CLAUDE CHEVALLEY

Sur la théorie du corps de classes dans les corps finis et les corps locaux

Thèses de l'entre-deux-guerres, 1934

<http://www.numdam.org/item?id=THESE_1934__155__365_0>

Sur la théorie du corps de classes dans les corps finis et les corps locaux

par

Claude CHEVALLEY à Paris.

Introduction

La théorie des corps de nombres algébriques a été développée pour étudier certaines questions d'arithmétique élémentaire : principalement le théorème de Fermat ainsi que la théorie des formes quadratiques, à propos desquelles Gauss introduisait déjà les nombres $a + bi$, a et b étant des entiers ordinaires, $i = \sqrt{-1}$. Mais la théorie ne se constitua vraiment en corps de doctrines indépendant que quand Kummer et Dedekind eurent surmonté la difficulté qui avait arrêté Gauss, à savoir que les théorèmes fondamentaux (plus grand commun diviseur, décomposition en facteurs premiers) de l'arithmétique ordinaire ne s'étendent pas aux entiers algébriques. Ces deux auteurs ont montré qu'on retrouvait toutes ces lois en remplaçant la notion de nombre par la notion d'idéal[1]. Dans chaque corps de nombres algébriques fini k, on trouve une infinité d'idéaux premiers $\mathfrak{p}$, et tous les idéaux sont composés à partir de ceux-là exactement comme les nombres rationnels à partir des nombres premiers. Mais ces idéaux premiers ne restent plus des idéaux premiers dans un corps k' contenant k, et une question essentielle de la théorie va être la suivante : comment les idéaux de k vont ils se représenter comme produits d'idéaux premiers de k'.

Etant donné un idéal premier déterminé de k, on sait répondre à la question (voir notamment les travaux de O. Ore). Mais le problème est de trouver une loi générale de décomposition, permettant de trouver a priori tous les idéaux premiers ayant une loi de décomposition déterminée.

---

1) On trouvera dans les travaux de Mlle. Noether exposés notamment dans " Van der Waerden, Moderne Algebra ", une analyse très générale et profonde de la notion d'idéal qui a conquis l'algèbre et la géométrie analytique après l'arithmétique.

Ce problème n'est résolu que dans un cas particulier, celui où k' est relativement abélien par rapport à k et il est résolu dans ce cas par la théorie des corps de classes. Le principe de cette théorie remonte à Hilbert. Probablement par analogie avec ce qui se passe dans certains cas particuliers (sur-corps d'un corps quadratique imaginaire étudiés par Kronecker), Hilbert appelle corps de classes par rapport à k un sur-corps k' relativement abélien non ramifié (c'est-à-dire qu'aucun idéal premier de k n'est divisible par le carré d'un idéal premier de k'), et il admet les faits suivants: (Ueber die Theorie der relativ Abelschen Zahlkörper, Götting. Nachr. 1898)

1) k' étant corps de classes par rapport à k, il y a un sous-groupe H du groupe A des classes d'idéaux de k, tel que les idéaux premiers de H et ceux-là seuls se décomposent dans k' en idéaux de degré relatif 1. Si $\mathfrak{p}$ n'appartient pas à H, soit $\mathfrak{p}'$ la plus petite puissance de $\mathfrak{p}$ appartenant à H: $\mathfrak{p}$ se décompose dans k' en idéaux de degré relatif f.

2) Le groupe A/H est isomorphe au groupe de Galois de K par rapport à k.

3) Il existe un corps de classes maximum pour lequel le groupe H se réduit à la classe unité. Pour tout groupe de classes H, il existe un corps de classes et un seul qui est contenu dans ce corps maximum.

4) Les idéaux de k deviennent tous des idéaux principaux dans le corps de classes maximum.

Hilbert démontre des cas particuliers de ces propositions. Furtwängler, reprenant les méthodes de Hilbert, démontre dans leur généralité les 3 premières propositions (Furtwängler, Allgemeiner Existenzbeweis für den Klassenkörper eines beliebigen algebraischen Zahlkörpers, Math. Ann. 63, 1907).

La théorie n'incluait encore qu'une partie de l'étude des sur-corps relativement abéliens. L'idée de la généralisation aux corps relativement abéliens quelconques remonte à Weber qui proposa de remplacer dans la définition du corps de classes, les classes ordinaires par des groupes plus restreints d'idéaux, obtenus en appelant classe principale l'ensemble des idéaux principaux représentables par un nombre α qui est $\equiv 1$ modulo un idéal fixe (Weber, Ueber Zahlengruppen in algebraischen Körpern, Math. Ann. 48, 49, 50, 1897–1898). Mais il n'a pu au moyen de cette définition démontrer les théorèmes 1, 2.

La première théorie générale du corps relativement abélien a été donnée par Takagi (Ueber eine Theorie des relativ Abelschen Zahlkörpers, Journal Coll. Science, Tokyo, 41, 1920), qui a montré le premier comment on pouvait explicitement donner le groupe H pour

lequel un corps est corps de classes. Dans la théorie de Takagi, on construit tout d'abord le groupe H, et on appelle k' corps de classes si ce groupe H est d'indice égal au degré relatif de k'. On démontre alors les propriétés 1, 2, 3.

Un autre problème fondamental de la théorie des corps de nombres algébriques est celui de l'obtention de lois de réciprocité entre les nombres algébriques, analogues à la loi de réciprocité quadratique. Ce problème est en effet intimement lié au théorème de Fermat. Cette théorie s'est développée parallèlement à celle du corps de classes. Le lien profond entre ces deux théories est constitué par la *loi fondamentale de réciprocité* de M. Artin (Beweis des allgemeinen Reziprozitätsgesetzes, Abhand. Math. Sem. Hamburg, 5, 1927) qui permet de réaliser effectivement l'isomorphie entre le groupe A/H et le groupe de Galois relatif d'un corps de classes. Toutes les lois de réciprocité connues sont des conséquences de cette loi générale.

On trouvera exposée la théorie du corps de classes et celle des lois de réciprocité dans un ouvrage de M. Hasse "Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper."[1 bis)]

La théorie de Takagi, qu'on trouvera exposée dans le mémoire cité de Takagi ou dans le Bericht de Hasse, présente l'inconvénient d'être extrêmement compliquée, et, à son point de départ, assez artificielle. On trouvera dans ce travail un exposé nouveau de la théorie du corps de classes.

L'affirmation essentielle de la théorie nous a paru pouvoir se décomposer en deux parties: l'une affirme que les lois de décomposition dépendent d'une division en classes des idéaux définie par un certain sous-groupe H du groupe des idéaux; la seconde précise quel est ce groupe H; or la première assertion est intimement liée à la loi générale de réciprocité. Nous démontrons d'abord ici (théorème A du chap. VI), qu'on peut construire un groupe H pour lequel les propriétés 1, 2 sont vraies. Nous appelons ce groupe le groupe de Artin associé au surcorps. La démonstration est très courte et n'exige pas l'emploi des moyens analytiques (fonctions ζ, séries $L(s, \chi)$, etc). Il faut ensuite démontrer que ce groupe H coïncide avec le groupe défini par Takagi (théorème B du chapitre VI). Nous montrons que si cela est vrai pour les corps relativement circulaires (obtenus par adjonction de racines de

1 bis) Parue aussi dans Jahresbericht Deutscher Mathematiker-Vereinigung, 35 (1926) et Ergänzungsband VI (1930).

l'unité), cela est toujours vrai—et cela par une réduction purement arithmétique.—Au contraire pour démontrer que la proposition est vraie dans le cas des corps circulaires, nous sommes obligés d'employer les moyens analytiques. La démonstration ainsi obtenue est plus simple que celle de la théorie de Takagi-Hasse, car elle évite la réduction du cas "cyclique de degré l premier" au cas "cyclique de degré l^n", réduction qui était extrêmement compliquée. La simplification provient de l'emploi d'un théorème dû à Herbrand (théorème des unités) et d'un mode de raisonnement qui a été depuis systématisé par Herbrand sous la forme d'un lemme de théorie des groupes (lemme de Herbrand). De plus, nous obtenons en même temps que le théorème réciproque, la loi de réciprocité de M. Artin qui exigeait antérieurement une démonstration séparée.

La démonstration de la propriété 3 (théorème d'existence) est également nouvelle et plus simple que dans l'ancienne théorie. Le principe de cette démonstration a été trouvé simultanément par Herbrand et par l'auteur, d'une manière indépendante. Enfin, le fait que nous possédons déjà la loi de réciprocité nous permet d'éviter les réductions successives de la démonstration du théorème d'existence dans la théorie de Takagi-Hasse.

D'autre part, nous avons développé entièrement la théorie du corps de classes "local", c'est-à-dire des extensions abéliennes des corps de nombres p-adiques de Hensel. Cette théorie est identique à la théorie des restes normiques, dont l'origine remonte à Hilbert. Elle avait été faite pour les corps abéliens par Hasse: "Die Normenresttheorie relativ Abelscher Zahlkörper als Klassenkörpertheorie im Kleinen, Journal de Crelle, 162, 1930", et Schmidt: "Zur Klassenkörpertheorie im Kleinen, Journal de Crelle, 162, 1930)," d'une manière indirecte, comme conséquence de la théorie du corps de classes. Nous donnons ici des démonstrations directes et purement arithmétiques.[1ter] Nous fondons également la théorie des restes normiques pour les sur corps non relativement abéliens, ce qui donne un des rares résultats connus de la théorie de ces corps.

Nous avons cherché à rester aussi élémentaires que possible au cours de ce travail. Nous présupposons connue la théorie élémentaire des idéaux d'un corps de nombres algébriques (on en trouvera un exposé très clair dans le livre de M. Hecke, Theorie der algebraischen

1ter) Depuis que ces lignes ont été écrites, j'ai appris que M. Schmidt a aussi développé, mais sans la publier, une théorie directe du corps de classes local. Cette théorie est différente de celle ici exposée.

Zahlen); la théorie de Galois et les faits fondamentaux de la théorie des groupes finis (voir notes 2 et 12).

Le chapitre I est consacré à la théorie des groupes. Nous y rappelons les faits qui nous serviront dans la suite et y démontrons quelques lemmes qui seront d'application constante.

Le chapitre II est consacré à la démonstration de quelques résultats de la théorie des groupes de décomposition et d'inertie de Hilbert.

Le chapitre III définit les groupes de congruence de Weber et donne leurs propriétés essentielles.

Le chapitre IV contient les résultats fondamentaux de la théorie des corps relativement cycliques, théorème normique de Hilbert, théorie des corps kummériens. Les démonstrations de ces théorèmes sont nouvelles. On y trouvera aussi un théorème inédit sur la base relative d'un corps galoisien, qui est démontré par une méthode analogue à celle employée par Herbrand pour le théorème des unités. La démonstration qu'on en donne est dûe à Monsieur Hasse, qui a bien voulu nous la communiquer, après lecture d'une démonstration antérieure et plus compliquée de l'auteur. Ce théorème a été également démontré par M. Deuring, mais par des méthodes différentes.

Le chapitre V est consacré à l'étude des "valeurs absolues" d'un corps de nombres algébriques, en particulier des corps de nombres p-adiques de Hensel. La démonstration qu'on y trouvera du fait que toutes les valeurs absolues possibles sont celles des types connus est une legère modification d'une démonstration trouvée cette année par M. Artin (la première démonstration remonte à Ostrowski).

Le chapitre VI pose la définition du corps de classes et contient les énoncés des théorèmes fondamentaux A et B dont nous avons parlé, ainsi que la démonstration du théorème A.

Le chapitre VII est consacré aux corps circulaires, dont l'étude est nécessaire pour le démonstration du théorème B qui fait l'objet du chapitre VIII. Le chapitre IX contient la théorie du corps de classes local, et le chapitre X la démonstration du théorème d'existence.

La plupart des résultats de ce travail ont été communiqués à l'Académie des Sciences de Paris dans des notes: Sur la théorie des Restes Normiques, C. R. 1930, p. 246; Nouvelle Démonstration du Théorème d'Existence en théorie du Corps de Classes (en collaboration avec J. Herbrand), 1931, p. 814; Sur la Structure de la Théorie du Corps de Classes, 1932.

Qu'il me soit permis d'exprimer ici ma reconnaissance à Monsieur Garnier dont les conseils m'ont été précieux; à Messieurs Vessiot et

Montel, qui ont bien voulu s'intéresser à mes travaux, à Monsieur Artin et à Monsieur Hasse qui m'ont permis de faire connaître ici diverses simplifications de la théorie, et enfin à Monsieur Iyanaga qui a bien voulu relire avec moi ce travail.

De plus, je remercie aussi vivement la Faculté des Sciences de l'Université de Tokyo, et tout particulièrement Monsieur Takagi, qui a bien voulu proposer ce mémoire pour l'impression dans ce Journal.

Chapitre I.

Démonstration de quelques lemmes de théorie des groupes.

Nous n'aurons presque à considérer au cours de ce travail que des groupes abéliens. Nous allons ici donner quelques propriétés de ces groupes, qui seront d'un usage constant.[2]

Tout d'abord, rappelons qu'un ensemble d'éléments est dit former un *groupe* quand il existe une loi de composition entre les éléments de cet ensemble jouissant des propriétés suivantes:

1) A et B étant deux éléments, la loi de composition definit un troisième élément C représenté par AB et défini univoquement par la donnée de A, B.

2) On a $A(BC) = (AB)C$.

3) L'égalité $AB = AB'$ entraîne $B = B'$. L'égalité $AB = A'B$ entraîne $A = A'$.

4) A et B étant deux éléments quelconques, il y a un élément X tel que $AX = B$, et un élément Y tel que $YA = B$.

De ces axiomes résulte l'existence et l'unicité d'un élément E, appelé élément unité, (et généralement représenté par 1) tel que $AE = A$ pour tout élément du groupe. Si $AB = E$ on a aussi $BA = E$, et l'élément B se représente par A^{-1}.

G étant un groupe, un ensemble d'éléments de G qui, en vertu de la loi de composition régnant dans G forme lui-même un groupe, est appelé un *sous-groupe*. L'ensemble formé de tous les éléments de G et l'ensemble formé du seul élément unité sont des sous-groupes. Les sous-groupes différant des précédents sont appelés sous-groupes propres.

Les principaux groupes que nous aurons à considérer seront:

Le groupe des nombres $\neq 0$ d'un corps de nombres algébriques, la loi de composition étant la multiplication.

Le groupe des idéaux (éventuellement des idéaux premiers à un idéal donné) d'un corps algébrique, la loi de composition étant la multiplication.

Le groupe des nombres d'un corps, la loi de composition étant l'addition. (Quand nous parlerons simplement d'un groupe de nombres, nous conviendrons que la loi de composition est la muliplication;

2) Voir pour la théorie des groupes finis, par exemple: de Séguier, Eléments de la théorie des groupes abstraits, Gauthier-Villars, 1904 ou Speiser, die Theorie der Gruppen von endlicher Ordnung, 2me. édition, Springer, 1927.

quand nous voudrons parler d'un groupe de nombres dans lequel la loi de composition est l'addition, nous dirons groupe additif).

Le groupe des automorphismes d'un corps ou groupe de Galois.

Et certains groupes dérivés des précédents.

Un groupe est dit abélien quand la loi de composition est commutative, c'est-à-dire quand pour deux éléments quelconques A, B on a : $AB = BA$. C'est le cas des groupes que nous venons d'énumérer, sauf éventuellement des groupes de Galois.

G étant un groupe abélien, et H un sous-groupe, on appelle *classe* de G suivant H (en allemand Nebengruppe) l'ensemble $\mathfrak{K}$ des éléments de G ne différant de l'un d'eux A que par multiplication par un élément X de H. A est dit un *représentant* de $\mathfrak{K}$. Tout élément de $\mathfrak{K}$ est un représentant. Le fait remarquable est que ces classes $\mathfrak{K}$ forment elles-mêmes un groupe. En effet, soient deux classes $\mathfrak{K}$, $\mathfrak{K}'$. Choisissons dans chacune un représentant ; soient A, A' ces éléments. Soit $\mathfrak{K}''$ la classe qui contient AA'. On s'assure immédiatement que $\mathfrak{K}''$ ne dépend pas de la manière dont A, A' ont été choisis dans $\mathfrak{K}$, $\mathfrak{K}'$: $\mathfrak{K}''$ ne dépend que de $\mathfrak{K}$, $\mathfrak{K}'$ et nous poserons $\mathfrak{K}'' = \mathfrak{K}\mathfrak{K}'$. On montre facilement que cette loi de composition satisfait aux propriétés 1, 2, 3, 4, énoncées plus haut. Donc ces classes $\mathfrak{K}$ forment un groupe qu'on appelle *groupe quotient* de G par H.

Cette notion ne se généralise pas entièrement pour un groupe G quelconque. Il faut encore que H soit un sous-groupe *invariant* de G, c'est-à-dire que, A étant un élément de G, et X un élément de H, $A^{-1}XA$ soit encore dans H. Dans ces conditions, A étant un élément de G, et X parcourant les éléments de H, les ensembles d'éléments AX et XA sont identiques et forment une classe $\mathfrak{K}$. Ces classes $\mathfrak{K}$ forment encore un groupe qui sera le groupe quotient.

Notations. Ce groupe quotient se désigne par G/H. Tout élément de G appartient à un élément de G/H, qu'on appelle sa classe (mod. H). Si deux éléments A, A' appartiennent au même élément de G/H, on dit que A, A' sont congrus mod. H et on écrit $A \equiv A'$ (mod. H). Ces congruences peuvent être multipliées membre à membre. La congruence $A \equiv A'$ (mod. H) a lieu si et seulement si AA'^{-1} est dans H.

G étant un groupe, et A, A',.....étant des éléments (ou des systèmes d'éléments) de G, on désignera par $(A, A', \ldots\ldots)$ le plus petit groupe contenu dans G et contenant tous ces éléments (ou tous les éléments de tous ces systèmes). g, g' désignant deux sous-groupes, (g, g') sera encore représenté par gg'. L'ensemble des éléments communs à g, g', ensemble qui forme un groupe, sera désigné par $[g, g']$.

Si G est un groupe ne contenant qu'un nombre fini d'éléments, ce nombre est appelé ordre de G. Rappelons (théorème de Cauchy) que dans ce cas l'ordre de tout sous-groupe est un diviseur de l'ordre du groupe.

Si H est un sous-groupe invariant de G et si G/H ne contient qu'un nombre fini d'éléments, on dit que H est d'indice fini dans G et le nombre d'éléments de G/H est appelé indice de H dans G et représenté par $(G:H)$. Si H' est un sous-groupe invariant de G contenant H, on a

$$(G:H) = (G:H')(H':H).$$

Si G ne contient qu'un nombre fini d'éléments et s'il existe un élément A_0 tel que tout élément de G soit de la forme A_0^x, on dit que G est cyclique. (A_0^x se définit pour les entiers x positifs, négatifs, ou nuls par les formules

$$A_0^0 = 1, \quad A_0^{1+x} = A_0 A_0^x, \quad A_0^{x-1} = A_0^x A_0^{-1}.)$$

Si G est un groupe quelconque ne contenant qu'un nombre fini d'éléments, A étant un de ses éléments, le groupe (A) est un groupe cyclique. Son ordre est appelé *ordre de* A dans G.

Homomorphie. Isomorphie.

Soient G, G' deux groupes. Supposons qu'il existe une loi associant à tout élément A de G un élément univoquement défini A' de G' (nous écrirons $A \to A'$) jouissant de la propriété suivante: si aux éléments A, B de G sont associés les éléments A', B', à l'élément AB est associé l'élément $A'B'$; nous dirons que la loi définit une représentation de G dans G'; l'ensemble des éléments de G' qui se trouvent correspondre à des éléments de G forme un sous-groupe de G' qui est appelé image de G dans la représentation. Si ce sous-groupe est égal à G' lui-même, la représentation est appelée *homomorphie*; on dit que G est homomorphe à G' et on écrit $G \sim G'$. Si enfin à deux éléments distincts de G sont associés des éléments distincts de G', on dit que G est *isomorphe* à G' et on écrit $G \simeq G'$.[3] [4]

Si H est un sous-groupe invariant de G, le groupe G est toujours homomorphe à G/H, la loi de correspondance étant la loi qui associe à tout élément de G la classe (mod. H) à laquelle il appartient.

Lemme 1 (Principe de réduction de Hasse). *Soient G, H deux*

3) Ces mots d'homomorphisme et d'isomorphisme sont plus commodes que les mots " isomorphisme meriédrique " et " isomorphisme holoédrique " souvent employés.

4) Un homomorphisme d'un groupe sur lui-même est encore appelé automorphisme.

groupes abéliens (sous-groupes d'un même groupe quelconque). Les groupes GH/H et $G/[G, H]$ sont isomorphes.[5]

Soit $\mathfrak{K}$ un élément quelconque de $G/[G, H]$. C'est le système des éléments de G ne différant de l'un d'eux A que par multiplication par un élément X de $[G, H]$. Tous les éléments AX appartiennent à GH et ne diffèrent de A que par multiplication par un élément X de H. Ils appartiennent donc à une classe $\mathfrak{K}'$ de GH/H. Nous dirons que $\mathfrak{K}'$ est la classe associée à $\mathfrak{K}$. Si $\mathfrak{K}_1 \to \mathfrak{K}_1'$, $\mathfrak{K}_2 \to \mathfrak{K}_2'$, à $\mathfrak{K}_1\mathfrak{K}_2$ correspond $\mathfrak{K}_1'\mathfrak{K}_2'$. Donc nous avons une représentation. Si d'autre part $\mathfrak{K}'$ est une classe de GH/H, $\mathfrak{K}'$ contient un élément AX, A étant dans G et X dans H. Si $\mathfrak{K}$ est la classe de G (mod. $[G, H]$) qui contient A, $\mathfrak{K} \to \mathfrak{K}'$. Donc la correspondance est une homomorphie. Enfin si aux classes $\mathfrak{K}_1$, $\mathfrak{K}_2$ est associée la même classe $\mathfrak{K}'$, il en résulte que, A_1 désignant un élément de $\mathfrak{K}_1$ et A_2 un élement de $\mathfrak{K}_2$, $A_1A_2^{-1}$ est dans H. Mais cet élément est aussi dans G, donc dans $[G, H]$ et on a $\mathfrak{K}_1 = \mathfrak{K}_2$. La correspondance est donc une isomorphie.

Lemme 2 (Principe d'isomorphie de Hasse). *Si un groupe abélien G est homomorphe à un groupe G'/H', les éléments de G dont le correspondant dans cette homomorphie est H' forment un groupe H. Les groupes G/H, G'/H' sont isomorphes.*

Soit A un élément de G; désignons par $\mathfrak{K}'_A$ la classe (mod. H') qui lui est associée par l'homomorphie donnée. Donc

$$\mathfrak{K}'_{A_1A_2} = \mathfrak{K}'_{A_1}\mathfrak{K}'_{A_2}.$$

Si A_2 est dans H, on a $\mathfrak{K}'_{A_1A_2} = \mathfrak{K}'_{A_1}$. Donc $\mathfrak{K}'_A$ ne dépend que de la classe $\mathfrak{K}$ (mod. H) à laquelle appartient A. On voit tout de suite que la correspondance $\mathfrak{K} \to \mathfrak{K}'$ est une isomorphie de G/H et de G'/H'.

Nous emploierons dans la suite une méthode de notations due à M. Hasse qui permet de simplifier beaucoup l'écriture. On désignera par une lettre spéciale des éléments jouissant d'une certaine propriété, éléments qui seront en général des nombres ou des idéaux. La propriété étant supposée telle que le produit de deux éléments ayant la propriété ait encore la propriété, l'ensemble des éléments ayant la propriété considérée forme un groupe que l'on désigne encore par la même lettre que ses éléments.

Par exemple désignons par α les nombres ayant une propriété P; les idéaux principaux représentables par un nombre ayant la propriété P seront désignés par (α), et les unités par ε. Soit β un sous-groupe

5) Le théorème est encore vrai si G, H sont des groupes quelconques, à condition que H soit un sous-groupe invariant de GH. Car alors $[G, H]$ est aussi invariant dans G et le théorème se démontre de la même manière.

d'indice fini du groupe α. Nous nous proposons de comparer les nombres $((\alpha):(\beta))$ et $(\alpha:\beta)$. On a

$$(\alpha:\beta)=\frac{(\alpha\varepsilon:\beta)}{(\alpha\varepsilon:\alpha)}=\frac{(\alpha\varepsilon:\beta\varepsilon)\,(\beta\varepsilon:\beta)}{(\alpha\varepsilon:\alpha)}.$$

D'après le lemme 1, on a $\alpha\varepsilon/\alpha\simeq\alpha/[\alpha,\varepsilon]$, $\beta\varepsilon/\beta\simeq\beta/[\beta,\varepsilon]$. D'après le lemme 2, on a $(\alpha\varepsilon:\beta\varepsilon)=((\alpha):(\beta))$. D'où

$$(\alpha:\beta)=((\alpha):(\beta))\,\frac{(\beta:[\beta,\varepsilon])}{(\alpha:[\alpha,\varepsilon])}$$

La formule est valable toutes les fois que les indices qui y figurent sont finis.

Lemme 3 (Lemme de Herbrand). *Soient G un groupe; g un sous-groupe de G d'indice fini, T_1 et T_2 deux homomorphismes de G sur lui-même tels que pour tout élément A de G on ait $T_1T_2(A)=T_2T_1(A)=1$, et que $T_1g\subset g$, $T_2g\subset g$, $\gamma_i(i=1,2)$ le groupe des éléments A tels que $T_i(A)=1$. On a*

$$\frac{(\gamma_1:T_2G)}{(\gamma_2:T_1G)}=\frac{([g,\gamma_1]:T_2g)}{([g,\gamma_2]:T_1g)},$$

la formule devant être interprètée dans ce sens que si les indices qui figurent au second membre sont tous deux finis il en est de même de ceux qui figurent au premier membre et les deux membres sont égaux.

En effet écrivons

$$(G:g)=(G:g\gamma_2)\,(g\gamma_2:g).$$

En vertu du lemme 2, $(G:g\gamma_2)=(T_2G:T_2g)$. En vertu du lemme 1, $(g\gamma_2:g)=(\gamma_2:[g,\gamma_2])$. Par hypothèse $([g,\gamma_2]:T_1g)$ est fini. Comme $(\gamma_2:[g,\gamma_2])$ est fini,

$$(\gamma_2:T_1g)=(\gamma_2:[g,\gamma_2])\,([g,\gamma_2]:T_1g)$$

et $(\gamma_2:T_1g)$ est fini, donc à fortiori $(\gamma_2:T_1G)$ (T_1G est contenu dans γ_2 en vertu de $T_2T_1(A)=1$ pour tout A). De plus on a

$$(G:g)=(T_2G:T_2g)\,\frac{(\gamma_2:T_1g)}{([g,\gamma_2]:T_1g)}=(T_2G:T_2g)\,(T_1G:T_1g)\,\frac{(\gamma_2:T_1G)}{([g,\gamma_2]:T_1g)}.$$

On a une formule analogue en permutant les indices 1 et 2 dans le calcul qu'on vient de faire; en divisant ces formules membre à membre, on obtient le resultat cherché.

Produit direct. Base d'un groupe abélien fini.

Soient $G_1, G_2,\ldots, G_r$ des groupes. Considérons formellement tous les systèmes S obtenus en prenant dans chacun des G_i un élément A_i. Nous écrirons $S=(A_1, A_2,\ldots, A_r)$; S et S' étant deux de ces systèmes:

$$S=(A_1, A_2,\ldots, A_r),\qquad S'=(A_1', A_2',\ldots, A_r'),$$

appelons produit de ces deux systèmes le système

$$SS' = (A_1A_1', A_2A_2', \cdots, A_rA_r').$$

On voit tout de suite que cette loi de composition des systèmes S a les caractères 1), 2), 3), 4) énoncés plus haut. Donc les systèmes S forment un groupe qu'on appelle *produit direct* des G_i et qu'on désigne par $G_1 \times G_2 \times \cdots \times G_r$. Ce produit direct contient un sous-groupe isomorphe à G_i composé des éléments $(1, 1, \cdots, A_i, \cdots, 1)$ où A_i parcourt les éléments de G_i. On désignera encore généralement par A_i l'élément précédent. On a

$$(A_1, A_2, \cdots, A_r) = \prod_i A_i, \qquad A_iA_j = A_jA_i$$

et les A_i sont appelés les composants de $(A_1, A_2, \cdots, A_r)$. La condition nécessaire et suffisante pour que $\Pi A_i = 1$ est que tous les A_i soient égaux à 1.

Si chacun des G_i est d'ordre fini N_i, leur produit direct a pour ordre le produit des N_i.

Ceci posé, soit G un groupe abélien fini quelconque. On a le théorème fondamental suivant :

Théorème de la base. *Un groupe abélien fini G est produit direct de groupes cycliques.*

1) Soit N l'ordre de G et soit $N = \prod_{i=1}^{r} p_i^{\alpha_i}$ la décomposition de N en facteurs premiers. G étant abélien les éléments σ dont l'ordre est une puissance de p_i forment un groupe G_{p_i}.[6] Déterminons pour chaque i un entier n_i tel que

$$n_i \prod_{j \neq i} p_j^{\alpha_j} \equiv 1 \qquad (\text{mod. } p_i^{\alpha_i})$$

et à tout élément σ de G associons l'élément

$$T_i\sigma = \sigma^{n_i \Pi_{j \neq i} p_i^{\alpha_j}}.$$

$T_i\sigma$ est toujours dans G_{p_i}, et si σ est dans G_{p_i}, $T_i\sigma$ est égal à σ. Associons maintenant à σ l'élément $(T_1\sigma, \cdots, T_r\sigma)$ du produit direct des G_{p_i}. La formule $\sigma = \Pi T_i\sigma$ montre immédiatement qu'on a un isomorphisme de G et de ce produit direct.

2) Il suffit donc de démontrer le théorème dans le cas où $N = p^a$, p étant un nombre premier. Déterminons par récurrence une suite de sous-groupes G_i de G de la manière suivante : $G_0 = 1$; G_{i-1} étant déterminé, on a $G_i = (G_{i-1}, \sigma_i')$ où σ_i' est parmi les éléments de G un de ceux qui

6) En effet, si $\sigma^{p^\alpha} = 1$, $\sigma'^{p^\beta} = 1$, $\beta \geqslant \alpha$, on a $(\sigma\sigma')^{p^\beta} = \sigma^{p^\beta}\sigma'^{p^\beta} = 1$.

appartiennent dans G/G_{i-1} à une classe (mod. G_{i-1}) d'ordre maximum p^{n_i}. Donc $n_{i+} \leq n_i$. Démontrons par récurrence le théorème suivant: il existe dans G_i un élément d'ordre égal à p^{n_i}, soit σ_i; tout élément de G_i se met sous la forme $\prod_{j=1}^{i} \sigma_j^{x_j}$; si σ est un élément de G et si $\sigma^{p^{n_{i+1}}} = \prod_{j=1}^{i} \sigma_j^{\eta_j}$, on a $\eta_j \equiv 0$ (mod. $p^{n_{i+1}}$). Supposons le théorème démontré pour $i-1$ et soit $\sigma_i'^{p^{n_i}} = \sigma_1^{\xi_1} \ldots \sigma_{i-1}^{\xi_{i-1}}$. Donc les ξ_i sont tous $\equiv 0$ (mod. p^{n_i}). Posons

$$\sigma_i = \sigma_i' \sigma_1^{-\xi_1 p^{-n_i}} \sigma_2^{-\xi_2 p^{-n_i}} \ldots \sigma_{i-1}^{-\xi_{i-1} p^{-n_i}}.$$

La plus petite puissance de σ_i dans G_{i-1} est $\sigma_i p^{n_i}$ et ce dernier élément est égal à 1. On a donc $G_i = G_{i-} \times (\sigma_i)$, et, τ désignant un élément de G, soit $\tau^{p^{n_{i+1}}} = \sigma_1^{\xi_1} \ldots \sigma_i^{\xi_i}$, d'où $\tau^{p^{n_i}} = \sigma_1^{\xi_1 p^{n_i - n_{i+1}}} \ldots \sigma_i^{\xi_i p^{n_i - n_{i+1}}}$. Or cet élément est dans G_{i-1}, donc le dernier facteur est égal à 1, et pour $j < i$, $\xi_i p^{n_i - n_{i+1}}$ est divisible par p^{n_i}, ce qui démontre le lemme pour la valeur i.

On a $G_i = (\sigma_1) \times (\sigma_2) \times \ldots \times (\sigma_i)$, et, l'ordre de G_i augmentant constamment avec i, G_i est égal à G pour une valeur assez grande de i, ce qui démontre le théorème[7].

Les éléments σ_i construits sont tels que tout élément de G se mette d'une manière et d'une seule sous la forme $\sigma = \Pi \sigma_i^{x_i}$, $0 \leq x_i < p^{n_i}$. On dit qu'ils forment une base de G.

Nous aurons souvent à utiliser le fait suivant: soit A un groupe abélien, et soit H un sous-groupe de A d'indice fini. Donc le groupe A/H est fini, et par suite produit direct de groupes cycliques, que nous pouvons mettre sous la forme K_i/H, les K_i étant des sous-groupes de A contenant $H (i = 1, 2, \ldots, r)$. Soit H_i le groupe composé des K_j, $j \neq i$. Le groupe A/H_i est cyclique comme isomorphe à K_i/H, car tout élément de A se met sous la forme ax, où a est dans K_i, x dans H_i. De plus H est la partie commune aux H_i. En effet, un élément de A/H se met sous la forme $a_1 a_2 \ldots a_r$, où a_i est dans K_i/H, et il n'appartient à H_i/H que si $a_i = 1$. Cet élément n'est donc H lui-même que si tous les a_i sont égaux à 1.

Réciproquement si les H_i sont des sous-groupes de A d'indices finis n_i, soit H leur partie commune. Si $(A : H)$ est égal au produit des n_i, le groupe A/H est produit direct des groupes A/H_i. En effet, associons à chaque élément a de A l'élément $a_1 a_2 \ldots a_r$ du produit direct des A/H_i, a_i étant la classe modulo H_i qui contient a. On a un homomorphisme de A sur le produit direct des A/H_i. Si chacun des a_i est égal à 1, a doit

7) Cette élégante démonstration est dûe à M. de Séguier, loc. cit. (2).

être dans chacun des H_i, donc dans H. Donc on a une isomorphie de A/H sur un sous-groupe du produit direct des A/H_i. Si $(A : H)$ est égal au produit des n_i, ce sous-groupe est égal au produit direct lui-même.

Les mêmes considérations faites en remplaçant A/H par le groupe de Galois d'une extension relativement abélienne montrent que : si K est relativement abélien par rapport à k, K est composé de corps K_i relativement cycliques par rapport à k, et le groupe de Galois de K est isomorphe au produit direct des groupes de Galois des K_i. Cette isomorphie peut être réalisée en associant à chaque automorphisme σ de K l'automorphisme σ_i de K_i qu'on obtient en soumettant les nombres de K_i à l'automorphisme σ.

Réciproquement, si les K_i sont des corps relativement cycliques par rapport à k, le corps K composé des K_i a un groupe de Galois qui, au moyen de la correspondance précédente, est isomorphe à un sous-groupe du produit direct des groupes de Galois des K_i. Si le degré de K par rapport à k est le produit des degrés relatifs des K_i, ce sous-groupe est le produit direct tout entier.

Caractères d'un groupe abélien fini.

Soit G un groupe abélien fini. On appelle caractère de G toute fonction $\chi(\sigma)$ d'un élément de G qui est $\neq 0$ et qui satisfait à la condition suivante : Si σ, σ' sont deux éléments quelconques, on a

$$\chi(\sigma\sigma') = \chi(\sigma) \cdot \chi(\sigma').$$

Il en résulte $\chi(\sigma) = \chi(\sigma)\chi(1)$. Donc $\chi(1) = 1$. Si $\sigma^n = 1$, on a $(\chi(\sigma))^n = 1$. Donc $\chi(\sigma)$ est toujours une racine de l'unité. Supposons G décomposé en produit direct de groupes cycliques G_i, et soit $\sigma = \sigma_1 \cdots \sigma_r$ la décomposition correspondante d'un élément. On a

$$\chi(\sigma) = \chi(\sigma_1) \cdots \chi(\sigma_r)$$

et $\chi(\sigma_i)$ est un caractère de G_i. Réciproquement, si pour chaque i, χ_i est un caractère de G_i, la fonction $\chi(\sigma) = \Pi\chi_i(\sigma_i)$ est un caractère de G. Or, pour un groupe cyclique formé des puissances d'une substitution τ d'ordre n_i, un caractère est bien défini par la valeur de $\chi(\tau)$, qui est une racine n_i-ème de l'unité. Il y a donc n_i de ces caractères qui sont distincts. La réduction précédente montre que G possède Πn_i caractères distincts, donc autant que d'éléments. De plus le produit de deux caractères χ, χ' (c'est-à-dire la fonction $\chi(\sigma)\chi'(\sigma)$) est encore un caractère : les caractères de G forment un groupe. Pour G_i ce groupe est cyclique d'ordre n_i. Donc pour tout groupe abélien G, le groupe des caractères est isomorphe à G.

Considérons un élément σ de G et la somme $\sum_{\chi} \chi(\sigma)$ étendue à tous les caractères χ. Soit χ_0 un caractère quelconque : On a

$$\chi_0(\sigma)\sum_{\chi}\chi(\sigma) = \sum_{\chi}\chi\chi_0(\sigma) = \sum_{\chi}\chi(\sigma).$$

Si $\sigma \neq 1$, il y a toujours un χ_0 tel que $\chi_0(\sigma) \neq 1$. Soit en effet $\sigma = \sigma_1 \cdots \sigma_r$, la décomposition d'un élément σ, et soit par exemple $\sigma_1 \neq 1$. Posons $\chi_1(\sigma_1) \neq 1$, $\chi_2(\sigma_2) = \cdots = \chi_r(\sigma_r) = 1$. Le caractère $\chi_1\chi_2 \cdots \chi_r$ sera différent de 1 pour σ. Il en résulte que

$$\begin{cases} \text{si} \quad \sigma \neq 1 & \sum\chi(\sigma) = 0, \\ \text{si} \quad \sigma = 1 & \sum_{\chi}\chi(\sigma) = n \quad \text{(ordre du groupe).} \end{cases}$$

De même considérons un caractère χ quelconque, et la somme $\sum_{\sigma}\chi(\sigma)$ étendue à tous les éléments σ de G. Considérons un élément σ_0 et formons

$$\chi(\sigma_0)\sum_{\sigma}\chi(\sigma) = \sum_{\sigma}\chi(\sigma\sigma_0) = \sum_{\sigma}\chi(\sigma);$$

il y a un caractère χ_0 (caractère principal) égal à 1 pour tous les éléments σ. Si $\chi \neq \chi_0$ il y a au moins un σ_0 tel que $\chi(\sigma_0) \neq 1$. Donc

$$\begin{cases} \sum_{\sigma}\chi(\sigma) = 0 & \text{si} \quad \chi \neq \chi_0, \\ \sum_{\sigma}\chi(\sigma) = n & \text{si} \quad \chi = \chi_0. \end{cases}$$

Représentations[8].

On dit qu'on a une représentation de degré d d'un groupe G quand on a une homomorphie de G avec un groupe de substitutions linéaires à d variables :

$$\sigma \to x_i' = \sum a_{ij}^{(\sigma)} x_j \qquad (i, j = 1, 2, \ldots d)$$

de déterminants $\neq 0$. Deux représentations sont équivalentes quand elles se déduisent l'une de l'autre par un changement linéaire de variables.

8) Nous ne pouvons ici donner les démonstrations des théorèmes que nous ne faisons qu'énoncer. On trouvera les démonstrations dans Speiser loc. cit. (2), ou, au point de vue des nombres hypercomplexes dans " Van der Waerden, Moderne Algebra ", Springer, 1930, 2me partie.

Etant données deux représentations, P, P', on en déduit une représentation $P + P'$ de la manière suivante : si les substitutions de P opèrent sur d variables x_i, celles de P' sur d' variables y_i, on forme $d + d'$ variables z_i, et on astreint les d premières à subir les opérations de P, les d' dernières à subir celles de P'. A la place de $P + P$, on écrit $2P$, etc.

On démontre les faits suivants :

G étant un groupe fini, il existe h représentations (dites irréductibles) $P_1, P_2, \cdots, P_h$, telles que toute représentation soit equivalente à une représentation de la forme $n_1P + \cdots + n_hP_h$ et à une seule.

On appelle caractère de σ dans la représentation P le nombre $\sum_j a_{jj}^{(\sigma)}$; les caractères ainsi définis coincident, dans le cas des répresentations irréductibles des groupes abéliens avec ceux dont on a parlé plus haut. Si on désigne par $\chi_i(\sigma)$ les caractères dans les représentations P_i, on a

$$\chi(\sigma) = n_1\chi_1(\sigma) + \cdots + n_h\chi_h(\sigma)$$

et ces égalités, écrites pour tous les σ, déterminent entièrement les n_i.

Donc si dans deux représentations P, P' les caractères de chaque substitution sont égaux, ces représentations sont équivalentes.

Les nombres n_i s'interprètent de la manière suivante : il y a n_i systèmes de formes linéaires des variables sur lesquelles opère P dont chacun est formé de formes subissant les opérations de P_i.

Si le groupe G est abélien, les représentations irréductibles de P_i sont de degré 1 et elles sont fournies par les formules $x' = \chi(\sigma)x$, $\chi(\sigma)$ désignant un des caractères précédemment définis.

Champs de Galois.

Dans un corps de nombres algébriques, les entiers forment un groupe additif Σ. Un idéal $\mathfrak{a}$ est un sous-groupe de Σ et on sait que $\Sigma/\mathfrak{a}$ est un groupe ne contenant qu'un nombre fini d'éléments, nombre égal à la norme $N(\mathfrak{a})$ de l'idéal $\mathfrak{a}$. On peut encore entre les classes $\mathfrak{K}$ de $\Sigma/\mathfrak{a}$ définir une multiplication : $\mathfrak{K}$ et $\mathfrak{K}'$ étant deux classes (mod. $\mathfrak{a}$) le produit d'un élément α de $\mathfrak{K}$ par un élément α' de $\mathfrak{K}'$ appartient à une classe $\mathfrak{K}\mathfrak{K}'$ qui ne dépend que de $\mathfrak{K}$ et de $\mathfrak{K}'$. En effet si α_1, α_1' sont deux autres éléments pris respectivement dans $\mathfrak{K}$, $\mathfrak{K}'$, on a $\alpha_1 = \alpha + a$, $\alpha_1' = \alpha' + a'$ où a, a' sont dans $\mathfrak{a}$; d'où, $\mathfrak{a}$ étant un idéal, $\alpha_1\alpha_1' = \alpha\alpha' + a''$, a'' étant dans $\mathfrak{a}$.

