Journal of the Mathematical Society of Japan Vol. 1, No. 3, May, 1951.

Sur la Théorie du Corps de Classes sur le Corps des Nombres Rationnels

S. IYANAGA et T. TAMAGAWA

La théorie du corps de classes, telle qu'elle a été fondée par notre vénéré Maître auquel ce Volume est dédié, donne la perspective à toutes les extensions abéliennes d'un corps de nombres algébriques quelconque de degré fini [1]. Mais il y a des faits qui s'échappent encore à la théorie générale, concernant spécialement la théorie du corps de classes sur le corps des nombres rationnels. Nous en indiquerons deux dans ce qui suit.

Dans le § 1 de ce travail, nous donnerons une forme explicite au symbole de restes normiques de Hasse [2] pour les corps circulaires, et partant, à la correspondance de Chevalley [3] entre le groupe des idèles rationnels et le groupe galoisien de l'extension abélienne maximale du corps des rationnels. Dans le § 2, nous généraliserons la théorie classique du genre des corps quadratiques [4], pour le cas des extensions cycliques du corps des rationnels. Nous n'avons pas réussi à étendre ces resultats pour le cas où le corps de base soit un corps de nombres algébriques quelconque: la formulation même des résultats correspondants pour ce cas général nous semble difficile à trouver.

Notations

Pendant tout le cours de ce travail nous nous servirons des notations suivantes:

R: le corps des nombres rationnels,

R^*: le groupe multiplicatif des éléments $\neq 0$ de R, (le signe * sera employé dans le même sens aussi pour les autres corps)

p: un nombre premier rationnel,

p_∞: le diviseur à l'infini de R,

R_p: le corps des nombres p-adiques,

$R_\infty = R_{p_\infty}$: le corps des nombres réels,

J: le groupe (multiplicatif) des idèles de R,

P: le groupe des idèles principaux de R,

$a = (a_p)$: un idèle de R avec les composantes p-adiques a_p,

A: l'extension abélienne maximale de R,

k : un corps circulaire, c'est-à-dire, une extension abélienne finie de R,
$G(k/R)$: le groupe galoisien de k/R,
$\mathfrak{G}=G(A/R)$: le groupe galoisien de A/R, topologisé d'après Krull.

§ 1 Sur le symbole de restes normiques

Soient G le groupe multiplicatif de toutes les racines de l'unité, et G_p le sous-groupe de G composé de toutes les p^ν-ièmes racines de l'unité ($\nu = 0, 1, 2, \ldots$) pour un p donné. G se décompose alors en produit direct restreint :

$$G=\underset{p}{\Pi'}G_p\,, \tag{1}$$

où p dans le second membre parcourt tous les diviseurs premiers, excepté celui à l'infini, de R.[1]

L'extention abélienne maximale A de R s'obtient d'après Kronecker par l'adjonction à R de tous les éléments de G. Tout élément σ de $\mathfrak{G}=G(A/R)$ induit donc un automorphisme du groupe G, et réciproquement tout automorphisme de G détermine évidemment un élément de $\mathfrak{G}$. G_p étant des sous-groupes caractéristiques de G, σ induit aussi un automorphisme σ_p de G_p, et réciproquement, σ_p pour tous les p déterminent le σ d'après (1).

Soit donc ζ une p^ν-ième racine primitive de l'unité. σ_p induit alors un automorphisme du groupe cyclique $G_{p,\nu}=\{1, \zeta, \zeta^2 \ldots \zeta^{p^\nu-1}\}$, et on aura $\zeta^{\sigma_p}=\zeta^{u_{p,\nu}}$, $u_{p,\nu}$ étant un entier rationnel premier à p. Il est clair que l'on a $u_{p,\nu+1} \equiv u_{p,\nu} (\text{mod. } p^\nu)$, de sorte que $u_{p,\nu}$ converge vers une limite p-adique u_p, quand ν tend vers l'infini. u_p est une unité p-adique, car $u_{p,1}$ est premier à p. Cette unité p-adique u_p caractérise complètement l'automorphisme σ_p, car G_p s'interprète comme la limite inductive de $G_{p,\nu}$. Nous écrirons $\sigma_p = \varphi_p(u_p)$.

