IX
Les énoncés de la théorie du corps de classe

1. Compléments sur les corps p-adiques

Soit p un nombre premier. Soit K un *corps p-adique*. C'est-à-dire une extension finie de $\mathbf{Q}_p$ (attention le terme corps p-adique peut désigner, suivant les auteurs, des extensions infinies de $\mathbf{Q}_p$). Notons $\mathcal{O}_K$ la clôture intégrale de $\mathbf{Z}_p$ dans K, v la valuation discrète de K, $\mathcal{P}$ l'idéal premier non nul de $\mathcal{O}_K$, k le corps résiduel et q le nombre d'éléments de k. Posons $U_K^{(n)} = 1 + \mathcal{P}^n\mathcal{O}_K$ lorsque n est un entier > 0 et $U_K^{(0)} = \mathcal{O}_K^*$.

On a la suite décroissante de sous-groupes ouverts :

$$... \subset U_K^{(n+1)} \subset U_K^{(n)} \subset ... \subset U_K^{(1)} = 1 + \mathcal{P}\mathcal{O}_K \subset U_K^{(0)} = \mathcal{O}_K^*.$$

Soit π une uniformisante de $\mathcal{P}$. Notons (π) le sous-groupe de K^* engendré par π. Il est isomorphe à $\mathbf{Z}$.

Proposition 1. — *On a les isomorphismes canoniques de groupes*

$$K^* \simeq (\pi) \times \mathcal{O}_K^*,$$

et

$$U_K^{(0)}/U_K^{(1)} \simeq k^*.$$

De plus le groupe quotient $U_K^{(n)}/U_K^{(n+1)}$ est un k-espace vectoriel de dimension 1.
Démonstration. — La première assertion résulte du fait que la valuation discrète v définit une suite exacte de groupes abéliens

$$0 \longrightarrow \mathcal{O}_K^* \longrightarrow K^* \longrightarrow \mathbf{Z} \longrightarrow 0,$$

et qu'on a $v(\pi) = 1$.

Le deuxième isomorphisme provient de l'homomorphisme de groupes canonique et surjectif $\mathcal{O}_K^* \longrightarrow k^*$. Le noyau de cet homomorphisme est $U_K^{(1)}$.

On a un isomorphisme canonique de k-espaces vectoriels entre $U_K^{(n)}/U_K^{n+1)}$ et k déduit de l'application $U_K^{(n)} \longrightarrow k$ qui à $1 + a\pi^n$ associe $a + \mathcal{P}$. Cette dernière application est un homomorphisme surjectif de groupes de noyau $U_K^{(n+1)}$.

Remarque . — On a même un isomorphisme canonique de groupes

$$K^* \simeq (\pi) \times \mu_{q-1} \times U_K^{(1)}.$$

L'isomorphisme d'espaces vectoriels $U_K^{(n)}/U_K^{n+1)} \simeq k$ construit dans la démonstration de la proposition 1 est non canonique puisqu'il dépend du choix d'une uniformisante de $\mathcal{P}$. Lorsque K est égal à $\mathbf{Q}_p$, on dispose d'une uniformisante canonique de $p\mathbf{Z}_p$, c'est-à-dire p.

2. Les groupes de classe de rayon et les cycles arithmétiques

Soit K un corps de nombres. On appelle *cycle arithmétique* (voir le concept de *diviseur d'Arakelov*) un produit formel

$$\prod_{v \in \Omega_K} \mathcal{P}_v^{n_v}$$

où n_v est un entier ≥ 0 lorsque v est une place non archimédienne, où $n_v \in \{0, 1\}$ lorsque v est une place archimédienne réelle, $n_v = 0$ lorsque v est une place archimédienne non réelle et où $\mathcal{P}_v$ est l'idéal maximal de $\mathcal{O}_K$ associé à v lorsque v est une place non archimédienne et où on a $n_v = 0$ pour presque tout $v \in \Omega_K$. Le *support* d'un cycle arithmétique est l'ensemble des places v telles que $n_v \neq 0$.

Attention la terminologie cycle arithmétique n'est pas standard. Le terme utilisé par Hasse en allemand est "Erklärungsmodul".

