THÉORIE DE GALOIS

3. Théorie de Galois infinie

On se propose d'étendre la théorie de Galois aux extensions *algébriques* mais non nécessairement finies d'un corps k.

3.1. Extensions galoisiennes infinies

Commençons par étendre la définition des extensions galoisiennes ; on se fonde pour cela sur la caractérisation établie au théorème 7.

Proposition 3.1 — *Soit k'/k une extension algébrique. Les conditions suivantes sont équivalentes :*

(i) k est le sous-corps de k' invariant par $\mathrm{Aut}(k'/k)$;

(ii) l'extension k'/k est séparable et tout polynôme irréductible $f \in k[\mathrm{X}]$ admettant une racine dans k' est scindé dans k' (l'extension est normale*) ;*

(iii) k' est la réunion des extensions finies galoisiennes de k dans k'.

Démonstration. $(i) \Rightarrow (ii)$ Soit $x \in k'$ et soit m_x son polynôme minimal sur k. L'ensemble $\mathscr{R}$ des racines de m_x dans k' est stable sous l'action de $\mathrm{Aut}(k'/k)$ et le polynôme

$$f = \prod_{\alpha \in \mathscr{R}} (\mathrm{X} - \alpha)$$

est donc à coefficients dans k. Comme $f(x) = 0$, ce polynôme est divisible par m_x et donc finalement $f = m_x$ puisque f est unitaire et $\deg(f) \leqslant \deg(m_x)$.

$(ii) \Rightarrow (iii)$ Soit $x \in k'$ de polynôme minimal $m_x \in k[\mathrm{X}]$. Le polynôme m_x étant séparable et scindé sur k', son corps de décomposition dans k' fournit une extension finie galoisienne de k dans k' contenant x.

$(iii) \Rightarrow (i)$ Soit $\overline{k}$ une clôture algébrique de k' (donc également de k) et soit $x \in k' - k$. Comme x est séparable sur k, il existe un k-homomorphisme σ de $k(x)$ dans $\overline{k}$ tel que $\sigma(x) \neq x$. L'inclusion $i : k(x) \to \overline{k}$ et l'homomorphisme $\sigma : k(x) \to \overline{k}$ fournissant deux clôtures algébriques de $k(x)$, il existe un k-automorphisme $\overline{\sigma}$ de $\overline{k}$ tel que $\sigma = \overline{\sigma} \circ i$. Si K/k est une extension finie galoisienne de k dans $\overline{k}$, K est engendré sur k par les racines d'un polynôme séparable $f \in k[\mathrm{X}]$ (théorème 7) et donc $\overline{\sigma}(\mathrm{K}) = \mathrm{K}$ car $\overline{\sigma}$ permute les racines de f. On a ainsi $\overline{\sigma}(k') = k'$, et $\overline{\sigma}_{|k'}$ est un k-automorphisme de k' ne fixant pas x. □

Une extension algébrique k'/k est dite *galoisienne* si elle satisfait aux trois conditions équivalentes de la proposition. Vu (iii), cette définition coïncide avec la précédente lorsque l'extension est finie. On pose $\mathrm{Gal}(k'|k) = \mathrm{Aut}(k'/k)$ pour toute extension galoisienne k'/k et on parle du *groupe de Galois* de l'extension.

Exemple 3.2 — Étant donnée une clôture algébrique $\overline{k}$ de k, le sous-corps $k(\mu_\infty)$ de $\overline{k}$ engendré par les racines de l'unité d'ordre premier à la caractéristique de k est une extension galoisienne de k.

3.2. Groupe de Galois absolu

Étant donnée une clôture algébrique $\overline{k}$ de k, deux extensions finies séparables k_1 et k_2 de k dans $\overline{k}$ sont toujours contenues dans une même extension finie galoisienne : il existe en effet des polynômes séparables f_1 et f_2 dans $k[\mathrm{X}]$ tels que k_1 (resp. k_2) soit un sous-corps du corps de décomposition de f_1 (resp. f_2) dans $\overline{k}$ (corollaire 9) et, par suite, le corps de décomposition du polynôme séparable $f = \mathrm{ppcm}(f_1, f_2)$ dans $\overline{k}$ est une extension finie galoisienne contenant k_1 et k_2.

