Théorie de Galois

Jean-François Dat

2023-2024

La "théorie de Galois" moderne est l'étude des extensions de corps et de leurs groupes d'automorphismes. Elle est née d'un problème bien concret que se posaient les mathématiciens du 19^{me} siècle, qui était de savoir si toutes les "équations algébriques" étaient "résolubles par radicaux". En d'autres termes, tout polynôme irréductible de $\mathbb{Q}[X]$ admet-il une solution (dans $\mathbb{C}$) qui s'exprime avec les opérations $+, -, \times, \div$ et $\sqrt[n]{x}$? Les formules classiques du trinôme, de Cardan (troisième degré) et Ferrari (quatrième degré) montraient que c'était possible jusqu'en degré 4, mais Abel a exhibé un polynôme de degré 5 pour lequel ce n'était pas possible. Galois a ensuite compris exactement quand c'est possible. En fait, il est même rare que ce soit possible en degré $\geqslant 5$. Pour ce faire, Galois a étudié les ensembles de symétries des solutions d'équations polynomiales (que l'on appelle maintenant "groupes de Galois") et a remarqué que la solubilité par radicaux d'une équation polynomiale était équivalente à la résolubilité de son groupe de symétries (au sens de la théorie des groupes moderne, qui n'existait pas à l'époque). Le groupe de symétrie d'une équation de degré n se plonge dans le groupe symétrique $\mathfrak{S}_n$. Pour $n < 5$, le groupe $\mathfrak{S}_n$ est résoluble, ce qui explique l'existence des formules classiques. Par contre le groupe $\mathfrak{A}_5$ est simple et n'est donc pas résoluble et Galois a justement exhibé une équation dont le groupe de symétrie est $\mathfrak{A}_5$.

1 Extensions de corps

1.1 Quelques définitions

1.1.1 Définition.– *Soit k un corps. Une "extension" K de k est un corps K muni d'un morphisme de corps $k \longrightarrow K$.*

Remarquons qu'un morphisme de corps est simplement un morphisme d'anneaux, donc une extension de k n'est rien d'autre qu'une k-algèbre qui est un corps. Le terme "extension" se justifie par le fait qu'un morphisme de corps est toujours injectif. On abuse souvent en notant simplement $k \subset K$. Une *sous-extension* de K est alors un sous-corps K' de K qui contient k.

Notation. – Soit $k \subset K$ une extension de corps et $\alpha \in K$. On notera
— $k[\alpha]$ la sous-k-algèbre de K engendrée par α.

— $k(\alpha)$ la sous-extension de K engendrée par α.

Comme d'habitude "engendrée" signifie "la plus petite contenant α". Concrètement, $k[\alpha]$ est l'image de l'unique morphisme de k-algèbres $k[X] \longrightarrow K$ qui envoie X sur α, donc $k[\alpha]$ est engendrée, en tant que k-module, par les puissances de α. Comme on a évidemment $k[\alpha] \subset k(\alpha)$, on voit que $k(\alpha) = \mathrm{Frac}(k[\alpha])$. En revanche, $k(\alpha)$ *n'est pas toujours l'image d'un morphisme* $k(X) \longrightarrow K$.

Exemple. – $k = \mathbb{Q} \subset K = \mathbb{C}$, $\alpha = i$. Dans ce cas, $\mathbb{Q}[i] = \mathbb{Q} \oplus \mathbb{Q}i$ est un corps, donc $\mathbb{Q}[i] = \mathbb{Q}(i)$ est de dimension 2 sur $\mathbb{Q}$ alors que $\mathbb{Q}(X)$ est de dimension infinie sur $\mathbb{Q}$. Comme un morphisme de corps est injectif, il n'y a pas de morphisme de corps $\mathbb{Q}(X) \longrightarrow \mathbb{Q}(i)$.

1.1.2 *Alternative algébrique/transcendant.*

Proposition. – *Soit $k \subset K$ une extension de corps et $\alpha \in K$. Notons $\varphi_\alpha : k[X] \longrightarrow K$ le morphisme de k-algèbres qui envoie X sur α. On a alors l'alternative suivante :*

i) Soit φ_α est injectif, auquel cas il induit un isomorphisme $k[X] \xrightarrow{\sim} k[\alpha]$ qui se prolonge uniquement en un isomorphisme $k(X) \xrightarrow{\sim} k(\alpha)$. En particulier, $k[\alpha]$ et $k(\alpha)$ sont de dimension infinie sur k.

ii) Soit φ_α n'est pas injectif, auquel cas on a les propriétés suivantes :

(a) Son noyau est engendré par un unique polynôme unitaire irréductible $f_\alpha \in k[X]$

(b) φ_α induit un isomorphisme $k[X]/(f_\alpha) \xrightarrow{\sim} k[\alpha]$

(c) $k[\alpha]$ est de dimension finie sur k, égale au degré $\deg(f_\alpha)$

(d) $k(\alpha) = k[\alpha]$.

Démonstration. Dans le cas i), les seules choses à prouver sont l'existence et l'unicité du prolongement de φ_α en un isomorphisme $k(X) \xrightarrow{\sim} k(\alpha)$. Mais celles-ci découlent de la propriété universelle du corps des factions, puisque φ_α envoie tout élément $f \in k[X]$ non nul sur un élément inversible dans K.

Dans le cas ii), le fait que $\mathrm{Ker}(\varphi_\alpha)$ est engendré par un seul polynôme provient du fait que $k[X]$ est principal. Ce polynôme est bien défini à multiplication par un inversible près ; on peut le rendre unitaire en multipliant par un $\lambda \in k^\times$, et cela le rend unique puisque $k[X]^\times = k^\times$. Par ailleurs, φ_α induit un isomorphisme $k[X]/\mathrm{Ker}(\varphi_\alpha) \xrightarrow{\sim} k[\alpha]$ (propriété universelle des quotients), et puique $k[\alpha] \subset K$ est intègre, $\mathrm{Ker}(\varphi_\alpha)$ est un idéal premier et donc f_α est irréductible. On a donc prouvé (a) et (b). Le point (b) implique que, en notant $n = \deg f_\alpha$, la famille $\{1, \alpha, \cdots \alpha^{n-1}\}$ est une k-base du k-espace vectoriel $k[\alpha]$. Quant au point (d), il s'agit se prouver que $k[\alpha]$ est un corps. On peut le voir de deux manières : soit en rappelant que tout idéal premier de $k[X]$ est maximal, soit en invoquant le lemme d'intérêt indépendant suivant :

Lemme. – *Une algèbre A intègre de dimension finie sur un corps k est un corps.*

Démonstration. La multiplication par $x \in A \setminus \{0\}$ est un endomorphisme k-linéaire injectif de A, donc bijectif par le théorème du rang. Il existe en particulier y tel que $xy = 1$. □

□

DÉFINITION. – *Dans le contexte de la proposition, on dit que α est* transcendant sur *k dans le cas i), et on dit qu'il est* algébrique sur *k dans le cas ii). Dans ce dernier cas, f_α est appelé* polynôme minimal *de α.*

Exemples. – Considérons l'extension $\mathbb{Q} \subset \mathbb{C}$. Les nombres complexes i, j ou $\sqrt{2}$ sont algébriques sur $\mathbb{Q}$. Les premiers nombres transcendants construits furent les "nombres de Liouville", qui admettent de bonnes approximations par les nombres rationnels. Lindemann prouva ensuite que les nombres de la forme e^a avec a algébrique sont transcendants. Comme $e^{i\pi} = 1$, cela implique que π est transcendant, ce qui montre au passage l'impossibilité de la "quadrature du cercle". Par contre, on ne sait toujours pas si des nombres comme e^π ou $\pi + e$ sont transcendants.

Remarque. – En fait il y a "beaucoup plus" de nombres complexes transcendants qu'il n'y en a d'algébriques. Plus précisément, le sous-ensemble $\overline{\mathbb{Q}} \subset \mathbb{C}$ formé de tous les nombres algébriques est dénombrable. En effet, chaque nombre algébrique annule un polynôme à coefficients entiers. Ces polynômes sont en bijection avec les suites presque nulles d'entiers, et ces suites forment un ensemble dénombrable (exercice !). Il s'ensuit que l'ensemble $\mathbb{C} \setminus \overline{\mathbb{Q}}$ des nombres transcendants est indénombrable.

1.1.3 *Indépendance algébrique.* Soit $k \subset K$ une extension de corps, et soit $(\alpha_i)_{i\in I}$ une famille d'éléments de K indexée par un ensemble I. Comme dans le paragraphe précédent, on note

— $k[(\alpha_i)_{i\in I}]$ la sous-k-algèbre de K engendrée par les α_i

— $k((\alpha_i)_{i\in I})$ la sous-extension de K engendrée par les α_i.

DÉFINITION. – *On dit que la famille $(\alpha_i)_{i\in I}$ est* algébriquement indépendante *sur k si le morphisme de k-algèbres $k[(X_i)_{i\in I}] \longrightarrow K$ qui envoie X_i sur α_i pour tout i est injectif.*

Lorsque les α_i sont algébriquement indépendants, le morphisme de la définition se prolonge uniquement en un isomorphisme $k((X_i)_{i\in I}) := \mathrm{Frac}(k[(X_i)_{i\in I}]) \xrightarrow{\sim} k((\alpha_i)_{i\in I})$.

Exemple. – Si l'on prend "au hasard" n éléments dans $\mathbb{C}$, ils ont toutes les chances d'être algébriquement indépendants. Par contre, il est très difficile de prouver l'indépendance de nombres donnés à l'avance, par exemple on ne sait pas si e et π sont algébriquement indépendants. Il est conjecturé que les valeurs de la fonction ζ de Riemann aux entiers impairs $\zeta(3), \zeta(5)$, etc... sont algébriquement indépendantes (sur $\mathbb{Q}$). La célébrité du théorème d'Apery, qui montre "simplement" l'irrationnalité de $\zeta(3)$, donne une idée de l'envergure de cette conjecture.

Remarque. – Si $I = I_1 \sqcup I_2$ (réunion disjointe), on a $k((\alpha_i)_{i\in I}) = k((\alpha_i)_{i\in I_1})((\alpha_i)_{i\in I_2})$. De plus, la famille $(\alpha_i)_{i\in I}$ est algébriquement indépendante sur k si et seulement si la famille $(\alpha_i)_{i\in I_1}$ est algébriquement indépendante sur k et la famille $(\alpha_i)_{i\in I_2}$ est algébriquement indépendante sur $k((\alpha_i)_{i\in I_1})$.

1.1.4 DÉFINITION.– *Une extension $k \subset K$ est dite :*
— finie *si K est de dimension finie comme k-ev. On note alors $[K : k] := \dim_k(K)$ et on l'appelle* degré *de K sur k.*
— algébrique *si tout élément $\alpha \in K$ est algébrique sur k.*
— de type fini *si K est engendrée, en tant qu'extension de corps, par une famille finie d'éléments.*
— monogène *si K est engendrée, en tant qu'extension de corps, par un seul élément.*
— transcendante pure *si K est engendrée par une famille algébriquement indépendante sur k.*

Remarque. – Vu les définitions, une extension finie est algébrique et une extension est algébrique si et seulement si elle est réunion de sous-extensions finies. De plus, une extension algébrique est finie si et seulement si elle est de type fini. Enfin, si α est algébrique sur k, alors $k(\alpha)$ est finie et $[k(\alpha) : k] = \deg(f_\alpha)$.

Exemple. – L'extension $k \subset k(X_1, \cdots, X_n)$ est de type fini et transcendante pure.

1.1.5 *Le Nullstellensatz.* On pourrait penser qu'une extension $k \subset K$ puisse avoir une propriété intermédiaire entre être *finie* et *de type fini*, à savoir que *K soit une k-algèbre de type fini*. Mais le théorème suivant montre qu'on n'obtient rien de nouveau.

THÉORÈME. – *Soit $k \subset K$ une extension de corps telle que K soit une k-algèbre de type fini. Alors $k \subset K$ est une extension finie (i.e. K est de dimension finie sur k).*

Démonstration. On raisonne par récurrence sur le nombre n de générateurs de K comme k-algèbre. Si $n = 0$, il n'y a rien à montrer. Supposons donc $n \geqslant 1$ et choisissons $\alpha_1, \cdots, \alpha_n$ tels que $K = k[\alpha_1, \cdots, \alpha_n]$. On a a fortiori $K = k(\alpha_1)[\alpha_2, \cdots, \alpha_n]$, donc notre hypothèse de récurrence assure que l'extension $k(\alpha_1) \subset K$ est finie et il nous reste à montrer que α_1 est algébrique sur k. Choisissons une base $\beta_1 := 1, \beta_2, \cdots, \beta_m$ de K sur $k(\alpha_1)$, se sorte que

$$K = k(\alpha_1)\beta_1 \oplus \cdots \oplus k(\alpha_1)\beta_m.$$

La multiplication dans K est déterminée par les formules $\beta_i\beta_j = \sum_{k=1}^m a_{ijk}\beta_k$ avec $a_{ijk} \in k(\alpha_1)$. Par ailleurs, écrivons chaque $\alpha_1, \cdots, \alpha_n$ sous la forme $\alpha_i = \sum_{j=1}^m b_{ij}\beta_j$ avec $b_{ij} \in k(\alpha_1)$. Soit alors $A := k[a_{ijk}, b_{ij}]_{i,j,k}$ la sous-k-algèbre de $k(\alpha_1)$ engendrée par les a_{ijk} et les b_{ij}. On a manifestement $k[\alpha_1, \cdots, \alpha_n] \subset A\beta_1 \oplus \cdots \oplus A\beta_m$. Mais comme $k[\alpha_1, \cdots, \alpha_n] = K$, on en déduit que $A = k(\alpha_1)$, et en particulier que *$k(\alpha_1)$ est une k-algèbre de type fini.* Pour conclure que α_1 est nécessairement algébrique, il suffit donc de montrer qu'un corps de fractions rationnelles $k(X)$ n'est pas une k-algèbre de type fini. En effet, si $\frac{f_1}{g_1}, \cdots, \frac{f_r}{g_r}$ sont des fractions rationnelles, et si g est n'importe quel polynôme premier aux g_i (par exemple $g = g_1g_2 \cdots g_i + 1$), alors $\frac{1}{g} \notin k[\frac{f_1}{g_1}, \cdots, \frac{f_r}{g_r}] \subset k(X)$. □

Voici une formulation équivalente mais plus "géométrique".

THÉORÈME. – *Si $\mathfrak{m}$ est un idéal maximal de $k[X_1, \cdots, X_n]$, alors son corps résiduel $K = k[X_1, \cdots, X_n]/\mathfrak{m}$ est une extension finie de k.*

Application géométrique : ici on prend $k = \mathbb{C}$ et on admet que ce corps est "algébriquement clos", au sens où toute extension algébrique de $\mathbb{C}$ est égale à $\mathbb{C}$. Nous allons justifier le nom *Nullstellensatz* qui signifie "théorème des zéros" en allemand. Soient $f_1, \cdots, f_r \in \mathbb{C}[X_1, \cdots, X_n]$ des polynômes en n variables. On note

$$V_{f_1,\cdots,f_r} := \{z = (z_1, \cdots, z_n) \in \mathbb{C}^n, \forall i = 1, \cdots, r,\ f_i(z) = 0\}$$

le lieu d'annulation de ces polynômes dans $\mathbb{C}^n$. Toute une branche des mathématiques, appelée *géométrie algébrique*, est née de l'étude de ces lieux (d'ailleurs appelés "sous-ensembles algébriques"). La première question que se sont posée les mathématiciens est de savoir quand ce lieu est non vide. Hilbert y a répondu de la manière suivante :

COROLLAIRE. – *On a $V_{f_1,\cdots,f_r} \neq \emptyset$ si et seulement si l'idéal $(f_1, \cdots, f_r) \subset \mathbb{C}[X_1, \cdots, X_n]$ engendré par les f_i est propre (i.e. différent de l'idéal unité).*

Démonstration. Notons $I := (f_1, \cdots, f_r)$ et remarquons que $V_{f_1,\cdots,f_r} = V_I$ où

$$V_I := \{z \in \mathbb{C}^n, \forall f \in I, f(z) = 0\}.$$

Si I est l'idéal unité, on a $V_I = \emptyset$ car l'unité 1 ne s'annule nulle part et appartient à I. Supposons donc I propre. Dans le cours d'algèbre commutative, on montre en utilisant le lemme de Zorn qu'il existe au moins un idéal maximal $\mathfrak{m}$ de $\mathbb{C}[X_1, \cdots, X_n]$ contenant I. D'après le théorème précédent, le corps résiduel $\mathbb{C}[X_1, \cdots, X_n]/\mathfrak{m}$ est une extension finie de $\mathbb{C}$. Puisque $\mathbb{C}$ est algébriquement clos, on a donc $\mathbb{C}[X_1, \cdots, X_n]/\mathfrak{m} \xrightarrow{\sim} \mathbb{C}$. Soient alors $z_1, \cdots, z_n$ les images de $X_1, \cdots, X_n$ dans $\mathbb{C}$ (i.e. leurs résidus modulo $\mathfrak{m}$). Pour tout polynôme $g \in \mathbb{C}[X_1, \cdots, X_n]$, on a donc $\bar{g} = g(z_1, \cdots, z_n)$ dans $\mathbb{C}$ (où $\bar{g}$ est le résidu de g modulo $\mathfrak{m}$). En particulier, si $g \in \mathfrak{m}$, on a donc $g(z_1, \cdots, z_n) = 0$. Ainsi $(z_1, \cdots, z_n) \in V_{\mathfrak{m}} \subset V_I$ donc $V_I \neq \emptyset$. □

Remarque. – Au passage, la preuve montre que $V_{f_1,\cdots,f_r}$ s'identifie à l'ensemble des idéaux maximaux de $\mathbb{C}[X_1, \cdots, X_n]$ contenant les f_i, c'est-à-dire, après passage au quotient, à l'ensemble des idéaux maximaux de l'anneau $\mathbb{C}[X_1, \cdots, X_n]/(f_1, \cdots, f_r)$.

1.1.6 *Clôture algébrique relative.*

LEMME. – *Soit $k \subset k' \subset K$ une tour d'extensions de corps.*

i) K est finie sur k si et seulement si K est finie sur k' et k' est finie sur k. De plus, on a dans ce cas l'égalité $[K : k] = [K : k'][k' : k]$.

ii) K est algébrique sur k si et seulement si K est algébrique sur k' et k' est algébrique sur k.

Démonstration. i) L'équivalence est claire. Pour l'égalité, posons $n = [K : k']$ et $m = [k' : k]$. Alors $K \simeq k'^n$ en tant que k'-ev, et $k' \simeq k^m$ en tant que k-ev. Il s'ensuit que $K \simeq (k^m)^n = k^{mn}$ en tant que k-ev. En pratique, si $\alpha_1, \cdots, \alpha_n$ est une base de K sur k' et si $\beta_1, \cdots, \beta_m$ est une base de k' sur k, alors $\{\alpha_i\beta_j, i = 1, \cdots, n; j = 1, \cdots, m\}$ est une base de K sur k.

ii) L'implication $\Rightarrow$ est claire. Pour l'autre implication, soit $\alpha \in K$. Notons $f_\alpha = X^n + a_1 X^{n-1} + \cdots + a_n \in k'[X]$ son polynôme minimal sur k'. Ainsi α est algébrique sur le corps $k(a_1, \cdots, a_n)$. Or chacun des a_i est algébrique sur k, donc $k(a_1, \cdots, a_n)$ est fini sur k (par une récurrence à l'aide de i)). Il s'ensuit que $k(a_1, \cdots, a_n, \alpha)$ est fini sur k et en particulier α est algébrique sur k. □

La proposition suivante montre que toute extension contient une unique sous-extension algébrique maximale.

PROPOSITION. – *Soit $k \subset K$ une extension de corps. L'ensemble K_{alg} de tous les éléments de K algébriques sur k est un corps. On l'appelle* clôture algébrique de k dans K.

Démonstration. Soient $\alpha, \beta \in K$ algébriques sur k. Alors $k(\alpha)$ est fini sur k et, comme β est a fortiori algébrique sur $k(\alpha)$, $k(\alpha, \beta)$ est fini sur $k(\alpha)$. Il s'ensuit que $k(\alpha, \beta)$ est fini sur k. En particulier, $\alpha + \beta$ et $\alpha\beta$ sont algébriques sur k. □

Exemple. – L'ensemble $\overline{\mathbb{Q}}$ introduit plus haut est la clôture algébrique de $\mathbb{Q}$ dans $\mathbb{C}$.

1.1.7 *Bases de transcendance et degré de transcendance.* Une extension non algébrique $k \subset K$ contient toujours une sous-extension $k \subset K'$ transcendante pure et telle que $K' \subset K$ soit algébrique. En effet, il suffit de prendre pour K' l'extension engendrée par une famille algébriquement indépendante maximale (pour l'inclusion). L'exemple suivant montre que K' est loin d'être unique.

Exemple. – Supposons $k = \mathbb{C}$. Il est facile de voir que l'élément $X^2 - Y^3 + 1$ de $\mathbb{C}[X, Y]$ est irréductible. Puisque $\mathbb{C}[X, Y]$ est un anneau factoriel, cet élément engendre donc un idéal premier, i.e. la $\mathbb{C}$-algèbre $A = \mathbb{C}[X, Y]/(X^2 - Y^3 + 1)$ est intègre. Soit $K = \text{Frac}(A)$ son corps des fractions. On peut l'écrire $K = \mathbb{C}(Y)[X]/(X^2 - Y^3 + 1)$, ce qui montre que K est une extension de degré 2 du corps $\mathbb{C}(Y)$ transcendant pur sur $\mathbb{C}$. Mais on peut aussi l'écrire $K = \mathbb{C}(X)[Y]/(Y^3 - X^2 - 1)$, ce qui montre qu'il est de degré 3 sur le corps $\mathbb{C}(X)$ transcendant pur.

On voit néanmoins dans cet exemple que les sous-corps purement transcendants sont à une indéterminée. Ceci se généralise ainsi.

THÉORÈME. – *Soit $k \subset K$. Les familles maximales d'éléments de K algébriquement indépendants sur k sont toutes de même cardinal. On les appelle* bases de transcendance de K sur k *et leur cardinal est appelé* degré de transcendance *de l'extension $k \subset K$ et noté* $\text{deg.tr.}(K/k)$.

Démonstration. Nous ne prouvons ce résultat que lorsque K admet une famille algébriquement indépendante maximale *finie*. Supposons donc qu'il existe des éléments algébriquement indépendants $\alpha_1, \cdots, \alpha_n$ tels que K est algébrique sur $k(\alpha_1, \cdots, \alpha_n)$. Soit alors $\beta_1, \cdots, \beta_m$ une autre famille algébriquement indépendante. Il nous suffira de montrer que $m \leqslant n$. Nous allons utiliser plusieurs fois le lemme suivant.

LEMME. – *Soient α, β deux éléments de K, chacun transcendant sur un sous-corps k' mais algébriquement liés sur ce sous-corps. Alors α est algébrique sur $k'(\beta)$.*

Démonstration. Il existe un polynôme irréductible $f \in k'[X,Y]$ tel que $f(\alpha,\beta)=0$. Développons $f = \sum_{k\in\mathbb{N}} g_k(Y)X^k$ avec $g_k \in k'[Y]$. Puisque f est non nul, les polynômes g_k sont non tous nuls. Puisque β est transcendant, les éléments $g_k(\beta)$ sont donc eux aussi non tous nuls. Il s'ensuit que α est racine d'un polynôme non nul à coefficients dans $k'(\beta)$. □

Revenons à la preuve du théorème. Posons $I_0 := \{1, \cdots, n\}$. Puisque β_1 est transcendant sur k, l'ensemble

$$\{I \subset I_0, \beta_1 \text{ est transcendant sur } k((\alpha_i)_{i\in I})\}$$

contient $I = \emptyset$ et est donc non vide. Choisissons I_1 maximal dans cet ensemble. Puisque β_1 est algébrique sur $k(\alpha_1, \cdots, \alpha_n)$, on a $I_1 \subsetneq I_0$. Pour chaque $j \in I_0 \setminus I_1$, les éléments β_1 et α_j sont algébriquement liés sur $k((\alpha_i)_{i\in I_1})$ et le lemme nous assure que α_j est algébrique sur $k(\beta_1)((\alpha_i)_{i\in I_1})$. Il s'ensuit que K est algébrique sur $k(\beta_1)((\alpha_i)_{i\in I_1})$.

En particulier, β_2 est algébrique sur $k(\beta_1)((\alpha_i)_{i\in I_1})$, mais transcendant sur $k(\beta_1)$. Donc il existe $I_2 \subsetneq I_1$ maximal tel que β_2 est transcendant sur $k(\beta_1)((\alpha_i)_{i\in I_2})$ et, comme ci-dessus, K est alors algébrique sur $k(\beta_1,\beta_2)((\alpha_i)_{i\in I_2})$. Par récurrence, on trouve un sous-ensemble I_m de I_0 tel que K est algébrique sur $k(\beta_1, \cdots, \beta_m)((\alpha_i)_{i\in I_m})$. Comme la suite $I_0 \supsetneq I_1 \supsetneq \cdots \supsetneq I_m$ est strictement décroissante, on a $0 \leqslant |I_m| \leqslant n-m$, ce qui montre que $m \leqslant n$. □

Exemple. – Comme $\mathbb{Q}(X_1, \cdots, X_n)$ est dénombrable pour tout n, on voit que $\mathbb{C}$ est de degré de transcendance infini sur $\mathbb{Q}$.

LEMME. – *Soit $k \subset k' \subset K$ deux extensions de corps. K est de degré de transcendance fini sur k si et seulement si il en est de même de k' sur k et de K sur k'. De plus, on a alors* $\text{deg.tr.}(K/k) = \text{deg.tr.}(K/k') + \text{deg.tr.}(k'/k)$.

Démonstration. Clair. □

1.2 Corps algébriquement clos, clôtures algébriques

1.2.1 DÉFINITION.– *Un corps K est dit algébriquement clos si les conditions équivalentes suivantes sont satisfaites :*

— *tout polynôme $f \in K[X]$ possède une racine dans K*

— *tout polynôme $f \in K[X]$ est scindé*

— *les éléments irréductibles de $K[X]$ sont les polynômes de degré 1.*

On rappelle qu'une "racine de f dans K" est un élément $x \in K$ tel que $(X-x)|f$ (ce qui équivaut à $f(x)=0$), et que "f est scindé" signifie que f se factorise $f = \lambda(X-\alpha_1)\cdots(X-\alpha_n)$. On rappelle aussi le célèbre théorème suivant.

THÉORÈME. – $\mathbb{C}$ *est algébriquement clos.*

Démonstration. Soit $f = X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n$. Raisonnons par l'absurde, et supposons que f ne s'annule pas sur $\mathbb{C}$. Montrons que $z \mapsto |f(z)|$ atteint son minimum sur $\mathbb{C}$. On a $f(0) = a_n \neq 0$. Comme $\lim_{|z|\to+\infty} |f(z)| = +\infty$, il existe donc $R > 0$ tel que $|z| > R \Rightarrow |f(z)| > |a_n|$. Comme le disque $D = \{z \in \mathbb{C}, |z| \leqslant R\}$ est compact, $|f|$ y atteint son minimum. Celui-ci est inférieur à $|f(0)| = |a_n|$ et est donc le minimum de $|f|$ sur $\mathbb{C}$.

Quitte à faire un changement de variable $X \mapsto X+z_0$ on peut supposer que f atteint son minimum en 0. Quittes à multiplier f par une constante, on peut supposer que $f(0) = 1$. Alors, si k est l'ordre d'annulation en 0 de $f - 1$, on a $f(z) = 1 + a_{n-k}z^k + o(z^k)$ au voisinage de $z = 0$. Soit maintenant θ tel que $a_{n-k}e^{ik\theta} = -|a_{n-k}|$ (ie $k\theta = \pi - \arg(a_{n-k})$). Alors $f(re^{i\theta}) = 1 - |a_{n-k}|r^k + o(r^k)$, et donc $|f(re^{i\theta})| < 1$ pour r assez petit non nul, ce qui contredit le fait que 1 est le minimum de $|f|$. □

1.2.2 Définition.– *Soit k un corps. Une* clôture algébrique de k *(absolue) est une extension algébrique $k \subset \overline{k}$ avec $\overline{k}$ algébriquement clos.*

Lemme. – *Soit $k \subset K$ une extension avec K algébriquement clos. Alors la clôture algébrique (relative) K_{alg} de k dans K est une clôture algébrique (absolue) de k.*

Démonstration. Par construction, K_{alg} est algébrique sur k. Il s'agit donc de montrer que K_{alg} est algébriquement clos. Soit donc $f \in K_{\text{alg}}[X]$. Puisque K est algébriquement clos, f admet une racine α dans K. Cet élément α est algébrique sur K_{alg}, et donc aussi sur k. Donc il appartient à K_{alg}. □

Exemple. – $\overline{\mathbb{Q}}$ est une clôture algébrique de $\mathbb{Q}$.

