Théorie de Galois

Cours de Maîtrise — Saint-Etienne 2002/2003

Bruno Deschamps

Table des matières

Chapitre 1

Introduction à la théorie des corps

1.1 Généralités

1.1.1 Anneaux et corps

Définition.— *On appelle anneau tout ensemble A non vide muni de deux lois de compositions internes $+$ et $.$ telles que $(A,+)$ soit un groupe abélien et telles que $.$ soit associative et distributive par rapport à $+$.*

• *On dit que A est unitaire s'il existe $e \in A$ tel que pour tout $a \in A$, $a.e = e.a = a$. Si A est unitaire, l'élément e est unique, on le note 1_A ou 1 s'il n'y a pas d'ambiguité.*

• *On dit que A est intégre si chaque élément de A est régulier, c'est-à-dire si pour tout $a, b, c \in A$ $(a \neq 0)$ on a $a.b = a.c \Rightarrow b = c$ et $b.a = c.a \Rightarrow b = c$.*

• *On dit que A est commutatif si $.$ est une loi commutative.*

Soit A un anneau unitaire. Un élément $a \in A$ est dit inversible dans A s'il existe $b \in A$ tel que $a.b = b.a = 1$. L'élément b est alorts unique et s'appelle l'inverse de a. On le note a^{-1}. L'ensemble des éléments inversible de A s'appelle le groupe des unités de A. C'est un groupe pour $.$, on le note $U(A)$.

Définition.— *On appelle corps tout anneau unitaire A tel que $U(A) = A - \{0\}$. Si A est commutatif, on parle de corps commutatif, dans le cas contraire, on parle de corps gauche.*

Définition.— *Soient A et B deux anneaux unitaires, on appelle morphisme d'anneaux, toute application $f : A \to B$ vérifiant*

$$\forall x, y \in A,\ f(x+y) = f(x) + f(y),\ f(xy) = f(x)f(y) \text{ et } f(1_A) = 1_B$$

Lemme.— *Sous les hypothèses de la définition précédente, on a*

$$f(U(A)) \subset U(B)$$

et $\forall a \in U(A)$, $f(a^{-1}) = (f(a))^{-1}$.

Proposition.— • *Tout corps est un anneau intègre.*

• *Soit A un anneau commutatif. A est un corps ssi A ne possède que deux idéaux, $\{0\}$ et A.*

• *Soit k un corps commutatif et A un anneau unitaire. Tout morphisme d'anneau $f : k \to A$ est injectif.*

Exemple : Soit $n \in \mathbb{N}^*$. Les propositions suivantes sont équivalentes :

i) n est premier,

ii) $\mathbb{Z}/n\mathbb{Z}$ est intègre,

iii) $\mathbb{Z}/n\mathbb{Z}$ est un corps.

Si p désigne un nombre premier, on note $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Définition.— *Soit $(K, +, .)$ un corps. On appelle sous-corps de K, toute partie k de K stable par $+$ et $.$ telle que $(k, +, .)$ soit un corps.*

Lemme.— *Soit K un corps et $(k_i)_i$ une famille de sous-corps de K. Alors $\bigcap_i k_i$ est un sous-corps de K.*

Si k est un sous-corps de K et A une partie de K, l'intersection des sous-corps de K contenant k et A est donc un sous-corps de K (l'intersection ne se fait pas sur un ensemble vide car K contient A et k). Ce corps est le plus petit sous-corps (au sens de l'inclusion) de K contenant k et A.

Définition.— *On appelle corps engendré dans K par A sur k le plus petit sous-corps (au sens de l'inclusion) de K contenant k et A. On le note $k(A)$.*

Proposition.— *Soit $k \subset K$ deux corps et $A \subset K$. On a*

$$\begin{aligned} k(A) &= \left\{ \frac{P(a_1, \cdots, a_n)}{Q(b_1, \cdots, b_m)} / \ n, m \in \mathbb{N};\ P \in k[X_1, \cdots, X_n], \right. \\ &\quad Q \in k[X_1, \cdots, X_m]; \\ &\quad \left. (a_1, \cdots, a_n) \in A^n, (b_1, \cdots, b_m) \in A^m;\ Q(b_1, \cdots, b_m) \neq 0 \right\} \\ &= \left\{ \frac{\sum_{i \in I} \lambda_i \prod_{k_i \in J_i} a_{k_i}}{\sum_{i' \in I'} \lambda_{i'} \prod_{k_{i'} \in J_{i'}} b_{k_{i'}}} / \ I, I', J_i, J_{i'} \ finis, \right. \\ &\quad \left. a_{k_i}, b_{k_{i'}} \in A;\ \lambda_i, \lambda_{i'} \in k \right\} \end{aligned}$$

Preuve:

Définition.— *Soit K un corps et k_0 et k_1 deux sous-corps de K. On appelle compositum dans K des corps k_0 et k_1 le corps $k_0 \bullet k_1 = k_0(k_1) = k_1(k_0)$. Par extension, si $(k_i)_i$ désigne une famille de sous-corps de K, on appelle compositum des corps k_i dans le corps K, le plus petit sous-corps de K contenant k_i pour tout i. On note ce corps $\bullet_i k_i$.*

Soit A un anneau unitaire. L'application $f : \mathbb{Z} \to A$ définie par $f(n) = 1 + \cdots + 1$ (n fois) est un morphisme d'anneau. Son noyau est étant un idéal, est donc de la forme $n\mathbb{Z}$ avec $n \in \mathbb{N}$ (si $n = 0$, f est injectif).

Définition.— *Avec les notation précédente, on appelle caractéristique de A l'entier n.*

Lemme.— *La caractéristique d'un corps est soit nul, soit égale à un nombre premier.*

Définition.— *Un corps est dit premier s'il ne possède pas d'autre sous-corps que lui-même. Soit K un corps, on appelle sous-corps premier de K l'intersection de tous ces sous-corps. Le sous-corps premier d'un corps est donc un corps premier.*

Proposition.— *Un corps premiers est isomorphe soit à $\mathbb{Q}$ soit à un $\mathbb{Z}/p\mathbb{Z}$ pour p premier. Si K est un corps et F sont sous-corps premier. On a:*

$$car(K) = 0 \iff F \simeq \mathbb{Q} \text{ et } car(K) = p \iff F \simeq \mathbb{F}_p$$

1.1.2 Polynômes

Proposition.— *Soit K un corps commutatif, l'anneau $K[X]$ est euclidien (donc en particulier principal).*

Corollaire.— *Soit K un corps commutatif et k un sous-corps de K. Soit $P, Q \in k[X] \subset K[X]$. Le p.g.c.d de P et Q est le même dans $k[X]$ et dans $K[X]$.*

Définition.— *Soit K un corps commutatif et $P \in K[X]$. On dit qu'un élément $\alpha \in K$ est racine de P si $P(\alpha) = 0$.*

Proposition.— *Soit K un corps commutatif et $P \in K[X]$ un polynôme de degré $n \geq 1$. Si $\alpha \in K$ est racine de P, alors il existe $Q \in K[X]$ de degré $n-1$ tel que $P(X) = (X - \alpha)Q(X)$.*

En conséquence de quoi, un polynôme $P \in K[X]$ de degré $n \geq 1$, possède au maximum n racines.

Preuve: Posons $P(X) = \sum_{k=0}^{n} a_k X^k$ et prenons $\alpha \in K$, alors on a

$$P(X) - P(\alpha) = \sum_{k=0}^{n} a_k (X^k - \alpha^k)$$

or, pour tout $k = 1, \cdots, n$, on a

$$X^k - \alpha^k = (X - \alpha) \sum_{i=0}^{k-1} X^i \alpha^{k-i}$$

On a donc

$$P(X) - P(\alpha) = (X - \alpha)Q(X)$$

avec $Q(X) = \sum_{k=1}^{n} \sum_{i=0}^{k-1} a_k X^i \alpha^{k-i}$ qui est visiblement un polynôme de degré $n-1$.

Si α est racine de P, la proposition en découle alors.

Corollaire.— *Si $P \in K[X]$ un polynôme et $\alpha \in K$ une racine de P, il existe un polynôme $Q \in K[X]$ et un entier $d > 0$ tel que $P(X) = (X - \alpha)^d Q(X)$ et $Q(\alpha) \neq 0$. On dit alors que α est racine de P d'ordre d.*

Preuve: S'obtient par récurrence finie.

On dit qu'un polynôme $P \in K[X]$ est totalement décomposé si ses seuls facteurs irréductibles sont de degré 1, ce qui revient à dire que la somme des ordres de ses racines est égale à son degré.

Lemme.— *Soit K un corps commutatif, les propositions suivantes sont équivalentes :*

i) Tout polynôme $P \in K[X]$ de degré ≥ 1 admet une racine,

ii) tout polynôme $P \in K[X]$ est totalement décomposé.

Preuve: S'obtient par récurrence finie.

Définition.— *On dit qu'un corps commutatif K est algébriquement clos, s'il satisfait au propriétés du lemme précédent.*

1.2 Extensions

1.2.1 Généralités

Définition.— *Soit k un corps. On appelle extension du corps k, toute paire (K, φ) où K est un corps et $\varphi : k \to K$ un morphisme de corps.*

Si K est un corps k un sous-corps de K, alors l'injection canonique de k dans K définie une extension du corps k. Réciproquement, si K est une extension d'un corps k (par un morphisme φ), alors $\varphi(k)$ est un sous-corps de K isomorphe à k. On identifie alors souvent k et $\varphi(k)$. L'extension se note alors K/k.

Définition.— *Soit K_1/k et K_2/k deux extensions d'un même corps (pour fixé les idées notons $\varphi_1 : k \to K_1$ et $\varphi_1 : k \to K_2$ les morphismes associés). On appelle k-isomorphisme (ou k-plongement) de K_1 vers K_2 tout morphisme de corps $\psi : K_1 \to K_2$ tel que pour tout $x \in k$, on ait $\psi \circ \varphi_1(x) = \varphi_2(x)$. On note $Isom_k(K_1, K_2)$ l'ensemble des k-isomorphisme de K_1 vers K_2.*

Définition.— *Soit K/k une extension et $\varphi : k \to K$ le morphisme associé. On appelle extension intermédiaire de K/k tout sous-corps K_0 de K contenant $\varphi(k)$. K_0/k est alors une extension.*

Proposition.— *Soit K un corps de caractéristique p premier (resp. 0). On a l'extension $K/\mathbb{F}_p$ (resp. $K/\mathbb{Q}$).*

Preuve:

Si K/k désigne une extension de corps, le corps K a naturellement une structure de k-espace vectoriel. On peut donc parler de la dimension de K en tant que k-e.v.

Définition.— *Soit K/k une extension de corps. On appelle degré de l'extension K/k la dimension $dim_k(K)$. On note ce nombre (éventuellement égal à $+\infty$) $[K : k]$. Si $[K : k] < +\infty$, on dit que K/k est finie.*

Si M/L et L/K sont deux extensions, alors M/K est une extension. On a alors :

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

Preuve: Si l'une des deux extensions est infinie le résultat est clair. Supposons $[L : K] = n$ et $[M : L] = m$ et notons $(a_1, \cdots, a_n)$ une K-base de L et $(b_1, \cdots, b_m)$ une L-base de M. Soit $x \in M$, il existe donc $\beta_1, \cdots, \beta_m$ des éléments de L tels que

$$x = \beta_1 b_1 + \cdots + \beta_m b_m$$

Maintenant, pour tout $i = 1, \cdots m$, il existe des éléments $\alpha_{i1}, \cdots, \alpha_{in}$ de K tels que

$$\beta_i = \alpha_{i1} a_1 + \cdots + \alpha_{in} a_n$$

et par suite

$$x = \sum_{i,j} \alpha_{ij} b_i a_j$$

donc la famille $(b_i a_j)_{ij}$ est une famille K-génératrice de M. Montrons qu'elle est K-libre. Supposons donné une famille (λ_{ij}) d'éléments de K tels que

$$\sum_{i,j} \lambda_{ij} b_i a_j = 0$$

En posant

$$\omega_i = \lambda_{i1} a_1 + \cdots + \lambda_{in} a_n \in L$$

on a $\omega_1 b_1 + \cdots + \omega_m b_m = 0$ et comme la famille $(b_1, \cdots, b_m)$ est une L-base de M, on en déduit que $\omega_i = 0$ pour tout i, c'est-à-dire

$$\lambda_{i1} a_1 + \cdots + \lambda_{in} a_n = 0$$

mais comme $(a_1, \cdots, a_n)$ est une K-base de L, on en déduit que $\lambda_{ij} = 0$ pour tout i et tout j.

Corollaire.— *Soit K/k une extension et K_0 une extension intermédiaire. Alors $[K : k]$ est divisible par $[K : K_0]$ et $[K_0 : k]$. En particulier, si $[K : k] = p$ premier, alors les seuls sous-extensions de K/k sont K et k.*

Définition.— *Soit K/k une extension et P une partie de K. L'ensemble des extensions intermédiaires de K/k qui contiennent P admet, au sens de l'inclusion, un plus petit élément (l'intersection). On la note $k(P)$ et on l'appelle la sous-extension de K/k engendré par P. Lorsque $P = \{a_1, \cdots, a_n\}$, on note plus volontier $k(\{a_1, \cdots, a_n\}) = k(a_1, \cdots, a_n)$.*

Définition.— *Une extension K/k est dite de type fini s'il existe une partie $P \subset K$ finie telle que $K = k(P)$. On dit que K/k est monogène s'il existe $\alpha \in K$ tel que $K = k(\alpha)$. On dit alors que α est un élément primitif de l'extension K/k.*

Remarque : Si K/k est une extension de degré premier, alors K/k est monogène. De manière plus précise, tout élément $\alpha \in K - k$ est primitif.

1.2.2 Extensions algébriques

Définition.— *Soit K/k une extension et $\alpha \in K$. On dit que α est algébrique sur k, s'il existe un polynôme $P \in k[X]$ tel que $P(\alpha) = 0$. Dans le cas contraire, on dit que α est transcendant sur k.*

Si tout élément de K est algébrique sur k, on dit que K/k est une extension algébrique, dans le cas contraire, on dit que K/k est transcendante.

Soit K/k une extension et $a \in K$. On considère l'application $\Phi_a : k[X] \to K$ définie par :

$$\Phi_a(P(X)) = P(a)$$

L'application Φ_a est un morphisme de k-algèbre. On note $k[a]$ son image. $k[a]$ est donc le sous-k-espace vectoriel de K engendré par la famille $(a^n)_{n\in\mathbb{N}}$. On remarque que le sous-corps $k(a)$ de K est constitué des éléments de la forme $P(a)/Q(a)$ où $P, Q \in k[X]$ et $Q(a) \neq 0$, c'est-à-dire que $k(a) = Frac(k[a])$.

Proposition.— *Soit K/k une extension et $\alpha \in K$. Les propositions suivantes sont équivalentes :*

i) α est algébrique,

ii) $dim_k\ k[\alpha] < +\infty$,

iii) Φ_α n'est pas injectif.

Preuve: *i)* $\Rightarrow$ *ii)* Soit $P(X) = \sum_{i=0}^{d} a_i X^i \neq 0$ un polynôme annulateur de α. Montrons par récurrence que pour tout $n \geq d$, α^n est combinaison linéaire sur k de $1, \alpha, \cdots, \alpha^{d-1}$.
Pour $n = d$, on a $\alpha^d = -\sum_{i=0}^{d-1} a_i \alpha^i$
Supposons la propriété vérifiée au rang $n \geq d$. On a donc

$$\alpha^n = \sum_{i=0}^{d-1} \lambda_i \alpha^i$$

avec $\lambda_i \in k$. On a alors

$$\begin{array}{rcl} \alpha^{n+1} & = & \alpha.\alpha^n \\ & = & \sum_{i=0}^{d-1} \lambda_i \alpha^{i+1} \\ & = & \sum_{i=1}^{d-1} \lambda_{i-1} \alpha^i + \lambda_{d-1} \alpha^d \\ & = & \sum_{i=1}^{d-1} \lambda_{i-1} \alpha^i - \sum_{i=0}^{d-1} \lambda_{d-1} a_i \alpha^i \end{array}$$

La proposition est donc vérifiée et par suite $(1, \cdots, \alpha^{d-1})$ est une famille génératrice de $k[\alpha]$ qui est donc de dimension $\leq d$ sur k.

ii) $\Rightarrow$ *iii)* La famille $(\alpha^i)_i$ est k-liée puisqu'infinie. Il existe donc un entier n et des éléments $a_0, \cdots, a_n$ de k tel que

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$$

c'est à dire $P \in Ker(\Phi_\alpha)$ avec

$$P(X) = \sum_{i=0}^{n} a_i X^i \neq 0$$

donc Φ_α n'est pas injectif.

iii) $\Rightarrow$ *i)* Soit $P \in Ker(\Phi_\alpha)$ non nul, alors $P(\alpha) = 0$ et par suite α est algébrique.

Soit $\alpha \in K$ algébrique. Le noyau de Φ_α (c'est-à-dire l'ensemble des polynômes qui admettent α pour racine) est donc un idéal non nul de $k[X]$. Comme $k[X]$ est principal, il existe un et un seul polynôme normalisé $Min_k(\alpha)(X) \in k[X]$, tel que $Ker\ \Phi_\alpha =< Min_k(\alpha)(X) >$. On appelle ce polynôme, le polynôme minimal de α. On a alors :

Proposition.— *Soit K/k une extension, $\alpha \in K$ un élément algébrique et P un polynôme de $k[X]$. Les propositions suivantes sont équivalentes :*

i) $P = Min_k(\alpha)$,

ii) *P est irréductible, unitaire et $P(\alpha) = 0$.*

Preuve: *i)* $\Rightarrow$ *ii)* Il faut montrer que P est irréductible. Si ce n'est pas le cas, alors $P = P_1P_2$ avec $d^\circ P_i > 0$ et comme $P(\alpha) = 0$ on a $P_1(\alpha) = 0$ ou $P_2(\alpha)$, mais comme $d^\circ P_i < d^\circ P$, ceci contredit la minimalité de P.

ii) $\Rightarrow$ *i)* On a $P \in Ker(\Phi_\alpha)$ et comme ce dernier est engendré par $Min_k(\alpha)$ on en déduit que $Min_k(\alpha)|P$, mais comme P est irréductible et que $Min_k(\alpha)$ n'est pas constant, on en déduit que $P|Min_k(\alpha)$. Ces deux polynômes étant unitaire, on a bien $P = Min_k(\alpha)$.

