \trianglerighteq \cdots \trianglerighteq G_{m-1} \trianglerighteq G_m = \{1\}$$

où tous les G_{i-1}/G_i sont cycliques. Soit E un corps de décomposition de P sur K' et posons $K_i = E^{G_i}$. On obtient une chaîne de corps

$$K \subseteq K(\zeta) = K' = K_0 \subseteq \cdots \subseteq K_{m-1} \subseteq K_m = E$$

où chaque K_i est cyclique sur K_{i-1}. Un théorème précédent permet d'affirmer que $K_i = K_{i-1}(\alpha_i)$ où $\alpha_i^{[K_i:K_{i-1}]}$ est un élément de K_{i-1} et cela, pour tout i. Par conséquent, P est résoluble.

Pour la réciproque, il suffit de montrer que G_P est le quotient d'un groupe résoluble par la proposition précédente. Ainsi, il suffit de trouver une extension résoluble E de K telle que P se décompose dans $E[X]$. On sait qu'il existe une tour d'extensions de corps

$$K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_m$$

telle que $K_i = K_{i-1}(\alpha_i)$ pour $\alpha_i^{r_i} \in K_{i-1}$ et F_m contient un corps de décomposition de P. Soit n le produit des r_i et considérons Ω une extension galoisienne sur K contenant (une copie de) K_m et une racine primitive n-ième de l'unité. Par exemple, on peut choisir un élément primitif α pour K_m sur K et considérons Ω comme étant un corps de décomposition de $Q(X)(X^n - 1)$ où Q est le polynôme minimal de α sur K. On considère le groupe de Galois de Ω/K et on pose E la clôture galoisienne de $K_m(\zeta)$ dans Ω. Par un résultat sur la théorie fondamentale de Galois, E est le compositum des corps $\sigma K_m(\zeta)$, pour $\sigma \in \mathrm{Gal}(\Omega/K)$ et donc il est généré sur K par les éléments

$$\zeta, \alpha_1, \ldots, \alpha_m, \sigma\alpha_1, \ldots, \sigma\alpha_m, \sigma'\alpha_1, \ldots.$$

On adjoint un-à-un à K ces éléments pour obtenir une chaîne de corps

$$K \subseteq K(\zeta) \subseteq K(\zeta, \alpha_1) \subseteq \cdots \subseteq K' \subseteq K'' \subseteq \cdots \subseteq E$$

où chaque corps K'' est obtenu par son prédécesseur K' en adjoignant une r-ième racine d'un élément de K', pour $r = r_1, \ldots, r_m$ ou n. Par des résultats précédents, chacune de ces extensions est abélienne (et même cyclique) et donc E est une extension résoluble de K. □

8 Cohomologie galoisienne

Le but de cette section de prouver le théorème 90 d'Hilbert dans sa version multiplicative et additive.

8.1 L'indépendance linéaire des caractères

Théorème 8.1 (Dedekind)**.** *Soient K un corps et $\sigma_1, \dots, \sigma_n$ des automorphismes distincts de K. Si pour $a_1, \dots, a_n \in K$,*

$$a_1\sigma_1 + \cdots + a_n\sigma_n = 0,$$

alors chaque a_i est nul. On dira que $\sigma_1, \dots, \sigma_n$ sont linéairement indépendants sur K.

Démonstration. Si on considère seulement un automorphisme, il est clair qu'il soit linéairement indépendant. Supposons par l'absurde qu'il y ait r, où r est minimal, coefficients non nuls dans cette relation. Alors $r \geq 2$. Supposons sans perte de généralité qu'ils s'agissent des coefficients $a_1, \dots, a_r$. Pour tout $x \in K$,

$$a_1\sigma_1(x) + \cdots + a_r\sigma_r(x) = 0.$$

Soit $y \in K$ où σ_1 diffère de σ_r. Un tel élément existe vu que nous les avons supposés distincts. Pour tous x, $y \in K$, l'égalité est vérifiée en xy :

$$a_1\sigma_1(x)\sigma_1(y) + \cdots + a_r\sigma_r(x)\sigma_r(y) = 0.$$

En multipliant la première relation par $\sigma_r(y)$ et en soustrayant le résultat par la seconde, on obtient que

$$a_1[\sigma_r(y) - \sigma_1(y)]\sigma_1(x) + \cdots + a_{r-1}[\sigma_r(y) - \sigma_{r-1}(y)]\sigma_{r-1}(x) = 0$$

qui est plus petite que la relation de l'hypothèse par l'absurde et dont au moins le premier coefficient est non nul. □

8.2 Le premier groupe de cohomologie

Définition 8.2. Soit G un groupe. Un *G-module* est un groupe abélien M muni d'une action de G sur M.

