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

Deux Théorèmes d'Arithmétique

Claude CHEVALLEY

Nous nous proposons de démontrer deux théorèmes de la théorie des corps de nombres algébriques, qui n'ont l'un avec l'autre d'aucun autre rapport que celui d'être tous deux utilisés par A. Weil dans son mémoire "Sur la théorie du corps de classes", qui parait dans le même numéro de ce journal.

I

Soit K un corps de nombres algébriques de degré fini sur le corps des rationnels. Un groupe multiplicatif E d'éléments $\neq 0$ de K sera dit "à engendrement fini" si E possède un ensemble fini de générateurs. C'est ainsi que le groupe des unités de K est un groupe à engendrement fini; plus généralement, si on se donne un nombre fini d'idéaux premiers $\mathfrak{p}_1, \ldots, \mathfrak{p}_h$ de K, le groupe des éléments $x \neq 0$ de K tels que l'idéal fractionnaire principal engendré par x soit un produit de puissances (d'exposants positifs, nuls ou négatifs) de $\mathfrak{p}_1, \cdots, \mathfrak{p}_h$ est un groupe à engendrement fini, comme il est bien connu. Nous nous proposons de démontrer le théorème suivant:

Théorème 1. *Soient K un corps de nombres algébriques de degré fini, et E un sous-groupe à engendrement fini du groupe multiplicatif des éléments $\neq 0$ de K. Soit m un entier >0, et soit b un entier rationnel quelconque. Il existe alors un entier rationnel a, premier à b, qui jouit de la propriété suivante: tout élément x de E qui est $\equiv 1 \pmod{a}$ est puissance m-ième d'un élément de E.*

La condition $x \equiv 1 \pmod{a}$ doit s'interprêter au sens des congruences multiplicatives de H. Hasse; elle signifie que $x-1$ est de la forme ayz^{-1}, où y et z sont des entiers de K et z est premier à a dans l'anneau des entiers de K.

1. Désignons par E_0 l'ensemble des nombres $\neq 0$ de K dont une puissance (d'exposant $\neq 0$) appartient à E. C'est évidemment un sous-groupe du groupe des éléments $\neq$ de K. Ce groupe est encore à engendrement fini. En effet, soit $\{x_1, \cdots, x_r\}$ un système fini de générateurs de E. Décomposons les idéaux fractionnaires engendrés par les x_i en produits

de puissances d'idéaux premiers ; soient $\mathfrak{p}_1, \cdots, \mathfrak{p}_h$ les idéaux premiers qui interviennent dans ces décompositions. Il est clair que E_0 est contenu dans le groupe des $x \neq 0$ tels que l'id'al fractionnaire engendré par x soit un produit de puissances de $\mathfrak{p}_1, \cdots, \mathfrak{p}_h$. Ce groupe étant à engendrement fini, il en sera de même de E_0. Le groupe E_0/E est un groupe à engendrement fini dont tous les éléments sont d'ordres finis ; c'est donc un groupe fini ; soit n son ordre. Si un élément x de E est puissance mn-ième d'un nombre y de K, y^n est dans E, et x est puissance m-ième d'un élément de E. Remplaçant m par mn, on voit qu'il suffira de montrer l'existence d'un entier a, premier à b, tel que tout élément $\equiv 1 \pmod{a}$ de E soit puissance m-ième d'un nombre de K. C'est l'assertion que nous nous proposons désormais de démontrer.

2. Montrons qu'on peut se ramener au cas où m est puissance d'un nombre premier p. Supposons en effet l'assertion vraie dans ce cas particulier. Posons, dans le cas général, $m = p_1^{e_1} \cdots p_r^{e_r}$, où les p_i sont des nombres premiers distincts. Il existe par hypothèse des entiers a_i $(1 \leq i \leq r)$ premiers à b tel que, pour chaque i, tout nombre $\equiv 1 \pmod{a_i}$ de E soit puissance $p_i^{e_i}$-ième d'un nombre de K. Soit a le *p.p.c.m.* des a_i $(1 \leq i \leq r)$; a est donc premier à b. Soit x un nombre de E qui est $\equiv 1 \pmod{a}$; alors, pour tout i, x est puissance $p_i^{e_i}$-ième d'un nombre de K. Puisque m est le *p.p.c.m* des $p_i^{e_i}$, il en résulte que x est puissance m-ième d'un nombre de K. Nous supposerons donc à partir de maintenant que $m = p^e$, p étant un nombre premier.

