Cours Théorie de Galois 2023-09

Lionel Fourquaux

prérequis : extensions de corps
corps de rupture & de décomposition (stem field / splitting field)
corps finis
groupes de permutations
groupes finis

bibliographie :

S. Lang, Algebra
J.S. Milne, Fields and Galois Theory
I. Stewart, Galois Theory
J.P. Serre, Topics in Galois Theory
Weizhe Zhang, Lectures in Algebra
R. & A. Douady, Algèbre et théories galoisiennes
H. Lebesgue, Leçons sur les constructions géométriques
J.-P. Serre, Galois Cohomology
F Borceux & G. Janelidze, Galois Theories
J.W.S. Cassels & A. Fröhlich (ed), Algebraic Number Theory

remerciements : L. Illusie (notes de cours 1998 - 1999)
D. Madore (suggestions)

Chapitre I : Théorie de Galois des extensions finies

① Extensions normales, séparables et galoisiennes.

Si L/K est une extension finie, on s'intéresse au groupe

$$\mathrm{Aut}_K(L) := \{ \text{automorphismes } K\text{-linéaires du corps } L \}.$$

de ses symétries.

Exercice : Un automorphisme du corps L est K-linéaire ssi sa restriction à K est id_K.

Exercice : Calculer $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$, $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}))$.

Prop : $|\mathrm{Aut}_K(L)| \leq [L:K]$ si L/K finie

(En particulier, $\mathrm{Aut}_K(L)$ est fini.)

Plus généralement :

Prop : L finie sur K, L' : $|\mathrm{Hom}_K(L, L')| \leq [L:K]$.

Si L/K est monogène (= simple (ENS)) : $L = K(x)$, $x \in L$, soit P = polynôme minimal de x sur K.

$$K[X]/(P) \xrightarrow{\sim} L$$
$$Q \bmod P \longmapsto Q(x)$$

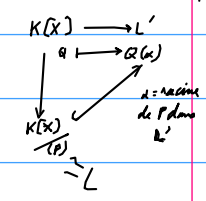
$$\deg P = n := [L:K].$$

Si $f \in \mathrm{Hom}_K(L, L')$, on a $0 = f(P(x)) = P(f(x))$,
donc $f(x) \in \{\text{racines de } P \text{ dans } L'\}$.

De plus, l'application $\begin{cases} \mathrm{Hom}_K(L, L') \longrightarrow L' \\ f \longmapsto f(x) \end{cases}$

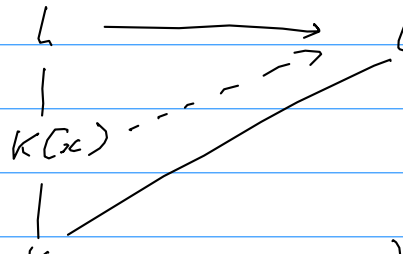
est injective : si $f, g \in \mathrm{Hom}_K(L, L')$ vérifient $f(x) = g(x)$,
alors $\forall Q \in K[X]$ $f(Q(x)) = Q(f(x)) = Q(g(x)) = g(Q(x))$,
donc $f = g$.
Ceci montre la propriété grand L/K est monogène.

En fait, l'image de cette application est l'ensemble des racines de P dans L'.



Dans le cas général, on procède par récurrence :

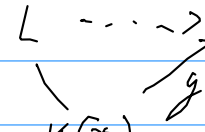
- si $L = K$, on $\mathrm{Hom}_K(L, L') = \{K \hookrightarrow L'\}$
  $\#$ extension L'/K
  (par déf !)
- sinon, soit $x \in L \setminus K$



$$\mathrm{res}_{K[x]} : \begin{cases} \mathrm{Hom}_K(L, L') \longrightarrow \mathrm{Hom}_K(K[x], L') \\ f \longmapsto f|_{K[x]} \end{cases}$$

On a $|\mathrm{Hom}_K(K[x], L')| \leq [K[x] : K]$,

et si $g \in \mathrm{Hom}_K(K[x], L')$, on a



$$\mathrm{res}_{K[x]}^{-1}(\{g\}) = \mathrm{Hom}_{K[x]}(L, L')$$

donc $|\mathrm{res}_{K[x]}^{-1}(\{g\})| \leq [L : K[x]]$ par hyp. rec. ∎

cf notes page suivante

Remarques sur la preuve précédente.

$$\mathrm{res}_{K(x)}^{-1}(\{g\}) = \mathrm{Hom}_{K(x)}(L, L')$$

↑

Ceci dépend quand même de g : la structure de $K(x)$-e.v. sur L' est donnée par g : $\left(K(x) \xrightarrow[g]{} L'\right)$.

On a bien $\left|\mathrm{Hom}_{K(x)}(L, L')\right| \leq [L : K(x)]$ par hyp rec.

↑

Celui-ci ne dépend plus de g.

Problème : parfois le groupe $\mathrm{Aut}_K(L)$ est « trop petit »
(i.e. $L^{\mathrm{Aut}_K(L)} \supsetneq K$.)

Exemple : $\mathrm{Aut}_{\mathbb{Q}}\left(\mathbb{Q}(\sqrt[3]{2})\right) = \{\mathrm{id}\}$

(Exercice : remarquer que $\mathrm{Hom}_{\mathbb{Q}}\left(\mathbb{Q}(\sqrt[3]{2}), \mathbb{R}\right) = \{\mathrm{id}\}$
car $X^3 - 2$ n'a qu'une seule racine dans $\mathbb{R}$
(croissance))

Exercice : $L = K(x)$ x de polynôme minimal $P \in K[X]$.
$n := \deg P \left(= [L : K]\right)$. M = extension de K
inutile → (~~où P est scindé (ex : corps de décomposition, ou clôture algébrique)~~)

Montrer que $\left|\mathrm{Hom}_K(L, M)\right|$ = nbre de racines de P dans M.
$= n$ si $\mathrm{car}\, K = 0$.

Exercice : Déterminer $\mathrm{Hom}_{\mathbb{Q}}\left(\mathbb{Q}(\sqrt[3]{2}), \mathbb{C}\right)$.

Ici, le « problème » vient de $\sqrt[3]{2}\, e^{\pm \frac{2i\pi}{3}} \notin \mathbb{Q}(\sqrt[3]{2})$ $\left(\subseteq \mathbb{R}\right)$.

Ce n'est pas le seul problème :

Exemple : $\mathbb{F}_p(X)$
$10 \mid p$
$\mathbb{F}_p(X^p)$

$\mathrm{Aut}_{\mathbb{F}_p(X^p)}\left(\mathbb{F}_p(X)\right) = \{\mathrm{id}\}$

(exercice : utiliser l'exercice précédent, en notant que
$T^p - X^p = (T - X)^p$
dans $\mathbb{F}_p(X)[T]$.)

On va exclure ces deux situations.

Déf : Une extension L/K algébrique est normale si $\forall x \in L$ le poly minimal de x sur K est scindé sur L.

Prop : On a équivalence de : (L/K est algébrique finie, $\bar{K}$ = clôture algébrique de K.)

(i) L/K est normale

(ii) L est le corps de décomposition d'un certain poly sur K

(iii) Tous les morphismes K-linéaire de L dans $\bar{K}$ ont même image

□ (iii) $\Rightarrow$ (i) :

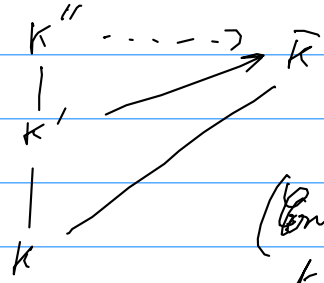
Soit $x \in L$ de poly minimal $P \in K[X]$.

Soit $x' \in \bar{K}$ racine de P.

$\begin{cases} K[X] \longrightarrow \bar{K} \\ X \longmapsto x' \end{cases}$ se factorise en $K[x] \longrightarrow \bar{K}$,

qui s'étend en $L \longrightarrow \bar{K}$

Exercice :



K''/K algébrique

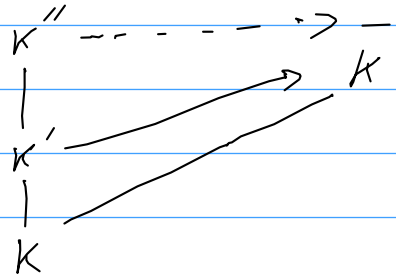
$K' \to \bar{K}$ s'étend en $K'' \to \bar{K}$.

(Considérer d'abord le cas où K''/K' est monogène, puis traiter le cas général par récurrence.)

détails ajoutés page suivante

L'image de L dans $\bar{K}$ contient x' et ne dépend pas de x' par (iii), donc P est scindé sur l'image de L donc sur L' (car l'image est $\simeq L$), d'où (i).

ajout : solution de l'exercice



* si $K'' = K'[x]$ (cas monogène)

soit $P :=$ poly. mini de x sur K'

$y :=$ racine de P dans $\bar{K}$

(NB : prendre l'image des coeffs par la flèche $K' \to \bar{K}$ ci-dessus)

$\begin{cases} K'[X] \longrightarrow \bar{K} \\ X \longmapsto y \end{cases}$ évaluation (prolonge $K' \to \bar{K}$)

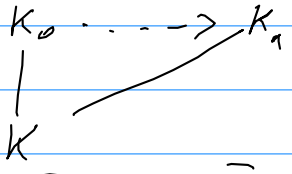
se factorise en $K'' \simeq K'[X]/(P) \longrightarrow \bar{K}$.

* si $K'' = K'[x_0, x_1, \dots)$: par récurrence.

(fini ou dénombrable)

* si K''/K' algébrique : par Zorn (on considère les sous-extensions $K''/L/K'$ + $L \hookrightarrow \bar{K}$ compatible avec $K' \hookrightarrow \bar{K}$, ordonnées par $\subseteq$ + compatibilité des $L \hookrightarrow \bar{K}$. Zorn $\to$ élément maximal $L \hookrightarrow \bar{K}$, et $L = K''$ sinon on pourrait trouver un $L[x] \hookrightarrow \bar{K}$ plus grand)

Ceci montre l'unicité de la clôture algébrique :



($K' = K$)

On obtient $\bar{K}_0 \hookrightarrow \bar{K}_1$, mais $\bar{K}_1/K$ est algébrique, donc $\bar{K}_0 \simeq \bar{K}_1$.

(i) $\Rightarrow$ (ii) : Si $L = K(x_0, \dots, x_{n-1})$,

$P_0, \dots, P_{n-1}$ poly min de $x_0, \dots, x_{n-1}$ sur K,

alors L est corps de décomp. de $\prod_{i=0}^{n-1} P_i$.

(ii) $\Rightarrow$ (iii) :

Si L est corps de décomp de $P \in K[X]$ sur K, soit L' le sous-corps de $\bar{K}$ engendré par les racines de P dans $\bar{K}$. C'est $L \longrightarrow \bar{K}$ a pour image L' (car L est engendré par les racines de P). □

Exercice : $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ n'est pas normale.

Exercice : Toute extension algébrique de corps finis est normale.

Prop : • Si $M/L/K$ avec M/K normale, alors M/L est normale

• L'intersection et la composition de 2 ext normales sont normales.

preuve : exercice (montrer qu'il n'y a qu'une seule image dans $\bar{K}$.)

Exercice : $\bar{K}/K$ est normale ($\bar{K}$ = clôture algébrique)

Exercice : Toute ext algébrique finie est contenue dans une ext. normale finie.

[indication : L/K $L = K[x_0, \dots, x_{n-1}]$ $P_0, \dots, P_{n-1}$ poly minim, prendre le corps de décomp de $\prod P_i$.]

Exercice : M.q. $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ et $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ sont normales, mais $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ n'est pas normale.

Exercice : $P \in K[X]$, L = corps de décomp de P.
M.q. $[L:K] \leq (\deg P)!$

□ $n := \deg P$ $\quad x \in L$ t.q. $P(x) = 0$.

L
| ← corps de décomp de $\frac{P(X)}{X-x}$
$K[x]$
| $\leq n$
K

par récurrence,
$[L:K[x]] \leq (\deg P - 1)! = (n-1)!$

donc $[L:K] \leq n!$ ■

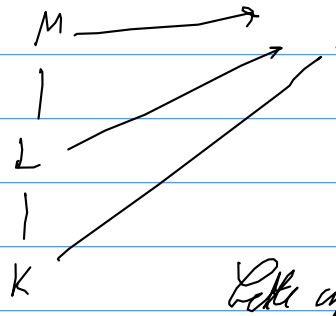
Déf : Si L/K est une ext. finie, on définit
$$[L:K]_s := |\mathrm{Hom}_K(L, \bar{K})|.$$

Prop : $[L:K]_s \leq [L:K]$.

□ déjà vu ☒

Prop : Si $M/L/K$ finies, on a
$$[M:K]_s = [M:L]_s [L:K]_s.$$

□



On considère $\begin{cases} \mathrm{Hom}_K(M, \bar{K}) \to \mathrm{Hom}_K(L, \bar{K}) \\ f \mapsto f_L \end{cases}$

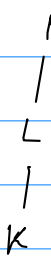
détaillé page suivante

Cette application est surjective
(car si M monogène $+$ récurrence)
et les fibres s'identifient à $\mathrm{Hom}_L(M, \bar{K})$,
d'où l'égalité. ☒

(NB : Ceci utilise l'unicité de la clôture algébrique.)

Déf : On dit que L/K est séparable si $[L:K]_s = [L:K]$.

Coro :



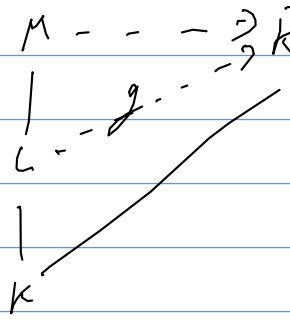
M/K séparable $\Leftrightarrow$ M/L et L/K séparables.

□ D'après les 2 prop. ci-dessus. ☒

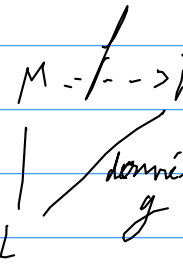
---

ajout : détails de la preuve précédente.

$$[M:K]_s = [M:L]_s \, [L:K]_s$$



On fixe $g : L \hookrightarrow \bar{K}$
et on compte les $f : M \hookrightarrow \bar{K}$
t.q. $f|_L = g$.



Ce sont les éléments de
$\mathrm{Hom}_L(M, \bar{K})$
où l'extension $\bar{K}/L$ est donnée par g.

$\bar{K}$ est une clôture algébrique de L car :

$\bar{K}/L/K$ $\quad$ $\bar{K}/K$ algébrique donc $\bar{K}/L$ algébrique.

$\forall P(X) \in L[X]$ irréductible $\quad$ P^g est scindé sur $\bar{K}$.

$\uparrow$
image
dans $\bar{K}(X)$
via $L \hookrightarrow \bar{K}$

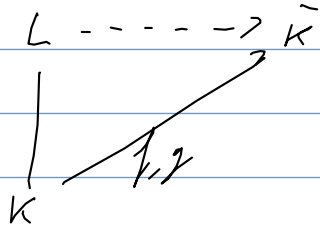
(Utile : Une clôture algébrique est algébriquement close.)

Enfin, on a $|\mathrm{Hom}_L(M, \bar{K})| = [M:L]_s$ par déf.

⚠ La notation $[M:L]_s$ affirme implicitement que $|\mathrm{Hom}_L(M, \bar{K})|$ ne dépend pas de $g : L \hookrightarrow \bar{K}$.

Montrons - le.

On veut montrer :

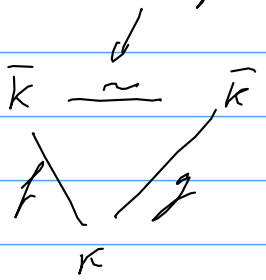


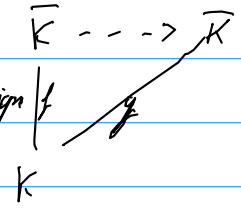
$$\left|\mathrm{Hom}_{K,f}(L,\bar{K})\right| = \left|\mathrm{Hom}_{K,g}(L,\bar{K})\right|$$

échangés par composition avec l'isomorphisme ci-dessous.

isomorphisme K-linéaire.

Cela revient à montrer que





On a déjà montré l'existence d'une telle flèche (par : axiome maximalité + récurrence + Zorn)

injectivité : $\bar{K}$ est un corps.

surjectivité : tout élément de $\bar{K}$ (de $\bar{K}^{g}$) est algébrique sur K, et $\bar{K}$ (de $\bar{K}^{f}$) est alg. clos, donc son image par $\bar{K} \dashrightarrow \bar{K}$ contient tous les algébriques sur K.

Déf : L/K finie est séparable si $\forall x \in L$ le poly mini de x sur K est à racines simples (dans L).

$\Rightarrow$: L/K séparable, donc $K(x)/K$ séparable,
soit P = poly mini de x sur K,
alors $\deg P = [K(x):K] = [K(x):K]_s = |\{\text{racines de } P \text{ dans } \bar{K}\}|$
donc les racines de P dans $\bar{K}$ sont simples,
donc dans L aussi.

$\Leftarrow$: $L = K(x_0, \dots, x_{n-1})$

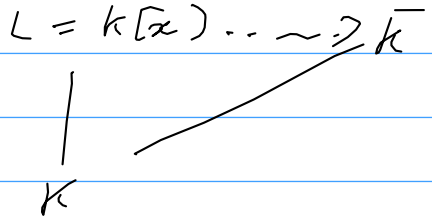
$L = K(x_0, x_1, \dots, x_{n-1})$
|
⋮
|
$K(x_0)$
|
K

Il suffit de montrer que chaque extension monogène est séparable.

L
|
$M(x)$
|
M
|
K

P poly mini de x sur K à racines simples dans L, donc dans $M(x)$, est un multiple du poly mini de x sur M.

On est ramené au cas où L/K est monogène.



P = poly minimal de x sur k.

P à racines simples dans L

On veut montrer $\left|\{\text{racines de } P \text{ dans } \bar{k}\}\right| = \deg P$.

Dans L, x est racine simple de P, donc $P'(x) \neq 0$, donc $P' \neq 0$. Or $\frac{P}{\text{pgcd}(P,P')}$ a x pour racine et divise P, donc c'est P par minimalité de P, donc $\text{pgcd}(P,P') = 1$, donc P est à racines simples dans $\bar{k}$, d'où l'égalité. □

Déf alternative : L/K ext. algébrique est séparable si $\forall x \in L$ le poly mini de x sur k est à racines simples (dans L).

(Ceci fonctionne même si L/K non finie)

Déf : $L_{sep} = \{x \in L \mid$ le poly mini de x sur k est à racines simples dans $L\}$

Prop : L_{sep} est un sous-corps de L contenant k.

□ Si $x, x' \in L_{sep}$, alors $k(x)$ et $k(x')$ sont séparées donc $k(x,x') = k(x)(x')$ aussi. □

Prop : L'ext. L_{sep}/k est séparable.

□ Par construction □

---

ajout : $k(x)/K$ est. monogène
Alors $K(x)/K$ est séparable ssi le poly mini de x sur K est à racines simples dans $\bar{K}$.
(On dira que x est séparable sur K } sur poly mini est séparable sur K)

⚠ La déf de « séparable » pour un poly non irréductible varie selon les livres.

□ $\Rightarrow$: vu ci-dessus

$\Leftarrow$: $\left|\mathrm{Hom}_K(K(x), \bar{K})\right| = \left|\{\text{racines de } P \text{ dans } \bar{K}\}\right| = \deg P$

(1ère égalité : déjà vu ; 2ème égalité : par hypothèse P à racines simples)

donc $[K(x):K]_s = [K(x):K]$
i.e. $K(x)/K$ séparable. ⊠

On en déduit : $K(x_0, \dots, x_{m-1})/K$ est séparable ssi $x_0, \dots, x_{m-1}$ sont séparables sur K.

□ $K(x_0, \dots, x_{m-1})$
|
$K(x_0, \dots, x_{m-2})$
|
⋮
|
$K(x_0)$
|
K

et il suffit de vérifier la séparabilité à chaque niveau.

⊠

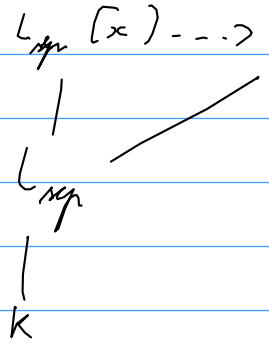
ajout : $[L:L_{sep}]_s = 1$ (i.e. L/L_{sep} est purement inséparable)

□ On a ici L/K finie.

$L \dashrightarrow \bar{K}$
|
L_{sep}
|
K

Il s'agit de montrer qu'il n'y a qu'un seul prolongement de $L_{sep} \to \bar{K}$ en $L \to \bar{K}$.

Soit $x \in L$. Soit $P :=$ poly mini de x sur L_{sep}.



Si P était séparable, alors $L_{sep}(x) / L_{sep}$ serait séparable, donc $L_{sep}(x)/K$ aussi donc $x \in L_{sep}$, et $L_{sep}(x) \hookrightarrow \bar{K}$ est $L_{sep} \hookrightarrow \bar{K}$.

Si P n'est pas séparable, on considère $\gcd(P, P')$.
C'est un diviseur non constant de P or $\deg P' < \deg P$,
donc $P' = 0$ et $\gcd(P, P') = P$.
Comme $P' = 0$ on a car $k = p > 0$,
et $P(X) = Q(X^p)$ $Q' \neq 0$.
Le polynôme $Q(X) \in L_{sep}[X]$ est irréductible sur L_{sep} (car $P(X)$ est irréductible sur L_{sep}) et a x^{p^e} comme racine.
De plus, $\gcd(Q, Q') = 1$ donc x^{p^e} est séparable
$\Leftarrow$ car $\begin{cases} Q' \neq 0 \\ Q \text{ irréductible} \end{cases}$
sur L_{sep}, donc $x^{p^e} \in L_{sep}$
donc $P(X) = X^{p^e} - x^{p^e}$ $(= (X-x)^{p^e})$,
donc $\left| \{ \text{racines de } P \text{ dans } \bar{K} \} \right| = 1$, donc $[L_{sep}(x) : L_{sep}]_s = 1$.

On en déduit $[L : L_{sep}]_s = 1$ par récurrence. ☐

Déf : La clôture séparable de K est $(\bar{K})_{sp}$.

Déf : L/K est totalement inséparable si $[L:K]_s = 1$
purement

Th (de l'élément primitif) : L/K finie séparable dans L/K est monogène.

□ Par récurrence, il suffit de considérer le cas $L = K[x,y]$, avec $K(y)/K$ séparable

fin cours n°1

Rem : On n'a pas besoin de $K(x)/K$ séparable.

On peut supposer K infini (sinon L est fini, et $L^\times$ est cyclique, donc L/K monogène).

P = poly mini de x sur K

Q = ——— y ——— (à racines simples dans $\bar{K}$)

α_i = racines de P dans $\bar{K}$ ← peut être remplacé par un corps de décomp. de PQ.

β_i ——— Q ———

$\forall i,j$ t.q. $\alpha_i \neq x$, $\beta_j \neq y$: $\alpha_i + \lambda\beta_j = x + \lambda y \iff \lambda = \dfrac{\alpha_i - x}{y - \beta_j} \neq 0$

Soit $\lambda \in K$ t.q. λ distincts de tous les

$Q(X)$ et $P(x + \lambda y - \lambda X)$ ont y pour racine, et n'ont pas d'autre racine commune par construction, donc $\gcd\big(\underbrace{Q(X)}_{\in K[x+\lambda y](X)},\ P(x+\lambda y - \lambda X)\big) = X - y$

donc $y \in K(x+\lambda y)$, donc $K(x,y) = K[x+\lambda y]$. ∎

Exercice : $\mathbb{F}_p(X,Y)/(\mathbb{F}_p(X^p,Y^p)$ n'est pas monogène.

Exercice : $[L:K]_s = [L_{sep}:K]$

$[L:K]_s \mid [L:K]$

Exercice : Toute ext L/K se décompose en

L

| purement totalement inséparable

L_{sep}

| séparable

K

Déf : Un corps K est parfait si $\mathrm{car}\, K = 0$ ou ($\mathrm{car}\, K = p > 0$ et $x \mapsto x^p$ bijective)

↓

i.e. injective.

Exc : $x \mapsto x^p$ très injective.

Prop : Toute ext$^{\text{alg}}$ de K parfait est séparable et parfaite

□ Il suffit de considérer le cas monogène.

i.e. de montrer que $Q \in K[X]$ irréductible est à racines simples dans $\bar{K}$.

$\gcd(Q, Q')$ est un diviseur de Q,

donc $\gcd(Q,Q') = 1$ ($\Rightarrow Q$ à racines simples dans $\bar{K}$)

ou $\gcd(Q,Q') = Q$ i.e. $Q' = 0$.

Le cas $Q' = 0$ n'est possible que si $\mathrm{car}\, K = p > 0$ et $Q \in K[X^p]$ mais alors $Q = R^p$ car K parfait, ce qui contredit l'irréductibilité de Q. ☒

parfait : par dim finie.

Exercice : Les corps finis sont parfaits.

pourra être écrite par la suivante

ajout : détails de la preuve de : tout extension algébrique d'un corps parfait K est séparable et parfaite.

Lemme : Soit $P \in K(X)$ irréductible non constant ∨ (K pas forcément parfait)
On a équivalence de :
(i) P est à racines simples dans $\bar{K}$
(ii) $\operatorname{pgcd}(P, P') = 1$
(iii) $\operatorname{car} K = 0$ ou ($P(X)$ n'est pas de la forme $P(X) = Q(X^p)$, $p = \operatorname{car}(K) > 0$)
(iv) P a une racine simple dans $\bar{K}$.

○ $\neg(i) \Rightarrow \neg(ii)$:

$P(X) = (X-\alpha)^2 Q(X)$ dans $\bar{K}[X]$

$P'(X) = 2(X-\alpha)Q(X) + (X-\alpha)^2 Q'(X)$

donc $X-\alpha \mid \operatorname{pgcd}(P, P')$.

$\neg(ii) \Rightarrow \neg(iii)$:

$\operatorname{pgcd}(P, P') \mid P$, $\operatorname{pgcd}(P, P') \neq 1$
P irréductible

donc $\operatorname{pgcd}(P, P') = P$, donc $P \mid P'$,
or $\deg P' < \deg P$, donc $P' = 0$.

P non constant, donc $\operatorname{car} K \neq 0$ et

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

$\forall i \quad a_i = 0$ ou $p \mid i$ $(p = \operatorname{car} K)$

$\neg(iii) \Rightarrow \neg(iv)$:

$P(X) = Q(X^p)$ car $K = p > 0$

$= R(X)^p$ dans $\bar{K}$

donc toutes les racines sont de ↑ parfait multiplicité $\geq p$.

(i) $\Rightarrow$ (iv) : évident. □

preuve de la proposition :

L/K algébrique, K parfait.

Soit $x \in L$, soit $P(X) \in K(X)$ son poly minimal sur K.
On veut montrer :
- x est séparable sur K (i.e. $P(X)$ vérifie les conditions du lemme précédent)
- car $K = 0$ ou (car $K = p > 0$ et $\exists y \in L$ $x = y^p$)

Si car $K = 0$ c'est immédiat.
Si car $K = p > 0$:
Si P ne vérifie pas le lemme, alors
$$P(X) = Q(X^p), \quad Q(X) \in K(X)$$
or K est parfait, donc $\exists R(X) \in K(X)$
$$P(X) = R(X)^p,$$
ce qui contredit l'irréductibilité de P.

On considère le polynôme $X^p - x \in K(X)$,
et son corps de décomposition L'
De qui précède, L'/K est séparable,
or $\exists y \in L$ $y^p = x$, donc $X^p - x = (X-y)^p$
dans $L'[X]$. Comme le poly minimal de y sur K
divise $X^p - x$, et est séparable, c'est $X - y$
et $y \in K$. □

Prop : K est parfait ssi toute ext alg de K est séparable.

□ $\Rightarrow$: on vient de le montrer.

$\Leftarrow$: Si $a \in K$, on considère L = corps de rupture de $X^p - a$ $(p = \mathrm{car}\, K > 0)$
et c'est le même argument qu'avant.

∎

Th (Artin) : Si G sous-groupe fini de $\mathrm{Aut}_K(L)$, alors $[L : L^G] \leq |G|$.

□ Soit $x \in L$, $\{\sigma_i\}_{i \in I} \subseteq G$ maximal t.q. les $\sigma_i(x)$ soient distincts

$\forall \tau \in G \quad \tau\sigma_i(x) \in \{\sigma_i(x)\}$

(sinon on pourrait rajouter $\tau\sigma_i$ à la famille)

donc $(\tau\sigma_i(x))_{i \in I}$ est une permutation de $(\sigma_i(x))_{i \in I}$

(par injectivité de τ)

Soit $P(X) := \prod_{i \in I} (X - \sigma_i(x))$ ← racines distinctes

$P(X) \in L^G[X]$ par relations coeff - racines.

$x = \sigma_i^{-1}\sigma_i(x) \in \{\sigma_i(x)\}$ (car $\tau = \sigma_i^{-1}$)

donc x est racine de P.

Donc $L[x]/L^G$ est séparable de degré $\leq |G|$ $(\forall x \in L)$,

donc L/L^G est séparable.

Si $L / M / L^G$ (fini), par th de l'él^t primitif, M/L^G est monogène

$M = L^G(x)$

donc $[M : L^G] \leq |G|$ par le calcul ci-dessus.

Ceci est vrai $\forall M$, donc $[L : L^G]$ est finie, et $[L : L^G] \leq |G|$ (et est séparable). □

Cor : $G = \mathrm{Aut}_{L^G}(L)$

□ $G \subseteq \mathrm{Aut}_{L^G}(L)$: évident.

$$[L : L^G] \leq |G| \leq |\mathrm{Aut}_{L^G}(L)| \leq [L : L^G]$$

(↑ déf d'Artin ; ↑ déjà vu)

donc $G = \mathrm{Aut}_{L^G}(L)$. ☒

Déf : Une extension algébrique L/K est dite galoisienne si elle est normale et séparable.

Prop : Si L/K galoisienne finie alors $|\mathrm{Aut}_K(L)| = [L : K]$.

□ $L = K[x]$ par th de l'él primitif.

$P :=$ poly minimal de x sur K. Admet d racines simples sur L

$$|\mathrm{Aut}_K(L)| = |\{\text{racines de } P \text{ dans } L\}|$$
$$= \deg P$$
$$= [L : K].$$

☒

Prop : L/K finie. On a équivalence de :

(i) L/K galoisienne
(ii) L est corps de décomp. sur K d'un $P \in K[X]$ à racines simples dans L
(iii) $L^{\mathrm{Aut}_K(L)} = K$.

□ (i) $\Rightarrow$ (ii) : On sait de l'él. primitif, L/K est monogène $L = K(x)$.
P : poly minimal de L sur K.
L/K séparable $\Rightarrow$ P à racines simples dans L
L/K normale $\Rightarrow$ P scindé sur L
$\Rightarrow$ L corps de décomposition de P.

(ii) $\Rightarrow$ (iii) :

Soient $G := \mathrm{Aut}_K(L)$

$K' := L^G$

On a $K \subseteq K'$.

$G = \mathrm{Aut}_{K'}(L)$ par corollaire précédent

$|\mathrm{Aut}_K(L)| = [L:K]$

$|\mathrm{Aut}_{K'}(L)| = [L:K']$

} car L/K, L/K' galoisiennes

donc $[L:K] = |G| = [L:K']$

donc $K = K'$.

(iii) $\Rightarrow$ (i) : Soit $G = \mathrm{Aut}_K(L)$

Soit $x \in L$.

Soit $P :=$ poly mini de x sur K.

Soit $\{x_i\} \subseteq L$ l'orbite de x sous l'action de G

Soit $Q(X) := \prod (X - x_i)$.

relations coeff-racines $\Rightarrow$ $Q(X) \in L^G[X] \underset{(iii)}{=} K[X]$.

On a $Q(x) = 0$ donc $P \mid Q$

Q est scindé à racines simples sur L, donc P aussi.

Ceci est vrai $\forall x \in L$ donc L/K est normale et séparable, i.e. galoisienne. ☐

Exercice : Tout ext. algébrique de corps fini est galoisienne.

Exercice : $\mathbb{C}/\mathbb{R}$ est galoisienne.

ajout : Si L/K est une extension finie séparable, il existe une extension M/L telle que M/K soit galoisienne.

□ Par th de l'él^t primitif, on peut supposer L/K monogène : $L = K(x)$.
Soit $P \in K[X]$ le poly minimal de x sur K.
Soit M le corps de décomposition de P.
Alors L s'identifie à un sous-corps de M, engendré par n'importe quelle racine de P.

$$\left(\begin{array}{ccc} L \simeq K[X]/(P) & \hookrightarrow & M \\ Q(X) & \longmapsto & Q(\alpha) \end{array} \right)$$

α = racine de P dans M

Il suffit de montrer que M/K est galoisienne.
C'est un corps de décomposition donc elle est normale.
L/K est séparable donc P est séparable,
donc le corps M (engendré par les racines de P) est séparable sur K.
Donc M/K est galoisienne. □

La plus petite (= intersection) ext. galoisienne de K contenant L est appelée clôture galoisienne de K

② Correspondance de Galois.

Déf : Si L/K galoisienne, on note $\mathrm{Gal}(L/K) := \mathrm{Aut}_K(L)$.

(Si L/K galoisienne finie, on a $|\mathrm{Gal}(L/K)| = [L:K]$.)

Ex : Les applications

$$\left\{ \begin{array}{c} \text{corps } M \text{ t.q.} \\ K \subset M \subset L \end{array} \right\} \longleftrightarrow \left\{ \text{sous-groupes de } \mathrm{Gal}(L/K) \right\}$$

$$M \longmapsto \mathrm{Gal}(L/M)$$

$$L^G \longleftarrow G$$

sont des bijections réciproques l'une de l'autre. (décroissantes)

□ • $L^{\mathrm{Gal}(L/M)} = M$ car L/M galoisienne

• $\mathrm{Gal}(L/L^G) = G$ par corollaire déjà vu. ☒

Prop : $[L^H : L^G] = [G:H]$ (si $H \subseteq G \subseteq \mathrm{Gal}(L/K)$ sous-groupes)

□ $H = \{\mathrm{id}\}$ suffit par multiplicativité

($[L:L^G] \leq |G|$ par Artin)

$|G| = |\mathrm{Gal}(L/L^G)|$ car $G = \mathrm{Gal}(L/L^G)$.

