CHAPITRE 1

Préliminaires

Nous noterons $\mathbb{N}$ l'ensemble des entiers naturels, $\mathbb{Z}$ l'anneau des entiers rationnels, $\mathbb{Q}$ le corps des nombres rationnels, $\mathbb{R}$ le corps des nombres réels, et $\mathbb{C}$ le corps des nombres complexes.

§1.1 Généralités sur les extensions de corps

Soient K et L deux corps ; si $K \subset L$, on dit que L est une extension de K ; L est alors un K-espace vectoriel, et on dit que L est une extension finie de K si L est un K-espace vectoriel de dimension finie ; cette dimension se note alors

$$[L : K] .$$

Un élément $\alpha \in L$ est dit algébrique sur K s'il existe un polynôme non nul $P \in K[X]$ tel que $P(\alpha) = 0$, c'est-à-dire si l'homomorphisme canonique

$$\beta : K[X] \to L ,$$

qui laisse invariants les éléments de K et envoie X sur α, a un noyau non nul. Ce noyau est alors engendré par un polynôme irréductible $p \in K[X]$, et l'image de β, c'est-à-dire le sous-anneau $K[\alpha]$ de L engendré sur K par α, est isomorphe au corps $K[X]/p(X)$. Si on impose à ce polynôme p d'être unitaire, alors p est unique ; on dit que p est le polynôme irréductible de α sur K.

Inversement, si l'homomorphisme β associé à un élément α de L est injectif, alors on dit que α est transcendant sur K.

Une extension L de K est dite algébrique (sur K) si tout élément de L est algébrique sur K. Par exemple une extension finie est algébrique.

Si E est une partie d'une extension L d'un corps K, on note $K(E)$ le sous-corps de L engendré par E sur K (appelé aussi sous-corps de L obtenu en adjoignant à K les éléments de E), c'est-à-dire l'intersection des sous-corps de L contenant K et E. De même on note $K[E]$ le sous-anneau de L engendré par E sur K. Une extension L d'un corps K est dite de type fini s'il existe une partie finie $E = \{x_1,\dots,x_n\}$ de L telle que

$$L = K(E) = K(x_1,\dots,x_n) .$$

En particulier une extension finie est de type fini, et toute extension algébrique de type fini est finie. D'ailleurs, tous les corps que nous considérerons seront de caractéristique nulle ; alors toute extension finie L d'un corps K est simple, c'est-à-dire qu'il existe $\alpha \in L$ (algébrique sur K) tel que $L = K(\alpha)$ (théorème de l'élément primitif).

Si α est algébrique sur K, on a

$$K(\alpha) = K[\alpha] ,$$

et le degré du polynôme minimal de α sur K est égal à $[K(\alpha) : K]$; on appelle ce nombre degré de α sur K.

Un corps Ω est dit algébriquement clos si tout polynôme non constant (c'est-à-dire de degré supérieur ou égal à 1) de $\Omega[X]$ a au moins une racine dans Ω. Le

corps $\mathbb{C}$ des nombres complexes en fournit un exemple. Si K est un corps, il existe des extensions algébriques de K qui sont algébriquement closes ; si Ω est un corps algébriquement clos contenant K, l'ensemble des éléments de Ω algébriques sur K est appelé clôture algébrique de K dans Ω, et noté $\bar{K}$. Ainsi, nous noterons $\bar{\mathbb{Q}}$ la clôture algébrique de $\mathbb{Q}$ dans $\mathbb{C}$; c'est le sous-corps de $\mathbb{C}$ formé des nombres complexes algébriques sur $\mathbb{Q}$.

§1.2 Corps de nombres

Un nombre complexe est dit algébrique (resp. transcendant) s'il est algébrique sur $\mathbb{Q}$ (resp. transcendant sur $\mathbb{Q}$).

Soit $\alpha \in \bar{\mathbb{Q}}$ un nombre algébrique, et soit p le polynôme irréductible de α sur $\mathbb{Q}$. On peut écrire p sous la forme

$$p(X) = X^n + \frac{a_{n-1}}{b_{n-1}} X^{n-1} + \ldots + \frac{a_0}{b_0},$$

où, pour tout $i = 0,\ldots,n-1$, a_i et b_i sont deux nombres entiers rationnels premiers entre eux, avec $b_i > 0$. Soit c_n le plus petit commun multiple de $b_0,\ldots,b_{n-1}$; notons

$$c_j = \frac{c_n}{b_j} a_j, \quad \text{pour } 0 \leqslant j \leqslant n-1.$$

Le polynôme

$$c_n\, p(X) = c_n X^n + c_{n-1} X^n + c_{n-1} X^{n-1} + \ldots + c_0 \in \mathbb{Z}[X]$$

est appelé le polynôme minimal de α sur $\mathbb{Z}$.

Pour un nombre algébrique α, les trois propriétés suivantes sont équivalentes.

(i) Le polynôme minimal de α sur $\mathbb{Z}$ est unitaire, ce qui revient à dire que le polynôme irréductible de α sur $\mathbb{Q}$ est à coefficients entiers rationnels.

(ii) Il existe un polynôme unitaire (non nul) $Q \in \mathbb{Z}[X]$ tel que $Q(\alpha) = 0$.

(iii) Il existe un sous-$\mathbb{Z}$-module $M \neq 0$ de $\bar{\mathbb{Q}}$, de type fini, tel que $\alpha M \subset M$.

On dit alors que α est entier algébrique (sur $\mathbb{Z}$). La condition (iii) montre que l'ensemble des entiers algébriques forme un sous-anneau de $\bar{\mathbb{Q}}$. L'intersection de cet anneau avec une extension finie K de $\mathbb{Q}$ (c'est-à-dire un corps de nombres) est l'anneau des entiers de K .

Soit $\alpha \in \bar{\mathbb{Q}}$; l'ensemble

$$D_\alpha = \{\lambda \in \mathbb{Z} \ ; \ \lambda\alpha \text{ est entier algébrique}\}$$

est un idéal non nul de $\mathbb{Z}$; un élément positif de cet ensemble est appelé un dénominateur de α , et le générateur positif de cet idéal est appelé le dénominateur de α; on le note

$$d(\alpha) \ .$$

Pour voir que l'idéal D_α est non nul, on écrit le polynôme minimal de α sous la forme

$$c_n X^n + \ldots + c_o \ ,$$

et on constate que c_n est un dénominateur de α , puisque $c_n \alpha$ vérifie la condition (ii) précédente, avec

$$Q(X) = X^n + c_{n-1} X^{n-1} + c_{n-2} c_n X^{n-2} + \ldots + c_o c_n^{n-1} = \sum_{j=a}^{n} c_j c_n^{n-j-1} X^j \ .$$

On peut remarquer que c_n n'est pas obligatoirement le dénominateur de α (considérer le polynôme

$$4X^2 + 2X + 1$$

par exemple).

Soit K un sous-corps de $\mathbb{C}$, et soit α un nombre complexe algébrique sur K ; notons

$$P(X) = X^n + a_{n-1} X^{n-1} + \ldots + a_0$$

le polynôme irréductible de α sur K, et

$$\alpha_1, \ldots, \alpha_n$$

les n racines complexes de P (avec $\alpha_1 = \alpha$). Ces racines sont deux à deux distinctes (car, pour tout $j = 1, \ldots, n$, P est le polynôme irréductible de α_j sur K, donc α_j n'est pas racine de la dérivée P' de P), et on a

$$P(X) = \prod_{j=1}^{n} (X - \alpha_j).$$

On dit que $\alpha_1, \ldots, \alpha_n$ sont <u>les conjugués de</u> α <u>sur</u> K. Il existe alors n K-isomorphismes $\sigma_1, \ldots, \sigma_n$ de $L = K(\alpha)$ dans $\mathbb{C}$, déterminés par

$$\sigma_j(\alpha) = \alpha_j \ , \quad (1 \leqslant j \leqslant n).$$

On définit une application <u>norme</u> de L sur K par

$$N_{L/K}(\beta) = \prod_{i=1}^{n} \sigma_i(\beta) \ , \text{ pour } \beta \in L \ . \text{ Ainsi } N_{L/K}(\alpha) = (-1)^n a_0 \in K$$

(où $a_0 = P(0)$). Remarquons que la norme d'un nombre algébrique non nul est non nulle, et que la norme sur $\mathbb{Q}$ d'un entier algébrique est un entier rationnel.

Quand $K = \mathbb{Q}$ et $\alpha \in \bar{\mathbb{Q}}$, on note

$$|\bar{\alpha}| = \max_{1 \leqslant j \leqslant n} |\alpha_j| \ ; \tag{1.2.1}$$

on définit <u>la taille</u> ("size") $s(\alpha)$ <u>de</u> α par

(1.2.2) $$s(\alpha) = \max(\mathrm{Log}|\bar{\alpha}|\ ,\ \mathrm{Log}\ d(\alpha)).$$

Rappelons que $d(\alpha)$ désigne le dénominateur de α, c'est-à-dire le plus petit des entiers rationnels $d > 0$ tels que $d.\alpha$ soit entier algébrique.

