JOURNAL
DE
MATHÉMATIQUES
PURES ET APPLIQUÉES
FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874
PAR JOSEPH LIOUVILLE

CLAUDE CHEVALLEY

Généralisation de la théorie du corps de classes pour les extensions infinies

Journal de mathématiques pures et appliquées 9^e série, tome 15 (1936), p. 359-371.
<http://www.numdam.org/item?id=JMPA_1936_9_15__359_0>

Généralisation de la théorie du corps de classes pour les extensions infinies;

PAR C. CHEVALLEY.

Introduction.

k étant un corps de nombres algébriques de degré fini, la théorie du corps de classes associe à toute extension abélienne finie Z de k un groupe composé d'idéaux de k qui la caractérise complètement.

On peut aussi se demander s'il est possible de caractériser, au moyen d'éléments constructibles dans k, les extensions abéliennes infinies de k. Si l'on remarque que le groupe associé au corps composé de deux extensions finies Z', Z'' de k est l'intersection des groupes associés à ces deux corps, il vient à l'idée de chercher à associer à une extension infinie Z l'intersection des groupes associés dans k aux extensions finies Z' de k contenues dans Z. Mais on s'aperçoit rapidement que le groupe d'idéaux ainsi construit ne caractérise nullement Z; si par exemple k est le corps des nombres rationnels, et si Z est le corps engendré par toutes les racines de l'unité dont les ordres sont des puissances d'un même nombre premier p, le groupe que l'on construirait ainsi se compose du seul élément unité.

Dans le présent Mémoire, il est montré que l'on peut caractériser les extensions abéliennes, finies ou infinies, de k par des groupes dont les éléments sont non plus des idéaux, mais des objets d'une nature différente, les éléments-idéaux, définis au paragraphe I.

La famille de tous les groupes d'éléments idéaux associés à des extensions abéliennes de k peut être caractérisée dans k, et ceci au

moyen d'une topologie dans le groupe de tous les éléments-idéaux. Ce fait constitue le « théorème d'existence » de la théorie développée.

Nous nous appuyons sur les résultats, supposés connus, de la théorie classique du corps de classes (1). On peut aussi développer directement cette dernière en employant partout le langage des éléments-idéaux; cette méthode a l'avantage d'introduire quelques simplifications en divers points.

Enfin, signalons un résultat qui se déduit de la théorie ici exposée, sans que nous ayons pu, dans ce Mémoire, en donner la démonstration : *une extension abélienne infinie* Z *d'un corps de degré fini k est bien déterminée dès qu'on connaît toutes les extensions* Zk_p *correspondant aux corps de nombres p-adiques* k_p *pour tous les diviseurs premiers p de k.* (On sait qu'il n'en est pas ainsi pour les extensions galoisiennes infinies.)

I. — Les éléments idéaux.

Nous désignerons dans tout ce Mémoire par k un corps de nombres algébriques de degré fini. On trouve dans k une infinité de diviseurs premiers p, définis par les divers types de valeurs absolues de k : ce sont ou bien des *diviseurs premiers finis*, correspondant aux valeurs absolues non archimédiennes, c'est-à-dire aux idéaux premiers au sens de Dedekind, ou bien des *diviseurs premiers infinis*, correspondant aux valeurs absolues archimédiennes, c'est-à-dire aux conjugués réels ou aux paires de conjugués imaginaires de k.

A chaque diviseur premier p correspond une fermeture p-adique k_p de k, qui est un corps contenant un corps isomorphe à k et dans lequel se prolonge la valeur absolue qui définit p. On désignera par L_p une isomorphie appliquant k dans k_p et conservant cette valeur absolue. Si p est fini, la valeur absolue dans k_p définit pour les éléments de k_p l'*ordre pour p*, qui est une fonction de ces éléments dont la valeur est un entier rationnel (ou $+\infty$) et dont les propriétés sont bien

(1) *Voir*, pour la théorie du corps de classes, HASSE, *Bericht über neuere Untersuchungen und Probleme aus der Theorie des alg. Zahlkörper* (*Jahresb. d. D. M. V.*, vol. 35 et 36 et Ergänzungsband VI) ou CHEVALLEY, *La théorie du corps de classes* (*Journ. of Coll. of Sciences*, Tokyo, 1933).

connues (¹). Les éléments de k_p qui sont d'ordre o, si p est fini, tous les éléments $\neq$ o de k_p, si p est infini, sont appelés les *unités p-adiques*.

Nous désignerons par k_p^* le groupe multiplicatif des éléments $\neq$ o de k_p. Formons le produit direct de tous les groupes k_p^*, p parcourant tous les diviseurs premiers de k. Les éléments de ce produit direct sont les systèmes obtenus en prenant un élément et un seul (le p-composant) dans chaque k_p^*.

DÉFINITION I. — *On appelle élément idéal de k un élément du produit direct de tous les k_p^* dont presque tous les composants sont des unités* (²).