Cette notion de cycle étend la notion d'idéal entier, puisque tout idéal entier de $\mathcal{O}_K$ est produit d'idéaux premier et s'identifie donc à un cycle arithmétique à support dans les places non archimédiennes.

On a une relation de divisibilité évidente entre les cycles arithmétiques de K qui prolonge la relation de divisibilité des idéaux : Soient $\mathcal{M} = \prod_{v \in \Omega_K} \mathcal{P}_v^{n_v}$ et $\mathcal{M}' = \prod_{v \in \Omega_K} \mathcal{P}_v^{n'_v}$ deux cycles arithmétiques ; On dira que $\mathcal{M}$ divise $\mathcal{M}'$ si on a $n_v \leq n'_v$ $(v \in \Omega_K)$. On dira que ces deux cycles sont premiers entre eux si on a $n_v n'_v = 0$ $(v \in \Omega_K)$. On peut parler de plus petit commun multiple, plus grand commun diviseur etc.

On note 1 le cycle arithmétique à support vide.

Soit $\mathcal{M} = \prod_{v \in \Omega_K} \mathcal{P}_v^{n_v}$. Posons alors

$$U_v^{n_v} = U_{K_v}^{(n_v)}$$

lorsque v est une place non archimédienne,

$$U_v^{n_v} = \mathbf{R}_+^*,$$

lorsque v est une place réelle et $n_v = 1$,

$$U_v^{n_v} = \mathbf{R}^*$$

lorsque v est une place réelle et $n_v = 0$ et

$$U_v^{n_v} = \mathbf{C}^*,$$

lorsque v est une place complexe.

Pour $x \in K_v^*$, on note $x \equiv 1 \pmod{\mathcal{P}_v^{n_v}}$ lorsqu'on a $x \in U_v^{n_v}$ (cela coïncide avec la notation usuelle lorsque v est non archimédienne). On généralise cette notation à $x = (x_v)_{v\in\Omega_K} \in \mathbf{A}_K$ en posant $x \equiv 1 \pmod{\mathcal{M}}$ lorsqu'on a $x_v \equiv 1 \pmod{\mathcal{P}_v^{n_v}}$ $(v \in \Omega_K)$.

Posons alors

$$\mathbf{A}_K^*(\mathcal{M}) = \{x \in \mathbf{A}_K^* / x \equiv 1 \pmod{\mathcal{M}}\}.$$

On a $\mathbf{A}_K^*(\mathcal{M}) \subset \mathbf{A}_K^*(\mathcal{M}')$ lorsque $\mathcal{M}'|\mathcal{M}$. On a

$$\mathbf{A}_K^*(1) = \prod_{v\in\Omega_{K,\infty}} K_v^* \times \prod_{v\in\Omega_K - \Omega_{K,\infty}} \mathcal{O}_v^*.$$

C'est l'ensemble des $\Omega_{K,\infty}$-idèles.

Le sous-groupe

$$C_K^{\mathcal{M}} = \mathbf{A}_K^*(\mathcal{M})K^*/K^*$$

du groupe C_K des classes d'idèles est le *sous-groupe de congruence de niveau* $\mathcal{M}$ de C_K. L'application qui à $\mathcal{M}$ associe $C_K^{\mathcal{M}}$ est décroissante.

On note $\mathcal{I}(K)^{\mathcal{M}}$ le sous-groupe du groupe $\mathcal{I}(K)$ des idéaux fractionnaires de K engendré par les idéaux de $\mathcal{O}_K$ premiers à $\mathcal{M}$. On note $\mathcal{P}(K)^{\mathcal{M}}$ le sous-groupe de $\mathcal{I}(K)^{\mathcal{M}}$ engendré par les idéaux principaux de K de la forme $a\mathcal{O}_K$ avec $a \equiv 1 \pmod{\mathcal{M}}$ et $a \in K^*$.

Le groupe quotient

$$\mathcal{C}\ell(K)^{\mathcal{M}} = \mathcal{I}(K)^{\mathcal{M}}/\mathcal{P}(K)^{\mathcal{M}}$$

est le *groupe des classes d'idéaux de rayon* $\mathcal{M}$. Lorsque $\mathcal{M} = 1$, on retrouve le groupe des classes au sens habituel.