Il découle de cette observation que l'ensemble k^{s} des éléments de $\overline{k}$ séparables sur k est un sous-corps de $\overline{k}$, la *clôture séparable* de k dans $\overline{k}$. Les clôtures séparables de k dans deux clôtures algébriques sont évidemment isomorphes en tant qu'extensions de k. Comme, en outre, k^{s} est la réunion des extension finies galoisiennes de k dans $\overline{k}$, l'extension k^{s}/k est donc galoisienne.

Définition 3.3 — *Le groupe* $\mathrm{Gal}(k^{\mathrm{s}}|k)$ *est le* groupe de Galois absolu *du corps k ; il est bien défini à un isomorphisme près.*

Remarques 3.4 — 1. Étant donnés une extension galoisienne $\mathrm{K}|k$ et un sous-corps k' de K contenant k, l'extension K/k' est galoisienne.

2. On a évidemment $k^{\mathrm{s}} = \overline{k}$ si le corps k est parfait. Dans le cas contraire, $\mathrm{car}(k) = p$ et l'extension $\overline{k}/k^{\mathrm{s}}$ est *purement inséparable* : pour tout $\alpha \in \overline{k}$, il existe un nombre entier n tel que $\alpha^{p^n} \in k^{\mathrm{s}}$. En effet, le polynôme minimal f de α sur k s'écrit de manière unique sous la forme $f = g(\mathrm{X}^q)$ avec $q = p^n$ et $g \in k[\mathrm{X}]$ irréductible et séparable ; comme g est scindé sur k^{s}, $\alpha^q \in k^{\mathrm{s}}$.

3. L'application de restriction

$$\mathrm{Aut}(\overline{k}/k) \to \mathrm{Aut}(k^{\mathrm{s}}/k), \quad \sigma \mapsto \sigma_{|k^{\mathrm{s}}}$$

est un isomorphisme. Il suffit de le vérifier lorsque k est un corps de caractéristique $p > 0$. Étant donnés un k-automorphisme σ de $\overline{k}$ induisant l'identité sur k^{s} et $\alpha \in \overline{k}$, il existe un nombre entier $n \geq 0$ tel que $\alpha^{p^n} \in k^{\mathrm{s}}$ et $\sigma(\alpha)$ est donc une racine du polynôme $\mathrm{X}^{p^n} - \alpha^{p^n}$; comme $\mathrm{X}^{p^n} - \alpha^{p^n} = (\mathrm{X} - \alpha)^{p^n}$, $\sigma(\alpha) = \alpha$ et donc $\sigma = \mathrm{id}$.

4. Une bonne partie de la théorie des nombres contemporaines consiste en l'étude du groupe de Galois absolu de $\mathbb{Q}$.

3.3. Topologie du groupe de Galois

Le groupe de Galois d'une extension possède une structure naturelle de *groupe topologique* qu'il est nécessaire de faire intervenir pour prolonger la correspondance de Galois aux extensions infinies. L'exemple ci-dessous montre qu'un prolongement naïf est voué à l'échec.

Exemple 3.5 — Soit p un nombre premier et soit $\overline{\mathbb{F}}_p$ une clôture algébrique du corps fini $\mathbb{F}_p$. Le groupe de Galois absolu $\Gamma = \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ de $\mathbb{F}_p$ contient en particulier l'automorphisme de Frobenius F, défini par $\mathrm{F}(x) = x^p$ et engendrant un sous-groupe cyclique inifini $\Gamma_0 = \langle \mathrm{F} \rangle$. Le sous-corps de $\overline{\mathbb{F}}_p$ fixé par Γ_0 est le même que celui fixé par Γ ; pour autant, l'inclusion $\Gamma_0 \subset \Gamma$ est *stricte*.

