Théorie de Galois

texte rédigé par MM. ALZINGRE et GUILLOTIN
d'après trois exposés de P. GABRIEL devant la régionale de Strasbourg

A. Extension de corps.

I. Extension de corps.

Pour simplifier, nous appelons *corps* toute partie K de l'ensemble $\mathbb{C}$ des nombres complexes telle qu'on ait :

i) $K \supset \mathbb{Q}$ (ensemble des nombres rationnels).

ii) Si $(x, y) \in K^2$, alors $x+y$ et $x.y$ appartiennent à K.

iii) Si $x \in K$ et $x \neq 0$, alors $x^{-1} \in K$.

Si K et L sont deux tels corps et si $K \subset L$, on dit que K est un *sous-corps* de L, ou que L est une *extension* de K. On note comme d'habitude $\mathbb{R}$ l'ensemble des nombres réels : c'est un sous-corps de $\mathbb{C}$ et une extension de $\mathbb{Q}$.

Autres exemples.

1) $K = \mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} \mid (a, b) \in \mathbb{Q}^2\}$.

2) Soient $x_1, \ldots, x_n$ des nombres complexes et K un corps. L'ensemble des nombres complexes de la forme $\dfrac{P(x_1, \ldots, x_n)}{Q(x_1, \ldots, x_n)}$, où P et Q parcourent les polynômes de n variables à coefficients dans K tels que $Q(x_1, \ldots, x_n) \neq 0$ forment une extension de K qu'on note $K(x_1, \ldots, x_n)$ et qu'on dit *engendrée par* $x_1, \ldots, x_n$.

Définition.

Si le corps L *est une extension du corps* K ($K \subset L \subset \mathbb{C}$), *on dit qu'une suite* $l_1, \ldots, l_n$ *dans* L *est une* base de L sur K *si tout* $l \in L$ *s'écrit, d'une manière et d'une seule, sous la forme :*

$$l = a_1 l_1 + \ldots + a_n l_n \qquad \text{avec} \qquad a_i \in K \qquad \text{et} \qquad l_i \in L$$

L *est un espace vectoriel sur* K *de dimension finie n. On note* $n = [L : K]$.

Exemple. — $\mathbb{R} \subset \mathbb{C}$ base $\{1, i\}$; $\quad \mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$ base $\{1, \sqrt{2}\}$.

Remarque. — Si $[L : K] = 1$ alors $L = K$.

Proposition.

L étant une extension de dimension finie de K *et* M *une extension de dimension finie de* L, *alors* M *est une extension de dimension finie de* K *et l'on a:*

$$[M : K] = [M : L] \times [L : K]$$

base de M *sur* L : $\{m_1, \ldots, m_p\}$,
base de L *sur* K : $\{l_1, \ldots, l_n\}$.

On se propose de montrer que les $l_i m_j$ constituent une base de M sur K. Soit $m \in M$:

$$m = a_1 m_1 + \ldots + a_p m_p \qquad a_i \in L$$

Or
$$a_i = a_{i1} l_1 + \ldots + a_{in} l_n \qquad a_{ij} \in K$$

$$m = \sum_{i=1}^{p} a_i m_i = \sum_i (\sum_j a_{ij} l_j) = \sum_{i,j} a_{ij} l_j m_i$$

La décomposition est unique. Soit $m = \sum_{i,j} a_{ij} l_j m_i = \sum_{i,j} b_{ij} l_j m_i$.

L'unicité du développement d'un élément de L sur K et d'un élément de M sur L entraîne $\sum_j a_{ij} l_j = \sum_j b_{ij} l_j$, puis $a_{ij} = b_{ij}$.

Remarque :

Si $\begin{cases} [N : K] = [L : K], \\ \text{et} \\ K \subset L \subset N \end{cases}$ alors $[N : L] = 1$ et $N = L$

II. Nombre algébrique.

Définition.

Soit $K \subset \mathbb{C}$ *et* $x \in \mathbb{C}$. *On dit que* x est algébrique sur K *s'il existe un polynôme* P *non identiquement nul, à coefficients dans* K, *admettant* x *pour racine :*

$$P = X^n + p_{n-1} X^{n-1} + \ldots + p_0, \qquad p_i \in K$$
$$P(x) = 0$$

(Les polynômes P, Q, M considérés dans la suite seront unitaires, c'est-à-dire tel que le terme de plus haut degré ait un coefficient égal à 1). Soient P et Q deux tels polynômes de degré minimum. P—Q est un polynôme à coefficients dans K, s'annulant pour x et de degré inférieur à celui de P et de Q. Les deux polynômes P et Q sont donc identiques d'où,

Définition.

On appelle polynôme minimal *de x sur* K *le polynôme unitaire, à coefficients dans* K, *admettant x pour racine et de degré minimum.*

Caractérisation du polynôme minimal.

Les propositions suivantes sont équivalentes :

a) M *est le polynôme minimal de x sur* K ;

b) M *est un polynôme irréductible sur* K, *admettant x pour racine.*

1) Si $M(x) = 0$ et $M = R.S$, alors M n'est pas minimal, car

$$M(x) = 0 = R(x).S(x).$$

Un des polynômes R ou S s'annule pour x et est de degré inférieur à M. Donc M n'est pas minimal et $a \Rightarrow b$.

2) Si $M(x) = 0$ et si M n'est pas minimal, alors M n'est pas irréductible. Soit en effet N le polynôme minimal de x sur K ; par division de M, on a :

$$M = N.A + R \qquad M(x) = N(x).A(x) + R(x)$$
$$M(x) = 0,\ N(x) = 0, \qquad \text{donc} \qquad R(x) = 0$$

R est un polynôme à coefficients dans K, nul pour x et de degré inférieur à celui du polynôme minimal N, donc $R \equiv 0$ et $M = N.A$. Donc : $b \Rightarrow a$.