On a $$\mathfrak{R}(\mathfrak{R}'\mathfrak{R}'') = (\mathfrak{R}\mathfrak{R}')\mathfrak{R}'', \quad \mathfrak{R}\mathfrak{R}' = \mathfrak{R}'\mathfrak{R},$$
$$\mathfrak{R}(\mathfrak{R}' + \mathfrak{R}'') = \mathfrak{R}\mathfrak{R}' + \mathfrak{R}\mathfrak{R}''.$$

Mais les classes $\mathfrak{R}$ ne forment pas un groupe. Par contre si $\mathfrak{a}$ est un idéal premier, les classes $\mathfrak{R} \neq 0$ (0 désigne l'élément unité de $\Sigma/\mathfrak{a}$, c'est-à-dire la classe composée des nombres de $\mathfrak{a}$) forment un groupe, car dans ce cas, si α, α' sont deux nombres premiers à $\mathfrak{a}$, il existe toujours un nombre β tel que $\alpha \equiv \beta\alpha'$ (mod. $\mathfrak{a}$).

Or, un groupe additif dans lequel les éléments $\neq 0$ forment par une autre loi de composition (multiplication) un groupe abélien, la multiplication étant distributive par rapport à l'addition, est appelé un corps. L'importance des corps provient du fait que les identités et les algorithmes algébriques sur les polynomes sont valables dès que les coefficients appartiennent à un corps. Par exemple : $f(x)$ et $g(x)$ étant deux polynomes, ils ont un plus grand commun diviseur $d(x)$ de la forme $\lambda f(x) + \mu g(x)$.

De l'identité $f(x) = f(a) + (x - a) \cdot \varphi(x)$ résulte que la condition nécessaire et suffisante pour que l'équation $f(x) = 0$ admette la racine a est que $f(x)$ soit divisible par $x - a$; si une équation $(x) = 0$ de degré n admet les racines $x_1, x_2, \cdots, x_n$, on a

$$f(x) = a_0(x - x_1)(x - x_2) \cdots (x - x_n)$$

et l'équation n'admet aucune autre racine.

Si un polynome $f(x)$ est irréductible dans un corps (c'est-à-dire n'y admet aucun diviseur non constant de degré inférieur au sien) et si un autre polynome $g(x)$ à coefficients dans ce corps a dans un sur-corps une racine commune avec $f(x)$, $g(x)$ est divisible par $f(x)$.

Ceci posé, le groupe des classes modulo un idéal premier nous a donné l'exemple d'un corps qui ne possède qu'un nombre fini d'éléments. Un tel corps est appelé *champ de Galois*. Nous allons étudier ces corps.

h désignant un entier positif ordinaire, on conviendra que dans un corps R quelconque, h représentera la somme de h éléments égaux à l'élément unité de la multiplication. Le groupe additif des nombres d'un champ de Galois R étant fini, l'élément unité de la multiplication y est d'ordre fini p ; p est un nombre premier, car si on avait une décomposition $p = p'p''$, p' et p'' étant $< p$, on aurait $p' \neq 0$, $p'' \neq 0$, et $p'p'' = 0$ ce qui est impossible dans un corps. Ce nombre p s'appelle *caractéristique* du corps. De la formule $(1 + \cdots + 1)x = x + \cdots + x$ résulte que $px = 0$ pour tout x. Donc, dans le groupe additif, tout élément $\neq 0$ est d'ordre p. Le groupe lui-même est d'ordre p^φ. Donc :

Le nombre d'éléments d'un champ de Galois est la puissance d'un nombre premier.

Considérons maintenant le groupe multiplicatif des nombres $\neq 0$ de R. Ce groupe est d'ordre $p^\varphi - 1$. Soit d le plus petit nombre tel que pour tout élément a du groupe, on ait $a^d = 1$ (d divise $p^\varphi - 1$). Il en résulte que les $p^\varphi - 1$ éléments du groupe sont solutions de l'équation $x^d - 1 = 0$, ce qui n'est possible que si $d \geq p^\varphi - 1$ d'où $d = p^\varphi - 1$. D'autre part décomposons ce groupe multiplicatif en produit direct de groupes cycliques d'ordres q^β (les q étant des nombres premiers). d sera évidemment le p.p.c.m. des q^β et $p^\varphi - 1$ leur produit. L'égalité ne peut avoir lieu que si pour chaque q il n'y a qu'un composant cyclique (a_q) dont l'ordre est une puissance de q. Mais dans ce cas les puissances de l'élément Πa_q engendrent le groupe entier qui est cyclique. Donc:

Le groupe multiplicatif d'un champ de Galois à p^φ éléments est le groupe cyclique à $p^\varphi - 1$ éléments. Tout élément a du champ satisfait à l'équation

$$a^{p^\varphi} = a.$$

Il résulte de là que, $f(x)$ étant un polynome dans le champ de Galois considéré, on a

$$(f(x))^{p^\varphi} = f(x^{p^\varphi}).$$

Soit r un champ de Galois à p^φ éléments et soit R un champ de Galois à p^F éléments contenant r. Il existe un élément x de R tel que tout autre élément $\neq 0$ de R soit une puissance de x. D'autre part soit f le degré de l'équation de plus bas degré à laquelle satisfait x dans r. Par un raisonnement bien connu[9]), on voit que toute fraction rationnelle de x à coefficients dans r se met et d'une seule manière sous la forme $\alpha_0 + \alpha_1 x + \ldots + \alpha_{f-1} x^{f-1}$, les α_i étant dans r. Donc quand les α_i parcourent indépendamment les éléments de r, l'élément précédent parcourt tous les éléments de R. Il en résulte que R possède $p^{\varphi f}$ éléments, d'où

$$F = \varphi f.$$

De plus si $f(x) = 0$ est l'équation de degré f à laquelle satisfait x, les racines de cette équation sont $x, x^{p^\varphi}, \ldots, x^{p^{\varphi(f-1)}}$. *Elles sont toutes distinctes.*

9) Exactement comme en théorie des corps de nombres algébriques, quand on démontre que tout nombre du corps engendré par le nombre θ se met sous la forme $a_0 + a_1\theta + \ldots + a_{n-1}\theta^{n-1}$, les a_i étant rationnels.

Chapitre II.

Corps de décomposition et corps d'inertie.

Soit un corps fini de nombres algébriques k et soit K un sur-corps relativement galoisien de k. Soit G le groupe de Galois de K par rapport à k. La correspondance biunivoque établie par la théorie de Galois entre les corps K' compris entre k et K et les sous-groupes G' de G sera traduite en disant que K' *appartient* à G' ou que G' *appartient* à K'.

Soit $\mathfrak{P}$ un idéal premier de K de degré absolu F; soit p le nombre premier rationnel divisible par $\mathfrak{P}$. Hilbert a attaché à $\mathfrak{P}$ une série remarquable de sous-groupes de G que nous allons définir en partie[10].

1) L'ensemble des opérations de G changeant $\mathfrak{P}$ en lui même forme le *groupe de décomposition* G_Z de $\mathfrak{P}$.

Le corps appartenant à G_Z est le *corps de décomposition* K_Z. L'idéal premier de K_Z divisible par $\mathfrak{P}$ sera désigné par $\mathfrak{P}_Z$.

2) L'ensemble des opérations σ de G telles que, pour tout entier A de K on ait

$$\sigma A \equiv A \qquad (\text{mod. } \mathfrak{P})$$

forme le *groupe d'inertie* G_T de $\mathfrak{P}$.

Le corps appartenant au groupe d'inertie est le *corps d'inertie* K_T. L'idéal premier de K_T divisible par $\mathfrak{P}$ sera désigné par $\mathfrak{P}_T$.

On désignera par r le champ de Galois formé par les classes d'entiers de k modulo $\mathfrak{p}$, où $\mathfrak{p}$ est l'idéal premier de k divisible par $\mathfrak{P}$; de même R_Z, R_T, R seront définis d'une manière analogue par $\mathfrak{P}_Z$ et K_Z, $\mathfrak{P}_T$ et K_T, $\mathfrak{P}$ et K. On a

$$r \subset R_Z \subset R_T \subset R.$$

Les notions précédentes n'ont été introduites que par rapport à une extension parfaitement déterminée K/k. Mais il résulte immédiatement des définitions que :

Théorème 1. *Si k' est un corps contenu entre K et k, appartenant au groupe G', les groupes de décomposition et d'inertie de $\mathfrak{P}$ pour l'extension K/k' sont $[G_Z, G']$ et $[G_T, G']$.*

Soit

$$\mathfrak{p} = (\mathfrak{P}_1\mathfrak{P}_2 \cdots \mathfrak{P}_g)^e$$

la décomposition de $\mathfrak{p}$ en facteurs premiers dans K, chacun des facteurs étant de degré relatif f; e sera appelé *exposant relatif* des $\mathfrak{P}_i$. On a $efg = n$

10) Toute la théorie est exposée dans "Hasse, Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper", Leipzig, 1930.

(n étant le degré relatif de K) comme on le voit en prenant les normes relatives des deux membres par rapport à k. On suppose $\mathfrak{P} = \mathfrak{P}_1$.

Choisissons g^* opérations $\sigma_1 = 1, \sigma_2, \dots \sigma_{g^*}$ de G telles que tout élément de G se mette et d'une seule manière sous la forme $\sigma_i\sigma$, σ étant dans G_Z. Remarquons que toutes les opérations de $\sigma_i G_Z$ changent $\mathfrak{P}$ en le même idéal premier $\sigma_i\mathfrak{P}$ qu'on peut supposer être $\mathfrak{P}_i$. Si $i \neq j$, on a $\sigma_i\mathfrak{P} \neq \sigma_j\mathfrak{P}$, car sinon on aurait $\sigma_j^{-1}\sigma_i\mathfrak{P} = \mathfrak{P}$, $\sigma_j^{-1}\sigma_i$ serait dans G_Z, ce qui n'est pas. Comme tous les idéaux $\mathfrak{P}_i$ se déduisent de l'un d'eux par des opérations de G, on a $g^* = g$. Donc :

Théorème 2. *L'ordre du groupe de décomposition G_Z est* $\dfrac{n}{g} = ef$.

Appliquons ce théorème à l'extension K/K_Z. En vertu du Th. 1, on a ici $G_Z' = G'$. Donc :

Théorème 3. *L'idéal premier $\mathfrak{P}_Z$ de K_Z n'est divisible que par un idéal premier de K.*

D'autre part G_T est un sous-groupe invariant de G_Z. Soit en effet A un entier quelconque de K, τ une opération de G_T, σ une opération de G_Z. On a par hypothèse $\tau(\sigma^{-1}A) \equiv \sigma^{-1}A \pmod{\mathfrak{P}}$, d'où $\sigma\tau\sigma^{-1}A \equiv A \pmod{\mathfrak{P}}$ et $\sigma\tau\sigma^{-1}$ est dans G_T.

Or les opérations σ de G_Z changent tous les éléments d'une classe modulo $\mathfrak{P}$ en les éléments d'une autre classe. Elles peuvent donc être considérées comme des automorphismes du champ de Galois R formé par ces classes, laissant invariants tous les éléments de R_Z. Or, A représentant un élément de R, le polynome $\prod_\sigma(x - \sigma A)$, le produit étant étendu aux opérations de G_Z, est à coefficient dans R_Z. D'autre part A (dont nous supposons que ses puissances engendrent tous les éléments $\neq 0$ de R) satisfait dans R_Z à une équation irréductible de degré f^*, ayant pour racines les $A^{p^{\overset{Fi}{f^*}}}$ (voir p. 382). Le premier membre $\varphi(x)$ de cette équation doit donc diviser $\prod_\sigma(x - \sigma A)$. D'autre part, σ étant un automorphisme de R par rapport à R_Z, tout σA est racine de $\varphi(x) = 0$. Donc le nombre des σA distincts est égal à f^* ; mais ce nombre est aussi égal à l'indice $(G_Z : G_T)$. Donc $(G_Z : G_T)$ est égal à f^*. De plus il y a une substitution σ de G_Z telle que $\sigma A = A^{p^{\overset{F}{f^*}}}$ et toute opération de G_Z est de la forme $\sigma^i\tau$, τ étant dans G_T.

Appliquons les considérations précédentes à l'extension K/K_T. En vertu du théorème 1, on a ici $G_Z' = G'$, $G_T' = G'$, $K_Z' = K_T$, $K_T' = K_T$. D'où $f'^* = 1$, $R = R_Z' = R_T$. Le degré relatif de $\mathfrak{P}$ par rapport à $\mathfrak{P}_T$ étant $(R : R_T)$, $\mathfrak{P}$ est de degré relatif 1 par rapport à $\mathfrak{P}_T$. $\mathfrak{P}_T$ n'étant divisible dans K que par un seul idéal premier (Th. 3), on voit que :

Théorème 4. *Tout nombre de K est congru* (mod. $\mathfrak{P}$) *à un nombre de K_T. L'idéal $\mathfrak{P}$ est de degré relatif 1 par rapport à K_T, et $\mathfrak{P}_T$ est une puissance de $\mathfrak{P}$.*

L'application de la formule $efg = n$ à l'extension K/K_T montre que si $\mathfrak{P}_T = \mathfrak{P}^{e^*}$, e^* est égal à $(K : K_T)$, donc à l'ordre de G_T. L'idéal $\mathfrak{P}_T$ divisant $\mathfrak{p}$, on a $e^* \leq e$. D'autre part G_Z est d'ordre ef, et on a vu que $(G_Z : G_T) = f^*$. Donc $ef = e^*f^*$. Mais $f^* = (R : R_Z)$, $f = (R : r)$. D'où $f^* \leq f$. Des formules $e^* \leq e, f^* \leq f, e^*f^* = ef$, on déduit $e^* = e$, $f^* = f$. Donc G_T est d'ordre e et $\mathfrak{P}_T = \mathfrak{P}^e$, ce qui montre que $\mathfrak{p}$ n'est pas divisible par le carré de $\mathfrak{P}_T$. Comme $\mathfrak{P}_T$ est le seul facteur premier de $\mathfrak{P}_Z$ dans K_T et que $\mathfrak{P}_Z$ n'est pas divisible par son carré, on a $\mathfrak{P}_Z = \mathfrak{P}_T$. Enfin, de $f^* = f$ résulte $R_Z = r$, donc que $\mathfrak{P}_Z$ est de degré relatif 1 par rapport à k. Donc :

Théorème 5. *L'idéal $\mathfrak{P}_Z$ est par rapport à k de degré relatif 1. Il reste idéal premier dans K_T, c'est-à-dire $\mathfrak{P}_Z = \mathfrak{P}_T$. On a $\mathfrak{P}_T = \mathfrak{P}^e$.*

Théorème 6. *Le groupe G_Z/G_T est cyclique. G_Z contient une substitution σ définie à la multiplication près par un élément de G_T et telle que pour tout entier M de K on ait :*

$$\sigma M \equiv M^{N\mathfrak{p}} \qquad (\text{mod. } \mathfrak{P}).$$

Soit k' un corps compris entre k et K et appartenant au groupe G'. Soient e', f', g', les nombres définis pour l'extension K/k' comme e, f, g le sont pour l'extension K/k : Si $\mathfrak{p}'$ est l'idéal premier de k' divisible par $\mathfrak{P}$, on a dans K

$$\mathfrak{p}' = (\mathfrak{P}_1\mathfrak{P}_2 \dots \mathfrak{P}_{g'})^{e'}.$$

1) La condition nécessaire et suffisante pour que $f' = f$, $e' = e$, c'est-à-dire pour que $\mathfrak{p}$ soit de degré et d'exposant relatifs 1 par rapport à k est que $G_Z' = G_Z$, car G_Z' est alors d'ordre ef et contenu dans G_Z, d'où, d'après le théorème 1 $G' \supset G_Z$. Donc :

Théorème 7. *K_Z contient tout corps k' contenu dans K dans lequel l'idéal premier $\mathfrak{p}'$ divisible par $\mathfrak{P}$ est de degré et d'exposant relatif 1 par rapport à k.*

2) La condition nécessaire et suffisante pour que $e' = e$, c'est-à-dire pour que $\mathfrak{p}'$ soit d'exposant relatif 1 est que $G_T' = G_T$, d'où $G' \supset G_T$. Donc :

Théorème 8. *K_T contient tout sous-corps k' de K contenant k dans lequel l'idéal premier $\mathfrak{p}'$ divisible par $\mathfrak{P}$ est d'exposant relatif 1 par rapport à k.*

Cas abélien.

Envisageons le cas où K est abélien par rapport à k, c'est-à-dire où G est abélien. Remarquons que dans le cas général si $\sigma\mathfrak{P}$ est un idéal premier conjugué de $\mathfrak{P}$ il suit tout de suite de la définition que les groupes de décomposition et d'inertie de $\sigma\mathfrak{P}$ sont $\sigma G_Z \sigma^{-1}$, $\sigma G_T \sigma^{-1}$. Dans le cas présent ils se confondent donc avec G_Z, G_T.

Définitions. Un idéal premier d'un corps k est dit *complètement décomposé* dans un corps K contenant k quand il se décompose dans K en produits d'idéaux premiers distincts de dégré relatif 1 (donc en nombre égal au degré relatif de K). Il est dit *complètement ramifié* dans K s'il est puissance d'un idéal premier de K de degré relatif 1. Il est dit *ramifié* dans K s'il est divisible par le carré d'un idéal premier de K.

Dès lors les théorèmes 7 et 8 donnent dans le cas actuel :

Théorème 7a. *Le corps de décomposition de $\mathfrak{P}$ est le plus grand corps contenu dans K dans lequel $\mathfrak{p}$ soit complètement décomposé.*

Théorème 8a. *Le corps d'inertie de $\mathfrak{P}$ est le plus grand corps contenu dans K dans lequel $\mathfrak{p}$ ne soit pas ramifié.*

Ces corps, qui ne dépendent que de $\mathfrak{p}$, ainsi que les groupes correspondants, sont aussi appelés corps et groupes de décomposition et d'inertie de $\mathfrak{p}$ dans K.

Considérons un idéal premier $\mathfrak{p}$ non ramifié dans K. Alors G_Z est cyclique, et pour chaque facteur premier $\mathfrak{P}$ de $\mathfrak{p}$ dans K, G_Z est engendré par une substitution σ telle que, pour tout entier A de K, on ait

$$\sigma A \equiv A^{N\mathfrak{p}} \qquad (\text{mod. } \mathfrak{P}).$$

D'où τ étant une opération quelconque de G,

$$\tau\sigma\tau^{-1} A \equiv A^{N\mathfrak{p}} \qquad (\text{mod. } \tau\mathfrak{P}).$$

Or $\tau\sigma\tau^{-1} = \sigma$; donc $\sigma A - A^{N\mathfrak{p}}$ est divisible par tous les facteurs premiers de $\mathfrak{p}$ dans K, donc aussi par leur produit $\mathfrak{p}$ Donc :

Théorème 9. *K étant relativement abélien par rapport à k, soit $\mathfrak{p}$ un idéal premier de k non ramifié dans K. Il existe un automorphisme σ de K d'ordre f, engendrant le groupe de décomposition de $\mathfrak{p}$ et tel que pour tout entier A de K on ait*

$$\sigma A \equiv A^{N\mathfrak{p}} \qquad (\text{mod. } \mathfrak{p}).$$

On désigne la substitution précédente par la symbole $\left(\frac{K/k}{\mathfrak{p}}\right)$, ou, quand il n'y a pas d'ambiguité possible, par $\left(\frac{K}{\mathfrak{p}}\right)$. Ce symbole est appelé *symbole de Frobenius*. Nous allons en donner quelques propriétés.

a) K' étant un corps compris entre k et K, on a $\left(\frac{K}{\mathfrak{p}}\right) \to \left(\frac{K'}{\mathfrak{p}}\right)$, la flèche indiquant que l'automorphisme du second membre résulte de l'application aux nombres de K' de l'automorphisme du premier membre. Cela résulte immédiatement de la définition.

b) Si K et K' sont des sur-corps relativement abéliens de k dans lesquels l'idéal premier $\mathfrak{p}$ n'est pas ramifié, cet idéal n'est pas non plus ramifié dans KK'. En effet le groupe de Galois de KK' (rappelons que l'on désigne par KK' le plus petit corps contenant K et K') par rapport à k est un sous-groupe du produit direct des groupes de Galois de K et de K' (voir p. 378). D'après la définition du groupe d'inertie, une opération du groupe d'inertie de $\mathfrak{p}$ dans KK' induit des automorphismes de K, K' qui appartiennent aux groupes d'inertie de $\mathfrak{p}$ dans ces deux corps, donc qui sont égaux à 1. Donc $\left(\frac{KK'}{\mathfrak{p}}\right)$ est défini, et en vertu de a) on a

$$\left(\frac{KK'}{\mathfrak{p}}\right) \to \left(\frac{K}{\mathfrak{p}}\right), \quad \left(\frac{KK'}{\mathfrak{p}}\right) \to \left(\frac{K'}{\mathfrak{p}}\right).$$

Il en résulte

$$\left(\frac{KK'}{\mathfrak{p}}\right) = \left(\frac{K}{\mathfrak{p}}\right)\left(\frac{K'}{\mathfrak{p}}\right).$$

c) k' étant un sur-corps quelconque de k, Kk' est un corps relativement abélien par rapport à k', dont le groupe de Galois peut être considéré comme un sous-groupe du groupe de Galois de K par rapport à k. En effet un automorphisme de Kk' par rapport à k', appliqué aux nombres de K, donne un automorphisme de K laissant invariants les nombres de k. Soit $\mathfrak{p}$ un idéal premier de k non ramifié dans K et soit $\mathfrak{q}$ un diviseur premier quelconque de $\mathfrak{p}$ dans k'. L'idéal $\mathfrak{q}$ n'est pas ramifié dans Kk', car une opération du groupe d'inertie de $\mathfrak{q}$ dans Kk' induit dans le groupe de K par rapport à k une opération du groupe d'inertie de $\mathfrak{p}$. Soit f le degré relatif de $\mathfrak{p}$ par rapport à k. On a par hypothèse, pour tout entier A de K,

$$\left(\frac{Kk'}{\mathfrak{p}}\right)A \equiv A^{N\mathfrak{q}} = A^{N\mathfrak{p}^f} \pmod{\mathfrak{q}}.$$

Mais on a aussi

$$\left(\frac{K}{\mathfrak{p}}\right)^f A \equiv A^{N\mathfrak{p}^f} \pmod{\mathfrak{q}}.$$

Donc :

$$\left(\frac{Kk'}{\mathfrak{q}}\right) \to \left(\frac{K}{\mathfrak{p}}\right)^f.$$

Chapitre III.

Congruences multiplicatives. Idéaux à l'infini. Groupes de congruence.

Congruences multiplicatives.

L'importance dans toute la théorie du corps de classes des groupes multiplicatifs de nombres rend gênant le fait que les congruences ordinaires ne peuvent être divisées membre à membre : par exemple de $7 \equiv 7 \pmod 7$ et de $7 \equiv 14 \pmod 7$ on ne peut pas déduire $1 \equiv 2 \pmod 7$.

C'est pourquoi M. Hasse a introduit, par une legère modification des définitions, une nouvelle sorte de congruences, les *congruences multiplicatives* (dans le mémoir cité dans l'introduction p. 367). Ces congruences seront presque exclusivement employées dans la suite : nous leur reserverons le symbole $(\text{mod. } \mathfrak{m})$ jusqu'ici employé pour désigner les congruences ordinaires ou *additives*. Pour ces dernières, nous remplacerons le symbole $(\text{mod. } \mathfrak{m})$ par $(\text{mod. } {}^+\mathfrak{m})$.

Définition. Soit $\mathfrak{m}$ un idéal entier. Un nombre α est dit congru à 1 $(\text{mod. } \mathfrak{m})$ quand $\alpha - 1$ est divisible par $\mathfrak{m}$, (c'est-à-dire quand $\alpha - 1$ se met sous la forme $\frac{\beta}{\gamma}$ où β est divisible par $\mathfrak{m}$ et γ premier à $\mathfrak{m}$, β et γ étant des entiers).

Deux nombres $\alpha, \beta \neq 0$ sont dits congrus $(\text{mod. } \mathfrak{m})$ si $\frac{\alpha}{\beta}$ est $\equiv 1 \pmod{\mathfrak{m}}$.

Si $\alpha \equiv \beta \pmod{\mathfrak{m}}$ et $\alpha' \equiv \beta' \pmod{\mathfrak{m}}$, on a $\alpha\alpha' \equiv \beta\beta' \pmod{\mathfrak{m}}$ et $\frac{\alpha}{\alpha'} \equiv \frac{\beta}{\beta'} \pmod{\mathfrak{m}}$.

On a

$$\frac{\alpha\alpha'}{\beta\beta'} - 1 = \left(\frac{\alpha}{\beta} - 1\right)\frac{\alpha'}{\beta'} + \frac{\alpha'}{\beta'} - 1.$$

Or, $\frac{\alpha'}{\beta'}$ étant $\equiv 1 \pmod{\mathfrak{m}}$ est premier à $\mathfrak{m}$ (c'est-à-dire, se met sous la forme du quotient de deux entiers premiers à $\mathfrak{m}$). $\frac{\alpha}{\beta} - 1$ et $\frac{\alpha'}{\beta'} - 1$ sont divisibles par $\mathfrak{m}$, donc aussi $\frac{\alpha\alpha'}{\beta\beta'} - 1$. Pour démontrer la seconde partie, montrons que si $\alpha \equiv \alpha' \pmod{\mathfrak{m}}$, on a $\frac{1}{\alpha} \equiv \frac{1}{\alpha'} \pmod{\mathfrak{m}}$. Le nombre $\frac{\alpha}{\alpha'} - 1$ est divisible par $\mathfrak{m}$. Donc $\frac{\alpha'}{\alpha}$ est premier à $\mathfrak{m}$. Or

$$\frac{\alpha'}{\alpha} - 1 = \frac{\alpha' - \alpha}{\alpha} = \frac{\alpha'}{\alpha} \cdot \frac{\alpha' - \alpha}{\alpha'} = -\frac{\alpha'}{\alpha}\left(\frac{\alpha}{\alpha'} - 1\right),$$

ce qui démontre notre proposition, en même temps que le fait que si $\alpha \equiv \alpha' \pmod{\mathfrak{m}}$ on a aussi $\alpha' \equiv \alpha \pmod{\mathfrak{m}}$.

On démontre de même facilement que $\alpha \equiv \alpha \pmod{\mathfrak{m}}$ et que si $\alpha \equiv \beta \pmod{\mathfrak{m}}$, $\beta \equiv \gamma \pmod{\mathfrak{m}}$, on a aussi $\alpha \equiv \gamma \pmod{\mathfrak{m}}$.

Si α, β sont des nombres qui se mettent sous la forme du quotient de deux entiers, le dénominateur étant premier à $\mathfrak{m}$, la congruence $\alpha \equiv \beta \pmod{\mathfrak{m}}$ entraîne $\alpha \equiv \beta \pmod{\mathfrak{m}}^+$. Si au contraire les numérateurs sont premiers à $\mathfrak{m}$, la congruence $\alpha \equiv \beta \pmod{\mathfrak{m}}^+$ entraîne $\alpha \equiv \beta \pmod{\mathfrak{m}}$.

Signature. Idéaux à l'infini.

Soit k un corps fini de nombres algébriques et soient $k^{(1)}, k^{(2)}, \ldots, k^{(r_1)}$ les conjugués réels de k. α étant un nombre $\neq 0$, appelons $\alpha^{(i)}$ le conjugué de α dans $k^{(i)}$, et appelons *signature* de α un symbole (± 1, $\pm 1, \ldots, \pm 1$) contenant r_1 nombres, le i-éme. nombre étant $+1$ si $\alpha^{(i)} > 0$, -1 dans le cas contraire.

Lemme. *$\mathfrak{m}$ étant un idéal entier de k, μ_0 un nombre $\neq 0$ de k, il y a une infinité de nombres $\alpha \equiv \mu_0 \pmod{\mathfrak{m}}$ et ayant une signature quelconque donnée à l'avance.*

Donnons-nous un nombre θ qui engendre le corps k. Donc θ est différent de tous ses conjugués. On peut supposer les conjugués réels de k rangés dans un ordre tel que $\theta^{(i)} < \theta^{(i+1)}$. On peut choisir des nombres rationnels ρ_i tels que

$$\rho_0 < \theta^{(1)} < \rho_1 < \theta^{(2)} < \ldots\ldots < \rho_{r_1-1} < \theta^{(r_1)} < \rho_{r_1}.$$

Soit $\varphi_i = (\theta - \rho_{i-1})(\theta - \rho_i)$. Le nombre φ_i a pour signature un symbole composé de nombres $+1$ sauf à la i-éme. place où on trouve un nombre -1. Il en résulte qu'on pourra trouver un produit φ de nombres φ_i ayant une signature quelconque donnée à l'avance. Soit m un nombre entier rationnel divisible par $\mathfrak{m}$. N étant entier rationnel, on peut trouver un nombre N_0 tel que pour $N \geq N_0$ le nombre $\mu_0 + mN\varphi$ satisfasse aux conditions imposées.

Il est commode d'introduire dans l'étude de k r_1 symboles purement formels $\mathfrak{p}_{\infty,1}, \mathfrak{p}_{\infty,2}, \ldots \mathfrak{p}_{\infty,r_1}$, appelés *idéaux premiers à l'infini*[11]. $\mathfrak{m}_0$ étant un idéal entier on appellera *modules* des symboles formels $\mathfrak{m}_0 \mathfrak{p}_{\infty,i_1} \ldots \mathfrak{p}_{\infty,i_k}$

11) Ces symboles ont été introduits par M. Hasse. Leur nom provient probablement de ce qu'ils jouent un rôle analogue a celui des points a l'infini d'une surface de Riemann au point de vue de la théorie arithmétique des fonctions algébriques.

$= \mathfrak{m}_0 \prod_j \mathfrak{p}_{\infty, i_j}$. $\mathfrak{m}$ étant un semblable module, nous donnerons un sens à la congruence $\alpha \equiv \beta \pmod{\mathfrak{m}}$. Par définition, on aura le droit d'écrire cette congruence si et seulement si :

1) $\alpha \equiv \beta \pmod{\mathfrak{m}_0}$.

2) Dans la signature de $\frac{\alpha}{\beta}$, les nombres des places $i_1, i_2, \ldots i_k$ sont égaux à $+1$.

Ces congruences peuvent être multipliées entre elles comme les congruences multiplicatives ordinaires.

$\mathfrak{m}$ étant un module $\mathfrak{m}_0 \prod \mathfrak{p}_{\infty, i_j}$, $\mathfrak{m}_0$ sera appelé partie finie de $\mathfrak{m}$. On dit que $\mathfrak{m}$ est divisible par un idéal quand cet idéal divise $\mathfrak{m}_0$. $\mathfrak{m}$ est divisible par un autre module $\mathfrak{m}'$ si la partie finie de $\mathfrak{m}'$ divise $\mathfrak{m}_0$ et si tous les idéaux premiers infinis de $\mathfrak{m}'$ figurent dans $\mathfrak{m}$.

Le p.g.c.d. de deux modules $\mathfrak{m}$, $\mathfrak{m}'$ est le module dont la partie finie est le p.g.c.d. des parties finies de $\mathfrak{m}$, $\mathfrak{m}'$, et dont les idéaux premiers infinis sont ceux qui figurent à la fois dans $\mathfrak{m}$ et dans $\mathfrak{m}'$. On définit de même le p.p.c.m. Deux modules sont premiers entre eux si leur p.g.c.d. est 1 ; il en résulte en particulier qu'aucun idéal premier infini ne figure dans les deux modules à la fois. De même pour un module et un idéal.

Soit K un sur-corps relativement galoisien de k de degré relatif n. Donc pour chaque $k^{(i)}$ il y a n conjugués (d'ailleurs identiques) de K contenant $k^{(i)}$. Si ces corps sont imaginaires, nous dirons conventionnellement que $\mathfrak{p}_{\infty, i}$ est *ramifié* dans K. Si ces corps sont réels, nous dirons que $\mathfrak{p}_{\infty, i}$ est *complètement décomposé* dans K. Dans ce cas à chacun de ces conjugués réels de K correspond un idéal premier à l'infini $\mathfrak{P}^{(j)}_{\infty, i}$. Nous remarquerons que les conditions $\alpha \equiv \beta \pmod{\mathfrak{p}_{\infty, i}}$ et $\alpha \equiv \beta \pmod{\prod_j \mathfrak{P}^{(j)}_{\infty, i}}$ sont équivalentes et nous écrirons $\mathfrak{p}_{\infty, i} = \prod_j \mathfrak{P}^{(j)}_{\infty, i}$. $\mathfrak{m}$ étant un module quelconque de k, nous considérerons $\mathfrak{m}$ comme égal dans K au module qu'on obtient en y remplaçant les idéaux infinis complètement décomposés par leur expression au moyen de la formule précédente, et en laissant tomber les autres[12].

Lemme. *$\mathfrak{m}$ et $\mathfrak{m}'$ étant deux modules, la condition nécessaire et suffisante pour que le système de congruences $x \equiv \alpha \pmod{\mathfrak{m}}$ et $x \equiv \alpha' \pmod{\mathfrak{m}'}$ soit résoluble est que $\alpha \equiv \alpha' \pmod{\mathfrak{f}}$, $\mathfrak{f}$ étant le p.g.c.d. de $\mathfrak{m}$ et de $\mathfrak{m}'$.*

La condition est évidemment nécessaire. Supposons la remplie. Soient $\mathfrak{m}_0$, $\mathfrak{m}_0'$ les parties finies de $\mathfrak{m}$, $\mathfrak{m}'$. La partie finie de $\mathfrak{f}$ est $(\mathfrak{m}_0, \mathfrak{m}_0')$.

12) α et β étant des nombres de k, la congruence $\alpha \equiv \beta \pmod{\mathfrak{m}}$ peut être vraie dans K sans l'être dans k. Mais A, B étant deux nombres de K, la congruence $A \equiv B \pmod{\mathfrak{m}}$ entraîne $N_{Kk}(A) \equiv N_{Kk}(B) \pmod{\mathfrak{m}}$.

On sait que l'on peut déterminer un nombre x_0 tel que $x_0 \equiv \alpha \pmod{\mathfrak{m}_0}$ et $x_0 \equiv \alpha' \pmod{\mathfrak{m}_0'}$. Le nombre x est assujetti aux conditions suivantes : x est congru (mod. $\mathfrak{m}_0$) et (mod. $\mathfrak{m}_0'$) à x_0 ; de plus sa signature est assujettie à des conditions qui, en vertu de $\alpha \equiv \alpha' \pmod{\mathfrak{f}}$ ne sont pas contradictoires. Il existe donc un symbole $(\pm 1, \pm 1, \cdots, \pm 1)$ qui satisfait à ces conditions et d'après le lemme démontré p. 389, un nombre $x \equiv x_0 \pmod{\mathfrak{m}_0 \mathfrak{m}_0'}$ et ayant cette signature.

Groupes de congruence.

Soit $\mathfrak{m}$ un module dans un corps de nombres algébriques k.

Définition. L'ensemble des idéaux principaux (β) qui sont représentables par un nombre $\beta \equiv 1 \pmod{\mathfrak{m}}$ est un groupe qu'on appelle *rayon* (mod. $\mathfrak{m}$) et qu'on représente par $S_{\mathfrak{m}}$.

On désignera toujours dans la suite par $A_{\mathfrak{m}}^{k}$ le groupe des idéaux d'un corps k premiers à un module $\mathfrak{m}$. (S'il n'y a pas d'ambiguité possible, on pourra supprimer l'indice supérieur k.)

Théorème. *$S_{\mathfrak{m}}$ est dans $A_{\mathfrak{m}}$ un sous-groupe d'indice fini.*

En effet distinguons dans $A_{\mathfrak{m}}$ le groupe $\bar{A}_{\mathfrak{m}}$ des idéaux principaux premiers à $\mathfrak{m}$. $A_{\mathfrak{m}}/\bar{A}_{\mathfrak{m}}$ est fini comme étant isomorphe au groupe des classes de k. α représentant les nombres premiers à $\mathfrak{m}$ et β les nombres $\equiv 1 \pmod{\mathfrak{m}}$, on a $\bar{A}_{\mathfrak{m}}/S_{\mathfrak{m}} \simeq (\alpha)/(\beta) \simeq \alpha/\varepsilon\beta$, ε représentant les unités de k. Pour prouver que $(\bar{A}_{\mathfrak{m}} : S_{\mathfrak{m}})$ est fini, il suffit de montrer que $(\alpha : \beta)$ est fini.

Or $(\alpha : \beta)$ est fini. En effet, désignons par $\mathfrak{m}_0$ la partie finie de $\mathfrak{m}$, par β_0 les nombres $\equiv 1 \pmod{\mathfrak{m}_0}$. $(\beta_0 : \beta)$ est fini, car β_0 n'est susceptible que d'un nombre fini de signatures distinctes et s'il a la signature $(+1, +1, \cdots, +1)$, il appartient certainement au groupe β ; donc, tous les nombres β_0 ayant une même signature appartiennent à la même classe (mod. $\mathfrak{m}$). D'autre part $(\alpha : \beta_0)$ est fini, et égal au nombre des classes d'entiers premiers à $\mathfrak{m}_0$ (mod. $\mathfrak{m}_0$).

Définition. Le groupe $A_{\mathfrak{m}}/S_{\mathfrak{m}}$ est appelé *groupe des classes d'idéaux* (mod. $\mathfrak{m}$). $\mathfrak{a}$ et $\mathfrak{a}'$ étant deux idéaux de $A_{\mathfrak{m}}$, on écrit $\mathfrak{a} \equiv \mathfrak{a}' \pmod{\mathfrak{m}}$ si et seulement si $\frac{\mathfrak{a}}{\mathfrak{a}'}$ est dans $S_{\mathfrak{m}}$. Ces congruences peuvent être multipliées et divisées membre à membre.

On appelle *groupe de congruence* (mod. $\mathfrak{m}$) un sous-groupe de $A_{\mathfrak{m}}$ contenant $S_{\mathfrak{m}}$. H étant un groupe de congruence, $A_{\mathfrak{m}}/H$ et $(A_{\mathfrak{m}} : H)$ sont appelés respectivement *groupe quotient et indice* de H.

H étant un groupe de congruence (mod. $\mathfrak{m}$), et $\mathfrak{n}$ un module multiple de $\mathfrak{m}$, l'ensemble des idéaux de H premiers à $\mathfrak{n}$ forme un groupe de

congruence (mod. $\mathfrak{n}$). Il y a intérêt pour la suite à ne pas distinguer ces deux groupes. Nous poserons donc la définition suivante :

Deux groupes de congruences H et H' sont dits *égaux* s'il existe un idéal $\mathfrak{a}$ tel que les idéaux premiers à $\mathfrak{a}$ qui se trouvent dans H et H' soient les mêmes.

Un groupe de congruence H est dit définissable (mod. $\mathfrak{m}$) s'il existe un groupe de congruence (mod. $\mathfrak{m}$) et égal à H. On dit encore que $\mathfrak{m}$ est un *module de définition* de H. Si $\mathfrak{m}$ est un module de définition, il en est de même de tous ses multiples, ce qui prouve que deux groupes de congruence ont toujours des modules de définition communs.

Si deux groupes de congruence sont égaux, ils ont même groupe quotient et par suite même indice.

Il suffit évidemment de démontrer cette propriété dans le cas où l'un, H', de ces groupes est un groupe de congruence (mod. $\mathfrak{m}'$) formé des idéaux de l'autre, H, premiers à $\mathfrak{m}'$. Or considérons une classe $\mathfrak{K}$ de $A_{\mathfrak{m}}$ suivant $H_{\mathfrak{m}}$. Tous les idéaux de $\mathfrak{K}$ premiers à $\mathfrak{m}'$ tomberont dans une même classe $\mathfrak{K}'$ de $A_{\mathfrak{m}'}$ suivant H'. Montrons d'abord qu'il y a toujours de tels idéaux. Soit $\mathfrak{b}$ un idéal de $\mathfrak{K}$.

Prenons dans la classe absolue de $\mathfrak{b}$ un idéal $\mathfrak{c}$ premier à $\mathfrak{m}\mathfrak{m}'$. On a $\mathfrak{c}\mathfrak{b}^{-1} = (\beta)$ où β est un nombre nécessairement premier à $\mathfrak{m}$. Il existe un nombre β' premier à $\mathfrak{m}\mathfrak{m}'$ tel que $\beta\beta' \equiv 1 \pmod{\mathfrak{m}}$. L'idéal $\mathfrak{b}(\beta\beta')$ appartient à $\mathfrak{K}$ et est premier à $\mathfrak{m}'$.

Dans ces conditions la correspondance $\mathfrak{K} \longrightarrow \mathfrak{K}'$ est un isomorphisme de $A_{\mathfrak{m}}/H$ et de $A_{\mathfrak{m}'}/H'$, ce qui démontre le lemme.

Le p.g.c.d. $\mathfrak{f}$ *de deux modules de définition* $\mathfrak{m}$, $\mathfrak{m}'$ *d'un groupe de congruence* H *est encore un module de définition de* H.

En effet il existe par hypothèse un module $\mathfrak{n}$ que l'on peut supposer multiple de $\mathfrak{m}$ et de $\mathfrak{m}'$, tel que tout idéal de $S_{\mathfrak{n}}$ appartienne à H. Soit α un nombre premier à $\mathfrak{n}$ et $\equiv 1 \pmod{\mathfrak{f}}$. Il en résulte qu'on peut déterminer un nombre $\beta \equiv \alpha \pmod{\mathfrak{m}'}$ et tel que $\beta \equiv 1 \pmod{\mathfrak{m}'}$ et que $(\beta, \mathfrak{n}) = 1$. De $\beta \equiv 1 \pmod{\mathfrak{m}}$ on déduit que (β) est dans H. De $\frac{\beta}{\alpha} \equiv 1 \pmod{\mathfrak{m}}$ on déduit que $\left(\frac{\beta}{\alpha}\right)$ est dans H. Donc (α) est dans H, ce qui démontre le lemme.

Il en résulte que le p.g.c.d. de tous les modules de définition d'un groupe H est encore un module de définition de H. Ce module est appelé *conducteur* du groupe.

Chapitre IV.

La théorie du corps relativement cyclique.