Corollaire.— *Soit K/k une extension et $\alpha \in K$. Les propositions suivantes sont équivalentes :*

i) α *est algébrique,*

ii) $[k(\alpha) : k] < +\infty$*,*

iii) $k(\alpha) = k[\alpha]$*.*

Preuve: $i \Rightarrow iii$ On a $k[\alpha] \subset k(\alpha)$. Le corps $k(\alpha)$ est le sous-corps de K constitué des éléments $P(\alpha)/Q(\alpha)$ avec $P, Q \in k[X]$ et $Q(\alpha) \neq 0$. Soit M le polynôme minimal de α. Les polynômes M et Q sont premiers entre eux, donc, d'après Bezout, il existe $U, V \in k[X]$ tel que $UM + VQ = 1$ et par suite $1/Q(\alpha) = V(\alpha) \in k[\alpha]$ et donc $P(\alpha)/Q(\alpha) \in k[alpha]$ c'est-à-dire $k(\alpha) \subset k[\alpha]$.

$iii \Rightarrow i$ Il existe un entier n et des éléments non tous nul $a_0, \cdots, a_n$ de k tel que $\alpha^{-1} = a_0 + \cdots + a_n\alpha^n$. On a donc

$$a_n\alpha^{n+1} + \cdots + a_0\alpha - 1 = 0$$

ce qui prouve que α est algébrique sur k.

$iii \Rightarrow ii$ On sait que $(i) \Leftrightarrow iii))$ α est algébrique, donc que $dim_k k[\alpha] < +\infty$. On a donc $[k(\alpha) : k] < +\infty$.

$ii \Rightarrow i$ Comme $k[\alpha]$ est un sous-k-espace vectoriel de $k(\alpha)$ on a donc $dim_k k[\alpha] < +\infty$ et par suite, α est algébrique sur k.

Proposition.— *Soit* K/k *une extension et* $\alpha \in K$ *un élément algébrique. On a* $[k(\alpha) : k] = d^\circ Min_k(\alpha) = n$ *et la famille* $(1, \alpha, \cdots, \alpha^{n-1})$ *est une* k*-base de* $k(\alpha)$*.*

Preuve: On sait que $k(\alpha) = k[\alpha]$. La même preuve que pour la proposition ???, montre que la famille $(1, \alpha, \cdots, \alpha^{n-1})$ est k-génératrice de $k[\alpha]$. Supposons qu'il existe une équation de dépendance linéaire non trivial pour cette famille

$$\lambda_0 + \cdots + \lambda_{n-1}\alpha^{n-1} = 0$$

Le polynôme $P(X) = \sum_{i=0}^{n-1} \lambda_i X^i \neq 0$ est alors anulateur de α ce qui contredit la minimalité de $Min_k(\alpha)$.

Définition.— *Soit* K/k *une extension et* $\alpha \in K$ *un élément algébrique. On appelle degré de* α*, le degré de son polynôme minimal.*

Si M/K désigne une extension et $M/L/K$ une extension intermédiaire, alors tout élément de M algébrique sur K est algébrique sur L et son degré sur L est plus petit que son degré sur K.

Proposition.— *Toute extension finie est algébrique. De manière plus précise, si* L/K *est une extension de degré* n*, alors tout élément de* K *a un degré* $\leq n$ *sur* k*.*

Preuve: Soit $\alpha \in K$. La famille $1, \cdots, \alpha^n$ comptant $n + 1$ éléments est liée dans K, donc il existe des éléments non tous nuls $a_0, \cdots, a_n \in k$ tel que

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$$

Le polynôme $P(X) = a_0 + \cdots + a_nX^n \in k[X]$ est donc annulateur de α et par suite $Min_k(\alpha)$ divise P donc le degré de α est plus petit que n.

Lemme.— *Soit* L/K *une extension et* $A \subset L$*. On a alors* $K(A) = \bigcup_{J \subset A \ finie} K(J)$.

Preuve: Il est clair que $\bigcup_{J\subset A \ finie} K(J) \subset K(A)$. Maintenant, il est clair aussi que $A \subset \bigcup_{J\subset A \ finie} K(J)$. Pour montrer notre résultat, il suffit de prouver que $\bigcup_{J\subset A \ finie} K(J)$ est un corps. Soit $x, y \in \bigcup_{J\subset A \ finie} K(J)$ $(y \neq 0)$, il existe donc $J_x \subset A$ et $J_y \subset A$ finies telles que $x \in K(J_x)$ et $y \in K(J_y)$. Alors $J_x \cup J_y$ est une partie finie de A et comme $x - y$ et xy^{-1} sont dans $K(J_x \cup J_y) \subset \bigcup_{J\subset A \ finie} K(J)$ on en déduit bien que $\bigcup_{J\subset A \ finie} K(J)$ est un corps.

Corollaire.— *Soit L/K une extension et $A \subset L$. Les propriétés suivantes sont équivalentes :*

i) $K(A)/K$ est algébrique,

ii) $\forall \alpha \in A$, α est algébrique sur K.

Preuve: *i)* $\Rightarrow$ *ii)* Evident.

ii) $\Rightarrow$ *i)* Soit $J \subset A$ une partie finie. Posons $J = \{\alpha_1, \cdots, \alpha_n\}$. On a $[K(\alpha_1) : K] < +\infty$. Comme α_2 est algébrique sur K, il l'est sur $K(\alpha_1)$ et donc $[K(\alpha_1, \alpha_2) : K(\alpha_1)] < +\infty$, comme $[K(\alpha_1, \alpha_2) : K] = [K(\alpha_1, \alpha_2) : K(\alpha_1)].[K(\alpha_1) : K]$ on en déduit que $[K(\alpha_1, \alpha_2) : K] < +\infty$. Par récurrence finie, on en déduit que $K(J)/K$ est une extension finie et par suite algébrique. Pour finir, il suffit de remarquer que $K(A) = \bigcup_{J\subset A \ finie} K(J)$.

Corollaire.— *Soit $L = K(\alpha_1, \cdots, \alpha_n)$ une extension de type finie d'un corps K. Les propositions suivantes sont équivalentes :*

i) L/K est algébrique,

ii) $[L : K] < +\infty$,

iii) α_i est algébrique pour tout $i = 1, \cdots, n$.

Preuve: *i)* $\Rightarrow$ *ii)* Par transitivité des degré, on a

$$[L : K] = [L : K(\alpha_1, \cdots, \alpha_{n-1})].\cdots.[K(\alpha_1) : K]$$

comme toutes ces dimensions sont finies, on en déduit bien le résultat.

ii) $\Rightarrow$ *iii)* Immédiat.

iii) $\Rightarrow$ *i)* C'est une conséquence de la proposition précédente.

Corollaire.— *Soient M/L et L/K deux extensions. Les propositions suivantes sont équivalentes :*

i) M/K est algébrique,

ii) M/L et L/K sont algébriques.

Preuve: *i)* $\Rightarrow$ *ii)* Evident.

ii) $\Rightarrow$ *i)* Soit $\alpha \in M$ et $P(X) = \sum_{i=0}^{n} a_i X^i = Min_L(\alpha)$. Les éléments a_i sont algébriques sur K, donc le corps $K^{'} = K(a_0, \cdots, a_n)$ est de dimension fini sur K. Le polynôme $P \in K^{'}[X]$ est annulateur de α, donc α est algébrique sur $K^{'}$. Donc $K^{'}(\alpha)/K^{'}$ est fini et par transitivité des degré $K^{'}(\alpha)/K$ est fini et comme $K(\alpha) \subset K^{'}(\alpha)$ on en déduit que α est algébrique sur K.

1.2.3 Clôture algébrique

Proposition.— *Soit K/k une extension. L'ensemble A des éléments de K algébriques sur k forme un corps, extension algébrique de k. On l'appelle clôture algébrique de k dans K. Si K est algébriquement clos alors A l'est aussi.*

Preuve: On a $A \subset K$, pour montrer que A est un sous-corps de K, il suffit de prouver que si $x, y \in A$ avec $y \neq 0$ alors $x - y \in A$ et $xy^{-1} \in A$. Maintenant, par hypothèse x et y sont algébrique sur k, donc $[k(x, y) : k] < +\infty$ donc $k(x, y)/k$ est une extension algébrique et comme $x - y \in k(x, y)$ et $xy^{-1} \in k(x, y)$ on en déduit bien que $x - y \in A$ et $xy^{-1} \in A$. Le fait que A/k soit une extension algébrique est immédiat.

Si K est supposé algébriquement clos, montrons que A l'est aussi. Soit $P(X) = \sum_{i=0}^{n} a_i X^i \in A[X]$ un polynôme non constant. Posons $K_0 = k(a_0, \cdots, a_n)$. Comme les a_i sont algébriques sur k, on en déduit que $[K_0 : k] < +\infty$. Soit maintenant $\alpha \in K$ tel que $P(\alpha) = 0$. L'élément α est donc algébrique sur K_0 et par suite $[K_0(\alpha) : K_0] < +\infty$ et donc $[K_0(\alpha) : k] < +\infty$ et donc α est algébrique sur k, donc $\alpha \in A$.

Proposition.— *Soit K/k une extension telle que K soit algébriquement clos. Les propositions suivantes sont équivalentes :*

i) K/k est algébrique,

ii) K/k ne possède pas d'extension intermédiaire stricte qui soit algébriquement close.

Preuve: *i)* $\Rightarrow$ *ii)* Soit K_0 un sous-corps strict de K. Il existe donc $\alpha \in K$ tel que $\alpha \notin K_0$. Comme K/K_0 est une extension algébrique, α possède un polynôme minimal sur K_0, $P \in K_0[X]$. Le polynôme P est de degré > 1 sinon, α serait dans K_0. Le polynôme P étant irréductible n'est pas totalement décomposé sur K_0 ce qui montre bien que ce corps n'est pas algébriquement clos.

ii) $\Rightarrow$ *i)* Supposons K/k transcendante. Le corps A obtenu dans la proposition précédente est une extension intermédiaire de K algébriquement close et différente de K car A/k est une extension algébrique.

Définition.— *Soit K/k une extension. On dit que K est une clôture algébrique de k si K vérifie les deux propriétés équivalentes de la proposition précédente.*

Lemme.— *Soit K un corps et $P \in K[X]$ un polynôme irréductible de degré ≤ 1. Le corps $K[X]/(P)$ est une extension finie de K dans laquelle P admet une racine.*

Preuve: Puisque P est irréductible, l'anneau $K[X]/(P)$ est bien un corps et l'injection canonique $K \to K[X]$ se factorisant, on en déduit que $K[X]/(P)$ est une extension de K. Posons $n = d^\circ P$ et $\alpha = \overline{X}$. Il est clair que $1, \alpha, \cdots, \alpha^{n-1}$ forment une base de $K[X]/(P)$ vu comme K-espace vectoriel. Par ailleurs, il est aussi clair que $P(\alpha) = 0$.

Proposition.— *Soit K/k une extension. Les propositions suivantes sont équivalentes :*

i) K est une clôture algébrique de k,

ii) K/k est une extension algébrique maximale,

iii) K/k est algébrique et tout polynôme non constant de $k[X]$ admet toutes ses racines dans K.

Preuve: *i)* $\Rightarrow$ *ii)* K/k est algébrique. Si K/k n'est pas maximale, alors il existe une extension K_0/K stricte et par suite tout élément $\alpha \in K_0 - K$ fournit un polynôme $(Min_K(\alpha))$ de $K[X]$ de degré ≥ 2 n'ayant pas de racine dans K, donc K n'est pas algébriquement clos.

ii) $\Rightarrow$ *iii)* Soit $P \in k[X]$ ne possédant pas toutes ses racines sur K. P vu dans $K[X]$ possède donc un facteur irréductible Q de degré ≥ 2. Le corps $K_Q = K[X]/(Q)$ est une extension algébrique stricte de K, mais alors K_Q/k est algébrique ce qui contredit la maximalité du K/k.

iii) $\Rightarrow$ *i)* Il faut montrer que K est algébriquement clos. Si ce n'est pas le cas, alors il existe $P \in K[X]$ sans racine dans K. Soit Q un facteur irréductible de P de degré ≤ 2. Le corps de $K_Q = K[X]/(Q)$ est une extension stricte de K. Soit $\alpha \in K_Q - K$. Comme K_Q/K et K/k sont algébriques, α est algébrique sur k. Le polynôme minimal $Min_k(\alpha)$ ne peut pas être totalement décomposé sur K, sinon on aurait $\alpha \in K$, d'où l'absurdité.

Si K/k est une extension avec K algébriquement clos, la clôture algébrique A de k dans K est donc une clôture algébrique de k. Ainsi tout corps contenu dans un corps algébriquement clos possède une clôture algébrique. En fait, de manière générale, on a :

Théorème.— (Steiniz) *Tout corps k admet une clôture algébrique.*

Preuve: (D'après Lang) On considère l'anneau $D = K[X_f]$ des polynômes à coefficients dans K en les variables X_f où f parcourt l'ensemble des polynômes de $K[X]$ de degré ≤ 1. Soit I l'idéal de D engendré par les polynômes $f(X_f)$ pour f parcourant $K[X]$.

• L'idéal I est strict. En effet, $1 \notin I$, sinon il existerait des indices $f_1, \cdots, f_n$ et des polynômes $g_1, \cdots, g_n \in D$ tels que

$$\sum_{i=1}^{n} g_i f_i(X_{f_i}) = 1$$

Maintenant, il existe une extension L/K telle que chaque polynôme $f_i(X_{f_i})$ admette une racine. En évaluant l'égalité en un uplet contenant ces racines, on a alors $0 = 1$ ce qui est absurde.

• Le théorème de Krull assure qu'il existe un idéal maximal $\overline{I}$ contenant I. Considérons le corps $E = D/\overline{I}$. C'est une extension de K. En effet, la surjection canonique $s : D \to E$ induit un morphisme de corps de K sur E. Notons $x_f = s(X_f)$ et considérons le corps $E_1 = K(x_f)_f$. Chaque x_f est algébrique sur K, donc E_1/K est algébrique. Par ailleurs, tout polynôme $f \in K[X]$ admet une racine dans E_1 (à savoir x_f).

On construit de la même facon une extension algébrique E_2/E_1 telle que tous polynôme $f \in E_1[X]$ admette une racine dans E_2 et, par réccurence, on construit une suite d'extension $(E_n)_n$ telle que pour tout n, E_{n+1}/E_n est algébrique et tout polynôme $f \in E_n$ admet une racine dans E_{n+1}.

• Considérons alors le corps $L = \bigcup_n E_n$. L/K est algébrique et tout polynôme $f \in L[X]$ appartient à $E_n[X]$ pour un certain n, donc admet une racine dans $E_{n+1} \subset L$. L est bien algébriquement clos.

Proposition.— *Soit L/K et M/K deux extension de corps et $\alpha \in L$ et $\beta \in M$ deux élements algébriques sur K. Les propositions suivantes sont équivalentes :*

i) $Min_K(\alpha) = Min_K(\beta)$,

ii) il existe un (unique) K*-isomorphisme* $\sigma \in Isom_k(K(\alpha), K(\beta))$ *tel que* $\sigma(\alpha) = \beta$.

Preuve: *i)* $\Rightarrow$ *ii)* Commencons par montrer l'unicité. Soit σ_1 et σ_2 deux K-isomorphismes de $Isom_k(K(\alpha), K(\beta))$ tels que $\sigma_i(\alpha) = \beta$ pour $i = 1, 2$. On sait que $1, \alpha, \cdots, \alpha^{n-1}$ est une base du K-espace vectoriel $K(\alpha)$. Comme σ_1 et σ_2 sont des morphismes de corps et que $\sigma_1(\alpha) = \sigma_2(\alpha)$, on en déduit que $\sigma_1(\alpha^d) = \sigma_2(\alpha^d)$ pour tout $d = 0, \cdots, n-1$ et comme σ_1 et σ_2 sont en particulier des applications K-linéaires, on en déduit bien que $\sigma_1 = \sigma_2$.

Montrons maintenant l'existence de σ. Considérons le polynôme

$$P = \sum_{i=0}^{n} a_i X^i = Min_K(\alpha) = Min_K(\beta)$$

On sait que $1, \alpha, \cdots, \alpha^{n-1}$ et $1, \beta, \cdots, \beta^{n-1}$ forment des bases de $K(\alpha)$ et de $K(\beta)$. Définissons σ de la manière suivante : si $x \in K(\alpha)$ alors il existe un unique n-uplet $\lambda_0, \cdots, \lambda_{n-1} \in K$ tel que $x = \lambda_0 + \cdots + \lambda_{n-1}\alpha^{n-1}$. On pose alors

$$\sigma(x) = \lambda_0 + \cdots + \lambda_{n-1}\beta^{n-1}$$

On a bien $\sigma(\alpha) = \beta$ et σ est une application K-linéaire. Reste à vérifier que σ est bien un morphisme de corps. Puisque σ est K-linéaire, il suffit pour cela de montrer que l'image d'un produit de deux éléments de la K-base $1, \alpha, \cdots, \alpha^{n-1}$ est le produit des images de ces éléments, c'est-à-dire finalement que pour tout entier d, $\sigma(\alpha^d) = \beta^d$. Cette propriété est visiblement vraie pour $d = 0, \cdots, n-1$. Montrons la pour $d \geq n$.
Pour $d = n$, on a $\alpha^n = \alpha^n - P(\alpha) = -\sum_{i=0}^{n-1} a_i\alpha^i$ et donc

$$\begin{array}{rcl} \sigma(\alpha^n) & = & -\sum_{i=0}^{n-1} a_i\sigma(\alpha^i) \\ & = & -\sum_{i=0}^{n-1} a_i\beta^i \\ & = & \beta^n - P(\beta) \\ & = & \beta^n \end{array}$$

Supposons la propriété vraie au rang $d \geq n$. Alors $\sigma(\alpha^d) = \beta^d$. Soit $\lambda_0, \cdots, \lambda_{n-1} \in K$ tels que

$$\alpha^d = \lambda_0 + \cdots + \lambda_{n-1}\alpha^{n-1}$$

on a alors

$$\beta^d = \lambda_0 + \cdots + \lambda_{n-1}\beta^{n-1}$$

On a donc

$$\begin{array}{rcl} \alpha^{d+1} & = & \lambda_0\alpha + \cdots + \lambda_{n-1}\alpha^n \\ & = & \lambda_0\alpha + \cdots - \lambda_{n-1}\sum_{i=0}^{n-1} a_i\alpha^i \end{array}$$

et ainsi,

$$\begin{array}{rcl} \sigma(\alpha^{d+1}) & = & \lambda_0\beta + \cdots + \lambda_{n-1}\sigma(\alpha^n) \\ & = & \lambda_0\beta + \cdots - \lambda_{n-1}\sum_{i=0}^{n-1} a_i\beta^i \\ & = & \lambda_0\beta + \cdots + \lambda_{n-1}\beta^n \\ & = & \beta^{d+1} \end{array}$$

ce qui achève la preuve.

ii) $\Rightarrow$ *i)* Soit $P_1 = Min_K(\alpha)$ et $P_2 = Min_K(\beta)$. Comme $P_1(\alpha) = 0$ et que $\sigma(P_1(\alpha)) = P_1(\sigma(\alpha)) = P_1(\beta) = 0$, on en déduit que P_1 est un polynôme annulateur

de β, donc $P_2|P_1$. Maintenant, il est clair que σ est bijectif puisqu'il envoie la base $1, \cdots, \alpha^{n-1}$ sur la base $1, \cdots, \beta^{n-1}$. En appliquant le même raisonnement que précédement à σ^{-1}, on en déduit que $P_1|P_2$ et comme ces deux polynômes sont unitaires, on trouve finalement $P_1 = P_2$.

