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

J. HERBRAND

Sur la théorie des groupes de décomposition, d'inertie et de ramification

Journal de mathématiques pures et appliquées 9^e série, tome 10 (1931), p. 481-498.
<http://www.numdam.org/item?id=JMPA_1931_9_10__481_0>

Sur la théorie des groupes de décomposition, d'inertie et de ramification ;

Par J. HERBRAND.

Jacques Herbrand, *jeune mathématicien d'un rare talent, a péri dans un accident de montagne en juillet* 1931.

Nous voulons saluer ici la mémoire de ce jeune homme, auquel le plus brillant avenir semblait réservé, et qui a emporté avec lui les dons les plus précieux. Récemment, J. Herbrand avait remis au Journal de Mathématiques *deux beaux travaux : « Sur la théorie des groupes de décomposition, d'inertie et de ramification », et « Sur les classes des corps circulaires ». On trouvera ci-dessous le premier de ces deux Mémoires.* M. Cl. Chevalley, *ami et émule de J. Herbrand, a bien voulu nous donner son concours pour la correction des épreuves, et c'est à lui qu'est due l'importante addition qui figure en Note à la page* 491.

H. V.

Introduction.

Hilbert (1) a introduit dans la théorie des nombres les notions de groupe et de corps de décomposition, de ramification et d'inertie. On

(1) *Voir* Hilbert, *Theorie des algebraischen Zahlenkörper* (*Jahresbericht des deutschen Math. Veireinigung*, 1898). Traduction française dans les *Annales de Toulouse*, 1909. Les seules notions utilisées dans ce qui suit sont celles exposées au Livre II de cet Ouvrage. Quand nous renverrons à un théorème de Hilbert, il s'agira d'un théorème de cet Ouvrage.

Les principaux résultats du présent Mémoire ont été exposés dans une Note aux *Comptes rendus de l'Académie des Sciences* (de Paris), 191, p. 980.

sait le rôle important joué par ces notions. Nous allons, dans le présent Mémoire, résoudre le problème suivant (la solution est donnée par les théorèmes II et III).

Soient un corps k, K *un sur-corps galoisien de k*, $\mathfrak{P}$ *un idéal premier de* K; $\overline{\mathrm{K}}$ *un sous-corps de* K, *galoisien par rapport à k*; $\overline{\mathfrak{P}}$ *l'idéal premier de* $\overline{\mathrm{K}}$ *divisible par* $\mathfrak{P}$. *Connaissant les groupes de décomposition, d'inertie et de ramification de* $\mathfrak{P}$ *par rapport à k, déterminer ceux de* $\overline{\mathfrak{P}}$.

Pour les groupes de décomposition et d'inertie (que nous ne traitons que pour être complets), la solution était déjà, en principe, connue. Elle est d'ailleurs très simple (§ 1). Nous donnons au paragraphe 3 quelques applications et terminons (§ 4) par l'étude du corps composé à partir de deux autres; nous appliquons les théorèmes obtenus dans ce dernier paragraphe à une question de la théorie du corps de classes.

Notations pour les paragraphes 1, 2 et 3.

Soient k un corps de nombres algébriques, K un sur-corps galoisien de k, N son degré relatif, G le groupe de Galois de K par rapport à k, d'ordre N; $\mathfrak{P}$ un idéal premier de K, F son degré relatif, $\mathfrak{p}$ l'idéal premier de k divisible par $\mathfrak{P}$, $\mathfrak{P}^{\mathrm{E}}$ la puissance de $\mathfrak{P}$ contenue dans $\mathfrak{p}$, p le nombre premier rationnel divisible par $\mathfrak{p}$; on a

$$\mathrm{E} = \mathrm{E}_0 p^{\mathrm{M}},$$

E_0 étant premier à p.

Soient G_0 le groupe de décomposition de $\mathfrak{P}$, composé des substitutions σ telles que

$$\alpha \equiv 0 \pmod{\mathfrak{P}}$$

entraîne

$$\sigma\alpha \equiv 0 \pmod{\mathfrak{P}},$$

G_1 le groupe d'inertie, G_i le $(i-1)^{\text{ième}}$ groupe de ramification. $\mathrm{G}_i (i \geq 1)$ est composé des σ telles que

$$\sigma\mathrm{A} \equiv \mathrm{A} \pmod{\mathfrak{P}^i}$$

pour tous les A entiers et premiers à $\mathfrak{P}$.

Soit N_i l'ordre de G_i; on a donc

$$N_0 = EF, \qquad N_1 = E, \qquad N_2 = p^M.$$

Soit maintenant $\overline{K}$ un sous-corps de K, sur-corps de k; g le groupe de K par rapport à $\overline{K}$, $\overline{\mathfrak{P}}$ l'idéal premier de $\overline{K}$ qui contient $\mathfrak{P}$.

Appelons g_i le groupe commun à g et à G_i, n_i son ordre. On sait que :

THÉORÈME I. — *g_0 est groupe de décomposition, g_1 groupe d'inertie, g_i, $(i-1)^{\text{ième}}$ groupe de ramification, de $\mathfrak{P}$ par rapport à $\overline{K}$.*

Cela résulte de la définition même de ces groupes.

Supposons maintenant $\overline{K}$ galoisien par rapport à k.

Soit γ le groupe quotient de G par g; c'est donc le groupe de $\overline{K}$ par rapport à k.

Soit Γ_i le plus petit groupe contenant g et G_i, γ_i' le groupe quotient de Γ_i par g, μ_i' son ordre; on a évidemment (1),

$$\mu_i' = \frac{N_i}{n_i},$$

γ_i peut être considéré comme un sous-groupe de γ.

Appelons f le degré de $\mathfrak{P}$ par rapport à $\overline{K}$; soit $\overline{\mathfrak{P}}^e$ la plus grande puissance de $\mathfrak{P}$ par laquelle est divisible $\overline{\mathfrak{P}}$; posons

$$e = e_0 p^m,$$

e_0 étant premier à p.