Nous emploierons désormais l'abréviation « e. i. » pour « élément idéal ». $\mathfrak{a}$ étant un e. i., nous désignerons son p-composant par $\mathfrak{a}_p$.

Les e. i. de k forment un groupe, le p-composant du produit $\mathfrak{ab}$ de deux e. i. $\mathfrak{a}$, $\mathfrak{b}$ étant $\mathfrak{a}_p\mathfrak{b}_p$. Ce groupe s'appellera le *groupe fondamental* de k et se désignera par k^*.

DÉFINITION II. — *On appelle principal un e. i. $\mathfrak{a}$ de k quand il existe un nombre α de k tel que, pour chaque p, $\mathfrak{a}_p$ se déduise de α par l'isomorphie L_p. Le groupe formé des e. i. principaux sera appelé sous-groupe principal de k et désigné par P_k.*

Le groupe P_k est évidemment isomorphe au groupe multiplicatif des nombres $\neq$ o de k. Il n'y aura pas d'inconvénient à identifier les nombres avec les e. i. principaux correspondants : c'est ce que nous ferons dans la suite.

p étant un diviseur premier, si tous les q-composants d'un e. i. $\mathfrak{a}$ pour les diviseurs premiers $q \neq p$ sont $= 1$, on dit que $\mathfrak{a}$ est primaire (pour p). On peut alors identifier $\mathfrak{a}$ à un élément de k_p^* et écrire $\mathfrak{a} = \mathfrak{a}_p$.

Une isomorphie τ entre k et l'un de ses conjugués k^τ fait correspondre à chaque diviseur premier p de k un diviseur premier p^τ de k^τ, et se prolonge par une isomorphie entre k_p et $k_{p^\tau}^\tau$. Si l'on fait subir cette isomorphie à chaque composant d'un e. i. $\mathfrak{a}$ de k, on obtient un

---

(¹) *Voir*, par exemple, CHEVALLEY, *loc. cit.* (¹), p. 360.

(²) Les éléments idéaux peuvent être considérés comme formant une partie de l'ensemble des nombres idéaux définis par M. PRÜFER, *Neue Begründung der algebraischen Zahlentheorie* (*Mat. Ann.*, 94, 1925, p. 198).

e. i. de k^τ qu'on désigne par $\mathfrak{a}^\tau$. La correspondance $\mathfrak{a} \rightleftharpoons \mathfrak{a}^\tau$ est une isomorphie qui prolonge τ entre k^* et $(k^\tau)^*$.

Soit maintenant K une extension finie de k. Si P est un diviseur premier de K, il divise un diviseur premier p de k, et K_P contient k_p. Si à chaque e. i. $\mathfrak{a}$ de k on fait correspondre l'e. i. de K dont le P-composant est $\mathfrak{a}_p$ pour tous les P qui divisent p, on obtient une isomorphie entre k^* et un sous-groupe de K^*. Nous pourrons donc considérer que K^* contient k^* (bien entendu, des notions telles que « primaire », « principal », ... n'ont pas le même sens dans k et dans K ; des faits parallèles se retrouvent d'ailleurs en théorie des idéaux).

DÉFINITION III. — K *étant une extension finie de* k, $\overline{K}$ *une extension galoisienne finie de* k *contenant* K, $\tau_1, \tau_2, \ldots, \tau_n$ *les isomorphies distinctes de* K *avec ses conjugués* K^{τ_i} *contenus dans* $\overline{K}$, $\mathfrak{A}$ *un e. i. de* K, *on appelle norme relative* (*de* K *à* k) *de* $\mathfrak{A}$ *l'e. i.* $\mathfrak{A}^{\tau_1}.\mathfrak{A}^{\tau_2}\ldots\mathfrak{A}^{\tau_n}$. *On le désigne par* $N_{K/k}\mathfrak{A}$.

Nous allons montrer que c'est un e. i. de k dont les composants sont donnés par la formule

$$\mathfrak{a}_p = \Pi_P N_{K_P/k_p} \mathfrak{A}_P,$$

le produit étant étendu aux diviseurs premiers P de p dans K. Il suffit évidemment de se limiter au cas où $\mathfrak{A}$ est un e. i. primaire dans K pour un diviseur premier P. Nous désignerons par $\overline{P}$ un diviseur premier de $\overline{K}$ divisant P, par $\mathfrak{g}$ le groupe de Galois de $\overline{K}/k$, par $\mathfrak{h}$ celui de $\overline{K}/K$, par $\mathfrak{z}$ le groupe de décomposition de $\overline{P}$ dans l'extension $\overline{K}/k$, par $\mathfrak{a}$ le produit $\prod_{i=1}^{n} \mathfrak{A}^{\tau_i}$. On a

$$\mathfrak{a}_{\overline{P}} = \prod_{i=1}^{n} \mathfrak{A}_{\overline{P}_i}^{\tau_i}, \qquad \text{où} \quad \overline{P}_i = \overline{P}^{\tau_i^{-1}}.$$

