IV. Premier choix de E

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **25.09.2024**

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

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 inclue dans le corps des réels; alors les autres indices sont en nombre pair $2r_2$. On peut numéroter 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

$$x \to (\mathrm{Log} |\sigma_1(x)|, \ldots, \mathrm{Log} |\sigma_{r_1+r_2}(x)|) .$$

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

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

Nous cherchons à majorer $u_a(Q)$.

Un polynôme de degré donné ne peut prendre une certaine valeur qu'un nombre de fois au plus égal à son degré.

D'où l'inégalité

$$u_a(Q) \leq \deg Q \,.\, \mathrm{card}\,(\{ Q(x) \mid x \in A \quad \text{et} \quad h(x) \leq a \} \cap U)\,.$$

Désignons par w le nombre de racines de l'unité contenues dans K. D'après la caractérisation du noyau de $L_{|U}$ et l'inégalité précédente, on obtient:

$$(1) \qquad u_a(Q) \leq w \,.\, \deg Q \,.\, \mathrm{card}\,(J \cap R)\,,$$

où on a posé

$$J = L(\{ Q(x) \mid x \in A \quad \text{et} \quad h(x) \leq u \})\,, \quad R = L(U)\,.$$

Pour majorer le nombre d'éléments de $J \cap R$, nous procéderons en deux étapes:

1° L'image J est contenue dans une certaine boule B de l'espace $\mathbf{R}^{r_1+r_2}$.

2° On majore le nombre d'éléments de R contenus dans la boule B.

Première étape.

Soit S un réel ≥ 1 qui sera fixé ultérieurement. On suppose que le polynôme satisfait à la condition

$$| Q |_1 \leq S\,.$$

Désignons par $\|\ \ \|$ la norme euclidienne de $\mathbf{R}^{r_1+r_2}$.

Démontrons le résultat suivant:

Lemme 5. *Soit $a \geq 2$. Il existe une constante C_0 explicite, qui ne dépend que de S et de K, telle que si x vérifie $h(x) \leq a$ et si $Q(x)$ est non nul on ait l'inégalité:*

$$\| L(Q(x)(\| \leq C_0 \,.\, \mathrm{Log}\, a \,.\, \deg Q\,.$$

Démonstration:

Posons $x' = Q(x)$ pour un certain x de hauteur majorée par a et tel que $Q(x)$ soit non nul.

On a d'abord l'inégalité évidente

$$\| L(x') \| \leq (r_1 + r_2) \max_i \left(| \mathrm{Log} \,| \sigma_i(x') | \,| \right).$$

Pour majorer $|\operatorname{Log}|\sigma_i(x')||$, on majore $\operatorname{Log}|\sigma_i(x')|$ puis on le minore. Autrement dit, on encadre $|\sigma_i(x')|$.

— *majoration des* $|\sigma_i(x')|$.

Reprenons la notation

$$Q = b_0X^d + b_1X^{d-1} + \ldots + b_d .$$

On a alors l'inégalité

$$|\sigma_i(x')| \leqq \sum_{j=0}^{d} |\sigma_i(b_jx^{d-j})| .$$

On en déduit facilement l'inégalité

$$|\sigma_i(x')| \leqq S\,a^d .$$

— *minoration des* $|\sigma_i(x')|$.

Le procédé est classique. Du fait que x' est entier non nul, il a une norme au moins égale à 1 en module. D'où l'inégalité

$$|\sigma_i(x')| \geqq \prod_{j\neq i} |\sigma_j(x')|^{-1} .$$

Grâce à la majoration précédente des $|\sigma_j(x')|$, on obtient l'inégalité

$$|\sigma_i(x')| \geqq |Sa^d|^{1-n} \geqq |Sa^d|^{-n} .$$

De cet encadrement des $|\sigma_i(x')|$, on déduit la majoration

$$|\operatorname{Log}|\sigma_i(x')|| \leqq n \,.\, \operatorname{Log}(Sa^d) .$$

D'où l'inégalité

$$||L(x')|| \leqq (r_1+r_2)\,n \,.\, \operatorname{Log}(Sa^d) .$$

Si on pose

$$\lambda = 1 + \frac{\operatorname{Log} S}{\operatorname{Log} 2},$$

en tenant compte de l'hypothèse $a \geqq 2$, on voit que l'on a

$$\operatorname{Log}(Sa^d) \leqq \lambda \operatorname{Log} a .$$

D'où finalement l'inégalité

$$||L(x')|| \leqq \deg Q \,.\, C_0 \,.\, \operatorname{Log} a$$

où on a posé

$$C_0 = n(r_1 + r_2) . \lambda .$$

Ceci achève la démonstration du lemme.