Remarque :

1) Si $P(x) = 0$, P est divisible par le polynôme minimal de x sur K.

2) Un polynôme irréductible sur K est minimal pour chacune de ses racines.

III. Calcul de la dimension sur K d'une extension K(x).

Théorème.

Si n est le degré du polynôme minimal de x sur K, *l'extension* K(x) admet pour base sur K les nombres $1, x, \ldots, x^{n-1}$.

On se propose de montrer que tout $z \in K(x)$ est une combinaison linéaire unique des éléments de la base :

$$z = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1} \qquad a_i \in K$$

Unicité de la combinaison linéaire :

$$z = a_0 + \ldots + a_{n-1}x^{n-1} = A(x) = b_0 + \ldots + b_{n-1}x^{n-1} = B(x)$$

d'où

$$(a_0 - b_0) + \ldots + (a_{n-1} - b_{n-1})x^{n-1} = 0$$

Le polynôme A—B à coefficients dans K, de degré n—1, admet x pour racine. Or le degré du polynôme minimal est n, donc A ≡ B.

Existence d'une combinaison linéaire.

Un élément z de K(x) est de la forme $\frac{A(x)}{B(x)}$ où A et B sont des polynômes à coefficients dans K. On se propose de montrer que z est un élément de K', si l'on pose $K' = \{a_0+\ldots+a_{n-1}x^{n-1} \mid a_i \in K\}$.

1) *Si* $z = A(x)$, *alors* $z \in K'$.
Soit M le polynôme minimal de x.
Si $d^0A < n$ évident.
Si $d^0A > n$. On effectue la division $A = MC+R$, $d^0R < n$; d'où $A(x) = M(x).C(x)+R(x)$. Or $M(x) = 0$. Par suite $A(x) = R(x) \in K'$.

2) *Si* $(a, b) \in K'$, *alors* $a.b \in (K')^2$.
soit $a = A(x)$, $b = B(x)$, $d^0A \leq n-1$, $d^0B \leq n-1$.
$a.b = A(x)B(x) = (A.B)(x)$.
D'après le 1), $(A.B)(x) \in K'$.

3) *Si* $a \in K'$, *alors* $a^{-1} \in K'$ $(a \neq 0)$.
K' est un sous-espace vectoriel de $\mathbb{C}$ sur K de dimension n. On considère l'endomorphisme f_a de K' tel que,

$$f_a : K' \to K'$$
$$b \to a.b$$

f_a est un endomorphisme injectif d'un espace vectoriel de dimension finie, donc f est bijectif.
Le nombre 1 est atteint et il existe b tel que $a.b = 1$; l'inverse de a appartient à K'.

4) *Si* $z = \frac{A(x)}{B(x)} \in K(x)$, *alors* $z \in K'$, *car* $z = A(x).\left(\frac{1}{B(x)}\right)$.

D'après 3), $\frac{1}{B(x)} \in K'$.

D'après 2), $A(x).\left(\frac{1}{B(x)}\right) \in K'$, *donc* $K(x) = K'$.

IV. Exemples.

1) Si un polynôme M du 2e degré à coefficients dans K n'a pas de racines dans K, M est le polynôme minimal de chacune des racines x', x''.

$$M = X^2+bX+c \qquad (b, c) \in K^2, \qquad M(x) = 0, \ x \in \mathbb{C}, \ x \notin K$$

En effet, si M n'est pas le polynôme minimal de x, il existe un polynôme P de degré 1 qui annule x :

$$P = X - a,\ a \in K \qquad P(x) = x - a = 0;\ \text{ or } x \notin K \text{ et } a \in K$$

ce qui donne une contradiction.

La dimension de $K(x')$ sur K est 2; la base est $\{1, x\}$.

$$K(x) = \{a + bx \mid a, b \in K\}$$

2) Si un polynôme M du 3e degré à coefficients dans K n'a pas de racines dans K, M est le polynôme minimal de chacune des racines x', x'', x'''.

$$M = X^3 + bX^2 + cX + d \qquad (b, c, d) \in K^3, \qquad M(x') = 0\ x' \in \mathbb{C}\ x' \notin K.$$

Si M n'est pas le polynôme minimal, M est un produit de deux polynômes R, S à coefficients dans K de degrés strictement inférieurs à 3, $M = R.S$.

$$R = X - \alpha \qquad S = X^2 + \beta X + \gamma \qquad M = (X - x')(X - x'')(X - x''')$$

R est l'un des facteurs; α est égale à l'une des racines x', x'', x'''; or $\alpha \in K$ et x', x'', x''' n'appartiennent pas à K.

La dimension de $K(x')$ sur K est 3 et $\{1, x', x'^2\}$ est une base

$$K(x') = \{a + bx' + cx'^2 \mid a, b, c \in K\}$$

3) Cas particuliers :

$K = \mathbb{Q}$, $x' = \sqrt[3]{2}$, $M = X^3 - 2$, M est un polynôme à coefficients rationnels, sans racines rationnelles.

$$[Q(\sqrt[3]{2}) : Q] = 3 \qquad \mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4}\ \ (a, b, c) \in \mathbb{Q}^3\}$$

V. Application au problème de la duplication du cube.

Le segment de longueur unité étant donné, on se propose de montrer qu'il est impossible de construire le segment de longueur $\sqrt[3]{2}$, avec la règle et le compas, sans faire de choix arbitraire.

a) On peut, à la règle et au compas, construire les segments de longueur n, $\frac{1}{n}$, $\frac{m}{n}$ et les points à coordonnées rationnelles. On peut également construire les intersections de droites et de cercles faisant intervenir des longueurs rationnelles :

$$(x - a)^2 + (y - b)^2 = r^2 \qquad (a, b, r, m - p \in \mathbb{Q}^4$$
$$y = mn + p$$

Les coordonnées x, y, x', y' des points d'intersection sont données par l'équation aux abscisses (E) $(x-a)^2+(mn+p-b)^2 = r^2$ et l'équation $y = mn+p$.