1.2.3 Définition.– *Si on a deux extensions $k \subset K$ et $k \subset K'$, un* morphisme d'extensions *est un morphisme k-linéaire de corps $K \longrightarrow K'$. Il induit donc l'identité sur k. Comme un tel morphisme est toujours injectif, on parle aussi de* plongement *ou plus précisément de k-*plongement *si on veut préciser le corps de base.*

Par définition, on a donc

$$\{k\text{-plongements } K \longrightarrow K'\} = \mathrm{Hom}_{k-\mathrm{alg}}(K, K').$$

L'exemple fondamental est celui des extensions monogènes :

1.2.4 Lemme.– *Supposons que $K = k(\alpha)$ est une extension algébrique de k engendrée par un élément $\alpha \in K$. Alors l'application* $\mathrm{ev}_\alpha : \iota \mapsto \iota(\alpha)$ *induit une bijection*

$$\{k\text{-plongements } k[\alpha] \longrightarrow K'\} \xrightarrow{\sim} \{\beta \in K', f_\alpha(\beta) = 0\}.$$

Démonstration. On a un isomorphisme $k[X]/(f_\alpha) \xrightarrow{\sim} K$, $X \mapsto \alpha$. Partons donc de la bijection

$$\mathrm{ev}_X : \mathrm{Hom}_{k-\mathrm{alg}}(k[X], K') \xrightarrow{\sim} K', \ \varphi \mapsto \mathrm{ev}_X(\varphi) := \varphi(X)$$

donnée par la propriété universelle des polynômes. Par la propriété universelle des quotients, on peut identifier $\mathrm{Hom}_{k-\mathrm{alg}}(k(\alpha), K')$ au sous-ensemble de $\mathrm{Hom}_{k-\mathrm{alg}}(k[X], K')$ formé des morphismes φ tels que $\varphi(f_\alpha) = 0$. Or, pour tout $f \in k[X]$, on a $f(\varphi(X)) = \varphi(f)$, donc la bijection ci-dessus envoie $\mathrm{Hom}_{k-\mathrm{alg}}(k(\alpha), K')$ sur le sous-ensemble de K' formé des $\beta \in K'$ tels que $f_\alpha(\beta) = 0$. □

1.2.5 Proposition.– *Si $k \subset \overline{k}$ est une clôture algébrique de k, alors toute extension algébrique de k se plonge dans $\overline{k}$.*

Démonstration. Soit K une extension algébrique de k et soit $K' \subset K$ une sous-extension munie d'un plongement $\iota : K' \hookrightarrow \overline{k}$. Le point clef est que pour tout $\alpha \in K$, le plongement ι admet un prolongement à $K'(\alpha)$. En effet, cela découle du lemme précédent en remplaçant k par K' (plongé dans $\overline{k}$ via ι) et K' par $\overline{k}$, et en utilisant le fait que le polynôme minimal de α dans $K'[X]$ a une racine dans $\overline{k}$ (qui est algébriquement clos). Remarquons cependant que ce prolongement est loin d'être canonique puiqu'il dépend du choix de la racine x de f_α choisie, et même de α, puisque $K'(\alpha)$ admet certainement d'autres générateurs.

On contourne le problème de non-unicité des prolongements en invoquant le lemme de Zorn. Considérons l'ensemble $\mathcal{P}$ des paires (K', ι') formées d'une sous-extension $K' \subset K$ de k et d'un plongement $\iota : K' \hookrightarrow \overline{k}$. Cet ensemble est non vide puisque (k, i) lui appartient, où i désigne l'inclusion de k dans $\overline{k}$. Il est de plus partiellement ordonné par la relation d'ordre $(K', \iota') \leqslant (K'', \iota'') \Leftrightarrow (K' \subset K''$ et $\iota' = \iota''_{|K'})$. Cet ordre est "inductif", au sens où toute suite croissante possède un majorant. En effet, si $(K'_n, \iota'_n)_{n\in\mathbb{N}}$ est une suite croissante, alors $K' := \bigcup_n K'_n$ est un sous-corps et on définit un plongement ι' en envoyant $x \in K'$ sur $\iota'_n(x)$, qui ne dépend pas du choix de n tel que $x \in K'_n$. Alors la paire (K', ι') majore tous les (K'_n, ι'_n). Maintenant, le lemme de Zorn nous dit alors que tout ensemble ordonnée inductif non vide possède un élément maximal. Soit donc (K', ι') maximal dans $\mathcal{P}$. S'il existait $\alpha \in K \setminus K'$, la construction du début de la preuve contredirait la maximalité de (K', ι'). Donc $K' = K$. □

Corollaire. – *Deux clôtures algébriques $\overline{k}$ et $\overline{k}'$ de k sont isomorphes, en tant qu'extensions de k.*

Démonstration. D'après la proposition, il existe un plongement $\overline{k}' \hookrightarrow \overline{k}$. L'image K de ce plongement est un corps isomorphe à $\overline{k}'$, donc algébriquement clos. Tout élément α de $\overline{k}$ est algébrique sur k, donc a fortiori sur K. Son polynôme minimal f_α sur K est de degré 1 puisque K est algébriquement clos, donc de la forme $X - a_0$. Il s'ensuit que $\alpha = a_0 \in K$, puis que $K = \overline{k}$ et $\overline{k}' \xrightarrow{\sim} \overline{k}$. □

Remarque. – Il n'y a généralement pas d'isomorphisme canonique. Par exemple, $\mathbb{C}$, $\mathbb{R}[X]/(X^2+1)$ et $\mathbb{R}[X]/(X^2+X+1)$ sont des clôtures algébriques de $\mathbb{R}$ mais il n'y a pas d'isomorphisme canonique entre ces corps. On peut paraphraser le corollaire en disant : *une clôture algébrique est unique à isomorphisme **non** unique prés.*

Remarque. – Soit K une extension finie de k. Supposons que K soit monogène et choisissons un élément $\alpha \in K$ tel que $K = k(\alpha)$. Alors, en notant $f_\alpha \in k[X]$ le polynôme minimal de α, le lemme 1.2.4 fournit une bijection $\iota \mapsto \iota(\alpha)$

$$\{\text{Plongements } k\text{-linéaires } \iota : K \hookrightarrow \overline{k}\} \leftrightarrow \{\text{Racines de } f_\alpha \text{ dans } \overline{k}\}.$$

1.2.6 *Construction d'une clôture algébrique.* Nous allons maintenant prouver l'existence de clôtures algébriques pour tout corps k. Commençons par un moyen inductif de construction de corps :

LEMME. – *Soit $k_0 \xrightarrow{\tau_0} k_1 \xrightarrow{\tau_1} \cdots \xrightarrow{\tau_{n-1}} k_n \xrightarrow{\tau_n} \cdots$ une suite de morphismes de corps. Alors il existe un corps k_∞ muni de plongements $\iota_n : k_n \hookrightarrow k_\infty$ tels que $\iota_n \circ \tau_{n-1} = \iota_{n-1}$ pour tout $n > 0$, et qui satisfait la propriété universelle suivante : pour tout corps K et toute collection $\sigma_n : k_n \longrightarrow K$ de plongements telle que $\sigma_n \circ \tau_{n-1} = \sigma_{n-1}$ pour tout $n > 0$, il existe un unique plongement $k_\infty \xrightarrow{\sigma} K$ tel que $\sigma \circ \iota_n = \sigma_n$ pour tout n.*

Démonstration. Si la suite de morphismes donnée était une suite d'inclusions $k_0 \subset k_1 \subset \cdots \subset k_n \subset \cdots$ à l'intérieur d'un "gros" corps $\mathbb{K}$, il suffirait de prendre $k_\infty := \bigcup_n k_n$. La subtilité ici est qu'on se donne des corps "abstraits" non contenus dans un gros corps, et qu'il faut donc construire de façon "externe" leur "réunion".

Pour cela, considérons la somme directe $\bigoplus_{n\in\mathbb{N}} k_n$. C'est un k_0-ev et même une k_0-algèbre sans unité (un idéal de $\prod_{n\in\mathbb{N}} k_n$). Par définition des sommes directes, on a des inclusions $\tilde{\iota}_n : k_n \hookrightarrow \bigoplus_{m\in\mathbb{N}} k_m$ qui envoient un élement $x_n \in k_n$ sur la suite nulle partout sauf au rang n où elle vaut x_n. Soit R le sev engendré par les éléments $\tilde{\iota}_n(\tau_{n-1}(x_{n-1})) - \tilde{\iota}_{n-1}(x_{n-1}) = (0, \cdots, 0, -x_{n-1}, \tau_{n-1}(x_{n-1}), 0, 0, \cdots)$ pour $n \in \mathbb{N}^*$ et $x_{n-1} \in k_{n-1}$. Posons

$$k_\infty := \left(\bigoplus_n k_n\right)/R \quad \text{et} \quad \iota_n : k_n \xrightarrow{\tilde{\iota}_n} \bigoplus_{m\in\mathbb{N}} k_m \twoheadrightarrow k_\infty.$$

Par définition, pour tout $n > 0$ on a $\tilde{\iota}_{n-1}(k_{n-1}) \subset \tilde{\iota}_n(k_n) + R$ donc $\iota_{n-1}(k_{n-1}) \subset \iota_n(k_n)$. Comme on a aussi $k_\infty = \sum_{n\in\mathbb{N}} \iota_n(k_n)$, on en déduit que $k_\infty = \bigcup_n \iota_n(k_n)$. Par ailleurs, grâce à l'injectivité des τ_i on voit que toute suite $(x_m)_{m\in\mathbb{N}}$ dans R admet au moins deux termes non nuls. Il s'ensuit que pour tout n on a $\tilde{\iota}_n(k_n) \cap R = \{0\}$ et donc ι_n est injective. Ainsi ι_n induit un isomorphisme k_0-linéaire de k_n sur son image $\iota_n(k_n)$ pour tout n, et chaque inclusion $\iota_{n-1}(k_{n-1}) \subset \iota_n(k_n)$ correspond au morphisme τ_{n-1} via ces isomorphismes. En d'autres termes le diagramme suivant est commutatif :

$$\begin{array}{ccc} k_n & \xrightarrow[\iota_n]{\sim} & \iota_n(k_n) \\ {\scriptstyle\tau_{n-1}}\uparrow & & \uparrow \\ k_{n-1} & \xrightarrow[\iota_{n-1}]{\sim} & \iota_{n-1}(k_{n-1}) \end{array}$$

On peut maintenant munir le k_0-ev k_∞ d'une multiplication : pour $x, y \in k_\infty$, choisissons n assez grand pour que $x, y \in \iota_n(k_n)$ et posons $xy := \iota_n(\iota_n^{-1}(x)\iota_n^{-1}(y))$. Alors cette définition

ne dépend pas du choix de n et fait de k_∞ une k_0-algèbre. Comme cette algèbre est réunion des sous-corps $\iota_n(k_n)$, c'est un corps.

La propriété universelle de k_∞ muni des ι_n se prouve sur le même principe : si $x \in k_\infty$ est dans l'image de ι_n on pose $\sigma(x) := \sigma_n(\iota_n^{-1}(x))$, et on a tout fait pour que cela ne dépende pas du choix de n. L'unicité de σ découle du fait que $k_\infty = \bigcup_n \iota_n(k_n)$. □

Nous appliquerons ce lemme sous les hypothèses du suivant :

LEMME. – *Avec les notations du lemme précédent. Supposons que pour tout $n \geqslant 0$ et tout polynôme $f_n \in k_n[X]$, le polynôme $\tau_n(f_n) \in k_{n+1}[X]$ admette une racine dans k_{n+1}. Alors k_∞ est algébriquement clos.*

Démonstration. Soit $f \in k_\infty[X]$. Il existe n tel que les coefficients de f soient dans $\iota_n(k_n)$. Alors f est de la forme $\iota_n(f_n)$ pour un (unique) polynôme $f_n \in k_n[X]$. Par hypothèse, le polynôme $\tau_n(f_n) \in k_{n+1}[X]$ admet une racine x_{n+1} dans k_{n+1}. Il s'ensuit que $\iota_{n+1}(x_{n+1})$ est une racine du polynôme $\iota_{n+1}(\tau_n(f_n)) = \iota_n(f_n) = f$ dans k_∞. Donc k_∞ est algébriquement clos. □

Ainsi, pour prouver l'existence de clôtures algébriques, il suffira d'utiliser inductivement la proposition suivante :

PROPOSITION. – *Soit k un corps. Il existe une extension algébrique K de k dans laquelle tout polynôme $f \in k[X]$ admet une racine.*

Remarque. (Corps de rupture) – Avant de donner la preuve, remarquons qu'il est facile de construire une extension K_f de k dans laquelle un polynôme irréductible $f \in k[X]$ donné admet une racine. Il suffit de prendre $K_f := k[X]/(f)$, qui est un corps puisque (f) est un idéal maximal, et dans lequel X (ou plutôt son image) est une racine de f. Un tel corps K_f s'appelle *corps de rupture* de f.

On peut alors tout aussi facilement construire inductivement une extension $K_{f_1,\cdots,f_n}$ de k dans lequel chacun des polynômes f_i donnés admet une racine. On peut même le faire pour une famille $(f_n)_{n\in\mathbb{N}}$ en utilisant le premier lemme par exemple. Mais en général, l'ensemble des polynômes irréducibles n'est pas nécessairement dénombrable. La preuve qui suit adapte cette idée au cas général.

Démonstration. Notons $(f_i)_{i\in I}$ la famille des polynômes irréducibles unitaires de $k[X]$. Considérons l'anneau de polynômes $\mathcal{R} := k[(X_i)_{i\in I}]$ dont les indéterminées sont indexées par I, et son idéal $\mathcal{I}$ engendré par les $f_i(X_i)$ pour $i \in I$.

Supposons que cet idéal est propre. Alors, par Zorn, il est contenu dans un idéal maximal $\mathfrak{m}$ de $\mathcal{R}$, dont le quotient $K := \mathcal{R}/\mathfrak{m}$ est un corps contenant k. Par construction, l'image de X_i dans K est une racine de f_i dans K. De plus, K est engendré par les images de X_i (en tant qu'extension), donc K est algébrique et satisfait la proposition.

Il nous suffit donc de prouver que $\mathcal{I}$ est bien un idéal propre de $\mathcal{R}$. Raisonnons par l'absurde et supposons que $\mathcal{I} = \mathcal{R}$. Alors il existe un sous-ensemble *fini* $J \subset I$ et des éléments $g_j \in \mathcal{R}$ tels que $\sum_{j\in J} g_j f_j(X_j) = 1$. Puisque J est fini, on a expliqué ci-dessus

qu'il existe une extension K_J de k dans laquelle chaque f_j possède une racine, disons x_j. Considérons alors l'unique morphisme de k-algèbres $\mathcal{R} \longrightarrow K_J$ qui envoie X_i sur x_i si $i \in J$ et sur 0 si $i \notin J$. Ce morphisme envoie $f_j(X_j)$ sur $f_j(x_j) = 0$, donc aussi $\sum_{j\in J} g_j f_j(X_j)$ sur 0. Comme $0 \neq 1$ dans le corps K_J on obtient une contradiction. □

1.2.7 Théorème.– *Tout corps possède une clôture algébrique.*

Démonstration. Soit $k = k_0$ un corps. La proposition précédente nous fournit une extension algébrique k_1 dans laquelle tout polynôme $f \in k_0[X]$ possède une racine. Inductivement on en déduit une suite d'extensions algébrique $k_0 \subset k_1 \subset \cdots \subset k_n \subset \cdots$ satisfaisant les hypothèse du second lemme ci-dessus. Mais alors la construction du premier lemme nous fournit un corps algébriquement clos k_∞ contenant k et algébrique sur k. □

1.3 Automorphismes. Extensions normales

Nous commençons cette section en fixant une clôture algébrique $\overline{k}$ de k.

1.3.1 *Automorphismes de $\overline{k}$.* On note généralement

$$\mathrm{Aut}(\overline{k}/k) := \mathrm{Aut}_{k-\mathrm{alg}}(\overline{k}) = \mathrm{Hom}_{k-\mathrm{alg}}(\overline{k}, \overline{k})$$

le groupe des automorphismes de l'extension $\overline{k} \supset k$. Notons que si $\overline{k}'$ est une autre clôture algébrique de k alors tout isomorphisme d'extensions $\psi : \overline{k}' \xrightarrow{\sim} \overline{k}$ induit un isomorphisme $\sigma \mapsto \psi^{-1}\sigma\psi : \mathrm{Aut}(\overline{k}/k) \xrightarrow{\sim} \mathrm{Aut}(\overline{k}'/k)$.

Lemme. – *Soit $K \supset k$ une extension algébrique de k et soient $\iota_1, \iota_2 : K \hookrightarrow \overline{k}$ deux k-plongements de K dans $\overline{k}$. Alors il existe un automorphisme $\sigma \in \mathrm{Aut}(\overline{k}/k)$ tel que $\iota_2 = \sigma \circ \iota_1$.*

Démonstration. C'est une conséquence de la proposition 1.2.5. En effet, le plongement ι_2 fournit une clôture algébrique de K. Le plongement ι_1 fait de $\overline{k}$ une extension algébrique de K. La proposition 1.2.5 nous fournit alors un morphisme de K-extensions $\sigma : \overline{k} \longrightarrow \overline{k}$. Mais attention, ici le terme de gauche est une extension de K via ι_1 et celui de droite via ι_2. On a donc $\sigma \circ \iota_1 = \iota_2$ par définition d'un morphisme de K-extensions. Par ailleurs, σ est k-linéaire puisque ι_1 et ι_2 le sont. Donc $\sigma \in \mathrm{Aut}(\overline{k}/k)$. □

1.3.2 *Conjugaison dans $\overline{k}$.*

Proposition. – *Pour $\alpha, \beta \in \overline{k}$, les propriétés suivantes sont équivalentes :*

i) Il existe $\sigma \in \mathrm{Aut}(\overline{k}/k)$, $\sigma(\alpha) = \beta$.

ii) $f_\alpha = f_\beta$ (polynômes minimaux sur k.)

Lorsque ces propriétés sont satisfaites, on dit que α et β sont conjugués.

Démonstration. Pour $\sigma \in \mathrm{Aut}(\overline{k}/k)$, notons encore $\sigma : \overline{k}[X] \longrightarrow \overline{k}[X]$ l'unique automorphisme de k-algèbres qui prolonge σ et envoie X sur X. Ainsi pour tout polynôme $f \in \overline{k}[X]$

et tout $x \in \overline{k}$, on a $\sigma(f(x)) = \sigma(f)(\sigma(x))$. De plus, puisque le polynôme minimal f_x de x sur k est dans $k[X]$, on a $\sigma(f_x) = f_x$.

i) $\Rightarrow$ *ii)*. Supposons que $\beta = \sigma(\alpha)$ pour un $\sigma \in \mathrm{Aut}(\overline{k}/k)$. Alors, $f_\alpha(\beta) = f_\alpha(\sigma(\alpha)) = \sigma(f_\alpha)(\sigma(\alpha)) = \sigma(f_\alpha(\alpha)) = 0$. Donc $f_\beta | f_\alpha$. De même $f_\alpha | f_\beta$ et finalement $f_\alpha = f_\beta$.

ii) $\Rightarrow$ *i)*. Si $f_\alpha = f_\beta$, il existe un unique isomorphisme de k-algèbres $k[\alpha] \xrightarrow{\sim} k[\beta]$ qui envoie α sur β (passer par l'intermédiaire $k[X]/(f)$ avec $f = f_\alpha = f_\beta$). En composant avec l'inclusion $k[\beta] \subset \overline{k}$, on obtient un plongement $\iota : k[\alpha] \hookrightarrow \overline{k}$ qui envoie α sur β. Mais alors le lemme précédent appliqué à $K = k[\alpha]$, ι_1 l'inclusion naturelle et $\iota_2 = \iota$ nous fournit un plongement $\sigma : \overline{k} \longrightarrow \overline{k}$ qui prolonge ι, et envoie donc α sur β. □

Exemple. – Si $k = \mathbb{R}$ et $\overline{k} = \mathbb{C}$, on a $\mathrm{Aut}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}, z \mapsto \bar{z}\}$ et la notion de conjugaison de la proposition redonne celle de conjugaison complexe usuelle.

Exemple. – Soit $k = \mathbb{Q}$ et $\overline{k} = \overline{\mathbb{Q}}$. L'ensemble des conjugués de $\sqrt[3]{2}$ est $\{\sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2}\}$, où $j = \frac{-1+i\sqrt{3}}{2}$ est une racine 3-ème primitive de l'unité.

1.3.3 *Sous-extensions normales de $\overline{k}$.*

Proposition. – *Soit K une sous-extension de $\overline{k}$. Les propriétés suivantes sont équivalentes :*

i) Pour tout $\alpha \in K$, les racines de f_α dans $\overline{k}$ appartiennent à K.

ii) Pour tout $\sigma \in \mathrm{Aut}(\overline{k}/k)$, on a $\sigma(K) \subset K$.

Si ces propriétés sont satisfaites on dit que K est une sous-extension normale de $\overline{k}$.

Démonstration. *i)* $\Rightarrow$ *ii)*. Soit $\sigma \in \mathrm{Aut}(\overline{k}/k)$ et $\alpha \in K$. La proposition précédente nous dit que $\sigma(\alpha)$ est une racine de f_α, donc l'hypothèse i) implique que $\sigma(\alpha) \in K$. D'où ii).

ii) $\Rightarrow$ *i)*. Soit $\alpha \in K$ et β une autre racine de f_α. Alors $f_\beta = f_\alpha$ et la proposition précédente nous fournit σ tel que $\sigma(\alpha) = \beta$. Puisque K est stable par σ (hypothèse ii)), on a bien $\beta \in K$. □

Corollaire. – *Soit $K \subset \overline{k}$ une sous-extension normale. L'application de restriction $\sigma \mapsto \sigma_{|K}$ induit un morphisme de groupes surjectif*

$$\mathrm{Aut}(\overline{k}/k) \twoheadrightarrow \mathrm{Aut}(K/k)$$

dont le noyau est $\mathrm{Aut}(\overline{k}/K)$.

Démonstration. Le ii) de la proposition précédente nous dit que l'application est bien définie. C'est évidemment un morphisme de groupes. Enfin, le dernier lemme nous assure que tout automorphisme γ de K se prolonge en un automorphisme σ de $\overline{k}$: il suffit d'appliquer ce lemme à ι_1 l'inclusion naturelle et ι_2 la composée de γ et de l'inclusion naturelle. D'où la surjectivité annoncée. Le noyau est formé des automorphismes $\sigma \in \mathrm{Aut}(\overline{k}/k)$ tels que $\sigma_{|K} = \mathrm{id}_K$, c'est-à-dire des automorphismes de K-algèbres de $\overline{k}$ comme annoncé. □

Exemple. – Soit $k = \mathbb{Q}$ et $\overline{k} = \overline{\mathbb{Q}}$.

— L'extension $\mathbb{Q}[j]$ de $\mathbb{Q}$ est normale (de degré 2) puisque tout $\sigma \in \mathrm{Aut}(\overline{\mathbb{Q}})$ envoie j sur j ou j^2, donc laisse stable $\mathbb{Q}[j]$.
— L'extension $\mathbb{Q}[\sqrt[3]{2}]$ de $\mathbb{Q}$ (de degré 3) n'est pas normale, car il existe $\sigma \in \mathrm{Aut}(\overline{\mathbb{Q}})$ tel que $\sigma(\sqrt[3]{2}) = j\sqrt[3]{2} \notin \mathbb{Q}[\sqrt[3]{2}]$.
— L'extension $\mathbb{Q}[j, \sqrt[3]{2}]$ de $\mathbb{Q}$ est normale (de degré 6).

1.3.4 *Extensions normales.* Ici nous ne travaillons pas à l'intérieur d'une clôture $\overline{k}$ fixée.

PROPOSITION. – *Soit $K \supset k$ une extension algébrique. Les propriétés suivantes sont équivalentes :*

i) Pour tout $\alpha \in K$, le polynôme f_α est scindé dans $K[X]$.

ii) Si ι_1, ι_2 sont deux plongements de K dans une clôture algébrique $\overline{k}$ alors $\iota_1(K) = \iota_2(K)$.

iii) L'image de K par tout plongement dans une clôture algébrique est une sous-extension normale au sens du paragraphe précédent.

Si ces propriétés sont satisfaites, $K \supset k$ est dite normale

Démonstration. *i) $\Rightarrow$ ii).* Soit $\alpha \in K$. Puisque f_α est scindé, chacun des plongements ι_1, ι_2 induit une bijection de l'ensemble des racines de f_α dans K dans celui des racines de f_α dans $\overline{k}$. En particulier $\iota_2(\alpha)$ est une racine de f_α, donc de la forme $\iota_1(\beta)$ et en particulier dans $\iota_1(K)$. Ceci montre $\iota_2(K) \subset \iota_1(K)$ et l'autre inclusion suit par symétrie.

ii) $\Rightarrow$ iii). Soit $\iota : K \hookrightarrow \overline{k}$. Pour tout $\sigma \in \mathrm{Aut}(\overline{k}/k)$, ii) implique que $\sigma(\iota(K)) = \iota(K)$, donc $\iota(K)$ est une sous-extension normale de $\overline{k}$.

iii) $\Rightarrow$ i). On peut plonger K dans une clôture algébrique $\iota : K \hookrightarrow \overline{k}$. Le polynôme $\iota(f_\alpha)$ est alors scindé dans $\overline{k}[X]$: on peut l'écrire $\iota(f_\alpha) = \prod_{i=1}^m (X - x_i)^{v_i}$. Mais iii) implique que les x_i sont dans $\iota(K)$, disons $x_i = \iota(\alpha_i)$. Il s'ensuit que $f_\alpha = \prod_i (X - \alpha_i)^{v_i}$ est scindé dans $K[X]$. □

Exemple. – Reprenons l'exemple du paragraphe précédent de manière "abstraite" (i.e. non plongée dans $\overline{\mathbb{Q}}$). L'extension $\mathbb{Q}[X]/(X^2 + X + 1) \supset \mathbb{Q}$ est normale et l'extension $\mathbb{Q}[X]/(X^3 - 2) \supset \mathbb{Q}$ ne l'est pas.

1.3.5 *Corps de décomposition d'un polynôme.* Voici l'exemple fondamental d'extension normale.

DÉFINITION. – *Soit $f \in k[X]$. Un* corps de décomposition *de f est une extension K de k telle que*

— *f est* scindé *dans $K[X]$, c-à-d $\exists x_1, \cdots, x_n \in K$ tels que $f = \lambda \prod_{i=1}^n (X - x_i)$,*
— *K est engendrée par les racines x_i de f.*

COROLLAIRE. – *Tout polynôme admet un corps de décomposition, et celui-ci est unique à isomorphisme (non unique) près. De plus, ce corps est un extension normale de k.*

Démonstration. Soit $\overline{k}$ une clôture algébrique de k. Le polynôme f se scinde en $f = \lambda \prod_{i=1}^{n}(X - x_i)$ avec $\lambda \in k$ et $x_1, \cdots, x_n \in \overline{k}$. Alors le sous-corps $K_f = k(x_1, \cdots, x_n)$ de $\overline{k}$ est un corps de décomposition de f. Soit maintenant $K' \supset k$ un autre corps de décomposition de f. Alors K' est algébrique sur k donc se plonge dans $\overline{k}$. Son image est engendrée par les racines de f donc égale à K_f. Donc K' est isomorphe à K_f. Ceci montre aussi que K_f est normale. □

Exemple. – Le corps de décomposition de $X^3 - 2$ sur $\mathbb{Q}$ est le corps $\mathbb{Q}[j, \sqrt[3]{2}]$.

Exercice. – Soient $n, m \in \mathbb{N}$. Montrer que le corps de décomposition de $X^n - m$ est $\mathbb{Q}[\zeta_n, \sqrt[n]{m}]$ où $\zeta_n = \exp(2i\pi/n)$ et $\sqrt[n]{m}$ est l'unique racine n-ème réelle positive de m.

Remarque. – L'action de $\mathrm{Aut}(K_f/k)$ sur K_f permute l'ensemble $f^{-1}(0)$ des racines de f dans K_f. Comme celles-ci engendrent K_f, on a une injection dans le groupe de permutations

$$\mathrm{Aut}(K_f/k) \hookrightarrow \mathfrak{S}_{f^{-1}(0)}.$$

L'idée basique de la théorie de Galois est d'utiliser le groupe $\mathrm{Aut}(K_f/k)$ comme groupe de symétries de l'équation algébrique $f = 0$. Néanmoins, ce groupe peut parfois être trivial : prenons $k = \mathbb{F}_p(T)$ et $f = X^p - T$. Dans ce cas $K_f = \mathbb{F}_p(T)[X]/(X^p - T) = \mathbb{F}_p(T^{1/p})$. En fait, f se factorise en $X^p - T = (X - T^{1/p})^p$ dans K_f, ce qui montre que $T^{1/p}$ est la seule racine p-ème de T (avec multiplicité p). Donc le groupe $\mathfrak{S}_{f^{-1}(0)}$ est trivial et $\mathrm{Aut}(K_f/k)$ aussi. Ce phénomène appelé "inséparabilité" est étudié dans les sections suivantes.

