Introduction aux travaux de Jacques Herbrand

Toulouse, 19-22 avril 2022

Photographie de J. Herbrand, probablement prise par Natascha Artin

Jacques Herbrand *(au centre)*
au cours de l'excursion où il trouva la mort

(Cl. Suzanne Lautman.)

Quelques dates

12 février 1908. Naissance de Jacques Herbrand à Paris. Il est enfant unique. Son père, d'origine belge, est négociant en tableaux anciens.

1924? J.H. passe le concours général. Il est classé premier.

Septembre 1925 J.H. entre à l'ENS, classé premier. Il suit peu de cours mais fréquente régulièrement le Séminaire Hadamard au collège de France. Il se lie d'amitié avec C. Chevalley, entré un an après lui. À l'ENS il rencontre aussi A. Weil, A. Lautman et J. Dieudonné. J.H. lit les Principia Mathematica et s'intéresse à la logique mathématique.

1928 J.H passe l'agrégation, encore classé premier. Il commence à travailler à sa thèse, sous la direction (nominale) d'Ernest Vessiot, alors directeur de l'ENS.

Avril 1929 J.H. soumet sa thèse, intitulée *Recherches sur la Théorie de la Démonstration.* Elle est acceptée le 20 juin mais la soutenance de thèse n'a lieu qu'un année plus tard, le 11 juin 1930. Les rapporteurs de la thèse sont A. Denjoy et M. Fréchet.

Octobre 1929. Début du service militaire, qui dure une année.

1930-1931. Séjour en Allemagne financé par une bourse Rockefeller. J.H. se tourne vers la théorie des nombres. Il rencontre E. Noether à Halle, P. Bernays et D. Hilbert à Berlin, R. Courant à Götttingen et H. Hasse à Marburg. J.H. correspond abondamment avec H. Hasse pendant cette période et écrit aussi deux lettres à K. Gödel.

27 juillet 1931 Mort lors d'une excursion en montagne près du hameau de la Bérarde dans l'Isère.

Travaux

[1928] *Sur la théorie de la démonstration.*
C.R.A.S. 186:1274–1276, 1928.

[1929a] *Non-contradiction des axiomes arithmétiques.*
C.R.A.S. 188:303–304, 1929.

[1929b] *Sur quelques propriétés des propositions vraies et leurs applications.*
C.R.A.S. 188:1076–1078, 1929.

[1929c] *Sur le problème fondamental des mathématiques.*
C.R.A.S. 189:554–556, 1929.

[1930a] *Thèses présentées à la faculté des Sciences de Paris pour obtenir le grade de docteur ès sciences mathématiques.*
1ère thèse : Recherches sur la Théorie de la Démonstration. 2ème thèse : propositions données par la faculté, Les Équations de Fredholm. Soutenues le 11 juin 1930 devant la commission d'examen. Président: M. Vessiot, Examinateurs: MM. Denjoy, Fréchet.

[1930b] *Les bases de la logique hilbertienne.*
Revue de Métaphysique et de Morale 37:243–255, 1930.

[1930c] *Nouvelle démonstration et généralisation d'un théorème de Minkowski.*
C.R.A.S. 191:1282–1285, 1930.

[1931a] *Sur le problème fondamental de la logique mathématique.*
Revue de Métaphysique et de Morale 24:12–56, 1931.

[1931b] *Sur la théorie des corps de nombres de degré infini.*
C.R.A.S. 193:594, 1931.

[1931c] (avec C. Chevalley) *Nouvelle démonstration du théorème d'existence en théorie du corps de classes.*
C.R.A.S. 193:814–815, 1931.

[193d] *Sur la théorie des groupes de décomposition, d'inertie et de ramification.*
J. de Math. Pures et Appliquées (J. Liouville) 9:481–498, 1931.

[1932a] *Sur la non-contradiction de l'Arithmétique.*
Crelle 166:1–8, 1932.

[1932b] *Sur les classes des corps circulaires.*
J. de Math. Pures et Appliquées (J. Liouville) 9:417–441, 1932.

[1932c] *Sur les théorèmes du genre principal et des idéaux principaux.*
Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg 9:84–92, 1932.

[1932d] *Théorie arithmétique des corps de nombres de degré infini – I. Extensions algébriques finies de corps infinis.*
Math. Ann. 106:473–501, 1932.

[1932e] *Une propriété du discriminant des corps algébriques.*
Annales de l'ENS 49:105–112, 1932.

[1932f] *Zur Theorie der algebraischen Funktionen.*
Math. Ann. 106:502, 1932.

[1933] *Théorie arithmétique des corps de nombres de degré infini – II. Extensions algébriques de degré infini.*
Math. Ann. 108:699–717, 1933.

[1936] *Le Développement Moderne de la Théorie des Corps Algébriques – Corps de classes et lois de réciprocité.*
Mémorial des Sciences Mathématiques, Fascicule LXXV.
Gauthier-Villars, Paris, 1936. Avec un appendice de C. Chevalley.

[1968] *Écrits Logiques.*
P.U.F., Paris, 1968. Ed. par Jean van Heijenoort.

Correspondance. Apparemment non publiée (?)

Principales sources

Proceedings of the Herbrand symposium. Logic colloquium 81. Held in Marseille, July 16–24, 1981.
Edited by J. Stern. Studies in Logic and the Foundations of Mathematics, 107. North-Holland Publishing Co., Amsterdam, 1982. xi+384 pp.

Actes du colloque Jacques Herbrand (Paris, février 2008).
Gazette de la SMF 118. Avec des contributions de G. Comte, T. Coquand, U. Kohlenbach et K.A. Ribet.

L'article de C.-P. Wirth, J. Siekmann, C. Benzmüller et S. Autexier

Jacques Herbrand: life, logic, and automated deduction.
Handbook of the history of logic. Vol. 5. Logic from Russell to Church, 195–254, Elsevier/North-Holland, Amsterdam, 2009.

recense une très grand nombre de travaux sur J. Herbrand et son héritage scientifique.

Aperçu des travaux de J. Herbrand

Les contributions principales de J.H. sont

(1) Une construction d'une procédure de décision pour des énoncés en logique du premier ordre. Cette construction est le point de départ de la théorie de la démonstration automatique et a donné lieu à de nombreux travaux en informatique théorique.

(2) Un raffinement du théorème de Kummer reliant les nombres de Bernoulli aux groupes de classes des corps cyclotomiques.

(3) Une nouvelle approche au théorème principal de la théorie du corps de classe et une nouvelle démonstration du théorème de la norme de Hasse.

(4) L'usage systématique de limites inductives et projectives dans l'étude d'extensions infinies de corps.

(5) Une formule dans la théorie de la ramification des corps locaux.

Prérequis pour ce cours.

• Connaissance du language de la logique du premier ordre (symboles logiques, quantificateurs, déduction formelle).

• Connaissance du langage des anneaux et des corps (par ex. idéaux, polynômes, quotient d'un anneau par un idéal).

• Notions de bases en algèbre linéaire (par ex. matrices, déterminants).