3. Montrons que, dans le cas où $p=2$, on peut se ramener au cas où -1 est un carré dans K. Supposons en effet que l'assertion soit démontrée dans ce cas particulier, que $p=2$ et que -1 ne soit pas un carré dans K. Soit k le plus grand entier tel que $K(\sqrt{-1})$ contienne une racine primitive 2^k-ième. Il y a alors par hypothèse un entier a, premier à b, tel que tout nombre $x \equiv 1 \pmod{a}$ de E soit puissance 2^{e+k}-ième d'un nombre y de $K(\sqrt{-1})$. Montrons que x est puissance 2^e-ième d'un nombre de K. Si y est dans K, il n'y a rien à démontrer. Sinon, soit f le plus petit entier >0 tel que y^{2^f} soit dans K; soit $\bar{y}$ le conjugué de y par rapport à K. On a donc $\bar{y}^{2^{f-1}} = -y^{2^{f-1}}$, d'où $(\bar{y}y^{-1})^{2^{f-1}} = -1$, il en résulte que $\bar{y}y^{-1}$ est une racine primitive 2^f-ième de l'unité, d'où $f \leq k$; on a $x = (y^{2^f})^{2^{e+k-f}}$, ce qui montre que x est puissance 2^e-ième d'un nombre de K.

4. Nous supposerons à partir de maintenant que, si $p=2$, -1 est un carré dans K. Nous allons montrer que l'on peut se ramener au cas où K contient une racine m-ième primitive de l'unité. Supposons l'assertion démontrée dans ce cas, et soit ζ une racine primitive m-ième de l'unité. Il existe donc un entier a, premier à b, tel que tout élément $x\equiv 1 \pmod{a}$ de E soit puissance m-ième dans $K(\zeta)$. Nous allons en déduire que x est puissance m-ième dans K. Si $0\leq h\leq e$, nous poserons $\zeta_h=\zeta^{p^{e-h}}$; ζ_h est donc une racine primitive p^h-ième de l'unité. Pour montrer que x est puissance m-ième dans K, il suffira de montrer que, s'il est puissance m-ième dans $K(\zeta_{h+1})$, il est aussi puissance m-ième dans $K(\zeta_h)$ $(0\leq h<e)$. Nous supposerons donc que $x=y^m$, y dans $K(\zeta_{h+1})$. Si y est dans $K(\zeta_h)$, il n'y a rien à démontrer. Nous supposerons donc que y n'est pas dans $K(\zeta_h)$, donc que $K(\zeta_{h+1})\neq K(\zeta_h)$.

Si $h=0$, le degré de $K(\zeta_{h+1})/K(\zeta_h)$ divise $p-1$; il en est donc de même du degré d de $K(y)/K$. Si z est la norme de y par rapport à K, on a $x^d=z^m$; puisque d est premier à m, x est puissance m-ième dans K.

Supposons maintenant $h>0$; puisque nous supposons $K(\zeta_{h+1})\neq K(\zeta_h)$, $K(\zeta_{h+1})$ est cyclique de degré p sur $K(\zeta_h)$; nous désignerons par s un générateur du groupe de Galois de cette extension. On notera qu'il résulte de l'hypothèse faite que, dans ce cas, $h\geq 2$ si $p=2$. Puisque y^m est dans K, $(sy)y^{-1}$ est une racine m-ième de l'unité, donc de la forme ζ^f, où f est un entier. Par ailleurs, s peut se prolonger en un automorphisme de $K(\zeta)$, qui change ζ en ζ^g, où g est un entier. Puisque s laisse ζ_h invariant, g est $\equiv 1 \pmod{p^h}$. Puisque s est d'ordre p (en tant qu'automorphisme de $K(\zeta_{h+1})$), on a $s^p y=y$, d'où $f(1+g+\cdots+g^{p-1})\equiv 0 \pmod{p^e}$. Posons $g=1+up^h$, u étant un entier. On a alors $1+g+\cdots+g^{p-1}=(g^p-1)(g-1)^{-1}=u^{-1}p^{-h}((1+up^h)^p-1)$. Se souvenant que $h\geq 2$ si $p=2$, on voit tout de suite que $1+g+\cdots+g^{p-1}\equiv p \pmod{p^2}$, d'où $f\equiv 0 \pmod{p^{e-1}}$. Cela signifie que $(sy)y^{-1}$ est une racine p-ième de l'unité. Or $K(\zeta_h)$ contient les racines p-ièmes de l'unité; puisque ζ_{h+1}^p est dans $K(\zeta_h)$ mais que ζ_{h+1} n'y est pas, $(s\zeta_{h+1})\zeta_{h+1}^{-1}$ est une racine primitive p-ième de l'unité. On en conclut qu'il existe un exposant v tel que $s(y\zeta_{h+1}^v)=y\zeta_{h+1}^v$. Puisque $\zeta_{h+1}^m=1$, on a $x=(y\zeta_{h+1}^v)^m$, ce qui montre que x est puissance m-ième d'un nombre de $K(\zeta_h)$.