Proposition 2. — *L'homomorphisme de groupes*

$$\mathbf{A}_K^* \longrightarrow \mathcal{I}(K)$$

qui à $(x_v)_{v\in\Omega_K}$ *associe* $\prod_{v\notin\Omega_{K,\infty}} \mathcal{P}_v^{v(x_v)}$ *induit après passages aux quotients un isomorphisme de groupes*

$$C_K/C_K^{\mathcal{M}} \simeq \mathcal{C}\ell(K)^{\mathcal{M}}.$$

Démonstration. — Posons

$$\mathbf{A}_K^* < \mathcal{M} >= \{x = (x_v)_{v\in\Omega_K} \in \mathbf{A}_K^* / x_v = 1 (\mathcal{P}_v \not| \mathcal{M})\}.$$

Soit $\alpha = (\alpha_v)_{v\in\Omega_K} \in \mathbf{A}_K^*$. D'après le théorème d'approximation faible, il existe $a \in K^*$ tel que

$$a\alpha_v \equiv 1 \pmod{\mathcal{P}_v}$$

pour tout $\mathcal{P}_v|\mathcal{M}$. Posons alors

$$a\alpha_v = \beta_v\gamma_v$$

avec $\beta_v = 1$ (si $\mathcal{P}_v \not| \mathcal{M}$), $\beta_v = \alpha_v a$ (si $\mathcal{P}_v | \mathcal{M}$), avec $\gamma_v = 1$ (si $\mathcal{P}_v | \mathcal{M}$) et $\gamma_v = \alpha_v a$ (si $\mathcal{P}_v \not| \mathcal{M}$). Posons $\beta = (\beta_v)_{v \in \Omega_K} \in \mathbf{A}_K^*$ et $\gamma = (\gamma_v)_{v \in \Omega_K} \in \mathbf{A}_K^*$. On a alors $\beta \in \mathbf{A}_K^* < \mathcal{M} >$ et $\gamma \in \mathbf{A}_K^*(\mathcal{M})$. On a

$$\alpha = \beta\gamma a^{-1} \in \mathbf{A}_K^* < \mathcal{M} > .\mathbf{A}_K^*(\mathcal{M}).K^*.$$

Cela prouve qu'on a

$$\mathbf{A}_K^* = \mathbf{A}_K^* < \mathcal{M} > .\mathbf{A}_K^*(\mathcal{M}).K^*.$$

On a alors

$$\begin{aligned} C_K/C_K^{\mathcal{M}} &= \mathbf{A}_K^* < \mathcal{M} > .\mathbf{A}_K^*(\mathcal{M}).K^*/\mathbf{A}_K^*(\mathcal{M}).K^* \\ &= \mathbf{A}_K^*(\mathcal{M})/(\mathbf{A}_K^*(\mathcal{M}) \cap (\mathbf{A}_K^* < \mathcal{M} > .K^*)). \end{aligned}$$

L'homomorphisme de groupes $\mathbf{A}_K^* \longrightarrow \mathcal{I}(K)$ qui à $(x_v)_{v \in \Omega_K}$ associe $\prod_{v \notin \Omega_{K,\infty}} \mathcal{P}_v^{v(x)}$ induit un homomorphisme de groupes

$$\mathbf{A}_K^*(\mathcal{M}) \longrightarrow \mathcal{I}(K)$$

dont l'image est $\mathcal{I}(K)^{\mathcal{M}}$. Il définit par passage au quotient un homomorphisme surjectif de groupes

$$\mathbf{A}_K^*(\mathcal{M}) \longrightarrow \mathcal{I}(K)^{\mathcal{M}}/\mathcal{P}(K)^{\mathcal{M}}.$$

Le noyau de ce dernier homomorphisme coïncide avec $\mathbf{A}_K^*(\mathcal{M}) \cap (\mathbf{A}_K^* < \mathcal{M} > .K^*)$. Cela prouve qu'on a l'isomorphisme cherché.