Plan du cours.

Nous allons passer en revue

(1) Le théorème de Herbrand en théorie de la preuve.

(2) Les résultats de Herbrand sur les groupes de classes des corps cyclotomiques.

(3) Le lemme de Herbrand.

(4) Le théorème de la norme de Hasse.

(5) La théorie du corps de classe. Application du lemme de Herbrand au théorème de la norme de Hasse.

Il est possible que je ne parvienne pas à couvrir tout le matériel. Je compte privilégier la clarté sur la quantité.

Deux extraits de la notice nécrologique de C. Chevalley et A. Lautman

"Il aimait en effet extrêmement la philosophie, la philosophie des sciences tout d'abord, mais aussi et surtout celle qui traite abstraitement des sentiments et des désirs de l'âme. Il n'y cherchait pas un système de l'homme; le problème pratique ne l'intéressait pas; il n'en parlait, ni n'en discutait jamais. Il était pris par un travail incessant d'analyse intérieure et recherchait dans cette attitude de tension morale soutenue la difficile rigueur qui fut le constant désir de son être. Sa pensée gardait ainsi toujours le même idéal, soit qu'il se récitât la *prose pour des Esseintes*, soit qu'il se mît à l'étude de l'arithmétique ou de l'algèbre moderne."

"Cette pratique toujours poursuivie de la pensée rigoureuse allait ainsi, de l'avis de tous, donner au monde savant un de ses grands esprits, mais il semblait à Herbrand, certains jours, qu'elle entraînait sa conscience dans un monde aussi stérile que le vide qu'il trouvait parfois au plus profond du dépouillement de lui-même. Il souffrait de la dure loi qui l'engageait sans trêve dans ces abstractions, où il sentait son être disparaître comme dans une mort; et c'est dans un espoir de pleine harmonie intérieure qu'il formait le projet d'une vie héroïque où soutenir le génie de son esprit. Cette plénitude de joie et d'ardeur dont il se croyait parfois privé pour toujours, c'est dans les émotions puissantes de la haute montagne qu'il s'en approchait le plus. Il est mort dans une ascension, et toutes ces pensées qu'il avait formées, tous ces sentiments qu'il avait éprouvés, il ne les poursuivra plus; mais ses amis en avaient tant compris près de lui la sublime beauté qu'ils ne pourront jamais s'écarter des voies que leur montrait cet être adoré."

Un extrait de l'article de J.H. *Les bases de la logique Hilbertienne*

"... mais il ne faut pas se cacher que le rôle des mathématiques est peut-être uniquement de nous fournir des raisonnements et des formes, et non pas de chercher quels sont ceux qui s'appliquent à tel objet. Pas plus que le mathématicien qui étudie l'équation de propagation des ondes n'a à se demander si, dans la nature, les ondes satisfont effectivement à cette équation; pas plus, en étudiant la théorie des ensembles ou l'arithmétique, il ne doit se demander si les ensembles ou les nombres auxquels il pense intuitivement satisfont bien aux hypothèses de la théorie qu'il considère. Il doit se borner à développer les conséquences de ces hypothèses et à les présenter de la manière la plus suggestive; le reste est le rôle du physicien ou du philosophe."

Le théorème de Herbrand en théorie de la preuve

Je suppose connu la notion de formule et de proposition en logique du 1er ordre avec quantificateurs. Voici un peu de terminologie:

- Un *terme* est une variable, une constante ou une expression du type $f(t_1, \ldots, t_n)$, où f est une fonction et les t_i sont des termes.
- Un *atome* est une expression du type $P(t_1, \ldots, t_n)$, où P est un prédicat et les t_i sont des termes.
- Un *littéral* est un atome ou la négation d'un atome.
- Une *clause* est une disjonction de littéraux.
- Une formule est en forme *prenex* si elle est de la forme

$$(Q_1 x_1)(Q_2 x_2) \ldots (Q_n x_n) W$$

où W est une formule sans quantificateurs et Q_i est soit $\forall$ ou $\exists$.

Lemme. Soit W une formule. Alors W est équivalente à une formule sous forme prenex

$$(Q_1 x_1)(Q_2 x_2) \ldots (Q_n x_n) V$$

où V est une conjonction de clauses.

La "skolemisation" décrit une procédure pour obtenir une formule comme dans le lemme, qui a de plus la propriété que $Q_i = \forall$ pour tout i. L'idée est d'introduire des fonctions supplémentaires pour éliminer les quantificateurs existentiels.

Au lieu d'en donner une description abstraite, nous allons considérer un exemple. La méthode générale s'en extrapole facilement.

Exemple de skolemisation. Considérons la formule

$$(\exists x)(\forall y)(\forall z)(\exists u)(\forall v)(\exists w)P(x, y, z, u, v, w)$$

Pour éliminer le $\exists x$ on introduit une nouvelle constante c et on obtient la formule équivalente

$$(\forall y)(\forall z)(\exists u)(\forall v)(\exists w)P(c, y, z, u, v, w)$$

Pour éliminer $\exists u$ on introduit une nouvelle fonction f à deux variables et on obtient

$$(\forall y)(\forall z)(\forall v)(\exists w)P(c, y, z, f(y, z), v, w)$$

Pour finir, on introduit une nouvelle fonction à trois variables g et on obtient

$$(\forall y)(\forall z)(\forall v)P(c, y, z, f(y, z), v, g(y, z, v))$$

On voit donc que pour toute formule, il existe une formule (effectivement calculable) équivalente de la forme

$$(\forall x_1)(\forall x_2)\ldots(\forall x_n)W$$

où W est une formule sans quantificateurs, qui est une conjonction de clauses.

Si on cherche une procédure générale pour démontrer ou infirmer une formule, on peut donc se restreindre à des formules de ce type.

L'univers de Herbrand

Soit S un ensemble de clauses. On va chercher à construire un modèle (un univers) adapté à S.

L'univers de Herbrand de S est formé de la façon suivante.

Si aucune constante n'apparaît dans S, on définit $H_0 = \{a\}$. Sinon H_0 consiste en l'ensemble des constantes apparaissant dans S.

Pour $i \geq 1$, on définit l'ensemble H_i comme l'union de H_{i-1} avec l'ensemble des $f(t_1, \ldots, t_n)$, où f est une fonction apparaissant dans S et $t_1, \ldots, t_n \in H_{i-1}$.

Par exemple, si $S = \{P(a), P(f(x))\}$ alors

$$H_0 = \{a\}$$

$$H_1 = \{a, f(a)\}$$

$$H_2 = \{a, f(a), f(f(a))\} \quad \text{etc.}$$

L'univers de Herbrand de S est $\cup_{i \geq 0} H_i$.

Modèles de Herbrand

Un *modèle de Herbrand* de S est un modèle de S dont l'ensemble sous-jacent est H et tel que pour toute fonction $f(t_1, \ldots, t_n)$ apparaissant dans S et $m_1, \ldots m_n \in H_i$, l'évaluation de f en $m_1, \ldots m_n$ soit $f(m_1, \ldots, m_n) \in H_{i+1}$, pour tout $i \geq 0$.