La propriété fondamentale de la taille est la suivante

(1.2.3) Si α est un nombre algébrique de degré inférieur ou égal à n, on a

$$-2\ n\ s(\alpha) \leqslant \mathrm{Log}|\alpha| .$$

Pour cela, on remarque que la norme

$$N_{\mathbb{Q}(\alpha)/\mathbb{Q}}\ (d(\alpha).\alpha) = \prod_{j=1}^{n} d(\alpha).\alpha_j$$

sur $\mathbb{Q}$ de $d(\alpha).\alpha$ est un entier rationnel non nul, donc que

$$\prod_{j=1}^{n} d(\alpha).|\alpha_j| \geqslant 1 .$$

On en déduit

(1.2.4) $$-n\ \mathrm{Log}\ d(\alpha) - (n-1)\ \mathrm{Log}|\bar{\alpha}| \leqslant \mathrm{Log}|\alpha| ,$$

d'où la relation (1.2.3).

Dans le calcul de la taille de certains nombres algébriques, nous aurons à utiliser les propriétés (évidentes) suivantes :

$$d(\alpha.\beta) \leqslant d(\alpha).d(\beta)\ ;\ |\overline{\alpha.\beta}| \leqslant |\bar{\alpha}|.|\bar{\beta}|\ ;$$

$$d(\alpha+\beta) \leqslant d(\alpha).d(\beta)\ ;\ |\overline{\alpha+\beta}| \leqslant |\bar{\alpha}| + |\bar{\beta}|\ ;$$

$$d(a.\alpha) \leqslant a.d(\alpha)\ ;\ |\overline{a.\alpha}| = a.|\bar{\alpha}|\ ;$$

$$d(\alpha^m) \leqslant (d(\alpha))^m\ ;\ |\overline{\alpha^m}| = |\bar{\alpha}|^m ,$$

pour $\alpha, \beta \in \bar{\mathbb{Q}}$, et $a, m \in \mathbb{N}$.

On en déduit, pour $\alpha_1, \ldots, \alpha_m \in \bar{\mathbb{Q}}$,

$$s(\alpha_1 \ldots \alpha_m) \leqslant s(\alpha_1) + \ldots + s(\alpha_m) ;$$

$$s(\alpha_1 + \ldots + \alpha_m) \leqslant s(\alpha_1) + \ldots + s(\alpha_m) + \operatorname{Log} m .$$

Si, de plus, $\alpha_1, \ldots, \alpha_m$ sont entiers algébriques, on a

$$s(\alpha_1 + \ldots + \alpha_m) < \max_{1 \leqslant h \leqslant m} s(\alpha_h) + \operatorname{Log} m .$$

Remarque. La taille de 0 n'a pas été définie. On laisse au lecteur le soin d'examiner ce que deviennent les différentes relations concernant la fonction s lorsque certains des nombres algébriques incriminés s'annulent. Un abus de notation commode est le suivant : au lieu d'écrire

$$\alpha \neq 0 \quad \text{ou} \quad s(\alpha) < A ,$$

on écrit simplement

$$s(\alpha) < A .$$

Les nombres algébriques dont nous aurons à calculer la taille seront donnés comme valeurs de polynômes à coefficients entiers rationnels en des points algébriques. Pour cette raison nous introduisons les notions de hauteur et de taille pour des polynômes.

Soit $P \in \mathbb{C}[X_1, \ldots, X_q]$ un polynôme non nul en q variables à coefficients complexes. On note

$$\deg_{X_i} P$$

le degré de P par rapport à X_i, et

$$H(P)$$

la hauteur de P , c'est-à-dire le maximum des valeurs absolues des coefficients de P.

Maintenant, si $P \in \overline{\mathbb{Q}}[X_1,\dots,X_q]$ a ses coefficients entiers algébriques, on note

$$|\bar{P}|$$

le maximum des valeurs absolues des conjugués des coefficients de P , et on définit la taille de P par

$$t(P) = \max\{\operatorname{Log} |\bar{P}| \ , \ \max_{1\leqslant i\leqslant q} 1 + \deg_{X_i} P\} \ .$$

Remarquons que, pour $P \in \mathbb{Z}[X_1,\dots,X_q]$, on a

$$H(P) = |\bar{P}| \ .$$

On déduit alors facilement des propriétés de la fonction s le résultat suivant.

(1.2.5) Soient $\alpha_1,\dots,\alpha_q$ des nombres algébriques, et soit $P \in \mathbb{Z}[X_1,\dots,X_q]$ un polynôme, de degré inférieur ou égal à r_i par rapport à X_i $(1 \leqslant i \leqslant q)$.

Alors $P(\alpha_1,\dots,\alpha_q) = \beta$ est un nombre algébrique,

$$d(\alpha_1)^{r_1}\dots d(\alpha_q)^{r_q}$$

est un dénominateur de β , et on a

$$s(\beta) \leqslant \operatorname{Log} H(P) + \sum_{i=1}^{q} (r_i \, s(\alpha_i) + \operatorname{Log}(r_i+1)).$$

Pour raffiner un peu quelques inégalités, nous utiliserons également la norme euclidienne sur $\mathbb{C}[X_1,\dots,X_q]$:

pour

$$P(X_1,\dots,X_q) = \sum_{\lambda_1=0}^{r_1} \dots \sum_{\lambda_q=0}^{r_q} p(\lambda_1,\dots,\lambda_q) X_1^{\lambda_1}\dots X_q^{\lambda_q} \ ,$$

on définit

$$\|P\| = \left(\sum_{\lambda_1=0}^{r_1} \cdots \sum_{\lambda_q=0}^{r_q} |p(\lambda_1,\ldots,\lambda_q)|^2 \right)^{\frac{1}{2}}$$

On a donc (Parseval) :

$$(1.2.6) \qquad \|P\| = \left(\int_{H_q} |P(e^{2i\pi y_1},\ldots,e^{2i\pi y_q})|^2 dy_1 \ldots dy_q \right)^{\frac{1}{2}} ,$$

où H_q est l'hypercube

$$\{(y_1,\ldots,y_q) \in \mathbb{R}^q \ , \ 0 \leqslant y_j \leqslant 1 \ , \ (1 \leqslant j \leqslant q)\} .$$

On a de manière évidente

$$(1.2.7) \qquad H(P) \leqslant \|P\| \leqslant H(P). \prod_{k=1}^{q} (1 + \deg_{X_k} P)^{\frac{1}{2}} ,$$

et

$$(1.2.8) \qquad \|P\| \leqslant \max_{|x_1|=1,\ldots,|x_q|=1} |P(x_1,\ldots,x_q)| .$$

§1.3 Un lemme de Siegel pour les corps de nombres

Les démonstrations de transcendance que nous allons étudier débutent toutes par la construction d'une fonction auxiliaire. Cette construction repose sur la possibilité de résoudre un système d'équations linéaires homogènes. Pour des raisons évidentes de dimension d'espaces vectoriels, il est immédiat qu'un système d'équations linéaires homogène à coefficients dans un corps K possède au moins une solution non triviale dans K, dès que le nombre m d'équations est inférieur (strictement) au nombre n d'inconnues. Mais, de plus, on cherche une solution qui ne soit pas trop grande. Ceci est permis par un lemme de Siegel, dont la démonstration repose sur le principe des tiroirs de Dirichlet : si $\varphi : E \to F$ est une application d'un ensemble E à n éléments dans un ensemble $F = \bigcup_{1 \leqslant j \leqslant m} F_j$, et si $m < n$, alors l'un au moins

des ensembles $F_1,\dots,F_m$ contient les images par φ de deux éléments distincts de E. Il revient au même de dire, plus simplement, qu'une application d'un ensemble à n éléments dans un ensemble à m éléments n'est pas injective si $m < n$.

Lemme 1.3.1. Soit K un corps de nombres, de degré δ sur $\mathbb{Q}$. Soient $a_{i,j}$ $(1 \leqslant i \leqslant n\ ,\ 1 \leqslant j \leqslant m)$ des éléments de K entiers sur $\mathbb{Z}$. Soient $\sigma_1,\dots,\sigma_\delta$ les différents isomorphismes de K dans $\mathbb{C}$, et soit A un entier rationnel vérifiant

$$A \geqslant \max_{\substack{1\leqslant j\leqslant m\\ 1\leqslant h\leqslant\delta}} \sum_{i=1}^{n} |\sigma_h(a_{i,j})| .$$

Si on a $n > \delta m$, alors le système

$$\sum_{i=1}^{n} a_{i,j}\, x_i = 0 \quad ,\quad (1 \leqslant j \leqslant m) ,$$

admet une solution non triviale $(x_1,\dots,x_n) \in \mathbb{Z}^n$, vérifiant

$$\max_{1\leqslant i\leqslant n} |x_i| \leqslant (\sqrt{2}.A)^{\frac{m\delta}{n-m\delta}} .$$

Remarque. Pour résoudre un système

$$\sum_{i=1}^{n} a_{i,j}\, x_i = 0 \ ,\ (1 \leqslant j \leqslant m) ,$$

à coefficients dans K, on se ramène au cas où les $a_{i,j}$ sont entiers sur $\mathbb{Z}$ en multipliant la j-ième équation par un dénominateur commun d_j de

$$a_{1,j},\dots,a_{n,j} .$$

Il suffit alors que l'on remplace A par

$$A \max_{1\leqslant j\leqslant m} d_j .$$

Avant de démontrer le lemme 1.3.1, nous commençons par résoudre un système d'inéquations linéaires.

