Extensions des corps

Robert Rolland

26 mars 2000

Table des matières

Chapitre 1

Extensions des corps.

1.1 Généralités

Soit L un corps contenant un sous corps K. Nous dirons que L est une **extension** de K et nous noterons L/K.

Le corps L a alors une structure d'espace vectoriel sur K. La dimension de cet espace vectoriel est appelée le **degré de l'extension** et est notée $[L : K]$. Si le degré de l'extension est fini on dit que **l'extension est finie**.

Les extensions successives ont la propriété suivante

Proposition 1.1.1 *Soient L/K et M/L deux extensions finies successives. Alors*

$$[M : K] = [M : L][L : K].$$

Preuve. Il suffit de considérer une base $(e_1, \cdots, e_m)$ de L sur K et une base $(f_1, \cdots, f_n)$ de M sur L. Tout élément $x \in M$ se décompose sous la forme

$$x = \sum_{i=1}^{n} x_i f_i,$$

avec $x_i \in L$.
Mais chaque x_i se décompose sous la forme

$$x_i = \sum_{j=1}^{m} x_{i,j} e_j,$$

avec $x_{i,j} \in K$, si bien que

$$x = \sum_{i=1}^{n} \sum_{j=1}^{m} x_{i,j} e_j f_i,$$

La famille $(e_j f_i)_{i,j}$ est donc génératrice sur K.
Pour montrer que cette famille est linéairement indépendante remarquons que si

$$\sum_{i,j} a_{i,j} e_j f_i = 0,$$

alors pour tout i, on a

$$\sum_{j} a_{i,j} e_j = 0,$$

et donc pour tout (i,j) le coefficient $a_{i,j}$ est nul. □

Un élément $\alpha \in L$ est dit **algébrique** sur K s'il existe un polynôme non nul $f(X) \in K[X]$ tel que $f(\alpha) = 0$. Si α n'est pas algébrique sur K on dit qu'il est **transcendant** sur K.

On dit que l'extension L/K est une **extension algébrique** si tous les éléments de L sont algébriques sur K.

Soit $S \subset L$. Le plus petit sous corps de L qui contienne à la fois K et S est noté $K(S)$, et appelé le **corps engendré** par S sur K. Lorsque $S = \{\alpha_1, \cdots, \alpha_n\}$ est une partie finie de L on note $K(\alpha_1, \cdots, \alpha_n)$ le corps engendré par S sur K. une **extension simple** de K est une extension $K(\alpha)/K$ où $\alpha \in L$.

1.2 Extensions simples

Nous commençons par l'étude des extensions simples car elles sont plus faciles à étudier, et qu'on peut obtenir des extensions engendrées par une partie finie, par des extensions simples successives.

Proposition 1.2.1 *Soient L/K une extension, et α_1, α_2 deux éléments de L. Alors*

$$K(\alpha_1, \alpha_2) = K(\alpha_1)(\alpha_2).$$

Preuve. Le corps $K(\alpha_1)(\alpha_2)$ est par définition le plus petit corps contenant à la fois α_2 et le corps $K(\alpha_1)$. Donc il contient K, α_1, α_2 et par suite il contient $K(\alpha_1, \alpha_2)$. Réciproquement, $K(\alpha_1, \alpha_2)$ contient $K(\alpha_1)$ et α_2, par suite il contient $K(\alpha_1)(\alpha_2)$. □

Ce résultat s'étend facilement à un nombre fini déléments.

Supposons que $L = K(\alpha)$ où $\alpha \in L$. Nous allons étudier l'extension L/K suivant que α est algébrique ou non.

1.2.1 Extensions algébriques simples

Supposons donc $L = K(\alpha)$ où α est algébrique sur K. Soit I l'ensemble des polynômes de $K[X]$ qui s'annulent au point α. Cet ensemble est un idéal. Soit $f(X)$ l'unique polynôme normalisé qui engendre I. Ce polynôme est irreductible de degré au moins 1. Le polynôme $f(X)$ est appelé **polynôme minimal** de α. C'est le polynôme de $K[X]$, normalisé de plus petit degré tel que $f(\alpha) = 0$.