On notera que les prédicats de S ne sont pas fixés dans H (seulement les fonctions).

Lemme. Si S a un modèle alors S a un modèle de Herbrand.

Preuve. Soit M un modèle de S. Il y a une application naturelle $\phi : H \to M$, qui envoie les constantes de S dans leurs réalisations dans M et qui est compatible aux réalisations des fonctions sur H et M. Pour tout prédicat $P(t_1, \ldots, t_n)$ apparaissant dans S, et tout $h_1, \ldots, h_n \in H$ on définit la réalisation P_H de P dans H par la formule

$$P(h_1, \ldots, h_n) = P_M(\phi(h_1), \ldots, \phi(h_n))$$

où P_M est la réalisation de P dans M. Ceci fait de H un modèle de S.■

Corollaire. (théorème de Löwenheim-Skolem)
Si S est dénombrable alors S a un modèle dénombrable.

Preuve. Le modèle de Herbrand de S est alors dénombrable par construction.

N.B. Les travaux de Löwenheim et Skolem sont cités par Herbrand. Voir l'article de Wirth, Siekmann, Benzmüller et Autexier, par. 3.12 pour une discussion du point de vue de J.H. sur le théorème de Löwenheim-Skolem.

La théorie propositionnelle associée au modèle de Herbrand

Définition. On définit $E(S)$ comme l'ensemble des évaluations des éléments de S pour toutes les valeurs possibles de leurs variables en des éléments de H, où H est l'univers de Herbrand de S.

On voit $E(S)$ comme un ensemble de clauses sans variables.

Une clause sans variable peut-être vue comme un énoncé purement propositionnel (ie sans variable ni constante).

Exemple. $(P(a) \vee Q(f(a))) \wedge (P(f(a)) \vee Q(f(a)))$ peut être vu comme la proposition

$$(P_1 \vee P_2) \wedge (P_3 \vee P_2).$$

Lemme. S est satisfaisable ssi $E(S)$ est satisfaisable vu comme ensemble d'énoncés propositionnels.

Esquisse de preuve. Si $E(S)$ est satisfaisable comme ensemble d'énoncés propositionnels alors on peut utiliser la détermination des valeurs de vérité de $E(S)$ pour construire un modèle de Herbrand H pour S (ie déterminer les valeurs des prédicats de S dans H). Réciproquement, si S est satisfaisable, alors S a un modèle, et donc un modèle de Herbrand par le lemme ci-dessus et on peut alors tirer des valeurs de vérité pour $E(S)$ de ce modèle.

Illustration. Soit $S = \{Q(y), P(f(x))\}$. Alors

$$H = \{a, f(a), f(f(a)), \dots\}$$

et

$$E(S) = \{P(f(a)), P(f(f(a))), \dots\} \cup \{Q(a), Q(f(a)), \dots\}$$

Si $E(S)$ est satisfaisable vu comme ensemble d'énoncés propositionnels, on peut par définition donner des valeurs de vérité à tous les éléments de $E(S)$ telles que la table de vérité de tous sous-ensemble fini de $E(S)$ n'est pas celle d'une contradiction.

On sait donc calculer la valeur de vérité de Q pour tous les éléments de H mais pas celle de P (il manque la valeur en a). On donne alors simplement une valeur arbitraire à P en a.

Corollaire. Soit S un ensemble de clauses. Alors S n'est pas satisfaisable ssi $E(S)$ a un sous-ensemble fini qui n'est pas satisfaisable comme ensemble d'énoncés propositionnels.

Preuve. Par le lemme, S n'est pas satisfaisable ssi $E(S)$ n'est pas satisfaisable. Par ailleurs $E(S)$ n'est pas satisfaisable ssi $E(S)$ a un sous-ensemble fini qui n'est pas satisfaisable au vu du théorème de compacité de la logique propositionnelle.

N.B. J.H. donne une preuve "finitiste" de cet énoncé (n'utilisant pas le théorème de compacité, qui n'était d'ailleurs pas encore connu à son époque). Cette preuve contient des erreurs, voir

Dreben, Burton; Andrews, Peter; Aanderaa, Stål
False lemmas in Herbrand. Bull. Amer. Math. Soc. 69 (1963), 699–706

et aussi la discussion de ces erreurs par J. van Heijenoort dans la préface des *Écrits logiques*.

Théorème de Herbrand. (reformulation concrète du corollaire) Si un ensemble de clauses est contradictoire (ie n'est pas satisfaisable) alors on peut exhiber une contradiction propositionnelle en remplaçant dans certaines clauses les variables par des itérations d'évaluations de fonctions en les constantes (ou en une constante artificielle si S n'a pas de constantes).

Exemple trivial. Soit $S = \{P(x), \sim P(a)\}$. Si on évalue x en a on obtient

$$P(a) \wedge (\sim P(a))$$

qui est une contradiction propositionnelle. Donc S est contradictoire.

Un exemple plus complexe donné par T. Coquand

4.1. Théorème fondamental, exemple

Voici un exemple simple qui illustre le Théorème Fondamental. Étant donnés trois symboles de constantes a, b et c et un symbole de fonction f à deux arguments et le symbole de relation $\leqslant$, considérons la théorie :

$$\forall x\, y\, z.\ x \leqslant y \wedge y \leqslant z \ \rightarrow\ x \leqslant z, \quad \forall x.\ x \leqslant x, \ \forall x\, y.\ x \leqslant f(x,y), \ \forall x\, y.\ y \leqslant f(x,y)$$

$$\forall x.\ \neg(a \leqslant x \wedge b \leqslant x \wedge c \leqslant x)$$

Celle-ci exprime que $\leqslant$ est une relation de préordre, que f majore ces deux arguments et que a, b et c ne sont pas majorés par un même élément. C'est une théorie contradictoire. De manière sémantique, si on a un préordre et un majorant pour deux éléments, on a un majorant pour trois éléments et donc le dernier axiome est incompatible avec les précédent. Le Théorème Fondamental dit que l'on doit observer cette contradiction à un niveau purement propositionnel en regardant les instantiations closes de ces axiomes. En effet parmi ces instantiations, nous avons

$$a \leqslant f(a,b), \quad b \leqslant f(a,b), \quad f(a,b) \leqslant f(f(a,b),c), \quad c \leqslant f(f(a,b),c)$$

$$a \leqslant f(a,b) \wedge f(a,b) \leqslant f(f(a,b),c) \rightarrow a \leqslant f(f(a,b),c)$$

$$b \leqslant f(a,b) \wedge f(a,b) \leqslant f(f(a,b),c) \rightarrow b \leqslant f(f(a,b),c)$$

$$\neg(a \leqslant f(f(a,b),c) \wedge\ b \leqslant f(f(a,b),c) \wedge\ c \leqslant f(f(a,b),c))$$

qui sont contradictoires de manière purement propositionnelle (sans faire intervenir d'énoncés quantifiés).

Le théorème de Herbrand peut être implémenté sur un ordinateur.