Remarques. — La proposition 2 permet d'appeler sans ambiguïté le groupe $C_K/C_K^{\mathcal{M}}$ *groupe des classes d'idèles de rayon* $\mathcal{M}$.

Le sous-groupe

$$K_{\mathcal{M}} = K \cap \mathbf{A}_K^*(\mathcal{M})$$

de K^* est le *rayon* modulo $\mathcal{M}$.

Certains auteurs ont considèré des notions un peu plus générales que les cycles arithmétiques : des produits formels de la forme

$$\prod_{v \in \Omega_K} \mathcal{P}_v^{n_v}$$

où $n_v \in \mathbf{Z}$ si v est non archimédienne et $n_v \in \mathbf{R}$ si v est archimédienne. Ce sont des *diviseurs compactifiés* de $\mathcal{O}_K$.

Cette terminologie inspirée par la géométrie algébrique.

Proposition 3. — *Soit* $\mathcal{M} = \prod_v \mathcal{P}_v^{n_v}$ *un cycle arithmétique. Les groupes* $C_K/C_K^{\mathcal{M}}$ *et* $\mathcal{C}\ell(K)^{\mathcal{M}}$ *sont finis.*

Démonstration. — Il suffit de le vérifier pour $C_K/C_K^{\mathcal{M}}$ d'après la proposition 2. Par ailleurs le groupe des classe ordinaire, qui s'identifie à C_K/C_K^1 (voir le lemme VIII–1), est fini. Il suffit donc de prouver la finitude du groupe quotient

$$C_K^1/C_K^{\mathcal{M}} \simeq \mathbf{A}_K^*(1)K^*/\mathbf{A}_K^*(\mathcal{M})K^*$$

et donc du quotient

$$\mathbf{A}_K^*(1)/\mathbf{A}_K^*(\mathcal{M}) \simeq \prod_{v\in\Omega_K} \mathcal{O}_v/U_v^{n_v}.$$

Les facteurs de ce dernier quotient sont le groupe trivial lorsque $n_v = 0$, c'est-à-dire pour presque tout $v \in \Omega_K$; Les facteurs non triviaux sont finis d'après la proposition 1. Cela prouve la finitude cherchée.

Remarque . — On a démontré au passage que l'indice de $C_K^{\mathcal{M}}$ dans C_K est égal au produit du nombre de classes et de l'indice de $C_K^{\mathcal{M}}$ dans C_K^1. Ce dernier indice est égal au produit des indices locaux $U_v^{n_v}$ dans U_v^0. C'est donc

$$N_{\mathcal{M}} = 2^{r_0} N_{\mathcal{M}_0},$$

où r_0 est le nombre de places réelles v telles que $n_v \neq 0$ et où $N_{\mathcal{M}_0}$ est la norme de l'idéal formé par la partie non archimédienne de $\mathcal{M}$.

Proposition 4. — *Tout sous-groupe ouvert d'indice fini de C_K contient un sous-groupe de congruence.*
Démonstration. — Un tel sous-groupe correspond à un sous-groupe ouvert G d'indice fini de $\mathbf{A}_K^*$ contenant K^*. Comme on a $\mathbf{A}_K^* = \mathbf{A}_K^*(1).K^*$ et $K^* \cap \mathbf{A}_K^*(1) = \mathcal{O}_K^*$, il définit un sous-groupe ouvert H d'indice fini de $\mathbf{A}_K^*(1)$ contenant $\mathcal{O}_K^*$. ainsi H contient un ouvert de la forme $\prod_{v\in S} W_v \prod_{v\in\Omega_K - S} \mathcal{O}_v^*$ où S est un ensemble fini de places contenant $\Omega_{K,\infty}$, et W_v est un ouvert de K_v^*.

La projection de H dans chaque composante de

$$\mathbf{A}_K^*(1) = \prod_{v\in\Omega_{K,\infty}} K_v^* \times \prod_{v\in\Omega_K - \Omega_{K,\infty}} \mathcal{O}_v^*$$

est d'indice fini.