1.4 Caractéristique et endomorphisme de Frobenius

1.4.1 *Caractéristique d'un corps.* Soit A un anneau commutatif. Il existe un *unique* morphisme d'anneaux $\mathbb{Z} \longrightarrow A$. En effet, un tel morphisme doit envoyer 1 sur 1_A et n sur $1_A + \cdots + 1_A$ (n fois). Le noyau de ce morphisme est appelé *idéal caractéristique* de A. Lorsque $A = k$ est un corps, deux cas peuvent se produire :

— l'idéal caractéristique est nul auquel cas on dit que k *est de caractéristique nulle.*

— l'idéal caractéristique est premier, donc engendré par un unique nombre premier p, auquel cas on dit que k *est de caractéristique* p.

Remarque. – Si p est un nombre premier, on dit plus généralement qu'un anneau A est "de caractéristique p" si l'idéal caractéristique de A est égal à (p). Dans ce cas, le morphisme $\mathbb{Z} \longrightarrow A$ se factorise par $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$, le corps fini à p éléments, et A est donc une $\mathbb{F}_p$-algèbre. Réciproquement, toute $\mathbb{F}_p$-algèbre est un anneau de caractéristique p.

1.4.2 *Sous-corps premier.* On appelle *sous-corps premier* d'un corps k le plus petit sous-corps de k, c'est-à-dire l'intersection de tous les sous-corps de k. Deux cas peuvent se produire :

— Si k est de caractéristique nulle, alors k contient $\mathbb{Z}$ donc $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$ et le sous-corps premier de k est donc $\mathbb{Q}$.

— Si k est de caractéristique $p > 0$, alors k contient $\mathbb{F}_p$, qui est donc le sous-corps premier de k.

1.4.3 *Endomorphisme de Frobenius.*

PROPOSITION. – *Soit A un anneau de caractéristique p. Alors l'application*

$$F_A : A \longrightarrow A,\ a \mapsto a^p$$

est un endomorphisme de $\mathbb{F}_p$-algèbres. On l'appelle endomorphisme de Frobenius de A.

Démonstration. Soit $a, b \in A$. On a clairement $(ab)^p = a^p b^p$. Par ailleurs on a $(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k$ avec $\binom{p}{k} = \frac{p!}{k!(p-k)!}$. Maintenant, pour $0 < k < p$, p ne divise ni $k!$ ni $(p-k)!$. Mais p divise $p!$, donc divise $\binom{p}{k}$. Il s'ensuit que, dans A, on a $(a+b)^p = a^p + b^p$. □

Remarque. – Les endomorphismes de Frobenius "commutent" avec n'importe quel morphisme de $\mathbb{F}_p$-algèbres : si $\varphi : A \longrightarrow B$ est un tel morphisme, alors $\varphi \circ F_A = F_B \circ \varphi$.

Pour un corps k de caractéristique p, notons

$$k^F := \{x \in k,\ F_k(x) = x\}$$

l'ensemble des points fixes de l'endomorphisme de Frobenius. C'est un sous-corps de k, puisque F_k est un endomorphisme de corps.

LEMME. – *k^F est le sous-corps premier $\mathbb{F}_p$ de k.*

Démonstration. Pour $x \in k$, on a $F_k(x) = x \Leftrightarrow x^p = x \Leftrightarrow (X-x) | (X^p - X)$ dans $k[X]$. Par ailleurs, pour tout $a \in \mathbb{F}_p$ on a $a^p = a$. Comme les polynômes irréductibles $X - a$ sont deux à deux premiers entre eux lorsque a décrit $\mathbb{F}_p$, on a la factorisation $X^p - X = \prod_{a \in \mathbb{F}_p} (X-a)$ dans $\mathbb{F}_p[X]$ et dans $k[X]$. Donc $x \in \mathbb{F}_p$. □

Plus généralement, pour tout $r \in \mathbb{N}^*$, le sous-ensemble

$$k^{F^r} := \{x \in k, F_k^r(x) = x\}$$

des points fixes de l'endomorphisme $F_k^r = F_k \circ F_k \circ \cdots \circ F_k$ est un sous-corps de k. Le cas où k est une clôture algébrique de $\mathbb{F}_p$ est particulièrement intéressant.

1.4.4 *Corps finis.* Choisissons une clôture algébrique $\overline{\mathbb{F}}_p$ de $\mathbb{F}_p$ et notons F son automorphisme de Frobenius.

THÉORÈME. – *Le corps $\overline{\mathbb{F}}_p^{F^r}$ est un corps de décomposition du polynôme $X^{p^r} - X$ sur $\mathbb{F}_p$. Réciproquement, toute extension finie de $\mathbb{F}_p$ est un corps de décomposition du polynôme $X^{p^{[k:\mathbb{F}_p]}} - X$ sur $\mathbb{F}_p$.*

Démonstration. Pour $x \in \overline{\mathbb{F}}_p$, on a $F^r(x) = x \Leftrightarrow (x$ racine de $X^{p^r} - X)$. Ainsi $\overline{\mathbb{F}}_p^{F^r}$ est l'ensemble des racines de $X^{p^r} - X$ dans $\overline{\mathbb{F}}_p$. Comme c'est un corps, c'est donc en particulier un corps de décomposition de $X^{p^r} - X$.

Réciproquement, soit k une extension finie de $\mathbb{F}_p$. Notons $r := [k : \mathbb{F}_p]$ sa dimension sur $\mathbb{F}_p$. Alors k est fini de cardinal $|k| = p^r$, donc son groupe multiplicatif $k^\times$ est de cardinal

$p^r - 1$ donc tout élément $x \in k^\times$ vérifie $x^{p^r-1} = 1$. Il s'ensuit que tout élément x de k est racine du polynôme $X(X^{p^r}-1) = X^{p^r} - X$. En particulier, k est un corps de décomposition de ce polynôme. □

Comme tout corps fini est extension finie de son corps premier, ce théorème donne une recette pour "construire" tous les corps finis. Il dit aussi que, à isomorphisme près, il y a au plus un corps de cardinal p^r pour p premier et $r \in \mathbb{N}^*$. Pour compléter le théorème, il reste à calculer le cardinal de $\overline{\mathbb{F}}_p^{F^r}$, ce qui revient à compter les racines de $X^{p^r} - X$ (il y en a au plus p^r).

1.5 Polynômes et extensions séparables.

1.5.1 *Dérivation des polynômes.* Soit A une k-algèbre. Une *dérivation* ∂ de A est un endomorphisme k-linéaire de A qui vérifie l'axiome :

$$\forall f, g \in A, \;\; \partial(fg) = \partial(f)g + f\partial(g).$$

Ainsi, on constate par récurrence que $\partial(f^n) = nf^{n-1}\partial(f)$ pour tout $n \in \mathbb{N}$ et en particulier $\partial(\lambda) = \lambda\partial(1) = 0$ pour tout $\lambda \in k$.

Sur l'algèbre $A = k[X]$, toute dérivation est donc uniquement déterminée par sa valeur en X. Notons ∂ l'unique dérivation de $k[X]$ telle que $\partial(X) = 1$. Pour un polynôme $f = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0$ on a donc

$$\partial f = na_nX^{n-1} + (n-1)a_{n-1}X^{n-2} + \cdots + a_1.$$

On appelle ∂f le *polynôme dérivé* de f et on le note f' en l'absence d'ambiguïté.

Remarque. – Soit $\tau : k \to k'$ un morphisme de corps. Notons aussi $\tau : k[X] \longrightarrow k'[X]$ le morphisme d'anneaux qui prolonge τ et envoie X sur X. Alors $\forall f \in k[X]$, $\tau(f)' = \tau(f')$.

LEMME. – *Soit $f \in k[X]$ tel que $f' = 0$.*

i) Si k est de caractéristique nulle, alors $\deg(f) = 0$.

ii) Si k est de caractéristique $p > 0$, alors il existe un unique polynôme $g \in k[X]$ tel que $f = g(X^p)$.

Démonstration. i) est clair. ii) En écrivant $f = \sum_n a_nX^n$ et $f' = \sum_n na_nX^{n-1} = 0$, on voit que $a_n \neq 0 \Rightarrow p|n$ donc $f = \sum_{m\in\mathbb{N}} a_{pm}X^{pm} = g(X^p)$ pour $g = \sum_m a_{pm}X^m$. L'unicité de g est claire. □

1.5.2 *Polynômes séparables.*

DÉFINITION. – *Un polynôme $f \in k[X]$ est dit* séparable *si l'idéal (f, f') de $k[X]$ est l'idéal unité (ie f et f' sont premiers entre eux).*

Soit $f \in k[X]$. Si $\overline{k}$ est une clôture algébrique de k, alors f se scinde dans $\overline{k}[X]$ en $f = a_n(X-\alpha_1)^{v_1}\cdots(X-\alpha_m)^{v_m}$ où a_n est le terme dominant de f (ie $n = \deg(f)$), $\sum_{i=1}^m v_i = n$ et les $\alpha_i \in \overline{k}$ sont *supposés distincts*. Les α_i sont donc les racines de f dans $\overline{k}$ et v_i est la "*multiplicité*" de la racine α_i.

PROPOSITION. – *Pour $f \in k[X]$, les propriétés suivantes sont équivalentes :*

i) f est séparable.

ii) f et f' n'ont pas de racine commune dans une clôture algébrique de k.

iii) Toutes les racines de f dans une clôture algébrique de k sont de multiplicité 1.

iii') f possède $\deg(f)$ *racines distinctes dans toute clôture algébrique.*

iii") Si $\overline{k}$ est une clôture algébrique de k, la $\overline{k}$-algèbre $\overline{k}[X]/(f)$ est réduite (auquel cas, elle est isomorphe à $\overline{k}^{\deg(f)} = \overline{k}\times\overline{k}\times\cdots\times\overline{k}$).

Démonstration. *i)* $\Rightarrow$ *ii)*. Soit $\overline{k}$ une clôture algébrique de k. Si $g, h \in k[X]$ sont tels que $fg + f'h = 1$, alors la même égalité dans $\overline{k}[X]$ montre que f et f' n'y ont pas de diviseur irréductible commun, donc pas de racine commune.

ii) $\Rightarrow$ *iii)*. Montrons la contraposée. Supposons donc que f possède une racine double α dans une clôture algébrique $\overline{k}$. Il existe donc $g \in \overline{k}[X]$ tel que $f = (X-\alpha)^2\cdot g$. Il s'ensuit que $f' = (X-\alpha)(2g + (X-\alpha)g')$, ce qui montre que α est une racine commune à f et f'.

iii) $\Rightarrow$ *i)*. Montrons encore la contraposée. Si (f, f') n'est pas l'idéal unité de $k[X]$ alors f et f' admettent un diviseur irréductible commun, disons $h \in k[X]$. Il existe donc $g \in k[X]$ tel que $f = hg$. En dérivant, on obtient $f' = h'g + hg'$. Comme $h|f'$, on en déduit que $h|h'g$. Deux choses peuvent se produire :

— Si $h' \neq 0$, alors h ne divise pas h' car $\deg(h') < \deg(h)$, donc d'après le lemme d'Euclide, h divise g. Il s'ensuit que h^2 divise f. Or h admet une racine dans $\overline{k}$ et celle-ci est donc une racine double de f.

— Si $h' = 0$, alors d'après le lemme précedent, k est de caractéristique $p > 0$ et $h = e(X^p)$ pour un $e \in k[X]$. Alors e admet une racine α dans $\overline{k}$ et donc $X^p - \alpha$ divise h dans $k[X]$. Mais α admet une racine p-ème β dans $\overline{k}$, donc $X^p - \alpha = (X-\beta)^p$ et β est racine multiple de h et donc de f.

L'équivalence entre *iii)* et *iii')* est évidente. Il reste à vérifier que *iii)* $\Leftrightarrow$ *iii")*. Pour cela, on scinde $f = a_n(X-\alpha_1)^{v_1}\cdots(X-\alpha_m)^{v_m}$ dans $\overline{k}[X]$ avec les α_i distincts deux à deux, et on constate grâce aux restes chinois que

$$\overline{k}[X]/(f) = \prod_{i=1}^m \overline{k}[X]/(X-\alpha_i)^{v_i}.$$

Cet anneau est réduit si et seulement si chacun de ses facteurs $\overline{k}[X]/(X-\alpha_i)^{v_i}$ est réduit, ce qui équivaut à $v_i = 1$. Dans ce cas on a $m = \deg(f)$ et donc $\overline{k}[X]/(f) \simeq \overline{k}^{\deg(f)}$. □

Remarque. – On voit grâce à la propriété iii) que si f divise un polynôme séparable alors f est séparable.

Application. (Corps finis) – On peut maintenant compléter le théorème 1.4.4. Puisque le polynôme $X^{p^r} - X$ est séparable (son polynôme dérivé est $f' = -1$), il admet p^r racines distinctes dans $\overline{\mathbb{F}}_p$. Il s'ensuit, d'après le théorème 1.4.4, que son corps de décomposition $\overline{\mathbb{F}}_p^{F^r}$ est de cardinal p^r. On obtient ainsi le théorème de classification des corps finis :

1.5.3 THÉORÈME.– *Pour toute puissance p^r d'un nombre premier, il existe un corps $\mathbb{F}_{p^r}$ de cardinal p^r, unique à isomorphisme près. C'est un corps de décomposition du polynôme $X^{p^r} - X$ sur $\mathbb{F}_p$. Tout corps fini est de cette forme.*

Démonstration. Soit k un corps fini. Il est nécessairement de caractéristique non nulle, disons p. Il est de degré fini, disons r, sur son corps premier $\mathbb{F}_p$, donc, d'après le théorème 1.4.4, c'est le corps de décomposition de $X^{p^r} - X$. Voici pour l'unicité. L'existence vient du théorème 1.4.4 et de la séparabilité de $X^{p^r} - X$, comme expliqué ci-dessus. □

1.5.4 *Extensions séparables.*

DÉFINITION. – *Soit $K \supset k$ une extension algébrique. On dit que*
— *$\alpha \in K$ est séparable sur k, si son polynôme minimal $f_\alpha \in k[X]$ est séparable.*
— *K est séparable sur k si tout élément de K est séparable sur k.*

Afin de donner un analogue de la proposition 1.5.2 pour les extensions, il faut se demander quel est l'analogue, pour une extension, de la notion de racine d'un polynôme. Pour cela, il faut se rappeler la bijection suivante, pour $f \in k[X]$ irréductible :

$$\mathrm{Hom}_{k-\mathrm{alg}}(K[X]/(f), \overline{k}) \xrightarrow{\sim} \{\alpha \in \overline{k}, f(\alpha) = 0\}$$

donnée par $\iota \mapsto \iota(\overline{X})$ où $\overline{X}$ est l'image de X dans $K[X]/(f)$. Ainsi l'analogue de la notion de racine est la notion de plongement. Le lemme suivant nous dit que, tout comme un polynôme f possède au plus $\deg(f)$ racines, une extension finie $K \supset k$ admet au plus $[K : k]$ plongements.

PROPOSITION. – *Soit $K \supset k$ une extension finie et $\overline{k}$ une clôture algébrique de k. Alors le nombre de k-plongements de K dans $\overline{k}$ vérifie l'inégalité*

$$|\mathrm{Hom}_{k-\mathrm{alg}}(K, \overline{k})| \leqslant [K : k].$$

Démonstration. La propriété universelle de l'extension des scalaires fournit une bijection

$$\mathrm{Hom}_{k-\mathrm{alg}}(K, \overline{k}) \xrightarrow{\sim} \mathrm{Hom}_{\overline{k}-\mathrm{alg}}(\overline{k} \otimes_k K, \overline{k}), \quad \iota \mapsto \tau,$$

caractérisée par l'égalité $\tau(\lambda \otimes \alpha) = \lambda\iota(\alpha)$. Posons $I := \mathrm{Hom}_{\overline{k}-\mathrm{alg}}(\overline{k} \otimes_k K, \overline{k})$ et considérons le morphisme produit

$$\Pi\tau : \ \overline{k} \otimes_k K \longrightarrow \overline{k}^I, \ \lambda \otimes \alpha \mapsto (\tau(\lambda \otimes \alpha))_{\tau \in I}.$$

Le lemme suivant nous dit que ce morphisme est surjectif, donc

$$[K : k] = \dim_{\overline{k}}(\overline{k} \otimes_k K) \geqslant \dim_{\overline{k}}(\overline{k}^I) = |\mathrm{Hom}_{k-\mathrm{alg}}(K, \overline{k})|.$$

LEMME. – *Soit A une $\overline{k}$-algèbre commutative de dimension finie. Alors le morphisme*

$$\Pi\tau : A \longrightarrow \overline{k}^{\mathrm{Hom}_{\overline{k}-\mathrm{alg}}(A,\overline{k})}, \quad a \mapsto (\tau(a))_{\tau\in\mathrm{Hom}_{\overline{k}-\mathrm{alg}}(A,\overline{k})}$$

est surjectif et son noyau est le nilradical de A.

Démonstration. Fixons un morphisme $\tau : A \longrightarrow \overline{k}$ de $\overline{k}$-algèbres. Alors τ est surjectif puisque $\tau(\lambda \cdot 1_A) = \lambda$ pour tout $\lambda \in \overline{k}$. Donc $\mathfrak{m} := \mathrm{Ker}(\tau)$ est un idéal maximal de A, et τ se factorise en $\tau : A \twoheadrightarrow A/\mathfrak{m} \xrightarrow{\overline{\tau}} \overline{k}$ avec $\overline{\tau}$ bijectif. En fait, $\overline{\tau}$ est déterminé par $\mathfrak{m}$. En effet, la composée $\iota_{\mathfrak{m}} : \overline{k} \longrightarrow A \longrightarrow A/\mathfrak{m}$ fait de $A/\mathfrak{m}$ une extension finie de $\overline{k}$, donc est un isomorphisme puisque $\overline{k}$ est algébriquement clos. Mais alors, $\overline{\tau} \circ \iota_{\mathfrak{m}}$ est un automorphisme de la $\overline{k}$-algèbre $\overline{k}$, donc est l'identité. Il s'ensuit que τ coïncide avec le morphisme $\tau_{\mathfrak{m}} : A \twoheadrightarrow A/\mathfrak{m} \xrightarrow{\iota_{\mathfrak{m}}^{-1}} \overline{k}$. On a donc montré que

$$\mathrm{Hom}_{\overline{k}-\mathrm{alg}}(A,\overline{k}) = \{\tau_{\mathfrak{m}}, \mathfrak{m} \in \mathrm{Max}(A)\}$$

et que l'application $\Pi\tau$ de l'énoncé se factorise en

$$A \longrightarrow \prod_{\mathfrak{m}\in\mathrm{Max}(A)} A/\mathfrak{m} \xrightarrow{\sim} \overline{k}^{\mathrm{Hom}_{\overline{k}-\mathrm{alg}}(A,\overline{k})}$$

où la première flèche est $a \mapsto (a \,(\mathrm{mod}\,\mathfrak{m}))_{\mathfrak{m}\in\mathrm{Max}(A)}$ et la seconde est le produit $\prod_{\mathfrak{m}} \iota_{\mathfrak{m}}^{-1}$. Le théorème des restes chinois nous dit alors que $\Pi\tau$ est surjective. De plus, son noyau est $\bigcap_{\mathfrak{m}\in\mathrm{Max}(A)} \mathfrak{m}$. Or, puisque A est de longueur finie comme A-module, on sait que A est annulé par un produit fini d'idéaux maximaux. Il est donc annulé par une puissance convenable de $\bigcap_{\mathfrak{m}\in\mathrm{Max}(A)} \mathfrak{m}$, ce qui signifie que $\bigcap_{\mathfrak{m}\in\mathrm{Max}(A)} \mathfrak{m}$ est nilpotent, donc inclus dans le nilradical $\mathcal{N}(A)$ de A. Réciproquement, puisque le quotient $A/\bigcap_{\mathfrak{m}\in\mathrm{Max}(A)} \mathfrak{m}$ est réduit, on a aussi $\mathcal{N}(A) \subset \bigcap_{\mathfrak{m}\in\mathrm{Max}(A)} \mathfrak{m}$, d'où l'égalité. □

□

THÉORÈME. – *Soit $K \supset k$ une extension finie. On a équivalence entre :*

i) K est séparable sur k

ii) Pour toute clôture algébrique $\overline{k}$ de k on a l'égalité $|\mathrm{Hom}_{k-\mathrm{alg}}(K,\overline{k})| = [K : k]$.

iii) Pour toute clôture algébrique $\overline{k}$ de k, la $\overline{k}$-algèbre $\overline{k} \otimes_k K$ est réduite (auquel cas elle est isomorphe à $\overline{k}^{[K:k]} = \overline{k} \times \overline{k} \times \cdots \times \overline{k}$).

Démonstration. L'équivalence *ii)* ⇔ *iii)* découle immédiatement du lemme ci-dessus, via le raisonnement de la preuve de la proposition.

i) ⇒ *ii)*. Commençons par la remarque suivante. Soit $K' \subset K$ une sous-k-extension de K, et considérons l'application de restriction

$$\mathrm{Hom}_{k-\mathrm{alg}}(K,\overline{k}) \longrightarrow \mathrm{Hom}_{k-\mathrm{alg}}(K',\overline{k}), \ \iota \mapsto \iota_{|K'}.$$

La proposition 1.2.5 nous dit que cette application est surjective. De plus, la fibre au-dessus de $\iota' : K' \hookrightarrow \overline{k}$ est l'ensemble $\mathrm{Hom}_{K'-\mathrm{alg},\iota'}(K, \overline{k})$ des plongements $K \hookrightarrow \overline{k}$ qui prolongent ι', *i.e.* des morphismes de K'-algèbres pour lesquels $\overline{k}$ est muni de la structure de K'-algèbre donnée par ι'. On a donc

$$|\mathrm{Hom}_{k-\mathrm{alg}}(K, \overline{k})| = \sum_{\iota' \in \mathrm{Hom}_{k-\mathrm{alg}}(K', \overline{k})} |\mathrm{Hom}_{K'-\mathrm{alg},\iota'}(K, \overline{k})|.$$

En particulier, si on sait que $|\mathrm{Hom}_{K'-\mathrm{alg},\iota'}(K, \overline{k})| = [K : K']$ pour tout ι et $|\mathrm{Hom}_{k-\mathrm{alg}}(K', \overline{k})| = [K' : k]$, alors on obtient

$$(*) \qquad |\mathrm{Hom}_{k-\mathrm{alg}}(K, \overline{k})| = [K' : k][K : K'] = [K : k].$$

Cette remarque nous permet de faire un raisonnement par récurrence sur le nombre de générateurs r de K sur k. Si $r = 1$, K est de la forme $K = k[\alpha_1] = k[X]/(f_{\alpha_1})$ et on a vu ci-dessus que $\mathrm{Hom}_{k-\mathrm{alg}}(K, \overline{k})$ est en bijection avec l'ensemble des racines f_{α_1} qui est de cardinal $\deg(f_{\alpha_1}) = [K : k]$ puisque α_1 est séparable. Supposons K engendré par r éléments $\alpha_1, \cdots, \alpha_r$ et notons $K' := k[\alpha_1, \cdots, \alpha_{r-1}]$. Par récurrence, on peut supposer que $|\mathrm{Hom}_{k-\mathrm{alg}}(K', \overline{k})| = [K' : k]$. De plus, puisque K est engendrée sur K' par (au plus) 1 élément α_r, on a $|\mathrm{Hom}_{K'-\mathrm{alg},\iota'}(K, \overline{k})| = [K : K']$ pour tout plongement $\iota' : K' \hookrightarrow \overline{k}$ (un tel plongement fait de $\overline{k}$ une clôture algébrique de K'). On conclut par $(*)$.

iii) $\Rightarrow$ *i)*. Avant de prouver cette implication, remarquons que pour toute sous-extension $K' \subset K$, le morphisme canonique de $\overline{k}$-algèbre $\overline{k} \otimes_k K' \longrightarrow \overline{k} \otimes_k K$ est injectif. En effet, si $(e_i)_{i \in I}$ est une base du k-ev K telle que $(e_i)_{i \in I'}$ soit une base du k-ev K', alors $(1 \otimes e_i)_{i \in I}$ est une base du $\overline{k}$-ev $\overline{k} \otimes_k K$ et la sous-famille $(1 \otimes e_i)_{i \in I'}$ est une base du $\overline{k}$-ev $\overline{k} \otimes_k K'$. Il s'ensuit donc que si $\overline{k} \otimes_k K$ est réduite, alors $\overline{k} \otimes_k K'$ l'est aussi. Appliquons ceci à $K' = k[\alpha]$ pour $\alpha \in K$ quelconque. Alors $\overline{k} \otimes_k k[\alpha]$ est réduite, donc puisque $k[\alpha] \simeq k[X]/(f_\alpha)$, f_α est séparable d'après le iii") de la proposition 1.5.2. Comme α était quelconque, K est séparable sur k. □

Application. – Si $f \in k[X]$ est séparable, $k[X]/(f)$ est une extension séparable de k. Cela découle en effet de l'implication *iii)* $\Rightarrow$ *i)*.

Corollaire. (De la preuve) – *Soit $k \subset K' \subset K$ une tour d'extensions finies. Si K est séparable sur K' qui est séparable sur k, alors K est séparable sur k.*

Démonstration. On répète l'argument utilisé pour l'implication *i)* $\Rightarrow$ *ii)* pour obtenir l'égalité $(*)$ de cette preuve, qui montre que K est séparable sur k. □

Application. – Une extension finie K engendrée par des éléments séparables est séparable (récurrence sur le nombre de générateurs). En particulier, un corps de décomposition d'un polynôme séparable de $k[X]$ est séparable sur k.

Remarque. – Pour une extension algébrique $K \supset k$ *infinie*, l'assertion ii) du théorème n'a pas de sens. Mais le raisonnement utilisé donne l'équivalence :

$$K \text{ séparable sur } k \Leftrightarrow \overline{k} \otimes_k K \text{ est réduite.}$$

1.5.5 *Théorème de l'élément primitif.* Le corollaire suivant est assez spectaculaire pour qu'on lui donne un nom évocateur.

COROLLAIRE. (Théorème de l'élément primitif) – *Toute extension finie séparable $K \supset k$ est monogène (i.e. engendrée par un seul élément).*

Démonstration. Soit $\alpha \in K$, et considérons l'application de restriction

$$\mathrm{Hom}_{k-\mathrm{alg}}(K, \overline{k}) \longrightarrow \mathrm{Hom}_{k-\mathrm{alg}}(k[\alpha], \overline{k}), \quad \iota \mapsto \iota_{|k[\alpha]}.$$

On a vu que cette application est surjective, que la source est de cardinal $[K : k]$ (puisque K est supposée séparable) et la cible de cardinal $[k[\alpha] : k] = \deg(f_\alpha)$ (puisque α est séparable). On a donc l'équivalence

$$K = k[\alpha] \Leftrightarrow [K : k] = [k[\alpha] : k] \Leftrightarrow (\iota \mapsto \iota_{|k[\alpha]} \text{ est injective}).$$

Par ailleurs, l'application $\iota' \mapsto \iota'(\alpha)$, est une injection de $\mathrm{Hom}_{k-\mathrm{alg}}(k[\alpha], \overline{k})$ dans $\overline{k}$ (puisque c'est même une bijection sur l'ensemble des racines de f_α dans $\overline{k}$). On a donc

$$K = k[\alpha] \Leftrightarrow (\iota \mapsto \iota(\alpha) \text{ est injective}) \Leftrightarrow \alpha \notin \bigcup_{\iota_1 \neq \iota_2} \mathrm{Ker}(\iota_1 - \iota_2).$$

Notons que chaque $\mathrm{Ker}(\iota_1 - \iota_2)$ est un k-sev propre de K. Lorsque k est infini, il nous suffira donc d'invoquer le lemme suivant :

LEMME. – *Soit k un corps infini et V un k-ev de dimension finie. Alors le complémentaire d'une union finie de k-sev propres est non-vide.*

Démonstration. On raisonne par récurrence sur $d = \dim_k(V)$. Pour $d = 1$, l'assertion est claire (et vraie pour k fini d'ailleurs). Supposons $d > 1$ et donnons-nous des k-sev propres $V_1, \cdots, V_r$. On peut supposer que les V_i sont des hyperplans deux à deux distincts. Alors $V_1 \cap V_i$ est un k-sev propre de V_1 pour tout $i > 1$ donc, par hypothèse de récurrence, il existe $v_1 \in V_1 \setminus \bigcup_{i>1} V_i$. Choisissons $w_1 \in V \setminus V_1$ et considérons la droite affine $D = w_1 + kv_1$. On a $D \cap V_1 = \emptyset$. De plus, pour $i > 1$ on a $|D \cap V_i| < 1$. En effet, si $w_1 + \lambda v_1$ et $w_1 + \mu v_1$ sont dans V_i, alors $(\mu - \lambda)v_1 \in V_i$ donc $\mu = \lambda$. Il s'ensuit que $D \cap \bigcup_{i=1}^r V_i$ est fini, donc de complémentaire non vide puisque la droite D est infinie. □

Reste à traiter le cas où k est fini. Pour cela on peut supposer $k = \mathbb{F}_p$. Alors $K = \mathbb{F}_{p^r}$ pour $r = [K : k]$ et $K^\times$ est le groupe des racines $p^r - 1$-ème de l'unité (ie les racines des $X^{p^r} - 1$). Le lemme suivant nous dit que ce groupe est cyclique. Mais alors tout générateur α de ce groupe est aussi un générateur de $\mathbb{F}_{p^r}$ sur $\mathbb{F}_p$. □

LEMME. – *Soit k un corps et $G \subset k^\times$ un sous-groupe fini de $k^\times$. Alors G est cyclique.*

Démonstration. Notons $n = |G|$. On veut montrer qu'il existe un élément d'ordre n dans G. Soit m le ppcm des ordres de tous les éléments de G. Le résultat de structure des groupes abéliens finis (modules de torsion sur l'anneau principal $\mathbb{Z}$) implique qu'il existe

un élément $x \in G$ d'ordre m (en fait, cela se prouve directement et facilement : exercice). Il suffit donc de montrer $m = n$. Or, par définition on a $x^m = 1$ pour tout $x \in G$, donc G est formé de racine m-èmes de l'unité, et donc $|G| = n \leqslant m$. Comme $m|n$, on a donc $m = n$. □

Remarque. – Une extension finie non séparable n'est pas nécessairement monogène. Prenons par exemple $K = \mathbb{F}_p(X, Y) \supset k = \mathbb{F}_p(X^p, Y^p)$. On vérifie assez facilement que la famille des $X^i Y^j$, $0 \leqslant i, j < p$ est une base de K sur k, de sorte que $[K : k] = p^2$. Et pourtant pour tout $\alpha \in K$, on a $\alpha^p \in k$ donc $[k[\alpha] : k] = \deg(f_\alpha) \leqslant p$.