Supposons donné un ensemble fini de clauses S.

On considère les sous-ensembles H_i de l'univers de Herbrand H de S et on forme toutes les propositions de $E(S)$ obtenues en évaluant les variables des clauses de S en des éléments de H_i. On cherche ensuite des contradictions propositionnelles parmi ces propositions.

L'un des premiers articles en informatique théorique décrivant cette procédure est

Gilmore, P. C. *A proof method for quantification theory: its justification and realization*. IBM J. Res. Develop. 28–35 (1960)

On notera que le nombre de formules à considérer augmente très rapidement et que la méthode des tables de vérités est exponentielle en le nombre de propositions.

On cherche donc des méthodes plus efficaces pour trouver des contradictions propositionnelles et aussi pour réduire d'emblée le nombre de propositions à considérer.

Un grand progrès a été fait ici avec le *Principe de Résolution* de Robinson, voir

Robinson, J. A.: *A machine oriented logic based on the resolution principle.* J. ACM 12, no. 1, 23–41 (1965).

Le théorème de Herbrand est lié au théorème d'élimination des coupures de Gentzen (le "Hauptsatz"), voir

Gerhard G.: *Untersuchungen über das logische Schliessen.* Mathematische Zeitschrift 39:176–210, 405–431 (1935).

La plupart des preuves modernes du théorème de Herbrand se fondent sur le théorème d'élimination des coupures. Voir par ex. par. 2.5.1 dans

S. R. Buss, *An Introduction to Proof Theory* in Handbook of Proof Theory, S. R. Buss, Ed., Elsevier, vol. 137, pp. 1–78 (1998).

Le théorème de Herbrand sur les groupes de classe des corps cyclotomiques

Soit $K \subseteq \mathbb{C}$ un corps de nombres.

Concrètement, il s'agit d'un corps de la forme $\mathbb{Q}[x]/(P(x))$ où $P(x) \in \mathbb{Q}[x]$ est un polynôme irréductible (ie qui ne peut s'écrire comme un produit de polynômes de plus petit degré). On notera que K est alors en particulier un $\mathbb{Q}$-espace vectoriel de dimension finie $\deg(P)$.

Soit $\mathcal{O}_K \subseteq K$ l'ensemble des éléments annulés par un polynôme à coefficients dans $\mathbb{Z}$ et de coefficient dominant 1. On peut montrer que c'est un sous-anneau de K.

Example. Si $\mathbb{Q}(i) = \mathbb{Q}[x]/(x^2+1)$ alors

$$\mathbb{Z}[i] := \{a + b \cdot i \mid a, b \in \mathbb{Z}\} = \mathcal{O}_{\mathbb{Q}(i)}$$

L'anneau $\mathbb{Z}[i]$ s'appelle l'anneau des entiers de Gauss.

Le *groupe des classse* $\mathrm{Cl}(\mathcal{O}_K) = \mathrm{Cl}(K)$ de $\mathcal{O}_K$ est l'ensemble des classes d'isomorphie de $\mathcal{O}_K$-modules projectifs de rang 1, muni du produit donné par le produit tensoriel.

Le produit sur $\mathrm{Cl}(K)$ munit cet ensemble d'une structure de groupe, dont l'unité est la classe d'isomorphie de $\mathcal{O}_K$. L'inverse d'un $\mathcal{O}_K$-module projectif de rang 1 est alors donné par son dual.

On peut décrire $\mathrm{Cl}(K)$ en terme des idéaux de l'anneau $\mathcal{O}_K$. Chaque idéal de $\mathcal{O}_K$ est un $\mathcal{O}_K$-module projectif de rang 1 et définit donc un élément de $\mathrm{Cl}(K)$. Réciproquement tout $\mathcal{O}_K$-module projectif de rang 1 est isomorphe à un idéal de $\mathcal{O}_K$.

Le *groupe de Galois* $\mathrm{Gal}(K|\mathbb{Q})$ de K est l'ensemble des automorphismes de K en tant que corps, muni de sa structure de groupe naturelle.

Si $K = \mathbb{Q}[x]/(P(x))$ comme plus haut alors l'orbite de l'élément $x(\mathrm{mod}(P(x))$ sous $\mathrm{Gal}(K|\mathbb{Q})$ est fini, car il consiste en racines de $P(x)$ et ces dernières sont en nombre fini.

Par ailleurs, un élément $\gamma \in \mathrm{Gal}(K|\mathbb{Q})$ agit trivialement sur $x(\mathrm{mod}(P(x))$ ssi γ est l'identité. On a donc une identification

$$\mathrm{Gal}(K|\mathbb{Q}) \simeq \mathrm{Orb}(x(\mathrm{mod}(P(x)))$$

et $\mathrm{Gal}(K|\mathbb{Q})$ est ainsi un groupe fini.

Le groupe $\mathrm{Gal}(K|\mathbb{Q})$ préserve $\mathcal{O}_K$. Par ailleurs $\mathrm{Gal}(K|\mathbb{Q})$ agit naturellement sur $\mathrm{Cl}(K)$ par la formule

$$\gamma(I) := I \otimes_{\mathcal{O}_K,\gamma} \mathcal{O}_K$$

où $\mathcal{O}_K$ à droite est vu comme un $\mathcal{O}_K$-module via γ.

Si $I \subseteq \mathcal{O}_K$ est un idéal, alors $\gamma(I)$ est isomorphe comme $\mathcal{O}_K$-module à l'image de I par γ (qui est aussi un idéal).

Par ailleurs on peut montrer

Théorème (H. Minkowski) Le groupe des classes $\mathrm{Cl}(K)$ est fini.

La démonstration du théorème repose sur un théorème de Minkowski sur les réseaux euclidiens.

Le corps cyclotomiques

Un *corps cyclotomique* est un corps de nombres de la forme $\mathbb{Q}(e^{2i\pi/n})$ avec $n \geq 1$.

Exemple. $\mathbb{Q}(i)$ est un corps cyclotomique (pour $n = 4$).

N.B. On peut montrer (c'est difficile) que l'ordre du groupe des classes de $\mathbb{Q}(e^{2i\pi/n})$ tend vers l'infini lorsque n tend vers l'infini.

On dispose d'un homomorphisme de groupes naturel

$$\phi : \mathrm{Gal}(\mathbb{Q}(e^{2i\pi/n}|\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^*$$

donné par la formule $\gamma(e^{2i\pi/n}) = e^{2i\phi(\gamma)\pi/n}$.

On peut montrer que ϕ est bijectif.

Le groupe $(\mathbb{Z}/n\mathbb{Z})^*$ agit donc naturellement sur $\mathrm{Cl}(\mathbb{Q}(e^{2i\pi/n}))$.

Le théorème de Herbrand concerne la structure galoisienne du groupe des classes d'un corps cyclotomique de la forme $\mathbb{Q}(e^{2i\pi/p})$, où p est un nombre premier.

Pour le formuler, nous aurons encore besoin d'une définition et de deux résultats d'algèbre linéaire.