$= [L:L^G]$ car L/L^G galoisienne ☒

Prop : Si G sous groupe de $\mathrm{Gal}(L/K)$
$\sigma \in \mathrm{Gal}(L/K)$
$M = L^G$ $(\leftrightarrow G)$
alors $\sigma M \leftrightarrow \sigma G \sigma^{-1}$

▷ exercice ☒

fin cours n°2

Prop : L^G/K galoisienne $\Leftrightarrow G \triangleleft \mathrm{Gal}(L/K)$
et dans ce cas, $\mathrm{Gal}(L^G/K) \simeq \mathrm{Gal}(L/K)/G$.

▷ L^G/K galoisienne $\Leftrightarrow L^G/K$ normale
$\Leftrightarrow L^G$ stable par $\mathrm{Gal}(L/K)$
$\Leftrightarrow G \triangleleft \mathrm{Gal}(L/K)$ (car L/K normale, groupe)

$\mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(L^G/K)$ par restriction
$\ker = \mathrm{Gal}(L/L^G) = G$
surjectivité par $[L^G : K] = \dfrac{[L:K]}{[L:L^G]}$. ☒

Exemple : $\mathbb{Q}(\sqrt[4]{2}, i)$

$X^4 - 2$ est irréductible sur $\mathbb{Q}$ (par Eisenstein)

$X^4 - 2 = (X^2 - \sqrt{2})(X^2 + \sqrt{2})$

$= (X - \sqrt[4]{2})(X + \sqrt[4]{2})(X - i\sqrt[4]{2})(X + i\sqrt[4]{2})$

donc $\mathbb{Q}(\sqrt[4]{2}, i)$ = corps de décomposition de $X^4 - 2$ sur $\mathbb{Q}$

donc $\mathbb{Q}(\sqrt[4]{2}, i) / \mathbb{Q}$ galoisienne.

$\mathbb{Q}(\sqrt[4]{2}, i)$

2 | car $i \notin \mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{R}$ et $i^2 = -1$

$\mathbb{Q}(\sqrt[4]{2})$

4 | car $X^4 - 2$ irréductible sur $\mathbb{Q}$

$\mathbb{Q}$

donc $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = 8$

$|\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})| = 8$ groupe d'ordre 8

sous-extensions :

$\mathbb{Q}(\sqrt[4]{2})$, $\mathbb{Q}(i\sqrt[4]{2})$: non normales, d'indice 2

$\longleftrightarrow$ sous-groupes non distingués d'ordre 2

$\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i)$, $\mathbb{Q}(i\sqrt{2})$: galoisiennes d'indice 4

$\longleftrightarrow$ sous-groupes distingués d'ordre 4

$\mathbb{Q}(i, \sqrt{2})$: galoisienne, d'indice 2

$\longleftrightarrow$ sous-groupe distingué d'ordre 2

$\mathrm{Gal}\left(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}\right)$ contient la conjugaison complexe + non abélien.

$\mathbb{Q}(\sqrt[4]{2}, i)$ corps de rupture de $X^4 - 2$ sur $\mathbb{Q}(i)$

4 racines : $\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}$

$\mathbb{Q}(\sqrt[4]{2}, i)$ — 4 — $\mathbb{Q}(i)$ — 2 — $\mathbb{Q}$

$\mathbb{Q}(\sqrt[4]{2}, i) \simeq \mathbb{Q}(i)[X] \simeq \mathbb{Q}(i\sqrt[4]{2}, i)$

$\mathbb{Q}(i)[X]/(X^4 - 2)$

$\mathbb{Q}(i)$

On a un élément de $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}(i))$ qui envoie $\sqrt[4]{2} \to i\sqrt[4]{2} \to -\sqrt[4]{2} \to -i\sqrt[4]{2}$

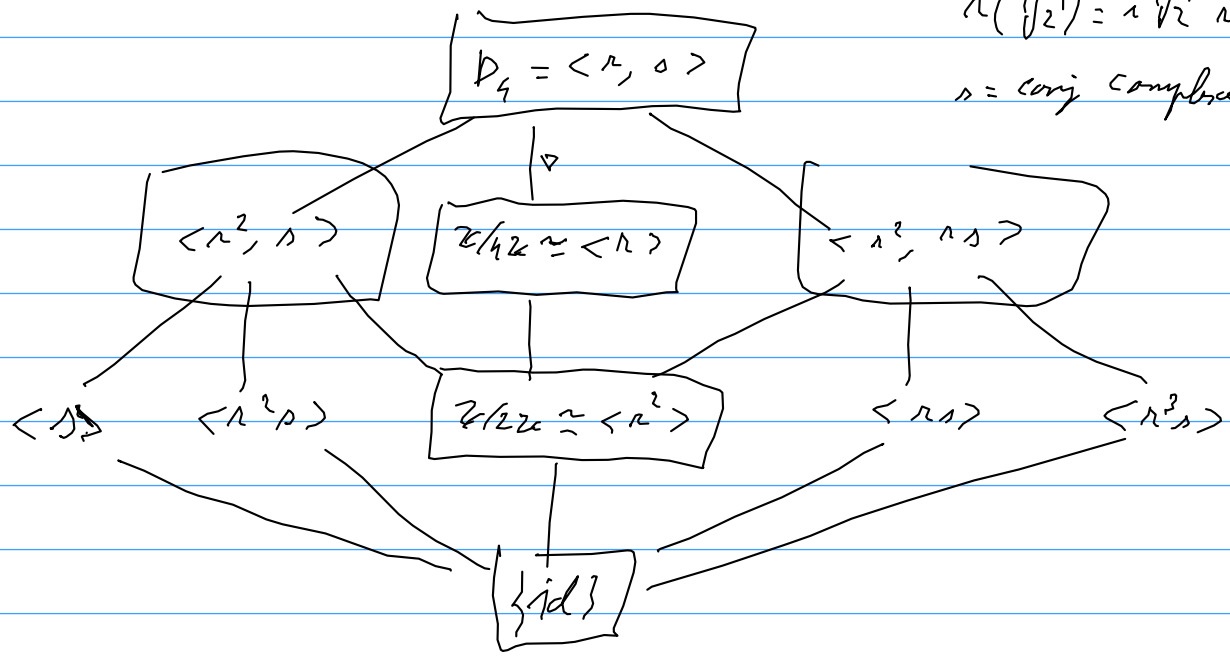
donc d'ordre 4.

$0 \to \mathbb{Z}/4\mathbb{Z} \to \mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}) \to \mathbb{Z}/2\mathbb{Z} \to 0$

conjugaison complexe. $\mapsto 1$

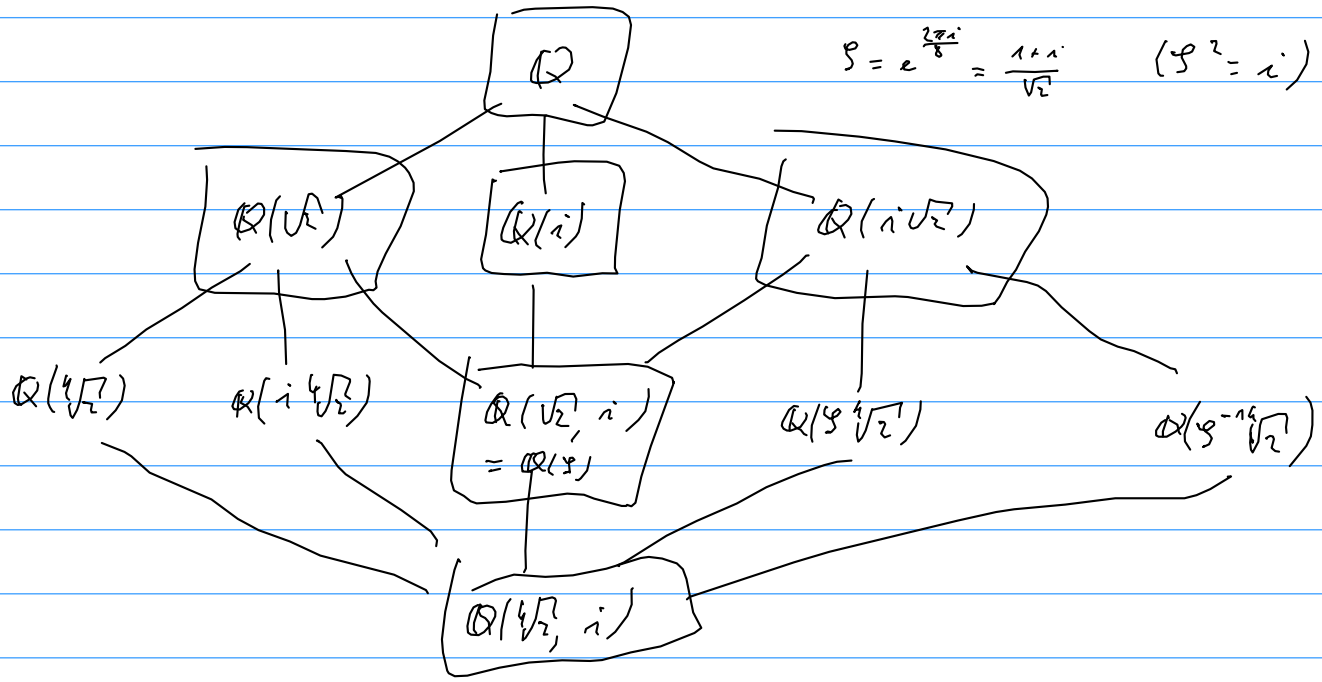
Fin du cours n°3

$\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}) \simeq D_4$



$r(\sqrt[4]{2}) = i\sqrt[4]{2}$ $r(i) = i$

s = conj complexe



$\zeta = e^{\frac{2\pi i}{8}} = \frac{1+i}{\sqrt{2}}$ $(\zeta^2 = i)$

et en $K \neq \mathbb{Q}$

Exercice : Si $[L:K] = 2^N$ que peut-on dire de l'extension L/K ? du groupe $\mathrm{Gal}(L/K)$?

(3) Exemples et applications

$\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{ \mathrm{id}, \text{conjugaison} \} \simeq \mathbb{Z}/2\mathbb{Z}$

(simple mais très utile !)

a) Corps finis

$\mathbb{F}_{q^d} / \mathbb{F}_q \qquad q = p^* \qquad$ est galoisienne (déjà vu)

$\varphi_q : \begin{cases} \mathbb{F}_{q^d} \longrightarrow \mathbb{F}_{q^d} \\ x \longmapsto x^q \end{cases} \in \mathrm{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$

$\varphi_q^e = \mathrm{id} \iff \{ \text{racines de } x^{q^e} - x \} \supseteq \mathbb{F}_{q^d}$,

donc $\begin{cases} \varphi_q^d = \mathrm{id} \\ \text{si } e < d, \quad \varphi_q^e \neq \mathrm{id} \end{cases}$

Exercice : Déterminer le polynôme minimal et le polynôme caractéristique de φ_q comme application $\mathbb{F}_q$ - linéaire.

On en déduit que φ_q est d'ordre d dans le groupe $\mathrm{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$ or $|\mathrm{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)| = d$ (puisque $\mathbb{F}_{q^d}/\mathbb{F}_q$ est galoisienne), donc le groupe $\mathrm{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$ est cyclique, engendré par φ_q.

$\mathrm{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q) \simeq \mathbb{Z}/d\mathbb{Z}$.

Les sous-groupes de $\mathbb{Z}/d\mathbb{Z}$ sont les $e\mathbb{Z}/d\mathbb{Z}$ pour $e \mid d$, donc la correspondance de Galois affirme que :

Les sous-corps de $\mathbb{F}_q^d$ sont les

$$\{x \in \mathbb{F}_{q^d} \;/\; \varphi_q^e(x) = x\} \quad (\simeq \mathbb{F}_{q^e})$$

pour chaque $e \mid d$.

↑ i.e. les racines de $X^{q^e} - X$.

b) Des groupes $\mathfrak{S}_p$.

Soit p un nombre premier. On veut montrer qu'il existe une extension $L/\mathbb{Q}$ telle que $\mathrm{Gal}(L/\mathbb{Q}) \simeq \mathfrak{S}_p$.

Lemme : Si $R(X) \in \mathbb{Q}[X]$ vérifie
- R est irréductible sur $\mathbb{Q}$
- $\deg R = p$
- R a exactement 2 racines non réelles,

si L est un corps de décomposition de R sur $\mathbb{Q}$, alors $\mathrm{Gal}(L/\mathbb{Q}) \simeq \mathfrak{S}_p$.

○ Par construction, l'extension $L/\mathbb{Q}$ est galoisienne, et est engendrée par les p racines de R dans L.
L'action de $\mathrm{Gal}(L/\mathbb{Q})$ sur ces racines donne donc un morphisme de groupes injectif
$$\mathrm{Gal}(L/\mathbb{Q}) \hookrightarrow \mathfrak{S}_p.$$
(Rem : ceci montre $[L:\mathbb{K}] \leq p!$)
La conjugaison complexe donne un élément d'ordre 2 de $\mathrm{Gal}(L/\mathbb{Q})$, dont l'image est une transposition.

D'autre part, $\mathbb{Q}[X]/(R)$ est un sous-corps de L, de degré p sur $\mathbb{Q}$ donc $p \mid [L:\mathbb{Q}]$,
donc $p \mid |\mathrm{Gal}(L/\mathbb{Q})|$,
donc (lemme de Cauchy) $\mathrm{Gal}(L/\mathbb{Q})$ contient un élément d'ordre p,
ou son image dans $\mathfrak{S}_p$ est précisément un p-cycle.

Comme $\mathfrak{S}_p$ est engendré par un p-cycle et une transposition, on en déduit $\mathrm{Gal}(L/\mathbb{Q}) \simeq \mathfrak{S}_p$. ☒

Il reste à montrer l'existence d'un tel polynôme.

Soit $R_0(X) = (X^2+2) \prod_{i=0}^{p-3} (X - 2i)$.

Le polynôme R_0 a exactement $p-2$ racines réelles, qui sont simples.
Posons $R(X) := R_0(X) - \frac{2}{n}$ $n \in \mathbb{Z}$, $n >> 0$, $2 \nmid n$.
Pour $n >> 0$, le polynôme R a aussi $p-2$ racines réelles, simples, donc 2 racines non réelle.
De plus $n R(X) = n R_0(X) - 2$ vérifie le critère d'Eisenstein pour le nbre premier 2. (Son coefficient constant est -2.) Il est donc irréductible.
Donc le polynôme R convient.

c) Une application à l'irréductibilité.

Soit $P(X) \in K(X)$, et soit L le corps de décomposition de P séparable (i.e. sans racine multiple dans L)
Soit R l'ensemble de racines de P dans L. $|R| = \deg P$
Alors $Gal(L/K)$ agit sur R.

- La factorisation de P sur K donne une partition de R :
- L'action de $Gal(L/K)$ ——————————.

Soit $\alpha, \beta \in R$. S'il existe $\sigma \in Gal(L/K)$ tel que $\beta = \sigma(\alpha)$, et si $P_\alpha \in K(X)$ est le poly minimal de α sur K,
alors $P_\alpha(\beta) = P_\alpha(\sigma(\alpha)) = \sigma(P_\alpha(\alpha)) = \sigma(0) = 0$.
($P_\alpha(\alpha) = 0 \in K(X)$)

Réciproquement, si $\alpha, \beta \in R$ sont racines d'un même facteur irréductible Q de P, alors

$$K(\alpha) \simeq K[X]/(Q) \simeq K(\beta)$$

σ prolonge en un automorphisme K-linéaire de L, qui envoie α sur β.

Les deux partitions sont donc les mêmes. La factorisation de P sur K est :

$$P(X) = \prod_{\text{orbites } G \text{ de } R \text{ sous } Gal(L/K)} \ \prod_{\alpha \in G} (X - \alpha)$$

$\in K(X)$ car coeff fixés par toute permutation des racines α.

En particulier si $Gal(L/K)$ agit transitivement sur R, alors P est irréductible.

d) Extensions cyclotomiques

$$\Phi_n(X) = \prod_{i \in (\mathbb{Z}/n\mathbb{Z})^*} (X - \zeta^i)$$

ζ = racine ~~primitive~~ n-ième dans $\bar{K}$
générateur de $\mu_n(\bar{K})$

L'ensemble μ_n des racines n-ièmes de l'unité dans $\bar{K}$ est un sous-groupe fini de $\bar{K}^\times$ (noyau de $\{\bar{K}^\times \to \bar{K}^\times, x \mapsto x^n\}$), donc est cyclique.

$K(\mu_n)$ est un corps de décomposition de Φ_n et de $X^n - 1$.

$\frac{d}{dX}(X^n - 1) = nX^{n-1}$, $0^{n-1} \neq 0$,

donc $K(\mu_n)/K$ est séparable ssi $\mathrm{car}\, K \nmid n$.

On suppose désormais $\mathrm{car}\, K \nmid n$.

$K(\mu_n)/K$ est galoisienne, et $\mu_n \simeq \mathbb{Z}/n\mathbb{Z}$.

$\mathrm{Gal}(K(\mu_n)/K)$ agit sur μ_n, ce qui donne

$$\mathrm{Gal}(K(\mu_n)/K) \hookrightarrow \mathrm{Aut}(\mu_n) \simeq (\mathbb{Z}/n\mathbb{Z})^*$$

χ caractère cyclotomique

$\forall \zeta \in \mu_n(K) \quad \forall \sigma \in \mathrm{Gal}(K(\mu_n)/K) \quad \sigma(\zeta) = \zeta^{\chi(\sigma)}$.

Exercice : $\chi = 1$ si $K = \mathbb{C}$.

Exercice : Φ_n est irréductible sur K ssi χ est un isomorphisme.

e) $\mathbb{C}$ est algébriquement clos

$\mathbb{C}$ = corps de décomposition de X^2+1 sur $\mathbb{R}$

$\longrightarrow$ extension galoisienne, $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \simeq \mathbb{Z}/2\mathbb{Z}$.

Soit L une extension finie de $\mathbb{C}$.
Quitte à agrandir L, on peut supposer que $L/\mathbb{R}$ est galoisienne.
(Par le th de l'élément primitif, $L/\mathbb{R}$ est monogène)

Soit $G := \mathrm{Gal}(L/\mathbb{R})$. Comme $\mathbb{C} \subseteq L$, on a $2 \mid |G|$.
Soit H un 2-Sylow de G. Soit $M := L^H$.
Alors $[M:\mathbb{R}] = [G:H]$ est impair.
Par le th de l'élément primitif, $M/\mathbb{R}$ est monogène, donc c'est un corps de rupture pour un polynôme $P(X) \in \mathbb{R}[X]$, irréductible sur $\mathbb{R}$,
a $\deg P = [M:\mathbb{R}]$ est impair.
analyse ici $\longrightarrow$ P a une racine dans $\mathbb{R}$
donc $\deg P = 1$, donc $M = \mathbb{R}$, donc $G = H$.
Donc G est un 2-groupe.

<u>lemme :</u> Un 2-groupe G non trivial a un sous-groupe d'indice 2.

□ Par récurrence sur $|G|$.
- si G est abélien, soit $x \in G$ d'ordre 2,
  alors • OK si $G = \langle x \rangle$
  • sinon on est ramené à $G/\langle x \rangle$.
  (prendre n'importe quel élément $\neq 1$, puis prendre x une puissance convenable de cet élément.)
- sinon, on est ramené à $G/Z(G)$, et $Z(G)$ est non trivial (formule des classes). □

Or $\mathrm{Gal}(L/\mathbb{C})$ est un sous-groupe de G, donc aussi un 2-groupe. Soit H' un sous-groupe de $\mathrm{Gal}(L/\mathbb{C})$ d'indice 2 (si $L \neq \mathbb{C}$) et soit $K' := L^{H'}$.
Alors $[K' : \mathbb{C}] = 2$, et K' est monogène, or tout élément de $\mathbb{C}$ a une racine carrée, donc tout polynôme de degré 2 est scindé sur $\mathbb{C}$, donc c'est impossible.
Donc $L = \mathbb{C}$.
Donc $\mathbb{C}$ est algébriquement clos.

fin cours n°4

(On a utilisé 2 ingrédients :
- les poly de degré impair sur $\mathbb{R}$ ont une racine
- tout nbre complexe a une racine carrée

+ th de Galois et th des groupes pour combiner les deux.)

I/ Constructions (à la règle et) au compas.

Un point $P \in \mathbb{R}^2$ est constructible s'il existe une suite de points $P_0, P_1, \dots, P_{m-1}$, avec $\begin{cases} P_0 = (0,0) \\ P_1 = (1,0) \\ P_{m-1} = P \end{cases}$

telle que $\forall i \in \{2, \dots, m-1\}$ P_i est

(• l'intersection de 2 droites passant par des couples de pts distincts dans $\{P_0, \dots, P_{i-1}\}$

• l'intersection de deux cercles de centres l'un des pts $\{P_0, \dots, P_{i-1}\}$ et passant par l'un de ces pts

• l'intersection d'une telle droite et d'un tel cercle).

Un nombre $z \in \mathbb{R}$ est constructible s'il existe une tour d'extensions $K_{m-1} \ni z$ avec $[K_{i+1} : K_i] = 2$.

$\vdots$

$K_0 = \mathbb{Q}$

Prop : Il y a équivalence de :

(i) un pt est constructible.

(ii) ses coordonnées sont des réels constructibles

(iii) son affixe est constructible

□ (i) $\Rightarrow$ (ii) : On note K_i l'ext de $\mathbb{Q}$ engendrée par les coordonnées de $P_0, P_1, \dots, P_{i+1}$.

On a $K_0 = \mathbb{Q}$, et les coordonnées de P_{m-1} sont dans K_{m-1}.

Il reste à montrer $[K_{i+1} : K_i] \leq 2$.

↑ On pourra enlever les répétitions dans la suite (K_i).

Dans le cas d'une intersection de droite, on a $[K_{i+1} : K_i] = 1$.
Pour droites et cercles, $[K_{i+1} : K_i] \leq 2$ (Eq. de degré 2)
Pour 2 cercles, le faisceau engendré contient une droite définie sur K_i, donc on est ramené au cas d'une droite et d'un cercle définis sur K_i.

(ii) $\Rightarrow$ (i) :

On décompose en 4 lemmes :

(a) Lemme : Si $(x, 0)$ et $(y, 0)$ sont constructibles, alors (x, y) aussi. $(\forall x, y \in \bar{\mathbb{Q}} \cap \mathbb{R})$

(b) Lemme : $\forall x \in \mathbb{Q}$ $(x, 0)$ est constructible.

(c) Lemme : Si $\begin{cases} \forall x \in K & (x, 0) \text{ est constructible} \\ [K[\alpha] : K] = 2 & \alpha \in \mathbb{R} \end{cases}$
alors $(\alpha, 0)$ est constructible

(d) Lemme : Si $\begin{cases} \forall x \in K & (x, 0) \text{ est constructible} \\ \alpha^2 \in \bar{\mathbb{Q}} \cap \mathbb{R} & \text{est constructible} \end{cases}$
alors $\forall x \in K[\alpha]$ $(x, 0)$ est constructible.

preuve des lemmes : (a) par construction (15)
(b) par (16), (17) et (23)
(c) par (16), (17), (22), (23) et (19)
(d) par (16), (17), (22) et (23)

Pour montrer l'implication :
(a) ramène au cas d'un point $(x, 0)$.
(b) + (d) montrent que $(x, 0)$ est constructible si x l'est. (par récurrence)

Il reste un point à vérifier : on pourrait avoir un réel constructible dont la tour n'est pas contenue dans $\mathbb{R}$.

$$\begin{array}{ccc} & \alpha \notin K_{n-1} & \subset \mathbb{C} \\ \widehat{\mathbb{R}} & | \leq 2 & \not\subset \mathbb{R} \\ & \vdots & \\ & | \leq 2 & \\ & K_0 = \mathbb{Q} & \end{array}$$

Notons L_j = l'ext de $\mathbb{Q}$ engendrée par les parties réelles et imaginaires des éléments de K_j.

On a $L_0 = \mathbb{Q}$, $\alpha \in L_{n-1}$, $K_j \subseteq L_j[i]$

Si $K_j = K_{j+1}$, alors $L_j = L_{j+1}$.

Si $[K_{j+1} : K_j] = 2$, alors $K_{j+1} = K_j(\sqrt{\delta})$ $\delta \in K_j$
(par résolution des éq. de degré 2).

$\delta = x + iy$ $\quad \sqrt{\delta} \in \left\{ \pm \sqrt{\frac{x + \sqrt{x^2+y^2}}{2}} \pm i \sqrt{\frac{-x + \sqrt{x^2+y^2}}{2}} \right\}$

donc $L_{j+1} = L_j\left(\sqrt{\frac{\pm x + \sqrt{x^2+y^2}}{2}}\right)$

$$\left[L_{j+1} : L_j\left(\sqrt{x^2+y^2}\right) \right] \leq 2$$

$$\left[L_j\left(\sqrt{x^2+y^2}\right) : L_j \right] \leq 2$$

On peut donc trouver une tour contenue dans $\mathbb{R}$.

(ii) $\Rightarrow$ (iii) :

si x et y sont constructibles, alors $x+iy$ est racine de $X^2 - 2xX + (x^2+y^2)$

↑ degré 2

donc $x+iy$ est constructible.

NB : Les éléments de $\bar{\mathbb{Q}}$ constructibles forment un corps.

□ Soit $x, y \in \bar{\mathbb{Q}}$ constructibles

$x \in K_{m-1}$ $\quad$ $y \in L_{m'-1}$

$|\leq 2$ $\quad$ $|\leq 2$

$\vdots$ $\quad$ $\vdots$

K_0 $\quad$ L_0

$|\leq 2$ $\quad$ $|\leq 2$

$\mathbb{Q}$ $\quad$ $K_{m-1}L_{m'-1}$ $\quad$ $\mathbb{Q}$

$|\leq 2$

x, y

alors $K_{m-1}L_0$

$|\leq 2$

K_{m-1}

$\vdots$

$|\leq 2$

$\mathbb{Q}$

□

(iii) $\Rightarrow$ (ii) :

Si $x+iy$ est constructible,
on pose L_y = l'ext de $\mathbb{Q}$ engendrée par les parties réelles et imaginaires des éléments de K_y.

$x, y \in L_{n-1}$, et on a une tour prouvant que x et y sont constructibles.

□

Feuille de construction

① Symétrie axiale

A, B, C $(A \neq B)$

but : image de C par la symétrie axiale de droite (AB).

cercle (A, C) ∩ cercle (B, C) = {C, C'}

AC = AC', BC = BC', donc (AB) médiatrice de [CC'].

→ C' est l'image de C par la symétrie d'axe (AB).

② Médiatrice

A, B $(A \neq B)$

but : 2 pts de la médiatrice de [AB].

cercle (A, B) ∩ cercle (B, A) = 2 pts de la médiatrice.

③ Report de distance

A B C

but : cercle de centre A et de rayon AB.

médiatrice de [AB] = (PQ) par ②

symétrique de C par rapport à (PQ) par ①

par symétrie axiale, AC' = BC donc le cercle (A, C') a pour rayon BC.

④ Hexagone régulier

A, B

but : hexagone régulier de centre A et de sommet B.

$P_0 = B$

cercle (A, B) ∩ cercle (B, A) = $\{P_1, P_5\}$

cercle (A, B) ∩ cercle (P_1, A) = $\{P_0, P_2\}$

cercle (A, B) ∩ cercle (P_5, A) = $\{P_0, P_4\}$

cercle (A, B) ∩ cercle (P_2, A) = $\{P_1, P_3\}$

alors AP_0P_1, AP_1P_2, AP_2P_3, AP_4P_5, AP_5P_0 sont équilatéraux,
donc $\widehat{P_0AP_1} = \widehat{P_1AP_2} = \widehat{P_2AP_3} = \widehat{P_4AP_5} = \widehat{P_5AP_0} = \frac{\pi}{3}$,
donc $\widehat{P_3AP_1} = \frac{\pi}{3}$ aussi, et $P_0P_1P_2P_3P_4P_5$ est un hexagone régulier
de centre A et de sommet $B = P_0$.

(5) Symétrie centrale

A, B

but : symétrique de B par rapport à A (i.e. C t.q. A milieu de $[BC]$).

Par (4), on construit un hexagone régulier $P_0P_1P_2P_3P_4P_5$ de centre A et tel que $P_0 = B$. Alors $C := P_3$ convient (car $\widehat{BAC} = 3 \cdot \frac{\pi}{3} = \pi$, $AB = AC$).

(6) intersection droite – cercle de centre donné non sur la droite

A, B, $\mathcal{C} = \text{cercle}(C, D)$.

but : $(AB) \cap \mathcal{C} = \{P, Q\}$.

$C' =$ symétrique de C par rapport à (AB) par (5)

$\mathcal{C}' =$ cercle de centre C' et de rayon CD par (3)

alors $\mathcal{C}' =$ image de $\mathcal{C}$ par symétrie / (AB)

donc $\{P, Q\} = \mathcal{C} \cap \mathcal{C}'$.

(7) $\sqrt{2}$

A, B

but : segment de longueur $AB\sqrt{2}$

Par (4), on construit un hexagone $P_0P_1P_2P_3P_4P_5$ de centre A tel que $P_0 = B$.

Le triangle $P_0P_2P_4$ est équilatéral

(car $\widehat{P_0AP_2} = \widehat{P_2AP_4} = \widehat{P_4AP_0} = \frac{2\pi}{3}$ + loi des cosinus)

donc (loi des cosinus) $P_0P_2 = AB\sqrt{1+1-2\cos\frac{2\pi}{3}} = AB\sqrt{3}$

De même, $P_1P_3 = AB\sqrt{3}$.

Soit $M \in \text{cercle}(P_0, P_2) \cap \text{cercle}(P_3, P_1)$
alors le triangle $P_0 M P_3$ est isocèle en M,
et A est le milieu de $[P_0 P_3]$, donc (AM) est la hauteur issue de M, et

$$AM = \sqrt{P_0M^2 - P_0A^2} \qquad \text{(Pythagore)}$$

$$= \sqrt{3AB^2 - AB^2}$$

$$= AB\sqrt{2}.$$

Donc AM convient.

(8) Parallélogramme

A, B, C

But : D tel que $ABCD$ parallélogramme.

(i.e. $\overrightarrow{AD} = \overrightarrow{BC}$)

On a $AD = BC$ et $CD = AB$,
donc D est l'un des pts d'intersection du cercle de centre A et de rayon BC et du cercle de centre C et de rayon AB (par (3)).

(9) Carré

A B

But : carré $ABCD$.

On a $\begin{cases} AC = \sqrt{2}\,AB \\ BC = AB \end{cases}$

donc C est l'un des pts d'intersection du cercle de centre A et de rayon $\sqrt{2}\,AB$ (par (7) + (3)) et du cercle de centre B et de rayon AB (par (3)).
On obtient D par (8) (ou par (1) : symétrique de B par rapport à (AC)).

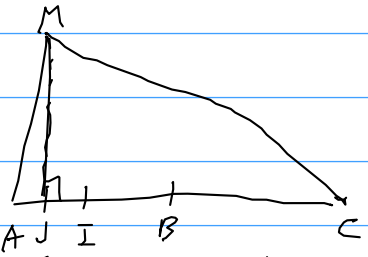
(10) Milieu

A, B

but : I = milieu de (AB).

Soit C = symétrique de A par rapport à B (par (5))

Soient $\{M, M'\}$ = cercle$(A,B) \cap$ cercle(C,A)



On ne la construit pas, c'est pour la preuve.

Notons J le projeté orthogonal de M sur (AB).

$$\begin{cases} AM^2 = AJ^2 + MJ^2 \\ CM^2 = JC^2 + MJ^2 \end{cases} \quad \text{(Pythagore)}$$

or $AM = AB$ et $CM = 2AB$,

donc $JC^2 - AJ^2 = CM^2 - AM^2 = 3AB^2$

$(JC - AJ)\underbrace{(JC + AJ)}_{= AC = 2AB} = 3AB^2$

$$\begin{cases} JC - AJ = \frac{3}{2}AB \\ JC + AJ = 2AB \end{cases}$$

donc $AJ = \frac{1}{4}AB$, donc J est le milieu de $[AI]$,

donc (MM') est la médiatrice de $[AI]$,

donc I est le symétrique de A par rapport à (MM') (par (4)).

(11) Projection orthogonale.

P, droite (AB).

but : projeté orthogonal de P sur (AB).

Si $P \in (AB)$, c'est P. On peut supposer $P \notin (AB)$.

Par ⑥, on obtient $\{A, C\} = (AB) \cap \text{cercle}(P, A)$.
Le triangle APC est isocèle en P, donc le projeté est le milieu de [AC], qu'on obtient par ⑩.

⑫ Abscisse d'un point

$A = (0, 0)$
$B = (1, 0)$
$P = (x, y)$
but : $(x, 0)$
Par ⑪ on projette P sur (AB).

⑬ Echange de coordonnée

$A = (0, 0)$
$B = (1, 0)$
$P = (x, y)$
but : (y, x)
Par ⑨ on construit $C = (1, 1)$
puis on construit par ① le symétrique de P par rapport à la droite (AC).

⑭ Ordonnée d'un point

$A = (0, 0)$
$B = (1, 0)$
$P = (x, y)$
but : $(y, 0)$
On utilise ⑬ + ⑫.

(15) Point de coordonnées données

$A = (0,0)$

$B = (1,0)$

$C = (x,0)$

$D = (y,0)$

but : $P = (x,y)$

Par (9) on construit $E = (0,y)$,

puis par (8) on construit $P = (x,y)$

(EACP est un parallélogramme)

(rectangle)

(16) Somme

$A = (0,0)$

$B = (x,0)$

$C = (y,0)$

but : $P = (x+y, 0)$.

Par (2) on construit la médiatrice Δ de $[BC]$.

C'est l'ensemble des pts d'abscisse $\frac{x+y}{2}$.

Par (4) on construit le symétrique de A par rapport à Δ, c'est P.

(17) Différence

$A = (0,0)$

$B = (x,0)$

$C = (y,0)$

but : $P = (x-y, 0)$

Par (5) on construit $C' = (-y, 0)$, et on utilise (16).