Exemple. – On a vu que le corps $\mathbb{Q}(\sqrt[3]{2})$ n'est pas normal sur $\mathbb{Q}$, mais qu'il le devient si on lui adjoint j (on obtient alors le corps de décomposition de $X^2 - 3$, de degré 6 sur $\mathbb{Q}$). Le théorème de l'élément primitif nous dit que ce corps est monogène, mais pas comment trouver un générateur. Nous verrons plus loin comment en trouver, et montrerons que par exemple $j + \sqrt[3]{2}$ est de degré 6, et engendre donc $\mathbb{Q}(j, \sqrt[3]{2})$.

2 Théorie de Galois

2.1 Extensions Galoisiennes. Correspondance de Galois

2.1.1 Définition.– *Une extension finie $K \supset k$ est dite Galoisienne si elle est normale et séparable. On note alors* $\mathrm{Gal}(K/k) := \mathrm{Aut}(K/k)$ *le groupe des automorphismes de la k-algèbre K et on l'appelle* groupe de Galois *de K sur k.*

Le théorème suivant résume les caractérisations utiles des extensions Galoisiennes.

2.1.2 Théorème.– *Soit $K \supset k$ une extension finie. On a équivalence entre :*

i) *K est Galoisienne sur k*

ii) *Pour tout $\alpha \in K$, on a $f_\alpha = \prod_{\beta \in \mathrm{Aut}(K/k)\cdot\alpha}(X - \beta)$ dans $K[X]$.*

iii) *K est le corps de décomposition d'un polynôme séparable.*

iv) $|\mathrm{Aut}_{k-\mathrm{alg}}(K)| = [K : k]$

v) $K^{\mathrm{Aut}(K/k)} = k$ *(points fixes dans K pour l'action de* $\mathrm{Aut}(K/k)$*).*

Démonstration. *i)* $\Leftrightarrow$ *ii)*. Par définition, K est Galoisienne sur k si et seulement si $\forall \alpha \in K$, f_α est séparable et scindé dans $K[X]$. Par ailleurs on a déjà vu que les racines de f_α dans une clôture algébrique $\overline{k}$ sont permutées transitivement par $\mathrm{Aut}(\overline{k}/k)$. Plongeons donc K dans $\overline{k}$. Comme $\mathrm{Aut}(\overline{k}/k)$ stabilise K, on en déduit que $\mathrm{Aut}(K/k)$ permute transitivement les racines de f_α dans K, de sorte que $\mathrm{Aut}(K/k)\alpha = \{\text{racines de } f_\alpha \text{ dans } K\}$.

i) $\Leftrightarrow$ *iii)*. On a déjà vu qu'un corps de décomposition d'un polynôme séparable f est une extension normale (corollaire 1.3.5) et séparable (à la suite du corollaire 1.5.4). Réciproquement, si K est Galoisienne, elle est monogène puisque séparable, et contient toutes les racines du polynôme minimal f_α d'un générateur α. C'est donc un corps de décomposition de f_α.

i) $\Rightarrow$ *iv)*. Soit $\overline{k}$ une clôture algébrique de k. Puisque K est séparable sur k on a $|\mathrm{Hom}_{k-\mathrm{alg}}(K,\overline{k})| = [K : k]$. Fixons un plongement $\iota_1 \in \mathrm{Hom}_{k-\mathrm{alg}}(K,\overline{k})$ et considérons l'application $\mathrm{Aut}_{k-\mathrm{alg}}(K) \longrightarrow \mathrm{Hom}_{k-\mathrm{alg}}(K,\overline{k})$, $\sigma \mapsto \iota_1 \circ \sigma$. Cette application est injective puisque ι_1 est injective. Elle est aussi surjective puisque tout autre plongement $\iota_2 : K \hookrightarrow \overline{k}$ a la même image K' dans $\overline{k}$ que ι_1, si bien que la composée $\sigma : \iota_1^{-1} \circ \iota_2$ est un automorphisme de K tel que $\iota_2 = \iota_1 \circ \sigma$. On a donc $|\mathrm{Aut}(K/k)| = [K : k]$.

iv) $\Rightarrow$ *v)*. Notons $k' := K^{\mathrm{Aut}(K/k)}$, qui est évidemment un sous-corps de K contenant k. On a donc $\mathrm{Aut}(K/k') = \mathrm{Aut}(K/k)$. Choisissons un plongement $\iota : K \hookrightarrow \overline{k'}$ de K dans une clôture algébrique de k'. Alors l'application $\sigma \mapsto \iota \circ \sigma$ est une injection de $\mathrm{Aut}(K/k')$ dans $\mathrm{Hom}_{k'-\mathrm{alg}}(K,\overline{k'})$. D'après la proposition 1.5.4 on a donc $|\mathrm{Aut}(K/k')| \leqslant [K : k']$. Or, on a aussi $[K : k'] \leqslant [K : k] = |\mathrm{Aut}(K/k)| = |\mathrm{Aut}(K/k')|$. Donc $[K : k'] = [K : k]$, puis $[k' : k] = 1$ et finalement $k' = k$.

v) $\Rightarrow$ *ii)*. Soit $\alpha \in K$, et posons $g_\alpha := \prod_{\beta \in \mathrm{Aut}(K/k)\cdot\alpha}(X - \beta) \in K[X]$. On sait que g_α divise f_α puisque chaque $\beta \in \mathrm{Aut}(K/k)\alpha$ est une racine de f_α. Puisque f_α est irréductible dans $k[X]$, il nous suffira donc de montrer que $g_\alpha \in k[X]$. Pour cela, étendons l'action de $G := \mathrm{Aut}(K/k)$ à $K[X]$ comme d'habitude : G agit sur les coefficients des polynômes. Sous l'hypothèse *v)*, on voit qu'un polynôme $f \in K[X]$ est dans $k[X]$ si et seulement si il est fixe par G. Or pour tout $\sigma \in G$, on a

$$\sigma(g_\alpha) = \prod_{\beta \in G\alpha} (X - \sigma(\beta)) = \prod_{\gamma \in \sigma G\alpha} (X - \gamma) = \prod_{\gamma \in G\alpha} (X - \gamma) = g_\alpha.$$

Donc g_α est fixe par G et appartient à $k[X]$. □

2.1.3 *Exemple* (*Corps finis*)– L'extension $\mathbb{F}_{p^r} \supset \mathbb{F}_p$ est Galoisienne puisque c'est un corps de décomposition du polynôme séparable $X^{p^r} - X$. Soit F l'endomorphisme de Frobenius de $\mathbb{F}_{p^r}$, qui est un automorphisme, donc un élément de $\mathrm{Gal}(\mathbb{F}_{p^r}/\mathbb{F}_p)$. On a bien-sûr $F^r = \mathrm{id}$. De plus, pour $s < r$, on a vu que le sous-corps des points fixes $\mathbb{F}_{p^r}^{F^s}$ est l'ensemble des racines de $X^{p^s} - X$, donc de cardinal $< p^r$. Il s'ensuit que F est d'ordre r et donc que $\mathrm{Gal}(\mathbb{F}_{p^r}/\mathbb{F}_p)$ est cyclique d'ordre r, engendré par F.

2.1.4 *Exemple* (*Extensions cyclotomiques*)– L'extension n-cyclotomique d'un corps k est "le" corps de décomposition k_n du polynôme $X^n - 1$, c'est-à-dire "l'"extension engendrée par les racines n-èmes de l'unité. Si k est de caractéristique $p > 0$ et si $n = p^k n'$ avec $(n', p) = 1$, on a $X^n - 1 = (X^{n'} - 1)^{p^k}$ donc $k_n = k_{n'}$. On supposera donc que $(n, p) = 1$ sans perte de généralité. L'extension $k_n \supset k$ est Galoisienne puisque $X^n - 1$ est séparable. Cherchons à calculer $\mathrm{Gal}(k_n/k)$. Il est clair que tout $\sigma \in \mathrm{Gal}(k_n/k)$ stabilise le sous-groupe $\mu_n(k_n)$ des racines n-èmes de l'unité dans k_n, et est entièrement déterminé par son action sur $\mu_n(k_n)$ (puisque celui-ci engendre k_n sur k). De plus, σ agit par automorphismes de groupes sur $\mu_n(k_n)$, donc on obtient ainsi une injection

$$\mathrm{Gal}(k_n/k) \hookrightarrow \underset{\mathrm{grp}}{\mathrm{Aut}}(\mu_n(k_n)).$$

Maintenant, on a vu au cours de la preuve du théorème 1.5.5 que le groupe $\mu_n(k_n)$ est cyclique d'ordre n. On sait calculer le groupe des automorphismes d'un groupe cyclique

d'ordre n : si ζ_n est un générateur de $\mu_n(k_n)$ (*i.e.* une racine n-ème "primitive" de l'unité), alors $\sigma(\zeta_n)$ en est un autre générateur, donc de la forme $\zeta_n^{a_\sigma}$ pour un $a_\sigma \in \mathbb{Z}$, uniquement déterminé modulo n, et tel que $(a_\sigma, n) = 1$. On obtient ainsi une injection

$$\chi_{n,k} : \mathrm{Gal}(k_n/k) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times, \quad \sigma \mapsto (a_\sigma \,(\mathrm{mod}\, n)).$$

On ne peut pas dire grand chose de plus sans information supplémentaire sur k. Voici quelques exemples :

— $k = \mathbb{F}_p$. Dans ce cas, on sait que k_n doit être de la forme $\mathbb{F}_{p^r} = k_{p^r-1}$. Donc r est le plus petit entier tel que $n|p^r - 1$, c'est-à-dire l'ordre de p dans $(\mathbb{Z}/n\mathbb{Z})^\times$. On a vu que $\mathrm{Gal}(\mathbb{F}_{p^r}/\mathbb{F}_p)$ est cyclique d'ordre r, engendré par le Frobenius F. Il en est donc de même de $\mathrm{Gal}(k_n/k)$ et, par définition du Frobenius et de χ_n, on a $\chi_{n,\mathbb{F}_p}(F) = (p \,(\mathrm{mod}\, n))$.

— $k = \mathbb{Q}$. On a donc $\mathbb{Q}_n = \mathbb{Q}(e^{2i\pi/n})$. Si c désigne la conjugaison complexe, un automorphisme de $\mathbb{C}$ qui préserve nécessairement le sous-corps algébriquement clos $\overline{\mathbb{Q}}$ et la sous-extension normale $\mathbb{Q}_n$, alors on voit que $\chi_{n,\mathbb{Q}}(c) = (-1 \,(\mathrm{mod}\, n))$ puisque c envoie $e^{2i\pi/n}$ sur $e^{-2i\pi/n}$. En fait nous allons démontrer :

THÉORÈME. – *$\chi_{n,\mathbb{Q}}$ est un isomorphisme* $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^\times$.

D'après la discussion précédente, ceci équivaut à l'égalité

$$[\mathbb{Q}(e^{2i\pi/n}) : \mathbb{Q}] = \varphi(n) := |(\mathbb{Z}/n\mathbb{Z})^\times|$$

(indicatrice d'Euler). Pour la prouver, notons

$$\Phi_n(X) := \prod_{0 \leqslant i < n,\, (a,n)=1} (X - e^{2\pi i.a/n}) = \prod_{\zeta \,\mathrm{d'ordre}\, n} (X - \zeta) \in \overline{\mathbb{Q}}[X],$$

où le second produit est indexé par les racines n-èmes primitives de 1. On a donc la factorisation

$$X^n - 1 = \prod_{d|n} \Phi_d(X) \text{ dans } \overline{\mathbb{Q}}[X].$$

En fait, $\Phi_n(X) \in \mathbb{Q}_n[X]$ est invariant par $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$ puisque tout conjugué d'une racine primitive n-ème est une racine primitive n-ème. On a donc, d'après le v) du théorème, $\Phi_n(X) \in \mathbb{Q}[X]$ (on peut aussi le voir par récurrence grâce au produit ci-dessus). Du coup, $\mathbb{Q}_n$ est aussi un corps de décomposition de Φ_n et, puisque $\deg(\Phi_n) = \varphi(n)$, il nous suffira d'utiliser le résultat suivant vu en TD (exercice 9) :

LEMME. – Φ_n est irréductible dans $\mathbb{Q}[X]$.

2.1.5 *Exemple (Extensions radicales)*– Soit $a \in k^\times$ et $n \in \mathbb{N}$. Notons μ_n le groupe des racines n-èmes de l'unité et *supposons que* $|\mu_n| = n$ (ie k contient toutes les racines n-èmes de l'unité). Considérons une extension K de k engendrée par un élément α tel que $\alpha^n = a$ (ie $f_\alpha | X^n - a$). Alors K est le corps de décomposition du polynôme $X^n - a$ sur k. En effet,

toute autre racine de $X^n - a$ est de la forme $\alpha\zeta$ avec $\zeta \in \mu_n$, donc appartient à K. Cette observation donne aussi des informations sur $\mathrm{Gal}(K/k)$. En effet, tout $\sigma \in \mathrm{Gal}(K/k)$ est déterminé par son action sur α, qui est de la forme $\alpha\zeta_\sigma$ pour un $\zeta_\sigma \in \mu_n$. Pour un autre σ', on a alors $(\sigma'\sigma)(\alpha) = \sigma'(\alpha\zeta_\sigma) = \sigma'(\alpha)\zeta_\sigma = \alpha\zeta_{\sigma'}\zeta_\sigma$, d'où l'on tire que l'application

$$\mathrm{Gal}(K/k) \longrightarrow \mu_n,\ \sigma \mapsto \zeta_\sigma$$

est un morphisme de groupes (injectif). Comme tout sous-groupe de μ_n est un μ_m pour $m|n$, on obtient ainsi un isomorphisme

$$\mathrm{Gal}(K/k) \xrightarrow{\sim} \mu_m$$

pour $m := [K : k]$ qui montre en particulier que $\mathrm{Gal}(K/k)$ est cyclique. Cherchons à deviner m à partir de a. L'élément $N\alpha = \prod_\sigma \sigma(\alpha)$ est un élément de $K^{\mathrm{Gal}(K/k)} = k$. On a $N\alpha = \alpha^m \prod_\sigma \zeta_\sigma$, donc on voit que $\alpha^m \in k$ et donc que $a = (\alpha^m)^{n/m} \in (k^\times)^{n/m}$. On obtient ainsi que m est l'ordre de a dans le quotient $k^\times/(k^\times)^n$, et en particulier que le polynôme $X^n - a$ est irréductible dans $k[X]$ si et seulement si a est d'ordre n dans $k^\times/(k^\times)^n$. En résumé on a prouvé la première partie de :

Théorème. – *Soit k un corps tel que $|\mu_n(k)| = n$. Pour tout $a \in k$, l'extension $k[\sqrt[n]{a}]$ engendrée par une racine n-ème de a est Galoisienne de degré m égal à l'ordre de a dans $k^\times/(k^\times)^n$, et on a un isomorphisme*

$$\mathrm{Gal}(k[\sqrt[n]{a}]/k) \xrightarrow{\sim} \mu_m,\ \sigma \mapsto \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}.$$

Réciproquement, toute extension $K \supset k$ de groupe de Galois cyclique d'ordre n est de la forme $k[\sqrt[n]{a}]$ pour un $a \in k$.

Il nous reste à justifier la réciproque. Pour cela on utilise le fait que $\mathrm{Gal}(K/k) = \mathrm{Hom}_{k-\mathrm{alg}}(K, K)$ est un ensemble linéairement indépendant dans le K-ev $\mathrm{Hom}_{k-\mathrm{ev}}(K, K)$. Ceci découle du lemme général suivant appliqué à $\Gamma = K^\times$.

Lemme. – *Soient Γ un groupe et K un corps. Toute famille de caractères $\chi : \Gamma \longrightarrow K^\times$ deux à deux distincts est k-linéairement indépendante dans le K-ev K^Γ.*

Démonstration. Supposons le contraire, et choisissons une famille $\chi_1, \cdots, \chi_n$ *minimale* parmi les familles de caractères k-liées. Il existe donc $\lambda_1, \cdots, \lambda_n \in K$, tous non nuls, et tels que $L := \sum_i \lambda_i\chi_i = 0$ dans K^Γ. Pour tous $\gamma, \delta \in \Gamma$ on a $\sum_i \lambda_i\chi_i(\delta)\chi_i(\gamma) = 0$, d'où de nouvelles relations de dépendance linéaire $L_\delta := \sum_i \lambda_i\chi_i(\delta)\chi_i = 0$ pour chaque δ. Choisissons δ tel que $\chi_n(\delta) \neq \chi_1(\delta)$. En soustrayant $L_\delta - \chi_n(\delta)L$, on obtient une nouvelle relation de dépendance linéaire $\sum_i \lambda_i(\chi_i(\delta) - \chi_n(\delta))\chi_i = 0$ dont le coefficient de χ_1 est non nul, et celui de χ_n est nul, contredisant la minimalité de la famille choisie. □

Soit alors σ un générateur de $\mathrm{Gal}(K/k)$, de sorte que $\mathrm{Gal}(K/k) = \{1, \sigma, \sigma^2, \cdots, \sigma^{n-1}\}$, et soit $\zeta \in K$ une racine primitive n-ème de l'unité. L'indépendance linéaire des σ^i assure

qu'il existe $x \in K$ tel que $\alpha := x+\zeta^{-1}\sigma(x)+\cdots+\zeta^{1-n}\sigma^{n-1}(x)$ est *non nul*. Alors $\sigma(\alpha) = \zeta\alpha$, donc les $\sigma^i(\alpha) = \zeta^i\alpha$ pour $0 \leqslant i < n$ sont 2 à 2 distincts et

$$f_\alpha = \prod_{i=0}^{n-1}(X - \sigma^i(\alpha)) = \prod_{i=0}^{n-1}(X - \zeta^i\alpha) = X^n - \alpha^n.$$

En particulier, on a $\alpha^n \in k^\times$ et, puisque f_α est de degré n, on a $K = k[\alpha]$ comme voulu.

Le corollaire immédiat suivant nous sera utile :

COROLLAIRE. – *Soit k un corps tel que $|\mu_n(k)| = n$ et soit $K \supset k$ une extension engendrée par des éléments $\alpha_1, \cdots, \alpha_r$ tels que $\alpha_i^n \in k$. Alors $K \supset k$ est Galoisienne de groupe de Galois abélien.*

Démonstration. L'extension est normale puisqu'elle contient tous les conjugués des générateurs α_i (qui sont de la forme $\alpha_i\zeta_n^j$). C'est donc un corps de décomposition du polynôme $(X^n - \alpha_1)\cdots(X^n - \alpha_r)$. Elle est séparable, puisqu'engendrée par des éléments séparables. Elle est donc galoisienne. Considérons l'application

$$\mathrm{Gal}(K/k) \longrightarrow \prod_{i=1}^{r}\mathrm{Gal}(k(\alpha_i)/k),\ \sigma \mapsto (\sigma_{|k(\alpha_1)}, \cdots, \sigma_{|k(\alpha_r)}).$$

Elle est bien définie puisque chaque extension $k(\alpha_i) \supset k$ est galoisienne, elle injective puisque les α_i engendrent K, et c'est un morphisme de groupes. Donc $\mathrm{Gal}(K/k)$ est un sous-groupe d'un produit de groupes cycliques et est donc abélien. □

2.1.6 *Problèmes inverses.* Dans les exemples ci-dessus, tous les groupes de Galois étaient abéliens. L'énoncé suivant est un corollaire immédiat et utile de la caractérisation v) du théorème 2.1.2, qui montre que tout groupe fini est un groupe de Galois.

COROLLAIRE. – *Soit G un groupe fini d'automorphismes d'un corps K. Alors K^G est un corps et l'extension $K \supset K^G$ est Galoisienne de groupe* $\mathrm{Gal}(K/K^G) = G$.

Démonstration. Clairement, $G \subset \mathrm{Aut}(K/K^G)$. Donc $K^G \subset K^{\mathrm{Aut}(K/K^G)} \subset K^G$. Le v) du théorème nous dit donc que l'extension $K \supset K^G$ est Galoisienne. Reste à montrer que $G = \mathrm{Aut}(K/K^G)$. Pour cela, soit α un élément primitif de l'extension K/K^G. Son polynome minimal f_α est de degré $[K : K^G]$. Le polynôme $g_\alpha := \prod_{\beta\in G.\alpha}(X - \alpha) \in K[X]$ est invariant par G, donc est dans $K^G[X]$. Comme il annule α, il est divisible par f_α, donc de degré $\geqslant [K : K^G]$. On en déduit que $[K : K^G] \leqslant |G.\alpha| \leqslant |G|$, et donc l'inclusion $G \subset \mathrm{Aut}(K/K^G)$ est une égalité. □

Exemple. – Le groupe de permutations $\mathfrak{S}_n$ agit sur $K_n := k(X_1, \cdots, X_n)$ par permutation des indéterminées. Tout groupe fini G se plonge dans un $\mathfrak{S}_n$ (par exemple $n = |G|$ en faisant agir G sur lui-même par translations à gauche). Alors l'extension $K_n \supset K_n^G$ est Galoisienne de groupe G. On voit ainsi que tout groupe fini est un groupe de Galois. Le *problème de Galois inverse*, encore ouvert, demande quels groupes finis G peuvent être groupes de Galois d'une extension Galoisienne $K \supset \mathbb{Q}$ (on pense qu'ils le sont tous).

2.1.7 *Correspondance de Galois.* Nous allons établir une bijection remarquable entre sous-extensions d'une extension galoisienne et sous-groupes de son groupe de Galois. Commençons par le résultat suivant.

PROPOSITION. – *Soit $K \supset k$ une extension Galoisienne et $k \subset K' \subset K$ une sous-extension. Alors :*

i) K est Galoisienne sur K' et $K' = K^{\mathrm{Gal}(K/K')}$.

ii) Pour tout $\sigma \in \mathrm{Gal}(K/k)$, on a $\mathrm{Gal}(K/\sigma(K')) = \sigma\mathrm{Gal}(K/K')\sigma^{-1}$.

iii) K' est Galoisienne sur k si et seulement si $\mathrm{Gal}(K/K')$ est distingué dans $\mathrm{Gal}(K/k)$. Dans ce cas, l'application $\sigma \mapsto \sigma_{|K'}$ induit un isomorphisme

$$\mathrm{Gal}(K/k)/\mathrm{Gal}(K/K') \xrightarrow{\sim} \mathrm{Gal}(K'/k).$$

Démonstration. i) Si K est un corps de décomposition d'un polynôme séparable $f \in k[X]$ sur k, alors c'est aussi un corps de décomposition du même f sur K', lequel est toujours séparable. Donc K est Galoisienne sur K' et l'égalité $K' = K^{\mathrm{Gal}(K/K')}$ découle du v) du théorème.

ii) Soit $\tau \in \mathrm{Gal}(K/k)$. On a $\tau \in \mathrm{Gal}(K/\sigma(K')) \Leftrightarrow (\forall \alpha \in K', \tau(\sigma(\alpha')) = \sigma(\alpha')) \Leftrightarrow (\forall \alpha \in K', \sigma^{-1}\tau\sigma(\alpha) = \alpha) \Leftrightarrow \sigma^{-1}\tau\sigma \in \mathrm{Gal}(K/K')$.

iii) Si $\mathrm{Gal}(K/K')$ est distingué dans $\mathrm{Gal}(K/k)$ alors d'après ii) on a

$$\forall \sigma \in \mathrm{Gal}(K/k),\ \sigma(K') = K^{\mathrm{Gal}(K/\sigma(K'))} = K^{\sigma\mathrm{Gal}(K/K')\sigma^{-1}} = K^{\mathrm{Gal}(K/K')} = K',$$

donc K' est normale sur k. Comme elle est aussi séparable, elle est bien Galoisienne. Réciproquement, supposons K' Galoisienne sur k. Alors tout automorphisme de K/k laisse K' stable et induit donc un automorphisme de K'/k. On obtient par restriction des automorphismes, un morphisme de groupes $\sigma \mapsto \sigma_{|K'}$

$$\mathrm{Gal}(K/k) \longrightarrow \mathrm{Gal}(K'/k)$$

dont le noyau est le sous-groupe des automorphismes de K/k qui sont l'identité sur K', c'est-à-dire $\mathrm{Gal}(K/K')$, qui est donc distingué. Pour voir que ce morphisme est surjectif, on peut plonger K dans une clôture algébrique $\overline{k}$ et rappeler que la restriction $\mathrm{Gal}(\overline{k}/k) \longrightarrow \mathrm{Gal}(K'/k)$ est surjective. On peut aussi remarquer que le cardinal de l'image est $[K : k][K : K']^{-1} = [K' : k]$. □

Fixons maintenant une extension finie Galoisienne $K \supset k$. Notons $\mathcal{SE}(K)$ l'ensemble des sous-extensions $K' \supset k$ contenues dans K, ordonné par inclusion. Notons aussi $G := \mathrm{Gal}(K/k)$ et $\mathcal{SG}(G)$ l'ensemble des sous-groupes de G, lui aussi ordonné par inclusion. On a deux applications, manifestement décroissantes :

$$\begin{array}{ccc} \mathcal{SE}(K) & \to & \mathcal{SG}(G) \\ K' & \mapsto & \mathrm{Gal}(K/K') \end{array} \quad \text{et} \quad \begin{array}{ccc} \mathcal{SG}(G) & \to & \mathcal{SE}(K) \\ G' & \mapsto & K^{G'} \end{array}$$

THÉORÈME. – *Ces deux applications sont des bijections réciproques, qui échangent sous-extensions Galoisiennes et sous-groupes distingués.*

Démonstration. Découle de la proposition et du corollaire précédent. □

Exemple. – Le corps de décomposition K de X^3-2 sur $\mathbb{Q}$ est une extension Galoisienne de $\mathbb{Q}$. On a vu que $K = \mathbb{Q}(j, \sqrt[3]{2})$ est de degré 6 sur $\mathbb{Q}$, puisque de degré 2 sur $\mathbb{Q}(\sqrt[3]{2})$ qui est de degré 3 sur $\mathbb{Q}$. Donc $\mathrm{Gal}(K/\mathbb{Q})$ est un groupe d'ordre 6. Puisque $\mathrm{Gal}(K/\mathbb{Q})$ se plonge dans le groupe des permutations $\mathfrak{S}_3$ de l'ensemble $\{\sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2}\}$ qui est aussi d'ordre 6, on voit que $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathfrak{S}_3$. Donnons une autre description susceptible de se généraliser. $\mathrm{Gal}(K/\mathbb{Q})$ contient le sous-groupe $\mathrm{Gal}(K/\mathbb{Q}(j))$ d'ordre 3, donc isomorphe à $\mathbb{Z}/3\mathbb{Z}$, et le sous-groupe $\mathrm{Gal}(K/\mathbb{Q}(\sqrt[3]{2}))$, d'ordre 2 donc isomorphe à $\mathbb{Z}/2\mathbb{Z}$. Le premier est distingué puisque $\mathbb{Q}(j)$ est Galoisien sur $\mathbb{Q}$, mais pas le second. Il s'ensuit que $\mathrm{Gal}(K/\mathbb{Q})$ est un produit semi-direct

$$\mathrm{Gal}(K/\mathbb{Q}) = \mathrm{Gal}(K/\mathbb{Q}(\sqrt[3]{2})) \ltimes \mathrm{Gal}(K/\mathbb{Q}(j)) \simeq \mathbb{Z}/2\mathbb{Z} \ltimes \mathbb{Z}/3\mathbb{Z}.$$

On peut en déduire la structure des extensions intermédiaires : il y a exactement trois sous-extensions de degré 3, à savoir $\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(j\sqrt[3]{2})$ et $\mathbb{Q}(j^2\sqrt[3]{2})$, correspondant aux trois sous-groupes d'ordre 2, et une sous-extension de degré 2, Galoisienne, à savoir $\mathbb{Q}(j)$.