Désignons par U_p le groupe multiplicatif des unités p-adiques, et posons

$$U_0=\underset{p}{\Pi'}U_p\,,$$

le symbole Π désignant cette fois le produit direct complet.

---

1) Le symbole Π désignera tantôt le produit des nombres, le produit direct des groupes tantôt restreint, tantôt complet. L'accent au symbole $\underset{p}{\Pi'}$ signifiera toujours que p parcourt seulement les diviseurs premiers finis.

U_p étant topologisé p-adiquement, U_0 est aussi muni de la topologie du produit direct. On a alors

Proposition I U_0 est comme groupe topologique isomorphe à $\mathfrak{G}$.

La démonstration est immédiate par ce qui précède. A $u=\Pi' u_p \in U_0$ correspond $\sigma=\Pi'\sigma_p$, avec les $\sigma_p=\varphi_p(u_p)$.

Nous désignerons par φ_0 l'application isomorphe de U_0 sur $\mathfrak{G}$ donnée par cette Proposition.

Examinons maintenant la structure du groupe des idèles J. Désignons par U_∞ le groupe multiplicatif des nombres positifs de R_∞ et posons $U=U_0\times U_\infty$. Ce groupe U peut être identifié avec un sous-groupe de J. Les éléments de ce sous-groupe U seront appelés les *idèles unitaires*. On a $J=P.U$ par le Théorème fondamental de l'arithmétique élémentaire.

Et, puisqu'on a évidemment $P\cap U=(1)$, nous avons de plus

$$J=P\times U=P\times U_0\times U_\infty, \tag{2}$$

de sorte que tout élément $a\in J$ s'exprime uniquement en forme

$$a=a u_0 u_\infty \tag{2'}$$

avec $a\in P$, $u_0\in U_0$, $u_\infty\in U_\infty$.

Nous poserons

$$\varphi(a)=\varphi_0(u_0). \tag{3}$$

où u_0 est déterminé d'après (2), (2'). φ est alors une application homomorphe du groupe J sur $\mathfrak{G}$, le noyau de l'homomorphisme étant $P\times U_\infty$.

Soit a_p un élément de $R_p{}^*$. a_p peut être identifié avec l'élément de J qui a seule composante non-neutre a_p. Cet élément de J se représente aussi par a_p.

Soit, d'autre part, k un corps circulaire, et $G(k/R)$ le groupe galoisien correspondant. L'homomorphisme naturel de $\mathfrak{G}$ sur $G(k/R)$ se désignera par θ_k. $\theta_k\sigma$ pour $\sigma\in\mathfrak{G}$ sera donc un automorphisme de k/R.

Théorème I On a la formule

$$\theta_k\varphi(a_p)=\left(\frac{a_p, k}{p}\right), \tag{4}$$

le second membre étant le symbole de restes normiques de Hasse.

Démonstration Tous les deux membres de (4) représentent des applications homomorphes de R_p^* dans $G(k/R)$, et satisfassent à la "formule du produit" :

$$\prod_p \theta_k\varphi(a_p) = \prod_p \left(\frac{a_p, k}{p}\right) = 1 \tag{5}$$

pour $\prod_p a_p = a \in P$.

Or, on sait que le symbole de Hasse se caratérise comme l'application homomorphe de R_p^* dans $G(k/R)$ pour tous les p, satisfaisant à (5) pour laquelle on a, à un nombre fini de p près, la formule

$$\left(\frac{a_p, k}{p}\right) = \left(\frac{k}{p}\right)^{-\nu},$$

où $\left(\frac{k}{p}\right)$ est le symbole de Artin, et ν désigne l'entier de sorte que l'on ait $p^{-\nu} a_p \in U_p$.

Il n'y a donc qu'a vérifier que $\theta_k\varphi$ jouit des mêmes propriétés. Comme il est clair que $\theta_k\varphi(\varepsilon_p) = 1$ pour $\varepsilon_p \in U$, d'après la définition même de φ, on a seulement à montrer que

$$\theta_k\varphi(\overline{p}) = \left(\frac{k}{p}\right)^{-1} \tag{6}$$

pour un $\overline{p} \in R_p^*$ avec $p^{-1} \cdot \overline{p} \in U_p$, et cela à un nombre fini de p près.