Pour tout entier $n \geqslant 1$, désignons par π_n l'isomorphisme canonique $\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \mathrm{Gal}(\mathbb{F}_{p^n}|\mathbb{F}_p)$ envoyant 1 sur F. Si $m|n$, la restriction $\mathrm{Gal}(\mathbb{F}_{p^n}|\mathbb{F}_p) \to \mathrm{Gal}(\mathbb{F}_{p^m}|\mathbb{F}_p)$ correspond, dans cette identitification, à l'homomorphisme canonique de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$. Par conséquent, toute suite $\underline{a} = (a_n)_{n \geqslant 1}$ de nombres entiers naturels vérifiant la condition

$$(\forall\, m, n \in \mathbb{N} - \{0\},\ m|n \Longrightarrow\ a_n \equiv a_m \pmod{m})$$

définit naturellement un $\mathbb{F}_p$-automorphisme $\sigma_{\underline{a}}$ de $\overline{\mathbb{F}}_p$ dont la restriction au sous-corps $\mathbb{F}_{p^n}$ est F^{a_n}. Pour que cet automorphisme appartienne à Γ_0, il faut et il suffit qu'il existe $a \in \mathbb{N}$ tel que $a_n \equiv a \pmod n$ pour tout n.

Choisissons un nombre premier ℓ et soit $(a_n)_{n\geqslant 1}$ une suite de nombres entiers telle que, si $n = \ell^\alpha n'$ avec $\operatorname{pgcd}(\ell, n') = 1$, alors

$$a_n \equiv 0 \pmod{n'} \ \text{ et } \ a_n \equiv 1 + \ell + \ldots + \ell^{\alpha-1} \pmod{\ell^\alpha}.$$

Cette suite satisfait à la condition précédente en vertu du théorème chinois des restes mais il n'existe nombre entier naturel a tel que $a_n \equiv a \pmod n$ pour tout n.

Soit k un corps et soit K/k une extension galoisienne de k.

Proposition 3.6 — *Il existe une unique structure de groupe topologique sur* $\operatorname{Gal}(\mathrm{K}/k)$ *telle qu'un système fondamental de voisinages de l'identité soit formé des sous-groupes de la forme* $\operatorname{Gal}(\mathrm{K}|k')$*, où k' est une extension finie galoisienne de k dans* K.

Démonstration. De manière générale, si G est un groupe et $\mathscr{V}$ est une famille de sous-groupes distingués stable par intersection finie, il existe une unique structure de groupe topologique sur G telle que $\mathscr{V}$ soit un système fondamental de voisinages de l'origine : la stabilité de $\mathscr{V}$ permet de munir G d'une topologie telle que $g\mathscr{V}$ soit un système fondamental de voisinage de $g \in \mathrm{G}$ et l'application $(\mathrm{G}\times\mathrm{G} \to \mathrm{G},\ (g,h) \mapsto gh^{-1})$ est continue puisque $g\mathrm{H}h^{-1}\mathrm{H} = gh^{-1}(h\mathrm{H}h^{-1})\mathrm{H} = gh^{-1}\mathrm{H}$ pour tous $g,h \in \mathrm{G}$, $\mathrm{H} \in \mathscr{V}$.

La famille de sous-groupes distingués de Γ considérée ici convient car deux extensions finies galoisiennes de k dans K sont contenues dans une extension finie galoisienne commune. □

Tous les groupes de Galois considérés sont munis de la topologie que l'on vient de décrire. Si l'extension galoisienne K/k est finie, la topologie obtenue sur $\operatorname{Gal}(\mathrm{K}|k)$ est la topologie discrète.

Soit K/k une extension galoisienne et désignons par Λ l'ensemble des extensions finies galoisiennes de k dans K. Le groupe $\prod_{k'\in\Lambda}\operatorname{Gal}(k'|k)$ est muni de la topologie produit ; c'est un groupe topologique compact et totalement discontinu (tout point admet un système fondamental de voisinage ouverts et fermés).

Proposition 3.7 — *L'application naturelle*

$$\operatorname{Gal}(\mathrm{K}|k) \to \prod_{k'\in\Lambda}\operatorname{Gal}(\mathrm{K}|k'),\ \ \sigma \mapsto (\sigma_{|k'})_{k'\in\Lambda}$$

est un homomorphisme injectif de groupes topologiques d'image fermée. En particulier, le groupe topologique $\operatorname{Gal}(\mathrm{K}|k)$ *est compact et totalement discontinu.*