On peut aussi maintenant montrer que $\alpha = j + \sqrt[3]{2}$ est un générateur de K sur $\mathbb{Q}$. En effet, soit σ le générateur de $\mathrm{Gal}(K/\mathbb{Q}(\sqrt[3]{2}))$ et soit τ le générateur de $\mathrm{Gal}(K/\mathbb{Q}(j))$ qui envoie $\sqrt[3]{2}$ sur $j\sqrt[3]{2}$. Alors on calcule que l'ensemble des conjugués de $j + \sqrt[3]{2}$

$$\{\alpha, \sigma(\alpha), \tau(\alpha), \tau^2(\alpha), \sigma\tau(\alpha), \sigma\tau^2(\alpha)\} = \{j+\sqrt[3]{2}, j^2+\sqrt[3]{2}, j+j\sqrt[3]{2}, j+j^2\sqrt[3]{2}, j^2+j^2\sqrt[3]{2}, j^2+j\sqrt[3]{2}\}$$

est de cardinal 6, donc $\deg(f_\alpha) = 6$ et α engendre K sur $\mathbb{Q}$.

Voici une généralisation de cet exemple (cf aussi exercice 24 du TD) :

2.1.8 *Exemple* (*Extensions de Kummer sur* $\mathbb{Q}$)– Soit $a \in \mathbb{Q}$. On s'intéresse au groupe de Galois du corps de décomposition K de $X^n - a$ sur $\mathbb{Q}$. Puisque le ratio de deux racines n-èmes de a est une racine de l'unité, on constate facilement que $K = \mathbb{Q}[\sqrt[n]{a}, \zeta_n]$ où $\zeta_n := e^{2\pi i/n}$ et $\sqrt[n]{a}$ désigne une racine n-ème de a dans $\overline{\mathbb{Q}} \subset \mathbb{C}$. Le groupe de Galois $G := \mathrm{Gal}(\mathbb{Q}[\zeta_n, \sqrt[n]{a}]/\mathbb{Q})$ contient donc deux sous-groupes remarquables,

$$H_1 := \mathrm{Gal}(\mathbb{Q}[\zeta_n, \sqrt[n]{a}]/\mathbb{Q}[\zeta_n]) \text{ et } H_a := \mathrm{Gal}(\mathbb{Q}[\zeta_n, \sqrt[n]{a}]/\mathbb{Q}[\sqrt[n]{a}]),$$

dont l'intersection $H_1 \cap H_a$ est égale à $\{\mathrm{id}\}$ puisque ses éléments fixent ζ_n et $\sqrt[n]{a}$.

Puisque $\mathbb{Q}[\zeta_n]$ est Galoisienne sur $\mathbb{Q}$ de groupe $(\mathbb{Z}/n\mathbb{Z})^\times$, le sous-groupe H_1 est distingué de quotient $G/H_1 \simeq (\mathbb{Z}/n\mathbb{Z})^\times$, en particulier on a $|G| = |H_1|\varphi(n)$. On a aussi, d'après l'exemple 2.1.5, un plongement $H_1 \hookrightarrow \mu_n$ et on sait que $n_1 := |H_1|$ est l'ordre de a dans le quotient $\mathbb{Q}(\zeta_n)^\times/(\mathbb{Q}(\zeta_n)^\times)^n$.

Par ailleurs, on a l'égalité $|G| = |H_a|[\mathbb{Q}[\sqrt[n]{a}] : \mathbb{Q}]$, et le caractère cyclotomique nous fournit un plongement $\chi_{n,\mathbb{Q}[\sqrt[n]{a}]} : H_a \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$.

Supposons que le polynôme cyclotomique Φ_n reste irréductible dans $\mathbb{Q}[\sqrt[n]{a}][X]$. Ceci équivaut à l'égalité $[\mathbb{Q}[\sqrt[n]{a},\zeta_n] : \mathbb{Q}[\sqrt[n]{a}]] = \varphi(n)$, et donc à l'égalité $[\mathbb{Q}[\sqrt[n]{a}] : \mathbb{Q}] = n_1$ et aussi à l'égalité $|G| = |H_1||H_a|$. Ainsi, dans ce cas, G est produit semi-direct de H_1 par H_a. Utilisant les descriptions de H_1 et H_a on obtient l'isomorphisme

$$\mathrm{Gal}(\mathbb{Q}[\zeta_n, \sqrt[n]{a}]/\mathbb{Q}) \xrightarrow{\sim} \mu_{n_1} \rtimes (\mathbb{Z}/n\mathbb{Z})^\times : \ \sigma \mapsto \left(\frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}, \sigma_{|\mu_n}\right),$$

où le produit semi-direct est pris pour l'action de conjugaison de H_a sur H_1. Explicitons cette action ; pour $\sigma \in H_1$ et $\tau \in H_a$, on a $(\tau\sigma\tau^{-1})(\sqrt[n]{a}) = (\tau\sigma)(\sqrt[n]{a}) = \tau(\sqrt[n]{a}\zeta_\sigma) = \sqrt[n]{a}.\tau(\zeta_\sigma) = \sqrt[n]{a}.\zeta_\sigma^{a_\tau}$, donc c'est l'action naturelle $(a,\zeta) \mapsto \zeta^a$ de $(\mathbb{Z}/n\mathbb{Z})^\times$ sur μ_{n_1}.

Notons que l'on peut très bien avoir $n_1 = 1$ (par exemple lorsque a est une puissance n-ème dans $\mathbb{Q}$). A l'autre extrême, on a $n_1 = n$ si et seulement si $X^n - a$ est irréductible dans $\mathbb{Q}[\zeta_n][X]$ et, dans ce cas, notre hypothèse sur Φ_n est automatique puisqu'on a alors $[\mathbb{Q}[\sqrt[n]{a},\zeta_n] : \mathbb{Q}[\sqrt[n]{a}]] = n\varphi(n)[\mathbb{Q}[\sqrt[n]{a}] : \mathbb{Q}]^{-1} = \varphi(n)$.

Enfin, sans hypothèse sur Φ_n, la même formule que ci-dessus nous donne toujours un plongement $G \hookrightarrow \mu_n \rtimes (\mathbb{Z}/n\mathbb{Z})^\times$ tel que la composée $G \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ avec la projection sur $(\mathbb{Z}/n\mathbb{Z})^\times$ soit surjective. Mais l'image de ce plongement peut être délicate à décrire.

Remarque. – Si l'on part de a tel que $X^n - a$ est irréductible dans $\mathbb{Q}[X]$, alors l'hypothèse sur Φ_n ci-dessus équivaut à l'hypothèse que $X^n - a$ *reste irréductible dans* $\mathbb{Q}[\zeta_n][X]$, ce qui n'est pas facile à vérifier en pratique. Néanmoins, si n et $\varphi(n)$ sont premiers entre eux (en particulier si n est premier), alors l'égalité $|H_1|\varphi(n) = n|H_a|$ et les relations $|H_a||\varphi(n)$ et $|H_1||n$ montrent que $|H_1| = n$ et $|H_a| = \varphi(n)$, donc l'hypothèse est vérifiée.

Voici un exemple où l'hypothèse n'est pas vérifiée : prenons $a = -3$ et $n = 6$. Le polynôme $X^6 + 3$ est irréductible dans $\mathbb{Q}[X]$ (par le critère d'Eisenstein par exemple) et le corps $\mathbb{Q}[\sqrt[6]{-3}]$ contient une racine carrée de -3 donc contient $\zeta_6 = -\zeta_3$. Dans ce cas, on a donc $K = \mathbb{Q}[\sqrt[6]{-3}]$, $H_a = \{1\}$ et H_1 d'ordre 3 de quotient G/H_1 d'ordre 2. Le groupe G est d'ordre 6 non-abélien car la sous-extension $\mathbb{Q}[\sqrt[3]{-3}]$ n'est pas normale. On a donc $G \simeq \mathfrak{S}_3$. Via le plongement $G \hookrightarrow \mu_6 \rtimes (\mathbb{Z}/6\mathbb{Z})^\times$ considéré ci-dessus, G s'identifie au sous-groupe engendré par $(\zeta_3, 1)$ et $(\zeta_2, -1)$.

2.1.9 *Sous-extensions étrangères et produits semi-directs.* (cf aussi exercice 25 du TD.) Soit $K \supset k$ une extension algébrique séparable et soient K_1, K_2 des sous-extensions finies sur k. Voici un cadre général pour montrer qu'un groupe de Galois est un produit semi-direct.

PROPOSITION. – *Notons K_{12} le sous-corps de K engendré par K_1 et K_2. Les 4 propriétés suivantes sont équivalentes :*

i) $[K_{12} : k] = [K_1 : k][K_2 : k]$

ii) $[K_{12} : K_1] = [K_2 : k]$

iii) le morphisme canonique $K_1 \otimes_k K_2 \longrightarrow K_{12}$, $x_1 \otimes x_2 \mapsto x_1x_2$ est un isomorphisme.

iv) $\forall \alpha \in K_2$, le polynôme minimal $f_\alpha \in k[X]$ de α sur k reste irréductible dans $K_1[X]$.

Si de plus K_1 ou K_2 est normale sur k, alors ces propriétés sont aussi équivalentes à

v) $K_1 \cap K_2 = k$

Démonstration. L'équivalence *i)* $\Leftrightarrow$ *ii)* découle de l'égalité $[K_{12} : k] = [K_{12} : K_1][K_1 : k]$. L'équivalence *ii)* $\Leftrightarrow$ *iii)* découle de la surjectivité du morphisme considéré en *iii)* (par définition du "corps engendré") et du fait que l'extension des scalaires (ici de k à K_1) conserve la dimension.

iii) $\Rightarrow$ *iv)* L'isomorphisme considéré en *iii)* induit un isomorphisme de $K_1 \otimes_k k[\alpha]$ sur son image, qui n'est autre que $K_1[\alpha]$, ce qui montre que le degré de α sur K_1 est le même que sur k.

iv) $\Rightarrow$ *ii)* Prenons α tel que $k[\alpha] = K_2$, et notons f_α son polynôme minimal sur k. On a donc $[K_2 : k] = \deg(f_\alpha)$. Par ailleurs, on a $K_{12} = K_1[\alpha]$ et *iv)* dit que f_α est aussi le polynôme minimal de α sur K_1. Donc $[K_{12} : K_1] = \deg(f_\alpha) = [K_2 : k]$.

iv) $\Rightarrow$ *v)* ne nécessite aucune hypothèse supplémentaire. Si $\alpha \in K_1 \cap K_2$ alors le polynôme minimal de α sur K_1 est $X - \alpha$. D'après *iv)* il vit dans $k[X]$, donc $\alpha \in k$.

v) $\Rightarrow$ *iv)*. Notons d'abord que l'équivalence entre *iv)* et *i)* montre que la propriété *iv)* est symétrique si on échange les rôles de K_1 et K_2, ce qui n'est pas évident a priori. Supposons maintenant K_2 normale sur k, pour fixer les idées. Alors pour $\alpha \in K_2$, le polynôme minimal $f_\alpha \in k[X]$ de α sur k est scindé dans $K_2[X]$. Soit $g_\alpha \in K_1[X]$ le polynôme minimal de α sur K_1. Alors g_α divise f_α donc appartient à $K_2[X]$ puisque ses coefficients sont des polynômes en les racines de g_α dans K_2. Il s'ensuit que $g_\alpha \in (K_1 \cap K_2)[X] = k[X]$ et donc que $g_\alpha = f_\alpha$. □

Remarque. – L'hypothèse supplémentaire est nécessaire pour que *v)* implique les autres propriétés. Par exemple, $\mathbb{Q}(\sqrt[3]{2}) \cap \mathbb{Q}(j\sqrt[3]{2}) = \mathbb{Q}$, mais $\mathbb{Q}(\sqrt[3]{2}, j\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}], j)$ est de degré 6 et non 9.

COROLLAIRE. – *Dans le contexte de la proposition, supposons K_{12} et K_1 galoisiennes sur k. Alors* $\mathrm{Gal}(K_{12}/k)$ *est le produit semi-direct de son sous-groupe distingué* $\mathrm{Gal}(K_{12}/K_1)$ *par son sous-groupe* $\mathrm{Gal}(K_{12}/K_2)$. *Plus précisément, l'application $(\sigma, \tau) \mapsto \sigma\tau$ est un isomorphisme*

$$\mathrm{Gal}(K_{12}/K_1) \rtimes \mathrm{Gal}(K_{12}/K_2) \xrightarrow{\sim} \mathrm{Gal}(K_{12}/k)$$

où le produit semi-direct est relatif à l'action de conjugaison.

Démonstration. $\mathrm{Gal}(K_{12}/K_2)$ est en effet distingué puisque K_2 est Galoisienne. L'intersection $\mathrm{Gal}(K_{12}/K_2) \cap \mathrm{Gal}(K_{12}/K_1)$ est le sous-groupe des automorphismes qui fixent K_1 et K_2 et donc aussi le corps K_{12} qu'ils engendrent. Cette intersection est donc $\{\mathrm{id}\}$. Il s'ensuit que l'application de l'énoncé est injective. Comme les deux ensembles sont de même cardinal, elle est bijective. Enfin, la formule $(\sigma\tau)(\sigma'\tau') = (\sigma.\tau\sigma'\tau^{-1})(\tau\tau')$ montre que c'est un morphisme de groupes. □

2.1.10 *Clôture normale (Galoisienne) d'une extension.* La notion de corps de décomposition d'un polynôme a un analogue pour les extensions de corps : c'est la notion de *clôture normale.*

DÉFINITION. – *Soit $K \supset k$ une extension algébrique. On dit qu'une extension $\widetilde{K} \supset k$ est une clôture normale de K si elle est normale et engendrée par toutes les images $\iota(K)$ de k-plongements $\iota : K \hookrightarrow \tilde{K}$.*

Lorsque $K \supset k$ est une extension séparable finie, on dit aussi que $\widetilde{K} \supset k$ est une *clôture Galoisienne* de $K \supset k$. En effet dans ce cas, $\widetilde{K}$ est aussi séparable et finie sur k.

Exemple. – Le corps de décomposition d'un polynôme irréductible séparable $f \in k[X]$ est une clôture Galoisienne du corps de rupture de f.

PROPOSITION. – *Toute extension admet une clôture normale, unique à isomorphisme près.*

Démonstration. Choisissons une clôture algébrique $\overline{k}$ et notons $\widetilde{K}$ le sous-corps de $\overline{k}$ engendré par toutes les images $\iota(K)$, où $\iota \in \mathrm{Hom}_{k-\mathrm{alg}}(K, \overline{k})$. C'est clairement une clôture normale de K, et si $\widetilde{K}'$ en est une autre, on peut la plonger dans $\overline{k}$, son image par ce plongement est nécessairement $\widetilde{K}$, et on obtient ainsi un isomorphisme $\widetilde{K}' \xrightarrow{\sim} \widetilde{K}$. □

Alternativement, si K est plongé dans une clôture algébrique $\overline{k}$, sa clôture normale dans K est le corps engendré par les images $\sigma(K)$ où σ décrit $\mathrm{Aut}(\overline{k}/k)$.

Exemple. – Si $K = k(\alpha_1, \cdots, \alpha_n)$ avec $\alpha_i \in \overline{k}$, alors $\widetilde{K} = K(\{\alpha_i^{(j)}\}_{i=1,\cdots,n;j=1,\cdots r_j})$ où $\alpha_i^{(j)}$, $j = 1, \cdots, r_i$ désignent les conjugués de α_i dans $\overline{k}$. En d'autres termes K est le corps de décomposition du polynôme $f_{\alpha_1} f_{\alpha_2} \cdots f_{\alpha_n}$.

Exemple. – La clôture Galoisienne de $\mathbb{Q}(\sqrt[3]{2}, \sqrt[5]{3})$ dans $\overline{\mathbb{Q}}$ est $\mathbb{Q}(\sqrt[3]{2}, \sqrt[5]{3}, e^{2i\pi/15})$.

2.2 Résolubilité par radicaux des équations algébriques

Comme on l'a déjà mentionné dans l'introduction de ce chapitre, la théorie de Galois permet de résoudre le problème de la résolubilité par radicaux des équations algébriques. C'est ce que nous allons expliquer ici.

2.2.1 *Groupe de Galois d'un polynôme.* Soit $f \in k[X]$ un polynôme séparable. On appelle *groupe de Galois de f* le groupe de Galois G_f d'un corps de décomposition K_f de f sur k. Ce groupe permute les racines de f, et son action sur K_f est déterminée par celle sur les racines de f car celles-ci engendrent K_f. Ainsi G_f s'identifie à un sous-groupe du groupe des permutations des racines de f. Si on numérote les racines $\alpha_1, \cdots, \alpha_n$ de f dans K_f, alors G_f s'identifie à un sous-groupe de $\mathfrak{S}_n$.

LEMME. – *Le polynôme f est irréductible dans $k[X]$ si et seulement si G_f permute transitivement les racines de f dans K_f.*

Démonstration. On a déjà vu cela plusieurs fois. Répétons l'argument. Si f est irréductible et α, β sont deux racines, il existe un unique k-isomorphisme $k[\alpha] \xrightarrow{\sim} k[\beta]$ qui envoie α sur β et celui-ci se prolonge en un automorphisme $K_f \xrightarrow{\sim} K_f$ car K_f est normale. Réciproquement, la propriété ii) des extensions Galoisiennes nous dit que si G_f agit transitivement sur les racines de f, alors f est le polynôme minimal de chacune de ses racines, et en particulier est irréductible. □

Si on a au contraire une factorisation $f = f_1 f_2$ dans $k[X]$, alors soit K_{f_i} le sous-corps de K_f engendré par les racines de f_i. Puisque K_{f_i} est galoisienne sur k, on a un morphisme surjectif $G_f \twoheadrightarrow G_{f_i}$ de noyau $\mathrm{Gal}(K_f/K_{f_i})$. Le morphisme produit $G_f \longrightarrow G_{f_1} \times G_{f_2}$ est lui injectif puisque K_f est engendré par $K_{f_1}.K_{f_2}$.

2.2.2 *Résolubilité par radicaux et groupes résolubles.* Rappelons qu'un polynôme $f \in \mathbb{Q}[X]$ est dit "résoluble par radicaux" si ses racines peuvent s'exprimer en appliquant successivement des opérations parmi $+, -, \cdot, \div$ et $\sqrt[n]{x}$ à des nombres rationnels.

Définition. – *Un groupe fini G est dit résoluble s'il admet une suite décroissante $G = G_0 \supset G_1 \supset \cdots \supset G_r = \{1\}$ de sous-groupes distingués tels que G_i/G_{i+1} est abélien.*

Exercice. – Soit H un sous-groupe de G. Montrer que :
— G résoluble $\Rightarrow$ H résoluble.
— Si H est distingué, G résoluble $\Leftrightarrow$ (H et G/H résolubles).

Le théorème de Galois s'exprime ainsi :

Théorème. – *Le polynôme f est résoluble par radicaux si et seulement si son groupe de Galois est résoluble.*

Démonstration. Supposons d'abord f résoluble par radicaux. Ceci équivaut à ce que K_f soit inclus dans le "dernier étage" K_r d'une tour d'extensions $\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_r$, telle que pour tout $i = 1, \cdots, r$, on a $K_i = K_{i-1}(\alpha_i)$ avec $\alpha_i^{n_i} \in K_{i-1}$ pour un $n_i \in \mathbb{N}$. On peut choisir cette tour de sorte que K_1 soit n-cyclotomique avec n le ppcm des n_i. Alors chaque extension $K_i \supset K_{i-1}$ est Galoisienne de groupe de Galois abélien, d'après 2.1.5 et 2.1.4. Malheureusement K_i n'est pas nécessairement Galoisienne sur $\mathbb{Q}$ pour $i > 2$. Remplaçons donc K_i par sa clôture Galoisienne K_i' dans $\overline{\mathbb{Q}}$. On a donc une tour $\mathbb{Q} = K_0 \subset K_1 = K_1' \subset K_2' \subset \cdots \subset K_r'$ d'extensions Galoisiennes avec $K_i' = K_{i-1}'(\alpha_i^{(j)}, j = 1, \cdots, r_i)$ où les $\alpha_i^{(j)}$ désignent les conjugués de α_i dans $\overline{\mathbb{Q}}$. Alors $(\alpha_i^{(j)})^{n_i}$ est un conjugué de $\alpha_i^{n_i}$ donc appartient à K_{i-1}', et le corollaire 2.1.5 nous dit que $\mathrm{Gal}(K_i'/K_{i-1}')$ est abélien.

Traduisons cela via la correspondance de Galois. Notons $G_i' := \mathrm{Gal}(K_r'/K_i')$, qui est un sous-groupe de $G_0' = \mathrm{Gal}(K_r'/\mathbb{Q})$. Alors les G_i' sont distingués dans G_0', et les quotients successifs G_i'/G_{i+1}' sont abéliens. Le groupe G_0' est donc résoluble. Il s'ensuit que le groupe $G_f := \mathrm{Gal}(K_f/\mathbb{Q})$, qui est un quotient de G_0 puisque $K_f \subset K_r'$, est aussi résoluble. En effet, si $G_{f,i}$ désigne l'image de G_i' dans G_f, alors chaque $G_{f,i}$ est distingué dans G_f et les quotients successifs $G_{f,i}/G_{f,i+1}$ sont abéliens, puisque quotients de G_i/G_{i+1}.

Réciproquement, supposons maintenant que $G_f = \mathrm{Gal}(K_f/\mathbb{Q})$ est résoluble. Notons K'_f le corps engendré par K_f et les racines n-èmes de l'unité où $n = [K_f : \mathbb{Q}]$. C'est aussi une extension Galoisienne de $\mathbb{Q}$, dont le groupe de Galois G'_f se surjecte sur G_f avec noyau $\mathrm{Gal}(K'_f/K_f)$ abélien (d'ordre divisant $\varphi(n)$). Donc G'_f est aussi un groupe résoluble. Notons $G'_{f,1} := \mathrm{Gal}(K'_f/\mathbb{Q}(e^{2i\pi/n}))$, qui est un sous-groupe distingué de G'_f de quotient $G'_f/G'_{f,1}$ abélien (isomorphe à $(\mathbb{Z}/n\mathbb{Z})^\times$). Puisque G'_f est résoluble, il existe des sous-groupes $G'_{f,1} \supset G'_{f,2} \supset \cdots \supset G'_{f,r} = \{1\}$ tels que $G'_{f,i+1}$ soit distingué dans $G'_{f,i}$ de quotient $G'_{f,i}/G'_{f,i+1}$ abélien. En fait, puisque tout groupe abélien fini est produit de groupes cycliques, on peut même supposer que $G'_{f,i}/G'_{f,i+1}$ est cyclique pour $i \geqslant 1$. Notons que pour $i \geqslant 1$, l'ordre de $G'_{f,i}/G'_{f,i+1}$ divise celui de $G'_f/G'_{f,1}$ qui est égal au degré $[K'_f : \mathbb{Q}(e^{2i\pi/n})]$, lequel divise $[K_f : \mathbb{Q}] = n$. Soit alors $K'_{f,i} := (K'_f)^{G_i}$. La correspondance de Galois nous dit que la tour

$$\mathbb{Q} \subset \mathbb{Q}(e^{2i\pi/n}) = K'_{f,1} \subset K'_{f,2} \subset \cdots \subset K'_{f,r} = K'_f$$

est formée d'extensions Galoisiennes telles que $K'_{f,i}/K'_{f,i+1}$ est de groupe de Galois cyclique d'ordre n_i divisant n. D'après le théorème 2.1.5, une telle extension est de la forme $K'_{f,i} = K'_{f,i+1}(\sqrt[n_i]{a_i})$. Il s'ensuit que f est résoluble par radicaux. □

2.2.3 *Résolubilité des équations de degré au plus* 4. À l'époque de Galois, on savait déjà depuis longtemps que les polynômes de degré au plus 4 étaient résolubles par radicaux. En voici une explication conceptuelle. Soit $n := \deg(f)$. On a vu que l'action de permutation de $G_f := \mathrm{Gal}(K_f/K)$ sur l'ensemble des racines de f fournit un plongement $G_f \hookrightarrow \mathfrak{S}_n$ (une fois qu'on a numéroté les racines). Or, pour $n \leqslant 4$, le groupe $\mathfrak{S}_n$ est résoluble. En effet, $\mathfrak{S}_2 = \mathbb{Z}/2\mathbb{Z}$ est abélien, $\mathfrak{S}_3$ se surjecte sur $\mathbb{Z}/2\mathbb{Z}$ (signature) avec pour noyau $\mathfrak{A}_3 = \mathbb{Z}/3\mathbb{Z}$, et $\mathfrak{S}_4$ se surjecte sur $\mathbb{Z}/2\mathbb{Z}$ avec pour noyau $\mathfrak{A}_4$ dont le sous-groupe $\{\mathrm{id}, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$ isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$ est distingué de quotient isomorphe à $\mathbb{Z}/3\mathbb{Z}$. Comme tout sous-groupe d'un groupe résoluble est résoluble (exercice), il s'ensuit que G_f est bien résoluble dès que $\deg(f) \leqslant 4$.

2.2.4 *Non-résolubilité d'une équation de degré* 5. C'est à Abel qu'est attribué le premier exemple d'équation algébrique non résoluble par radicaux. Mais la théorie de Galois donne une explication plus conceptuelle aux exemples d'Abel.

Lemme. – *Le groupe $\mathfrak{S}_n$, $n \geqslant 5$ n'est pas résoluble.*

Démonstration. Il suffit de montrer que $\mathfrak{A}_n$ n'est pas résoluble. Pour cela, il suffit de montrer que $\mathfrak{A}_n$ ne possède aucun quotient abélien. Ceci équivaut à montrer que le sous-groupe $[\mathfrak{A}_n, \mathfrak{A}_n]$ engendré par les commutateurs $xyx^{-1}y^{-1}$ d'éléments de $\mathfrak{A}_n$ est égal à $\mathfrak{A}_n$. En effet, tout morphisme $\mathfrak{A}_n \longrightarrow G$ avec G abélien est trivial sur $[\mathfrak{A}_n, \mathfrak{A}_n]$.

Rappelons que $\mathfrak{A}_n$ est engendré par les 3-cycles. En effet, il suffit de voir que le produit de deux transpositions $\tau = (i,j)(k,l)$ est un produit de 3-cycles. Si $\{i,j\} = \{k,l\}$ on a $\tau = \mathrm{id}$, si $|\{i,j\} \cap \{k,l\}| = 1$, alors, en supposant que $j = k$ par exemple, on a $\tau = (i,j,l)$, et si $\{i,j\} \cap \{k,l\} = \emptyset$ alors $\tau = (i,j)(j,k)(j,k)(k,l) = (i,j,k)(j,k,l)$.

Il nous suffit donc de voir que tout 3-cycle est un commutateur dans $\mathfrak{A}_n$. On a la formule $(i,j,k) = (i,j)(j,k) = (i,j)(i,k)(i,j)^{-1}(i,k)^{-1}$ qui montre que (i,j,k) est un commutateur dans $\mathfrak{S}_n$. Pour passer à un commutateur dans $\mathfrak{A}_n$, choisissons, $l \neq m$ distincts de (i,j,k), ce qui est possible car $n \geqslant 5$. Alors, (l,m) commute à (i,j) et (i,k), donc en posant $\tau = (i,j)(l,m)$ et $\sigma = (i,k)(l,m)$, on a $\tau\sigma\tau^{-1}\sigma^{-1} = (i,j,k)$, et $\tau, \sigma \in \mathfrak{A}_n$. □

Remarque. – En fait, on a beaucoup mieux : pour $n \geqslant 5$, le groupe $\mathfrak{A}_n$ est *simple*, i.e. ne possède aucun sous-groupe distingué propre et non trivial.