Prenons un nombre naturel m assez grand pour qu'on ait $R(\zeta) \supset k$, ζ étant une m-ième racine primitive de l'unité. On peut alors supposer $R(\zeta) = k$ sans perdre la généralité. Dans ces conditions, nous vérifierons (6) pour p non diviseurs de m. $\left(\frac{k}{p}\right)$ est alors l'automorphisme $(\zeta \to \zeta^p)$. Il n'y a donc qu'a faire voir que $\varphi(\overline{p})$ opéré sur ζ^p donne ζ.

Soit q^μ un facteur primaire de m. ζ comme un éléme dnte G, se décompose d'après (1) en forme

$$\zeta = \zeta_q \ldots \text{ avec } \zeta_q \in G_q,$$

et l'effet de $\varphi(\overline{p})$ sur ζ se détermine par ceux de $\varphi(\overline{p})$ sur ζ_q. Comme $\overline{p} \in R_p^*$ et $p \neq q$, $\overline{p}$ est en effet une unité q-adique, et puisque $p \in P$, on a de plus $\varphi(\overline{p}) = \varphi(\overline{p}p^{-1})$. $\varphi_q(\overline{p}) = \varphi_q(\overline{p}p^{-1}) = \varphi_q(p^{-1})$, d'où il est aisé à voir que

$$(\zeta_q^p)^{\varphi q(p^{-1})}=\zeta_q,$$

et enfin $(\zeta^p)^{\varphi(p)}=\zeta$ c. q. f. d.

D'après ce Théorème, on serait en droit d'écrire

$$\varphi(a_p)=\left(\frac{a_p, A}{p}\right) \tag{4'}$$

Si l'on introduit dans J la topologie naturelle (voir Weil [5]), P, U_0, U_∞ forment des sous-groupes fermés de J, P discret, U_0 compact, U_∞ localement compact, et J devient le produit topologique de ces trois groupes. φ donne un homomorphisme continu de J sur $\mathfrak{G}$, et si $J \ni a=(a_p)$, le produit infini $\Pi\varphi(a_p)$ converge dans $\mathfrak{G}$, et $=\varphi(a)$. En vertu du Théorème précédant, il est clair qu'on a

Théorème 2 L'application φ définie par (3) donne la correspondance de Chevalley entre J et $\mathfrak{G}$[2].

§ 2 Sur la theorie du genre

Considérons d'abord un corps circulaire arbitraire k. Les groupes des idèles et des idèles principaux de k seront désignés respectivement par J_k, P_k. On connait ce que signifie la norme $N_{k/R}(J_k)=N_k$ de J_k dans R, et que PN_k forme un sous-groupe d'indice $(k:R)$ de J. A tout sous-groupe H de J d'indice fini contenant P correspond un corps circulaire k, de sorte que $H=PN_k$, et $\theta_k\varphi$ du Théorème 1 donne l'isomorphisme entre $G(k/R)$ et J/PN_k.

D'autre part, la décomposition (2) du groupe J indique qu'à tout sous-groupe H de J d'indice fini contenant P correspond biunivoquement un sous-groupe H_0 d'indice fini de U_0, par les relations: $H \to H \cap U_0 = H_0$, $H_0 \to H_0P=H$.

A tout corps circulaire k correspond donc un sous-groupe d'indice fini de U_0, que nous écrirons $H_0(k)$. Il est facile à voir, que le degré de ramification e_p de p dans k est donné par

$$e_p=(U_p : H_0(k) \cap U_p). \tag{7}$$

---

2) Après la rédaction de ce travail, M. Iwasawa nous écrit de Princeton, qu'il connait aussi ce résultat. Nos résultats étant d'ailleurs tellement simples, que nous doutons s'ils ne sont tous connus des connaisseurs de la théorie des idèles. Aussi nous ne prétendon pas à notre priorité en publiant ces résultats. Nous les publions pour la commodité des chercheurs.