Si $\overline{P}_i$ ne divise pas P, on a $\mathfrak{A}_{\overline{P}_i} = 1$. Il suffit donc, pour calculer le produit précédent, de se limiter à l'ensemble des indices i tels que $\overline{P}_i$ divise P ; les τ_i correspondants forment un système de représentants des classes de $\mathfrak{h}\mathfrak{z}$ suivant $\mathfrak{h}$. On peut les supposer pris dans $\mathfrak{z}$, et ils

forment alors un système de représentants des classes de $\mathfrak{z}$ suivant $\mathfrak{h} \cap \mathfrak{z}$, ce qui signifie que le produit écrit est égal à $N_{K_p/k_p}\mathfrak{A}_p$, ce qui démontre la formule.

Il est clair que, si $\mathfrak{B}$ est un autre e. i. de K, on a

$$N_{K/k}\mathfrak{A}\mathfrak{B} = N_{K/k}\mathfrak{A} . N_{K/k}\mathfrak{B}.$$

D'autre part, si $\mathfrak{A}$ est un nombre de K, la notion introduite coïncide avec la notion ordinaire de norme.

La notion de congruence [mutiplicative (1)] s'étend aux e. i. Pour la définir, il faut d'abord introduire la notion de *diviseur*. On appelle diviseur de K toute expression de la forme $m = \prod_{i=1}^{n} p_i^{e_i}$, où $p_1, p_2, \ldots, p_r$ sont des diviseurs premiers distincts, les e_i étant des entiers > 0. Deux diviseurs sont à considérer comme égaux quand ils ont la même expression aux valeurs près des exposants des diviseurs premiers infinis : autrement dit, p étant un diviseur premier infini, tous les diviseurs $p^e (e > 0)$ sont à considérer comme égaux. Les notions de divisibilité, p. g. c. d., ... se définissent tout de suite pour les diviseurs au moyen de leurs expressions formelles. p étant un diviseur premier qui figure dans l'expression de m, avec l'exposant e, le diviseur p^e s'appelle la contribution de p à m et se désigne par m_p. m étant un diviseur, $\mathfrak{a}$, $\mathfrak{b}$ étant des e. i. de k, on dit qu'ils sont congrus $(\mathrm{mod}\, m)$ et l'on écrit $\mathfrak{a} \equiv \mathfrak{b} (\mathrm{mod}\, m)$ si les conditions suivantes sont réalisées : a, pour tout diviseur premier fini p divisant m, l'ordre pour p de $\mathfrak{a}_p \mathfrak{b}_p^{-1} - 1$ est $\geq e$, si $p^{\text{ième}}$ est la contribution de p à m; b, pour tout diviseur premier infini p divisant m et réel, $\mathfrak{a}_p \mathfrak{b}_p^{-1}$ est positif dans k_p. La relation ainsi définie est réflexive, symétrique, transitive; les congruences $(\mathrm{mod}\, m)$ peuvent être multipliées ou divisées membre à membre. Appliquées aux nombres $\neq 0$ de k, elles donnent les *congruences multiplicatives* de Hasse.

A côté de la notion de congruence, il y a intérêt à introduire une notion plus forte, celle de *surcongruence* : les e. i. $\mathfrak{a}$, $\mathfrak{b}$ sont dits sur-

(1) Pour la notion de congruence multiplicative, *voir* HASSE ou CHEVALLEY, *loc. cit.* (1), p. 360.

congrus $(\mathrm{mod}\, m)$, et l'on écrit $\mathfrak{a} \equiv \mathfrak{b}\,(\mathrm{mod}\, m)$ si : a, on a $\mathfrak{a} \equiv \mathfrak{b}\,(\mathrm{mod}\, m)$; b, pour tout diviseur premier p ne divisant pas m, $\mathfrak{a}_p \mathfrak{b}_p^{-1}$ est une unité p-adique. C'est encore une relation reflexive, symétrique et transitive; les surcongruences $(\mathrm{mod}\, m)$ peuvent être multipliées et divisées membre à membre.

Les e. i. $\equiv 1\,(\mathrm{mod}\, 1)$ sont appelés les e. i. unités; ils forment un groupe U_k dont l'intersection avec P_k est le groupe des unités de k. Les classes de surcongruence $(\mathrm{mod}\, 1)$, c'est-à-dire les classes de k^* suivant U_k, forment un groupe qui est isomorphe au groupe des idéaux de Dedekind de k; nous pourrons donc appeler *idéaux* ces classes de surcongruence; $\mathfrak{a}$ étant un e. i. nous noterons par $(\mathfrak{a})$ l'idéal correspondant à la classe $(\mathrm{mod}\, U_k)$ qui contient $\mathfrak{a}$; nous dirons que cet idéal est *représenté* par $\mathfrak{a}$. Si $\mathfrak{a}$ est un nombre de k, cette notation coïncide avec celle des idéaux principaux.