Rappel de quelques faits de la théorie générale des corps[13].

k étant un corps quelconque, rappelons qu'on appelle extension de k tout corps K contenant un sous-corps isomorphe à k, deux sous-corps étant isomorphes quand il existe entre leur éléments une correspondance bi-univoque conservant l'addition et la multiplication. Dans ce cas nous considérerons toujours k comme un sous-corps de K.

Une extension est de degré fini n quand elle contient n éléments $\omega_1, \omega_2, \cdots, \omega_n$ tels que tout élément de K se mette et d'une seule manière sous la forme $\sum_{i=1}^{n} \alpha_i \omega_i$, les α_i étant des éléments de k. Ces n éléments sont *linéairement indépendants* par rapport à k, c'est-à-dire qu'il n'existe aucune relation de la forme $\sum_{i=1}^{n} \alpha_i \omega_i = 0$, les α_i étant des nombres de k non tous nuls. Ils forment une *base relative* de K par rapport à k. On obtient toutes les bases relatives en faisant subir à $\omega_1, \omega_2, \cdots, \omega_n$ les substitutions linéaires inversable à coefficients dans k.

Le degré de l'extension K de k se désigne par $(K:k)$. Si K' est un corps compris entre k et K, on a

$$(K:k) = (K:K')(K':k).$$

Tout élément θ d'une extension de k de degré n satisfait dans k à une équation de degré n, qu'on obtient de la manière suivante : soit

$$\theta\omega_i = \sum_{j=1}^{n} \lambda_{ij}\omega_j \qquad (i = 1, 2, \cdots, n).$$

Le nombre θ est racine de l'équation caractéristique de la matrice (λ_{ij}), c'est-à-dire de l'équation

$$\begin{vmatrix} \lambda_{11} - x & \lambda_{12} & \cdots & \lambda_{1n} \\ \lambda_{21} & \lambda_{22} - x & \cdots & \lambda_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ \lambda_{n1} & \lambda_{n2} & \cdots & \lambda_{nn} - x \end{vmatrix} = 0.$$

Cette équation, qui est indépendante de la base choisie, est appelée l'équation normale à laquelle satisfait θ. Si θ satisfait dans k à une

13) Voir pour la théorie des corps et la théorie de Galois: Hasse, Höhere Algebra, Sammlung Göschen, de Gruyter, 1927.

équation irréductible $\varphi(x) = 0$ de degré d, dont le premier coefficient est 1, le corps $k(\theta)$, le plus petit sous-corps de K contenant k et θ, est une extension de degré d de k. Si $\omega_1, \cdots, \omega_{n/d}$ forment une base relative de K par rapport à $k(\theta)$, les nombres $\omega_i \theta^j$ $(i = 1, 2, \cdots, n/d;\ j = 0, 1, 2, \cdots, d-1)$ forment une base relative de K par rapport à k. En calculant l'équation normale au moyen de cette base relative, on trouve que cette équation normale est $(\varphi(x))^{n/d} = 0$.

Le dernier terme de l'équation normale de θ est appelé *norme* de θ par rapport à k, et désigné par $N_{Kk}(\theta)$. On a

$$N_{Kk}(\theta) \cdot N_{Kk}(\theta') = N_{Kk}(\theta\theta').$$

Si k est de caractéristique 0 (c'est-à-dire si la somme d'un nombre quelconque d'éléments tous égaux à 1 n'est jamais nulle) ou si k est un champ de Galois, une équation irréductible dans k n'a dans une extension quelconque que des racines simples. De plus toute extension de degré fini n est obtenue par adjonction d'un nombre satisfaisant à une équation irréductible de degré n. Les corps k satisfaisant à ces conditions sont appelés parfaits. Ils seront seuls considérés dans la suite.

Théorème de Hilbert. Corps kummeriens.

Introduisons d'abord une notation qui nous sera très utile. K étant un sur-corps relativement abélien de k, soient σ_i les diverses opérations du groupe de Galois relatif. $f(\sigma_i)$ étant un polynome à coefficients entiers rationnels, de la forme $\sum a_{ij\ldots k}\, \sigma_i^{a_i} \sigma_j^{a_j} \ldots \sigma_k^{a_k}$, et A désignant un nombre de k, on posera

$$A^{f(\sigma_i)} = \prod \sigma_i^{a_i} \sigma_j^{a_j} \ldots \sigma_k^{a_k} (A^{a_{ij\ldots k}}),$$

Π représentant le produit algébrique des nombres écrits à droite de ce signe.

On a evidemment

$$A^{f(\sigma_i)+g(\sigma_i)} = A^{f(\sigma_i)} A^{g(\sigma_i)}, \qquad A^{f(\sigma_i)g(\sigma_i)} = (A^{f(\sigma_i)})^{g(\sigma_i)}$$

et $N_{Kk}(A) = A^{\Sigma\sigma_i}$.

Ceci posé, nous avons le

Théorème normique de Hilbert. *K étant un sur-corps relativement cyclique de k, soit σ une opération engendrant le groupe de Galois relatif.*

Tout nombre A de K dont la norme relative par rapport à k est 1 est de la forme $B^{1-\sigma}$, B étant un autre nombre de K.

Soit en effet θ un nombre de K différent de tous ses conjugués relatifs par rappart à k. Posons $m = (K:k)$ et

$$B_i = \theta^i + \frac{1}{A}\sigma\theta^i + \frac{1}{A^{1+\sigma}}\sigma^2\theta^i + \ldots + \frac{1}{A^{1+\sigma+\ldots+\sigma^{m-2}}}\cdot\sigma^{m-1}\theta^i.$$

Ces nombres B_i ne sont pas tous nuls, car considérés comme des formes linéaires par rapport aux variables $1, \frac{1}{A}, \ldots, \frac{1}{A^{1+\sigma+\ldots+\sigma^{m-2}}}$, leur déterminant est $\neq 0$.[14] Or chacun de ces nombres B_i satisfait à la relation

$$\sigma B_i = AB_i.$$

D'où, si $B_i \neq 0$, $A = (B_i^{-1})^{1-\sigma}$, ce qui démontre le théorème de Hilbert.

Conséquence[15] : Théorème de Lagrange.

K étant un sur-corps relativement cyclique de k de degré relatif n, si k contient une racine primitive n-ème de l'unité, ζ, on a $K=k(\sqrt[n]{\alpha})$, α étant un nombre de k.

En effet ζ, considéré comme nombre de K satisfait à la condition

$$N_{Kk}(\zeta) = \zeta^n = 1.$$

Donc il existe un nombre A de K tel que $\zeta = A^{\sigma-1}$, On a $\sigma^i A = \zeta^i A$, donc A est distinct de tous ses conjugués par rapport à k, et $K = k(A)$. De plus $(\sigma A)^n = \zeta^n A^n = A^n$, ce qui prouve que A^n est un nombre α de k.

k étant un corps satisfaisant aux conditions du théorème de Lagrange, un corps $k(\sqrt[n]{\alpha})$ est appelé *corps kummerien* par rapport à k.

Dans ce qui va suivre, nous supposerons toujours que k est un corps contenant les racines n-èmes. de l'unité. On désignera par g_n^k le groupe des puissances n-èmes. des nombres $\neq 0$ de k.

Lemme I. *α étant un nombre de k, le corps $k(\sqrt[n]{\alpha})$ est un sur-corps relativement cyclique de k de degré relatif égal à l'indice $((g_n^k, \alpha): g_n^k)$.*

Le corps $k(\sqrt[n]{\alpha})$ est évidemment relativement galoisien. Soit σ une opération du groupe relatif de Galois : on a $\sigma\sqrt[n]{\alpha} = \theta\sqrt[n]{\alpha}$, θ étant une racine n-ème. de l'unité, et la correspondance $\sigma \to \theta$ est un isomorphisme du groupe de Galois et d'un sous-groupe du groupe des racines n-èmes.

---

14) Le carré de ce déterminant est le discriminant de l'équation à laquelle satisfait θ dans k.

15) Le fait que ce théorème soit une conséquence du théorème de Hilbert montre que le théorème de Hilbert est la généralisation du théorème de Lagrange.

de l'unité, qui est cyclique. Donc le groupe de Galois est cyclique. Soit σ une opération engendrant ce groupe : si $\sigma\sqrt[n]{\alpha} = \theta\sqrt[n]{\alpha}$, l'ordre du groupe est l'ordre d de la racine de l'unité θ. Mais ce nombre est aussi le plus petit exposant x tel que $\sigma(\sqrt[n]{\alpha})^x = (\sqrt[n]{\alpha})^x$ donc tel que $(\sqrt[n]{\alpha})^x$ soit dans $k : d$ est le plus petit exposant x tel que $\alpha^x = \beta^n$, β étant dans k, ce qui démontre le lemme I. De plus on voit que d est toujours un diviseur de n.

Lemme II. *Tout nombre B du corps $k(\sqrt[n]{\alpha})$ dont la n-ème. puissance est dans k est de la forme $B = \beta(\sqrt[n]{\alpha})^x$, β étant dans k.*

Soit d le degré relatif de $k(\sqrt[n]{\alpha})$, et soit σ une opération engendrant le groupe de Galois relatif. Donc $\sigma\sqrt[n]{\alpha} = \theta\sqrt[n]{\alpha}$, θ étant une racine primitive d-ème. de l'unité. B^n étant dans k, on a $\sigma B = \zeta B$, ζ étant une racine n-ème. de l'unité. ζ est donc dans k et $\sigma^d B = \zeta^d B$. On a donc $\zeta^d = 1$, ζ est une racine d-ème. de l'unité, donc de la forme θ^x. On a

$$\sigma B = \theta^x B, \qquad \sigma(\sqrt[n]{\alpha})^x = \theta^x(\sqrt[n]{\alpha})^x,$$

$$\sigma(B(\sqrt[n]{\alpha})^{-x}) = B(\sqrt[n]{\alpha})^{-x}.$$

Donc $B(\sqrt[n]{\alpha})^{-x} = \beta \subset k$.

Théorème. *Soit g un groupe de nombres de k contenant g_n^k comme sous-groupe d'indice fini N. Soit K le sur-corps de k obtenu par adjonction des racines n-èmes. de tous les éléments α de g. On a*

$$(K : k) = N.$$

En effet choissons une base du groupe abélien g/g_n^k et dans chaque classe de base un élément α_i. Donc tout élément de g se met sous la forme

$$\alpha = \alpha_1^{\nu_1}\alpha_2^{\nu_2}\dots\alpha_r^{\nu_r}\beta^n$$

et α n'est puissance n-ème. exacte que si tous les $\alpha_i^{\nu_i}$ sont puissances n-èmes. exactes. Soit pour chaque i, $\alpha_i^{n_i}$ la plus petite puissance de α_i qui est dans g_n^k. On a $N = n_1 n_2 \dots n_r$, de plus $K = k(\sqrt[n]{\alpha_1}, \sqrt[n]{\alpha_2}, \dots, \sqrt[n]{\alpha_r})$.

Ceci posé le théorème est démontré pour $r = 1$ (Lemme I). Supposons le démontré pour $r - 1$ éléments de base et démontrons le pour r. Soit $k_1 = k(\sqrt[n]{\alpha_1})$. Soit dans k_1, g_1 le groupe $(g_n^{k_1}, \alpha_2, \dots, \alpha_r)$. On a $K = k_1(\sqrt[n]{\alpha_2}, \dots, \sqrt[n]{\alpha_r})$, et par suite $(K : k_1) = (g_1 : g_n^{k_1})$. Déterminons cet indice. Supposons qu'un élément $\alpha_2^{\nu_2}\dots\alpha_r^{\nu_r}$ soit la n-ème. puissance d'un élément B_1 de k_1. Donc B_1^n est dans k et d'après le lemme II, $B_1 = \beta(\sqrt[n]{\alpha_1})^{\nu_1}$, $\beta \subset k$. D'où

$$\alpha_1^{-\nu_1}\alpha_2^{\nu_2}\cdots\alpha_r^{\nu_r} = \beta^n,$$

ce qui éxige que $\nu_2 \equiv 0 \pmod{n_2}, \cdots, \nu_r \equiv 0 \pmod{n_r}$. On en déduit $(K:k_1) = (g_1 : g_n^{k_1}) = n_2 \cdots n_r$. D'où

$$(K:k) = (K:k_1)(k_1:k) = N,$$

ce qui démontre le théorème.

Une base relative particulière.

Théorème. *Soit K un sur-corps relativement galoisien d'un corps k. Le corps K possède une base relative par rapport à k formée d'un nombre et de ses conjugués par rapport à k.*

Soit $(\omega_1, \omega_2, \cdots, \omega_n)$ une base relative quelconque de K. Soient G le groupe de Galois relatif et σ les opérations de G. On a

$$(1) \qquad \omega_i^\sigma = \sum_j \lambda_{i,j}^{(\sigma)} \omega_j, \qquad \lambda_{i,j}^{(\sigma)} \subset k.$$

Nous associerons à σ la substitution linéaire $x_i' = \sum_j \lambda_{i,j}^{(\sigma)} x_j$. On voit tout de suite que nous avons défini une représentation de G. Si on remplace $(\omega_1, \omega_2, \cdots, \omega_n)$ par une autre base, cette représentation se changera en une représentation équivalente. Nous désignerons par $f(\sigma)$ le caractère de σ dans cette représentation, que nous désignerons elle-même par P_{Kk}.

Si le théorème est vrai, P_{Kk} doit être équivalente à la représentation obtenue au moyen d'une base composée d'un nombre et de ses conjugués relatifs. Soient $\omega_i = \omega^{\sigma_i}$ les nombres d'une telle base. La représentation correspondante est facile à trouver : si $\sigma\sigma_i = \sigma_k$, on a

$$(2) \qquad \lambda_{i,j}^{(\sigma)} = 0 \quad \text{si } j \neq k, \qquad \lambda_{i,k}^{(\sigma)} = 1.$$

D'où

$$\sum_i \lambda_{i,i}^{(\sigma)} = 0 \quad \text{si } \sigma \neq 1, \qquad \sum_i \lambda_{i,i}^{(1)} = n.$$

Autrement dit, on doit avoir $f(\sigma) = 0$ si $\sigma \neq 1$, $f(1) = n$. Réciproquement, si ces conditions sont réalisées, la représentation P_{Kk} est équivalente à celle fournie par les formules (2). On pourra donc obtenir par un changement linéaire de variables une base $(\omega_1', \omega_2', \cdots, \omega_n')$ dont les éléments, par application des opérations σ, subissent les transformations definies par les formules (2). Une telle base est composée d'un nombre et de ses conjugués. On appelle d'habitude *régulière* la représentation du groupe G définie par les formules (2). Soient R_σ la matrice des nombres définis par les formules (2), A_σ la matrice $(\lambda_{i,j}^{(\sigma)})$, Ω la matrice (ω_i^σ) dont chaque colonne est composée d'un élément de la base et de ses conjugués.

Appliquons à la formule (1) un automorphisme τ quelconque de G: les nombres $\lambda_{ij}^{(\sigma)}$ étant dans k, il vient

$$(3) \qquad \omega_i^{\tau\sigma} = \Sigma \lambda_{ij}^{(\sigma)} \omega_j^{\tau}.$$

Or la multiplication à gauche d'une matrice par R_σ a pour effet une permutation des lignes de la matrice, amenant la ligne de rang j sur la ligne de rang k défini par $\tau\sigma = \sigma_k$. D'où

$$(\omega_i^{\tau\sigma}) = R_\sigma \Omega.$$

Mais les formules (3) donnent

$$(\omega_i^{\tau\sigma}) = \Omega \Lambda_\sigma$$

et par suite on a

$$R_\sigma \Omega = \Omega \Lambda_\sigma.$$

Remarquons que le déterminant de la matrice Ω, son carré étant le discriminant du système de nombres $(\omega_1, \omega_2, \cdots, \omega_n)$, n'est par nul. Donc l'équation peut s'écrire

$$\Lambda_\sigma = \Omega^{-1} R_\sigma \Omega.$$

Mais la trace de Λ_σ est $f(\sigma)$ et on sait que deux matrices transformées l'une de l'autre ont même trace, ce qui démontre la proposition[15b]

Théorème des unités.

Nous supposerons maintenant que k est un corps fini de nombres algébriques. Nous rangerons l'ensemble des conjugués de k dans un ordre tel que, $k^{(i)}$ représentant ces divers conjugués, $k^{(1)}, k^{(2)}, \cdots, k^{(r_1)}$ soient réels, et que $k^{(r_1+\lambda)}$ et $k^{(r_1+r_2+\lambda)}$ soient imaginaires conjugués ($\lambda = 1, 2, \cdots, r_2$). Donc, N désignant le degré de k, on a $N = r_1 + 2r_2$.

K désignant un sur-corps relativement galoisien de k, chaque $k^{(i)}$ est contenu dans un conjugué $K^{(i)}$ de K. Si $k^{(i)}$ est imaginaire, $K^{(i)}$ l'est aussi. Si $k^{(i)}$ est réel, $K^{(i)}$ peut être réel ou imaginaire. Nous supposerons que pour $1 \leq i \leq \rho_1$ $K^{(i)}$ est réel, et pour $\rho_1 < i \leq r_1 = \rho_1 + \rho_2$, $K^{(i)}$ est imaginaire.

Soit G le groupe de Galois de K par rapport à k. G est isomorphe au groupe de Galois de $K^{(i)}$ par rapport à $k^{(i)}$, l'isomorphisme étant réalisé en associant entre elles des opérations qui se déduisent l'une de l'autre par application d'un isomorphisme bien determiné de k sur $k^{(i)}$. Si $\rho_1 < i \leq \rho_1 + \rho_2$, il y a entre $k^{(i)}$ et $K^{(i)}$ un sous-corps maximum

15b) Cette élégante démonstration est due à M. Hasse.

réel de $K^{(i)}$, appartenant à un sous-groupe d'ordre 2 du groupe de Galois de $K^{(i)}$ par rapport à $k^{(i)}$, qui par l'isomorphisme précédent, donne un sous-groupe d'ordre 2 de G engendré par une opération σ_i. Si i n'est pas entre ρ_1 et $\rho_1 + \rho_2$, on posera $\sigma_i = 1$. Ceci posé, nous allons démontrer le théorème suivant dû à Herbrand[16].

Théorème des unités. *Il existe dans* K $r_1 + r_2$ *unités* E_i *jouissant des propriétés suivantes*:

1) *On a* $\sigma_i E_i = E_i$.

2) *Pour chaque* i *prenons dans chaque classe de* G *modulo* (σ_i) *un élément* $\tau_j^{(i)}$. *Entre toutes les unités* $E_i^{\tau_j^{(i)}}$ *il n'y a qu'une relation multiplicative*[17] *de la forme*:

$$\prod_{i,j} E_i^{a_{i,j}\tau_j^{(i)}} = 1,$$

les $a_{i,j}$ étant des nombres entiers.

Le théorème de Dirichlet nous apprend qu'il existe dans K un système $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_{R-1}$ de $R-1$ unités indépendantes, où $R = n\rho_1 + \frac{n}{2}\rho_2 + nr_2$, n désignant le degré de K par rapport à k, et par conséquent, R représentant le nombre total des $\tau_i^{(j)}$, tel que toute autre unité ε de K se mette sous la forme

$$\varepsilon = \zeta \varepsilon_1^{u_1} \varepsilon_2^{u_2} \dots \varepsilon_{R-1}^{u_{R-1}},$$

ζ étant une racine de l'unité. σ désignant les opérations de G, on aura

$$\varepsilon_i^{\sigma} = \zeta_{i,\sigma}\, \varepsilon_1^{u_{i,1}^{(\sigma)}} \varepsilon_2^{u_{i,2}^{(\sigma)}} \dots \varepsilon_{R-1}^{u_{i,R-1}^{(\sigma)}}.$$

Nous associerons à σ la transformation linéaire à R variables définie par les formules

$$(1) \qquad x_i' = \sum_{j=1}^{R-1} u_{i,j}^{(\sigma)} x_j, \quad \text{si } i \leq R-1; \qquad x_R' = x_R.$$

On verifie tout de suite que cette correspondance définit une représentation P de G. Nous l'appellerons représentation de G au moyen des unités. Les unités cherchées, et leurs conjuguées, devront s'exprimer

16) Voir Herbrand, Nouvelle démonstration et généralisation d'un théorème de Minkowski, C.R. (1930), p. 1282. Cf. une démonstration plus simple dans: Artin, Über Einheiten relativ galoisscher Zahlkörper, Crelle 167.

17) Etant données des unités $E_1, E_1, \dots, E_\rho$ nous entendons par relation entre ces unités toute relation de la forme $E_1^{a_1} E_2^{a_2} \dots E_\rho^{a_\rho} = 1$, les a_i étant des entiers rationnels. Pleusieurs relations serait dites indépendantes si les forme linéaires $\sum a_i x_i$ qu'on peut construire avec leurs coefficients sont indépendantes. Une relation est une conséquence d'autres relations quand sa forme linéaire est une combinaison linéaire des formes linéaires relatives aux autres relations.

au moyen des ε_i, et elles devront subir quand on leur applique les transformations σ des transformations particulières : si $\sigma\tau_j \equiv \tau_{j'}$ (mod. (σ_i)) on devra avoir

$$\sigma E_i^{\tau_j} = E_i^{\tau_{j'}}.$$

Soit (2) $$E_i^{\tau_j} = \zeta \Pi_\chi \varepsilon_\chi^{\lambda_{i,j,\chi}}$$

(ζ désigne une racine quelconque de l'unité). Les R formes linéaires $y_{i,j} = \sum_\chi \lambda_{i,j,\chi} x_\chi$ devront subir, quand les x subissent les opérations de la représentation P, les transformations d'une représentation $P_0^{K/k}$ définie par

(3) $$y'_{i,j} = y_{i,j'}.$$

Réciproquement, si nous pouvons démontrer que P et $P_0^{K/k}$ sont équivalentes, nous pourrons toujours trouver R formes linéaires indépendantes à coefficients entiers rationnels $y_{i,j}$ des x subissant les transformations (3). Les unités (2) correspondantes élevées au besoin à une certaine puissance repondront à la question, car les R formes $y_{i,j}$, considérées comme fonctions des variables $x_1, x_2, \cdots, x_{R-1}$ en y annulant le coefficient de x_R, ne seront liées que par une relation.

Or, si K_1 est un sous-corps de K contenant k et appartenant au groupe G_1, la représentation de G_1 au moyen des unités de K est précisément la représentation de G_1 obtenue au moyen de la représentation P. Je dis que P_0^{K/K_1} est aussi la représentation de G_1 obtenue au moyen de P_0. Il suffit de montrer que, σ étant une opération de G_1, le caractère $\varphi_k(\sigma)$ dans $P_0^{K/k}$ est égal au caractère $\varphi_{K_1}(\sigma)$ de σ dans P_0^{K/K_1}. Or, si $\sigma \neq 1$, $\varphi_k(\sigma)$ est égal au nombre des σ_i égaux à σ. Ces σ_i sont donc dans G_1 ; soient d'autre part $K_1^{(i)}$ les divers conjugués de K_1. Cherchons les substitutions $\bar{\sigma}_i$ définies pour l'extension K/K_1 comme les σ_i le sont pour K/k. $\bar{\sigma}_i$ n'est different de 1 que si $K_1^{(i)}$ est réel, $K^{(i)}$ imaginaire ; dans ce cas $K_1^{(i)}$ est contenu dans le plus grand corps réel contenu dans $K^{(i)}$ et $\bar{\sigma}_i = \sigma_i$, σ_i est dans G_1. Si σ_i n'est pas dans G_1, $\bar{\sigma}_i = 1$. Or $\varphi_{K_1}(\sigma)$ est le nombre des $\bar{\sigma}_i$ égaux à σ. D'où $\varphi_{K_1}(\sigma) = \varphi_k(\sigma)$. D'autre part $\varphi_{K_1}(1) = \varphi_k(1) = R$.

Ceci posé, désignons par $f(\sigma)$ le caractère de σ dans la représentation au moyen des unités de K du groupe G. Nous voulons montrer que pour chaque σ, $f(\sigma) = \varphi_k(\sigma)$. Or prenons un σ determiné quelconque et désignons par G_1 le groupe engendré par σ, par K_1 le corps appartenant à G_1 : nous venons de voir que $f(\sigma)$ est le caractère de σ dans la représentation de G_1 au moyen des unités de K et que $\varphi_k(\sigma) = \varphi_{K_1}(\sigma)$. Il suffit donc de démontrer l'égalité en question dans le cas des

extensions cycliques (G_1 est cyclique). Nous ferons alors la démonstration par récurrence sur le degré de l'extension ; supposons donc K extension cyclique de degré n et le théorème démontré pour toutes les extensions cycliques de degré $< n$. On a $f(\sigma^a) - \varphi(\sigma^a) = 0$ pour $(a, n) > 1$. Les nombres $f(\sigma^a) - \varphi(\sigma^a)$ pour lesquels $(a, n) = 1$ étant rationnels, et se déduisant les uns des autres par des automorphismes du corps $R(\zeta)$ par rapport à R (ζ désignant une racine n-ème. de l'unité) sont égaux. D'autre part leur somme est nulle, ce qui achève la démonstration.

On peut transformer le résultat du théorème de Herbrand d'une manière qui sera commode dans la suite[18]. Tout d'abord posons $\varepsilon_i = \prod_j E_i^{\tau_j^{(i)}}$. Comme $\sigma_i E_i = E_i$, ε_i est une unité de k, et $\varepsilon_i^2 = N_{Kk}(E_i)$ si $\sigma_i \neq 1$, $\varepsilon_i = N_{Kk}(E_i)$ si $\sigma_i = 1$. Il existe par hypothèse une relation entre les unités $E_i^{\tau_j^{(i)}}$:

$$\prod_{i,j} E_i^{a_{i,j}\tau_j^{(i)}} = 1.$$

Prenons la norme de cette relation : il vient une relation

$$\prod_i \varepsilon_i^{A_i} = 1$$

qui doit être équivalente à la première quand on y remplace les ε_i par leurs expressions.

Or on peut dans un système d'unités satisfaisant aux conditions du théorème des unités, remplacer certaines unités E_i par des puissances de ces unités sans qu'il cesse de satisfaire aux conditions. Nous remplacerons E_i par $E_i^{A_i}$, de manière que la relation fondamentale prenne la forme

$$\varepsilon_1 \varepsilon_2 \ldots \varepsilon_r = 1.$$

Posons $n_i = \frac{n}{2}$ si $\sigma_i \neq 1$, et $n_i = n$ si $\sigma_i = 1$, et

$$H_i = \frac{E_i^{n_i}}{\varepsilon_i}$$

et considérons le système formé par les unites

$$(2) \qquad \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{r-1}, H_i^{\tau_j^{(i)}}.$$

18) Cette transformation de la forme du résultat est dûe à M. Artin. Cf. 16)

Cherchons quelles relations peuvent exister entre les unités de ce système. Remarquons qu'on peut construire avec les unités (2) le système d'unités $E_i^{n_i \tau_j^{(\sigma)}}$ qui ne sont liées que par une relation. Le système contenant $R + r - 1$ unités, ces unités sont liées par r relations indépendantes ($r = r_1 + r_2$). Mais nous connaissons déja r relations indépendantes, à savoir les relations $N_{Kk}(H_i) = 1$. Toute autre relation doit donc être une conséquence de celles-là.

Nous remarquerons que les relations $N_{Kk}(H_i) = 1$ sont elles-mêmes conséquences des relations

$$H_i^{\sum_j \tau_j^{(\sigma)}} = 1 \tag{3}$$

qui forment un système equivalent.

Extensions cycliques. Nombre des classes ambiges[19].

Soit k un corps fini de nombres algébriques, et soit K une extension relativement cyclique de degré relatif n. Soit G le groupe de Galois de K par rapport à k et soit σ un élément primitif de G (c'est-à-dire engendrant G).

Soit $\mathfrak{K}$ une classe d'idéaux au sens absolu de K. Si $\mathfrak{a}$ est un idéal de $\mathfrak{K}$, $\sigma\mathfrak{a}$ appartient à une classe qui ne dépend pas du choix de $\mathfrak{a}$ dans $\mathfrak{K}$. Cette classe se désigne par $\mathfrak{K}^\sigma = \sigma\mathfrak{K}$. Si $\mathfrak{K} = \sigma\mathfrak{K}$, on dit que la classe $\mathfrak{K}$ est ambige. On désignera par a le nombre des classes ambiges. C'est ce nombre que nous voulons calculer.

A cet effet, désignons par $\mathfrak{D}^*$ les idéaux qui appartiennent à des classes ambiges. Ils forment évidemment un groupe caractérisé par

$$\mathfrak{D}^{*1-\sigma} = (\theta)$$

où θ est un nombre. De plus les nombres θ qu'on obtient ainsi forment un groupe. Ils sont caractérisés par le fait que (θ) est la puissance $1-\sigma$ d'un idéal qui est nécessairement dans une classe ambige.

On désignera encore par :
$\mathfrak{a}$, α, A les idéaux $\neq 0$ de k, les nombres $\neq 0$ de k, les nombres $\neq 0$ de K,

19) Le calcul fait ici est la généralisation au cas "cyclique quelconque" du calcul fait par Takagi dans le cas "cyclique de degré premier," calcul dont l'idée essentielle se trouve dèja dans le "Zahlbericht" de Hilbert, dans la démonstration du théorème suivant: si un sur-corps relativement cyclique de degré premier de k est non ramifié, il y a au moins un idéal de k qui n'est pas principal dans k mais qui est principal dans le sur-corps. L'extension au cas "cyclique de degré quelconque" a été rendue possible par le théorème des unités de Herbrand.

$\mathfrak{D}$ les idéaux tels que $\mathfrak{D}^{1-\sigma} = (1)$,
A les nombres de $\mathfrak{K}$ dont la puissance $1-\sigma$ est une unité.

On a $$a = (\mathfrak{D}^* : (A)) = (\mathfrak{D}^* : \mathfrak{D}(A))\,(\mathfrak{D}(A) : (A))$$

Etudions d'abord le second facteur. Remarquons que le groupe (A) n'est autre que la partie commune aux groupes $\mathfrak{D}$ et (A) : car si un idéal $\mathfrak{D}$ est principal, soit $\mathfrak{D} = (A^*)$, on a $(A^*)^{1-\sigma} = 1$, $A^{*1-\sigma}$ est une unité et A^* est un nombre A. Réciproquement (A) représente un idéal qui est toujours un idéal $\mathfrak{D}$. Donc (voir le lemme p. 373.)

$$(\mathfrak{D}(A) : (A)) = (\mathfrak{D} : [\mathfrak{D}, (A)]) = (\mathfrak{D} : (A)) = \frac{(\mathfrak{D} : (\alpha))}{((A) : (\alpha))},$$

la justification de cette transformation venant de ce que $(\mathfrak{D} : (\alpha))$ est fini, comme nous allons le voir :

$$(\mathfrak{D} : (\alpha)) = (\mathfrak{D} : \mathfrak{a})\,(\mathfrak{a} : (\alpha)),$$

car tout idéal $\mathfrak{a}$ est un idéal $\mathfrak{D}$. Le second facteur est le nombre h_0 des classes de k. Calculons le premier facteur. Pour cela, nous allons chercher la structure des idéaux $\mathfrak{D}$. Soit $\mathfrak{p}$ un idéal premier du sous-corps, et soit dans K, $\mathfrak{p} = (\mathfrak{P}_1 \mathfrak{P}_2 \dots \mathfrak{P}_g)^{e_\mathfrak{p}}$ la décomposition de $\mathfrak{p}$ en facteurs premiers. $\mathfrak{D}$ se met sous la forme $\mathfrak{P}_1^{a_1} \mathfrak{P}_2^{a_2} \dots \mathfrak{P}_g^{a_g} \mathfrak{D}_\mathfrak{p}$ où $\mathfrak{D}_\mathfrak{p}$ est premier à $\mathfrak{p}$, et $\mathfrak{P}_1^{a_1} \mathfrak{P}_2^{a_2} \dots \mathfrak{P}_g^{a_g}$ doit être lui-même un idéal $\mathfrak{D}$. Mais les opérations σ^x permutent transitivement les idéaux $\mathfrak{P}_i$; ce n'est donc possible que si $a_1 = a_2 = \dots = a_g$. Or tout idéal $(\mathfrak{P}_1 \mathfrak{P}_2 \dots \mathfrak{P}_g)^\alpha$ se met et d'une seule manière sous la forme $(\mathfrak{P}_1 \mathfrak{P}_2 \dots \mathfrak{P}_g)^{\alpha'} \mathfrak{a}$, où $0 \leq \alpha' < e_\mathfrak{p}$. Donc les idéaux $\mathfrak{D}$ sont de la forme

$$\prod_\mathfrak{p} (\mathfrak{P}_1 \mathfrak{P}_2 \dots \mathfrak{P}_g)^{\alpha'} \mathfrak{a},$$

le produit étant étendu aux idéaux premiers $\mathfrak{p}$ de k qui sont ramifiés dans K; réciproquement tous ces idéaux sont des idéaux $\mathfrak{D}$. Comme d'autre part un idéal $\mathfrak{D}$ ne se met que d'une manière sous la forme précédente, nous avons un système complet de représentants des classes de $\mathfrak{D}$ modulo $\mathfrak{a}$, d'où $(\mathfrak{D} : \mathfrak{a}) = \prod_\mathfrak{p} e_\mathfrak{p}$, le produit étant étendu à tous les idéaux premiers $\mathfrak{p}$ finis de k.

Reste à calculer $((A) : (\alpha))$. On désignera par E les unités de K, par H les unités de K de norme relative 1 par rapport à k. On a $((A) : (\alpha)) = (AE : \alpha E)$. Toute unité étant un nombre A, ceci s'écrit encore $(A : \alpha E)$. L'opération $A \to A^{1-\sigma}$ est un homomorphisme du groupe A sur le groupe $A^{1-\sigma}$. L'ensemble des nombres A tels que $A^{1-\sigma}$ appartienne au groupe $E^{1-\sigma}$ est l'ensemble des αE. Par suite

$$(\Delta : \alpha E) = (\Delta^{1-\sigma} : E^{1-\sigma}).$$

Or par définition, $\Delta^{1-\sigma}$ est une unité, dont la norme est $\Delta^{(1-\sigma)(1+\sigma+\ldots+\sigma^{n-1})} = 1$, donc une unité H. Réciproquement, d'après le théorème de Hilbert, toute unité H est la puissance $1-\sigma$ d'un nombre de K qui est nécessairement un nombre Δ. Donc

$$(\Delta^{1-\sigma} : E^{1-\sigma}) = (H : E^{1-\sigma}).$$

Nous avons donc :

$$(\mathfrak{D}(A) : (A)) = \frac{h_0 \Pi e_\mathfrak{p}}{(H : E^{1-\sigma})}.$$

Transformons maintenant $(\mathfrak{D}^* : \mathfrak{D}(A))$. Appliquons l'homomorphisme $\mathfrak{D}^* \to \mathfrak{D}^{*1-\sigma}$: le groupe $\mathfrak{D}^{*1-\sigma}$ étant identique au groupe (θ), il vient

$$(\mathfrak{D}^* : \mathfrak{D}(A)) = ((\theta) : (A)^{1-\sigma}) = (\theta : A^{1-\sigma}E),$$

car tout E est un nombre θ. Appliquons maintenant l'homomorphisme $\theta \to N_{Kk}(\theta)$. En vertu du théorème de Hilbert, tout nombre dont la norme est de la forme $N_{Kk}(E)$ est de la forme $A^{1-\sigma}E$. Donc, on a

$$(\mathfrak{D}^* : \mathfrak{D}(A)) = (N_{Kk}(\theta) : N_{Kk}(E)).$$

Or de $(\theta) = \mathfrak{D}^{*1-\sigma}$ on déduit $(N_{Kk}(\theta)) = \mathfrak{D}^{*(1-\sigma)(1+\sigma+\ldots+\sigma^{n-1})} = 1$, donc $N_{Kk}(\theta) = \varepsilon$, ε désignant les unités de k. Remarquons que la puissance n-ème de tout ε est un $N_{Kk}(E)$, car $\varepsilon^n = N_{Kk}(\varepsilon)$. Donc $(\varepsilon : N_{Kk}(E))$ est fini et on peut écrire

$$(\mathfrak{D}^* : \mathfrak{D}(A)) = \frac{(\varepsilon : N_{Kk}(E))}{(\varepsilon : N_{Kk}(\theta))},$$

d'où

$$a = \frac{h_0 \Pi e_\mathfrak{p}}{(\varepsilon : N_{Kk}(\theta))} \times \frac{(\varepsilon : N_{Kk}(E))}{(H : E^{1-\sigma})}.$$

Or le second facteur se laisse transformer au moyen du théorème des unités. Désignons par $\bar{E}$ les unités qui se laissent construire au moyen d'un système d'unités de la nature du système (ε_i, H_i) construit à la fin du paragraphe précédent ; par $\bar{H}$ le groupe des unités $\bar{E}$ dont la norme relative par rapport à k est 1. Comme le groupe contient $R-1$ unités indépendantes, $(E : \bar{E})$ est fini. Nous allons appliquer le lemme de Herbrand (voir p. 375) dans le cas particulier suivant (se reporter à l'énoncé du lemme pour les notations) :

G : groupe des E ; g : groupe des $\bar{E}$,

T_1 automorphisme $E \to E^{1-\sigma}$; T_2 automorphisme $E \to N_{Kk}(E)$;

γ_1 groupe des ε ; γ_2 groupe des H.

On s'assure que les conditions d'application du lemme de Herbrand sont satisfaites. Désignant par $\bar{\varepsilon}$ les unités de k contenues dans le groupe $\bar{E}$, on a

$$\frac{(\varepsilon : N_{Kk}(E))}{(H : E^{1-\sigma})} = \frac{(\bar{\varepsilon} : N_{Kk}(\bar{E}))}{(H : E^{1-\sigma})}$$

à condition que les deux indices qui figurent au second membre soient finis, ce dont nous nous assurerons en les calculant.

Nous allons maintenant rester dans le groupe $\bar{E}$. Nous pouvons donc sans crainte de confusion supprimer les barres de surlignement. Tout élément du groupe se met sous la forme $E_i = \varepsilon_1^{a_1}\varepsilon_2^{a_2}\dots\varepsilon_{r-1}^{a_{r-1}} \prod_i H_i^{f_i(\sigma)}$. Nous pouvons toujours supposer que le groupe ne contient aucune racine de l'unité. Dans ces conditions une unité $\prod_i H_i^{f_i(\sigma)}$ ne peut être une unité ε que si elle est égale à 1 : car sa norme ε^n par rapport à k est 1. Donc

$$(\varepsilon : N_{Kk}(E)) = (\varepsilon_1^{a_1}\varepsilon_2^{a_2}\dots\varepsilon_{r-1}^{a_{r-1}} : \varepsilon_1^{na_1}\varepsilon_2^{na_2}\dots\varepsilon_{r-1}^{na_{r-1}}) = n^{r-1}$$

Les unités $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_{r-1}$ étant indépendantes, toute unité H se met sous la forme $H = \prod_i H_i^{f_i(\sigma)}$. Le groupe de Galois étant cyclique, tout élément $\sigma_i \neq 1$ est égal à $\sigma^{n/2}$ (les notations σ_i, n_i et plus loin ρ_1, ρ_2 sont les mêmes que dans la démonstration du théorème des unités). Par suite $f_i(\sigma)$ est un polynome en σ de degré $n_i - 1$, et on a les relations

$$H_i^{1+\sigma+\dots+\sigma^{n_i-1}} = 1,$$

dont toute autre est une conséquence. Ceci posé, si H est de la forme $E^{1-\sigma}$, on peut supposer que l'expression de E ne contient pas les ε_i. Alors

$$E = \prod_i H_i^{g_i(\sigma)} \qquad E^{1-\sigma} = \prod_i H_i^{g_i(\sigma)(1-\sigma)}$$

Dans la seconde formule, $g_i(\sigma)(1-\sigma)$ doit, en remplaçant σ^{n_i} par 1, être ramené à être un polynome de degré $< n_i$ et on devra alors avoir

$$f_i(\sigma) - g_i(\sigma)(1-\sigma) - \lambda_i(1-\sigma^{n_i}) = \rho_i(1+\sigma+\dots+\sigma^{n_i-1}),$$

où les λ_i sont des entiers, car $g_i(\sigma)$ est à coefficients entiers. Mais le premier membre est à coefficients entiers, donc ρ_i est aussi entier. Il en résulte $f_i(1) \equiv 0 \pmod{n_i}$. Réciproquement, si cette condition est réalisée, soit $f_i(1) = \lambda_i n_i$, et

$$\lambda_i(1+\sigma+\dots+\sigma^{n_i-1}) = h_i(\sigma)(1-\sigma) + \lambda_i n_i.$$

D'où $f_i(\sigma) = (1-\sigma)f_i^*(\sigma) + \lambda_i(1+\sigma+\ldots+\sigma^{n_i-1}) - (1-\sigma)h_i(\sigma)$,

$f_i(\sigma)$ est de la forme demandée.

Or chaque $f_i(1)$ peut prendre (mod. n_i), n_i valeurs differentes. On en déduit

$$(H: E^{1-\sigma}) = \prod_i n_i.$$

Or i varie de 1 à r, et $n_i = \frac{n}{2}$ si et seulement si $\rho_1 < i \leq \rho_1 + \rho_2$. D'où

$$(H: E^{1-\sigma}) = 2^{-\rho_2} n^r$$

et par suite

$$\frac{(\varepsilon: N_{Kk}(E))}{(H: E^{1-\sigma})} = \frac{2^{\rho_2}}{n},$$

ce qui donne finalement

$$a = \frac{h_0 2^{\rho_2} \prod_{\mathfrak{p}} e_{\mathfrak{p}}}{n(\varepsilon: N_{Kk}(\theta))}.$$

Remarquons encore que les nombres θ sont caracterisés par le fait que leur norme relative soit une unité. En effet un nombre dont la norme est une unité représente un idéal $\mathfrak{A}$ dont la norme est 1. $\mathfrak{p}$ désignant un idéal premier de k, soit $\mathfrak{p} = (\mathfrak{P}_1 \mathfrak{P}_2 \ldots \mathfrak{P}_g)^e$ la décomposition de $\mathfrak{p}$ en facteurs premiers dans K; soit $\mathfrak{A} = \prod_{i=1}^{g} \mathfrak{P}_i^{a_i} \mathfrak{A}_{\mathfrak{p}}$, $\mathfrak{A}_{\mathfrak{p}}$ étant premier à $\mathfrak{p}$. On peut supposer que σ change $\mathfrak{P}_i$ en $\mathfrak{P}_{i+1}$ $(i < g)$, et $\mathfrak{P}_g$ en $\mathfrak{P}_1$. Ceci posé, la norme par rapport à k de $\prod_i \mathfrak{P}_i^{a_i}$ doit être 1, d'où $\sum_i a_i = 0$. On peut donc trouver g nombres b_i tel que $a_i = b_i - b_i + 1$, en posant $b_{g+1} = b_1$. On en déduit $\prod_i \mathfrak{P}_i^{a_i} = (\prod_i \mathfrak{P}_i^{b_i})^{1-\sigma}$, ce qui démontre que $\mathfrak{A} = \mathfrak{B}^{1-\sigma}$. $\mathfrak{A}$ étant principal, $\mathfrak{B}$ est un idéal $\mathfrak{D}^*$ et par suite $\mathfrak{A} = (\theta)$.