Théorème 1.2.1 *Le corps $L = K(\alpha)$ est isomorphe au quotient*

$$K[X]/(f(X)).$$

Preuve. Remarquons tout d'abord que l'idéal $I = (f(X))$ est un idéal maximal. Donc $K[X]/(f(X))$ est un corps. Soit ϕ l'homomorphisme de $K[X]$ dans L défini par $\phi(P(X)) = P(\alpha)$. Le noyau de ϕ est l'idéal $(f(X))$. Donc le corps $K[X]/(f(X))$ est isomorphe à $\phi(K[X])$. Montrons que $\phi(K[X]) = K(\alpha)$. Il est clair que $K \subset \phi(K[X])$ et que $\alpha \in \phi(K[X])$. Donc $K(\alpha) \subset \phi(K[X])$. De plus la définition de ϕ montre que $\phi(K[X]) \subset K(\alpha)$. □

Corollaire 1.2.1 *L'extension $K(\alpha)/K$ est finie et de degré le degré du polynôme minimal de α.*

Preuve. Soit n le degré du polynôme minimal. Il suffit de remarquer que si on note β la classe du polynôme X dans $K[X]/(f(X))$ alors $(1, \beta, \cdots, \beta^{n-1})$ est une base de $K[X]/(f(X))$ sur K. □
Nous verrons plus loin que toute extension finie est algébrique, et donc que en particulier $K(\alpha)/K$ est algébrique.

1.2.2 Extensions transcendantes simples

Supposons donc $L = K(\alpha)$ où α est transcendant sur K.

Théorème 1.2.2 *Le corps $L = K(\alpha)$ est isomorphe au corps $K(X)$ des fractions rationnelles sur K.*

Preuve. Soit ϕ l'homomorphisme de $K(X)$ dans L qui à tout $r(X)$ de $K[X]$ associe $r(\alpha)$. Comme aucun polynôme non nul s'annule en α, Le noyau de ϕ est réduit à $\{0\}$. Par suite $K(X)$ est isomorphe à $\phi(K(X))$. Mais clairement $\phi(K(X))$ contient K et α. Donc $\phi(K(X))$ contient L et par suite lui est égal. □

1.3 Extensions finies - Extensions algébriques

Proposition 1.3.1 *Soient L/K une extension, et $a \in L$ un élément transcendant. Alors l'extension L/K n'est pas finie.*

Preuve. Il suffit de constater que pour tout entier $n > 0$, les éléments $1, a, a^2, \cdots, a^n$ sont indépendants sur K puisque

$$\sum_{i=0}^{n} u_i a^i,$$

où $u_i \in K$, ne peut être nul que si le polynôme

$$f(X) = \sum_{i=0}^{n} u_i X^i$$

est identiquement nul.

Corollaire 1.3.1 *Une extension finie est algébrique.*

Théorème 1.3.1 *Une extension L/K est finie si et seulement si elle est engendrée sur K par un famille finie d'éléments algébriques de L.*

Preuve. Supposons $L = K(\alpha_1, \cdots, \alpha_n)$ où les éléments α_i sont algébriques sur K. Alors $L = K(\alpha_1, \cdots, \alpha_{n-1})(\alpha_n)$. Par suite $L/K(\alpha_1, \cdots, \alpha_{n-1})$ est finie. De proche en proche on conclut que L/K est finie.
Supposons que L/K soit finie. Alors on sait que que L/K est algébrique. Soit $(e_1, \cdots, e_n)$ une base de L sur K. Alors $L = K(e_1, \cdots, e_n)$. □

Théorème 1.3.2 *Soient α_1 et α_2 deux élémenta algébriques. Alors $\alpha_1 + \alpha_2$, $\alpha_1\alpha_2$, $1/\alpha_1$, sont algébriques.*

Preuve. Il suffit de dire que $K(\alpha_1, \alpha_2)$ est une extension algébrique de K et que $\alpha_1 + \alpha_2$, $\alpha_1\alpha_2$ et $1/\alpha_1$ sont dans cette extension. □

On en déduit tout de suite que

Corollaire 1.3.2 *Soit L/K une extension. L'ensemble $\tilde{K}$ des éléments de L qui sont algébriques sur K est un sous corps de L contenant K.*

Le sous corps $\tilde{K}$ est appelé la **clôture algébrique** de K dans L. C'est bien entendu une extension algébrique de K.

Proposition 1.3.2 *Soient L/K et M/L deux extensions algébriques successives. Alors M/K est une extension algébrique.*

Preuve. Soit $x \in M$. Alors x est algébrique sur L. Soit $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ le polynôme minimal de x dans l'extension M/L. Soit $L_1 = K(a_0, \cdots, a_{n-1})$, alors x est algébrique sur L_1. Par suite $L_1(x)$ est une extension finie de L_1 et L_1 une extension finie de K, donc $L_1(x)$ est une extension finie de K, ce qui prouve que $L_1(x)$ est une extension algébrique de K et donc x est algébrique. □

Lorsqu'on a une extension L/K et une tour

$$K \subset K_1 \subset \cdots \subset K_m$$

d'extensions algébriques successives de telle sorte que $K_i \subset L$, alors $K_i \subset \tilde{K}$.