Démonstration. Cette application est clairement d'un homomorphisme injectif de groupes topologiques. Son image est l'ensemble H des familles $(\sigma_{k'})_{k'\in\Lambda}$ telles que, pour toutes extensions $k_1, k_2 \in \Lambda$ avec $k_1 \subset k_2$, σ_{k_1} soit la restriction de σ_{k_2} à k_1. Par suite, si $g = (\sigma_{k'})_{k'\in\Lambda}$ n'appartient pas à H et si $k_1, k_2 \in \Lambda$ sont deux extensions telles que $k_1 \subset k_2$ et σ_{k_1} ne soit la restriction de σ_{k_2} à k_1, alors $gu \notin \mathrm{H}$ pour tout u appartenant au noyau de la projection

$$\prod_{k'\in\Lambda}\operatorname{Gal}(k'|k) \to \operatorname{Gal}(k_1|k)\times\operatorname{Gal}(k_2|k).$$

Ce noyau étant ouvert par définition de la topologie produit, cela prouve que H est fermé. □

3.4. Extension de la correspondance de Galois

Nous sommes maintenant en mesure de prolonger la correspondance de Galois aux extensions algébriques quelconques.

Théorème 3.8 — *Soit* K/k *une extension galoisienne et soit* $\Gamma = \mathrm{Gal}(\mathrm{K}|k)$. *Les applications*

$$\{\textit{sous-groupes fermés de } \mathrm{Gal}(\mathrm{K}/k)\} \underset{v}{\overset{u}{\rightleftarrows}} \{\textit{sous-corps de } \mathrm{K} \textit{ contenant } k\}$$

définies par $u(\mathrm{H}) = \mathrm{K}^{\mathrm{H}}$ *et* $v(k') = \mathrm{Gal}(\mathrm{K}|k')$ *sont des bijections décroissantes réciproques. Les sous-groupes ouverts (resp. distingués) correspondent aux extensions finies (resp. galoisiennes) de* k *dans* K.

Démonstration. Si k' est une extension finie de k dans K, alors $\mathrm{Gal}(\mathrm{K}|k')$ est un sous-groupe ouvert de Γ car il contient le sous-groupe ouvert $\mathrm{Gal}(\mathrm{K}|k'')$, où k'' est une extension finie galoisienne de k dans K contenant k'. Par ailleurs, tout sous-groupe ouvert H de Γ est également fermé puisque son complémentaire $\bigcup_{g\in\Gamma-\mathrm{H}} g\mathrm{H}$ est ouvert. On en déduit que $\mathrm{Gal}(\mathrm{K}|k')$ est un sous-groupe fermé de Γ pour toute extension k' de k dans K car

$$\mathrm{Gal}(\mathrm{K}|k') = \bigcap_{\substack{k\subset k''\subset k' \\ k''/k \text{ finie}}} \mathrm{Gal}(\mathrm{K}|k'').$$

En outre, $k' = u(\mathrm{Gal}(\mathrm{K}|k'))$ puisque l'extension K/k' est galoisienne.

Considérons maintenant un sous-groupe H de Γ et soient $k' = \mathrm{K}^{\mathrm{H}}$, $\mathrm{H}' = \mathrm{Gal}(\mathrm{K}|k')$; l'inclusion $\mathrm{H} \subset \mathrm{H}'$ est triviale. Soit réciproquement σ un k'-automorphisme de K et soit k_1 une extension finie galoisienne de k dans K. Désignant par H_1 et H'_1 les images respectives de H et H' par l'homomorphisme de restriction $\Gamma \to \mathrm{Gal}(k_1|k)$,

$$k_1^{\mathrm{H}_1} = \{x \in k_1 \mid \sigma(x) = x, \text{ pour tout } \sigma \in \mathrm{H}\} = k' \cap k_1$$

et donc $\mathrm{H}_1 = \mathrm{Gal}(k_1|k_1 \cap k')$ en vertu de la correspondance de Galois pour les extensions finies. Comme $\mathrm{H}'_1 \subset \mathrm{Gal}(k_1|k_1 \cap k')$, $\mathrm{H}_1 = \mathrm{H}'_1$ et il existe ainsi un élément τ de H tel que $\tau_{|k_1} = \sigma_{|k_1}$. Par suite, $\sigma\mathrm{Gal}(\mathrm{K}|k_1) \cap \mathrm{H} \neq \varnothing$ et, comme k_1 est arbitraire, ceci montre que σ est adhérent à H. En particulier, si H est un sous-groupe fermé de Γ, alors $\mathrm{H} = \mathrm{Gal}(\mathrm{K}|\mathrm{K}^{\mathrm{H}})$.