5. Supposons donc à partir de maintenant que K contienne une racine primitive m-ième de l'unité. Soit L le sur-corps de K obtenu par adjonc-

tion des racines m-ièmes des nombres de E; puisque E est à engendrement fini, L est un sur-corps relativement abélien de degré fini de K. Le degré de L/K est une puissance de p. Soient $L_1, \cdots, L_s$ tous les sous-corps de L qui contiennent K et qui sont de degré p sur K. Pour chaque L_j, il y a une infinité d'idéaux premiers de K qui restent premiers dans L_j; on peut donc trouver un idéal. premier $\mathfrak{q}_j$ de K qui ne divise pas mb et qui reste premier dans L_j. Soit q_j le nombre premier contenu dans $\mathfrak{q}_j$, et soit a le *p.p.c.m.* des q_j $(1 \leq j \leq s)$. Soit x un nombre de E qui est congrû a 1 (mod a), et soit M le corps $K(x^{1/m})$. On a donc $x \equiv 1 \pmod{\mathfrak{q}_j}$; puisque $\mathfrak{q}_j$ ne divise pas m, il en résulte que x est puissance m-ième dans la complétion $\mathfrak{q}_j$-adique de K, donc que les diviseurs premiers de $\mathfrak{q}_j$ dans M sont de degré relatif 1 par rapport à K (M est en effet contenu dans la complétion $\mathfrak{q}_j$-adique de K). Cela signifie que M ne peut contenir aucun des L_j. Or, M est contenu dans L; il en résulte que $M=K$, donc que x est puissance m-ième dans K. Le théorème est donc démontré.

Remarque. Nous avons démontré en cours de route le résultat suivant, qui parait digne d'un certain interêt en lui-même. Soient p un nombre premier, $m=p^e$ une puissance de p, et K un corps qui n'est pas de caractéristique p; supposons de plus que -1 soit un carré dans K si $p=2$. Si ζ est une racine primitive m-ième de l'unité, tout élément de K qui est puissance m-ième dans $K(\zeta)$ l'est déjà dans K.

On peut d'ailleurs se passer de ce résultat pour démontrer le théorème 1, en appliquant directement la méthode de la section 5. Formons en effet le corps L obtenu par adjonction à K des racines m-ièmes des nombres de E et de leurs conjugués par rapport à K (nous ne supposons plus ici que K contient une racine primitive m-ième de l'unité). Soient G le groupe de Galois de L/K, et H_j $(1 \leq j \leq s)$ tous les sous-groupes de G distincts de G lui-même. Il est bien connu que, pour chaque j, la réunion des conjugués de H_j est distincte de G; on peut donc trouver un élément s_j de G qui n'a aucun conjugué dans H_j. A chaque idéal premier $\mathfrak{q}$ de K, non ramifié dans L, on peut faire correspondre la classe d'éléments conjugués de G formée par les substitutions de Frobenius $((L/K)/\mathfrak{Q})$ relatives aux diviseurs premiers $\mathfrak{Q}$ de $\mathfrak{q}$ dans L. En vertu du théorème de Tschebotarow, il existe une infinité d'idéaux premiers $\mathfrak{q}$, non ramifiés dans L, pour lesquels cette classe contient s_j; il existe donc, pour chaque j, un idéal premier $\mathfrak{q}_j$, non ramifié dans L et ne divisant pas bm, dont la classe associée contient