On a

$$n_0 = ef, \qquad n_1 = e, \qquad n_2 = p^m.$$

Soient enfin γ_0 le groupe de décomposition de $\overline{\mathfrak{P}}$ par rapport à k,

---

(1) Nous nous servons du théorème suivant : *Étant donnés deux sous-groupes de G, g et g' dont l'un g est invariant, soient $[g, g']$ le plus grand groupe appartenant à la fois à g et à g', (g, g') le plus petit groupe qui les contienne tous deux; $[g, g']$ est invariant dans g', et les groupes quotients de (g, g') par g, et de g' par $[g, g']$, sont isomorphes.*

On énonce en général ce théorème en supposant aussi g' invariant : c'est inutile (*voir* SPEISER, *Gruppentheorie*, Th. 25).

γ_1 son groupe d'inertie, γ_i son $(i-1)^{\text{ième}}$ groupe de ramification, μ_i l'ordre de γ_i.

Le degré de $\mathfrak{P}$ par rapport à k est évidemment $\frac{F}{f}$ et la plus haute puissance de $\mathfrak{P}$ par laquelle est divisible $\mathfrak{p}$ est $\frac{E}{e}$. On a donc

$$\mu_0 = \frac{EF}{ef}, \qquad \mu_1 = \frac{E}{e}, \qquad \mu_2 = p^{M-m},$$

car μ_2 est égal à la plus haute puissance de p contenue dans μ_1.

1. *Détermination des groupes* $\gamma_0, \gamma_1, \gamma_2$:

THÉORÈME II. — *γ'_0 est groupe de décomposition, γ'_1 groupe d'inertie, γ'_2 premier groupe de ramification de $\mathfrak{P}$ par rapport à k.*

Cherchons les substitutions σ de G pour lesquelles $\overline{A} \equiv o(\mathfrak{P})$ entraîne $\sigma\overline{A} \equiv o(\mathfrak{P})$ pour tout $\overline{A}$ de $\overline{K}$, entier et premier à $\mathfrak{P}$. Ces substitutions forment un groupe Γ'_0; ce groupe contient g, pour lequel $\overline{A} = \sigma\overline{A}$; il contient aussi G_0, donc il contient Γ_0.

Or γ_0 n'est évidemment autre que le groupe quotient de Γ'_0 par g, donc γ_0 contient γ'_0.

Mais l'ordre de γ_0 est $\frac{E}{e}\frac{F}{f}$, c'est aussi l'ordre de γ'_0. Donc,

$$\gamma_0 = \gamma'_0.$$

Cherchons de même les substitutions σ de G telles que $\sigma\overline{A} \equiv \overline{A}(\mathfrak{P})$ pour tout $\overline{A}$ de $\overline{K}$, entier et premier à $\mathfrak{P}$. On conclura de même que

$$\gamma_1 = \gamma'_1.$$

L'ordre de γ_1 est $\frac{E}{e}p^{M-m}$, celui de γ'_2 est $\frac{N_2}{n_2} = p^{M-m}$; γ_2 étant invariant dans γ_1 et d'ordre p^{M-m} doit coïncider avec γ'_2. En effet, dans le cas contraire, ils seraient contenus tous deux dans un sous-groupe de γ_1, dont l'ordre serait une puissance de p [d'après la remarque de la Note (1) de la page 483], ce qui est impossible. Donc,

$$\gamma_2 = \gamma'_2.$$

2. *Détermination des groupes* $\gamma_i (i \geq 1)$. — Elle aura lieu sur la base

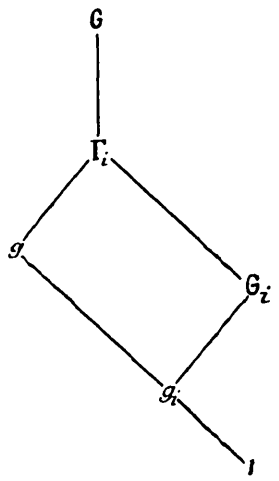
du théorème 40 de Hilbert. Soient $\alpha_1, \alpha_2, \ldots, \alpha_n$ des nombres formant une base des entiers de K (tout autre entier étant une combinaison linéaire à coefficients entiers de ceux-là), $u_1, u_2, \ldots, u_n$ des indéterminées,

$$\Xi = u_1\alpha_1 + u_2\alpha_2 + \ldots + u_n\alpha_n$$

est dite la forme fondamentale de K. On définit de même la forme fondamentale ζ de $\overline{K}$. Dans ce qui suit, le signe $\_\_$ entre deux polynomes en u signifie que leurs contenus (c'est-à-dire l'idéal P. G. C. D. des coefficients) sont les mêmes. On sait que la signification de Ξ résulte du fait que la différente de K par rapport à k est le contenu du produit des $\Xi - \sigma\Xi$, σ parcourant toutes les substitutions de G différentes de la substitution unité.

On voit, en outre, que la contribution (¹) de $\mathfrak{P}$ à $\Xi - \sigma\Xi$ est $\mathfrak{P}^i$ si, et seulement si, σ est dans G_i sans être dans G_{i+1}.

Fig. 1.



Prenons un $\tau\zeta$ de ζ (τ dans G); soient $\sigma_1, \sigma_2, \ldots, \sigma_n$ les éléments de g. Le théorème précité revient à l'équivalence suivante :

$$\zeta - \tau\zeta \simeq (\Xi - \sigma_1\tau\Xi)(\Xi - \sigma_2\tau\Xi)\ldots(\Xi - \sigma_n\tau\Xi).$$

Supposons que τ, considéré comme élément de γ, appartienne à γ_i et

(¹) On appelle « contribution d'un idéal $\mathfrak{a}$ à un idéal $\mathfrak{b}$ », la plus haute puissance de $\mathfrak{a}$ par laquelle est divisible $\mathfrak{b}$.

non à γ_{i+1} ; alors la contribution de $\mathfrak{P}$ au contenu du premier membre est égale à $\overline{\mathfrak{P}}^i$, donc celle de $\mathfrak{P}$ à $\mathfrak{P}^{n_i}$. Cherchons celle de $\mathfrak{P}$ au deuxième membre.

