Cours 1

Corps globaux, théorie du corps de classes

Références :

- Cassels - Fröhlich, <u>Algebraic Number Theory</u>, Chapitres II et VII.
- Hartshorne, <u>Algebraic Geometry</u>, § I.6.
- Szamuely, <u>Galois Groups and Fundamental Groups</u>.

Si K est un corps, on notera
$$\mathrm{Gal}_K = \mathrm{Gal}(K^{sep}/K)$$
le groupe de Galois d'une clôture séparable K^{sep} de K. C'est un groupe profini, dont les sous-groupes ouverts correspondent bijectivement aux extensions finies séparables de K.

Les corps qui nous intéressent le plus dans le cadre du programme de Langlands sont les corps globaux :

Déf : Un corps global est un corps K qui est soit une extension finie de $\mathbb{Q}$ (un corps de nombres), soit une extension finie du corps $\mathbb{F}_p(T)$ des fractions rationnelles sur $\mathbb{F}_p$, p premier (un corps de fonctions).

Rq : Un corps de fonctions de car. p est de façon équivalente un corps de t.f sur $\mathbb{F}_p$ de degré de transcendance 1.

Déf : Une place de K est une classe d'équivalence de normes multiplicatives $|.| : K \to \mathbb{R}_{\geq 0}$ non triviales.

(équivalence : même topologie.)

Ex: K corps de nombres. Les places de K correspondent bijectivement aux idéaux maximaux de $\mathcal{O}_K$ (anneau des entiers de K) et aux normes archimédiennes données par les plongements $K \hookrightarrow \mathbb{C}$.

Ex: $K = \mathbb{F}_q(T)$ (q puissance de p).

- Si $P(T) \in \mathbb{F}_q[T]$ irréd., $0 < c < 1$, on pose
$$\left| P(T)^a \frac{f(T)}{g(T)} \right|_P = c^a, \quad a \in \mathbb{Z}, \quad f(T), g(T) \in \mathbb{F}_q[T] \text{ premiers à } P.$$

- Pour $0 < c < 1$,
$$\left| \frac{f(T)}{g(T)} \right|_\infty = c^{\deg g - \deg f}$$
$$\left(\text{“} |\cdot|_\infty = |\cdot|_{T^{-1}} \text{”} \right)$$

On a ainsi énuméré toutes les places de K.

Si v est une place de K, on note K_v le complété de K pour v. Si v est non-archimédienne, on note $\mathcal{O}_v \subseteq K_v$ l'anneau des entiers de K_v, i.e.
$$\mathcal{O}_v = \{ x \in K_v, \ |x|_v \leq 1 \}.$$

Pour étudier un corps global et son arithmétique, il est souvent utile de procéder localement, c-à-d. d'étudier d'abord ces complétions locales.

Un moyen pratique d'organiser l'information donnée par ceux-ci est d'utiliser les adèles/idèles.

Déf: On note $\mathbb{A}_K$ le sous-ensemble de $\prod_{v \text{ place de } K} K_v$ défini par la condition $x_v \in \mathcal{O}_v$ pour presque tout v.
On munit $\mathbb{A}_K$ d'une topologie en décrétant qu'une base d'ouverts est formée par les $\prod_v U_v$, avec U_v ouvert de K_v $\forall v$ et $U_v = \mathcal{O}_v$ pour presque tout v.
L'addition et la multiplication terme à terme font de $\mathbb{A}_K$ un anneau topologique.

Rq: Si $S \subseteq Pl(K)$ fini,
$$\mathbb{A}_K^S = \prod_{v \in S} K_v \prod_{v \notin S} \mathcal{O}_v$$ est ouvert dans $\mathbb{A}_K$
et la topologie induite est la topologie produit.

Déf: Le groupe <u>des idèles</u> $\mathbb{I}_K$ de K est le groupe $\mathbb{A}_K^\times$ des éléments inversibles de $\mathbb{A}_K$ muni de la topologie induite par la top. produit sur $\mathbb{A}_K \times \mathbb{A}_K$ via
$$\mathbb{A}_K^\times \hookrightarrow \mathbb{A}_K \times \mathbb{A}_K, \quad x \mapsto (x, x^{-1})$$
($\neq$ top induite par $\mathbb{A}_K^\times \hookrightarrow \mathbb{A}_K$.)

Rq : On peut plonger K, resp. $K^\times$, dans $\mathbb{A}_K$, resp. $\mathbb{I}_K$, en envoyant x sur $(x_v = x)_v$.

