

JACQUES MARTINET

Le théorème de Herbrand sur les unités

Séminaire de théorie des nombres de Bordeaux (1968-1969), exp. n° 10, p. 1-11

[<http://www.numdam.org/item?id=STNB_1968-1969____A10_0>](http://www.numdam.org/item?id=STNB_1968-1969____A10_0)

© Université Bordeaux 1, 1968-1969, tous droits réservés.

L'accès aux archives du séminaire de théorie des nombres de Bordeaux implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

LE THEOREME DE HERBRAND SUR LES UNITES

par

Jacques MARTINET

-:-:-:-

§ 1. - Le théorème de Minkowski

THEOREME (Minkowski, [6]). Soit K une extension galoisienne du corps $\mathbb{Q}$ des rationnels, de degré fini. Il existe une unité de K qui engendre avec ses conjugués un sous-groupe d'indice fini du groupe des unités.

Démonstration. On s'appuie sur le résultat suivant, qui se rencontre au cours de la démonstration du théorème de Dirichlet (voir par exemple [2]).

Soit K un corps de nombres contenu dans $\mathbb{C}$, dont le groupe des unités n'est pas fini. Il existe une unité ε de K , vérifiant $|\varepsilon| > 1$, $|\sigma \varepsilon| < 1$, pour tout isomorphisme σ de K dans $\mathbb{C}$, outre que l'identité ou, éventuellement, la conjugaison complexe.

On utilise alors le :

LEMME (Minkowski, [6]). - Soit $a_{i,j}$ une matrice réelle à n lignes et n colonnes. Si les inégalités suivantes sont vérifiées :

$$1^\circ) \quad a_{i,i} > 0 \quad \text{pour } 1 \leq i \leq n ,$$

$$2^\circ) \quad a_{i,k} < 0 \quad \text{pour } 1 \leq i , k \leq n , i \neq k ,$$

$$3^\circ) \quad \sum_{j=1}^n a_{i,j} > 0 \quad \text{pour } 1 \leq i \leq n ,$$

alors , $\det(a_{i,j}) \neq 0$.

Preuve du lemme (d'après Artin, [1]). - On suppose $\det(a_{i,j}) = 0$.

Il existe alors n nombres réels non tous nuls $x_i (1 \leq i \leq n)$, tels que $\sum_{j=1}^n a_{i,j} x_j = 0$. Soit i un indice pour lequel $|x_i| = \max_{1 \leq j \leq n} |x_j|$. Quitte à

changer les signes des x_i , on peut supposer $x_i > 0$. On écrit alors

$$a_{i,i} x_i + \sum_{k \neq i} a_{i,k} x_k = 0 . \text{ En majorant } x_k \text{ par } x_i , \text{ on obtient}$$

$$x_i (a_{i,i} + \sum_{k \neq i} a_{i,k}) \leq 0 , \text{ c. q. f. d. .}$$

Démonstration du théorème de Minkowski. - On note σ_i les isomorphismes de K dans $\mathbb{C}$, avec la convention :

$$\text{- pour } 1 \leq i \leq r_1 , \sigma_i(K) \subset \mathbb{R} ,$$

$$\text{- pour } r_1 + 1 \leq i \leq r_2 , \sigma_i(K) \not\subset \mathbb{R} ,$$

$$\text{- pour } r_1 + 1 \leq i \leq r_2 , \text{ le conjugué complexe de } \sigma_i \text{ est } \sigma_{i+r_2} .$$

Rappelons qu'étant données $r = r_1 + r_2 - 1$ unités $\eta_1, \dots, \eta_r$ de K , on appelle régulateur de $\eta_1, \dots, \eta_r$ la valeur absolue du déterminant d'un mineur d'ordre r extrait du tableau

$$\begin{pmatrix} \log |\sigma_i \eta_j| \end{pmatrix}_{\substack{1 \leq i \leq r+1 \\ 1 \leq j \leq r}} ,$$

et que $\eta_1, \dots, \eta_r$ sont indépendantes si et seulement si leur régulateur n'est pas nul.