Un sous groupe d'indice fini de $\mathbf{C}^*$ ne peut être que $\mathbf{C}^*$ lui-même. Un sous-groupe d'indice fini de $\mathbf{R}^*$ est égal à $\mathbf{R}^*$ ou $\mathbf{R}_+^*$. Enfin un sous-groupe d'indice fini de $\mathcal{O}_{\mathcal{P}}^*$ contient un sous-groupe de la forme $U_{\mathcal{P}_v}^n$ (voir la structure de $\mathcal{O}_{\mathcal{P}}^*$ donnée par la proposition 1).

On en déduit que H contient un groupe de la forme

$$\prod_{v\in\Omega_K} U_v^{n_v}.$$

Comme H est d'indice fini, on en déduit que $n_v = 0$ pour presque tout $v \in \Omega_K$. En posant $\mathcal{M} = \prod_v \mathcal{P}_v^{n_v}$, on obtient que H contient $\mathbf{A}_K^*(\mathcal{M})$.

Le groupe G contient donc $\mathbf{A}_K^*(\mathcal{M})K^*$. Cela achève de prouver la proposition.

Remarque . — On peut montrer que tout sous-groupe ouvert de $\mathbf{A}_K^*$ contenant K^* est d'indice fini. Cela se déduit du fait que le noyau de la valeur absolue $||.|| : C_K \to \mathbf{R}_+^*$ est compacte. Par ailleurs, il existe des sous-groupes d'indice fini non-ouverts dans C_K.

3. Extensions abéliennes

Soit $L|K$ une extension de corps. On dit qu'il s'agit d'une *extension abélienne* si c'est une extension galoisienne et si le groupe de Galois $\mathrm{Gal}(L/K)$ est abélien.

On voit facilement que la composée de deux extensions abéliennes (contenues dans un corps commun) est abélienne. De plus l'intersection de deux extensions abéliennes est abélienne.

Tout groupe G admet un plus grand groupe quotient abélien G^{ab}. C'est l'*abélianisé* de G. Il est obtenu comme quotient de G par son sous-groupe des commutateurs. Il en résulte que toute extension galoisienne $L|K$ admet une plus grande sous extension $L'|K$ qui est abélienne de groupe de Galois $\mathrm{Gal}(L/K)^{\mathrm{ab}}$.

La théorie du corps de classe vise à étudier les extensions abéliennes de K lorsque K est un corps p-adique ou un corps de nombres (signalons qu'il existe des généralisations de cette théorie dans diverses directions, mentionnons tout spécialement la théorie du corps de classe pour les corps de fonctions).

4. La théorie du corps de classe local

Soit p un nombre premier. Soit K un corps p-adique.

Le théorème principal est la loi de réciprocité locale. On peut rendre le théorème 1 ci-dessous plus explicite par la théorie de Lubin-Tate. On peut le rendre plus précis en faisant intervenir les groupes de ramifications.

THÉORÈME 1. — *L'application qui à L associe $\mathrm{N}_{L/K} L^*$ est une correspondance bijective et décroissante entre les extensions abéliennes finies de K et les sous-groupes d'indice finis de K^*.*

Soit L/K une extension abélienne et finie. On a un isomorphisme de groupes

$$\mathrm{Gal}(L/K) \longrightarrow K^*/\mathrm{N}_{L/K} L^*.$$

De plus on a

$$\mathrm{N}_{L_1L_2/K} (L_1L_2)^* = \mathrm{N}_{L_1/K} L_1^* \cap \mathrm{N}_{L_2/K} L_2^*$$

et

$$\mathrm{N}_{L_1\cap L_2/K} (L_1 \cap L_2)^* = (\mathrm{N}_{L_1/K} L_1^*)(\mathrm{N}_{L_1/K} L_2^*).$$

L'homomorphisme de groupes $K^*/\mathrm{N}_{L/K} L^* \longrightarrow \mathrm{Gal}(L/K)$ réciproque de celui dont il est question dans le théorème est l'*homomorphisme de reste normique*, ou *isomorphisme de réciprocité* ou *homomorphisme d'Artin local*. Chronologiquement la théorie du corps de classe global a précédé la théorie du corps de classe local. Mais il est plus naturel d'établir d'abord la théorie locale avant de l'utiliser comme ingrédient pour la théorie globale.