s_j. Si L_j est le sous-corps de L qui correspond à H_j par la théorie de Galois, aucun diviseur premier de $\mathfrak{q}_j$ dans L_j n'est de degré relatif 1 par rapport à K. Si q_j est le nombre premier contenu dans $\mathfrak{q}_j$, il suffit alors de prendre pour a le *p.p.c.m.* des q_j; car alors, si x est un nombre $\equiv 1 \pmod{a}$, pour chaque j, $\mathfrak{q}_j$ admet au moins un diviseur premier de degré relatif 1 dans le corps $K(x^{1/m})$.

II.

Soit k le corps des nombres $\mathfrak{p}$-adiques d'un corps de nombres algébriques de degré fini, $\mathfrak{p}$ étant un idéal premier de ce corps. La théorie du corps de classes local donne alors les résultats suivants :

Si K est un sur-corps de degré fini de k, et A une extension abélienne de degré fini de K, le symbole normique $(x, A/K)$ donne un homomorphisme du groupe multiplicatif K^* des éléments $\neq 0$ de K sur les groupe de Galois de A/K; le noyau de cet homomorphisme se compose des normes relatives par rapport à K d'éléments $\neq 0$ de A;

si τ est un isomorphisme de A avec un corps τA, et $x \in K^*$, $(\tau x, \tau A/\tau K)$ est $\tau(x, A/K)\tau^{-1}$;

si A' est un sous-corps de A contenant K, $(x, A'/K)$ est l'automorphisme de A'/K induit par $(x, A/K)$;

soit K' un sur-corps de degré fini de K, et soit x' un élément $\neq 0$ de K'; désignant par AK' le corps composé se A et de K', et identifiant de la manière habituelle le groupe de Galois de AK'/K' à un sous-groupe de celui de A/K, $(x', AK'/K')$ est égal à $(N_{K'/K}x', A/K)$ (théorème de translation);

si L est un sur-corps de degré fini de K et A le plus grand sous-corps de L contenant K et abélien sur K, tout élément $x \neq 0$ de K tel que $(x, A/K) = 1$ est norme relative par rapport à K d'un élément de L (théorème de limitation).

La démonstration du théorème que nous avons en vue ne se servira que des propriétés que nous venons d'énoncer. Or, si on se limite à la considération d'extensions séparables, ces propriétés restent valables pour une classe de corps bien plus vaste que celle des corps des nombres $\mathfrak{p}$-adiques. Il résulte en effet des travaux de M. Moriya et T. Nakayama (Moriya, Die Theorie der Klassenkörper im Kleinen über diskret perfekten

Köıpern, I, II, Proc. Imp. Acad. Tokyo, 18 (1942) ; III, en collaboration avec T. Nakayama, Proc. Imp. Acad. Tokyo, 19 (1943)) ; qu'il suffit de supposer ce qui suit : k est complet par rapport à une valuation discrète v, et pour tout entier $n>0$, le corps des résidus de v admet une extension et une seule de degré n, qui est séparable. Ces conditions sont en particulier satisfaites si k est un corps local attaché à une place d'un corps de fonctions algébriques sur un corps fini.

Nous utiliserons les notations suivantes :

Z : un sur-corps de k, galoisien et de degré fini par rapport à k ;

K : un sous-corps de Z contenant k ;

A : le plus grand sous-corps de Z contenant K et abélien sur K ;

B : le plus grand sous-corps de Z contenant k et abélien sur k ;

G : le groupe de Galois de Z/k ;

Γ : le groupe de Galois de Z/K.

Le groupe Γ est donc un sous-groupe de G ; le groupe de Galois de A/K est le quotient de Γ par son groupe des commutateurs Γ', et celui de B/k est le quotient de G par son groupe des commutateurs G'. L'opération de transfert (Verlagerung ; cf. Zassenhaus, Lehrbuch der Gruppentheorie, p. 128) est un homomorphisme $s\rightarrow t(s)$ de G dans Γ/Γ' ; le noyau de cet homomorphisme contient G'. On peut donc aussi considérer t comme un homomorphisme de G/G' dans Γ/Γ', c'est-à-dire du groupe de Galois de B/k dans celui de A/K.