Les nombres x, y, x', y' appartiennent à un corps $K_1 = \mathbb{Q}(x)$ où x est l'une des racines de (E). Si x est rationnel, $K_1 = \mathbb{Q}$; sinon K_1 est de dimension 2 sur $\mathbb{Q}$.

On peut maintenant construire les points de coordonnées ξ, η appartenant à K_1. Les points d'intersection de droites et de cercles utilisant des segments de mesure appartenant à K_1 ont des coordonnées appartenant à un corps K_2 de dimension 2 sur K_1.

On peut poursuivre cette construction :

$$\mathbb{Q} \subset K_1 \subset K_2, \ldots, \subset K_p \subset K_{p+1}, \ldots$$

b) Soit L un sous-corps de $\mathbb{R}$. Dire que pour tout $z \in L$, on peut construire, à la règle et au compas, un segment de longueur z, c'est dire qu'il existe une suite décroissante de corps

$$K_n = L \supset K_{n-1} \subset \ldots \supset K_1 \supset K_0 = \mathbb{Q}$$

tel que $[K_{i+1} : K_i] = 2$.

La dimension de L sur $\mathbb{Q}$ est : $[L : \mathbb{Q}] = 2^n$.

c) En particulier, pour pouvoir construire un segment de longueur $\sqrt[3]{2}$, il devrait exister un tel corps L contenant $\mathbb{Q}(\sqrt[3]{2})$.

Alors :
$$\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) \subset L$$
$$[L : Q] = [L : \mathbb{Q}(\sqrt[3]{2})] \times [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$$
$$[L : \mathbb{Q}] = 2^n [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3.$$

Si L existait, 3 devrait diviser 2^n.

B. Homomorphisme d'une extension de corps.

I. Homomorphisme de corps.

Définition.

Soient K *et* L *deux corps. Une application* σ *de* K *dans* L *est un homomorphisme si :*

i) $\sigma(x+y) = \sigma(x)+\sigma(y)$.

ii) $\sigma(x.y) = \sigma(x).\sigma(y)$.

iii) $\sigma(1) = 1$.

σ est un isomorphisme, si σ est une bijection.

σ est un automorphisme de K, si K = L et si σ est une bijection.

Remarque. — Un homomorphisme σ est toujours injectif.

Si $x \in K$ et $x \neq 0$ alors $x^{-1} \in K$ et $\sigma(x.x^{-1}) = \sigma(1) = 1$

$$\sigma(x.x^{-1}) = \sigma(x).\sigma(x^{-1}) = 1$$

Donc : $$x \neq 0 \Rightarrow \sigma(x) \neq 0 \quad \text{et} \quad [\sigma(x)]^{-1} = \sigma(x^{-1}).$$

De même, $\sigma(x-y) = \sigma(x)-\sigma(y)$.

Si $x-y \neq 0$, on a donc :

$$\sigma(x) \neq \sigma(y).$$

Exemples.

a) $K = L = \mathbb{Q}(\sqrt{2})$ $\quad \sigma(a+b\sqrt{2}) = a-b\sqrt{2}$ $\quad (a, b) \in \mathbb{Q}^2$.

b) $K = L = \mathbb{C}$ $\quad \sigma(a+ib) = a-ib$ $\quad (a, b) \in \mathbb{R}^2$.

Si $x \in \mathbb{R}$, $\sigma(x) = x$.

Définition.

Si k est un sous-corps de K *et de* L *qui reste invariant élément par élément par l'homomorphisme* σ, *on dit que* σ est un k-homomorphisme de K dans L :

$$\forall x \in k, \quad \sigma(x) = x.$$

Dans l'exemple *b*), σ est un $\mathbb{R}$-homomorphisme.

II. Homomorphisme d'une extension K(x) dans $\mathbb{C}$.

Définition.

On appelle nombre conjugué *d'un nombre x algébrique sur* K *une racine quelconque y du polynôme minimal* M *de x sur* K.

On considère les extensions K(x) et K(y),

$$K(x) = \{a_0+\ldots+a_{n-1}x^{n-1} \mid a_i \in K\}; \quad K(y) = \{b_0+\ldots+b_{n-1}y^{n-1}\} b_i \in K$$

et l'application σ, $\quad \sigma : K(x) \to K(y)$.

$$a_0+a_1x+\ldots+a_{n-1}x^{n-1} \to a_0+a_1y+\ldots+a_{n-1}y^{n-1}.$$

Proposition.

σ *est un* K-*isomorphisme de* K(x) *sur* K(y).

1) σ est une bijection.

2) σ est un homomorphisme.

$$\sigma(1) = 1 \qquad \sigma(a+b) = \sigma(a)+\sigma(b)$$

$$\sigma(a.b) = \sigma(a).\sigma(b) \text{ : on a, en effet}$$

$\left.\begin{array}{l} a = A(x) \\ b = B(x) \end{array}\right\}$ A et B étant des polynômes à coefficients dans K de degré $<n$.

$$a.b = (A.B)(x) \qquad A.B = M.Q+R \qquad d^0R \leq n-1$$

$$(A.B)(x) = M(x)Q(x)+R(x); \text{ or } M(x) = 0$$

d'où $a.b = R(x)$

et $\sigma(a.b) = R(y)$

de même $\sigma(a).\sigma(b) = A(y).B(y) = R(y)$ $\Big]$ d'où $\sigma(a.b) = \sigma(a).\sigma(b)$.

3) σ est un K-isomorphisme. $\sigma(a_0) = a_0$.

4) $\sigma(x) = y$.

Corollaire.