Notre but est maintenant de produire un polynôme de degré 5 dont le groupe de Galois est $\mathfrak{S}_5$. Pour cela, le lemme suivant sera utile :

LEMME. – *Si n est premier, le groupe $\mathfrak{S}_n$ est engendré par toute paire d'éléments (σ, τ) formée d'un n-cycle et d'une transposition.*

Démonstration. Soit $\tau = (i,j)$ avec $i \neq j$. Comme n est premier, l'unique puissance de σ qui envoie i sur j est encore un n-cycle. On peut donc supposer que $j = \sigma(i)$. On a alors $\sigma^s\tau\sigma^{-s} = (\sigma^s(i), \sigma^{s+1}(i))$ pour tout $s = 0, \cdots, n-1$. Soit alors $r > s$. On a

$$\begin{aligned} & (\sigma^{r-1}(i), \sigma^r(i)) \cdots (\sigma^{s+1}(i), \sigma^{s+2}(i))(\sigma^s(i), \sigma^{s+1}(i))(\sigma^{s+1}(i), \sigma^{s+2}(i)) \cdots (\sigma^{r-1}(i), \sigma^r(i)) \\ = \; & (\sigma^s(i), \sigma^r(i)), \end{aligned}$$

ce qui montre que le sous-groupe engendré par σ et τ contient toutes les transpositions, donc est égal à $\mathfrak{S}_n$. □

Nous voulons donc trouver un polynôme de degré 5 dont le groupe de Galois contient un 5-cycle et une transposition. Remarquons alors :

LEMME. – *Soit $f \in k[X]$ séparable. Si f est irréductible de degré premier p, alors G_f contient un p-cycle du groupe des permutations des racines de f.*

Démonstration. Tout corps de rupture de f est de degré p (isomorphe à $k[X]/(f)$ puisque f est irréductible), donc $p|[K_f : k]$ et G_f contient donc un élément d'ordre p. Mais les seuls éléments d'ordre p de $\mathfrak{S}_p$ sont les p-cycles. □

Pour trouver des polynômes irréducibles, le critère suivant est très utile.

PROPOSITION. (Critère d'Eisenstein) – *Soit $f = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{Z}[X]$. Supposons qu'il existe un nombre premier p tel que p divise a_i pour tout i, mais p^2 ne divise pas a_0. Alors f est irréductible dans $\mathbb{Q}[X]$.*

Démonstration. Soit $f = gh$ une factorisation dans $\mathbb{Q}[X]$ avec g et h unitaires. On a déjà expliqué qu'on a alors $g, h \in \mathbb{Z}[X]$. Ecrivons $g = X^m + b_{m-1}X^{m-1} + \cdots + b_0$ et $h = X^r + c_{r-1}X^{r-1} + \cdots + c_0$. Alors $b_0c_0 = a_0$ donc p ne divise pas b_0 ou ne divise pas c_0. Supposons que p ne divise pas c_0 et soit k le plus petit entier tel que p ne divise pas b_k (qui existe bien puisque $b_m = 1$). Alors l'égalité $a_k = \sum_{i+j=k} b_ic_j$ montre que p ne divise pas a_k, donc $k = n$ et $h(X) = 1$. □

On voudrait maintenant un moyen de produire une transposition dans le groupe de Galois d'un polynôme irréductible de $\mathbb{Q}[X]$. L'astuce pour cela est d'utiliser la conjugaison complexe, qui au moins fournit un automorphisme d'ordre 2. Supposons en effet que f possède exactement 2 racines dans $\mathbb{C} \setminus \mathbb{R}$. Alors la conjugaison complexe permute ces deux racines et fixe toutes les autres. Elle fournit donc une transposition dans G_f.

COROLLAIRE. – *Le groupe de Galois du polynôme $f = X^5 - 10X + 5 \in \mathbb{Q}[X]$ est $\mathfrak{S}_5$. En particulier, f n'est pas résoluble par radicaux.*

Démonstration. Le critère d'Eisenstein avec $p = 5$ montre que f est irréductible dans $\mathbb{Q}[X]$, donc le dernier lemme assure que G_f contient un 5-cycle. Par ailleurs, le tableau des variations de la fonction $\mathbb{R} \longrightarrow \mathbb{R}$, $x \mapsto f(x)$ montre que f a trois racines réelles, donc G_f contient une transposition. Il s'ensuit que $G_f \simeq \mathfrak{S}_5$. □

2.3 Nombres constructibles à la règle et au compas

Voici une autre illustration des implications de la théorie de Galois sur des problèmes classiques de l'antiquité. Cf aussi exercice 2 du TD.

DÉFINITION. – *Dans le plan euclidien $\mathbb{R}^2$, un point P est dit :*
- *0-constructible si $P \in \{(0,0),(1,0)\}$*
- *n-constructible s'il est $(n-1)$-constructible ou s'il existe des points $n-1$-constructibles $A \neq B$ et $C \neq D$ tels que P soit dans l'une des intersections suivantes, supposée transverse :*
  - *des droites (AB) et (CD)*
  - *ou de la droite (AB) et du cercle de centre C passant par D*
  - *ou des cercles de centres respectifs C et A, passant respectivement par D et B.*

Un nombre complexe $z \in \mathbb{C}$ est dit constructible *si le point correspondant est n-constructible pour un $n \in \mathbb{N}$.*

La géométrie élémentaire classique nous apprend à projeter un point orthogonalement sur une droite à la règle et au compas, ce dont on déduit :

LEMME. – *Un complexe est constructible si et seulement si ses parties réelles et imaginaires le sont.*

Notons $E \subset \mathbb{C}$ l'ensemble des nombres constructibles.

THÉORÈME. – *E est un sous-corps de $\mathbb{C}$ stable par extraction de racine carrée.*

Démonstration. Exercice. La stabilité par soustraction est claire, utiliser Thalès pour la multiplication de réels, la construction de l'inversion géométrique pour le passage à l'inverse, puis Pythagore pour la racine carrée d'un réel positif (en utilisant l'égalité $(x+1)^2 = (x-1)^2 + 4x$). □

L'équation d'un cercle et celle d'une droite montrent que les coordonnées de leurs point(s) d'intersection sont solutions d'une équation du second degré en les coordonnées

des points utilisés pour définir le cercle et la droite. Les nombres constructibles sont donc algébriques. Plus précisément, on a :

THÉORÈME. (Wantzel) – *Un complexe z est constructible si et seulement si il existe une suite de corps $K_0 = \mathbb{Q} \subset K_1 \subset \cdots \subset K_r$ tels que $[K_i : K_{i-1}] = 2$ et $z \in K_r$.*

Démonstration. Exercice. On remarquera que toute extension quadratique est obtenue par extraction d'une racine carrée. □

Ici intervient la théorie de Galois, et notamment la notion de conjugué.

THÉORÈME. – *Un nombre algébrique $z \in \overline{\mathbb{Q}}$ est constructible si et seulement si l'extension algébrique de $\mathbb{Q}$ engendrée par ses conjugués est de degré une puissance de 2.*

Démonstration. Remarquons tout d'abord que si z est constructible alors ses conjugués le sont aussi. En effet, si $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ et si $K_0 = \mathbb{Q} \subset K_1 \subset \cdots \subset K_r$ est une tour d'extensions quadratiques contenant z, alors $\sigma(K_0) = \mathbb{Q} \subset \sigma(K_1) \subset \cdots \subset \sigma(K_r)$ est une tour d'extensions quadratiques contenant $\sigma(z)$. Soit alors K_z le corps engendré par les conjugués de z. Il est contenu dans E et engendré par un élément primitif α. Puisque α est constructible, il est contenu dans une tour d'extensions quadratiques, donc K_z aussi, et K_z est bien de degré une puissance de 2.

Réciproquement, supposons que le corps K_z est de degré une puissance de 2. Comme c'est le corps de décomposition du polynôme minimal f_z de z, c'est une extension Galoisienne dont le groupe de Galois G_z est un 2-groupe. Or, tout 2-groupe possède un sous-groupe (distingué) d'indice 2. Inductivement, il existe donc une suite décroissante $G_0 = G_z \supset G_1 \supset \cdots \supset G_r = \{1\}$ de sous-groupes de G_z telle que $[G_i : G_{i+1}] = 2$. En prenant les corps de points fixes $K_i = K_z^{G_i}$, on obtient une tour d'extensions quadratiques comme dans le théorème précédent. □

Ce résultat s'applique au problème classique de savoir quels polygones réguliers peuvent être construits à la règle et au compas. Si n est le nombre de côtés, c'est équivalent à déterminer si $\exp(2i\pi/n)$ est constructible. Par le théorème précédent, c'est encore équivalent à ce que $[\mathbb{Q}(\exp(2i\pi/n)) : \mathbb{Q}]$ soit de degré une puissance de 2. Or on a vu que $[\mathbb{Q}(\exp(2i\pi/n)) : \mathbb{Q}] = \varphi(n)$. Par la formule usuelle de $\varphi(n)$, on obtient donc :

COROLLAIRE. – *Un polygone régulier à n côtés est constructible à la règle et au compas si et seulement si $n = 2^a p_1 p_2 \cdots p_r$ avec p_i des premiers distincts de la forme $p_i = 1 + 2^{a_i}$.*

Remarquons que pour que $p = 1 + 2^a$ soit premier, il faut que a soit lui-même une puissance de 2. En effet, si on écrit $a = 2^b m$ avec m impair, on a $1 + 2^a = 1 - (-2^{2^b})^m$ qui est divisible par $1 + 2^{2^b}$. Les nombres de la forme $p = 1 + 2^{2^b}$ sont appelés "nombres de Fermat" car Fermat avait émis l'hypothèse qu'ils soient tous premiers, ce qui est vrai jusqu'à $b = 4$, mais faux pour $5 \leqslant b \leqslant 23$ et inconnu au-delà. En particulier, 17 est un nombre de Fermat premier, et la constructibilité du polygone régulier à 17 côtés avait été établie par Gauss.

2.4 Spécialisation et applications

2.4.1 Soit A un anneau principal de corps des fractions K. Fixons un élément irréductible $p \in A$ et notons $k = A/pA$ le corps résiduel.

Soit maintenant $f \in A[X]$ un polynôme unitaire et soit K_f "son" corps de décomposition sur K. On a donc une décomposition $f = (X - \alpha_1) \cdots (X - \alpha_n)$ dans $K_f[X]$.

Notons $A_f := A[\alpha_1, \cdots, \alpha_n]$ la sous-A-algèbre de K_f engendrée par les racines α_i de f.

LEMME. – *En tant que A-module, A_f est libre de rang $[K_f : K]$.*

Démonstration. Par définition, A_f est le A-module engendré par tous les monômes $\alpha_1^{n_1} \cdots \alpha_n^{n_n}$ avec $n_1, \cdots, n_n \in \mathbb{N}$. Mais puisque chaque α_i est annulé par f, qui est unitaire de degré n, on a $\alpha_i^m \in A + A\alpha_i + \cdots + A\alpha_i^{n-1}$ pour tout $m \in \mathbb{N}$. On en déduit que A_f est engendré par les monômes $\alpha_1^{n_1} \cdots \alpha_n^{n_n}$ avec $n_1, \cdots, n_n < n$. En particulier, A_f est un A-module de type fini. Comme il est contenu dans un K-espace vectoriel, il est sans torsion. Donc il est libre de rang fini et on a $\mathrm{rg}_A(A_f) \leqslant \dim_K(K_f)$ avec égalité si A_f engendre K_f comme K-espace vectoriel, ce qui est bien le cas par définition. □

Notons $\overline{f}$ l'image de f dans $k[X]$. Soit $\mathfrak{m} \subset A_f$ un idéal maximal de A_f qui contient p, et soit $k_f := A_f/\mathfrak{m}$ le corps résiduel. C'est une extension finie de $A/pA = k$, engendrée par les images $\overline{\alpha}_i$ des α_i. La factorisation $\overline{f} = (X - \overline{\alpha}_1) \cdots (X - \overline{\alpha}_n)$ montre donc que k_f est un corps de décomposition de $\overline{f}$ sur k.

LEMME. – *Si $\overline{f}$ est séparable dans $k[X]$, alors f est séparable dans $K[X]$.*

Démonstration. Si $\overline{f}$ est séparable, les $\overline{\alpha}_i$ sont tous distincts, donc les α_i aussi et f est séparable aussi. □

Nous supposons dorénavant que $\overline{f}$ est séparable. Notons $G_f = \mathrm{Gal}(K_f/K)$ et $G_{\overline{f}} := \mathrm{Gal}(k_f/k)$ les groupes de Galois correspondants. Notre but est de comparer G_f et $G_{\overline{f}}$.

L'action de G_f sur K_f stabilise manifestement A_f puisqu'elle permute les α_i. Cette action induit à son tour une action sur l'ensemble des idéaux de A_f qui stabilise l'ensemble $\mathrm{Max}(A_f)$ des idéaux maximaux, ainsi que le sous-ensemble $\mathrm{Max}(A_f/p)$ des idéaux maximaux contenant p. Notons alors $G_{f,\mathfrak{m}}$ le fixateur de l'élément $\mathfrak{m} \in \mathrm{Max}(A_f/p)$. On a donc $G_{f,\mathfrak{m}} = \{\sigma \in G_f, \sigma(\mathfrak{m}) = \mathfrak{m}\}$, donc $G_{\mathfrak{m},f}$ est aussi le stabilisateur de $\mathfrak{m}$ dans G_f. L'action de $G_{f,\mathfrak{m}}$ sur A_f par automorphisme de A-algèbres passe alors au quotient pour donner une action sur k_f par automorphismes de A/p-algèbres. On a donc un morphisme $G_{f,\mathfrak{m}} \longrightarrow G_{\overline{f}}$, $\sigma \mapsto \overline{\sigma}$ caractérisé par $\forall a \in A_f, \overline{\sigma}(\overline{a}) = \overline{\sigma(a)}$ où $\overline{a}$ désigne la réduction de a modulo $\mathfrak{m}$.

THÉORÈME. – *Le morphisme $G_{f,\mathfrak{m}} \longrightarrow G_{\overline{f}}$ est un isomorphisme.*

Démonstration. En suivant l'action sur les racines, on constate que ce morphisme s'inscrit

dans le diagramme commutatif suivant :

$$\begin{array}{ccccc} G_{f,\mathfrak{m}} & \hookrightarrow & G_f & \hookrightarrow & \mathfrak{S}_{\{\alpha_1,\cdots,\alpha_n\}} = \mathfrak{S}_n \\ & \searrow^{\sigma\mapsto\overline{\sigma}} & & & \| \\ & & G_{\overline{f}} & \hookrightarrow & \mathfrak{S}_{\{\overline{\alpha}_1,\cdots,\overline{\alpha}_n\}} = \mathfrak{S}_n \end{array}.$$

Son injectivité en découle immédiatement, et en particulier l'inégalité $|G_{f,\mathfrak{m}}| \leqslant |G_{\overline{f}}|$.

Par ailleurs, soit $M := G_f \cdot \mathfrak{m} \subset \mathrm{Max}(A_f/pA_f)$ l'orbite de l'idéal maximal $\mathfrak{m}$ sous G_f. Le théorème des restes chinois nous donne un morphisme surjectif de k-algèbres

$$A_f/pA_f \twoheadrightarrow \prod_{\mathfrak{n}\in M} A_f/\mathfrak{n},$$

d'où l'inégalité $\dim_k(A_f/pA_f) = [K_f : K] = |G_f| \geqslant \sum_{\mathfrak{n}\in M} \dim_k(A_f/\mathfrak{n})$. Or chaque $A_f/\mathfrak{n}$ est un corps de décomposition de f, donc $\dim_k(A_f/\mathfrak{n}) = [k_f : k] = |G_{\overline{f}}|$. Puisque $|M| = [G_f : G_{f,m}]$, l'inégalité devient $|G_f| \geqslant [G_f : G_{f,m}]|G_{\overline{f}}|$, et implique donc l'inégalité $|G_{f,m}| \geqslant |G_{\overline{f}}|$. Puisqu'on a déjà vu l'autre inégalité, on a $|G_{\overline{f}}| = |G_{f,\mathfrak{m}}|$, et donc le morphisme de l'énoncé est aussi bijectif. □

Remarque. – Sous l'hypothèse $\overline{f}$ séparable, le théorème nous fournit donc un plongement $i_{\mathfrak{m}} : G_{\overline{f}} \hookrightarrow G_f$. Ce plongement dépend a priori de deux choix : d'une part le choix de $\mathfrak{m}$ et d'autre part celui d'un isomorphisme de k-extensions $A_f/\mathfrak{m} \xrightarrow{\sim} k_{\overline{f}}$. Si l'on fixe $\mathfrak{m}$, le plongement $i_{\mathfrak{m}}$ n'est donc bien défini qu'à "conjugaison à la source près". Que se passe-t-il si maintenant on choisit un autre $\mathfrak{m}'$? La preuve ci-dessus implique que le morphisme $A_f/pA_f \twoheadrightarrow \prod_{\mathfrak{n}\in M} A_f/\mathfrak{n}$ est un isomorphisme, ce qui signifie que $M = \mathrm{Max}(A_f/pA_f)$, i.e. que G_f agit transitivement sur $\mathrm{Max}(A_f/pA_f)$. Il existe donc $\sigma \in G_f$ tel que $\sigma(\mathfrak{m}) = \mathfrak{m}'$. On a alors $\sigma G_{f,\mathfrak{m}}\sigma^{-1} = G_{f,\mathfrak{m}'}$, et les plongements $i_{\mathfrak{m}'}$ et $\tau \mapsto \sigma i_{\mathfrak{m}}(\tau)\sigma^{-1}$ de $G_{\overline{f}}$ dans G_f sont conjugués "à la source". En d'autre termes, on a construit une *classe de conjugaison canonique* de plongements $G_{\overline{f}} \hookrightarrow G_f$.

2.4.2 *Application aux polynômes dans* $\mathbb{Z}[X]$. Supposons ici $A = \mathbb{Z}$. Dans ce cas $k = \mathbb{F}_p$ et on sait que $G_{\overline{f}}$ est cyclique engendré par le Frobenius F. Soit alors $\overline{f} = \overline{f}_1\overline{f}_2\cdots\overline{f}_r$ la décomposition de $\overline{f}$ en produit d'irréductibles dans $\mathbb{F}_p[X]$, et soit $n_i := \deg(\overline{f}_i)$. Cela correspond à une partition de l'ensemble des racines

$$R(\overline{f}) = \{\overline{\alpha}_1, \cdots, \overline{\alpha}_n\} = \bigsqcup_{i=1}^{r} R(\overline{f}_i).$$

Cette partition est respectée par F, et F agit transitivement sur chaque $R(\overline{f}_i)$. Ainsi, l'image de F dans $\mathfrak{S}_n$ est un produit $c_1\cdots c_r$ de cycles disjoints de longueurs respectives $n_1, \cdots, n_r$. On a donc prouvé :

Corollaire. – *Soit $f \in \mathbb{Z}[X]$ de degré n et p premier tel que $\overline{f} \in \mathbb{F}_p[X]$ est séparable et de décomposition en irréductibles $\overline{f} = \overline{f}_1\overline{f}_2\cdots\overline{f}_r$. Alors G_f, vu comme sous-groupe de $\mathfrak{S}_n$, contient un produit $c_1\cdots c_r$ de cycles disjoints de longueurs respectives* $\deg(\overline{f}_i)$.

Pour appliquer cet énoncé, il faut donc être capable de factoriser $\overline{f}$. Pour cela, il est utile de remarquer que $\overline{f}$ possède un facteur irréductible de degré r si et seulement si il admet une racine dans $\mathbb{F}_{p^r}$ qui n'est dans aucun $\mathbb{F}_{p^s}$ pour $s|r$, $s \neq r$. Par ailleurs, $\overline{f}$ admet une racine dans $\mathbb{F}_{p^r}$ si et seulement si il n'est pas premier à $X^{p^r} - X$, ce qui peut se vérifier par divisions euclidiennes successives et/ou un peu d'astuce.

Exemple. – Condidérons le polynôme $f = X^5 - X - 1$.

– Modulo 2. On vérifie que $\overline{f}$ n'a pas de racine dans $\mathbb{F}_2$, mais il en a deux dans $\mathbb{F}_4$ puisque $\overline{f} \equiv X^2 - X - 1 \,(\mathrm{mod}\,(\mathrm{X}^4 - \mathrm{X}))$ et $\overline{f}_1 := X^2 - X - 1 = X^2 + X + 1 | X^4 - X$. Il s'ensuit que $\overline{f} = \overline{f}_1 \overline{f}_2$ avec $\overline{f}_2$ irréductible de degré 3. Le corollaire nous dit que G_f contient une permutation de type $(2, 3)$, et le cube de cette permutation est donc une transposition.

– Modulo 3. On vérifie que $\overline{f}$ n'a pas de racine dans $\mathbb{F}_3$, donc pas de facteur de degré 1. Puis on calcule le pgcd avec $X^9 - X$ (d'abord avec $X^4 - 1$ puis avec $X^4 + 1$) pour constater que $\overline{f}$ n'a pas de racine dans $\mathbb{F}_9$, donc pas de facteur de degré 2. Il s'ensuit que $\overline{f}$ est irréductible et G_f contient donc un 5-cycle.

– Conclusion. $G_f \simeq \mathfrak{S}_5$.

Exemple. (Corps cyclotomiques) – Considérons le polynôme cyclotomique $f = \Phi_n$. Le polynôme $f \bmod p$ est séparable si p ne divise pas n (la réciproque est vraie sauf si $p = 2$ et n est congru à 2 modulo 4). Comme le groupe de Galois $G_f = (\mathbb{Z}/n\mathbb{Z})^\times$ est abélien, le plongement $\iota : G_{\overline{f}} \hookrightarrow G_f$ construit dans le théorème est canonique (et pas seulement à conjugaison près). On voudrait calculer l'image du Frobenius $\iota(F)$ à travers l'isomorphisme $G_f \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^\times$ donné par le caractère cyclotomique $\chi_{n,\mathbb{Q}}$. Pour cela, on constate sur la construction de ι et les définitions de $\chi_{n,\mathbb{Q}}$ et $\chi_{n,\mathbb{F}_p}$ que le diagramme suivant est commutatif

$$\begin{array}{ccc} G_f & \xrightarrow{\chi_{n,\mathbb{Q}}} & (\mathbb{Z}/n\mathbb{Z})^\times = \mathrm{Aut}(\mu_n) \subset \mathfrak{S}_{\{\text{rac. prim. } n^{emes} \text{ de } 1\}} \\ \iota \uparrow & & \| \\ G_{\overline{f}} & \xrightarrow{\chi_{n,\mathbb{F}_p}} & (\mathbb{Z}/n\mathbb{Z})^\times = \mathrm{Aut}(\mu_n) \subset \mathfrak{S}_{\{\text{rac. prim. } n^{emes} \text{ de } 1\}} \end{array} .$$

On a donc $\chi_{n,\mathbb{Q}}(\iota(F)) = \chi_{n,\mathbb{F}_p}(F) = p \in (\mathbb{Z}/n\mathbb{Z})^\times$. On peut en déduire la forme de la factorisation de la réduction $\bar{\Phi}_n$ dans $\mathbb{F}_p[X]$ (toujours sous l'hypothèse $(p, n) = 1$). En effet, soit r l'ordre de p dans $(\mathbb{Z}/n\mathbb{Z})^\times$. Alors les orbites de l'action de p sur les racines primitives n-èmes de l'unité donnée par $\xi \mapsto \xi^p$ sont de cardinal r et il y en a $s := \varphi(n)/r$. Il s'ensuit que $\bar{\Phi}_n = f_1 \cdots f_s$ dans $\mathbb{F}_p[X]$ avec f_i irréductibles de degré r premiers entre eux deux à deux. En particulier :

— $\bar{\Phi}_n$ est scindé dans $\mathbb{F}_p[X]$ si et seulement si $p \equiv 1[n]$.

— $\bar{\Phi}_n$ est irréductible dans $\mathbb{F}_p[X]$ si et seulement si p est un générateur de $(\mathbb{Z}/n\mathbb{Z})^\times$ (et on voit donc que Φ_n n'est jamais irréductible dans $\mathbb{F}_p[X]$ si $(\mathbb{Z}/n\mathbb{Z})^\times$ n'est pas cyclique).

Exemple. (Corps quadratiques) – Soit $d \in \mathbb{Z}$ sans facteur carré et $f = X^2 - d$. Si l'on choisit une racine carrée $\sqrt{d}$ dans $\overline{\mathbb{Q}}$, alors $K_f = \overline{\mathbb{Q}}[\sqrt{d}]$ et l'application $\varepsilon_{d,\mathbb{Q}} : \sigma \mapsto \frac{\sigma(\sqrt{d})}{\sqrt{d}}$ est un isomorphisme $G_f \xrightarrow{\sim} \{\pm 1\}$ qui ne dépend pas du choix de $\sqrt{d}$. On voit que $\overline{f} =$

$f \bmod p$ est séparable si et seulement si $(p, 2d) = 1$. Dans ce cas, puisque G_f est abélien, le plongement $\iota : G_{\overline{f}} \hookrightarrow G_f$ est encore canonique et on aimerait calculer $\iota(F)$. Pour cela, on vérifie sur la construction que le diagramme suivant est commutatif

$$\begin{array}{ccc} G_f & \xrightarrow{\varepsilon_{d,\mathbb{Q}}} & \{\pm 1\} \\ \uparrow{\scriptstyle \iota} & & \| \\ G_{\overline{f}} & \xrightarrow{\varepsilon_{d,\mathbb{F}_p}} & \{\pm 1\} \end{array}.$$

On a donc $\varepsilon_{d,\mathbb{Q}}(\iota(F)) = \varepsilon_{d,\mathbb{F}_p}(F)$. Concrètement, on a $\varepsilon_{d,\mathbb{F}_p}(F) = -1$ si et seulement si $\overline{f} = X^2 - \overline{d}$ est irréductible, c'est-à-dire si et seulement si d n'est pas un carré modulo p. Il s'ensuit que le signe $\varepsilon_{d,\mathbb{F}_p}(F)$ n'est autre que le symbole de Legendre $\left(\frac{d}{p}\right)$.

Application. (Loi de réciprocité quadratique) – Soit q un premier impair. Un calcul élémentaire montre que

$$\prod_{0 \leqslant i < j < q} (\zeta_q^i - \zeta_q^j)^2 = (-1)^{\frac{q(q-1)}{2}} q^q = (-1)^{\frac{q-1}{2}} q^q.$$

Il s'ensuit que $\mathbb{Q}(\zeta_q) \supset \mathbb{Q}(\sqrt{q^*})$ où on a posé $q^* = (-1)^{\frac{q-1}{2}} q$. Par la correspondance de Galois, on a donc un morphisme surjectif $\mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}(\sqrt{q^*})/\mathbb{Q})$. Via le caractère cyclotomique $\chi_{q,\mathbb{Q}}$ et le caractère quadratique $\varepsilon_{q^*,\mathbb{Q}}$, ce morphisme devient un morphisme surjectif $(\mathbb{Z}/q\mathbb{Z})^\times \twoheadrightarrow \{\pm 1\}$. Mais puisque q est premier, le groupe $(\mathbb{Z}/q\mathbb{Z})^\times$ est cyclique, donc il existe un unique tel morphisme surjectif, et de plus, son noyau est le sous-groupe des carrés dans $(\mathbb{Z}/q\mathbb{Z})^\times$ (ie l'image de $x \mapsto x^2$).

Notons maintenant $f = \Phi_q$ et $g = X^2 - q^*$, fixons p premier impair différent de q, et notons $\overline{f}$, $\overline{g} \in \mathbb{F}_p[X]$ les réductions de f et g. Alors $\overline{f}$ et $\overline{g}$ sont séparables et $k_{\overline{f}}$ contient un corps de décomposition $k_{\overline{g}}$ de $\overline{g}$ (puisqu'on a toujours $(\prod_{i<j}(\zeta_q^i - \zeta_q^j))^2 = (q^*)^q$). D'où un morphisme surjectif $G_{\overline{f}} \twoheadrightarrow G_{\overline{g}}$. On vérifie à nouveau sur leur construction que les plongements ι sont compatibles à ces morphismes surjectifs, i.e. que le diagramme suivant est commutatif

$$\begin{array}{ccc} G_f & \twoheadrightarrow & G_g \\ \uparrow{\scriptstyle \iota_f} & & \uparrow{\scriptstyle \iota_g} \\ G_{\overline{f}} & \twoheadrightarrow & G_{\overline{g}}. \end{array}$$

(pour cela, on remarque que $A_f = \mathbb{Z}[\zeta_q]$ contient $A_g = \mathbb{Z}[\delta_q]$ où $\delta_q = \prod_{i<j}(\zeta_q^i - \zeta_q^j)$ et que si $\mathfrak{m}_f \in \mathrm{Max}(A_f)$ contient p alors $\mathfrak{m}_g := \mathfrak{m} \cap A_g \in \mathrm{Max}(A_g)$ et contient toujours p, de sorte que la surjection $G_f \longrightarrow G_g$ envoie $G_{f,\mathfrak{m}_f}$ dans $G_{g,\mathfrak{m}_g}$.)

