Raconte-moi... le corps de classes

Tamás Szamuely

Les corps de classes sont les extensions finies galoisiennes d'un corps de nombres K dont le groupe de Galois est abélien. L'objectif de leur théorie est de les classifier en fournissant en même temps des renseignements sur leur comportement arithmétique. Du point de vue d'aujourd'hui l'importance de cette classification est qu'elle constitue un pas important vers la compréhension de cet objet plein de mystère qu'est le groupe de Galois absolu de K. Mais elle est en même temps le point culminant des recherches de quelques-uns des plus éminents arithméticiens du passé, il convient donc de commencer en jetant un regard en arrière.

Loi de réciprocité quadratique et symbole de Hilbert

L'histoire commence, comme souvent en arithmétique, avec Gauss, plus précisément avec sa loi de réciprocité quadratique. Rappelons que pour un nombre premier p et un entier b premier à p le *symbole de Legendre* $\left(\frac{b}{p}\right)$ vaut 1 si l'équation quadratique $x^2 = b$ admet une solution modulo p et -1 sinon. La loi de réciprocité quadratique est l'égalité

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\frac{b-1}{2}} \tag{1}$$

pour $a \neq b$ nombres premiers impairs. Elle est traditionnellement flanquée de ses deux lois supplémentaires : $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ et $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ pour p premier impair. Par multiplicativité du symbole de Legendre ces lois permettent un calcul facile du symbole quand b est fixé et p varie.

Hilbert a réinterprété la loi de réciprocité de Gauss comme une formule de produit en introduisant les symboles qui portent son nom. En langage moderne, on les définit en utilisant les complétés $\mathbf{R}$ et $\mathbf{Q}_p$ de $\mathbf{Q}$. Rappelons que les normes multiplicatives sur le corps $\mathbf{Q}$ sont, à des puissances près, les suivantes : la valeur absolue usuelle et, pour tout nombre premier p, la norme définie par $||a||_p := p^{-v_p(a)}$, où $v_p(a)$ est l'exposant de p dans la décomposition

primaire de a. En faisant converger les suites de Cauchy on obtient le corps $\mathbf{Q}_\infty := \mathbf{R}$ des réels dans le premier cas et les corps de nombres p-adiques $\mathbf{Q}_p$ dans le second. Ceci étant dit, on définit le symbole de Hilbert $(a,b)_p$ pour $a, b \in \mathbf{Q}_p \setminus \{0\}$ ($p = \infty$ inclus) comme étant 1 si l'équation $x^2 - ay^2 = b$ admet une solution non triviale en (x, y) et -1 sinon. La relation (non immédiate) avec le symbole de Legendre est la suivante : pour $b \in \mathbf{Z}$ premier à p et $p \neq 2, \infty$ on a

$$(a,b)_p = \left(\frac{b}{p}\right)^{v_p(a)}. \tag{2}$$

D'après Hilbert, pour $a, b \in \mathbf{Q} \setminus \{0\}$ on a la formule

$$\prod_p (a,b)_p = 1, \tag{3}$$

p parcourant l'ensemble des premiers et ∞ (le produit est fini par (2) ci-dessus). Pour $a \neq b$ nombres premiers impairs on a $(a,b)_p = 1$ pour $p \nmid 2ab$ ($p = \infty$ inclus) et (3) se réduit à (1) en vertu de la formule $(a,b)_2 = (-1)^{\frac{a-1}{2}\frac{b-1}{2}}$ qui s'établit aisément.

Hilbert a en outre montré que la formule (3) s'étend à un corps de nombres algébriques (i.e. une extension finie K de $\mathbf{Q}$), avec la seule différence qu'on considère les complétés K_P par rapport aux normes étendant les normes p-adiques et la valeur absolue usuelle sur $\mathbf{Q}$. Notant $\mathcal{O}_K$ l'anneau des entiers de K (i.e. le sous-anneau formé des éléments satisfaisant une équation polynomiale unitaire à coefficients entiers), les premières sont associées à des idéaux premiers $P \subset \mathcal{O}_K$ par un procédé analogue au cas $K = \mathbf{Q}$, et les secondes à la valeur absolue complexe après avoir choisi un plongement $K \hookrightarrow \mathbf{C}$.