Définition.— *Deux éléments algébriques d'une extension K/k sont dit conjugués, s'ils ont le même polynôme minimal.*

Proposition.— *Soit L/K une extension algébrique et σ un élément de $Isom_K(L, L)$. Si $\alpha \in L$, on note $\mathcal{C}_\alpha$ l'ensemble des conjugués de α sur K dans L. La restriction de l'application σ à $\mathcal{C}_\alpha$ est une bijection de $\mathcal{C}_\alpha$ dans lui-même. En particulier, σ est un automorphisme de corps. On note alors $Isom_K(L, L) = Aut_K(L)$. Cet ensemble est un groupe pour la composition.*

Preuve: L'ensemble $\mathcal{C}_\alpha$ est fini puisque $P = Min_K(\alpha)$ ne possède qu'un nombre fini de racines dans L. Soit $\beta \in \mathcal{C}_\alpha$. On alors $0 = \sigma(P(\beta)) = P(\sigma(\beta))$ donc $\sigma(\beta) \in \mathcal{C}_\alpha$ ce qui justifie bien que l'image de $\mathcal{C}_\alpha$ par σ est incluse dans $\mathcal{C}_\alpha$. Maintenant σ est injective et comme $\mathcal{C}_\alpha$ est fini on en déduit bien que σ restreinte à $\mathcal{C}_\alpha$ est bijective.

On sait que σ est injective, montrons qu'elle est surjecive. Soit $\alpha \in L$. On a $\alpha \in \mathcal{C}_\alpha$, et comme σ est une bijection sur $\mathcal{C}_\alpha$, il existe $\beta \in \mathcal{C}_\alpha \subset L$ tel que $\sigma(\beta) = \alpha$, ce qui prouve bien la surjectivité de σ.

Proposition.— *Soit L/K une extension monogène ($L = K(\alpha)$), M/K une extension quelconque. Pour tout $\sigma \in Isom_K(L, M)$, $\sigma(\alpha)$ est une racine de $Min_K(\alpha)$ et réciproquement, si β est une racine de $Min_K(\alpha)$ dans M, il existe un unique $\sigma \in Isom_K(L, M)$ tel que $\sigma(\alpha) = \beta$. Il y a donc une correspondance bijective entre les éléments de $Isom_K(L, M)$ et les racines de $Min_K(\alpha)$ dans L.*

Preuve: Il est clair que si $\sigma \in Isom_K(L, M)$, alors $0 = \sigma(P(\alpha)) = P(\sigma(\alpha))$, donc $\sigma(\alpha)$ est bien une racine de P dans M.

Soit $\beta \in M$ une racine, la proposition ??? montre qu'il existe un unique élément $\sigma \in Isom_k(k(\alpha), k(\beta))$ tel que $\sigma(\alpha) = \beta$, donc il existe bien un élément $\mu \in Isom_k(L, M)$ tel que $\mu(\alpha) = \beta$. Comme $\mu(\alpha) = \beta$, on a $\mu(k(\alpha)) \subset k(\beta)$, on a nécessairement $\mu = \sigma$.

Théorème.— (Steiniz) *Soit k un corps et $\overline{k}$ une clôture algébrique. Soit K/k une extension algébrique et $\sigma \in Isom_k(K, \overline{k})$. Si L/K est une extension algébrique, alors il existe $\widetilde{\sigma} \in Isom_k(L, \overline{k})$ tel que $\widetilde{\sigma}_{|K} = \sigma$.*

Preuve: Examinons pour commencer le cas monogène $L = K(a)$. Soit $P = Min_K(a)$ et soit $\alpha \in overlinek$ une racine du polynôme $\sigma(P) \in \overline{k}[X]$. On vérifie alors, comme dans la prop ???, que l'application $\widetilde{\sigma} : K(a) \to \overline{k}$ donnée par $\widetilde{\sigma}(x) = \sigma(x)$ pour $x \in K$ et $\widetilde{\sigma}(a) = \alpha$ définie bien l'élément $\widetilde{\sigma} \in Isom_k(L, \overline{k})$ recherché.

Pour le cas général, considérons l'ensemble $\mathcal{E}$ des couples $(K_0, \widetilde{\sigma}_{K_0})$ où K_0 est une extension intermédiaire de L/K et $\widetilde{\sigma}_{K_0} \in Isom_k(K_0, \overline{k})$ tel que la restriction de $\widetilde{\sigma}_{K_0}$ à K soit égale à σ. On ordonne $\mathcal{E}$ de la manière suivante, $(K_0, \widetilde{\sigma}_{K_0}) \leq (K_1, \widetilde{\sigma}_{K_1})$ ssi $K_0 \subset K_1$ et la restriction de $\widetilde{\sigma}_{K_1}$ à K_0 vaut $\widetilde{\sigma}_{K_0}$. L'ensemble ordonné $(\mathcal{E}, \leq)$ est alors inductif. En effet, prenons $(K_i, \widetilde{\sigma}_{K_i})_i$ une chaîne dans $\mathcal{E}$ et considérons $M = \bigcup_i K_i$. L'ensemble M est un corps (puisqu'il s'agit d'une chaine) et c'est une extension intermédiaire de L/K. Sur M définissons $\widetilde{\sigma}$ par :

$$\widetilde{\sigma}(x) = \widetilde{\sigma}_{K_i}(x) \text{ si } x \in K_i$$

L'application $\widetilde{\sigma}$ est bien définie puisque $(K_i, \widetilde{\sigma}_{K_i})_i$ est une chaîne, c'est un élément de $Isom_k(M, \overline{k})$ dont la restriction à K est σ. Ainsi le couple $(M, \widetilde{\sigma}) \in \mathcal{E}$ est un majorant de la chaîne $(K_i, \widetilde{\sigma}_{K_i})_i$, c'est-à-dire que $\mathcal{E}$ est inductif. Le lemme de Zorn affirme alors qu'il existe dans $\mathcal{E}$ un élément $(K_0, \widetilde{\sigma}_{K_0})$ maximal. Si $K_0 \neq L$ alors il existe $a \in L - K_0$ et d'après le cas monogène, il existe un élément $\mu \in Isom_k(K_0(a), \overline{k})$ tel que $\mu_{|K_0} = \widetilde{\sigma}_{K_0}$. Mais alors, $\mu_{|K} = \sigma$ et donc $(K_0(a), \mu) \in \mathcal{E}$ et $(K_0, \widetilde{\sigma}_{K_0}) < (K_0(a), \mu)$ ce qui contredit la maximalité de $(K_0(a), \mu)$.

Si K_1 et K_2 sont deux extensions d'un même corps k, on dira que K_1 et K_2 sont k-isomorphes s'il existe un k-isomorphisme bijectif de K_1 sur K_2.

Corollaire.— (Steiniz) *Si K_1 et K_2 sont deux clôtures algébriques d'un même corps k, alors K_1 et K_2 sont k-isomorphes.*

Preuve: D'après ce qui précède, il existe $\sigma_1 \in Isom_k(K_1, K_2)$ et $\sigma_2 \in Isom_k(K_2, K_1)$. Mais alors $\sigma_2 \circ \sigma_1 \in Isom_k(K_1, K_1) = Aut_k(K_1)$ donc σ_2 est surjective et définit donc un k-isomorphisme bijectif de K_2 sur K_1.

Les clôtures algébriques d'un corps K donnée sont donc toutes K-isomorphes. C'est pour ceci que l'on parlera de *la clôture algébrique*, $\overline{K}$, de K pour désigner un choix arbitraire d'une clôture.

Corollaire.— *Soit L/K une extension algébrique. Toute clôture algébrique de K est une clôture algébrique de L et réciproquement.*

Preuve:

1.2.4 Extensions transcendantes

On rappelle que, si K désigne un corps, le corps $K(X)$ est défini comme étant le corps des fractions de l'anneau de polynômes $K[X]$. **Proposition.**— *Soit K/k une extension et $\alpha \in K$. Les propositions suivantes sont équivalentes :*

i) α est transcendant,

ii) $[k(\alpha) : k] = +\infty$,

iii) $dim_k\ k[\alpha] = +\infty$,

iv) $k(\alpha) \neq k[\alpha]$,

v) Φ_α est injectif,

vi) $k(\alpha)$ est k-isomorphe à $k(X)$.

Preuve: L'équivalence des propriétés i) à v) est juste la reformulation du théorème ???.

v) $\Rightarrow$ *vi)* Comme Φ_α est injective et que $k[\alpha]$ est engendré par les α^n on en déduit que Φ_a est un k-isomorphisme de $k[X]$ sur $k[\alpha]$ qui induit donc un k-isomorphisme bijectif de $k(X)$ sur $k(\alpha)$.

vi) $\Rightarrow$ *ii)* Soit φ un k-isomorphisme bijectif de $k(X)$ dans $k(\alpha)$. C'est en particulier un isomorphisme de k-espaces vectoriels, donc $dim_k k(\alpha) = dim_k k(X) = +\infty$.

Exemple de nombres complexes transcendants:

1.2.5 Corps de rupture et corps de décomposition

Définition.— *Soit k un corps et $P \in k[X]$ un polynôme irréductible. On appelle corps de rupture de P toute extension K/k telle que :*

- *K/k algébrique,*
- *P admet une racine dans K,*
- *P n'admet aucune racine dans les extensions intermédiaires strictes de K/k.*

Proposition.— *Soit k un corps et $P \in k[X]$ un polynôme irréductible. On a :*

- *$k[X]/(P)$ est un corps de rupture de P,*
- *une corps K est un corps de rupture de P ssi il existe $\alpha \in K$ tel que $P(\alpha) = 0$ et $K = k(\alpha)$,*
- *deux corps de ruptures de P sont k-isomorphes.*

Preuve: • Puisque P est irréductible, l'anneau $k[X]/(P)$ est bien un corps et l'injection canonique $k \to k[X]$ se factorisant, on en déduit que $k[X]/(P)$ est une extension de k. Posons $n = d^\circ P$ et $\alpha = \overline{X}$. Il est clair que $1, \alpha, \cdots, \alpha^{n-1}$ est une base de $k[X]/(P)$ vu comme k-espace vectoriel. Par ailleurs, il est aussi clair que $P(\alpha) = 0$.

Supposons qu'il existe une sous-extension stricte M de $k[X]/(P)$ admettant une racine β de P. On a $[M : k] < n$ et donc $d^\circ Min_k(\beta) < n$, mais comme P est annulateur de β on a alors que $Min_k(\beta)$ divise P strictement ce qui est absurde puisque P est irréductible et que $Min_k(\beta)$ n'est pas constant.

• Soit K/k une extension et $\alpha \in K$ tel que $P(\alpha) = 0$ et $K = k(\alpha)$. Pour montrer que K est un corps de rupture, il suffit de montrer que P n'a pas de racine dans unze sous-extension stricte. Supposons donnée une telle sous-extension M avec $\beta \in M$ tel que $P(\beta) = 0$. Comme $[M : k] < [K : k] = d^\circ P$, on en déduit que $d^\circ Min_k(\beta) < d^\circ$, ce qui, comme précédement, est absurde.

Réciproquement, soit K un corps de rupture. Il existe donc $\alpha \in K$ tel que $P(\alpha) = 0$. Si $K \neq k(\alpha)$, alors $k(\alpha)$ est une sous-extension stricte de K/k où P possède une racine ce qui est contraire au fait que K est un corps de rupture.

• Soit K/k un corps de rupture de P et $\alpha \in K$ une racine de P. On sait donc que $K = k(\alpha) = k[\alpha]$. Considérons l'application $\varphi : k[X] \to K$ donnée par $\varphi(Q) = Q(\alpha)$. Le morphisme φ est surjectif et son noyau est précisément (P), on en déduit donc que $K = k(\alpha) = k[\alpha] \simeq k[X]/(P)$, le dernier isomorphisme étant visiblement un k-isomorphisme. Donc tout les corps de ruptures sont k-isomorphes à $k[X]/(P)$.

Corollaire.— *Soit k un corps, K/k une extension et $P \in k[X]$ un polynôme irréductible. Dans K, il y a au plus n corps de ruptures où n désigne le nombre de racines de P dans K.*

Preuve: Immédiat.

Définition.— *Soit k un corps et $P \in k[X]$ un polynôme. On appelle corps de décomposition (ou corps des racines) de P toute extension K/k telle que :*

- *K/k algébrique,*
- *P est totalement décomposé dans K,*
- *P n'est totalement décomposé dans aucune extensions intermédiaires strictes de*

K/k.

Proposition.— *Soit k un corps, $\overline{k}$ une clôture algébrique de k et $P \in k[X]$ un polynôme irréductible. Dans $\overline{k}$, P ne possède qu'un seul corps de décomposition, c'est le corps $K = k(\alpha_1, \cdots, \alpha_n)$ où $\alpha_1, \cdots, \alpha_n \in overlinek$ sont tels que $P(X) = a(X - \alpha_1) \cdots (X - \alpha_n)$ dans $\overline{k}[X]$.*

Preuve: Soit K un corps de décomposition de P dans $\overline{k}$. On a donc $k(\alpha_1, \cdots, \alpha_n) \subset K$, comme dans $k(\alpha_1, \cdots, \alpha_n)$, P se décompose totalement, on en déduit bien que $K = k(\alpha_1, \cdots, \alpha_n)$.

Corollaire.— *Soit k un corps et $P \in k[X]$ un polynôme irréductible. Tous les corps de décomposition de P sont k-isomorphes et si K désigne un tel corps alors $[M : k] \leq n!$ avec $n = d^\circ P$.*

Preuve: Soit K_1 et K_2 deux corps de décompositions de P et $\overline{K_1}$ et $\overline{K_2}$ des clôtures algébriques de K_1 et K_2. Puisque K_1/k et K_2/k sont des extensions algébriques, on en déduit que $\overline{K_1}$ et $\overline{K_2}$ sont des clôtures algébriques de k et par le théorème de Steiniz, $\overline{K_1}$ et $\overline{K_2}$ sont k-isomorphes. Soit $\varphi : \overline{K_1} \to \overline{K_2}$, un k-isomorphisme (bijectif). Le corps $\varphi(K_1)$ est un sous-corps de $\overline{K_2}$ où P se décompose totalement, donc $K_2 \subset \varphi(K_1)$. De même, on a $K_1 \subset \varphi^{-1}(K_2)$, mais comme $[K_1 : k] = [\varphi(K_1) : k]$ et $[K_2 : k] = [\varphi^{-1}(K_2) : k]$, donc $K_2 = \varphi(K_1)$ et $K_1 = \varphi^{-1}(K_2)$, ce qui montre bien que K_1 et K_2 sont k-isomorphes.

Soit $K = k(\alpha_1, \cdots, \alpha_n)$ un corps de décomposition de P. On a $[k(\alpha_1) : k] = n$. Le polynôme minimal de α_2 sur $k(\alpha_1)$ est un diviseur de P, c'est forcément un diviseur strict puisque P n'est plus irréductible sur $k(\alpha_1)$. Donc $[k(\alpha_1, \alpha_2) : k(\alpha_1)] \leq n - 1$, et par récurrence, on en déduit que pour tout $i = 1, \cdots, n - 1$, $[k(\alpha_1, \cdots, \alpha_{i+1}) : [k(\alpha_1, \cdots, \alpha_i)] \leq n - i$. Maintenant, comme

$$[k(\alpha_1, \cdots, \alpha_n) : k] = [k(\alpha_1, \cdots, \alpha_n) : k(\alpha_1, \cdots, \alpha_{n-1})]. \cdots . [k(\alpha_1) : k]$$

on trouve bien $[K : k] \leq 2.3. \cdots .n = n!$.

1.3 Corps finis

1.3.1 Théorème de Wedderburn

Pour tout entier $n \in \mathbb{N}^*$, on note $\Phi_n(X) = \prod_{\xi} (X - \xi)$ (ξ parcourt l'ensemble des racines primitives n-ième de l'unité) le n-ième polynôme cyclotomique. On rappelle que $\Phi_n(X)$ est un polynôme irréductible de $\mathbb{Z}[X]$.

Lemme.— *Soit n et d deux entiers. Les propositions suivantes sont équivalentes :*

i) d divise n,

ii) $X^d - 1$ divise $X^n - 1$ dans $\mathbb{Z}[X]$.

et dans cette situation, si $d < n$ alors $\Phi_n(X)$ divise $\dfrac{X^n - 1}{X^d - 1}$ dans $\mathbb{Z}[X]$.

Preuve: Si $n = kd$, alors

$$X^n - 1 = (X^d - 1)(1 + X^d + X^{2d} + \cdots + X^{(k-1)d})$$

Donc $X^d - 1$ divise $X^n - 1$ dans $\mathbb{Z}[X]$.

Réciproquement, si $X^d - 1$ divise $X^n - 1$, en particulier, les racines de $X^d - 1$

dans $\mathbb{C}$ sont des racines de $X^n - 1$. Soit ξ une racine primitive d-ième de l'unité, $\xi^d - 1 = 0$ donc $\xi^n - 1 = 0$ donc $n = kd$.