Pour qu'une extension k' de k dans K soit galoisienne, il faut et il suffit que l'on ait $\sigma(k') = k'$ pour tout $\sigma \in \Gamma$; vu la correspondance que l'on vient d'établir, cela revient à demander que $\mathrm{Gal}(\mathrm{K}|k')$ soit un sous-groupe distingué de Γ, auquel cas $\mathrm{Gal}(k'|k) \cong \mathrm{Gal}(\mathrm{K}|k)/\mathrm{Gal}(\mathrm{K}|k')$. Enfin, si H est un sous-groupe ouvert de Γ, il existe par hypothèse une extension galoisienne finie k' de k dans K telle que $\mathrm{Gal}(\mathrm{K}|k') \subset \mathrm{H}$; on a alors $\mathrm{K}^{\mathrm{H}} \subset k'$ et l'extension $\mathrm{K}^{\mathrm{H}}/k$ est ainsi finie. Noter que l'on a

$$(\Gamma : \mathrm{H}) = (\mathrm{Gal}(k'|k) : \mathrm{Gal}(k'|\mathrm{K}^{\mathrm{H}}) = [k^{\mathrm{H}} : k].$$

□

4. Reformulation fonctorielle

Soient k un corps, k^{s} une clôture séparable de k et $\Gamma = \mathrm{Gal}(k^{\mathrm{s}}|k)$ le groupe de Galois absolu de k. La théorie de Galois peut se reformuler sous la forme d'une équivalence de catégories.

4.1. Algèbres étales

Définition 4.1. — *Une k-algèbre finie* A *est dite*

(i) diagonalisable *s'il existe un nombre entier $n \geqslant 1$ tel que* A *soit isomorphe à la k-algèbre produit k^n ;*

(ii) étale *s'il existe une extension* K *de k telle que la* K*-algèbre* $\mathrm{A} \otimes_k \mathrm{K}$ *soit diagonalisable. On dit alors que* K diagonalise A.

On désigne par $k - \mathbf{alg}_{\mathbf{f}}^{\mathbf{t}}$ la catégorie dont
- les objets sont les k-algèbres étales ;
- les flèches sont les homomorphismes de k-algèbres

Lemme 4.2. — *Soit* B *une k-algèbre, non nécessairement commutative. Toute famille $\mathscr{F} \subset \mathrm{Hom}_{k-\mathbf{vect}}(\mathrm{B}, k)$ constituée d'homomorphismes d'algèbres est libre.*

Démonstration. Si $\mathscr{F}$ n'est pas libre, considérons une relation de dépendance linéaire non triviale faisant intervenir un nombre minimal d'éléments de $\mathscr{F}$. Cette relation peut s'écrire sous la forme

$$\lambda_1\sigma_1 + \ldots + \lambda_n\sigma_n = 0,$$

où $n \geqslant 2$, $\lambda_i \neq 0$ pour tout i et $\sigma_i \neq \sigma_j$ si $i \neq j$. Quel que soit $s \in \mathrm{B}$, cette relation fournit l'identité

$$\lambda_1\sigma_1(s)\sigma_1 + \ldots + \lambda_n\sigma_n(s)\sigma_n = 0$$

puis

$$\lambda_2(\sigma_1(s) - \sigma_2(s))\sigma_2 + \ldots + \lambda_n(\sigma_1(s) - \sigma_n(s))\sigma_n = 0$$

par combinaison linéaire. Comme $\sigma_1 \neq \sigma_2$, on peut choisir $s \in \mathrm{B}$ tel que $\sigma_1(s) \neq \sigma_2(s)$ et on obtient de la sorte une relation de dépendance linéaire non triviale contredisant la minimalité de la relation initiale. □

Lemme 4.3. — *Soit* A *une k-algèbre finie diagonalisable (resp. étale). Toute sous-k-algèbre et toute k-algèbre quotient de* A *est diagonalisable (resp. étale).*

Démonstration. □

Proposition 4.4. — *Soit* A *une k-algèbre finie.*

(i) Pour toute extension K/k*, le cardinal de l'ensemble* $\mathrm{Hom}_{k-\mathbf{alg}}(\mathrm{A}, \mathrm{K})$ *est majoré par* $[\mathrm{A} : k]$. *Pour qu'il y ait égalité, il faut et il suffit que* K *diagonalise* A.