Chapitre V.

Théorie des valeurs absolues et des corps locaux.

Corps à valeurs absolues. Suites convergentes. Limites.

Soit un corps quelconque k. Nous dirons que nous avons défini dans k une *valeur absolue*[20] si à chaque élément a de k nous avons associé un nombre réel $\varphi(a)$ non toujours égal ni à 1 ni à 0 satisfaisant aux conditions suivantes :

1) $$\varphi(a) \geq 0,$$

2) $$\varphi(ab) = \varphi(a) \times \varphi(b),$$

3) $$\varphi(a + b) \leq \varphi(a) + \varphi(b).$$

De la propriété 2) résulte $\varphi(0) = 0$ et que, si $b \neq 0$, on a $\varphi(b) \neq 0$. On en déduit $\varphi(\pm 1) = 1$.

Soit une suite (a_n) d'éléments de k. On dit que cette suite a une limite égale à a quand pour tout nombre positif ε il existe un entier n_0 tel que pour $n \geq n_0$ on ait $\varphi(a - a_n) < \varepsilon$. On s'assure facilement que :

Si les suites (a_n), (b_n) ont pour limites a, b, les suites $(a_n \pm b_n)$, $(a_n b_n)$ ont pour limites $a \pm b$, ab ; si $b \neq 0$, la suite $\left(\frac{a_n}{b_n}\right)$ a pour limite $\frac{a}{b}$.

Une suite qui a une limite est convergente au sens du critère de Cauchy, c'est-à-dire que pour tout nombre positif ε il existe un entier n_0 tel que, n étant un entier $\geq n_0$ et p un entier positif quelconque, on ait $\varphi(a_{n+p} - a_n) < \varepsilon$. Mais la réciproque n'est pas vraie en général. Aussi appellerons-nous en général *suites convergentes* les suites qui satisfont au critère de Cauchy. Il est facile de démontrer que :

Si (a_n), (b_n) sont des suites convergentes, il en est de même des suites $(a_n \pm b_n)$, $(a_n b_n)$. Si la suite (b_n) n'a pas pour limite 0, la suite $\left(\frac{a_n}{b_n}\right)$ est encore convergente.

Corps des suites convergentes.

Convenons de dire que deux suites convergentes (a_n), (a_n') sont équivalentes, et écrivons $(a_n) \sim (a_n')$ si $(a_n - a_n')$ est une suite de limite

20) La notion de valeur absolue a été introduite pour la première fois par M. Ostrowski.

0. On constate tout de suite que cette relation d'équivalence est réflexive, transitive, symétrique, que si (a_n) est équivalente à (a_n'), et (b_n) équivalente à (b_n'), les suites $(a_n \pm b_n)$, $(a_n b_n)$ sont respectivement équivalentes à $(a_n' \pm b_n')$, $(a_n' b_n')$ et que, si (b_n) n'est pas une suite de limite 0, $\left(\frac{a_n}{b_n}\right)$ est équivalente à $\left(\frac{a_n'}{b_n'}\right)$.

Nous rangerons les suites convergentes en classes, en rangeant dans une même classe toutes les suites équivalentes à l'une d'elles. Si A, B sont deux de ces classes, si (a_n) est une suite de A, et si (b_n) est une suite de B, la suite $(a_n + b_n)$ appartient à une classe qui ne dépend pas du choix de (a_n), (b_n) dans A, B: cette classe sera désignée par $A + B$. On définit de même $A - B$ et AB. Les suites de limite 0 forment une classe que nous désignerons par 0. Si $B \neq 0$, on définit encore $\frac{A}{B}$. L'addition et la multiplication que nous venons de définir entre ces classe jouissent des propriétés de l'addition et de la multiplication dans un corps. Donc nos classes forment un corps que l'on appelle *fermeture* du corps k par rapport à la valeur absolue considérée. Soit $\bar{k}$ ce corps.

Le corps $\bar{k}$ contient un sous-corps isomorphe à k, formé des classes de suites convergentes qui ont une limite dans k. Nous considérerons $\bar{k}$ comme un sur-corps de k.

Le corps $\bar{k}$ possède une valeur absolue qui prolonge celle de k, c'est-à-dire, qui pour tout élément de k coincide avec la valeur absolue précédemment définie. En effet soit (a_n) une suite convergente appartenant à une classe A. La suite des nombres $\varphi(a_n)$ est convergente (critère de Cauchy). Soit α sa limite. Nous poserons $\varphi(A) = \alpha$. On s'assure facilement que la fonction de A ainsi définie satisfait aux propriétés 1), 2), 3). De plus, si A est un élément a de k, on peut poser $a_n = a$, d'où $\varphi(A) = \varphi(a)$.[20b]

Si A est un élément quelconque de $\bar{k}$, et ε un nombre positif quelconque, il y a toujours un élément a de k tel que $\varphi(A-a) < \varepsilon$.

20b) D'ailleurs si $\varphi'(A)$ est une autre valeur absolue de $\bar{k}$ prolongeant la valeur absolue $\varphi(a)$ de k, toute suite de nombres de k qui est convergente "au sens de $\varphi(a)$" est aussi convergente "au sens $\varphi'(a)$" puisque dans k $\varphi'(a) = \varphi(a)$. Soit A un élément de $\bar{k}$ et soit une suite (a_n) de k telle que $\lim \varphi(A - a_n) = 0$. La suite (a_n) a "au sens $\varphi'(a)$" une limite A' dans la fermeture $\bar{k}^*$ de k pour la valeur absolue φ'. A' ne dépend que de A, et la correspondance $A \to A'$ est une isomorphie de $\bar{k}$ et de $\bar{k}^*$ telle que $\varphi'(A') = \varphi(A)$. En particulier si k est le corps des nombres rationnels, si $\varphi(a)$ est la valeur absolue $|a|^\alpha$, $0 < \alpha \leq 1$, $\bar{k}$ est le corps des nombres réels et on voit que toute valeur absolue $\varphi'(a)$ du corps des nombres réels qui est égale, pour a rationnel, à la valeur absolue $|a|^\alpha$, est donné par $\varphi(a) = \bar{a}^\alpha$, $\bar{a}$ étant le nombre déduit de a par un automorphisme du corps des nombres réels.

Dans $\bar{k}$ toute suite convergente a une limite. En effet soit (A_n) une suite convergente de $\bar{k}$. Choisissons pour chaque n un élément a_n de k tel que $\varphi(a_n - A_n) < \varepsilon$. La suite (a_n) sera également convergente. Elle a pour limite dans $\bar{k}$ la classe A à laquelle elle appartient. Donc $\lim (A - a_n) = 0$ et $\lim (A - A_n) = 0$, ce qui démontre notre proposition.

Si par exemple k est le corps des nombres rationnels et si on considère la valeur absolue ordinaire, $\bar{k}$ est le corps des nombres réels.

Valeurs absolues du corps des rationnels.[21]

Cherchons quelles sont les diverses valeurs absolues possibles du corps R des nombres rationnels. Remarquons que, a étant un entier positif, et $\varphi(x)$ une valeur absolue, on a

$$\varphi(a) = \varphi(1 + 1 + \cdots + 1) \leq a.$$

Soit p un entier > 1 quelconque. Tout nombre a se met, et d'une seule manière sous la forme

$$1) \qquad a = a_0 + a_1 p + \cdots + a_n p^n, \qquad 0 \leq a_i < p.$$

D'où $$\varphi(a) \leq \varphi(a_0) + \varphi(a_1)\varphi(p) + \cdots + \varphi(a_n)(\varphi(p))^n.$$

Supposons $\varphi(p) \leq 1$: on a $\varphi(a) \leq (n+1)p$. Remplaçons a par a^ν : n se trouve remplacé par un entier $n' < (n+1)^\nu$ et on a $\varphi(a)^\nu \leq ((n+1)^\nu + 1)p$, d'où $\varphi(a) \leq ((n+1)^\nu + 1)^{1/\nu} p^{1/\nu}$, quantité qui tend vers 1 quand $\nu \to \infty$. Donc :

S'il existe un entier $p > 1$ tel que $\varphi(p) \leq 1$, on a pour tout entier a, $\varphi(a) \leq 1$. Si alors $\varphi(x)$ n'est pas toujours égal à 1, il y a au moins un nombre premier p tel que $\varphi(p) < 1$. Soit q un autre nombre premier ; pour chaque n, il existe des entiers λ, μ tels que $\lambda p^n + \mu q^n = 1$, et $\varphi(\lambda) \leq 1$, $\varphi(\mu) \leq 1$. Si on avait $\varphi(q) < 1$, on pourrait choisir un entier n tel que $\varphi(p^n) < \frac{1}{2}$ et $\varphi(q^n) < \frac{1}{2}$, d'où $\varphi(\lambda p^n + \mu q^n) < 1$, ce qui est impossible. Donc pour tout nombre premier $q \neq p$, on a $\varphi(q) = 1$. Soit $\varphi(p) = \alpha$; on a pour tout entier rationnel $a \neq 0$, $\varphi(a) = \alpha^\nu$, si $a = p^\nu a'$, a' premier à p. Le nombre α doit être < 1. En effet on peut trouver deux nombres a, b non divisibles par p tels que $a + b$ soit divisible par une puissance p^ν de p aussi grande qu'on veut : la formule $\varphi(a + b) \leq \varphi(a) + \varphi(b)$ donne $\alpha^\nu < 2$, d'où $\alpha < 1$. Réciproquement, pour tout $\alpha < 1$, la fonction $\varphi(a)$ donne une valeur absolue. Donc :

21) La théorie exposée dans ce paragraphe est due à M. Artin. Cf. Artin, Über die Bewertungen algebraischer Zahlkörper, Crelle, 167.

Théorème 1. *$\varphi(a)$ désignant dans le corps des rationnels une valeur absolue, s'il existe un entier $a > 1$ tel que $\varphi(a) \leq 1$ il existe un nombre premier p tel que, p^ν désignant la participation de p au nombre rationnel a* (c'est-à-dire la puissance de p qui figure dans la décomposition de a en facteurs premiers), *on ait*

$$\varphi(a) = \alpha^\nu, \qquad \alpha < 1.$$

Les valeurs absolues ainsi définies seront appelées du premier type.

Envisageons maintenant l'autre cas, celui où pour tout entier a on a $\varphi(a) \geq 1$. Soit pour un entier p positif quelconque, $\varphi(p) = p^\alpha$, $0 < \alpha \leq 1$. On a, en reprenant la formule (1),

$$\varphi(a) \leq (n+1)p(\varphi(p))^n = p(n+1)p^{\alpha n} \leq p(n+1)a^\alpha.$$

Soit p^{n_ν} la plus haute puissance de p qui est $\leq a^\nu$, on a

$$\varphi(a^\nu) \leq p(n_\nu + 1)a^{\alpha\nu}.$$

Comme $(n_\nu + 1)^{1/\nu} \to 1$ si $\nu \to \infty$, on a $\varphi(a) \leq a^\alpha$. D'autre part soit $a = p^{n+1} - b$, d'où $\varphi(a) \geq p^{\alpha(n+1)} - \varphi(b)$. On a $b \leq p^{n+1} - p^n = p^n(p-1)$, $\varphi(b) \leq p^{\alpha n}(p-1)^\alpha$, d'où $\varphi(a) \geq p^{\alpha n}(p^\alpha - (p-1)^\alpha) = \lambda p^{\alpha n}$, où λ est un facteur ne dépendant que de p et de α. On a $\varphi(a^\nu) \geq \lambda p^{\alpha n_\nu}$; or $\dfrac{a^\nu}{p^{n_\nu}} \leq p$, d'où $p^{\alpha n_\nu} \geq \dfrac{a^{\alpha\nu}}{p^\alpha}$ et

$$\varphi(a^\nu) \geq \frac{\lambda}{p^\alpha} a^{\alpha\nu}; \qquad \varphi(a) \geq \left(\frac{\lambda}{p^\alpha}\right)^{\frac{1}{\nu}} a^\alpha.$$

En faisant tendre ν vers l'infini, il vient $\varphi(a) \geq a^\alpha$, d'où $\varphi(a) = a^\alpha$. Donc :

Théorème 2. *$\varphi(a)$ désignant dans le corps des rationnels une valeur absolue, si pour au moins un entier a on a $\varphi(a) > 1$, on a, pour tout nombre rationnel, $\varphi(a) = |a|^\alpha$, α étant un nombre compris entre 0 et 1.*

Les valeurs absolues définies par le Théorème 2 seront appelées valeurs absolues du second type.

Considérons maintenant un corps algébrique k quelconque, et soit $\varphi(a)$ une valeur absolue dans k ; k contient le corps R, et φ y induit une valeur absolue φ^*. Nous supposerons d'abord que cette valeur absolue est du second type. La fermeture de R par rapport à cette valeur absolue est donc isomorphe au corps des nombres réels. Soit $\bar{k}$ la fermeture de k par rapport à la valeur absolue φ : $\bar{k}$ contient un sous-corps $\bar{R}$ isomorphe au corps des nombres réels, et pour tout élément a de $\bar{R}$ on a $\varphi(a) = |\bar{a}|^\alpha$, φ désignant la valeur absolue de $\bar{k}$ qui prolonge celle de k,

et $\bar{a}$ l'élément correspondant à a dans l'isomorphie appliquant $\bar{R}$ sur le corps des nombres réels. Considérons $k\bar{R}$. Ce corps est algébrique par rapport à $\bar{R}$. Mais $\bar{R}$ étant isomorphe au corps des nombres réels, ou bien $k\bar{R} = \bar{R}$, ou bien $k\bar{R} = \bar{K}$, $\bar{K}$ désignant un corps isomorphe au corps des nombres complexes. Dans le premier cas il existe une isomorphie de k sur un corps de nombres réels, telle qu'on ait $\varphi(a) = |\bar{a}|^{\alpha}$, $\bar{a}$ étant l'élément qui correspond à l'élément a de k dans cette isomorphie. Envisageons le second cas. On a $\bar{K} = \bar{R}(i)$, i étant solution de l'équation $x^2 + 1 = 0$, et tout nombre de $\bar{K}$ se met sous la forme $a + bi$, a et b étant dans $\bar{R}$. Or,

$$a + bi = \sqrt{a^2 + b^2}\left(\frac{a}{\sqrt{a^2 + b^2}} + \frac{b}{\sqrt{a^2 + b^2}}i\right).$$

On sait que si x, y satisfont à $x^2 + y^2 = 1$, si on pose

$$(x + iy)^n = X_n + iY_n,$$

n étant un entier positif ou négatif, on a $X_n^2 + Y_n^2 = 1$; donc, $\varphi(X_n + iY_n)$ reste borné quel que soit n, ce qui n'est possible que si $\varphi(x + iy) = 1$. On a donc

$$\varphi(a + bi) = (\sqrt{a^2 + b^2})^{\alpha} = |a + bi|^{\alpha}.$$

Il en résulte que k est isomorphe à un corps de nombres complexs tel que $\bar{a}$ désignant le correspondant de a dans cette isomorphie on ait

$$\varphi(a) = |\bar{a}|^{\alpha}.$$

Donc :

Théorème 3. *Si dans un corps algébrique k, une valeur absolue $\varphi(x)$ est telle que $\varphi(a) > 1$ pour au moins un entier rationnel a, il existe une isomorphie de k sur un corps de nombres algébriques telle que, $\bar{a}$ désignant le correspondant d'un élément a de k, on ait*

$$\varphi(a) = |\bar{a}|^{\alpha}, \qquad 0 < \alpha \leq 1.$$

Corps locaux.

R désignant le corps des nombres rationnels et p un nombre premier positif, on désignera par R_p la fermeture de R par rapport à la valeur absolue $|a| = \varphi(a)$ définie au Théorème 1 (fermeture qui ne dépend évidemment pas du nombre α). Les éléments de R_p s'appellent *nombres p-adiques.*

Soit (a_n) une suite convergente de nombres de R. Donc si $|a_n| = \alpha^{\nu_n}$ les ν_n convergent aussi, ou tendent vers l'infini. Dans le second cas on

a lim $a_n = 0$. Dans le premier cas les ν_n sont tous égaux à partir d'un certain rang à un entier ν, et si lim $a_n = a$, on a $|a| = \alpha^\nu$. Ce nombre ν (indépendant de α) s'appelle *ordre* de a ; on le désigne s'il y a lieu par $\nu(a)$. On a

$$\nu(ab) = \nu(a) + \nu(b),$$

$$\nu(a + b) \geq \text{min. } (\nu(a), \nu(b)).$$

Désignons par Σ l'ensemble des éléments a pour lesquels $\nu(a) \geq 0$. Il en résulte que si Σ contient a, b, il contient aussi $a - b$ et ab (on dit que Σ est un *anneau*). Nous appellerons les éléments de Σ *les entiers* de R_p. Ces nombres sont en effet ceux qui peuvent être considérés comme limite d'entiers de R. On appelle *unités* de Σ les nombres a de Σ dont l'inverse appartient encore à Σ, donc les nombres d'ordre 0. Le nombre p est d'ordre 1, et par suite tout nombre de R_p se met et d'une seule manière sous la forme $p^\nu\varepsilon$, ν étant un entier rationnel quelconque, ε une unité. Il en résulte que les seuls idéaux de Σ sont les idéaux (p^ν). (Rappelons qu'on appelle *idéal* un ensemble E de nombres qui est tel que si a, b sont des nombres de E, $a - b$ soit dans E; que, λ étant un nombre quelconque de Σ, $a\lambda$ soit dans E; qu'il existe un entier rationnel m tel que ma soit toujours entier.) Le seul idéal premier est (p). Σ étant considéré comme groupe additif, $\Sigma/(p^\nu)$ pour ν positif, contient p^ν éléments, car tout nombre de R_p est congru à un nombre rationnel (mod. p^n) quel que soit n (les congruences se définissent pour tout idéal dans un anneau exactement comme les congruences par rapport aux idéaux de nombres algébriques).

Soit Z le champ de Galois formé des classes de restes d'entiers rationnels modulo p. $f(x)$ étant un polynome à coefficients entiers dans R_p, si on remplace chaque coefficient par l'élément de Z auquel il appartient, on obtient un polynome $f^*(x)$ à coefficients dans Z. Ceci posé, il se présente le fait remarquable suivant :

$f(x)$ étant un polynome irréductible de R_p il est impossible que $f^*(x)$ se décompose dans Z en le produit de deux polynomes premiers entre eux de degrés > 0.

Supposons en effet que $f^*(x) = g^*(x)h^*(x)$, les polynomes g^*, h^* étant premiers entre eux et de degrés > 0. Rappelons qu'on dit que deux polynomes sont congrus suivant un certain module quand les coefficients des termes de même degré dans ces polynomes sont congrus suivant le module en question. Ceci posé, on peut trouver des polynomes $g_1(x)$, $h_1(x)$ à coefficients dans R_p tels que

$$f(x) \equiv g_1(x)h_1(x) \pmod{p}; \quad g_1^*(x) = g^*(x); \quad h_1^*(x) = h^*(x).$$

On peut de plus supposer que le produit des termes de plus haut degré de g_1, h_1 est le terme de plus haut degré de f.

Démontrons par récurrence que, pour tout entier $\nu > 0$, on peut trouver des polynomes $g_\nu(x)$, $h_\nu(x)$ tels que

1) $$f(x) \equiv g_\nu(x)h_\nu(x) \pmod{p^\nu}; \quad g_\nu^*(x) = g^*(x); \quad h_\nu^*(x) = h^*(x),$$

le terme de plus haut degré de $f(x)$ étant le produit des termes de plus haut degré de $g_\nu(x)$, $h_\nu(x)$. Supposons le théorème démontré pour tous les entiers $\leq \nu$, et posons

2) $$g_{\nu+1}(x) = g_\nu(x) + p^\nu u_\nu(x),$$
$$h_{\nu+1}(x) = h_\nu(x) + p^\nu v_\nu(x),$$

et cherchons à déterminer $u_\nu(x)$, $v_\nu(x)$, de manière à avoir une congruence analogue à (1) pour l'exposant $\nu + 1$. Il vient

$$h_\nu(x)u_\nu(x) + g_\nu(x)v_\nu(x) \equiv \frac{f(x) - g_\nu(x)h_\nu(x)}{p^\nu} \pmod{p}.$$

Le second membre est un polynome $\varphi(x)$ à coefficients entiers de R_p. La condition nécessaire et suffisante pour que la congruence soit satisfaite est que

3) $$h_\nu^*(x)u_\nu^*(x) + g_\nu^*(x)v_\nu^*(x) = \varphi^*(x).$$

Soient r, s les degrés de $g_\nu(x)$, $h_\nu(x)$. $\varphi^*(x)$ est un polynome de degré $\leq r + s - 1$. De plus $g_\nu^*(x)$, $h_\nu^*(x)$ sont par hypothèse premiers entre eux. On sait qu'il est alors possible de déterminer des polynomes $u_\nu^*(x)$, $v_\nu^*(x)$ de degrés respectivement plus petits que r et s donnant lieu à l'égalité (3), et par suite des polynomes $u_\nu(x)$, $v_\nu(x)$ de degrés respectivement plus petits que r, s donnant lieu à la congruence imposés. On s'assure tout de suite que les polynomes définis par les formules (2) satisfont à toutes les conditions imposées.

Il est clair que quand $\nu \to \infty$, les coefficients des polynomes $g_\nu(x)$, $h_\nu(x)$ convergent vers ceux de polynomes $g(x)$, $h(x)$ tels que $f(x) = g(x)h(x)$, ce qui montre que $f(x)$ n'est pas irréductible.

Ceci posé, considérons une extension algébrique k déduite de R_p par adjonction d'un nombre satisfaisant à une equation irréductible dans R_p de degré n. Ces extensions seront appelées *corps locaux*.

Comme en théorie des corps de nombres algébriques on va définir les entiers de k comme étant les nombres de k tels que l'équation normale à laquelle ils satisfont dans R_p soit à coefficients entiers.

Désignons par f le plus petit exposant positif tel qu'il y ait une norme $N(\alpha)$ d'un nombre de k qui soit d'ordre f. Alors, l'ordre de la norme de tout nombre de k est un multiple de f; si $N(\beta)$ est d'ordre $f\lambda(\beta)$, appelons $\lambda(\beta)$ *l'ordre* de β. Il est clair que $\lambda(\beta_1\beta_2) = \lambda(\beta_1) + \lambda(\beta_2)$. Nous allons encore montrer que :

Les nombres de k d'ordre ≥ 0 sont les entiers de k.

Il suffit de montrer que les nombres d'ordre ≥ 0 sont des entiers, la reciproque étant évidente. Soit donc β un nombre tel que $N(\beta)$ soit un entier de R_p. Soit $\varphi(x) = 0$ l'équation irréductible de premier coefficient 1 à laquelle satisfait β dans R_p. Le dernier terme de cette équation est entier. Supposons qu'il y ait des coefficients non entiers : il existerait une puissance p^κ de p telle que tous les coefficients de $p^\kappa\varphi(x)$ soient entiers, l'un d'eux, et non le dernier, n'étant pas divisible par p. Donc on a $p^\kappa\varphi(x) = x^r(a_0 + \ldots) + p\psi(x)$, et en vertu du théorème qu'on vient de démontrer, $\varphi(x)$ ne serait par irréductible ce qui conduit à une contradiction.

Soient β_1, β_2 deux éléments quelconques $\neq 0$ de k, et supposons par exemple $\lambda(\beta_2) \geq \lambda(\beta_1)$. Donc $\frac{\beta_2}{\beta_1}$ est entier, et aussi $1 + \frac{\beta_2}{\beta_1}$, et $\lambda(\beta_1 + \beta_2) = \lambda(\beta_1) + \lambda\left(1 + \frac{\beta_2}{\beta_1}\right)$ ce qui démontre que $\lambda(\beta_1 + \beta_2) \geq \min.(\lambda(\beta_1), \lambda(\beta_2))$.

Donc l'ordre $\lambda(x)$ que nous venons de définir dans k satisfait aux mêmes conditions que l'ordre $\nu(x)$ que nous avions défini dans R_p, et nous pouvons raisonner sur lui comme nous l'avons fait sur $\nu(x)$. Il y a un nombre Π de k tel que $\lambda(\Pi) = 1$, et tout nombre de k se met sous la forme $\Pi^\lambda\varepsilon$, λ étant l'ordre du nombre considéré, et ε étant une unité, c'est-à-dire un nombre d'ordre 0. Les seuls idéaux de l'anneau des entiers sont les idéaux (Π^λ); le seul idéal premier est (Π), qu'on désignera par $\mathfrak{p}$. En particulier (p) représente un idéal qui est de la forme $\mathfrak{p}^e$. Si on appelle $N(\mathfrak{a})$ l'idéal engendré par les normes des éléments de $\mathfrak{a}$, on a

$$N(\mathfrak{p}^x) = (p)^{fx}.$$

D'où, puisque $N(p) = p^n$, $ef = n$. e s'appelle *exposant* et f *degré* de $\mathfrak{p}$.

On démontrera alors exactement comme dans la théorie des corps de nombres algébriques ordinaires que : il existe n entiers $\omega_1, \omega_2, \ldots, \omega_n$ de k tels que tout entier se mette, et d'une seule manière, sous la forme $\Sigma a_i\omega_i$, a_i entiers de R_p; de même, pour tout idéal $\mathfrak{a}$, il existe n entiers $\alpha_1, \alpha_2, \ldots, \alpha_n$ de $\mathfrak{a}$ tels que tout nombre de $\mathfrak{a}$ se mette et d'une seule manière sous la forme $\Sigma a_i\alpha_i$, les a_i étant des entiers de R_p.

Il en résulte, (p) étant considéré comme un idéal dans k et comme sous-groupe du groupe additif des entiers, que toute classe de restes de k modulo p contiendra un nombre et un seul de la forme $\Sigma a_i\omega_i$, les a_i étant des entiers rationnels tels que $0 \leq a_i < p$. Donc le nombre de ces classes de restes est p^n. D'autre part, choisissons dans chaque classe de restes de k modulo $\mathfrak{p}$ un nombre α_i. Toute classe de restes modulo p contiendra un nombre et un seul de la forme $\alpha_0^* + \alpha_1^* \Pi + \cdots + \alpha_{e-1}^* \Pi^{e-1}$, les α_i^* étant choisis parmi les α_i. Il en résulte que le nombre des classes de restes modulo $\mathfrak{p}$ est $p^{n/e} = p^f$.

Enfin, la théorie du corps relatif est fondée sur les faits suviants : si k' est un corps local compris entre R_p et k, soient $\mathfrak{p}'$ son idéal premier, e' et f' l'exposant et le degré de $\mathfrak{p}'$, Π' un nombre de k' tel que $\mathfrak{p}' = (\Pi')$. Alors (Π') resprésente dans k un idéal $\mathfrak{p}^{\bar{e}}$ et on a

$$(p) = \mathfrak{p}'^{e'} = \mathfrak{p}^{e'\bar{e}}.$$

Donc $e'\bar{e} = e$. De plus la norme relative de k par rapport à k' de Π représente dans k' un idéal $\mathfrak{p}'^{\bar{f}}$, et de la formule $N(\Pi) = N_{k'R_p}(N_{kk'}(\Pi))$, on déduit $f'\bar{f} = f$. Les nombres $\bar{e}, \bar{f}$ sont appelés *exposant relatif* et *degré relatif* de $\mathfrak{p}$ par rapport à k'. On dit que $\mathfrak{p}'$ est *non ramifié* dans k (ou que k est non ramifié par rapport à k'), si $\bar{e} = 1$; si $\bar{f} = 1$, on dit que $\mathfrak{p}'$ est *complètement ramifié* dans k.[22]

Enfin remarquons que si $\alpha^{\nu(a)}$ représente une valeur absolue de R_p, $\nu(a)$ étant l'ordre de a, la fonction

$$\varphi(x) = \alpha^{\frac{1}{e}\lambda(x)}$$

représente une valeur absolue de k prolongeant celle donnée dans R_p. *C'est la seule.* En effet, soit dans k, $\varphi_1(x)$ une valeur absolue telle que, si x est dans R_p, on ait $\varphi_1(x) = \varphi(x)$. Si x est entier, on a $\varphi(x) \leq 1$. En effet x satisfait dans R_p à une équation $x^n + a_1x^{n-1} + \ldots = 0$ à coefficients entiers. Donc, pour tout exposant N, on a $x^N = A_1x^{n-1} + A_2x^{n-2} + \cdots + A_n$, les A_i étant des entiers de R_p, donc $\varphi_1(A_i) \leq 1$. Donc, quel que soit N, $(\varphi_1(x))^N$ est borné, $\varphi_1(x) \leq 1$. Si x est une unité, $\varphi_1(x) = 1$, car x^{-1} est encore un entier. Si donc $\varphi_1(x)$ n'est pas toujours égale à 1, il faut en vertu de l'expression des entiers de k que $\varphi_1(\Pi) \neq 1$ où Π est

22) La méthode ici employée pour définir les corps locaux et obtenir leurs propriétés est derivée de deux articles de M. Hasse: "Über die Einzigkeit der beiden Fundamentalsätze des elementaren Zahlentheorie", Journal de Crelle, 155, 1926 et "Über p-adische Schiefkörper und ihre Bedeutung für die Arithmetik hypercomplexer Zahlsysteme", Math. Ann. 104, 1931.

un nombre tel que $(\Pi) = \mathfrak{p}$. Mais on a $p = \Pi^e\varepsilon$, ε étant une unité, $\varphi_1(p) = \alpha$, d'où $\varphi_1(\Pi) = \alpha^{1/e}$ et

$$\varphi_1(x) = \varphi_1(\Pi^{\lambda(x)}\varepsilon) = \alpha^{\frac{1}{e}\lambda(x)},$$

ce qui démontre nôtre proposition.

L'analyse dans un corps local.

Soit k un corps local.

Théorème. *La condition nécessaire et suffisante pour qu'une suite* (a_n) *soit convergente est que* $\lim (a_{n+1} - a_n) = 0$.

La condition est évidemment nécessaire. Supposons la remplie. Soit $\lambda(x)$ l'ordre défini plus haut. Pour tout entier positif m il existe donc un entier n_0 tel que, si $n \geq n_0$, on ait $\lambda(a_{n+1} - a_n) \geq m$. On a donc $a_{n+1} \equiv a_n \pmod{\mathfrak{p}^m}$ et par suite $a_n \equiv a_{n+1} \equiv \cdots \equiv a_{n+i} \pmod{\mathfrak{p}^m}$ quel que soit i. Le critère de Cauchy est donc verifié.

On en déduit que la condition nécessaire et suffisante pour qu'un produit infini $\prod_1^\infty (1 + a_n)$ converge vers une valeur $\neq 0$ est que $\lim a_n = 0$.

On a une proposition analogue au principe de Bolzano-Weierstrass :

De toute suite (a_n) *bornée* (c'est-à-dire telle que la valeur absolue de a_n soit bornée) *on peut extraire une suite convergente.*

En effet, la suite étant bornée, on peut trouver un nombre b tel que tous les éléments de la suite (ba_n) soient d'ordre positif. Ceci posé, définissons par récurrence une suite S_n de la manière suivante :

S_0 est la suite (ba_n).

S_{h-1} étant formée, il existe au moins une classe de restes $\pmod{\mathfrak{p}^h}$ qui contient une infinité de nombres de S_{h-1}. Ces nombres formeront S_h.

Ecrivons toutes ces suites les unes au dessous des autres et prenons la suite diagonale. Ce sera évidemment une suite convergente extraite de la suite (ba_n). La suite correspondante extraite de la suite (a_n) est aussi convergente.

Nous allons définir dans k des fonctions analogues aux fonctions exponentielle et logarithmique de l'analyse classique. x représentant un élément de k, cherchons la condition de convergence de la série

$$1 + x + \frac{x^2}{2!} + \cdots + \frac{x^n}{n!} + \cdots$$

Nous désignerons par χ l'ordre de x pour l'idéal premier $\mathfrak{p}$ de k, par e l'exposant de $\mathfrak{p}$, par p le nombre premier contenu dans $\mathfrak{p}$; l'ordre de x^n est χn. Soit p^ν la plus haute puissance de p ne dépassant pas n. L'ordre de $n!$ est

$$e\left(\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\cdots+\left[\frac{n}{p^\nu}\right]\right)\leq \frac{en}{p^\nu}\,\frac{p^\nu-1}{p-1}.$$

Donc l'ordre de $\frac{x^n}{n!}$ est $\geq n\left[\chi-\frac{e}{p-1}+\frac{e}{p^\nu(p-1)}\right]$. La série sera donc convergente si $\chi>\frac{e}{p-1}$. Elle représentera une fonction que nous désignerons par $\exp x$. On remarquera que si $\chi>\frac{e}{p-1}$, $n>1$ on a

$$n\chi-\frac{en}{p^\nu}\,\frac{p^\nu-1}{p-1}-\chi>(n-1)\,\frac{e}{p-1}-\frac{en}{p^\nu}\,\frac{p^\nu-1}{p-1}=\frac{e(n-p^\nu)}{p^\nu(p-1)}\geq 0,$$

ce qui montre que le terme $\frac{x^n}{n!}$ est d'ordre $>\chi$. Donc $\exp x-1$ est d'ordre χ.

On a $$\exp(x+y)=\exp x\cdot\exp\cdot y,$$

car cette égalité se démontre en analyse par un calcul formel qui reste valable tant que les séries sont convergentes.

Considérons maintenant la série

$$\xi-\frac{\xi^2}{2}+\cdots+(-1)^{n+1}\frac{\xi^n}{n}+\cdots$$

Soit χ l'ordre de ξ en $\mathfrak{p}$, et soit $n=p^u n'$ avec $(n',p)=1$. L'ordre en $\mathfrak{p}$ de $\frac{\xi^n}{n}$ est $\chi n-eu$. La série sera donc convergente dès que $\chi>0$. Elle représente une fonction que nous désignerons par $\mathrm{Log}\,(1+\xi)$. Remarquons que si x est en $\mathfrak{p}$ d'un ordre $>\frac{e}{p-1}$, $\exp x$ est $\equiv 1$ (mod. $\mathfrak{p}$) et par suite $\mathrm{Log}\,(\exp x)$ est défini. On démontre par un calcul formel que ce nombre est égal à x. Il en résulte que si y_1, y_2 sont $\equiv 1$ (mod. $\mathfrak{p}^{\left[\frac{e}{p-1}\right]+1}$) on a

$$\mathrm{Log}\,y_1y_2=\mathrm{Log}\,y_1+\mathrm{Log}\,y_2.$$

D'autre part le seul nombre $\equiv 1$ (mod. $\mathfrak{p}^{\left[\frac{e}{p-1}\right]+1}$) dont le logarithme soit 0 est 1. En effet si x est d'ordre λ en $\mathfrak{p}$ et si $\lambda>\frac{e}{p-1}$, $\exp x$ est

$\equiv 1 \pmod{\mathfrak{p}^\lambda}$ mais non $\pmod{\mathfrak{p}^{\lambda+1}}$. E étant un nombre de k qui est tel que $\operatorname{Log} E \equiv 0 \pmod{\mathfrak{p}}$, et a un nombre de $k \equiv 0 \pmod{\mathfrak{p}^{\left[\frac{e}{p-1}\right]}}$, on peut poser

$$E^a = \exp(a \operatorname{Log} E),$$

car $\exp(a \log E)$ est défini. Cette fonction jouit évidemment de la propriété

$$E^{a+b} = E^a \times E^b.$$

D'autre part elle est toujours $\equiv 1 \pmod{\mathfrak{p}^{\left[\frac{e}{p-1}\right]+\rho}}$ si ρ est l'ordre de $\operatorname{Log} E$. Soit X un nombre quelconque $\equiv 1 \pmod{\mathfrak{p}^{\left[\frac{e}{p-1}\right]+\rho}}$. Posons

$$x = \frac{\operatorname{Log} X}{\operatorname{Log} E}.$$

Donc $x \equiv 0 \pmod{\mathfrak{p}^{\left[\frac{e}{p-1}\right]}}$, et E^x est défini. On a $\operatorname{Log} E^x = \operatorname{Log} X$ donc $X = E^x$.

La correspondance $X \to x$ définit un isomorphisme du groupe (multiplicatif) des nombres $\equiv 1 \pmod{\mathfrak{p}^{\left[\frac{e}{p-1}\right]+\rho}}$ et du groupe additif des nombres $x \equiv 0 \pmod{\mathfrak{p}^{\left[\frac{e}{p-1}\right]}}$. Soit n un entier quelconque. Le groupe des nombres qui sont $\equiv 0 \pmod{n\mathfrak{p}^{\left[\frac{e}{p-1}\right]}}$ correspond dans cette isomorphie au groupe des X^n. Il en résulte que pour tout entier $n > 0$, il y a un nombre κ tel que :

Tout nombre de k qui est $\equiv 1 \pmod{\mathfrak{p}^\kappa}$ est la puissance n-ème. d'un nombre de k.

Il en résulte en particulier que :

Le groupe des puissances n-èmes. des nombres $\neq 0$ de k est un sous-groupe d'indice fini du groupe des nombres $\neq 0$ de k.

Corps de nombres $\mathfrak{p}$-adiques.

Soit maintenant k un corps de nombres algébriques fini quelconque, et soit $\varphi(x)$ une valeur absolue de k qui induise dans le corps R des nombres rationnels une valeur absolue du premier type, relative à un nombre premier p. Soit $\bar{k}$ la fermeture de k par rapport à $\varphi(x)$: $\bar{k}$ contient un sous-corps isomorphe au corps des nombres p-adiques, que nous désignerous par R_p. Considérons kR_p. C'est un corps algébrique fini par rapport à R_p, donc un corps local. Si pour un nombre rationnel a on a $\varphi(a) = \alpha^{\nu(a)}$, $\nu(a)$ étant l'ordre de a, on a nécessairement pour tout élément x de kR_p, $\varphi(x) = \alpha^{\frac{1}{e}\lambda(x)}$, $\lambda(x)$ étant

l'ordre défini au paragraphe précédent dans un corps local, et e l'exposant de l'idéal premier de kR_p. Or, en vertu des propriétés de la fonction $\lambda(x)$, les entiers de k pour lesquels $\lambda(x) \geq 1$ forment dans k un idéal $\mathfrak{p}$. Cet idéal est premier, car, x_1 et x_2 étant des entiers, si $x_1 x_2$ est dans $\mathfrak{p}$, de la formule $\lambda(x_1 x_2) = \lambda(x_1) + \lambda(x_2)$ résulte que l'un au moins des nombres $\lambda(x_1)$, $\lambda(x_2)$ est ≥ 1. D'ailleurs $\mathfrak{p}$ est la partie commune à l'idéal premier de kR_p et au système des entiers de k. Le nombre $\lambda(x)$ est alors défini de la manière suivante: x étant un entier de k, si $(x) = \mathfrak{p}^\lambda \mathfrak{a}$, $(\mathfrak{a}, \mathfrak{p}) = 1$, on a $\lambda(x) = \lambda$. Donc:

$\varphi(x)$ étant dans un corps fini de nombres algébriques k une valeur absolue telle qu'il existe un entier rationnel p de valeur absolue < 1, il existe dans k un idéal premier $\mathfrak{p}$ tel que, $\lambda(x)$ désignant l'exposant avec lequel $\mathfrak{p}$ intervient dans la décomposition de (x) en facteurs premiers, on ait $\varphi(x) = \alpha_0^{\lambda(x)}$, $0 < \alpha_0 < 1$.

Le nombre $\lambda(x)$ s'appelle *ordre de x pour $\mathfrak{p}$*.

La fermeture de k pour $\varphi(x)$ est d'ailleurs kR_p. En effet soit θ un nombre engendrant k, et soit

$$\omega_n = a_n^{(0)} + a_n^{(1)}\theta + \ldots + a_n^{(n-1)}\theta^{n-1}$$

une suite convergente de nombres de k. Les dénominateurs des nombres rationnels $a_n^{(i)}$ sont divisibles par des puissances bornées de p, car sans cela, la suite (ω_n) ne serait pas convergente. Donc, on peut de chaque suite $a_n^{(i)}$ extraire une suite convergeant vers un nombre $a^{(i)}$ de R_p. Si $\omega = \lim \omega_n$, on a

$$\omega = a^{(0)} + a^{(1)}\theta + \ldots + a^{(n-1)}\theta^{n-1},$$

ce qui démontre notre assertion.

Ce corps kR_p s'appelle corps des nombres $\mathfrak{p}$-adiques de k. On le désigne par $k_\mathfrak{p}$. Ce corps est un corps local, car c'est une extension finie de R_p. Réciproquement Hensel a démontré que tout corps local pouvait être obtenu de cette manière.

Soit K un sur-corps de k; soit $\mathfrak{P}$ un diviseur premier de $\mathfrak{p}$ dans K d'exposant relatif e, de degré relatif f. $K_\mathfrak{P}$ est un sur-corps de degré relatif ef de $k_\mathfrak{p}$. Cette proposition résulte du fait que e, f sont aussi l'exposant et le degré relatifs de l'idéal premier de $K_\mathfrak{P}$ par rapport à $k_\mathfrak{p}$. Pour e, c'est évident. Pour f, c'est une conséquence du lemme suivant:

Tout nombre d'un corps de nombres $\mathfrak{p}$-adiques $k_\mathfrak{p}$ est congru (mod. $\mathfrak{p}^n$) *à un nombre de k, quelque soit n.*

En effet soit a un nombre de $k_\mathfrak{p}$ et $a = \lim a_n$, a_n étant dans k.

L'ordre de $a - a_n$ augmente indéfiniment avec n, ce qui démontre la proposition.

Remarquons que si n est assez grand, l'ordre de a_n est égal à l'ordre de a. Soit λ_0 ce nombre. Choisissons n' assez grand pour que $a_{n'} - a$ soit d'ordre $\geq n + \lambda_0$: on aura aussi $a \equiv a_{n'} \pmod{\mathfrak{p}^n}$. Donc, dans la proposition précédente, la congruence additive peut être remplacée par une congruence multiplicative.