Exemple 8.3. Soit L une extension galoisienne de K. Alors, $(L, +)$ et $(L^\times, \cdot)$ sont des $\mathrm{Gal}(L/K)$-modules.

Définition 8.4. Soit M un G-module. Un *morphisme croisé* (ou 1-cocycle) de M est une application $f\colon G \to M$ telle que, pour tous σ et $\tau \in G$,

$$f(\sigma\tau) = f(\sigma) + \sigma f(\tau).$$

Remarque 8.5. Cette condition implique que $f(1) = f(1 \cdot 1) = f(1) + f(1)$ et donc $f(1) = 0$.

On notera l'ensemble des morphismes croisés de G dans M par $\mathrm{Z}^1(G, M)$. Étant donné que la somme et la différence de morphismes croisés est encore un morphisme croisé, $\mathrm{Z}^1(G, M)$ possède une structure de groupe.

Remarque 8.6. Soit $f\colon G \to M$ un morphisme croisé. Quel que soit le $\sigma \in G$,

$$f(\sigma^2) = f(\sigma) + \sigma f(\sigma) \tag{5}$$
$$f(\sigma^3) = f(\sigma \cdot \sigma^2) = f(\sigma) + \sigma f(\sigma) + \sigma^2 f(\sigma) \tag{6}$$
$$\cdots \tag{7}$$
$$f(\sigma^n) = f(\sigma) + \sigma f(\sigma) + \cdots + \sigma^{n-1} f(\sigma). \tag{8}$$

Ainsi, si G est un groupe cyclique d'ordre n et généré par σ, un morphisme croisé $f\colon G \to M$ est déterminé par sa valeur en σ, notons là x, et x satisfait l'équation

$$x + \sigma x + \cdots + \sigma^{n-1}x = 0. \tag{9}$$

De plus, si $x \in M$ satisfait (9) alors $f(\sigma^i) = x + \sigma x + \cdots + \sigma^{i-1}x$ définit un morphisme croisé de G dans M. Par conséquent, pour un groupe fini cyclique $G = \langle\sigma\rangle$, il y a une correspondance donnée par $f \leftrightarrow f(\sigma)$ entre

$$\mathrm{Z}^1(G, M) \longleftrightarrow \{x \in M \text{ satisfaisant (9)}\}.$$

On peut remarquer que chaque $x \in M$ induit un morphisme croisé de la forme

$$f(\sigma) = \sigma x - x$$

pour tout $\sigma \in G$. En effet, si on considère σ et τ des éléments de G, il s'en suit que

$$f(\sigma) + \sigma f(\tau) = \sigma x - x + \sigma\tau x - \sigma x = \sigma\tau x - x = f(\sigma\tau).$$

De tels morphismes croisés sont appelés **principaux** (ou 1-cobord). On notera l'ensemble des morphismes croisés principaux de G dans M par $\mathrm{B}^1(G, M)$. À nouveau, la somme et la différence de tels morphismes est encore un morphisme croisé principal et donc $\mathrm{B}^1(G, M)$ dispose d'une structure de groupe. Plus précisément, $\mathrm{B}^1(G, M)$ est un sous-groupe normal de $\mathrm{Z}^1(G, M)$ car M est abélien.

Remarque 8.7. Si G agit trivialement sur M, c'est-à-dire si $\sigma m = m$ pour tous $\sigma \in G$ et $m \in M$, alors un morphisme croisé est simplement un morphisme et il n'y a aucun morphisme croisé principal non nul.

On appelle *premier groupe de cohomologie* de G dans M le groupe abélien quotient

$$\mathrm{H}^1(G, M) = \mathrm{Z}^1(G, M)\big/_{\mathrm{B}^1(G, M)}.$$

Théorème 8.8 (Hilbert 90 – multiplicatif)**.** *Soit L une extension galoisienne d'un corps K dont le groupe de Galois associé est G. Alors $H^1(G, L^\times) = 1$, i.e. chaque morphisme croisé $G \to L^\times$ est principal.*