Lemme 1.3.2. Soient $u_{i,j}$ $(1 \leqslant i \leqslant \nu\ ,\ 1 \leqslant j \leqslant \mu)$ des nombres réels ; soit U un nombre entier vérifiant

$$U > \max_{1 \leqslant j \leqslant \mu} \sum_{i=1}^{\nu} |u_{i,j}| ,$$

et soient X et ℓ deux nombres entiers positifs tels que

$$\ell^{\mu} < (X+1)^{\nu} .$$

Alors il existe des éléments $\xi_1,\ldots,\xi_\nu$ de $\mathbb{Z}$, non tous nuls, tels que

$$\max_{1 \leqslant i \leqslant \nu} |\xi_i| \leqslant X$$

et

$$\max_{1 \leqslant j \leqslant \mu} \Big|\sum_{i=1}^{\nu} u_{i,j}\, \xi_i\Big| \leqslant \frac{UX}{\ell} .$$

Démonstration du lemme 1.3.2

Considérons l'application φ de l'ensemble

$\mathbb{N}(\nu,X) = \{(\xi_1,\ldots,\xi_\nu) \in \mathbb{Z}^{\nu}\ ;\ 0 \leqslant \xi_i \leqslant X\ (1 \leqslant i \leqslant \nu)\}$ dans $\mathbb{R}^{\mu}$, qui, à $(\xi_1,\ldots,\xi_\nu)$, fait correspondre $(\eta_1,\ldots,\eta_\mu)$, avec

$$\eta_j = \sum_{i=1}^{\nu} u_{i,j}\, \xi_i \qquad (1 \leqslant j \leqslant \mu).$$

Pour $1 \leqslant j \leqslant \mu$, on note $-V_j$ (resp. W_j) la somme des éléments négatifs (resp. positifs) de l'ensemble

$$u_{1,j},\ldots,u_{\nu,j} .$$

On aura donc

$$V_j + W_j \leqslant U \qquad \text{pour tout } j = 1,\ldots,\mu .$$

On remarque que, si $(\xi_1,\dots,\xi_\nu) \in \mathbb{N}(\nu,X)$, alors l'image $(\eta_1,\dots,\eta_\mu) = \varphi(\xi_1,\dots,\xi_\nu)$ appartient à l'ensemble

$$E = \{(\eta_1,\dots,\eta_\mu) \in \mathbb{R}^\mu \ ; \ -V_jX \leqslant \eta_j \leqslant W_jX\} \ .$$

On partage chacun des intervalles $[-V_jX, W_jX]$ en ℓ intervalles (de longueur $\leqslant \frac{UX}{\ell}$), ce qui fait que E est partagé en ℓ^μ sous ensembles E_k $(1 \leqslant k \leqslant \ell^\mu)$. La condition

$$\ell^\mu < (1+X)^\nu = \operatorname{Card} \mathbb{N}(\nu,X)$$

permet d'appliquer le principe des tiroirs : il existe deux éléments distincts ξ^* et ξ^{**} de $\mathbb{N}(\nu,X)$, dont les images par φ appartiennent au même sous-ensemble E_k de E. Notons ξ la différence $\xi^* - \xi^{**}$, et η l'image $\varphi(\xi)$. On aura

$$\xi = (\xi_1,\dots,\xi_\nu) \neq 0 \ , \text{ avec } \max_{1\leqslant i\leqslant \nu} |\xi_i| < X \ ,$$

et

$$\eta = (\eta_1,\dots,\eta_\mu) \quad , \text{ avec } \max_{1\leqslant j\leqslant \mu} |\eta_j| \leqslant \frac{UX}{\ell} \ ,$$

d'où le lemme 1.3.2 .

Nous sommes maintenant en mesure de démontrer le lemme 1.3.1.

Numérotons les différents plongements $\sigma_1,\dots,\sigma_\delta$ de K dans $\mathbb{C}$, de telle manière que l'on ait

$$\sigma_h(K) \subset \mathbb{R} \quad \text{pour} \quad 1 \leqslant h \leqslant r \ ,$$

et

$$\sigma_{r+s+k} = \bar{\sigma}_{r+k} \ \text{(conjugué complexe de } \sigma_{r+k}) \ \text{pour} \ 1 \leqslant k \leqslant s \ ,$$

où r et s sont deux entiers vérifiant $\delta = r+2s$. On définit des applications

$\tau_1,\dots,\tau_\delta$ de K dans $\mathbb{R}$ par :

$$\tau_h = \begin{cases} \sigma_h & \text{pour} \quad 1 \leqslant h \leqslant r \ ; \\ \mathrm{Re}\ \sigma_h & \text{pour} \quad r+1 \leqslant h \leqslant r+s \\ \mathrm{Im}\ \sigma_h & \text{pour} \quad r+s+1 \leqslant h \leqslant \delta = r+2s \ . \end{cases}$$

Choisissons deux entiers X et ℓ :

$$X = [(\sqrt{2}\ A)^{\frac{m\delta}{n-m\delta}}] \ , \text{ et}$$

$$\ell = 1 + [\sqrt{2}\ AX] \ ,$$

où [ ] désigne la partie entière, de telle manière que l'on ait

$$X \leqslant (\sqrt{2}\ A)^{\frac{m\delta}{n-m\delta}} \ ,$$

et

$$(1+X)^{n-m\delta} > (\sqrt{2}\ A)^{m\delta} \ ,$$

donc (puisque $A \geqslant 1$) ,

$$(1+X)^n > (1+\sqrt{2}\ AX)^{m\delta} \geqslant \ell^{m\delta} \ .$$

Le lemme 1.3.2 (avec $\nu = n$, $\mu = m\delta$, $U = A$) montre qu'il existe des entiers rationnels $x_1,\dots,x_n$, non tous nuls, vérifiant

$$\max_{1\leqslant i\leqslant n} |x_i| \leqslant (\sqrt{2}\ A)^{\frac{m\delta}{n-m\delta}} \ ,$$

et

$$\max_{\substack{1\leqslant h\leqslant \delta \\ 1\leqslant j\leqslant m}} \Big|\sum_{i=1}^{n} \tau_h(a_{i,j})x_i\Big| \leqslant \frac{AX}{1+[\sqrt{2}\ AX]} \ .$$

On en déduit

$$\max_{\substack{1\leqslant h\leqslant r \\ 1\leqslant j\leqslant m}} \Big|\sum_{i=1}^{n} \sigma_h(a_{i,j})x_i\Big| \leqslant \frac{AX}{1+[\sqrt{2}\ AX]} \ ,$$

et

$$\max_{\substack{r+1\leqslant h\leqslant \delta \\ 1\leqslant j\leqslant m}} \left|\sum_{i=1}^{n} \sigma_h(a_{i,j})x_i\right| \leqslant \frac{\sqrt{2}\ AX}{1+[\sqrt{2}\ AX]} ,$$

d'où

$$\left|N_{K/\mathbb{Q}}\left(\sum_{i=1}^{n} a_{i,j}\ x_i\right)\right| \leqslant 2^{s} \left(\frac{AX}{1+[\sqrt{2}\ AX]}\right)^{\delta} .$$

Dans cette dernière inégalité, le membre de gauche est un entier rationnel, et le membre de droite est majoré (puisque $s \leqslant \frac{\delta}{2}$) par

$$\left(\frac{\sqrt{2}\ AX}{1+[\sqrt{2}\ AX]}\right)^{\delta} < 1 .$$

D'où

$$\sum_{i=1}^{n} a_{i,j}\ x_i = 0 \quad \text{pour} \quad 1 \leqslant j \leqslant m .$$

§1.4 Extensions transcendantes

Soient K un corps et $\mathbf{A}$ un anneau contenant K. On dit que des éléments $x_1,\ldots,x_n$ de $\mathbf{A}$ forment une partie de $\mathbf{A}$ algébriquement libre sur K (ou bien que $x_1,\ldots,x_n$ sont algébriquement indépendants sur K) si l'homomorphisme canonique

$$\beta : K[X_1,\ldots,X_n] \to K[x_1,\ldots,x_n]$$

(de l'anneau des polynômes sur K à n indéterminées, sur le sous-anneau de $\mathbf{A}$ engendré par $x_1,\ldots,x_n$), qui est l'identité sur K et qui envoie X_i sur x_i ($1 \leqslant i \leqslant n$), est un isomorphisme.