(ii) Si A *est une k-algèbre étale, elle est diagonalisée par une extension finie séparable de k.*

Démonstration. (i) Posons

$$\mathrm{X} = \mathrm{Hom}_{k-\mathbf{alg}}(\mathrm{A}, \mathrm{K}) = \mathrm{Hom}_{k-\mathbf{alg}}(\mathrm{A} \otimes_k \mathrm{K}, \mathrm{K})$$

et considérons l'application K-linéaire canonique

$$u : \mathrm{Hom}_{\mathbf{ens}}(\mathrm{X}, \mathrm{K}) \to \mathrm{Hom}_{k-\mathbf{vect}}(\mathrm{A}, \mathrm{K}), \quad f \mapsto \sum_{\sigma \in \mathrm{X}} f(\sigma)\sigma.$$

Il s'agit d'une application injective en vertu du lemme précédent et l'application contragrédiente $u^{\vee}$ s'identitifie à l'homomorphisme de K-algèbres

$$\mathrm{A} \otimes_k \mathrm{K} \to \bigoplus_{\sigma \in \mathrm{X}} \mathrm{K}e_{\sigma}$$

envoyant $a \otimes \lambda$ sur $\sum_{\sigma \in \mathrm{X}} \lambda \sigma(a) e_\sigma$.

La majoration $|\mathrm{X}| \leqslant [\mathrm{A} : k]$ découle de l'injectivité de u et il y a clairement égalité si K diagonalise A. Réciproquement, si $|\mathrm{X}| = [\mathrm{A} : k]$, alors $u^\vee$ est un isomorphisme et donc A est diagonalisée par K.

(ii) Si A est étale, il existe une extension K de k diagonalisant A. Quel que soit l'homomorphisme $\sigma \in \mathrm{Hom}_{k-\mathbf{alg}}(\mathrm{A}, \mathrm{K})$, $\sigma(\mathrm{A})$ est une sous-k-algèbre finie de K, donc une extension finie de k dans K. La k-algèbre $\sigma(\mathrm{A})$ étant un quotient de A, elle est diagonalisée par K ; on a donc $|\mathrm{Hom}_{k-\mathbf{alg}}(\sigma(\mathrm{A}), \mathrm{K})| = [u(\mathrm{A}) : k]$, ce qui prouve que l'extension $\sigma(\mathrm{A})/k$ est séparable. □

***Proposition* — *Les conditions suivantes sont équivalentes pour toute k-algèbre finie* A.**

(i) Pour toute extension K/k*, l'anneau* $\mathrm{A} \otimes_k \mathrm{K}$ *est réduit.*

(ii) L'anneau $\mathrm{A} \otimes_k \overline{k}$ *est réduit.*

(iii) A *est isomorphe au produit d'un nombre fini d'extensions finies séparables de k.*

(iv) A *est étale.*

Démonstration. L'implication $(i) \Rightarrow (ii)$ est triviale.

$(ii) \Longrightarrow (iii)$ Étant donné un élément x de A, la sous-k-algèbre $k[x]$ engendrée par x est canoniquement isomorphe à $k[\mathrm{X}]/(m_x)$, où m_x est le polynôme minimal de x sur k. L'injection $k[\mathrm{X}]/(m_x) \hookrightarrow \mathrm{A}$ induisant une injection $\overline{k}[\mathrm{X}]/(m_x) \cong k[\mathrm{X}]/(m_x) \otimes_k \overline{k} \hookrightarrow \mathrm{A} \otimes_k \overline{k}$, l'anneau $\overline{k}[\mathrm{X}]/(m_x)$ est réduit et il en découle immédiatement que le polynôme m_x est séparable. Soient alors $x_1, \ldots, x_n$ des générateurs de A sur k, de polynômes minimaux respectifs $m_1, \ldots, m_n$ sur k ; l'application canonique $\prod_{i=1}^n k[\mathrm{X}]/(m_i) \to \mathrm{A}$ est un épimorphisme de k-algèbres et il existe un sous-ensemble I de $\{1, \ldots, n\}$ tel que A soit isomorphe à la k-algèbre $\prod_{i \in \mathrm{I}} k[\mathrm{X}]/(m_i)$.