(18) Cercle de diamètre donné

A B

But : cercle de diamètre [AB]

Il suffit de construire le milieu de [AB] par (10)

(19) Racine carrée

$A = (0,0)$

$B = (x,0)$

$C = (y,0)$

But : $(\sqrt{xy}, 0)$

Par (5) on construit $B' = (-x, 0)$

$C' = (-y, 0)$

Par (18) on construit $\mathcal{C}$ de diamètre $[B'C]$

$\mathcal{C}'$ _____ $[BC']$

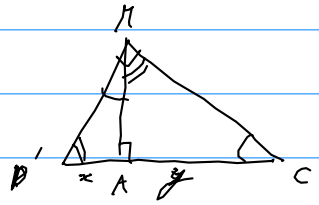
$\mathcal{C} \cap \mathcal{C}' = \{M\ M'\}$

(MM') est l'axe des ordonnées,

et $B'MC$ est rectangle en M

Les triangles $B'MC$, $B'AM$ et MAC sont semblables, donc

$\frac{AM}{x} = \frac{y}{AM}$



$AM^2 = xy$ $\quad AM = \sqrt{xy}$

donc $M = (0, \sqrt{xy})$. On conclut par (13).

(20) x^2/y

$A = (0,0)$

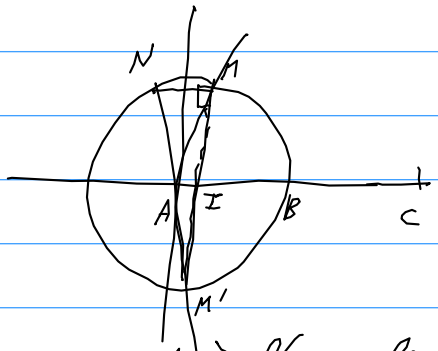
$B = (x,0)$

$C = (y,0)$

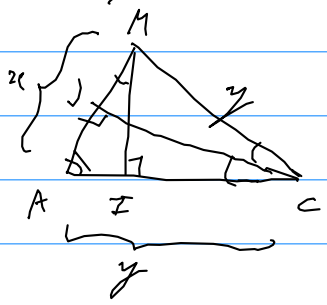
but : $D = \left(\frac{x^2}{y}, 0\right)$

$\{M, M'\}$ = cercle $(A,B) \cap$ cercle (C,A)

N = symétrique de M' par rapport à A (par (5))



M et M' sont symétriques par rapport à l'axe des abscisses, donc $(MM') \perp$ abscisses, soit I le pt d'intersection.



Le triangle MCA est isocèle en C. Soit J le milieu de $[AM]$

Les triangles MIA et CJA sont semblables donc

$$\left(\frac{AI}{x} =\right) \frac{AI}{AM} = \frac{AJ}{AC} \left(= \frac{x}{2y}\right)$$

donc $AI = \frac{x^2}{2y}$.

Le triangle $M'NM$ est rectangle en M, donc $(MN) \parallel$ abscisses, donc (Thalès) $MN = 2AI = \frac{x^2}{y}$. On (8) on obtient D, en complétant le parallélogramme $MNAD$.

La construction précédente suppose $x < 2y$
(existence des intersections M et M').
Pour s'y ramener, on remplace y par Ny
$N > 0$ entier (calcul de Ny par (16)),
et $\frac{x^2}{y} = N \frac{x^2}{Ny}$ (calcul par (16) à nouveau).

(21) $\frac{xy}{z}$

On construit $\sqrt{xy}$ par (19), puis $\frac{xy}{z} = \frac{(\sqrt{xy})^2}{z}$ par (20).

(22) xy

(21) avec $z = 1$

(23) $\frac{x}{z}$

(21) avec $y = 1$.

fin comme n°5

Rem : (hors sujet)

(24) cercle de Carlyle :

s, p

$A = (0, 1)$

$B = (s, p)$

$\mathcal{C}$ = cercle de diamètre $[AB]$

Mq les intersections de $\mathcal{C}$ avec l'axe des abscisses sont $(x_0, 0)$ et $(x_1, 0)$, où x_0, x_1 sont les racines de $X^2 - sX + p$. ($s = x_0 + x_1$, $p = x_0 x_1$)

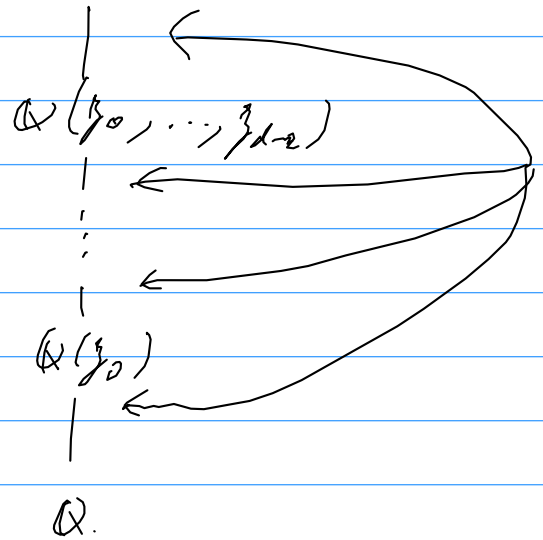
Expliquer comment faire la construction au compas seul dans le cas $p \neq -1$. Expliquer comment faire si $p = -1$ (idée : remplacer (s, p) par $(2s, 4p)$.)

Prop : $\zeta \in \bar{\mathbb{Q}}$ est constructible si la clôture galoisienne de $\mathbb{Q}(\zeta)$ a pour degré une puissance de 2.

$\Rightarrow$: $[\mathbb{Q}(\zeta) : \mathbb{Q}]$ est une puissance de 2

idem pour les autres racines du poly minimal de ζ sur $\mathbb{Q}$: $\zeta_0 = \zeta, \dots \zeta_{d-1}$

$\mathbb{Q}(\zeta_0, \dots, \zeta_{d-1})$ ← clôture galoisienne.



(Rem : Si $[L:K] \leq 2$, alors $[LK' : K'] \leq 2$.)

$\Leftarrow$: $\zeta \in L$ $\quad [L:\mathbb{Q}] = 2^n$ $\quad L/\mathbb{Q}$ galoisienne.

Par correspondance de Galois, il suffit de trouver

$\{id\} = G_0 \subseteq G_1 \subseteq \dots \subseteq G_n = Gal(L/\mathbb{Q})$

sous-groupes.

où $[G_{i+1} : G_i] = 2$.

cf lemme suivant. ∎

Lemme : Si G est un p-groupe, alors

$$\exists G_i \qquad 1 = G_0 \subsetneq \dots \subsetneq G_d = G$$

$$[G_{i+1} : G_i] = p .$$

□ Par récurrence sur $|G|$:

- vrai si $G = 1$
- vrai si $|G| = p$: $1 \subsetneq G$
- vrai si G a un sous-groupe distingué H non trivial.

$$1 \subsetneq H \subsetneq G$$

et il suffit d'appliquer l'hyp rec. à H et G/H. ☒

Lemme : Si G est un p-groupe, $|G| \geq p^2$, alors G a un sous-groupe distingué non trivial.

□ - Si G n'est pas abélien, $Z(G)$ convient (formule des classes $\Rightarrow$ $Z(G) \neq 1$)

- Si G est abélien $\exists x \in G$ d'ordre p (lemme de Cauchy) et $\langle x \rangle$ convient. ☒

Prop : Les polygones réguliers constructibles sont ceux à $2^* p_0 \dots p_k$ côtés, où p_i = premiers de Fermat distincts.

□ - Par formule de Bézout, on se ramène à p^k, p premier.

- $p = 2$: ok par bissectrices.
- $p \neq 2$: le polynôme cyclo Φ_{p^k} est irréductible de degré $\varphi(p^k) = p^k - p^{k-1}$, les est cyclotomiques sont galoisiens, donc on veut que $\varphi(p^k)$ soit une puissance de 2.

Comme $p \neq 2$, on doit avoir $k = 1$, $p - 1 =$ puissance de 2,
donc $p^k = p =$ nbre premier de Fermat.

□

g) Le théorème de la base normale.

Th (Dedekind : indépendance linéaire des caractères) :

K = corps
G = groupe

$\{$ morphismes de groupes $G \to K^\times\}$ est une famille $(K-)$ libre du K-ev des applications $G \to K$.

□ Soient $\chi_0, \dots, \chi_{m-1} : G \to K^\times$ morphismes de groupes.
$\lambda_0, \dots, \lambda_{m-1} \in K$ tq. $\sum_{i=0}^{m-1} \lambda_i \chi_i = 0$

On veut montrer $\lambda_0 = \dots = \lambda_{m-1} = 0$.

méthode : récurrence sur m.

$m = 0$: OK

$m = 1$: $\lambda_0 \chi_0 = 0$, or $\chi_0(1_G) = 1_K$, donc $\lambda_0 = 0$.

$m \geq 2$:

On a $|G| \geq 2$, car si $|G| = 1$ alors le seul morphisme de groupe est le morphisme trivial, et $m \leq 1$.

Soit $g \in G \setminus \{1_G\}$. On a

$$\sum_{i=0}^{m-1} \lambda_i \chi_i(g \cdot) = 0$$

donc $$\sum_{i=0}^{m-1} \lambda_i \chi_i(g) \chi_i = 0$$

De plus, $\sum_{i=0}^{m-1} \lambda_i \chi_0(g) \chi_i = 0$,

donc $$\sum_{i=1}^{m-1} \lambda_i (\chi_i(g) - \chi_0(g)) \chi_i = 0.$$

Par hyp. réc, $\forall i \geq 1 \quad \lambda_i(\chi_i(g) - \chi_0(g)) = 0$.

Ceci est vrai $\forall g$, et $x_i \neq x_0$ $(\forall i \geq 1)$,
donc $\forall i \geq 1 \quad \lambda_i = 0$
Enfin, $\lambda_0 x_0 = 0$, donc $\lambda_0 = 0$. ☒

Corollaire : Si K, L corps, les morphismes de corps $K \to L$ sont L-linéairement indépendants.

□ Ils se restreignent en morphismes de groupes $K^\times \to L^\times$. ☒

Corollaire : Si L/K est une ext. finie séparable,
$n := [L:K]$, M/K est. (par $\bar{K}$, on obtient galoisienne de L)
$\sigma_0, \dots, \sigma_{n-1} : L \to M$ morphismes de corps K-linéaires distincts
$(e_i)_{0 \leq i < n}$ K-base de L.

Alors $\left(\sigma_j(e_i)\right)_{0 \leq i,j < n} \in GL_n(M)$.

□ Si $\left(\sigma_j(e_i)\right)$ n'était pas inversible, il existerait $\lambda_0, \dots, \lambda_{n-1} \in M$ t.q. $\forall i \cdot \sum_{j=0}^{n-1} \lambda_j \sigma_j(e_i) = 0$,

or (e_i) est une K-base de L donc par K-linéarité des σ_j : $\forall x \in L \quad \sum_{j=0}^{n-1} \lambda_j \sigma_i(x) = 0$,
ce qui contredit le corollaire précédent. ☒

Exercice : Trouver une autre preuve, en prenant d'abord une base $1, x, x^2, \dots, x^{n-1}$ avec $L = K[x]$, puis par changement de base pour passer à (e_i).

Th (base normale) : Soit L/K galoisienne finie. Alors $\exists x \in L$ t.q. $(\sigma(x))_{\sigma \in Gal(L/K)}$ soit une K-base de L.

□ **preuve si K est fini :**

$K = \mathbb{F}_q$ $\qquad \varphi_q : \begin{cases} L \longrightarrow L \\ x \longmapsto x^q \end{cases}$

$L = \mathbb{F}_{q^n}$ $\qquad Gal(L/K) = \{ id, \varphi_q, \dots, \varphi_q^{n-1} \}$.

Le polynôme minimal de φ_q est $X^n - 1$ c'est aussi son poly caractéristique, donc (réduction de Frobenius) il existe un vecteur cyclique $x \in L$, i.e.

$x, \varphi_q(x), \dots, \varphi_q^{n-1}(x)$ est une K-base de L.

preuve si K est infini :

On note $G = Gal(L/K)$.

X_σ, $\sigma \in G$ des variables

$\longrightarrow$ anneau de polynômes $L[X_\sigma ; \sigma \in G]$

(en $n := [L : K]$ variables)

$$F(\underline{X}) = \det\left((X_{\sigma\tau})_{\sigma,\tau \in G}\right)$$

En évaluant en $X_{id} = 1$, $X_\sigma = 0 \ \forall \sigma \neq id$,

on trouve $F(?, 0, \dots, 0) = \pm 1 \neq 0$,

donc $F \neq 0$.

Lemme : Si $\forall \alpha \in L \quad F(\sigma(\alpha)\,;\ \sigma \in G) = 0$, alors $F = 0$

preuve du lemme :

On fixe une base $(\alpha_\tau)_{\tau \in G}$ de L sur K, et on écrit F en $X_\sigma = \sum_{\tau \in G} \sigma(\alpha_\tau) Y_\tau$

$\in L[Y_\tau\,;\ \tau \in G]$

$$\forall y_\tau \in K \quad F\left(\sum_{\tau \in G} \sigma(\alpha_\tau) y_\tau\right) = F\left(\sigma\left(\sum_{\tau \in G} \alpha_\tau y_\tau\right)\right) = 0$$

or k est infini, donc (par récurrence sur le nbre de variables)

$$F\left(\sum_{\tau \in G} \sigma(\alpha_\tau)\, Y_\tau\right) = 0,$$

or $\left(\sigma(\alpha_\tau)\right)_{\sigma, \tau \in G} \in GL_n(L)$ d'après le corollaire précédent,

donc $F = 0$.

On a donc : $\exists \alpha \in L \quad F(\sigma(\alpha)\,;\ \sigma \in G) \neq 0$.

i.e. $\det\left(\left((\sigma\tau)(\alpha)\right)_{\sigma, \tau \in G}\right) \neq 0$.

Si $(\varepsilon(\alpha))_{\varepsilon \in G}$ était K-liée, on aurait

$$\sum_{\varepsilon \in G} a_\varepsilon\, \varepsilon(\alpha) = 0 \qquad a_\varepsilon \in K$$

donc $\forall \sigma \in G \quad \sum_{\varepsilon \in G} a_\varepsilon\, (\sigma\tau)(\alpha) = 0$,

donc $\det\left(\left((\sigma\tau)(\alpha)\right)_{\sigma, \tau \in G}\right) = 0$.

donc $(\tau(\alpha))_{\tau \in G}$ est K-libre, et $[L:K] = |G|$,

donc $\mathcal{E}$ est une base. □

Cela veut dire que l'action de $\mathrm{Gal}(L/K)$ sur L est la représentation régulière.

Utilisation algorithmique : l'action de Gal est simple à décrire dans cette base.

4) Norme et trace

L/K est finie

Si $x \in L$, on définit :

$$m_x : \begin{cases} L \longrightarrow L \\ y \longmapsto xy \end{cases}$$ application K-linéaire

$$\mathrm{Tr}_{L/K}(x) := \mathrm{Tr}(m_x) \qquad N_{L/K}(x) := \det(m_x)$$

$\mathrm{Tr}_{L/K} : L \longrightarrow K$ est K-linéaire

$N_{L/K} : L \longrightarrow K$ induit un morphisme de groupes $L^\times \longrightarrow K^\times$.

Prop : Si L/K est séparable, on a :

$$\mathrm{Tr}_{L/K}(x) = \sum_{\sigma \in \mathrm{Hom}_K(L, \bar{K})} \sigma(x)$$

$$N_{L/K}(x) = \prod_{\sigma \in \mathrm{Hom}_K(L, \bar{K})} \sigma(x)$$

Si L/K est galoisienne, on peut remplacer $\mathrm{Hom}_K(L, \bar{K})$ par $\mathrm{Gal}(L/K)$.

D Il suffit de montrer que le polynôme caractéristique de m_x ($\det(X \mathrm{id}_L - m_x)$) vérifie

$$\det(X \mathrm{id}_L - m_x) = \prod_{\sigma \in \mathrm{Hom}_K(L, \bar{K})} (X - \sigma(x)).$$

Si $L = K(x)$, alors le poly minimal P de x sur K est égal au polynôme caractéristique, et ses racines (simples) dans $\bar{K}$ sont les $\sigma(x)$, $\sigma \in \mathrm{Hom}_K(L, \bar{K}) \longrightarrow \mathrm{Ok}$.

Dans le cas général, soit $\alpha \in L$ t.q. $L = K[\alpha]$ (th de l'él. primitif). Il existe $Q \in K(X)$ t.q. $x = Q(\alpha)$, et $m_x = Q(m_\alpha)$, or les valeurs propres de $Q(m_\alpha)$ dans $\bar{K}$ sont les $Q(\sigma(\alpha)) = \sigma(x)$, $\sigma \in \mathrm{Hom}_K(K, \bar{K}) \longrightarrow \mathrm{Ok}$. ☒

Exemples : $\mathrm{Tr}_{K/K}(x) = x$, $N_{K/K}(x) = x$

$\mathrm{Tr}_{\mathbb{C}/\mathbb{R}}(z) = 2\mathrm{Re}(z)$, $N_{\mathbb{C}/\mathbb{R}}(z) = |z|^2$

$\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x) = \sum_{i=0}^{n-1} x^{q^i}$, $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x) = \prod_{i=0}^{n-1} x^{q^i} = x^{\frac{q^n-1}{q-1}}$.

Exercice : Si $x \in L$ n'est pas séparable sur $K \subseteq L$, alors $\mathrm{Tr}_{L/K}(x) = 0$.

fin cours n°6

Prop : Si $M/L/K$ finies, alors

$\mathrm{Tr}_{M/K} = \mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{M/L}$

$N_{M/K} = N_{L/K} \circ N_{M/L}$

1. Trace

On note $(e_i)_{0 \le i < m}$ une K-base de L

$(f_j)_{0 \le j < n}$ une L-base de M

alors $(e_i f_j)_{\substack{0 \le i < m \\ 0 \le j < n}}$ est une K-base de M. (exercice !)

sources :
- Keith Conrad, Trace and norm, II (tracenorm2.pdf)
- A. J. Scholl, Transitivity of Trace and Norm

Soit $x \in M$, on a

$\forall j \quad x f_j = \sum_{i=0}^{n-1} b_{ij} f_i$

$\forall i,j,l \quad b_{ij} e_l = \sum_{k=0}^{m-1} a_{ij,kl} e_k$

donc $x e_l f_j = \sum_{i=0}^{n-1} b_{ij} e_l f_i$

$= \sum_{i=0}^{n-1} \sum_{k=0}^{m-1} a_{i,j,k,l} e_k f_i$

$$\mathrm{Tr}_{M/L}(x) = \sum_{i=0}^{n-1} b_{ii}$$

$$\mathrm{Tr}_{L/K}\left(\mathrm{Tr}_{M/L}(x)\right) = \sum_{i=0}^{n-1} \mathrm{Tr}_{L/K}(b_{ii}) = \sum_{i=0}^{n-1}\sum_{k=0}^{m-1} a_{ij,ik,k}$$

$$= \mathrm{Tr}_{M/K}(x).$$

- norme :
  - si $x \in L$, on a $N_{M/L}(x) = x^{[M:L]}$ $\left(\det \begin{pmatrix} x & & \\ & \ddots & \\ & & x \end{pmatrix}\right)$

$$N_{M/K}(x) = N_{L/K}(x)^{[M:L]}$$

$$\left(\det \begin{pmatrix} A & & \\ & \ddots & \\ & & A \end{pmatrix} \text{ où } A = \text{matrice de } \times x \text{ dans une } K\text{-base de } L\right)$$

M / $L \ni x$ / K

- si $M = L[x]$, $n := [M:L]$, $(e_i)_{0\le i<m}$ une K-base de L, $P(X) = \sum_{j=0}^{n} a_j X^j \in L[X]$ $(a_m = 1)$ le poly mini de x sur L

alors dans la base $(x^j e_i)_{\substack{0\le i<m \\ 0\le j<n}}$ la matrice de $\times x$ est

$$\begin{pmatrix} 0 & \cdots & 0 & -A_0 \\ I_m & \ddots & & \vdots \\ & \ddots & 0 & -A_{n-2} \\ 0 & & I_m & -A_{n-1} \end{pmatrix}$$

où A_j = matrice de $\times a_j$ dans la base (e_i)

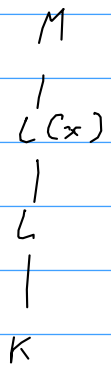
donc $N_{L/K}(x) = \begin{vmatrix} 0 & & -A_0 \\ I_m & \ddots & \vdots \\ & \ddots & -A_{n-1} \end{vmatrix} = (-1)^{m(m-1)} \begin{vmatrix} -A_0 & & \\ -A_1 & I_m & \\ \vdots & & \ddots \\ -A_{n-1} & & I_m \end{vmatrix}$

$$= (-1)^{m^2 n} \det(A_0)$$

$$= (-1)^{mn} \det(A_0)$$

or $\det(A_0) = N_{L/K}\left((-1)^n N_{M/L}(x)\right) = (-1)^{mn} N_{L/K}(N_{M/L}(x))$.

• cas général



$$N_{M/K}(x) = N_{L(x)/K}\left(N_{M/L(x)}(x)\right) \quad \text{par le 1er cas } (x \in L(x))$$

$$= N_{L/K}\left(N_{L(x)/L}\left(N_{M/L(x)}(x)\right)\right) \quad \text{par le 2e cas}$$

$$= N_{L/K}\left(N_{M/L}(x)\right) \quad \text{par le 1er cas } (x \in L(x))$$

□

Exercice : Trouver une preuve plus simple quand M/K est galoisienne. (Utiliser $N_{L/K}(x) = \prod_{\sigma \in Gal(L/K)} \sigma(x)$.)

séparable

Prop : Si L/K finie, alors $\begin{cases} L^2 \longrightarrow K \\ x,y \longmapsto \mathrm{Tr}_{L/K}(xy) \end{cases}$ est une forme bilinéaire non dégénérée.

□ Les éléments de $\mathrm{Hom}_K(L, \bar{K})$ sont $\bar{K}$-linéairement indépendants, donc si $x \in L$ vérifie

$$\forall y \in L \quad \mathrm{Tr}_{L/K}(xy) = 0$$

i.e. $$\sum_{\sigma \in \mathrm{Hom}_K(L,\bar{K})} \sigma(x)\sigma(y) = 0$$

i.e. $$\sum_{\sigma \in \mathrm{Hom}_K(L,\bar{K})} \sigma(x)\sigma = 0$$

on a $\forall x \in \mathrm{Hom}_K(L, \bar{K}) \quad \sigma(x) = 0$ (↑ injectif)

donc $x = 0$. ∎

Rem : Ceci montre, si L/K est finie séparable, que $\mathrm{Tr}_{L/K}$ est surjective (car K-linéaire et $\neq 0$).

Chapitre II : Un peu de cohomologie galoisienne.

① Cohomologie des groupes : H^0 et H^1.

cf. aussi : Cassels & Fröhlich, chap IV : M.F. Atiyah & C.T.C. Wall, Cohomology of Groups

G groupe (éventuellement topologique)

M A-module (par ex. groupe abélien)
+ action de G sur M (continue si G topologique)
A-linéaire (NB : si M = A-module, alors M est un $\underline{A[G]}$-module
χ
anneau des combinaisons formelles A-linéaires d'éléments de G)

Déf : $H^0(G,M) := M^G = \{x \in M \mid \forall \sigma \in G \ \ \sigma(x) = x\}$

$B^1(G,M) := \left\{ \begin{cases} G \to M \\ \sigma \mapsto x - \sigma(x) \end{cases} ; \ x \in M \right\}$ (cobords)
C'est un A-module, dont les éléments vérifient la propriété : $\forall \sigma, \tau \in G \quad c_{\sigma\tau} = c_\sigma + \sigma(c_\tau)$.
(exercice) (En notant $c_\sigma := c(\sigma)$.)
On définit alors :

$Z^1(G,M) := \{ c : G \to M \mid \forall \sigma, \tau \in G \ \ c_{\sigma\tau} = c_\sigma + \sigma(c_\tau) \}$
(continues si G topologique) (cocycles)

$H^1(G,M) := Z^1(G,M) / B^1(G,M)$.
(C'est un A-module)

Exercice : Si $c \in Z^1(G,M)$, alors $c_e = 0_M$ où e = él. neutre de G.

Rem : Il est possible de définir H^0 et H^1 dans le cas où M est un groupe pas forcément commutatif (donc pas un $\mathbb{Z}$-module).

Pour cela, on définit Z^1 de manière analogue :

$$Z^1(G, M) := \{ c : G \to M \mid \forall \sigma, \tau \in G \quad c_{\sigma\tau} = c_\sigma \sigma(c_\tau) \},$$

puis on définit une relation d'équivalence sur Z^1 : deux cocycles c, c' sont cohomologues si il existe $x \in M$ t.q. $\forall \sigma \in G \quad x c'_\sigma = c_\sigma \sigma(x)$.

Exercice : C'est une relation d'équivalence, et si M est commutatif on retrouve l'équivalence mod B^1.

Déf : $H^1(G, M) := Z^1(G, M)/\sim$

C'est un ensemble pointé, i.e. ensemble + élément distingué (classe de l'élément neutre)

(Ça permet de définir une notion de suite exacte, par exemple.)

Exemples : • Si G agit trivialement sur M, alors :

$$H^0(G,M) = M$$
$$B^1(G,M) = 0$$
$$Z^1(G,M) = \mathrm{Hom}_{\text{groupes (top)}}(G,M)$$
$$H^1(G,M) = \text{———————}.$$

• Si $G = 1$, alors

$$H^0(1,M) = M$$
$$H^1(1,M) = 0$$

• Si $G \simeq \mathbb{Z}/n\mathbb{Z}$ $(G = \langle\sigma\rangle)$, alors :

$$H^0(G,M) = M^{\sigma = id}$$

$$\begin{cases} H^1(G,M) \hookrightarrow \mathrm{coker}(id - \sigma) \\ \varepsilon \longmapsto \varepsilon_\sigma \end{cases}.$$

(Ce n'est pas un isom. en général : si $\mathbb{Z}/n\mathbb{Z}$ agit trivialement sur M, on a

$$H^1(\mathbb{Z}/n\mathbb{Z}, M) = n\text{-torsion de } M$$
$$\mathrm{coker}(id - \sigma) = M.$$)

Exercice : L'image de $H^1 \hookrightarrow \mathrm{coker}(id - \sigma)$ est

$$\ker\left(\sum_{\sigma \in G} \sigma\right) / \mathrm{im}(id - \sigma).$$

Si $\left.\begin{matrix}\varphi : G \to G' \\ f : M' \to M\end{matrix}\right\}$ sont des morphismes (de ce qu'il faut) compatibles i.e.

$$\forall \sigma \in G \quad \forall x \in M' \quad \sigma(f(x)) = f((\varphi\sigma)(x)),$$

alors ils induisent des morphismes

$H^i(G, \cdot)$ est un foncteur.

$$H^0(G', M') \longrightarrow H^0(G, M) \qquad (x \mapsto f(x))$$
$$H^1(G', M') \longrightarrow H^1(G, M) \qquad (c \mapsto f \circ c \circ \varphi).$$

(exercice : vérifier)

En particulier, si H est un sous-groupe (fermé) de G, on obtient

$$\mathrm{Res} : H^i(G, M) \longrightarrow H^i(H, M) \qquad \text{(Restriction)}$$

Si H est un sous-groupe (fermé) distingué, on a

$$\mathrm{Inf} : H^i(G/H, M^H) \longrightarrow H^i(G, M) \qquad \text{(inflation)}$$

et on a une suite exacte

$$0 \longrightarrow H^1(G/H, M^H) \xrightarrow{\mathrm{Inf}} H^1(G, M) \xrightarrow{\mathrm{Res}} H^1(H, M).$$

□ • Si $c \in Z^1(G/H, M^H)$ vérifie $\mathrm{Inf}(c) = 0$,
il existe $x \in M$ t.q.
$$\forall \sigma \in G \quad c_\sigma = x - \sigma(x)$$
alors $\forall \tau \in H \quad x - \tau(x) = c_\tau = c_e = 0_M$,

donc $\tau(x) = x$
donc $x \in M^H$, donc $c \in B^1(G/H, M^H)$.

• Res o Inf $= 0$ car $H \longrightarrow G \longrightarrow G/H$ (la composée) est triviale

• Soit $c \in Z^1(G, M)$ tel qu'il existe $x \in M$ t.q.
$$\forall \sigma \in H \quad c_\sigma = x - \sigma(x).$$
Quitte à retrancher $\sigma \mapsto x - \sigma(x)$ de c, on peut supposer $\forall \sigma \in H \quad c_\sigma = 0$.
On a $\forall \sigma \in G \ \forall \tau \in H \quad c_{\sigma\tau} = c_\sigma + \sigma(c_\tau)$
$= c_\sigma$,
donc c induit une application $G/H \longrightarrow M$.
De plus, $\forall \sigma \in H \ \forall \tau \in G \quad c_{\sigma\tau} = c_\sigma + \sigma(c_\tau)$
$= \sigma(c_\tau)$
or $c_{\sigma\tau} = c_{\tau\sigma'}$ car H distingué, $\sigma' \in H$
$= c_\tau$,
donc c est à valeurs dans M^H.
Donc c vient d'un élément de $H^1(G/H, M^H)$. ⊠

Rappel : cas de l'action triviale

Si G agit trivialement sur M :

$$H^1(G, M) = \mathrm{Hom}_{\text{groupes}}(G, M)$$

$$\mathrm{Res} : \begin{cases} \mathrm{Hom}(G, M) \longrightarrow \mathrm{Hom}(H, M) \\ f \longmapsto f|_H \end{cases}$$

$$\mathrm{Inf} : \begin{cases} \mathrm{Hom}(G/H, M) \longrightarrow \mathrm{Hom}(G, M) \\ f \longmapsto f \circ \pi \end{cases}$$

où $\pi : G \twoheadrightarrow G/H$ proj. canonique.

$$1 \longrightarrow H \longrightarrow G \longrightarrow G/H \longrightarrow 1$$

donne (par $\mathrm{Hom}(\cdot, M)$) :

$$1 \longrightarrow \mathrm{Hom}(G/H, M) \longrightarrow \mathrm{Hom}(G, M) \longrightarrow \mathrm{Hom}(H, M)$$

Déf : Si H est un sous-groupe (fermé) de G, et si M est un A-module muni d'une action (continue) de H, l'induit de H à G est le A-module :

$$\mathrm{Ind}_H^G(M) = \left\{ \begin{array}{l} \text{applications (continues) } f : G \longrightarrow M \\ \text{t.q. } \forall \sigma \in H \quad \forall x \in G \quad f(\sigma x) = \sigma(f(x)) \end{array} \right\}$$

On a une action de G sur $\mathrm{Ind}_H^G(M)$ définie par

$$\forall \sigma \in G \quad \sigma(f)(x) = f(\underbrace{x\sigma}_{\in G})$$

Prop : $\left\{ \begin{array}{ccc} \mathrm{Ind}_H^G(M) & \longrightarrow & M \\ f & \longmapsto & f(R_G) \end{array} \right.$ est un morphisme de A-modules, compatible avec l'injection $H \subseteq G$.

□ morphisme : exercice

compatibilité : si $\sigma \in H$ et $f \in \mathrm{Ind}_H^G(M)$, on a

$$\sigma(f)(R_G) \underset{\text{déf de l'action de } G}{=} f(R_G \sigma) = f(\sigma) = f(\sigma R_G) = \underset{\text{déf de } \mathrm{Ind}_H^G(M) \text{ + } \sigma \in H}{\sigma(f(R_G))}$$

Prop : Le morphisme ci-dessus induit un isomorphisme

$$\mathrm{Hom}_G(N, \mathrm{Ind}_H^G(M)) \simeq \mathrm{Hom}_H(N, M)$$

pour tout A-module N avec action de G.

Ind_H^G est le foncteur adjoint à droite de la restriction (de l'action) à H

□ $\mathrm{Hom}_G(N, \mathrm{Ind}_H^G(M)) \xrightarrow{\sim} \mathrm{Hom}_H(N, M)$

$$\varphi \longmapsto (x \longmapsto \varphi(x)(R_G))$$

$$(x \longmapsto y \longmapsto \psi(y(x))) \longmapsto \psi$$

sont l'isomorphisme et sa réciproque. □

fin cours n°7

Rem : . Si M est muni d'une action de G, on obtient

$$id_M \in Hom_H(M, M) \xrightarrow{\sim} Hom_G(M, Ind_H^G(M))$$

$$\downarrow$$

$$\begin{cases} x \longmapsto \sigma \longmapsto \sigma(x) \\ M \longrightarrow Ind_H^G(M) \end{cases}$$

section de $\begin{cases} Ind_H^G(M) \longrightarrow M \\ f \longmapsto f(e_\sigma) \end{cases}$

(Ce n'est en général pas un isomorphisme.)

. Si $H = 1$, M un A-module, alors

$Ind_1^G(M) = \{$ applications $f : G \longrightarrow M \}$.

Lemme de Shapiro

Prop : Le morphisme $\mathrm{Ind}_H^G(M) \to M$ induit des isomorphismes

$$H^i(G, \mathrm{Ind}_H^G(M)) \longrightarrow H^i(H, M) \qquad (\forall i \in \{0,1\})$$

D $\quad H^0(G, \mathrm{Ind}_H^G(M)) = \{ f : G \to M^H \text{ constantes} \}$

$$H^0(G, \mathrm{Ind}_H^G(M)) \xrightarrow{\sim} H^0(H, M)$$
$$f \longmapsto f(e_G)$$
$$(g \mapsto x) \longleftarrow\!\shortmid\ x$$

$$\begin{cases} H^1(G, \mathrm{Ind}_H^G(M)) \longrightarrow H^1(H, M) \\ c \longmapsto (\sigma \mapsto c_\sigma(e_G)) \end{cases}$$

source : J. Stix Grading degree for dimension in the section conjecture: the non-abelian Shapiro lemma + variants

On a $Z^1(G, \mathrm{Ind}_H^G(M)) = \{ c : G \times G \to M \mid \dots \}$

(cocycle) $\quad \forall \sigma, \tau, x \in G \qquad c_{\sigma\tau}(x) = c_\sigma(x) + c_\tau(x\sigma)$

(Ind_H^G) $\quad \forall \sigma, x \in G \ \forall \tau \in H \qquad c_\sigma(\tau x) = \tau(c_\sigma(x))$

Si $c \in Z^1(G, \mathrm{Ind}_H^G(M))$, on a bien $\sigma \mapsto c_\sigma(e_G) \in Z^1(H, M)$.

Montrons la surjectivité. Soit $c' \in Z^1(H, M)$.