Dans ces conditions, tout sous-ensemble de $\{x_1,\ldots,x_n\}$ forme une partie algébriquement libre de $\mathbf{A}$ sur K ; en particulier, chacun des éléments $x_1,\ldots,x_n$ est transcendant sur K. Deux éléments x_1,x_2 sont algébriquement indépendants sur K

si et seulement si x_1 est transcendant sur K et x_2 est transcendant sur $K(x_1)$.

Inversement, si l'homomorphisme β n'est pas injectif, c'est-à-dire s'il existe un polynôme non nul

$$P \in K[X_1,\ldots,X_n]$$

tel que

$$P(x_1,\ldots,x_n) = 0 ,$$

alors on dit que $x_1,\ldots,x_n$ sont <u>algébriquement dépendants</u> sur K.

Une partie E (finie ou non) de A est <u>algébriquement libre</u> sur K si toute partie finie de E est algébriquement libre sur K.

Soit L une extension d'un corps K ; une partie B de L est une <u>base de transcendance de</u> L <u>sur</u> K si B vérifie l'une des trois propriétés équivalentes suivantes.

(i) B est une partie maximale algébriquement libre de L sur K.

(ii) B est une partie algébriquement libre de L sur K, et L est une extension algébrique de $K(B)$.

(iii) B est une partie minimale de L telle que L soit une extension algébrique de $K(B)$.

Toute extension L de K admet des bases de transcendance, et deux telles bases sont équipotentes ; si L admet une base de transcendance finie, le nombre $n \geqslant 0$ d'éléments de cette base est appelé <u>degré de transcendance de</u> L <u>sur</u> K (ou <u>dimension algébrique de</u> L <u>sur</u> K) et <u>noté</u>

$$n = \dim_K L .$$

Ainsi une extension de type fini a un degré de transcendance fini. On remarque que, si $K \subset L \subset M$ sont trois corps, alors on a

$$\dim_K M = \dim_K L + \dim_L M ,$$

dès que l'un des deux membres a un sens.

Notons qu'une extension de K est algébrique si et seulement si elle a un degré de transcendance nul sur K.

Deux exemples d'extensions transcendantes seront utilisés. Le premier est $K = \mathbb{Q}$, $L = \mathbb{C}$; on dit que des nombres complexes sont <u>algébriquement indépendants</u> s'ils sont algébriquement indépendants sur $\mathbb{Q}$ (ou sur $\bar{\mathbb{Q}}$, cela revient au même). Le deuxième exemple utilise comme corps L le corps des fonctions méromorphes sur un ouvert connexe U de $\mathbb{C}$; on définit une injection

$$\mathbb{C} \subset L$$

en faisant correspondre à $\alpha \in \mathbb{C}$ l'application constante $z \mapsto \alpha$ de U dans $\mathbb{C}$. Soit

$$f_0 : U \to \mathbb{C}$$

l'application identité : $f_0(z) = z$ pour tout $z \in U$, et soit

$$K = \mathbb{C}(f_0)$$

(que l'on écrit quelquefois $K = \mathbb{C}(z)$). On dit qu'une fonction méromorphe $f : U \to \mathbb{C}$ est <u>algébrique</u> (resp. <u>transcendante</u>) si f est un élément de L algébrique sur K (resp. transcendant sur K), c'est-à-dire s'il existe (resp. s'il n'existe pas) un polynôme non nul $P \in \mathbb{C}[X_1, X_2]$ tel que

$$P(z, f(z)) = 0 \quad \text{pour tout} \quad z \in U .$$

Par exemple, pour des raisons évidentes de périodicité, une fonction exponentielle

$$z \mapsto \exp(\ell z)$$

(où $\ell \in \mathbb{C}$, $\ell \neq 0$) est transcendante. Plus généralement, on a le résultat suivant.

Lemme 1.4.1. Soient $b_1,\dots,b_h$ des nombres complexes. Les fonctions entières

$$z \ , \ e^{b_1 z},\dots,e^{b_h z}$$

sont algébriquement indépendantes sur $\mathbb{C}$ si et seulement si les nombres

$$b_1,\dots,b_h$$

sont $\mathbb{Q}$-linéairement indépendants.

Démonstration du lemme 1.4.1

Il est clair qu'une relation

$$\lambda_1 b_1 +\dots+ \lambda_h b_h = 0 \quad , \quad \text{où} \quad \lambda_j \in \mathbb{Z} \ , \ (1 \leqslant j \leqslant h) \ ,$$

entraîne

$$(e^{b_1 z})^{\lambda_1}\dots(e^{b_h z})^{\lambda_h} = 1 \quad \text{pour tout} \quad z \in \mathbb{C} \ .$$

Supposons maintenant les nombres $b_1,\dots,b_h$ $\mathbb{Q}$-linéairement indépendants, et soit

$$P \in \mathbb{C}[X_0,\dots,X_h]$$

un polynôme non nul. Il s'agit de démontrer que la fonction entière

$$F : z \mapsto P(z , e^{b_1 z},\dots,e^{b_h z})$$

n'est pas la fonction nulle.

Ecrivons le polynôme P sous la forme

$$P(X_0,\dots,X_h) = \sum_{\lambda_0=0}^{\delta_0} \dots \sum_{\lambda_h=0}^{\delta_h} p_{\lambda_0,\dots,\lambda_h} X_0^{\lambda_0}\dots X_h^{\lambda_h} ;$$

ainsi

$$F(z) = \sum_{(\lambda)} p(\lambda)\, z^{\lambda_0} \exp(\lambda_1 b_1 +\dots+ \lambda_h b_h)z ,$$

où on a noté $(\lambda) = (\lambda_0,\dots,\lambda_h)$.

Les nombres

$$\lambda_1 b_1 +\dots+ \lambda_h b_h \quad , \quad 0 \leqslant \lambda_j \leqslant \delta_j \ (1 \leqslant j \leqslant h) ,$$

sont deux à deux distincts ; écrivons les

$$w_1,\dots,w_q ,$$

avec $q = (\delta_1+1)\dots(\delta_\ell+1)$. On peut écrire alors la fonction F sous la forme

$$F(z) = \sum_{i=1}^{p} \sum_{j=1}^{q} a_{i,j}\, z^{i-1}\, e^{w_j z} ,$$

où $p = \delta_0+1$, et $a_{i,j}$ $(1 \leqslant i \leqslant p \ , \ 1 \leqslant j \leqslant q)$ sont des nombres complexes non tous nuls (car $P \neq 0$). Il nous reste donc à démontrer le résultat suivant

(1.4.2) Soient $P_1,\dots,P_q$ des polynômes non nuls de $\mathbb{C}[X]$; soient $w_1,\dots,w_q$ des nombres complexes deux à deux distincts. Alors la fonction entière

$$F : z \mapsto \sum_{k=1}^{q} P_k(z)\, e^{w_k z}$$

n'est pas identiquement nulle.

On démontre (1.4.2) par récurrence sur q ; le cas $q = 1$ est immédiat ; supposons $q > 1$, et notons p_i le degré du polynôme P_i $(1 \leqslant i \leqslant q)$. On remarque qu'il existe des polynômes $Q_1,\dots,Q_{q-1}$ de $\mathbb{C}[X]$, de degré $p_1,\dots,p_{q-1}$ respectivement, tels que

$$\frac{d^{p_q+1}}{dz^{p_q+1}} e^{-w_q z} F(z) = \sum_{j=1}^{q-1} Q_j(z)\, e^{(w_j-w_q)z} .$$

D'après l'hypothèse de récurrence, le membre de droite n'est pas identiquement nul, donc $F \neq 0$.

§1.5 Généralités sur les fonctions complexes

Soient f et g deux fonctions réelles de variable réelle. On note

$$f(x) \ll g(x) \qquad \text{pour } x \to +\infty,$$

ou, plus simplement,

$$f \ll g ,$$

s'il existe deux nombres réels positifs A et C tels que

$$x > A \implies f(x) \leqslant C.g(x) .$$

Soient ρ un réel positif et f une fonction entière (c'est-à-dire une application holomorphe de $\mathbb{C}$ dans $\mathbb{C}$). On dira que f est d'ordre (strict) inférieur ou égal à ρ si

$$\text{Log } |f|_R = \text{Log} \sup_{|z|=R} |f(z)| \ll R^{\rho} \qquad \text{pour } R \to +\infty. \tag{1.5.1}$$

Une fonction méromorphe est d'ordre inférieur ou égal à ρ si elle est quotient de deux fonctions entières d'ordre inférieur ou égal à ρ .