Soit ξ une racine primitive n-ième de l'unité. Comme $d < n$, $\xi^d - 1 \neq 0$, donc ξ est racine de $\dfrac{X^n - 1}{X^d - 1}$. Ceci étant valable pour toutes les racines primitives n-ièmes de l'unité et comme $\Phi_n(X)$ et $\dfrac{X^n - 1}{X^d - 1}$ sont des polynômes normalisés, $\Phi_n(X)$ divise $\dfrac{X^n - 1}{X^d - 1}$ dans $\mathbb{Z}[X]$.

Lemme.— *Soit p un nombre premier et $k \in \mathbb{N}^*$. Posons $q = p^k$. Si n et d sont deux entiers alors les propositions suivantes sont équivalentes :*

i) d divise n,

ii) $q^d - 1$ divise $q^n - 1$.

Preuve: Si $n = kd$, d'après le lemme précèdant, en évaluant les polynômes en $X = q$, on a $q^d - 1$ divise $q^n - 1$ dans $\mathbb{Z}$.

Réciproquement supposons que $q^d - 1$ divise $q^n - 1$ dans $\mathbb{Z}$. On a donc $q^n \equiv 1[q^d - 1]$. Effectuons la division euclidienne de n par d: on a $n = kd + r$ avec $k \in \mathbb{N}$ et $0 \leq r < d$. Supposons que $r \neq 0$, on a $q^n = q^{kd}.q^r$, mais comme $q^{kd} \equiv 1[q^d - 1]$ on a $q^n = q^{kd}.q^r \equiv q^r[q^d - 1]$ et donc $q^r \equiv 1[q^d - 1]$. Mais $q^d - 1$ ne peut pas diviser $q^r - 1$ car $q^r - 1 < q^d - 1$. Donc $r = 0$ et d divise n.

Théorème.— (Wedderburn) *Tout corps fini est commutatif.*

Preuve: Soit F un corps fini et $Z = Z(F)$ son centre. Le corps F est donc un Z-espace vectoriel et si $q = \sharp Z$ alors $\sharp F = q^n$ avec $n = dim_Z F$.

Sur F^*, on définit la relation d'équivalence $\simeq$ par:

$$\forall (x, x^{'}) \in F^*,\ x \simeq x^{'} \Longleftrightarrow \exists y \in F^* / \ x^{'} = yxy^{-1}$$

Pour $x \in F^*$, on pose $N(x) = \{y \in F / \ yx = xy\}$.

$N(x)$ est un sous-corps de F contenant Z. Donc, on a $\sharp N(x) = q^{\delta(x)}$ avec $\delta(x) = dim_Z N(x)$ (on a $\delta(x) = n$ si et seulement si $x \in Z^*$).

Soit $x \in F^*$. On note $\bar{x}$ la classe d'équivalence de x modulo $\simeq$. Il est clair que l'on a $\bar{x} = \{yxy^{-1} / \ y \in F^*\}$. Sur F^* on introduit la relation d'équivalence $\equiv$ définie par

$$y \equiv y^{'} \text{ ssi } yxy^{-1} = y^{'}xy^{'-1}$$

Il est clair que $\sharp \bar{x} = \sharp (F^* / \equiv)$. Maintenant

$$y \equiv y^{'} \Longleftrightarrow y^{'-1}y \in N(x)^{'*}$$

Par conséquent le cardinal des classes d'équivalences de $\equiv$ vaut exactement $\sharp N(x)^*$, et par suite on a $\sharp \bar{x} = \dfrac{\sharp F^*}{\sharp N(x)^*}$. En particulier, comme $\sharp N(x)^* = q^{\delta(x)} - 1$ et que $\sharp F^* = q^n - 1$, on a $q^{\delta(x)} - 1$ divise $q^n - 1$, ce qui implique d'après le lemme que $\delta(x)$ divise n.

Les classes d'équivalence d'une relation d'équivalence sur un ensemble définissent une partition de cet ensemble. Donc on a:

$$\sharp F^* = \sum_{i=1}^{h} \sharp \bar{x}_i$$

et donc:

$$q^n - 1 = \sum_{i=1}^{h} \frac{q^n - 1}{q^{\delta(x_i)} - 1}$$

Si $x_k \in Z^*$, alors $\bar{x}_k = Z^*$. Alors x_k est le seul des x_i pour lequel $\delta(x_k) = n$. Dans ce cas $\sharp x_k = \sharp Z^* = q - 1$. On en déduit donc que:

$$q^n - 1 = q - 1 + \sum_{i/\ \delta(x_i)<n} \frac{q^n - 1}{q^{\delta(x_i)} - 1}$$

D'après le lemme

$$\Phi_n(q) \text{ divise } q^n - 1 \text{ et } \frac{q^n - 1}{q^{\delta(x_i)} - 1}$$

pour $\delta(x_i) < n$. On déduit que $\Phi_n(q)$ divise $q - 1$.

Si ξ est une racine primitive n-ième de l'unité alors si $n > 2$, $\xi \notin \mathbb{R}$. Posons $\xi = \alpha + i\beta$, avec $(\alpha, \beta) \in \mathbb{R}^2$. On a

$$\begin{array}{rcccl} |q-\xi|^2 & = & (q-\alpha)^2 + \beta^2 & = & q^2 + \alpha^2 + \beta^2 - 2\alpha q \\ & = & q^2 + 1 - 2\alpha q & > & q^2 + 1 - 2q \\ & = & |q-1|^2 & & \end{array}$$

ceci parce que $|\xi_n| = 1 = \alpha^2 + \beta^2$ et que $\alpha < 1$ (sinon ξ est réel). Ainsi $|q - \xi| > |q - 1|$ et par suite $|\Phi_n(q)| > |q - 1|$, donc

$$\frac{|q-1|}{|\Phi_n(q)|} < 1$$

ce qui est absurde car ce nombre est un entier positif non nul.

Si $n = 2$, alors $\xi_2 = -1$ et à nouveau $|q - \xi_2| > |q - 1|$ ce qui est absurde pour les mêmes raisons que précédemment.

On en déduit que $n = 1$ et donc que $F = Z$, c'est à dire que F est commutatif.

1.3.2 Corps finis

Si F désigne un corps fini alors sa caractéristique est un nombre premier p et par suite $\sharp F = p^n$ avec $n = dim_{\mathbb{Z}/p\mathbb{Z}} F$. Réciproquement:

Théorème.— *Pour tout nombre premier p et tout entier $n \in \mathbb{N}$, il existe un unique corps fini (à isomorphisme près) de cardinal $q = p^n$. On note $\mathbb{F}_q$ ce corps.*

Preuve: Montrons tout d'abord qu'un tel corps existe. Notons $\overline{\mathbb{F}}_p$ une clôture algébrique de $\mathbb{Z}/p\mathbb{Z}$ (elle est unique à isomorphes près, d'après le théorème de Steiniz). Le polynôme $P(X) = X^q - X$ a une dérivée égale à

$$P'(X) = qX^{q-1} - 1 = -1$$

(nous sommes en caractéristique p). Sa dérivée étant égale à une constante, P est premier avec sa dérivée. Donc P n'a que des racines simples dans $\overline{\mathbb{F}}_p$. Soit F l'ensemble de ces racines. Il est clair que F est un corps, car: si $(x, y) \in F^2$ alors $(x.y)^q = x^q.y^q = x.y$ donc $x.y \in F$, si $x \neq 0$ alors

$$(x^{-1})^q = (x^q)^{-1} = x^{-1}$$

et donc $x^{-1} \in F$,

$$(-x)^q = -x^q = -x$$

donc $-x \in F$ et enfin

$$(x+y)^q = \sum_{k=0}^{q} C_q^k x^k + y^{q-k} = x^q + y^q = x + y$$

(car C_q^k est divisible par p donc nul dans $\overline{\mathbb{F}}_p$ pour $k = 1, \cdots, q-1$) et donc $(x+y) \in F$.

Comme $\sharp F = q$, F est bien un corps à q éléments. Notons au passage que c'est le corps de décomposition dans $\overline{\mathbb{F}}_p$ du polynôme $X^q - X$.

Prenons maintenant un corps $F^{'}$ de cardinal q. Grâce au théorème de Wedderburn, on sait que $F^{'}$ est commutatif. Il est de caractéristique p, sa clôture algébrique est isomorphe à $\overline{\mathbb{F}}_p$, il est donc isomorphe à un sous-corps de $\overline{\mathbb{F}}_p$. On peut donc le voir directement comme un sous corps de $\overline{\mathbb{F}}_p$ (ceci veut dire qu'une fois choisie $\overline{\mathbb{F}}_p$ une clôture algébrique de $\mathbb{F}_p$, $F^{'}$ est isomorphe, modulo le choix d'un isomorphisme entre $\overline{\mathbb{F}}_p$ et $\overline{F}^{'}$, à un sous-corps de $\overline{\mathbb{F}}_p$).

Maintenant, pour tout $x \in F^{'}$, $x^q = x$. En effet, F étant un corps, F^* est un groupe multiplicatif d'ordre $q-1$. D'après le théorème de Lagrange, si $x \in F^*$, alors $x^{q-1} = 1$ et par suite $x^q = x$. Il est clair que $x = 0$ vérifie aussi cette égalité.

Comme $\sharp F = q$ il s'ensuit que $F^{'}$ est le corps de décomposition du polynôme $X^q - X$ dans $\overline{\mathbb{F}}_p$. Mais comme il y a unicité du corps de décomposition on en déduit que $F^{'} = F = \mathbb{F}_q$.

Proposition.— *Soit p un nombre premier et $n, m \in \mathbb{N}^*$. Posons $q = p^n$ et $q^{'} = p^m$. Les propositions suivantes sont équivalentes :*

i) $\mathbb{F}_{q'}$ est une extension de $\mathbb{F}_q$,

ii) il existe $k \in \mathbb{N}^*$ tel que $m = kn$.

Preuve: *i)* $\Rightarrow$ *ii)* $\mathbb{F}_{q'}$ étant une extension de $\mathbb{F}_q$, on peut le voir comme $\mathbb{F}_q$-espace vectoriel, sa dimension $k > 0$ sur $\mathbb{F}_q$ est finie sinon le corps serait infini. On a donc $q^{'} = q^k$, c'est à dire que $m = kn$.

ii) $\Rightarrow$ *i)* Supposons $m = kn$. Si $x \in \mathbb{F}_q$ alors $x^q = x$ et donc par récurrence, $x^{q^k} = x$ c'est-à-dire $x^{q^{'}} = x$ c'est-à-dire $x \in \mathbb{F}_{q'}$.

Proposition.— *Le groupe multiplicatif $\mathbb{F}_q^*$ est cyclique. De manière générale, si K est un corps commutatif, tout sous-groupe fini Γ de $(K^*, .)$ est cyclique.*

Preuve: Si $x \in \Gamma$, pour tout $n \in \mathbb{N}$, $x^n \in \Gamma$. Γ étant fini, pour tout $x \in \Gamma$, il existe $n \in \mathbb{N}$ tel que $x^n = 1$ (n est l'ordre de x dans Γ). Considérons un élément $\alpha \in \Gamma$ d'ordre maximal N (i.e. si $x \in \Gamma$ est d'ordre n, alors $n \leq N$). Nous allons montrer que α génère Γ.

Soit $\beta \in \Gamma$ d'ordre n. Supposons que n ne divise pas N, il existe donc un nombre premier p et un entier e tel que p^e divise n et p^e ne divise pas N. Soit $f < e$ l'entier tel que $p^f | N$ et $p^{f+1} \not| N$. Considérons alors $\gamma = \alpha^{p^f} \beta^{n/p^e}$, l'ordre de α est N/p^f et celui de β^{n/p^e} est p^e, or p^e et N/p^f sont premiers entre eux, donc l'ordre de γ vaut $p^e.(N/p^f) > N$ (en effet, si a et b sont deux éléments d'un groupe abélien d'ordres respectifs s et t premiers entres eux alors l'ordre $o \leq p.p.c.m(s,t)$ de ab vérifie $a^o = b^{-o}$ et par suite $a^{os} = 1 = b^{-os}$ ce qui implique $t | os$ et donc $t | o$. De même, on a $s | ot$ et donc $s | o$, donc $p.p.c.m(s,t) | o$ et donc $o = p.p.c.m(s,t) = st$). Par conséquent γ a un ordre strictement plus grand que celui de α ce qui est absurde par hypothèse. Donc n divise N.

L'équation $X^n = 1$ a pour solution dans Γ les $\alpha^{k\frac{N}{n}}$ pour $k = 0, \cdots n-1$. Or β

est solution de cette équation, donc il existe $k \in \{0, \cdots, n-1\}$ tel que $\beta = \alpha^{k\frac{N}{n}}$. Ainsi Γ est cyclique.

Proposition.— *Un corps fini n'est jamais algébriquement clos.*

Preuve: Soit $F = \{x_1, \cdots, x_n\}$ un corps fini. Considérons le polynôme $P(X) = (X - x_1) \cdots (X - x_n) + 1$, c'est un polynôme de degré n et qui vérifie $P(x) = 1 \neq 0$ pour tout $x \in F$. Donc F n'est pas algébriquement clos.

Chapitre 2

Théorie de Galois

2.1 Extension séparable

2.1.1 Eléments séparables

Définition.— • *Soit k un corps et $P \in k[X]$ un polynôme irréductible. On dit que P est séparable si P ne possède que des racines simples dans $\overline{k}$.*

• *Un élément algébrique α d'une extension L/K est dit séparable, si $Min_K(\alpha)$ est un polynôme séparable.*

• *Une extension algébrique L/K est dite séparable si tout les éléments de L sont séparables.*

Proposition.— *Soit k un corps et $P \in k[X]$ un polynôme irréductible non constant. Les propositions suivantes sont équivalentes :*

i) P est séparable,

ii) $P^{'} \neq 0$.

Preuve: *ii)* $\Rightarrow$ *i)* Si $P^{'} \neq 0$ alors comme P est irréductible et que $d^{\circ}P^{'} < d^{\circ}P$, P et $P^{'}$ sont premier entre eux, donc n'ont pas de racine commune dans $\overline{k}$, donc P est à racines simples.

i) $\Rightarrow$ *ii)* Si $P^{'} = 0$, alors $car(k) = p \neq 0$. Il existe donc un polynôme $Q \in k[X]$ tel que $P(X) = Q(X^p)$. Le polynôme Q étant non constant possède dans $\overline{k}$ une racine α. On a donc $P(X) = (X^p - \alpha)Q_1(X^p)$. Soit maintenant β une racine dans $\overline{k}$ de $X^p - \alpha$. On a $X^p - \alpha = X^p - \beta^p = (X - \beta)^p$ et donc β est racine d'ordre au moins p de P, c'est-à-dire que P n'est pas séparable.

Corollaire.— *Soit k un corps et $P \in k[X]$ un polynôme irréductible.*

• *Si $car(k) = 0$ alors P est séparable. En particulier, toute extension algébrique en caractéristique nulle est séparable.*

• *Si $car(k) = p$, alors il existe un entier n et un polynôme $Q \in k[X]$ irréductible et séparable tel que $P(X) = Q(X^{p^n})$. En particulier, les racines de P dans $\overline{k}$ ont toutes la même multiplicité.*

Preuve: • c'est évident.

• Si P est séparable, alors on prend $Q = P$ et $n = 0$. Sinon, il existe $P_1 \in k[X]$ tel que $d^{\circ}P_1 \geq 1$ et tel que $P(X) = P_1(X^p)$. Le polynôme P_1 est irréductible, sinon P ne le serait pas. Si le polynôme P_1 est séparable, on prend $Q = P_1$ et $n = 1$,

sinon on recommence : il existe $P_2 \in k[X]$ irréductible tel que $d^\circ P_2 \geq 1$ et tel que $P_1(X) = P_2(X^p)$ etc. Cette récurence est finie, car $d^\circ P_{i+1} = d^\circ P_i - p$ et chaque P_i est non constant. Soit n l'indice pour lequel P_n est séparable, on prend alors $Q = P_n$ et on a bien $P(X) = Q(X^{p^n})$ avec Q irréductible et séparable.

Soit $\alpha_1, \cdots, \alpha_m$ les racines de Q dans $\overline{k}$. Elles sont distinctes deux à deux. Pour tout $i = 1, \cdots, m$ prenons β_i une racine de $X^{p^n} - \alpha_i$. Les β_i sont distinctes deux à deux et on a:

$$\begin{aligned} P(X) &= Q(X^{p^n}) = A\prod_{i=1}^{m}(X^{p^n} - \alpha_i) = A\prod_{i=1}^{m}(X^{p^n} - \beta_i^{p^n}) \\ &= A\prod_{i=1}^{m}(X - \beta_i)^{p^n} = A\left(\prod_{i=1}^{m}(X - \beta_i)\right)^{p^n} \end{aligned}$$

ce qui justifie que les β_i sont les racines de P et que leur ordre est p^n pour tout $i = 1, \cdots, m$.

2.1.2 Caractérisation de la séparabilité

Proposition.— *Soit L/K une extension monogène ($L = K(\alpha)$). On a $\sharp Isom_K(L, \overline{K}) \leq [L : K]$ et il y a égalité si et seulement si α est séparable.*

Preuve: On sait qu'il y a une bijection entre $Isom_K(L, \overline{K})$ et les racines de $P = Min_K(\alpha)$ dans $\overline{K}$. Comme le nombre de racines de P est plus petit que son degré, qui par ailleurs vaut $[L : K]$, on en déduit l'inégalité. De même, il y a égalité ssi P a $[L : K]$ racines distinctes dans $\overline{K}$, c'est-à-dire si P a $d^\circ P$ racine, c'est-à-dire si P est séparable.

Proposition.— *Soit L/K et M/L deux extensions algébriques. Il existe une bijection entre $Isom_K(M, \overline{K})$ et $Isom_K(L, \overline{K}) \times Isom_L(M, \overline{K})$.*

Preuve: Soit $\rho \in Isom_K(M, \overline{K})$, d'après le théorème de Steiniz, il existe un relevé $\widetilde{\rho}$ de ρ à $\overline{K}$ tout entier. Dans la suite, $\widetilde{\rho}$ désignera un relevé arbitraire de ρ, relevé choisi une fois pour toute.