Supposons K relativement galoisien par rapport à k. Soit G_Z le groupe de décomposition de $\mathfrak{P}$, et soit σ une opération de G_Z. Si la suite (a_n) de nombres de K est convergente dans $K_{\mathfrak{P}}$ et a pour limite a, la suite σa_n est aussi convergente et a pour limite un élément σa. La correspondance $a \to \sigma a$ est un automorphisme de K laissant invariants les nombres de $k_{\mathfrak{p}}$. En effet, la correspondance conserve la somme et le produit, et est évidemment bi-univoque en vertu de l'existence de σ^{-1}. On obtient ainsi ef automorphismes distincts de K. Comme $K_{\mathfrak{P}}$ est de degré relatif ef par rapport à $k_{\mathfrak{p}}$, on obtient ainsi tous ses automorphismes. Donc:

Si K est galoisien par rapport à k, le groupe de Galois de $K_{\mathfrak{P}}$ par rapport à $k_{\mathfrak{p}}$ est isomorphe au groupe de décomposition de $\mathfrak{P}$ dans l'extension K/k.

La théorie du groupe d'inertie s'étend sans en changer un mot aux extensions de corps locaux.

La théorie des restes normiques.

Soit un corps de nombres algébriques fini k et soit dans k un module $\mathfrak{m}$ quelconque. Soit K une extension finie de k. Un nombre α de k est dit *reste normique* (mod. $\mathfrak{m}$) de K quand il existe un nombre A de K tel que $\alpha \equiv N_{Kk}(A) \pmod{\mathfrak{m}}$.

Théorème. *K étant extension galoisienne de k, la condition nécessaire et suffisante pour qu'un nombre α de k soit reste normique de K* (mod. $\mathfrak{p}^n$), *$\mathfrak{p}$ étant un idéal premier de k, et n un exposant positif quelconque, est que α, considéré comme un nombre de $k_{\mathfrak{p}}$, soit norme relative par rapport à $k_{\mathfrak{p}}$ d'un nombre de $K_{\mathfrak{P}}$, $\mathfrak{P}$ désignant un facteur premier de $\mathfrak{p}$ dans K.*

1) Supposons qu'il existe un nombre A de $K_{\mathfrak{P}}$ tel que

$$\alpha = N_{K_{\mathfrak{P}} k_{\mathfrak{p}}}(A).$$

Soit $\mathfrak{p} = \mathfrak{P}^e \mathfrak{Q}$, où $\mathfrak{Q}$ est un idéal premier à $\mathfrak{P}$. Déterminons dans K un nombre A_n tel que

$$A_n \equiv A \pmod{\mathfrak{P}^{ne}}, \qquad A_n \equiv 1 \ (\mathfrak{Q}^n).$$

Si σ est une opération du groupe de Galois de K appartenant au groupe de décomposition G_Z de $\mathfrak{P}$, on a $\sigma A_n \equiv \sigma A \pmod{\mathfrak{P}^{ne}}$; si σ n'appartient pas à G_Z, on a $\sigma A_n \equiv 1 \pmod{\mathfrak{P}^{ne}}$. En faisant le produit de ces congruences, on obtient

$$N_{Kk}(A_n) \equiv N_{K\mathfrak{P}k_\mathfrak{p}}(A) = \alpha \pmod{\mathfrak{P}^{ne}}.$$

Les termes extrêmes de cette congruence étant dans k, la congruence a lieu (mod. $\mathfrak{p}^n$).

2) Supposons que pour chaque n il existe un nombre A_n de K tel que $\alpha \equiv N_{Kk}(A_n) \pmod{\mathfrak{p}^n}$. G étant le groupe de Galois de K par rapport à k, choisissons g éléments $\sigma_1, \sigma_2, \ldots, \sigma_g$ de ce groupe tels que tout élément du groupe se mette et d'une seule manière sous la forme $\tau\sigma_i$, τ étant dans G_Z. Posons

$$A_n' = \prod_{i=1}^{g} \sigma_i A_n$$

On a $N_{Kk}(A_n) = N_{K\mathfrak{P}k_\mathfrak{p}}(A_n') \equiv \alpha \pmod{\mathfrak{P}^{ne}}$. Il en résulte que la suite (A_n') est bornée. On peut donc en extraire une suite convergeant dans $K_\mathfrak{P}$ vers un nombre A, et on a $\alpha = N_{K\mathfrak{P}k_\mathfrak{p}}(A)$, ce qui démontre le théorème.

k étant un corps local, on appelle *groupe associé* à K dans k le groupe des nombres $\neq 0$ de k qui sont normes relatives par rapport à k de nombres de K. L'étude de ce groupe associé fera l'objet de la théorie du corps de classes local. Nous allons maintenant considerer le cas où K est relativement cyclique par rapport à k.

Extensions cycliques des corps locaux.

Soient k un corps local, K une extension relativement cyclique de k. On désignera dans ce paragraphe par

α les nombres $\neq 0$ de k ; ε les unités de k,

A les nombres $\neq 0$ de K ; E les unités de K,

H les nombres de K de norme relative 1 par rapport à k,

σ une opération dont les puissances engendrent le groupe de Galois de K par rapport à k,

$\mathfrak{p}$ l'idéal premier de k ; $\mathfrak{P}$ celui de K ; on posera

$$\mathfrak{p} = \mathfrak{P}^e, \quad N_{Kk}(\mathfrak{P}) = \mathfrak{p}^f, \quad ef = n,$$

ϖ un nombre de k tel que $\mathfrak{p} = (\varpi)$; Π un nombre de K tel que $\mathfrak{P} = (\Pi)$.

On se propose de déterminer l'indice du groupe associé à K dans k. Remarquons d'abord que cet indice est fini, car la puissance n-ème de tout nombre de k appartient au groupe associé.

L'indice cherché est $(\alpha : N_{Kk}(A))$, c'est-à-dire $(\varpi^{\nu}\varepsilon : N_{Kk}(\Pi^{\nu}E))$. Soit $N_{Kk}(\Pi) = \varpi^{f}\varepsilon_0$; l'indice précedent s'écrit $(\varpi^{\nu}\varepsilon_0\varepsilon : \varpi^{\nu f}\varepsilon_0 N_{Kk}(E))$, ou encore

$$(\varpi^{\nu}\varepsilon_0\varepsilon : \varpi^{\nu f}\varepsilon_0\varepsilon)\,(\varpi^{\nu f}\varepsilon_0\varepsilon : \varpi^{\nu f}\varepsilon_0 N_{Kk}(E)).$$

Le premier facteur est evidemment égal à f. Le second est égal à $(\varepsilon : N_{Kk}(E))$. C'est ce nombre que nous voulons calculer.

A cet effet, remarquons qu'il existe dans K un sous-groupe d'indice fini du groupe des E, qui est isomorphe au groupe additif des entiers de $K \equiv 0 \pmod{\mathfrak{P}^x}$, x étant un entier assez grand. En effet, si $x > \dfrac{e}{p-1}$ la fonction $\operatorname{Log} E$ définit une isomorphie du groupe multiplicatif des nombres $\equiv 1 \pmod{\mathfrak{P}^x}$ avec le groupe additif des nombres $\equiv 0 \pmod{\mathfrak{P}^x}$. D'autre part, on a demontré qu'il existe une base relative de K par rapport à k formée d'un nombre Ω et de ses conjugués. Mettons un entier de K sous la forme $\sum_{i=0}^{n-1}\alpha_i\Omega^{\sigma^i}$. Les dénominateurs des α_i ne sont divisibles que par des puissances de $\mathfrak{p}$ qui restent bornées pour tous les entiers. Il en résulte qu'il existe un entier x' tel que tous les nombres $\Sigma\alpha_i\Pi^{x'}\Omega^{\sigma^i}$, où les α_i sont des entiers de k, soient $\equiv 0 \pmod{\mathfrak{P}^x}$, et le groupe additif formé par ces nombres est un sous-groupe d'indice fini du groupe additif de tous les nombres $\equiv 0 \pmod{\mathfrak{P}^x}$. Posons

$$E_0' = \exp(\Pi^{x'}\Omega)$$

et désignons par E' tous les nombres de la forme $E_0'^{f(\sigma)}$, $f(\sigma)$ étant un polynome à coefficients entiers dans k. D'après ce qu'on vient de dire, le groupe E' est un sous-groupe d'indice fini du groupe des E.

Ceci posé, nous allons appliquer le lemme de Herbrand avec les conventions suivantes :

G : groupe des E ; g : groupe des E',

T_1 : automorphisme $E \to E^{1-\sigma}$; T_2 : automorphisme $E \to N_{Kk}(E)$,

γ_1 : groupe des ε ; γ_2 : groupe des H.

Il vient

$$\frac{(\varepsilon : N_{Kk}(E))}{(H : E^{1-\sigma})} = \frac{(\varepsilon' : N_{Kk}(E'))}{(H' : E'^{1-\sigma})},$$

où $\varepsilon' = [\varepsilon, E']$, $H' = [H, E']$. La formule est valable si les deux indices qui figurent au second membre sont finis, ce que nous allons prouver en les calculant.

Remarquons d'abord que par suite de la définition de Ω, il n'y a aucune relation de la forme $E_0'^{f(\sigma)} = 1$, si $f(\sigma)$ est de degré $\leqq n-1$. Cherchons les unités ε' : si $\varepsilon' = E_0'^{f(\sigma)}$ on doit avoir $E_0'^{\sigma f(\sigma)} = E_0'^{f(\sigma)}$, avec $f(\sigma)$ de degré au plus $n-1$. Ce n'est possible que si $f(\sigma)(1-\sigma) = \rho(1-\sigma^n)$ avec un nombre ρ nécessairement entier. Donc $f(\sigma) = \rho(1+\sigma+\cdots+\sigma^{n-1})$ et $[\varepsilon' : N_{Kk}(E')] = 1$. De même si $H' = E_0'^{f(\sigma)}$, on a $f(\sigma)(1+\sigma+\cdots+\sigma^{n-1}) = g(\sigma)(1-\sigma^n)$, $g(\sigma)$ étant à coefficients entiers. Donc $f(\sigma) = (1-\sigma)\,g(\sigma)$ et par suite $(H' : E'^{1-\sigma}) = 1$. On a donc

$$(\varepsilon : N_{Kk}(E)) = (H : E^{1-\sigma}).$$

Or le second membre se laisse calculer facilement. D'après le théorème de Hilbert, le groupe H est identique au groupe $A^{1-\sigma}$, c'est-à-dire au groupe $\Pi^{\nu(1-\sigma)}E^{1-\sigma}$. Soit $\Pi^{1-\sigma} = H_0$, et soit H_0^x la plus petite puissance de H_0 contenue dans le groupe $E^{1-\sigma}$. On a donc

$$\Pi^{x(1-\sigma)} = E_0^{1-\sigma}; \qquad \Pi^x = E_0\alpha, \qquad (\Pi^x) = (\alpha).$$

Le plus petit nombre repondant à la question est donc e. D'où

$$(\varepsilon : N_{Kk}(E)) = (H : E^{1-\sigma}) = e,$$

$$(\alpha : N_{Kk}(A)) = ef = n.$$

Donc :

Le groupe associé dans un corps local k à un sur-corps relativement cyclique K est dans le groupe des nombres $\neq 0$ de k d'indice égal à $(K : k)$.

De plus, nous avons montré que :

Le groupe des normes d'unités de K par rapport à k est dans le groupe des unités de k d'indice égal à l'exposant par rapport à k de l'idéal premier de K.

On remarquera enfin qu'il existe un module $\mathfrak{p}^a$ tel que tout nombre $\equiv 1 \pmod{\mathfrak{p}^a}$ soit norme relative d'un nombre de K : car il existe un module $\mathfrak{p}^{a'}$ tel que tout nombre $\equiv 1 \pmod{\mathfrak{p}^{a'}}$ soit puissance n-ème d'un nombre de k.

Chapitre VI.

Théorie du Corps de Classes.

Nous sommes maintenant en mesure d'aborder le problème de la théorie du corps de classes, c'est-à-dire celui de la décomposition d'un idéal premier d'un corps de nombres algébriques fini dans un sur-corps relativement abélien.

Au cours de ce chapitre nous désignerons par k un corps fini de nombres algébriques quelconque. Le problème sera résolu quand nous aurons démontré les deux théorèmes suivants :

Théorème A. *K étant un sur-corps relativement abélien de k, soit $\mathfrak{d}$ le discriminant relatif de K. Il existe dans le groupe A des idéaux de k premiers à $\mathfrak{d}$ un sous-groupe H jouissant des propriétés suivantes :*

1) *$\mathfrak{p}$ étant un idéal premier de k, premier à $\mathfrak{d}$, $\mathfrak{p}^f$ étant la plus petite puissance de $\mathfrak{p}$ contenue dans H, $\mathfrak{p}$ se décompose dans K en idéaux premiers de degré relatif f.*

2) *le groupe A/H est isomorphe au groupe de Galois de K par rapport à k.*

Théorème B. 1) *Il existe un module $\mathfrak{m}_0$ composé d'idéaux premiers de k ramifiés dans K, tel que H soit groupe de congruence* (mod. $\mathfrak{m}_0$).

2) *$\mathfrak{m}$ étant un multiple quelconque de $\mathfrak{m}_0$, le groupe $H_\mathfrak{m}$ des idéaux de H premiers à $\mathfrak{m}$ est le groupe des classes d'idéaux* (mod. $\mathfrak{m}$) *qui contiennent des normes par rapport à k d'idéaux de K.*

Le théorème B nous apprend que le groupe H visé au théorème A est un groupe de congruence. Nous dirons que le corps K est *corps de classes* par rapport à k pour un groupe H' de congruence si ce groupe est égal à H.

Nous avons dit que la première définition générale du corps de classes avait été donnée par Weber. Dans le langage ici employé, cette définition équivalait au fait qu'il existe un groupe H satisfaisant aux conditions du théorème A et à la condition 1) du théorème B. On voit que dans cette définition le groupe n'était pas donné explicitement. C'est pourquoi il n'a pas été possible de fonder la théorie du corps de classes sur cette base : on manquait de point de départ et d'orientation dans les raisonnements à faire.

La méthode de Takagi a été la suivante : il considère le groupe défini sans ambiguité au théorème B et appelle K corps de classes quand l'indice de ce groupe de congruence est égal au degré relatif de K par rapport à k. Il montre que tout corps abélien est corps de classes en ce

sens, et peut ensuite démontrer que le groupe défini au théorème B répond encore aux conditions du théorème A.

Le succès de la méthode de Takagi provient donc du fait que l'on a un groupe bien déterminé sur lequel on peut raisonner pour montrer qu'il possède telles ou telles propriétés.

Depuis Takagi, le plus gros progrès de la théorie fut dû à M. Artin, qui a démontré la loi générale de réciprocité, qui s'énonce ainsi :

K étant corps de classes par rapport à k pour le groupe H, $\mathfrak{p}$ désignant un idéal premier de k non ramifié dans K, le symbole de Frobenius $\left(\frac{K}{\mathfrak{p}}\right)$ *ne dépend que de la classe* (mod. *H*) *à laquelle appartient* $\mathfrak{p}$. *Si* $\mathfrak{p}_1$ *appartient à la classe* $\mathfrak{K}_1$, $\mathfrak{p}_2$ *à la classe* $\mathfrak{K}_2$, $\mathfrak{p}_3$ *à la classe* $\mathfrak{K}_1\mathfrak{K}_2$, *on a*

$$\left(\frac{K}{\mathfrak{p}_3}\right) = \left(\frac{K}{\mathfrak{p}_1}\right)\left(\frac{K}{\mathfrak{p}_2}\right).$$

Ce théorème joue un rôle fondamental dans la théorie et ses applications. C'est de lui que nous partirons ici pour construire la théorie du corps de classes.

Il nous faut d'abord définir le symbole $\left(\frac{K}{\mathfrak{a}}\right)$ pour un idéal non premier. Pour cela, supposant $\mathfrak{a}$ premier au discriminant relatif de K par rapport à k, nous décomposerons $\mathfrak{a}$ en facteurs premiers : $\mathfrak{a} = \prod_i \mathfrak{p}_i^{a_i}$ et nous poserons

$$\left(\frac{K}{\mathfrak{a}}\right) = \prod_i \left(\frac{K}{\mathfrak{p}_i}\right)^{a_i}.$$

Il en résulte

$$\left(\frac{K}{\mathfrak{ab}}\right) = \left(\frac{K}{\mathfrak{a}}\right)\left(\frac{K}{\mathfrak{b}}\right).$$

Donc les idéaux $\mathfrak{a}$ tels que $\left(\frac{K}{\mathfrak{a}}\right) = 1$ forment un groupe. C'est ce groupe que nous appellerons *Groupe de Artin* associé à K dans k.

Nous montrerons que le groupe de Artin satisfait aux conditions des théorèmes A), B), ce qui démontrera son identité avec le groupe défini au théorème B, que nous appellerons désormais *Groupe de Takagi*, et par suite la loi générale de réciprocité, car pour un idéal $\mathfrak{a}$ quelconque, il est évident que $\left(\frac{K}{\mathfrak{a}}\right)$ ne dépend que de la classe à laquelle appartient $\mathfrak{a}$ suivant le groupe de Artin.

Remarquons encore qu'en vertu des propriétés du symbole de Frobenius, il est clair que le groupe de Artin satisfait à la condition 1) du théorème A. D'autre part, $\mathfrak{K}$ étant une classe de A (mod. *H*) la

correspondance $\mathfrak{K} \to \sigma = \left(\frac{K}{\mathfrak{a}}\right)$, $\mathfrak{a}$ étant un idéal de la classe $\mathfrak{K}$, définit un isomorphisme de A/H avec un sous-groupe du groupe de Galois, formé de toutes les substitutions σ telles qu'il existe un idéal $\mathfrak{a}$ pour lequel $\left(\frac{K}{\mathfrak{a}}\right) = \sigma$. Si donc nous montrons que pour toute opération σ il y a un tel idéal $\mathfrak{a}$, le théorème A sera démontré.

Remarquons encore que, $\mathfrak{m}$ désignant un multiple quelconque du discriminant relatif de K, $A_{\mathfrak{m}}$ le groupe des idéaux de k premiers à $\mathfrak{m}$, $H_{\mathfrak{m}} = [A_{\mathfrak{m}}, H]$, le groupe $A_{\mathfrak{m}}/H_{\mathfrak{m}}$ est encore isomorphe à un sous-groupe du groupe de Galois relatif de K.

Propriétés du groupe de Artin.

On peut étendre au symbole $\left(\frac{K}{\mathfrak{a}}\right)$ les propriétés de la substitution de Frobenius. Soient K, K' deux sur-corps relativement abéliens de k, et soit $\mathfrak{a}$ un idéal de k premier aux discriminants relatifs de ces deux corps.

1) Si $k \subset K' \subset K$, on a

$$\left(\frac{K}{\mathfrak{a}}\right) \to \left(\frac{K'}{\mathfrak{a}}\right).$$

2) Le groupe de Galois de KK' étant considéré comme sous-groupe du produit direct des groupes de Galois de K, K', on a

$$\left(\frac{KK'}{\mathfrak{a}}\right) = \left(\frac{K}{\mathfrak{a}}\right)\left(\frac{K'}{\mathfrak{a}}\right).$$

Il suffit, pour démontrer ces propriétés, de décomposer $\mathfrak{a}$ en facteurs premiers et d'appliquer les propriétés correspondantes de la substitution de Frobenius. Il en résulte que :

1) Si $K' \subset K$, le groupe de Artin associé à K' contient le groupe de Artin associé à K.

2) Le groupe de Artin associé à KK' est la partie commune aux groupes de Artin associés à K, K'.

Soit k' une extension finie quelconque de k. Soient $\mathfrak{p}$ un idéal premier de k non ramifié dans K, $\mathfrak{q}$ un facteur premier de degré relatif f de $\mathfrak{p}$ dans k'. On a vu (p. 387) que

$$\left(\frac{K/k}{\mathfrak{p}}\right)^f = \left(\frac{Kk'/k'}{\mathfrak{q}}\right).$$

Nous pouvons maintenant écrire cette formule sous la forme

$$\left(\frac{Kk'/k'}{\mathfrak{q}}\right) = \left(\frac{K/k}{N_{k'k}(\mathfrak{q})}\right),$$

qui se prête immédiatement à la généralisation : si $\mathfrak{A}$ est un idéal de k' tel que $N_{k'k}(\mathfrak{A})$ soit premier au discriminant relatif de K, on a

$$\left(\frac{Kk'}{\mathfrak{A}}\right) = \left(\frac{K}{N_{Kk}(\mathfrak{A})}\right).$$

D'où résulte que : *les idéaux premiers au discriminant relatif de K par rapport à k du groupe de Artin associé à Kk' dans k' sont ceux dont la norme par rapport à k est dans le groupe de Artin associé à K dans k.*

Démonstration du théorème A.

Soit K un sur-corps relativement abélien de k, et soit G le groupe de Galois de K par rapport à k. On a vu que, pour démontrer le théorème A, il suffit de prouver que pour toute opération σ de G il existe un idéal $\mathfrak{a}$ de k tel que $\left(\frac{K}{\mathfrak{a}}\right) = \sigma$. Or il suffit de le prouver dans le cas où l'ordre de σ est la puissance d'un nombre premier : car, nous avons vu que toute opération σ d'un groupe abélien se laisse décomposer en produit d'opérations σ_i dont les ordres sont des puissances de nombres premiers. Si $\left(\frac{K}{\mathfrak{a}_i}\right) = \sigma_i$, on a $\left(\frac{K}{\Pi\mathfrak{a}_i}\right) = \sigma$. Supposons donc que l'ordre de σ soit une puissance de nombre premier, p^α, et soit k' le sous-corps de K appartenant au groupe engendré par σ. Donc, K est par rapport à k' un sur-corps relativement cyclique dont le degré est la puissance d'un nombre premier. Or nous montrerons plus loin[24] que dans ce cas, étant donné un idéal quelconque, il y a un idéal premier, ne le divisant pas, qui reste premier dans K. Soit $\mathfrak{q}$ un tel idéal, que nous supposerons premier au discriminant relatif de K par rapport à k. Donc $\left(\frac{K/k'}{\mathfrak{q}}\right)$ engendre le groupe de K par rapport à k' et par suite $\sigma = \left(\frac{K/k'}{\mathfrak{q}}\right)^x$. Donc

$$\sigma = \left(\frac{K/k}{N_{k'k}(\mathfrak{q}^x)}\right)$$

en vertu de la troisième propriété du symbole $\left(\frac{K}{\mathfrak{a}}\right)$ donnée au paragraphe précédent, ce qui démontre le théorème.

---

24) Voir p. 442.

Conséquences.

On remarquera qu'il résulte de la démonstration précédente que pour chaque opération σ du groupe de Galois, il existe un idéal $\mathfrak{a}$ premier à un idéal donné $\mathfrak{m}$ à l'avance quelconque et tel que $\left(\frac{K}{\mathfrak{a}}\right) = \sigma$. Il suffit de choisir les idéaux $\mathfrak{a}_i$ premiers à l'idéal donné. Il en résulte que, $\mathfrak{m}$ désignant un multiple quelconque du discriminant relatif de K, $A_\mathfrak{m}$ le groupe des idéaux de k premiers à $\mathfrak{m}$, $H_\mathfrak{m}$ le groupe des idéaux de H premiers à $\mathfrak{m}$, le groupe $A_\mathfrak{m}/H_\mathfrak{m}$ est isomorphe au groupe de Galois de K par rapport à k.

Soient K, K' deux sur-corps relativement abéliens de k, et H, H' les groupes de Artin associés à ces deux corps. Supposons $H \subset H'$. Il en résulte $[H, H'] = H$. Soit $\mathfrak{d}$ le discriminant relatif de KK'. Les groupes $A_\mathfrak{d}/[H, H']_\mathfrak{d}$ et $A_\mathfrak{d}/H_\mathfrak{d}$ sont respectivement isomorphes aux groupes de Galois relatifs des corps KK' et K. Il faut donc que $KK' \subset K$, c'est-à-dire que $K' \subset K$. Nous avons déja montré p. 426 que, réciproquement, la condition $K' \subset K$ entraîne $H' \supset H$. Donc :

K et K' étant deux sur-corps relativement abéliens de k, H et H' les groupes de Artin associés dans k à ces corps, les conditions $H \subset H'$ et $K' \subset K$ sont équivalentes.

Nous dirons que plusieurs sur-corps de k, $K_1, K_2, \cdots, K_r$ sont *étrangers* les uns aux autres par rapport à k quand le degré relatif de leur corps composé est égal au produit des degrés relatifs des composants. Si $r = 2$, et si l'un des corps est galoisien par rapport à k, la condition est équivalente à la condition $[K_1, K_2] = k$.

Les K_i étant des corps étrangers par rapport à k ($i = 1, 2, \cdots, r$), et relativement abéliens, soit H_i le groupe de Artin associé à K_i. L'indice dans le groupe des idéaux de k premiers au discriminant relatif de $K_1 K_2 \cdots K_r$ de $[H_1, H_2, \cdots, H_r]$ est égal au produit des indices des groupes H_i' des idéaux des H_i premiers à ce discriminant relatif. Il en résulte que si on prend pour chaque i une classe $\mathfrak{R}_i$ (mod. H_i), la partie commune à toutes ces classes est un ensemble qui n'est pas vide, et qui contient même des idéaux premiers à un idéal donné quelconque.

Chapitre VII.

Les corps circulaires.

Dans ce chapitre, k désignera encore un corps de nombres algébriques fini quelconque.

On appelle *corps circulaire* par rapport à k un sur-corps $k(\zeta)$ de k engendré par adjonction d'une racine de l'unité.

Soit R le corps des nombres rationnels, et supposons que ζ soit une racine m-ème de l'unité. Le groupe de Galois de $k(\zeta)$ par rapport à k est un sous-groupe du groupe de Galois de $R(\zeta)$ par rapport à R. Donc:

$k(\zeta)$ est un sur-corps relativement abélien de k; son degré relatif divise $\varphi(m)$[25]*; si $m = q^n$ est une puissance d'un nombre premier $q \neq 2$, ce corps est relativement cyclique par rapport à k.*

Constitution du groupe de Artin.

$k(\zeta)$ étant un sur-corps circulaire de k engendré par adjonction d'une racine primitive m-ème de l'unité, le discriminant relatif de $k(\zeta)$ ne contient que des facteurs premiers de m. En effet, il en est ainsi du discriminant de l'équation $x^m - 1 = 0$.

Nous allons chercher quels sont les idéaux premiers à m qui appartiennent au groupe de Artin. A cet effet, considérons d'abord un idéal premier $\mathfrak{p}$ de k ne divisant pas m. Soit $\left(\frac{k(\zeta)}{\mathfrak{p}}\right) = \sigma$. On a

$$\sigma\zeta \equiv \zeta^{N(\mathfrak{p})} \pmod{\mathfrak{p}}.$$

Mais $\sigma\zeta$, comme conjugué de ζ, est une puissance ζ^a de ζ. D'où

$$\zeta^a(1-\zeta^{N(\mathfrak{p})-a}) \equiv 0 \pmod{\mathfrak{p}}.$$

ζ^a étant une unité, est premier à $\mathfrak{p}$. Donc le second facteur est divisible par $\mathfrak{p}$. Or, si ce facteur est $\neq 0$, il divise $\prod_{i=1}^{m-1}(1-\zeta^i)$, produit qui est égal à $\left(\frac{x^m-1}{x-1}\right)_{x=0} = m$, donc non divisible par $\mathfrak{p}$. Donc le second facteur est nul, et on a

$$\sigma\zeta = \zeta^{N(\mathfrak{p})}$$

---

25) Rappelons que $\varphi(m)$ est la fonction d'Euler donnant le nombre des entiers positifs $< m$ et premiers à m. Que le degré de $R(\zeta)$ par rapport à R divise $\varphi(m)$ est facile à voir, car tout conjugué de ζ est de la forme ζ^a, $(a, m) = 1$.

Cette équation détermine d'ailleurs σ. Il en résulte, pour un idéal $\mathfrak{a}$ entier premier à m, que

$$\left(\frac{K}{\mathfrak{a}}\right)\zeta = \zeta^{N(\mathfrak{a})}.$$

L'idéal n'appartiendra au groupe de Artin que si $\zeta^{N(\mathfrak{a})} = \zeta$, ce qui exige que

$$N(\mathfrak{a}) \equiv 1 \pmod{m}. \tag{1}$$

Si $\mathfrak{a}$ n'est pas entier, soit $\mathfrak{a} = \mathfrak{a}'\,\mathfrak{a}''^{-1}$, $\mathfrak{a}'$, $\mathfrak{a}''$ entiers et premiers à m. La condition nécessaire et suffisante pour que $\mathfrak{a}$ appartienne au groupe de Artin est que $\left(\frac{K}{\mathfrak{a}'}\right) = \left(\frac{K}{\mathfrak{a}''}\right)$, d'où $N(\mathfrak{a}') \equiv N(\mathfrak{a}'') \pmod{m}$, et $N(\mathfrak{a}) \equiv 1 \pmod{m}$.

Donc les idéaux premiers à m du groupe de Artin sont ceux qui satisfont à la condition (1).

Corps absolument circulaires.

R désignant le corps des nombres rationnels, soit ζ une racine primitive m-ème. de l'unité. Les idéaux premiers à m contenus dans le groupe de Artin associés à $R(\zeta)$ dans R sont les idéaux (a) tels que $|a| \equiv 1 \pmod{m}$[26], ce qui permet de retrouver immédiatement la loi de décomposition des nombres premiers dans $R(\zeta)$. Ce groupe de Artin est d'indice $\varphi(m)$ dans le groupe des idéaux de R premiers à m. Donc $R(\zeta)$ est de degré au moins égal à $\varphi(m)$. D'autre part un automorphisme σ de ce corps change ζ en ζ^a avec $(a, m) = 1$. Donc le nombre de ces automorphismes est au plus $\varphi(m)$, ce qui montre que $R(\zeta)$ est de degré $\varphi(m)$ (ce qui fournit une démonstration de l'irréductibilité des équations de division du cercle). Soit $\Phi_m(x) = 0$ l'équation irréductible à laquelle satisfait ζ. On a

$$\Phi_m(x) = \prod_a (x - \zeta^a), \quad (a, m) = 1, \quad 1 \leq a < m.$$

Comme $x^m - 1 = \prod_a (x - \zeta^a)$, $0 \leq a < m$, on a

$$x^m - 1 = \prod_d \Phi_d(x), \tag{1}$$

d parcourant les diviseurs de m. D'ailleurs cette formule détermine de proche en proche tous les $\Phi_d(x)$ d'une manière univoque.

---

26) Soit p_∞ l'idéal premier infini de R. Le groupe de Artin associé à $R(\zeta)$ dans R donne un exemple de groupe de congruence définissable modulo mp_∞, mais en général pas modulo m.

Introduisons la fonction $\mu(x)$ de Möbius : x étant un entier, on a $\mu(x) = 0$ si x est divisible par le carré d'un nombre premier, $\mu(x) = (-1)^\lambda$ si x est produit de λ nombres premiers distincts, $\mu(1) = 1$. Montrons que

$$\Phi_m(x) = \prod_d (x^d - 1)^{\mu\left(\frac{m}{d}\right)}, \quad d : \text{diviseur de } m.$$

Il suffit de montrer que ce polynome satisfait à l'équation (1). Pour cela formons

$$\prod_d \prod_{d'} (x^{d'} - 1)^{\mu\left(\frac{d}{d'}\right)}, \quad d \text{ diviseur de } m, \quad d' \text{ diviseur de } d.$$

Chaque facteur $x^{d'} - 1$ intervient avec l'exposant $\sum_d \mu\left(\frac{d}{d'}\right)$, d parcourant les multiples de d' qui sont diviseurs de m ; cet exposant est égal à $\sum_x \mu(x)$, x parcourant les diviseurs de $\frac{m}{d'}$. On vérifie tout de suite que cette somme vaut 0 sauf si $\frac{m}{d'} = 1$, auquel cas elle vaut 1. Donc le facteur $x^m - 1$ reste seul. En particulier si q est un nombre premier,

$$\Phi_{q^\nu}(x) = 1 + x^{q^{\nu-1}} + x^{2q^{\nu-1}} + \cdots + x^{(q-1)q^{\nu-1}}$$

Considérons dans ce cas le nombre $1 - \zeta$. Soit σ un automorphisme du groupe de Galois changeant ζ en $\zeta^{a'}$, et soit a un entier tel que $aa' \equiv 1 \pmod{q^\nu}$. Les nombres $\frac{1-\zeta^a}{1-\zeta}$ et $\frac{1-\zeta}{1-\zeta^a} = \frac{1-(\zeta^a)^{a'}}{1-(\zeta^a)}$ sont des entiers, donc des unités. Donc $(1-\zeta)$ représente un idéal invariant par les opérations σ. D'autre part $N(1-\zeta) = \Phi_{q^\nu}(1) = q$, donc l'idéal $(1-\zeta) = \mathfrak{q}$ est premier du premier degré et on a $(q) = \mathfrak{q}^{\varphi(q^\nu)}$.

Remarquons enfin que le groupe de Galois de $R(\zeta)$, où ζ est une racine primitive m-ème. de l'unité, est isomorphe au groupe A/H, A désignant le groupe des nombres rationnels positifs premiers à m, H le sous-groupe de A formé des nombres $\equiv 1 \pmod{m}$. Si m est de la forme q^α, q premier, ce groupe est cyclique, sauf si $q = 2$, $\alpha > 2$, auquel cas il est produit direct d'un groupe d'ordre 2 et d'un groupe cyclique d'ordre $2^{\alpha-2}$.

Application. Loi quadratique de réciprocité.

Considérons un nombre premier p positif et $\equiv 1 \pmod 4$. Le corps $R(\sqrt{p})$ est contenu dans le corps des racines p-èmes. de l'unité. En effet, le corps des racines p-èmes. de l'unité, qui est cyclique de degré

$p-1$ contient un sous-corps quadratique, dont le discriminant ne peut être divisible que par p, donc qui est $R(\sqrt{p})$. Soit q un nombre premier quelconque $\neq p$; pour que q se décompose totalement dans $R(\sqrt{p})$, il faut et suffit que le corps de décomposition de q dans le corps Z des racines p-èmes. de l'unité contienne $R(\sqrt{p})$, donc que $\left(\frac{Z}{q}\right)$ soit dans le sous-groupe du groupe de Galois de Z auquel appartient $R(\sqrt{p})$. Ce sous-groupe est le groupe formé des carrés des opérations du groupe. Les nombres q répondant à la question sont donc ceux tels que

$$\left(\frac{Z}{q}\right) = \sigma^2, \quad \left(\frac{Z}{x}\right) = \sigma,$$

donc

$$q \equiv x^2 \pmod{p}.$$

Mais l'étude élémentaire de la théorie du corps quadratique montre aussi que la condition nécessaire et suffisante cherchée est que la congruence $p \equiv x^2 \pmod{q}$ soit résoluble. Ces deux conditions sont donc équivalentes, et par suite :

p et q étant deux nombres premiers positifs dont l'un est $\equiv 1 \pmod{4}$, si p est reste quadratique de q, q est reste quadratique de p.

Nous avons obtenu la loi de réciprocité en comparant la loi de décomposition fournie par la théorie du corps de classes avec la loi de décomposition qu'on obtient de manière élémentaire. Cette méthode est générale et conduit dans les cas plus généraux aus lois de réciprocité généralisées.

Un théorème d'existence.

Nous aurons besoin du théorème d'arithmétique élémentaire suivant :

Soient p, n deux nombres positifs, $p > 1$, $n > 2$. Il existe un nombre premier q divisant $p^n - 1$, mais non $p^{n'} - 1$ pour $n' < n$, sauf si $p = 2$, $n = 6$[27].

Remarquons d'adord que si q divise $p^n - 1$ et $p^{n'} - 1$ il divise aussi $(p^n - 1) - p^{n-n'}(p^{n'} - 1) = p^{n-n'} - 1$: Donc, par application de l'algorithme d'Euclide, il divise $p^d - 1$, où $d = (n, n')$. Il nous suffira donc de prouver qu'il y a un nombre premier q tel que q divise $p^n - 1$ mais

27) On trouvera une autre démonstration de ce théorème dans: "Birkhoff et Vandiver, On the integral divisors of $a^n - b^n$," Annals of Mathematics, 1902-3.

aucun des nombres p^d-1, d étant un diviseur de n différent de n. Soit ζ une racine primitive n-ième de l'unité. Ecrivons

$$p^n-1=(p-1)(p-\zeta)(p-\zeta^2)\cdots(p-\zeta^{n-1}).$$

Si nous pouvons prouver qu'il existe un idéal premier $\mathfrak{q}$ divisant $p-\zeta$, mais ne divisant aucun des nombres $p-\zeta^a$ où $(a, n)>1$, nous aurons démontré le lemme, car le nombre premier q divisible par $\mathfrak{q}$ répondra à la question. Or, soit $\mathfrak{q}$ un idéal premier divisant $p-\zeta$ et $p-\zeta^a$.

Ecrivons :

$$(1)\qquad p-\zeta-(p-\zeta^a)=\zeta(\zeta^{a-1}-1),$$

$\mathfrak{q}$ doit donc diviser $\zeta^{a-1}-1$. Ce n'est possible que si $\frac{n}{(a-1, n)}$ est puissance d'un nombre premier. En effet, si u divise v, ζ^u-1 divise ζ^v-1. Donc si t^α est un diviseur de $\frac{n}{(n, a-1)}$, $\zeta^{a-1}-1$ divise $\zeta^{\frac{n}{t^\alpha}}-1$ qui divise t. Donc si $\frac{n}{(n, a-1)}$ a plusieurs facteurs premiers distincts, $\zeta^{a-1}-1$ est une unité.

Donc $\frac{n}{(n, a-1)}$ n'a qu'un facteur premier q qui ne peut être que le nombre premier contenu dans $\mathfrak{q}$, et q divise n : $n=q^\alpha n'$, $(n', q)=1$. Soit K le corps $R(\zeta)$, R étant le corps des rationnels, et soit K' le corps $R(\zeta^{q^\alpha})$. G désignant le groupe de Galois de $R(\zeta)$, K' appartient au groupe des substitutions σ de G telles que

$$\sigma\zeta=\zeta^u,\qquad u\equiv 1\left(\mathrm{mod.}\ \frac{n}{q^\alpha}\right).$$

Soit G_Z le groupe de décomposition de q dans K, et soit σ une opération de G_Z changeant ζ en ζ^u, donc $p-\zeta$ en $p-\zeta^u$. Il en résulte que $p-\zeta^u$ sera divisible par $\mathfrak{q}$, donc que $\frac{n}{(n, u-1)}$ est une puissance de q. Donc $u-1=\frac{n}{q^\beta}\lambda$, $\beta\leq\alpha$ et $u\equiv 1\left(\mathrm{mod.}\ \frac{n}{q^\alpha}\right)$. G_Z est contenu dans le groupe de K par rapport à K' et q se décompose dans K' en idéaux premiers du premier degré distincts. D'autre part K est de degré $\varphi(q^\alpha)$ par rapport à K' (il résulte de K' par adjonction des racines q^α-ièmes de l'unité et n est premier à q) et q doit être divisible par $\mathfrak{q}^{\varphi(q^\alpha)}$, car K contient le corps des racines q^α-ièmes de l'unité (voir p. 431). Par suite, K_T étant le corps d'inertie de q, on a $(K: K_T)\geq\varphi(q^\alpha)$. Mais $K_T\supset K_Z$ et K_Z contient K'. Comme $(K: K')=\varphi(q^\alpha)$, on a $K_T=K_Z=K'$. Donc $\mathfrak{q}$ est un idéal du premier degré, et q se décompose dans K' en

idéaux distincts du premier degré. Donc, en vertu de la loi de décomposition dans K', $q \equiv 1 \pmod{n'}$. Donc ζq^{a-1} est une racine q^a-ième de l'unité, et $\zeta q^{a-1} - 1$ est divisible par $\mathfrak{q}$. En vertu de (1), $p - \zeta q^a$ est aussi divisible par $\mathfrak{q}$.

Si $q \neq 2$ le groupe G_Z est cyclique. Il comporte un automorphisme σ changeant ζ en ζ^a avec $a \equiv 1 \left(\text{mod. } \frac{n}{q^a}\right)$, mais $\not\equiv 1 \left(\text{mod. } \frac{n}{q^{a-1}}\right)$; ζ^{a-1} est donc une racine primitive q^a-ième de l'unité. Il en résulte que $(1 - \zeta^{a-1})$ n'est divisible que par la première puissance de $\mathfrak{q}$ et en vertu de la formule (1) il en est de même de $p - \zeta$. Si $q = 2$, n est pair, K' est le corps des racines n'-ièmes de l'unité, n' étant impair, et 2 doit se décomposer totalement: D'où $2 \equiv 1 \pmod{n'}$, ce qui est impossible si $n' \neq 1$. Donc $n = 2^\alpha$, et $\alpha \geq 1$ puisque $n > 2$, et G_Z est identique au groupe de K. Il comporte une opération σ changeant ζ en ζ^{-1}. Or $\zeta^2 - 1$ est divisible exactement par $\mathfrak{q}^2$, donc $p - \zeta$ n'est pas divisible par une puissance de $\mathfrak{q}$ supérieure à 2.

Enfin, si $\mathfrak{q}'$ est un facteur premier de q différent de $\mathfrak{q}$, soit $\mathfrak{q}' = \sigma^{-1}\mathfrak{q}$. Donc σ n'appartient pas à G_Z. Si $\sigma\zeta = \zeta^a$, $\zeta^{a-1} - 1$ n'est pas divisible par $\mathfrak{q}$. Or si $p - \zeta$ était divisible par $\mathfrak{q}'$, $\sigma(p - \zeta) = p - \zeta^a$ serait divisible par $\mathfrak{q}$, donc aussi $\zeta^{a-1} - 1$, ce qui n'est pas.

Donc: si $p - \zeta$ a avec un nombre $p - \zeta^a$ un facteur premier $\mathfrak{q}$ commun, $p - \zeta$ n'est dvisible par aucun des conjugués de $\mathfrak{q}$; la contribution de $\mathfrak{q}$ à $p - \zeta$ est $\mathfrak{q}$ si q est impair, au plus $\mathfrak{q}^2$ si $q = 2$, le nombre q est nécessairement le plus grand facteur premier de n $\left(\text{comme il résulte de } q \equiv 1 \left(\text{mod. } \frac{n}{q^a}\right), \text{ qui donne } q > \frac{n}{q^a}\right)$; enfin l'idéal $\mathfrak{q}$ est du premier degré.