II. — Le groupe attaché à une extension abélienne finie.

LEMME I. — *$\mathfrak{a}$ et m étant respectivement un e. i. et un diviseur de k, il y a toujours un nombre $\alpha \equiv \mathfrak{a}\,(\mathrm{mod}\, m)$.*

En effet, on sait que le système de congruences $\alpha \equiv \mathfrak{a}_p\,(\mathrm{mod}\, m_p)$ est toujours résoluble.

Soit alors $\overline{\mathrm{H}}$ un groupe de congruence dans k défini $(\mathrm{mod}\, m)$.

DÉFINITION I. — *On appelle sous-groupe de k^* défini par $\overline{\mathrm{H}}$ le groupe engendré par P_k et par les e. i. $\mathfrak{a} \equiv 1\,(\mathrm{mod}\, m)$ tels que $(\mathfrak{a}) \in \overline{\mathrm{H}}$.*

Si $\overline{\mathrm{H}}'$ est un groupe de congruence « égal » à $\overline{\mathrm{H}}$, le groupe H' défini par $\overline{\mathrm{H}}'$ est le même que le groupe H défini par $\overline{\mathrm{H}}$. Soit en effet n un diviseur, multiple des modules de définition m, m' de $\overline{\mathrm{H}}$, $\overline{\mathrm{H}}'$ tel que les idéaux premiers à n de ces deux groupes soient les mêmes. Soit $\alpha\mathfrak{a}$ un e. i. de H, $\alpha \in P_k$, $\mathfrak{a} \equiv 1\,(\mathrm{mod}\, m)$, $(\mathfrak{a}) \in \overline{\mathrm{H}}$. Prenons un nombre $\alpha' \equiv \mathfrak{a}\,(\mathrm{mod}\, n)$: on a $\alpha\mathfrak{a} = \alpha\alpha' . \mathfrak{a}\alpha'^{-1}$, avec $\mathfrak{a}\alpha'^{-1} \equiv 1\,(\mathrm{mod}\, n)$, $\alpha' \equiv 1\,(\mathrm{mod}\, m)$. Donc $(\mathfrak{a}\alpha'^{-1})$ est premier à n et est dans $\overline{\mathrm{H}}$; il est donc aussi dans $\overline{\mathrm{H}}'$, et par suite $\mathrm{H}' \supset \mathrm{H}$; on voit de même que $\mathrm{H} \supset \mathrm{H}'$, et par suite $\mathrm{H} = \mathrm{H}'$.

Inversement, la connaissance de H permet de former $\overline{\overline{H}}$ et tous les groupes qui lui sont égaux. Le conducteur f de $\overline{\overline{H}}$ est le p. g. c. d. des diviseurs m tels que H contienne tous les e. i. $\mathfrak{a} \equiv 1 \pmod{m}$; on obtient le groupe de congruence « égal » à $\overline{\overline{H}}$ le plus général en prenant un multiple quelconque n de f et en formant le groupe des idéaux $(\mathfrak{a})$ représentables par des e. i. $\mathfrak{a} \equiv 1 \pmod{n}$ appartenant à H.

Donnons-nous maintenant une extension abélienne finie Z de k, corps de classes sur k pour un groupe $\overline{\overline{H}}_{Z/k}$ défini à une « égalité » près. Nous pouvons, en vertu de ce qui précède, poser la définition suivante :

DÉFINITION II. — *Le sous-groupe de k^* défini par $\overline{\overline{H}}_{Z/k}$ sera appelé groupe associé à Z dans k. Il se désignera par $H_{Z/k}$. On dira que Z est corps de classes sur k pour ce groupe.*

La connaissance de $H_{Z/k}$ permettant de déterminer $\overline{\overline{H}}_{Z/k}$, on a le *théorème d'unicité :*

THÉORÈME I. — *Le corps Z est bien déterminé par la connaissance de $H_{Z/k}$.* Autrement dit : *il y a au plus un corps de classes sur k pour un sous-groupe donné de k.*

LEMME II. — *Si f est le conducteur de Z/k, tout e. i. $\mathfrak{e} \equiv 1 \pmod{f}$ est norme relative d'un e. i. de Z.*

Choisissons en effet pour chaque diviseur premier p de k un diviseur premier P de p dans Z. Si p divise f, on a $\mathfrak{e}_p \equiv 1 \pmod{f_p}$; sinon, $\mathfrak{e}_p$ est une unité p-adique. Dans tous les cas, $\mathfrak{e}_p$ est la norme prise de Z_P à k_p d'un élément $\mathfrak{E}_P$ de Z_P. Si $\mathfrak{E}$ est l'e. i. de Z dont les P-composants sont les $\mathfrak{E}_P$, tous les autres composants étant $= 1$, on a $\mathfrak{e} = N_{Z/k}\mathfrak{E}$.