Si n est le degré du polynôme minimal de x sur K, *il y a n* K-*homomorphismes de* K(x) *dans* $\mathbb{C}$; *les images de x par ces* K-*homomorphismes sont les nombres conjugués de x sur* K.

a) Pour tout y conjugué de x, il existe un K-homomorphisme associant y à x. Le nombre des K-homomorphismes de K(x) dans $\mathbb{C}$ est donc supérieur ou égal au nombre des conjugués de x sur K.

b) Si σ est un K-homomorphisme de K(x) dans $\mathbb{C}$, alors $\sigma(x)$ est un nombre conjugué de x.

Soit en effet $M = m_0+\ldots+X^n$ le polynôme minimal de x, $m_i \in K$

$$M(x) = 0 \quad \text{entraîne} \quad \sigma(M(x)) = 0$$

$$\sigma(x^n+m_{n-1}x^{n-1}+\ldots+m_0) = 0$$

$$\sigma(x)^n+\sigma(m_{n-1}).\sigma(x)^{n-1}+\ldots+\sigma(m_0) = 0$$

Or $m_i \in K$ donc $\sigma(m_i) = m_i$.

$\sigma(x)$ est donc une racine du polynôme minimal M.

Tout nombre z étant de la forme $z = a_0+\ldots+a_{n-1}x^{n-1}$, σ est défini par la valeur $\sigma(x)$.

Le nombre des K-homomorphismes de K(x) dans $\mathbb{C}$ est donc au plus égal au nombre de conjugués de x.

c) Le nombre des racines du polynôme minimal M est égal au degré de M qui n'a donc que des racines simples.

Si M admettait des racines multiples, M et M′ auraient des racines communes et le P.G.C.D. de M et de M′ serait un polynôme à coefficients dans K de degré supérieur ou égal à 1. Donc le P.G.C.D. diviserait M et M′ ne serait pas irréductible.

On a établi en *a*) et *b*) que le nombre des K-homomorphismes de K(x) sur $\mathbb{C}$ est égal au nombre des racines de M; le *c*) entraîne le corollaire.

Exemple : $K = \mathbb{Q}$ $\quad x = \sqrt[3]{2}$ $\quad M = X^3 - 2$

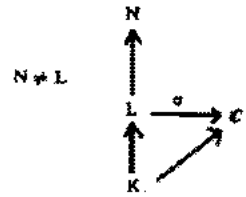
$\sqrt[3]{2}$ à trois conjugués $\quad \sqrt[3]{2}, \quad j\sqrt[3]{2}, \quad j^2\sqrt[3]{2}$

Il existe donc trois $\mathbb{Q}$-homomorphismes dans $\mathbb{C}$ du corps engendré par $\sqrt[3]{2}$ et $\mathbb{Q}$. A savoir : $\sigma_1(\sqrt[3]{2}) = \sqrt[3]{2}, \quad \sigma_2(\sqrt[3]{2}) = j\sqrt[3]{2}, \quad \sigma(\sqrt[3]{2}) = j^2\sqrt[3]{2}$.

III. Homomorphisme d'une extension.

Théorème.

Si L *est une extension de* K, N *une extension de* L, *la dimension de* N *sur* K *étant finie, alors tout* K*-homomorphisme de* L *dans* $\mathbb{C}$ *peut être prolongé à* N.



La démonstration procède par récurrence sur la dimension de N sur L.

① Si $[N : L] = 1$, c'est évident.

② On suppose que le théorème est vrai pour

$$[N : L] < r$$

Soit N une extension de L telle que $[N : L] = r$.

Il existe un $x \in N$ qui n'appartient pas à L. Soit M le polynôme minimal de x sur L.

Le transformé de M par σ est désigné par M^σ,

$$M = X^n + \ldots + m_0 \qquad m_i \in L$$
$$M^\sigma = X^n + \sigma(m_{n-1})X^{n-1} + \ldots + \sigma(m_0).$$

Les coefficients de M^σ appartiennent à $\sigma(L)$. On montre que M^σ est un polynôme irréductible : soient $M^\sigma = R.S$ et $r = \sigma^{-1}$; comme σ est injectif, on aurait $(M^\sigma)^r = M = R^r.S^r$, donc M ne serait pas irréductible.

M^σ est donc le polynôme minimal d'une de ses racines y.

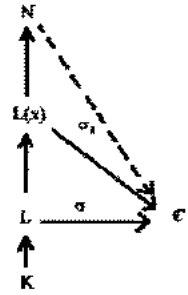
On considère les corps $L(x)$ et $(\sigma L)(y)$,

$$L(x) = \{a_0 + \ldots + a_{n-1}x^{n-1} | a_i \in L\}$$
$$(\sigma L)(y) = \{b_0 + \ldots + b_{n-1}y^{n-1} | b_i \in \sigma(L)\}$$

On définit l'application σ_1 de $L(x)$ dans $(\sigma L)(y)$:

$$\sigma_1 : \quad L(x) \to (\sigma L)(y)$$
$$a_0 + \ldots + a_{n-1}x^{n-1} \mapsto \sigma(a_0) + \ldots + \sigma(a_{n-1})y^{n-1}$$

σ_1 est un isomorphisme de $L(x)$ sur $(\sigma L)(y)$ qui laisse K invariant et qui coïncide avec σ sur L.

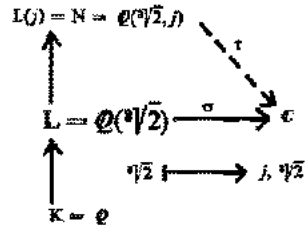


Or, $[N : L(x)] = \dfrac{[N : L]}{[L(x) : L]} < [N : L] = r.$

Le K-homomorphisme σ_1 de $L(x)$ dans $\mathbb{C}$ se prolonge à N, la dimension de N sur $L(x)$ étant inférieure à r.

Exemple :

σ est un $\mathbb{Q}$-homomorphisme. On choisit $x = j$ dont le polynôme minimal est $M = X^2+X+1$ (irréductible dans L).