On appelle "*différentiels de* R" les caractères de J qui annulent $P \times U_\infty$. Un différentiel χ se détermine évidemment par sa contraction $\bar{\chi}$ sur U_0, et tout caractère $\bar{\chi}$ de U_0 s'étend à un différentiel. Soient χ un différentiel, $\bar{\chi}_p$ le caractère de U_0 ayant la même contraction que χ sur U_p, et de sorte que $\bar{\chi}_p(\varepsilon_q)=1$ pour tout $\varepsilon_q \in U_q$, $q \neq p$. Soit enfin χ_p le différentiel extention de $\bar{\chi}_p$. On a alors évidemment

$$\chi = \prod_p \chi_p , \tag{8}$$

et le degré de ramification e_p de p coincide avec l'ordre de χ_p.

Soit Z l'extension cyclique correspondant à χ. Le degré $(Z:R)$ est alors égal au p.p.c.m. des e_p. Soient J_Z, P_Z, U_Z les groupes des idèles principaux, des idèles unitaires de Z respectivement. Les *idèles unitaires* de Z sont les idèles, dont tous les composantes sont des unités $\mathfrak{p}$-adiques, où $\mathfrak{p}$ sont les diviseurs de Z. Ceci est clair quand $\mathfrak{p}$ est un diviseur fini ; quand $\mathfrak{p}$ est à l'infini, et Z est complexe, tout élément non nul de $Z_\mathfrak{p}$ s'appelle une unité $\mathfrak{p}$-adique, mais quand Z est réel, il convient d'appeler ainsi seuls les éléments *positifs* de $Z_\mathfrak{p}$. Le groupe quotient $J_Z/P_Z U_Z$ est alors isomorphe au groupes des classes d'idéaux *au sens étroit* de Z, et dans le corps des rationnels, $J/PN_{Z/R}(U_Z)$ est isomorphe au groupe quotient $R^*/$(le groupe des restes normiques modulo le conducteur de Z/k).

Dans ce qui suit, nous désignerons les éléments de J_Z par $\mathfrak{a}$, $\mathfrak{b}$,.... Le symbole N signifiera toujours la norme de Z à R sauf avis contraire, σ désignera un élément générateur du groupe $G(Z/R)$. Les deux Propositions suivantes sont des traductions faciles des faits connus en langage des idèles.

Proposition 2 (Lemme de Hilbert) Si $N(\mathfrak{a})=1$, il existe un idèle $\mathfrak{b}$ de sorte qu'on ait $\mathfrak{a}=\mathfrak{b}^{1-\sigma}$ [3]

Proposition 3 (Lemme de Hasse) On a la formule :

$$N(J_Z) \cap P = N(P_Z)^{4)}.$$

De ces Propositions s'ensuit le Théorème suivant.

Théorème 3 Si

---

3) Hilbert l.c. Satz 90. La démonstration de cette Proposition se réduit immédiatement au cas où $\mathfrak{a} = \mathfrak{a}_\mathfrak{p} \in k_\mathfrak{p}^*$. Il faut prendre une précaution spéciale, d'ailleurs facile, au cas où $\mathfrak{p}$ se décompose dans Z. Nous laissons au lecteur le soin de compléter la démonstration.

4) Voir Chevalley l.c. p. 409.

$$N\mathfrak{a} \in PN(U_Z), \tag{9}$$

il existent des idèles $\mathfrak{b}$, $\mathfrak{u} \in U_Z$, et $a_Z \in P_Z$ de soite qu'on ait

$$\mathfrak{a}=\mathfrak{b}^{1-\sigma}\,\mathfrak{u}\,a_Z \tag{10}$$

Démonstration Par l'hypothèse nous pouvons écrire $N\mathfrak{a}=aN\mathfrak{u}$ avec $a \in P$, $\mathfrak{u} \in U_Z$. En vertu de la Proposition 3, on a $a=N(\mathfrak{a}\mathfrak{u}^{-1})=Na_Z$ avec $a_Z \in P_Z$, et par suite, par la Proposition 2, $\mathfrak{a}\mathfrak{u}^{-1}a_Z^{-1}=\mathfrak{b}^{1-\sigma}$, c. q. f. d.

Il va sans dire que de (10) s'ensuit (9). Les idèles de J_Z, pour lesquels (9) ou (10) soit vérifié, forment un sous-groupe H_Z de J_Z. Nous appellerons ce sous-groupe H_Z le *genre principal* de Z, et les éléments du groupe quotient J_Z/H_Z les *genres* de Z.