Corollaire 1.3.3 *Soit L/K une extension transcendante et soit $\tilde{K}$ la clôture algébrique de K dans L. Alors la dimension de L sur $\tilde{K}$ est infinie.*

Preuve. Si la dimension de L sur $\tilde{K}$ était finie, alors L serait algébrique sur $\tilde{K}$ et donc sur K. □

1.4 Plongements, K-isomorphismes

Soient K_1 et K_2 deux corps. Soit s un homomorphisme de K_1 dans K_2. Comme pour $x \neq 0$ on a $s(x) = (s(x^{-1}))^{-1}$, le noyau de s est réduit à $\{0\}$, donc s est injective. L'application s est appelé un **plongement** de K_1 dans K_2. Si L_1/K_1 et L_2/K_2 sont deux extensions et si s est un plongement de de K_1 dans K_2, nous nous intéressons aux plongements σ de L_1 dans L_2 qui prolongent s, c'est-à-dire qui vérifient pour tout $x \in K_1$ la condition $\sigma(x) = s(x)$. On les appelle les **extensions** de s. Dans le cas où $K_1 = K_2 = K$ et où s est l'identité sur K c'est-à-dire que σ est un plongement de L_1 dans L_2 vérifiant pour tout $x \in K$ la relation $\sigma(x) = x$, on dit que σ est un **K-plongement** de L_1 dans L_2.
Si en outre σ est surjective (et par conséquent bijective) on dit que c'est un **K-isomorphisme**.
La proposition suivante envisage le cas important où $L_1/K_1 = L_2/K_2 = L/K$.

Proposition 1.4.1 *Soit L/K une extension et σ un K-plongement de L dans L. Alors σ est un K-isomorphisme.*

Preuve. Soit $\alpha \in L$ et $f(X)$ le polynôme minimal de α sur K. Soit S l'ensemble des racines de $f(X)$ qui sont dans L. On sait par hypothèse que $\alpha \in S$. De plus si $\beta \in S$ alors $f(\sigma(\beta)) = \sigma(f(\beta)) = 0$, et donc $\sigma(\beta) \in S$. Comme σ est injective, sa restriction à l'ensemble fini S est bijective. Par suite il existe $\beta \in S$ tel que $\sigma(\beta) = \alpha$. Ce qui prouve que σ est surjective. □

Théorème 1.4.1 *Soient L/K une extension, $\alpha \in L$ un élément algébrique sur K de polynôme minimal $f(X)$ et Θ un corps algébriquement clos. Si s est un plongement de K dans Θ alors*

1) si β est une racine de $f^s(X)$ alors s peut être étendu en un plongement σ de $K(\alpha)$ dans Θ de telle sorte que $\sigma(\alpha) = \beta$.

2) Toute extension de s en un plongement σ de $K(\alpha)$ dans Θ doit être tel que $\sigma(\alpha)$ soit une racine de $f^s(X)$.

3) le nombre d'extensions de s à $K(\alpha)$ est égal au nombre de racines distinctes de $f(X)$ (en particulier lorsque toutes les racines sont distinctes, ce nombre est le degré de $f(X)$, c'est-à-dire le degré de l'extension $K(X)/K$).

Preuve. Rappelons que si $f(X) = \sum a_i X^i$ alors $f^s(X) = \sum s(a_i)X^i$.

Ce dernier polynôme est aussi irréductible sur $s(K)$ mais se décompose entièrement sur Θ. Donc $f^s(X)$ est polynôme minimal sur $s(K)$ de chacune de ses racines dans Θ. Soit β une racine de $f^s(X)$ dans Ω. Alors

$$K(\alpha) = \{g(\alpha) | g(X) \in K[X] \text{ et } deg(g(X)) < deg(f(X))\},$$

et comme $deg(f^s(X)) = deg(f(X))$,

$$s(K)(\beta) = \{h(\beta) | h(X) \in s(K)[X] \text{ et } deg(h(X)) < deg(f(X))\}.$$

On peut donc définir une application σ de $K(\alpha)$ dans $s(K)(\beta)$ en posant

$$\sigma(g(\alpha)) = g^s(\beta).$$

On voit que σ répond à la question.
Les assertions 2) et 3) en découlent. □

On peut maintenant généraliser le théorème précédent.

Théorème 1.4.2 *Soit L/K une extension algébrique et Θ un corps algébriquement clos. Si s est un plongement de K dans Θ alors il existe une extension σ de s à L.*
De plus, si $\alpha \in L$, si $p(X)$ est le polynôme minimal de α sur K et si $\beta \in \Theta$ est une racine de $p^s(X)$ alors on peut construire σ de telle sorte que $\sigma(\alpha) = \beta$.
Si de plus l'extension L/K est finie, le nombre de plongements σ qui prolongent s est $\leq [L : K]$.

