

III. Majoration des hauteurs de \$P_1\$ et \$P_2\$

Objektyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **18 (1972)**

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **26.04.2024**

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.

Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.

Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

utiliserons le plongement logarithmique du corps K et le fait que l'image par ce plongement du groupe des unités est un réseau; il suffira de majorer la norme des images de $Q(x)$ pour des points x de hauteur bornée. Dans le second cas, nous utiliserons simplement le fait que si x a tous ses conjugués assez grands il en est de même de $Q(x)$ et donc que $Q(x)$ ne peut pas être une unité.

II. UNE REMARQUE PRÉLIMINAIRE

Soit P un polynôme unitaire à coefficients dans A qui soit le produit de deux polynômes P_1 et P_2 à coefficients dans A . Les valeurs de ces polynômes en un point x de A donnent lieu à des remarques évidentes: Si $P(x)$ est un élément irréductible de A , l'un des deux éléments $P_1(x)$ et $P_2(x)$ au moins est une unité; si $P(x)$ est une unité, les deux éléments $P_1(x)$ et $P_2(x)$ de A sont des unités; d'où l'inégalité ¹⁾:

LEMME 1:.. *En désignant, pour chaque partie E de A , et tout polynôme Q sur A , par $u(Q, E)$ et $i(R, E)$ le nombre d'éléments de E où la valeur de Q est une unité, respectivement un élément irréductible, on a l'inégalité*

$$i(P, E) + 2u(P, E) \leq u(P_1, E) + u(P_2, E).$$

III. MAJORATION DES HAUTEURS DE P_1 ET P_2

Considérons provisoirement un polynôme g à coefficients complexes et qui ne s'annule pas à l'origine.

Posons

$$g = a_0 X^d + a_1 X^{d-1} + \dots + a_d.$$

Pour simplifier, nous supposons g unitaire. Si g est le produit de deux polynômes unitaires g_1 et g_2 , nous cherchons à majorer les coefficients de g_1 et g_2 . Pour ceci, on utilisera le fait que les coefficients de g_1 sont certaines fonctions des racines du polynôme g . Plus précisément, la somme des coefficients de g_1 est égale à la somme de 2^{d_1} (d_1 désigne le degré de g_1)

¹⁾ Pour plus de détails, voir (1).

produits de certaines racines de g affectés du coefficient ± 1 ¹⁾. Il est clair que chacun de ces produits est majoré en module par le produit des modules des racines de g qui ont un module supérieur à 1. Pour majorer ce produit nous utiliserons un lemme classique de la théorie des fonctions analytiques.

LEMME 2. Soit $f(z) = \sum_0^\infty b_m z^m$ une fonction holomorphe dans le disque $|z| \leq 1$ et telle que $f(0)$ soit non nulle. Soient $\zeta_1, \dots, \zeta_v$ les racines de f dans le disque $|z| < 1$ (répétées chacune autant de fois que son ordre de multiplicité). On a l'inégalité :

$$|b_0| \left(\prod_{j=1}^v |\zeta_j| \right)^{-1} \leq \left(\sum_0^\infty |b_m|^2 \right)^{\frac{1}{2}}.$$

Démonstration :

Posons

$$h(z) = f(z) \prod_{j=1}^v \frac{1 - \bar{\zeta}_j z}{z - \zeta_j} = \sum_0^\infty c_m z^m.$$

La fonction h est holomorphe dans le disque $|z| \leq 1$. De plus, les modules de f et de h coïncident sur le cercle $|z| = 1$. D'où l'égalité :

$$\frac{1}{2\pi} \int_0^{2\pi} |f(e^{i\theta})|^2 d\theta = \frac{1}{2\pi} \int_0^{2\pi} |h(e^{i\theta})|^2 d\theta.$$

En appliquant la formule de Parseval, on en déduit la relation

$$\sum_0^\infty |b_m|^2 = \sum_0^\infty |c_m|^2$$

Mais on a l'égalité

$$|c_0| = |h(0)| = |b_0| \left(\prod_{j=1}^v |\zeta_j| \right)^{-1}.$$

En reportant cette valeur de $|c_0|$ dans l'égalité précédente, on obtient immédiatement l'inégalité

¹⁾ Si g_1 est de la forme $\alpha_0 X^{d_1} + \alpha_1 X^{d_1-1} + \dots + \alpha_{d_1}$ et si $\zeta_1, \zeta_2, \dots, \zeta_{d_1}$ désignent les zéros de g_1 (chaque racine figurant un nombre de fois égal à son ordre multiplicité), on sait qu'au signe près, chaque coefficient α_k de g_1 est la somme de tous les produits de la forme $\zeta_{j_1} \dots \zeta_{j_k}$, où les indices $j_1, \dots, j_k$ sont tous distincts. Ainsi α_k est la somme de $\binom{d_1}{k}$ produits de cette forme. La somme des α_k est donc égale à la somme de 2^{d_1} produits du type $(-1)^k \zeta_{j_1} \dots \zeta_{j_k}$.

$$|b_0| \left(\prod_{j=1}^v |\zeta_j| \right)^{-1} \leq \left(\sum_0^\infty |b_m|^2 \right)^{\frac{1}{2}}.$$

Ceci achève la démonstration du lemme.