Soient $\pi : G \to H\backslash G$ la projection canonique

$\rho : H\backslash G \to G$ un choix de relèvements

$\omega := \rho \circ \pi : G \to G$

$\gamma : \begin{cases} G \to H \\ \sigma \mapsto \sigma\,\omega(\sigma)^{-1} \end{cases}$ ($\in H$ par déf de ρ)

Soit $c \in Z^1(G, \mathrm{Ind}_H^G(M))$ défini par :

$$\forall \sigma, x \in G \quad c_\sigma(x) := c'_{\gamma(x\sigma)} - c'_{\gamma(x)}.$$

On a alors

$$\forall \sigma, \tau, x \in G \quad c_{\sigma\tau}(x) = c'_{\gamma(x\sigma\tau)} - c'_{\gamma(x)}$$

$$= c'_{\gamma(x\sigma\tau)} - c'_{\gamma(x\sigma)} + c'_{\gamma(x\sigma)} - c'_{\gamma(x)}$$

$$= c_\tau(x\sigma) + c_\sigma(x)$$

$$= c_\sigma(x) + \sigma(c_\tau)(x)$$

et

$$\forall \sigma, x \in G \quad \forall \tau \in H$$

$$c_\sigma(\tau x) = c'_{\gamma(\tau x \sigma)} - c'_{\gamma(\tau x)}$$

Or $\gamma(\tau x) = \tau x\, w(\tau x)^{-1}$

et $w(\tau x) = \rho(\pi(\tau x)) = \rho(\pi(x)) = w(x)$

donc $\gamma(\tau x) = \tau\gamma(x)$

$$c_\sigma(\tau x) = c'_{\tau\gamma(x\sigma)} - c'_{\tau\gamma(x)}$$

$$= c'_\tau + \tau\left(c'_{\gamma(x\sigma)}\right) - c'_\tau - \tau\left(c'_{\gamma(x)}\right)$$

$$= \tau\left(c'_{\gamma(x\sigma)} - c'_{\gamma(x)}\right)$$

$$= \tau\left(c_\sigma(x)\right)$$

donc on a bien $c \in Z^1(G, \mathrm{Ind}_H^G(M))$.

De plus $c_\sigma(e_G) = c'_{\gamma(\sigma)} - c'_{\gamma(e_G)}$,

donc $\forall \sigma \in H \quad c_\sigma(e_G) = c'_{\sigma\gamma(e_G)} - c'_{\gamma(e_G)}$

$$= -c'_\sigma + (\sigma - \mathrm{id})\left(c'_{\gamma(e_G)}\right),$$

qui est cohomologue à c'. (On prendra même choisi ρ de sorte que $\gamma(e_G) = e_G$)

Montrons l'injectivité. Soient $c, c' \in Z^1(G, \mathrm{Ind}_H^G(M))$ et $x \in M$ t.q.

$$\forall \sigma \in H \quad c_\sigma(\ell_\sigma) - c'_\sigma(\ell_\sigma) = x - \sigma(x),$$

et soit $f \in \mathrm{Ind}_H^G(M)$ défini par

$$\forall \sigma \in G \quad f(\sigma) := x - c_\sigma(\ell_\sigma) + c'_\sigma(\ell_\sigma).$$

(Rem : $\forall \sigma \in H \; f(\sigma) = \sigma(x)$.)

On a $\forall \tau \in H \; \forall \sigma \in G$

$$\begin{aligned} f(\tau\sigma) &= x - c_{\tau\sigma}(\ell_\sigma) + c'_{\tau\sigma}(\ell_\sigma) \\ &= x - \big(c_\tau + \tau(c_\sigma)\big)(\ell_\sigma) + \big(c'_\tau + \tau(c'_\sigma)\big)(\ell_\sigma) \\ &= x - c_\tau(\ell_\sigma) - c_\sigma(\tau) + c'_\tau(\ell_\sigma) + c'_\sigma(\tau) \\ &= x - \big(c_\tau(\ell_\sigma) - c'_\tau(\ell_\sigma)\big) - \tau\big(c_\sigma(\ell_\sigma) - c'_\sigma(\ell_\sigma)\big) \\ &\qquad \text{car } \tau \in H \\ &= x - \big(x - \tau(x)\big) - \tau\big(x - f(\sigma)\big) \\ &= \tau(f(\sigma)) \end{aligned}$$

[donc on a bien $f \in \mathrm{Ind}_H^G(M)$],

alors $\forall \sigma, \tau \in G$

$$\begin{aligned} c_\sigma(\tau) - c'_\sigma(\tau) &= \big(\tau(c_\sigma) - \tau(c'_\sigma)\big)(\ell_\sigma) \\ &= \big(c_{\tau\sigma} - c_\tau - c'_{\tau\sigma} + c'_\tau\big)(\ell_\sigma) \\ &= \big(c_{\tau\sigma}(\ell_\sigma) - c'_{\tau\sigma}(\ell_\sigma)\big) - \big(c_\tau(\ell_\sigma) - c'_\tau(\ell_\sigma)\big) \\ &= f(\tau\sigma) + f(\tau) \\ &= \big(f - \sigma(f)\big)(\tau) \end{aligned}$$

donc $\forall \sigma \in G \quad c_\sigma - c'_\sigma = f - \sigma(f)$,

donc c et c' sont cohomologues. ∎

On retrouve l'application de restriction :
si M est un $A[G]$-module on a vu

$$\begin{cases} M \longrightarrow \mathrm{Ind}_H^G(M) \\ x \longmapsto (\sigma \mapsto \sigma(x)) \end{cases}$$

d'où $H^i(G, M) \longrightarrow H^i(G, \mathrm{Ind}_H^G(M)) \simeq H^i(H, M)$

exercice : c'est Res.

Si $[G:H] < \infty$ on peut définir un morphisme de $A[G]$-modules :

$$\begin{cases} \mathrm{Ind}_H^G(M) \longrightarrow M \\ f \longmapsto \sum_{\bar{\sigma} \in G/H} \sigma(f(\sigma^{-1})) \end{cases}$$

↑ Ceci ne dépend pas du relèvement σ de $\bar{\sigma}$.

(exercice : vérifier)

qui donne la corestriction :

$$\mathrm{Cor} : H^i(H, M) \simeq H^i(G, \mathrm{Ind}_H^G(M)) \longrightarrow H^i(G, M)$$

Exercice : En 0 : $\begin{cases} H^0(H, M) \to H^0(G, M) \\ x \mapsto \sum_{\bar{\sigma} \in G/H} \sigma(x) \end{cases}$.

$\mathrm{Cor} \circ \mathrm{Res} : H^i(G, M) \longrightarrow H^i(G, \mathrm{Ind}_H^G(M)) \longrightarrow H^i(G, M)$

↑ induit par $x \mapsto (\sigma \mapsto \sigma(x))$

↑ induit par $f \mapsto \sum_{\bar{\sigma} \in G/H} \sigma(f(\sigma^{-1}))$

$$\sum_{\bar{\sigma} \in G/H} \sigma(\alpha^{-1}(x)) = [\alpha : H]\, x$$

donc $\mathrm{Cor} \circ \mathrm{Res} = [G:H]\, \mathrm{id}$.

Corollaire : • Si $[G:H] < \infty$, alors Res et Cor sont de $[G:H]$-torsion.
• Si $|G| < \infty$, alors $H^1(G, M)$ est de $|G|$-torsion.
En effet, $\mathrm{Res} : H^1(G, M) \longrightarrow H^1(1, M) = 0$,
et on applique le point précédent.

Si $0 \to M' \xrightarrow{\iota} M \xrightarrow{\pi} M'' \to 0$ est une suite exacte de $A[G]$-modules, alors on a

$$0 \to \underset{\| M'^G}{H^0(G, M')} \to \underset{\| M^G}{H^0(G, M)} \to \underset{\| M''^G}{H^0(G, M'')} \quad \text{exacte}$$

(exercice : facile)

Le foncteur $H^1(G, \cdot)$ donne une suite

$$H^1(G, M') \to H^1(G, M) \to H^1(G, M'') \qquad (\text{composée} = 0)$$

qui est aussi exacte : si $c \in Z^1(G, M)$ est nul dans $H^1(G, M'')$, c'est qu'il existe $x \in M''$ tq.

$$\forall \sigma \in G \quad \pi(c_\sigma) = x - \sigma(x).$$

Soit $\tilde{x} \in M$ tq $\pi(\tilde{x}) = x$, quitte à soustraire $\sigma \mapsto \tilde{x} - \sigma(\tilde{x})$ de c, on peut supposer

$$\forall \sigma \in G \quad \pi(c_\sigma) = 0$$

$$\text{i.e. } c_\sigma \in M',$$

ce qui montre l'exactitude.

On définit un morphisme

$$\delta : H^0(G, M'') \longrightarrow H^1(G, M')$$

de la manière suivante :

Si $x \in H^0(G, M'') \ (= M''^G)$,

soit $\tilde{x} \in M$ t.q. $\pi(\tilde{x}) = x$,

et soit $c \in Z^1(G, M')$ défini par

$\forall \sigma \in G \quad i(c_\sigma) = \tilde{x} - \sigma(\tilde{x}) \quad (\in i(M') \text{ car } \pi(\tilde{x} - \sigma(\tilde{x})) = x - \sigma(x) = 0)$

Si $\check{x}$ est un autre relèvement de x

$\rightarrow c_\sigma = \check{x} - \sigma(\check{x})$

alors $i(c_\sigma - \check{c}_\sigma) = \underbrace{(\tilde{x} - \check{x})}_{\in i(M')} - \sigma(\tilde{x} - \check{x})$

donc c définit un élément de $H^1(G, M')$ qui ne dépend pas du choix de $\tilde{x}$.

Par construction, δ est à valeurs dans $\ker(H^1(G, M') \to H^1(G, M))$.

Prop : La suite

$$0 \to H^0(G, M') \to H^0(G, M) \to H^0(G, M'') \xrightarrow{\delta} H^1(G, M') \to H^1(G, M) \to H^1(G, M'')$$

est exacte.

D. • Si x vient de $H^0(G, M)$ dans la déf de δ, on peut prendre $\tilde{x} \in M^G$, d'où $\delta(x) = c = 0$.

• Réciproquement, si $x \in \ker \delta$, il existe $x' \in M'$ t.q. $\forall \sigma \in G \quad \tilde{x} - \sigma(\tilde{x}) = i(x' - \sigma(x'))$,

donc $\tilde{x} - i(x') \in M^G$, donc $x \in \pi(M^G)$.

• Si $\bar{c} \in \ker(H^1(G, M') \to H^1(G, M))$,

il existe $\tilde{x} \in M$ t.q. $\forall \sigma \in G \quad i(c_\sigma) = \tilde{x} - \sigma(\tilde{x})$,

donc $x := \pi(\tilde{x}) \in H^0(G, M'')$, et $\delta(x) = \bar{c}$. ∎

Ajout : cas de l'action triviale

G agit trivialement sur M

$H^0(G, M) = M$

$H^1(G, M) = \mathrm{Hom}_{\text{groupes}}(G, M)$

$\mathrm{Inf}_H^G(M) = \{\text{applications } G \to M\}$ (où $H \backslash G \to M$)

+ action par $\sigma \cdot f = f(\cdot \sigma)$

$H^0\left(G, \mathrm{Inf}_H^G(M)\right) = \{\text{applications } H\backslash G \to M \text{ constantes}\} \simeq M$

$\mathrm{Cor} : \begin{cases} M \to M \\ x \mapsto [G:H]\, x \end{cases}$

$\mathrm{Cor} : \begin{cases} \mathrm{Hom}(H, M) \to \mathrm{Hom}(G, M) \\ f \mapsto \left(\sigma \mapsto \sum_{\tilde{\tau} \in H\backslash G} f(\tilde{\tau} \sigma \tau'^{-1})\right) \end{cases}$

τ' choix de relèvements ; où τ' relève $\tilde{\tau}\sigma \in H\backslash G$.

$\delta = 0$, et la suite exacte donne

$0 \to M' \to M \to M'' \to 0$ exacte

$0 \to \mathrm{Hom}(G, M') \to \mathrm{Hom}(G, M) \to \mathrm{Hom}(G, M'')$ exacte

fin cours n°8

② Cohomologie galoisienne

C'est le cas où G est un groupe de Galois.

Th (Hilbert 90) :
Si L/K galoisienne finie, alors
$$H^1(\mathrm{Gal}(L/K), L^\times) = 1 .$$
($L^\times$: $\mathbb{Z}$-module + action de $\mathrm{Gal}(L/K)$)

▭ Soit $\varepsilon \in Z^1_{L\text{-linéaire}}(\mathrm{Gal}(L/K), L^\times)$. (On a en particulier $\varepsilon_{\mathrm{id}} = 1$.)
Par indépendance des éléments de $\mathrm{Gal}(L/K)$, on a
$$\sum_{\sigma \in \mathrm{Gal}(L/K)} \varepsilon_\sigma \sigma \neq 0 .$$
Soit $x \in L$ t.q. $\underbrace{\sum_{\sigma \in \mathrm{Gal}(L/K)} \varepsilon_\sigma \sigma(x)}_{y} \neq 0$

On a alors
$$\forall \tau \in \mathrm{Gal}(L/K) \quad \tau(y) = \sum_\sigma \tau(\varepsilon_\sigma)(\varepsilon\sigma)(x)$$
$$= \sum_\sigma \frac{\varepsilon_{\tau\sigma}}{\varepsilon_\tau} (\tau\sigma)(x)$$
$$= \frac{1}{\varepsilon_\tau} \underbrace{\sum_\sigma \varepsilon_{\tau\sigma} (\tau\sigma)(x)}_{y}$$
donc $\varepsilon_\tau = \dfrac{y}{\tau(y)}$.

On a donc $\varepsilon \in B^1(\mathrm{Gal}(L/K), L^\times)$. ▭

Th (Hilbert 90 additif) :

On a $H^1(\mathrm{Gal}(L/K), L) = 0$.

▷ Le th de la base normale montre que

$$L \simeq \underset{\mathbb{Z}[\mathrm{Gal}(L/K)]\text{-module}}{\mathrm{Ind}_1^{\mathrm{Gal}(L/K)} K}$$

donc $H^1(\mathrm{Gal}(L/K), L) \simeq H^1(\mathrm{Gal}(L/K), \mathrm{Ind}_1^{\mathrm{Gal}(L/K)} K)$

$\simeq H^1(1, K)$

$\simeq 0$. ◁

Rem : Plus généralement, on a

$$H^1(\mathrm{Gal}(L/K), GL_n(K)) = 1.$$

↑ non commutatif ! (H^1 ensemble pointé)

cf. Serre, Corps locaux, chap X.

$$H^1(\mathrm{Gal}(L/K), SL_n(K)) = 1$$

Rem : Cas d'une extension cyclique : $\mathrm{Gal}(L/K) \simeq \mathbb{Z}/n\mathbb{Z}$, $\sigma \leftrightarrow 1$

$$1 \simeq H^1(\mathrm{Gal}(L/K), L^\times) \simeq \frac{N_{L/K}^{-1}(\{1_K\})}{\left\{\frac{x}{\sigma(x)} \,;\, x \in L^\times\right\}}$$

(déjà vu : cf. $H^1(\mathbb{Z}/n\mathbb{Z}, M) \hookrightarrow \mathrm{coker}(\mathrm{id} - \sigma)$.)

Donc si $y \in L^\times$ vérifie $N_{L/K}(y) = 1$, alors

$\exists x \in L^\times \quad y = \frac{x}{\sigma(x)}$.

Application : triplets pythagoriciens.

$\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$

conjugaison complexe $\longleftrightarrow 1$

Si $x+iy \in \mathbb{Q}[i]$ vérifie $N_{\mathbb{Q}(i)/\mathbb{Q}}(x+iy) = 1$

i.e. si $x, y \in \mathbb{Q}$ vérifient $x^2+y^2 = 1$,

alors $\exists\, u+iv \in \mathbb{Q}[i]$ $\quad x+iy = \dfrac{u+iv}{u-iv}$

$$= \frac{(u+iv)^2}{u^2+v^2}$$

$$= \frac{u^2-v^2}{u^2+v^2} + i\,\frac{2uv}{u^2+v^2}$$

i.e. $\exists\, u, v \in \mathbb{Q}$ $\quad x = \dfrac{u^2-v^2}{u^2+v^2}$ et $y = \dfrac{2uv}{u^2+v^2}$.

On retrouve les points de $\{(x,y) \in \mathbb{Q}^2 \,/\, x^2+y^2 = 1\}$.

(3) Extensions cycliques.

a) $n \geq 1$ entier

K = corps

t.q. : car $K \nmid n$

K contient une racine primitive n-ième de 1

$(\mu_n(\bar{K}) \subseteq K)$

Prop : (i) Si L/K est une extension cyclique de degré n (i.e. L/K galoisienne et $Gal(L/K) \simeq \mathbb{Z}/n\mathbb{Z}$) alors $\exists \alpha \in L$ $L = K[\alpha]$, et $\alpha^n \in K$ (i.e. le poly mini de α sur K est de la forme $X^n - a$, $a \in K$).

(ii) Réciproquement, si $a \in K$, toute extension $K[\alpha]/K$ où α est racine de $X^n - a$ est cyclique, de degré d/n, et $\alpha^d \in K$.

□ (i) : $Gal(L/K) = \langle \sigma \rangle$

On a $N_{L/K}(\varphi^{-1}) = \varphi^{-n} = 1$,

$\varphi \in K$

donc (H90) $\exists \alpha \in L^\times$ $\varphi^{-1} = \frac{\alpha}{\sigma(\alpha)}$

i.e. $\sigma(\alpha) = \varphi\alpha$

Comme $\varphi \in K$, on en déduit $\forall i \in \mathbb{Z}$ $\sigma^i(\alpha) = \varphi^i \alpha$

Donc α a n conjugués distincts, or $[L:K] = n$,

donc $L = K[\alpha]$, et le poly mini de α est

$$\prod_{i=0}^{n-1} (X - \varphi^i \alpha) = X^n - \alpha^n \in K[X].$$

(ii) : $X^n - a$ est scindé sur $K[\alpha]$, de racines $\varphi^i\alpha$, $0 \leq i < n$.

Donc $K(\alpha)/K$ est galoisienne.

On a une application $\begin{cases} \mathrm{Gal}(K[\alpha]/K) \longrightarrow \mu_n \simeq \mathbb{Z}/n\mathbb{Z} \\ \sigma \longmapsto \dfrac{\alpha}{\sigma(\alpha)} \end{cases}$

$$\in H^1\left(\mathrm{Gal}(K[\alpha]/K), \mu_n(\bar{K})\right)$$

$$= \mathrm{Hom}_{\text{groupes}}\left(\mathrm{Gal}(K[\alpha]/K), \mu_n(\bar{K})\right)$$

car $\mu_n(\bar{K}) \subseteq K$ donc l'action sur μ_n est triviale.

Ce morphisme est injectif : si $\sigma \mapsto 1$, alors $\dfrac{\alpha}{\sigma(\alpha)} = 1$, donc $\alpha \in K[\alpha]^{\langle\sigma\rangle}$, or α engendre $K[\alpha]$ donc $|\langle\sigma\rangle| = 1$, donc $\sigma = 1$.

Donc $\mathrm{Gal}(K[\alpha]/K) \hookrightarrow \mathbb{Z}/n\mathbb{Z}$, et tout sous-groupe d'un groupe cyclique est cyclique, donc $\mathrm{Gal}(K[\alpha]/K)$ est cyclique. Si $d = |\mathrm{Gal}(K[\alpha]/K)| \ (= [K[\alpha] : K])$, alors $d \mid n$. L'image de $\mathrm{Gal}(K[\alpha]/K)$ dans μ_n est engendrée par $\zeta^{n/d}$.

Si σ est un générateur de $\mathrm{Gal}(K[\alpha]/K)$, alors $\sigma^d = \mathrm{id}$, et $\sigma(\alpha^d) = \sigma(\alpha)^d = \alpha^d \underbrace{\left(\frac{\alpha}{\sigma(\alpha)}\right)^d}_{=1} = \alpha^d$,

donc $\alpha^d \in K[\alpha]^{\langle\sigma\rangle} = K$. ∎

Exemple : Toute extension de degré 2 de K est de la forme $K[\sqrt{a}]$.

($\bar{K}/2\mathbb{Z}$ est cyclique, $-1 \in \bar{K}$.) ↑ avec car $K \neq 2$

ex. $K(a^{1/n})/K$, $K(b^{1/n})/K$ cycliques de degré n

Prop : Si $a, b \in K$, $a^{1/n}, b^{1/n} \in \bar{K}$ alors $K(a^{1/n}) = K(b^{1/n})$ ssi a et b engendrent le même sous-groupe de $K^\times / K^{\times n}$.

$\square$ $\Leftarrow$:

si $b = a^i t^n$ $\quad i \in \mathbb{Z}$, $t \in K^\times$,

alors $b^{1/n} = a^{i/n} \underbrace{t}_{\in K^\times} \zeta^* \in K(a^{1/n})$,

donc $K(b^{1/n}) \subseteq K(a^{1/n})$,

et réciproquement.

$\Rightarrow$: si $K(a^{1/n}) = K(b^{1/n})$,

alors $b^{1/n} \in K(a^{1/n})$,

$$b^{1/n} = \sum_{i=0}^{n-1} u_i a^{i/n}, \quad u_i \in K.$$

Soit σ générateur de $\mathrm{Gal}(K(a^{1/n})/K) \simeq \mathbb{Z}/n\mathbb{Z}$,

alors $\sigma(a^{1/n}) = a^{1/n} \zeta^k$

$\sigma(b^{1/n}) = b^{1/n} \zeta^l$ $\quad k, l \in (\mathbb{Z}/n\mathbb{Z})^\times$

Il faut que ζ^k, ζ^l soient des racines primitives n-ièmes pour avoir n conjugués différents

et $\sigma(b^{1/n}) = \sum_{i=0}^{n-1} u_i \zeta^{ik} a^{i/n}$

donc $\forall i \in \{0, \dots, n-1\}$ $u_i \zeta^l = u_i \zeta^{ik}$.

Soit $i_0 \in \{0, \dots, n-1\}$ t.q. $l \equiv i_0 k$,

$(k, l \in (\mathbb{Z}/n\mathbb{Z})^\times)$

alors $u_i = 0$ si $i \neq i_0$,

et $b^{1/n} = u_{i_0} a^{i_0/n}$

(+ réciproquement en échangeant a et b). $\square$

b) Extensions d'Artin-Schreier

K = corps car $K = p > 0$

Th (Artin-Schreier) :

(i) Soit L/K ext. cyclique de degré p. Alors $\exists \alpha \in L$ t.q. $L = K(\alpha)$ et $\alpha^p - \alpha \in K$.
(i.e. $\exists a \in K$ t.q. le poly minimal de α sur K soit $X^p - X - a$.)

(ii) Réciproquement si $a \in K$, le poly $X^p - X - a \in K[X]$ est soit scindé soit irréductible sur K. S'il est irréductible alors son corps de rupture est une ext. cyclique de degré p de K.

▷ (i) : car $K = p$, $[L : K] = p$,
donc $\mathrm{Tr}_{L/K}(1) = 0$.

Or $H^1(\mathrm{Gal}(L/K), L) = 0$ $\mathrm{Gal}(L/K) = \langle \sigma \rangle$

$\| Z$

$\ker \mathrm{Tr}_{L/K} / \mathrm{im}(\mathrm{id} - \sigma)$

donc $\exists \alpha \in L$ $\alpha - \sigma(\alpha) = 1$

i.e. $\sigma(\alpha) = \alpha - 1$

$\forall i \in \mathbb{Z}/p\mathbb{Z}$ $\sigma^i(\alpha) = \alpha - i$

p conjugués distincts

On a donc $[K[\alpha] : K] \geq p$
or $\alpha \in L$ donc $K[\alpha] = L$.

De plus $\sigma(\alpha^p - \alpha) = (\alpha - 1)^p - (\alpha - 1) = \alpha^p - \alpha$
donc $a := \alpha^p - \alpha \in K$ et $X^p - X - a$ est le poly minimal de α (car annulateur de degré p).

(ii) : $a \in K$

Si $\alpha \in \bar{K}$ racine de $X^p - X - a$, alors

$\forall i \in \mathbb{Z}/p\mathbb{Z}$ $\alpha + i$ est aussi racine

(p racines distinctes)

Donc :

- si $X^p - X - a$ a une racine dans K, alors il est scindé sur K.
- sinon, soit L un corps de rupture d'un facteur irréductible de $X^p - X - a \in K[X]$. Soit $\alpha \in L$ racine de $X^p - X - a$ dans $K[X]$

alors $X^p - X - a$ est scindé sur L, de racines $\alpha + i$, $i \in \mathbb{Z}/p\mathbb{Z}$. ($\rightarrow L/K$ galoisienne)

Si $\sigma \in Gal(L/K) \setminus \{id\}$, alors

$\alpha - \sigma(\alpha) \in (\mathbb{Z}/p\mathbb{Z})^\times$

si $\alpha - \sigma(\alpha) = 0$, alors $\alpha \in L^{\langle\sigma\rangle}$

mais α engendre L donc $\sigma = id$.

donc $\alpha - \sigma(\alpha)$ est un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$,

donc α a p conjugués distincts (tous les $\alpha + i$, $i \in \mathbb{Z}/p\mathbb{Z}$)

et $Gal(L/K) \simeq \langle\sigma\rangle$.

donc L/K cyclique.

donc $X^p - X - a$ irréductible sur K.

□

Rem : On les extensions cycliques de degré p^*, cf. travaux de Witt (Alio dans Lang, Algebra).

(4) Théorie de Kummer.

$n \geq 1$ entier

K corps car $K \nmid n$. $\zeta \in K$ racine primitive n-ième de 1.

But : classifier les extensions de K abéliennes d'exposant n.

Rem : Un groupe abélien fini d'exposant n est un sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^k$, k entier ≥ 0.

Si L/K galoisienne finie, on a une suite exacte
$G = \mathrm{Gal}(L/K)$

$$1 \longrightarrow \mu_n(K) \longrightarrow L^\times \xrightarrow[x \mapsto x^n]{} L^{\times n} \longrightarrow 1$$

On en déduit

$$1 \to \underbrace{H^0(G, \mu_n(K))}_{= \mu_n(K) \text{ (action triviale)}} \to \underbrace{H^0(G, L^\times)}_{= K^\times} \xrightarrow[x \mapsto x^n]{} \underbrace{H^0(G, L^{\times n})}_{= K^\times \cap L^{\times n}} \to \underbrace{H^1(G, \mu_n(K))}_{= \mathrm{Hom}_{\text{groupe}}(G, \mu_n(K)) \text{ (action triviale)}} \to \underbrace{H^1(G, L^\times)}_{= 1 \text{ par Hilbert 90}}$$

d'où

$$\frac{K^\times \cap L^{\times n}}{K^{\times n}} \simeq \mathrm{Hom}_{\text{groupe}}(G, \mu_n(K))$$

$$\alpha^n \in K^\times \ (\alpha \in L^\times) \longmapsto \left(\sigma \mapsto \frac{\alpha}{\sigma(\alpha)}\right).$$

fin cours n°9

Si G est d'ordre n

Rem : $\check{} \mathrm{Hom}_{\text{groupe}}(G, \mu_n(K))$ est le dual de Pontryagin de G.

Il est $\simeq G$ non canoniquement (exercice).

(On a $\mathrm{Hom}_{gr}(\mathrm{Hom}_{gr}(G, \mu_n), \mu_n) \simeq G$ canoniquement.)

preuve de la remarque : cf théorie des représentations des groupes abéliens.

$\mathrm{Hom}_{gr}(G, \mu_n(K)) \simeq \mathrm{Hom}_{gr}(G, \mathbb{C}^\times)$ car G est d'exposant n.

$G \simeq \prod \mathbb{Z}/n_i\mathbb{Z}$

$\mathrm{Hom}(G, \mathbb{C}^\times) \simeq \prod \mathrm{Hom}(\mathbb{Z}/n_i\mathbb{Z}, \mathbb{C}^\times)$

$\simeq \prod \mathbb{Z}/n_i\mathbb{Z}$

$\simeq G$

Il suffit de montrer $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{C}^\times) \simeq \mathbb{Z}/n\mathbb{Z}$.

$$\begin{cases} \mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{C}^\times) \xrightarrow{\sim} \mu_n(\mathbb{C}) \simeq \mathbb{Z}/n\mathbb{Z} \\ f \longmapsto f(1) \end{cases}$$

Morphisme canonique avec le bidual :

$$\begin{cases} G \longrightarrow \mathrm{Hom}(\mathrm{Hom}(G, \mathbb{C}^\times), \mathbb{C}^\times) \\ \sigma \longmapsto (f \mapsto f(\sigma)) \end{cases}$$

On égalité des cardinaux, il suffit de montrer l'injectivité.

Lemme : Si H sous-groupe de G, G abélien,

$\mathrm{Hom}(G, \mathbb{C}^\times) \xrightarrow{\text{res}} \mathrm{Hom}(H, \mathbb{C}^\times)$.

□ G étant fini, il suffit (par récurrence) de le montrer dans le cas où G/H est cyclique. Si $\langle \bar{x} \rangle = G/H$, soit $\zeta \in \mathbb{C}^\times$ t.q. $f(x^{(G:H)}) = \zeta^{(G:H)}$.

On définit $F : G \to \mathbb{C}^\times$ par $F(x^i h) = \zeta^i f(h)$, $i \in \mathbb{Z}$, $h \in H$

alors $F \in \mathrm{Hom}(G, \mathbb{C}^\times)$ et $F|_H = f$. ☐

Si $\sigma \in G$, $\sigma \neq 1_G$, on a $\mathrm{Hom}(\langle\sigma\rangle, \mathbb{C}^\times) \simeq \langle\sigma\rangle \neq 1$ (cyclique $\neq 1$)

donc (par le lemme) $\exists f \in \mathrm{Hom}(G, \mathbb{C}^\times)$ $f|_{\langle\sigma\rangle} \neq 1$

i.e. $f(\sigma) = 1$,

ce qui montre l'injectivité.

Rem : Le foncteur $\mathrm{Hom}(\cdot, \mathbb{C}^\times)$ est exact sur les groupes abéliens finis.

Si $1 \to H \to G \to G/H \to 1$, G abélien fini,

on a $1 \to \mathrm{Hom}(G/H, \mathbb{C}^\times) \to \mathrm{Hom}(G, \mathbb{C}^\times) \to \mathrm{Hom}(H, \mathbb{C}^\times)$,

et la surjectivité à droite a été démontrée

Corollaire : Les sous-groupes de $\mathrm{Hom}(G, \mathbb{C}^\times)$ sont de la forme $\mathrm{Hom}(G/H, \mathbb{C}^\times)$.

En effet, si $A \subseteq \mathrm{Hom}(G, \mathbb{C}^\times)$, alors

le foncteur $\mathrm{Hom}(\cdot, \mathbb{C}^\times)$ donne

$$G \longrightarrow \mathrm{Hom}(A, \mathbb{C}^\times)$$

Soit H le noyau de ce morphisme, on a

$$G/H \simeq \mathrm{Hom}(A, \mathbb{C}^\times),$$

donc $\mathrm{Hom}(G/H, \mathbb{C}^\times) \simeq A$.

ajout : Si $A \subseteq \mathrm{Hom}(G, \mathbb{C}^\times)$, (non-groupe)

alors $A \simeq \mathrm{Hom}(G/H, \mathbb{C}^\times)$,

où $H = \{\sigma \in G \mid \forall \varphi \in A \ \ \varphi(\sigma) = 1\}$

En effet, $A \subseteq \mathrm{Hom}(G, \mathbb{C}^\times)$

donne $\mathrm{Hom}(\mathrm{Hom}(G, \mathbb{C}^\times), \mathbb{C}^\times) \longrightarrow \mathrm{Hom}(A, \mathbb{C}^\times)$

$f \longmapsto f|_A$

or $G \simeq \mathrm{Hom}(\mathrm{Hom}(G, \mathbb{C}^\times), \mathbb{C}^\times)$

$\sigma \longmapsto (\varphi \mapsto \varphi(\sigma))$

donc $G \longrightarrow \mathrm{Hom}(A, \mathbb{C}^\times)$

$\sigma \longmapsto (\varphi \mapsto \varphi(\sigma))$

et $H := \ker\left(\begin{cases} G \longrightarrow \mathrm{Hom}(A, \mathbb{C}^\times) \\ \sigma \longmapsto (\varphi \mapsto \varphi(\sigma)) \end{cases}\right)$

donc $H = \{\sigma \in G \mid \forall \varphi \in A \ \ \varphi(\sigma) = 1\}$.

Th : L'application

$$\left\{\begin{array}{l}\text{sous-corps } L \text{ de } \bar{K} \\ \text{obtenus d'exposant un } K \\ \text{fini}\end{array}\right\} \longrightarrow \left\{\begin{array}{l}\text{sous-groupes de } K^\times \\ \text{dont } K^{\times n} \text{ est un sous-groupe} \\ \text{d'indice fini}\end{array}\right\}$$

$$L \longmapsto K^\times \cap L^{\times n}$$

est une bijection, de réciproque

$$K[B^{1/n}] \longleftarrow B$$

$K[B^{1/n}]$: sous-corps de $\bar{K}$ engendré par les racines n-ièmes de éléments de B.

Rem : Si $B = K^\times \cap L^{\times n}$, on a $[L:K] = [B : K^{\times n}]$.

(En effet, $[B : K^{\times n}] = \left| \frac{K^\times \cap L^{\times n}}{K^{\times n}} \right| = |\mu_n| = |G| = [L:K]$.)

0 On note $B(L) := K^\times \cap L^{\times n}$. On a alors $L \supseteq K[B(L)^{1/n}]$ et $B \subseteq B(K[B^{1/n}])$. On en déduit

$$[L:K] \geq [K[B(L)^{1/n}] : K] = [B(K[B(L)^{1/n}]) : K^{\times n}]$$
$$\geq [B(L) : K^{\times n}] = [L:K]$$

Donc $L = K[B(L)^{1/n}]$.

Réciproquement, si B sous-gp de $K^\times$ donc $K^{\times n}$ est un sous-gp d'indice fini, soit $L := K[B^{1/n}]$.

$L = K[a_0^{1/n}, \dots]$ où $B/K^{\times n} = \{\bar{a}_0, \dots\}$ (fini)

et les ext. $K[a_i^{1/n}]/K$ sont cycliques, donc L/K est abélienne
de degré $|n$ d'exposant n

Exercice

$$\begin{array}{c} B/K^{\times n} \\ \cap \\ B(L)/K^{\times n} \end{array} \xrightarrow{\sim} \mathrm{Hom}(G, \mu_n) \qquad G = \mathrm{Gal}(L/K)$$

$$a \longmapsto \left(\sigma \mapsto \frac{a^{1/n}}{\sigma(a^{1/n})}\right)$$

Un sous-groupe de $\mathrm{Hom}(G, \mu_n)$ est de la forme $\mathrm{Hom}(G/H, \mu_n)$,
(où $H = \{\sigma \in G \mid \forall \chi \in \text{sous-groupe}\ \ \chi(\sigma) = 1\}$)
(cf remarques précédentes),

donc $B/K^{\times n} \xrightarrow{\sim} \mathrm{Hom}(G/H, \mu_n)$.