Le passage à une extension finie K est également nécessaire si l'on veut généraliser la loi de réciprocité à des équations radicielles de degré supérieur. En effet, fixons $n \geq 2$ et supposons que K contient l'ensemble μ_n des racines n-ièmes de l'unité. Si $P \subset \mathcal{O}_K$ est un idéal premier ne contenant pas n, de corps résiduel $\mathcal{O}_K/P \cong \mathbf{F}_q$, la réduction modulo P identifie $\mu_n \subset \mathcal{O}_K$ à un sous-groupe du groupe multiplicatif $\mathbf{F}_q^\times$; en particulier, n divise $q-1$. Pour $b \in \mathcal{O}_K$ non contenu dans P le symbole $\left(\frac{b}{P}\right)_n := b^{\frac{q-1}{n}} \bmod P$ admet donc un sens comme élément de μ_n ; comme $\mathbf{F}_q^\times$ est cyclique, on a $\left(\frac{b}{P}\right)_n = 1$ si et seulement si l'équation $x^n = b$ est résoluble modulo P. Toujours sous les hypothèses ci-dessus sur K, P et b, le symbole de Hilbert se généralise au cas $n > 2$ en substituant $\left(\frac{b}{P}\right)_n$ à $\left(\frac{b}{p}\right)$ dans la formule (2). On peut montrer que ce symbole généralisé $(a,b)_P$ est égal à 1 si et seulement si b est le terme

constant du polynôme minimal d'un élément de $K_P(\sqrt[n]{a})$ sur K_P ; pour $n = 2$ on retrouve donc le symbôle de Hilbert classique sur $\mathbf{Q}_p$. Mais pour avoir une formule de produit comme dans (3) il faut savoir définir les symboles $(a, b)_P$ sans hypothèses restrictives.

Invariant de Hasse et loi de réciprocité d'Artin

Hasse a résolu ce problème en recourant à des méthodes d'algèbre non-commutative. Soit $E|F$ une extension galoisienne de corps, de groupe de Galois G cyclique d'ordre n. Fixant un générateur $\sigma \in G$ et un élément non nul $b \in F$, on définit *l'algèbre cyclique* $(E, b)_\sigma$ comme étant la F-algèbre associative engendrée par E et par un élément y satisfaisant les relations

$$y^n = b, \quad \lambda y = y\sigma(\lambda)$$

pour tout $\lambda \in E$. C'est une algèbre simple centrale sur F (i.e. elle ne contient pas d'idéal bilatère non trivial et son centre est F) ; sa dimension sur F est n^2. Dans le cas où $\mu_n \subset F$, on peut trouver un élément $x \in E$ tel que $x^n =: a \in F$ et $E = F(x)$. De plus, on sait que $\sigma(x) = \omega x$ avec une racine primitive ω de l'unité, d'où la présentation plus simple

$$(E, b)_\sigma = (a, b)_\omega := \langle x, y \,|\, x^n = a,\ y^n = b,\ xy = \omega yx \rangle.$$

Le cas particulier $n = 2$, $a = b = \omega = -1$ et $F = \mathbf{R}$ n'est autre que l'algèbre des quaternions de Hamilton.

Considérons maintenant le cas où $F = K_P$ est un corps p-adique. Soit π un générateur de l'idéal maximal de son anneau des entiers $\mathcal{O}_{K_P}$, et soit K_n l'unique extension non ramifiée de degré n de K_P (i.e. l'unique extension de degré n telle que π engendre l'idéal maximal de $\mathcal{O}_{K_n}$). Notons $Fr \in \mathrm{Gal}(K_n|K_P)$ la substitution de Frobenius, i.e. le générateur de $\mathrm{Gal}(K_n|K_P)$ qui se réduit modulo P au générateur $t \mapsto t^q$ de l'extension résiduelle (ici q est le cardinal de $\mathcal{O}_{K_P}/P$). On a alors le résultat fondamental de Hasse : *toute algèbre simple centrale A de dimension n^2 sur K_P est isomorphe à une algèbre cyclique de la forme* $(K_n, \pi^r)_{Fr}$, où $0 \leq r < n$ est un entier uniquement déterminé par A : c'est *l'invariant de Hasse* de A.

Dans le cas où $\mu_n \subset K_P$, on peut alors définir le symbole de Hilbert généralisé comme suit : on fixe un générateur $\omega \in \mu_n$, et pour $a, b \in K_P \setminus \{0\}$ on pose $(a, b)_P := \omega^{-r}$, où r est l'invariant de Hasse de l'algèbre cyclique $(a, b)_\omega$ définie ci-dessus. On peut montrer que cette définition redonne les cas particuliers considérés précédemment. C'est là un fait non trivial, mais ce

qui l'est encore moins, c'est la formule de produit

$$\prod_P (a,b)_P = 1 \tag{4}$$

pour $a, b \in K \setminus \{0\}$, où K est un corps de nombres contenant μ_n. (Noter que sous cette dernière hypothèse il n'y a pas de complété de K isomorphe à $\mathbf{R}$ si $n > 2$.) La formule (4) est une forme de la *loi de réciprocité d'Artin* : elle couvre toutes les lois de réciprocités particulières trouvées précédemment au cours du 19-ième siècle et résout le neuvième problème sur la célèbre liste de Hilbert.