Soit alors $\mathfrak{a}$ un e. i. de $H_{Z/k}$: on a $\mathfrak{a} = \alpha\mathfrak{a}_1$, $\alpha \in P_k$, $(\mathfrak{a}_1) \in \overline{\overline{H}}_{Z/k}$. Donc $(\mathfrak{a}_1) = (\alpha_1).N_{Z/k}(\mathfrak{A}_1)$, $(\mathfrak{A}_1)$ étant un idéal de Z premier à f, que l'on peut supposer représenté par un e. i. $\mathfrak{A}_1 \equiv 1 \pmod{f}$. Donc $\mathfrak{a} = \alpha\alpha_1 N_{Z/k}\mathfrak{A}_1.\mathfrak{e}$, où $\mathfrak{e} \equiv 1 \pmod{f}$, et par suite $\mathfrak{e} = N_{Z/k}\mathfrak{E}$, $\mathfrak{E} \in Z^*$. Par suite, tout e. i. de $H_{Z/k}$ se met sous la forme $\beta N_{Z/k}\mathfrak{B}$, $\beta \in P_k$, $\mathfrak{B} \in Z^*$. Inversement, soit $\mathfrak{a}$ un e. i. de cette forme. Soit B un nombre de Z tel que $B \equiv \mathfrak{B} \pmod{f}$; on a $\mathfrak{a} = \beta N_{Z/k}B.N_{Z/k}(\mathfrak{B}B^{-1})$, avec $\mathfrak{B}B^{-1} \equiv 1 \pmod{m}$ et par suite $\mathfrak{a} \in H_{Z/k}$. Donc :

THÉORÈME II. — *Le groupe* $H_{Z/k}$ *est engendré par* P_k *et par les normes relatives des e. i. de* Z.

$\mathfrak{a}$ étant un e. i. quelconque de k, mettons-le sous la forme $\alpha\mathfrak{a}_1$, $\alpha \in P_k$, $\mathfrak{a}_1 \equiv 1 \pmod{f}$, et posons

$$(\mathfrak{a}, Z/k) = \left(\frac{Z/k}{(\mathfrak{a}_1)}\right).$$

La valeur du second membre est indépendante de la décomposition $\mathfrak{a} = \alpha\mathfrak{a}_1$ de $\mathfrak{a}$; soit en effet $\mathfrak{a} = \alpha'\mathfrak{a}'_1$ une autre décomposition du même type. L'idéal $(\mathfrak{a}_1\mathfrak{a}_1'^{-1})$ appartient au rayon $(\bmod f)$; d'où

$$\left(\frac{Z/k}{(\mathfrak{a}_1)}\right) = \left(\frac{Z/k}{(\mathfrak{a}'_1)}\right).$$

Le symbole $(\mathfrak{a}, Z/k)$ ainsi défini sera appelé le *symbole de Artin généralisé*. Les propriétés suivantes de ce symbole résultent immédiatement de sa définition :

I. Si $\mathfrak{a}$, $\mathfrak{b}$ sont des e. i. de k, on a

$$(\mathfrak{ab}, Z/k) = (\mathfrak{a}, Z/k)\,(\mathfrak{b}, Z/k).$$

II. *Si* $k \subset Z' \subset Z$, $(\mathfrak{a}, Z'/k)$ *est l'automorphie de* Z' *produite par* $(\mathfrak{a}, Z/k)$.

De plus, en vertu des relations entre $H_{Z/k}$ et $\overline{H}_{Z/k}$, on voit que :

III. *Le groupe des e. i.* $\mathfrak{a}$ *pour lesquels* $(\mathfrak{a}, Z/k) = 1$ *est* $H_{Z/k}$.

D'ailleurs $(\mathfrak{a}, Z/k)$ décrit, quand $\mathfrak{a}$ parcourt les éléments de k^*, le groupe de Galois de Z/k tout entier, car il en est ainsi de $\left(\frac{Z/k}{(\mathfrak{a}_1)}\right)$. Donc :

IV. *Le symbole* $(\mathfrak{a}, Z/k)$ *définit une isomorphie entre* $k^*/H_{Z/k}$ *et le groupe de Galois de* Z/k.

Si nous désignons par ${}^p\mathfrak{a}$ l'e. i. dont le p-composant est $\mathfrak{a}_p$, tous les autres composants étant $= 1$, nous poserons

$$\left(\frac{\mathfrak{a}, Z/k}{p}\right) = ({}^p\mathfrak{a}, Z/k)^{-1}.$$

Le symbole ainsi défini est le symbole de *restes normiques* pour les e. i. Dans le cas où $\mathfrak{a}$ est un nombre α de k, cette définition coïncide avec la définition de Hasse du symbole de restes normiques. En effet, si p ne divise pas f, on a, en désignant par r l'ordre de α pour p,