Nous nous proposons de démontrer le théorème suivant :

Théorème 2. *Soit x un élément $\neq 0$ de k. On a alors*

$$(x, A/K)=t((x, B/k)).$$

Ce résultat est en relation assez étroite avec ceux obtenus par Nakayama (Über die Beziehungen zwischen den Faktorensystemen und der Normklassengruppe eines galoisschen Erweiterungsköıpers, Math. Ann. 112 (1936)), par Akizuki (Eine homomorphe Zuordnung der galoisschen Gruppe zu den Elementen einer Untergruppe der Normklassengruppe, Math. Ann. 112, (1936)) et Shafarevich (On Galois groups of p-adic fields, C.R. Acad. des Sciences U.R.S.S., 53 (1946)). Il serait probablement possible de déduire notre théorème des résultats obtenus par les auteurs que nous

venons de citer ; mais il n'est pas plus difficile de le démontrer directement, et c'est ce que nous allons maintenant faire.

Soit s un élément de G qui induise l'automorphisme $(x, B/k)$ de B. Désignons par S le sous-groupe engendré par s ; on peut alors représenter G comme la réunion d'un certain nombre r d'ensembles mutuellement disjoints de la forme $\Gamma t_i S$ $(1 \leq i \leq r)$; soit f_i le plus petit entier >0 tel que $t_i s^{f_i} t_i^{-1}$ soit dans Γ ; on sait alors que $t(s)$ est la classe modulo Γ' de l'élément

$$\Pi_{i=1}^{r} t_i s^{f_i} t_i^{-1}$$

Soit L le corps des invariants du sous-groupe S de G. Montrons que x est norme relative par rapport à k d'un élément y de L. Il suffit en vertu du théorème de limitation de montrer que x est norme relative d'un élément du plus grand sous-corps L_1 de L contenant k et abélien par rapport à k. Or $(x, L_1/k)$ est l'automorphisme induit sur L_1 par $(x, B/k)$, donc par s, et s laisse invariants les éléments de L, donc aussi de L_1 ; $(x, L_1/k)$ est donc l'identité, ce qui demontre notre assertion. Soit donc $x = N_{L/k} y$, $y \in L$; soit $s' = (y, Z/L)$ (on observera que Z est cyclique sur L). L'automorphisme de BL/L induit par s' est $(y, BL/L)$ qui est égal à $(x, B/k)$ en vertu du théorème de translation. On en déduit que s et s' induisent le même opération sur B/k, donc que $s' \equiv s \pmod{G'}$ et par suite que $t(s) = t(s')$; on peut donc supposer que $s = s'$.

Soient $u_1 S, \cdots, u_n S$ les classes distinctes de G suivant S ; $u_1, \cdots, u_n$ induisent donc tous les isomorphismes distincts de L/k avec ses conjugués dans Z, et on a $x = \Pi_{j=1}^{n} u_j(y)$. Chacun des ensembles $\Gamma t_i S$ est la réunion d'un certain nombre des ensembles $u_j S$; on peut supposer que, pour chaque $i (1 \leq i \leq r)$, ceux des u_j qui sont dans $\Gamma t_i S$ sont dans Γt_i, et que t_i lui-même est l'un d'eux.

Soit L_i le corps $t_i(L)$, et soit $y_i = t_i(y)$. Tout élément de Γ induit un isomorphisme de $K(L_i)$ avec un sous-corps de Z, et cet isomorphisme coincide avec l'identité sur K. Pour que les isomorphismes produits par des éléments γ et γ' de Γ coincident, il faut et suffit que $\gamma^{-1}\gamma'$ appartienne au groupe de Galois $t_i S t_i^{-1}$ de Z/L_i, c'est-à-dire que γt_i et $\gamma' t_i$ induisent le même isomorphisme de L, donc que $\gamma t_i S = \gamma' t_i S$. On voit donc que celles des opérations u_j qui sont dans $\Gamma t_i S$ produisent tous les isomorphismes distincts de $K(L_i)$ avec ses conjugués par rapport à K dans Z ; le produit