D'abord, le nombre des $\sigma_u\tau$ compris dans G_i est égal à n_i ou à o, selon que τ est dans Γ_i ou n'y est pas. En effet, s'il y a des $\sigma_u\tau$ dans G_i, τ est évidemment dans Γ_i. Supposons réciproquement τ dans Γ_i, décomposons G_i suivant g_i,

$$G_i = g_i\rho_1 + g_i\rho_2 + \ldots + g_i\rho_{\mu_i}.$$

Les éléments de Γ_i sont évidemment les suivants :

$$g\rho_1 + g\rho_2 + \ldots + g\rho_{\mu_i}.$$

On a donc

$$\tau = \sigma_j\rho_k.$$

Les $\sigma_u\tau$ sont de forme $\sigma_u\sigma_j\rho_k$; pour qu'un d'entre eux, $\sigma_u\tau$ soit dans g_i, il faut que $\sigma_u\sigma_j$ soit dans g_i ; on voit donc bien qu'il y a n_i des σ_u qui satisfont à cette condition.

Supposons donc τ compris dans $\Gamma_1, \Gamma_2, \ldots, \Gamma_{i'}$ et non dans $\Gamma_{i'+1}$. Le nombre des $\sigma_u\tau$ compris dans G_j et non dans G_{j+1} $(j \leqq i'-1)$ est $n_j - n_{j+1}$, celui des $\sigma_u\tau$ compris dans $G_{i'}$ est $n_{i'}$ et aucun $\sigma_u\tau$ n'est dans $G_{i'+1}$. La contribution de $\mathfrak{P}$ au deuxième membre est donc une puissance de $\mathfrak{P}$ d'exposant :

$$\begin{aligned}&(n_1 - n_2) + 2(n_2 - n_3) + \ldots \\ &\quad + (i'-1)(n_{i'-1} - n_{i'}) + i' n_{i'} = n_1 + n_2 + \ldots + n_{i'}.\end{aligned}$$

Donc,

$$ei = n_1 + n_2 + \ldots + n_{i'}.$$

Donc, si τ est dans γ_i et non dans γ_{i+1}, il y a un i' satisfaisant à cette équation, tel que τ soit dans $\gamma_{i'}$ et non dans $\gamma_{i'+1}$.

Si l'on se rappelle que $e = n_1$, on a donc le théorème :

THÉORÈME III. — *On peut diviser la suite $n_1, n_2, n_3, \ldots$ en segments de somme n_1, autrement dit, on peut déterminer une suite d'indices*

$$2 < i_1 < i_2 < \ldots,$$

telle que

$$\begin{aligned}
&n_2 + n_3 \quad + \ldots + n_{i_1-1} = n_1,\\
&n_{i_1} + n_{i_1+1} + \ldots + n_{i_2-1} = n_1,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
&n_{i_s} + n_{i_s+1} + \ldots + n_{i_{s+1}-1} = n_1,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots,
\end{aligned}$$

et l'on a alors

$$\begin{aligned}
&\gamma'_2 = \gamma'_3 \quad = \ldots = \gamma'_{i_1-1} = \gamma_2,\\
&\gamma'_{i_1} = \gamma'_{i_1+1} = \ldots = \gamma'_{i_2-1} = \gamma_3,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
&\gamma'_{i_s} = \gamma'_{i_s+1} = \ldots = \gamma'_{i_{s+1}-1} = \gamma_{s+2},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots.
\end{aligned}$$

En particulier, *tous les* $\frac{N_i}{n_i}$ *sont les mêmes dans un même segment.*

Pour le groupe d'inertie et le premier groupe de ramification, on retrouve le résultat du théorème II. On remarquera que dans le cas où G (ou même G_1 seulement) est abélien, les résultats de Hasse (¹) permettent de préciser beaucoup la nature des choses; son théorème (V) donne, en effet, ce qui suit :

Supposons

$$\begin{aligned}
&G_2,\ G_3,\ \ldots,\ G_{w_1+1} \quad \text{d'ordre } p^{M_1},\\
&G_{w_1+2},\ \ldots.\ G_{w_1+w_2+1} \quad \text{d'ordre } p^{M_2},
\end{aligned}$$

et, en général,

$$G_{w_1+w_2+\ldots+w_{s-1}+2},\ \ldots.\ G_{w_1+w_2+\ldots+w_s} \quad \text{d'ordre } p^{M_s},$$

les M_i étant des entiers décroissants.

On a alors les congruences :

$$\begin{aligned}
&w_1 \equiv 0 \pmod{E},\\
&w_2 \equiv 0 \pmod{Ep^{M_1-M_2}},
\end{aligned}$$

et, en général,

$$w_s \equiv 0 \pmod{Ep^{M_s-M_{s+1}}}.$$

(¹) Hasse, *Führer, Discriminante une Verzweigungskörper Relativ-Abelscher Zahlkörper* (*Journal für die reine und angewandte Mathematik*, t. 162, p. 169).

On passe de ses notations aux nôtres par les formules

$$w_s = v_s - v_{s-1}, \quad \text{si } v > 1 \quad \text{et} \quad w_1 = v_1,$$
$$M_s = r_s + r_{s+1} + \ldots.$$

Un semblable résultat s'applique évidemment à la suite des groupes g_i (et des groupes γ_i).

Il en résulte en particulier qu'à l'intérieur d'un même segment, tous les groupes g_i sont égaux.

3. *Applications du théorème III.* — En l'appliquant aux différents sous-groupes invariants de G, ce théorème peut donner des relations entre les ordres des différents groupes de ramification; par exemple, dans un cas simple :

THÉORÈME IV. — *Si* G_i *contient un sous-groupe invariant* g *d'ordre* p, *non contenu dans* G_{i+1}, *on a*

$$\begin{aligned} &G_{i+1} = G_{i+2} = \ldots = G_{i+p}, \\ &G_{i+p-1} = G_{i+p+2} = \ldots = G_{i+2p}, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned}$$

Aux groupes G_i, G_{i+1}, g vont correspondre des corps K_i, K_{i+1}, $\bar{k}$. Appliquons le théorème III en remplaçant le corps k par le corps K_i, le corps $\overline{K}$ par le corps $\bar{k}$.