Il s'ensuit que la surjection $(\mathbb{Z}/q\mathbb{Z})^\times \twoheadrightarrow \{\pm 1\}$ envoie $\overline{p}$ sur $\left(\frac{q^*}{p}\right)$. On en déduit la propriété remarquable suivante : *q^* est un carré dans $\mathbb{F}_p^\times$ si et seulement si p est un carré dans $\mathbb{F}_q^\times$*. Autrement dit $\left(\frac{q^*}{p}\right) = \left(\frac{p}{q}\right)$. Un petit calcul utilisant la multiplicativité

$\left(\frac{d_1 d_2}{p}\right) = \left(\frac{d_1}{p}\right)\left(\frac{d_2}{p}\right)$ et le fait (élémentaire) que $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ montre alors la fameuse "loi de réciprocité quadratique"

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Remarque culturelle. (Le théorème de Chebotarev) – Comme remarqué plus haut, le théorème de spécialisation nous fournit, pour chaque premier p tel que $\overline{f} := f \bmod p$ est séparable, une *classe de conjugaison canonique* de plongements $G_{\overline{f}} \hookrightarrow G_f$. Les images du Frobenius $F \in G_{\overline{f}}$ dans G_f sont appelées *substitutions de Frobenius* et forment une classe de conjugaison C_p dans G_f. Le théorème de Chebotarev (conjecturé par Frobenius qui avait prouvé un résultat un peu plus faible) affirme que pour toute classe de conjugaison C de G_f, l'ensemble des premiers p tels que $C = C_p$ est infini, et a même pour densité "naturelle" $|C|/|G|$, ce qui signifie que la suite

$$\frac{|\{p \leqslant N, C = C_p\}|}{|\{p \leqslant N\}|} \underset{N \mapsto \infty}{\longrightarrow} \frac{|C|}{|G|}.$$

Dans le cas particulier de $f = \Phi_n$, on a $G_f \simeq (\mathbb{Z}/n\mathbb{Z})^\times$ abélien, donc une classe de conjugaison est un singleton $C = \{\bar{a}\}$ pour un $a \in \mathbb{Z}$ premier à n. Alors, vu le calcul de $\iota(F)$ ci-dessus, on a $C = C_p$ si et seulement si $p \equiv a[n]$. On retrouve ainsi le théorème de densité de Dirichlet, qui affirme que l'ensemble des premiers congrus à a modulo n est infini, de densité $1/\varphi(n)$. En fait, les idées de Dirichlet sont utilisées dans la preuve de Chebotarev.

Dans le cas particulier $f = X^2 - d$, le théorème de Chebotarev nous dit que d est un carré dans $\mathbb{F}_p$ pour "la moitié" des nombres premiers p (ie pour p dans un sous-ensemble de densité $1/2$).

2.4.3 *Un théorème de Hilbert.* Supposons ici $A = \mathbb{Q}[T]$. Tout élément $t \in \mathbb{Q}$ fournit une spécialisation de $f_T(X) \in A[X]$ en un polynôme $f_t(X) \in \mathbb{Q}[X]$, et le théorème précédent nous fournit un plongement $G_{f_t} \hookrightarrow G_{f_T}$, unique à conjugaison près. Hilbert a prouvé le théorème suivant, que nous citons pour la culture.

THÉORÈME. – *Supposons f_T irréducible dans $\mathbb{Q}(T)[X]$. Alors l'ensemble des $t \in \mathbb{Q}$ pour lesquels $G_{f_t} \xrightarrow{\sim} G_{f_T}$ est infini.*

Notons que pour un t comme dans le théorème, f_t est irréductible puisque l'action de G_{f_t} sur les racines est transitive comme celle de G_{f_T}. Notons aussi que le même énoncé est trivialement faux si on remplace $\mathbb{Q}$ par $\mathbb{C}$ ou $\mathbb{F}_p$.

2.5 Polynômes symétriques et résolvantes

Considérons maintenant le corps $K = k(a_1, \cdots, a_n)$ des fractions rationnelles en n indéterminées, et le polynôme $f = X^n + a_1 X^{n-1} + \cdots + a_n \in K[X]$. Nous allons montrer que ce polynôme est séparable sur K et son groupe de Galois est $G_f = \mathfrak{S}_n$.

2.5.1 *Actions du groupe symétrique.* Faisons agit $\mathfrak{S}_n$ sur $\mathbb{N}^n$ par la formule

$$\sigma \cdot \nu = ((\sigma \cdot \nu)_1, \cdots, (\sigma \cdot \nu)_n) \text{ avec } (\sigma \cdot \nu)_i := \nu_{\sigma^{-1}(i)} \text{ si } \nu = (\nu_1, \cdots, \nu_n).$$

On a alors l'égalité $(\sigma\sigma') \cdot \nu = \sigma \cdot (\sigma' \cdot \nu)$ qui montre qu'on a ainsi défini une action à gauche de $\mathfrak{S}_n$ sur $\mathbb{N}^n$.

Par la propriété universelle de l'algèbre de monoïde $\mathbb{Z}[\mathbb{N}^n]$ cette action s'étend en une action de $\mathfrak{S}_n$ sur $\mathbb{Z}[\mathbb{N}^n]$ par automorphisme d'anneaux. Explicitement, on a

$$\sigma(f) = \sum_{\nu \in \mathbb{N}^n} a_\nu X^{\sigma \cdot \nu} = \sum_{\nu \in \mathbb{N}^n} a_{\sigma^{-1} \cdot \nu} X^\nu \quad \text{pour } f = \sum_{\nu \in \mathbb{N}^n} a_\nu X^\nu.$$

Identifions $\mathbb{Z}[\mathbb{N}^n]$ à $\mathbb{Z}[X_1, \cdots, X_n]$ comme dans ..... On a donc $X^\nu = X_1^{\nu_1} \cdots X_n^{\nu_n}$ et

$$X^{\sigma \cdot \nu} = X_1^{\nu_{\sigma^{-1}(1)}} \cdots X_n^{\nu_{\sigma^{-1}(n)}} = X_{\sigma(1)}^{\nu_1} \cdots X_{\sigma(n)}^{\nu_n}.$$

Il s'ensuit que $\sigma(X_i) = X_{\sigma(i)}$ pour tout i. En d'autres termes, l'automorphisme $f \mapsto \sigma(f)$ de l'anneau $\mathbb{Z}[X_1, \cdots, X_n]$ est l'unique automorphisme tel que $\sigma(X_i) := X_{\sigma(i)}$.

2.5.2 *Polynômes symétriques élémentaires.* Pour $j = 1, \cdots, n$, on pose

$$\Sigma_j := \sum_{1 \leqslant i_1 < \cdots < i_j \leqslant n} X_{i_1} X_{i_2} \cdots X_{i_j} = \sum_{\substack{I \subset \{1, \cdots, n\} \\ |I| = j}} X_I \text{ avec } X_I := \prod_{i \in I} X_i.$$

Par exemple on a $\Sigma_1 = X_1 + X_2 + \cdots + X_n$ et $\Sigma_n = X_1 X_2 \cdots X_n$. Noter que $\mathfrak{S}_n$ agit sur les sous-ensembles de $\{1, \cdots, n\}$ par $(\sigma, I) \mapsto \sigma(I)$, et que cette action préserve évidemment le cardinal. Comme on a aussi $\sigma(X_I) = X_{\sigma(I)}$, il s'ensuit que $\sigma(\Sigma_n) = \Sigma_n$ pour toute permutation $\sigma \in \mathfrak{S}_n$. En d'autres termes, on a

$$\Sigma_1, \cdots, \Sigma_n \in \mathbb{Z}[X_1, \cdots, X_n]^{\mathfrak{S}_n},$$

on dit que ce sont des polynômes "symétriques". Ces polynômes encodent les relations entre racines et coefficients des polynômes.

Lemme. – *On a dans* $\mathbb{Z}[X_1, \cdots, X_n][T]$ *l'égalité*

$$(T - X_1)(T - X_2) \cdots (T - X_n) = T^n - \Sigma_1 T^{n-1} + \Sigma_2 T^{n-2} + \cdots + (-1)^n \Sigma_n$$

Démonstration. On laisse au lecteur le soin de faire une récurrence sur n. □

Si on se donne un n-uplet $\alpha_1, \cdots, \alpha_n$ d'éléments d'un anneau commutatif A, alors en "spécialisant" l'identité du lemme par le morphisme $\mathbb{Z}[X_1, \cdots, X_n][T] \longrightarrow A[X]$ qui envoie T sur X et α_i sur X_i, on obtient dans $A[X]$ l'égalité

$$(X - \alpha_1) \cdots (X - \alpha_n) = X^n - \Sigma_1(\alpha_1, \cdots, \alpha_n) X^{n-1} + \cdots + (-1)^n \Sigma_n(\alpha_1, \cdots, \alpha_n).$$

Le spectaculaire théorème suivant justifie la terminologie de "polynôme symétrique *élémentaire*".

2.5.3 THÉORÈME.– *Les Σ_i sont algébriquement indépendants dans $\mathbb{Z}[X_1, \cdots, X_n]$ et engendrent le sous-anneau $\mathbb{Z}[X_1, \cdots, X_n]^{\mathfrak{S}_n}$. En d'autres termes, l'unique morphisme d'anneaux $\mathbb{Z}[Y_1, \cdots, Y_n] \longrightarrow \mathbb{Z}[X_1, \cdots, X_n]$ qui envoie Y_i sur Σ_i est injectif et son image est $\mathbb{Z}[X_1, \cdots, X_n]^{\mathfrak{S}_n}$, ce que l'on écrit de manière un peu imprécise :*

$$\mathbb{Z}[X_1, \cdots, X_n]^{\mathfrak{S}_n} = \mathbb{Z}[\Sigma_1, \cdots, \Sigma_n].$$

Démonstration. Voir exercice 11 du TD. □

2.5.4 *Application : discriminant d'un polynôme.* D'après le théorème, il existe un unique polynôme $\Delta \in \mathbb{Z}[\Sigma_1, \cdots, \Sigma_n]$ tel que

$$\prod_{i<j}(X_i - X_j)^2 = (-1)^{n(n-1)/2} \prod_{i \neq j}(X_i - X_j) = \Delta(\Sigma_1, \cdots, \Sigma_n).$$

En effet, le terme de gauche est manifestement un polynôme symétrique en les X_i.

DÉFINITION. – *Soit A un anneau et $f = X^n + a_1 X^{n-1} + \cdots + a_{n-1}X + a_n \in A[X]$ un polynôme unitaire. On définit le* discriminant *de f par*

$$\mathrm{Disc}(f) := \Delta\left(-a_1, \cdots, (-1)^n a_n\right) \in A.$$

Exemple. – Soit $A = \mathbb{Z}[X_1, \cdots, X_n]$ et f_{univ} le polynôme scindé de degré n "universel"

$$f_{\mathrm{univ}} := (T - X_1)(T - X_2) \cdots (T - X_n) \in \mathbb{Z}[X_1, \cdots, X_n][T].$$

Alors $\mathrm{disc}(f_{\mathrm{univ}}) = \Delta$, puisque $f_{\mathrm{univ}} = T^n - \Sigma_1 T^{n-1} + \cdots + (-1)^n \Sigma_n$. On remarque aussi (calcul) que

$$\mathrm{disc}(f_{\mathrm{univ}}) = (-1)^{n(n-1)/2} \prod_{i=1}^{n} f'(X_i).$$

PROPOSITION. – *Soit k un corps et $f \in k[X]$ unitaire. Pour toute extension K pour laquelle f se scinde $f = (X - \alpha_1) \cdots (X - \alpha_n)$ dans $K[X]$, on a*

$$\mathrm{disc}(f) = \prod_{i<j}(\alpha_i - \alpha_j)^2 = (-1)^{n(n-1)/2} \prod_{i=1}^{n} f'(\alpha_i).$$

En particulier, f est séparable si et seulement si $\mathrm{disc}(f) \neq 0$.

Démonstration. Découle de l'exemple universel par le morphisme $\mathbb{Z}[X_1, \cdots, X_n][T] \longrightarrow K[X]$ qui envoie T sur X et X_i sur α_i. □

Exercice. – Montrer que $\mathrm{disc}(X^n + aX + b) = (-1)^{n(n-1)/2}((1-n)^{n-1}a^n + n^n b^{n-1})$.

Voici un autre exemple d'utilisation du discriminant :

PROPOSITION. – *Soit $f \in k[X]$ séparable et G_f son groupe de Galois, vu comme un sous-groupe du groupe de permutation $\mathfrak{S}_n$ des racines de f dans un corps de décomposition K_f de f. Alors, si* $\mathrm{car}(k) \neq 2$ *on a* $G_f \subset \mathfrak{A}_n \Leftrightarrow \mathrm{disc}(f) \in (k^\times)^2$.

Démonstration. Soit $\alpha_1, \cdots, \alpha_n$ les racines de f dans K_f. Notons $\tau \mapsto \sigma_\tau$ l'injection de G_f dans $\mathfrak{S}_n$ associée à cette numérotation des racines. On a donc $\tau(\alpha_i) = \alpha_{\sigma_\tau(i)}$ pour tout i.

Posons $D := \prod_{i<j}(\alpha_i - \alpha_j) \in K_f$. Les deux racines carrées de $\mathrm{disc}(f)$ dans K_f sont D et $-D$. Ainsi $\mathrm{disc}(f) \in k^2 \Leftrightarrow D \in k$. Puisque $k = K_f^{G_f}$, étudions l'action de G_f sur D. Pour tout $\tau \in G_f$ on a, en notant ε la signature $\mathfrak{S}_n \longrightarrow \{\pm 1\}$,

$$\tau(D) = \prod_{i<j}(\alpha_{\sigma_\tau(i)} - \alpha_{\sigma_\tau(j)}) = \varepsilon(\sigma_\tau)\prod_{i<j}(\alpha_i - \alpha_j) = \varepsilon(\sigma_\tau)D.$$

Si $\mathrm{car}(k) \neq 2$, il s'ensuit que $D \in K_f^{G_f} = k \Leftrightarrow G_f \subset \mathfrak{A}_n$. □

Remarque. – Si $\mathrm{disc}(f) \notin k^2$, l'extension intermédiaire $k \subset k(\sqrt{\mathrm{disc}(f)}) \subset K_f$ est quadratique sur k et $\mathrm{Gal}(K_f/k(\sqrt{\mathrm{disc}(f)})) = G_f \cap \mathfrak{A}_n$.

2.5.5 *Application : résolvantes.* Le discrimant Δ peut être vu comme le $\mathfrak{S}_n$-symétrisé du polynôme $\mathfrak{A}_n$-invariant $\psi = \prod_{i<j}(X_i - X_j)$ et le critère ci-dessus nous dit que $G_f \subset \mathfrak{A}_n$ si et seulement si le polynôme $(T - \psi(\alpha_1, \cdots, \alpha_n)(T + \psi(\alpha_1, \cdots, \alpha_n)) = T^2 - \mathrm{disc}(f)$ a une racine dans K.

Plus généralement, si $\psi \in k[X_1, \cdots, X_n]$ est H-invariant pour un sous-groupe $H < \mathfrak{S}_n$, on pose

$$R_\psi(T) := \prod_{\sigma \in \mathfrak{S}_n/H}(T - \sigma.\psi) \in k[X_1, \cdots, X_n]^{\mathfrak{S}_n}[T] = k[\Sigma_1, \cdots, \Sigma_n][T],$$

que l'on peut spécialiser à un polynôme $f = X^n + a_1X^{n-1} + \cdots + a_n \in k[X]$ en

$$R_{\psi,f}(T) = R_\psi(-a_1, \cdots, (-1)^n a_n)(T) \in k[T].$$

Ce polynôme est de degré $[\mathfrak{S}_n : H]$, et on a le critère suivant :

PROPOSITION. – *Si $R_{\psi,f}(T)$ possède une racine simple dans k, alors G_f est contenu dans un conjugué de H dans $\mathfrak{S}_n$.*

Démonstration. Comme plus haut, soient $\alpha_1, \cdots, \alpha_n$ les racines de f dans K_f. Notons $\tau \mapsto \sigma_\tau$ l'injection de G_f dans $\mathfrak{S}_n$ associée à cette numérotation des racines.

Posons $\overline{\psi} := \psi(\alpha_1, \cdots, \alpha_n) \in K_f$, et plus généralement $\overline{\sigma\psi} := \psi(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)})$ pour $\sigma \in \mathfrak{S}_n$. On a donc $\overline{\sigma\sigma'\psi} = \overline{\sigma\psi}$ si $\sigma' \in H$ et on a $\overline{\sigma_\tau\sigma\psi} = \tau(\overline{\sigma\psi})$ pour $\tau \in G_f$.

Les racines de $R_{\psi,f}$ sont les $\overline{\sigma\psi}$ pour σ décrivant $\mathfrak{S}_n/H$ (ou plutôt un ensemble de représentants de $\mathfrak{S}_n/H$). Supposons que $\overline{\sigma\psi}$ est racine de $R_{\psi,f}$ dans k. Alors $\overline{\sigma_\tau\sigma\psi} = \tau(\overline{\sigma\psi}) = \overline{\sigma\psi}$ pour tout $\tau \in G_f$. Si de plus, $\overline{\sigma\psi}$ est racine simple, alors $\sigma_\tau\sigma H = \sigma H$ et $\sigma_\tau \in \sigma H\sigma^{-1}$. L'action de G_f se fait donc à travers $\sigma H\sigma^{-1}$. □

Encore plus généralement, soient deux sous-groupes $H \subset G \subset \mathfrak{S}_n$ et supposons que G_f agisse à travers G sur les racines (pour un ordre préalablement choisi). On peut alors simplement G-symétriser un polynôme H-invariant ψ en posant

$$R^G_{\psi,f}(T) = \prod_{\sigma \in G/H} (T - \psi(\alpha_{\sigma(1)}, \cdots, \alpha_{\sigma(n)}) \in K_f[X].$$

Ce polynôme de degré $[G : H]$ est alors G_f-invariant, donc dans $k[X]$. Comme ci-dessus, s'il admet une racine simple dans k alors l'action de G_f se fait à travers un conjugué de H. Sinon, si K désigne le sous-corps de K_f engendré par une racine simple de $R^G_{\psi,f}$, alors $\mathrm{Gal}(K_f/K)$ agit à travers un conjugué de H.

Remarque. – Ce principe de "calcul de G_f" est un avatar du "principe de Lagrange" pour résoudre le polynôme f, *i.e.* contruire K_f. Supposons en effet H distingué dans G et $R^G_{\psi,f}$ séparable. Si on sait construire le corps de décomposition K_1 de $R^G_{\psi,f}$ (qui est de degré $\leqslant \deg(f)$), on sait que le corps K_f de décomposition de f sur K_1 sera de groupe contenu dans H. Le principe de Lagrange est donc de bien choisir ψ pour être capable de résoudre la "résolvante" $R^G_{\psi,f}$, puis inductivement construire ainsi K_f (en se ramenant à construire des extensions successives de groupes de Galois cycliques). Bien-sûr ce principe ne peut fonctionner que si G est résoluble.

Exemple : polynômes cubiques sur $\mathbb{Q}$. Lagrange considérait la résolvante associée à $\psi = (X_1 + jX_2 + j^2X_3)^3$ qui est invariant par le groupe H engendré par le cycle $(1, 2, 3)$ (il faut donc adjoindre j à $\mathbb{Q}$, et on peut rapprocher cela du discriminant en degré 2, qui est associé à $(X_1 - X_2)^2$). Le polynôme

$$R_\psi(T) = (T - (X_1 + jX_2 + j^2X_3)^3)(T - (X_1 + j^2X_2 + jX_3)^3) \in \mathbb{Z}[X_1, X_2, X_3]^{\mathfrak{S}^3}[T]$$

est de degré 2 en T et la preuve du théorème 2.5.3 suggère un procédé inductif de calcul de ses coefficients en tant qu'éléments de $\mathbb{Z}[\Sigma_1, \Sigma_2, \Sigma_3]$. Écrivons $R_\psi(T) = T^2 + AT + B$. Alors, par homogénéité, on voit que A est de la forme $A = \lambda\Sigma_1^3 + \mu\Sigma_1\Sigma_2 + \nu\Sigma_3$ avec $\lambda, \mu, \nu \in \mathbb{Z}$. En regardant les coefficients de X_1^3, resp. $X_1^2X_2$ et $X_1X_2X_3$, on obtient les égalités $\lambda = 2$, $3\lambda + \mu = -3$ et $\lambda + 3\mu + \nu = 2$, d'où $A = 2\Sigma_1^3 - 9\Sigma_1\Sigma_2 + 27\Sigma_3$. Pour B, l'homogénéité nous dit que $B \in \langle \Sigma_1^6, \Sigma_1^4\Sigma_2, \Sigma_1^3\Sigma_3, \Sigma_1^2\Sigma_2^2, \Sigma_1\Sigma_2\Sigma_3, \Sigma_2^3, \Sigma_3^2 \rangle_{\mathbb{Z}}$. En regardant les coefficients de X_1^6, $X_1^5X_2$, $X_1^4X_2X_3$, $X_1^4X_2^2$, $X_1^3X_2^2X_3$, $X_1^3X_2^3$ et $X_1^2X_2^2X_3^2$, on obtient un système linéaire triangulaire d'équations linéaires en les coefficients de B dans la base des polynômes invariants homogènes de degré 6. Donc, facile à résoudre modulo les calculs... Mais on peut s'épargner les calculs en spécialisant à un polynôme $f = X^3 + aX + b$ sans terme en X^2 (facile de s'y ramener). Dans ce cas, le Σ_1 spécialisé est 0. Or, si $\Sigma_1 = 0$, on calcule que $B = ((1-j^2)X_1+(j-j^2)X_2)^3((1-j)X_1+(j^2-j)X_2)^3 = 27(X_1^2+X_2^2+X_1X_2)^3 = -27\Sigma_2^3$. On obtient donc $R_{\psi,f} = T^2 + 27bT - 27a^3$. On sait résoudre un tel trinôme. Si $\overline{\psi}_1$, $\overline{\psi}_2$ en sont les racines, on a donc (pour une numérotation convenable des racines) $\overline{\psi}_1 = (\alpha_1 + j\alpha_2 + j^2\alpha_3)^3$ et $\overline{\psi}_2 = (\alpha_1 + j^2\alpha_2 + j\alpha_3)^3$. Après extraction de racine cubique, et tenant compte de l'égalité $\alpha_1 + \alpha_2 + \alpha_3 = 0$, on trouve donc les α_i en résolvant un système linéaire 3×3.

Exemple : polynômes de degré 4 sur $\mathbb{Q}$. Lagrange utilisait la résolvante associée au polynôme $\psi = (X_1 + X_2)(X_3 + X_4)$ qui est invariant par le sous-groupe H d'indice 3 de $\mathfrak{S}_4$ engendré par $(1,3,2,4)$ et $(1,2)$. Avec le même genre de calculs que ci-dessus, on peut montrer que si $f = X^4 + aX^2 + bX + c$ alors $R_{\psi,f} = T^3 - 2aT^2 + (a^2 - 4c)T + b^2$. Par l'exemple précédent, on sait construire les trois racines $\overline{\psi}_1, \overline{\psi}_2, \overline{\psi}_3$ de $R_{\psi,f}$. Pour une bonne numérotation de ces racines, on a $\overline{\psi}_i = (\alpha_1 + \alpha_{1+i})(\alpha_? + \alpha_!)$ pour chaque $i = 1,2,3$ et où $\{1,2,3,4\} = \{1, 1+i, ?, !\}$. Mais alors, en utilisant $\sum \alpha_i = 0$, on obtient que $\alpha_1 + \alpha_{1+i}$ est une racine carrée de $-\overline{\psi}_i$ pour $i = 1,2,3$. Puis après extraction de ces racines, on n'a plus qu'à résoudre un système linéaire pour obtenir les α_i.

2.5.6 *Application : groupe de Galois du polynôme "général".* Commençons par un corollaire du théorème 2.5.3 concernant les fractions rationnelles symétriques. Remarquons au passage que l'action de $\mathfrak{S}_n$ sur $k[X_1, \cdots, X_n]$ se prolonge uniquement à $k(X_1, \cdots, X_n)$.

Corollaire. – *On a $k(X_1, \cdots, X_n)^{\mathfrak{S}_n} = k(\Sigma_1, \cdots, \Sigma_n)$.*

Démonstration. On a une inclusion claire, à savoir $\supset$. Pour l'autre inclusion, soit $\phi \in k(X_1, \cdots, X_n)^{\mathfrak{S}_n}$. Puisque $k[X_1, \cdots, X_n]$ est factoriel, on peut écrire ϕ de manière unique sous la forme $\phi = \frac{f}{g}$ avec $(f,g) = 1$ et f, g unitaires (choisir un ordre total sur $\mathbb{N}^n$ pour définir "unitaire"). On a alors, pour tout $\sigma \in \mathfrak{S}_n$, $\phi = \sigma(\phi) = \frac{\sigma(f)}{\sigma(g)}$ et aussi $(\sigma(f), \sigma(g)) = 1$ et $\sigma(f), \sigma(g)$ unitaires. Il s'ensuit que $f = \sigma(f)$ et $g = \sigma(g)$. Donc $f, g \in k[\Sigma_1, \cdots, \Sigma_n]$ et finalement $\phi \in k(\Sigma_1, \cdots, \Sigma_n)$. □

Changeons maintenant de point de vue. Soit k un corps, et $K := k(a_1, \cdots, a_n)$ le corps des fractions rationnelles en les n indéterminées $a_1, \cdots, a_n$. On s'intéresse au polynôme "général" $f = X^n + a_1 X^{n-1} + \cdots + a_n \in K[X]$, dont on veut déterminer un corps de décomposition et le groupe de Galois G_f. Pour cela, considérons le corps $L := k(\alpha_1, \cdots, \alpha_n)$ des fractions rationnelles à n-indéterminées $\alpha_1, \cdots, \alpha_n$. Le théorème 2.5.3 nous dit que les éléments $\Sigma_i(\alpha_1, \cdots, \alpha_n) \in L$ sont algébriquements indépendants sur k. Il existe donc un unique plongement

$$K \hookrightarrow L,\ a_i \mapsto (-1)^i \Sigma_i(\alpha_1, \cdots, \alpha_n).$$

Théorème. – *Le polynôme f est séparable et irréductible dans $K[X]$. Le corps L est un corps de décomposition de f sur K dans lequel les α_i sont les racines de f. L'action du groupe de Galois G_f sur les α_i identifie G_f à $\mathfrak{S}_n$.*

Démonstration. Via le morphisme d'anneaux $\mathbb{Z}[X_1, \cdots, X_n][T] \longrightarrow L[X]$ qui envoie X_i sur α_i et T sur X, la factorisation du lemme 2.5.2 implique la factorisation $(X - \alpha_1) \cdots (X - \alpha_n) = X^n + a_1 X^{n-1} + \cdots + a_n$ dans $L[X]$. Il s'ensuit que les α_i sont les racines de f dans L, donc f est séparable et L est un corps de décomposition de f. L'action de $\mathrm{Gal}(L/K)$ sur les α_i nous fournit un plongement $\mathrm{Gal}(L/K) \hookrightarrow \mathfrak{S}_n$. Mais le corollaire ci-dessus nous dit que $K = L^{\mathfrak{S}_n}$, et le corollaire 2.1.6 implique que $\mathrm{Gal}(L/K) = \mathfrak{S}_n$. En particulier, $\mathrm{Gal}(L/K)$ agit transitivement sur les racines de f, donc f est irréductible, en vertu du lemme 2.2.1. □

Remarque. – On peut se demander quelle implication peut avoir un tel résultat sur les polynômes qui nous intéressent vraiment, à savoir ceux où les a_i sont des éléments de k. Il se trouve que la réponse dépend fortement de k. Par exemple si $k = \mathbb{C}$, tout polynôme f obtenu par spécialisation des a_i en des éléments de $\mathbb{C}$ est scindé, donc son groupe de Galois est trivial ! Si $k = \mathbb{R}$ et $n > 2$, une spécialisation de f n'est jamais irréductible et son groupe de Galois est trivial ou égal à $\mathbb{Z}/2\mathbb{Z}$. Si $k = \mathbb{F}_p$, une spécialisation de f peut être irréductible, mais son groupe de Galois est toujours abélien. Mais pour $k = \mathbb{Q}$, un résultat de Hilbert affirme que pour une infinité de spécialisations de f, le polynôme spécialisé est irréductible et son groupe de Galois est $\mathfrak{S}_n$!

2.6 Base normale et Hilbert '90

2.6.1 *Indépendance algébrique des plongements.* Nous avons vu précédemment que des plongements distincts d'une extension finie $K \supset k$ dans une clôture algébrique $\overline{k}$ de k sont $\overline{k}$-linéairement indépendants dans $\mathrm{Hom}_{k-\mathrm{ev}}(K, \overline{k})$ (c'est une conséquence du Lemme 2.1.5). La proposition suivante renforce nettement cette propriété.