Soit alors $a_{i,j} = \log |\sigma_i^{-1} \sigma_j \varepsilon|$. Le choix de ε montre que

$$a_{i,i} > 0$$

$$a_{i,j} < 0 \quad \text{pour } i \neq j$$

$$\sum_{j=1}^r a_{i,j} = \log \left| \prod_j \sigma_i^{-1} \sigma_j \varepsilon \right| > 0.$$

On voit donc que le régulateur des r unités $\sigma_j \varepsilon$ ($1 \leq j \leq r$) n'est pas nul. Ces unités sont donc indépendantes, et engendrent par conséquent un sous-groupe d'indice fini du groupe des unités.

§ 2. - Enoncé du théorème de Herbrand ([4], [5])

On se donne un corps de nombres k , une extension galoisienne finie K de k , et on pose $G = \text{Gal}(K/k)$. Si k_i est un conjugué de k , et K_i un conjugué de K contenant k_i , $\text{Gal}(K_i/k_i)$ est isomorphe à G . On suppose k_i réel pour $1 \leq i \leq r_1$, k_i imaginaire pour $r_1+1 \leq i \leq r_1+r_2$, deux tels que k_i n'étant pas imaginaires conjugués. Soit $r = r_1+r_2-1$ et $n = [K:k]$.

Comme K/k est galoisien, les conjugués de K au-dessus d'un même corps k_i sont tous réels ou tous imaginaires. Notons K_i l'un d'entre eux. Pour $r_1+1 \leq i \leq r_1+r_2$, K_i est imaginaire. On convient que K_i est réel pour $1 \leq i \leq \rho_1$, imaginaire pour $\rho_1+1 \leq i \leq \rho_1+\rho_2 = r_1$.

Si K_i est imaginaire et k_i réel, on note σ_i l'élément de G induit par la conjugaison complexe. (On retourne dans G de manière évidente à partir de $\text{Gal}(K_i/k_i)$). Dans les autres cas, on pose $\sigma_i = 1$.

K possède $n\rho_1$ conjugués réels, et $n\rho_2 + n \cdot 2r_2$ conjugués imaginaires. Le nombre de Dirichlet R de K est égal à $n(\rho_1 + r_2) - \frac{n}{2}\rho_2 - 1$ (noter que $\rho_2 > 0$ entraîne n pair).

THEOREME (Herbrand). - On peut trouver dans K $r+1$ unités

$E_1, \dots, E_{r+1}$ possédant les propriétés :

1°) $\sigma_i E_i = E_i$ (i. e. : l'image de E_i dans K_i est dans le sous-corps réel maximal de K_i).

2°) R quelconques des $R+1$ unités $(\sigma E_i)_{1 \leq i \leq r+1}$ sont
 $\sigma \in G \bmod \{1, \sigma_i\}$
indépendantes (i. e. : engendrent un sous-groupe d'indice fini du groupe fini des unités de K).

§ 3. - Démonstration d'après Artin ([1])

Soient $\varphi_i (1 \leq i \leq r+1)$ les valeurs absolues archimédiennes de k prolongeant la valeur absolue usuelle de $\mathbb{Q}$, et $\overline{\varphi_i}$ un prolongement de φ_i à K . On définit $\varphi_{i,\sigma}$ par $\varphi_{i,\sigma}(\alpha) = \varphi_i(\sigma^{-1}\alpha)$, pour $\alpha \in K$, et $\sigma \in G$. On obtient toutes les valeurs absolues de K en prenant les $\varphi_{i,\sigma}$ pour $1 \leq i \leq r+1$, $\sigma \in G \bmod \{1, \sigma_i\}$. (On a bien $R+1$ valeurs absolues). Pour tout i , on peut choisir une unité E'_i vérifiant

$$\varphi_{i,1}(E'_i) > 1, \varphi_{j,\sigma}(E'_i) < 1 \text{ pour } j \neq i \text{ ou } j = i, \sigma \neq 1 \text{ et } \sigma \neq \sigma_i.$$

On pose $E_i = E'_i$ si K_i est réel ou k_i imaginaire, $E_i = E'_i \times \sigma_i E'_i$ si K_i est imaginaire et k_i réel.

Pour $\rho_1 + 1 \leq i \leq \rho_1 + \rho_2$, $\varphi_{i,1}(E_i) = \varphi_{i,1}(E_i'^2) > 1$, et $\varphi_{j,\sigma}(E_i) = \varphi_{j,\sigma}(E_i'^2) < 1$ pour $j \neq i$ ou $j = i, \sigma \notin \{1, \sigma_i\}$.