Démonstration. Soit f un morphisme croisé $G \to L^\times$. En notation multiplicative, cela signifie que f satisfait

$$f(\sigma\tau) = f(\sigma) \cdot \sigma(f(\tau))$$

pour tous $\sigma, \tau \in G$. Il faut trouver un $x \in L^\times$ pour lequel $f(\sigma) = \sigma x/x$ quel que soit le $\sigma \in G$. Comme les $f(\tau) \in L^\times$ sont non nuls, l'indépendance linéaire des automorphismes implique que

$$\sum_{\tau\in G} f(\tau)\tau\colon L \to L$$

n'est pas l'application nulle, ou encore qu'il existe un α dans L pour lequel

$$\beta := \sum_{\tau\in G} f(\tau)\tau\alpha \neq 0.$$

Par conséquent, pour σ un élément de G,

$$\begin{aligned}
\sigma\beta &= \sum_{\tau\in G} \sigma(f(\tau)) \cdot \sigma\tau\alpha && (10)\\
&= \sum_{\tau\in G} f(\sigma)^{-1} f(\sigma\tau) \cdot \sigma\tau\alpha && (11)\\
&= f(\sigma)^{-1} \sum_{\tau\in G} f(\sigma\tau) \cdot \sigma\tau\alpha && (12)
\end{aligned}$$

et cela vaut précisément $f(\sigma)^{-1}\beta$ car G est un groupe et τ parcourt G. Il s'en suit que $f(\sigma) = \beta/\sigma\beta = \sigma\beta^{-1}/\beta^{-1}$. □

Définition 8.9. Soit L une extension galoisienne de K dont le groupe de Galois est G. On définit la *norme* d'un élément $\alpha \in L$ comme

$$\operatorname{Nm} \alpha = \prod_{\sigma \in G} \sigma\alpha.$$

On constate que pour tout $\tau \in G$, $\tau(\operatorname{Nm} \alpha) = \prod_{\sigma \in G} \tau\sigma\alpha = \operatorname{Nm} \alpha$ et donc $\operatorname{Nm} \alpha$ est un élément de K. L'application

$$L^\times \to K^\times \colon \alpha \mapsto \operatorname{Nm} \alpha$$

est clairement un morphisme puisque les σ sont des éléments du groupe de Galois de L/K.

Exemple 8.10. L'application de norme $\mathbf{C}^\times \to \mathbf{R}^\times$ est $z \mapsto |z|^2$.

Nous allons nous intéresser à déterminer le noyau de l'application de norme. Il est clair que les éléments de la forme $\beta/\tau\beta$ sont de norme 1 puisque G est un groupe et

$$\operatorname{Nm} \frac{\beta}{\tau\beta} = \prod_{\sigma \in G} \frac{\sigma\beta}{\sigma\tau\beta} = \frac{\prod_{\sigma \in G} \sigma\beta}{\prod_{\sigma \in G} \sigma\tau\beta} = 1.$$

Le prochain résultat énonce la réciproque dans le cadre des extensions cycliques.

Corollaire 8.11 (Hilbert 90 – multiplicatif)**.** *Soit L une extension finie cyclique de K et considérons σ un générateur de* $\operatorname{Gal}(L/K)$*. Soit $\alpha \in L^\times$, si $\operatorname{Nm} \alpha = 1$, alors $\alpha = \beta/\sigma\beta$ pour un certain $\beta \in L$.*

Démonstration. Posons n le degré de l'extension L/K. L'hypothèse sur α est telle que

$$\alpha \cdot \sigma\alpha \cdot \ldots \cdot \sigma^{n-1}\alpha = 1$$

et, par une remarque précédente, il y a un morphisme croisé $f \colon \langle\sigma\rangle \to L^\times$ pour lequel $f(\sigma) = \alpha$. Le théorème précédent permet d'affirmer que f est principal, ce qui signifie qu'il existe un $\beta \in L$ tel que $\alpha = f(\sigma) = \beta/\sigma\beta$. □

Définition 8.12. Soit L une extension galoisienne de K dont le groupe de Galois est G. On définit la *trace* d'un élément $\alpha \in L$ par

$$\operatorname{Tr} \alpha = \sum_{\sigma \in G} \sigma\alpha.$$

On constate également que pour tout $\tau \in G$, $\tau(\operatorname{Tr} \alpha) = \sum_{\sigma \in G} \tau\sigma\alpha = \operatorname{Tr} \alpha$ et donc que $\operatorname{Tr} \alpha$ est un élément de K. L'application

$$L \to K \colon \alpha \mapsto \operatorname{Tr} \alpha$$

est un morphisme pour les mêmes raisons que précédemment.