Exemples. Une fraction rationnelle est d'ordre inférieur ou égal à ρ quel que soit $\rho > 0$. Les fonctions sinus, cosinus, exponentielles sont d'ordre inférieur ou égal à 1. Si $n \in \mathbb{Z}$, $n > 0$, la fonction $z \mapsto \exp(z^n)$ est d'ordre inférieur ou égal à n. Si f est une fonction paire ($f(-z) = f(z)$ pour tout $z \in \mathbb{C}$) d'ordre inférieur

ou égal à ρ, alors $f(\sqrt{z})$ est d'ordre inférieur ou égal à $\frac{\rho}{2}$. Enfin la fonction

$$z \mapsto \exp(\exp z)$$

n'est pas d'ordre fini.

Principe du maximum ; lemme de Schwarz.

Soit f une fonction holomorphe dans un ouvert contenant le disque fermé $\{z \in \mathbb{C} ; |z| \leqslant R\}$. Le principe du maximum s'énonce alors (sous une forme faible, la seule que nous aurons à utiliser) :

$$\sup_{|z| \leqslant R} |f(z)| = \sup_{|z|=R} |f(z)| \overset{\text{déf.}}{=\!=} |f|_R .$$

Dans chacune des démonstrations de transcendance, nous utiliserons le principe du maximum pour majorer, sur un disque $|z| \leqslant r$, une fonction f holomorphe sur un ouvert contenant un disque $|z| \leqslant R$, avec $0 < r < R$, lorsque la fonction f possède de nombreux zéros sur le disque $|z| \leqslant r$.

Le cas le plus simple est le lemme de Schwarz :

(1.5.2) Si f est une fonction holomorphe dans un ouvert contenant un disque $|z| \leqslant R$, telle que $f(0) = 0$, alors, pour tout $z \in \mathbb{C}$, $|z| \leqslant R$, on a

$$|f(z)| \leqslant \frac{|z|}{R} |f|_R .$$

La démonstration du lemme de Schwarz est un exemple typique de celles que nous aurons à effectuer. Le développement de Taylor à l'origine de la fonction f s'écrit

$$f(z) = a_1 z + a_2 z^2 + \ldots + a_n z^n + \ldots ,$$

puisque $f(0) = 0$. Soit g la fonction définie par

$$g(z) = a_1 + a_2 z + \ldots + a_n z^{n-1} + \ldots ;$$

g est holomorphe dans un ouvert contenant $|z| \leqslant R$, et $f(z) = z.g(z)$ dans cet ouvert. D'après le principe du maximum, on a

$$|g(z)| \leqslant |g|_R \quad \text{pour tout } z \in \mathbb{C} , |z| \leqslant R ,$$

donc

$$|f(z)| = |z.g(z)| \leqslant |z|.|g|_R \leqslant |z|.\frac{|f|_R}{R}$$

pour tout $z \in \mathbb{C}$, $|z| \leqslant R$.

Zéros de fonctions entières

L'analyticité des fonctions holomorphes permet de montrer facilement qu'une fonction holomorphe non nulle dans un ouvert connexe U a ses zéros isolés.

En effet, soit $z_o \in U$, et soit Δ un disque ouvert de centre z_o inclus dans U . Dans Δ , f est égale à la somme de sa série de Taylor calculée en z_o :

$$f(z) = \sum_{n \geqslant 0} a_n (z-z_o)^n .$$

Si f n'est pas la fonction nulle dans U , alors (en vertu de la connexité de U), f n'est pas la fonction nulle dans Δ , donc les nombres a_n , $(n \geqslant 0)$ ne sont pas tous nuls. Soit

$$h = \inf\{n \geqslant 0 \ ; \ a_n \neq 0\} .$$

La fonction

$$g(z) = \sum_{k \geqslant 0} a_{k+h} (z-z_o)^k$$

est holomorphe dans Δ , donc continue en z_o , et

$$f(z) = (z-z_o)^h . g(z) \quad \text{pour tout } z \in \Delta .$$

Il existe un voisinage ouvert V de z_0 dans Δ tel que

$$|g(z)| > \frac{|a_h|}{2} \quad \text{pour tout } z \in V ,$$

car $a_h = g(z_0) \neq 0$. Dans l'ouvert V , la fonction f admet au plus un zéro (z_0).

Notons en passant le résultat suivant : <u>si</u> f <u>est une fonction holomorphe non nulle dans un ouvert connexe</u> U , <u>pour tout</u> $z_0 \in U$ <u>il existe un entier</u> $n \geqslant 0$ <u>tel que</u>

$$\frac{d^n}{dz^n} f(z_0) \neq 0 .$$

Nous aurons besoin de renseignements plus précis sur les zéros de fonctions entières. Nous utiliserons pour cela la <u>formule de Jensen</u> : soit f une fonction holomorphe non nulle dans un disque ouvert de centre 0 et de rayon $R > 0$. Soit r un nombre réel, $0 < r < R$, soient $a_1,\dots,a_p$ les zéros non nuls de f (comptés avec leur ordre de multiplicité) dans le disque $|z| \leqslant r$, et soit $c_k z^k$ ($k \geqslant 0$ entier) le premier terme non nul du développement de Taylor de f à l'origine. Alors on a

$$(1.5.3) \qquad \frac{1}{2\pi}\int_0^{2\pi} \operatorname{Log}|f(re^{i\theta})|\,d\theta = \operatorname{Log}|c_k| + k \operatorname{Log} r + \sum_{h=1}^{p} \operatorname{Log}\frac{r}{|a_h|} .$$

Pour démontrer la relation (1.5.3), on remarque que la fonction

$$G(z) = z^{-k}.f(z).\prod_{h=1}^{p} \frac{r^2 - z\bar{a}_h}{r(z-a_h)}$$

est holomorphe dans le disque $|z| < R$, et sans zéros dans le disque $|z| \leqslant r$. Donc la fonction $\operatorname{Log}|G(z)|$ est harmonique dans un disque $|z| < r+\varepsilon$ (avec $\varepsilon > 0$), et par conséquent

$$\operatorname{Log}|G(0)| = \frac{1}{2\pi}\int_0^{2\pi} \operatorname{Log}|G(re^{i\theta})|\,d\theta .$$

Or

$$|G(re^{i\theta})| = r^{-k}.|f(re^{i\theta})| \quad , \quad 0 \leqslant \theta \leqslant 2\pi \ ,$$

et

$$G(0) = c_k.\prod_{h=1}^{p} \frac{-r}{a_h} \ ,$$

d'où le résultat. Pour plus de détails, voir par exemple [Rudin, théorème 15.18].

La formule de Jensen montre que, si f est une fonction entière non nulle d'ordre inférieur ou égal à ρ, alors le nombre $n(f,R)$ de zéros de f dans le disque $|z| < R$ vérifie

$$n(f,R) \ll R^{\rho} \quad \text{pour} \quad R \to +\infty \tag{1.5.4}$$

Une conséquence qui nous sera très utile est la suivante : si f est une fonction méromorphe non nulle d'ordre inférieur ou égal à ρ, et si $x_1,\ldots,x_n$ sont des nombres complexes $\mathbb{Q}$-linéairement indépendants, avec $n > \rho$, alors l'un au moins des nombres

$$f(k_1x_1 + \ldots + k_nx_n) \quad , \quad k_i \in \mathbb{Z} \ , \ k_i \geqslant 1 \ (1 \leqslant i \leqslant n)$$

est non nul.

Nous allons démontrer un résultat plus précis que (1.5.4).

(1.5.5) Soit f une fonction entière non nulle, et soit $\lambda > 1$. Pour $R > 0$ réel, on note $n(f,R)$ le nombre de zéros de f (comptés avec leur ordre de multiplicité) dans le disque $|z| < R$. Alors on a

$$n(f,R) \ll \mathrm{Log}|f|_{\lambda R} \quad \text{pour} \quad R \to +\infty.$$

Notons $a_1,\ldots,a_p,\ldots$ les zéros non nuls de f, avec $|a_p| \leqslant |a_{p+1}|$ pour tout $p \geqslant 1$. Si ces zéros sont en nombre fini, le résultat est trivial.