Ces unités E_i vérifient évidemment la condition $\sigma_i E_i = E_i$.

La méthode de Minkowski prouve immédiatement l'indépendance de R d'entre elles.

On peut énoncer le théorème de Herbrand de la façon suivante :

Il existe $r+1$ unités E_i de K , telles que les "seules relations" entre les E_i sont $\sigma_i E_i = E_i$ et $\prod_{\substack{1 \leq i \leq r+1 \\ \sigma \in G \bmod \{1, \sigma_i\}}} (\sigma E_i)^{m_i(\sigma)} = 1$.

En effet, les $R+1$ unités σE_i ($1 \leq i \leq r+1$, $\sigma \in G \bmod \{1, \sigma_i\}$) sont dépendantes.

On a donc une relation $\prod_{i, \sigma} (\sigma E_i)^{m_i(\sigma)} = 1$ des $m_i(\sigma)$ étant des entiers non tous nuls. Cette relation est la seule, car le groupe engendré est de rang r .

En faisant opérer G , on voit que $m_i(\sigma) = m_i(1)$. En remplaçant E_i par $E_i^{m_i(1)}$, on obtient le résultat cherché.

§ 4. - Une conséquence du théorème de Herbrand, d'après Artin ([1]).

On pose $n_i = n$ si $1 \leq i \leq \rho_1$ ou $i \geq r_1+1$, $n_i = \frac{n}{2}$ si $\rho_1+1 \leq i \leq \rho_1+\rho_2=r_1$. On note N_i la norme de K relativement à k si $n_i = n$, et la norme du sous-corps de K fixe pour σ_i relativement à k si $n_i = \frac{n}{2}$.

THEOREME. Il existe $r+1$ unités $H_1, \dots, H_{r+1}$ de K , possédant les propriétés :

$$1^\circ) \quad \sigma_i H_i = H_i$$

$$2^\circ) \quad N_i(H_i) = 1$$

3°) Les conjugués des suites H_i engendrent avec r unités indépendantes de k un sous-groupe d'indice fini.

Démonstration. - Soit $\eta_i = N_i(E_i)$, où les E_i vérifient le théorème du § 3. La seule relation entre les η_i est $\eta_1 \eta_2 \dots \eta_{r+1} = 1$; les unités $\eta_1, \dots, \eta_r$ sont donc indépendantes. Il suffit alors de poser $H_i = \frac{E_i^{n_i}}{\eta_i}$ pour vérifier le théorème ci-dessus.

§ 5. - Rappels sur les représentations

Rappels. - On se donne un groupe fini G , un corps K dont la caractéristique ne divise pas $\text{card } G$. On appelle représentation de G un K -espace vectoriel de dimension finie sur lequel G opère, autrement dit un $K[G]$ -module. Un sous-espace stable V' de V s'appelle une sous-représentation.

THEOREME DE MASCHKE. Tout sous-espace stable possède une supplémentaire stable (à cause de l'hypothèse "la caractéristique de K ne divise pas $\text{card } G$ ").

COROLLAIRE. Toute représentation est somme directe de représentations irréductibles (i. e. : de sous-espaces stables V_i , tels que les seuls sous-espaces stables de V_i soient (0) et V_i).

Interprétation : $K[G]$ est semi-simple, car $\text{caract}(K) \nmid \text{card } G$. Une représentation V est donc un module semi-simple, qui est somme directe de ses sous-modules simples V_i .

Exemples - 1 - La représentation unité I . On prend V de dimension 1, G opérant trivialement.

2 - Les représentations induites. Soit H un sous-groupe de G , V une représentation de H . On appelle représentation de G induite par V la représentation $W = K[G] \otimes_{K[H]} V$ (extension des scalaires).

3 - La représentation régulière A . On prend un espace vectoriel V , de dimension $n = \text{card } G$, avec pour base $(e_s)_{s \in G}$. On fait opérer G sur V par $s e_t = e_{st}$. On obtient la représentation régulière : V s'identifie à $K[G]_s$ ($K[G]$ est un $K[G]$ -module à gauche sur lui-même), et $A = K[G] \otimes_K I$ est induite pour la représentation unité de 1_G .