Ici $M^\sigma = M$ car les coefficients de M sont rationnels.
Donc σ se prolonge à N.

— Base de L sur $\mathbb{Q}$:

$$M_1 = X^3 - 2 \qquad [L : \mathbb{Q}] = 3 \qquad \{1, \sqrt[3]{2}, \sqrt[4]{4}\}$$

— Base de N sur L :

$$M_2 = X^2 + X + 1 \qquad [N : L] = 2 \qquad \{1, j\}$$

— Base de N sur $\mathbb{Q}$:

$[N : R] = 6$ $\quad 1, j, \sqrt[3]{2}, \sqrt[3]{4}, j\sqrt[3]{2}, j\sqrt[3]{4}$, c'est-à-dire : $\{1, \sqrt[3]{2}, \sqrt[3]{4}, j, j\sqrt[3]{2}, j\sqrt[3]{4}\}$

L'image par τ de j sera j ou j^2. On peut choisir σ de trois manières et τ de deux manières. Il existe donc six $\mathbb{Q}$-homomorphismes de N dans $\mathbb{C}$.

Corollaire 1.

Si N *est une extension de* K *de dimension* n, *il y a* n K-*homomorphismes de* N *dans* $\mathbb{C}$.

En effet, cela est clair lorsque $N = K$. Supposons donc le corollaire démontré pour les extensions de dimensions $< n$ et soit $x \in N$, $x \notin K$. Si $r = [K(x) : K]$, nous avons vu qu'il y avait r K-homomorphismes σ de $K(x)$ dans $\mathbb{C}$; soient ρ et τ deux extensions de σ à N (de telles extensions existent d'après notre théorème) : l'application $x \to \rho^{-1}\tau(x)$ est alors un $K(x)$-homomorphisme ν de N dans $\mathbb{C}$, et l'on a $\tau = \rho\nu$. Cette formule met en correspondance biunivoque les prolongements τ de σ à N et les $K(x)$-homomorphismes ν de N dans $\mathbb{C}$.

Par hypothèse de récurrence, il y a $[N : K(x)]$ homomorphismes ν. Tout σ a donc $[N : K(x)]$ prolongements; comme il y a $[K(x) : K]$ homomorphismes σ, le corollaire résulte de la formule :

$$[N : K(x)] \times [K(x) : K] = [N : K].$$

Corollaire 2.

Si N *est une extension de dimension* n *sur* K, *il existe un élément* x *de* N *tel que* $N = K(x)$.

Soit $\{x_1, \ldots, x_n\}$ une base de N sur K. Tout élément a de N s'écrit d'une manière et d'une seule :

$$a = a_1x_1 + \ldots + a_nx_n, \qquad a_i \in K$$

N étant de dimension n, d'après le corollaire 1, il existe n K-homomorphismes de N dans $\mathbb{C}$: $\sigma_1, \ldots, \sigma_n$.

$$\sigma_i(a) = a_1\sigma_i(x_1) + \ldots + a_n\sigma_i(x_n) = L_i(a_1, \ldots, a_n).$$

Les L_i sont des formes linéaires à coefficients complexes. Les n K-homomorphismes étant distincts, si i est différent de j, il existe un élément a de N tel que $\sigma_i(a) \neq \sigma_j(a)$; donc les formes L_i et L_j sont distinctes.

Le polynôme $\Delta = \prod_{i<j} (L_i - L_j)$ est un polynôme à n variables a_i, à coefficients complexes et non identiquement nul. Il existe donc une suite de nombres $\alpha_1, \ldots, \alpha_n$ rationnels (ou appartenant à K) telle que :

$$\Delta(\alpha_1, \ldots, \alpha_n) \neq 0 \qquad (1)$$

En posant $\alpha = \alpha_1 x_1 + \ldots + \alpha_n x_n$, d'après (1) si i est différent de j, $L_i(\alpha_1, \ldots, \alpha_n)$ est différent de $L_j(\alpha_1, \ldots, \alpha_n)$ et les images de α par σ_i et σ_j sont distinctes.

Les n K-homomorphismes σ_i de N dans $\mathbb{C}$ induisent des K-homomorphismes de $K(\alpha)$ dans $\mathbb{C}$. Les n images de α étant distinctes, le degré du polynôme minimal M de α est au moins égal à n.

$$[K(\alpha) : K] = d^0 M \geq n$$

Or
$$[K(\alpha) : K] = \frac{[N : K]}{[N : K(\alpha)]} \geq n$$

L'inégalité précédente impose $[N : K(\alpha)] = 1$, d'où $N = K(\alpha)$.

Exemple.

$$N = \mathbb{Q}(\sqrt{2}, \sqrt{3})$$
$$\alpha = \sqrt{2} + \sqrt{3}$$

Les conjugués de α sont : $\sqrt{2}+\sqrt{3}$, $\sqrt{2}-\sqrt{3}$, $-\sqrt{2}+\sqrt{3}$, $-\sqrt{2}-\sqrt{3}$.

$$N = \mathbb{Q}(\sqrt{2}+\sqrt{3}).$$

C. Théorème fondamental de Galois.

I. Extension normale.

Définition.

N est une extension normale de K, si et seulement si, N est obtenu en adjoignant à K toutes les racines d'un polynôme P à coefficients dans K.

$P = X^r + \ldots + p_0$ $\quad p_i \in K$, $\quad x_1, \ldots, x_r$ système complet de racines.

$$N = K(x_1, \ldots, x_r)$$

Exemple.

$K = \mathbb{Q}$ $\quad L = \mathbb{Q}(\sqrt{2})$ $\quad P = X^2 - 2$

$L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ $\quad P = (X^2-2).(X^2-3)$

$L = \mathbb{Q}(\sqrt[3]{2}, j)$ $\quad P = (X^3+X+1).(X^3-2)$

mais $L = \mathbb{Q}(\sqrt[3]{2})$ n'est pas une extension normale car toutes les racines de X^3-2 n'appartiennent pas à L.