Si $\sigma \in H$, alors $\forall a \in B \quad \sigma(a^{1/n}) = a^{1/n}$

donc $\sigma = \mathrm{id}$ $\quad (L = K[B^{1/n}])$

Donc $H = 1$, et $B = B(L)$. ∎

Rem: On obtient une dualité parfaite

$$\frac{K^\times \cap L^{\times n}}{K^{\times n}} \times \mathrm{Gal}(L/K) \longrightarrow \mu_n(K).$$

Exercice : Trouver un analogue pour les extensions d'Artin–Thrédy

Appliqué à $\mathbb{C}/\mathbb{R}$, on trouve

$$\{\mathbb{R},\mathbb{C}\} = \left\{\begin{array}{l}\text{sous-corps de } \mathbb{C}\\ \text{contenant } \mathbb{R}, \text{ abéliens}\\ \text{finis d'exposant 2}\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\text{sous-groupes}\\ \text{de } \mathbb{R}^\times/\mathbb{R}_+^\times \simeq \{\pm 1\}\end{array}\right\}$$

(qui est évident).

Appliqué à $\overline{\mathbb{F}}_p/\mathbb{F}_p$, on trouve

$$\left\{\begin{array}{l}\text{sous-corps de } \overline{\mathbb{F}}_p\\ \text{finis d'exposant 2}\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\text{sous-groupes}\\ \text{de } \mathbb{F}_p^\times/\mathbb{F}_p^{\times 2} \simeq \mathbb{Z}/2\mathbb{Z}\end{array}\right\}$$

$$= \{\mathbb{F}_p, \mathbb{F}_{p^2}\}$$

Appliqué à $\overline{\mathbb{Q}}/\mathbb{Q}$, on trouve

$$\left\{\begin{array}{l}\text{sous-corps de } \overline{\mathbb{Q}}\\ \text{abéliens finis d'exposant 2}\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\text{sous-groupes finis}\\ \text{de } \mathbb{Q}^\times/\mathbb{Q}^{\times 2}\end{array}\right\}.$$

$$\mathbb{Q}(\sqrt{-1}, \sqrt{p_0}, \sqrt{p_1}, \ldots) \qquad \mathbb{Q}^\times/\mathbb{Q}^{\times 2} \simeq (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$$

choix dans $\{-1\} \cup \{\text{premiers}\}$

$$\mathbb{Q}(\sqrt{a_0}, \sqrt{a_1}, \ldots) \qquad (a_i \in \mathbb{Z}\setminus\{0\}, \text{ sans facteur carré})$$

$\mathbb{Q}(\sqrt{a_0}, \sqrt{a_1}, \ldots)$: fini

(5) Résolubilité par radicaux.

Rappels : Un groupe G est résoluble s'il existe des sous-groupes

$$1 = G_0 \subseteq G_1 \subseteq \dots \subseteq G_k = G$$

tels que $\forall i$ $\begin{cases} G_{i+1}/G_i \text{ soit abélien.} \\ G_i \text{ distingué dans } G_{i+1} \end{cases}$

Les groupes abéliens sont résolubles.

Rem : Tout groupe abélien fini est un produit de groupes cycliques, donc si G est abélien on peut trouver

$$1 = G_0 \subseteq G_1 \subseteq \dots \subseteq G_k = G$$

avec G_{i+1}/G_i cyclique.

En appliquant ceci aux quotients (abéliens) successifs dans la déf de « résoluble », on trouve que si G est fini on peut remplacer « abélien » par « cyclique » dans la déf.

Prop : Un sous-groupe d'un groupe résoluble est résoluble.
Un quotient d'un groupe résoluble par un sous-groupe distingué est résoluble.

□ Si $1 = G_0 \subseteq G_1 \subseteq \dots \subseteq G_k = G$, $H \subseteq G$,

alors $1 = G_0 \cap H \subseteq G_1 \cap H \subseteq \dots \subseteq G_k \cap H = H$,

et $G_i \cap H \subseteq G_i \twoheadrightarrow G_i/G_{i-1}$ a pour noyau $G_{i-1} \cap H$

donc $\dfrac{G_i \cap H}{G_{i-1} \cap H} \hookrightarrow \dfrac{G_i}{G_{i-1}}$ (abélien)

donc $\dfrac{G_i \cap H}{G_{i-1} \cap H}$ est abélien.

Si H est distingué, on a

$$1 = G_0H/H \subseteq G_1H/H \subseteq \dots \subseteq G_nH/H = G/H$$

$G_i \twoheadrightarrow G_iH/H$ a pour noyau $G_i \cap H$

donc on obtient $\dfrac{G_i}{G_i \cap H} \simeq \dfrac{G_iH}{H}$,

$G_i \twoheadrightarrow \dfrac{G_iH}{G_{i-1}H}$ a pour noyau $G_i \cap G_{i-1}H$ ($\supset G_{i-1}$)

donc on obtient $\dfrac{G_i}{G_{i-1}} \twoheadrightarrow \dfrac{G_iH}{G_{i-1}H}$

($\dfrac{G_i}{G_{i-1}}$ abélien)

donc $\dfrac{G_iH}{G_{i-1}H}$ est abélien. □

(fin des rappels)

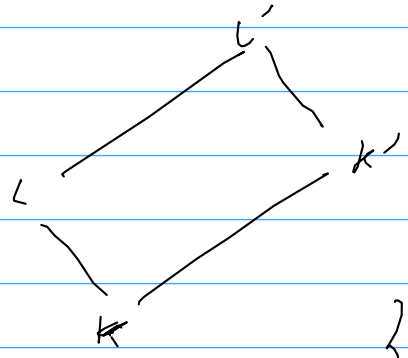
Soit K corps, $\mathrm{car}\, K = 0$

soit $P(X) \in K[X]$, $n := \deg P$.

Si L = corps de décomp de P sur K

K'/K extension

L' = corps de décomp de P sur K'



L/K et L'/K' sont galoisiennes

$$\begin{cases} \mathrm{Gal}(L'/K') \longrightarrow \mathrm{Gal}(L/K) \\ \sigma \longmapsto \sigma|_L \end{cases}$$

Si corps n°10

Si $\alpha_0, \dots, \alpha_{n-1}$ sont les racines de P dans L',

on a $\alpha_0, \dots, \alpha_{n-1} \in L$ et $\begin{cases} L = K[\alpha_0, \dots, \alpha_{n-1}] \\ L' = K'[\alpha_0, \dots, \alpha_{n-1}] \end{cases}$

Si $\sigma \in \mathrm{Gal}(L'/K')$ vérifie $\sigma|_L = \mathrm{id}_L$, alors $\forall i\ \sigma(\alpha_i) = \alpha_i$,

donc $\sigma = \mathrm{id}_{L'}$.

On a donc $\mathrm{Gal}(L'/K') \hookrightarrow \mathrm{Gal}(L/K)$.

↙ mêmes hypothèse qu'avant

Déf : $P(X)$ est dit résoluble par radicaux s'il existe une tour d'extensions

$$K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \dots \subseteq K_n$$

t.q. P soit scindé sur K_n, et K_{i+1}/K_i est :

- soit une extension monogène engendrée par une racine ℓ ième
- soit une extension monogène engendrée par une racine de $X^m - a$, $a \in K_i$.

Prop : $P(X)$ est résoluble par radicaux si le groupe de Galois du corps de décomposition de $P(X)$ sur K est résoluble.

□ $\Leftarrow$: Soit L le corps de décomposition de $P(X)$ sur K.
Soit $n := [L : K]$.
Soit $K' := K(\mu_{n!})$ l'extension de K engendrée par les racines $n!$ - ièmes de 1.
Soit L' le corps de décomp. de $P(X)$ sur K'.
$Gal(L'/K')$ est un sous-groupe de $Gal(L/K)$, donc est résoluble.

$$1 = G_0 \subseteq \dots \subseteq G_m = Gal(L'/K').$$

G_{i+1}/G_i cyclique

Soit $K_i := L'^{G_i}$. On a $L' = K_0 \supseteq \dots \supseteq K_m = K' \supseteq K$

L

$Gal(K_i/K_{i+1}) \simeq G_{i+1}/G_i$ est cyclique,
$[K_i : K_{i+1}] \leq [L' : K'] \leq [L : K] = n$,
donc $K_{i+1} (\supseteq K')$ contient une racine $[K_i : K_{i+1}]$ - ième de 1, donc K_i / K_{i+1} est un corps de rupture (et de décomposition) d'un $X^{[K_i : K_{i+1}]} - a$, $a \in K_{i+1}$.

→ OK

$\Rightarrow$: $K = K_0 \subseteq \dots \subseteq K_m$

$K_{i+1} = K_i[\alpha_{i+1}]$ $\quad \alpha_{i+1}^{n_{i+1}} \in K_i$

(éventuellement $= 1 \dots$)

Soit ζ une racine $\left(\prod_{i=0}^{m-1} n_i\right)$ - ième primitive de 1.

Soit L une clôture galoisienne de $K_m[\zeta]$.

Notons que $L = K\left[\zeta, \ \sigma(\alpha_i) \ ; \ \begin{matrix} 0 \le i < m \\ \sigma \in Gal(L/K) \end{matrix}\right]$.

(car c'est une extension normale de K, contenant $K_m(\zeta)$, et contenue dans L.)

Soient $\{\sigma_0, \dots, \sigma_{k-1}\} = Gal(L/K)$

$\beta_0, \dots, \beta_{nk-1} = \sigma_0(\alpha_0), \dots, \sigma_{k-1}(\alpha_0), \sigma_0(\alpha_1), \dots, \sigma_{k-1}(\alpha_1), \dots, \sigma_{k-1}(\alpha_{m-1})$

$L_i = K[\zeta, \beta_0, \dots, \beta_{i-1}]$

alors $L_0 = K[\zeta]$, $L_{mk} = L \supseteq K_m$

(donc L est scindé sur L_{mk-1})

L_{i+1}/L_i est monogène, engendrée par β_i,

et $\forall j \quad \beta_i^{n_j} \left(= \sigma_x(\alpha_j^{n_j})\right) \in L_i$.

$\uparrow$

K_{j-1}

$K[\zeta]$ contient les racines n_j - ièmes de 1.

donc L_{i+1}/L_i est galoisienne.

$K[\beta]/K$ est abélienne. Donc $\mathrm{Gal}(L/K)$ est résoluble.

Si M = sous-corps de L engendré par les racines de P, alors $\mathrm{Gal}(M/K)$ est un quotient de $\mathrm{Gal}(L/K)$, donc est résoluble. □

Rem: On peut étendre ce théorème à la caractéristique $p>0$ mais il faut d'autres opérations :
- racines p-ièmes ($\leftarrow$ non séparable)
- racines de $X^p - X - a$, a sous-corps.

Rem: Comme $\mathfrak{S}_5$ n'est pas résoluble, on en déduit qu'il existe des polynômes de degré 5 non résolubles par radicaux.

Chapitre III : Compléments

(I) Extensions de degré infini

algébrique

L/K extension galoisienne, possiblement de degré infini.

⚠ $\bar{K}/K$ n'est pas forcément galoisienne (car pas forcément séparable) mais K^{sep}/K l'est. ($K^{sep} = \bar{K}$ si $\mathrm{car} K = 0$).

i.e. $\forall x \in L$ le poly min de x sur K est scindé à racines simples sur L

$$\mathrm{Aut}_K(L) \hookrightarrow \prod_{\substack{K \subset M \subset L \\ M/K \text{ galoisienne} \\ [M:K] < \infty}} \mathrm{Gal}(M/K) \quad \text{morphisme de groupes.}$$

$$f \longmapsto f|_M$$

injectivité : si $\forall M \quad f|_M = \mathrm{id}_M$,

soit $x \in L$, soit M = clôture galoisienne de $K[x]$,

alors $f|_M = \mathrm{id}_M$ donc $f(x) = x$,

donc $f = \mathrm{id}_L$.

(En général ce n'est pas surjectif. Voyez-vous pourquoi ?)

Les groupes $\mathrm{Gal}(M/K)$ sont finis, on les munis de la topologie discrète (i.e. toutes les parties sont ouvertes et fermées).
Le produit $\prod \mathrm{Gal}(M/K)$ est muni de la topologie produit.

rappels sur la topologie produit

$(X_i)_{i \in I}$ famille d'espaces topologiques

$\pi_j : \prod_{i \in I} X_i \longrightarrow X_j$ projections

La topologie produit sur $\prod_{i \in I} X_i$ est la topologie la plus grossière (= la moins d'ouverts possible) qui rende les applications π_i continues.

→ Les ouverts de $\prod_{i \in I} X_i$ sont les réunions (pas forcément finies) de parties

$\prod_{i \in I} U_i$ où $\forall i$ U_i ouvert de X_i.

$\{ i \in I \ / \ U_i \neq X_i \}$ fini

Exercice : Une suite $(y^{(n)})_{n \in \mathbb{N}}$ d'éléments de $\prod_{i \in I} X_i$ converge ssi $\forall i \in I$ $(\pi_i(y^{(n)}))_{n \in \mathbb{N}}$ converge dans X_i

Déf : $\mathrm{Gal}(L/K) := \mathrm{Aut}_K(L)$ avec la topologie induite sur $\mathrm{Aut}_K(L)$ par la topologie produit de $\prod_M \mathrm{Gal}(M/K)$.

C'est un groupe topologique ! (Exercice : vérifier la continuité du produit et de l'inversion.)

Rem : La topologie de $\mathrm{Gal}(L/K)$ est appelée topologie de Krull.

Prop : L'image de $\mathrm{Gal}(L/K)$ dans $\prod \mathrm{Gal}(M/K)$ est l'intersection des fermés $F(M,M') \subseteq \prod \mathrm{Gal}(M/K)$,
où $\forall M, M'$ sont finis galoisiens de K contenus dans L et tq $M \subseteq M'$
$$F(M,M') = \left\{ (\sigma_N) \in \prod \mathrm{Gal}(N/K) \;/\; \sigma_{M'}|_M = \sigma_M \right\}.$$

□ Les $F(M,M')$ sont des fermés : le complémentaire de $F(M,M')$ est
$$\left\{ (\sigma_N) \;/\; \sigma_{M'}|_M \neq \sigma_M \right\} = \bigcup_{\substack{\tau_{M'} \in \mathrm{Gal}(M'/K) \\ \tau_M \in \mathrm{Gal}(M/K) \\ \tau_{M'}|_M \neq \tau_M}} \left\{ (\sigma_N) \;;\; \sigma_M = \tau_M \right\}$$
$\sigma_{M'} = \tau_{M'}$ ↑ ouvert

Si $\sigma \in \mathrm{Gal}(L/K)$, alors $(\sigma|_{M'})|_M = \sigma|_M$, donc l'image de $\mathrm{Gal}(L/K)$ est dans $F(M,M')$.
Réciproquement, soit $(\sigma_M) \in \bigcap_{M \subseteq M'} F(M,M')$.

Si $x \in L$, et si M, N sont finis galoisiens de K contenus dans L et contenant x, on a $\sigma_M = \sigma_{MN}|_M$ et $\sigma_N = \sigma_{MN}|_N$,
donc $\sigma_M(x) = \sigma_{MN}(x) = \sigma_N(x)$
donc $\sigma_M(x)$ ne dépend pas du choix de M.
On pose $\sigma(x) := \sigma_M(x)$.
Alors $\sigma \in \mathrm{Aut}_K(L)$ (exercice) et $\forall M$ $\sigma|_M = \sigma_M$ (exercice). ∎

Corollaire : $\mathrm{Gal}(L/K)$ est compact.

□

Les groupes $\mathrm{Gal}(M/K)$ sont compacts, donc par le th de Tychonoff le produit $\prod_M \mathrm{Gal}(M/K)$ est compact.
Donc $\mathrm{Gal}(L/K)$ est homéomorphe (par déf) à un fermé d'un compact. ☐

Corollaire : $\mathrm{Gal}(L/K) \simeq \varprojlim_M \mathrm{Gal}(M/K)$.

□ Les morphismes de projection donnent $\varprojlim_M \mathrm{Gal}(M/K) \longrightarrow \prod_M \mathrm{Gal}(M/K)$,

et l'image est dans l'intersection de $F(M, M')$ par déf de $\varprojlim$,

donc on trouve un morphisme de groupes

$$\varprojlim_M \mathrm{Gal}(M/K) \longrightarrow \mathrm{Gal}(L/K)$$

t.q. le diagramme avec les restrictions à M commute.
La propriété universelle de $\varprojlim_M \mathrm{Gal}(M/K)$ donne le morphisme réciproque. ☐

Rem : La topologie de Krull sur $\mathrm{Gal}(L/K)$ est la topologie induite de $\varprojlim_M \mathrm{Gal}(M/K)$ (avec topologie discrète). On peut se servir de $\varprojlim_M \mathrm{Gal}(M/K)$ comme définition de $\mathrm{Gal}(L/K)$.

Rem : $\mathrm{Gal}(L/K)$ est profini (limite proj de groupes finis)

ajout : autre preuve de $\mathrm{Gal}(L/K) = \varprojlim \mathrm{Gal}(M/K)$.

$$L = \bigcup_M M = \varinjlim_M M$$

où M parcourt les sous-extensions de L/K finies galoisiennes

(↖ pour les inclusions $(\subseteq)$)

donc $\mathrm{Aut}_K(L) = \mathrm{Hom}_K(L, L)$

$$= \mathrm{Hom}_K\left(\varinjlim_M M, L\right)$$

$$= \varprojlim_M \mathrm{Hom}_K(M, L)$$

$$= \varprojlim_M \mathrm{Hom}_K(M, M) \quad \leftarrow \text{car } M \text{ est normale sur } K$$

$$= \varprojlim_M \mathrm{Gal}(M/K)$$

fin

cours n°11

Prop : Les sous-groupes

$$G(S) := \{ \sigma \in \mathrm{Gal}(L/K) \mid \forall x \in S \quad \sigma(x) = x \}$$

où $S \subseteq L$ fini

forment une base de voisinages ouverts et fermés de id_L dans $\mathrm{Gal}(L/K)$.

Si S est stable par $\mathrm{Gal}(L/K)$, alors $G(S)$ est distingué.

$G(S) = \bigcap_{x \in S} G(\{x\})$

□ • Ce sont des voisinages de id_L :

si M est la clôture galoisienne (dans L) de $K(S)$,

alors $\{ \sigma \in \mathrm{Gal}(L/K) \mid \sigma|_M = \mathrm{id}_M \}$ est un ouvert de $\mathrm{Gal}(L/K)$ (pour dif de sa topologie), contenu dans $G(S)$.

• Ils sont donc ouverts (par translation, ils sont voisinages de chacun de leurs éléments).

• Ils sont donc fermés (par translation, le complémentaire est réunion d'ouverts).

• Pour montrer que tout ouvert de $\mathrm{Gal}(L/K)$ contient un $G(S)$, il suffit de considérer un ouvert de la forme

$$\{ \sigma \in \mathrm{Gal}(L/K) \mid \forall i \in I \quad \sigma|_{M_i} \in U_i \} \ni \mathrm{id}_L$$

pour I fini

M_i / K galoisiennes finies

$U_i \subseteq \mathrm{Gal}(M_i/K)$ $\quad (U_i \ni \mathrm{id}_{M_i})$

Si $M_i = K(\alpha_i)$, $\quad S = \{ \alpha_i \; ; \; i \in I \}$, alors :

$$\forall \sigma \in G(S) \quad \forall i \in I \qquad \sigma(\alpha_i) = \alpha_i \text{ donc } \sigma|_{M_i} = \mathrm{id}_{M_i} \in U_i$$

donc $G(S)$ convient.

• Si S est stable par $\mathrm{Gal}(L/K)$,

si $\sigma \in \mathrm{Gal}(L/K)$, on a $G(\sigma S) = \sigma G(S) \sigma^{-1}$,

or $G(\sigma S) = G(S)$, donc $\sigma G(S) \sigma^{-1} = G(S)$ ∎

Corollaire : Si $x \in L$, l'application $\begin{cases} \mathrm{Gal}(L/K) \longrightarrow L \\ \sigma \longmapsto \sigma(x) \end{cases}$ (avec topologie discrète sur L) est continue.

□ Soit $X \subseteq L$, on veut montrer que

$$\{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(x) \in X\} = \bigcup_{y \in X} \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(x) = y\}$$

est ouvert.

Or $\{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(x) = y\} = \begin{cases} \emptyset \text{ si } y \text{ n'est pas conjugué à } x \\ \sigma_0 G(\{x\}) \text{ si } \sigma_0(x) = y. \end{cases}$

ouverts.

■

Prop : Si $U \subseteq \mathrm{Gal}(L/K)$, l'adhérence de U est

$$\bar{U} = \left\{ \sigma \in \mathrm{Gal}(L/K) \mid \forall M \text{ est finie de } K \text{ contenue dans } L \quad \exists \tau \in U \quad \sigma|_M = \tau|_M \right\}.$$

Rem : on peut même ne considérer que les M/K galoisiennes. (car toute ext. finie est contenue dans une ext. finie galoisienne)

□ On a :

$$\sigma \in \bar{U} \iff \forall S \subseteq_{\text{finie}} L \quad \sigma G(S) \cap U \neq \emptyset$$

$$\iff \forall S \subseteq_{\text{finie}} L \quad \exists \tau \in U \quad \sigma\tau^{-1} \in G(S)$$

$$\iff \forall M \text{ est finie de } K \text{ contenue dans } L \quad \exists \tau \in U \quad (\sigma\tau^{-1})|_M = \mathrm{id}_M$$

$$\iff \forall M \ldots \quad \exists \tau \in U \quad \sigma|_M = \tau|_M.$$

■

Prop : Les composantes connexes de $Gal(L/K)$ sont les singletons.
(« $Gal(L/K)$ est totalement discontinu »)

□ Par translation, il suffit de montrer que $\{id_L\}$ est une composante connexe.

$$\{id_L\} = \bigcap_{S \text{ finie stable par } Gal(L/K)} G(S)$$

($G(S)$ ouverts et fermés)

(car $\forall x \in L$ si $S = \{\text{conjugués de } x\}$ on a $\sigma \in G(S) \Rightarrow \sigma(x) = x$)

Si G_0 = composante connexe de id_L, alors

$\forall S$ $\quad G_0 \cap G(S)$ = ouvert, fermé, non vide, de G_0

donc $G_0 \cap G(S) = G_0$

$G_0 \subseteq G(S)$

donc $G_0 \subseteq \bigcap G(S) = \{id_L\}$, donc $G_0 = \{id_L\}$. ☒

Rem : Un groupe est profini ssi il est compact + totalement discontinu.
(cf. Milne, prop 2.25)

cf. aussi : Cassels & Fröhlich, chap V : K. Gruenberg, Profinite Groups (theorem 1)

Prop : $L^{Gal(L/K)} = K$

□ Si $x \in L^{Gal(L/K)}$, M = clôture galoisienne de $K(x)$,

alors $x \in M^{Gal(M/K)} = K$

(cas des ext. finies) ☒

Prop (th d'Artin, cas infini) : (i.e. compact)

G = sous-groupe fermé de $Gal(L/K)$

Alors L/L^G est galoisienne, et $Gal(L/L^G) = G$.

□ L/L^G est galoisienne car L/K l'est.

Si M = est finie (galoisienne) de L^G contenue dans L, on note

$H_M := \{\sigma|_M \,;\, \sigma \in G\}$.

On a $H_M \subseteq \mathrm{Gal}(M/L^G)$, et $M^{H_M} = \{x \in M \mid \forall \sigma \in G \ \sigma(x) = x\}$
$= M \cap L^G$
$= L^G$

donc (correspondance de Galois finie) $H_M = \mathrm{Gal}(M/L^G)$,

donc $\forall \sigma \in \mathrm{Gal}(L/L^G)$ $\forall M$ est finie galoisienne de L^G contenue dans L

$\sigma|_M \in \mathrm{Gal}(M/L^G) = H_M$
i.e. $\exists \tau \in G \quad \sigma|_M = \tau|_M$

donc $\mathrm{Gal}(L/L^G) \subseteq \bar{G}$,
or $G \subseteq \mathrm{Gal}(L/L^G)$ par déf. de L^G,
et G est fermé donc $G = \bar{G}$,
donc $\mathrm{Gal}(L/L^G) = G$. ☒

Ceci permet de démontrer le th fondamental de la théorie de Galois, dans le cas des extensions de degré infini :

Th : Soit L/K galoisienne,
soit $G := \mathrm{Gal}(L/K)$.
(i) Si $L/M/K$, alors L/M est galoisienne, $\mathrm{Gal}(L/M)$ est un sous-groupe fermé de G, et $L^{\mathrm{Gal}(L/M)} = M$.
(ii) Si H est un sous-groupe de G, alors $\mathrm{Gal}(L/L^H)$ est l'adhérence de H.

□ (i) : L/M galoisienne car L/K galoisienne
$\mathrm{Gal}(L/M) = \bigcap_{\substack{S \subseteq M \\ S \text{ finie}}} G(S)$ est fermé
(intersection de fermés)
$L^{\mathrm{Gal}(L/M)} = M$: vu ci-dessus.

(ii) $H \subset \underbrace{Gal(L/L^H)}_{\text{fermé par (i)}}$ donc $\overline{H} \subseteq Gal(L/L^H)$.

Si $\sigma \in Gal(L/L^H) \setminus \overline{H}$, alors $\exists S$ $\sigma G(S) \cap H = \emptyset$

et si $M :=$ clôture galoisienne de $K(S)$, alors

$$\sigma Gal(L/M) \cap H = \emptyset$$

or l'application (le morphisme de groupes) $\begin{cases} Gal(L/K) \longrightarrow Gal(M/K) \\ \tau \longmapsto \tau|_M \end{cases}$

est surjective (par prolongement) et de noyau $Gal(L/M)$,

donc on en déduit $\sigma|_M \notin \underbrace{\{\tau|_M ; \tau \in H\}}_{\text{sous-groupe de } Gal(M/K)}$,

$M^{\{\tau|_M ; \tau \in H\}} = M^H \subseteq L^H$, donc $\sigma|_{M^H} = id$,

or $Gal(M/M^H) = \{\tau|_M ; \tau \in H\}$ par corresp. de Galois pour les ext. finies,

donc $\sigma|_M \in Gal(M/M^H) = \{\tau|_M ; \tau \in H\}$: contradiction. ☒

On en déduit que

$$\left\{\begin{array}{c}\text{sous-ext} \\ \text{de } L/K\end{array}\right\} \xrightarrow{\sim} \left\{\begin{array}{c}\text{sous-groupes} \\ \text{fermés de} \\ Gal(L/K)\end{array}\right\}$$

$$M \longmapsto Gal(L/M)$$

$$L^H \longleftarrow H$$

sont des bijections inverses l'une de l'autre, décroissantes,

les ext. t.q. M/K galoisienne correspondent aux sous-groupes distingués de $\mathrm{Gal}(L/K)$ et les ext. finies M/K correspondent aux sous-groupes ouverts ($\Leftrightarrow$ fermés) de $\mathrm{Gal}(L/K)$.

Exemple : $\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$

$$\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) = \varprojlim_{\text{restrictions}} \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \simeq \mathbb{Z}/n\mathbb{Z}$$

$$= \varprojlim_{n \text{ entier} \geq 1} \mathbb{Z}/n\mathbb{Z}$$

$\left\{ \begin{array}{ccc} \mathbb{Z}/m\mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \text{ si } n \mid m \\ x & \mapsto & x \end{array} \right.$

$$= \varprojlim_{n} \prod_{p \text{ premier}} \mathbb{Z}/p^{v_p(n)}\mathbb{Z} \qquad \text{(th chinois)}$$

↑ Ceci est aussi une limite projective (sans flèche) (donc on peut échanger)

$$= \prod_{p \text{ premier}} \varprojlim_{v \geq 0} \mathbb{Z}/p^v\mathbb{Z}$$

$\varprojlim_{v \geq 0} \mathbb{Z}/p^v\mathbb{Z} = \mathbb{Z}_p$

$$\boxed{\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) \simeq \prod_{p \text{ premier}} \mathbb{Z}_p} \qquad (\text{noté } \hat{\mathbb{Z}})$$

Rem : $\mathrm{Gal}(K^{sep}/K)$ est appelé le groupe de Galois absolu de K.

Rem : $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ est très compliqué !

(II) Algèbres étales et théorie de Galois.

(a) Algèbres étales sur un corps

K = corps. Les algèbres considérées ici sont associatives, commutatives unitaires

Déf : Une K-algèbre A est dite **diagonalisable** s'il existe un entier $n \geq 0$ t.q. $A \simeq K^n$ (K-algèbre).

Une K-algèbre A est dite **étale** s'il existe une extension L/K telle que la L-algèbre $L \otimes_K A$ soit diagonalisable.

Rem : Si $M \in M_n(K)$, alors $K[M]$ est diagonalisable ssi la matrice M est diagonalisable (exercice).

Exercice : $K[X]/(P)$ est diagonalisable ssi P est scindé à racines simples sur K.

Exercice : $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \simeq \mathbb{C}^2$ ($\mathbb{C}$-algèbre).

fin cours n°12

Prop : Si A est une K-algèbre finie (i.e. $\dim_K A < +\infty$), alors on a équivalence de :

(i) A est étale

(ii) $\forall L/K$ extension $L \otimes_K A$ est réduite (i.e. sans nilpotent $\neq 0$)

(iii) A est un produit fini d'extensions finies séparables de K.

□ (i) $\Rightarrow$ (iii) :

Par (i), $\exists L'/K$ extension t.q. $L' \otimes_K A \simeq L'^n$.

Soit L/K extension. Soit $L'' := LL'$ (on s'impose quel corps contenant L et L'). On a $L'' \otimes_K A \simeq L'' \otimes_L (L \otimes_K A) \simeq L''^n$,

or $L \subseteq L''$ donne $L \otimes_K A \longrightarrow L'' \otimes_K A \simeq L''^n$ (L''-alg).

D'autre part, $A \underset{K\text{-ev.}}{\simeq} K^m$ donc $L \otimes_K A \longrightarrow L'' \otimes_K A$

$\wr$ L-ev. $\qquad$ $\wr$ L''-ev.

$L^m \longrightarrow L''^m$

$\subseteq$

donc $L \otimes_K A \hookrightarrow L'' \otimes_K A \underset{L''\text{-alg}}{\simeq} L''^m$

$\uparrow$ réduit

donc $L \otimes_K A$ est réduite.

(iii) $\Rightarrow$ (viii) :

$A \simeq K \otimes_K A$ est réduite par hypothèse.

Si $S \subseteq \{\text{idéaux max de } A\}$, S fini, on a

$A \longrightarrow\!\!\!\!\rightarrow \prod_{m \in S} A/m$ par th chinois

$\uparrow$ corps et K-algèbre donc extension de K

$\dim_K A < +\infty$ donc $|S| \leq \dim_K A < +\infty$,

donc $|\{\text{idéaux max de } A\}| \leq \dim_K A < +\infty$,

et on peut prendre $S = \{\text{idéaux max de } A\}$.

$\ker\left(A \longrightarrow\!\!\!\!\rightarrow \prod A/m\right) = \bigcap_{m \in S} m = \{\text{nilpotents de } A\}$

$\wr$ cf lemme en annexe

$= \{0\}$ car (iii)

donc $A \simeq \prod_{m \in S} A/m$

Soit $M := A/m$ M/K extension.

Soit $x \in M$, $P(x) \in K[X]$ son poly minimal.

Si x n'était pas séparable, alors :

car $K = p > 0$

$P(x) = Q(X^p)$

Soit L = extension de K où les coeffs de Q ont une racine p-ième.

$P(x) = Q(X^p) = R(x)^p \qquad R(x) \in L[X]$

alors $L \otimes_K M \supseteq L \otimes_K K[x] \simeq \frac{L[X]}{(P)} = \frac{L[X]}{(R)^p}$,

donc $R(x)$ est nilpotent d'ordre p dans $\frac{L[X]}{(R)^p}$,

donc $L \otimes_K M$ n'est pas réduite : contradiction.

Donc M/K est séparable.

(iii) $\Rightarrow$ (i) :

$A \simeq \prod L_i \qquad L_i/K$ séparables finies

$L :=$ extension de K engendrée par tous les L_i (clôtures galoisiennes des $L_i^\vee$)

$L \otimes_K A \simeq \prod L \otimes_K L_i$

$L_i = K(\alpha_i)$ (th. él^t primitif)

$P_i(X) =$ poly minimal de α_i sur K

$L_i \simeq \frac{K[X]}{(P_i)} \qquad L \otimes_K L_i \simeq \frac{L[X]}{(P_i)}$

P_i est scindé à racines simples sur L, $\simeq L$

donc $\frac{L[X]}{(P_i)} \simeq \frac{L[X]}{\prod (X - \beta_j)} \overset{\text{th chinois}}{\simeq} \prod \frac{L[X]}{(X-\beta_j)} \simeq L^{\deg P_i}$

CQFD

Exercice : Si K est parfait, alors A étale $\Leftrightarrow$ A réduite.

A anneau commutatif unitaire

Th : $\bigcap_{\substack{\mathfrak{p} \text{ idéal} \\ \text{premier de } A}} \mathfrak{p} = \{\text{nilpotents de } A\}$

$\supseteq$: Si x nilpotent, $\mathfrak{p}$ idéal premier,
alors $\exists n > 0 \quad x^n = 0 \in \mathfrak{p}$,
donc $x \in \mathfrak{p}$.

$\subseteq$: $\{\text{nilpotents de } A\}$ est un idéal,
donc on peut (quitte à quotienter) supposer que A est réduit.

Soit $x \in A \setminus \{0\}$. On considère le localisé $A\left[\frac{1}{x}\right]$.
Dans $A\left[\frac{1}{x}\right]$, $1 = 0$ ssi $\exists n > 0 \quad x^n = 0$,
or x n'est pas nilpotent, donc $1 \neq 0$, donc $A \neq 0$.
Soit m un idéal maximal de $A\left[\frac{1}{x}\right]$,
soit m' l'image réciproque de m par $A \to A\left[\frac{1}{x}\right]$,
alors $A/m' \hookrightarrow \underbrace{A\left[\frac{1}{x}\right]/m}_{\text{corps}}$ par déf de m',

donc A/m' intègre, donc m' premier.
Or x est inversible dans $A\left[\frac{1}{x}\right]$, donc $x \notin m$,
donc $x \notin m'$, donc $x \notin \bigcap_{\mathfrak{p} \text{ premier}} \mathfrak{p}$.