Si donc $p - \zeta$ n'avait que des facteurs premiers de cette espèce, $(p - \zeta)$ devrait se réduire à un idéal premier $\mathfrak{q}$, ou, si $n = 2^\alpha$, au carré d'un idéal premier. Désignons par $F(m)$ la norme de $p - \theta$, θ étant une racine primitive m-ème. de l'unité, la norme étant prise de $R(\theta)$ à R. Supposons d'abord que $n \neq q^a$. Alors on devrait avoir $F(n) = q$, $F(n') \equiv 0 \pmod{q}$, car $\mathfrak{q}$ divise $p - \zeta^q$. Or $F(n)$ se laisse calculer. Si $\Phi_n(x) = 0$ est l'équation irréductible à laquelle satisfait ζ, on a $F(n) = \Phi_n(p)$ et

$$\Phi_n(x) = \prod_d (x^d - 1)^{\mu\left(\frac{n}{d}\right)}, \quad d: \text{ diviseur de } n,$$

$\mu(x)$ désignant la fonction de Möbius. D'où

$$\Phi_n(p) = \prod_d (p^d - 1)^{\mu\left(\frac{n}{d}\right)}$$

Remplaçons les facteurs p^d-1 pour lesquels $\mu\left(\frac{n}{d}\right)<0$ par p^d, les facteurs p^d-1 pour lesquels $\mu\left(\frac{n}{d}\right)>0$ par p^{d-1}. Remarquant que le degré de $\Phi_n(x)$ est $\varphi(n)$, et que la somme des $\mu\left(\frac{n}{d}\right)$ pour lesquels $\mu\left(\frac{n}{d}\right)>0$ est 2^{m-1}, m désignant le nombre des facteurs premiers de n, il vient

$$F(n) > p^{\varphi(n)-2^{m-1}}$$

De même

$$F(n') < p^{\varphi(n')+2^{m-2}}$$

D'où

$$\frac{F(n)}{q} \geq \frac{F(n)}{F(n')} > p^{\varphi(n)-\varphi(n')-3\cdot 2^{m-2}}$$

Or $\varphi(n)-\varphi(n') = \varphi(n')\,(q^{\alpha-1}(q-1)-1)$ et $\varphi(n') = \prod_t t^{\alpha-1}(t-1)$. Si $t \neq 2$, le facteur correspondant de ce produit est ≥ 2. Comme n' a $m-1$ facteurs premiers, on a $\varphi(n') \geq 2^{m-2}$. D'autre part si $q>3$, ou si $q=3$, $\alpha>1$ on a $q^{\alpha-1}(q-1)\geq 3$, et par suite $F(n)>q$. Reste le cas $q=3$, d'où $n'=2$, $n=6$. On a $F(n)=p^2-p+1$, nombre qui est >3 si $p>2$; si $p=2$, on trouve le cas d'exception annoncé. Si $n=q^\alpha$, on a $F(n)=p^{q^{\alpha-1}(q-1)}+\ldots+p^{q^{\alpha-1}}+1$, nombre qui est $>q$, si $q\neq 2$ et >4, si $q=2$, $\alpha>1$. Notre proposition est donc complètement démontrée.

Examinons encore le cas $n=2$: on a $p^2-1=(p-1)(p+1)$. Un facteur premier de $p-1$ ne divise $p+1$ que s'il est égal à 2; la proposition sera donc encore vraie dans ce cas sauf si p est de la forme 2^x-1.

En tous cas, nous pouvons dire que:

Etant donnés des entiers n, p quelconques, $p>1$, il existe une infinité de nombres premiers q tels que le plus petit exposant f pour lequel $p^f \equiv 1$ (mod. q) soit divisible par n.

Soit k un corps de nombres algébriques fini quelconque, et soit $\mathfrak{a}$ un idéal entier de k. n étant un entier quelconque >1, on peut trouver une infinité de nombres premiers q tels que le plus petit exposant positif f pour lequel $N(\mathfrak{a})^f \equiv 1$ (mod. q) soit divisible par n. Donc:

Etant donné un corps k et dans ce corps un idéal entier $\mathfrak{a}$, on peut trouver une infinité de nombres premiers q tels que, H désignant le groupe de

Artin associé dans k au corps $k(\zeta)$, où ζ est une racine primitive q-ème. de l'unité, $\mathfrak{a}$ appartienne (mod. H) *à une classe dont l'ordre est un multiple de n.*

En particulier, si K' est un sur-corps donné fini de k, on peut supposer que K' et $k(\zeta)$ sont étrangers par rapport à k.

Les corps circulaires sont corps de classes.

Soit K un sur-corps relativement abélien de k. Soit A le groupe des idéaux de k premiers à un idéal $\mathfrak{m}$ divisible par le discriminant relatif de K, et soit H un sous-groupe d'indice fini jouissant, pour les idéaux premiers à $\mathfrak{m}$, de la propriété 1) énoncée au théorème A. Le groupe A/H est un groupe abélien fini. Si χ est un caractère de ce groupe, nous désignerons par $\chi(\mathfrak{a})$ le caractère de la classe à laquelle appartient $\mathfrak{a}$ (mod. H) et nous appellerons séries L associées à H les séries

$$L(s, \chi) = \sum_{\mathfrak{a}} \frac{\chi(\mathfrak{a})}{N(\mathfrak{a})^s},$$

$\mathfrak{a}$ parcourant les idéaux entiers de k premiers à $\mathfrak{m}$. Ces séries sont convergentes pour $s > 1$, et on a la formule analogue à la formule d'Euler

$$L(s, \chi) = \prod_{\mathfrak{p}} \left(1 - \frac{\chi(\mathfrak{p})}{(N\mathfrak{p})^s}\right)^{-1}$$

où $\mathfrak{p}$ parcourt les idéaux premiers ne divisant pas $\mathfrak{m}$. D'où

$$\log L(s, \chi) = \sum_{\mathfrak{p}} \sum_{\nu=1}^{\infty} \frac{\chi(\mathfrak{p}^\nu)}{\nu N(\mathfrak{p})^{\nu s}}.$$

Nous allons former $\sum_{\chi} \log L(s, \chi)$, la somme étant étendue aux divers caractères χ. Des formules données pour les caractères, il résulte

$$\sum_{\chi} \chi(\mathfrak{a}) = 0, \qquad \text{si } \mathfrak{a} \text{ n'est pas dans } H;$$

$$\sum_{\chi} \chi(\mathfrak{a}) = (A : H) = h, \qquad \text{si } \mathfrak{a} \text{ est dans } H.$$

Donc

$$\log \prod_{\chi} L(s, \chi) = \sum_{\mathfrak{p}^\nu \subset H} \frac{h}{\nu N(\mathfrak{p}^\nu)^s}$$

Mais, par hypothèse, la condition $\mathfrak{p}^\nu \subset H$ est équivalente à la suivante : ν est multiple du degré relatif f par rapport à k des facteurs premiers $\mathfrak{P}$ de $\mathfrak{p}$ dans K. Soit $\nu = \mu f$. On a $N(\mathfrak{p})^{\nu s} = N(\mathfrak{P})^{\mu s}$ et le nombre g des

diviseurs premiers de $\mathfrak{p}$ dans K est $\frac{n}{f}$, si $n = (K:k)$. Donc $\frac{1}{\nu} = \frac{1}{\mu}\frac{g}{n}$ et

$$\log \prod_{\chi} L(s,\chi) = \frac{h}{n} \sum_{\mu,\mathfrak{P}} \frac{1}{\mu N(\mathfrak{P})^{\mu s}} = \frac{h}{n} \log \prod_{\mathfrak{P}} \left(1 - \frac{1}{N(\mathfrak{P})^s}\right)^{-1},$$

où $\mathfrak{P}$ parcourt les idéaux premiers de K premiers à $\mathfrak{m}$. Désignons par $\varphi(s)$ le produit $\prod \left(1 - \frac{1}{N(\mathfrak{P})^s}\right)$ étendu aux idéaux premiers en nombre fini divisant $\mathfrak{m}$, et remarquons que la fonction $\zeta_K(s)$ du sur-corps, égale par définition à

$$\sum \frac{1}{N(\mathfrak{A})^s},$$

où $\mathfrak{A}$ parcourt les idéaux entiers de K, est égale à $\prod \left(1 - \frac{1}{N(\mathfrak{P})^s}\right)^{-1}$, le produit étant étandu à tous les idéaux premiers de K. Il vient

$$\prod_{\chi} L(s,\chi) = (\varphi(s)\zeta_K(s))^{\frac{h}{n}}. \tag{1}$$

Supposons maintenant que H soit un groupe de congruence (mod. $\mathfrak{m}$). Désignons par $\mathfrak{K}$ les différentes classes de A (mod. H), et posons

$$Q_{\mathfrak{K}}(s) = \sum_{\mathfrak{a} \subset \mathfrak{K}} \frac{1}{N(\mathfrak{a})^s}.$$

On démontre[28] que les idéaux $\mathfrak{a}$ se repartissent également dans toutes les classes $\mathfrak{K}$, dans ce sens que les limites $\frac{1}{s-1} Q_{\mathfrak{K}}(s)$ $(s \to 1)$ sont toutes égales à une même constante c, et que

$$Q_{\mathfrak{K}}(s) = \frac{c}{s-1} + q_{\mathfrak{K}}(s),$$

$q_{\mathfrak{K}}(s)$ restant bornée pour $s = 1$. Or on a

$$L(s,\chi) = \sum \chi(\mathfrak{K})\, Q_{\mathfrak{K}}(s) = \frac{c}{s-1} \sum_{\mathfrak{K}} \chi(\mathfrak{K}) + l(s,\chi),$$

$l(s,\chi)$ restant bornée pour $s = 1$. Si donc χ est différent du caractère χ_0 toujours égal à 1, $L(s,\chi)$ reste elle-même bornée pour $s = 1$. Si $\chi = \chi_0$, cette fonction a un pôle d'ordre 1. Donc le premier membre de la formule (1) a un pôle d'ordre 1 pour $s = 1$; $\zeta_K(s)$ ayant aussi un pôle d'ordre 1 pour $s = 1$, il faut que $\frac{h}{n} = 1$.

---

28) Voir Weber, Lehrbuch der Algebra, 2-me. édition, vol. III.

Or, considérons le cas où K est corps circulaire par rapport à k, engendré par adjonction d'une racine m-ème de l'unité. Le groupe de Artin H est un groupe de congruence définissable modulo $m\Pi\mathfrak{p}_\infty$, les $\mathfrak{p}_\infty$ étant les idéaux premiers infinis de k. Soit $\mathfrak{m}$ un module multiple du précédent, et soit H^* le groupe de Takagi associé à K (mod. $\mathfrak{m}$). La norme $\mathfrak{a}$ par rapport à k d'un idéal $\mathfrak{A}$ de K premier à $\mathfrak{m}$ est dans le groupe H, et H contient le rayon (mod. $\mathfrak{m}$). Donc H^* est contenu dans H. Si $\mathfrak{p}$ est un idéal premier premier à $\mathfrak{m}$ et si $\mathfrak{p}'$ est la plus petite puissance de $\mathfrak{p}$ contenue dans H, $\mathfrak{p}'$ est norme d'un idéal premier de K et $\mathfrak{p}'$ est contenu dans H^*. Comme $H^* \subset H$, $\mathfrak{p}'$ est la plus petite puissance de $\mathfrak{p}$ contenue dans H^*. Donc H^* satisfait à la condition 1) du Théorème A. Comme c'est un groupe de congruence, son indice h est égal à $(K:k)$. Or H^* est contenu dans le groupe des idéaux de H premiers à $\mathfrak{m}$, qui est aussi d'indice $(K:k)$. Donc :

$\mathfrak{m}$ désignant un multiple quelconque de $m\Pi\mathfrak{p}_\infty$, le groupe de Takagi associé (mod. $\mathfrak{m}$) *au corps circulaire $k(\zeta)$ dans k, ζ étant une racine m-ème de l'unité, est composé des idéaux du groupe de Artin qui sont premiers à $\mathfrak{m}$. Autrement dit : $k(\zeta)$ est corps de classes pour ce groupe.*

Chapitre VIII.

Démonstration du théorème B.

Le groupe de Takagi associé à un sur-corps relativement cyclique[29].

Soient k un corps fini de nombres algébriques, K un sur-corps relativement cyclique de k de degré relatif n, dont le groupe de Galois est engendré par une opération σ. On désignera par $\mathfrak{m}$ un module quelconque de k et par:

A le groupe des idéaux premiers à $\mathfrak{m}$ de k,

$\bar{A}$ le groupe des idéaux premiers à $\mathfrak{m}$ de K,

$\bar{H}_0$ le groupe des idéaux principaux de K premiers à $\mathfrak{m}$,

H_1 le groupe des classes d'idéaux (mod. $\mathfrak{m}$) de k qui contiennent des normes relatives d'idéaux principaux de K; on posera $(A : H_1) = h_1$,

H le groupe de Takagi associé à K dans k,

$\bar{H}_1$ le groupe des idéaux de K premiers à $\mathfrak{m}$ dont la norme relative par rapport à k appartient à H_1; ce groupe s'appelle le *genre principal* de K,

$\bar{H}_1'$ le groupe des idéaux de K premiers à $\mathfrak{m}$ et équivalents à un idéal de la forme $\mathfrak{A}^{1-\sigma}$, $\mathfrak{A}$ premier à $\mathfrak{m}$,

$S_{\mathfrak{m}}$ le rayon de k (mod. $\mathfrak{m}$).

Nous allons maintenant calculer le nombre $(A : H_1) = h$.

Considérons le groupe $\bar{A}$ comme homomorphe au groupe $H/S_{\mathfrak{m}}$, la correspondance étant définie en associant à tout idéal $\mathfrak{A}$ de $\bar{A}$ la classe (mod. $\mathfrak{m}$) qui contient $N_{Kk}(\mathfrak{A})$. En vertu du principe d'isomorphie, on a

$$(\bar{A} : \bar{H}_1) = (H : H_1) = \frac{(A : H_1)}{(A : H)} = \frac{h_1}{h}.$$

Or $\bar{H}_1$ contient évidemment $\bar{H}_1'$. Donc

$$(\bar{A} : \bar{H}_1) = \frac{(\bar{A} : \bar{H}_1')}{(\bar{H}_1 : \bar{H}_1')}.$$

Désignons par C les classes (mod. 1) de K (c'est-à-dire les classes ordinaires d'idéaux). Remarquant que chacune de ces classes contient des idéaux premiers à $\mathfrak{m}$, on a

$$(\bar{A} : \bar{H}_1') = (C : C^{1-\sigma}),$$

29) Ce calcul est la généralisation directe au cas "cyclique de degré quelconque" du calcul correspondant de la théorie de Takagi.

où $C^{1-\sigma}$ désigne la classe qui contient les puissances $1-\sigma$ des idéaux de la classe C. Or la formule $C \to C^{1-\sigma}$ définit un homomorphisme du groupe C sur le groupe $C^{1-\sigma}$ et, dans cet homomorphisme, les classes qui donnent l'élément unité du groupe $C^{1-\sigma}$ sont les classes ambiges. Donc $(C : C^{1-\sigma})$ est égal au nombre a des classes ambiges.

Reste à calculer h_1. Pour cela désignons par ν les nombres de k qui sont congrus (mod. $\mathfrak{m}$) à la norme relative d'un nombre K premier à $\mathfrak{m}$, par α les nombres de k premiers à $\mathfrak{m}$. On a

$$(A : H_1) = (A : (\alpha))\,((\alpha) : (\nu)) = h_0((\alpha) : (\nu)),$$

h_0 étant le nombre des classes de k. On a, en désignant par ε les unités de k, qui sont des nombres α,

$$((\alpha) : (\nu)) = (\alpha : \nu\varepsilon) = \frac{(\alpha : \nu)}{(\nu\varepsilon : \nu)} = \frac{(\alpha : \nu)}{(\nu : [\nu, \varepsilon])}.$$

Soit $\mathfrak{m} = \prod_i \mathfrak{p}_i^{a_i}$, les $\mathfrak{p}_i$ étant des idéaux premiers finis où infinis, avec $a_i = 1$ si $\mathfrak{p}_i$ est infini. Désignons pour chaque i par ν_i les nombres congrus (mod. $\mathfrak{p}_i^{a_i}$) à la norme relative d'un nombre de K premier à $\mathfrak{p}_i$, cette dernière condition tombant si $\mathfrak{p}_i$ est infini, par α_i les nombres de k premiers à $\mathfrak{p}_i$. Je dis que $(\alpha : \nu)$ est le produit des $(\alpha_i : \nu_i)$. Soit $\mathfrak{R}$ une classe du groupe α (mod. ν). Les nombres de $\mathfrak{R}$ sont tous dans la même classe $\mathfrak{R}_i$ (mod. ν_i). Associons à $\mathfrak{R}$ l'élément $\mathfrak{R}_1 . \mathfrak{R}_2 \ldots . \mathfrak{R}_r$ du produit direct des α_i/ν_i. Au produit de deux classes est évidemment associé le produit des éléments correspondants du produit direct. A deux classes $\mathfrak{R}$ différentes sont associés des éléments différents du produit direct. En effet, il suffit de montrer que si un nombre α, donc premier à $\mathfrak{m}$, appartient à tous les groupes ν_i, il appartient au groupe ν. Par hypothèse,

$$\alpha \equiv N_{Kk}(A_i) \pmod{\mathfrak{p}_i^{a_i}}, \quad (A_i, \mathfrak{p}_i) = 1.$$

Or on peut trouver un nombre A_i' tel que

$$A_i' \equiv A_i \pmod{\mathfrak{p}_i^{a_i}}, \quad A_i' \equiv 1 \pmod{\mathfrak{p}_j^{a_j}} \text{ pour } j \neq i.$$

On a $\alpha \equiv N_{Kk}(A_1' A_2' \cdots A_r') \pmod{\mathfrak{m}}$ et le nombre $A_1' A_2' \cdots A_r'$ est premier à $\mathfrak{m}$. Enfin tout élément $\mathfrak{R}_1 \mathfrak{R}_2 \cdots \mathfrak{R}_r$ du produit direct est ainsi obtenu. En effet choisissons dans chaque classe $\mathfrak{R}_i$ un nombre α_i: on peut trouver un nombre α tel que

$$\alpha \equiv \alpha_i \pmod{\mathfrak{p}_i^{a_i}}.$$

La classe $\mathfrak{R}$ de α donne précisément $\mathfrak{R}_1 \mathfrak{R}_2 \cdots \mathfrak{R}_r$.

Donc $$(\alpha : \nu) = \prod_i (\alpha_i : \nu_i).$$

Tout revient donc à calculer les $(\alpha_i : \nu_i)$. Supposons d'abord $\mathfrak{p}_i$ fini. Soient $\mathfrak{P}_i$ un facteur premier de $\mathfrak{p}_i$ dans K, $k_{\mathfrak{p}_i}$ et $K_{\mathfrak{P}_i}$ respectivement les corps des nombres $\mathfrak{p}_i$-adiques et $\mathfrak{P}_i$-adiques de k, K. Choisissons pour chaque i le plus petit exposant b_i tel que tout nombre $\equiv 1 \pmod{\mathfrak{p}_i^{b_i}}$ soit norme relative par rapport à $k_{\mathfrak{p}_i}$ d'un nombre de $K_{\mathfrak{P}_i}$ (voir p. 423). Par définition, $\mathfrak{p}_i^{b_i}$ est appelé $\mathfrak{p}_i$-conducteur de K par rapport à k, et désigné par $\mathfrak{f}_{\mathfrak{p}_i}$. Nous supposerons que $\mathfrak{m}$ est divisible par les $\mathfrak{p}_i$-conducteurs de tous les idéaux premiers finis de k ramifiés dans K.

Dans ces conditions, la condition nécessaire et suffisante pour que α_i soit un nombre ν_i est que α_i soit norme par rapport à $k_{\mathfrak{p}_i}$ d'un nombre de $K_{\mathfrak{P}_i}$ (voir p. 420) qui sera nécessairement premier à $\mathfrak{P}_i$, puisque α_i est premier à $\mathfrak{p}_i$ On en conclut (voir p. 423)

$$(\alpha_i : \nu_i) = e_{\mathfrak{p}_i},$$

où $e_{\mathfrak{p}_i}$ désigne l'exposant de $\mathfrak{P}_i$ par rapport à k.

Si $\mathfrak{p}_i$ est infini, nous dirons que le $\mathfrak{p}_i$-conducteur de K est $\mathfrak{p}_i$ si $\mathfrak{p}_i$ est ramifié dans K, 1 dans le cas contraire. Nous supposerons encore $\mathfrak{m}$ divisible par les $\mathfrak{p}_i$-conducteurs de tous les idéaux premiers à l'infini ramifiés. Ces idéaux sont en nombre ρ_2 (en reprenant les notations du théorème des unités), et pour chacun d'eux $(\alpha_i : \nu_i) = 2$. En effet, soit $k^{(i)}$ le conjugué réel de k correspondant à $\mathfrak{p}_i$, $K^{(i)}$ le conjugué correspondant de K, qui est imaginaire. La norme relative de tout nombre de $K^{(i)}$ par rapport à $k^{(i)}$ est un nombre positif. Au contraire, si $\mathfrak{p}_i$ est non-ramifié, c'est-à-dire si $K^{(i)}$ est réel, il y a des nombres négatifs de $k^{(i)}$ qui sont normes relatives de nombres de $K^{(i)}$ (en effet, il résulte du lemme de la page 389 qu'il y a un nombre de $K^{(i)}$ positif dont tous les conjugués par rapport à $k^{(i)}$ distincts de lui-même sont négatifs), et $(\alpha_i : \nu_i) = 1$. Donc

$$(\alpha : \nu) = 2^{\rho_2} \Pi e_{\mathfrak{p}_i}.$$

Ceci posé, on a

$$h = \frac{h_1}{(\bar{A} : \bar{H}_1)} = \frac{h_0 \Pi e_{\mathfrak{p}_i} 2^{\rho_2} (\bar{H}_1 : \bar{H}_1')}{a(\varepsilon : [\nu, \varepsilon])},$$

et en remplaçant a par sa valeur (p. 406)

$$h = n([\mathfrak{k} : \mathfrak{k}] : N_{Kk}(\theta))(\bar{H}_1 : \bar{H}_1'),$$

d'où résulte en particulier $h \geq n$.

De cette inégalité résulte le fait suivant que nous avons déjà employé :

Si $n = (K:k)$ est la puissance l^a d'un nombre premier l, il y a un idéal premier de k premier à un idéal donné quelconque $\mathfrak{m}$ qui reste premier dans K.

En effet, supposons qu'il n'en soit pas ainsi. Soit $\mathfrak{d}$ le discriminant relatif de K. Tout idéal premier $\mathfrak{p}$ premier à $\mathfrak{m}\mathfrak{d}$ aurait un corps de décomposition $\neq k$. Mais tout corps compris entre K et k et $\neq k$ contient le sous-corps K_1 de K de degré l par rapport à k. Donc presque tous les idéaux premiers de k se décomposeraient totalement dans K_1. Il en résulterait que tout idéal de k premier à $\mathfrak{m}\mathfrak{d}$ serait norme d'un idéal de K_1, et que, par suite, pour tout module $\mathfrak{n}$ multiple de $\mathfrak{m}\mathfrak{d}$, le groupe de Takagi associé dans k à K_1 serait d'indice 1, ce qui est en contradiction avec l'inégalité qu'on vient d'obtenir.

Démonstration du théorème B. Cas cyclique.

Soient k un corps fini de nombres algébriques, et soit K un sur-corps relativement cyclique de degré n de k. Soient σ une opération engendrant le groupe de Galois de K par rapport à k, A le groupe des idéaux de k premiers au discriminant ralatif $\mathfrak{d}$ de K, H le groupe de Artin associé à K dans k, $\mathfrak{m}$ un module quelconque dans k.

Choisissons un sur-corps K' relativement circulaire par rapport à k, engendré par adjonction d'une racine q-ème. de l'unité, q étant premier, et étranger à K, dont le degré relatif soit multiple de n. Soit σ' une opération engendrant le groupe relatif de K' par rapport à k. Le groupe relatif de KK' est le produit direct des groupes de K, K'. Soit K_Z le sous-corps de KK' appartenant au groupe $(\sigma\sigma')$. Choisissons un idéal $\mathfrak{A}$ de K_Z premier à $\mathfrak{m}\mathfrak{d}(q)$ tel que

$$\left(\frac{KK'}{\mathfrak{A}}\right) = \sigma\sigma',$$

ce qui est possible en vertu du Théorème A. Soit $\mathfrak{a} = N_{K_Z k}(\mathfrak{A})$. On a (voir p. 427)

$$\left(\frac{KK'}{\mathfrak{a}}\right) = \sigma\sigma', \quad \left(\frac{K}{\mathfrak{a}}\right) = \sigma, \quad \left(\frac{K'}{\mathfrak{a}}\right) = \sigma'.$$

Soit alors $\mathfrak{p}^a$ un idéal primaire (c'est-à-dire puissance d'un idéal premier) de k, premier à $\mathfrak{m}\mathfrak{d}$. On peut, nous l'avons vu (voir p. 435), trouver un corps circulaire K'' par rapport à k, engendré par une racine de l'unité d'ordre premier et premier à $\mathfrak{p}$, étranger à KK', tel que, H'' désignant le groupe de Artin associé à K'' dans k, $\mathfrak{p}^a$ appartienne (mod. H'') à une classe dont l'ordre est un multiple de n. Soit $\mathfrak{K}''$ cette classe, et soit

$$\left(\frac{K''}{\mathfrak{p}^a}\right) = \sigma'', \qquad \left(\frac{K}{\mathfrak{p}^a}\right) = \sigma^x,$$

Le groupe de Galois de $KK'K''$ est produit direct des groupes de Galois de K, K', K''. Soit K_1 le sous-corps de $KK'K''$ appartenant au groupe $(\sigma^x\sigma'^x\sigma'')$. Choisissons un idéal $\mathfrak{B}_1$ de K_1 premier à $\mathfrak{m}\mathfrak{d}(q)$ tel que

$$\left(\frac{KK'K''}{\mathfrak{B}_1}\right) = \sigma^x\sigma'^x\sigma''.$$

Dans $KK'K''$, le corps K_Z appartient au groupe $(\sigma\sigma', \sigma'')$. Il est donc contenu dans K_1. Soit $\mathfrak{B} = N_{K_1K_Z}(\mathfrak{B}_1)$, $\mathfrak{b} = N_{K_Zk}(\mathfrak{B})$. On a

$$\left(\frac{KK'K''}{\mathfrak{B}}\right) = \sigma^x\sigma'^x\sigma'', \quad \left(\frac{KK'}{\mathfrak{B}}\right) = \sigma^x\sigma'^x.$$

Donc $\left(\frac{KK'}{\mathfrak{B}^{-1}\mathfrak{A}^x}\right) = 1$. Mais KK' est corps circulaire par rapport à K_Z. En effet K_ZK' appartient dans KK' au groupe commun aux groupes $(\sigma\sigma')$ et (σ). σ' étant d'ordre multiple de n et σ d'ordre n, ce groupe se réduit à l'unité, et on a $K_ZK' = KK'$. L'idéal $\mathfrak{B}^{-1}\mathfrak{A}^x$, qui appartient au groupe de Artin associé à KK' dans K_Z et qui est premier à $\mathfrak{m}$ appartient donc aussi au groupe de Takagi associé à KK' dans K_Z (mod. $\mathfrak{m}(q)$), et *à fortiori* (mod. $\mathfrak{m}$), et on a

$$\mathfrak{B}^{-1}\mathfrak{A}^x = (B)N_{KK',\,K_Z}(\mathfrak{C}), \qquad B \equiv 1 \text{ (mod. } \mathfrak{m}),$$

$\mathfrak{C}$ étant un idéal de KK' premier à $\mathfrak{m}$. D'où on déduit

$$\begin{aligned}\mathfrak{b}^{-1}\mathfrak{a}^x &= (\beta)N_{KK',\,k}(\mathfrak{C}) \\ &= (\beta)N_{Kk}(\mathfrak{c}), \qquad \beta \equiv 1 \text{ (mod. } \mathfrak{m}),\end{aligned}$$

$\mathfrak{c}$ étant un idéal de K premier à $\mathfrak{m}$.

Soit K_Z' le sous-corps de KK'' appartenant au groupe $(\sigma^x\sigma'')$. On a $\left(\frac{KK''}{\mathfrak{p}^a}\right) = \sigma^x\sigma''$. Je dis que $\mathfrak{p}^a$ est norme relative d'un idéal de K_Z'. En effet, soit

$$\left(\frac{KK''}{\mathfrak{p}}\right) = \tau, \qquad \tau^a = \sigma^x\sigma'',$$

et soit φ l'ordre de τ. Le corps $K_Z{}^*$ contenu dans KK'' et appartenant au groupe (τ) est le corps de décomposition de $\mathfrak{p}$ dans KK''. $\mathfrak{p}$ est norme par rapport à k d'un idéal premier $\mathfrak{P}$ de ce corps. D'autre part K_Z' est sur-corps de $K_Z{}^*$ de degré relatif (a, φ). Donc $\mathfrak{P}^{(a,\varphi)}$ est norme

par rapport à K_Z^* d'un idéal premier $\mathfrak{P}'$ de K_Z'. On a $\mathfrak{p}^a = N_{K'_Z k}(\mathfrak{P}'^{(a,\varphi)})$. Soit $\Omega = \mathfrak{P}'^{(a,\varphi)}$. On a

$$\left(\frac{KK''}{\Omega}\right) = \sigma^x \sigma''.$$

D'autre part K_1 contient K'_Z. Soit $\mathfrak{B}' = N_{K_1 K'_Z}(\mathfrak{B}_1)$. On a

$$\left(\frac{KK''}{\mathfrak{B}'}\right) = \sigma^x \sigma''$$

et

$$\left(\frac{KK''}{\mathfrak{B}'\Omega^{-1}}\right) = 1.$$

Mais KK'' est relativement circulaire par rapport à K_Z', car $KK'' = K_Z' K''$. Donc, en raisonnant comme plus haut,

$$\mathfrak{B}'\Omega^{-1} = (B')N_{KK'', K'_Z}(\mathfrak{C}'), \quad B' \equiv 1 \text{ (mod. } \mathfrak{m}), \quad (\mathfrak{C}', \mathfrak{m}) = 1$$

et prenant la norme par rapport à k,

$$\mathfrak{b}\mathfrak{p}^{-a} = (\beta')N_{Kk}(\mathfrak{c}'), \quad \beta' \equiv 1 \text{ (mod. } \mathfrak{m}) \quad (\mathfrak{c}', \mathfrak{m}) = 1.$$

Il résulte des deux égalités trouvées que

$$\mathfrak{a}^x \mathfrak{p}^{-a} = (\beta'')N_{Kk}(\mathfrak{C}''), \quad \beta'' \equiv 1 \text{ (mod. } \mathfrak{m})$$

$\mathfrak{C}''$ étant un idéal de K premier à $\mathfrak{m}$.

On a $\mathfrak{p}^a \equiv \mathfrak{a}^x$ (mod. H) ; la formule précédente montre que l'on a aussi $\mathfrak{p}^a \equiv \mathfrak{a}^x$ (mod. H^*), où H^* est le groupe de Takagi associé (mod. $\mathfrak{m}$) à K dans k.

Soit maintenant $\mathfrak{n}$ un idéal quelconque de k premier à $\mathfrak{m}\mathfrak{d}$ et soit $\mathfrak{n} = \Pi\mathfrak{p}^a$ la décomposition de $\mathfrak{n}$ en facteurs premiers. Chacun des $\mathfrak{p}^a$ peut être remplacé par un idéal $\mathfrak{a}^x$ sans changer la classe à laquelle appartient $\mathfrak{n}$ modulo $[H, H^*]$. Donc il existe une puissance $\mathfrak{a}^X$ de $\mathfrak{a}$ telle que $\mathfrak{n}$ soit congru à $\mathfrak{a}^X$ modulo $[H, H^*]$. Or supposons $\mathfrak{n}$ contenu dans H. Comme $\mathfrak{a}$, en vertu de la formule $\left(\frac{K}{\mathfrak{a}}\right) = \sigma$, appartient (mod. H) à une classe d'ordre n, X est nécessairement multiple de n ; dans ces conditions, $\mathfrak{a}^X$ est norme relative d'un idéal de K, et $\mathfrak{a}^X$ appartient aussi à H^*. Donc :

H^* étant le groupe de Takagi associé (mod. $\mathfrak{m}$) à K, H^* contient les idéaux de H premiers à $\mathfrak{m}$.

Or prenons pour $\mathfrak{m}$ le produit $\mathfrak{m}_0$ des $\mathfrak{p}$-conducteurs de tous les idéaux premiers, finis ou infinis, de k ramifiés dans K. Dans ces

conditions tout idéal de H est premier à $\mathfrak{m}_0$ et on a vu (p. 441) que l'indice $(A:H)$ est multiple de n. Mais H^* contient H, donc $(A:H^*)$ divise $(A:H)=n$. Donc $H^*=H$.

Si maintenant $\mathfrak{m}$ est un multiple quelconque de $\mathfrak{m}_0$, le groupe de Takagi $H_{\mathfrak{m}}{}^*$ associé (mod. $\mathfrak{m}$) à K contient le groupe des idéaux de H premiers à $\mathfrak{m}$, $H_{\mathfrak{m}}$. Ce dernier étant encore d'indice n le raisonnement se fait comme dans le cas précédent et on a $H_{\mathfrak{n}}=H_{\mathfrak{m}}{}^*$.

Le théorème B est donc démontré pour les extensions cycliques.

Démonstration du théorème B. Cas général.

Le théorème B étant démontré pour les extensions cycliques, supposons le démontré pour toutes les extensions abéliennes composées de r corps cycliques au plus.

k étant un corps fini de nombres algébriques, un sur-corps relativement abélien composé de $r+1$ corps relativement cycliques se met sous la forme KK_1, K étant composé de r corps relativement cycliques, et K_1 étant relativement cyclique. Soient H, H_1 les groupes de Artin associés à K, K_1 dans k ; il y a des modules $\mathfrak{m}_0$, $\mathfrak{m}_1$ tels que H, H_1 soient respectivement les groupes de Takagi associés à K, K_1 (mod. $\mathfrak{m}_0$) et (mod. $\mathfrak{m}_1$). Soit $\overline{\mathfrak{m}}$ le p.p.c.m. de $\mathfrak{m}$ et de $\mathfrak{m}_1$. $\overline{\mathfrak{m}}$ n'est composé que d'idéaux ramifiés dans KK_1. Soit $\bar{H}_{\overline{\mathfrak{m}}}$ le groupe de Takagi associé (mod. $\overline{\mathfrak{m}}$) à KK_1 dans k. Le groupe $\bar{H}_{\overline{\mathfrak{m}}}$ est évidemment contenu dans H, H_1, donc leur partie commune $[H, H_1]$ qui est le groupe de Artin associé à KK_1.

D'autre part soit $\bar{H}'$ le groupe des idéaux de K_1 premiers à $\overline{\mathfrak{m}}$ dont la norme par rapport à k tombe dans $\bar{H}_{\overline{\mathfrak{m}}}$, et soient $A_{\overline{\mathfrak{m}}}$, $A'_{\overline{\mathfrak{m}}}$ les groupes des idéaux de k, K_1 premiers à $\overline{\mathfrak{m}}$. En vertu du principe d'isomorphie[30] on a, en désignant par $H_1{}^*$ le groupe des idéaux de H_1 premiers à $\overline{\mathfrak{m}}$, qui est le groupe de Takagi associé à K_1 (mod. $\overline{\mathfrak{m}}$) dans k,

$$(A'_{\overline{\mathfrak{m}}}:\bar{H}')=(H_1{}^*:\bar{H}_{\overline{\mathfrak{m}}}).$$

Or $\bar{H}'$ contient le groupe de Takagi associé à KK_1 dans K_1 (mod. $\overline{\mathfrak{m}}$), donc aussi le groupe de Takagi associé à KK_1 dans K_1 (mod. $\mathfrak{n}$), $\mathfrak{n}$ étant un multiple de $\overline{\mathfrak{m}}$. Or ce groupe de Takagi, en choisissant convenablement $\mathfrak{n}$, sera identique au groupe des idéaux premiers à $\mathfrak{n}$ du groupe de Artin associé à KK_1 dans K_1. En effet, par hypothèse, le théorème B

30) La correspondance $\mathfrak{A}\to N_{K,k}(\mathfrak{A})$ donne une homomorphie de A sur H_1, donc aussi sur H_1/H.

est déja démontré pour l'extension KK_1/K_1. Il en résulte que $(A_{\bar{\mathfrak{m}}}' : \bar{H}') \leq (KK_1 : K_1)$ et puisque $(A_{\bar{\mathfrak{m}}} : H_1^*) = (K_1 : k)$,

$$(A_{\bar{\mathfrak{m}}} : \bar{H}_{\bar{\mathfrak{m}}}) \leq (KK_1 : k).$$

Or, $\bar{H}_{\bar{\mathfrak{m}}}$ étant contenu dans $[H, H_1]$

$$(A_{\bar{\mathfrak{m}}} : \bar{H}_{\bar{\mathfrak{m}}}) \geq (A_{\bar{\mathfrak{m}}} : [H, H_1]) = (KK_1 : k).$$

D'où $[H, H_1] = \bar{H}_{\bar{\mathfrak{m}}}$. Si maintenant $\mathfrak{m}$ est un multiple quelconque de $\bar{\mathfrak{m}}$, le groupe de Takagi associé (mod. $\mathfrak{m}$) à KK_1 dans k, soit $\bar{H}_{\mathfrak{m}}^*$, sera contenu dans $\bar{H}_{\bar{\mathfrak{m}}}$, donc dans le groupe $\bar{H}_{\mathfrak{m}}$ des idéaux de $\bar{H}_{\bar{\mathfrak{m}}}$ premiers à $\mathfrak{m}$. D'autre part exactement comme tout-à-l'heure pour $\bar{\mathfrak{m}}$, on démontre $(A_{\mathfrak{m}} : \bar{H}_{\mathfrak{m}}^*) \leq (KK_1 : k)$. Comme $(A_{\mathfrak{m}} : \bar{H}_{\mathfrak{m}}) = (KK_1 : k)$, il vient $\bar{H}_{\mathfrak{m}} = \bar{H}_{\mathfrak{m}}^*$, ce qui achève de démontrer le théorème B.

Le genre principal. Le théorème de Hasse.

Soit k un corps fini de nombres algébriques et soit K un sur-corps relativement cyclique de degré relatif n. Soit $\mathfrak{m}_0$ un module tel que le groupe de Takagi associé à K dans k (mod. $\mathfrak{m}_0$) soit d'indice n dans le groupe des idéaux de k premiers à $\mathfrak{m}_0$. Revenons à la formule de la p. 441. On a $h = n$, et on en déduit

1) $([\varepsilon, \nu] : N_{Kk}(\theta)) = 1$, ce qui signifie que toute unité de k qui est reste normique de K (mod. $\mathfrak{m}_0$) est norme d'un nombre de K,

2) $\bar{H}_1 = \bar{H}_1'$, c'est-à-dire :

Le genre principal de K se compose des classes absolues de la forme $C^{1-\sigma}$.

Ce qui revient à dire ceci : si un idéal $\mathfrak{A}$ de K premier à $\mathfrak{m}_0$ est tel que $N_{Kk}(\mathfrak{A})$ soit congru (mod. $\mathfrak{m}_0$) à la norme par rapport à k d'un idéal principal, cet idéal $\mathfrak{A}$ est de la forme $(A)\mathfrak{B}^{1-\sigma}$, A étant un nombre de K, $\mathfrak{B}$ un idéal de K.

Ceci posé, soit un nombre α de k qui est reste normique de K modulo tout module de k. Soit $\mathfrak{p}$ un facteur premier de (α), et soit $\mathfrak{P}$ un facteur premier de $\mathfrak{p}$ dans K de degré relatif f. En écrivant $\alpha \equiv N_{Kk}(A)$ (mod. $\mathfrak{p}$), on voit que (α) et $(N_{Kk}(A))$ doivent être divisible par la même puissance de $\mathfrak{p}$, donc que $\mathfrak{p}$ figure dans (α) avec un exposant multiple de f. Donc $(\alpha) = \Pi \mathfrak{p}_i^{\nu_i f_i} = \Pi N_{Kk}(\mathfrak{P}_i^{\nu_i})$ et (α) est la norme d'un idéal $\mathfrak{A}$ de K. Dans la classe de $\mathfrak{A}$ nous pouvons choisir un idéal $\mathfrak{A}'$ premier à $\mathfrak{m}_0$. On a $\mathfrak{A}' = (A')\mathfrak{A}$, et

$$N_{Kk}(\mathfrak{A}') = \frac{(\alpha)}{N_{Kk}(A')}.$$

Or $\frac{\alpha}{N_{Kk}(A')}$ est reste normique (mod. $\mathfrak{m}_0$), donc $\mathfrak{A}'$ appartient au genre principal, et par suite $\mathfrak{A}' = (A'')\mathfrak{B}^{1-\sigma}$, d'où

$$(\alpha) = (N_{Kk}(A'A'')), \qquad \alpha = \varepsilon N_{Kk}(A'A'').$$

Or ε est encore reste normique (mod. $\mathfrak{m}_0$), donc norme d'un nombre de K. D'où le

Théorème de Hasse[31]. *Un nombre de k qui, pour tout module $\mathfrak{m}$, est reste normique* (mod. $\mathfrak{m}$) *d'un sur-corps K relativement cyclique est norme relative d'un nombre de K.*

Ce théorème n'est pas vrai pour les corps K non cycliques.

Applications.