Théorème 8.13 (Hilbert 90 – additif)**.** *Soit L une extension galoisienne de K dont le groupe de Galois associé est G. Alors, si on désigne par L son groupe additif, $H^1(G, L) = 0$, i.e. chaque morphisme croisé $G \to L$ est principal.*

Démonstration. Soit $f \colon G \to L$ un morphisme croisé. Comme la trace est une somme d'automorphismes, où chaque coefficient vaut 1, la trace n'est pas l'application nulle. Il existe ainsi un $\alpha \in L$ pour lequel $\operatorname{Tr} \alpha$ n'est pas nulle. On pose

$$\beta := \frac{1}{\operatorname{Tr} \alpha} \sum_{\tau \in G} f(\tau)\tau\alpha.$$

Par conséquent, pour σ un élément de G,

$$\sigma\beta = \frac{1}{\operatorname{Tr}\alpha}\sum_{\tau\in G}\sigma f(\tau)\sigma\tau\alpha \tag{13}$$

$$= \frac{1}{\operatorname{Tr}\alpha}\sum_{\tau\in G}(f(\sigma\tau) - f(\sigma))\sigma\tau\alpha \tag{14}$$

$$= \beta - f(\sigma). \tag{15}$$

Cela permet ainsi de conclure, en considérant $-\beta$ au lieu de β. □

Nous allons désormais nous intéresser au noyau de l'application de trace. Il est encore une fois clair que les éléments de la forme $\beta - \tau\beta$ sont de trace 0 puisque G est un groupe et

$$\operatorname{Tr}\beta - \tau\beta = \sum_{\sigma\in G}\sigma\beta - \sigma\tau\beta = \sum_{\sigma\in G}\sigma\beta - \sum_{\sigma\in G}\sigma\tau\beta = 0.$$

Le prochain résultat énonce, comme précédemment, la réciproque dans le cadre des extensions cycliques.

Corollaire 8.14 (Hilbert 90 – additif)**.** *Soit L une extension finie cyclique de K et considérons σ un générateur de* $\operatorname{Gal}(L/K)$*. Soit $\alpha \in L$, si* $\operatorname{Tr}\alpha = 0$*, alors $\alpha = \beta - \sigma\beta$ pour un certain $\beta \in L$.*

Démonstration. Posons n le degré de l'extension L/K. L'hypothèse sur α est telle que

$$\alpha + \sigma\alpha + \cdots + \sigma^{n-1}\alpha = 0$$

et, par une remarque précédente, il y a un morphisme croisé $f\colon \langle\sigma\rangle \to L$ pour lequel $f(\sigma) = \alpha$. Le théorème précédent permet d'affirmer que f est principal, ce qui signifie qu'il existe un $\beta \in L$ tel que $\alpha = f(\sigma) = \beta - \sigma\beta$. □

9 Annexe : les polynômes cyclotomiques

Soit n un naturel non nul, on pose $\mathbf{U}_n$ l'ensemble des racines primitives n-ième de l'unité dans $\mathbf{C}$, c'est-à-dire des racines n-ième de l'unité qui sont exactement d'ordre n.

Théorème 9.1. *Le n-ième polynôme cyclotomique $\Phi_n(X) = \prod_{\zeta \in \mathbf{U}_n}(X - \zeta)$ est à coefficients dans $\mathbf{Z}$ et est irréductible dans $\mathbf{Q}[X]$.*

Démonstration. Remarquons tout d'abord que le degré de Φ_n est

$$\#\mathbf{U}_n = \#\{k \leq n \mid \text{pgcd}(k, n) = 1\} = \varphi(n).$$

Lorsque $n = p$ est premier, tous les éléments de $\mathbf{U}_p$, sauf 1, engendrent $\mathbf{U}_p$ et ainsi on retrouve

$$\Phi_p(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + \cdots + X + 1.$$

Considérons ζ_n et soient $0 \leq k \leq n-1$ et $d = \text{ord}(\zeta_n^k)$. Alors, d divise n. De plus, comme $(\zeta_n^k)^d = 1$, on obtient que $\zeta_n^k \in \mathbf{U}_d$ et comme d est l'ordre de ζ_n^k, on a même que $\zeta_n^k \in U_d$. Ainsi, $(X - \zeta_n^k)$ divise $\Phi_d(X)$ et donc $(X - \zeta_n^k)$ divise $\prod_{d|n} \Phi_d(X)$. Comme les ζ_n^k sont deux à deux distincts pour $0 \leq k \leq n-1$, on obtient que

$$X^n - 1 = \prod_{k=0}^{n-1}(X - \zeta_n^k) \mid \prod_{d|n} \Phi_d(X).$$

Ces deux polynômes sont de même degré, le degré du second est $\sum_{d|n} \varphi(d) = n$. Ils sont également moniques donc on conclut que

$$X^n - 1 = \prod_{d|n} \Phi_d(X).$$

Pour montrer que $\Phi_n(X)$ est à coefficients dans $\mathbf{Z}$, on procède par récurrence sur n. Pour Φ_1, c'est vrai puisque $\Phi_1 = X - 1$. Supposons que cela soit vrai jusqu'à $n - 1$. On pose

$$P = \prod_{\substack{d|n \\ d \neq n}} \Phi_d \in \mathbf{Z}[X]$$

et donc $X^n - 1 = \Phi_n(X)P(X)$. En utilisant la division euclidienne dans $\mathbf{Z}[X]$, $X^n - 1 = P(X)Q(X) + R(X)$ où $\deg(R) < \deg(P)$. Par unicité de la division euclidienne, $R(X) = 0$ et donc $\Phi_n = Q \in \mathbf{Z}[X]$ et cela prouve le résultat à l'étape n.