Suite d'Albert–Brauer–Hasse–Noether

Dans le cas où K ne contient pas μ_n, on ne peut pas associer de symbole à deux éléments a, b de K, mais les arguments précédents se généralisent quand même. Rappelons que d'après un théorème de Wedderburn toute algèbre simple centrale A sur un corps F est isomorphe à une algèbre de matrices sur un corps gauche de centre F uniquement déterminé par A. Deux algèbres simples centrales A et B sont dites Brauer équivalentes si elles sont associées au même corps gauche. Le produit tensoriel $(A, B) \mapsto A \otimes_F B$ induit une structure de groupe abélien sur les classes d'équivalence de Brauer sur F ; c'est le groupe de Brauer $\mathrm{Br}(F)$ de F. Le groupe $\mathrm{Br}(F)$ est un groupe abélien de torsion, et les algèbres cycliques de dimension n^2 considérées ci-dessus en représentent des éléments d'ordre divisant n. Le théorème de Hasse cité ci-dessus se reformule ainsi : la partie de n-torsion de $\mathrm{Br}(K_P)$ est isomorphe à $\mathbf{Z}/n\mathbf{Z}$, l'isomorphisme étant induit par l'invariant de Hasse. Quand on fait varier n, ces isomorphismes se recollent en un isomorphisme $\mathrm{Br}(K_P) \cong \mathbf{Q}/\mathbf{Z}$ (ici on identifie $\mathbf{Z}/n\mathbf{Z}$ au sous-groupe $\frac{1}{n}\mathbf{Z}/\mathbf{Z}$ de $\mathbf{Q}/\mathbf{Z}$). Par ailleurs, d'après un théorème de Frobenius le groupe $\mathrm{Br}(\mathbf{R})$ est d'ordre 2, donc isomorphe à $\frac{1}{2}\mathbf{Z}/\mathbf{Z}$, la classe non triviale étant représentée par les quaternions de Hamilton.

Pour K un corps de nombres on a alors la suite exacte

$$0 \to \mathrm{Br}(K) \to \bigoplus_P \mathrm{Br}(K_P) \xrightarrow{\Sigma} \mathbf{Q}/\mathbf{Z} \to 0 \tag{5}$$

due a Brauer, Hasse, Noether et indépendemment à Albert. Ici K_P parcourt les divers complétés de K ($\mathbf{R}$ et $\mathbf{C}$ inclus – mais on sait que $\mathrm{Br}(\mathbf{C}) = 0$). Le morphisme Σ est la somme des morphismes $\mathrm{Br}(K_P) \to \mathbf{Q}/\mathbf{Z}$ décrits ci-dessus, et les morphismes $\mathrm{Br}(K) \to \mathrm{Br}(K_P)$ sont induits par les changements de base $A \mapsto A \otimes_K K_P$; c'est un fait non trivial que ces morphismes sont

nuls pour tout sauf un nombre fini de P. Dans le cas où $\mu_n \subset K$, on peut restreindre les morphismes de la suite au sous-groupe de $\mathrm{Br}(K)$ engendré par la classe d'une algèbre cyclique $(a,b)_\omega$ considérée ci-dessus et on retrouve la formule (4) en identifiant $\frac{1}{n}\mathbf{Z}/\mathbf{Z}$ à μ_n au moyen de la racine de l'unité ω. (En fait, une conséquence importante de la suite exacte (5) est que toute classe de $\mathrm{Br}(K)$ peut être représentée par une algèbre cyclique.)