Lorsque K est non plus un corps local, mais une extension finie de $\mathbf{R}$ (c'est-à-dire $\mathbf{R}$ ou $\mathbf{C}$) le théorème 1 est encore vrai en le sens suivant. Soit L une extension finie de K

(*i.e.* on a $K = L$ sauf lorsque $K = \mathbf{R}$ et $L = \mathbf{C}$). Le groupe $\mathrm{Gal}(L/K)$ est canoniquement isomorphe à $K^*/\mathrm{N}_{L/K}\, L^*$. En effet ces deux groupes sont triviaux sauf lorsque $K = \mathbf{R}$ et $L = \mathbf{C}$; Dans ce dernier cas les groupes $\mathrm{Gal}(L/K)$ et $K^*/\mathrm{N}_{L/K}\, L^*$ sont d'ordre 2, puisqu'on a $\mathrm{N}_{\mathbf{C}/\mathbf{R}}\, \mathbf{C}^* = \mathbf{R}_+^*$. L'isomorphisme canonique

$$\mathrm{Gal}(L/K) \longrightarrow K^*/\mathrm{N}_{L/K}\, L^*$$

s'appelle encore homomorphisme d'Artin.

Remarques. — Soit $L|K$ une extension finie et non ramifiée. L'image de l'application norme $\mathrm{N}_{L/K}$ contient $\mathcal{O}_K^*$ (on le verra lorsqu'on étudiera la ramification).

Lorsque $L|K$ est abélienne et non-ramifiée, l'image inverse d'une substitution de Frobenius par l'homomorphisme de restes normiques est un générateur de $K^*/\mathrm{N}_{L/K}\, L^*$. Cela résulte directement de l'homomorphisme de réciprocité local et du fait que la substitution de Frobenius est un générateur du groupe de Galois dans le cas non ramifié.

On normalise l'homomorphisme de restes normiques de telle sorte que l'image d'une uniformisante de K soit égale à la subsitution de Frobenius.

Lorsque $L|K$ est encore abélienne et finie mais pas nécessairement non ramifiée, l'image de l'application norme est d'indice fini dans K^*. Elle contient donc un sous-groupe $U_K^{(n)}$, pour n entier minimal. Cet entier n est le *conducteur* (au sens additif) de l'extension $L|K$. On peut aussi appeler conducteur l'idéal $\mathcal{P}^n$ de $\mathcal{O}_K$. Lorsque l'extension $L|K$ est non ramifiée on a $n = 0$. On verra le lien entre l'entier n et les groupes de ramification de l'extension $L|K$.

5. La théorie du corps de classe global

On considère maintenant K un corps de nombres. Soient $L|K$ une extension abélienne et finie. Soit v et w des places de K et L. Notons K_v et L_w leurs complétés respectifs en ces places. Le groupe $\mathrm{Gal}(L_w/K_v)$ s'identifie à un sous-groupe (de décomposition en w si v est non-archimédienne) de $\mathrm{Gal}(L/K)$ (voir la leçon sur les extensions de corps complets). Lorsque w varie parmi les places au-dessus de v, ces sous-groupes de $\mathrm{Gal}(L/K)$ sont conjugués les uns des autres, et donc égaux puisque $\mathrm{Gal}(L/K)$ est un groupe abélien. Notons ψ_v l'homomorphisme d'Artin local correspondant.

Notons C_K et C_L les groupes de classes d'idèles de K et L. Rappelons que, pour toute place w de L, L_w^* s'identifie à un sous-groupe de C_L via le plongement $L_w^* \longrightarrow \mathbf{A}_K^*$. On a une application norme $\mathrm{N}_{L/K} : C_L \longrightarrow C_K$ déduite de l'application norme $\mathbf{A}_L* \longrightarrow \mathbf{A}_K^*$ (elle-même définie par la norme sur chaque composante ; Attention au conflit de terminologie entre cette application norme et celle qui s'appelle aussi valeur absolue). La composante en v de $\mathrm{N}_{L/K}\, C_L$ n'est autre que $\mathrm{N}_{L_w/K_v}\, L_w^*$.