$(iii) \Longrightarrow (iv)$ Si A est isomorphe au produit d'une famille finie $(k_i)_{i \in \mathrm{I}}$ d'extensions finies séparables de k,

$$\mathrm{Hom}_{k-\mathbf{alg}}(\mathrm{A}, \overline{k}) \simeq \prod_{i \in \mathrm{I}} \mathrm{Hom}_{k-\mathbf{alg}}(k_i, \overline{k})$$

est de cardinal $\prod_{i \in \mathrm{I}} [k_i : k] = [\mathrm{A} : k]$ et donc A est diagonalisée par $\overline{k}$.

$(iv) \Longrightarrow (i)$ Soit k_0 une extension de k diagonalisant A. Quelle que soit l'extension K de k, K et k_0 sont contenues dans une extension commune K_0 de k et $\mathrm{A} \otimes_k \mathrm{K}$ est isomorphe à un sous-anneau de $\mathrm{A} \otimes_k \mathrm{K}_0$; comme ce dernier est isomorphe à l'anneau produit K_0^n pour un certain entier $n \geqslant 1$, il est réduit et il en de de même de $\mathrm{A} \otimes_k \mathrm{K}$. □

Remarques

4.2. Γ-ensembles finis

Pour qu'une action de Γ sur un espace discret X soit continue, il faut et il suffit que les stablisateurs soient des sous-groupes ouverts ; comme les sous-groupes ouverts de Γ sont d'indice fini, les orbites sont alors finies.

On désigne par $\Gamma - \mathbf{ens}_0$ la catégorie dont

- les objets sont les ensembles finis munis d'une action continue du groupe Γ ;
- les flèches sont les applications Γ-équivariantes.

Pour tout Γ-ensemble fini X, on désigne par $\mathrm{Hom}_\Gamma(\mathrm{X}, k^{\mathrm{s}})$ l'ensemble des applications Γ-équivariantes de X dans k^{s}. Il s'agit naturellement d'une k-alg|'ebre.
|textbf*Proposition 4 — Soit* X *un* Γ*-ensemble fini [...]*

4.3. Équivalence de Galois

Nous allons définir maintenant deux foncteurs contravariants

$$k-\mathbf{alg}_0 \underset{\mathrm{F}}{\overset{\mathrm{S}}{\rightleftarrows}} \Gamma-\mathbf{ens}_0\ .$$

(i) Pour toute k-algèbre finie étale A, $\mathrm{S}(\mathrm{A})$ est l'ensemble $\mathrm{Hom}_{k-\mathbf{alg}}(\mathrm{A},k^{\mathrm{s}})$ muni de l'action de Γ provenant de son action naturelle sur k^{s}.

(ii) Pour toute flèche $f\in\mathrm{Hom}_{k-\mathbf{alg}}(\mathrm{A},\mathrm{B})$, $\mathrm{S}(f)$ est l'application $\mathrm{S}(\mathrm{B})\to\mathrm{S}(\mathrm{A})$, $u\mapsto u\circ f$.

(i') Pour tout Γ-ensemble fini X, $\mathrm{F}(\mathrm{X})$ est l'ensemble $\mathrm{Hom}_\Gamma(\mathrm{X},k^{\mathrm{s}})$ des applications Γ-équivariantes de X dans k^{s}, que l'on équipe de sa structure naturelle de k-algèbre. Notons que le groupe Γ opère naturellement sur la k^{s}-algèbre des applications de X dans k^{s} via

$$(\gamma u)(x)=\gamma u(\gamma^{-1}x)$$

pour tous $u\in\mathrm{Hom}_{\mathbf{ens}}(\mathrm{X},k^{\mathrm{s}})$, $\gamma\in\Gamma$ et $x\in\mathrm{X}$ et $\mathrm{Hom}_\Gamma(\mathrm{X},k^{\mathrm{s}})$ n'est pas autre chose que la sous-k-algèbre des éléments invariants sous cette action.