Extensions abéliennes de corps p-adiques

On va expliquer maintenant comment les idées ci-dessus permettent de décrire les extensions abéliennes d'un corps de nombres. Commençons par la théorie locale. Soient K_P un corps p-adique et $L_P|K_P$ une extension galoisienne, de groupe de Galois cyclique engendrée par un élément σ. Étant donné un élément non nul $b \in K_P$, soit r l'invariant de Hasse de l'algèbre cyclique $(L_P, b)_\sigma$. On peut montrer que l'application $b \mapsto \sigma^r$ définit un homomorphisme canonique $\rho_{L_P|K_P}$ du groupe multiplicatif $K_P^\times$ de K_P dans le groupe de Galois $\mathrm{Gal}(L_P|K_P)$; de plus, si $M_P|K_P$ est une autre extension cyclique de K_P contenant L_P, le composé de $\rho_{M_P|K_P}$ avec la projection naturelle $\mathrm{Gal}(M_P|K_P) \to \mathrm{Gal}(L_P|K_P)$ n'est autre que $\rho_{L_P|K_P}$. Utilisant cette compatibilité on peut étendre la définition de $\rho_{L_P|K_P} : K_P^\times \to \mathrm{Gal}(L_P|K_P)$ au cas où $\mathrm{Gal}(L_P|K_P)$ est un groupe abélien fini quelconque : on écrit L_P comme le composé d'extensions cycliques $L_i|K_P$ et on 'recolle' les morphismes $\rho_{L_i|K_P}$. Enfin, en passant à la limite projective sur les groupes de Galois des extensions finies abéliennes $L_P|K_P$ contenues dans une clôture algébrique fixée $\overline{K}_P$ de K_P, on obtient un morphisme $\rho_{K_P} : K_P^\times \to \mathrm{Gal}(\overline{K}_P|K_P)^{\mathrm{ab}}$, où $\mathrm{Gal}(\overline{K}_P|K_P)^{\mathrm{ab}}$ est le plus grand quotient abélien du groupe de Galois absolu $\mathrm{Gal}(\overline{K}_P|K_P)$; c'est *l'application de réciprocité locale*. Le morphisme ρ_{K_P} est presqu'un isomorphisme : son noyau est trivial et son image est dense dans $\mathrm{Gal}(\overline{K}_P|K_P)^{\mathrm{ab}}$ pour la topologie profinie. Par contre, à niveau fini le morphisme $\rho_{L_P|K_P}$ est surjectif mais non injectif : son noyau est le groupe des normes $N_{L_P|K_P}(L_P^\times) \subset K_P^\times$.

Extensions abéliennes de corps de nombres

Pour traiter le cas d'un corps de nombres K, on considère, suivant Chevalley, le groupe I_K des *idèles* de K. C'est le sous-groupe du produit direct $\prod K_P^\times$ des groupes multiplicatifs de tous les complétés de K constitué des suites (a_P) où a_P est une unité p-adique (i.e. un élément de norme 1) pour tout sauf un nombre fini de P quand K_P est un corps p-adique. Le groupe multiplicatif $K^\times$ se plonge dans I_K par l'application diagonale ; le quotient $C_K := I_K/K^\times$

est le groupe des classes d'idèles de K. Maintenant si $L|K$ est une extension finie abélienne de K, elle induit pour tout P une extension locale $L_P|K_P$ dont le groupe de Galois s'identifie à un sous-groupe de $\mathrm{Gal}(L|K)$ (bien défini puisque $\mathrm{Gal}(L|K)$ est abélien). On considère pour tout P les applications $\rho_{L_P|K_P}$ décrites ci-dessus ; en outre, quand $L_P = \mathbf{C}$ et $K_P = \mathbf{R}$, on définit $\rho_{\mathbf{C}|\mathbf{R}} : \mathbf{R}^\times \to \mathrm{Gal}(\mathbf{C}|\mathbf{R})$ par $a \mapsto \tau^{(1-\mathrm{sgn}(a))/2}$, où τ est la conjugaison complexe. Noter que si $L_P|K_P$ est une extension non ramifiée de corps p-adiques et $u \in K_P^\times$ est une unité p-adique, on a $\rho_{L_P|K_P}(u) = 1$ (ceci résulte du fait que l'invariant de Hasse de la K_P-algèbre cyclique $(L_P, u)_{Fr}$ est 0). Comme $L_P|K_P$ est non ramifiée pour tout sauf un nombre fini de P, on peut donc définir une application $\rho_{L|K} : I_K \to \mathrm{Gal}(L|K)$ comme étant induite par le produit des applications $\rho_{L_P|K_P}$ pour tous les complétés K_P. De plus, $\rho_{L|K}$ est triviale sur l'image diagonale de $K^\times$ dans I_K grâce à la loi de réciprocité d'Artin. (Pour le voir, on se réduit au cas où $L|K$ est cyclique et pour $b \in K^\times$ on suit l'image de la classe de l'algèbre cyclique $(L, b)_\sigma$ par les morphismes de la suite (5).)