Revenons au polynôme g . D'après le lemme 2, le produit des racines de g situées dans le disque $|z| \leq 1$ a un inverse dont le module est majoré par la quantité $\left(\sum_0^d |a_i|^2 \right)^{\frac{1}{2}} |a_0|^{-1}$. Puisque g est unitaire le produit de toutes ses racines a pour module $|a_d|$. Ceci montre que le produit de racines de g situées à l'extérieur du disque $|z| \leq 1$ a un module majoré par $\left(\sum_0^d |a_i|^2 \right)^{\frac{1}{2}}$. De cette majoration et des remarques qui précèdent le lemme 2, on déduit que la somme des modules des coefficients du polynôme g_1 est majorée par $2^{d_1} \left(\sum_0^d |a_i|^2 \right)^{\frac{1}{2}}$. D'où:

LEMME 3. Soit $g = a_0 X^d + a_1 X^{d-1} + \dots + a_d$ un polynôme unitaire à coefficients complexes qui ne s'annule pas à l'origine. Soit g_1 un polynôme unitaire de degré d_1 qui divise g . Alors, la somme des modules des coefficients de g_1 est majorée par $2^{d_1} \left(\sum_0^d |a_i|^2 \right)^{\frac{1}{2}}$.

Cette majoration va nous permettre de majorer les hauteurs des polynômes P_1 et P_2 en fonction de celle de P . Auparavant, il nous faut introduire plusieurs définitions.

Soit n le degré du corps de nombres K . On sait qu'il y a exactement n isomorphismes distincts σ_i du corps K dans le corps des complexes.

Soit Q un polynôme unitaire à coefficients dans K . Si Q est égal à $b_0 X^d + b_1 X^{d-1} + \dots + b_d$, on pose

$$|Q|_1 = \max_i \sum_0^d |\sigma_i(b_j)|, \quad |Q|_2 = \max_i \left(\sum_0^d |\sigma_i(b_j)|^2 \right)^{\frac{1}{2}}.$$

Soit P un polynôme unitaire à coefficients dans A et qui ne s'annule pas à l'origine et soit P_1 un polynôme unitaire à coefficients dans A qui divise P . En appliquant le lemme 3 aux différents polynômes $\sigma_i P$ et $\sigma_i P_1$ (notations évidentes !), on obtient la majoration suivante:

LEMME 4. Soit P un polynôme unitaire à coefficients dans A qui ne s'annule pas à l'origine. Soit P_1 un polynôme unitaire à coefficients dans A et qui divise P . On a l'inégalité:

$$|P_1|_1 \leq 2^{d_1} |P|_2,$$

où d_1 désigne le degré de P_1 .

IV. PREMIER CHOIX DE E

Si x est un élément de A , on définit la hauteur de x par la formule

$$h(x) = \max_i |\sigma_i(x)|.$$

Soit Q un polynôme unitaire à coefficients dans A et qui ne s'annule pas à l'origine. Nous nous proposons de majorer le nombre de points x de A de hauteur au plus égale à a et tels que $Q(x)$ soit une unité.

Nous allons utiliser le plongement logarithmique de K^* . Il nous faut encore introduire quelques définitions.

Soit r_1 le nombre des indices i tels que l'image de K par σ_i soit incluse dans le corps des réels; alors les autres indices sont en nombre pair $2r_2$. On peut numérotter les σ_i de sorte que l'image de σ_i soit contenue dans $\mathbf{R}$ pour $i \leq r_1$ et que $\sigma_{j+r_2} = \bar{\sigma}^j$ pour $r_1 + 1 \leq j \leq r_1 + r_2$.

Le plongement logarithmique de K^* dans $\mathbf{R}^{r_1+r_2}$ est l'application L définie par la flèche

$$x \rightarrow (\text{Log } |\sigma_1(x)|, \dots, \text{Log } |\sigma_{r_1+r_2}(x)|).$$

Soient A^* l'ensemble des entiers non nuls et U l'ensemble des unités de A . On sait que le noyau de la restriction de L à A^* est constitué par les racines de l'unité contenues dans K .

L'image $L(U)$ est contenue dans l'hyperplan W d'équation

$$\sum_{i=1}^{r_1} y_i + 2 \sum_{j=r_1+1}^{r_1+r_2} y_j = 0.$$

Ceci ne fait que traduire le fait que x est une unité si et seulement si sa norme a pour module 1.

On montre facilement que l'image $L(U)$ est un sous-groupe discret de W ; son rang est donc majoré par $r = r_1 + r_2 - 1$. En fait le théorème de Dirichlet dit que le rang de $L(U)$ est exactement r , mais cette majoration nous suffira.

Revenons au polynôme Q et posons

$$u_a(Q) = \text{Card} \{ x \mid x \in A, h(x) \leq a \text{ et } Q(x) \in U \}$$