Proposition. – *Supposons k infini et soit $K \supset k$ une extension de corps. Toute famille $\iota_1, \cdots, \iota_n$ de k-plongements distincts de K dans $\overline{k}$ est* algébriquement indépendante*, au sens suivant :*

$$\forall f \in \overline{k}[X_1, \cdots, X_n],\ (\forall x \in K,\ f(\iota_1(x), \cdots, \iota_n(x)) = 0) \Rightarrow f = 0.$$

Démonstration. Posons $\iota := (\iota_1, \cdots, \iota_n) : K \longrightarrow \overline{k}^n$, qui est une application k-linéaire, et notons $W := \iota(K)$ son image, qui est un k-sev de dimension finie de $\overline{k}^n$. Comme $\overline{k}$ est infini, on sait que $\overline{k}[X_1, \cdots, X_n]$ s'identifie à la $\overline{k}$-algèbre des fonctions polynomiales $\overline{k}^n \longrightarrow \overline{k}$. Il s'agit alors de montrer que la restriction à W de toute fonction polynômiale non nulle $f : \overline{k}^n \longrightarrow \overline{k}$ n'est pas identiquement nulle. Remarquons que l'indépendance $\overline{k}$-linéaire des ι_i nous dit que c'est vrai au moins si f est homogène de degré 1, i.e. si f est une forme $\overline{k}$-linéaire sur $\overline{k}^n$. Ceci implique en particulier que W n'est contenu dans aucun $\overline{k}$-hyperplan de $\overline{k}^n$, et donc engendre $\overline{k}$-linéairement le $\overline{k}$-ev $\overline{k}^n$. Fixons alors une $\overline{k}$-base de $\overline{k}^n$ contenue dans W. Toute fonction polynômiale sur $\overline{k}^n$ est aussi une fonction polynomiale en les coordonnées dans cette nouvelle base. On est donc ramené à prouver l'énoncé suivant : *si f est une fonction polynômiale sur $\overline{k}^n$ nulle sur k^n, alors f est nulle.* C'est là que l'on utilise l'hypothèse k infini. En effet, si $\lambda_2, \cdots, \lambda_n$ sont fixés dans k^{n-1}, alors la fonction polynomiale $\overline{k} \longrightarrow \overline{k}$, $\lambda \mapsto f(\lambda, \lambda_2, \cdots, \lambda_{n-1})$ s'annule sur un ensemble infni, donc est nulle. En d'autres termes, $f_{|\overline{k} \times k^{n-1}}$ est nulle. Par récurrence, on montre de même que pour tout $r \leqslant n$, on a $f_{|\overline{k}^r \times k^{n-r}} \equiv 0$, et finalement que $f = 0$. □

2.6.2 *Théorème de la base normale.* Supposons maintenant l'extension $K \supset k$ finie et Galoisienne, et notons $G := \mathrm{Gal}(K/k)$. L'action de G sur K étant k-linéaire, on peut considérer K comme une "représentation k-linéaire" de G ou, de manière équivalente, comme un $k[G]$-module à gauche. Le théorème suivant affirme que K est isomorphe à la *représentation régulière* de G, i.e. que K est isomorphe à $k[G]$ comme $k[G]$-module à gauche.

THÉORÈME. – *Il existe $x \in K$ dont l'orbite sous $G = \mathrm{Gal}(K/k)$ est une k-base de K.*

Démonstration. Supposons d'abord k infini. Soit $x \in K$. S'il existe une relation de dépendance k-linéaire non triviale $\sum_{\sigma\in G} \lambda_\sigma \sigma(x) = 0$, alors pour tout $\tau \in G$, on a aussi $\tau(\sum_{\sigma\in G} \lambda_\sigma \sigma(x)) = \sum_{\sigma\in G} \lambda_\sigma . \tau\sigma(x) = 0$, donc la matrice $(\tau\sigma(x))_{\sigma,\tau\in G}$ a un déterminant nul. Pour définir sans ambiguïté de signe ce déterminant, numérotons $G = \{\sigma_1, \cdots, \sigma_n\}$ et transportons la loi de groupe de G sur $\{1, \cdots, n\}$ en définissant $i \cdot j$ par la condition $\sigma_i\sigma_j = \sigma_{i\cdot j}$. Posons alors $f = \det((X_{j\cdot i})_{i,j}) \in \overline{k}[X_1, \cdots, X_n]$. C'est un polynôme non nul car le coefficient de X_i^n dans f est un signe, pour tout i. Choisissons alors un k-plongement $\iota : K \hookrightarrow \overline{k}$. Les $\iota_i := \iota \circ \sigma_i$ sont les n k-plongements distincts de K dans $\overline{k}$. D'après le théorème précédent, il existe $x \in K$ tel que $0 \neq f(\iota_1(x), \cdots, \iota_n(x)) = \det((\iota_{j\cdot i}(x))_{i,j}) = \iota(\det(\sigma_j\sigma_i(x))_{i,j})$. Pour un tel x, il n'y a donc pas de relation de dépendance k-linéaire non-triviale entre les $\sigma_i(x)$, et l'orbite $\{\sigma(x), \sigma \in G\}$ de x est donc une k-base de K.

Supposons maintenant k fini et posons $n = [K : k]$. On sait que $G = \mathrm{Gal}(K/k)$ est cyclique d'ordre n engendré par le Frobenius φ. On sait aussi que les φ^i, $0 \leqslant i \leqslant n-1$ sont k-linéairement indépendants dans $\mathrm{End}_{k-\mathrm{ev}}(K)$. Il s'ensuit que le polynôme minimal de φ comme élément de $\mathrm{End}_{k-\mathrm{ev}}(K)$, qui divise $X^n - 1$, est en fait égal à $X^n - 1$. Munissons K de la structure de $k[X]$-module telle que X agit par φ. Puisque le degré du polynôme minimal de φ est la dimension de K, le théorème de structure des modules de torsion sur un anneau principal montre que K est un $k[X]$-module cyclique. Soit alors $x \in K$ un générateur de ce $k[X]$-module. Par définition, K est k-linéairement engendré par $x, \varphi(x), \cdots, \varphi^{n-1}(x)$. □

Remarquons qu'un élément primitif de l'extension $K \supset k$ ne satisfait pas nécessairement la conclusion du théorème en général. Par exemple $\sqrt{2}$ est primitif pour l'extension $\mathbb{Q}(\sqrt{2}) \supset \mathbb{Q}$ mais son orbite $\{\pm\sqrt{2}\}$ n'est visiblement pas une $\mathbb{Q}$-base de $\mathbb{Q}(\sqrt{2})$.

COROLLAIRE. – *En tant que $k[G]$-module (à gauche), K est isomorphe à $k[G]$.*

Démonstration. Choisissons x comme dans le théorème. Alors l'unique morphisme de $k[G]$-modules $k[G] \longrightarrow K$ qui envoie 1 sur x est un isomorphisme. □

2.6.3 1-*cohomologie des groupes.* Soit Γ un groupe et G un groupe muni d'une action de Γ (par automorphismes de groupes) notée $(\sigma, g) \mapsto {}^\sigma g$. On définit l'ensemble des 1-cocycles sur Γ à valeurs dans G

$$Z^1(\Gamma, G) := \{(g_\sigma)_{\sigma\in\Gamma},\ \forall \sigma, \sigma' \in \Gamma,\ g_{\sigma\sigma'} = g_\sigma . {}^\sigma g_{\sigma'}\}$$

La condition "de cocycle" qui apparaît est équivalente à demander que l'application $\sigma \mapsto (g_\sigma, \sigma)$ soit un morphisme de groupes $\Gamma \longrightarrow G \rtimes \Gamma$ (appelée "section du produit semi-direct"). Le groupe G agit sur $Z^1(\Gamma, G)$ de la manière suivante : si $h \in G$ et $z := (g_\sigma)_{\sigma\in\Gamma} \in Z^1(\Gamma, G)$, alors ${}^h z$ est le cocycle $\sigma \mapsto h g_\sigma ({}^\sigma h)^{-1}$. En termes de sections du produit semi-direct, h agit tout simplement par conjugaison. On pose alors

$$H^1(\Gamma, G) = Z^1(\Gamma, G)/G.$$

C'est un ensemble "pointé" (i.e. muni d'un élément particulier, à savoir ici la classe du cocycle trivial $\sigma \mapsto 1_G$. Si G est abélien, alors $Z^1(\Gamma, G)$ est aussi un groupe abélien, et $H^1(\Gamma, G)$ est le quotient de $Z^1(\Gamma, G)$ par le sous-groupe $\{\sigma \mapsto (h({}^\sigma h)^{-1}), h \in G\}$, donc c'est aussi un groupe abélien.

2.6.4 *Hilbert 90 généralisé et descente Galoisienne.* On va prouver le résultat suivant :

THÉORÈME. – *Soit $K \supset k$ une extension Galoisienne finie. Pout tout $n \in \mathbb{N}$, on a* $H^1(\mathrm{Gal}(K/k), \mathrm{GL}_n(K)) = \{1\}$.

Pour cela, introduisons la notion suivante :

DÉFINITION. – *Soit V un K-ev. Une action K-semilinéaire de* $\mathrm{Gal}(K/k)$ *sur V est une action k-linéaire qui vérifie de plus*

$$\forall \sigma \in \mathrm{Gal}(K/k),\ \forall v \in V, \forall \lambda \in K,\ \ \sigma(\lambda v) = \sigma(\lambda)\sigma(v).$$

Le premier exemple est K muni de l'action canonique de $\mathrm{Gal}(K/k)$. On en déduit les exemples "standard" par extension des scalaires : pour tout k-ev W, on munit le K-ev $K \otimes_k W$ de l'unique action k-linéaire de $\mathrm{Gal}(K/k)$ donnée sur les tenseurs élémentaires par $\sigma(\alpha \otimes w) := \sigma(\alpha)w$. Cette action est manifestement K-semilinéaire. Le point remarquable est que tout K-ev V muni d'une action K-semilinéaire de $\Gamma := \mathrm{Gal}(K/k)$ s'obtient de cette manière. Pour cela, remarquons d'abord que l'ensemble $V^\Gamma = \{v \in V, \forall \sigma \in \mathrm{Gal}(K/k), \sigma(v) = v\}$ est un k-sev de V. L'inclusion k-linéaire $V^\Gamma \subset V$ nous fournit alors une application K-linéaire $\psi_V : K \otimes_k V^\Gamma \longrightarrow V$, uniquement déterminée par la régle $\alpha \otimes v \mapsto \alpha v$. Cette application est aussi $\mathrm{Gal}(K/k)$-équivariante puisque $\forall \sigma \in \mathrm{Gal}(K/k), \forall \alpha \in K, \forall v \in V^\Gamma$, $\psi_V(\sigma(\alpha) \otimes v) = \sigma(\alpha)v = \sigma(\alpha v)$.

PROPOSITION. – *Soit V un K-ev muni d'une action K-semilinéaire de* $\mathrm{Gal}(K/k)$. *Alors le morphisme canonique $\psi_V : K \otimes_k V^G \longrightarrow V$ est un isomorphisme.*

Démonstration. Injectivité : Soit $(e_i)_{i\in I}$ une k-base de V. Un élément de $K \otimes_k V$ s'écrit de manière unique sous la forme $\sum_{i\in I} \alpha_i \otimes e_i$. Il est dans $\mathrm{Ker}(\psi_V)$ si et seulement si $\sum_{i\in I} \alpha_i e_i = 0$. En d'autres termes, l'injectivité de ψ_V équivaut à montrer que toute famille k-libre de V^G est K-libre dans V. Supposons la famille $(e_i)_{i\in I}$ K-liée et soit $J \subset I$ un sous-ensemble fini non vide minimal tel qu'il existe des α_j, $j \in J$ avec $\sum_{j\in J} \alpha_j e_j = 0$. Par minimalité, on a donc $\alpha_j \neq 0$ pour tout j. De plus, on peut supposer $\alpha_{j_0} = 1$ pour un $j_0 \in J$, quitte à multiplier tous les α_j par $\alpha_{j_0}^{-1}$. Mais alors, pour un $\sigma \in \Gamma$, on a aussi $0 = \sigma(\sum_{j\in J} \alpha_j e_j) = \sum_{j\in J} \sigma(\alpha_j)\sigma(e_j) = \sum_{j\in J} \sigma(\alpha_j)e_j$. Comme $\sigma(\alpha_{j_0}) = \alpha_{j_0}$, on en déduit $\sum_{j\in J\setminus\{j_0\}}(\alpha_j - \sigma(\alpha_j))e_j = 0$. Par minimalité de J, cette relation de dépendance linéaire doit être triviale, i.e. $\sigma(\alpha_j) - \alpha_j = 0$ pour tout j. Ceci étant vrai pour tout $\sigma \in \Gamma$, on a donc $\alpha_j \in K^\Gamma = k$ pour tout j, ce qui contredit l'indépendance k-linéaire des e_j.

Surjectivité : L'image $\mathrm{Im}(\psi_V) \subset V$ est un K-sev Γ-stable de V. Par passage au quotient, le K-ev $\overline{V} := V/\mathrm{Im}(\psi_V)$ est donc muni d'une action de Γ et celle-ci est toujours K-semilinéaire. Pour $v \in V$, posons $\mathrm{tr}_\Gamma(v) := \sum_{\sigma\in\Gamma} \sigma(v)$. De même on définit tr_Γ sur $\overline{V}$. On

a manifestement $\overline{\mathrm{tr}_\Gamma(v)} = \mathrm{tr}_\Gamma(\overline{v})$. De plus, puisque $\mathrm{tr}_\Gamma(v) \in V^\Gamma \subset \mathrm{Im}\Psi_V$, on en déduit que $\mathrm{tr}_\Gamma(\overline{v}) = 0$ pour tout $\overline{v} \in \overline{V}$. Or, pour tout $\alpha \in K$, on a $\mathrm{tr}_\Gamma(\alpha\overline{v}) = \sum_{\sigma\in\Gamma} \sigma(\alpha)\sigma(\overline{v})$. Supposons $\overline{V} \neq 0$ et soit $\lambda : \overline{V} \longrightarrow K$ une forme K-linéaire telle que $\lambda(\overline{v}) \neq 0$. Posons $\lambda_\sigma := \lambda(\sigma(\overline{v})) \in K$. On a donc $\sum_{\sigma\in\Gamma} \lambda_\sigma\sigma(\alpha) = 0$ pour tout $\alpha \in K$. Ceci donne une relation de dépendance K-linéaire entre les σ. Contradiction. □

Prouvons maintenant le théorème. Soit $\sigma \mapsto g_\sigma$ un cocycle dans $Z^1(\mathrm{Gal}(K/k), \mathrm{GL}_n(K))$. On peut alors "tordre" l'action canonique de $\mathrm{Gal}(K/k)$ sur K^n en posant $\forall\sigma \in \Gamma, \forall v \in K^n$, $\sigma * v := g_\sigma\sigma(v)$. Ceci définit une action K-semilinéaire sur $V = K^n$. La proposition ci-dessus nous dit que V est encore isomorphe à K^n muni de son action canonique, i.e. il existe $\psi : (K^n)_{\mathrm{can}} \xrightarrow{\sim} (K^n)_{\mathrm{tordu}}$. Soit h la matrice de cet isomorphisme. On a par définition $h \circ g_\sigma\sigma = \sigma \circ h$ et donc $hg_\sigma({}^\sigma h)^{-1} = \mathrm{id}$, ce qui montre que le cocycle a une classe triviale dans $H^1(\mathrm{Gal}(K/k), \mathrm{GL}_n(K))$.

2.6.5 *Hilbert 90 original.* Le théorème 90 de Hilbert était le cas $n = 1$ et $\mathrm{Gal}(K/k)$ cyclique. Il était utilisé pour obtenir le résultat suivant :

Corollaire. – *Supposons $K \supset k$ Galoisienne cyclique de groupe de Galois engendré par γ, et soit $\alpha \in K$ tel que*

$$N_{K/k}(\alpha) := \prod_{\sigma\in\mathrm{Gal}(K/k)} \sigma(\alpha) = 1.$$

Alors il existe β tel que $\alpha = \beta\gamma(\beta)^{-1}$.

Démonstration. La condition de norme dit que $\alpha\gamma(\alpha)\cdots\gamma^{n-1}(\alpha) = 1$ où $n = [K : k]$. Pour $\sigma = \gamma^i$, posons $g_\sigma := \alpha\gamma(\alpha)\cdots\gamma^{i-1}(\alpha)$, qui est donc indépendant du choix de i. On a alors $g_{\sigma\sigma'} = \alpha\cdots\gamma^{i+i'-1}(\alpha) = g_\sigma\gamma^i(g_{\sigma'}) = g_\sigma\sigma(g_{\sigma'})$. Donc $\sigma \mapsto g_\sigma \in Z^1(\mathrm{Gal}(K/k), K^\times)$. D'après le théorème précédent, il existe β tel que $g_\sigma = \beta\sigma(\beta)^{-1}$ pour tout $\sigma \in \mathrm{Gal}(K/k)$. En particulier, pour $\sigma = \gamma$, on a $g_\gamma = \alpha = \beta\gamma(\beta)^{-1}$. □

Application. – Résolvons l'équation $a^2 + b^2 = 1$ dans $\mathbb{Q}^2$. Pour une éventuelle solution (a, b), posons $\alpha := a+ib \in \mathbb{Q}(i)$. On a $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} = \{1, z \mapsto \overline{z}\}$ et $a^2+b^2 = \alpha\overline{\alpha} = N_{\mathbb{Q}(i)/\mathbb{Q}}(\alpha)$. D'après le corollaire ci-dessus, il existe donc $\beta = r+is \in \mathbb{Q}(i)$ tel que $\alpha = \beta\overline{\beta}^{-1}$. On en déduit que les solutions de $a^2 + b^2 = 1$ sont paramétrées par $a = \frac{r^2-s^2}{r^2+s^2}, b = \frac{2rs}{r^2+s^2}$ avec $r, s \in \mathbb{Q}$.

2.7 Extensions Galoisiennes infinies

Depuis le paragraphe 2.1, nos extensions Galoisiennes sont supposées finies. Mais les notions "normale" et "séparable" ont un sens pour toute extension $K \supset k$ algébrique pas nécessairement finie. On peut donc se demander si les extensions infinies normales et séparables sont encore contrôlées par leur groupe d'automorphismes. Nous allons voir que c'est bien le cas, mais qu'il y a une subtilité.

Commençons par énoncer ce qu'il reste du théorème 2.1.2 dans ce contexte plus général.

2.7.1 THÉORÈME.– *Soit $K \supset k$ une extension algébrique, et posons $G := \mathrm{Aut}_{k-\mathrm{alg}}(K)$. On a équivalence entre :*

i) K/k est normale est séparable,

ii) Pour tout $\alpha \in K$, on a $f_\alpha = \prod_{\beta \in G\cdot\alpha}(X-\beta)$ dans $K[X]$.

iii) $K^G = k$ (points fixes dans K pour l'action de $\mathrm{Aut}(K/k)$).

iv) K est réunion de sous-extensions Galoisiennes finies.

Démonstration. L'équivalence *i)* $\Leftrightarrow$ *iv)* est claire puisque K/k est normale si et seulement si K contient un corps de décomposition de chacun de ses éléments. Les autres équivalences se montrent comme dans le cas fini ou s'y ramènent. □

Une extension algébrique satisfaisant ces propriétés sera dite *Galoisienne* et on notera comme d'habitude $\mathrm{Gal}(K/k) := \mathrm{Aut}_{k-\mathrm{alg}}(K)$. Comme dans le cas fini, pour toute extension intermédiaire $K \supset K' \supset k$, l'extension K/K' est aussi Galoisienne et on a $K' = K^{\mathrm{Gal}(K/K')}$. En revanche, si $H < \mathrm{Gal}(K/k)$ est un sous-groupe, on a certainement $H \subset \mathrm{Gal}(K/K^H)$ mais cette inclusion est en général stricte. Le but de cette section est d'expliquer comment y remédier, après avoir donné un exemple concret.

Notre point de départ sera l'isomorphisme de groupes suivant

(2.7.1.1)

$$\mathrm{Gal}(K/k) \xrightarrow{\sim} \lim_{\longleftarrow k'} \mathrm{Gal}(k'/k) := \left\{ (\sigma_{k'})_{k'} \in \prod_{k'} \mathrm{Gal}(k'/k),\ \forall k' \subset k'',\ (\sigma_{k''})_{|k'} = \sigma_{k'} \right\}.$$

Dans le terme de droite, k' parcourt l'ensemble des sous-extensions Galoisiennes finies de k contenues dans K. La flèche envoie $\sigma \in \mathrm{Gal}(K/k)$ sur la famille $(\sigma_{|k'})_{k'}$. On en définit une inverse en envoyant une famille $(\sigma_{k'})_{k'}$ sur l'automorphisme σ de K défini ainsi : pour tout $\alpha \in K$, on choisit k' contenant α et on pose $\sigma(\alpha) := \sigma_{k'}(\alpha)$, ce qui ne dépend pas du choix de k' par la condition de cohérence qui définit la limite projective à l'intérieur du produit des $\mathrm{Gal}(k'/k)$.

Exemple. – Regardons $k = \mathbb{F}_p$ et $K = \overline{\mathbb{F}}_p$ une clôture algébrique. On sait alors que $\{k'\} = \{\mathbb{F}_{p^r}\}_{r\in\mathbb{N}}$ et que $k' = \mathbb{F}_{p^r}$ est contenu dans $k'' = \mathbb{F}_{p^s}$ si et seulement si r divise s. On sait aussi que $\mathrm{Gal}(\mathbb{F}_{p^r}/\mathbb{F}_p) = \mathbb{Z}/r\mathbb{Z}$, engendré par l'automorphisme de Frobenius. Il s'ensuit que

$$\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) \xrightarrow{\sim} \widehat{\mathbb{Z}} := \lim_{\longleftarrow r} \mathbb{Z}/r\mathbb{Z} = \left\{ (a_r)_{r\in\mathbb{N}} \in \prod_r \mathbb{Z}/r\mathbb{Z},\ \forall r|s,\ a_s \bmod r = a_r \right\}.$$

Notons que l'automorphisme de Frobenius F est encore un élément de $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ et que le sous-groupe $H = \langle F \rangle$ qu'il engendre s'identifie à l'image de $\mathbb{Z}$ par l'application canonique $\mathbb{Z} \longrightarrow \widehat{\mathbb{Z}}$. Cette application injective est très loin d'être un isomorphisme car $\widehat{\mathbb{Z}}$ est non-dénombrable ! Pourtant, on a l'égalité $\overline{\mathbb{F}}_p^H = \mathbb{F}_p = \overline{\mathbb{F}}_p^{\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)}$.

Cet exemple montre que l'énoncé de la correspondance de Galois pour les extensions finies n'est pas vrai en général. Pour corriger la situation, on utilise l'isomorphisme (2.7.1.1) pour munir $\mathrm{Gal}(K/k)$ de la topologie induite par la *topologie produit* sur $\prod_{k'} \mathrm{Gal}(k'/k)$, où chaque $\mathrm{Gal}(k'/k)$ est muni de la topologie discrète. Par définition, on a les propriétés suivantes :

i) Pour tout espace topologique Y, une application $Y \longrightarrow \mathrm{Gal}(K/k)$ est continue si et seulement si chacune des composées $Y \longrightarrow \mathrm{Gal}(K/k) \xrightarrow{\pi_{k'}} \mathrm{Gal}(k'/k)$ est continue.

ii) Pour toute k' Galoisienne finie contenue dans K, le sous-groupe $\mathrm{Gal}(K/k') = \pi_{k'}^{-1}(\{\mathrm{id}_{k'}\})$ est ouvert, et tout voisinage ouvert de id_K contient un tel sous-groupe.

Grâce à i), on montre facilement que

iii) Le produit $\mathrm{Gal}(K/k)\times\mathrm{Gal}(K/k) \longrightarrow \mathrm{Gal}(K/k)$ et l'inverse $\mathrm{Gal}(K/k) \longrightarrow \mathrm{Gal}(K/k)$ sont des applications continues. On dit que $\mathrm{Gal}(K/k)$ est un *groupe topologique.*

Notons que dans un groupe topologique G, tout sous-groupe ouvert $H < G$ est aussi fermé (puisque son complémentaire est une union de classes à droite modulo H, qui sont ouvertes). De même tout sous-groupe fermé d'indice fini est aussi ouvert.

2.7.2 Proposition.– *Mêmes notations que ci-dessus.*

i) Pour toute extension intermédiaire $k \subset K' \subset K$, le sous-groupe $\mathrm{Gal}(K/K')$ est fermé dans $\mathrm{Gal}(K/k)$, et il est ouvert si et seulement si $k \subset K'$ est finie. De plus, la topologie induite sur $\mathrm{Gal}(K/K')$ est la topologie définie comme ci-dessus pour l'extension K/K'

ii) Soit $H < \mathrm{Gal}(K/k)$ un sous-groupe. Alors $\mathrm{Gal}(K/K^H) = \overline{H}$ (adhérence).

Démonstration. i) Supposons d'abord K' finie sur k. Si K'/k est Galoisienne, on a déjà vu que $\mathrm{Gal}(K/K')$ est ouvert, par définition de la topologie. Si K'/k n'est pas Galoisienne, choisissons une extension Galoisienne finie K''/k contenant K'. Alors $\mathrm{Gal}(K/K'')$ est ouvert, donc $\mathrm{Gal}(K/K')$ aussi puisque c'est une union de classes à droite modulo $\mathrm{Gal}(K/K'')$, et que chacune de ces classes est ouverte par iii).

Supposons maintenant K' quelconque. On a $\mathrm{Gal}(K/K') = \bigcap_{k'} \mathrm{Gal}(K/k')$, où k' parcourt les sous-extensions k'/k finies contenues dans K'. Comme $\mathrm{Gal}(K/k')$ est ouvert, donc fermé, cette intersection est fermée.

Réciproquement, si $\mathrm{Gal}(K/K')$ est ouvert, la propriété ii) ci-dessus nous dit que $\mathrm{Gal}(K/K')$ contient un $\mathrm{Gal}(K/k')$ pour k'/k Galoisienne finie, et donc $K' = K^{\mathrm{Gal}(K/K')} \subset K^{\mathrm{Gal}(K/k')} = k'$ est aussi finie.

Enfin, la topologie induite sur $\mathrm{Gal}(K/K')$ est engendrée par les translatés de $\mathrm{Gal}(K/k')\cap \mathrm{Gal}(K/K')$ pour k'/k finie, tandis que la topologie "naturelle" est engendrée par les translatés de $\mathrm{Gal}(K/K'')$ pour K''/K' finie. Or, toute extension finie K''/K' est de la forme $k'.K'$ (corps engendré par $k' \cup K'$) pour une extension finie k' de k et, de plus, on a $\mathrm{Gal}(K/k') \cap \mathrm{Gal}(K/K') = \mathrm{Gal}(K/k'.K')$. Donc les deux topologies coïncident.

ii) H est évidemment contenu dans $\mathrm{Gal}(K/K^H)$, qui est fermé. Donc $\overline{H} \subset \mathrm{Gal}(K/K^H)$. Il nous reste donc à montrer que H est dense dans $\mathrm{Gal}(K/K^H)$. Par le dernier point de

i), on peut sans perte de généralité supposer $K^H = k$. On doit donc montrer que H est alors dense dans $\mathrm{Gal}(K/k)$. Comme tout ouvert de $\mathrm{Gal}(K/k)$ est réunion d'ouverts de la forme $x.\mathrm{Gal}(K/k')$, il suffit de montrer que pour toute k'/k Galoisienne finie dans K et tout $x \in \mathrm{Gal}(K/k)$, l'intersection $H \cap x\mathrm{Gal}(K/k')$ est non vide.

Fixons donc k'/k et x. Notons $\pi_{k'}(H)$ l'image de H dans $\mathrm{Gal}(k'/k)$. On a $(k')^{\pi_{k'}(H)} = k$, donc par la correspondance de Galois pour les extensions finies, on a $\pi_{k'}(H) = \mathrm{Gal}(k'/k) = \pi_{k'}(\mathrm{Gal}(K/k))$. En particulier, il existe $h \in H$ tel que $\pi_{k'}(h) = \pi_{k'}(x)$. On a donc $x^{-1}h \in \mathrm{Ker}\,\pi_{k'} = \mathrm{Gal}(K/k')$, et il s'ensuit que $h = x.(x^{-1}h) \in H \cap x\mathrm{Gal}(K/k')$, montrant que cette intersection est bien non vide. □

On voit donc que la correspondance de Galois prend ici la forme d'une bijection entre sous-extensions de K/k et sous-groupes *fermés* de $\mathrm{Gal}(K/k)$. Comme dans le cas fini, l'extension est Galoisienne si et seulement si le sous-groupe associé est distingué.

Exercice. – Montrer que $\mathrm{Gal}(K/k)$ est *compact* (en admettant le théorème de Tychonoff!) et *totalement discontinu* (i.e. que les seuls sous-ensembles connexes sont les singletons).

Exemples. – i) Le groupe $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ est le Graal de certains arithméticiens. Pourtant, le seul élément non trivial que l'on connaît est la conjugaison complexe !

ii) Soit $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \cdots, \sqrt{p_n}, \cdots)$ où p_n et le n-ème nombre premier. Alors $\mathrm{Gal}(K/\mathbb{Q}) = (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$, muni de la topologie produit.

iii) Soit $\mathbb{Q}_{\mathrm{cyclo}} := \bigcup_n \mathbb{Q}(\mu_n)$. Alors $\mathrm{Gal}(\mathbb{Q}_{\mathrm{cyclo}}/\mathbb{Q}) = \varprojlim_n (\mathbb{Z}/n\mathbb{Z})^\times = (\widehat{\mathbb{Z}})^\times$. Le théorème de Kronecker-Weber affirme que toute extension Galoisienne finie abélienne de $\mathbb{Q}$ est contenue dans $\mathbb{Q}_{\mathrm{cyclo}}$. Ceci équivaut à $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})_{\mathrm{ab}} \simeq (\widehat{\mathbb{Z}})^\times$.