D'après le théorème I, la suite des groupes d'inertie et de ramification de $\mathfrak{P}$ par rapport à K est alors

$$G_i \ (i \text{ fois}), \quad G_{i+1}, \quad G_{i+2}, \quad \ldots.$$

Par rapport à $\bar{k}$, elle est

$$g \ (i \text{ fois}), \quad 1, \quad 1, \quad \ldots.$$

Le théorème III montre alors l'identité des ordres de

$$G_{i+kp+1}, \quad G_{i+kp+2}, \quad \ldots, \quad G_{i+k+1\,p} \qquad (k \geq 0).$$

Si, en particulier, G_1 est abélien d'ordre Ep^n, il a évidemment un sous-groupe invariant d'ordre E auquel le théorème IV est applicable. Avec les notations de la fin du paragraphe **2**, il viendrait

$$w_1 \equiv w_2 \equiv \ldots \equiv w_i \equiv \ldots \equiv 0 \pmod{E},$$

ce qui est un cas particulier des congruences de Hasse.

Prenons pour k et $\overline{K}$ deux corps intermédiaires entre K_i et K_{i+1},

correspondant aux groupes g et $\bar{g}$, K_j étant le corps correspondant au groupe G_j. La suite des groupes d'inertie et de ramification de $\mathfrak{P}$ par rapport à K_i est alors la suivante (théorème I) :

$$g\ (i \text{ fois}).\quad G_{i+1},\quad G_{i+2},\quad \ldots.$$

Par rapport à K_{i-1}, elle est

$$\bar{g}\ (i \text{ fois}),\quad G_{i+1},\quad G_{i+2},\quad \ldots.$$

Le théorème III montre alors que les *i premiers corps de la suite des corps d'inertie et de ramification de* $\mathfrak{P}$ sont identiques à k, et les suivants à $\overline{K}$. On retrouve là les théorèmes que Hasse désigne par $\mathfrak{S}$ et $\mathfrak{V}$, dans son Mémoire déjà cité.

Il est probable que le théorème III permettrait de simplifier les démonstrations de ce Mémoire, mais cela nécessiterait une étude plus approfondie.

4. *Étude d'un corps composé à partir de deux autres.* — Soit un corps k^*; $\bar{k}$ et K deux sur-corps, $\overline{K}$ le plus petit corps contenant $\bar{k}$ et K, k le plus grand corps contenu dans k et K.

Supposons K galoisien par rapport à k^*, alors $\overline{K}$ l'est par rapport à $\bar{k}$ et a un groupe isomorphe à celui de K par rapport à k.

Soit $\overline{\mathfrak{P}}$ un idéal premier de $\overline{K}$; dans k, K, $\bar{k}$, k^*, il divise respectivement les idéaux premiers $\mathfrak{p}$, $\mathfrak{P}$, $\bar{\mathfrak{p}}$, $\mathfrak{p}^*$.

Le problème se pose de savoir quels sont les groupes de décomposition, d'inertie et de ramification de $\overline{\mathfrak{P}}$ par rapport à $\bar{k}$, connaissant ceux de $\mathfrak{P}$ par rapport à k^*.

Soient donc $\gamma_0, \gamma_1, \gamma_2, \ldots$, la suite des groupes de décomposition, d'inertie et de ramification de $\mathfrak{P}$ dans le groupe de K par rapport à k^*; $\bar{\gamma}_0, \bar{\gamma}_1, \bar{\gamma}_2, \ldots$ la suite des mêmes groupes pour $\overline{\mathfrak{P}}$ dans le groupe de $\overline{K}$ par rapport à $\bar{k}$.

Soient f le degré de l'idéal $\mathfrak{P}$ de K par rapport à k^*, $\bar{f}$ le degré de l'idéal $\overline{\mathfrak{P}}$ de $\overline{K}$ par rapport à $\bar{k}$, φ le degré de l'idéal $\bar{\mathfrak{p}}$ de $\bar{k}$ par rapport à k^*, $\bar{\mathfrak{p}}^e$ la contribution de $\bar{\mathfrak{p}}$ à $\mathfrak{p}^*$.

THÉORÈME IV. — 1° $\bar{\gamma}_0$ *est isomorphe à un sous-groupe de* γ_0, $\bar{\gamma}_1$ *est isomorphe à un sous-groupe de* γ_1, *et, en général,* $\bar{\gamma}_{n+1}$ *est isomorphe à un sous-groupe de* γ_{n+1}.

2° $\bar{f}$ *est un multiple de* $\frac{f}{(f,\varphi)}$ [(f,φ) *désignant le P. G. C. D. de* f *et de* φ].

3° *Si* $\bar{\mathfrak{p}}$ *n'est pas de ramification pour* k^*, *c'est-à-dire si* $e=1$, *on a*

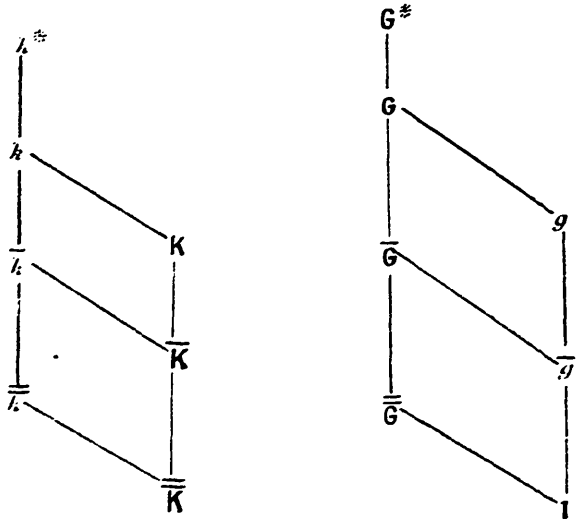
$$\bar{\gamma}_n=\gamma_n$$

pour tout n différent de 0 *et* 4°,

$$\bar{f}=\frac{f}{(f,\varphi)}.$$

Pour démontrer ce théorème (1), on peut supposer k et k^* confondus;

Fig. 2.