Preuve. On introduit une relation d'ordre $\prec$ dans l'ensemble $\mathcal{E}$ de toutes les extensions de s, τ de M dans Θ telles que M soit un corps intermédiaire entre K et L contenant α et que $\tau(\alpha) = \beta$. On a vu que $\mathcal{E}$ est non vide. La relation $\prec$ est définie par

$$\tau_1 \prec \tau_2 \Longleftrightarrow M_1 \subset M_2 \text{ and } \tau_2 | M_1 = \tau_1.$$

Cette relation est un ordre partiel sur $\mathcal{E}$. Si $(s_i)_i$ est une chaîne dans $\mathcal{E}$ alors l'application τ définie sur $\cup_i M_i$ par $\tau | M_i = s_i$ est une borne superieure pour $(s_i)_i$. Le lemme de Zorn implique donc l'existence d'un élément maximal σ dans $\mathcal{E}$. Cet élément maximal est forcément défini sur L sinon on pourrait l'étendre d'après le théorème précédent.

Pour démontrer la dernière partie posons $L = K(\alpha_1, \cdots, \alpha_r)$. Soit alors σ une extension de s à L. Considérons les restrictions

$$s_1 = \sigma|K(\alpha_1), s_2 = \sigma|K(\alpha_1, \alpha_2), \cdots, s_{r-1} = \sigma|K(\alpha_1, \cdots, \alpha_{r-1}), s_r = \sigma.$$

Ainsi d'après le théorème 1.4.1 il y a au plus $[K(\alpha_1) : K]$ prolongements s_1 possibles, puis au plus $[K(\alpha_1) : K][K(\alpha_1, \alpha_2) : K(\alpha_1)]$ prolongements possibles, etc.. On trouve ainsi que le nombre des prolongements σ possibles est au plus

$$\prod_i [K(\alpha_1, \cdots, \alpha_i) : K(\alpha_1, \cdots, \alpha_{i-1})] = [L : K]. \square$$

1.5 Corps de décomposition - Clôture algébrique

1.5.1 Adjonction d'une racine - Corps de rupture

Théorème 1.5.1 *Soit K un corps et $f(X) \in K[X]$ un polynôme non constant. Il existe une extension algébrique simple $L = K(\alpha)$ de K telle que $f(\alpha) = 0$. Si de plus $f(X)$ est irréductible dans K, cette extension est unique à un K-isomorphisme près, c'est-à-dire que si $L' = K(\alpha')$ est une autre extension telle que $f(\alpha') = 0$ alors il existe un K-isomorphisme σ de L sur L' tel que $\sigma(\alpha) = \alpha'$.*

Preuve. On peut supposer que $f(X)$ est irréductible et normalisé. Dans ce cas considérons le quotient $L = K[X]/(f(X))$. Comme $f(X)$ est irréductible l'idéal $(f(X))$ qu'il engendre est un idéal maximal, donc le quotient L est un corps. Considérons dans L l'élément α classe du polynôme X. Il est clair que $f(\alpha) = 0$. Dans l'extension K/L on considère le sous corps $K(\alpha)$. Le polynôme minimal de α est le polynôme f. Alors $K(\alpha) = K[X]/(f(X)) = L$. Le polynôme minimal de α est aussi celui de α', si bien que l'homomorphisme σ de $K[X]/(f(X))$ sur $K(\alpha')$ qui à la classe du polynôme PX associe $P(\alpha')$ est un K-isomorphisme. $\square$

Lorsque le polynôme $f(X)$ est irréductible, le corps $K(\alpha)$ ainsi construit est le **corps de rupture** de $f(X)$ sur K.

1.5.2 Corps de décomposition

Soit $f(X) \in K[X]$. Un **corps de décomposition** pour $f(X)$ sur K est une extension de K pour laquelle $f(X)$ se décompose en produit de facteurs linéaires et qui est engendré par l'ensemble de toutes les racines de $f(X)$.

Théorème 1.5.2 *Tout polynôme non nul de $K[X]$ admet un corps de décomposition unique à un K-isomorphisme près.*

Preuve. On raisonne par récurrence sur le degré de $f(X)$. Si ce degré est 1, l'extension K/K convient. Si ce degré est > 1, considérons un corps de rupture $L_1 = K(\alpha)$ d'un facteur irréductible de $f(X)$. Dans L_1 on peut donc écrire $f(X)$ sous la forme $f(X) = (X-\alpha)g(X)$. Par hypothèse de récurrence soit $L = L_1(x_1, x_2, \cdots, x_{d-1})$ un corps de décomposition de $g(X)$ sur L_1. Alors $L = K(\alpha, x_1, \cdots, x_{d-1})$ est un corps de décomposition de $f(X)$ sur K.
Pour l'unicité nous démontrerons le résultat suivant:
si s est un isomorphisme de K dans K', si L est un corps de décomposition de $f(X)$ sur K et si L' est un corps de décomposition de $f^s(X)$ sur K', alors il existe un isomorphisme σ de L sur L' qui prolonge s.
Faisons une récurrence sur $[L : K]$. Si $L = K$ il est clair que $L' = K'$. Sinon, soit $\alpha \in L \setminus K$ une racine de $f(X)$. Soit $g(X)$ le ploynôme minimal de α. C'est un facteur irréductible de $f(X)$. Donc $g^s(X)$ est un facteur irréductible de $f^s(X)$. Soit α' une racine de $g^s(X)$ dans L'. On pose $M = K(\alpha)$ et $M' = K'(\alpha')$. On sait en effet que M est un corps de rupture pour $g(X)$ donc $M \simeq K[X]/(g(X))$ et que de même $M' \simeq K'[X]/(g^s(X))$. Or il est clair que $K[X]/(g(X)) \simeq K'[X]/(g^s(X))$ grâce à s. Donc M est isomorphe à M' et de plus, en regardant en détail les isomorphismes précédents on voit que cet isomorphime s_1 prolonge s et vérifie $s_1(\alpha) = \alpha'$. En utilisant l'hypothèse de récurrence on conclut. □