Théorème 2. — *L'application qui à L associe $\mathrm{N}_{L/K}\, C_L$ est une correspondance bijective et décroissante entre les extensions abéliennes finies de K et les sous-groupes fermés d'indice fini de C_K.*

Soit L/K une extension abélienne et finie. On a un isomorphisme de groupes

$$\mathrm{Gal}(L/K) \longrightarrow C_K/\mathrm{N}_{L/K}\, C_L$$

compatible aux homomorphismes de restes normiques et aux plongements locaux. De plus on a

$$\mathrm{N}_{L_1L_2/K}\, C_{L_1L_2} = \mathrm{N}_{L_1/K}\, C_{L_1} \cap \mathrm{N}_{L_2/K}\, C_{L_2}$$

et

$$\mathrm{N}_{L_1\cap L_2/K}\, C_{L_1\cap L_2} = (\mathrm{N}_{L_1/K}\, C_{L_1})(\mathrm{N}_{L_1/K}\, C_{L_2}).$$

Ce théorème est dû à Artin, à la suite des travaux de nombreux mathématiciens antérieurs. La formulation en termes de classes d'idèles est postérieure et est due à Chevalley.

L'extension abélienne associée à un sous-groupe fermé et d'indice fini G de C_K est le *corps de classe* de G. L'homomorphisme $\psi : C_K/\mathrm{N}_{L/K}\, C_L \longrightarrow \mathrm{Gal}(L/K)$ inverse de celui du théorème 2 est *l'homomorphisme d'Artin*. Le fait qu'il soit compatible aux homomorphismes de restes normiques signifie que pour toute place v de K, la restriction de ψ à $K_v^*/\mathrm{N}_{L_w/K_v} L_w^*$ n'est autre que ψ_v lorsqu'on identifie $\mathrm{Gal}(L_w/K_v)$ à un sous-groupe de $\mathrm{Gal}(L/K)$ et $K_v^*/\mathrm{N}_{L_w/K_v} L_w^*$ à un sous-groupe de $C_K/\mathrm{N}_{L/K}\, C_L$. Autrement dit on a un diagramme commutatif d'homomorphismes de groupes

$$\begin{array}{ccc} \mathrm{Gal}(L_w/K_v) & \simeq & K_v^*/\mathrm{N}_{L_w/K_v} L_w^* \\ \downarrow & & \downarrow \\ \mathrm{Gal}(L/K) & \simeq & C_K/\mathrm{N}_{L/K} C_L, \end{array}$$

où les flèches horizontales sont les isomorphismes de réciprocité et les flèches verticales sont des injections.

Remarque . — La donnée des homomorphismes d'Artin locaux en chaque place v de K suffit à prouver l'existence de $\psi : \mathbf{A}_K^*/\mathrm{N}_{L/K}\, \mathbf{A}_L^* \longrightarrow \mathrm{Gal}(L/K)$. En effet soit $x = (x_v)_{v\in\Omega_K} \in \mathbf{A}_K^*$. Pour presque tout v on a $x_v \in \mathcal{O}_v^*$ et $L|K$ non ramifiée en v. On a donc $\psi_v(x_v) = 1$ pour presque tout v (voir la remarque à la fin de la section précédente). La fonction $\psi = \prod_{v\in\Omega_K} \psi_v : \mathbf{A}_K^* \longrightarrow \mathrm{Gal}(L/K)$ est donc bien définie. Son noyau contient $\mathrm{N}_{L/K}\, \mathbf{A}_L^*$ puisque le noyau de ψ_v contient $\mathrm{N}_{L/K}\, L_w$. Mais il n'est pas clair *a priori* qu'il contienne K^*. C'est même l'un des points essentiels de la théorie. Néanmoins, retenons que la donnée de tous les homomorphismes d'Artin locaux détermine l'homomorphisme d'Artin global.