Proposition.

Tout K-homomorphisme de N dans $\mathbb{C}$ laisse N globalement invariant et N possède $[N : K]$ *K-automorphismes.*

Soit σ : $N \to \mathbb{C}$ un K-homomorphisme.

1) $\sigma(P(x_i)) = \sigma(x_i)^r + p_{r-1}.\sigma(x_i)^{r-1} + \ldots + p_0$ car $p_i \in K$ $\sigma(p_i) = p_i$; $\sigma(x_i)$ est racine de P et $\sigma(x_i) \in N$.

Donc, si $x \in N$, $x = \dfrac{A(x_1, \ldots, x_n)}{B(x_1, \ldots, x_n)}$, $\sigma(x) \in N$.

2) σ est une application linéaire de l'espace vectoriel N sur K, dans $\mathbb{C}$

$$\sigma(x+y) = \sigma(x) + \sigma(y)$$
$$a \in K \quad \sigma(a.x) = a.\sigma(x)$$

σ est un endomorphisme injectif de l'espace vectoriel N sur K, donc σ est une bijection.

3) Il existe n K-homomorphismes de N dans $\mathbb{C}$; ces K-homomorphismes sont des K-automorphismes de N.

II. Groupe de Galois d'une extension normale.

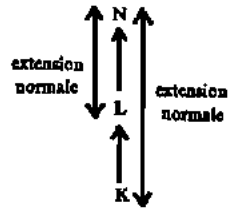
Définition.

L'ensemble $\Gamma(N|K)$ *des* K*-automorphismes de* N *est un groupe pour la composition des applications appelé groupe de Galois de l'extension normale* N.

En effet, si $g, h \in \Gamma(N|K)$, $g \circ h \in \Gamma(N|K)$ et $g^{-1} \in \Gamma(N|K)$.

Proposition.

Si N *est une extension normale de* K, *et contient une extension* L *de* K, *alors le groupe de Galois* $\Gamma(N|L)$ *est un sous-groupe de* $\Gamma(N|K)$.



Un L-automorphisme σ de N laisse L invariant élément par élément, donc K. σ est un K-automorphisme de N

$$\Gamma(N|L) \subset \Gamma(N|K).$$

Remarque.

Si $L = K$ $\Gamma(N|L) = \Gamma(N|K)$

Si $L = N$ $\Gamma(N|L) = \Gamma(N|N)$ le groupe se réduit à l'identité.

Si $L \supset L'$ $\Gamma(N|L) \subset \Gamma(N|L')$

III. Théorème fondamental de la théorie de Galois.

Théorème.

Soit N *une extension normale de* K. *L'application, qui associe à une extension* L *de* K, *contenue dans* N *le groupe de Galois* $\Gamma(N|L)$, *est une bijection de l'ensemble de ces extensions dans l'ensemble des sous-groupes de* $\Gamma(N|K)$.

Soient $\mathfrak{e}$ l'ensemble des extensions de K incluses dans N et $\mathfrak{G}$ l'ensemble des sous-groupes de $\Gamma(N|K)$.

$$\Gamma(N|.) : \mathfrak{e} \to \mathfrak{G}$$
$$L \mapsto \Gamma(N|L)$$

Pour construire l'application réciproque I de $\Gamma(N|.)$, on considère l'application qui associe à un sous-groupe H de $\Gamma(N|K)$ l'ensemble des éléments de N invariants par H.

$$I : \mathfrak{G} \to \mathfrak{e}$$
$$H \mapsto I(H) = \{n \in N | h(x) = n,\ \forall h \in H\}$$

Pour établir que I est l'application réciproque de $\Gamma(N|.)$ on démontre que

a) $\quad \forall L \quad I(\Gamma(N|L)) = L$

b) $\quad \forall H \quad \Gamma(N|I(H)) = H$

a) On pose $L' = I(\Gamma(N|L))$ et on montre $L' = L$.

L est invariant par un élément de $\Gamma(N|L)$, donc $L \subset L'$. Un élément de $\Gamma(N|L)$ laisse L' invariant, donc $\Gamma(N|L) \subset \Gamma(N|L')$

$$\text{card } \Gamma(N|L) = [N : L] \qquad \text{card } \Gamma(N|L') = [N|L'] = \frac{[N : L]}{[L : L']}$$

Or $\qquad \text{card } \Gamma(N|L) \leq \text{card } \Gamma(N|L')$

$$[N : L] \leq \frac{[N : L]}{[L' : L]}$$

Cette inégalité entraîne $[L' : L] = 1$, d'où $L = L'$.

b) On pose $H' = \Gamma(N|I(H))$ et on montre $H' = H$.

1. Le groupe H' est formé des I(H)-automorphismes de N. Or H, par construction de I, laisse invariant I(H), donc $H \subset H'$.

Soient $n = \text{card } H$, $n' = \text{card } H'$; on a : $n \leq n'$ (1)

2. L'extension N est engendrée par I(H) et un élément x dont on désigne par M le polynôme minimal sur I(H).

$$N = I(H)(x) \qquad d^{\circ}M = \text{card } \Gamma(N|I(H)) = n'.$$

Soient $h_1, \ldots, h_n$ les éléments de H (h_1 étant l'automorphisme identique). On désigne par P le polynôme admettant pour racines $h_i(x)$.

$$P = [X - h_1(x)], \ldots, [X - h_n(x)] \qquad P(x) = 0 \text{ car } h_1(x) = x$$

en développant

$$P = X^n - X^{n-1}.(\sum_i h_i(x)) + X^{n-2}.(\sum_{i<j} h_i(x).h_j(x)) + \ldots + (-1)^n \Pi h_i(x).$$

On montre que les coefficients de P sont des éléments de I(H).
Par exemple :

$$h(\sum_i h_i(x)) = \sum_i h h_i(x)$$

hh_i parcourt tous les éléments du groupe H une fois et une seule donc

$$h(\sum_i h_i(x)) = \sum_i h_i(x).$$

Le polynôme P s'annule pour x, a ses coefficients appartenant à I(H). Il est donc divisible par le polynôme minimal M de x sur I(H) (*cf.* A, II, remarque).