K, resp $K^\times$, est discret dans $\mathbb{A}_K$, resp. $\mathbb{I}_K$.
Le quotient $\mathbb{A}_K / K$ est compact.
(Exo : vérifier ceci lorsque $K = \mathbb{Q}$!)
Dans le cas des idèles, on vérifie que $K^\times$ est

contenu dans $\mathbb{I}_K^1 = \ker\Big(\mathbb{I}_K \to \mathbb{R}_{>0}, (x_v) \mapsto \underbrace{\prod_v |x_v|_v}_{\text{bien déf.}}\Big)$
et le quotient $\mathbb{I}_K^1 / K^\times$ est compact.
Cela entraîne la finitude du groupe de classes :
Soit I_K le groupe des classes d'idéaux de K
= groupe ab. libre sur les places non-arch.
L'application $\mathbb{I}_K \to I_K$, $(x_v) \mapsto \sum \mathrm{ord}_v(x_v) \cdot v$
est surjective et l'image de $K^\times$ est le groupe des idéaux principaux. Elle est aussi continue si l'on munit I_K de la topologie discrète. Ainsi, le groupe des classes d'idéaux est un quotient discret de $\mathbb{I}_K^1 / K^\times$, compact, donc est fini.

Une différence majeure entre corps de nombres et corps de fonctions est le fait que ces derniers admettent une interprétation géométrique.

Soit k un corps parfait.

Déf : Une <u>courbe</u> sur k est un schéma intègre séparé X de t.f. sur k (= une variété) de dimension 1.

Elle est dite <u>lisse</u> ou <u>non singulière</u> si les anneaux locaux de X sont réguliers.

$\Leftrightarrow$ des anneaux de valuation discrète

Déf : Un <u>corps de fonctions sur k de dim 1</u> est un corps K de t.f sur k de degré de transcendance 1, t.q. k est alg. clos dans K.

<u>Th</u> : Le foncteur "corps des fonctions méromorphes" (= anneau local au pt générique) induit une équivalence entre les catégories {courbes projectives lisses sur k, morphismes non constants}

et {corps de fonctions sur k de dim 1}.

<u>Dém</u> (idée). Le foncteur inverse est construit comme suit. Soit K un corps de fonctions de dimension 1 sur k. Notons

$$X = \{\eta\} \cup \left\{ \begin{array}{l} \text{places non-archimédiennes de} \\ K, \text{ triviales sur } k \end{array} \right\}$$

Topologie : ouverts $= \emptyset$ et complémentaires dans X d'un nombre fini de points $\neq \eta$.

Faisceau structural :

$$U \subseteq X \text{ ouvert}, \quad \mathcal{O}_X(U) = \{f \in K,\ v(f) \geq 0\ \forall v \in U\} = \bigcap_{v \in U} \mathcal{O}_v.$$

On peut vérifier que X est une courbe projective lisse sur k, avec $k(X) = K$ et $H^0(X, \mathcal{O}_X) = k$. « ■ »

<u>Ex</u> : $X = \mathbb{P}^1_k$, $k(X) = k(T)$.

Le <u>programme de Langlands</u> s'attache à analyser la structure du groupe de Galois Gal_K d'un corps global en étudiant les représentations de celui-ci.

Dans le cas des corps de fonctions, on peut exploiter la géométrie de X, la courbe associée à ce corps de fonctions. Cette idée est le point de départ et le coeur du <u>programme de Langlands géométrique</u>.

Dans ce cours, nous n'allons rien dire sur le cas des corps de nombres et nous intéresser uniquement aux corps de fonctions.

Aujourd'hui : les représentations les plus simples de Gal_K sont celles de dim 1, i.e. les caractères. C'est l'objet de la <u>théorie du corps de classes</u>.

Soit K un corps global. Soit L/K ext. finie galoisienne gpe de Gal G

Si w est une place de K, notons

$G_w = \{ \sigma \in G, \ \sigma w = w \}$. groupe de décomposition en w

déterminé à conjugaison près par $v = w_{|K}$.

L'extension L_w/K_v est galoisienne et bijection $G_w \to Gal(L_w/K_v)$ est un isomorphisme.

Si v est non ramifié (vrai pour presque tout w)
$G_w \simeq Gal(L_w/K_v) \simeq Gal(k(w)/k(v))$
corps résiduels

groupe cyclique engendré par $x \mapsto x^{q_v}$
avec $q_v = |k(v)|$.

Il y a donc un unique élément $Frob_w \in G$ tq $Frob_w \in G_w$ et $Frob_w(x) \equiv x^{q_v}$ modulo $\mathfrak{p}_w$. $\forall x \in O_L$

La classe de conjugaison de $Frob_w$ dans G ne dépend que de $v = w_{|K}$ et sera notée $Frob_v$.