Les *nombres de Bernoulli* $B_i \in \mathbb{Q}$ sont définis par la formule

$$\frac{x}{e^x - 1} = \sum_{n=0}^{\infty} B_n x^n / n!$$

Par exemple, $B_0 = 1$, $B_4 = -1/30$, $B_{12} = -691/2730$. Les nombres de Bernoulli d'indice n impair avec $n > 1$ sont tous nuls.

Les nombres de Bernoulli sont aussi liés à la fonction zêta de Riemann

$$\zeta(s) = \sum_{n \geq 1} n^{-s}$$

($s \in \mathbb{C}$) par la formule

$$B_n = -n\zeta(1 - n)$$

valable pour $n > 1$.

Lemme. Soit $n \geq 1$ and p un nombre premier. Pour chaque élément e de $(\mathbb{Z}/p\mathbb{Z})^*$, il existe un unique élément $\bar{e} \in \mathbb{Z}/p^n\mathbb{Z}$ tel que $\bar{e}(\mathrm{mod}\, p) = e$ et $\bar{e}^{p-1} = 1$.

La démonstration est une application du "lemme de Hensel". On déduit du lemme que l'opération $e \mapsto \bar{e}$ définit un homomorphisme de groupe $(\mathbb{Z}/p\mathbb{Z})^* \to (\mathbb{Z}/p^n\mathbb{Z})^*$, appelé *caractère de Teichmüller*.

Lemme. Soit M un groupe abélien annulé par p^n $(n \geq 1)$. Supposons que $(\mathbb{Z}/p\mathbb{Z})^*$ agit sur M. Alors on a

$$M = \bigoplus_{k=0}^{p-2} M_k$$

où $e \in (\mathbb{Z}/p\mathbb{Z})^*$ agit par $\bar{e}^k$ sur M_k.

La démonstration du lemme suit essentiellement du fait que l'action de $(\mathbb{Z}/p\mathbb{Z})^*$ se "diagonalise" sur M parce que l'ordre $\#(\mathbb{Z}/p\mathbb{Z})^* = p - 1$ de $(\mathbb{Z}/p\mathbb{Z})^*$ est premier à p.

Théorème de Herbrand. Soit $p > 2$ un nombre premier et A le plus grand sous-groupe de $\mathrm{Cl}(\mathbb{Q}(e^{2i\pi/p}))$ qui est annulé par une puissance de p. Supposons que $A_k \neq 0$, où $k \in \{3, \ldots, p-2\}$ est un nombre impair et A_k est comme dans le précédent lemme. Alors p divise B_{p-k}.

On peut montrer qu'on a toujours $A_0 = A_1 = 0$. Qu'en est-il des A_k où k est pair ? À ce sujet, on a la

Conjecture.(Vandiver(-Kummer)) Soit $k \in \{0, \ldots, p-3\}$ un nombre pair. Alors $A_k = 0$.

On peut montrer qu'une forme équivalente de la conjecture de Vandiver est l'énoncé que p ne divise pas l'ordre du groupe des classes de $\mathbb{Q}(e^{2i\pi/p} + e^{-2i\pi/p})$. Ceci est démontré pour tout $p < 2^{31}$. Kurihara a démontré que $A_{p-3} = 0$.

Corollaire.(démontré par Kummer) Si p divise l'ordre de $\mathrm{Cl}(\mathbb{Q}(e^{2i\pi/p}))$ alors p divise B_{p-k} pour un entier $k \in \{3, \ldots, p-2\}$ impair.

Compléments

Kummer a introduit la notion d'idéal et démontré le précédent corollaire dans le cadre de ses recherches sur le dernier théorème de Fermat. On dit qu'un nombre premier est *régulier* si p ne divise pas l'ordre de $\mathrm{Cl}(\mathbb{Q}(e^{2i\pi/p}))$.

Théorème. (Kummer) Supposons que $p > 2$ est un nombre premier régulier. Si x, y, z sont des entiers premiers à p alors

$$x^p + y^p \neq z^p.$$

Les travaux d'Eichler, Brückner et Skula ont montré plus tard que la même conclusion est vérifiée si le nombre

$$\#\{\text{nombres de Bernoulli de la forme } B_{p-k} \text{ avec } k \in \{3, \ldots, p-2\} \text{ impair}\}$$

est $< \sqrt{p} - 2$.

En 1976, K. Ribet a démontré la réciproque du théorème de Herbrand:

Théorème. Soit $p > 2$ un nombre premier et A le plus grand sous-groupe de $\mathrm{Cl}(\mathbb{Q}(e^{2i\pi/p}))$ qui est annulé par une puissance de p. Supposons que p divise B_{p-k}, où $k \in \{3, \ldots, p-2\}$ est un nombre impair. Alors $A_k \neq 0$.

La démonstration de Ribet passe par la théorie du corps de classe, dont nous parlerons plus tard. Cette théorie permet de ramener la démonstration (via le "corps de classe de Hilbert") à la construction d'une certaine extension non-ramifiée de $\mathbb{Q}(e^{2i\pi/p})$. Cette extension est alors construite de manière géométrique, en utilisant des formes modulaires.

(1) On peut montrer que la conjecture de Vandiver implique le théorème de Ribet. Plus précisément, la conjecture de Vandiver implique que dans la situation du théorème, A_k est un groupe cyclique dont l'ordre est donné par p^m, où m est donné par une formule explicite contenant une combinaison linéaire de puissances du caractère de Teichmüller.

(2) Un résultat profond de B. Mazur et A. Wiles (lié à leur démonstration de la "conjecture principale de la théorie d'Iwasawa") montre que l'ordre de A_k est bien p^m (mais ne montre pas que A_k est cyclique).

(3) A. Kolyvagin a donné une preuve élémentaire (non géométrique) du théorème de Ribet comme application de sa théorie des "systèmes d'Euler".

Bibliographie

Kolyvagin, V. A.; *Euler systems.* The Grothendieck Festschrift, Vol. II, 435–483, Progr. Math., 87, Birkhäuser Boston, Boston, MA, 1990.

Mazur, B.; Wiles, A.; *Class fields of abelian extensions of* $\mathbb{Q}$. Invent. Math. 76 (1984), no. 2, 179–330.

Ribet, K. A.; *A modular construction of unramified p-extensions of* $\mathbb{Q}(\mu_p)$. Invent. Math. 34 (1976), no. 3, 151–162.

Washington, L. C.; *Introduction to cyclotomic fields.* Second edition. Graduate Texts in Mathematics, 83. Springer-Verlag, New York, 1997. xiv+487 pp.

Le lemme de Herbrand

Le lemme de Herbrand est un simple résultat d'algèbre linéaire.

Ce résultat a cependant beaucoup d'applications frappantes.

Le lemme de Herbrand n'apparaît pas dans les publications de J.H.

C'est C. Chevalley qui le lui attribue dans

C. Chevalley, *Sur la théorie du corps de classes dans les corps finis et les corps locaux.* Journ. Fac. Sci. Univ. Tokyo, 2 (1929-34), p. 365–476.

(le lemme est formulé à la page 375).