$$({}^{p}\alpha, \mathrm{Z}/k)^{-1} = \left(\frac{\mathrm{Z}/k}{p}\right)^{-r} = \left(\frac{\alpha, \mathrm{Z}/k}{p}\right),$$

si au contraire p divise f, on met ${}^{p}\alpha$ sous la forme $\alpha_0\mathfrak{a}_1$, $\alpha_0 \in \mathrm{P}_k$, $\mathfrak{a}_1 \equiv 1 \pmod{f}$; on a donc $\alpha_0 \equiv \alpha \pmod{f_p}$, $\alpha_0 \equiv 1 \left(\mathrm{mod}\,\frac{f}{f_p}\right)$ et par suite α_0 est un nombre auxiliaire au sens de M. Hasse pour α. L'idéal (α_0) vaut $p^b(\mathfrak{a}_1^{-1})$, où p^b est défini par $({}^{p}\alpha) = p^b$. Par suite la définition de M. Hasse conduit pour le symbole $\left(\frac{\alpha, \mathrm{Z}/k}{p}\right)$ à la valeur $\left(\frac{\mathrm{Z}/k}{(\mathfrak{a}_1)}\right)^{-1}$, qui est bien aussi celle que donne notre définition.

Il résulte de là que la condition nécessaire et suffisante pour que $\left(\frac{\mathfrak{a}, \mathrm{Z}/k}{p}\right) = 1$ est que, pour tout exposant $n > 0$, $\mathfrak{a}$ soit congru $(\mathrm{mod}\,p^n)$ à la norme relative d'un e. i. de Z, ou encore que, P désignant un diviseur premier de p dans Z, $\mathfrak{a}_p$ soit la norme, prise de Z_P à k_p d'un élément de Z_P.

D'autre part, il résulte immédiatement de la définition que l'on a la formule

$$(\mathfrak{a}, \mathrm{Z}/k) = \Pi_p \left(\frac{\mathfrak{a}, \mathrm{Z}/k}{p}\right)^{-1}.$$

Cette formule, comparée à la propriété II du symbole de Artin généralisé, conduit à la loi de réciprocité de Hilbert-Hasse

$$\Pi_p \left(\frac{\alpha, \mathrm{Z}/k}{p}\right) = 1.$$

Enfin, signalons que le symbole généralisé de Artin jouit, tout comme le symbole de Artin, d'une propriété de translation :

Si $\mathfrak{A}$ est un e. i. d'une extension finie K *de k, et si* Z *est une extension abélienne finie de k, on a*

$$(\mathfrak{A}, \mathrm{ZK}/\mathrm{K}) = (\mathrm{N}_{\mathrm{K}/k}\mathfrak{A}, \mathrm{Z}/k).$$

En effet, f étant le conducteur de Z/k, mettons $\mathfrak{A}$ sous la forme $\mathrm{A}\mathfrak{A}_1$,

$A \in P_k$, $\mathfrak{A}_1 \equiv 1 \pmod f$, d'où $N_{K/k}\mathfrak{A} = N_{k/k}A \cdot N_{K/k}\mathfrak{A}_1$ et

$$(\mathfrak{A}, ZK/K) = \left(\frac{ZK/K}{(\mathfrak{A}_1)}\right) = \left(\frac{Z/k}{N_{K/k}(\mathfrak{A}_1)}\right) = (N_{K/k}\mathfrak{A}, Z/k).$$

III. — Le groupe attaché à une extension abélienne infinie.

Désignons maintenant par Z une extension abélienne infinie de k, et par $\mathfrak{g}$ le groupe de Galois de Z/k, que nous considérerons comme un groupe topologique (1). Soit $\mathfrak{a}$ un élément de k^*, il y a toujours un élément σ de $\mathfrak{g}$ tel que, dans toute extension finie Z' de k contenue dans Z, l'automorphie produite par σ soit $(\mathfrak{a}, Z'/k)$. En effet, soit $Z_1 \subset Z_2 \subset \ldots \subset Z_n \subset \ldots$ une suite croissante d'extensions finies de k contenues dans Z et dont la réunion soit Z. On peut, pour chaque n, choisir un élément σ_n de $\mathfrak{g}$ produisant dans Z_n l'automorphie $(\mathfrak{a}, Z_n/k)$. Pour tout $h > 0$, $\sigma_{n+h}\sigma_n^{-1}$ laisse invariants les éléments de Z_n. Donc, la suite $\{\sigma_n\}$ converge dans $\mathfrak{g}$ vers un élément σ ayant la propriété indiquée; et c'est évidemment le seul élément ayant cette propriété. Nous le désignerons par $(\mathfrak{a}, Z/k)$; le symbole ainsi défini sera appelé *symbole de Artin généralisé*.

Il jouit évidemment des propriétés I, II (pour des extensions abéliennes Z, Z' finies ou infinies).