Ainsi, on obtient un morphisme $\overline{\rho}_{L|K} : C_K \to \mathrm{Gal}(L|K)$ et, faisant varier L et passant à la limite projective, un morphisme $\overline{\rho}_K : C_K \to \mathrm{Gal}(\overline{K}|K)^{\mathrm{ab}}$, avec les mêmes notations que dans le cas local. Ce morphisme, appelé *application de réciprocité globale*, est surjectif mais non injectif ; son noyau peut être décrit comme la composante connexe C_K^0 de 1 pour une topologie convenable sur C_K, induite par la topologie de produit restreint sur I_K par rapport aux groupes des unités p-adiques. En fait, l'isomorphisme $C_K/C_K^0 \xrightarrow{\sim} \mathrm{Gal}(\overline{K}|K)^{\mathrm{ab}}$ induit par $\overline{\rho}_K$ devient un isomorphisme de groupes topologiques quand on munit $\mathrm{Gal}(\overline{K}|K)^{\mathrm{ab}}$ de sa topologie profinie. La théorie de Galois infinie implique alors que les extensions finies abéliennes $L|K$ correspondent aux sous-groupes ouverts d'indice fini de $H \subset C_K$; classiquement, on appelle l'extension associée à un tel sous-groupe (un 'groupe de classes d'idèles') le *corps de classes* associé à H.

Corps de classes de rayon

Certains corps de classes ont une importance arithmétique particulière. Ils sont associés à des sous-groupes de congruence de C_K définis comme suit. Un *module* est un produit formel $\mathfrak{m} = \prod P^{n_P}$ où, comme précédemment, P correspond à un complété p-adique, réelle ou complexe K_P de K, et $n_P \geq 0$ est un entier, égal à 0 pour tout sauf un nombre fini de P. Pour K_P un corps p-adique on pose $U_P^0 = \mathcal{O}_{K_P}^\times$ et $U_P^{n_P} = 1 + P^{n_P}\mathcal{O}_{K_P}$ pour $n_P > 0$; pour $K_P = \mathbf{R}$ on déclare $U_P^0 = \mathbf{R}^\times$ et $U_P^{n_P} = \mathbf{R}_{>0}$ pour $n_P > 0$; enfin pour $K_P = \mathbf{C}^\times$ on a $U_P^{n_P} = \mathbf{C}$ pour tout n_P. Le produit $I_K^{\mathfrak{m}} := \prod_P U_P^{n_P}$

associé à $\mathfrak{m}$ est un sous-groupe de I_K ; on note $C_K^{\mathfrak{m}}$ son image dans C_K. Le fait fondamental est que les sous-groupes ouverts d'indice fini de C_K sont précisément ceux contenant un sous-groupe $C_K^{\mathfrak{m}}$ pour un $\mathfrak{m}$ convenable. En particulier, les sous-groupes $C_K^{\mathfrak{m}}$ sont ouverts d'indice fini et correspondent donc par le paragraphe précédent à des extensions finies abéliennes $K^{\mathfrak{m}}|K$; on les appelle *corps de classes de rayon*. Toute extension finie abélienne $L|K$ est donc contenue dans un corps de classes de rayon, ce qui permet d'obtenir des informations sur l'arithmétique de L, comme annoncé dans l'introduction. À titre d'exemple, un idéal premier P de $\mathcal{O}_K$ est ramifié dans L si et seulement si P apparaît avec un exposant non nul dans tout $\mathfrak{m}$ tel que $K^{\mathfrak{m}} \supset L$.

A ce point, la contrainte impitoyable de longueur nous oblige à mettre une fin abrupte à notre discussion. Nous sommes conscients du nombre astronomique des omissions, les plus cruelles étant sans doute le cas de caractéristique positive, les aspects analytiques, le lien avec le programme de Langlands, la théorie en dimension supérieure et maints autres développements plus récents. Qu'ils fassent l'objet de futurs articles !

Indications bibliographiques

De nos jours la théorie esquissée ci-dessus est présentée par des méthodes cohomologiques. Pour la théorie locale, le classique [4] de Serre est toujours d'actualité ; pour un aperçu complet récent voir [3]. Pour le point de vue des algèbres simples centrales, voir [2] ; pour les aspects historiques un bon point de départ (qui m'a été bien utile) est [1].

[1] K. Conrad, *History of class field theory*, disponible sur la page personnelle de l'auteur.

[2] P. Gille, T. Szamuely, *Central simple algebras and Galois cohomology*, 2nd ed., Cambridge University Press, 2017.

[3] D. Harari, *Cohomologie galoisienne et théorie du corps de classes*, EDP Sciences, 2017.

[4] J–P. Serre, *Corps locaux*, Hermann, Paris, 1962.