Vocabulaire : Si V' est une sous-représentation de V , on dit que V contient V' . Si V contient un sous-espace isomorphe à la somme directe de n copies de V' , n le plus grand possible, on dit que V contient n fois V' . On peut toujours écrire $V = \sum n_i V_i$, avec des V_i inducibles, et ceci est unique.

Soit V une représentation de G dans $\mathbb{C}$. On définit son caractère χ : c'est une application de G dans $\mathbb{C}$ définie par $\chi(\sigma) = \text{Tr}(x \mapsto \sigma x)$ ($\sigma \in G$, et $\text{Tr}(U)$ désigne la trace d'un endomorphisme U).

On a les résultats suivants :

- a) Deux représentations sont isomorphes si et seulement si elles ont même caractère.
- b) Tout caractère est combinaison linéaire à coefficients rationnels de caractères de représentations induites par des sous-groupes cycliques de G .

§ 6. - Réduction du théorème de Herbrand à un théorème de représentation

On garde les notations des paragraphes précédents.

Soit $V = U_K \otimes_Z \mathbb{Q}$, où G opère par $s(\varepsilon \otimes r) = s\varepsilon \otimes r$. V est une représentation de G sur $\mathbb{Q}$ de dimension R . Il suffira de trouver les "unités" de V engendrant V avec leurs conjugués conformément à l'énoncé du théorème. On peut remplacer V par $V \otimes_{\mathbb{Q}} \mathbb{C} = U_K \otimes_Z \mathbb{C}$.

On note A la représentation régulière, I la représentation unité. On introduit les représentations B_i de la façon suivante : soit i un indice compris entre $\rho_1 + 1$ et $\rho_1 + \rho_2 = r_1$, σ_i l'élément d'ordre 2 défini à partir de la conjugaison complexe de K_i / k_i . On appelle B_i la représentation induite par la représentation régulière du sous-groupe $\{1, \sigma_i\}$ de G . Remarquons qu'on pourrait définir B_i pour tout i : si $i \leq \rho$, ou $i \geq r_1 + 1$, $B_i \approx A$.

On note $X_{K,k}$ la représentation $(\rho_1 + r_2)A + \sum_{i=\rho_1+1}^{\rho_1+\rho_2} B_i$. La dimension de $X_{K,k}$ est $n(\rho_1 + r_2) + \frac{n}{2} \rho_2 = R + 1$.

THEOREME DE HERBRAND. $V + I = X_{K,k}$.

Cela est bien un énoncé équivalent au théorème que nous avons démontré. Tout le problème est de démontrer l'égalité ci-dessus. On va pour cela contrôler que chaque représentation irréductible de G est contenue le même nombre de fois dans $V + I$ et $X_{K,k}$.

§ 7. - Démonstration de légalité $V+I = X_{K,k}$

a) Regardons tout d'abord la représentation unité. Dans V , elle est contenu un nombre de fois égal à la dimension du sous-espace V^G de V fixe par G . Cette dimension est r (rang du groupe des unités de k). I est contenue $(r+1)$ fois dans $V+I$. Il suffit de contrôler que I est contenue une fois dans chacune des représentations A et B_i , ce qui résulte de résultats généraux, on se regarde directement sur une base.

b) LEMME SUR LES SOUS-GROUPES. Soit g un sous-groupe de G , $\bar{k}$ le sous-corps de K fixe par g . Alors $X_{K,k}$ considéré comme représentation de g coïncide avec $X_{K,\bar{k}}$.

Notons m l'indice de g dans G .

Si K_i est réel ou k_i imaginaire, on remarque que A , comme représentation de g est équivalente à ma (a : représentation régulière de g).

Supposons $p_1+1 \leq i \leq r_1$ (k_i réel, K_i imaginaire).