Définition. — *Nous appelerons groupe attaché à* Z *dans* k *et nous désignerons par* $H_{Z/k}$ *le groupe des e. i.* $\mathfrak{a}$ *pour lesquels on a*

$$(\mathfrak{a}, Z/k) = 1.$$

Il résulte de là le théorème suivant :

Si Z *est le plus petit corps contenant tous les corps d'une famille d'extensions abéliennes* Z' *de* k, $H_{Z/k}$ *est la partie commune à tous les groupes* $H_{Z'/k}$. *En particulier,* $H_{Z/k}$ *est la partie commune aux groupes associés à toutes les extensions abéliennes finies de* k *contenues dans* Z.

---

(1) Pour la topologie dans $\mathfrak{g}$, *voir* Krull, *Galoische Theorie der unendlichen algebraischen Erweiterungen* (*Math. Ann.*, **100**, 1928).

Il est clair que la propriété III est encore vraie pour le symbole $(\mathfrak{a}, Z/k)$ dans les extensions abéliennes infinies.

Pour aller plus loin, nous allons introduire dans k^* une topologie. m étant un diviseur entier de k, désignons par U_m le groupe des e. i. $\mathfrak{a} \equiv 1 \pmod{m}$. Soit $\mathcal{O}$ la famille des ensembles O jouissant de la propriété suivante : si $\mathfrak{a} \in O$, il existe un diviseur entier m tel que $\mathfrak{a}U_m \subset O$. Il est clair que toute réunion d'ensembles de la famille $\mathcal{O}$ appartient encore à cette famille; par suite, nous pouvons définir une topologie au sens de M. Sierpinski (1), en prenant pour ensembles ouverts les ensembles de $\mathcal{O}$. Cette topologie satisfait aux conditions suivantes :

a. L'intersection de deux ensembles ouverts O_1, O_2 *est un ensemble ouvert.* En effet, si $O_1 \cap O_2$ n'est pas vide, soit $\mathfrak{a}$ un élément de cet ensemble. Il existe des diviseurs entiers m_1, m_2 tels que $\mathfrak{a}U_{m_1} \subset O_1$, $\mathfrak{a}U_{m_2} \subset O_2$. Soit m le p. p. c. m. de m_1 et de m_2. On a

$$\mathfrak{a}U_m \subset \mathfrak{a}U_{m_1} \cap \mathfrak{a}U_{m_2} \subset O_1 \cap O_2.$$

b. Le produit de deux éléments de k^* *est fonction continue de l'ensemble de ces deux éléments.* Soient en effet $\mathfrak{a}$, $\mathfrak{b}$ deux éléments de k^* et O un ensemble ouvert tel que $\mathfrak{ab} \in O$; si m est un diviseur entier tel que $\mathfrak{ab}U_m \subset O$, on a aussi $\mathfrak{a}U_m . \mathfrak{b}U_m \subset O$; $\mathfrak{a}U_m$ et $\mathfrak{b}U_m$ étant des ensembles ouverts, ce fait démontre la proposition. On peut donc dire que k^*, muni de la topologie que nous venons d'y introduire, est un groupe topologique.

c. La topologie de k^* *peut être définie par une infinité dénombrable de voisinages.* En effet, il n'y a qu'une infinité dénombrable de diviseurs entiers m; d'autre part, m étant donné, les classes $\mathfrak{a}U_m$ sont en infinité dénombrable. Or, la famille des ensembles $\mathfrak{a}U_m$ forme une famille de voisinages qui définit la topologie.

Il y a lieu de noter que la topologie définie n'est pas une topologie de Hausdorf. En effet, soient $\mathfrak{a}$, $\mathfrak{a}'$ deux e. i. tels que $\mathfrak{a}_p = \mathfrak{a}'_p$ pour tous les diviseurs premiers p finis, et que $\mathfrak{a}_p \mathfrak{a}'_p > O$ pour les diviseurs premiers p infinis réels. Il est clair que tout ensemble ouvert (ou fermé) contenant $\mathfrak{a}$ contient aussi $\mathfrak{a}'$.

---

(1) SIERPINSKI, *Introduction to general Topology*, Toronto, 1934.

D'autre part, remarquons que le groupe $U_1 = U_k$ des e. i. unités est compact. En effet, pour qu'une suite (ε_n) d'e. i. de U_k converge, il faut et suffit, comme on le voit tout de suite, que pour chaque diviseur premier p fini $(\varepsilon_n)_p$ forme une suite convergente dans k_p, et que, pour chaque diviseur premier p infini réel $(\varepsilon_n)_p$ garde le même signe à partir d'un certain rang. Or, de toute suite d'e. i. de U_k, on peut extraire, par le procédé diagonal, une suite satisfaisant à ces conditions.