Donc $\bigcap_{\mathfrak{p} \text{ premier}} \mathfrak{p} = \{0\}$. ∎

Déf : A est dit de Jacobson si tout idéal premier de A est intersection d'idéaux maximaux.

Rem : Si A est de Jacobson, alors

$$\bigcap_{\substack{m \text{ idéal} \\ \text{max de } A}} m = \{ \text{nilpotents de } A \}.$$

Prop : Si A est un corps, alors A est de Jacobson.

□ Le seul idéal maximal de A est $\{0\}$, et c'est aussi seul idéal premier. ☒

Prop : Tout quotient d'un anneau de Jacobson est de Jacobson.

□ Si I idéal de A A de Jacobson,
les idéaux de A/I s'identifient aux idéaux de A contenant I. ☒

Prop : Si $x \in A$, non nilpotent, alors A Jacobson $\Rightarrow A\left[\frac{1}{x}\right]$ Jacobson

source : Matthew Emerton, Jacobson Rings

□ Les idéaux premiers de $A\left[\frac{1}{x}\right]$ s'identifient (via $A \to A\left[\frac{1}{x}\right]$) aux idéaux premiers de A qui ne contiennent pas x.
Un idéal maximal de A, qui ne contient pas x, donne un idéal maximal de $A\left[\frac{1}{x}\right]$.
Un idéal maximal de $A\left[\frac{1}{x}\right]$, réciproquement, donne un idéal premier $\mathfrak{p}$ de A, qui ne contient pas x (et maximal parmi les idéaux premiers qui ne contiennent pas x). Mais A est Jacobson, donc $\exists$ un idéal max de A tq $\mathfrak{p} \subseteq m$ et $x \notin m$, et $\mathfrak{p} = m$ par maximalité parmi les idéaux premiers qui ne contiennent pas x. Donc $\mathfrak{p}$ est maximal.

On trouve donc que les idéaux max de $A\left[\frac{1}{x}\right]$ correspondent (bijectivement) aux idéaux max de A qui ne contiennent pas x.

Pour montrer que $A\left[\frac{1}{x}\right]$ est Jacobson, il suffit donc de montrer que si $\mathfrak{p}$ est un idéal premier de A ne contenant pas x, alors

$$\bigcap_{\substack{m \text{ idéal max} \\ \text{de } A \text{ t.q. } x \notin m \\ \text{et } \mathfrak{p} \subseteq m}} m = \mathfrak{p} \qquad (\supseteq \text{ est immédiat})$$

Soit $y \in \bigcap_{\substack{m \text{ idéal max} \\ \text{de } A \text{ t.q.} \\ x \notin m \text{ et } \mathfrak{p} \subseteq m}} m$. Or $x \in \bigcap_{\substack{m \text{ idéal max} \\ \text{de } A \text{ t.q.} \\ x \in m \text{ et } \mathfrak{p} \subseteq m}} m$, donc

$$xy \in \bigcap_{\substack{m \text{ idéal max} \\ \text{de } A \text{ t.q. } \mathfrak{p} \subseteq m}} m = \mathfrak{p}$$

($\mathfrak{p}$: A Jacobson)

Or $\mathfrak{p}$ est premier et $x \notin \mathfrak{p}$, donc $y \in \mathfrak{p}$. ☒

Déf : Soit $f : A \to B$ un morphisme d'anneaux commutatifs unitaires. On dit que f est entier si tout élément de B est racine d'un polynôme unitaire à coefficients dans l'image de f.

Lemme : Soit $f : A \to B$ un morphisme entier. Alors

(i) L'image réciproque d'un idéal max de B est un idéal max de A.

(ii) Si f injectif, tout idéal max de A est de cette forme.

(iii) Si f injectif et A et B intègres, alors si I idéal de B, $I \neq 0 \Rightarrow f^{-1}(I) \neq 0$.

Atiyah & MacDonald, *Introduction to Commutative Algebra* chap 5

□ (i) Soit m idéal max de B

$$A \xrightarrow{f} B \twoheadrightarrow B/m \qquad \ker(A \to B/m) = f^{-1}(m)$$

(B/m corps)

donne $A/f^{-1}(m) \hookrightarrow B/m$

Soit $x \neq 0$ dans l'image de $A/f^{-1}(m)$.

Il a un inverse $x^{-1} \in B/m$.

Comme f est entier $\exists a_0, \dots, a_{d-1}$ $\in$ image de $A/f^{-1}(m)$

t.q. $x^{-d} + a_{d-1} x^{-(d-1)} + \dots + a_0 = 0$,

d'où $x^{-1} = -a_{d-1} - a_{d-2} x - \dots - a_0 x^{d-1} \in$ image de $A/f^{-1}(m)$.

Donc l'image de $A/f^{-1}(m)$ est un corps, donc $f^{-1}(m)$ est maximal.

(ii) Soit m un idéal max de A, soit $S = A \setminus m$, alors S est une partie stable par $\times$ pour A et pour B, donc on a des localisés $S^{-1}A$ et $f(S)^{-1}B$, et

$$\begin{array}{ccc} A & \hookrightarrow & B \\ \downarrow & & \downarrow \\ S^{-1}A & \hookrightarrow & f(S)^{-1}B \end{array}$$

fonctorialité de la localisation

et le morphisme $S^{-1}A \to f(S)^{-1}B$ est entier :

si $\frac{x}{f(s)} \in f(S)^{-1}B$ on a $x^n + a_{n-1}x^{n-1} + \dots + a_0 = 0$,

donc $\left(\frac{x}{f(s)}\right)^n + \frac{a_{n-1}}{f(s)}\left(\frac{x}{f(s)}\right)^{n-1} + \dots + \frac{a_0}{f(s)^n} = 0$.

Soit m' un idéal maximal de $f(S)^{-1}B$.
Son image réciproque dans $S^{-1}A$ est un idéal maximal de $S^{-1}A$. Or $S^{-1}A$ est un anneau local d'unique idéal max $S^{-1}m$. Donc l'image réciproque de m' dans $S^{-1}A$ est $S^{-1}m$, et l'image réciproque de celui-ci dans A est m.
Soit $\mathfrak{p}$ l'image réciproque de m' dans B.
Par commutativité du diagramme, $f^{-1}(\mathfrak{p}) = m$.
De plus, $\mathfrak{p}$ est un idéal premier de B ne rencontrant pas S. Soit m'' un idéal max de B contenant $\mathfrak{p}$, donc $f^{-1}(m'')$ est un idéal max de A (par (i)) contenant m, donc $f^{-1}(m'') = m$.

(iii) : Soit I idéal de B. Par contraposition, supposons $f^{-1}(I) = \{0\}$.
Soit $S = A \setminus \{0\}$. Comme A est intègre, c'est une partie stable par $\times$ ($0 \in \{0\}$ est premier).

$$\begin{array}{ccc} A & \hookrightarrow & B \\ \downarrow & & \downarrow \\ \text{Frac}(A) = S^{-1}A & \hookrightarrow & f(S)^{-1}B \end{array}$$

$f^{-1}(I) = \{0\}$
donc $f(S) \cap I = \emptyset$
$f(S)^{-1}I$ est un idéal de $f(S)^{-1}B$

Tout élément de $f(S)^{-1}B$ est entier sur $\text{Frac}(A)$, donc si $x \in f(S)^{-1}B \setminus \{0\}$,

$$x^d + a_{d-1}x^{d-1} + \dots + a_0 = 0$$

Comme $x \neq 0$ $f(S)^{-1}B$ intègre, on peut supposer $a_0 \neq 0$

$$x\,(x^{d-1} + a_{d-1}x^{d-2} + \dots + a_1) = \underbrace{-a_0}_{\text{inversible}}$$

donc x inversible dans $f(S)^{-1}B$. Donc $f(S)^{-1}B$ est un corps.

Les idéaux de $f(S)^{-1}B$ sont $\{0\}$ et $f(S)^{-1}B$,
donc $f(S)^{-1}I \in \{\{0\}, f(S)^{-1}B\}$.
Comme B est intègre, $f(S)^{-1}I = f(S)^{-1}B \iff I = B$,
or $f^{-1}(I) = \{0\}$, $f(B) \ni 1_A$,
donc $f(S)^{-1}I = 0$, donc $I = 0$. ☐

On en déduit :

Lemme : Si $f : A \to B$ est entier, A Jacobien,
alors B est Jacobien.

▷ Soit $\mathfrak{p}$ un idéal premier de B,
alors $f^{-1}(\mathfrak{p})$ est premier, et

$$A/f^{-1}(\mathfrak{p}) \hookrightarrow B/\mathfrak{p}$$

Les deux anneaux sont intègres.

$A/f^{-1}(\mathfrak{p})$ est Jacobien, donc

$$\bigcap_{\substack{\mathfrak{m} \text{ idéal max} \\ \text{de } A/f^{-1}(\mathfrak{p})}} \mathfrak{m} = \{0\}$$

Par (i) et (ii) du lemme précédent, on en déduit

$$f^{-1}\left(\bigcap_{\substack{\mathfrak{m} \text{ idéal max} \\ \text{de } B/\mathfrak{p}}} \mathfrak{m}\right) = \bigcap_{\substack{\mathfrak{m} \text{ idéal max} \\ \text{de } B/\mathfrak{p}}} f^{-1}(\mathfrak{m}) = \{0\}$$

On trouve tous les idéaux max de $A/f^{-1}(\mathfrak{p})$

Par (iii), on a donc

$$\bigcap_{\substack{\mathfrak{m} \text{ idéal max} \\ \text{de } B/\mathfrak{p}}} \mathfrak{m} = \{0\}.$$

Donc B est Jacobien. ☐

Lemme : Si $f : A \hookrightarrow B$, A et B intègres, A Jacobson, et $\exists a \in A \setminus \{0\}$ tq $A\left[\frac{1}{a}\right] \longrightarrow B\left[\frac{1}{f(a)}\right]$ entier, alors $\bigcap_{\substack{m \text{ idéal max} \\ \text{de } B}} m = 0$.

▷ A Jacobson donc $A\left[\frac{1}{a}\right]$ Jacobson (localisé), donc $B\left[\frac{1}{f(a)}\right]$ Jacobson.

Soit m' idéal max de $B\left[\frac{1}{f(a)}\right]$.

abus de notation : $f : A\left[\frac{1}{a}\right] \to B\left[\frac{1}{f(a)}\right]$ induit par f.

On (i), $f^{-1}(m')$ est un idéal max de $A\left[\frac{1}{a}\right]$, donc $f^{-1}(m') \cap A$ est un idéal max de A qui ne contient pas a.

(corps)

$$\begin{array}{ccc} A/(f^{-1}(m') \cap A) & \hookrightarrow & B/(m' \cap B) \\ \downarrow & & \downarrow \\ A\left[\frac{1}{a}\right]/f^{-1}(m') & \xrightarrow[\text{entier}]{} & B\left[\frac{1}{a}\right]/m' \end{array}$$

(corps)

Donc $B/(m' \cap B)$ est un sous-anneau de $B\left[\frac{1}{a}\right]/m'$, qui est une extension algébrique de $A/(f^{-1}(m') \cap A)$, donc tous ses éléments non nuls ont un inverse dans $B/(m' \cap B)$, donc c'est un corps, donc $m' \cap B$ est un idéal max de B.

$$\bigcap_{\substack{m \text{ idéal max} \\ \text{de } B}} m \subseteq \bigcap_{\substack{m' \text{ idéal max} \\ \text{de } B\left[\frac{1}{a}\right]}} (m' \cap B) \subseteq \bigcap_{\substack{m' \text{ idéal max} \\ \text{de } B\left[\frac{1}{a}\right]}} m' = 0$$

$B\left[\frac{1}{a}\right]$ Jacobson

Lemme : Si $\bigcap_{\substack{m \text{ idéal max} \\ \text{de } A}} m = \{0\}$ alors $\bigcap_{\substack{m' \text{ idéal max} \\ \text{de } A[X]}} m' = \{0\}$.

□ Comme $\bigcap_{\substack{m \text{ idéal max} \\ \text{de } A}} m = \{0\}$,

on a $\bigcap_{\substack{m \text{ idéal max} \\ \text{de } A}} mA[X] = \{0\}$.

Il suffit donc de montrer, pour tout idéal max m de A :

$$\bigcap_{\substack{m' \text{ idéal max de } A[X] \\ \text{t.q. } mA[X] \subseteq m'}} m' = mA[X]$$

i.e. $\bigcap_{\substack{m' \text{ idéal max} \\ \text{de } A[X] \\ / mA[X]}} m' = 0$

$$A[X]/mA[X] \simeq (A/m)[X].$$

↑ corps

i.e. $\bigcap_{\substack{P \in (A/m)[X] \\ P \text{ irréductible}}} (P) = 0$,

ce qui est vrai (A/m infini $\longrightarrow$ un polynôme $\neq 0$ n'a qu'un nbre fini de racines

A/m fini $\longrightarrow$ il y a des irréductibles de tout degré)

□

Th : Si A est Jacobson, alors $A[X]$ est Jacobson.

Rem : La réciproque est vraie (A est un quotient de $A[X]$).

□ Soit $\mathfrak{p}$ un idéal premier de $A[X]$.
Soit A' l'image de A dans $B := A[X]/\mathfrak{p}$.

B est intègre, donc A' aussi.
$A' \subseteq B$ se prolonge en $A'[X] \twoheadrightarrow B$.

A' est un quotient de A (par le noyau de $A \twoheadrightarrow B$)
A est Jacobson, donc A' aussi,
or 0 est un idéal premier de A',
donc $\bigcap_{\mathfrak{m} \text{ idéal max de } A'} \mathfrak{m} = 0$, donc $\bigcap_{\mathfrak{m} \text{ idéal max de } A'[X]} \mathfrak{m} = 0$.

Si $A'[X] \xrightarrow{\sim} B$, ceci conclut la preuve.

Sinon, soit I le noyau de $A'[X] \twoheadrightarrow B$.
A' est intègre, $(\mathrm{Frac}\, A')[X]$ est principal,
donc $\exists\, a \in A' \setminus \{0\}$ t.q. $I\left[\frac{1}{a}\right]$ soit principal dans $A'\left[\frac{1}{a}\right]$
$I\left[\frac{1}{a}\right] = (f)$, f unitaire,

$B\left[\frac{1}{a}\right] \simeq \dfrac{A'\left[\frac{1}{a}\right][X]}{(f)}$ ← $A'\left[\frac{1}{a}\right]$-module de type fini, car f est unitaire.

donc on a :

$$\begin{cases} A' \subseteq B & A' \text{ et } B \text{ intègres} \\ & A' \text{ Jacobson} \\ A'\left[\frac{1}{a}\right] \longrightarrow B\left[\frac{1}{a}\right] & \text{entier (car } B\left[\frac{1}{a}\right] \text{ est de type fini sur } A'\left[\frac{1}{a}\right]) \end{cases}$$

donc (cf. un lemme précédent)
$\bigcap_{\mathfrak{m} \text{ idéal max de } B} \mathfrak{m} = \{0\}$, ce qui conclut la preuve. ∎

Th : Si A est Jacobson, alors toute A-algèbre de type fini est Jacobson.

□ Toute A-algèbre de type fini est un quotient d'un $A[X_0, \dots, X_{n-1}]$, qui est Jacobson par le th précédent (+ récurrence). ⊠

Corollaire : Si K est un corps, toute K-algèbre de type fini est Jacobson.

□ car K est Jacobson. ⊠

Corollaire : Si K est un corps, si A est une K-algèbre de type fini, alors

$$\bigcap_{\mathfrak{m} \text{ idéal max de } A} \mathfrak{m} = \{ \text{nilpotents de } A \}.$$

□ cf remarque en début d'année. ⊠

Corollaire : A étale $\iff$ $K^{sep} \otimes_K A$ diagonalisable

(cf. preuve de (iii) $\Rightarrow$ (i))

Corollaire : Si L/K est finie, alors

L étale $\iff$ L/K séparable.
(comme K-algèbre)

Prop : Les produits finis, produits tensoriels finis, quotients de K-algèbres diagonalisables (resp. étales) sont diagonalisables (resp étale).

- diagonalisable : facile
  étale : s'en déduit par $\otimes_K K^{sep}$. □

Prop : Si A étale, L/K extension, alors $L \otimes_K A$ est étale.

- $L^{sep} \geq K^{sep}$, donc $L^{sep} \otimes_K A$ diagonalisable □

(b) Classification des algèbres étales sur un corps.

K corps $\quad K^{sep}$ = clôture séparable

$G = Gal(K^{sep}/K)$

Si A = K-algèbre étale (finie), on définit

$$\mathcal{F}(A) := \mathrm{Hom}_{K\text{-algèbre}}(A, K^{sep})$$

G agit sur $\mathcal{F}(A)$ par l'action sur K^{sep}.

Rem : On a $\mathcal{F}(\prod A_i) = \bigsqcup \mathcal{F}(A_i)$ (union disjointe)

Comme A est un produit fini d'extensions finies séparables de K, on a $|\mathcal{F}(A)| \leq \dim_K A$ (donc $\mathcal{F}(A)$ est fini).

De plus, il existe K^{sep} / L / K (finie) t.q. $Gal(K^{sep}/L)$ agit trivialement sur $\mathcal{F}(A)$ — ce qui montre la continuité de l'action de G sur $\mathcal{F}(A)$! (Exercice : le vérifier)

↳ muni de la topologie discrète.

Prop : $\mathcal{F}$ est un foncteur (contravariant) de la catégorie des K-algèbres finies étales vers la catégorie des ensembles finis munis d'une action continue de G.

□ Si $f : A \to B$ est un morphisme de K-algèbres, avec A et B finies étales, alors on a

$$\begin{cases} \mathcal{F}(B) \longrightarrow \mathcal{F}(A) \\ h \longmapsto h \circ f \end{cases}$$

compatible à l'action de G.

∎

Réciproquement, si S est un ensemble fini muni d'une action continue de G,

on note $\mathcal{A}(S) := \{$ applications $f : S \longrightarrow K^{sep}$ / $\forall \sigma \in G \quad \forall s \in S \quad \sigma(f(s)) = f(\sigma(s))\}$

(K-algèbre) $= \mathrm{Hom}_G(S, K^{sep})$

- Si G agit transitivement sur S :

Soit $s \in S$,

soit $H := $ le stabilisateur de s (pour l'action de G)

soit $L := (K^{sep})^H$.

H est un sous-groupe ouvert de G (par continuité) (et fermé !)

donc L/K est finie (+ séparable par construction).

On a $\begin{cases} \mathcal{A}(S) \longrightarrow L \\ f \longmapsto f(s) \end{cases}$

- injectif car G agit transitivement sur S
- surjectif par construction de L (si $y \in L$, on définit $\forall \sigma \in G \ f(\sigma(s)) = \sigma(y)$)

donc $\mathcal{A}(S) \underset{K\text{-algèbre}}{\simeq} L$

De plus, $\mathcal{F}(L) = \mathrm{Hom}_{K\text{-alg}}(L, K^{sep})$

$S \underset{\text{ens. + action de } G}{\simeq} G/H$ et $G/H \simeq \mathcal{F}(L)$

$s \longleftrightarrow \bar{1}_G$ $\qquad \sigma \longmapsto \sigma|_L$

donc $S \underset{\text{ens. + action de } G}{\sim} \mathcal{F}(L)$.

$s \longleftrightarrow (L \subseteq K^{sep})$

Réciproquement, si L/K finie séparable,

$\mathcal{F}(L) = \mathrm{Hom}_K(L, K^{sep})$

Soit $\sigma \in \mathcal{F}(L)$. $\sigma : L \hookrightarrow K^{sep}$

$G = \mathrm{Gal}(K^{sep}/K)$ agit transitivement sur $\mathcal{F}(L)$,

et le stabilisateur de σ est $\mathrm{Gal}(K^{sep}/\sigma(L))$,

donc $\mathcal{A}(\mathcal{F}(L)) \underset{K\text{-alg}}{\simeq} \sigma(L) \xrightarrow{\sim} L$.

- Dans le cas général, $S = \coprod_{\text{orbites}} S_i$ union disjointe finie

$\mathcal{A}(S) \simeq \prod \mathcal{A}(S_i)$ donc $\mathcal{A}(S)$ finie étale

$\mathcal{F}(\mathcal{A}(S)) \simeq \coprod S_i = S$

On obtient un foncteur contravariant, essentiellement surjectif.

Prop : $\mathcal{F}$ est une équivalence de catégories (contravariante) de quasi-inverse $\mathcal{A}$.

□ Il reste à vérifier que

$$\left\{ \begin{array}{ccc} \mathrm{Hom}_{K\text{-alg}}(A, B) & \longrightarrow & \mathrm{Hom}(\mathcal{F}(B), \mathcal{F}(A)) \\ f & \longmapsto & (h \mapsto h \circ f) \end{array} \right.$$

est une bijection.

$$\mathrm{Hom}_{K\text{-alg}}(A, B) \simeq \mathrm{Hom}_{K^{sep}\text{-alg}}(K^{sep} \otimes_K A, K^{sep} \otimes_K B)^G,$$

(extension des scalaires)

or $K^{sep} \otimes A \simeq \prod_{\mathcal{F}(A)} K^{sep}$

donc $\mathrm{Hom}_{K^{sep}\text{-alg}}(K^{sep} \otimes_K A, K^{sep} \otimes_K B) \simeq \mathrm{Hom}_{\text{ensembles}}(\mathcal{F}(B), \mathcal{F}(A))$

finalement, $\mathrm{Hom}_{ens}(\mathcal{F}(B), \mathcal{F}(A))^G \simeq \mathrm{Hom}_G(\mathcal{F}(B), \mathcal{F}(A))$. ∎

Rem : Géométriquement (via le foncteur Spec) les K-algèbres étales correspondent aux variétés algébriques de dimension 0.
On obtient un foncteur

$$\left\{ \text{variétés de dim } 0 \right\} \longrightarrow \left\{ G\text{-ensembles} \right\}$$
$$V \longmapsto V(K^{sep})$$

fin cours n°13

Chapitre IV : Théorie de Galois et corps de nombres.

(a) Factorisation des idéaux

$K/\mathbb{Q}$ extension finie (i.e. K corps de nombres)

$\mathcal{O}_K$ = entiers de K $\quad (\mathcal{O}_{\mathbb{Q}} = \mathbb{Z})$.

L/K est finie $\quad \mathcal{O}_L$ est un $\mathcal{O}_K$-module de type fini, pas forcément libre !

Samuel, Théorie algébrique des nombres.

cf. aussi : Lesieur Bertelich, chap. I : A. Fröhlich, Local Fields.

$\mathcal{O}_K, \mathcal{O}_L$ sont des anneaux de Dedekind $\longrightarrow$ existence et unicité de la factorisation en produit d'idéaux premiers.

cf. annexe page suivante $\longrightarrow$

Rem : $\mathcal{O}_K$ est principal (par ex $K = \mathbb{Q}$), on peut montrer que $\mathcal{O}_L$ est un $\mathcal{O}_K$-module libre de rang $[L:K]$.

$\mathfrak{p}$ idéal premier ($\neq 0$) de $\mathcal{O}_K$. Alors $\mathfrak{p}\mathcal{O}_L$ est un idéal ($\neq 0$) de $\mathcal{O}_L$.

décomposition $\longrightarrow$ $\quad \mathfrak{p}\mathcal{O}_L = \prod_{i=0}^{m-1} \mathfrak{P}_i^{e_i}$ $\quad$ $\mathfrak{P}_i$ idéaux premiers de $\mathcal{O}_L$, distincts.

Rem : $\mathcal{O}_K \cap \mathfrak{P}_i = \mathfrak{p}$ (le morphisme $\mathcal{O}_K \to \mathcal{O}_L$ est entier, donc $\mathcal{O}_K \cap \mathfrak{P}_i$ est un idéal maximal de $\mathcal{O}_K$, et cet idéal contient $\mathfrak{p}$.)

$\mathcal{O}_K/\mathfrak{p}$ corps, $\quad \mathcal{O}_L/\mathfrak{P}_i$ corps

(car les anneaux de Dedekind sont de hauteur 1, donc ces idéaux sont maximaux)

Déf : On dit que $\mathfrak{p}$ se ramifie dans l'extension L/K si $\exists i$ $e_i > 1$. (L/K est ramifiée en $\mathfrak{p}$.)

On a une extension $\quad \mathcal{O}_L/\mathfrak{P}_i$ / $\mathcal{O}_K/\mathfrak{p}$ $\quad$ (ce sont des corps finis, dans le cas des corps de nombres)

$f_i := [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}]$.

(A intègre)
i.e. $\forall x \in K$ x entier sur A $\Rightarrow x \in A$.

cf Samuel, chap II §7

Th : A anneau intégralement clos, $K := \mathrm{Frac}\, A$, $[L:K] = n < +\infty$, $A' = \{x \in L \mid x \text{ entier sur } A\}$, L/K séparable

Alors A' est un sous-A-module d'un A-module libre de rang n.

□ **lemme :** Il existe un K-base de L formée d'éléments de A'.

En effet, si $x \in L$, soit $\sum_{i=0}^{d} a_i X^i \in K[X]$ son polynôme minimal, soit $a \in \mathcal{O}_K \setminus \{0\}$ tel que $\forall i \; a a_i \in \mathcal{O}_K$ (par ex : a = produit des dénominateurs des a_i), alors

$$\sum_{i=0}^{d} \underbrace{a^{d+1-i} a_d^{d-i} a_i}_{\in \mathcal{O}_K} (a a_d x)^i = a^{d+1} a_d^{d} \sum_{i=0}^{d} a_i x^i = 0$$

donc $\underbrace{a a_d}_{\neq 0} x \in A'$.

Partant d'une K-base de L, il suffit donc de multiplier chaque élément de la base par un élément de $\mathcal{O}_K \setminus \{0\}$ bien choisi pour avoir une K-base de L formée d'éléments de A'.

Soit $(e_i)_{0 \le i \le n}$ une K-base de L formée d'éléments de A'. Soit $(f_i)_{0 \le i \le n}$ la base duale pour la forme bilinéaire $x, y \mapsto \mathrm{Tr}_{L/K}(xy)$.

(On utilise ici L/K séparable.)

Si $x \in A'$, on a $x = \sum_{i=0}^{n-1} c_i \omega_i$, $c_i \in K$

et $c_i = \mathrm{Tr}_{L/K}(\underbrace{x e_i}_{\in A'}) =$ somme des conjugués de $x e_i$ (dans $\bar{K}$)

$\in A$

□

Corollaire : Si de plus A est principal, alors A' est libre de rang n.

□ C'est un sous-module d'un module libre de rang n ($+$ A principal) donc c'est un module libre de rang $\leq n$. De plus, il contient une K-base de L (cf. dém. précédente), donc il est de rang n. □

Exemple : $K = \mathbb{Q}$ $\quad L = \mathbb{Q}(\sqrt[3]{2})$ $\quad \mathcal{O}_K = \mathbb{Z}$ $\quad \mathcal{O}_L = \mathbb{Z}[\sqrt[3]{2}]$ (exercice !)

Pour chercher la décomposition de $p\mathcal{O}_L$, on travaille dans $\mathcal{O}_L/p\mathcal{O}_L$.

$$\mathbb{Z}[\sqrt[3]{2}]/(2) \simeq \frac{\mathbb{F}_2[X]}{(X^3-2)} \simeq \frac{\mathbb{F}_2[X]}{(X)^3}$$

$$(2) = (\sqrt[3]{2})^3$$

voir aussi l'exemple ajouté page suivante

$$\mathbb{Z}[\sqrt[3]{2}]/(3) \simeq \frac{\mathbb{F}_3[X]}{(X^3-2)} \simeq \frac{\mathbb{F}_3[X]}{(X+1)^3}$$

$$(3) = (3, 1+\sqrt[3]{2})^3$$

$$\mathbb{Z}[\sqrt[3]{2}]/(5) \simeq \frac{\mathbb{F}_5[X]}{(X^3-2)} \simeq \frac{\mathbb{F}_5[X]}{(X+2)(X^2-2X-1)}$$

↑ irréductible

$$(5) = (5, 2+\sqrt[3]{2})(5, \sqrt[3]{4} - 2\sqrt[3]{2} - 1)$$

Th : On a $\sum_{i=0}^{m-1} e_i f_i = [L:K]$.

□ Notons que $\mathcal{O}_L/p\mathcal{O}_L$ est une $\underbrace{\mathcal{O}_K/p}_{\text{corps}}$-algèbre.

On a

$$\mathcal{O}_L \supseteq \mathcal{O}_0 \supseteq \mathcal{O}_0^2 \supseteq \dots \supseteq \mathcal{O}_0^{e_0} \supseteq \mathcal{O}_0^{e_0}\mathcal{O}_1 \supseteq \dots \supseteq \mathcal{O}_0^{e_0}\mathcal{O}_1^{e_1} \supseteq \dots \supseteq \underbrace{\mathcal{O}_0^{e_0}\cdots\mathcal{O}_{m-1}^{e_{m-1}}}_{=p\mathcal{O}_L}$$

À chaque étape, le quotient est un anneau qui n'a (par factorisation) pas d'autre idéal que 0 et tout l'anneau, i.e. c'est un corps. Si $\mathcal{O}_i$ est l'idéal que l'on ajoute

ajout : example fait en cours

$L = \mathbb{Q}(i)$ $\quad K = \mathbb{Q}$

$\mathcal{O}_L = \mathbb{Z}[i]$ $\quad \mathcal{O}_K = \mathbb{Z}$

- $p = (3)$

$$\frac{\mathbb{Z}[i]}{(3)} \simeq \frac{\mathbb{Z}[X]}{(3, X^2+1)} \simeq \frac{\mathbb{F}_3[X]}{(X^2+1)} \simeq \mathbb{F}_9$$

(3) idéal premier de $\mathbb{Z}[i]$ $\quad e = 1$, $f = 2$ $\quad (m = 1)$

- $p = (2)$

$$\frac{\mathbb{Z}[i]}{(2)} \simeq \frac{\mathbb{F}_2[X]}{(X^2+1)} \simeq \frac{\mathbb{F}_2[X]}{(X+1)^2}$$

$(2) = (1+i)^2$ $\quad e = 2$, $f = 1$ $\quad (m = 1)$

- $p = (5)$

$$\frac{\mathbb{Z}[i]}{(5)} \simeq \frac{\mathbb{F}_5[X]}{(X^2+1)} \simeq \frac{\mathbb{F}_5[X]}{(X-2)} \times \frac{\mathbb{F}_5[X]}{(X+2)} \simeq \mathbb{F}_5^2$$

$(5) = (2+i)(2-i)$ $\quad e_0 = 1$, $f_0 = 1$

$e_1 = 1$, $f_1 = 1$

$(m = 2)$

à cette étape, c'est une extension de $\mathcal{O}_L/\mathfrak{P}_i$, et ses idéaux sont les sous-$\mathcal{O}_L/\mathfrak{P}_i$-modules donc (e.v.)
c'est un $\mathcal{O}_L/\mathfrak{P}_i$-e.v. sans s.e.v non triviaux,

donc ce quotient est de dim 1 sur $\mathcal{O}_L/\mathfrak{P}_i$, donc de dim f_i sur $\mathcal{O}_K/\mathfrak{p}$.

On trouve donc $\sum_{i=0}^{m-1} e_i f_i = \dim_{\mathcal{O}_K/\mathfrak{p}} \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$:

Il reste à montrer que $\dim_{\mathcal{O}_K/\mathfrak{p}} \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L = [L:K]$.

(Rem : Si $\mathcal{O}_K$ est principal, on a $\mathcal{O}_L \simeq \mathcal{O}_K^{[L:K]}$ ($\mathcal{O}_K$-mod),

donc (par $\otimes_{\mathcal{O}_K} \mathcal{O}_K/\mathfrak{p}$) $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \simeq \left(\mathcal{O}_K/\mathfrak{p}\right)^{[L:K]}$.

Mais $\mathcal{O}_K$ n'est pas toujours principal. En revanche, ses localisés le sont !)

Soit $S := \mathcal{O}_K \setminus \mathfrak{p}$, alors $S^{-1}\mathcal{O}_K$ est un anneau local, d'unique idéal maximal $S^{-1}\mathfrak{p}$.

Lemme : $S^{-1}\mathcal{O}_K$ est un idéal principal.

En effet (par factorisation dans $\mathcal{O}_K$), les idéaux de $S^{-1}\mathcal{O}_K$ sont les puissances de $\mathfrak{p}$. Si $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$, (ils sont distincts)
alors on a forcément $(\pi) = \mathfrak{p}$; donc tous les idéaux de $S^{-1}\mathcal{O}_K$ sont principaux. ($S^{-1}\mathcal{O}_K$ est intègre, car $\mathcal{O}_K$ est intègre).

Alors $S^{-1}\mathcal{O}_L$ est un $S^{-1}\mathcal{O}_K$-module.

↑ Car les éléments sont entiers sur $S^{-1}\mathcal{O}_L$ (précédente)

Donc (cf annexe) $S^{-1}\mathcal{O}_L$ est un $S^{-1}\mathcal{O}_K$-module libre de rang $[L:K]$.

En spécialisant par $S^{-1}\mathfrak{p}$, on en déduit que $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ est de dim $[L:K]$ sur $\mathcal{O}_K/\mathfrak{p}$. ∎

Prop : Si L/K est galoisienne, alors $\mathrm{Gal}(L/K)$ agit transitivement sur $\{\mathfrak{P}_i \,;\, 0 \le i < m\}$.

Rem : l'ensemble des idéaux premiers de $\mathcal{O}_K$ s'identifie à l'ensemble des orbites de l'action de $\mathrm{Gal}(L/K)$ sur l'ensemble des idéaux premiers de $\mathcal{O}_L$.

La preuve s'appuie sur :

Lemme (d'évitement des idéaux premiers) :
Soit A = anneau (commutatif unitaire),
soient $\mathfrak{p}_0, \dots, \mathfrak{p}_{k-1}$ idéaux premiers de A (famille finie)
et $\mathfrak{a}$ idéal de A tq. $\forall i \ \mathfrak{a} \not\subset \mathfrak{p}_i$,
alors $\exists x \in \mathfrak{a} \ \ \forall i \ \ x \notin \mathfrak{p}_i$.