Formulation du Lemme

Si $f : A \to A$ est un endomorphisme d'un groupe abélien A, on notera A_f le noyau de f et A^f l'image de f.

Soit $\mu, \nu : A \to A$ deux endomorphismes de groupes abéliens tels que $\mu\nu = \nu\mu = 0$. On a alors $A^\nu \subseteq A_\mu$ et $A^\mu \subset A_\nu$ et on définit

$$H_{\mu\nu} = A_\mu / A^\nu \quad \text{et} \quad H_{\nu\mu} = A_\nu / A^\mu$$

Le *quotient de Herbrand* de A est par définition la quantité

$$q(A) = q_{\mu,\nu}(A) := \frac{\#H_{\mu\nu}}{\#H_{\nu\mu}}$$

si $\#H_{\mu\nu}$ et $\#H_{\nu\mu}$ sont finis.

Lemme de Herbrand. Soit

$$0 \to A \to B \to C \to 0$$

une suite exacte de groupes abéliens munis d'endomorphismes μ_A, ν_A, μ_B, ν_B, μ_C, ν_C tels que

$$\mu_A\nu_A,\ \nu_A\mu_A,\ \mu_B\nu_B,\ \nu_B\mu_B,\ \mu_C\nu_C,\ \nu_C\mu_C$$

soient tous nuls. Alors

$$q(B) = q(A)q(C)$$

si $q(A), q(B), q(C)$ sont des quantités finies.

Esquisse de preuve

La suite exacte du lemme donne lieu à un diagramme

$$\begin{array}{ccccc} H_{\mu_A\nu_A}(A) & \longrightarrow & H_{\mu_B\nu_B}(B) & \longrightarrow & H_{\mu_C\nu_C}(C) \\ {\scriptstyle\delta_\nu}\uparrow & & & & \downarrow{\scriptstyle\delta_\mu} \\ H_{\nu_C\mu_C}(C) & \longleftarrow & H_{\nu_B\mu_B}(B) & \longleftarrow & H_{\nu_A\mu_A}(A) \end{array}$$

Ici δ_μ (et symétriquement δ_ν) est défini de la manière suivante.

Soit $c \in C_{\mu_C}$ représentant un élément de $H_{\mu_C\nu_C}(C) = C_{\mu_C}/C^{\nu_C}$.

Soit $b \in B$ une préimage de C dans B. Puisque $\mu_C(c) = 0$ on par exactitude de la suite $\mu_B(b) \in A$.

On a $\nu_A(\mu_B(b)) = \nu_B(\mu_B(b)) = 0$ donc $\mu_B(b) \in A_{\nu_A}$.

On définit alors

$$\delta_\mu(c) = \mu_B(b) \,(\mathrm{mod}\, A^{\mu_A}).$$

On vérifie que le diagramme de la page précédente est exact.

On en conclut que

$$\begin{aligned} &\#H_{\mu_A\nu_A}(A)\cdot\#H_{\mu_B\nu_B}(B)^{-1}\cdot\#H_{\mu_C\nu_C}(C)\\ \cdot&\#H_{\nu_A\mu_A}(A)^{-1}\cdot\#H_{\nu_B\mu_B}(B)\cdot\#H_{\nu_C\mu_C}(C)^{-1}=1 \end{aligned}$$

ie

$$\frac{\#H_{\mu_A\nu_A}(A)}{\#H_{\nu_A\mu_A}(A)}\cdot\frac{\#H_{\nu_B\mu_B}(B)}{\#H_{\mu_B\nu_B}(B)}\cdot\frac{\#H_{\mu_C\nu_C}(C)}{\#H_{\nu_C\mu_C}(C)}=q(A)q(B)^{-1}q(C)=1$$

et cette équation est la conclusion du lemme.

Un cas particulier : la cohomologie des groupes finis

Soit $\sigma : A \to A$ un automorphisme d'un groupe abélien A et supposons que $\sigma^n = \mathrm{Id}_A$. Soit G le groupe engendré par σ.

Puisque

$$x^n - 1 = (x-1)(x^{n-1} + \cdots + x + 1)$$

on a

$$(\sigma - \mathrm{Id}_A)(\sigma^{n-1} + \cdots + \sigma + \mathrm{Id}_A) = (\sigma^{n-1} + \cdots + \sigma + \mathrm{Id}_A)(\sigma - \mathrm{Id}_A) = \sigma^n - 1 = 0$$

et ainsi

$$\mu := \sigma - \mathrm{Id}_A$$

et

$$\nu := \sigma^{n-1} + \cdots + \sigma + \mathrm{Id}_A$$

satisfont les hypothèses $\mu\nu = \nu\mu = 0$ du lemme de Herbrand.

On note que ν ne dépend que de G et ainsi A_ν et A^ν ne dépendent que de G (ie ne dépendent pas du choix du générateur $\sigma \in G$).

De même $A_\mu = \{\text{éléments } G\text{-invariants de } A\}$ ne dépend que de G.

Pour finir $A^\mu = \mathrm{image}(\sigma - \mathrm{Id}_A)$ ne dépend aussi que de G.

En effet, soit σ^k un autre générateur de G. Alors

$$\sigma^k - \mathrm{Id}_A = (\sigma - \mathrm{Id}_A)(\sigma^{k-1} + \cdots + \sigma + \mathrm{Id}_A)$$

et donc

$$\mathrm{image}(\sigma^k - \mathrm{Id}_A) \subseteq \mathrm{image}(\sigma - \mathrm{Id}_A)$$

Puisque σ est aussi une puissance de σ^k, on conclut symétriquement qu'on a aussi

$$\mathrm{image}(\sigma - \mathrm{Id}_A) \subseteq \mathrm{image}(\sigma^k - \mathrm{Id}_A)$$

et ainsi

$$\mathrm{image}(\sigma - \mathrm{Id}_A) = \mathrm{image}(\sigma^k - \mathrm{Id}_A).$$

Les groupes

$$H_{\mu\nu} = A_\mu / A^\nu \quad \text{et} \quad H_{\nu\mu} = A_\nu / A^\mu$$

ne dépendent ainsi que de G et de A. On note classiquement

$$\hat{H}^0(G, A) = H_{\mu\nu} \quad \text{et} \quad \hat{H}^1(G, A) = H_{\nu\mu}.$$

On conclut du lemme de Herbrand que si

$$0 \to A \to B \to C \to 0$$

est une suite exacte de groupes munis d'une action de G, alors on a

$$\frac{\#\hat{H}^0(G, A)}{\#\hat{H}^1(G, A)} \cdot \frac{\#\hat{H}^0(G, C)}{\#\hat{H}^1(G, C)} = \frac{\#\hat{H}^0(G, B)}{\#\hat{H}^1(G, B)}$$

si les quantités apparaissant dans cette égalité sont finies.

Le théorème de la norme de Hasse

Soit K un corps de nombres. Pour chaque idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$, on peut définir le complété $K_\mathfrak{p}$ de K en $\mathfrak{p}$.