Le lemme équivaut à dire que J est contenu dans la boule B de rayon $b = \deg Q . C_0 . \operatorname{Log} a$. Remarquons que b est au moins égal à Log 2.

Deuxième étape.

LEMME 6. *Soit b un réel au moins égal à Log 2. Il existe une constante C_1 explicite, qui ne dépend que de K, telle que le nombre d'éléments du réseau R contenus dans la boule B de rayon b soit majoré par $C_1 b^r$.*

Démonstration :

Soit D le parallélotope fondamental de R.

Il est clair que le nombre m de points de R contenus dans la boule B est majoré par le nombre de mailles de R qui rencontrent B. De plus toutes les mailles qui rencontrent B sont contenues dans la boule B' de rayon $b + S$, où S désigne le diamètre de D.

En comparant les volumes (calculés dans W), on obtient l'inégalité

$$m . \operatorname{vol}(D) \leqq \operatorname{vol} B'.$$

Soit V le volume de la boule unité. L'inégalité précédente conduit à

$$m \leqq V(b+S)^r (\operatorname{vol} D)^{-1}.$$

Comme b est au moins égal à Log 2, le nombre $b + S$ est majoré par μb où μ vaut $1 + \dfrac{S}{\operatorname{Log} 2}$.

D'où l'inégalité

$$m \leqq C_1 b^r ,$$

où on a posé

$$C_1 = V\mu (\operatorname{vol} D)^{-1} .$$

On voit que connaissant K on peut calculer explicitement S et vol D, donc C_1 est bien explicite. Ceci achève la démonstration du lemme.

Conclusion.

THÉORÈME 1. *Soit P un polynôme unitaire à coefficients entiers et qui ne s'annule pas à l'origine. Pour tout $a \geqq 2$, il existe une constante C calculable explicitement et qui ne dépend que de $\deg P$, $|P|_2$ et K, telle que si P est réductible alors on a l'inégalité :*

$$i_a(P) + 2u_a(P) \leqq C(\operatorname{Log} a)^r .$$

(Où $i_a(P)$ désigne le nombre de points x de hauteur majorée par a et tels que $P(x)$ soit un élément irréductible de A).

Démonstration :

Soient P_1 et P_2 deux polynômes à coefficients dans A et de produit P. D'après le lemme 1, nous avons l'inégalité

$$i_a(P) + 2u_a(P) \leqq u_a(P_1) + u_a(P_2) .$$

Soit S le nombre $2^{d-1}|P|_2$; le lemme 4 montre que $|P_1|_1$ et $|P_2|_1$ sont majorés par S.

Nous pouvons maintenant appliquer les lemmes 5 et 6 aux polynômes P_1 et P_2. En tenant compte de l'inégalité (1), nous obtenons les majorations

$$\begin{aligned} u_a(P_1) + u_a(P_2) &\leqq w\, C_1 (C_0 \operatorname{Log} a)^r \big((\deg P_1)^{r+1} + (\deg P_2)^{r+1}\big) \\ &\leqq 2w\, C_1 (C_0 \operatorname{Log} a)^r (\deg P)^{r+1} . \end{aligned}$$

Ceci achève la démonstration du théorème.

Remarque. L'inégalité $a \geqq 2$ n'a été introduite que pour éviter des complications inutiles. Le théorème reste vrai pourvu que l'on suppose $a \geqq \alpha_0$ avec α_0 fixé, $\alpha_0 > 1$, mais cette fois la constante C dépend de α_0.

CRITÈRE 1. *S'il existe $a \geqq 2$ tel que l'on ait l'inégalité*

$$i_a(P) + 2u_a(P) > C(\operatorname{Log} a)^r$$

alors le polynôme P est irréductible dans $K[X]$.

V. DEUXIÈME CHOIX DE E

THÉORÈME 2. *Soit P un polynôme unitaire réductible qui ne s'annule pas à l'origine et à coefficients dans A. Désignons par S le nombre $2^{d-1}|P|_2$, où d est le degré de P.*