Ce théorème s'étend visiblement au cas d'un ensemble fini de polynômes. Il s'étend aussi au cas d'un ensemble quelconque de polynômes, mais la démonstration est plus technique. Nous la donnerons dans le paragraphe suivant.

1.5.3 Clôture algébrique

Un corps Ω est **algébriquement clos** si tout polynôme de $\Omega[X]$ de degré ≥ 1 possède une racine dans ω (et donc se décompose en facteurs linéaires dans Ω).

Si K est un corps on appelle **clôture algébrique** de K, tout extension algébrique de K qui est algébriquement close.

Théorème 1.5.3 *Soit L/K une extension. Les conditions suivantes sont équivalentes:*

1) L est une clôture algébrique de K.

2) L est une extension algébrique maximale de K.

Preuve. Supposons 1) et soit $K \subset L \subset L_1$ où L_1/K est algébrique (et donc aussi L_1/L). Soit $\alpha \in L_1$, et $f(X)$ le polynôme minimal de α sur K. Puisque L est une clôture algébrique de K, $f(X)$ se décompose sur L et donc $\alpha \in L$ par suite $L_1 = L$.
Supposons 2). Soit $h(X) \in L[X]$ et $L(\alpha)$ un corps de rupture de $h(X)$. Ce corps est une extension algébrique de L et donc il est égal à L. Par suite la racine α de $h(X)$ est dans L. □

Théorème 1.5.4 *Tout corps K a une extention algébrique Ω algébriquement close unique à un K-isomorphisme près.*

Preuve. Pour toute parie finie $I = \{f_1(X), \cdots, f_r(X)\}$ de $K[X]$ considérons l'anneau $A_I = K[X_{f_1(X)}, \cdots, X_{f_r(X)}]$ puis définissons

$$A = \bigcup_I A_I,$$

où I parcourt l'ensemble des parties finies de $K[X]$. L'ensemble A est lui même un anneau. Soit N l'idéal de A engendré par les éléments de la forme $f(X_{f(X)})$. L'idéal N diffère de A car sinon on pourrait écrire

$$q_1 f_1(X_{f_1(X)}) + \cdots + q_n f_n(X_{f_n(X)}) = 1,$$

avec $q_i \in A$. Mais il existe une extension L de K dans laquelle les polynômes $f_1(X), \cdots, f_n(X)$ ont une racine $\alpha_1, \cdots, \alpha_n$. En donnant les valeurs $\alpha_1, \cdots, \alpha_n$ aux variables $X_{f_1(X)}, \cdots, X_{f_n(X)}$ on obtient une contradiction. Par suite il existe un idéal maximal M contenant N. Alors $K_1 = A/M$ est un corps dans lequel tout polynôme $f(X) \in K[X]$ admet pour racine la classe de $X_{f(X)}$. De la même façon on peut construire K_2 extension de K_1 tel que tout polynôme de $K_1[X]$ a une racine dans K_2. et par récurrence une suite K_i. Prenons alors

$$\Theta = \cup_i K_i.$$

Tout polynôme $\in \Theta[X]$ a tous ses coefficients dans un certain K_i et donc a une racine dans K_{i+1}. On en conclut que Θ est une extension de K qui est algébriquement close.
Soit Ω la clôture algébrique de K dans Θ. On sait que Ω est une extension algébrique de K. Tout polynôme $h(X) \in \Omega[X]$ se décompose dans Θ. Les racines de $h(X)$ sont dans Θ et sont algébriques sur Ω. Mais puisque Ω est algébrique sur K, ces racines sont algébriques sur K et donc appartiennent à Ω. Par suite Ω est algébriquement clos et extension algébrique de K.
L'unicité découle du théorème 1.4.2 et de la maximalité d'une clôture algébrique. □

Théorème 1.5.5 *Toute famille de polynômes de $K[X]$ admet un corps de décomposition unique à un K-isomorphisme près.*