Voici une description formelle: $K_\mathfrak{p}$ est le corps de fractions de l'anneau

$$\mathcal{O}_{K,\mathfrak{p}} := \varprojlim_n \mathcal{O}_K/\mathfrak{p}^n.$$

Il y a une inclusion naturelle $K \hookrightarrow K_\mathfrak{p}$.

Exemple. Si $K = \mathbb{Q}$, alors $\mathcal{O}_K = \mathbb{Z}$. Soit $\mathfrak{p} = (p)$, où p est un nombre premier. Alors $\mathbb{Q}_\mathfrak{p} = \mathbb{Q}_p$ est le corps de fraction de

$$\varprojlim_n \mathbb{Z}/p^n\mathbb{Z} =: \mathbb{Z}_\mathfrak{p} = \mathbb{Z}_p.$$

L'anneau $\mathbb{Z}_p$ est l'anneau des *entiers p-adiques* et $\mathbb{Q}_p$ est le corps des *nombres p-adiques.*

Si $\mathfrak{p} \cap \mathbb{Z} = (p)$ alors $K_\mathfrak{p}$ contient une copie de $\mathbb{Q}_p$ et $K_\mathfrak{p}$ est un $\mathbb{Q}_p$-espace vectoriel de dimension finie (sans démonstration).

Soit $K \subseteq L$ une inclusion de corps.

On suppose que L est de dimension finie comme K-espace vectoriel.

Soit $\alpha \in L$. Soit $M_\alpha : L \to L$ l'application "multiplication par α". C'est un automorphisme de K-espaces vectoriels (mais pas de corps).

On définit la *norme* de α par la formule

$$N_{L|K}(\alpha) = \det(M_\alpha) \in L\backslash\{0\}$$

Exemple. Soit $K = \mathbb{Q}$ et $L = \mathbb{Q}(i)$. Les éléments $1, i$ forment une base de L comme $\mathbb{Q}$-espace vectoriel. Soit $\alpha = a + ib \in L$. On a

$$M_\alpha(c + id) = (a + ib)(c + id) = (ac - bd) + i(bc + ad)$$

et ainsi la matrice de M_α est

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

d'où $\det(M_\alpha) = a^2 + b^2$.

Soit K un corps de nombres. Soit $\alpha \in \mathbb{Q}^*$ et p un nombre premier.

On dira que α est *une norme en p* s'il existe un idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ et un élément $\alpha_{\mathfrak{p}} \in K_{\mathfrak{p}}$ tq $\mathfrak{p} \cap \mathbb{Z} = (p)$ et $N_{K_{\mathfrak{p}}|\mathbb{Q}_p}(\alpha_{\mathfrak{p}}) = \alpha$.

Théorème de la norme de Hasse (pour $\mathbb{Q}$). Si $\alpha > 0$ est une norme en p pour tous les nombres premiers p alors α est la norme d'un élément de K^*.

Nous verrons plus bas que le théorème de la norme de Hasse est une conséquence de certains résultats en théorie du corps de classe. J.H. a introduit son lemme pour démontrer ces résultats.

Le théorème de la norme est une manifestation du *principe local-global*. Ce principe affirme que dans beaucoup de circonstances il suffit de résoudre des équations "localement" (ie dans les complétés de K en des idéaux premiers) pour trouver une solution "globale" (ie dans K).

La théorie du corps de classes : préliminaires

Une *valeur absolue archimédienne* $|\cdot|_K$ sur K est une fonction sur K à valeurs dans $\mathbb{R}_{\geq 0}$ qui provient de la valeur absolue habituelle sur $\mathbb{C}$ via un plongement de corps $K \hookrightarrow \mathbb{C}$.

Exemple. Soit $K = \mathbb{Q}(e^{2i\pi/n})$. Soit $\iota : K \hookrightarrow \mathbb{C}$ l'inclusion naturelle.

On peut montrer que les plongements de K dans $\mathbb{C}$ sont précisément donnés par $\iota \circ \gamma$, où $\gamma \in \mathrm{Gal}(K|\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^*$.

On a donc

$$|1 + e^{2i\pi/n}|_{K,\iota\circ\gamma} = |1 + \gamma(e^{2i\pi/n})|$$

et ainsi, si γ correspond à 1, on a

$$|1 + e^{2i\pi/n}|_{K,\iota\circ\gamma} = |1 + e^{2i\pi/n}|$$

et si γ correspond à 2 on a

$$|1 + e^{2i\pi/n}|_{K,\iota\circ\gamma} = |1 + e^{4i\pi/n}|.$$

On peut compléter K le long d'une valeur absolue archimédienne, de façon à forcer les suites de Cauchy dans K à converger.

On peut montrer que si $|\cdot|_K$ provient d'un plongement de K dans $\mathbb{R}$, alors le complété de K est isomorphe à $\mathbb{R}$.

De même, si $|\cdot|_K$ provient d'un plongement de K dans $\mathbb{C}$ qui contient un nombre qui n'est pas réel, alors le complété de K est isomorphe à $\mathbb{C}$.

Exemple. Le complété de $\mathbb{Q}$ pour la valeur absolue ordinaire est $\mathbb{R}$.

Le complété de $\mathbb{Q}(i)$ pour la valeur absolue $|a+ib|_{\mathbb{Q}(i)} = \sqrt{a^2+b^2}$ est $\mathbb{C}$.

Soit K un corps de nombres.

On définit le groupe des *idèles* J_K de K comme le sous-groupe de

$$\Big(\prod_{\mathfrak{p}\,\text{idéal de }\mathcal{O}_K} K_{\mathfrak{p}}^*\Big) \times \Big(\prod_{|\cdot|_s\,\text{valeur absolue archimédienne de } K} K_s^*\Big)$$

des éléments $(a_{\mathfrak{p}}) \times (a_s)$ tq $a_{\mathfrak{p}}$ est un élément inversible de $\mathcal{O}_{K,\mathfrak{p}}$ pour presque tout idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$.

Ici

- K_s est le complété de K en $|\cdot|_s$.

- "pour presque tous les éléments" signifie "pour tous les éléments à part un nombre fini d'entre eux".

Il y a un homomorphisme injectif de groupes

$$K \hookrightarrow J_K$$

envoyant α sur lui-même dans chaque coordonnée.

Le groupe quotient $C_K := J_K/K^*$ s'appelle *le groupe des classes d'idèles* (terminologie de C. Chevalley).

Si $L \supseteq K$ est un corps de nombres contenant K, on dispose d'un homomorphisme de groupes

$$N_{L|K} : J_L \to J_K$$

"produit des normes locales".

Cet homomorphisme induit un homomorphisme

$$N_{L|K} : C_L \to C_K$$

qui va jouer un rôle fondamental dans le théorème principal de la théorie du corps de classes.

Le group C_K peut être vu comme une généralisation du groupe de classes $\mathrm{Cl}(K)$.

Il existe une surjection naturelle $C_K \to \mathrm{Cl}(K)$. Il existe une topologie naturelle sur C_K qui en fait un groupe compact. Ceci est la contrepartie topologique de la finitude de C_K.