On écrit $G = \bigcup_{i=1}^m g T_i$, $T_i \in G$.

$$T_i^{-1} k \text{ réel} \Leftrightarrow \sigma_i \in T_i^{-1} g T_i \Rightarrow \lambda_i = T_i \sigma_i T_i^{-1} \in G.$$

On indexe les T_i pour que $\lambda_i \in g$ pour $1 \leq i \leq p$ et $\lambda_i \notin g$ pour $p+1 \leq i \leq p+2q = m$. On a une somme directe de représentations, qui donne $pa + b_{p+1} + \dots + b_{p+q-1}$.

c) Réduction au cas cyclique. On passe par les caractères.

On suppose le théorème démontré lorsque $\text{gal}(K/k)$ est cyclique. $V+I$ et $X_{K,k}$ ont même caractère: en effet, la valeur du caractère en $\sigma \in G$ est celle calculée sur un sous-groupe cyclique contenant σ .

d) Preuve dans le cas cyclique. On écrit $V+I = \sum x_i c_i$ et $X_{K,k} = \sum g_i c_i$, où les c_i désignent des représentations irréductibles. Soit $c_0 = I$ et $c_1 : \sigma \rightarrow \omega$, où σ engendre G et ω est une racine de l'unité ayant même ordre que σ . On considère la différence f des caractères :

$$f(\sigma^a) = \sum_{i=0}^{n-1} z_i \omega^{ai}.$$

Si $(a, n) = 1$, $\rho = f(\sigma^a)$ est indépendant de a : c'est un nombre rationnel, et les $f(\sigma^a)$ sont conjugués.

Si $(a, n) > 1$, $f(\sigma^a) = 0$, par récurrence sur l'ordre de G . Mais $z_0 = 0$, car $x_0 = y_0$ (cela a déjà été vu). Donc,

$$\sum_{(a, m)} f(\sigma^a) = \varphi(m) \rho = 0.$$

Par conséquent, $f(\sigma^a) = 0$ pour $\forall a$, et $z_i = 0$. c. q. f. d.

§ 8. - Remarques diverses

Soit K une extension galoisienne du corps $\mathbb{Q}$ des nombres rationnels, G son groupe de Galois, et soit U_K le quotient du groupe des unités de K par le sous-groupe des racines de l'unité.

Problème. Soit n un entier. Peut-on trouver une unité ε de K dont l'image dans U_K engendre un sous-groupe d'indice premier à n ?

La réponse est positive si $K/\mathbb{Q}$ est cyclique de degré premier p . En effet, U_K est un $\mathbb{Z}[G]$ -module annulé par $(1+\sigma+\dots+\sigma^{p-1})$, σ désignant un générateur de G . On peut donc munir U_K d'une structure de module sur le quotient $\mathbb{Z}[G] / (1+\sigma+\dots+\sigma^{p-1})$. Ce dernier anneau est isomorphe

à l'anneau $\mathbb{Z}[\omega]$, clôture intégrale de $\mathbb{Z}$ dans le corps des racines p èmes de l'unité. C'est donc un anneau de Dedekind, et U_K est un module projectif de rang 1 sur $\mathbb{Z}[\omega]$, donc isomorphe à un idéal de $\mathbb{Z}[\omega]$, ce qui suffit à entraîner la propriété.

J'ignore les résultats dans le cas général. Quant à la question de savoir si on peut trouver une unité de K dont l'image dans U_K engendre U_K comme $\mathbb{Z}[G]$ -module, on peut s'attendre à une réponse négative. Voir à ce sujet A. Brumer [3].

-:-:-:-:-

BIBLIOGRAPHIE

- [1] E. ARTIN. - Über die Einheiten relativ galoisscher Zahlkörper. J.f. Math. 167 (1932) p. 153-156.
- [2] Z.I. BOREVICH et R. SHAFAREVICH. - Number theory. Academic Press (1966).
- [3] A. BRUMER. - On the group of units of an absolutely cyclic number field of prime degree. J. Math. Soc. Japan, 21, n° 3 (1969) p. 357-358.
- [4] J. HERBRAND. - Nouvelle démonstration et généralisation d'un théorème de Minkowski. C.R. A. S. 191 (1930) p. 1282-1285.
- [5] J. HERBRAND. - Sur les unités d'un corps algébrique. C.R. A. S. 192 (1931) p. 24-27.
- [6] MINKOWSKI. - Zur theorie der Einheiten in der algebraischen Zahlkörper - Göttinger Nachrichten (1900) p. 90-94.

-:-:-:-:-