Preuve. Il suffit de se placer dans la clôture algébrique de K et de prendre dans cette clôture le sous corps engendré par toutes les racines de tous les polynômes de la famille donnée.
Soient L_1 et L_2 deux corps de décomposition pour la famille. Soit L_2' une clôture algébrique de L_2. On peut donc étendre l'application d'inclusion de K dans L_2' en un K-plongement σ de L_1 dans L_2'. Soient $E_1(f) \subset L_1$ et $E_2(f) \subset L_2$ des corps de rupture d'un polynôme $f(X)$ de la famille. Soit σ_1 la restriction à $E_1(f)$ de σ. Soit R_i l'ensemble des racines de $f(X)$ dans $E_i(f)$. Comme $f^{\sigma_1}(X) = f(X)$, $\sigma_1(R_1) \subset R_2$. Or σ_1 est injective, R_1 et R_2 sont des ensembles finis et on a aussi $\sigma_1^{(-1)}(R_2) \subset R_1$. Donc $\sigma_1(R_1) = R_2$ On en déduit que

$$\sigma_1(E_1(f)) = \sigma_1(K(R_1)) = K(\sigma_1(R_1)) = K(R_2) = E_2(f).$$

Par suite σ_1 est un isomorphisme de $E_1(f)$ sur $E_2(f)$.
Posons $\bigvee_f E_i(f)$ le corps engendré dans L_i par tous les $E_i(f)$ lorsque f parcourt la famille de polynômes. On voit que $\bigvee_f E_i(f) = L_i$. De plus

$$\sigma(L_1) = \sigma(\bigvee_f E_1(f)) = \bigvee_f \sigma(E_1(f)) = \bigvee_f E_2(f)) = L_2.$$

On en conclut que σ est un isomorphisme de L_1 sur L_2. □

1.5.4 Extension normale

Soient K un corps, L une extension algébrique de K, Ω la clôture algébrique de L (donc aussi de K).

Théorème 1.5.6 *Les propriétés suivantes sont équivalentes:*
1) L est le corps de décomposition d'une famille de polynômes sur K.
2) Tout K-plongement de L dans Ω est un automorphisme de L.
3) Tout polynôme irréductible sur K qui a une racine dans L se décompose dans L.

Preuve.
1) implique 2):
Soit σ un K-plongement de L dans Ω. On sait que si on note Z l'ensemble de toutes les racines des polynômes de la famille dont L est le corps de décomposition alors $L = K(Z)$. La restriction de σ à Z est une bijection. En effet si α est une racine alors $\sigma(\alpha)$ aussi. D'autre part si β est racine d'un polynôme f irréductible sur K en restreignant σ (qui est injective) à l'ensemble fini des racines de f on voit qu'il existe une racine α de f telle que $\sigma(\alpha) = \beta$.
Donc $\sigma(Z) = Z$.
Par suite

$$\sigma(L) = \sigma(K(Z)) = K(\sigma(Z)) = K(Z) = L.$$

2) implique 3):
Soit $f(X)$ un polynôme irréductible sur K ayant une racine α dans L. Soit $\beta \in \Omega$ une racine de $f(X)$. L'injection de K dans Ω peut être étendue en σ de L dans Ω avec de plus $\sigma(\alpha) = \beta$. Par hypothèse σ est un automorphisme, donc $\beta \in L$.

3) implique 1):
Il suffit de voir que L est le corps de décomposition de la famille des polynômes minimaux des éléments de L.

Une extension algébrique L/K qui satisfait ces conditions équivalentes est une **extension normale**.

Chapitre 2

Séparabilité.

2.1 Polynômes séparables

Un polynôme irréductible $f(X) \in K[X]$ de degré $geq1$ est **séparable** s'il n'a aucune racine multiple dans la clôture algébrique de K.
Dans le cas contraire il est **inséparable**.

Théorème 2.1.1 *Un polynôme irréductible $f(X)$ est séparable si et seulement si $f'(X) \neq 0$.*
Si le corps K est de caractéristique nulle, tous les polynômes irréductibles sont séparables.
Si le corps est de caractéristique $p > 0$ alors un polynôme irréductible $f(X) = \sum a_i X^i$ est séparable si et seulement si $a_i \neq 0$ pour un certain $i \not\equiv 0 \mod p$.

Preuve. On sait que $f(X)$ a des racines multiples si et seulement si $f(X)$ et $f'(X)$ ont des racines communes. Donc $f(X)$ est séparable si et seulement si $f(X)$ et son polynôme dérivé $f'(X)$ sont premiers entre eux, c'est-à-dire si et seulement si $f(X) \neq 0$.
Si le corps est de caractéristique 0 on voit que la condition $f'(X) \neq 0$ est réalisée.
De même si le corps est de caractéristique $p > 1$, la condition $f'(X) \neq 0$ est réalisée si et seulement s'il existe un $a_i \neq 0$ pour un $i \not\equiv 0 \mod p$. □

Théorème 2.1.2 *Plaçons nous dans le cas où le corps K est de caractéristique p non nulle. Soit $f(X) \in K[X]$ un polynôme irréductible sur K.*
1) Si $f(X) = h(X^{p^d})$ où $h(X)$ est un polynôme non constant et d un entier strictement positif alors $f(X)$ est inséparable.