Revenons maintenant aux notations du début du paragraphe III. La correspondance $\mathfrak{a} \to (\mathfrak{a}, Z/k)$ est une application continue de k^* dans $\mathfrak{g}$. Il suffit, pour le voir, de montrer que, si $\mathfrak{h}$ est un voisinage de l'unité dans $\mathfrak{g}$, l'ensemble H des $\mathfrak{a}$ tels que $(\mathfrak{a}, Z/k) \in \mathfrak{h}$ est ouvert. Or, on peut prendre pour $\mathfrak{h}$ le groupe de Galois de Z/Z', Z' étant une extension finie de k contenue dans Z. H est alors le groupe $H_{Z'/k}$. Si f est le conducteur de Z', H contient donc U_f, et est par suite ouvert. (Il est d'ailleurs aussi fermé, étant d'indice fini.)

Il résulte de là que $H_{Z/k}$ est un sous-groupe fermé de k^*. Ce sous-groupe contient P_k, donc aussi l'adhérence (1) $\overline{P}_k$ de P_k. Or, la topologie dans k^* définit une topologie dans $k^*/\overline{P}_k$. Cette topologie est une topologie de Hausdorf, comme on le voit facilement. De plus, *elle est compacte*. Prenons en effet dans chaque classe absolue d'idéaux de k un idéal; soient $(\mathfrak{a}_1), (\mathfrak{a}_2), \ldots, (\mathfrak{a}_h)$ les idéaux obtenus, que nous supposons représentés par des e. i. $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_h$. L'ensemble $E = \sum_{i=1}^{h} \mathfrak{a}_i U_1$ est compact. Or, pour tout e. i. $\mathfrak{a}$, il existe un nombre α tel que $\mathfrak{a} \in \alpha E$, ce qui veut dire que dans toute classe de $k^* (\mathrm{mod} P_k)$ et, *a fortiori*, dans toute classe $(\mathrm{mod} \overline{P}_k)$, il existe un élément de E; d'où résulte le fait annoncé. Il en résulte que l'application $\mathfrak{a} \to (\mathfrak{a}, Z/k)$ transforme k^* en un sous-groupe compact en soi, donc fermé, de $\mathfrak{g}$. Ce groupe $\mathfrak{g}^*$ est donc le groupe de Galois de Z par rapport à un corps Z^* contenant k et contenu dans Z. Si Z' est une extension finie de k contenue dans Z, on a $(\mathfrak{a}, Z'/k) = 1$ quel que soit $\mathfrak{a}$; d'où $Z' = k$, $Z^* = k$ et $\mathfrak{g}^* = \mathfrak{g}$. Donc

(1) C'est-à-dire le plus petit ensemble fermé contenant P_k.

la propriété IV *du symbole* $(\mathfrak{a}, Z/k)$ *est encore vraie pour les extensions infinies.*

Soit maintenant A le corps composé de toutes les extensions abéliennes de k, et soit $\mathfrak{G}$ le groupe de Galois de A/k. On vient de voir que la correspondance $\mathfrak{a} \to (\mathfrak{a}, A/k)$ définit une homomorphie de $k^*/\overline{P}_k$ sur $\mathfrak{G}$. Cette homomorphie est une isomorphie. Soit en effet $\mathfrak{a}$ un e. i. n'appartenant pas à $\overline{P}_k$. Il existe un diviseur entier m tel que $\mathfrak{a}U_m$ n'ait aucun point commun avec P_k, donc tel que $\mathfrak{a}$ n'appartienne pas à $P_k U_m = H$. Soit $\overline{H}$ le groupe des idéaux $(\mathfrak{b})$ représentables par des e. i. $\mathfrak{b} \equiv 1 \pmod{m}$ appartenant à H. H est le groupe « défini » par $\overline{H}$ au sens du paragraphe II, car $\overline{H}$ est un groupe de congruence définissable $(\mathrm{mod}\, m)$. Soit Z le corps de classes sur k pour $\overline{H}$, donc aussi pour H. On a $(\mathfrak{a}, Z/k) \neq 1$, et $(\mathfrak{a}, A/k) \neq 1$, ce qui démontre notre proposition. Donc :

Le symbole $(\mathfrak{a}, A/k)$ *établit une isomorphie topologique entre* $k^*/\overline{P}_k$ *et le groupe de Galois* $\mathfrak{G}$ *de* A/k. *Si* Z *est une extension abélienne de* k, $H_{Z/k}$ *se compose des e. i.* $\mathfrak{a}$ *tels que* $(\mathfrak{a}, A/k)$ *appartienne au groupe de Galois de* A/Z. *Inversement, le groupe de Galois de* A/Z *est l'ensemble des* $(\mathfrak{a}, A/k)$ *pour* $\mathfrak{a} \in H_{Z/k}$.

Il en résulte que le corps Z est bien déterminé par la donnée de $H_{Z/k}$. On peut donc dire que Z est corps de classes sur k pour ce groupe. De plus, on a un théorème d'existence qui se formule de la manière suivante :

La famille des groupes $H_{Z/k}$ *pour les diverses extensions abéliennes* Z *de* k *se confond avec la famille des sous-groupes fermés de* k^* *contenant* P_k.