Cette définition et le Théorème 3 montrent deux choses. 1° On a

$$J_Z \supset H_Z \supset P_Z U_Z,$$

et le nombre des genres $g=(J_Z : H_Z)$ est égal au nombre des éléments C du groupe quotient $J_Z/P_Z U_Z$, pour lesquels on a $C^{1-\sigma}=1$. On appelle ces éléments C les *classes ambiges*. 2° Quand on applique homomorphiquement J_Z dans J/P par la formation de la norme, J_Z tombe sur $PN(J_Z)$ et H_Z sur $PN(U_Z)$. On a donc

$$J_Z/H_Z \cong PN(J_Z)/PN(U_Z). \tag{11}$$

Le Théorème suivant donne une information exacte sur le nombre g.

Théorème 4 On a la formule

$$g=\frac{\prod_p e_p}{n}, \tag{12}$$

où $n=(Z : R)$.

Démonstration On sait que $(J : PN(J_Z))=n$ d'après un résultat fondamental de la théorie du corps de classes. Puisqu'on a d'après (11)

$$\begin{aligned} g&=(J_Z : H_Z)=(JN(J_Z) : PN(U_Z)) \\ &=(J : PN(U_Z))/(J : PN(J_Z)) \\ &=(J : PN(U_Z))/n, \end{aligned}$$

on n'a qu'à montrer

$$(J : PN(U_Z))=\prod_p e_p .$$

Or, comme nous avons fait remarquer au début de ce paragraphe, le groupe quotient $J/PN(U_Z)$ peut être " transféré " sur $U_0/N(U_Z)$ en prenant l'intersection avec U_0. (Ici on fait usage de notre convention sur U_Z concernant les diviseurs à l'infini pour avoir $N(U_Z) \subset U_0$). On a par conséquent

$$\begin{aligned}(J : PN(U_Z)) &= (U_0 : N(U_Z)) \\ &= \prod_p (U_p : N(U_\ ) \cap U_p) \\ &= \prod_p (U_p : H_0(Z) \cap U_p) = \prod_p e_p. \quad \text{c. q. f. d.}\end{aligned}$$

Une condition nécessaire et suffisante pour qu'un élément $\mathfrak{a}$ de J soit contenu dans $PN(U_Z)$ est donnée par

$$\chi_p(\mathfrak{a}) = 1 \qquad \text{pour tous les } p.$$

D'autre part, $\mathfrak{a}$ est contenu dans $PN(J_Z)$, si et seulement si

$$\prod_{p_i} \chi_{p_i}(\mathfrak{a}) = 1,$$

où p_i sont des nombres premiers pour lesquels $\chi_{p_i} \neq 1$, $(i = 1, 2, \ldots, h)$.

Par conséquent, si ζ sont des racines e_{p_i}-ièmes arbitrairement données de l'unité satisfaisant à la seule condition $\prod_{i=1}^{h} \zeta_i = 1$, on peut trouver $\mathfrak{a} \in J_Z$ de sorte qu'on ait

$$\chi_{p_i}(N\mathfrak{a}) = \zeta_i . \qquad i = 1, 2, \ldots, h,$$

et le vecteur $(\zeta_1, \ldots, \zeta_h)$ dépend seulement au genre auquel $\mathfrak{a}$ appartient. Si l'on appelle ce vecteur le *système de caractères* du genre, on peut énoncer le Théorème suivant.

Théorème 5 Les genres de l'extension cyclique Z de R se caractérisent complètement par leurs systèmes de caractères.

Bibliographie

[1] T. Takagi: Ueber eine Theorie des relativ Abelschen Zahlkörpers, Journ. Coll. Sc. Tokyo 41 (1920).

[2] H. Hasse: Die Normenresttheorie relativ Abelscher Zahlkörper als Klassenkörpertheorie im Kleinen, Crelles Journ. 162 (1930).

[3] C. Chevalley: La théorie du corps de classes, Ann. of Math. 41 (1940)

[4] Voir D. Hilbert, Zahlbericht.

[5] A. Weil: Sur la théorie du corps des classes, dans ce même volume.