2) Si $f(X)$ est inséparable il existe un polynôme séparable $g(X) \in K[X]$ et un entier $d > 0$ tels que

$$f(X) = g(X^{p^d}).$$

Dans ce cas toutes les racines de $f(X)$ ont pour multiplicité d.

Preuve. Pour montrer le 1) il suffit de dériver le polynôme $h(X^{p^d})$ pour voir que le résultat est nul et donc que $f(X)$ est inséparable.
Pour montrer le 2) remarquons que si $f(X)$ est inséparable alors en vertu du théorème précédent les coefficients a_i non nuls ne peuvent exister que pour p divisant i. Donc $f(X) = g(X^p)$. Si $g(X)$ est séparable on a terminé, sinon on recommence avec le polynôme $g(X)$, et ainsi de suite.
Dans ce cas, soit α une racine de $f(X)$ alors α^{p^d} est une racine de $g(X)$. Donc $g(X) = (X - \alpha^{p^d})v(X)$, ou encore $f(X) = (X^{p^d} - \alpha^{p^d})v(X^{p^d})$. Mais $(X^{p^d} - \alpha^{p^d}) = (X - \alpha)^{p^d}$, donc $f(X) = (X - \alpha)^{p^d}u(X)$ (où $u(X) = v(X^{p^d})$). $u(X)$ ne peut avoir α pour racine sinon $v(X)$ aurait α^{p^d} pour racine, ce qui est impossible puisque $g(X)$ n'a pas de racines multiples. Donc $f(X)$ admet α pour racine avec une multiplicité p^d. □

Remarquons que si le corps K est fini, il possède $q = p^n$ él'ements, et dans ce cas tout polynôme irréductible est séparable. En effet sinon on aurait

$$f(X) = g(X^p) = a_0 + a_1X^p + \cdots + a_rX^{pr}$$

ou encore

$$f(X) = (b_0 + b_1X + \cdots + b_rX^r)^p$$

où $b_i = a_i^{q/p} = a_i^{p^{n-1}}$.

2.2 Extensions séparables

Soit L/K une extension algébrique. Un **élément α est séparable** sur K si son polynôme minimal est séparable.
L'extension L/K est séparable si tous les éléments de L sont séparables.

Théorème 2.2.1 *Soit L/K une extension finie de degré n, Ω une clôture algébrique de K et s un plongement de K dans Ω. L'extension L/K est*

séparable si et seulement s'il existe n distincts plongements de L dans Ω prolongeant s. En particulier en prenant pour s l'inclusion, l'extension L/K est séparable si et seulement s'il existe n distincts K-plongements de L dans Ω.

Théorème 2.2.2 *Pour des extensions algébriques successives L/K, M/L, on peut dire que M/K est séparable si et seulement si les extensions L/K et M/L le sont.*

2.3 Corps parfaits

Un **corps parfait** est un corps K qui est de caractéristique nulle, ou, qui étant de caractéristique p vérifie $K^p = K$ c'est-à-dire si l'endomorphisme ϕ_p qui à tout x associe x^p est surjectif.

Un corps algébriquement clos est parfait (l'équation $x^p = a$ a toujours une solution). Un corps fini est parfait (dans ce cas ϕ_p étant injectif est forcément surjectif).

Proposition 2.3.1 *Si K est un corps parfait, tout polynôme irréductible dont la dérivée est nulle est constant.*

Preuve. Soit $f \in K[X]$ un polynôme irréductible écrit sous la forme

$$f(X) = \sum_{n \geq 0} a_n X^n.$$

Alors

$$f'(X) = \sum_{n \geq 0} n a_n X^{n-1}.$$

Le polynôme $f'(X)$ est nul si et seulement si $na_n = 0$ pour tout $n \geq 1$. Si K est de caractéristique 0 ceci est équivalent à $a_n = 0$ pour $n \geq 1$, c'est-à-dire à $f(X)$ est constant.
Si la caractéristique de K est p, ceci est équivalent à $a_n = 0$ pour tout entier n non multiple de p et donc

$$f(X) = \sum_{n \geq 0} a_{pn} X^{pn}.$$

Puisque K est parfait $K^p = k$ et on peut don écrire $a_{pn} = c_n^p$. En posant

$$g(X) = \sum_{n \geq 0} c_n X^n,$$

on calcule

$$g(X)^p = f(X),$$

si bien que si le degré de $g(X)$ est strictement positif $f(X)$ n'est pas irréductible.□