Considérons $\sigma \in Isom_K(M, \overline{K})$ et notons

$$\begin{aligned} \sigma_L &= \sigma_{|L} && (\in Isom_K(L, \overline{K})) \\ \sigma^L &= (\widetilde{\sigma_L})^{-1} \circ \sigma && (\in Isom_L(M, \overline{K})) \end{aligned}$$

Considérons alors l'application $\Psi : Isom_K(M, \overline{K}) \to Isom_K(L, \overline{K}) \times Isom_L(M, \overline{K})$ définie par:

$$\Psi(\sigma) = (\sigma_L, \sigma^L)$$

L'application Ψ est injective car $\sigma = \widetilde{\sigma_L} \circ \sigma^L$. Elle est aussi surjective. En effet, soit $\rho \in Isom_K(L, \overline{K})$ et $\tau \in Isom_L(M, \overline{K})$, considérons alors $\sigma = \widetilde{\rho} \circ \tau$. On a $\sigma \in Isom_K(M, \overline{K})$ et $\sigma_L = \rho$ et $\sigma^L = (\widetilde{\sigma_L})^{-1} \circ \sigma = (\widetilde{\rho_L})^{-1} \circ \rho \circ \tau = \tau$. Ainsi Ψ est bijective.

Corollaire.— *Si L/K est une extension finie, alors $\sharp Isom_K(L, \overline{K}) \leq [L : K]$.*

Preuve: Soit $x_1, \cdots, x_n$ tels que $L = K(x_1, \cdots, x_n)$. On pose $K_0 = k$ et pour

$i = 1, \cdots, n$, $K_i = K(x_1, \cdots, x_i)$. On a:

$$\begin{array}{rcl} \sharp Isom_K(K_1, \overline{K}) & \leq & [K_1 : K_0] \\ \sharp Isom_{K_1}(K_2, \overline{K}) & \leq & [K_2 : K_1] \\ & \vdots & \\ \sharp Isom_{K_{n-1}}(K_n, \overline{K}) & \leq & [K_n : K_{n-1}] \end{array}$$

Donc,

$$\begin{array}{rcl} \prod_{i=1}^{n} \sharp Isom_{K_{i-1}}(K_i, \overline{K}) & \leq & \prod_{i=1}^{n} [K_i : K_{i-1}] \\ & = & [L : K] \end{array}$$

Par ailleurs, la proposition précédente montre, par récurrence immédiate, que $Isom_K(K_n, \overline{K})$ est en bijection avec $\prod_{i=1}^{n} Isom_{K_{i-1}}(K_i, \overline{K})$. Le résultat annoncé en découle alors.

Corollaire.— *Soit L/K est une extension finie. Les propositions suivantes sont équivalentes :*

i) L/K est séparable,

ii) $[L : K] = \sharp Isom_K(L, \overline{K})$.

Preuve: *i)* $\Rightarrow$ *ii)* Soit $x_1, \cdots, x_n$ tels que $L = K(x_1, \cdots, x_n)$. On pose $K_0 = k$ et pour $i = 1, \cdots, n$, $K_i = K(x_1, \cdots, x_i)$. L'extension L/K étant séparable, on a K_1/K_0 séparable, K_2/K_1 séparable etc., et donc

$$\begin{array}{rcl} \sharp Isom_K(K_1, \overline{K}) & = & [K_1 : K] \\ \sharp Isom_{K_1}(K_2, \overline{K}) & = & [K_2 : K_1] \\ & \vdots & \\ \sharp Isom_{K_{n-1}}(K_n, \overline{K}) & = & [K_n : K_{n-1}] \end{array}$$

Compte tenu de ce qui précède, on a finalement $[L : K] = \sharp Isom_K(L, \overline{K})$

ii) $\Rightarrow$ *i)* Soit $x \in L$, on a

$$\sharp Isom_K(L, \overline{K}) = \sharp Isom_K(K(x), \overline{K}) \times \sharp Isom_{K(x)}(L, \overline{K})$$

On a les inégalités

$$\begin{array}{rcl} \sharp Isom_K(K(x), \overline{K}) & \leq & [K(x) : K] \\ \sharp Isom_{K(x)}(L, \overline{K}) & \leq & [L : K(x)] \end{array}$$

et comme

$$[L : K] = [K(x) : K].[L : K(x)]$$

on en déduit les égalité

$$\begin{array}{rcl} \sharp Isom_K(K(x), \overline{K}) & = & [K(x) : K] \\ \sharp Isom_{K(x)}(L, \overline{K}) & = & [L : K(x)] \end{array}$$

or l'égalité $\sharp Isom_K(K(x), \overline{K}) = [K(x) : K]$ caractérise le fait que x est séparable sur K.

Corollaire.— *Soit L/K et M/L deux extensions algébriques. Les propositions suivantes sont équivalentes :*

i) M/K est séparable,

ii) L/K et M/L sont séparables.

Preuve: *i)* $\Rightarrow$ *ii)* Immédiat.

ii) $\Rightarrow$ *i)* Supposons pour commencer que L/K et M/L sont finies. Puisque ces extension sont séparables, on a

$$\begin{aligned} \sharp Isom_K(M,\overline{K}) &= \sharp Isom_K(L,\overline{K}).\sharp Isom_L(M,\overline{K}) \\ &= [L:K].[M:L] = [M:K] \end{aligned}$$

donc M/K est séparable.

Passons au cas général. Soit $x \in L$ et $P = \sum_{i=0}^{n} a_i X^i = Min_L(x)$. Considérons le corps $K_0 = K(a_0, \cdots, a_n)$ (qui est une extension finie de K). En utilisant le cas particulier, par récurrence immédiate (puisque a_0 est séparable sur K, que a_1 est séparable sur $K(a_0)$ etc.), on déduit que l'extension K_0/K est séparable. Maintenant, x est séparable sur K_0, donc, toujours en utilisant le cas fini, $K_0(x)/K$ est séparable, c'est-à-dire que x est séparable sur K.

Corollaire.— *Soit k un corps et $A \subset \overline{k}$. Les propositions suivantes sont équivalentes :*

i) $k(A)/k$ est séparable,

ii) quelque soit $x \in A$, x est séparable sur K.

Preuve: *i)* $\Rightarrow$ *ii)* Immédiat.

ii) $\Rightarrow$ *i)* On sait que $K(A) = \bigcup_{J \subset A \ finie} K(J)$. Soit $J = \{x_1, \cdots, x_n\} \subset A$. On a $K(x_1)/K$ séparable, $K(x_1, x_2)/K(x_1)$ séparable etc. Le corollaire précédent assure alors que $K(J)/K$ est séparable et par suite, tout élément de $K(A)$ est séparable sur K.

Lemme.— Soit K un corps infini et $P \in K[X_1, \cdots, X_n]$ un polynôme non nul. Il existe une infinité de n-uplets $(x_1, \cdots, x_n) \in K^n$ tels que $P(x_1, \cdots, x_n) \neq 0$.

Preuve: La propriété est vraie pour $n = 1$, car un polynôme en une variable n'a qu'un nombre fini de racines.
Supposons la propriété vraie pour $n - 1 \geq 0$. Considérons un polynôme non nul $P \in K[X_1, \cdots, X_n]$. Comme les anneaux $K[X_1, \cdots, X_n]$ et $K[X_1, \cdots, X_{n-1}][X_n]$ sont isomorphes, il existe un entier m, s entier $0 < i_1 < \cdots < i_s \leq m$ et $s+1$ polynômes non nuls $P_0, \cdots, P_s \in K[X_1, \cdots, X_{n-1}]$ tels que

$$P = P_0 X_n^m + P_1 X_n^{m-i_1} + \cdots + P_s X_n^{m-i_s}$$

Par hypothèse de récurrence, il existe $(x_1, \cdots, x_{n-1}$ tel que

$$P_0 P_1 \cdots P_s(x_1, \cdots, x_{n-1}) \neq 0$$

Le polynôme

$$g(X_n) = P_0(x_1, \cdots, x_{n-1}) X_n^m + \cdots + P_s(x_1, \cdots, x_{n-1}) X_n^{m-i_s} \in K[X_n]$$

est alors non nul et il existe donc $x_n \in K$ tel que $g(x_n) \neq 0$. Ainsi $P(x_1, \cdots, x_n) \neq 0$.

Corollaire.— Soit K un corps infini et V un espace vectoriel sur K de dimension finie. Si $V_1, \cdots, V_m$ désignent des sous-espaces vectoriels stricts de V, alors $\bigcup_i V_i \neq V$.

Preuve: Soit $n = dim_K V$, on identifie alors V à K^n. Comme pour chaque $i = 1, \cdots V$, $dim_K V_i < n$, il existe un hyperplan H_i de V tel que $V_i \subset H_i$ (théorème de la base incomplète). Maintenant, chaque H_i est le noyau d'une forme linéaire $f_i \in K[X_1, \cdots, X_n]$ non nulle. Considérons le polynôme $g = f_1 \cdots f_m$. On a alors

$$\bigcup_{i=1}^{m} H_i = \{(x_1, \cdots, x_n) \in K^n / \ g(x_1, \cdots, x_n) = 0\}$$

D'après le lemme précédent, il existe $(x_1, \cdots, x_n) \in K^n$ qui n'est pas un zéro de g, donc $(x_1, \cdots, x_n) \in V - \bigcup_{i=1}^{m} H_i$.

Théorème.— (élément primitif) Toute extension finie séparable est monogène.

Preuve: Soit L/K une extension finie séparable. Supposons que K soit un corps infini. Posons $[L : K] = n$ et $\{\sigma_1, \cdots, \sigma_n\} = Isom_K(L, \overline{K})$. Pour $i \neq j$, considérons

$$V_{ij} = \{x \in L / \ \sigma_i(x) = \sigma_j(x)\}$$

V_{ij} est un sous-K-espace vectoriel strict de L puisque $\sigma_i \neq \sigma_j$. Le corollaire précédent, assure alors que

$$\bigcup_{i \neq j} V_{ij} \neq L$$

Soit donc $x \in L - \bigcup_{i \neq j} V_{ij}$. les éléments $\sigma_1(x), \cdots, \sigma_n(x)$ sont distincts deux à deux et donc

$$n \leq \sharp Isom_K(K(x), \overline{K}) = [K(x) : K] \leq [L : K] = n$$

donc $K(x) = K$.

Supposons maintenant que K soit fini. Le corps L est donc lui aussi fini. Nous avons vu qu'alors $(L^*, .)$ était un groupe cyclique. Soit x un de ses générateurs, on a alors $L = K(x)$.

Lemme.— *Soit L/K une extension et A l'ensemble des éléments algébriques séparables sur K. A/K est une extension algébrique.*

Preuve: Soit $x, y \in A$ $(y \neq 0)$. $K(x, y)/K$ est séparable, donc $x - y$ et $xy^{-1} \in A$.

Définition.— *On appelle clôture séparable d'un corps K l'ensemble des éléments de $\overline{K}$ séparable sur K. On note ce corps K^{sep}.*

On dit que K est parfait si $K^{sep} = \overline{K}$.

Proposition.— *Soit K un corps. Si K est de caractéristique nulle alors K est parfait. Si K est de caractéristique p, alors les propositions suivantes sont équivalentes :*

i) K est parfait,

ii) le morphisme $x \mapsto x^p$ de K dans K est surjectif.

Preuve: *i)* $\Rightarrow$ *ii)* : Soit $a \in K$. Considérons le polynôme $P(X) = x^p - a$ et L son corps de décomposition sur K. Comme K est parfait, L/K est séparable et par suite galoisienne. Soit $b \in L$ une racine de P. Comme $P(b) = 0$, son polynôme

minimal divise donc $P(X) = (X - b)^p$ et comme b est séparable, ce polynôme est $X - b$ ce qui prouve que $b \in K$.

ii) $\Rightarrow$ *i)* : Soit $P \in K[X]$ un polynôme irréductible et inséparable. On a alors $P(X) = \sum_{i=0}^{n} a_i X^{ip}$. Soit $b_i \in K$ tel que $a_i = b_i^p$, on a donc:

$$P(X) = \sum_{i=0}^{n} (b_i X^i)^p = \left(\sum_{i=0}^{n} b_i X^i \right)^p$$

ce qui est contraire à l'irréductibilité de P.

2.2 Extension normale

2.2.1 Normalité

Définition.— *On dit qu'une extension algébrique L/K est normale si les conjugués (dans $\overline{K}$) de tous les éléments de L sont dans L.*

Proposition.— *Soit L/K une extension algébrique (on suppose L inclus dans une clôture algébrique $\overline{K}$ de K fixée). Les propositions suivantes sont équivalentes :*

i) L/K est normale,

ii) si $P \in K[X]$ est un polynôme irréductible possédant une racine dans L, alors P est totalement décomposé dans $L[X]$,

iii) pour tout $\sigma \in Isom_K(L, \overline{K})$, $\sigma(L) \subset L$,

iv) pour tout $\sigma \in Isom_K(L, \overline{K})$, $\sigma(L) = L$.

Preuve: *i)* $\Rightarrow$ *ii)* Soit $P \in K[X]$ un polynôme irréductible possédant une racine $\alpha \in L$. P est alors (à une constante multiplicative près) le polynôme minimal de α, donc les racines de P sont les conjugués sur K de α et figurent donc dans L, ainsi P est totalement décomposé dans L.

ii) $\Rightarrow$ *iii)* Soit $x \in L$ et P le polynôme minimal de x sur K. P est totalement décomposé dans L et $\sigma(x)$ est une racine de P pour tout $\sigma \in Isom_K(L, \overline{K})$, donc est dans L.

iii) $\Rightarrow$ *iv)* Soit σ un élément de $Isom_K(L, \overline{K})$. Comme $\sigma(L) \subset L$, on a alors $\sigma \in Isom_K(L, L) = Aut_K(L)$, donc $\sigma(L) = L$.

iv) $\Rightarrow$ *i)* Soit $\alpha \in L$ et $\beta \in \overline{K}$ un conjugué de α sur K. Il existe $\sigma \in Isom_K(L, \overline{K})$ tel que $\sigma(\alpha) = \beta$, donc $\beta \in L$ et L/K est normale.

Si L/K est une extension normale, on a donc

$$Isom_K(L, \overline{K}) = Isom_K(L, L) = Aut_K(L)$$

qui est donc un groupe.

Définition.— *Soit L/K une extension algébrique séparable. On appelle groupe de Galois de l'extension L/K le groupe $Aut_K(L)$. On le note $Gal(L/K)$.*

2.2.2 Caractérisation

Proposition.— *Soit L/K et M/L deux extensions algébriques. Si M/K est normale, alors M/L est normale.*

Preuve: Si β est un conjugué sur K d'un élément $\alpha \in M$, alors c'est aussi un conjugué sur L, puisque $Min_L(\alpha)$ divise $Min_K(\alpha)$.

Il est à noter que L/K n'a aucune raison de l'être aussi. De même, si L/K et M/L sont normale, il n'y a aucune raison pour que M/K soit normale. La normalité (au contraire de la séparabilité) n'est pas une notion tansitive.

Proposition.— *Soit K un corps, $A \subset \overline{K}$ une partie. Les propositions suivantes sont équivalentes :*

i) $K(A)/K$ est normale,

ii) les conjugués (dans $\overline{K}$) de tout $\alpha \in A$ sont dans $K(A)$.

Preuve: *i)* $\Rightarrow$ *ii)* Evident.

ii) $\Rightarrow$ *i)* Soit $x \in K(A)$. On peut écrire

$$x = \sum_i \prod_j \lambda_{ij} \alpha_{ij}^{n_{ij}}$$

avec $\alpha_{ij} \in A$, $\lambda_{ij} \in K$ et $n_{ij} \in \mathbb{N}$. Soit $\sigma \in Isom_K(K(A), \overline{K})$, alors $\sigma(\alpha_i j) \in A$ et comme

$$\sigma(x) = \sum_i \prod_j \lambda_{ij} \sigma(\alpha_{ij})^{n_{ij}}$$

on en déduit que $\sigma(x) \in K(A)$. Maintenant, si y est un conjugué de x dans $\overline{K}$, il existe un $\sigma \in Isom_K(K(A), \overline{K})$ tel que $\sigma(x) = y$, ce qui justifie que tout les conjugués de x sur K sont dans $K(A)$.

2.3 Extension galoisienne

Définition.— *Une extension algébrique L/K est dite galoisienne, si elle est normale et séparable. Si L/K est une extension galoisienne, le groupe $Aut_K(L) = Isom_K(L, \overline{K})$ s'appelle le groupe de Galois de l'extension L/K et se note $Gal(L/K)$.*

Si M/K est une extension galoisienne, alors pour toute extension intermédiaire L, l'extension M/L est aussi galoisienne (et $Gal(M/L)$ est alors un sous-groupe de $Gal(M/K)$) alors que l'extension L/K n'est pas forcément galoisienne.

Proposition.— *Soit L/K une extension algébrique de degré n. Alors $\sharp Aut_K(L) \leq n$ et $\sharp Aut_K(L) = n$ si et seulement si K/L est galoisienne.*

Preuve: Conséquence immédiate des parties précédentes.

Proposition.— *Soit L/K une extension algébrique de degré fini. Les propositions suivantes sont équivalentes :*

i) L/K est galoisienne,

ii) L est le corps de décomposition d'un polynôme de $K[X]$ dont les facteurs irréductibles sont séparables.

Preuve: *i)* $\Rightarrow$ *ii)* L/K est finie et séparable, donc possède un élément primitif α. On a $L = K(\alpha)$, mais comme L/K est normale, toutes les racines de $Min_K(\alpha)$ sont dans L. L est donc bien le corps de décomposition de $Min_K(\alpha)$ qui est séparable.

ii) $\Rightarrow$ *i)* Soit $P \in K[X]$ un polynôme et $P_1, \cdots, P_n \in K[X]$ ses facteurs irréductibles. Pour $i = 1, \cdots, n$ notons $(\alpha_{ij})_j$ les racines de P_i dans une clôture algébrique $\overline{K}$ fixée. Le corps de décomposition (dans $\overline{K}$) de P est donc le corps $K(\alpha_{ij})_{ij}$. Chaque α_{ij} est algébrique sur K et il y a un nombre fini de α_{ij}, donc L/K est finie. Maintenant, chaque α_{ij} est séparable sur K car le polynôme minimal de α_{ij} est (à un facteur multiplicatif près) le polynôme P_i qui est supposé séparable, donc L/K est séparable. Enfin, les conjugués de α_{ij_0} sur K sont les autres α_{ij} qui sont dans L, donc L/K est normale. L/K est donc bien une extension galoisienne finie.