Nous allons maintenant montrer qu'il s'agit du polynôme minimal des racines primitives. Soit ζ une racine primitive n-ième de l'unité, soit P son polynôme minimal dans $\mathbf{Q}$. On a que $P(X)$ divise $(X^n - 1)$ et donc il existe $Q \in \mathbf{Q}[X]$ tel que $X^n - 1 = P(X)Q(X)$, comme précédemment, $Q \in \mathbf{Z}[X]$. Soit p un nombre premier qui ne divise pas n et soit a une racine de P. Nous allons montrer que a^p est racine de P. Vu que $P(X)$ divise $(X^n - 1)$, on a que $a^n - 1 = 0$ et donc

$$0 = (a^p)^n - 1 = P(a^p)Q(a^p).$$

Par l'absurde, si $P(a^p) \neq 0$, alors $Q(a^p) = 0$ par intégrité. Or, a est racine de P qui est monique et irréductible dans $\mathbf{Q}[X]$, donc P est également le polynôme minimal de a. Ainsi, comme $Q(X^p)$ annule a, on a que $P(X)$ divise $Q(X^p)$ et donc $Q(X^p) = P(X)R(X)$ où $R(X) \in \mathbf{Z}[X]$. On réduit modulo p : en se rappelant que $x^p = x$ et par Frobenius,

$$\overline{Q}(X)^p = \overline{Q}(X^p) = \overline{P}(X)\overline{R}(X).$$

Soit $T(X) \in \mathbf{F}_p[X]$ un facteur irréductible de $\overline{P}(X)$, alors T divise $\overline{Q}^p$ et donc T divise $\overline{Q}$. Comme T divise $\overline{P}$, on a alors que T^2 divise $\overline{PQ} = X^n - 1$. Ainsi, $X^n - 1$ a une racine double dans une clôture algébrique de $\mathbf{F}_p$ et cela amène une contradiction car $X^n - 1$ est copremier avec sa dérivée par Bézout :

$$(n^{-1}X)nX^{n-1} - (X^n - 1) = 1.$$

Donc $P(a^p) = 0$. Finalement on montre que Φ_n est un polynôme minimal. Vu que ζ une racine de P, pour tout p premier qui ne divise pas n, ζ^p est également racine de P. Par élévation successive à des puissances premières, on a, pour tout naturel k copremier à n, que ζ^k est racine de P. Ainsi, toutes les racines primitives n-ièmes sont racines de P. Donc, Φ_n divise P. Comme $\Phi_n(\zeta) = 0$, on a aussi que P divise Φ_n. Les deux étant moniques, on obtient que $\Phi_n = P$ est irréductible dans $\mathbf{Q}[X]$. □

Références

[1] James Stuart Milne. *Fields and Galois Theory* (v5.00). 2021. Depuis `www.jmilne.org/math/`.

[2] James Stuart Milne. *Group Theory* (v4.00). 2021. Depuis `www.jmilne.org/math/`.

[3] Serge Lang. *Algebra* (revised third edition). Springer-Verlag New York. 2002.

[4] Yozo Matshushima. *Chapitre I Groupes topologiques*. Cours de l'institut Fourier, tome 1. 1966.

[5] Jean-Pierre Serre. *A Course in Arithmetic*. Springer-Verlag New York. 1973.

[6] Steve Awodey. *Category Theory* (second edition). Oxford University Press, Inc.198 Madison Ave. New York, NYUnited States.

[7] Nathanaël Mariaule. *Limites inductives et limites projectives*. Université de Mons. 2020.

[8] Joshua Ruiter. *Infinite Galois Theory*. October 8, 2019.

[9] Sélim Cornet. *Leçons d'algèbre et géométrie. Développement : Irréductibilité des polynômes cyclotomiques*. Université Paris 2 Panthéon-Assas.

[10] Jonatan Lindell. *Profinite Groups and Infinite Galois Extensions*. Uppsala University. November 2019.