Soit $p \geqslant 1$ un entier, tel que $|a_p| < |a_{p+1}|$, et soit r un nombre réel, $|a_p| < r \leqslant |a_{p+1}|$. D'après la formule (1.5.3) de Jensen, on a :

$$\sum_{h=1}^{p} \operatorname{Log} \frac{r}{|a_h|} \leqslant \operatorname{Log} |f|_r - \operatorname{Log} |c_k| - k \operatorname{Log} r ,$$

où $c_k = \frac{f^{(k)}(0)}{k!}$ est le coefficient du premier terme non nul de la série de Taylor de f en 0. Or on a

$$\sum_{h=1}^{p} \operatorname{Log} \frac{r}{|a_h|} = \sum_{h=1}^{p} \int_{|a_h|}^{r} \frac{dx}{x} = \int_0^r \frac{n(f,x)-k}{x}\, dx .$$

D'autre part, la croissance de la fonction $x \mapsto n(f,x)$, et l'inégalité

$$n(f,x) \geqslant k \quad \text{pour tout} \quad x \geqslant 0$$

montrent que l'on a

$$(n(f,R) - k)\operatorname{Log} \lambda \leqslant \int_R^{\lambda R} \frac{n(f,x)-k}{x}\, dx \leqslant \int_0^{\lambda R} \frac{n(f,x)-k}{x}\, dx .$$

On en déduit, en choisissant $r = \lambda R$

$$(1.5.6) \qquad n(f,R) \leqslant \frac{1}{\operatorname{Log} \lambda} (\operatorname{Log} |f|_{\lambda R} - \operatorname{Log} |c_k| - k \operatorname{Log} R)$$

ce qui démontre (1.5.5), donc aussi (1.5.4).

Enfin, nous dirons qu'un nombre complexe ℓ est un logarithme d'un nombre a si $e^{\ell} = a$. En particulier, un nombre ℓ est un logarithme d'un nombre algébrique si $e^{\ell} \in \overline{\mathbb{Q}}$; ainsi, le nombre $i\pi$ est un logarithme d'un nombre algébrique.

Si x est un nombre réel positif, on notera $\operatorname{Log} x$ le logarithme népérien de x.

§1.6 Références

Les résultats présentés dans ce chapitre 1 sont à peu près tous très classiques. De plus amples renseignements (avec démonstrations) sur la théorie des corps pourront être obtenus en consultant [Lang, A.] par exemple. La notion de "taille" que nous avons donnée est celle de "size" dans [Lang, T.] ; elle n'est pas universellement adoptée, et d'autres définitions sont légitimes (les exercices 1.2.a à 1.2.c proposent quelques comparaisons entre différentes notations).

Il existe de nombreuses variantes du lemme de Siegel ; les premières ont été obtenues par Dirichlet dans l'étude d'approximations de nombres algébriques [Schmidt, 1971] ; mentionnons également un théorème de Kronecker sur les approximations diophantiennes [Hille, 1942, lemme 2] ; l'énoncé 1.3.1 est dû à Maurice Mignotte. Nous établirons plus loin (lemme 4.3.1) un lemme de Siegel pour les extensions de $\mathbb{Q}$ de type fini.

Le lemme 1.4.1 sera considérablement amélioré au chapitre 6 ; mais, pour le début, ce résultat grossier sera suffisant.

La définition de l'"ordre" d'une fonction, telle qu'elle est donnée au §1.5, ne coïncide pas avec la notion classique (2.3.1) des livres de théorie des fonctions analytiques, par exemple [Rudin] (il manque un ε). Ici encore, nous avons suivi les notations de [Lang, T].

Le chapitre 1 ne prétend pas contenir tous les résultats utilisés dans la suite, mais seulement les principaux ; par exemple nous n'hésiterons pas à utiliser, sans les démontrer, les propriétés du résultant de deux polynômes (au chapitre 5).

EXERCICES

Exercice 1.2.a

Soit

$$P = \sum_{\lambda_1=0}^{m_1} \dots \sum_{\lambda_q=0}^{m_q} p(\lambda_1,\dots,\lambda_q) X_1^{\lambda_1} \dots X_q^{\lambda_q} \in \mathbb{C}[X_1,\dots,X_q]$$

un polynôme en q variables à coefficients complexes. On définit la hauteur de P par

$$H(P) = \max_{\lambda_1,\dots,\lambda_q} |p(\lambda_1,\dots,\lambda_q)| ,$$

la longueur de P par

$$L(P) = \sum_{\lambda_1=0}^{m_1} \dots \sum_{\lambda_q=0}^{m_q} |p(\lambda_1,\dots,\lambda_q)| ,$$

la norme euclidienne de P par

$$\|P\| = \Big(\sum_{\lambda_1=0}^{m_1} \dots \sum_{\lambda_q=0}^{m_q} |p(\lambda_1,\dots,\lambda_q)|^2\Big)^{\frac{1}{2}} ,$$

et la mesure de P par

$$M(P) = \exp \int_{H_q} \mathrm{Log}\,|P(e^{2i\pi u_1},\dots,e^{2i\pi u_q})|\, du_1 \dots du_q ,$$

avec $M(0) = 0$.

Vérifier les inégalités suivantes :

$$H(P) \leqslant L(P) \leqslant (1+m_1)\dots(1+m_q)\, H(P)$$

$$\|P\| \leqslant L(P) \leqslant (1+m_1)^{\frac{1}{2}} \dots (1+m_q)^{\frac{1}{2}}\, \|P\|$$

$$H(P) \leqslant \|P\| \leqslant (m_1+1)^{\frac{1}{2}} \dots (m_n+1)^{\frac{1}{2}} H(P)$$

$$M(P) \leqslant L(P) \leqslant 2^{m_1+\dots+m_q}\, M(P)$$

$$2^{-(m_1+\dots+m_q-\nu)}\, H(P) \leqslant M(P) \leqslant \|P\| ,$$

où ν est le nombre d'inconnues $X_1,\dots,X_q$, qui interviennent avec un degré $\geqslant 1$ dans P . [Mahler, 1961].

Exercice 1.2.b. Soit α un nombre algébrique, et soit $P \in \mathbb{Z}[X]$ le polynôme minimal de α sur $\mathbb{Z}$:

$$P(X) = \sum_{j=0}^{n} a_j X^j \quad , \quad n = [\mathbb{Q}(\alpha) : \mathbb{Q}] \ .$$

On note $\alpha_1, \ldots, \alpha_n$ les racines de P, c'est-à-dire les conjugués de α sur $\mathbb{Q}$ (avec $\alpha_1 = \alpha$ par exemple). On définit la <u>hauteur</u> de α par

$$H(\alpha) = H(P) = \max_{0 \leqslant j \leqslant n} |a_j| \ ,$$

la <u>longueur</u> de α par

$$L(\alpha) = L(P) = \sum_{j=0}^{n} |a_j| \ ,$$

la <u>norme euclidienne</u> de α par

$$\|\alpha\| = \|P\| = (\sum_{j=0}^{n} |a_j|^2)^{\frac{1}{2}} \ ,$$

<u>la mesure</u> de α par

$$M(\alpha) = M(P) = \exp \int_0^1 \mathrm{Log}|P(e^{2i\pi u})| \, du \ ,$$

et la <u>taille du polynôme minimal de</u> α par

$$\sigma(\alpha) = t(P) = \max(\mathrm{Log}H(\alpha), n+1).$$

Rappelons que l'on note

$$|\overline{\alpha}| = \max_{1 \leqslant i \leqslant n} |\alpha_i| \ .$$

1. Vérifier la relation

$$|\overline{\alpha}| \leqslant H(\alpha) + 1 \qquad \text{pour tout} \quad \alpha \in \overline{\mathbb{Q}} \ .$$

En déduire, pour $\alpha \neq 0$,

$$|\alpha| \geqslant [H(\alpha) + 1]^{-1} \ .$$

[Cijsouw, 1972, lemmes 1.2 et 1.3].

2. Vérifier l'inégalité

$$H(\alpha) \leqslant (2.d(\alpha).\max(1,|\bar{\alpha}|))^n ,$$

pour tout nombre algébrique α de degré $\leqslant n$

[Schneider, T., lemme 4] ; [Ramachandra, 1967, lemme 1] ; [Cijsouw, 1972, lemme 1.4].

3. Quelles inégalités lient les nombres

$$H(\alpha) , L(\alpha), \|\alpha\| , M(\alpha) , \sigma(\alpha) , |\bar{\alpha}| , [\mathbb{Q}(\alpha):\mathbb{Q}] ?$$

(Utiliser l'exercice 1.2.a).

4. Ecrire l'inégalité (1.2.3) en remplaçant la fonction s successivement par les fonctions

$$H , L , \|.\| , M \text{ et } \sigma .$$

5. Vérifier l'égalité

$$M(\alpha) = |a_n| . \prod_{h=1}^{n} \max(1,|\alpha_h|)$$

[Mahler, 1960].

Exercice 1.2.c

1) Montrer que, si P et Q appartiennent à $\mathbb{Z}[X]$, on a

$$L(P+Q) \leqslant L(P) + L(Q)$$

et

$$L(P.Q) \leqslant L(P).L(Q) .$$

[Mahler, 1969].

2) Soient α et β deux nombres algébriques non nuls de degré n et m respectivement. Vérifier

$$L(\alpha.\beta^{-1}) \leqslant 2^{n.m}.L^{m}(\alpha).L^{n}(\beta) .$$

[Feldman, 1968a, lemme 3].