(1) Nous faisons désormais les conventions habituelles d'écriture suivantes : le plus petit groupe contenant deux sous-groupes G et G′ d'un même groupe sera désigné par (G, G′); le plus grand groupe contenu à la fois dans G et G′, par [G, G′]; le groupe quotient d'un groupe G, par un de ses sous-groupes invariants g, par $G:g$; le plus petit corps contenant deux corps K et K′, par KK′. Pour exprimer l'isomorphisme de deux groupes G et G′, nous écrirons :

$$G\simeq G'.$$

on passe immédiatement de là au cas général, comme on le voit immédiatement. C'est ce que nous ferons désormais.

Soient $\bar{\bar{k}}$ le plus petit sur-corps de $\bar{k}$ galoisien sur k; $\bar{\bar{K}} = \bar{\bar{k}}K$; G, $\bar{G}$, $\bar{\bar{G}}$, g, $\bar{g}$ les groupes de $\bar{\bar{K}}$ par rapport respectivement aux corps k, $\bar{k}$, $\bar{\bar{k}}$, K, $\bar{K}'$.

$\bar{\bar{k}}$ et K n'ont en commun que des éléments de k (car sans cela un conjugué de $\bar{k}$ aurait avec K d'autres éléments en commun que ceux de k, ce qui est impossible); donc G est le produit direct de $\bar{\bar{G}}$ par g.

Les groupes $G:g$, $\bar{G}:\bar{g}$ et $\bar{\bar{G}}$ sont isomorphes entre eux; les γ_n et les $\bar{\gamma}_n$ pourront donc être considérés comme des sous-groupes de $\bar{\bar{G}}$ (1).

Soient $\bar{\bar{\mathfrak{P}}}$ un diviseur premier de $\bar{\mathfrak{P}}$ dans $\bar{\bar{K}}$; Γ_0 et Γ_1 ses groupes de décomposition et d'inertie. Posons

$$\bar{\Gamma}_0 = [\Gamma_0, \bar{G}] \qquad \text{et} \qquad \bar{\Gamma}_1 = [\Gamma_1, \bar{G}].$$

1° On a

$$\gamma_1 \simeq (\Gamma_1, g) : g.$$

γ_1 est donc le sous-groupe de $G:g$ correspondant à Γ_1, dans l'isomorphisme appliquant G sur $G:g$ et g sur 1.

---

(1) Cette proposition est inexacte comme le montre l'exemple suivant : $k = k' =$ corps des nombres rationnels; $\bar{k} = k(\sqrt[3]{2})$, $K = k(j)$, j désignant une racine cubique primitive de l'unité. On a $\bar{\bar{k}} = k(\sqrt[3]{2}, j)$, $[K.\bar{k}] = k$, $K \subsetneq \bar{\bar{k}}$. Mais la démonstration est indépendante de cette proposition. En effet elle n'a été utilisée qu'aux alinéas 1, 4, 5. Or :

1. Pour montrer que $\bar{\gamma}_0$, $\bar{\gamma}_1$ sont respectivement des sous-groupes de γ_0, γ_1 il suffit de remarquer que :

$$\bar{\gamma}_0 = (\bar{\Gamma}_0, \bar{g}) : \bar{g} \simeq (\bar{\Gamma}_0, \bar{g}, g) : g \qquad \text{et} \qquad (\bar{\Gamma}_0, \bar{g}, g) \subseteq (\Gamma_0, g)$$

et de même pour $\bar{\gamma}_1$.

4. Écrivons

$$\Gamma_1 = \Gamma_0 - \sigma\Gamma_0 - \ldots - \sigma^{F-1}\Gamma_0,$$

et soit x le plus petit exposant > 0 tel que $\sigma^x g$ soit dans (Γ_1, g), y le plus

Mettons les éléments de G sous la forme $\mu\nu$ (μ désignant un élément de $\overline{\overline{G}}$, et ν un élément de g); γ_1 est constitué de tous les μ faisant partie de ces $\mu\nu$.

De même, $\bar{\gamma}_1 = (\bar{\Gamma}_1, \bar{g}) : \bar{g}$. Donc, $\bar{\gamma}_1$ est constitué de tous les μ figurant dans les $\mu\nu$ contenus dans $\bar{\Gamma}_1$, sous-groupe de Γ_1,

Donc, $\bar{\gamma}_1$ est un sous-groupe de γ_1.

Le même raisonnement montrerait que $\bar{\gamma}_0$ est sous-groupe de γ_0.

2° Pour les $\bar{\gamma}_n$, nous emploierons une autre méthode, qui, d'ailleurs, s'appliquerait aussi sans difficultés à $\bar{\gamma}_0$ et $\bar{\gamma}_1$.

Une substitution σ de $\bar{G} : \bar{g}$ permute les éléments de $\bar{K}$ en laissant invariants ceux de $\bar{k}$; en particulier, elle permute ceux de K en laissant invariants ceux de k. On voit donc que l'on peut désigner par la même lettre deux éléments correspondants de $\bar{G} : \bar{g}$ et $G : g$.

σ étant un de ces éléments, $\bar{\gamma}_{ne-1}$ est constitué de ceux de ces σ pour lesquels

$$\sigma\alpha \equiv \alpha \qquad (\text{mod. } \bar{\mathfrak{P}}^{ne-1})$$

pour tous les α de $\bar{K}$ entiers et premiers à $\bar{\mathfrak{P}}$.