<u>Th</u> (Loi de réciprocité d'Artin)

i) Pour toute extension finie <u>abélienne</u> L de K, il existe un morphisme continu
$$\psi_{L/K} : \mathbb{I}_K \longrightarrow Gal(L/K) \quad \text{t.q.}$$
$$\psi_{L/K}(K^\times) = 1 \quad \text{et} \quad \psi_{L/K}(x) = \prod_{v \notin S} Frob_v^{\,ord_v(x_v)}$$
bien défini car $Gal(L/K)$ abélien

pour tout $x \in \mathbb{I}_K$ t.q. $x_v = 1 \quad \forall v \in S$

où $S = \{\text{places archimédiennes}\} \cup \{\text{places ramifiées}\}$.

ii) L'application $\psi_{L/K}$ est surjective de noyau $K^\times N_{L/K}(L^\times)$, i.e.

$$\psi_{L/K} : C_K / N_{L/K}(C_L) \simeq Gal(L/K).$$

(iii) Compatibilité naturelle pour un triplet

$$K \subset L \subset M.$$

(iv) Pour tout sous-groupe N d'indice fini de C_K, $\exists !$ L/K finie abélienne t.q. $N = N_{L/K}(C_L)$.
(dans K^{sep} fixée)

C'est une théorie difficile !
(couronnement du travail de nombreux mathématiciens de Gauß à Artin et Tate)

Le point (iii) permet de passer à la limite sur L:

On obtient ainsi

$$\psi_K : C_K \to Gal(K^{ab}/K) = \text{abélianisé de } Gal_K$$

(K^{ab} = ext. ab. maximale de K)

Supposons désormais que K est un <u>corps de fonctions</u>. Dans ce cas:

Ψ_K est un morphisme de groupes injectif, d'image le sous-groupe formé des éléments du groupe de Galois dont la restriction à $\bar{k}$ est une puissance entière du Frob.

(Corps de nombres : Ψ_K surjectif, mais noyau non trivial = composante connexe de l'identité.)

En particulier, la théorie du corps de classes nous dit que l'application

$$C_K / \prod_v \mathcal{O}_v^\times \longrightarrow \underbrace{\mathrm{Gal}_K^{nr,ab}}_{\substack{\text{groupe de Galois de l'ext} \\ \text{ab nr. maximale de } K \text{ (= corps} \\ \text{de classes de Hilbert)}}}$$

$$\mathbb{I}_K \ni (x_v) \longmapsto \prod_v \mathrm{Frob}_v^{\mathrm{ord}_v(x_v)}$$

est bien définie et est un isomorphisme sur les complétés profinis.

Par conséquent, pour tout groupe abélien fini G, on dispose d'une équivalence $\left\{ \begin{array}{c} \text{caractères continus} \\ \mathrm{Gal}_K^{nr} \to G \end{array} \right\} \xrightarrow{\sim} \left\{ \begin{array}{c} \text{caractères continus} \\ C_K / \prod_v \mathcal{O}_v^\times \to G \end{array} \right\}$

$$\chi \longmapsto \rho \quad \text{t.q.}$$

$\forall v$, $\chi(\mathrm{Frob}_v) = \rho(\pi_v)$ (π_v unif. de $\mathcal{O}_v$).

Le but du reste du cours d'aujourd'hui est d'expliquer une preuve géométrique de cette conséquence de la théorie du corps de classes non ramifiée (qui lui est en fait équivalente, par dualité de Pontryagin). Cette preuve est due à Deligne.

Pour cela, notons X la courbe projective lisse géom. connexe $/ k = \overline{\mathbb{F}_q} \cap K$ associée à notre corps de fonctions K.

Rappel : Y schéma, supposé connexe.

$\mathrm{Rev}(Y)$ = catégorie des morphismes finis étales surjectifs $Z \to Y$

Soit $\bar{y}$ un point géom. de Y. Le foncteur

$$F_{\bar{y}} : \mathrm{Rev}(Y) \longrightarrow \mathrm{EnsFinis}$$
$$Z \longmapsto Z \times_Y \bar{y}$$

peut être enrichi en une équivalence de catégories

$$\mathrm{Rev}(Y) \simeq \underbrace{\pi_1}(Y, \bar{y})\text{-}\mathrm{EnsFinis} \quad \text{action continue}$$

groupe profini ne dépendant pas de $\bar{y}$ à iso. top. près.

Ex : $Y = \mathrm{Spec}(L)$, $\pi_1(Y, \bar{y}) = \mathrm{Gal}(\bar{L}/L)$.
L corps $\bar{y} \hookrightarrow \bar{L}$ clôture alg.