Donc : $d^0M \leq d^0P$ ou $n' \leq n$ (2)

En comparant 1) et 2) on en déduit $H' = H$.

D. Extension cyclique.

I. Définition.

Soit N *une* extension normale *de* K ; N *est une* extension cyclique *de* K *si son groupe de Galois* $\Gamma(N|K)$ est cyclique.

Rappels concernant les groupes cycliques. Un groupe G est dit cyclique, d'ordre n, s'il existe un élément $g \in G$ tel que :

i) $g^n = 1$.

ii) $1 = g^0, g, g^2, \ldots, g^{n-1}$ sont des éléments distincts.

On dit que g engendre G.

Exemple.

$$G = \sqrt[n]{1} = \{e^{\frac{2ik\pi}{n}} \mid \text{produit usuel}\}$$

G est engendré par $\omega = e^{\frac{2i\pi}{n}}$

Propriétés.

1) Si G est cyclique, d'ordre n, et engendré par g, tout sous-groupe est cyclique et engendré par un élément g^p où p est un diviseur de n.

2) Si G est un groupe d'ordre p et si p est un nombre premier, alors G est cyclique.

II. Corps des racines $n^{ièmes}$ de l'unité, $\omega = e^{\frac{2i\pi}{n}}$

$K = \mathbb{Q} \subset N = \mathbb{Q}(\omega)$, $\quad X^n - 1 = (X-\omega).(X-\omega^2)\ldots(X-\omega^{n-1})$.

N est une extension normale.

On pose $\Gamma = \Gamma(\mathbb{Q}(\omega)|\mathbb{Q})$.

Tout élément z de N peut s'écrire $z = q_0 + \ldots + q_{n-1}\omega^{n-1}$ mais cette décomposition n'est pas unique car X^n-1 n'est pas le polynôme minimal de ω. Le polynôme minimal M divise X^n-1.

Un élément σ de Γ est déterminé par $\sigma(\omega)$, qui est une racine du polynôme M. On a $\sigma(\omega) = \omega^k$, $k \neq 0$, où k est défini modulo n. On peut donc décrire σ à l'aide de certains entiers k tels que :

$$1 \leq k < n, \qquad (k, n) = 1.$$

En effet, la dernière condition est nécessaire, sinon on pose :

$$p = (k, n) \qquad k = pr \qquad n = ps$$
$$(\omega^k)^s = \omega^{ks} = \omega^{prs} = \omega^{nr} = 1.$$

$\sigma(\omega)$ annulerait le polynôme X^s-1, alors que ω n'annule pas ce polynôme.

Soient σ et τ deux automorphismes décrits par k et l.

$$(\tau\sigma)(\omega) = \tau(\sigma(\omega)) = \tau(\omega^k) = [\tau(\omega)]^k = \omega^{lk}$$

On décrit $\tau\sigma$ par r $\quad \begin{cases} r = lk \text{ modulo } n \\ 0 < r < n \end{cases}$

Cette description impose la définition suivante :

groupe $G_n = \{k | 0 < k < n,\ (k, n) = 1$; multiplication modulo $n\}$

$$r = k * l = k.l \text{ (modulo } n)$$

Le groupe $\Gamma(\mathbb{Q}(\omega)|\mathbb{Q})$ est isomorphe à un sous-groupe de G_n.

Cas particulier.

$$n = 17 \qquad G_{17} = \{1, 2, \ldots, 16\}$$

G_{17} est cyclique et engendré par 3. On pose $g = 3$.

Les sous-groupes G', G'', G''' sont respectivement d'ordre 8, 4, 2 et engendrés par g^2, g^4 ou g^8, comme le montre le tableau suivant :

$$\begin{array}{l} g = 3 \quad g^3 = 10 \quad g^5 = 5 \quad g^7 = 11 \quad g^9 = 14 \quad g^{11} = 7 \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad g^{13} = 12 \quad g^{15} = 6 \end{array}$$

$$G' \left[\begin{array}{l} \qquad g^2 = 9 \quad g^6 = 15 \quad g^{10} = 8 \quad g^{14} = 2 \\ G'' \left[\begin{array}{l} \qquad g^4 = 13 \quad g^{12} = 4 \\ G''' \left[\begin{array}{l} g^8 = 16 \\ g^{16} = 1 \end{array} \right. \end{array} \right. \end{array} \right.$$

Le groupe $\Gamma(\mathcal{Q}(e^{\frac{2i\pi}{17}})|\mathcal{Q})$ est isomorphe à l'un des sous-groupes de G_{17}.

On peut montrer que Γ est isomorphe à G_{17}. Aux sous-groupes G', G'', G''', correspondent donc des extensions L', L'', L''' de $\mathcal{Q}$:

$G_{17} \supset G' \supset G'' \supset G''' \supset \{1\}$

$\mathcal{Q} \subset L' \subset L'' \subset L''' \subset Q(\omega)$

$[\mathcal{Q}(\omega) : L'''] = \text{card } G''' = 2$

$[\mathcal{Q}(\omega) : L''] = \text{card } G'' = 4$ d'où $[L''' : L''] = 2$

$[\mathcal{Q}(\omega) : L'] = \text{card } G' = 8$ d'où $[L'' : L'] = 2$

$[\mathcal{Q}(\omega) : Q] = \text{card } G = 16$ d'où $[L' : \mathcal{Q}] = 2$.