Désignons pour un instant par $\bar{\bar{\mathfrak{P}}}^r$, $\bar{\bar{\mathfrak{P}}}^e$, $\bar{\mathfrak{P}}^r$, respectivement les contributions de $\bar{\bar{\mathfrak{P}}}$, $\bar{\bar{\mathfrak{P}}}$, $\bar{\mathfrak{P}}$ à $\bar{\mathfrak{p}}$, $\bar{\mathfrak{P}}$, $\mathfrak{p}$. On a évidemment,

$$\bar{r}_1 e = r_1 \bar{e}.$$

---

petit exposant > 0 tel que σ^x soit dans $\bar{G}$. Alors $(\Gamma_0, g) : (\Gamma_1, g)$ est d'ordre x, donc aussi $\gamma_0 : \gamma_1$, et par suite $f = x$. D'autre part $(\Gamma_0, \bar{g}) = (\bar{\Gamma}_1, g, \bar{\sigma}^x)$. Soit z le plus petit exposant > 0 tel que σ^{xz} soit contenu dans $(\Gamma_1, \bar{g})$. Donc σ^{xz} est contenu dans (Γ_1, g), donc $yz \equiv 0 \pmod{x}$. D'autre part, $\overline{\sigma^{xy}}$ est contenu dans $\bar{G}$ et dans (Γ_1, g), puisque $\bar{g}$ est la partie commune à $\bar{G}$ et à g, et que $\Gamma_1 \subset \bar{G}$, cet élément est aussi continu dans $\Gamma_1, \bar{g}$, et par suite $z = \frac{x}{(x, y)}$. Or $\gamma_0 : \gamma_1$ est d'ordre z: donc $\bar{f} = z$.

3. Le fait que $\gamma_n, \bar{\gamma}_n$ sont des sous-groupes de G n'intervient pas dans la démonstration.

Enfin remarquons que sous les hypothèses du théorème IV *bis* la proposition en question devient exacte.

Or, d'après ce qu'on a démontré plus haut, $\overline{r}_1 \leqq r_1$ (car $\overline{r}_1$ et r_1 sont les ordres de $\overline{\gamma}_1$ et γ_1). Donc, $\overline{e} \leqq e$.

Appliquant l'égalité ci-dessus aux α de K entiers et premiers à $\mathfrak{P}$, on en tire alors

$$\sigma\alpha \equiv \alpha \pmod{\mathfrak{P}^{n-1}}.$$

Donc, tout élément de $\overline{\gamma}_{ne+1}$ est dans γ_{n+1}.

3° $\overline{f}\varphi$, degré de $\overline{\mathfrak{P}}$ par rapport à k est un multiple de f; donc, f est un multiple de $\frac{f}{(f,\varphi)}$.

4° Si $\overline{\mathfrak{p}}$ n'est pas un idéal de ramification, Γ_1 est dans $\overline{G}$; donc.

$$\Gamma_1 = \overline{\Gamma}_1 \qquad \text{et} \qquad \gamma_1 = \overline{\gamma}_1.$$

Décomposons Γ_0 suivant Γ_1 (qui est invariant dans Γ_1); le quotient étant cyclique (supposons-le d'ordre F), on peut écrire

$$\Gamma_0 = \Gamma_1 + \Gamma_1\alpha\beta + \ldots + \Gamma_1\alpha^{F-1}\beta^{F-1},$$

α étant un élément de $\overline{\overline{G}}$, β un élément de g.

Soient α^x la plus petite puissance de α qui soit dans γ_1, β^y la plus petite puissance de β qui soit dans $\overline{g}$. $\overline{\Gamma}_0$ est engendré par $\overline{\Gamma}_1$ et $\alpha^x\beta^y$. $\alpha^F\beta^F$ étant dans Γ_1, donc dans $\overline{G}$, β^F est dans $\overline{g}$, donc y divise F.

a. Calcul de f. — γ_0 est évidemment engendré par γ_1 et α; donc f est la plus petite puissance de α qui soit dans γ_1, et l'on a

$$f = x.$$

b. Calcul de $\overline{f}$. — $\overline{\gamma}_0$ est de même engendré par $\overline{\gamma}_1 = \gamma_1$ et par α^x; donc $\overline{f}$ est la plus petite puissance de α^x qui soit dans γ_1, et l'on a

$$\overline{f} = \frac{x}{(x,y)}.$$

c. Calcul de φ. — C'est le quotient de F, degré de $\overline{\overline{\mathfrak{P}}}$ par rapport à k, par le degré de $\overline{\overline{\mathfrak{P}}}$ par rapport à $\overline{k}$. Or, ce dernier est la plus petite puissance de $\alpha^x\beta^y$ qui soit dans Γ_1; y divisant F, c'est $\frac{F}{y}$; donc,

$$\varphi = y.$$

De ces résultats résulte, sous l'hypothèse faite,

$$\bar{f} = \frac{f}{(f, \bar{\varphi})}.$$

5° Γ_2, Γ_3, ... étant la suite des groupes de ramification de $\mathfrak{P}$ dans G, tous ces groupes sont dans $\overline{G}$ (sous l'hypothèse $e = 1$); ce sont aussi, d'après le théorème I, les groupes de ramification de $\overline{\mathfrak{P}}$ dans le groupe $\overline{G}$.

Le théorème III permet d'en déduire les groupes γ_n et $\bar{\gamma}_n$. Par exemple, γ_n est sous-groupe de $\overline{G}$ sur lequel s'applique Γ_p (pour un p déterminé par ce théorème) dans l'isomorphisme appliquant G sur $G : g$, donc sur $\overline{\overline{G}}$. Pour γ_n et $\bar{\gamma}_n$, ce p sera le même. Donc,

$$\gamma_n = \bar{\gamma}_n.$$

Remarque. — 1° Il est aisé de préciser légèrement la première partie du théorème IV :

Si $\bar{\gamma}_1$ est un sous-groupe d'indice r de γ_1, alors pour tout n, $\bar{\gamma}_{\frac{ne}{r}+1}$ est un sous-groupe de γ_{n+1}.

Avec les notations de la deuxième partie de la démonstration, il suffit de remarquer qu'on a alors $\bar{e} = \frac{e}{r}$.

2° On déduit immédiatement de la première partie du théorème IV, que :

Si un idéal premier $\mathfrak{p}^*$ de k^* est non ramifié par rapport à $\mathfrak{K}$, ou s'il n'a dans K que des facteurs tous différents du premier degré, il en est de même de tout facteur premier de $\mathfrak{p}^*$ dans $\bar{k}$ par rapport à $\bar{k}$K.

Ce résultat a été démontré directement par Hasse (*Journal für die reine und ang. Math.*, t. 158, p. 238, lemme 2), et reste vrai même si K n'est pas galoisien par rapport à k^*.