Lemme. *Soit k un corps fini de nombres algébriques. Si K est corps de classes sur k pour un groupe H'* (mod. $\mathfrak{m}$), *H' est le groupe de Takagi associé* (mod. $\mathfrak{m}$) *à K dans k.*

Soit H le groupe de Artin associé à K dans k. Le groupe H' étant égal à H, il résulte du théorème B qu'il y a un module $\mathfrak{n}$ multiple de $\mathfrak{m}$ tel que tout idéal premier à $\mathfrak{n}$ de H' soit congru (mod. $\mathfrak{n}$) à la norme relative d'un idéal premier à $\mathfrak{n}$ de K. Soit $\mathfrak{a}$ un idéal de H' : il y a un idéal $\mathfrak{a}' \equiv \mathfrak{a}$ (mod. $\mathfrak{m}$) qui est premier à $\mathfrak{n}$; on a $\mathfrak{a}' \equiv N_{Kk}(\mathfrak{A})$ (mod. $\mathfrak{n}$), donc $\mathfrak{a} \equiv N_{Kk}(\mathfrak{A})$ (mod. $\mathfrak{m}$) et $\mathfrak{a}$ appartient au groupe de Takagi associé (mod. $\mathfrak{m}$) à K. Réciproquement, soit $\mathfrak{a}$ un idéal de ce groupe de Takagi, donc $\mathfrak{a} \equiv N_{Kk}(\mathfrak{A})$ (mod. $\mathfrak{m}$), où $\mathfrak{A}$ est premier à $\mathfrak{m}$. Il existe un idéal $\mathfrak{A}'$ premier à $\mathfrak{n}$ et qui est congru (mod. $\mathfrak{m}$) à $\mathfrak{A}$. Donc $\mathfrak{a} \equiv N_{Kk}(\mathfrak{A}')$ (mod. $\mathfrak{m}$). Le second membre est dans H et premier à $\mathfrak{n}$, donc dans H'. H' étant définissable (mod. $\mathfrak{m}$), $\mathfrak{a}$ est aussi dans H'.

Ceci posé, nous pouvons démontrer un théorème qui nous servira à simplifier la démonstration du théorème d'existence[32] :

Si K est corps de classes sur k pour le groupe H, et si H' est un groupe contenant H, K contient un corps de classes K' pour H'.

En effet on peut supposer que les groupes H, H' sont des groupes de congruence (mod. $\mathfrak{m}$), $\mathfrak{m}$ étant un module qui est divisible par tous

31) Voir Hasse, Beweis eines Satzes und Widerlegung einer Vermutung über das allgemeine Normenrestsymbol, Gött. Nachr., 1931. Le théorème y est démontré par induction à partir du cas n premier.

32) Ces théorèmes peuvent être démontrés à priori, en donnant du corps de classes la définition de Takagi, d'une manière analytique. C'est la voie qui fut suivie par M. Artin dans son cours au semestre d'hiver à Hambourg

les idéaux premiers de k ramifiés dans K. Quand $\mathfrak{a}$ parcourt les idéaux de H', $\left(\frac{K}{\mathfrak{a}}\right)$ parcourt les opérations d'un sous-groupe g du groupe de Galois de K par rapport à k. Soit K' le corps appartenant à g. Donc, si $\mathfrak{a}$ est dans H', $\left(\frac{K'}{\mathfrak{a}}\right) = 1$, et réciproquement, si $\mathfrak{a}$ est premier à $\mathfrak{m}$ et si $\left(\frac{K'}{\mathfrak{a}}\right) = 1$, $\mathfrak{a}$ est dans H'. Donc H' est égal au groupe de Artin associé à K' dans k. De même :

Si K est corps de classes sur k pour le groupe H, et si $\bar{k}$ est un sur-corps fini de k, $K\bar{k}$ est corps de classes sur $\bar{k}$ pour le groupe $\bar{H}$ des idéaux de $\bar{k}$ dont la norme par rapport à k est dans H.

Supposons H groupe de congruence (mod. $\mathfrak{m}$). Alors $\bar{H}$ est aussi égal à un groupe de congrueuce (mod. $\mathfrak{m}$). On peut supposer que $\mathfrak{m}$ contient tous les idéaux de k ramifiés dans $K\bar{k}$. Alors $\bar{H}$ est égal au groupe des idéaux premiers à $\mathfrak{m}$ du groupe de Artin associé à $K\bar{k}$ dans $\bar{k}$, ce qui démontre notre proposition.

Il en résulte immédiatement le théorème d'unicité : *il y a un corps de classes au plus pour un groupe donné, à une égalité près.*

En effet, s'il y en avait deux, soient K, $\bar{k}$, en vertu de la proposition précédente, $K\bar{k}$ serait corps de classes sur $\bar{k}$ pour un groupe qui contiendrait tous les idéaux de $\bar{k}$ premiers à un certain module ; ce groupe serait d'indice 1, et on aurait $(K\bar{k} : \bar{k}) = 1$, $K \subset \bar{k}$. On démontrerait de même que $\bar{k} \subset K$, ce qui conduit à une contradiction.

Démonstration du théorème de Kronecker.

Le théorème B permet de démontrer facilement le théorème de Kronecker qui s'énonce ainsi :

Un corps absolument abélien est contenu dans un corps circulaire.

En effet, un corps K absolument abélien est corps de classes sur le corps R des rationnels pour un groupe de congruence, donc définissable (mod. mp), m étant un entier positif et p l'idéal premier à l'infini de R. Ce groupe contient donc le groupe H des nombres $\equiv 1$ (mod. mp), qui est le groupe pour lequel le corps K' des racines m-ièmes de l'unité est corps de classes. Donc K est contenu dans K'.

Chapitre IX.

La théorie du corps de classes local.

Désignons par k un corps local, par $\mathfrak{p}$ l'idéal premier de k, par A le groupe des nombres $\neq 0$ de k.

Rappelons qu'à tout sur-corps K de k nous avons associé le groupe H des nombres de k qui sont normes par rapport à k de nombres de K.

Nous dirons que K est *corps de classes* par rapport à k pour le groupe H quand l'indice $(A : H)$ de H est égal à $(K : k)$.

Nous avons montré que tout corps K relativement cyclique par rapport à k est corps de classes. Nous allons encore montrer que tout corps relativement abélien est corps de classes.

Un théorème général sur les normes.

Nous aurons besoin du théorème général suivant :

Soient k un corps parfait, K et K' deux sur-corps relativement cycliques de k de même degré, dont les groupes sont engendrés par des opérations σ, σ'. Soit K'' un sous-corps de KK', cyclique par rapport à k et tel que $[K'', K] = k$ et $[K'', K'] = k$. Un nombre α qui est norme par rapport à k d'un nombre de K et d'un nombre de K' est aussi norme par rapport à k d'un nombre de K''.

En effet, le groupe de Galois de KK' par rapport à k est le produit direct des groupes de Galois de K, K'. Les opérations σ, σ' peuvent être choisies de manière à ce que l'opération $\sigma\sigma'$ laisse les nombres de K'' invariants (en effet, si K'' appartient au groupe $(\sigma^\alpha \sigma'^\beta)$, les conditions $[K'', K] = [K'', K'] = k$ entraînent que α et β sont premiers à n, et donc que σ^α, σ'^β sont des opérations engendrant les groupes de K, K'). Il suffit alors de démontrer le théorème dans le cas où K'' est précisément le corps appartenant au groupe $(\sigma\sigma')$. Soit $(K : k) = (K' : k) = n$. On a par hypothèse

$$\alpha = \Gamma . \sigma\Gamma . \dots . \sigma^{n-1}\Gamma = \Delta . \sigma'\Delta . \dots . \sigma'^{n-1}\Delta,$$

Γ étant un nombre de K, donc tel que $\sigma'\Gamma = \Gamma$, et Δ un nombre de K', donc tel que $\sigma\Delta = \Delta$. On a donc

$$\Gamma\Delta^{-1} . \sigma\sigma'(\Gamma\Delta^{-1}) . \dots . (\sigma\sigma')^{n-1}(\Gamma\Delta^{-1}) = 1.$$

Donc $N_{KK', K''}(\Gamma\Delta^{-1}) = 1$, et en vertu du théorème de Hilbert il existe un nombre Ξ de KK' tel que

$$\Gamma\Delta^{-1} = \Xi^{1-\sigma\sigma'}.$$

Posons $\xi = \Gamma\Xi^{\sigma-1}$ et formons $\sigma'^{-1}\sigma^{-1}\xi$. Remarquons que $\Xi^{1-\sigma\sigma'} = \Xi^{1-\sigma+\sigma(1-\sigma')}$, de sorte que

$$\xi = \Xi^{\sigma(1-\sigma')}\Delta.$$

D'où $$\sigma^{-1}\xi = \Xi^{1-\sigma'}\Delta = \Xi^{1-\sigma\sigma'+\sigma'(\sigma-1)}\Delta = \Gamma\Xi^{\sigma'(\sigma-1)}$$

et $$\sigma'^{-1}\sigma^{-1}\xi = \Gamma\Xi^{\sigma-1} = \xi.$$

Donc ξ est dans K'', et on a

$$N_{K'',k}(\xi) = \xi.\sigma\xi.\ \ldots.\sigma^{n-1}\xi = \Gamma.\sigma\Gamma.\ \ldots.\sigma^{n-1}\Gamma = \alpha,$$

ce qui démontre le théorème.

Les sur-corps non ramifiés.

Tout sur-corps relativement galoisien d'un corps local k qui n'est pas ramifié est cyclique. Soit en effet K un tel sur-corps, et soit $\mathfrak{P}$ l'idéal premier de K. Le groupe de décomposition de $\mathfrak{P}$ est (comme toujours, quand il s'agit de corps locaux) égal au groupe de Galois de K par rapport à k. Le groupe d'inertie se réduit à l'unité puisque K n'est pas ramifié. Le groupe quotient du groupe de décomposition par le groupe d'inertie étant cyclique, la proposition est démontrée.

Il résulte de là que pour chaque degré n il y a au plus un sur-corps galoisien de degré relatif n non-ramifié: car s'il y en avait deux, leur corps composé ne serait pas non plus ramifié, et ne serait pas cyclique.[33]

Montrons maintenant que pour chaque degré n, il existe un sur-corps de degré relatif n non-ramifié. Soit p le nombre premier rationnel contenu dans $\mathfrak{p}$, et soit f le degré de l'idéal $\mathfrak{p}$. Soit χ une racine primitive $(p^{fn}-1)$-ième de l'unité. Remarquons qu'un nombre $\chi^a - 1$, s'il est différent de 0, est premier à p car le produit de ces nombres est $p^{fn} - 1$ qui est premier à p. Considérons le corps $k(\chi)$ et soit $\mathfrak{P}$ l'idéal premier de ce corps. Deux nombres de la forme χ^a, χ^b ne sont congrus (mod. $\mathfrak{P}$) que s'ils sont égaux, car $\chi^a - \chi^b = \chi^a(1 - \chi^{b-a})$. D'ailleurs, ces nombres χ^a forment un groupe multiplicatif d'ordre $p^{fn} - 1$, ce qui n'est possible que si le degré F de $\mathfrak{P}$ est multiple de fn. Le corps d'inertie de $\mathfrak{P}$ dans $k(\chi)$ est un sur-corps relativement

33) Si $K.K'$ sont deux sur-corps relativement galoisiens de k, le groupe relatif de Galois de KK' est sous-groupe du produit direct des groupes de Galois de K, K'. Un élément $\sigma\sigma'$ n'appartient au groupe d'inertie de $\mathfrak{p}$ dans KK' que si σ appartient au groupe d'inertie de $\mathfrak{p}$ dans K et σ' au groupe d'inertie de $\mathfrak{p}$ dans K' Si ces deux groupes se réduisent à 1, il en est de même du groupe d'inertie de $\mathfrak{p}$ dans KK'.

cyclique de k de degré relatif $\frac{F}{f}$. Il contient donc un sur-corps relativement cyclique non ramifié de k de degré relatif n. (On montre d'ailleurs que ce corps est $k(\chi)$ lui-même.) On remarquera que tout sur-corps relativement galoisien de k de degré relatif n étranger au corps que l'on vient de construire est complètement ramifié, et réciproquement tout sur-corps complètement ramifié est étranger au corps que l'on vient de construire.

Corps galoisiens.

Soit K un corps relativement galoisien par rapport à un corps local k. On démontre au moyen de la théorie de Galois relative à un idéal premier que K est toujours métacyclique par rapport à k[10]. Soit H le groupe associé dans K à k. Nous voulons démontrer l'inégalité

$$(K:k) \geq (A:H).$$

Nous opérerons par récurrence sur $(K:k)$. Si ce degré est premier, K est relativement cyclique, et l'inégalité (qui est une égalité, puisque K est alors corps de classes sur k) (voir p. 423) est vraie. Supposons la donc démontrée pour toutes les valeurs du degré relatif plus petites que n, et soit K un sur-corps de degré relatif n. Si n n'est pas premier, K, étant métacyclique, possède au moins un sous-corps $\bar{K}$ contenant k, différent de k et de K, et relativement métacyclique par rapport à k. Soient H_1 le groupe associé à $\bar{K}$ dans k, $\bar{A}$ le groupe des nombres $\neq 0$ de $\bar{K}$, $\bar{H}$ le groupe associé à K dans $\bar{K}$, $\bar{H}^*$ le groupe des nombres de $\bar{K}$ dont la norme par rapport à k tombe dans H. On a

$$(A:H) = (A:H_1)(H_1:H).$$

L'homomorphisme $\alpha \to N_{\bar{K}k}(\alpha)$ appliqué au groupe $\bar{A}$ donne (principe d'isomorphie)

$$(\bar{A}:\bar{H}^*) = (H_1:H)^{34}).$$

---

34) D'une manière générale soient k un corps local, $\bar{k}$ un sur-corps de degré fini de k, A, $\bar{A}$ les groupes des nombres $\neq 0$ de k, $\bar{k}$; H un sous-groupe de A d'indice fini, h le groupe associé à $\bar{k}$ dans k, $\bar{H}$ le groupe des nombres de $\bar{k}$ dont la norme par rapport à k est dans H. α étant un nombre de $\bar{k}$, la correspondance $\alpha \to N_{\bar{k}k}(\alpha)$ donne une homomorphie de $\bar{A}$ sur h, donc aussi sur $h/[h,H]$. Le groupe des éléments de $\bar{A}$ dont le correspondant est dans $[h,H]$ est $\bar{H}$ et on a, en vertu de principe d'isomorphie,

$$\bar{A}/\bar{H} \simeq h/[h,H], \qquad (A:[h,H]) = (A:h)(\bar{A}:\bar{H}).$$

Ce raisonnement sera plusieurs fois utilisé dans la suite.

Or il est évident que $\bar{H}^*$ contient $\bar{H}$. Donc, $(\bar{A}:\bar{H}^*) \leq (\bar{A}:\bar{H})$. Or le théorème est démontré par hypothèse pour l'extension $K/\bar{K}$ et pour $\bar{K}/k$. Donc

$$(A:H_1) \leq (\bar{K}:k), \qquad (\bar{A}:\bar{H}) \leq (K:\bar{K}).$$

D'où la démonstration de la formule annoncée[35].

De plus, si $(K:k) = (A:H)$, on a nécessairement

$$(A:H_1) = (\bar{K}:k), \qquad (\bar{A}:\bar{H}^*) = (\bar{A}:\bar{H}) = (K:\bar{K}).$$

On en déduit en particulier :

Si K est galoisien et corps de classes par rapport à k et si $\bar{K}$ est un sous-corps de K galoisien par rapport à k, K est corps de classes sur $\bar{K}$ pour le groupe des nombres de $\bar{K}$ dont la norme par rapport à k tombe dans le groupe H associé à K dans k.

Cela va nous permettre de généraliser le théorème de la page 449. Soient K, K' deux sur-corps relativement cycliques de degré n de k, et soit K'' un sur-corps relativement cyclique de degré n de k contenu dans KK'. Soit $[K, K'] = K_1$. Soient H, H' les groupes associés dans k à K, K'. Soient H_1, H_1' respectivement les groupes de nombres de K_1 dont les normes par rapport à k tombent dans H, H'. Alors les groupes associés à K, K' dans K_1 sont H_1, H_1'. Si α appartient à $[H, H']$, il est norme par rapport à k d'un nombre A de K_1 qui est dans $[H_1, H_1']$.

On est donc ramené au cas où $[K, K'] = k$. Décomposons n en facteurs premiers : soit $n = \prod_i p_i^{a_i}$. Le corps K est composé de corps K_i relativement cycliques par rapport à k, K_i étant de degré relatif $p_i^{a_i}$. De même pour K' et pour K''. Le corps K_i'' est un sous-corps de K_iK_i'. Un nombre α qui est norme d'un nombre de K et d'un nombre de K', est norme d'un nombre de K_i et d'un nombre de K_i'. On ne peut avoir en même temps $[K_i'', K_i] \neq k$ et $[K_i'', K_i'] \neq k$, car sinon ces deux corps contiendraient l'unique sous-corps de degré relatif p_i de K_i'', ce qui est impossible en vertu de $[K_i, K_i'] = k$. σ_i et σ_i' étant des opérations engendrant les groupes de K_i, K_i' par rapport à k, le corps K_i''' appartenant au groupe $(\sigma_i\sigma_i')$ est étranger à K_i et à K_i' par rapport à k. Si $[K_i, K_i''] = [K_i', K_i''] = k$, α est norme relative d'un nombre de K_i'' en vertu du théorème de la p. 449. Si par exemple $[K_i, K_i''] \neq k$, on voit en raisonant comme plus haut que $[K_i'', K_i'''] = k$. En vertu du théorème de la p. 449, α est norme relative d'un nombre de K_i'''. En

35) Il en résulte que si on peut démontrer que H est contenu dans unso us-groupe de A d'indice $\geq (K:k)$, K sera corps de classes.

appliquant le même théorème à K_i''' et à K_i', on voit que α est norme relative d'un nombre de K_i''. Il appartient donc au groupe H_i'' associé à K_i'' dans k. Or le groupe associé à K'' est contenu dans tous les groupes H_i'', donc dans leur partie commune. De $(A : H_i'') = p_i^{a_i}$ on déduit que cette partie commune est d'indice n dans A. Le groupe associé à K'' étant aussi d'indice n est identique à cette partie commune, et contient par suite α. Donc :

k étant un corps local, K, K' deux sur-corps relativement cycliques de même degré relatif de k, un nombre α de k qui est norme par rapport à k d'un nombre de K et d'un nombre de K' est aussi norme par rapport à k d'un nombre d'un sous-corps K'' de KK' cyclique par rapport à k.

Le théorème d'unicité pour les corps cycliques.

Soit k un corps local, et soit K un sur-corps relativement cyclique de degré n de k, complètement ramifié. Soit K' le sur-corps non ramifié de k de degré n. On a donc $[K, K'] = k$. Le groupe de Galois de KK' par rapport à k est le produit direct des groupes de Galois de K, K'. Prenons des opérations σ, σ' de ce groupe où σ laisse invariants les éléments de K' et produit un automorphisme primitif de K, et de même pour σ' en intervertissant K, K'. Soit K'' le sous-corps de KK' appartenant au groupe $(\sigma\sigma')$. K'' est étranger à K' et par suite complètement ramifié (voir p. 450). Prenons un nombre Π de K'' d'ordre 1 pour l'idéal premier de ce corps et posons : $\varpi = N_{K''k}(\Pi)$; ϖ est d'ordre 1 pour l'idéal premier $\mathfrak{p}$ de k. Supposons que ϖ^ν soit norme par rapport à k d'un nombre de K. Il est aussi égal à $N_{K''k}(\Pi^\nu)$. Donc, d'après le théorème ci-dessus, il est norme d'un nombre de K'. K' étant non ramifié de degré relatif n, cela n'est possible que si $\nu \equiv 0 \pmod{n}$. Donc la plus petite puissance de ϖ contenue dans le groupe associé à K dans k est ϖ^n. Ce groupe étant d'indice n dans A, A/H est cyclique. Donc :

Lemme. *k étant un corps local, A le groupe des nombres différents de 0 de k, K un sur-corps relativement cyclique complètement ramifié de k, H le groupe associé à K dans k, A/H est cyclique.*

On peut maintenant démontrer le

Théorème d'unicité : *k étant un corps local, K et K' deux sur-corps relativement cycliques de k distincts, les groupes H, H' qui leur sont associés dans k sont distincts.*

En effet soit $k^* = [K, K']$, et supposons $H = H'$, Chacun des corps K, K' est corps de classes sur k^* pour le groupe des nombres de k^*

dont les normes par rapport à k tombent dans H. On se ramène donc tout de suite au cas où $[K, K'] = k$ (en remplaçant k^* par k).

Soit f le plus petit exposant différent de 0 tel que H contienne un nombre d'ordre f en $\mathfrak{p}$, $\mathfrak{p}$ désignant l'idéal premier de k. Il résulte de l'étude faite du corps relativement cyclique que dans chacun des corps K, K' l'idéal premier a le degré relatif f par rapport à k. Mais cela exige $f = 1$, car sinon, K et K' contiendraient le sur-corps non ramifié cyclique de k de degré relatif f. Donc chacun des corps K et K' est complètement ramifié, et par suite A/H est cyclique. De plus, il y a un nombre ϖ d'ordre 1 pour $\mathfrak{p}$ qui est dans H, donc norme par rapport à k d'un nombre de K et d'un nombre de K'. Donc KK' ne contient aucun sur-corps non ramifié de k différent de k, car ϖ devrait être norme d'un nombre d'un tel sur-corps.

Soit alors $(K:k) = (K':k) = n$ et considérons le sur-corps K'' non ramifié de k de degré relatif n. Le groupe de Galois de $KK'K''$ par rapport à k est produit direct des groupes de Galois de K, K', K'' par rapport à k. Nous y choisirons trois opérations σ, σ', σ'', σ laissant invariants les nombres de $K'K''$ et produisant un automorphisme primitif de K, et de même pour σ' et σ'' en permutant circulairement les trois corps K, K', K''. Considérons le sous-corps K_2 de $KK'K''$ appartenant au groupe $(\sigma\sigma'')$. Le corps $[K_2, K'']$ appartient au groupe $(\sigma\sigma'', \sigma, \sigma')$ et par suite est égal à k. Donc K_2 est complètement ramifié. Choisissons un nombre Π d'ordre 1 pour l'idéal premier de K_2, et soit $\varpi = N_{K_2k}(\Pi)$. Exactement comme dans le raisonnement de la page 453, on voit que la plus petite puissance de ϖ qui soit norme par rapport à k d'un nombre de K est ϖ^n (car ϖ est norme relative d'un nombre de $[K_2, KK'']$). D'autre part K_2 contient K', donc ϖ est norme par rapport à k d'un nombre de K', et ϖ est dans H' ; d'où la contradiction.

Condition pour qu'un sur-corps soit abélien.

Nous nous proposons de démontrer le théorème suivant, k étant un corps local :

Théorème. *Soit τ un automorphisme de k, et soit k^* le corps des nombres de k invariants par τ. Soit K un sur-corps relativement abélien de k, corps de classes pour un groupe H contenant les nombres $\alpha^{1-\tau}$, α parcourant les nombres $\neq 0$ de k. Alors K est relativement abélien et corps de classes par rapport à k^*.*

En effet, soit f le degré par rapport à k^* de l'idéal premier de K.

Soit $\bar{k}$ le sur-corps non ramifié de degré f de k^*. Considérons K comme un sur-corps du corps $k\bar{k} = k_1$.

Remarquons qu'il suffit évidemment de démontrer que K est relativement abélien quand K est cyclique par rapport à k, car tout corps abélien est composé de corps cycliques. Nous supposons donc K cyclique par rapport à k. $\tau^i K$ désignant un conjugué de K par rapport à k^*, $\tau^i K$ sera corps de classes sur k pour le groupe $\tau^i H$ déduit de H par l'application de l'automorphisme τ^i de k. Or $\tau^i H = H$, donc, en vertu du théorème d'unicité, $\tau^i K = K$: K est galoisien par rapport à k^*, et même métacyclique. Soit H^* le groupe associé à K dans k^*, et soit A^* le groupe des nombres $\neq 0$ de k^*. Soit α un nombre de k tel que $N_{kk^*}(\alpha)$ soit dans H^*. Donc $N_{kk^*}(\alpha) = N_{kk^*}(A)$, A étant un nombre de K. Donc

$$\alpha = N_{Kk}(A)\beta,$$

où $N_{kk^*}(\beta) = 1$, d'où $\beta = \gamma^{1-\tau}$; donc β est dans H, et par suite aussi α. Donc H est le groupe des nombres de k dont la norme par rapport à k^* est dans H^*. Donc (principe d'isomorphie), h étant le groupe associé à k dans k^* (qui contient H^*), on a

$$(A : H) = (h : [h, H^*]) = (h : H^*)$$

et en tenant compte de ce que k est par rapport à k^* cyclique, et par suite aussi corps de classes,

$$(A^* : H^*) = (A^* : h)(h : H^*) = (k : k^*)(K : k) = (K : k^*),$$

ce qui démontre que K est corps de classes par rapport à k^*.

Donc K est corps de classes par rapport à k_1 pour le groupe H_1 des nombres de k_1 dont la norme par rapport à k^* est dans H^* (voir p. 452). D'ailleurs K est cyclique par rapport à k_1. Enfin il y a un automorphisme de k_1 par rapport à k^* prolongeant τ. Nous le désignerons encore par τ. K est complètement ramifié par rapport à $\bar{k}$, donc aussi par rapport à k_1.

Soit $(K : k_1) = n$ et soit K' le sur-corps non-ramifié de k_1 de degré relatif n. Reprenons les notations et les résultats de la démonstration du lemme de la p. 453; k_1 jouant le rôle que jouait k. Remarquons que

$$\varpi = \Omega \,.\, \sigma'\Omega \,.\, \ldots \,.\, \sigma'^{n-1}\Omega,$$

Ω étant un nombre tel que $\sigma\sigma'\Omega = \Omega$. Or KK' étant galoisien par rapport à k^*, τ peut être considéré comme un automorphisme de KK' par rapport à k^*. K' étant évidemment abélien par rapport à k^* (il

résulte de la composition de k et d'un corps non ramifié par rapport à k^*) τ est permutable avec σ'. K étant galoisien par rapport à k^*, on a $\tau\sigma\tau^{-1} = \sigma^a$, $(a, n) = 1$. Or

$$\varpi^\tau = \tau\Omega . \sigma'\tau\Omega . \ldots . \sigma'^{n-1}\tau\Omega$$

et $\tau\sigma\sigma'\tau^{-1} \cdot \tau\Omega = \tau\Omega$; donc ϖ^τ est norme d'un nombre du sous-corps K_1 de KK' appartenant au groupe $(\tau\sigma\sigma'\tau^{-1}) = (\sigma^a\sigma')$. Or $\varpi^{1-\tau}$ appartient aux groupes associés à K et à K' dans k_1[36]. Donc $\varpi^{1-\tau}$ est norme par rapport à k_1 d'un nombre de K_1, qui est sous-corps de KK', cyclique par rapport à k (voir p. 453). ϖ^τ et $\varpi^{1-\tau}$ étant normes chacun d'un nombre de K_1, il en est de même de ϖ. ϖ est donc norme par rapport à k_1 d'un nombre de K_1 et d'un nombre de K'' (on rappelle que K'' est le sous-corps de KK' appartenant au groupe $(\sigma\sigma')$). Considérons le corps K_1K'' : il appartient dans KK' au groupe partie commune des groupes $(\sigma\sigma')$ et $(\sigma^a\sigma')$. Soit α le plus petit nombre positif tel que $\alpha(a-1) \equiv 0 \pmod{n}$: cette partie commune est le groupe $(\sigma^a\sigma'^a)$. Le corps K_1K'' contient donc le sous-corps K_a de K qui appartient au sous-groupe (σ^a) du groupe de K par rapport à k_1. Donc ϖ est norme par rapport à k_1 d'un nombre de K_a, et $\varpi^{\frac{n}{a}}$ est norme par rapport à k_1 d'un nombre de K. Ce qui n'est possible que si $\alpha = 1$ donc $a \equiv 1 \pmod{n}$, donc $\sigma^a = 1$, $\tau\sigma = \sigma\tau$.

Il en résulte que K est abélien par rapport au sous-corps de k_1 formé des éléments invariants par τ, sous-corps qui est contenu dans $\bar{k}$. Donc K est abélien par rapport à $\bar{k}$, et complètement ramifié. Donc K est composé de corps cycliques et complètement ramifiés par rapport à $\bar{k}$. Il suffit maintenant pour chacun de ces corps de refaire le raisonnement précédent en remplaçant k_1 par $\bar{k}$, τ par un automorphisme primitif de $\bar{k}$ par rapport à k^* : chacun de ces sur-corps cycliques sera abélien par rapport à k^*, donc aussi K.

Enfin pour démontrer que K, dans le cas général où il n'est pas cyclique par rapport à k, est corps de classes par rapport à k^*, il suffit de reprendre le raisonnement du début de notre démonstration.

On remarquera que la condition que H contienne tous les nombres $\alpha^{1-\tau}$ est équivalente à la suivante : H contient tous les nombres de k dont la norme par rapport à k^* est 1.

---

36) $\varpi^{1-\tau}$, qui est, en vertu de sa forme même, de norme 1 par rapport à k^*, est dans le groupe H_1, pour lequel K est corps de classes sur k_1. Il appartient au groupe associé à K' parce que K' étant non-ramifié, est corps de classes sur k_1 pour le groupe des nombres de k_1 d'ordre multiple de $(K' : k)$, auquel appartient $\varpi^{1-\tau}$, qui est une unité.

Théorème d'existence. Corps cycliques de degré premier.

Soit k un corps local. Soit dans le groupe A des nombres $\neq 0$ de k, H un sous-groupe d'indice l premier. Il y a un sur-corps K de k corps de classes pour H.

1er cas. k contient les racines l-èmes. de l'unité.

Dans ce cas, les corps K_i relativement cycliques de degré l par rapport à k sont de la forme $k(\sqrt[l]{\alpha})$, α étant un nombre $\neq 0$ de k. Soit K le corps composé de tous les K_i. Le nombre $(K:k)$ est égal à $(\alpha:\alpha^l)$ qui est un nombre fini (voir p. 418), et le groupe de Galois de K par rapport à k est produit direct de groupes d'ordre l, donc isomorphe à α/α^l. Le nombre des corps K_i est le nombre des sous-groupes d'indice l du groupe de Galois, donc aussi le nombre des sous-groupes d'indice l du groupe des α, car tout sous-groupe d'indice l contient nécessairement le groupe α^l. Or chacun des corps K_i est corps de classes pour un de ces sous-groupes, et deux corps distincts sont corps de classes pour des sous-groupes distincts. Il en résulte que pour chaque sous-groupe, il y a un corps de classes.

2me cas. k ne contient pas les racines l-èmes. de l'unité. Soit $\bar{k}$ le corps déduit de k par adjonction des racines l-èmes. de l'unité. $\bar{k}$ est un sur-corps relativement cyclique de k. Son groupe de Galois est engendré par une opération τ dont l'ordre a divise $l-1$. Soient H^* le groupe associé à $\bar{k}$ dans k, $\bar{H}$ le groupe des nombres de $\bar{k}$ dont les normes relatives par rapport à k sont dans H, $\bar{A}$ le groupe des nombres $\neq 0$ de $\bar{k}$. En vertu du principe d'isomorphie, on a

$$(\bar{A}:\bar{H}) = (H^*:[H,H^*]) = (HH^*:H).$$

Or les nombres $(A:H)$, $(A:H^*)$ étant premiers entre eux, on a $HH^* = A$, donc $(\bar{A}:\bar{H}) = l$. Il existe donc un corps $\bar{K}$ corps de classes sur $\bar{k}$ pour le groupe $\bar{H}$. α étant un nombre quelconque de $\bar{k}$, le nombre $\alpha^{1-\tau}$ appartient à $\bar{H}$. Donc $\bar{K}$ est abélien de degré al par rapport à k. La norme par rapport à k d'un nombre de $\bar{K}$ est évidemment dans H et dans H^*, donc le groupe associé à $\bar{K}$ dans k est contenu dans $[H,H^*]$. Mais ce dernier groupe est d'indice al dans A, donc est le groupe associé à $\bar{K}$ (ce groupe associé étant aussi d'indice al). Or $\bar{K}$ contient un sous-corps K relativement cyclique d'ordre l par rapport à k. Le corps K est corps de classes sur k pour un groupe d'indice l dans A qui contient $[H,H^*]$. Il n'y a qu'un tel groupe et c'est H.

Théorème réciproque.

Nous sommes maintenant en mesure de préciser les énoncés du paragraphe 4.

1) *k étant un corps local, A le groupe des nombres $\neq 0$ de k, K un sur-corps relativement cyclique de degré n, H le groupe associé à K, A/H est cyclique.*

Le théorème est vrai si K est complètement ramifié (voir p. 453) ou si K est non ramifié. H est en effet alors le groupe des nombres dont l'ordre est multiple de n (voir p. 423). Soit maintenant un sur-corps K relativement cyclique quelconque et soit K_T le corps d'inertie de l'idéal premier de k dans K. Supposons A/H non cyclique, et soit H_T le groupe associé à K_T dans k. Le groupe A/H_T est cyclique, car K_T est sur-corps non ramifié de k. Il y a donc un groupe H' contenant H mais non H_T, d'indice premier l dans A.[37] Il y a un corps K' relativement cyclique par rapport à k et corps de classes pour H' (voir p. 457). Soit $\bar{H}'$ le groupe des nombres de K_T dont la norme par rapport à k tombe dans H', et soit A_T le groupe des nombres différents de 0 de K_T. On a $(A_T : \bar{H}') = (H_T : [H_T, H']) = l$. D'autre part la norme par rapport à K_T d'un nombre de $K'K_T$ est dans $\bar{H}'$. Donc $K'K_T$ est corps de classes sur K_T pour le groupe $\bar{H}'$; mais K est corps de classes sur K_T pour le groupe $\bar{H}''$ des nombres de K_T dont la norme par rapport à k est dans H; comme K est complètement ramifié par rapport à K_T, $A_T/\bar{H}''$ est cyclique; donc il n'y a qu'un groupe contenant $\bar{H}''$ et d'indice l dans A_T. Ce groupe est $\bar{H}'$. Or K contient un corps de degré relatif l par rapport à K_T, car $(K : K_T) = (H_T : H)$ est divisible par l par suite de l'existence de H'; ce corps est corps de classes pour un sous-groupe d'indice l de A_T contenant $\bar{H}''$, donc pour $\bar{H}'$. Ce corps est donc $K'K_T$. Donc $K'K_T$ est contenu dans K, qui ne peut donc être cyclique.

2) *Soient k un corps local, A le groupe des nombres différents de 0 de k, K un sur-corps relativement abélien de k, H le groupe associé à K dans k. Le groupe A/H est isomorphe au groupe de Galois de K par rapport à k. Il en résulte que K est corps de classes par rapport à k.*

En effet le théorème est démontré pour tous les corps K relativement

37) En effet, si pour chaque diviseur premier l de $(A:H)$ un sous-groupe de A/H d'indice l contenait nécessairement H_T/H, il n'y aurait pour chaque l qu'un tel sous-groupe, et A/H serait cyclique.

cycliques. Supposons le démontré pour tous les corps composés de r corps cycliques au plus. Remarquons d'abord qu'il en résulte que, H^* désignant un groupe contenant H et tel que A/H^* soit cyclique, K contient un corps de classes pour H^*. En effet, le nombre des groupes H^* est égal au nombre des sous-groupes à quotient cyclique du groupe de Galois de K, donc au nombre des sous-corps K^* de K qui sont cycliques par rapport à k. Or chacun de ces corps est corps de classes pour un groupe H^* et plusieurs K^* ne peuvent être corps de classes pour le même H^*, ce qui démontre la proposition.

Ceci posé, un sur-corps relativement abélien composé de $r+1$ corps cycliques se met sous la formé KK_1, K étant composé de r corps cycliques, K_1 étant cyclique. De plus on peut supposer K et K_1 étrangers par rapport à k. Soient H, H_1 les groupe associés à K, K_1 dans k. Je dis que $H^* = HH_1$ est égal à A. En effet A/H_1 est cyclique, donc aussi A/H^*. H^* contenant H et H_1, il résulte de la remarque précédente que dans K et K_1 on peut trouver des corps de classes pour H^*. Ces corps de classes doivent être identiques, et, puisque K et K_1 sont étrangers, ils se réduisent à k. Donc $H^* = A$. Il en résulte que $A/[H, H_1]$ est isomorphe au produit direct de A/H et de A/H_1, donc aussi au produit direct des groupes de Galois de K, K_1 par rapport à k, donc encore au groupe de Galois de KK_1 par rapport à k. D'autre part, la norme par rapport à k d'un nombre de KK_1 étant dans H et dans H_1, KK_1 est corps de classes pour $[H, H_1]$[35].

3) **Théorème d'Unicité**: *Soient k un corps local, K, K' deux sur-corps relativement abéliens de k, corps de classes pour les groupes H, H'. Si $H \supset H'$, on a $K \subset K'$ et réciproquement.*

En effet K est composé de corps K_i cycliques par rapport à k. Soient H_i les groupes associés à ces corps K_i. A désignant le groupe des nombres différents de 0 de k, on a vu que le groupe de Galois de K' par rapport à k est isomorphe à A/H', et qu'il en résulte que, pour tout groupe contenant H' et à quotient cyclique dans A, K' contient un corps de classes: en particulier pour les H_i. Mais en vertu du théorème d'unicité pour les corps cycliques, il en résulte que K_i est dans K', donc $K \subset K'$. Il en résulte: *Si K, K' sont des corps relativement abéliens, corps de classes pour les groupes H, H', KK' est corps de classes pour $[H, H']$ et $[K, K']$ est corps de classes pour HH'.*

4) **Théorème d'Existence**: *Soient k un corps local, A le groupe des nombres différents de 0 de k, H un sous-groupe d'indice fini de A. Il existe*

un corps K, relativement abélien par rapport à k et corps de classes sur k pour le groupe H.

En effet soit $(A : H) = n$. Le théorème est démontré quand n est premier (voir p. 457). Supposons le démontré pour toutes les valeurs de l'indice $< n$. Choisissons un groupe H_1 contenant H et d'indice l dans A, l premier. Soient $\bar{K}$ le corps de classes sur k pour H_1, $\bar{A}$ le groupe des nombres $\neq 0$ de $\bar{K}$, $\bar{H}$ le groupe des nombres de $\bar{K}$ dont la norme par rapport à k est dans H. On a (principe d'isomorphie) $(\bar{A} : \bar{H}) = \frac{n}{l}$. Donc par hypothèse, il existe un corps K abélien par rapport à $\bar{K}$ et corps de classes sur $\bar{K}$ pour le groupe $\bar{H}$. Or $\bar{K}$ est cyclique par rapport à k et $\bar{H}$ contient évidemment tous les nombres de $\bar{K}$ de norme relative 1 par rapport à k. Donc (voir p. 454) K est abélien par rapport à k et corps de classes pour son groupe associé, qui est, comme il résulte de la démonstration de la p. 454, le groupe des normes relatives des nombres de $\bar{H}$, donc H.

Extensions locales quelconques.

Nous nous proposons de démontrer le théorème suivant :

Soient k un corps local, K un sur-corps relativement abélien de k, corps de classes pour le groupe H de k ; $\bar{k}$ une extension finie quelconque de k. Le corps $K\bar{k}$ est corps de classes sur $\bar{k}$ pour le groupe $\bar{H}$ des nombre de $\bar{k}$ dont la norme par rapport à k tombe dans H.

1) Supposons d'abord $\bar{k}$ galoisien par rapport à k. Comme nous l'avons déja dit[9] on démontre que $\bar{k}$ est métacyclique par rapport à k. Nous dirons que l'extension $\bar{k}$ de k est n-métacyclique s'il existe une suite de corps k_i $(i = 0, 1, \ldots, n)$ avec $k_0 = k$, $k_n = \bar{k}$, k_i étant sur-corps relativement cyclique de k_{i-1}. Nous procèderons par récurrence sur n.

a) Si $n = 1$, $\bar{k}$ est cyclique sur k, $K\bar{k}$ est relativement abélien, donc corps de classes par rapport à k, et le théorème résulte de celui de la p. 452.

b) Supposons le théorème démontré pour toutes les extensions $(n-1)$-métacycliques. Il existe un sous-corps k^* de $\bar{k}$ tel que k^* soit $(n-1)$-métacyclique par rapport à k et que $\bar{k}$ soit cyclique par rapport à k^*. Le corps Kk^* est corps de classes sur k^* pour le groupe H^* des nombres de k^* dont la norme par rapport à k tombe dans H. Or

$K\bar{k} = Kk^* \bar{k}$ est corps de classes sur $\bar{k}$ pour le groupe des nombres de $\bar{k}$ dont la norme par rapport à k^* tombe dans H^*. Ce groupe est précisément $\bar{H}$.

2) Pour démontrer le théorème dans le cas général, nous démontrerons d'abord le cas particulier suivant :

Soient k un corps local, K une extension finie de k, H le groupe associé à K dans k. Le groupe H est le groupe associé dans k au plus grand corps abélien par rapport à k et contenu dans K.

Cet énoncé se déduit de l'énoncé général donné plus haut en faisant jouer à K le rôle que jouait $\bar{k}$, et au plus grand sous-corps de K abélien par rapport à k le rôle que jouait K. D'après la I^re^ partie de la démonstration, ce théorème est vrai quand K est relativement galoisien par rapport à k. Dans le cas général, nous désignerons par K^* un sur-corps relativement galoisien de k contenant K, par G le groupe de Galois de K^*, par g le groupe auquel appartient K.

a) Si le théorème est démontré dans le cas où l'ordre de g est de la forme p^a, p premier, il est démontré dans le cas général. Soit en effet $n = \Pi p_i^{a_i}$ l'ordre de g. On démontre (voir par exemple Speiser, Theorie der Gruppen von endlicher Ordnung, p. 65) que l'on peut, pour chaque p_i choisir un sous-groupe de g d'ordre $p_i^{\alpha_i}$, appelé groupe de Sylow. Soit g_i le groupe ainsi obtenu, et soit K_i le sous-corps de K^* appartenant à ce groupe. Soit H_i le groupe associé à K_i dans k. Chacun des H_i est contenu dans H, donc il en est de même de leur groupe composé $H_1 H_2 \cdots H_r$. Par hypothèse, H_i est le groupe associé au plus grand corps $\bar{K}_i$ contenu dans K_i et abélien par rapport à k. Donc $H_1 H_2 \cdots H_r$ est le groupe associé à $[\bar{K}_1, \bar{K}_2, \cdots, \bar{K}_r] = \bar{K}$.