Le groupe C_K a été introduit par C. Chevalley dans la continuation de ses travaux avec J.H. afin de donner une formulation succincte du théorème principal de la théorie du corps de classe.

La *théorie du corps de classes* (de $\mathbb{Q}$) cherche à classifier les corps de nombres L contenant K ($=$ extensions finies de K) qui sont engendrés par les racines de polynômes à coefficients dans K. Ces corps sont dits *galoisiens* sur K. On peut montrer que tout corps de nombres contenant K est un sous-corps d'un corps galoisien sur K.

Ce problème est extrêmement difficile et on ne connait de résultats généraux que si on se restreint au cas où le sous-groupe de $\mathrm{Gal}(L|\mathbb{Q})$ fixant K ($=$ le groupe de Galois de L sur K) est un groupe abélien.

Théorie du corps de classes. (T. Takagi, P. Furtwängler, E. Artin, C. Chevalley, J. Herbrand, F. K Schmidt et d'autres)

Soit $L \supseteq K$ un corps L galoisien sur K. On suppose que le groupe de Galois G de L sur K est un groupe abélien. Alors

- il existe une application canonique surjective $\mathrm{Art}_L : C_K \to G$;

- le noyau de Art_L est $N_{L|K}(C_K)$;

- pour tout sous-groupe ouvert N de C_K il existe un corps L galoisien sur K dont le groupe de Galois sur K est C_K/N et tq le noyau de Art_L est N.

Le lemme de Herbrand, la théorie du corps de classes et le théorème de la norme de Hasse

Soit K un corps de nombres.

Supposons que le groupe de Galois $\mathrm{Gal}(K|\mathbb{Q})$ est cyclique d'ordre n.

On va appliquer le lemme de Herbrand à la suite exacte

$$0 \to K^* \to J_K \to C_K \to 0.$$

On obtient le diagramme

$$\begin{array}{ccccc} \hat{H}^0(K^*) & \longrightarrow & \hat{H}^0(J_K) & \longrightarrow & \hat{H}^0(C_K) \\ \uparrow & & & & \downarrow \\ \hat{H}^1(C_K) & \longleftarrow & \hat{H}^1(J_K) & \longleftarrow & \hat{H}^1(K^*) \end{array}$$

En appliquant les définitions, on voit que

$$\hat{H}^0(K^*) = \mathbb{Q}^*/N_{K|\mathbb{Q}}(K^*)$$

et

$$\hat{H}^0(J_K) = J_{\mathbb{Q}}/N_{K|\mathbb{Q}}(J_K)$$

et ainsi

l'injectivité de l'application $\hat{H}^0(K^*) \to \hat{H}^0(J_K)$ *est équivalente au théorème de la norme de Hasse.*

Par ailleurs, on aussi

$$\hat{H}^0(C_K) = C_{\mathbb{Q}}/N_{K|\mathbb{Q}}(C_K)$$

et la théorie du corps de classes donne

$$C_{\mathbb{Q}}/N_{K|\mathbb{Q}}(C_K) \simeq \mathrm{Gal}(K|\mathbb{Q}),$$

ce qui fait que $\#\hat{H}^0(C_K) = n$.

Pour finir, on a aussi $\hat{H}^1(J_K) = 0$ et $\hat{H}^1(K^*) = 0$.

Ceci est un théorème célèbre de Hilbert (le "théorème de Hilbert 90", en fait dû à E. Kummer; ce théorème apparaît dans le *Zahlbericht* de Hilbert).

Comme le noyau de l'application

$$\hat{H}^0(K^*) \to \hat{H}^0(J_K)$$

est précisément $\hat{H}^1(C_K)$, le théorème de la norme de Hasse est ainsi équivalent à l'assertion que $\hat{H}^1(C_K) = 0$.

Ainsi, *le lemme de Herbrand montre que* $\hat{H}^1(C_K) = 0$ *ssi* $q(C_K) = n$.

C'est cet énoncé que J.H. que cherche à démontrer dans une lettre à H. Hasse.

Bibliographie

J'ai emprunté la présentation du lien entre le théorème de la norme de Hasse et le lemme de Herbrand à l'article de P. Roquette

Roquette, P. *Jacques Herbrand und sein Lemma.* Mitt. Math. Ges. Hamburg 34 (2014), 163–194.

La référence classique pour la théorie du corps de classes est l'ouvrage

Algebraic number theory. Second edition. Proceedings of an instructional conference organised by the London Mathematical Society. Papers from the conference held at the University of Sussex, Brighton, September 1–17, 1965. Edited by J. W. S. Cassels and A. Fröhlich. London Mathematical Society, London, 2010.

(en particulier la contribution de J. Tate). On trouve aussi dans ce livre un article de H. Hasse sur l'histoire de la théorie du corps de classes jusqu'en 1965.

Compléments

Il existe plusieurs approches à la démonstration du théorème principal de la théorie du corps de classes.

• L'approche "cohomologique" décrite par exemple par J. Tate dans le dernier ouvrage cité.

• L'approche analytique, décrite par exemple dans le livre de S. Lang

Algebraic number theory. Second edition. Graduate Texts in Mathematics, 110. Springer-Verlag, New York, 1994.

• L'approche "axiomatique" (c'est en fait l'approche cohomologique réduite à sa plus simple expression) de J. Neukirch. Voir

Neukirch, J.; *Klassenkörpertheorie.* Springer-Lehrbuch. Springer, Heidelberg, 2011.

• L'approche "géométrique", qui ne fonctionne pas pour les corps de nombres mais fonctionne sur des corps globaux en caractéristique positive. Cette approche est due à Lang et Rosenlicht et est décrite dans le livre

Serre, J.-P.; Groupes algébriques et corps de classes. Publications de l'Institut Mathématique de l'Université de Nancago, 7. Actualités Scientifiques et Industrielles 1264. Hermann, Paris, 1984.

• On peut pour certains corps de nombres décrire les extensions galoisiennes de groupe de Galois abélien via les valeurs de certaines fonctions analytiques.

Par exemple, pour $K = \mathbb{Q}$ on a le résultat classique

Théorème.(Kronecker-Weber) Soit K un corps de nombres. Si $\mathrm{Gal}(K|\mathbb{Q})$ est un groupe abélien, alors il existe un $n \geq 1$ tq $K \subseteq \mathbb{Q}(e^{2i\pi/n})$.

Lorsque $K = \mathbb{Q}(\sqrt{-D})$, il existe une variante du théorème de Kronecker-Weber faisant appel à la théorie de la multiplication complexe des courbes elliptiques.

On obtient un résultat semblable mais on doit remplacer $e^{2i\pi/n}$ par les coordonnées de points de torsion sur une courbe elliptique à multiplication complexe par $\mathcal{O}_{\mathbb{Q}(\sqrt{-D})}$.

Voir pour tout cela l'ouvrage *Algebraic Number Theory* cité plus haut.

• Le programme de Langlands donne une approche conjecturale à la théorie du corps de classes pour des extensions galoisiennes à groupe de Galois non abélien.