□ On peut supposer $\forall i,j \ \ i \neq j \Rightarrow \mathfrak{p}_j \not\subset \mathfrak{p}_i$
(sinon on enlève $\mathfrak{p}_j$)
Soient $\forall i,j \ \ x_{ij} \in \mathfrak{p}_j \setminus \mathfrak{p}_i$
$\forall i \ \ a_i \in \mathfrak{a} \setminus \mathfrak{p}_i$

$$\forall i \qquad b_i := a_i \prod_{j \neq i} x_{ij}$$

alors $b_i \in \mathfrak{a}$ (car $a_i \in \mathfrak{a}$)
$\forall j \neq i \ \ b_i \in \mathfrak{p}_j$ (car $x_{ij} \in \mathfrak{p}_j$)
$b_i \notin \mathfrak{p}_i$ (car $\mathfrak{p}_i$ premier et $a_i, x_{ij} \notin \mathfrak{p}_i$).

On pose $x := \sum_i b_i$, alors $x \in \mathcal{O}_L$ et $\forall i \; x \notin \mathfrak{P}_i$. ⊕

preuve des th :

$\exists i \;\; \mathfrak{p}\mathcal{O}_L = \prod \mathfrak{P}_i^{e_i}$,

soient i, j tq. $\forall \sigma \in \mathrm{Gal}(L/K) \;\; \sigma(\mathfrak{P}_j) \not\subseteq \mathfrak{P}_i$,

alors par le lemme, $\exists x \in \mathfrak{P}_i \;\; \forall \sigma \;\; x \notin \sigma(\mathfrak{P}_j)$,

or $N_{L/K}(x) = \prod_\sigma \underbrace{\sigma(x)}_{\in \mathcal{O}_L} \in \mathfrak{P}_i \cap \mathcal{O}_L = \mathfrak{p}$,

$\in \mathfrak{P}_i$ pour $\sigma = \mathrm{id}$

et d'autre part $\forall \sigma \;\; x \notin \sigma(\mathfrak{P}_j)$

$\sigma^{-1}(x) \notin \mathfrak{P}_j$

donc $\forall \sigma \;\; \sigma(x) \notin \mathfrak{P}_j$, or $\mathfrak{P}_j$ est premier,

donc $N_{L/K}(x) \notin \mathfrak{P}_j$, et $\mathfrak{p} \subseteq \mathfrak{P}_j$: contradiction.

Donc $\forall i, j \;\; \exists \sigma \in \mathrm{Gal}(L/K) \;\; \sigma(\mathfrak{P}_j) \subseteq \mathfrak{P}_i$

↑ ↗

idéaux maximaux de $\mathcal{O}_L$

$\sigma(\mathfrak{P}_j) = \mathfrak{P}_i$.

Par unicité de la factorisation + action de $\mathrm{Gal}(L/K)$, on en déduit :

- e_i ne dépend pas de i $\quad (e_i = e)$ indice de ramification
- f_i ne dépend pas de i $\quad (f_i = f)$ degré résiduel

donc $\mathfrak{p}\mathcal{O}_L = \prod_{i=0}^{m-1} \mathfrak{P}_i^e$ et $[L:K] = efm$.

Déf : Le groupe de décomposition de $\mathcal{O}_i$ est le sous-groupe de $\mathrm{Gal}(L/K)$ stabilisateur de $\mathcal{O}_i$:

$$D_{\mathcal{O}_i} := \{ \sigma \in \mathrm{Gal}(L/K) \mid \sigma(\mathcal{O}_i) = \mathcal{O}_i \}.$$

(Les $D_{\mathcal{O}_i}$ sont conjugués entre eux.)

On obtient alors un morphisme de groupes

$$D_{\mathcal{O}_i} \longrightarrow \mathrm{Aut}_{\mathcal{O}_K/\mathfrak{p}} (\mathcal{O}_L/\mathcal{O}_i).$$

On formule des dames, $m = \dfrac{|\mathrm{Gal}(L/K)|}{|D_{\mathcal{O}_i}|}$, donc $|D_{\mathcal{O}_i}| = \dfrac{[L:K]}{m} = ef$.

Les corps $\mathcal{O}_L/\mathcal{O}_i$ et $\mathcal{O}_K/\mathfrak{p}$ sont finis (corps de nombres), donc l'extension $\mathcal{O}_L/\mathcal{O}_i$ est galoisienne, de degré f

$$\begin{array}{ccc} & & \mathcal{O}_L/\mathcal{O}_i \\ & & | \\ & & \mathcal{O}_K/\mathfrak{p} \\ D_{\mathcal{O}_i} & \longrightarrow & \mathrm{Gal}(\mathcal{O}_L/\mathcal{O}_i \,/\, \mathcal{O}_K/\mathfrak{p}) \\ \| & & \| \\ ef & & f \end{array}$$

Déf : Le groupe d'inertie $I_{\mathcal{O}_i}$ est le noyau de ce morphisme

Prop : Le morphisme $D_{\mathcal{O}_i} \longrightarrow \mathrm{Gal}(\dots)$ est injectif.

□ Soit $M = L^{D_{\mathcal{O}_i}}$, alors $\mathfrak{p} := \mathcal{O}_i \cap \mathcal{O}_M$ est un idéal maximal de $\mathcal{O}_M (= \mathcal{O}_L \cap M)$. Comme $D_{\mathcal{O}_i} = \mathrm{Gal}(L/M)$ laisse fixe $\mathcal{O}_i$, et agit transitivement sur les idéaux premiers de la décomposition de $\mathfrak{p}$, on a $\mathfrak{p}\mathcal{O}_L = \mathcal{O}_i^{e'}$ pour un entier $e' \geq 1$.
Soit $f' := [\mathcal{O}_L/\mathcal{O}_i : \mathcal{O}_M/\mathfrak{p}]$ le degré résiduel.
On a $e'f' = [L:M] = |D_{\mathcal{O}_i}| = ef$
donc $e'|e$ ($\mathfrak{p}\mathcal{O}_M = \mathfrak{p}^*$..., d'où $\mathfrak{p}\mathcal{O}_L = \mathcal{O}_i^{*e'}$ ...)
et $f'|f$ (cf la tour $\mathcal{O}_L/\mathcal{O}_i$ / $\mathcal{O}_M/\mathfrak{p}$ / $\mathcal{O}_K/\mathfrak{p}$)

donc $e = e'$ et $f = f'$,

donc en particulier $[\mathcal{O}_M/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}] = 1$

i.e. $\mathcal{O}_M/\mathfrak{P} \simeq \mathcal{O}_K/\mathfrak{p}$ (induit par $\mathcal{O}_K \subseteq \mathcal{O}_M$)

Soit $x \in \mathcal{O}_L$ t.q. $\mathcal{O}_L/\mathfrak{P}_i = (\mathcal{O}_K/\mathfrak{p})[\bar{x}]$ (élément primitif),

soit $P(X) \in \mathcal{O}_M[X]$ son poly minimal sur M. (P unitaire)

Soit $\bar{P}(X) \in (\mathcal{O}_K/\mathfrak{p})[X]$ sa réduction mod $\mathfrak{P}$. ($\bar{P}$ unitaire)

Alors les racines de P dans L sont les $\sigma(x)^{\mathfrak{G}_L}$, $\sigma \in Gal(L/M)$
(car L/M est galoisienne, donc P est scindé sur L) $\quad \| \mathcal{D}_{\mathfrak{P}_i}$

donc les racines de $\bar{P}$ dans $\mathcal{O}_L/\mathfrak{P}_i$ sont les $\bar{\sigma}(\bar{x})$, $\bar{\sigma} \in \mathcal{D}_{\mathfrak{P}_i}/\mathfrak{g}_{\mathfrak{P}_i}$
(P scindé $\Rightarrow$ $\bar{P}$ scindé, en réduisant mod $\mathfrak{P}_i$)

(Ceci montre que $\mathcal{O}_L/\mathfrak{P}_i$ est une ext. galoisienne de $\mathcal{O}_K/\mathfrak{p}$, sans utiliser le fait que ce sont des corps finis.)

De plus, les conjugués de $\bar{x}$ sont des $\bar{\sigma}(\bar{x})$, $\bar{\sigma} \in \mathcal{D}_{\mathfrak{P}_i}/\mathfrak{g}_{\mathfrak{P}_i}$

d'où la surjectivité de $\mathcal{D}_{\mathfrak{P}_i} \longrightarrow Gal(\mathcal{O}_L/\mathfrak{P}_i \,/\, \mathcal{O}_K/\mathfrak{p})$.

□

Corollaire : • $Gal(\mathcal{O}_L/\mathfrak{P}_i \,/\, \mathcal{O}_K/\mathfrak{p}) \simeq \mathcal{D}_{\mathfrak{P}_i}/\mathfrak{g}_{\mathfrak{P}_i}$

• $|\mathfrak{g}_{\mathfrak{P}_i}| = e$.

• Si $e = 1$ ($\mathfrak{p}$ non ramifié)

alors $\underbrace{Gal(\mathcal{O}_L/\mathfrak{P}_i \,/\, \mathcal{O}_K/\mathfrak{p})}_{\text{cyclique d'ordre } f} \simeq \mathcal{D}_{\mathfrak{P}_i}$.

Rem : $\cdot\ \mathcal{I}_{\mathcal{O}_i} = \{ \sigma \in \mathrm{Gal}(L/K) \ / \ \forall x \in \mathcal{O}_L \quad \sigma(x) \equiv x \mod \mathcal{O}_i \}$

· Si $\mathfrak{p}$ n'est pas ramifié, l'automorphisme de Frobenius de $\mathcal{O}_L/\mathcal{O}_i$ (sur $\mathcal{O}_K/\mathfrak{p}$) donne un élément de $\mathcal{D}_{\mathcal{O}_i} \subseteq \mathrm{Gal}(L/K)$. En général, il dépend de $\mathcal{O}_i$: si l'on remplace $\mathcal{O}_i$ par $\mathcal{O}_j$, alors $\mathcal{D}_{\mathcal{O}_i}$ est remplacé par son conjugué $\mathcal{D}_{\mathcal{O}_j}$, et le Frobenius est remplacé par un conjugué.
Si l'extension L/K est abélienne, l'élément de $\mathrm{Gal}(L/K)$ correspondant au Frobenius est bien défini.
(On le note parfois $\left(\frac{L/K}{\mathfrak{p}}\right)$.)

· $\mathfrak{p}$ non ramifié $\iff$ $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ réduite (étale)
($\iff e = 1$)

fin cours n°14

$\mathcal{D}_\mathcal{O}$, $\mathcal{I}_\mathcal{O}$ sont des sous-groupes de $\mathrm{Gal}(L/K)$. Ils correspondent donc à des sous-corps de L ($L^{\mathcal{D}_\mathcal{O}}$ et $L^{\mathcal{I}_\mathcal{O}}$).

$$\begin{array}{ccccc}
\mathcal{O} & \subseteq & \mathcal{O}_L & \subseteq & L \\
 & & & & | \\
\cdot\ \mathcal{O}^{\mathcal{I}_\mathcal{O}} & \subseteq & \mathcal{O}_L^{\mathcal{I}_\mathcal{O}} & \subseteq & L^{\mathcal{I}_\mathcal{O}} \\
\mathcal{O}^{\mathcal{D}_\mathcal{O}} & & \mathcal{O}_L^{\mathcal{D}_\mathcal{O}} & \subseteq & L^{\mathcal{D}_\mathcal{O}} \\
 & & & & | \\
\mathfrak{p} & \subseteq & \mathcal{O}_K & \subseteq & K
\end{array}$$

$\mathrm{Gal}(L/L^{\mathcal{I}_\mathcal{O}}) \simeq \mathcal{I}_\mathcal{O}$ agit transitivement sur les idéaux de $\mathcal{O}_L$ au-dessus de $\mathcal{O}^{\mathcal{I}_\mathcal{O}}$ (y compris $\mathcal{O}$), or $\mathcal{O}$ est fixé par $\mathcal{I}_\mathcal{O}$, donc :

· $\mathcal{O}^{\mathcal{I}_\mathcal{O}}\mathcal{O}_L = \mathcal{O}^*$

· le groupe de décomposition de $\mathcal{O}/\mathcal{O}^{\mathcal{I}_\mathcal{O}}$ est $\mathcal{I}_\mathcal{O}$ tout entier

· le groupe d'inertie aussi

donc $\mathcal{O}^{\mathcal{I}_\mathcal{O}}\mathcal{O}_L = \mathcal{O}^e$, donc $\mathfrak{p}$ est non ramifié dans $L^{\mathcal{I}_\mathcal{O}}/K$, et $\mathcal{O}_L/\mathcal{O} = \mathcal{O}_L^{\mathcal{I}_\mathcal{O}}/\mathcal{O}^{\mathcal{I}_\mathcal{O}}$.

De même, $D_\mathfrak{P}$ $\left(= \mathrm{Gal}(L/L^{D_\mathfrak{P}})\right)$ est le groupe de décomposition de $\mathfrak{P}/\mathfrak{p}^{D_\mathfrak{P}}$, le groupe d'inertie est donc $I_\mathfrak{P}$ et on en déduit $\mathfrak{p}^{D_\mathfrak{P}} \mathcal{O}_L = \mathfrak{P}^e$ et $\left[\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_L^{D_\mathfrak{P}}/\mathfrak{p}^{D_\mathfrak{P}}\right) = f$,

donc $\mathcal{O}_L^{D_\mathfrak{P}}/\mathfrak{p}^{D_\mathfrak{P}} = \mathcal{O}_K/\mathfrak{p}$.

Réciproquement, si $K \subseteq M \subseteq L$, alors :

- si $\mathfrak{P} \cap \mathcal{O}_M$ a pour exposant 1 dans $\mathfrak{p}\mathcal{O}_M$, alors $\mathfrak{P}$ a pour exposant e dans $(\mathfrak{P} \cap \mathcal{O}_M)\mathcal{O}_L$, le groupe de ramification de $\mathfrak{P}$ pour l'extension L/M est $I_\mathfrak{P}$ tout entier, donc $I_\mathfrak{P}$ est un sous-groupe de $\mathrm{Gal}(L/M)$, et $M \subseteq L^{I_\mathfrak{P}}$.
- si de plus $\mathcal{O}_M/\mathfrak{P} \cap \mathcal{O}_M = \mathcal{O}_K/\mathfrak{p}$, on obtient $M \subseteq L^{D_\mathfrak{P}}$.

$L^{I_\mathfrak{P}}$ est la plus grande sous-extension de L non ramifiée en $\mathfrak{P}$.

$L^{D_\mathfrak{P}}$ est d'indice résiduel 1.

Th : L/K $\qquad L = K(x)$ (élt primitif)

On peut supposer $x \in \mathcal{O}_L$ (déjà vu).

$P(X) \in \mathcal{O}_K[X]$ poly mini de x sur K.

$\bar{P}(X) \in (\mathcal{O}_K/\mathfrak{p})[X]$ réduction de $P(X)$ mod $\mathfrak{p}$.

Si $\bar{P}$ est séparable, alors $\mathfrak{p}$ ne se ramifie pas dans L/K.

□ Soit M = clôture galoisienne de L/K (= corps de décomp de P).

$M = K[x_0, x_1, \dots, x_{d-1}]$ $\qquad x_i \in \mathcal{O}_M$ (racines de P).

$\mathfrak{P}$ idéal premier de $\mathcal{O}_M$ au-dessus de $\mathfrak{p}$

(i.e. $\mathfrak{P} \mid \mathfrak{p}\mathcal{O}_M$)

$$\mathcal{G}_{\mathfrak{P}} \longrightarrow \mathrm{Gal}(\mathcal{O}_M/\mathfrak{P} \;/\; \mathcal{O}_K/\mathfrak{p})$$

Si $\sigma \in \mathcal{G}_{\mathfrak{P}}$, alors $\bar{\sigma} = \mathrm{id}_{\mathcal{O}_M/\mathfrak{P}}$

donc $\bar{\sigma}(\bar{x}_i) = \bar{x}_i$

Or les $\bar{x}_i$ sont les racines de $\bar{P}$, qui est séparable, donc les $\bar{x}_i$ sont distincts

$\{x_i\} \xrightarrow{\text{mod } \mathfrak{P}} \{\bar{x}_i\}$ est une bijection

et σ permute les x_i (racines de P), donc : $\forall i \;\; \sigma(x_i) = x_i$,

or $M = K[x_0, \dots, x_{d-1}]$ donc $\sigma = \mathrm{id}_M$.

Donc $\mathcal{G}_{\mathfrak{P}} = \{\mathrm{id}_M\}$ donc $\mathfrak{p}$ ne se ramifie pas dans M/K, donc dans L/K non plus. ☒

(4) Application : irréductibilité des pol. cyclotomiques.

$L := \mathbb{Q}(\mu_n)$ $\qquad \mu_n = \langle \zeta \rangle$

$|$

$\mathbb{Q}$ $\qquad \Phi_n(X) = \prod_{i \in (\mathbb{Z}/n\mathbb{Z})^\times} (X - \zeta^i)$

$\chi : Gal(L/\mathbb{Q}) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$

(caractère cyclotomique)

Si p premier, $p \nmid n$, alors $pgcd(X^n - 1, nX^{n-1}) = 1$ sur $\mathbb{F}_p$,

donc $\overline{\Phi_n}(X) \in \mathbb{F}_p[X]$ est séparable,

donc p ne se ramifie pas dans $L/\mathbb{Q}$.

De plus $Gal(L/\mathbb{Q})$ est abélien, donc on a un Frobenius

$\left(\frac{L/\mathbb{Q}}{p}\right) \in Gal(L/\mathbb{Q})$.

On a $\left(\frac{L/\mathbb{Q}}{p}\right)(\zeta) = \zeta^{\chi\left(\left(\frac{L/\mathbb{Q}}{p}\right)\right)}$ dans L

$\left(\frac{L/\mathbb{Q}}{p}\right)(\bar{\zeta}) = \bar{\zeta}^p$ dans $Q/\mathfrak{P}$

($\mathfrak{P}$ au-dessus de p)

$\overline{\Phi_n}$ est séparable donc $\mu_n(L) \xrightarrow{\text{mod } \mathfrak{P}} \mu_n(Q/\mathfrak{P})$ est une bijection.

donc $\chi\left(\left(\frac{L/\mathbb{Q}}{p}\right)\right) = p$.

L'image de χ contient le sous-groupe engendré par tous les p premiers, $p \nmid n$, i.e. c'est $(\mathbb{Z}/n\mathbb{Z})^\times$ tout entier.

Donc χ est un isomorphisme, donc Φ_n est irréductible.

(c) Application : réciprocité quadratique

p, q premiers impairs distincts.

idée : voir $\mathbb{Q}(\sqrt{\pm q})$ comme une sous-extension d'une ext. cyclotomique.

$L := \mathbb{Q}(\mu_q)$ $\qquad Gal(L/\mathbb{Q}) \overset{\chi}{\simeq} (\mathbb{Z}/q\mathbb{Z})^\times \simeq \mathbb{Z}/(q-1)\mathbb{Z}$

$\mathbb{Z}/(q-1)\mathbb{Z}$ a un unique sous-groupe d'indice 2

$\longrightarrow$ L a un unique sous-corps de degré 2 sur $\mathbb{Q}$.

(corresp. de Galois)

$$\begin{array}{c} L \\ | \\ \mathbb{Q}(\sqrt{a}) \\ | \\ \mathbb{Q} \end{array} \quad \leftarrow \text{ a sans facteur carré}$$

Le seul nombre premier qui se ramifie dans $L/\mathbb{Q}$ est q.

Les nombres premiers qui se ramifient dans $\mathbb{Q}(\sqrt{a})/\mathbb{Q}$ sont

- les diviseurs premiers de a
- 2 si $a \not\equiv 1 \pmod 4$

$$\left(\mathcal{O}_{\mathbb{Q}(\sqrt{a})} = \begin{cases} \mathbb{Z}[\sqrt{a}] & \text{si } a \equiv 2 \text{ ou } 3 \pmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{a}}{2}\right] & \text{si } a \equiv 1 \pmod 4 \end{cases} \right)$$

Donc : $a \equiv 1 \pmod q$

$a \in \{\pm q\}$

donc $d = \begin{cases} q & \text{si } q \equiv 1 \pmod 4 \\ -q & \text{si } q \equiv -1 \pmod 4 \end{cases}$

Considérons $\left(\frac{L/\mathbb{Q}}{\mathfrak{p}}\right)\Big|_{\mathbb{Q}(\sqrt{a})} = \left(\frac{\mathbb{Q}(\sqrt{a})/\mathbb{Q}}{\mathfrak{p}}\right)$ c'est l'image de $\left(\frac{L/\mathbb{Q}}{\mathfrak{p}}\right)$

par $\mathrm{Gal}(L/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}(\sqrt{a})/\mathbb{Q})$

$\chi \mid 2$ $\qquad\qquad$ $\mid 2$

$(\mathbb{Z}/q\mathbb{Z})^\times \qquad\qquad \mathbb{Z}/2\mathbb{Z}$

i.e. $\left(\frac{\mathbb{Q}(\sqrt{a})/\mathbb{Q}}{\mathfrak{p}}\right) = \mathrm{id} \iff \chi\left(\left(\frac{L/\mathbb{Q}}{\mathfrak{p}}\right)\right)$ est un carré dans $\mathbb{F}_q^\times$

$\left(\frac{L/\mathbb{Q}}{\mathfrak{p}}\right) = \mathfrak{p}$

$\iff \left(\frac{\mathfrak{p}}{q}\right) = 1$

(i.e. $\left(\frac{\mathbb{Q}(\sqrt{a})/\mathbb{Q}}{\mathfrak{p}}\right)$ et $\left(\frac{\mathfrak{p}}{q}\right)$ se correspondent

par $\mathrm{Gal}(\mathbb{Q}(\sqrt{a})/\mathbb{Q}) \simeq \{\pm 1\}$).

D'autre part, $\mathcal{O}_{\mathbb{Q}(\sqrt{a})} = \mathbb{Z}\left[\frac{1+\sqrt{a}}{2}\right] \simeq \mathbb{Z}[X] \Big/ \left(X^2 - X + \frac{1-a}{4}\right)$

$\mathcal{O}_{\mathbb{Q}(\sqrt{a})} \Big/ \mathfrak{p}\mathcal{O}_{\mathbb{Q}(\sqrt{a})} \simeq \mathbb{F}_p[X] \Big/ \left(X^2 - X + \frac{1-a}{4}\right)$

$\uparrow$ discriminant $= a$

$\simeq \begin{cases} \mathbb{F}_p^2 & \text{si } \left(\frac{a}{\mathfrak{p}}\right) = 1 \\ \mathbb{F}_{p^2} & \text{si } \left(\frac{a}{\mathfrak{p}}\right) = -1 \end{cases}$

donc $\left(\frac{\mathbb{Q}(\sqrt{a})}{\mathfrak{p}}\right) = \mathrm{id} \iff \left(\frac{a}{\mathfrak{p}}\right) = 1$.

On a donc $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = \begin{cases} \left(\frac{q}{p}\right) \text{ si } q \equiv 1 \pmod 4 \\ \left(\frac{-1}{p}\right)\left(\frac{q}{p}\right) \text{ si } q \equiv -1 \pmod 4 \end{cases}$

$$= \begin{cases} \left(\frac{q}{p}\right) \text{ si } p \equiv 1 \pmod 4 \text{ ou } q \equiv 1 \pmod 4 \\ -\left(\frac{q}{p}\right) \text{ si } p \equiv q \equiv -1 \pmod 4 \end{cases}.$$

On retrouve donc la loi de réciprocité quadratique, en calculant chacun des membres de l'égalité

$$\left(\frac{L/\mathbb{Q}}{p}\right)\Big|_{\mathbb{Q}(\sqrt{a})} = \left(\frac{\mathbb{Q}(\sqrt{a})/\mathbb{Q}}{p}\right).$$

calculable car $L/\mathbb{Q}$ cyclotomique

calculable car $\mathbb{Q}(\sqrt{a})/\mathbb{Q}$ quadratique.

(d) Symbole d'Artin et réciprocité.

L/K est abélienne de corps de nombre — $\mathfrak{p}$ idéal maximal de $\mathcal{O}_K$ non ramifié dans L/K

$\longrightarrow$ Frobenius $\left(\frac{L/K}{\mathfrak{p}}\right) \in \mathrm{Gal}(L/K)$

Si $\mathfrak{a}$ idéal de $\mathcal{O}_K$ non ramifié dans L/K

$$\mathfrak{a} = \prod \mathfrak{p}_i^{v_i}$$

$$\left(\frac{L/K}{\mathfrak{a}}\right) := \prod_i \left(\frac{L/K}{\mathfrak{p}_i}\right)^{v_i}$$

$\mathfrak{a} \longmapsto \left(\frac{L/K}{\mathfrak{a}}\right)$ = symbole d'Artin.

ex : $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{d})$ $\quad d$ sans facteur carré

$\mathfrak{p}$ premier $\neq 2$, $\mathfrak{p} \nmid d$

alors $\mathcal{O}_K/\mathfrak{p} = \mathbb{F}_p$ $\qquad \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \simeq \begin{cases} \mathbb{F}_p^2 & \text{si } \left(\frac{d}{p}\right) = 1 \\ \mathbb{F}_{p^2} & \text{si } \left(\frac{d}{p}\right) = -1 \end{cases}$

$\mathrm{Gal}(L/K) \simeq \{\pm 1\}$

$$\left(\frac{L/K}{\mathfrak{p}}\right) = \begin{cases} 1 & \text{si } \left(\frac{d}{p}\right) = 1 \\ -1 & \text{si } \left(\frac{d}{p}\right) = -1 \end{cases} = \left(\frac{d}{p}\right)$$

Si a premier à $2d$:

$$\left(\frac{L/K}{a}\right) = \left(\frac{d}{a}\right) \qquad \text{(symbole de Jacobi)}.$$

Th (réciprocité d'Artin) :

$\exists \varepsilon > 0 \quad \forall a \in K^\times \quad (\forall v \in S \quad |a-1|_v < \varepsilon) \Rightarrow \left(\frac{L/K}{(a)^S}\right) = id$

où $S = \{$ idéaux premiers de $\mathcal{O}_K$ ramifiés dans L/K $\} \cup \{$ places à l'infini $\}$ (en plus grand).

$|a|_v = p^{-v_p(a)}$ si $v = v_p$ p premier au-dessus de p.

$|\cdot|_\infty$ = valeur absolue / module,

$(a)^S$ = idéal (a) privé des facteurs contenus dans S

On peut en déduire la réciprocité quadratique, cf. Cassels & Fröhlich, chap VII & ex 1.

(Exemple : $L = \mathbb{Q}(\sqrt{n})$, n sans facteur carré,
$S = \{$ diviseurs premiers de $2n\} \cup \{$ places à l'infini $\}$
Si $a \equiv 1 \pmod{8n}$, $a = \prod p_i^{v_i}$ $(v_i \in \mathbb{Z})$,
alors $\left(\frac{n}{a}\right) = 1$ par réciprocité quadratique.)

② Groupes de ramification supérieurs.

Le groupe d'inertie de $\mathcal{P}$ est

$$\mathcal{I}_{\mathcal{P}} := \left\{ \sigma \in \mathrm{Gal}(L/K) \;/\; \forall x \in \mathcal{O}_L \quad \sigma(x) \equiv x \pmod{\mathcal{P}} \right\}$$

cf. Serre, Corps locaux

On définit les groupes de ramification

$$G_i := \left\{ \sigma \in \mathrm{Gal}(L/K) \;/\; \forall x \in \mathcal{O}_L \quad \sigma(x) \equiv x \pmod{\mathcal{P}^{i+1}} \right\}$$

$$G_{-1} = \mathrm{Gal}(L/K)$$
$$G_0 = \mathcal{I}_{\mathcal{P}}$$
$$G_i = \{\mathrm{id}\} \quad \text{si } i \gg 0 .$$

G_i est un sous-groupe distingué de $G_{-1} = \mathrm{Gal}(L/K)$, donc de G_{i-1}.

Rem : Si $\mathfrak{p}$ n'est pas ramifié, tous ces groupes sont triviaux.

On note $\hat{L}$ le complété $\mathcal{P}$-adique de L.
$\hat{K}$ ——— $\mathfrak{p}$-adique de K.

On obtient $\mathcal{D}_{\mathcal{P}} \longrightarrow \mathrm{Gal}(\hat{L}/\hat{K})$ par prolongement par continuité,
et $\left\{ \begin{array}{ccc} \mathrm{Gal}(\hat{L}/\hat{K}) & \longrightarrow & \mathcal{D}_{\mathcal{P}} \\ \sigma & \longmapsto & \sigma|_L \end{array} \right.$ en est un inverse,

donc $\mathcal{D}_{\mathcal{P}} \simeq \mathrm{Gal}(\hat{L}/\hat{K})$.

Soit $\pi \in \mathcal{O} \setminus \mathcal{O}^2$.

Notons $\begin{cases} U_0 := \mathcal{O}_{\hat{L}}^\times \\ U_i := 1 + \pi^i \mathcal{O}_{\hat{L}} \end{cases}$. $\quad U_0 \supseteq U_1 \supseteq U_2 \supseteq \dots$

Prop : $\forall \sigma \in I_\mathcal{P}$, $i \geq 0$, alors :

$$\sigma \in G_i \iff \frac{\sigma(\pi)}{\pi} \in U_i$$

(dans $\hat{L}$)

□ • C'est immédiat pour $i = 0$, on suppose $i \geq 1$

• On peut remplacer K par $L^{I_\mathcal{P}}$, de sorte que $f = 1$, $[L:K] = e$.

$\Rightarrow$: $\sigma \in G_i$ donc $\sigma(\pi) \equiv \pi \pmod{\mathcal{P}^{i+1}}$,

donc (dans $\hat{L}$) $\frac{\sigma(\pi)}{\pi} - 1 \in \pi^i \mathcal{O}_{\hat{L}}$

$\Leftarrow$: $\frac{\sigma(\pi)}{\pi} \in 1 + \pi^i \mathcal{O}_{\hat{L}}$, donc $\sigma(\pi) \equiv \pi \pmod{\mathcal{P}^{i+1}}$

(car $\mathcal{O}_{\hat{L}} / \pi^{i+1} \simeq \mathcal{O}_L / \mathcal{P}^{i+1}$)

Lemme : $U_{\hat{K}}(\pi) = \mathcal{O}_{\hat{L}}$ ← cf. Serre, Corps locaux, chap I, § 6, prop 18

On a $\forall x \in \mathcal{O}_{\hat{K}}(\pi)$ $\sigma(x) \equiv x \pmod{\mathcal{P}^{i+1}}$,

or $\mathcal{O}_L \subseteq \mathcal{O}_{\hat{L}} = \mathcal{O}_{\hat{K}}(\pi)$ donc $\sigma \in G_i$. ☒

fin cours n°15

Rem : • $U_0 / U_1 \simeq \left(\mathcal{O}_{\hat{L}} / \pi \mathcal{O}_{\hat{L}}\right)^\times \simeq (\mathcal{O}_L / \mathcal{P})^\times$ (induit par la réduction mod $\mathcal{P}$)

NB : $\mathcal{O}_L / \pi \mathcal{O}_{\hat{L}} \simeq \mathcal{O}_L / \mathcal{P}$

• $U_i / U_{i+1} \simeq \pi^i \mathcal{O}_{\hat{L}} / \pi^{i+1} \mathcal{O}_{\hat{L}}$ (par $1 + x \leftarrow\!\shortmid x$)

$\simeq \mathcal{O}_{\hat{L}} / \pi \mathcal{O}_{\hat{L}} \simeq \mathcal{O}_L / \mathcal{P}$ ← groupe additif.

• G_i agit trivialement sur U_i / U_{i+1}

Corollaire : On a des morphismes de groupes injectifs

$$\begin{cases} G_i/G_{i+1} \hookrightarrow U_i/U_{i+1} & (U_i \geq 0) \\ \sigma \longmapsto \dfrac{\sigma(\pi)}{\pi} \end{cases}$$

cf Serre, Corps locaux, chap IV, §2, prop. 7.

□ $G_i \longrightarrow U_i \twoheadrightarrow U_i/U_{i+1}$

$\sigma \longmapsto \dfrac{\sigma(\pi)}{\pi}$

$\forall\, \sigma, \sigma' \in G_i$, on a

$$\frac{(\sigma\sigma')(\pi)}{\pi} = \frac{\sigma(\sigma'(\pi))}{\pi}$$

$$= \frac{\sigma(\pi)}{\pi}\,\sigma\left(\frac{\sigma'(\pi)}{\pi}\right)$$

$\frac{\sigma'(\pi)}{\pi} \in U_i$

$$\equiv \frac{\sigma(\pi)}{\pi}\,\frac{\sigma'(\pi)}{\pi} \mod U_{i+1}$$

$$\ker\left(G_i \longrightarrow U_i/U_{i+1}\right) = G_{i+1}. \quad \square$$

Rem : Le morphisme $G_i/G_{i+1} \hookrightarrow U_i/U_{i+1}$ ne dépend pas de π. En effet, si $u \in \mathcal{O}_L^\times$, $\sigma \in G_i$, alors $\sigma(u) \equiv u \pmod{\pi^{i+1}}$ donc $\frac{\sigma(u)}{u} \in U_{i+1}$.

Corollaire : Le groupe $\mathcal{D}_\mathfrak{p}$ est résoluble.

□ $\mathcal{D}_\mathfrak{p}/\mathcal{G}_\mathfrak{p} \simeq \mathrm{Gal}\left(\kappa_L/\mathfrak{p} \,/\, \kappa_K/\mathfrak{p}\right)$ cyclique

$\mathcal{G}_\mathfrak{p} = G_0 \qquad G_i/G_{i+1} \hookrightarrow \underbrace{U_i/U_{i+1}}_{\text{abélien}}$

$G_i = 1$ si $i \gg 0$ $\square$

Prop : car $O_K/\mathfrak{p} \nmid e \iff \forall i \geq 1 \quad G_i = 1$

$\square$ $\Longrightarrow$: $|G_0| = e$ donc $\forall i \geq 0$ G_i est d'ordre premier à p

or $G_i/G_{i+1} \hookrightarrow \hat{O}_L / \pi \hat{O}_L$ $\quad (\forall i \geq 1)$

$\uparrow$

$O_K/\mathfrak{p}$ - ev

$\forall i \geq 1$ $G_i \neq 0$ dans $O_K/\mathfrak{p}$, on en déduit $G_i/G_{i+1} = 1$

donc $\forall i \geq 1$ $G_i = 1$.

$\Longleftarrow$: $G_1 = 1$, $G_0/G_1 \hookrightarrow \left(\hat{O}_L/\pi\hat{O}_L\right)^\times$

donc $e = |G_0| \mid \left|\hat{O}_L/\pi\hat{O}_L\right|$

$= (\text{puissance de car } O_K/\mathfrak{p}) - 1$ ⚠

Déf : Si car $O_K/\mathfrak{p} \nmid e$, on dit que l'extension est modérément ramifiée

(et $e > 1$)

Si car $O_K/\mathfrak{p} \mid e$, on dit _____ sauvagement ramifiée.