des éléments $u_j y$ correspondants est donc $N_{K(L_i)/K} t_i(y)$, et on a

$$x = \Pi_{i=1}^{r} N_{K(L_i)/K} t_i(y)$$

$$(x, A/K) = \Pi_{i=1}^{s} (N_{K(L_i)/K} t_i(y), A/K)$$

Or le corps Z est cyclique sur L_i, donc aussi sur $K(L_i)$; posons $v_i = (t_i(y), ZL_i)$. Puisque $(y, Z/L) = s$, on a $v_i = t_i s t_i^{-1}$. Le groupe de Galois de $Z/K(L_i)$ est l'intersection avec Γ du groupe de Galois $t_i S t_i^{-1}$ de Z/L_i ; le degré de $K(L_i)/K$ est donc égal au nombre f_i défini plus haut ; on a $N_{K(L_i)/L_i} t_i(y) = (t_i(y))^{f_i}$, d'où, en vertu du théorème de translation, $(t_i(y), Z/K(L_i)) = t_i s^{f_i} t_i^{-1}$; l'opération $(t_i(y), AK(L_i)/K(L_i))$ est donc l'automorphisme de $AK(L_i)$ induit par $t_i s^{f_i} t_i^{-1}$; il en résulte, en vertu du théorème de translation, que $(N_{K(L_i)/K} t_i(y), A/K)$ est l'opération induite sur A par $t_i s^{f_i} t_i^{-1}$, donc que $(x, A/K)$ est induit par $\Pi^{r}_{i=1} t_i s^{f_i} t_i^{-1}$, ce qui démontre le théorème.

Soit maintenant k un corps de nombres algébriques de degré fini. Désignons par I_k le groupe des idèles de k, et par P_k le groupe des idèles principaux. Soit K une extension de degré fini de k, et soit A une extension abélienne de degré fini de K. Le symbole de Artin, que nous noterons $(\mathfrak{a}, A/K)$, fournit alors un homomorphisme de I_K sur le groupe de Galois de A/K ; le noyau de cet homomorphisme est le groupe engendré par P_K et par les normes par rapport à K d'idèles de A. De plus, on a les propriétés suivantes : si τ est un isomorphisme de A avec un corps τA, et $\mathfrak{a}$ un idèle de K, $(\tau\mathfrak{a}, \tau A/\tau K)$ est $\tau(\mathfrak{a}, A/K)\tau^{-1}$;

si A' est un sous-corps de A contenant K, $(\mathfrak{a}, A'/K)$ est l'automorphisme de A' induit par $(\mathfrak{a}, A/K)$;

si K' est un sur-corps de K de degré fini et $\mathfrak{a}'$ un idèle de K', $(N_{K'/K}\mathfrak{a}', A/K)$ est égal à $(\mathfrak{a}', AK'/K')$ (en identifiant de la manière habituelle le groupe de Galois de AK'/K' à un sous-groupe de celui de A/K) ;

si L est un sur-corps quelconque de K, et A le plus grand sous-corps de L contenant K et abélien sur K, tout idèle $\mathfrak{a}$ de K tel que $(\mathfrak{a}, A/K) = 1$ est dans le groupe engendré par P_K et par les normes relatives de L à K d'idèles de L.

On peut alors, en suivant exactement la même méthode que plus

haut, établir le résultat suivant. Soient Z une extension galoisienne de k, K un sous-corps de Z contenant k, A le plus grand sous-corps de Z contenant K et abélien sur K, B le plus grand sous-corps de Z contenant k et abélien sur k, G et Γ les groupes de Galois de Z par rapport à k et à K. Si $\mathfrak{a}$ est un idèle de k, et si s est une opération de G qui induit l'automorphisme $(\mathfrak{a}, B/k)$ sur B, alors $(\mathfrak{a}, A/K)$ est le transfert de s à Γ.

Mais il convient d'observer que ce résultat peut s'établir plus facilement en utilisant les propriétés des substitutions de Frobenius ; c'est ce qui a été fait par Artin dans son mémoire " Idealklassen in Oberkörpern und allgemeines Reziprozitätsgesetz, Hamb. Abhand., 1929).

Si k est un corps de fonctions algébriques d'une variable sur un corps fini, on sait également définir un symbole de Artin qui possède les propriétés énoncées plus haut tant qu'on se limite à la considération d'extensions séparables ; le résultat que nous avons énoncé est donc encore vrai dans ce cas.

Columbia University.