Théorème 2.3.1 *Pour qu'un corps K soit parfait il faut et il suffit que toute extension algébrique de k soit séparable.*

Preuve. Soit K parfait, L une extension algébrique de K et $x \in L$. Soit $f(X)$ le polynôme minimal de x sur K, c'est un polynôme non constant, et puisque K est parfait sa dérivée n'est pas nulle. On sait alors qu'il est séparable.
La condition est suffisante: c'est clair si la caractéristique de k est nulle. Sinon, soit $a \in k$ et b dans la clôture algébrique Ω de k tel que

$$a = b^p.$$

Le polynôme minimal $f(X)$ de b sur k divise $(X - b)^p = X^p - a$. Donc $f(X) = (X - b)^r$ et comme ses racines sont simples c'est que $r = 1$ et $b \in k$.
□

Compte tenu des résultats connus pour les extensions séparables, nous avons le théorème suivant:

Théorème 2.3.2 *Soit K un corps parfait et L/K une extension finie de degré n, Ω une clôture algébrique de K et s un plongement de K dans Ω.*
Il existe exactement n distincts plongements de L dans Ω prolongeant s.
Il existe exactement n distincts K-plongements de L dans Ω.

Théorème 2.3.3 *Soit K un corps parfait et L une extension de degré fini de L. Alors il existe un élément x de L tel que $L = K(x)$.*

Preuve. Supposons dans un premier temps que$K$ soit infini et posons $n = [L : K]$. Il existe n K-homomorphismes $\sigma_1, \cdots, \sigma_n$ de K dans la clôture algébrique Ω de K. Les équations

$$\sigma_i(x) = \sigma_j(x) \quad (1 \leq i, j \leq n, i \neq j)$$

définissent des hyperplans de L. Puisque K est infini, le complémentaire de ces hyperplans est non vide et contient donc au moins un élément x. Comme les conjugués de x sont tous différents, le degré de x est au moins n, donc $K = k(x)$.
Si maintenant K est fini, on sait qu'il y a un élément primitif d'après l'étude des corps finis.

2.4 Extensions galoisiennes

Une extension L/K **de degré fini** est **galoisienne** si elle est **normale et séparable**.

Si le corps K est **parfait**, une extension de degré fini est galoisienne si et seulement si elle est normale.

On sait par l'étude des extensions normales, qu'une extension algébrique L/K de degré fini est normale si et seulement si tout K-plongement de L dans la clôture algébrique Ω de K est un K-automorphisme.

Si l'extension algébrique L/K est galoisienne, on appelle **groupe de Galois** de L sur K le groupe des K-automorphismes de L. On notera $Gal(L/K)$ ce groupe. Compte tenu des résultats précédents on peut écrire

$$\sharp Gal(L/K) = [L : K].$$

Une situation classique d'obtention d'une extension galoisienne est le cas où le corps K est parfait et où L est le corps de décomposition d'un polynôme sur K.

Chapitre 3

Théorie de Galois.

3.1 Le théorème fondamental

Soit L/K une extension galoisienne et E un corps intermédiaire

$$K \subset E \subset L.$$

On vérifie que L est aussi une extension galoisienne sur E.

Si H est un sous groupe de $Gal(L/K)$, l'ensemble L^H des $x \in L$ invariants par H est un sous corps de L contenant K, appelé **corps des invariants** de H.

Le théorème fondamental de la théorie de Galois indique les relations entre les corps intermédiaires et les sous groupes du groupe de Galois.

Théorème 3.1.1 *Soit L/K une extension galoisienne. Soit $(\mathcal{E})$ l'ensemble des extensions intermédiaires de K contenues sans L et soit $(\mathcal{G})$ l'ensemble des sous groupes de $G = Gal(L/K)$. L'application*

$$H \mapsto L^H$$

est une bijection de $(\mathcal{G})$ sur $(\mathcal{E})$. La bijection réciproque est

$$E \mapsto Gal(L/E).$$

Remarquons que si $H = Gal(L/E)$ alors

$$[L : E] = \sharp H,$$

donc

$$[E : K] = \sharp G/\sharp H.$$

Corollaire 3.1.1 *Soient L/K une extension galoisienne, E une extension intermédiaire. Soit H le sous groupe de $Gal(L/K)$ correspondant à E.*

(a) Soit $\sigma \in G$. Le sous groupe de G correspondant à $\sigma(E)$ est le sous groupe conjugué $\sigma H \sigma^{-1}$.

(b) Pour que E soit une extension galoisienne de K il faut et il suffit que $\sigma(E) = E$ ou encore que H soit distingué dans G.

(c) S'il en est ainsi. l'homomorphisme de restriction

$$G \mapsto Gal(E/K)$$

définit par passage au quotient un isomorphisme

$$G/H \mapsto Gal(E/K).$$

Index