On a $G_0/G_1 \hookrightarrow U_0/U_1 \simeq (\mathcal{O}_L/\mathfrak{P})^\times$.

Prop : Si $\mathcal{D}_\mathfrak{P}/G_1$ est abélien, alors l'image de G_0/G_1 est contenue dans $(\mathcal{O}_K/\mathfrak{p})^\times$.

D Soit $\sigma \in G_0$, alors $\frac{\sigma(\pi)}{\pi} \in U_0/U_1 \underset{\text{mod } \mathfrak{P}}{\simeq} (\mathcal{O}_L/\mathfrak{P})^\times$.

Soit $\tau \in \mathcal{D}_\mathfrak{P}$, alors $\tau(\pi)$ est aussi une uniformisante de $\mathcal{O}_L$,

donc $\frac{\sigma(\pi)}{\pi} = \frac{\sigma(\tau(\pi))}{\tau(\pi)}$ dans U_0/U_1,

or $\mathcal{D}_\mathfrak{P}/G_1$ est abélien donc $\tau\sigma\tau^{-1} = \sigma$ dans G_0/G_1,

donc $\frac{\sigma(\pi)}{\pi} = \frac{(\tau\sigma\tau^{-1})(\pi)}{\pi} = \frac{(\tau\sigma\tau^{-1})(\tau(\pi))}{\tau(\pi)}$ dans U_0/U_1

donc $\frac{\sigma(\pi)}{\pi} = \frac{\tau(\sigma(\pi))}{\tau(\pi)} = \tau\left(\frac{\sigma(\pi)}{\pi}\right)$ dans $\mathcal{O}_L/\mathfrak{P}$.

Or $\mathcal{D}_\mathfrak{P} \twoheadrightarrow \mathrm{Gal}(\mathcal{O}_L/\mathfrak{P} \,/\, \mathcal{O}_K/\mathfrak{p})$,

donc $\frac{\sigma(\pi)}{\pi} \in (\mathcal{O}_L/\mathfrak{P})^{\mathrm{Gal}(\mathcal{O}_L/\mathfrak{P} \,/\, \mathcal{O}_K/\mathfrak{p})} = \mathcal{O}_K/\mathfrak{p}$. ☐

Une preuve du théorème de Kronecker - Weber.

$K/\mathbb{Q}$ extension finie abélienne.

source : Lucas Culler, The Kronecker-Weber theorem

Th (Kronecker - Weber) : Il existe une extension cyclotomique $\mathbb{Q}(\mu_m)/\mathbb{Q}$ telle que $K \hookrightarrow \mathbb{Q}(\mu_m)$.

Marcus, Number Fields (exercices du chap 4)

Rem :
- C'est l'un des premiers résultats de la théorie du corps de classes.
- Pour démontrer la loi de réciprocité quadratique, on a montré que $\mathbb{Q}(\sqrt{\pm q}) \subseteq \mathbb{Q}(\mu_q)$. (pour un bon choix de $\pm$).

Prop : Soit p un nombre premier modérément ramifié dans $K/\mathbb{Q}$. Alors il existe
- $K'/\mathbb{Q}$ est. finie abélienne
- $\mathbb{Q}(\mu_m)/\mathbb{Q}$ est. cyclotomique
- $L \subseteq \mathbb{Q}(\mu_m)$ sous-corps

t.q.
- tout nombre premier non ramifié dans $K/\mathbb{Q}$ est non ramifié dans $K'/\mathbb{Q}$
- p est non ramifié dans $K'/\mathbb{Q}$
- $KL = K'L$.

□ Soit $\mathfrak{P}$ idéal premier de $\mathcal{O}_K$, au-dessus de p.
On note G_i, $i \geq 0$ les groupes de ramification supérieurs.
Comme p est modérément ramifié, on a $G_1 = 1$.
Or $\mathrm{Gal}(K/\mathbb{Q})$ est abélien, donc $D_{\mathfrak{P}}$ $(\subseteq \mathrm{Gal}(K/\mathbb{Q}))$ aussi,
donc $D_{\mathfrak{P}}/G_1$ aussi, donc (prop. ci-dessus)

$$D_{\mathfrak{P}}/G_1 \hookrightarrow (\mathbb{Z}/p\mathbb{Z})^\times$$

$$\| = D_{\mathfrak{P}}$$

donc $e \mid p-1$.

$[\mathbb{Q}(\mu_p) : \mathbb{Q}] = p-1$

Soit L l'unique sous-corps de $\mathbb{Q}(\mu_p)$ tel que $[L:\mathbb{Q}] = e$.
Le nombre premier p est le seul à se ramifier dans $\mathbb{Q}(\mu_p)/\mathbb{Q}$,
donc dans $L/\mathbb{Q}$ aussi. De plus,

$$\mathbb{Z}[\mathfrak{P}]/(p) \simeq \mathbb{F}_p[X]/(X^{p-1} + \dots + 1)$$

Dans $\mathbb{F}_p[X]$: $X^{p-1} + \dots + 1 = \dfrac{X^p - 1}{X-1}$

$$X^p - 1 = (X-1)^p$$

donc $X^{p-1} + \dots + 1 = (X-1)^{p-1}$

Lemme : $\mathcal{O}_{\mathbb{Q}(\mathfrak{P})} = \mathbb{Z}[\mathfrak{P}]$

$$\mathbb{Z}[\mathfrak{P}]/(p) \simeq \mathbb{F}_p[X]/(X-1)^{p-1}$$

p est totalement ramifié $(e = p-1 = [\mathcal{O}/\mathfrak{P} : \mathbb{Q}])$
$f = 1$

Donc p est totalement ramifié dans $L/\mathbb{Q}$ aussi.

Soit $\mathfrak{P}'$ un idéal de $\mathcal{O}_{KL}$ au-dessus de $\mathfrak{P}$.
Soit $K' = (KL)^{\mathfrak{P}'/p}$.

Par construction, p est non ramifié dans $K'/\mathbb{Q}$.

Si p' est non ramifié dans $K/\mathbb{Q}$, $p' \neq p$, alors
p' est non ramifié dans $\mathbb{Q}(\mu_p)/\mathbb{Q}$ donc dans $L/\mathbb{Q}$,
donc p' ne divise pas $\mathrm{disc}(K/\mathbb{Q})$ et $\mathrm{disc}(L/\mathbb{Q})$,
donc p' ne divise pas $\mathrm{disc}(KL/\mathbb{Q})$
donc p' est non ramifié dans $KL/\mathbb{Q}$ donc dans $K'/\mathbb{Q}$.

Il reste à montrer $KL = K'L$, $K'/\mathbb{Q}$ abélienne

$$\mathrm{Gal}(K^L/\mathbb{Q}) \xhookrightarrow[\text{restriction}]{} \underbrace{\mathrm{Gal}(K/\mathbb{Q})}_{\text{abélien}} \times \underbrace{\mathrm{Gal}(L/\mathbb{Q})}_{\simeq \mathbb{Z}/e\mathbb{Z}} \qquad \left(\to KL/\mathbb{Q} \text{ abélienne}\right)$$

(quotient d'ordre e de $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$, $\simeq (\mathbb{Z}/p\mathbb{Z})^\times$)

$\cup$

induit $\quad \mathcal{G}_{\mathfrak{P}'/p} \hookrightarrow \mathcal{G}_{\mathfrak{P}/p} \times \mathbb{Z}/e\mathbb{Z}$

$\uparrow$ ordre $= e \mid p-1$

ordre premier à p

donc $\mathfrak{P}'$ est modérément ramifié,

$KL/\mathbb{Q}$ abélienne (donc $K'/\mathbb{Q}$ abélienne)

donc (comme pour $K/\mathbb{Q}$) $\mathcal{G}_{\mathfrak{P}'/p} \hookrightarrow \mathbb{F}_p^\times$,

donc $\mathcal{G}_{\mathfrak{P}'/p}$ cyclique, et s'injecte dans un groupe d'exposant e, ($\mathcal{G}_{\mathfrak{P}/p} \times \mathbb{Z}/e\mathbb{Z}$)

donc $\mathcal{G}_{\mathfrak{P}'/p}$ cyclique, d'ordre divisant e.

Lemme

$$\begin{array}{ccc} KL & & \mathfrak{P}' \\ | & & \\ K & & \mathfrak{P} \\ | & & \\ \mathbb{Q} & & p \end{array}$$

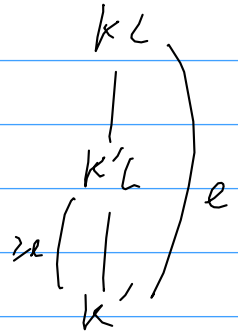
on a $\quad e = e_{\mathfrak{P}/p} \mid e_{\mathfrak{P}'/p}$

i.e. $\left|\mathcal{G}_{\mathfrak{P}'/p}\right|$ est multiple de e

Donc $\mathcal{G}_{\mathfrak{P}'/p} \simeq \mathbb{Z}/e\mathbb{Z}$

Comme $K' = (KL)^{\mathcal{G}(\mathcal{O}/\mathfrak{p})}$, on a $[KL : K'] = e$.

Comme $\mathfrak{p}$ est totalement ramifié dans $L/\mathbb{Q}$, d'indice e,
on obtient que $\mathfrak{p}$ est ramifié, d'indice multiple de e, dans $K'L/\mathbb{Q}$,
or $\mathfrak{p}$ est non ramifié dans $K'/\mathbb{Q}$,
donc $\mathfrak{p}$ est ramifié, d'indice multiple de e, dans $K'L/K'$,
donc $[K'L : K'] \geq e$, or $K' \subseteq KL$ donc $K'L \subseteq KL$, donc :



donc $KL = K'L$.

∎

Notons que si K' est contenu dans une ext. cyclotomique de $\mathbb{Q}$,
alors $KL = K'L$ aussi, donc K aussi.

Si $K/\mathbb{Q}$ est abélienne, on a $\mathrm{Gal}(K/\mathbb{Q}) \simeq \prod_i \mathbb{Z}/p_i^{m_i}\mathbb{Z}$,
donc on peut trouver des sous-extensions $K_i/\mathbb{Q}$
avec $\mathrm{Gal}(K_i/\mathbb{Q}) \simeq \mathbb{Z}/p_i^{m_i}\mathbb{Z}$ (: quotient de $\prod \mathbb{Z}/p_i^{m_i}\mathbb{Z}$)

De plus, K est engendré par les K_i (car $\mathrm{Gal}(K/\mathbb{Q}) \hookrightarrow \prod_i \mathrm{Gal}(K_i/\mathbb{Q})$).
Si chaque K_i est contenu dans une ext. cyclotomique, alors K aussi.
Il suffit donc de démontrer le th de K-W pour chaque K_i.
Si $\mathfrak{p}$ premier ramifié dans K_i/K, on a $e \mid p_i^{m_i}$, donc seul p_i
peut être sauvagement ramifié.
Comme $\mathfrak{p}$ ramifié $\iff \mathfrak{p} \mid \underbrace{\mathrm{disc}(K_i/K)}_{\text{entier} \neq 0}$, il y a un nbre
fini de premiers ramifiés.

On la prop précédente, on se ramène à montrer :

Prop : Si $K/\mathbb{Q}$ est une extension abélienne, de degré p^m,
non ramifiée sauf (éventuellement) en p,
alors K est contenu dans une ext. cyclotomique de $\mathbb{Q}$.

Prop : p premier $\neq 2$
ζ = racine primitive p-ième de 1, dans $\bar{\mathbb{Q}}$
Alors $\mathcal{O}_{\mathbb{Q}(\zeta)} = \mathbb{Z}[\zeta]$.

□ On a immédiatement $\zeta \in \mathcal{O}_{\mathbb{Q}(\zeta)}$ donc $\mathbb{Z}[\zeta] \subseteq \mathcal{O}_{\mathbb{Q}(\zeta)}$.

Soit $x = \sum_{i=0}^{p-2} \lambda_i \zeta^i \in \mathcal{O}_{\mathbb{Q}(\zeta)}$. $\lambda_i \in \mathbb{Q}$

Le poly mini de ζ est $X^{p-1} + X^{p-2} + \dots + 1$,
et c'est aussi le poly mini de ζ^i, $1 \leq i \leq p-2$,
donc $\mathrm{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\zeta^i) = -1$.

$$\mathrm{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1) = [\mathbb{Q}(\zeta) : \mathbb{Q}] = p-1.$$

Donc $\mathrm{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(x(1-\zeta)) = \sum_{i=0}^{p-2} \lambda_i \underbrace{\mathrm{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\zeta^i - \zeta^{i+1})}$

$$= \begin{cases} 0 \text{ si } 0 \leq i < p-2 \\ p \text{ si } i = p-2 \end{cases}$$

$$= p\lambda_{p-2}.$$

Si $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, on a
$\sigma(x(1-\zeta)) = \sigma(x)(1-\zeta^{\chi(\sigma)})$
$\in$ multiple de $1-\zeta$,
donc $\mathrm{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\underbrace{x(1-\zeta)}_{\in \mathcal{O}_{\mathbb{Q}(\zeta)}}) \in \underbrace{\mathbb{Q} \cap \mathcal{O}_{\mathbb{Q}(\zeta)}}_{=\mathbb{Z}} \cap (1-\zeta)\mathcal{O}_{\mathbb{Q}(\zeta)}$.

donc (cf. lemme suivant) $p\lambda_{p-2} \in p\mathbb{Z}$,
donc $\lambda_{p-2} \in \mathbb{Z}$.
En appliquant ceci à ζx, $\zeta^2 x$, ..., on en déduit $\forall i$ $\lambda_i \in \mathbb{Z}$,
i.e. $x \in \mathbb{Z}[\zeta]$.

∎

Lemme : $\mathbb{Z} \cap (1-\zeta)\mathcal{O}_{\mathbb{Q}(\zeta)} = p\mathbb{Z}$

□ $\prod_{i=1}^{p-1}(X-\zeta^i) = X^{p-1}+\dots+1$

donc $\prod_{i=1}^{p-1}(1-\zeta^i) = p$

donc $p\mathbb{Z} \subseteq (1-\zeta)\mathcal{O}_{\mathbb{Q}(\zeta)}$;

donc $\mathbb{Z} \cap (1-\zeta)\mathcal{O}_{\mathbb{Q}(\zeta)}$ est un idéal de $\mathbb{Z}$ contenant $p\mathbb{Z}$,
donc c'est $p\mathbb{Z}$ ou $\mathbb{Z}$.
Si $\mathbb{Z} \subseteq (1-\zeta)\mathcal{O}_{\mathbb{Q}(\zeta)}$, alors $1-\zeta \in \mathcal{O}_{\mathbb{Q}(\zeta)}^\times$
donc $\forall i \in \{1,\dots,p-1\}$ $1-\zeta^i \in \mathcal{O}_{\mathbb{Q}(\zeta)}^\times$
(par action de $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$),
donc $p = \prod_{i=1}^{p-1}(1-\zeta^i) \in \mathcal{O}_{\mathbb{Q}(\zeta)}^\times$,

donc $\frac{1}{p} \in \mathbb{Q} \cap \mathcal{O}_{\mathbb{Q}(\zeta)} = \mathbb{Z}$: absurde.

Donc $\mathbb{Z} \cap (1-\zeta)\mathcal{O}_{\mathbb{Q}(\zeta)} = p\mathbb{Z}$. □

On considère donc le cas suivant :

$K/\mathbb{Q}$ abélienne de degré p^m (p premier, $m \geq 1$)

non ramifiée hors de p.

Si $p = 2$

Lemme : Les seules extensions quadratiques de $\mathbb{Q}$ non ramifiées hors de 2 sont $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}(i\sqrt{2})$.

○ $\operatorname{disc}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) = \begin{cases} d \text{ si } d \equiv 1 \pmod 4 \\ 4d \text{ sinon} \end{cases}$

(d entier sans facteur carré)

donc $d \in \{\pm 1, \pm 2\}$, et $d \neq 1$ car sinon l'extension est de degré 1 ↯

Soit $\zeta := \underset{\text{primitive}}{\text{racine}} \sqrt[2^{m+2}]{}$ - ième de 1

$$\underset{\text{conjugaison complexe}}{\operatorname{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})} \simeq \left(\mathbb{Z}/2^{m+2}\mathbb{Z}\right)^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^m\mathbb{Z}$$

$$-1 \longleftrightarrow (1,0)$$

$L := \mathbb{Q}(\zeta) \cap \mathbb{R} = \mathbb{Q}(\zeta)^{\langle \text{conj. cplxe} \rangle}$ $\quad \operatorname{Gal}(L/\mathbb{Q}) \simeq \mathbb{Z}/2^m\mathbb{Z} \quad [L:\mathbb{Q}] = 2^m$

$\operatorname{Gal}(KL/\mathbb{Q}) \xrightarrow{\text{restriction}} \operatorname{Gal}(L/\mathbb{Q}) \simeq \mathbb{Z}/2^m\mathbb{Z}$

Soit : $\tau \longmapsto 1$

$F := (KL)^{\langle \tau \rangle}$, alors $F \cap L = L^{\langle \tau \rangle} = \mathbb{Q}$.

$$\underset{\tau}{\operatorname{Gal}(KL/\mathbb{Q})} \xrightarrow{\text{restrictions}} \underbrace{\operatorname{Gal}(K/\mathbb{Q})}_{\text{abélien d'ordre } 2^m} \times \underset{\mathbb{Z}/2^m\mathbb{Z}}{\operatorname{Gal}(L/\mathbb{Q})}$$

donc l'ordre de τ divise 2^m

or $\tau|_L$ est d'ordre 2^m (par déf de τ), donc τ est d'ordre 2^m

donc $[KL:F] = 2^m$ (par corresp de Galois, et déf de F).

ajout :

Si $F = \mathbb{Q}$, comme $[KL : F] = 2^m$,
on aurait $[KL : \mathbb{Q}] = 2^m$,
or $[L : \mathbb{Q}] = 2^m$ et $L \subseteq KL$, donc $KL = L$,
donc $K \subseteq L \subseteq \mathbb{Q}(\zeta)$, ce qui démontre Kronecker-Weber pour K.

On suppose désormais $F \neq \mathbb{Q}$

$\mathrm{Gal}(L/\mathbb{Q}) \simeq \mathbb{Z}/2^m\mathbb{Z}$ a un unique sous-groupe d'indice 2
donc $L/\mathbb{Q}$ contient une unique extension quadratique de $\mathbb{Q}$,
et $\mathbb{Q}(\zeta)/\mathbb{Q}$, donc $L/\mathbb{Q}$ aussi, est non ramifiée hors de 2,
donc cette extension quadratique aussi :
donc (cf. lemme) c'est $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$ ou $\mathbb{Q}(i\sqrt{2})$.
Comme $L \subseteq \mathbb{R}$, c'est $\mathbb{Q}(\sqrt{2})$.

$\mathrm{Gal}(KL/\mathbb{Q}) \hookrightarrow \underbrace{\mathrm{Gal}(F/\mathbb{Q})}_{\text{abélien}} \times \underbrace{\mathrm{Gal}(L/\mathbb{Q})}_{\text{cyclique}}$ donc $KL/\mathbb{Q}$ est abélienne,
donc $F/\mathbb{Q}$ aussi.

Si $F \cap \mathbb{R} \neq \mathbb{Q}$, alors

KL — $KL/\mathbb{Q}$ abélienne, non ramifiée hors de 2, $[KL:\mathbb{Q}]$ est une puissance de 2,
F — donc $(F\cap\mathbb{R})/\mathbb{Q}$ abélienne, non ramifiée hors de 2, $[F\cap\mathbb{R}:\mathbb{Q}]$ est une puissance de 2,
$F \cap \mathbb{R}$
$\mathbb{Q}$

donc $F\cap\mathbb{R}$ contient une extension quadratique de $\mathbb{Q}$,
non ramifiée hors de 2, contenue dans $\mathbb{R}$, donc c'est $\mathbb{Q}(\sqrt{2})$,
mais dans ce cas on aurait $\mathbb{Q}(\sqrt{2}) \subseteq F \cap L = \mathbb{Q}$: contradiction.
Donc $F \cap \mathbb{R} = \mathbb{Q}$, or $F \cap \mathbb{R} = F^{\langle \text{conj. complexe} \rangle}$
donc $[F:\mathbb{Q}] \leq 2$, or $F/\mathbb{Q}$ est non ramifiée hors de 2, et $F \neq \mathbb{Q}$,
donc F est $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$ ou $\mathbb{Q}(i\sqrt{2})$,
or $F \cap \mathbb{R} = \mathbb{R}$, donc F est $\mathbb{Q}(i)$ ou $\mathbb{Q}(i\sqrt{2})$

$\mathbb{Q}(i) \subseteq \mathbb{Q}(\zeta)$ car $\zeta^{2^m} \in \{\pm i\}$

$\mathbb{Q}(i\sqrt{2}) \subseteq \mathbb{Q}(\zeta)$ car $\zeta^{2^{m-1}} \in \left\{\frac{\pm 1 \pm i}{\sqrt{2}}\right\}$ donc $\zeta^{2^{m-1}} - \zeta^{-2^{m-1}} \in \{\pm i\sqrt{2}\}$

et $L \subseteq \mathbb{Q}(\zeta)$, donc $FL \subseteq \mathbb{Q}(\zeta)$.
De plus, $L \subseteq \mathbb{R}$, donc $[FL:L] = 2$,
donc $[FL:\mathbb{Q}] = 2^{m+1} = [\mathbb{Q}(\zeta):\mathbb{Q}]$,
donc $FL = \mathbb{Q}(\zeta)$, or $F \subseteq KL$ donc $FL \subseteq KL$,
donc $\mathbb{Q}(\zeta) \subseteq KL$, or $[KL:F] = 2^m$ donc $[KL:\mathbb{Q}] = 2^{m+1} = [\mathbb{Q}(\zeta):\mathbb{Q}]$
donc $KL = \mathbb{Q}(\zeta)$, donc $K \subseteq \mathbb{Q}(\zeta)$. D'où Kronecker-Weber
dans ce cas.

* Si $p \neq 2$

cf. R. J. Greenberg, An Elementary Proof of the Kronecker-Weber Theorem.

On a $\mathrm{Gal}(\mathbb{Q}(\mu_{p^{m+1}})/\mathbb{Q}) \simeq (\mathbb{Z}/p^{m+1}\mathbb{Z})^\times$

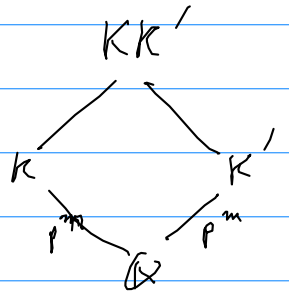
$\simeq \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^m\mathbb{Z}$ $(p \neq 2)$

$\simeq \mathbb{Z}/p^m(p-1)\mathbb{Z}$ (th. chinois)

↑ a un unique sous-groupe d'indice p^m

donc $\mathbb{Q}(\mu_{p^{m+1}})$ a un unique sous-corps K de degré p^m sur $\mathbb{Q}$.

Comme $\mathbb{Q}(\mu_{p^{m+1}})/\mathbb{Q}$ est non ramifiée hors de p, $K'/\mathbb{Q}$ aussi, donc $KK'/\mathbb{Q}$ aussi (en considérant le discriminant, ou la différente)



$\mathrm{Gal}(KK'/\mathbb{Q}) \hookrightarrow \underbrace{\mathrm{Gal}(K/\mathbb{Q})}_{\text{abélien d'ordre } p^m} \times \underbrace{\mathrm{Gal}(K'/\mathbb{Q})}_{\simeq \mathbb{Z}/p^m\mathbb{Z}}$ (par restriction)

donc $KK'/\mathbb{Q}$ est abélienne, de degré $p^{m'}$ $(m \leq m' \leq 2m)$, non ramifiée hors de p, et $\mathrm{Gal}(KK'/\mathbb{Q})$ est d'exposant divisant p^m.

Lemme : Si $K/\mathbb{Q}$ est galoisienne d'ordre p^m, p premier $\neq 2$, non ramifiée hors de p, alors $K/\mathbb{Q}$ est cyclique.

On en déduit que $KK'/\mathbb{Q}$ est cyclique,
or $\mathrm{Gal}(KK'/\mathbb{Q})$ est d'exposant divisant p^m,
donc d'ordre divisant p^m,
donc $KK' = K = K'$ (puisque $KK' \geq K$ et $KK' \geq k'$, $[K:\mathbb{Q}] = [K':\mathbb{Q}] = p^m$)
donc $K = K' \subseteq \mathbb{Q}(\mu_{p^{m+1}})$.
(par construction de K')

Montrons le lemme.

Soit $\mathfrak{P}$ un idéal premier de $\mathcal{O}_K$, au-dessus de p.
Soit $\mathcal{I}$ le groupe d'inertie associé,
alors $K^{\mathcal{I}}/\mathbb{Q}$ est l'extension maximale contenue dans K non ramifiée en p, or elle est non ramifiée hors de p (car $\subseteq K$),
donc $K^{\mathcal{I}}/\mathbb{Q}$ n'est ramifiée en aucun nombre premier
[i.e. son discriminant est $\neq 1$].

Th : (Hermite – Minkowski) : Si $K/\mathbb{Q}$ est de discriminant ± 1, alors $K = \mathbb{Q}$.
(cf. Samuel, chap IV.3, th 1 — cela se déduit du th. de Minkowski sur les réseaux.)

On a donc $K^{\mathcal{I}} = \mathbb{Q}$, i.e. $\mathrm{Gal}(K/\mathbb{Q}) = \mathcal{I}$: p est totalement ramifié ($(p) = \mathfrak{P}^e$, avec $e = [K:\mathbb{Q}] = p^m$).

Notons $G_0 = \mathcal{I}$, $G_1, G_2, \ldots$ les groupes de ramification supérieure. ($G_i = \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) \mid \forall x \in \mathcal{O}_K \ \sigma(x) \equiv x \pmod{\mathfrak{P}^{i+1}}\}$)

On a $G_i/G_{i+1} \hookrightarrow U_i/U_{i+1} \simeq \begin{cases} (\mathcal{O}_L/\mathfrak{P})^\times \simeq \mathbb{F}_p^\times & \text{si } i = 0 \\ \mathcal{O}_L/\mathfrak{P} \simeq \mathbb{F}_p & \text{si } i \geq 1 \end{cases}$

($\mathcal{O}_L/\mathfrak{P} \simeq \mathbb{F}_p$ car p est totalement ramifié : $f = 1$)

Or $|\mathcal{G}| = |\mathrm{Gal}(K/\mathbb{Q})| = p^m$, donc $\mathcal{G}$ est un p-groupe

$G_0/G_1 \hookrightarrow \mathbb{F}_p^\times$ cyclique d'ordre $p-1$
donc $G_0/G_1 = 1$ i.e. $G_1 = \mathcal{G} = \mathrm{Gal}(K/\mathbb{Q})$

$G_i/G_{i+1} \hookrightarrow \mathbb{F}_p$ donc $[G_i : G_{i+1}] \in \{1, p\}$ $\forall i \geq 1$.

Lemme : Si $m = 1$, alors $G_2 = 1$.
(montré plus loin)

Comme $\mathrm{Gal}(K/\mathbb{Q})$ est un p-groupe, il a un sous-groupe H d'indice p. Soit $K' := K^H$, alors $[K' : \mathbb{Q}] = p$, $K'/\mathbb{Q}$ est non ramifiée hors de p, $\mathcal{O} \cap \mathcal{O}_{K'}$ est un idéal premier de $\mathcal{O}_{K'}$ au-dessus de p.
Notons G'_i les groupes de ramification supérieure de $K'/\mathbb{Q}$.
Soit $i_0 \geq 2$ le plus petit entier tel que $G_{i_0} \neq \mathcal{G}$,
alors $[G_{i_0-1} : G_{i_0}] = p$ donc $[G_0 : G_{i_0}] = p$.

- Dans le cas $H = G_{i_0}$, on a $G'_i = \begin{cases} G_i/G_{i_0} & \text{si } i \leq i_0 \\ 1 & \text{si } i \geq i_0 \end{cases}$
(exercice ; cf. Serre, Corps locaux, chap IV § 1, corollaire de la prop 3)
on a $G'_2 = 1$ d'après le lemme, donc $G_2 = G_{i_0}$,
donc $i_0 = 2$.
- Dans le cas général, on a donc $\begin{cases} G_0 = G_1 = \mathcal{G} \\ [\mathcal{G} : G_2] = p \end{cases}$
Si $\sigma \in G_2$, on a $\sigma H \subsetneq G_1$.
Par Serre, Corps locaux, chap IV § 1 prop 3, on en déduit $\bar{\sigma} \in G'_2$,
où $\bar{\sigma}$ est l'image de σ dans $\mathcal{G}/H$ (i.e. $\bar{\sigma} = \sigma|_{K'}$),
donc $\sigma \in H$. Donc $G_2 \subseteq H$, or $[\mathcal{G} : H] = p = [\mathcal{G} : G_2]$,
donc $H = G_2$.

Le p-groupe $\mathrm{Gal}(K/\mathbb{Q})$ a donc un unique sous-groupe d'indice p (forcément distingué).

Prop : Soit G un p-groupe. Tout sous-groupe propre (i.e. $\neq G$) maximal de G est d'indice p.
(exercice, cf. Bertman, An Introduction to the Theory of Groups, chap. 4, th. 4.6)

Corollaire : Soit G est un p-groupe. Si G a un unique sous-groupe d'indice p, alors G est cyclique.

□ Soit H l'unique sous-groupe d'indice p de G.
Soit $x \in G$, $x \notin H$. Si $\langle x \rangle = G$, alors G est cyclique.
Si $\langle x \rangle \neq G$, soit K un sous-groupe propre de G, contenant $\langle x \rangle$, maximal. Alors K est un sous-groupe propre maximal de G, donc K est d'indice p, donc $K = H$, or $x \in K = H$: contradiction. ☒

Le groupe $\mathrm{Gal}(K/\mathbb{Q})$ est donc cyclique.

Il reste à montrer : si $m = 1$, alors $G_2 = 1$.
On a : $K/\mathbb{Q}$ de degré $p \neq 2$, non ramifiée hors de p.
$\mathfrak{P}$ idéal premier de $\mathcal{O}_K$ au-dessus de p.
On a vu que p est totalement ramifié : $p\mathcal{O}_K = \mathfrak{P}^p$.
On complète K pour la topologie $\mathfrak{P}$-adique, en $\hat{K}$.
$\rightarrow \hat{K}/\mathbb{Q}_p$ de degré p, totalement ramifiée
Soit π une uniformisante de $\mathcal{O}_{\hat{K}}$: $\mathfrak{P}\mathcal{O}_{\hat{K}} = (\pi)$
$(p) = (\pi)^p$ dans $\mathcal{O}_{\hat{K}}$.
Les groupes de ramification sont inchangés : $G_0 = G_1 \simeq \mathbb{Z}/p\mathbb{Z}$.
$G_0 = G_1 \supseteq G_2 \supseteq \dots$ $\quad [G_i : G_{i+1}) \in \{1, p\}$
Soit $i_0 \geq 2$ le plus petit entier tel que $G_{i_0} = 1$.

Soit $P(X) \in \mathbb{Z}_p[X]$, unitaire, le poly. min de π sur $\mathbb{Q}_p$.

On a $P(X) = \prod_{\sigma \in \mathcal{G}} (X - \sigma(\pi))$ $\quad (P(X) = X^p + a_{p-1}X^{p-1} + \dots + a_0$, $\pi \mid a_0$ donc $p \mid a_0$)

donc $P'(\pi) = \prod_{\sigma \in \mathcal{G} \setminus \{id\}} (\pi - \sigma(\pi))$

or $v_\pi(\pi - \sigma(\pi)) = i_0$ car $\sigma \in G_{i_0 - 1} \setminus G_{i_0}$,

donc $v_\pi(P'(\pi)) = (p-1) i_0$

D'autre part, $\deg P = p$, donc $P'(X) = p X^{p-1} + \dots + a_1$.
(coefficients entiers)

Comme p est totalement ramifié, on a

$$\frac{\mathcal{O}_K}{(p)} \simeq \frac{\mathbb{Z}_p[X]}{(p, P(X))} \simeq \frac{\mathbb{F}_p[X]}{(\bar{P}(X))}$$

$(p) = (\pi)^p$

$\bar{P}(X)$ est divisible par X et n'a pas d'autre diviseur, donc $P(X) \equiv X^p \pmod p$.

$a_i \equiv 0 \pmod p$, or $(p) = (\pi)^p$

donc $v_\pi(a_i) \equiv 0 \pmod p$.

$$P'(\pi) = p\pi^{p-1} + a_{p-1}(p-1)\pi^{p-2} + \dots + a_1$$

$$v_\pi(a_i \, i \, \pi^{i-1}) \equiv i - 1 \pmod p \qquad 1 \le i \le p-1$$

↖ deux à deux distincts

donc les termes de la somme ont des valuations distinctes

donc $v_\pi(P'(\pi)) = \min\left(v_\pi(p\pi^{p-1}), v_\pi(a_{p-1}(p-1)\pi^{p-2}), \dots, v_\pi(a_1)\right)$,

donc en particulier $v_\pi(p\pi^{p-1}) \ge v_\pi(P'(\pi))$

i.e. $2p - 1 \ge (p-1) i_0$

$$i_0 \le \frac{2p-1}{p-1} = 2 + \frac{1}{p-1} < 3,$$

or $i_0 \ge 2$, donc $i_0 = 2$, donc $G_2 = 1$.

Ceci conclut la preuve du lemme, et la preuve du théorème de Kronecker-Weber.

Appendice : Construction de la cohomologie des groupes.

biblio : . Cassels & Fröhlich chap IV Cohomology of Groups (Atiyah, Wall, Macdonald)

. Cartan & Eilenberg Homological Algebra
. Serre, Cohomologie galoisienne
. Serre, Corps locaux

G = groupe
M = A-module (par ex. groupe commutatif)
+ action A-linéaire de G
i.e. M est un $A[G]$-module

On a $\mathrm{Hom}_G(A, M) \simeq \left(\mathrm{Hom}_{\text{groupes}}(A, M)\right)^G \simeq M^G$

↑
action de G définie par
$\sigma \cdot \varphi = \sigma \circ \varphi \circ \sigma^{-1}$

or $\mathrm{Hom}_G(A, \cdot)$ est exact à gauche, donc $(\cdot)^G$ aussi.

Si $0 \to M' \to M \to M'' \to 0$ est une suite exacte de $A[G]$-modules, on obtient une suite exacte
$0 \to M'^G \to M^G \to M''$.