En déduire des majorations de

$$f(\alpha.\beta) \quad \text{et} \quad f(\alpha.\beta^{-1})$$

en fonction de $f(\alpha)$, $f(\beta)$, $n = [\mathbb{Q}(\alpha) : \mathbb{Q}]$ et $m = [\mathbb{Q}(\beta) : \mathbb{Q}]$, pour chacune des fonctions f de l'exercice 1.2.b :

$$H , L , \|.\|, M \text{ et } \sigma .$$

Exercice 1.2.d. Soient $\alpha_1,\ldots,\alpha_q$ des nombres algébriques de degré $d_1,\ldots,d_q$ respectivement. On note

$$d = [\mathbb{Q}(\alpha_1,\ldots,\alpha_q) : \mathbb{Q}] .$$

Soit $P \in \mathbb{Z}[X_1,\ldots,X_q]$ un polynôme de degré inférieur ou égal à N_i par rapport à X_i $(1 \leqslant i \leqslant q)$. Montrer que, si

$$P(\alpha_1,\ldots,\alpha_q) \neq 0 ,$$

alors on a

$$|P(\alpha_1,\ldots,\alpha_q)| \geqslant L(P)^{1-d} \cdot \prod_{i=1}^{q} \|\alpha_i\|^{-\frac{dN_i}{d_i}} .$$

(Utiliser l'exercice 4.2.d et consulter [Feldman, 1968b, lemme 2]).

En déduire une minoration de $|\alpha-\beta|$ (quand α et β sont deux nombres algébriques distincts) en fonction de

$$H(\alpha) , H(\beta) , [\mathbb{Q}(\alpha) : \mathbb{Q}] \text{ et } [\mathbb{Q}(\beta) : \mathbb{Q}] .$$

[Feldman et Shidlovskii, 1966, (1.9)].

Exercice 1.3.a. Soient $u_{i,j}$ $(1 \leqslant i \leqslant \nu\ ,\ 1 \leqslant j \leqslant \mu)$ des nombres réels, et soient $U_1,\dots,U_\mu$ des entiers rationnels positifs, tels que

$$U_j \geqslant \sum_{i=1}^{\nu} |u_{i,j}| \quad , \quad \text{pour} \quad 1 \leqslant j \leqslant \mu \ .$$

Soient $X_1,\dots,X_\nu$, $\ell_1,\dots,\ell_\mu$ des nombres entiers positifs tels que

$$\ell_1 \dots \ell_\mu < \prod_{i=1}^{\nu} (1+X_i).$$

Montrer qu'il existe des éléments $\xi_1,\dots,\xi_\nu$ de $\mathbb{Z}$, non tous nuls, tels que

$$|\xi_i| \leqslant X_i \quad \text{pour} \quad 1 \leqslant i \leqslant \nu \ ,$$

et

$$\Big|\sum_{i=1}^{\nu} u_{i,j}\, \xi_i\Big| \leqslant \frac{U_j}{\ell_j} \max_{1 \leqslant i \leqslant \nu} X_i \ .$$

Exercice 1.3.b. Soient $a_{i,j}$ $(1 \leqslant i \leqslant n\ ,\ 1 \leqslant j \leqslant m)$ des entiers algébriques. Pour $1 \leqslant j \leqslant m$, notons K_j le sous-corps de $\mathbb{C}$ obtenu en adjoignant à $\mathbb{Q}$ les n nombres

$$a_{1,j}\ ,\ldots,a_{n,j}\ ,$$

et

$$\delta_j = [K_j : \mathbb{Q}]$$

le degré de K_j. Soient $A_1,\ldots,A_m$ des entiers positifs vérifiant

$$A_j > \max_{1\leqslant h\leqslant \delta_j} \sum_{i=1}^{n} |\sigma_h^{(j)}(a_{i,j})| \quad \text{pour} \quad 1 \leqslant j \leqslant m\ ,$$

où

$$\sigma_1^{(j)},\ldots,\sigma_{\delta_j}^{(j)}$$

sont les différents plongements de K_j dans $\mathbb{C}$ $(1 \leqslant j \leqslant m)$. On suppose

$$n > \mu = \delta_1 +\ldots+ \delta_m\ .$$

Montrer qu'il existe des entiers rationnels non tous nuls

$$x_1,\ldots,x_n$$

vérifiant

$$\sum_{i=1}^{n} a_{i,j}\, x_i = 0 \quad \text{pour} \quad 1 \leqslant j \leqslant m\ ,$$

et

$$\max_{1\leqslant i\leqslant n} |x_i| \leqslant (2^{\frac{\mu}{2}} A_1^{\delta_1}\ldots A_m^{\delta_m})^{\frac{1}{n-\mu}}\ .$$

Montrer ensuite qu'on peut remplacer $2^{\frac{\mu}{2}}$ par 1 dans cette dernière inégalité, dans le cas particulier où les corps $K_1,\ldots,K_m$ sont totalement réels (c'est-à-dire $\sigma_h^{(j)}(K_j) \subset \mathbb{R}$ pour $1 \leqslant h \leqslant \delta_j$, $1 \leqslant j \leqslant m$).

Exercice 1.3.c. Soit K un corps de nombres. Montrer qu'il existe une constante $C_K > 0$ ayant la propriété suivante. Soient $a_{i,j}$ $(1 \leqslant i \leqslant n\ ,\ 1 \leqslant j \leqslant m)$ des éléments de K entiers sur $\mathbb{Z}$, avec $m > n$. Pour $1 \leqslant j \leqslant m$, soit

$$A_j = \max_{1 \leqslant i \leqslant n} s(a_{i,j}).$$

Alors il existe des éléments $x_1,\ldots,x_n$ de K, entiers sur $\mathbb{Z}$, non tous nuls, et tels que

$$\sum_{i=1}^{n} a_{i,j}\, x_i = 0 \quad \text{pour} \quad 1 \leqslant j \leqslant m\ ,$$

et

$$\max_{1 \leqslant i \leqslant n} s(x_i) \leqslant \frac{1}{n-m}\,(A_1 + \ldots + A_m + mC_K).$$

(Indications : utiliser le fait que l'anneau des entiers de K est un $\mathbb{Z}$-module de type fini et de rang $[K:\mathbb{Q}]$; écrire les inconnues $x_1,\ldots,x_n$ dans une base d'entiers de K

$$w_1,\ldots,w_\delta\ ,$$

et appliquer l'exercice précédent pour calculer C_K en fonction de δ et de

$$\max_{1 \leqslant h \leqslant \delta} s(w_h)).$$

Exercice 1.3.d. Soient $u_0,\dots,u_m$ des nombres réels. Soit H un nombre entier positif. Montrer qu'il existe des entiers rationnels $\xi_0,\dots,\xi_m$, non tous nuls, tels que

$$\max_{0\leqslant i\leqslant m} |\xi_i| \leqslant H$$

et

$$|u_0\xi_0 +\dots+ u_m\xi_m| \leqslant (|u_0| +\dots+ |u_m|).H^{-m} .$$

(Indication : utiliser le lemme 1.3.2 avec

$$\mu = 1 \ ; \ \nu = m+1 \ ; \ u_{i,1} = u_{i-1} \ , \ (1 \leqslant i \leqslant m+1) \ ,$$

et choisir pour ℓ le plus grand entier strictement inférieur à

$$(H+1)^{m+1} .$$

On pourra ainsi majorer $\frac{H}{\ell}$ par H^{-m}).

Exercice 1.3.e. Soient u un nombre réel, et $Q > 0$ un entier rationnel. Montrer qu'il existe $\frac{p}{q} \in \mathbb{Q}$ tel que

$$|u-\frac{p}{q}| < \frac{1}{qQ} \ , \ 0 < q < Q$$

(théorème de Dirichlet ; voir par exemple [Feldman et Shidlovskii, 1966, (1.5)]).

Exercice 1.3.f. Soient $u_0,\ldots,u_m$ des nombres complexes. Soit H un entier positif. Montrer qu'il existe des entiers rationnels $\xi_0,\ldots,\xi_m$, non tous nuls, tels que

$$\max_{0\leqslant i\leqslant m} |\xi_i| \leqslant H$$

et

$$|u_0\xi_0 +\ldots+ u_m\xi_m| < \sqrt{2}(|u_0| +\ldots+ |u_m|).H^{-\frac{1}{2}(m-1)} .$$

(Indication : les cas $m = 0$ et $m = 1$ sont triviaux ; si $m \geqslant 2$, utiliser le lemme 1.3.2 avec

$$\mu = 2 \; ; \; \nu = m+1 \; ; \; u_{i,1} = \mathrm{Re}(u_{i-1}) \; , \; u_{i,2} = \mathrm{Im}(u_{i-1}) \; , \; 1 \leqslant i \leqslant \nu) .$$

En déduire le résultat suivant : si $x_1,\ldots,x_q$ sont des nombres complexes, et si $N_1,\ldots,N_q$, H sont des nombres entiers positifs, il existe un polynôme non nul $P \in \mathbf{Z}[X_1,\ldots,X_q]$, de degré inférieur ou égal à N_h par rapport à X_h $(1 \leqslant h \leqslant q)$ et de hauteur inférieure ou égale à H, tel que

$$|P(x_1,\ldots,x_q)| \leqslant \sqrt{2}\; H^{-\frac{1}{2}M+1}.e^{c(N_1+\ldots+N_q)} ,$$

où

$$M = \prod_{k=1}^{q} (1+N_k)$$

et

$$c = 1 + \mathrm{Log}\, \max(1 , |x_1|,\ldots,|x_q|) .$$

(Remarquer que $M < e^{N_1+\ldots+N_q}$). Comment peut-on améliorer ce résultat quand tous les nombres x_k $(1 \leqslant k \leqslant r)$ sont réels ? (utiliser l'exercice 1.3.d).