Définition.— *Soit K un corps et $P \in K[X]$ un polynôme dont les facteurs irréductibles sont séparables. On appelle groupe de Galois du polynôme P le groupe $Gal(L/K)$ où L désigne le corps de décomposition du polynôme P.*

Si L désigne un corps et G un groupe d'automorphismes de corps de L, on note L^G (ou $inv(G)$) le sous-corps de L constitué des éléments de L laissé fixe par G :

$$L^G = \{x \in L/\ \forall \sigma \in G,\ \sigma(x) = x\}$$

Théorème.— (Artin) *Soit L un corps et G un groupe d'automorphismes fini de L. L'extension L/L^G est galoisienne de groupe de Galois G.*

Preuve: Posons $K = L^G$. On a

$$\sharp G \leq \sharp Isom_K(L, \overline{L}) \leq [L : K]$$

(à priori $\sharp Isom_K(L, \overline{L})$ et $[L : K]$ peuvent être infinis). Posons $G = \{\sigma_1, \cdots, \sigma_n\}$ et supposons qu'il existe une famille K-libre $\{x_1, \cdots, x_m\}$ d'éléments de L avec $m \geq n + 1$. On considère alors le système linéaire suivant :

$$(S) = \begin{cases} \sigma_1(x_1)X_1 + & \cdots & + \sigma_1(x_m)X_m & = & 0 \\ & & \vdots & & \\ & & \vdots & & \\ \sigma_n(x_1)X_1 + & \cdots & + \sigma_n(x_m)X_m & = & 0 \end{cases}$$

C'est un système à n équations et $m > n$ inconnues à coefficients dans L. Il existe donc une solution non trivial $Y = (y_1, \cdots, y_m) \in L^m$. Cette solution ne peut pas être dans K^m, car sinon pour tout $i = 1, \cdots, n$, on aurait

$$\sigma_i(y_1x_1 + \cdots + y_mx_m) = 0$$

et donc $y_1x_1 + \cdots + y_mx_m = 0$ ce qui serait en contradiction avec soit le fait que $\{x_1, \cdots, x_m\}$ est K-libre, soit le fait que Y est une solution non trivial. Quitte à renuméroter, on suppose que

$$Y = (y_1, \cdots, y_r, 0, \cdots, 0)$$

avec $y_i \neq 0$ pour $i = 1, \cdots, r$. Remarquons que $r \geq 2$ sinon $y_1 = 0$. Parmis, ces solution non nulles Y on en choisit une contenant un maximum de 0. Alors $y_1^{-1}Y$ est encore une telle solution. Soit $t \in \{2, \cdots, r)$ tel que $y_1^{-1}y_t \notin K$. Il existe donc $h \in \{1, \cdots, n\}$ tel que $\sigma_h(y_1^{-1}y_t) \neq y_1^{-1}y_t$ (σ_h existe bien, car sinon $y_1^{-1}y_t \in K$). Le vecteur $\sigma_h(y_1^{-1}Y)$ est encore solution de (S) puisque G étant un groupe, appliquer σ_h à (S) revient juste à permuter les équations. Donc $y_1^{-1}Y - \sigma_h(y_1^{-1}Y)$ est aussi une solution de (S), or cette solution est

$$(0, y_1^{-1}y_2 - \sigma_h(y_1^{-1}y_2), \cdots, y_1^{-1}y_r - \sigma_h(y_1^{-1}y_r), 0, \cdots, 0)$$

est une solution non nulle (puisque $\sigma_h(y_1^{-1}y_t) \neq y_1^{-1}y_t$) possédant plus de 0 que $y_1^{-1}Y$, ce qui est absurde. Donc $m \leq n$.

Ainsi, $[L : K] \leq n$ ce qui justifie l'égalité

$$\sharp G = \sharp Isom_K(L, \overline{L}) = [L : K]$$

On a donc $G = Isom_K(L, \overline{L})$ donc $Isom_K(L, \overline{L})) = Aut_K(L) = G$ et comme $\sharp Aut_K(L) = [L : K]$, L/K est bien une extension galoisienne, son groupe de Galois est alors $Gal(L/K) + Aut_K(L) = G$.

Si L/K est une extension algébrique, et K_0 une extension intermédiare, on note $gr(K_0)$ le sous-groupe de $Aut_K(L)$ constitué des éléments σ qui laisse fixe K_0 :

$$gr(K_0) = \{\sigma \in Aut_K(L)/\ \forall x \in L,\ \sigma(x) = x\}$$

Théorème.— (Galois) *Soit M/K une extension galoisienne finie. Alors*

1/ Pour tout corps intermédiaire L, on a $inv(gr(L)) = L$.

2/ Pour tout sous-groupe G de $Gal(M/K)$, on a $gr(inv(G)) = G$.

Les correspondances (dites galoisiennes) inv et gr sont donc des bijections (renversant l'inclusion) réciproques l'une de l'autre entre l'ensemble des extensions intermédiaires de L/K et l'ensemble des sous-groupes de $Gal(L/K)$.

Preuve: 1/ Soit $L^{'} = inv(gr(L))$. On a $L \subset L^{'} \subset M$. Soit $\sigma \in Isom_L(L^{'}, \overline{K})$ et $\widetilde{\sigma}$ un relevé de σ à M. On a $\widetilde{\sigma} \in Gal(M/L) = gr(L)$, donc $\sigma = Id$ et par suite $\sharp Isom_L(L^{'}, \overline{K}) = 1$. Comme l'extension $L^{'}/l$ est séparable (puisque M/L l'est), on en déduit que $[L^{'} : L] = 1$, c'est-à-dire $L = L^{'}$.

2/ C'est une conséquence immédiate du théorème d'Artin.

Les correspondances *inv* et *gr* sont donc des bijections réciproques l'une de l'autre entre l'ensemble des extensions intermédiaires de L/K et l'ensemble des sous-groupes de $Gal(L/K)$. en particulier, il n'y a qu'un nombre fini d'extensions intermédiaires de L/K. On remarque aisément que si $L_1 \subset L_2$ sont deux extensions intermédiaires, alors $inv(L_2) \subset inv(L_1)$ et que si $G_1 \subset G_2$ sont deux sous-groupes de $Gal(M/K)$ alors $gr(G_2) \subset gr(G_1)$.

Théorème.— *Soit M/K une extension galoisienne finie et L une extension intermédiare. Les propositions suivantes sont équivalentes:*

i) L/K est galoisienne,

ii) $Gal(M/L)$ est un sous-groupe distingué de $Gal(M/K)$.

Dans ces conditions, le groupe $Gal(L/K)$ est isomorphe au groupe quotient $Gal(M/K)/Gal(M/L)$.

Preuve: Soit $\sigma \in Gal(M/K)$, alors

$$inv(\sigma Gal(M/L)\sigma^{-1}) = \sigma(L)$$

En effet, soit $x \in inv(\sigma Gal(M/L)\sigma^{-1})$. Pour tout $\mu \in Gal(M/L)$, $\mu(\sigma^{-1}(x)) = \sigma^{-1}(x)$ et donc $\sigma^{-1}(x) \in L$ et par suite, $x \in \sigma(L)$.

Réciproquement, soit $x \in \sigma(L)$ (disons $x = \sigma(y)$ avec $y \in L$), alors pour tout $\mu \in Gal(M/L)$, on a $\sigma(\mu(\sigma^{-1}(x))) = \sigma(\mu(\sigma^{-1}(\sigma(y)))) = \sigma(y) = x$, donc $x \in inv(\sigma Gal(M/L)\sigma^{-1})$.

$i) \Rightarrow ii)$ Si L/K est galoisienne, alors pour tout $\sigma \in Gal(M/K)$, $\sigma(L) = L$ et donc $inv(\sigma Gal(M/L)\sigma^{-1}) = L$, c'est-à-dire $\sigma Gal(M/L)\sigma^{-1} \subset Gal(M/L)$, donc $Gal(M/L)$ est distingué dans $Gal(M/K)$.

$ii) \Rightarrow i)$ Supposons que $Gal(M/L)$ soit distingué dans $Gal(M/K)$. Alors pour tout $\sigma \in Gal(M/K)$,

$$L = inv(Gal(M/L)) = inv(\sigma Gal(M/L)\sigma^{-1}) = \sigma(L)$$

Soit $\mu \in Isom_K(L, \overline{K})$ et $\widetilde{\mu}$ un relevé de μ à $\overline{K}$. La restriction de $\widetilde{\mu}$ à M est un élément de $\sigma = Gal(M/K)$ puisque M/K est normale, et la restriction de σ à L vaut μ, donc $\mu(L) = L$. Ainsi,

$$Isom_K(L, \overline{K}) = Aut_K(L)$$

donc L/K est une extension normale. Elle est séparable puisque M/K l'est. L'extension L/K est bien galoisienne.

Considérons l'application de restriction

$$res : Gal(M/K) \to Gal(L/K)$$

Cette application est un morphisme de groupe, elle est surjective en vertu de ce que l'on vient de dire. Le noyau de res est $Gal(M/L)$. En effet soit $\sigma \in Gal(M/K)$ tel que $res(\sigma) = Id$, alors $\sigma(x) = x$ pour tout $x \in L$ donc $\sigma \in Gal(M/L)$. reciproquement, les éléments de $\sigma \in Gal(M/L)$ vérifie bien $res(\sigma) = Id$.

On en déduit alors, par factorisation du morphisme res, un isomorphisme

$$Gal(L/K) \simeq Gal(M/K)/Gal(M/L)$$

Proposition.— *Soit M/K une extension finie et L une extension intermédiare. On suppose que les extensions M/L et L/K sont galoisiennes. Les propositions suivantes sont équivalentes:*

i) M/K est galoisienne,

ii) Tout éléments de $Gal(L/K)$ se remonte en un élément de $Aut_K(L)$ (i.e. l'application de restriction $res : Aut_K(M) \to Gal(L/K)$ est surjective).

Preuve: $i) \Rightarrow ii)$ Soit $\sigma \in Gal(L/K)$, d'après le théorème de Steiniz, il existe un relevé $\widetilde{\sigma}$ de σ à $\overline{K}$. La restriction $\widetilde{\sigma}_M$ de $\widetilde{\sigma}$ à M est un élément de $Gal(M/K)$ et vérifie bien $res(\widetilde{\sigma}) = \sigma$.

$ii) \Rightarrow i)$ Par hypothèse, $res : Aut_K(M) \to Gal(L/K)$ est surjective. r est un morphisme de groupe et son noyau est $Gal(M/L)$. On a donc $\sharp Aut_K(M) = \sharp Gal(L/K).\sharp Gal(M/L) = [L : K].[M : L] = [M : K]$, et par suite, L/K est galoisienne.

Chapitre 3

Applications

3.1 Trace, norme et discriminant

3.1.1 Trace, norme et polynôme caractéristique dans une extension

Soit L/K une extension finie et $\alpha \in L$. L'application $\phi_\alpha : L \to L$ définie par $\phi_\alpha(y) = \alpha y$ est une application linéaire (L est vu comme K-espace vectoriel). Cette application linéaire possède un polyôme caractéristique P_α, une trace et un déterminant.

Définition.— *Soit L/K une extension finie et $\alpha \in L$, on appelle polynôme caractéristique (resp. trace, resp. norme) de α dans l'extension L/K le polynôme $P_{\alpha,L/K}$, noté $Car_{\alpha,L/K}$ (resp. l'élement $Tr(\phi_\alpha)$ noté $Tr_{L/K}(\alpha)$, resp. l'élément $Det(\phi_\alpha)$ noté $N_{L/K}(\alpha)$).*

Proposition.— *Soit L/K une extension de degré n.*

a) $\forall \alpha \in L$, $Tr_{L/K}(\alpha) \in K$ et $N_{L/K}(\alpha) \in K$.

b.1) $Tr_{L/K}$ est une forme linéaire sur L.

b.2) $\forall \alpha \in K$, $Tr_{L/K}(\alpha) = n\alpha$.

c.1) $\forall \alpha, \beta \in L$, $N_{L/K}(\alpha\beta) = N_{L/K}(\alpha)N_{L/K}(\beta)$.

c.2) $\forall \alpha \in K$, $N_{L/K}(\alpha) = \alpha^n$.

c.3) $\forall \alpha \in L$, $N_{L/K}(\alpha) = 0 \Leftrightarrow \alpha = 0$.

d.1) $\forall \alpha \in L$, $Car_{\alpha,L/K}(X) \in K[X]$.

d.2) $\forall \alpha \in L$, si $Car_{\alpha,L/K}(X) = (-1)^n(X^n + a_{n-1}X^{n-1} + \cdots + a_0)$, alors $Tr_{L/K}(\alpha) = -a_{n-1}$ et $N_{L/K}(\alpha) = (-1)^n a_0$.

Preuve: a) Immédiat.

b.1) Immédiat.

b.2) et c.2) $\forall \alpha \in K$, l'application ϕ_α vaut αId, donc $Tr_{L/K}(\alpha) = n\alpha$ et $N_{L/K}(\alpha) = \alpha^n$.

c.1) Immédiat.

c.3) La multiplication par $\alpha \neq 0$ étant un morphisme inversible, le déterminant de ce morphisme est donc non nul.

d.1) Immédiat.

d.2) Propriété bien connue d'algèbre linéaire.

Proposition.— *Soit M/L et L/K deux extensions finies. Pour tout $\alpha \in L$, on a :*

$$\begin{aligned} Tr_{M/K}(\alpha) &= [M:L]Tr_{L/K}(\alpha) \\ N_{M/K}(\alpha) &= \big(N_{L/K}(\alpha)\big)^{[M:L]} \\ Car_{\alpha,M/K}(X) &= \big(Car_{\alpha,L/K}(X)\big)^{[M:L]} \end{aligned}$$

Preuve: Soit $(e_1, \cdots, e_r)$ une K-base de L et $(f_1, \cdots, f_s)$ une L-base de M. La famille

$$\mathcal{B} = (e_1 f_1, \cdots, e_r f_1, \cdots\cdots, e_1 f_s, \cdots, e_r f_s)$$

est alors une K-base de M. Pour $x \in L$ si l'on note $A(x)$ la matrice de l'application (de $L \to L$) $y \mapsto xy$ dans la base $(e_1, \cdots, e_r)$, alors la matrice de l'application (de $M \to M$) $y \mapsto xy$ dans la base $\mathcal{B}$ est la matrice diagonale "par bloc" $Diag(A(x), \cdots, A(x))$, le résultat en découle.

Corollaire.— *Soit L/K une extension finie et $\alpha \in L$. On a*

$$Car_{\alpha,L/K}(X) = (-1)^{[L:K]} Min_K(\alpha)^{[L:K(\alpha)]}(X)$$

En conséquence de quoi, $Car_{\alpha,L/K}(X) = (-1)^{[L:K]} Min_K(\alpha)(X)$ ssi $L = K(\alpha)$.

Preuve: • cas $L = K(\alpha)$. Soit $P(X) = a_0 + \cdots a_{n-1}X^{n-1} + X^n$ le polynôme minimal de α sur L. Dans la base $(1, \cdots, \alpha^{n-1}$ la matrice de $x \mapsto \alpha x$ est la matrice de Frobenius $Frob(a_0, \cdots, a_{n-1}$. Il est bien connu que cette matrice a pour polynôme caractéristique le polynôme $(-1)^n P(X)$.

• cas général. En appliquant la proposition précédente à l'extension $L/K(\alpha)/K$, on trouve la formule annoncée.

Théorème.— *Soit L/K une extension finie et séparable. Pour tout $\alpha \in L$, on a*

$$\begin{aligned} Tr_{L/K}(\alpha) &= \sum_{\sigma \in Isom_K(L,\overline{K})} \sigma(\alpha) \\ N_{L/K}(\alpha) &= \prod_{\sigma \in Isom_K(L,\overline{K})} \sigma(\alpha) \end{aligned}$$

Preuve: • Si α est un élément primitif de l'extension L/K, alors $Car_{\alpha,L/K}(X) = (-1)^{[L:K]} Min_K(\alpha)(X) = \prod_{\sigma \in Isom_K(L,\overline{K})}(X - \sigma(\alpha))$, d'où les formules annoncées.

• Si α est quelconque, alors

$$\begin{aligned} Tr_{K(\alpha)/K}(\alpha) &= \sum_{\sigma \in Isom_K(K(\alpha),\overline{K})} \sigma(\alpha) \\ N_{K(\alpha)/K}(\alpha) &= \prod_{\sigma \in Isom_K(K(\alpha),\overline{K})} \sigma(\alpha) \end{aligned}$$

Maintenant si pour tout $\sigma \in Isom_K(K(\alpha), \overline{K})$ on note $\widetilde{\sigma}$ un relevé fixé une fois pour toute de σ à $\overline{K}$, alors on sait que l'application

$$\begin{array}{rccc} \Psi : & Isom_K(K(\alpha), \overline{K}) \times Isom_K(\alpha)(L, \overline{K}) & \longrightarrow & Isom_K(K(\alpha), \overline{K}) \\ & (\sigma, \tau) & \longmapsto & \widetilde{\sigma} \circ \tau \end{array}$$

est une bijection. Donc

$$\begin{aligned} \sum_{\mu \in Isom_K(L, \overline{K})} \mu(\alpha) &= \sum_{\sigma \in Isom_K(K(\alpha), \overline{K})} \sum_{\tau \in Isom_K(\alpha)(L, \overline{K})} \widetilde{\sigma}\tau(\alpha) \\ &= \sum_{\sigma \in Isom_K(K(\alpha), \overline{K})} \sum_{\tau \in Isom_K(\alpha)(L, \overline{K})} \widetilde{\sigma}(\alpha) \\ &= [L : K(\alpha)] \sum_{\sigma \in Isom_K(K(\alpha), \overline{K})} \sigma(\alpha) \\ &= [L : K(\alpha)] Tr_{K(\alpha)/K}(\alpha) \\ &= Tr_{L/K}(\alpha) \end{aligned}$$

De même, pour la norme:

$$\begin{aligned} \prod_{\mu \in Isom_K(L, \overline{K})} \mu(\alpha) &= \prod_{\sigma \in Isom_K(K(\alpha), \overline{K})} \prod_{\tau \in Isom_K(\alpha)(L, \overline{K})} \widetilde{\sigma}\tau(\alpha) \\ &= \prod_{\sigma \in Isom_K(K(\alpha), \overline{K})} \prod_{\tau \in Isom_K(\alpha)(L, \overline{K})} \widetilde{\sigma}(\alpha) \\ &= \left(\prod_{\sigma \in Isom_K(K(\alpha), \overline{K})} \sigma(\alpha) \right)^{[L:K(\alpha)]} \\ &= \left(N_{K(\alpha)/K}(\alpha) \right)^{[L:K(\alpha)]} \\ &= N_{L/K}(\alpha) \end{aligned}$$

Théorème.— *Soit L/K une extension finie non séparable. Pour tout $\alpha \in L$, on a $Tr_{L/K}(\alpha) = 0$.*

Preuve: • si α est séparable sur K. Alors $K(\alpha)/K$ est séparable et par suite, $L/K(\alpha)$ ne l'est pas. Soit $\beta \in L$ non séparable sur $K(\alpha)$ et $P = Min_{K(\alpha)}(\beta)$. P n'étant pas séparable, a un degré qui est multiple de $p = car(K)$, donc $[L : K]$ est divisible par p. Ainsi, $Tr_{L/K}(\alpha) = [L : K(\alpha)] Tr_{K(\alpha)/K}(\alpha) = 0$.