3° Il y a un cas particulier où le problème posé par le théorème IV est entièrement résoluble :

THÉORÈME IV *bis.* — *Si* K *et $\bar{\bar{k}}$ (plus petit sur-corps de $\bar{k}$ galoisien par*

rapport à k^*), ont par rapport à k^* des degrés premiers entre eux (auquel cas, on a évidemment $k = k^*$), on a

$$\bar{\gamma}_0 = \gamma_0,$$
$$\bar{\gamma}_1 = \gamma_1,$$

et, en général,

$$\bar{\gamma}_{i-1} = \gamma_{\left[\frac{i}{e}\right]+1},$$

$[x]$ désignant le plus petit entier égal ou supérieur à x.

Les notations sont les mêmes qu'au début de la démonstration du théorème IV. Soit encore $\Gamma_0, \Gamma_1, \Gamma_2, \ldots, \Gamma_i, \ldots$ la suite des groupes de décomposition, d'inertie et de ramification de $\bar{\mathfrak{P}}$ dans G.

G étant le produit direct des deux groupes g et $\bar{\bar{G}}$, dont les ordres sont premiers entre eux, chacun des Γ_i est le produit direct d'un sous-groupe Γ'_i de $\bar{\bar{G}}$, et d'un sous-groupe Γ''_i de g.

Soit $\bar{\Gamma}_i = [\Gamma_i, \bar{G}]$. De même $\bar{\Gamma}_i$ est le produit direct de Γ'_i de $\bar{\bar{G}}$ et de $\bar{\Gamma}''_i$ de g (et $\bar{\Gamma}''_i$ est un sous-groupe de Γ''_i).

Il suffit, dès lors, d'appliquer le théorème II pour voir que

$$\bar{\gamma}_0 = \gamma_0 \qquad \text{et} \qquad \bar{\gamma}_1 = \gamma_1.$$

Pour trouver les groupes de ramification, nous appliquons le théorème III. Mais remarquons que les groupes $\Gamma''_2, \Gamma''_3, \ldots, \Gamma''_i, \ldots$, ou bien les groupes $\Gamma''_2, \Gamma''_3, \ldots, \Gamma''_i, \ldots$, sont tous égaux à l'unité, car leurs ordres doivent être premiers entre eux et sont, d'autre part, des puissances d'un même nombre premier.

Si $\Gamma''_i = 1$ $(i \geqq 2)$, le théorème III montre que $\gamma_i = \bar{\gamma}_i = 1$ pour $i \geqq 2$.

Si $\Gamma''_i = 1$, on a aussi $\bar{\Gamma}''_i = 1$.

Appelons E et $\bar{E}$ les ordres de Γ''_1 et $\bar{\Gamma}''_1$. $\bar{\bar{\mathfrak{P}}}^E$ est la contribution de $\bar{\mathfrak{P}}$ à $\mathfrak{P}$, et $\bar{\bar{\mathfrak{P}}}^{\bar{E}}$ celle de $\bar{\bar{\mathfrak{P}}}$ à $\bar{\mathfrak{P}}$. De l'identité des ordres de γ_1 et $\bar{\gamma}_1$, on déduit immédiatement que la contribution de $\bar{\mathfrak{P}}$ à $\mathfrak{P}$ est $\bar{\mathfrak{P}}^e$ ($e = \bar{e}$ avec les notations de la deuxième partie de la démonstration du théorème IV); donc,

$$E = e\bar{E}.$$

L'application du théorème III donne alors

$$\Gamma'_{iE+2} = \Gamma'_{iE+3} = \ldots = \Gamma'_{i(E+1)+1} = \gamma_{i+2}$$

et

$$\bar{\Gamma}'_{iE+2} = \bar{\Gamma}'_{iE+3} = \ldots = \bar{\Gamma}'_{i(E+1)+1} = \bar{\gamma}_{i+2} \qquad (i \geq 0);$$

d'où

$$\bar{\gamma}_{ie+2} = \bar{\gamma}_{ie+3} = \ldots = \bar{\gamma}_{i(e+1)+1} = \gamma_{i+2}$$

c'est-à-dire

$$\bar{\gamma}_{i+1} = \gamma_{\left\lfloor \frac{i}{e} \right\rfloor + 1}.$$

5. *Applications.* — 1° Les résultats obtenus complètent en certains points ceux de Brauer (*Math. Annalen*, t. 83, p. 357 et suiv.).

2° Ils permettent de démontrer sans peine un très important théorème de Hasse (*Math. Zeitschrift*, t. 31, p. 559).

Si $\bar{k}$ est abélien par rapport à k^* et est corps de classes pour le groupe d'idéaux H *de* k^*, $\bar{\mathrm{K}} = \bar{k}\mathrm{K}$ *est aussi abélien par rapport à* $\bar{k}$, *et est donc corps de classes pour un groupe d'idéaux* $\bar{\mathrm{H}}$ *de* $\bar{k}$. $\bar{\mathrm{H}}$ *est alors formé des idéaux de* $\bar{k}$, *dont la norme par rapport à* k^* *est dans* H.

Il suffit d'utiliser la quatrième partie du théorème IV et seulement dans le cas d'un idéal $\mathfrak{p}^*$ non ramifié dans $\bar{\mathrm{K}}$ ($\Gamma_1 = 1$), où la démonstration est très simple.

Comme on peut toujours multiplier le conducteur par un idéal quelconque, on peut supposer que ce conducteur f est le même pour H et pour $\bar{\mathrm{H}}$ et qu'il est premier au discriminant de $\bar{\mathrm{K}}$ par rapport à k^*. Soit $\bar{\mathfrak{P}}$ un idéal premier quelconque de $\bar{\mathrm{K}}$ premier à f; il divise les idéaux $\mathfrak{p}^*$, $\mathfrak{P}$, $\bar{\mathfrak{p}}$ de k^*, K, $\bar{k}$.

La plus petite puissance de $\mathfrak{p}^*$ qui soit dans H est $\mathfrak{p}^{*f}$.