Ex, L alg clos, $\bar{y}$ pt générique de $\mathbb{P}^1_L$.
$\pi_1(\mathbb{P}^1_L, \bar{y}) = 0$

Déon : C'est une conséquence du th. de classification des fibrés sur $\mathbb{P}^1_L$ par Grothendieck. Soit $Z \xrightarrow{f} \mathbb{P}^1_L$ revêtement fini étale. Alors $f_* \mathcal{O}_Z$ est un fibré vectoriel sur $\mathbb{P}^1_L$. On peut donc l'écrire $f_* \mathcal{O}_Z = \bigoplus_{i=1}^{d} \mathcal{O}(k_i)$, $k_i \in \mathbb{Z}$.
Comme $f_* \mathcal{O}_Z$ a une structure d'algèbre, on a

$$m : f_* \mathcal{O}_Z \otimes f_* \mathcal{O}_Z \to f_* \mathcal{O}_Z$$

et aussi un accouplement parfait trace :

$$tr : f_* \mathcal{O}_Z \otimes f_* \mathcal{O}_Z \longrightarrow \mathcal{O}_{\mathbb{P}^1_L}.$$

Comme tr est parfait, $f_* \mathcal{O}_Z$ est autodual, donc $\exists$ au moins un k_i tq. $k_i \geq 0$. Supposons qu'il en existe un > 0. Prenons le plus grand, quitte à réordonner c'est k_1.
Alors m se restreint en $\mathcal{O}(2k_1) \to f_* \mathcal{O}_Z$

i.e. un élément de $H^0(\mathbb{P}^1_L, \underbrace{f_*\mathcal{O}_Z \otimes \mathcal{O}(-2k_1)}))$

$= 0$ pente < 0 par choix de k_1

Impossible car Z est réduit. Donc récursivement $k_i = 0 \ \forall i$, i.e. $f_*\mathcal{O}_Z \simeq H^0(Z, \mathcal{O}_Z) \otimes \mathcal{O}_{\mathbb{P}^1_L}$.

Comme L est alg. clos, la L-algèbre $H^0(Z, \mathcal{O}_Z)$ est isomorphe comme L-alg à L^d et donc

$Z \simeq \mathbb{P}^{1\,d}_L$. ∎

Plus général^t, on a $\pi_1(\mathbb{P}^r_L, \bar{\eta}) = 0 \ \forall \bar{\eta} \ \forall r \geq 1$.

(Indication : Par récurrence sur r, montrer que $\forall \bar{\eta}$, $\pi_1((\mathbb{P}^1_L)^r, \bar{\eta}) = 0 \ \forall r \geq 1$.

Puis utiliser $\mathbb{P}^r_L = (\mathbb{P}^1_L)^{(r)}$ (cf. cours 2) et le résultat suivant :

<u>Prop</u> (SGA 1) Γ groupe fini agissant sur Y schém. connexe de sorte que toute orbite de Γ est contenue dans un affine.

Alors Y/Γ bien défini (cf. cours 2)

et $\mathrm{Rev}(Y/\Gamma) \simeq \left\{ \begin{array}{l} \text{revêtements finis étales} \\ \Gamma\text{-équivariants de } Y \text{ tq} \\ \forall y \in Y,\ \Gamma_y \text{ agit trivial}^t \\ \text{sur la fibre en } y \end{array} \right\}$

$\Gamma_y \subseteq \Gamma$ fixe y et agit trivial^t sur $k(y)$.

Appliquer ici à $Y = (\mathbb{P}^1_L)^r$, $\Gamma = S_r$
et remarquer que $\Gamma_y = \Gamma$ si $y \in$ diagonale.)

<u>Ex.</u>: Soit $Y \to S$ morphisme propre plat entre variétés sur un corps, à fibres géométriques connexes.
On a une suite exacte (dite d'homotopie):

$$\pi_1(Y_{\bar{s}}, \bar{y}) \to \pi_1(Y, \bar{y}) \to \pi_1(S, \bar{s}) \to 0.$$

si $\bar{y} \mapsto \bar{s}$ point géom.

Retour à K et X. On a par construction

$$K = k(X).$$

Soit η le point générique de X, $\bar{\eta}$ pt géom au-dessus de η. Le morphisme canonique $\eta \to X$ induit un morphisme canonique

$$\pi_1(\eta, \bar{\eta}) \simeq \mathrm{Gal}_K \to \pi_1(X, \bar{\eta}).$$

qui induit lui-même un isomorphisme

$$\mathrm{Gal}_K^{nr} \simeq \pi_1(X, \bar{\eta})$$

(vrai plus généralt pour X intègre normal)

...

Par conséquent, pour G abélien fini,

$$\left\{ \begin{array}{c} \text{caractères continus} \\ \mathrm{Gal}_K^{nr} \to G \end{array} \right\} \simeq \left\{ \begin{array}{c} \text{caractères continus} \\ \pi_1(X) \to G \end{array} \right\}$$