• si α n'est pas séparable sur K. Le polynôme minimal de α est en la variable X^p, donc le coefficient de degré $d^\circ\alpha - 1$ est nul et par suite $Tr_{K(\alpha)/K}(\alpha) = 0$, donc $Tr_{L/K}(\alpha) = [L : K(\alpha)] Tr_{K(\alpha)/K}(\alpha) = 0$.

3.1.2 Discriminant

Discriminant d'une famille

Si L/K désigne une extension finie de degré n, alors l'application

$$\begin{array}{ccc} L\times L & \longrightarrow & K \\ (u,v) & \longmapsto & Tr_{L/K}(uv) \end{array}$$

est une forme bilinéaire symétrique.

Définition.— *Soit $(x_1,\cdots,x_n)\in L^n$, on appelle discriminant de la famille $(x_1,\cdots,x_n)$, le déterminant de Gram du système $(x_1,\cdots,x_n)$ pour la forme $Tr(uv)$. On note $disc_{L/K}(x_1,\cdots,x_n)$ cet élément de K. On a donc, par définition,*

$$disc_{L/K}(x_1,\cdots,x_n)=det\left((Tr(x_ix_j))_{i,j}\right)$$

Remarque: Si $(y_1,\cdots,y_n)\in L^n$ est telle qu'il existe $A=(a_{ij})_{i,j}\in\mathcal{M}_n(K)$ vérifiant

$$\forall j=1,\cdots,n\ y_j=\sum_{i=1}^{n}a_{ij}x_i$$

alors $disc_{L/K}(y_1,\cdots,y_n)=(det(A))^2 disc_{L/K}(x_1,\cdots,x_n)$. C'est un résultat classique sur le déterminant de Gram.

Proposition.— *Soit L/K une extension finie séparable de degré n et soit $\{\sigma_1,\cdots,\sigma_n\}=Isom_K(L,\overline{K})$. Pour tout $(x_1,\cdots,x_n)\in L^n$, on a*

$$disc_{L/K}(x_1,\cdots,x_n)=\left(det\left((\sigma_i(x_j))_{i,j}\right)\right)^2$$

Preuve: On sait que pour tout $x\in L$, on a $Tr(x)=\sum_{i=1}^{n}\sigma_i(x)$, on a donc $Tr(x_ix_j)=\sum_{k=1}^{n}\sigma_k(x_i)\sigma_k(x_j)$ et par suite, $Gram(x_1,\cdots,x_n)={}^tMM$ où M est la matrice $(\sigma_i(x_j))_{i,j}$.

Corollaire.— *Soit L/K une extension finie séparable de degré n. L'application*

$$\begin{array}{ccc} L\times L & \longrightarrow & K \\ (u,v) & \longmapsto & Tr_{L/K}(uv) \end{array}$$

est une forme bilinéaire symétrique non dégénérée (i.e. si $x\in L$ est tel que $Tr(xy)=0$ pour tout $y\in L$ alors $x=0$).

Preuve: Cette propriété équivaut au fait que si $(e_1,\cdots,e_n)$ désigne une K-base de L, alors $Gram(e_1,\cdots,e_n)$ est inversible, c'est donc à dire que $disc_{L/K}(e_1,\cdots,e_n)\neq 0$. On sait que $disc_{L/K}(e_1,\cdots,e_n)=\left(det\left((\sigma_i(e_j))_{i,j}\right)\right)^2$. Par le théorème de Dedekind, on sait que la famille $\{\sigma_1,\cdots,\sigma_n\}=Isom_K(L,\overline{K})$ est $\overline{K}$-libre, ce qui assure que $(\sigma_i(e_j))_{i,j}\in GL_n(\overline{K})$ et donc que $disc_{L/K}(e_1,\cdots,e_n)\neq 0$.

Théorème.— *Soit L/K une extension finie séparable de degré n et $\alpha\in L$. On note $P=Min_K(\alpha)$.*

- *Si α n'est pas primitif, alors $disc_{L/K}(1,\alpha,\cdots,\alpha^n)=0$.*
- *Si α est primitif, alors $disc_{L/K}(1,\alpha,\cdots,\alpha^n)=(-1)^{\frac{n(n-1)}{2}}N_{L/K}(P'(\alpha))$.*

Preuve: On a

$$disc_{L/K}(1,\alpha,\cdots,\alpha^n)=\left(det\left((\sigma_i(\alpha^j))_{i,j}\right)\right)^2=\left(det\left((\sigma_i(\alpha)^j)_{i,j}\right)\right)^2$$

La matrice $(\sigma_i(\alpha)^j)_{i,j}$ est la matrice de Vandermonde associée au n-uplet $(\sigma_1(\alpha), \cdots, \sigma_n(\alpha))$. On a donc

$$\begin{aligned} disc_{L/K}(1, \alpha, \cdots, \alpha^n) &= \left(\prod_{i>j}(\sigma_i(\alpha) - \sigma_j(\alpha))\right)^2 \\ &= (-1)^{\frac{n(n-1)}{2}} \prod_{i\neq j}(\sigma_i(\alpha) - \sigma_j(\alpha)) \\ &= (-1)^{\frac{n(n-1)}{2}} \prod_i \prod_{j\neq i}(\sigma_i(\alpha) - \sigma_j(\alpha)) \end{aligned}$$

• Si α n'est pas primitif, alors $[K(\alpha) : K] < n$ et par suite, il existe $i \neq j$ tel que $\sigma_i(\alpha) = \sigma_j(\alpha)$ d'où la nullité de $disc_{L/K}(1, \alpha, \cdots, \alpha^n)$.

• Si α est primitif, alors $P(X) = \prod_i(X - \sigma_i(\alpha))$ et donc $P^{'}(X) = \sum_i \prod_{j\neq i}(X - \sigma_j(\alpha))$. On a alors :

$$\sigma_i(P^{'}(\alpha)) = P^{'}(\sigma_i(\alpha)) = \prod_{j\neq i}(\sigma_i(\alpha) - \sigma_j(\alpha))$$

et par suite

$$\begin{aligned} disc_{L/K}(1, \alpha, \cdots, \alpha^n) &= (-1)^{\frac{n(n-1)}{2}} \prod_i \prod_{j\neq i}(\sigma_i(\alpha) - \sigma_j(\alpha)) \\ &= (-1)^{\frac{n(n-1)}{2}} \prod_i \sigma_i(P^{'}(\alpha)) \\ &= (-1)^{\frac{n(n-1)}{2}} N_{L/K}(P^{'}(\alpha)) \end{aligned}$$

Discriminant d'un polynôme

Lemme.— *Soit K un corps et $P \in K[X]$ un polynôme de degré ≥ 2. On pose $P(X) = \lambda \prod_{i=1}^n (X - r_i)$ avec $r_i \in \overline{K}$. On a*

$$\begin{aligned} \lambda^{2n-2}\left(\prod_{i>j}(r_i - r_j)\right)^2 &= (-1)^{\frac{n(n-1)}{2}} \lambda^{2n-2} \prod_{i\neq j}(r_i - r_j) \\ &= (-1)^{\frac{n(n-1)}{2}} \lambda^{n-2} \prod_{i=1}^n P^{'}(r_i) \end{aligned}$$

Preuve: On a $P^{'}(X) = \lambda \sum_i \prod_{j\neq i}(X - r_j)$.

Définition.— *Soit K un corps et $P \in K[X]$ un polynôme de degré ≥ 2. On appelle discriminant du polynôme P l'élément noté $Discr(P)$ égale à l'une des trois quantités introduites dans le lemme précédent.*

Proposition.— *Soit K un corps et $P \in K[X]$ un polynôme de degré ≥ 2.*

(a) $Discr(P) \in K$.

(b) $Discr(P) \neq 0$ si et seulement si P est séparable.

Preuve: (a) Posons $P(X) = \lambda(X^n + a_{n-1}X^{n-1} + \cdots + a_0)$. Le polynôme

$$S(X_1, \cdots, X_n) = \lambda^{2n-2} \left(\prod_{i>j} (X_i - X_j) \right)^2 \in K[X_1, \cdots, X_n]$$

est symétrique, il existe donc un polynôme $Q \in K[X_1, \cdots, X_n]$ tel que

$$S = Q(\sigma_1^n, \cdots, \sigma_n^n)$$

où σ_i^n désigne la i-ième fonction symétrique élémentaire d'ordre n. Ainsi,

$$\begin{array}{rcl} Discr(P) & = & S(r_1, \cdots, r_n) \\ & = & Q(\sigma_1^n(r_1, \cdots, r_n), \cdots, \sigma_n^n(r_1, \cdots, r_n)) \\ & = & Q(-a_{n-1}, \cdots, (-1)^n a_0) \\ & \in & K \end{array}$$

(b) Immédiat.

Exercice: Calculer $Discr(P)$ pour $P(X) = aX^2 + bX + c$, $P(X) = X^3 + pX + q$ et $P(X) = \Phi_p(X)$ (p premier).

Proposition.— *Soit K un corps, $P \in K[X]$ un polynôme unitaire irréductible de degré ≥ 2 et $\alpha \in \overline{K}$ une racine de P. On a*

$$Discr(P) = (-1)^{\frac{n(n-1)}{2}} N_{K(\alpha)/K}(P'(\alpha))$$

Preuve: Si P n'est pas séparable, alors $Discr(P) = 0$, mais comme $P' = 0$, on a bien $N_{K(\alpha)/K}(P'(\alpha)) = 0$.

Si P est séparable, alors

$$\begin{array}{rcl} Discr(P) & = & \left(\prod_{i>j} (r_i - r_j) \right)^2 \\ & = & \left(\prod_{i>j} (\sigma_i(\alpha) - \sigma_j(\alpha)) \right)^2 \text{ (où } \sigma_i \in Isom_K(K(\alpha), \overline{K})) \\ & = & disc_{K(\alpha)/K}(1, \alpha, \cdots, \alpha^{n-1}) \\ & = & (-1)^{\frac{n(n-1)}{2}} N_{K(\alpha)/K}(P'(\alpha)) \end{array}$$

3.1.3 Résultant

Définition.— *Soient n, m deux entiers non nuls et K un corps. On appelle résultant d'ordre (m,n) le polynôme*

$$R = \begin{vmatrix} X_m & & & & Y_n & & \\ \vdots & X_m & & & Y_{n-1} & \ddots & \\ \vdots & \vdots & \ddots & & \vdots & \ddots & Y_n \\ X_0 & \vdots & \ddots & X_m & \vdots & \vdots & Y_{n-1} \\ & X_0 & \ddots & \vdots & Y_0 & \vdots & \vdots \\ & & \ddots & \vdots & & \ddots & \vdots \\ & & & X_0 & & & Y_0 \end{vmatrix}$$

(déterminant $m+n$) de l'anneau $K[X_m,\cdots,X_0,Y_n,\cdots,Y_0]$.

Si $P(X) = a_mX^m + \cdots + a_0$ et $Q(X) = b_nX^n + \cdots + b_0$ désignent deux polynômes de $K[X]$, on appelle résultant des polynômes P et Q l'élement $\mathcal{R}(P,Q) = R(a_m,\cdots,a_0,b_n,\cdots,b_0)$.

Proposition.— *Soient $P(X) = a_mX^m + \cdots + a_0$ et $Q(X) = b_nX^n + \cdots + b_0$ deux polynômes de $K[X]$. Si l'on note*

$$S = \begin{pmatrix} a_m & & & & b_n & & \\ \vdots & a_m & & & b_{n-1} & \ddots & \\ \vdots & \vdots & \ddots & & \vdots & \ddots & b_n \\ a_0 & \vdots & \ddots & a_m & \vdots & \vdots & b_{n-1} \\ & a_0 & \ddots & \vdots & b_0 & \vdots & \vdots \\ & & \ddots & \vdots & & \ddots & \vdots \\ & & & a_0 & & & b_0 \end{pmatrix} \in \mathcal{M}_{m+n}(K)$$

alors

$$rg(S) = m + n - d^\circ p.g.c.d.(P,Q)$$

Preuve: L'application

$$\begin{array}{rccc} \Psi : & K_{n-1}[X] \times K_{m-1}[X] & \longrightarrow & K_{m+n-1}[X] \\ & (f,g) & \longmapsto & fP + gQ \end{array}$$

est clairement linéaire. La famille

$$\mathcal{B} = ((\mathcal{X}^{\setminus -\infty}, \prime), \cdots, (\infty, \prime), (\prime, \mathcal{X}^{\Updownarrow -\infty}), \cdots, (\prime, \infty))$$

est une base de $K_{n-1}[X]\times K_{m-1}[X]$ et si $\mathcal{C}$ désigne la base canonique de $K_{m+n-1}[X]$, alors $Mat_{\mathcal{B},\mathcal{C}}(\Psi) = S$.

Notons $D = p.g.c.d.(P,Q)$. Comme $(P)+(Q) = (D)$, on en déduit que $Im(\Psi) \subset (D) \cap K_{m+n-1}[X]$, et donc que

$$Im(\psi) \subset \{HD,\ H \in K_{m+n-1-d^\circ D}[X]\}$$

Soit $H \in K_{m+n-1-d^\circ D}[X]$, il existe donc f et g tels que $fP + gQ = HD$. En divisant :

$$\begin{array}{ll} f = h_1Q + r_1 & d^\circ r_1 < d^\circ Q = n \\ g = h_2P + r_2 & d^\circ r_2 < d^\circ P = m \end{array}$$

on obtient $HD = (h_1 + h_2)PQ + r_1P + r_2Q$, mais pour des raisons de degré, $h_1 + h_2 = 0$, donc $HD = r_1P + r_2Q$, c'est-à dire que $HD \in Im(\Psi)$. Donc $Im(\Psi) \simeq K_{m+n-1-d^\circ D}[X]$, d'où les rang de S.

Corollaire.— *Avec les notations précédentes, les propositions suivantes sont équivalentes :*

i) P et Q sont premier entres eux,

ii) $\mathcal{R}(P, Q) \neq 0$.

Preuve: Immédiat.

3.2 Corps finis

Soit p un nombre premier, n un entier non nul et $q = p^n$. On rappelle que $\mathbb{F}_q = \mathbb{F}_p(\xi)$ où ξ est une racine primitive $q-1$-ième de l'unité.

Proposition.— *L'extension $\mathbb{F}_q/\mathbb{F}_p$ est séparable et le corps $\mathbb{F}_p$ est parfait. En conséquence de quoi, l'application $\sigma : x \mapsto x^p$ est un $\mathbb{F}_p$-automorphisme de $\overline{\mathbb{F}_p}$.*

Preuve: Comme $\mathbb{F}_q = \mathbb{F}_p(\xi)$ et que $q-1$ est premier avec p, le polynôme minimal de ξ est séparable.

Maintenant, les extensions finies $L/\mathbb{F}_p$ sont exactement les corps $L = \mathbb{F}_q$ et donc $\overline{\mathbb{F}}_p = \bigcup_n \mathbb{F}_{p^n}$ et par suite ${\mathbb{F}_p}^{sep} = \overline{\mathbb{F}}_p$. Le corps $\mathbb{F}_p$ est donc parfait cette propriété équivalent à dire que $\sigma : x \mapsto x^p$ est un $\mathbb{F}_p$-automorphisme de $\overline{\mathbb{F}_p}$.

On appelle l'automorphisme σ *le frobenius.*

Théorème.— *(a) L'extension $\mathbb{F}_q/\mathbb{F}_p$ est galoisienne.*

(b) Le groupe $Gal(\mathbb{F}_q/\mathbb{F}_p)$ est cyclique d'ordre n, il est engendré par le frobenius.

(c) Un élément $\mu \in Gal(\mathbb{F}_q/\mathbb{F}_p)$ est un générateur de ce groupe ssi il existe s premier avec n tel que $\mu = \sigma^s$.

Preuve: (a) On sait déjà que l'extension $\mathbb{F}_q/\mathbb{F}_p$ est séparable. Les éléments $x \in \mathbb{F}_q$ satisfont $x^q - x = 0$ donc leurs conjugués aussi, donc sont dans $\mathbb{F}_q$ ce qui montre bien que l'extension est normale.

(b) La restriction du frobenius à $\mathbb{F}_q$ est un automorphisme de $\mathbb{F}_q$ puisque $\mathbb{F}_q/\mathbb{F}_p$ est galoisienne. On continue à le noter σ. Considérons $G =< \sigma >$, on sait que $G \subset Gal(\mathbb{F}_q/\mathbb{F}_p)$ et que $\sharp Gal(\mathbb{F}_q/\mathbb{F}_p) = n$. Soit $r < n$, les éléments invariants par σ^r sont au nombre de p^r, donc l'ordre de σ est $\leq n$. Pour des raison de cardinalité, on en déduit que σ est d'ordre n, ce qui justifie que $G = Gal(\mathbb{F}_q/\mathbb{F}_p)$ et que ce dernier groupe est cyclique.

(c) L'application

$$\begin{array}{rccc} \theta : & \mathbb{Z}/n\mathbb{Z} & \to & Gal(\mathbb{F}_q/\mathbb{F}_p) \\ & a & \mapsto & \sigma^a \end{array}$$

est un isomorphisme de groupe. Les générateurs de $Gal(\mathbb{F}_q/\mathbb{F}_p)$ correspondent donc à ceux de $\mathbb{Z}/n\mathbb{Z}$ qui sont bien les nombre a premiers avec n.