Or le groupe composé des g_i est le groupe g. En effet ce groupe est contenu dans g et son ordre est divisible par tous les $p_i^{\alpha_i}$. Donc K est la partie commune des K_i, et $\bar{K}$ est contenu dans K. Je dis que c'est le corps maximum contenu dans K et abélien par rapport à k. Supposons en effet qu'il y ait un corps K' contenant $\bar{K}$ comme sous-corps, contenu dans K et abélien par rapport à k. Donc K' doit être contenu dans chacun des K_i, et par suite des $\bar{K}_i$, donc aussi dans $\bar{K}$. On a vu que H contient le groupe associé à $\bar{K}$; $\bar{K}$ étant contenu dans K, H est aussi contenu dans ce groupe, et par suite lui est identique.

b) Si le théorème est démontré pour un corps K, il est aussi démontré pour un corps K', relativement cyclique de degré premier p par rapport à K. En effet, soient H, H' les groupes associés à K, K',

dans k, $\bar{A}$ le groupe des nombres différents de 0 de K, $\bar{H}$ le groupe associé à K' dans K, $\bar{H}^*$ le groupe des nombres de K dont la norme par rapport à k est dans H'. On a :

$$(\bar{A}: \bar{H}^*) = (H: H')$$

$$\bar{H}^* \supset \bar{H}, \qquad (\bar{A}: \bar{H}) \text{ divise } p.$$

Donc $(H: H')$ est égal à 1 ou à p. Soit $\bar{K}'$ le corps relativement abélien par rapport à k corps de classes pour H', et soit $\bar{K}$ le corps relativement abélien maximum contenu dans K, donc corps de classes sur k pour le groupe H. On a : $(\bar{K}': \bar{K}) = 1$ ou p. Donc, $(K\bar{K}': K) = 1$ ou p. Si $(K\bar{K}': K) = 1$, il faut que $\bar{K}'$ soit contenu dans K, donc soit identique à $\bar{K}$, et on a $H = H'$: la proposition est vraie dans ce cas. Si $(K\bar{K}': K) = p$, on a $(\bar{A}: \bar{H}) = (H: H') = p$, donc $\bar{H} = \bar{H}^*$. Le corps $K\bar{K}'$ est corps de classes sur K pour un groupe qui est certainement contenu dans $\bar{H}^*$ et qui est d'indice p dans $\bar{A}$. Ce groupe est $\bar{H}^*$, et, en vertu du théorème d'unicité, $K\bar{K}' = K'$. Donc $\bar{K}'$ est contenu dans K' et est corps relativement abélien maximum contenu dans K'. La proposition est encore démontrée dans ce cas.

c) Ceci permet de se ramener au cas où g est un groupe de Sylow de G. En effet, on démontre (voir par exemple Speiser, Theorie der Gruppen von endlicher Ordnung p. 80) que g étant un groupe d'ordre p^a, contenu dans un groupe de Sylow $\bar{g}$ de G, il existe une suite de groupes $g_0 = g, g_1, g_2, \cdots, g_r = \bar{g}$ telle que g_i contienne g_{i-1} comme sous-groupe invariant d'indice p. Soit K_i le sous-corps de K^* appartenant au groupe g_i. K_{i-1} contient K_i, par rapport auquel il est relativement cyclique de degré p. Il suffit d'appliquer plusieurs fois le raisonnement de b).

d) Supposons donc que g soit un groupe de Sylow d'ordre p^a de G. Soient H, H^* les groupes associés à K, K^* dans k, $\bar{A}$ le groupe des nombres différents de 0 de K, $\bar{H}^*$ le groupe des nombres de K dont la norme par rappor à k est dans H^*. Ecrivons :

$$(A: H^*) = (A: H)(H: H^*) = (A: H)(\bar{A}: \bar{H}^*).$$

Or $\bar{H}^*$ contient le groupe $\bar{H}$ associé à K^* dans K. Comme $(K^*: K) = p^a$, la puissance p^a-ième de tout nombre de K est dans $\bar{H}$. Donc $(\bar{A}: \bar{H}^*)$ est une puissance de p. Au contraire, si n est l'ordre de G, la puissance

$\frac{n}{p^a}$-ième de tout nombre de A est dans H: donc $(A:H)$ est premier à p, et est par suite le plus grand diviseur n^* de $(A:H^*)$ premier à p. Mais $(A:H^*)$ est le degré relatif par rapport à k du corps $\bar{K}^*$ maximum contenu dans K^* et abélien par rapport à k. n^* est le degré du plus grand sous-corps $\bar{K}$ de $\bar{K}^*$ dont le degré par rapport à k est premier à p. Or $K\bar{K}$ est contenu dans K^*. Comme $(K\bar{K}:K)$ est premier à p, et $(K^*:K)=p^a$, il faut que $K\bar{K}=K$, donc que $\bar{K}$ soit contenu dans K. Soit H' le groupe associé à $\bar{K}$ dans k: on a $H'\supset H$ et $(A:H')=(A:H)=n^*$, donc $H'=H$. Si K contenait un corps $\bar{K}'$ abélien par rapport à k et plus grand que $\bar{K}$, H devrait être contenu dans le groupe associé à ce corps, ce qui est impossible. Le lemme intermédiaire est donc complètement démontré.

e) Revenons aux notations de l'énoncé du théorème, et soient $\bar{A}$ le groupe des nombres différents de 0 de $\bar{k}$, h le groupe associé à $\bar{k}$ dans k. On a

$$(\bar{A}:\bar{H})=(h:[H,h])=(hH:H)=\frac{(A:H)}{(A:hH)}.$$

Soit k^* le plus grand corps contenu dans $\bar{k}$ et abélien par rapport à k. Donc k^* est corps de classes pour le groupe h, et $[K,k^*]$ est corps de classes sur k pour le groupe hH. Donc,

$$(A:hH)=([K,k^*]:k).$$

Mais $[K,k^*]=[K,\bar{k}]$. En effet, il est évident que $[K,k^*]\subset[K,\bar{k}]$. D'autre part $[K,\bar{k}]$ est un sous-corps de $\bar{k}$ abélien par rapport à k^*, donc contenu dans k^*, et dans K. Donc, $[K,\bar{k}]\subset[K,k^*]$, ce qui démontre l'égalité. Donc, puisque $(A:H)=(K:k)$,

$$(\bar{A}:\bar{H})=\frac{(K:k)}{([K,\bar{k}]:k)}=(K:[K,\bar{k}])=(K\bar{k}:\bar{k}).$$

Soit $\bar{H}'$ le groupe associé à $K\bar{k}$ dans $\bar{k}$. Comme $K\bar{k}$ est abélien par rapport à $\bar{k}$, on a

$(\bar{A}:\bar{H}')=(K\bar{k}:\bar{k})=(\bar{A}:\bar{H})$ et il est clair que $\bar{H}'\subset\bar{H}$. Donc $\bar{H}'=\bar{H}$, ce qui démontre le théorème.

De ce théorème résulte en particulier que: *Si k est un corps local, si K est un sur-corps de k qui est corps de classes sur k, K est relativement abélien par rapport à k.*

Application aux restes normiques.

Soit k un corps fini de nombres algébriques, et soit K une extension finie, relativement galoisienne de k. Soit $\mathfrak{p}$ un idéal premier de k, et soit $\mathfrak{P}$ un facteur premier de $\mathfrak{p}$ dans K. La condition nécessaire et suffisante pour qu'un nombre α de k soit, quel que soit n, reste normique de K (mod. $\mathfrak{p}^n$) est que α, considéré comme nombre de $k_\mathfrak{p}$, soit norme relative par rapport à $k_\mathfrak{p}$ d'un nombre de $K_\mathfrak{P}$ (voir p. 419). Mais pour cela il faut et il suffit que α soit norme par rapport à $k_\mathfrak{p}$ d'un nombre du corps $\bar{K}$ maximum contenu dans $K_\mathfrak{P}$ et abélien sur $k_\mathfrak{p}$. Or soit G_Z le groupe de décomposition de $\mathfrak{P}$ dans l'extension K de k. G_Z peut encore être considéré comme groupe de Galois de $K_\mathfrak{P}$ par rapport à $k_\mathfrak{p}$. Le corps $\bar{K}$ appartient à un sous-groupe g de G_Z. Soit K^* le sous-corps de K qui appartient au groupe g. K^* est le plus grand corps contenu entre K_Z (corps de décomposition de $\mathfrak{P}$) et K, et abélien par rapport à K_Z. Soit $\mathfrak{P}^*$ l'idéal premier de ce corps divisible par $\mathfrak{P}$. Le corps $\bar{K}$ est le corps des nombres $\mathfrak{P}^*$-adiques de K^*. Par suite :

La condition nécessaire et suffisante pour que α soit, quel que soit n, reste normique de K (mod. $\mathfrak{p}^n$) *est que α soit, pour les mêmes modules, reste normique de K^*.*

Chapitre X.

Le Théorème d'Existence.

Nombres Primaires et Hyperprimaires.

Soit k un corps fini de nombres algébriques contenant les racines n-èmes. de l'unité, et soit dans k $\mathfrak{p}$ un idéal premier fini ou infini.

1) Un nombre $\alpha \neq 0$ de k est dit *hyperprimaire* pour $\mathfrak{p}$ quand $\mathfrak{p}$ est complètement décomposé dans $k(\sqrt[n]{\alpha})$.

2) Un nombre $\alpha \neq 0$ de k est dit *primaire* pour $\mathfrak{p}$ quand $\mathfrak{p}$ est non-ramifié dans $k(\sqrt[n]{\alpha})$.

Si $\mathfrak{p}$ est un idéal premier infini, les deux notions coincident. Remarquons d'ailleurs que le cas ne se présente que pour $n = 2$, car sinon k et tous ses conjugués sont imaginaires. Si $n = 2$, soit $k^{(1)}$ le conjugué de k auquel appartient $\mathfrak{p}$. La condition nécessaire et suffisante pour que α soit hyperprimaire (ou primaire) pour $\mathfrak{p}$ est que le conjugué $\alpha^{(1)}$ de α dans $k^{(1)}$ soit positif. Donc: *si $\mathfrak{p}$ est un idéal premier infini, les nombres hyperprimaires pour $\mathfrak{p}$ forment, dans le groupe des nombres $\neq 0$ de k un sous-groupe d'indice* 2.

Supposons maintenant $\mathfrak{p}$ fini, et soit $k_\mathfrak{p}$ le corps des nombres $\mathfrak{p}$-adiques de k. La condition nécessaire et suffisante pour qu'un nombre α de k soit hyperprimaire pour $\mathfrak{p}$ est que $k_\mathfrak{p}(\sqrt[n]{\alpha}) = k_\mathfrak{p}$ (car le groupe de décomposition de $\mathfrak{p}$ dans l'extension $k(\sqrt[n]{\alpha})$ de k se réduit à 1), donc que α soit une puissance n-ème. d'un nombre de $k_\mathfrak{p}$. Mais on a vu p. 418 qu'il existe une puissance $\mathfrak{p}^\chi$ de $\mathfrak{p}$ telle que tout nombre de $k \equiv 1 \pmod{\mathfrak{p}^\chi}$ soit hyperprimaire. Le nombre χ étant choisi minimum, l'idéal $\mathfrak{p}^\chi$ s'appelle *module d'hyperprimarité* pour $\mathfrak{p}$. α désignant les nombres $\neq 0$ de k, α_0 les nombres hyperprimaires pour $\mathfrak{p}$, A les nombres $\neq 0$ de $k_\mathfrak{p}$, on a

$$(\alpha : \alpha_0) = (A ; A^n).$$

Nous allons calculer cet indice au moyen du lemme d'Herbrand, appliqué avec les conventions suivantes (voir pour les notations l'énoncé du lemme de Herbrand):

G: groupe des A; g groupe des nombres $B \equiv 1 \pmod{\mathfrak{p}^a}$ a étant un exposant que nous déterminerons;

T_1 automorphisme défini par $A \longrightarrow A^n$; T_2 automophisme défini par $A \longrightarrow 1$.

Le groupe γ_1 est composé des racines n-èmes. de l'unité. Donc γ_1 est d'ordre n fini. On a $\gamma_2 = G$, donc $([g, \gamma_2] : T_1 g) = (g : T_1 g)$. Cet indice

est fini, car on peut choisir un exposant a' tel que si Γ est un nombre $\equiv 1$ (mod. $\mathfrak{p}^{a'}$) on ait $\frac{1}{n}\operatorname{Log}\Gamma \equiv 0$ (mod. $\mathfrak{p}^a$), donc $\Gamma = B^n$, donc $T_1 g$ contient le groupe des nombres $\equiv 1$ (mod. $\mathfrak{p}^{a'}$). Ceci posé, le lemme d'Herbrand donne

$$\frac{n}{(A : A^n)} = \frac{([g, \gamma_1])}{(g : T_1 g)}.$$

On peut choisir a assez grand pour que 1) g ne contienne aucune racine n-ème. de l'unité $\neq 1, 2$) le groupe g soit isomorphe au groupe additif des entiers Γ de $k_\mathfrak{p}$ qui sont $\equiv 0$ (mod. $\mathfrak{p}^a$), l'isomorphie étant établie par la formule $\Gamma = \operatorname{Log} B$. Ceci fait, dans l'isomorphie précédente le groupe $T_1 g$ correspond au groupe additif des $n\Gamma$, et on a

$$(A : A^n) = n(\Gamma : n\Gamma).$$

Or soit Π un nombre de $k_\mathfrak{p}$ tel que $(\Pi) = \mathfrak{p}$, et désignons par Δ les entiers de $k_\mathfrak{p}$. On a

$$(\Gamma : n\Gamma) = (\Pi^a \Delta : n\Pi^a \Delta) = (\Delta : n\Delta).$$

Ce nombre est par définition la norme de l'idéal (n) de $k_\mathfrak{p}$. Si $\mathfrak{p}^{E_\mathfrak{p}}$ est la contribution de $\mathfrak{p}$ à (n), on a

$$(\alpha : \alpha_0) = (A : A^n) = nN(\mathfrak{p}^{E_\mathfrak{p}}),$$

le symbole N désignant la norme absolue, c'est-à-dire par rapport au corps des nombres rationnels.

On ne connait pas dans le cas le plus général de condition nécessaire et suffisante pour que α soit primaire pour $\mathfrak{p}$. Mais :

1) *Pour que α soit primaire ponr $\mathfrak{p}$, il est nécessaire que l'ordre de α pour $\mathfrak{p}$ soit multiple de n.*

En effet, soit $\mathfrak{P}$ un facteur premier de $\mathfrak{p}$ dans $k(\sqrt[n]{\alpha})$. Si $\mathfrak{P}$ figure dans $\sqrt[n]{\alpha}$ avec l'exposant μ, et si $\mathfrak{p}$ n'est pas ramifié, $\mathfrak{p}$ figure dans α avec l'exposant $n\mu$.

2) *Si $\mathfrak{p}$ ne divise pas n, la condition précédente est suffisante.*

En effet, supposons la réalisée. On peut, en multipliant α par la puissance n-ème. d'un nombre de k, ce qui ne change pas $k(\sqrt[n]{\alpha})$, le transformer en un nombre β entier et non divisible par $\mathfrak{p}$. La différente relative du nombre $\sqrt[n]{\beta}$, racine de l'équation $x^n - \beta = 0$ est $n\beta^{n-1}$ qui n'est pas divisible par $\mathfrak{p}$. Donc $\mathfrak{p}$ n'est pas ramifié.[38]

38) La différente relative de $\sqrt[n]{\beta}$ est le produit de $(\sqrt[n]{\beta} - \sigma\sqrt[n]{\beta})$, σ parcourant les opérations $\neq 1$ du groupe de Galois. *Si le groupe d'inertie de $\mathfrak{p}$ était $\neq 1$, σ étant une* opération de ce groupe et $\sqrt[n]{\beta}$ un entier, $\sqrt[n]{\beta} - \sigma\sqrt[n]{\beta}$ serait divisible par $\mathfrak{p}$.

Réduction.

Soit k un corps fini de nombres algébriques. Donnons nous dans k un groupe de congruence H quelconque définissable suivant un module $\mathfrak{m}$. Le problème du théorème d'existence est de démontrer qu'il existe un corps de classes K sur k pour H.

Désignons par n le plus petit exposant positif tel que la puissance n-ème. de tout idéal de k premier à $\mathfrak{m}$ soit dans H, et par ζ une racine primitive n-ème. de l'unité. Soit $\bar{H}$ le groupe des idéaux premiers à $\mathfrak{m}$ de $k(\zeta)$ dont la norme par rapport à k est dans H. La puissance n-ème. de tout ideal de $k(\zeta)$ premier à $\mathfrak{m}$ est dans $\bar{H}$. Supposons maintenant qu'il existe un corps de classes sur $k(\zeta)$ pour $\bar{H}$, soit $\bar{K}$. Nous nous proposons de démontrer qu'il existe aussi un corps de classes sur k pour le groupe H. Pour cela, nous allons prouver le lemme suivant, analogue à celui dont nous nous sommes servis dans la théorie du corps de classes local (voir p. 454):

Soient k un corps fini de nombres algébriques, K un sur-corps relativement abélien de k corps de classes sur k pour le groupe H. Soient g un groupe abélien d'automorphismes de k, et k^* le corps des nombres invariants par les opérations τ de g. Si H contient tous les idéaux $\mathfrak{a}^{1-\tau}$, $\mathfrak{a}$ étant un idéal de k premier à un module de définition $\mathfrak{m}$ de H, K est abélien par rapport à k^*.

En effet, tout d'abord H est invariant par les opérations τ, donc, en vertu du théorème d'unicité (p. 448) K coincide avec ses conjugués relatifs par rapport à k. On peut donc considérer les τ comme des automorphismes de K par rapport à k. Soit σ une opération quelconque du groupe de Galois de K par rapport à k, et soit $\mathfrak{a}$ un idéal de k tel que

$$(\mathfrak{a}, \mathfrak{m}) = 1, \qquad \left(\frac{K}{\mathfrak{a}}\right) = \sigma.$$

Donc $\mathfrak{a}$ est premier au discriminant relatif de K par rapport à k. Il en est de même de $\tau\mathfrak{a}$. Montrons que

$$\left(\frac{K}{\tau\mathfrak{a}}\right) = \tau\sigma\tau^{-1}.$$

Il suffit de démontrer la formule dans le cas où $\mathfrak{a}$ est un idéal premier $\mathfrak{p}$. Mais alors σ est défini par la condition que pour tout entier A de K on ait

$$\sigma A \equiv A^{N\mathfrak{p}} \qquad (\mathrm{mod}^{*}\ \mathfrak{p}),$$

d' où

$$\tau\sigma\tau^{-1}\tau A \equiv (\tau A)^{N\mathfrak{p}} \qquad (\mathrm{mod}^{*}\ \tau\mathfrak{p}).$$

ce qui prouve que $\left(\frac{K}{\tau\mathfrak{p}}\right) = \tau\left(\frac{K}{\mathfrak{p}}\right)\tau^{-1}$.

Ceci posé, de la condition $\mathfrak{a}^{1-\tau} \subset H$, on déduit

$$\left(\frac{K}{\mathfrak{a}}\right) = \left(\frac{K}{\tau\mathfrak{a}}\right),$$

d' où $\tau\sigma\tau^{-1} = \sigma$: chaque τ est permutable avec chaque σ, ce qui démontre le lemme.

Revenons aux notations du début de notre paragraphe. τ étant un automorphisme de $k(\zeta)$ par rapport à k, $\mathfrak{a}$ un idéal de $k(\zeta)$ premier à $\mathfrak{m}$, $\bar{H}$ contient $\mathfrak{a}^{1-\tau}$, car $\mathfrak{a}^{1-\tau}$ est de norme relative 1 par rapport à k. Donc $\bar{K}$ est un sur-corps relativement abélien de k, corps de classes sur k pour un groupe H'. H' est évidemment contenu dans un groupe égal à H, car les normes relatives d'idéaux de K' premiers à $\mathfrak{m}$ sont dans H, et on a vu (p. 447) que dans ces conditions $\bar{K}$ contient un sous-corps qui est corps de classes sur k pour le groupe H.

Théorème d'Existence.

La réduction du paragraphe II nous a montré qu'il suffit, pour démontrer le théorème d'existence, de démontrer le théorème suivant :

k étant un corps de nombres algébriques contenant les racines n-èmes. de l'unité ;

H étant dans k un groupe de congruence définissable (mod. $\mathfrak{m}$) et tel que la puissance n-ème. de tout idéal de k premier à $\mathfrak{m}$ soit dans H; il existe un corps de classes sur k pour le groupe H.

Pour le démontrer, nous construirons des groupes H particuliers pour lesquels on pourra affirmer l'existence d'un corps de classes, et qui seront assez généraux pour que tout groupe H donné contienne l'un d'eux.[39]

Définition. Deux modules $\mathfrak{m}_1$, $\mathfrak{m}_2$ de k sont dits *complémentaires* quand

1) Ils sont premiers entre eux,

2) Pour tout idéal premier $\mathfrak{p}$ divisant $\mathfrak{m}_1$ (ou $\mathfrak{m}_2$), $\mathfrak{m}_1$ (ou $\mathfrak{m}_2$) est aussi divisible par le module d'hyperprimarité de $\mathfrak{p}$.

3) Tout idéal premier divisant n et tout idéal premier infini divise l'un d'eux.

---

39) Cette manière de faire est dûe à M. Artin; on peut aussi, comme on était obligé de le faire dans la théorie de M. Takagi, compter le nombre des sous-groupes d'indice n à quotient cyclique et le nombre des sur-corps $k(\sqrt[n]{\alpha})$ satisfaisant à certaines conditions. Les calculs sont équivalents, mais la méthode est moins élégante.

Etant donnés deux modules complémentaires $\mathfrak{m}_1$, $\mathfrak{m}_2$ nous appellerons *groupes et corps associés* à ces modules les groupes et corps ainsi définis :

1) le groupe H_1 est le groupe des idéaux de la forme $\mathfrak{f}_2\mathfrak{a}_1^n(\beta_1)$, où $\mathfrak{f}_2$ désigne les idéaux dont tous les facteurs premiers divisent $\mathfrak{m}_2$, $\mathfrak{a}_1$ désigne les idéaux premiers à $\mathfrak{m}_1$, β_1 les nombres $\equiv 1 \pmod{\mathfrak{m}_1}$,

2) Le corps K_1 est le corps composé de tous les corps $k(\sqrt[n]{\omega_1})$, les ω_1 étant les nombres de k jouissant des propriétés suivantes :

ω_1 est primaire pour tout idéal premier ne divisant pas $\mathfrak{m}_1$; ω_1 est premier à $\mathfrak{m}_2$ et hyperprimaire pour tout idèal premier divisant $\mathfrak{m}_2$,

3) les définitions de H_2, K_2 se déduisent de celles de H_1, K_1 en permutant les indices 1 et 2.

Remarquons que les seuls idéaux premiers qui peuvent être ramifiés dans K_1 sont ceux qui divisent $\mathfrak{m}_1$. De plus, tout nombre β_1 est, quel que soit N reste normique (mod. $\mathfrak{p}_1^N$) de tout sous-corps relativement cyclique de K_1 (β_1 est en effet une puissance n-ième exacte dans $k_{\mathfrak{p}_1}$). Donc $\mathfrak{m}_1$ est divisible par les $\mathfrak{p}_1$-conducteurs (voir p. 441) de ces sous-corps, qui sont donc corps de classes pour des groupes définissables (mod. $\mathfrak{m}_1$). Donc K_1 est aussi corps de classes pour un groupe définissable (mod. $\mathfrak{m}_1$). De plus dans le groupe de Galois de K_1 par rapport à k, la puissance n-ème. de toute opération est 1. Donc K_1 est corps de classes pour un groupe qui contient le groupe $\mathfrak{a}_1^n$. Enfin, les facteurs premiers finis de $\mathfrak{m}_2$ sont complètement décomposés dans K_1, et appartiennent par suite au groupe pour lequel K_1 est corps de classes. Ce groupe contient donc H_1. Nous allons prouver que c'est H_1. A cet effet, nous allons calculer $(K_1 : k)$.

Transformons d'abord la forme des conditions auxquelles sont assujetis les ω_1. Désignant par α_i $(i = 1, 2)$ les nombres de k premiers à $\mathfrak{m}_i$; la seconde condition donne d'abord $\omega_1 = \alpha_2^n\beta_2$ (en effet, si $\mathfrak{q}$ est diviseur de $\mathfrak{m}_2$, ω_1 est puissance n-ième dans $k_\mathfrak{q}$, est par suite congru à une puissance n-ème. suivant toute puissance de $\mathfrak{q}$, en particulier suivant la contribution de $\mathfrak{q}$ à $\mathfrak{m}_2$). Si cette condition est réalisée, ω_1 est hyperprimaire pour tout idéal premier divisant $\mathfrak{m}_2$, et il ne reste plus qu'à satisfaire à la première condition pour les idéaux premiers ne divisant ni $\mathfrak{m}_1$, ni $\mathfrak{m}_2$. Mais ces idéaux premiers sont finis et ne divisent pas n : la condition de primarité est donc connue pour ces idéaux premiers et donne $(\omega_1) = \mathfrak{f}_1\mathfrak{a}_2^n$. Donc les nombres ω_1 sont ceux qui satisfont aux deux conditions

$$\omega_1 = \alpha_2^n\beta_2, \qquad (\omega_1) = \mathfrak{f}_1\mathfrak{a}_2^n.$$

Or, α désignant les nombres $\neq 0$ de k

$$(K_1 : k) = (\omega_1 \alpha^n : \alpha^n) = (\omega_1 : [\omega_1, \alpha^n]) = (\omega_1 : \alpha_2^n).$$

Introduisons les nombres θ assujetis à la seule condition $(\theta) = \mathfrak{f}_1 \mathfrak{a}_2^n$; tout ω_1 est un θ, et on a, ε désignant les unités de k,

$$(\omega_1 : \alpha_2^n) = \frac{(\theta : \alpha_2^n)}{(\theta : \omega_1)} = \frac{(\theta : \alpha_2^n \varepsilon)(\alpha_2^n \varepsilon : \alpha_2^n)}{(\theta : \omega_1)}$$

On a

$$(1) \qquad (\alpha_2^n \varepsilon : \alpha_2^n) = (\varepsilon : [\varepsilon, \alpha_2^n]) = (\varepsilon : \varepsilon^n) = n^{r+1},$$

où r désigne le nombre des unités fondamentales de k ; la formule résulte du fait que tout ε se met, et d'une seule manière, sous la forme

$$\varepsilon = \zeta^{a_0} \varepsilon_1^{a_1} \varepsilon_2^{a_2} \ldots\ldots \varepsilon_r^{a_r} \varepsilon^n, \qquad 0 \leq a_i < n,$$

ζ étant une racine n-ème. de l'unité. On a

$$(\theta : \alpha_2^n \varepsilon) = ((\theta) : (\alpha_2^n)) = \frac{(\mathfrak{f}_1 \mathfrak{a}_2^n : \mathfrak{a}_2^n)(\mathfrak{a}_2^n : (\alpha_2)^n)}{(\mathfrak{f}_1 \mathfrak{a}_2^n : (\theta))}.$$

Soit $d_i (i = 1, 2)$ le nombre des facteurs premiers finis de $\mathfrak{m}_i$. Si $\mathfrak{p}_1$, $\mathfrak{p}_2, \ldots\ldots, \mathfrak{p}_{d_1}$ sont ceux de $\mathfrak{m}_1$, un idéal $\mathfrak{f}_1 \alpha_2^n$ est de la forme $\mathfrak{p}_1^{u_1} \mathfrak{p}_2^{u_2} \ldots\ldots \mathfrak{p}_{d_1}^{u_{d_1}} \mathfrak{a}_2^n$, $0 \leq u_i < n$, d'où

$$(2) \qquad (\mathfrak{f}_1 \mathfrak{a}_2^n : \mathfrak{a}_2^n) = n^{d_1}.$$

La correspondance $\mathfrak{a}_2 \to \mathfrak{a}_2^n$ définit un isomorphisme du groupe $\mathfrak{a}_2$ et du groupe $\mathfrak{a}_2^n$ (car la puissance n-ème. d'un idéal $\neq 1$ est un idéal $\neq 1$). Dans cet isomorphisme, les groupes (α_2), (α_2^n) se correspondent. Donc

$$(3) \qquad (\mathfrak{a}_2 : (\alpha_2)^n) = (\mathfrak{a}_2 : (\alpha_2)) = h,$$

h désignant le nombre des classes de k. Les formules (1), (2), (3) montrent que tous les indices écrits sont finis, ce qui justifie nos calculs. Nous avons encore à transformer $(\theta : \omega_1)$ et $(\mathfrak{f}_1 \mathfrak{a}_2^n : (\theta))$. On a

$$(\theta : \omega_1) = (\theta : [\theta, \alpha_2^n \beta_2]) = (\theta \alpha_2^n \beta_2 : \alpha_2^n \beta_2) = (\theta \beta_2 : \alpha_2^n \beta_2) = \frac{(\alpha_2 : \alpha_2^n \beta_2)}{(\alpha_2 : \theta \beta_2)}.$$

Or toute unité ε est un nombre θ. Donc $(\alpha_2 : \theta\beta_2) = ((\alpha_2) : (\theta\beta_2))$.

D'autre part $(\mathfrak{f}_1 \mathfrak{a}_2^n : (\theta)) = (\mathfrak{f}_1 \mathfrak{a}_2^n (\beta_2) : (\theta\beta_2))$. En effet le second membre s'écrit $(\mathfrak{f}_1 \mathfrak{a}_2^n : [(\theta\beta_2), \mathfrak{f}_1 \mathfrak{a}_2^n])$. Or le groupe $[(\theta\beta_2), \mathfrak{f}_1 \mathfrak{a}_2^n]$ est précisément le groupe (θ). En effet, si $\mathfrak{f}_1 \mathfrak{a}_2^n = (\theta\beta_2)$, $\mathfrak{f}_1 \mathfrak{a}_2^n$ est principal et par suite est un (θ). Réciproquement tout θ est un $\mathfrak{f}_1 \mathfrak{a}_2^n$ et un $(\theta\beta_2)$ avec $\beta_2 = 1$; ce qui montre l'égalité des deux indices. Or on a

$$(\omega_1 : \alpha_2^n) = n^{r+1+d_1} h \frac{((\alpha_2) : (\theta\beta_2))}{(\mathfrak{f}_1\mathfrak{a}_2^n(\beta_2) : (\theta\beta_2))} \cdot \frac{1}{(\alpha_2 : \alpha_2^n\beta_2)}$$

$$= n^{r+1+d_1} \frac{(\mathfrak{a}_2 : (\theta\beta_2))}{(\mathfrak{f}_1\mathfrak{a}_2^n(\beta_2) : (\theta\beta_2))} \frac{1}{(\alpha_2 : \alpha_2^n\beta_2)} = n^{r+1+d_1} \frac{(\mathfrak{a}_2 : \mathfrak{f}_1\mathfrak{a}_2^n(\beta_2))}{(\alpha_2 : \alpha_2^n\beta_2)} = \frac{n^{r+1+d_1} h_2}{(\alpha_2 : \alpha_2^n\beta_2)},$$

ou h_2 est l'indice de H_2.

Par un raisonnement copié mot pour mot sur celui de la page 440, en remplaçant les normes par les puissances n-èmes., on verra que $(\alpha_2 : \alpha_2^n\beta_2)$ est égal au produit des indices $(\gamma_i : \gamma_i^n\delta_i)$, où γ_i représente les nombres de k premiers à un facteur premier $\mathfrak{q}_i$ de $\mathfrak{m}_2$, δ_i les nombres qui sont congrus à 1 suivant la contribution de $\mathfrak{q}_i$ à $\mathfrak{m}_2$. Mais nous avons calculé p. 466 cet indice qui vaut $nN(\mathfrak{q}_i E_{\mathfrak{q}_i})$ si $\mathfrak{q}_i$ est fini, et 2 si $\mathfrak{q}_i$ est infini. Donc, x_2 désignant le nombre des facteurs premiers infinis de $\mathfrak{m}_2$, on a

$$(\alpha_2 : \alpha_2^n\beta_2) = n^{d_2} 2^{x_2} \prod_{\mathfrak{q}_i} N(\mathfrak{q}_i E_{\mathfrak{q}_i}).$$

On a donc

$$(\omega_1 : \alpha_2^n) = n^{r+1+d_1-d_2} 2^{-x_2} h_2 \prod_{\mathfrak{q}_i} N(\mathfrak{q}_i E_{\mathfrak{q}_i})^{-1}.$$

De même, en permutant les indices 1, 2, on a

$$(\omega_2 : \alpha_1^n) = n^{r+1+d_2-d_1} 2^{-x_1} h_1 \prod_{\mathfrak{p}_i} N(\mathfrak{p}_i E_{\mathfrak{p}_i})^{-1}.$$

Or tout facteur premier de n figure soit parmi les $\mathfrak{p}_i$, soit parmi les $\mathfrak{q}_i$. Multiplions les deux formules membre à membre : il vient

$$(K_1 : k)(K_2 : k) = h_1 h_2 n^{2(r+1)} 2^{-(x_1+x_2)} N(n)^{-1}.$$

Distinguons deux cas : 1) $n \neq 2$, k et tous ses conjugués sont imaginaires, $x_1 = x_2 = 0$, et le degré de k est $2(r+1)$ donc $N(n) = n^{2(r+1)}$. 2) $n = 2$. Soient r_1 le nombre des conjugués réels de k, et $2r_2$ le nombre des conjugués imaginaires. On a $r + 1 = r_1 + r_2$, $x_1 + x_2 = r_1$, $N(n) = n^{r+2r_2}$.

Dans tous les cas, on a

$$(K_1 : k)(K_2 : k) = h_1 h_2.$$

Or le groupe de Takagi associé (mod. $\mathfrak{m}_1$) à K_1 dans k contient H_1 et est d'indice $(K_1 : k)$. Donc $h_1 \geq (K_1 : k)$ et de même $h_2 \geq (K_2 : k)$. De la formule précédente résulte que ces inégalités sont des égalités et par suite que K_1 est corps de classes sur k pour le groupe H_1.

Ceci posé, soit H un groupe de congruence quelconque satisfaisant aux conditions énoncées au début de ce paragraphe. Soit $\mathfrak{f}$ le conducteur de H; et donnons nous un idéal premier quelconque, $\mathfrak{q}$, appartenant à H (s'il est fini), ou, s'il est infini, ne divisant pas $\mathfrak{f}$. On peut former deux modules complémentaires $\mathfrak{m}_1$, $\mathfrak{m}_2$ tels que a) $\mathfrak{m}_1$ soit divisible par $\mathfrak{f}$, b) $\mathfrak{m}_2$

soit divisible par $\mathfrak{q}$ et ne soit divisible que par des idéaux premiers finis contenus dans H. En effet $\mathfrak{q}$ ne divise certainement par $\mathfrak{m}_1$: on peut prendre $\mathfrak{m}_2 = \mathfrak{q}^x$, x étant un entier convenable. Soient H_1, H_2 les groupes associés à ces deux modules complémentaires. Je dis que H_1 est contenu dans H. En effet, tout idéal (β_1) est contenu dans H, puisque H est définissable (mod. $\mathfrak{f}$) et à fortiori (mod. $\mathfrak{m}_1$); tout idéal $\mathfrak{a}_1^n$ est dans H, à cause des conditions imposées à H au début. Or il y a un corps de classes K_1 sur k pour H_1, donc aussi un corps de classes K pour H (voir p. 447). De plus $\mathfrak{q}$ se décompose totalement dans K_1, donc aussi dans K, résultat qui sera utilisé tout à l'heure.

Nous avons donc démontré le théorème d'existence:

k étant un corps fini de nombres algébriques, H un groupe de congruence dans k, il existe un sur-corps relativement abélien K corps de classes sur k pour le groupe H.

Nous allons maintenant démontrer le

Théorème du Conducteur:

K étant corps de classes sur k pour le groupe H, les idéaux premiers finis ou infinis divisant le conducteur $\mathfrak{f}$ de H sont ceux qui sont ramifiés dans K.

En effet on a vu (p. 441) que H possède un module de définition qui n'est composé que d'idéaux premiers ramifiés dans K. Le conducteur étant le p.g.c.d. des modules de définition il suffit de prouver que tout idéal premier $\mathfrak{q}$ ramifié dans K divise nécessairement ce conducteur.

1) 1er cas. K est cyclique de degré l premier par rapport à k; supposons que $\mathfrak{q}$ soit ramifié et ne divise pas $\mathfrak{f}$. Supposons d'abord $\mathfrak{q}$ fini. Soit ζ une racine primitive l-ième de l'unité, et soit $\bar{H}$ le groupe des idéaux premiers à $\mathfrak{f}$ de $k(\zeta)$ dont la norme par rapport à k tombe dans H. On a vu que $Kk(\zeta)$ est corps de classes sur $k(\zeta)$ pour le groupe $\bar{H}$ (voir p. 448). Soit $\bar{\mathfrak{q}}$ un facteur premier de $\mathfrak{q}$ dans $k(\zeta)$. Je dis que $\bar{\mathfrak{q}}$ est ramifié dans $Kk(\zeta)$. En effet $\mathfrak{q}$ est la puissance l-ième d'un idéal de K, donc l'exposant relatif par rapport à k d'un facteur premier de $\mathfrak{q}$ dans $Kk(\zeta)$ est multiple de l. Mais $(k(\zeta):k)$ divisant $l-1$, l'exposant relatif de $\bar{\mathfrak{q}}$ est premier à l, et il faut par suite que l'exposant relatif par rapport à $k(\zeta)$ d'un facteur premier de $\bar{\mathfrak{q}}$ soit divisible par l. Or il existe un module $\mathfrak{m}$ tel que le groupe des idéaux premiers à $\mathfrak{m}$ de $\bar{H}$ soit le groupe de Takagi associé (mod. $\mathfrak{m}$) à $Kk(\zeta)$ dans $k(\zeta)$. Soit $\mathfrak{Q}$ le facteur premier de $\bar{\mathfrak{q}}$ dans $Kk(\zeta)$. Choisissons un idéal $\mathfrak{A}$ premier à $\mathfrak{m}$ et congru à $\mathfrak{Q}$ (mod. $\mathfrak{f}$): On a

$$\bar{\mathfrak{q}} \equiv N_{Kk(\zeta),\, k(\zeta)}(\mathfrak{A}) \qquad (\mathrm{mod.}\ \mathfrak{f}).$$

Le second membre est dans $\bar{H}$; $\bar{H}$ étant définissable (mod. $\mathfrak{f}$), $\bar{\mathfrak{q}}$ est aussi

dans $\bar{H}$, ce qui nous amène à une contradiction, car nous avons vu que $\bar{\mathfrak{q}}$ est nécessairement complètement décomposé dans $K\bar{k}(\zeta)$.

Si maintenant $\mathfrak{q}$ est infini, on a $l = 2$; car si $l \neq 2$, $\mathfrak{q}$ ne peut être ramifié dans K. Or si $l = 2$, on a vu (p. 471) que, $\mathfrak{q}$ ne divisant pas $\mathfrak{f}$ est nécessairement complètement décomposé dans K, d'où la contradiction.

2) Cas général. Supposons le théorème démontré pour toutes les extensions abéliennes de degré relatif $< n$, et soit K corps de classes sur k pour un groupe H de conducteur $\mathfrak{f}$, avec $(K:k) = n$. K contient un souscorps K_1 de degré relatif premier l par rapport à k. Soit $\mathfrak{q}$ un idéal premier de k ramifié dans K. Si $\mathfrak{q}$ est ramifié dans K_1, il divise le conducteur du groupe de Artin associé à K_1 dans k, donc à fortiori celui de H. Sinon, soit $\mathfrak{q}_1$ un facteur premier de $\mathfrak{q}$ dans K_1. $\mathfrak{q}_1$ est ramifié dans K, donc divise le conducteur du groupe de Artin associé à K dans K_1, conducteur qui divise lui-même celui de H, ce qui achève la démonstration.

Récapitulation des Théorèmes de la Théorie du Corps de Classes.

Résumons l'ensemble des résultats auxquels nous sommes arrivés :

k désignant un corps fini quelconque de nombres algébriques,

1) K étant un sur-corps relativement abélien de k, le groupe de Artin H associé à K dans k est un groupe de congruence, ayant pour conducteur $\mathfrak{f}$ un module qui ne contient que des idéaux premiers ramifiés dans K, mais qui les contient tous.

2) A désignant le groupe des idéaux de k premiers à $\mathfrak{f}$, A/H est isomorphe au groupe de Galois de K par rapport à k, la correspondance étant définie par $\mathfrak{a} \rightarrow \sigma$ si

$$\left(\frac{K}{\mathfrak{a}}\right) = \sigma.$$

3) $\mathfrak{p}$ étant un idéal premier fini de k, le corps d'inertie de $\mathfrak{p}$ est corps de classes pour le groupe $HS_{\mathfrak{f}/\mathfrak{f}_\mathfrak{p}}$ où $\mathfrak{f}_\mathfrak{p}$ désigne la participation de $\mathfrak{p}$ à $\mathfrak{f}$. Si $\mathfrak{p}^f$ est la plus petite puissance de $\mathfrak{p}$ contenue dans ce groupe, $\mathfrak{p}$ se décompose en idéaux premiers de degré relatif f. Ce théorème n'a été démontré que si $\mathfrak{p}$ est non ramifié, c'est-à-dire si $\mathfrak{f}_\mathfrak{p} = 1$, $\mathfrak{f}/\mathfrak{f}_\mathfrak{p} = \mathfrak{f}$, $HS_{\mathfrak{f}/\mathfrak{f}_\mathfrak{p}} = H$. Supposons $\mathfrak{p}$ ramifié. Soit K_T le corps d'inertie de $\mathfrak{p}$ dans K. $\mathfrak{p}$ n'est pas ramifié dans K_T, donc K_T est corps de classes pour un groupe H_T dont le conducteur n'est pas divisible par $\mathfrak{p}$. Ce conducteur divisant $\mathfrak{f}$, divise $\mathfrak{f}/\mathfrak{f}_\mathfrak{p}$, et par suite H_T contient $HS_{\mathfrak{f}/\mathfrak{f}_\mathfrak{p}}$. Réciproquement

le corps de classes pour ce groupe est tel que $\mathfrak{p}$ n'y soit pas ramifié. Il est donc contenu dans K_T, ce qui prouve notre assertion.

4) Pour tout module $\mathfrak{m}$ multiple de $\mathfrak{f}$, les idéaux premiers à $\mathfrak{m}$ de H sont les idéaux de k qui sont congrus (mod. $\mathfrak{m}$) à la norme relative de K par rapport à k d'un idéal de K premier à $\mathfrak{m}$.

5) Si K est corps de classes sur k pour le groupe H, si $\bar{k}$ est un surcorps fini quelconque de k, $K\bar{k}$ est corps de classes sur $\bar{k}$ pour le groupe des idéaux de $\bar{k}$ dont la norme par rapport à k est dans H.

6) Si K, K' sont corps de classes sur k pour les groupes H, H', KK' est corps de classes pour $[H, H']$ et $[K, K']$ est corps de classes pour le groupe HH'.

7) Etant donné un groupe de congruence H dans k, il y a un corps de classes K sur k pour le groupe H.

Table des Matières.

Chapitre VI.

Chapitre VII.

Chapitre VIII.

Chapitre IX.

Chapitre X.