Une extension abélienne $L|K$ admet un *conducteur* qui est l'idéal de $\mathcal{O}_K$ défini comme le produit (fini car on a $n_v = 0$ pour presque tout v)

$$\prod_{v\in\Omega_K - \Omega_{K,\infty}} \mathcal{P}_v^{n_v}$$

où n_v est le conducteur de l'extension locale $L_w|K_v$. On peut même définir une composante archimédienne du conducteur pour obtenir un cycle arithmétique. Cette composante est donnée comme le produit des places réelles de K au dessus desquelles l'extension $L|K$ est non réelle.

6. Point de vue élémentaire et corps de classe

Soit $L|K$ une extension abélienne de corps de nombres. Soit $\mathcal{P}$ un idéal maximal de $\mathcal{O}_L$ au dessus d'un idéal maximal $\mathcal{Q}$ de $\mathcal{O}_K$ telle que l'extension $L|K$ soit non ramifiée en $\mathcal{P}$. La substitution de Frobenius en $\mathcal{P}$ ne dépend que de $\mathcal{Q}$. C'est donc un élément de $\mathrm{Gal}(L/K)$ qui l'on appelle *symbole d'Artin* et que l'on note $(\mathcal{Q}, L/K)$. Cette définition se généralise par multiplicativité à tout idéal fractionnaire I de K qui est à support en dehors des idéaux premiers ramifiés de l'extension L/K.

On trouve dans certains ouvrages la formulation suivante de la loi de réciprocité d'Artin.

THÉORÈME 3. — *Soient K un corps de nombres et L une extension abélienne de K. Notons A l'anneau des entiers de K. Il existe une famille de nombres entiers $n_{\mathcal{Q}}$ indexée par les idéaux premiers de A telle qu'on ait la propriété suivante. Soit $x \in K$ tel que $x \in 1 + \mathcal{P}^{n_{\mathcal{P}}}$ ($\mathcal{P}$ idéal ramifié de L/K) et $i(x) > 0$ pour tout homomorphisme de corps $i : K \longrightarrow \mathbf{R}$ qui ne se prolonge pas en un homomorphisme de corps $L \longrightarrow \mathbf{C}$. On a $(xA, L/K) = 1$.*

Par ailleurs tout élément de $\mathrm{Gal}(L/K)$ est de la forme $(\mathcal{P}, L/K)$ pour une infinité d'idéaux premiers $\mathcal{P}$ de A.

On pourra essayer de faire le lien entre la première assertion du théorème 3 et le théorème 2. La deuxième assertion du théorème 3 est une conséquence du théorème de densité de Chebotarev.

Soit $\mathcal{M}$ un cycle arithmétique de K. Le sous-groupe de congruence de niveau $\mathcal{M}$ de C_K est fermé et d'indice fini. Il lui correspond donc une extension abélienne $H^{\mathcal{M}}$ de K par la loi de réciprocité d'Artin. Cette extension s'appelle le *corps de classe de rayon $\mathcal{M}$*. On a donc

$$\mathrm{Gal}(H^{\mathcal{M}}/K) \simeq C_K/C_K^{\mathcal{M}} \simeq \mathcal{C}\ell(K)^{\mathcal{M}},$$

où le dernier isomorphisme est déduit de la proposition 1.

Lorsque $\mathcal{M} = 1$, le corps de classe de rayon $\mathcal{M}$ est le *corps de classe de Hilbert de K*. C'est la plus grande extension abélienne $H|K$ qui est partout non ramifiée et telle que toute place réelle de K reste réelle dans H. On a alors un isomorphisme de groupes

$$\mathrm{Gal}(H/K) \simeq \mathcal{C}\ell(K).$$

Lorsque $\mathcal{M} = \prod_{v \in \Omega_{K,\infty}} \mathcal{P}_v$, le corps de classe de rayon $\mathcal{M}$ est le *corps de classe de Hilbert étendu de K*. C'est la plus grande extension abélienne et partout non ramifiée de K.

Ces assertions se vérifient facilement (en admettant tout ce qui précède) en comparant les lois de réciprocités locales et globales et en utilisant le critère de non ramification.

Mentionnons sans démonstration que tout idéal de K devient principal dans le corps de classe de Hilbert de K. C'est le *Hauptidealsatz* de Hilbert. La démonstration repose principalement sur des arguments de théorie des groupes.