3.3 Corps cyclotomiques

3.3.1 Indicateur d'Euler

Définition.— *Soit $n \geq 1$ un entier, on note $\varphi(n)$ le nombre d'entier $\leq n$ premier avec n. On appelle φ "l'indicateur d'Euler" ou "la fonction indicatrice d'Euleur".*

Proposition.— *(a) Pour tout n, $\varphi(n) = \sharp\,(\mathbb{Z}/n\mathbb{Z})^*$.*

(b) Si a et b sont premiers entres eux alors $\varphi(ab) = \varphi(a)\varphi(b)$.

(c) Si $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ désigne la décomposition en facteurs premiers de n alors

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right) = p_1^{\alpha_1 - 1} \cdots p_k^{\alpha_k - 1}(p_1 - 1) \cdots (p_k - 1)$$

Preuve: (a) les inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$ sont exactement les éléments premiers à n, d'où la formule.

(b) Si a et b sont premier entres eux alors $\mathbb{Z}/ab\mathbb{Z} \simeq \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ et donc $(\mathbb{Z}/ab\mathbb{Z})^* \simeq (\mathbb{Z}/a\mathbb{Z})^* \times (\mathbb{Z}/b\mathbb{Z})^*$, la formule anoncée découlant alors de cet isomorphisme.

(c) Si p est un nombre premier et α un entier. Pour calculer $\varphi(p^\alpha)$, cherchons les entiers de $\{1, \cdots, p^k\}$ qui ne sont pas premier avec p^α. Ce sont exactement les entiers $m = pl$ avec $1 \leq pl \leq p^\alpha$, c'est à dire les entiers $m = pl$ avec $1 \leq l \leq p^{\alpha-1}$. Il y en a donc $p^{\alpha-1}$. On en déduit

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$$

Ecrivons la décomposition en facteurs premiers de n:

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$$

En appliquant les deux résultats précédents, on a donc:

$$\begin{array}{rcl} \varphi(n) & = & \varphi(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) \\ & = & \varphi(p_1^{\alpha_1}) \cdots \varphi(p_k^{\alpha_k}) \\ & = & p_1^{\alpha_1 - 1} \cdots p_k^{\alpha_k - 1}(p_1 - 1) \cdots (p_k - 1) \end{array}$$

ce qui en factorisant donne:

$$\varphi(n) = n \prod_{p|n} (1 - \frac{1}{p})$$

3.3.2 Racines de l'unité

Soit K un corps et $n \geq 1$ un entier. On apppelle racine n-ième de l'unité toute racine du polynôme $X^n - 1$. On note $U_n(K)$ l'ensemble des racines n-ième de l'unité.

Proposition.— *(a) Si $car(K) = 0$ alors il y a exactement n racines de l'unité.*

(b) Si $car(K) = p$ et si $n = p^r m$ avec $p \neq |m$ alors il y a exactement m racines de l'unité et $U_n(K) = U_m(K)$. La multiplicité des racines n-ièmes de l'unité est alors p^r.

Preuve: (a) Le polynôme $X^n - 1$ a une dérivée qui ne s'annulle qu'en 0 ce qui assure que ses racines sont simples.

(b) On a $X^n-1=(X^m-1)^{p^r}$. Le polynôme X^m-1 a une dérivée qui ne s'annulle qu'en 0 ce qui assure que ses racines sont simples. Ainsi le polynôme X^n-1 possède m racines de mmultiplicité p^r.

Proposition.— *L'ensemble $U_n(K)$ est un groupe multiplicatif, c'est un sous-groupe cyclique du groupe $(K^*,.)$.*

Preuve: C'est une conséquence du théorème qui affirme que tout sous-groupe multiplicatif d'un corps est cyclique. Ainsi, si $car(K)=0$ alors $U_n(K)$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$, et si $car(K)=p$ (et si $n=p^rm$ avec $p\neq|m$) alors $U_n(K)=U_m(K)$ est isomorphe à $\mathbb{Z}/m\mathbb{Z}$.

Définition.— *On appelle racine primitive n-ième de l'unité, tout générateur du groupe $U_n(K)$. On note $P_n(K)$ l'ensemble des racines primitives n-ièmes de l'unité.*

Lemme.— *Si n n'est pas divisible par $car(K)$, alors*

$$U_n(K)=\bigsqcup_{d|n}P_d(K)$$

en particulier, $n=\sum_{d|n}\varphi(d)$.

Preuve: Il est clair que pour tout $d|n$, $P_d(K)\subset U_n(K)$. Comme les éléments de $P_d(K)$ sont d'ordre d, pour $d\neq d^{'}$, on a $P_d(K)\cap P_d^{'}=\emptyset$ donc $\bigsqcup_{d|n}P_d(K)=\bigsqcup_{d|n}P_d(K)$ et par suite $\bigsqcup_{d|n}P_d(K)\subset U_n(K)$.
Réciproquement, si $\xi\in U_n(K)$ alors si d désigne l'ordre de ξ on a $d|n$ (théorème de Lagrange) et $\xi\in P_d(K)$. D'où l'inclusion réciproque.

Si n n'est pas divisible par $car(K)$ alors il y a $\varphi(n)=\sharp(\mathbb{Z}/n\mathbb{Z})^*$ racines primitives n-ième de l'unité. Si ξ_1 et ξ_2 sont des racines primitives n-ièmes de l'unité, alors il existe $a\in(\mathbb{Z}/n\mathbb{Z})^*$ tel que $\xi_2=\xi_1^a$ et réciproquement, pour tout $a\in(\mathbb{Z}/n\mathbb{Z})^*$ ξ_1^a est une racine primitive n-ième de l'unité.

3.3.3 Polynômes cyclotomiques

Définition.— *Soit K un corps et n un entier qui n'est pas divisible par $car(K)$. On appelle n-ième polynôme cyclotomique de K le polynôme*

$$\Phi_{n,K}(X)=\prod_{\xi\in P_n(K)}(X-\xi)$$

Quand $K=\mathbb{Q}$, on note plus simplement $\Phi_{n,K}=\Phi_n$.

Le polynôme $\Phi_{n,K}$ est donc de degré φ_n. Soit A un anneau factoriel et $P\in A[X]$. On appelle contenu de P l'élément $c(P)$ égal au p.g.c.d des coefficients de P.

Lemme de Gauss.— *Soit A un anneau factoriel, si $P,Q\in A[X]$ alors $c(PQ)=c(P)c(Q)$.*

Preuve: Supposons que $c(P)=c(Q)=1$ et $c(PQ)\neq1$. Soit p un élément irréductible de A tel que p divise tous les coefficients de PQ. Considérons alors l'anneau quotient:

$$B=A/pA$$

B est un anneau intègre, donc $B[X]$ l'est aussi. Soit ω l'homomorphisme d'anneau de $A[X]$ sur $B[X]$ provenant de la surjection canonique de A sur B. On a $\omega(PQ)=$

$\omega(P)\omega(Q) = 0$, mais comme $B[X]$ est intègre, on a donc soit $\omega(P) = 0$ soit $\omega(Q) = 0$. Les deux cas contredisent l'hypothèse $c(P) = c(Q) = 1$.

Prenons maintenant P et Q de contenu quelconque. En factorisant, on écrit $P(X) = c(P)P_1(X)$ et $Q(X) = c(Q)Q_1(X)$ où P_1 et Q_1 sont des polynômes de $A[X]$ de contenu 1. On a alors:

$$c(PQ) = c(c(P)c(Q))c(P_1)c(Q_1) = c(P)c(Q)$$

Corollaire.— *(a) Soit A un anneau factoriel et K son corps de fractions. Soit $P, Q \in A[X]$ sont deux polynômes tels que $P|Q$ dans $K[X]$. Si $c(P) = c(Q)$ alors $P|Q$ dans $A[X]$.*

(b) Si P est un polynôme normalisé non nul de $\mathbb{Z}[X]$ et que Q et R sont deux polynômes de $\mathbb{Q}[X]$ tels que Q soit normalisé et tels que $P(X) = Q(X)R(X)$ alors Q et R sont tous deux dans $\mathbb{Z}[X]$.

Preuve: (a) Par hypothèse, il existe un polynôme $R(X) \in K[X]$ tel que $P = QR$. En réduisant au même dénominateur, il existe donc $\alpha \in A$ et $R_1 \in A[X]$ tel que $R(X) = \dfrac{1}{\alpha}R_1(X)$. On a donc:

$$\alpha P(X) = Q(X)R_1(X)$$

en appliquant la formule précédente sur le contenu, on trouve alors:

$$\alpha c(P) = c(Q)c(R_1)$$

Comme $c(P) = c(Q)$, $\alpha = c(R_1)$ et ainsi $R(X) \in A[X]$.

(b) En regardant le terme de plus haut de degré de QR, on déduit immédiatement que R est aussi normalisé. En réduisant au même dénominateur chacun des polynômes Q et R, on écrit $Q(X) = \dfrac{1}{\alpha}Q_1(X)$ et $R(X) = \dfrac{1}{\beta}R_1(X)$ avec $(\alpha, \beta) \in \mathbb{N}^2$ et Q_1 et R_1 des polynômes de $\mathbb{Z}[X]$. Les termes de plus haut degré de Q_1 et R_1 sont respectivement α et β. Par conséquent $c(Q_1) \leq \alpha$ et $c(R_1) \leq \beta$, comme

$$\alpha\beta P(X) = Q_1(X)R_1(X)$$

en appliquant le lemme de Gauss, on a:

$$\alpha\beta = c(Q_1)c(R_1)$$

cette égalité ne peut-être alors réalisée que si $c(Q_1) = \alpha$ et $c(R_1) = \beta$, ainsi Q et R sont bien à coefficients entiers.

Proposition.— *Soit $n \in \mathbb{N}^*$.*

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

(b) $\Phi_n(X) \in \mathbb{Z}[X]$.

(c) $\Phi_n(X)$ est irréductible.

Preuve: (a) Provient de la formule $U_n(K) = \bigsqcup_{d|n} P_d(K)$.

(b) Montrons que $\Phi_n(X) \in \mathbb{Z}[X]$ par récurrence sur n.

Pour $n = 1$, c'est clair.

Supposons que pour $n - 1 \geq 1$, on ait $\Phi_k(X) \in \mathbb{Z}[X]$ pour tout $k = 1, \cdots, n-1$. On a alors

$$\Phi_n(X) = \frac{X^n - 1}{\prod_{d|n, d\neq n} \Phi_d(X)} \in \mathbb{Q}[X]$$

Le dénominateur de ce rapport est, par hypothèse de récurrence, dans $\mathbb{Z}[X]$, comme $X^n - 1$ et $\prod_{d|n,d\neq n} \Phi_d(X)$ sont normalisés, on en déduit d'après ce qui précède que $\Phi_n(X) \in \mathbb{Z}[X]$.

(c) Soit ξ une racine primitive n-ième de l'unité et P son polynôme minimal. Supposons que $\Phi_n(X)$ ne soit pas égal à P. On écrit donc

$$\Phi_n(X) = P(X)Q(X) \text{ avec } Q(X) \in \mathbb{Q}[X]$$

Comme $\Phi_n(X)$ et $P(X)$ sont normalisés, il s'ensuit (corollaire précédent) que P et Q sont dans $\mathbb{Z}[X]$, puisque $\Phi_n(X) \in \mathbb{Z}[X]$. Soit p un nombre premier ne divisant pas n. Supposons que ξ^p ne soit pas racine de P, comme $\Phi_n(\xi^p) = 0$, on a $Q(\xi_p) = 0$. Posons $H(X) = Q(X^p)$, on a $H(\xi) = 0$, donc H est un multiple de P, donc on peut écrire $H(X) = P(X)K(X)$ avec $K(X) \in \mathbb{Q}[X]$. Toujours d'après le corollaire précédent, on a $K(X) \in \mathbb{Z}[X]$.

On regarde maintenant $\overline{\Phi_n}, \overline{P}, \overline{Q}, \overline{H}, \overline{K}$ la réduction modulo p des polynômes Φ_n, P, Q, H, K. Puisque nous sommes en caractéristique p, on a:

$$\overline{H} = \overline{Q}(X^p) = \overline{Q^p}$$

Soit $\Psi \in \mathbb{F}_p[X]$ un facteur irréductible de $\overline{P}$, comme $\overline{H} = \overline{PK}$, Ψ divise $\overline{H}$ et donc $\overline{Q}$. Maintenant $\overline{\Phi_n} = \overline{PQ}$, donc Ψ^2 divise $\overline{\Phi_n}$, et par conséquent $X^n - \overline{1}$. Ainsi $X^n - \overline{1}$ admet une racine double, sa dérivée admet donc la même racine. Or $\left(X^n - \overline{1}\right)' = nX^{n-1}$ est soit nul, soit n'admet que 0 pour racine. Le premier cas est exclus car p ne divise pas n, le deuxième aussi puisque 0 n'est pas racine de $X^n - \overline{1}$.

Nous venons donc de prouver que pour tout nombre premier p ne divisant pas n, $P(\xi^p) = 0$. Prenons maintenant un entier $k = 1, \cdots, n$ premier avec n. On écrit $k = p_1.\cdots.p_l$ avec $p_1, \cdots, p_l$ des nombres premiers (non forcément distincts deux à deux). Il est clair qu'aucun des p_i ne divise n, on a donc $P(\xi^{p_1}) = 0$. Maintenant, ξ^{p_1} est une racine primitive n-ième de l'unité, si on applique à nouveau le raisonnement précédent, on trouve que pour tout p ne divisant pas n, on a $P((\xi^{p_1})^p) = 0$. Donc $P(\xi^{p_1 p_2}) = 0$, de proche en proche, on prouve finalement que $P(\xi^k) = 0$. Donc toutes les racines primitives n-ièmes de l'unité sont racine de P. On a bien $\Phi_n(X) = P(X)$.

Φ_n est donc automatiquement irréductible, puisque c'est le polynôme minimal d'un nombre algébrique.

3.3.4 Corps cyclotomiques

3.4 Extensions kummérienne

3.5 Résolubilité par radicaux

3.5.1 Extensions radicales

Définition.— *Une extension L/K est dite par radicaux ou radicale s'il existe une tour finie d'extensions*

$$K = K_0 \subset K_1 \subset \cdots \subset K_m = L$$

telle que pour tout $i = 0, \cdots n-1$ *il existe* $a_i \in K_{i+1}$ *tel que* $K_{i+1} = K_i(a_i)$ *et* $a_i^{n_i} \in K_i$ *pour un certain entier* $n_i \in \mathbb{N}^*$.

Un polyôme $P \in K[X]$ *est dit résoluble par radicaux, s'il existe une extension radicale* L/K *telle que* L *contienne le corps de décomposition de* P.

• Une extension radicale est bien sur une extension finie. En reprenant les notations de la définition, on voit que si L/K est radicale, alors $[L : K] \leq n_0.n_1 \cdots .n_{m-1}$.
• Si M/L et L/K sont radicales, on voit que M/K l'est aussi. La notion d'extensions radicales est donc transitive.
• Toute extension cyclotomique est radicale
• Si K désigne un corps de caractéristique $\neq 2$, alors tout polynôme de degré 2 à coefficients dans K est résoluble par radicaux.

Lemme.— *Soit* L/K *une extension radicale et* $\widetilde{L}$ *la clôture normale de* L. *L'extension* $\widetilde{L}/K$ *est radicale.*

Preuve :

3.5.2 Résolubilité par radicaux

Dans tout ce paragraphe, les corps considérés seront supposés être de caractéristique 0.

Proposition.— *Soit* L/K *une extension galoisienne finie,* n *un entier non nul et* ξ_n *une racine primitive* n*-ième de l'unité. Les propositions suivantes sont équivalentes :*

i) $Gal(L/K)$ *est résoluble,*

ii) $Gal(L(\xi_n)/K(\xi_n))$ *est résoluble,*

iii) $Gal(L(\xi_n)/K)$ *est résoluble.*

Preuve : *iii)* $\Rightarrow$ *i)* et *ii)* Les groupes $Gal(L/K)$ et $Gal(L(\xi_n)/K(\xi_n))$ sont respectivement quotient et sous-groupe de $Gal(L(\xi_n)/K)$, donc sont résolubles.

ii) $\Rightarrow$ *iii)* $Gal(L(\xi_n)/K(\xi_n))$ est un sous-groupe résoluble de $Gal(L(\xi_n)/K)$. Par ailleurs, $Gal(K(\xi_n)/K)$ est abélien donc résoluble et comme le groupe quotient $Gal(L(\xi_n)/K)/Gal(L(\xi_n)/K(\xi_n))$ est isomorphe à $Gal(K(\xi_n)/K)$, on en déduit que $Gal(L(\xi_n)/K)$ est résoluble.

i) $\Rightarrow$ *ii)* Le groupe $Gal(L/K(\xi_n))$ est un sous-groupe de $Gal(L/K)$, donc est résoluble. Considérons l'application

$$\begin{array}{ccc} Gal(L(\xi_n)/K(\xi_n)) & \longrightarrow & Gal(L/K(\xi_n)) \\ \sigma & \longmapsto & \sigma_{|L} \end{array}$$

Cette application est un morphisme injectif de groupe, donc $Gal(L(\xi_n)/K(\xi_n))$ est isomorphe à un sous-groupe de $Gal(L/K(\xi_n))$ et est donc résoluble.

Proposition.— *Soit* L/K *une extension galoisienne radicale. Le groupe* $Gal(L/K)$ *est résoluble.*

Preuve :

Théorème.— *Un polynôme* $P \in K[X]$ *est résoluble par radicaux si et seulement si le groupe de Galois de* P *sur* K *est résoluble.*

Preuve : Supposons que P soit résoluble par radicaux. Notons D le corps de décomposition de P. Il existe donc une extension radicale L/K telle que $D \subset L$. Si $\widetilde{L}$ désigne la clôture galoisienne de L, alors $\widetilde{L}/K$ est radicale. La proposition précédente affirme alors que $Gal(\widetilde{L}/K)$ est un groupe résoluble, mais comme $Gal(D/K)$ est un quotient de $Gal(\widetilde{L}/K)$, on en déduit que $Gal(D/K)$ est résoluble.

Réciproquement, supposons que $Gal(D/K)$ soit résoluble.