La plus petite puissance de $\bar{\mathfrak{p}}$ qui soit dans $\bar{\mathrm{H}}$ est $\bar{\mathfrak{p}}^{\bar{f}}$.

La plus petite puissance de $\bar{\mathfrak{p}}$ à norme dans H a pour norme la plus petite puissance de $\mathfrak{p}^{*g}$ qui soit une puissance de $\mathfrak{p}^{*f}$; $\bar{\mathfrak{P}}$ étant premier au discriminant de $\bar{\mathrm{K}}$, on a bien $e = 1$, et le théorème IV donne

$$\bar{f} = \frac{f}{(g, f)};$$

la puissance cherchée est donc $\bar{\mathfrak{p}}^{\bar{f}}$.

Donc, les puissances d'idéaux premiers qui sont dans H et celles qui ont leurs normes dans H sont les mêmes.

Les idéaux à norme dans H forment évidemment un groupe d'idéaux mod f, ayant mêmes puissances d'idéaux premiers que $\overline{H}$, et qui coïncide avec $\overline{H}$.

3° Appelons maintenant f et $\bar{f}$ les conducteurs exacts de H et de $\overline{H}$ (c'est-à-dire les plus petits conducteurs de ces groupes d'idéaux).

D'après le théorème précédent, $\bar{f}$ divise f (*voir* Hasse, *loco citato*).

Mais on peut préciser cette relation dans deux cas :

1° *Si* t *est premier au discriminant de* $\bar{k}$ *par rapport à* k^*, *on a* $\mathfrak{f} = \bar{\mathfrak{f}}$.

Il suffit de montrer que pour tout $\bar{\mathfrak{p}}$ de $\bar{k}$, la contribution de $\bar{\mathfrak{p}}$ à f et à $\bar{\mathfrak{f}}$ est la même.

Or, si $\bar{\mathfrak{p}}$ divise f, on aura $e = 1$. Le théorème IV nous montre alors que la suite des groupes de ramification de $\mathfrak{p}^*$ et de $\bar{\mathfrak{p}}$ est la même. Or, Hasse (¹) a donné l'exposant de la contribution d'un idéal au conducteur en fonction seulement des ordres de ses groupes de ramification.

Donc, si la contribution de $\mathfrak{p}^*$ à f est $\mathfrak{p}^{*a}$, celle de $\bar{\mathfrak{p}}$ à $\bar{\mathfrak{f}}$ est $\bar{\mathfrak{p}}^a$. Or, la contribution de $\bar{\mathfrak{p}}$ à $\mathfrak{p}^*$ est $\bar{\mathfrak{p}}$; donc, sa contribution à f est $\bar{\mathfrak{p}}^a$. La contribution de $\bar{\mathfrak{p}}$ à f et à $\bar{\mathfrak{f}}$ est bien la même.

D'une manière plus générale, ce raisonnement montre que :

Les idéaux premiers de $\bar{k}$ *qui ne divisent pas la différente de* $\bar{k}$ *par rapport à* k^* *entrent avec la même puissance dans* f *et* $\mathfrak{f}^*$, *car pour ces idéaux, on a* $e = 1$.

2° *Si le degré de* K *par rapport à* k^* *est premier au degré par rapport à* k^* *du plus petit sur-corps de* $\bar{k}$ *galoisien par rapport à* k^*, *on a*

$$\bar{\mathfrak{f}} = \frac{\mathfrak{f}}{\mathfrak{d}},$$

$\mathfrak{d}$ *étant le produit des* $\bar{\mathfrak{p}}^{e-1}$, *pour tous les idéaux premiers* $\bar{\mathfrak{p}}$ *de* $\bar{k}$ *divisant* f.

Il résulte de cet énoncé que, *dans ce cas*, f *et* $\bar{\mathfrak{f}}$ *sont divisibles par les mêmes idéaux premiers de* $\bar{k}$.

(¹) *Voir* le travail cité, Note (¹), p. 487.

Supposons γ_1, d'ordre $\tau_1 p^{m_1}$; γ_2, γ_3, ..., γ_{ω_1+1}, d'ordre p^{m_1}, et en général, $\gamma_{\omega_{i-1}+2}$, $\gamma_{\omega_{i-1}+3}$, ..., γ_{ω_i+1}, d'ordre p^{m_i}, les m_i étant des entiers décroissants.

D'après le théorème IV *bis*, γ_1 est d'ordre $\tau_1 p^{m_1}$; $\overline{\gamma}_2$, $\overline{\gamma}_3$, ..., $\overline{\gamma}_{e\omega_1+1}$ sont d'ordre p^{m_1}, et en général, $\overline{\gamma}_{e\omega_{i-1}+2}$, $\overline{\gamma}_{e\omega_{i-1}+3}$, ..., $\overline{\gamma}_{e\omega_i+1}$ d'ordre p^{m_i}.

D'après le théorème de Hasse employé il y a un instant, si $\mathfrak{p}^{1-a}$ est la contribution de $\mathfrak{p}^*$ à $\mathfrak{f}$, on a

$$a = \frac{\omega_1}{\tau_1} + \frac{\omega_2}{\tau_1 p^{m_2-m_1}} + \frac{\omega_3}{\tau_1 p^{m_3-m_1}} + \dots$$

Si $\overline{\mathfrak{p}}^{1-\overline{a}}$ est celle de $\overline{\mathfrak{p}}$ à $\overline{\mathfrak{f}}$, on a de même,

$$\overline{a} = \frac{e\omega_1}{\tau_1} + \frac{e\omega_2}{\tau_1 p^{m_2-m_1}} + \frac{e\omega_3}{\tau_1 p^{m_3-m_1}} + \dots = ea.$$

La contribution de $\overline{\mathfrak{p}}$ à $\mathfrak{p}^*$ étant $\overline{\mathfrak{p}}^r$, sa contribution à $\mathfrak{f}$ est donc $\overline{\mathfrak{p}}^{r(1-a)}$.

Sa contribution à $\overline{\mathfrak{f}}$ est $\overline{\mathfrak{p}}^{1-ea}$; le quotient de ces contributions est bien $\overline{\mathfrak{p}}^{e-1}$ comme il fallait le démontrer.