Soit $x \in L'$, $x \notin \mathcal{Q}$. Le polynôme minimal de x sur $\mathcal{Q}$ ne peut avoir que le degré 2, de sorte qu'on a $L' = \mathcal{Q}(x)$, c'est-à-dire qu'on obtient L' à partir de $\mathcal{Q}$ par adjonction d'une racine d'une équation du second degré à coefficients dans $\mathcal{Q}$. De même, on obtient L'' à partir de L' (resp. L''' à partir de L'', resp. $\mathcal{Q}(\omega)$ à partir de L''') par adjonction d'une racine carrée d'un élément de L' (resp. de L'', resp. de L'''). Cela signifie qu'on peut calculer $\omega = e^{\frac{2i\pi}{17}}$ en extrayant successivement un certain nombre de racines carrées (Gauss).

Si nous n'avions pas admis que Γ est isomorphe à G_{17}, on aurait abouti à la même conclusion, en envisageant tous les cas possibles *a priori*

$$\Gamma = G_{17}, \quad G', \quad G'', \quad G'''.$$

III. Caractérisation des extensions cycliques.

Soit K un corps contenant les racines $n^{\text{ièmes}}$ de l'unité

$$\mathcal{Q}(\omega) \subset K \subset \mathbb{C} \qquad \omega = e^{\frac{2i\pi}{n}}$$

a) Proposition.

Si $x \in \mathbb{C}$ est tel que $x^n \in K$, alors $K(x)$ est une extension cyclique de K.

On pose $x^n = a$. Alors $K(x)$ est une extension normale de K car $K(x)$ contient toutes les racines du polynôme $P = X^n - a$

$$P = (X - x).(X - \omega x)...(X - \omega^{n-1}x).$$

Un K-automorphisme σ de $K(x)$ est déterminé par $\sigma(x)$, conjugué de x donc racine de P, $\sigma(x) = \omega^k.x$.

σ est décrit par ce nombre ω^k.

Un autre K-automorphisme τ de $K(x)$ est décrit par ω^l. Le composé $\tau.\sigma$ est décrit par le produit $\omega^k.\omega^l$; en effet :

$$(\tau\sigma)(x) = \tau(\omega^k x) = \tau(\omega^k).\tau(x) = \omega^k.\omega^l.x = \omega^{k+1}.x$$

$$\omega^k \in K, \qquad \tau(\omega^k) = \omega^k$$

Le groupe $\Gamma(K(x)|K)$ est isomorphe à un sous-groupe de $\sqrt[n]{1}^*$.

Γ est donc cyclique et $K(x)$ est une extension cyclique de K.

b) Réciproque.

Si N *est une extension cyclique de dimension n sur* K, *alors il existe* $x \in N$ *tel que* $x^n \in K$, *et* $N = K(x)$.

1) $\Gamma(N|K)$ est cyclique, d'ordre n et engendré par σ; $\quad \sigma^n = 1$.
σ opère dans N

$$\sigma(x+y) = \sigma(x)+\sigma(y) \qquad \sigma(x.y) = \sigma(x).\sigma(y)$$
$$\text{si } \lambda \in K \qquad \sigma(\lambda.x) = \sigma(\lambda).\sigma(x) = \lambda.\sigma(x)$$

σ est donc un endomorphisme de l'espace vectoriel N sur K.

2) Lemme : N *est un espace vectoriel de dimension finie sur un corps* K. σ *est un endomorphisme de* N. σ *est diagonalisable si et seulement s'il existe un polynôme* P *à coefficients dans* K *ayant* r *racines distinctes dans* K *et tel que* $P(\sigma) = 0$.

3) Ici $P = X^n - 1$; P a ses racines dans le corps K, donc σ est diagonalisable, il existe une base de vecteurs propres.

Soit x un vecteur propre de valeur propre λ : $\quad \sigma(x) = \lambda.x$.

$$\sigma^n(x) = \lambda^n.x = x \quad \text{car} \quad \sigma^n = 1, \quad \text{donc} \quad \lambda^n = 1, \ \lambda = \omega^k$$
$$\sigma(x^{-1}) = \lambda^{-1}.x^{-1} \quad \text{donc} \quad \lambda^{-1} \text{ est valeur propre.}$$

Soit y un autre vecteur propre de valeur propre μ : $\quad \sigma(y) = \mu.y$

$$\sigma(x.y) = \sigma(x).\sigma(y) = \lambda.x\mu y = \lambda\mu.xy$$

donc le produit de deux valeurs propres est valeur propre.

Par suite, l'ensemble des valeurs propres est un sous-groupe de $\sqrt[n]{1}$ engendré par les puissances d'un certain élément ω^k où k divise n.

Si ce sous-groupe est un sous-groupe propre ($k \neq 1$, $k \neq n$), $\lambda^{\frac{n}{k}}$ est égale à 1 quel que soit la valeur propre λ considérée.

$\sigma^{\frac{n}{k}}$ est donc un endomorphisme qui transforme chaque vecteur de la base en lui-même; donc $\sigma^{\frac{n}{k}} = 1$, ce qui est contraire à l'hypothèse, σ générateur d'ordre n.

Donc, l'ensemble des valeurs propres est isomorphe au groupe $\sqrt[n]{1}$.

4) Soit la valeur propre $\quad \lambda = e^{\frac{2i\pi}{n}} = \omega, \quad$ il existe un nombre x tel que

$$\sigma(x) = \omega.x \qquad \sigma^k(x) = \omega^k.x$$

x a donc n conjugués distincts : $x, \omega x, \ldots, \omega^{n-1}.x$.

La dimension de $K(n)$ sur K est donc n; or, la dimension de N sur K est n, donc $N = K(x)$.

5) $\sigma(x^n) = (\sigma(x))^n = (\omega x)^n = \omega^n.x^n = x^n$.

x^n est donc invariant par σ, donc $\forall i$ par σ^i; x^n est donc un élément de K.