- Pour toute flèche $f\in\mathrm{Hom}_{\Gamma-\mathbf{ens}_0}(\mathrm{X},\mathrm{Y})$, $\mathrm{F}(f):\mathrm{F}(\mathrm{Y})\to\mathrm{F}(\mathrm{X})$ est l'homomorphisme de k-algèbres défini par $\mathrm{F}(f)(u)=u\circ f$.

Théorème* — *Les foncteurs* S *et* F *sont des anti-équivalences de catégories réciproques.

Démonstration. Pour toute k-algèbre finie étale A, l'application canonique

$$\mathrm{A}\times\mathrm{Hom}_{k-\mathbf{alg}}(\mathrm{A},k^{\mathrm{s}})\to k^{\mathrm{s}},\ \ (a,\sigma)\mapsto\sigma(a)$$

induit une flèche $\varphi_{\mathrm{A}}:(\mathrm{F}\circ\mathrm{S})(\mathrm{A})$. La collection des φ_{A} définit un morphisme de foncteurs $\varphi:\mathrm{id}\to\mathrm{F}\circ\mathrm{S}$.

Pour tout Γ-ensemble fini X, l'application canonique

$$\mathrm{X}\times\mathrm{Hom}_\Gamma(\mathrm{X},k^{\mathrm{s}})\to k^{\mathrm{s}},\ \ (x,u)\mapsto u(x)$$

induit une flèche $\psi:\mathrm{X}\to(\mathrm{S}\circ\mathrm{F})(\mathrm{X})$. La collection des ψ_{X} définit un morphisme de foncteurs $\psi:\mathrm{id}\to\mathrm{S}\circ\mathrm{F}$.

Il reste à démontrer que φ et ψ sont des isomorphismes de foncteurs.

Pour tout Γ-ensemble fini X, la k^{s}-algèbre

$$\mathrm{F}(\mathrm{X})\otimes_k k^{\mathrm{s}}=\mathrm{Hom}_\Gamma(\mathrm{X},k^{\mathrm{s}})\otimes_k k^{\mathrm{s}}$$

s'identifie canoniquement à $\mathrm{Hom}_\Gamma(\mathrm{X},k^{\mathrm{s}}\otimes_k k^{\mathrm{s}})$ si l'on fait agir Γ sur le premier facteur de $k^{\mathrm{s}}\otimes_k k^{\mathrm{s}}$ et si l'on utilise le second facteur pour définir la structure de k^{s}-algèbre. Le fait que X soit fini permet de remplacer k^{s} par une extension galoisienne finie K de k dans k^{s} suffisamment grande :

$$\mathrm{F}(\mathrm{X})\otimes_k\mathrm{K}=\mathrm{Hom}_\Gamma(\mathrm{X},\mathrm{K})\otimes_k\mathrm{K})\otimes_k\mathrm{K}\cong\mathrm{Hom}_\Gamma(\mathrm{X},K\otimes_k\mathrm{K}).$$

Pour toute k-algèbre étale A,

$$(\mathrm{F}\circ\mathrm{S})(\mathrm{A})\otimes_k k^{\mathrm{s}}=\mathrm{Hom}_\Gamma(\mathrm{S}(\mathrm{A}),k^{rms})\otimes_k k^{\mathrm{s}}$$

s'identifie à la k^{s}-algèbre

$$\varphi_{\mathrm{A}}\otimes\mathrm{id}:\mathrm{A}\otimes_k k^{\mathrm{s}}\to(\mathrm{F}\circ\mathrm{S})(\mathrm{A})\otimes_k k^{\mathrm{s}}$$

l'unique application k^{s}-linéaire

$$\mathrm{A}\otimes_k k^s\to\bigoplus_{\sigma\in\mathrm{S}(\mathrm{A})}k^{\mathrm{s}}e_\sigma$$

envoyant $a\otimes 1$ sur $\sum_{\sigma\in\mathrm{S}(\mathrm{A})}\sigma(a)e_\sigma$ est un isomorphisme de k^{s}-algèbres.