Comparer le cas $q = 1$ avec les résultats de K. Mahler, Acta Arith., 18 (1971) 63-76.

Exercice 1.3.g. Montrer qu'un nombre complexe σ est transcendant si et seulement si pour tout réel $w > 0$, il existe un entier $n > 0$ tel que l'inégalité

$$0 < |x_0 + x_1\sigma + \ldots + x_n\sigma^n| < \left(\max_{0 \leqslant i \leqslant n} |x_i|\right)^{-w}$$

ait une infinité de solutions $(x_0, \ldots, x_n) \in \mathbb{Z}^{n+1}$.

(Indication : utiliser les exercices 1.2.d et 1.3.f) [Mahler, 1969].

Exercice 1.4.a. Soient $\wp_1,\ldots,\wp_m$ des fonctions elliptiques de Weierstrass ; on note $(w_1^{(j)},w_2^{(j)})$ un couple de périodes fondamentales de $\wp_j$ $(1 \leqslant j \leqslant m)$.

a) Montrer que $\wp_1$ et $\wp_2$ sont algébriquement dépendantes (sur $\mathbb{C}$) si et seulement si il existe une matrice M carré 2×2 à coefficients rationnels telle que

$$(w_1^{(2)},w_2^{(2)}) = (w_1^{(1)},w_2^{(1)})M .$$

b) Montrer que les fonctions

$$e^z , \wp_1(z) , \wp_2(z)$$

sont algébriquement indépendantes si et seulement si les deux fonctions

$$\wp_1(z) , \wp_2(z)$$

le sont.

c) Si $\frac{1}{w_2^{(1)}},\ldots,\frac{1}{w_m^{(1)}}$ sont $\mathbb{Q}$-linéairement indépendants et engendrent un $\mathbb{R}$-espace vectoriel de dimension 1, montrer que les fonctions

$$\wp_1,\ldots,\wp_m$$

sont algébriquement indépendantes

[Ramachandra, 1967, lemme 7].

d) Soit ζ la fonction zêta de Weierstrass associée à une fonction elliptique $\wp$, et soient a, b deux nombres complexes, $(a,b) \neq (0,0)$. Montrer que les deux fonctions

$$\wp(z) , az + b\zeta(z)$$

sont algébriquement indépendantes

(Utiliser la relation de Legendre $w_1\eta_2 - w_2\eta_1 = 2i\pi$) [Schneider, T, p.60].

Exercice 1.4.b. Soient $f_1,\ldots,f_n$ des fonctions entières de $\mathbb{C}$ dans $\mathbb{C}$. Montrer que, si les fonctions entières

$$e^{f_1},\ldots,e^{f_n}$$

sont algébriquement indépendantes sur $\mathbb{C}(z)$, alors les fonctions

$$1, f_1,\ldots,f_n$$

sont $\mathbb{Q}$-linéairement indépendantes.

(Narasimhan [1971] avait énoncé la réciproque, mais P. Bundschuh a donné un contre exemple dans son article : Ein funktionentheoretisches Analogon zum Satz von Lindemann, à paraître dans Archiv der Math.).

Exercice 1.4.c. Montrer que les fonctions

$$x \mapsto \int_0^x e^{-t^2}\,dt$$

et

$$x \mapsto \int_x^\infty \frac{e^t}{t}\,dt$$

sont des fonctions transcendantes sur $\mathbb{C}$.

[Hamming, 1970].

Exercice 1.5.a. Soit f une fonction holomorphe dans un ouvert U de $\mathbb{C}$ contenant un disque fermé $|z| \leqslant R$. On suppose que f admet les zéros $z_1,\ldots,z_n$ dans le disque ouvert $|z| < R$.

1) Etablir la majoration

$$|f(0)| \leqslant R^{-n}.|z_1\ldots z_n|.|f|_R .$$

(Indication : utiliser le principe du maximum, sur le disque $|z| \leqslant R$, pour la fonction

$$f(z) \cdot \prod_{j=1}^{n} \frac{R^2-z\bar{z}_j}{R(z-z_j)} ;$$

voir [Hille, 1942, lemme 3]).

2) Soit $z_o \in \mathbb{C}$, $|z_o| < R$. Etablir la majoration

$$|f(z_o)| \leqslant |f|_R \cdot \sup_{|z|=R} \prod_{i=1}^{n} \left|\frac{z_o-z_i}{z-z_i}\right|$$

(Indication : utiliser le principe du maximum pour la fonction

$$f(z).\prod_{i=1}^{n} (z-z_i)^{-1} ;$$

voir [Waldschmidt, 1973b, lemme 1]).

Exercice 1.5.b. Soit f une fonction holomorphe dans un ouvert U de $\mathbb{C}$ contenant un disque fermé $|z| \leqslant R$; soit σ le nombre de zéros de f dans le disque $|z| \leqslant \rho$, avec $\rho < R$. Montrer que pour tout entier $s \geqslant 0$ et pour tout réel r vérifiant $0 < r \leqslant R$, on a

$$|f^{(s)}(0)| \leqslant \frac{s!}{r^s} \left(\frac{r+\rho}{R-\rho}\right)^{\sigma} . |f|_R .$$

(Utiliser la formule intégrale de Cauchy pour obtenir

$$r^s \frac{|f^{(s)}(0)|}{s!} \leqslant |f|_r \qquad \text{(inégalités de Cauchy)},$$

puis appliquer le deuxième résultat de l'exercice précédent).

Exercice 1.5.c. Soit f une fonction holomorphe non nulle dans un ouvert (connexe) contenant $|z| \leqslant R$, soit σ le nombre de zéros non nuls de f dans le disque $|z| \leqslant \rho$, et soit s le plus petit entier supérieur ou égal à 0 tel que $f^{(s)}(0) \neq 0$. Etablir la majoration

$$|f^{(s)}(0)| \leqslant s! \left(\frac{\rho}{R-\rho}\right)^{\sigma} . |f|_R$$

(Utiliser le principe du maximum pour la fonction

$$\frac{f(z)}{z^s . \prod_{i=1}^{\sigma} (z-x_i)} ,$$

où $x_1, \ldots, x_\sigma$ sont les zéros non nuls de f ; voir [Waldschmidt, 1973b, lemme 1]).

Exercice 1.5.d. Soit f une fonction entière dans $\mathbb{C}$. Soit $q \in \mathbb{C}[X]$ un polynôme unitaire, de degré n. On note $z_1,\dots,z_m$ les racines distinctes de Q dans $\mathbb{C}$, et $k_1,\dots,k_m$ leurs ordres de multiplicité respectifs ; ainsi

$$Q(X) = \prod_{j=1}^{m} (X-z_j)^{k_j} .$$

Soit Γ un cercle dont l'intérieur contient les points $z_1,\dots,z_m$; soit z un autre point de l'intérieur de Γ ; on considère m cercles $\Gamma_1,\dots,\Gamma_m$, tels que l'intérieur de Γ_j contienne z_j, mais ne contienne pas z, ni z_ℓ pour $\ell \neq j$ $(1 \leqslant j \leqslant m)$. Vérifier la relation

$$\frac{1}{2i\pi}\int_\Gamma \frac{f(\zeta)}{Q(\zeta)}\frac{d\zeta}{\zeta-z} = \frac{f(z)}{Q(z)} + \frac{1}{2i\pi}\sum_{j=1}^{m}\sum_{h=0}^{k_j-1}\frac{1}{h!}\frac{d^h}{dz^h}f(z_j)\int_{\Gamma_j}\frac{(\zeta-z_j)^h}{\zeta-z}\frac{d\zeta}{Q(\zeta)}$$

[Lang, T, chap.VI, lemme 6], ou [Baker, 1966, I, p.212].

Exercice 1.5.e. Soient f et g deux fonctions entières, d'ordre inférieur ou égal à ρ. On suppose que la fonction f/g est entière. Vérifier

$$\mathrm{Log} \sup_{|z|=R} \left|\frac{f(z)}{g(z)}\right| \ll R^\rho .$$