Approximation by rational numbers

Ex. 1. $\sqrt{2}$ has good approximations: $\forall n \in \mathbb{N}_+ \quad (1\pm\sqrt{2})^n = p_n \pm q_n\sqrt{2} \Rightarrow p_n^2 - 2q_n^2 = (-1)^n$

$\Rightarrow \left(\frac{p_{2n}}{q_{2n}} - \sqrt{2}\right)\left(\frac{p_{2n}}{q_{2n}} + \sqrt{2}\right) = \frac{1}{q_{2n}^2}$, $\left|\frac{p_{2n}}{q_{2n}} - \sqrt{2}\right| < \frac{1}{2\sqrt{2}\, q_{2n}^2}$ ($\frac{p_{2n}}{q_{2n}} + \sqrt{2} > 2\sqrt{2}$)

Ex. 2. $\sqrt{2}$ does not have very good approximations: $\forall p, q \in \mathbb{N}_+ \quad |p^2 - 2q^2| \geq 1 \Rightarrow$

$\left|\frac{p}{q} - \sqrt{2}\right| \geq \frac{1}{q^2} \cdot \frac{1}{\left(\frac{p}{q} + \sqrt{2}\right)}$. If $\left|\frac{p}{q} - \sqrt{2}\right| < c \Rightarrow \frac{p}{q} + \sqrt{2} < 2\sqrt{2} + c \Rightarrow \left|\frac{p}{q} - \sqrt{2}\right| > \frac{1}{(2\sqrt{2}+c)q^2}$

Important general principle: $\boxed{a \in \mathbb{Z},\ a \neq 0 \Rightarrow |a| \geq 1}$ (above, $a = p^2 - 2q^2$)

Def. $\alpha \in \mathbb{C}$ is an algebraic number of degree $n \geq 1$ if $\exists\ f \in \mathbb{Q}[X]$, $\deg(f) = n$, $f(\alpha) = 0$, but $\forall g \in \mathbb{Q}[X] \setminus \{0\}$ of $\deg(g) < n$ $g(\alpha) \neq 0$ (f is then unique up to $\mathbb{Q}^\times$).

Thm (Liouville) If $\alpha \in \mathbb{C}$ is algebraic of degree $n \geq 2$, then $\exists$ explicit constant $c(\alpha) > 0$ such that $\forall p, q \in \mathbb{Z},\ q \geq 0 \quad \left|\alpha - \frac{p}{q}\right| \geq \frac{c(\alpha)}{q^n}$. (*)

Pf. If $\alpha \notin \mathbb{R} \Rightarrow |\alpha - p/q| \geq |\mathrm{Im}(\alpha)| > 0$. If $\alpha \in \mathbb{R}$, let $f = a_0 X^n + \cdots + a_n \in \mathbb{Z}[X]$, $a_0 \neq 0$, $f(\alpha) = 0$. If $|\alpha - p/q| \geq 1$, then we can take $c(\alpha) = 1$. If $|\alpha - p/q| \leq 1$, then $f(\alpha) - f(p/q) = (\alpha - p/q) f'(\beta)$ for some $\beta \in \mathbb{R}$, $|\beta - \alpha| \leq 1$. But $f(\alpha) = 0$, $0 \neq q^n f(p/q) = a_0 p^n + \cdots + a_n q^n \in \mathbb{Z} \Rightarrow |q^n f(p/q)| \geq 1 \Rightarrow |\alpha - p/q| \geq \frac{1}{q^n |f'(\beta)|}$

$\Rightarrow$ result for $c(\alpha) = \min\left(1,\ 1 / \sup_{|\beta - \alpha| \leq 1} |f'(\beta)|\right)$.

Cor. If $\alpha \in \mathbb{R}$ and if $\forall k \geq 1\ \exists\ p_k, q_k \in \mathbb{Z}$, $q_k > 0$ with $|\alpha - p_k/q_k| < 1/q_k^{N_k}$, $\lim_{k \to +\infty} N_k = +\infty$, then α is not algebraic (Ex: $\alpha = \sum_{n \geq 1} 10^{-n!}$).

For $n \geq 3$, the exponent n in (*) can be improved to $n/2 + 1 + \varepsilon$ (Thue, 1909), $2\sqrt{n} + \varepsilon$ (Siegel 1921), $\sqrt{2n} + \varepsilon$ (Dyson, Gelfond, 1947) and $2 + \varepsilon$ (Roth, 1955 – Fields medal!), $\forall \varepsilon > 0$.

Unfortunately, the corresponding constant $c(\alpha, \varepsilon)$ can be made effective only for very special algebraic numbers α.

Dirichlet's Box Principle: given M objects in N boxes, with $M > N$

$\Rightarrow\ \exists$ box with $\geq M/N > 1$ objects.

Thm (Dirichlet). $\forall \alpha \in \mathbb{R}\ \forall M \in \mathbb{Z}_{\geq 2}\ \exists\ p, q \in \mathbb{Z}$, $1 \leq q \leq M \quad |q\alpha - p| < \frac{1}{M}$ ($\Rightarrow |\alpha - \frac{p}{q}| < \frac{1}{q^2}$)

Pf. Divide $[0,1)$ into M boxes $[0,1) = \bigsqcup_{0 \leq i < M} [i/M, (i+1)/M)$ and consider the $M+1$ numbers $\{j\alpha\} = j\alpha - [j\alpha] \in [0,1)$ ($j = 0, \ldots, M$). The Box Principle $\Rightarrow\ \exists\ j \neq j'$, $0 \leq j, j' \leq M$, $\exists\ i$ $\{j\alpha\}, \{j'\alpha\} \in [i/M, (i+1)/M)$

$\Rightarrow 0 \leq \{j'\alpha\} - \{j\alpha\} < 1/M$. Take $q = |j' - j|$ and $p = \mathrm{sgn}(j' - j)([j'\alpha] - [j\alpha])$;

then $|q\alpha - p| = |\{j'\alpha\} - \{j\alpha\}| < 1/M$.

Cor (the simplest case of Kronecker's thm) If $\alpha \in \mathbb{R}\setminus\mathbb{Q}$, then the subgroup $\mathbb{Z}\alpha + \mathbb{Z}$ is dense in $\mathbb{R}$: $\forall \beta\in\mathbb{R}\ \forall \varepsilon>0\ \exists q\in\mathbb{N}_+\ \exists p\in\mathbb{Z}\ |q\alpha-\beta-p|<\varepsilon$.

Pf. If $M\in\mathbb{N}$, $M\geq 2$, $1/M<\varepsilon$, then $\exists q_1\in\mathbb{Z}\setminus\{0\}$ such that $\{q_1\alpha\}<1/M$. As $\alpha\notin\mathbb{Q}$, $0<\{q_1\alpha\} \Rightarrow \exists k\in\mathbb{N}_+\ |k\{q_1\alpha\}-\{\beta\}|<1/M \Rightarrow q=kq_1$ satisfies $\{q\alpha-\beta\}<1/M<\varepsilon$.

Notation: (1) for $x\in\mathbb{R}$, let $((x))=\min\limits_{p\in\mathbb{Z}}|x-p| \in [0,1/2]$ be the distance to the nearest integer.

(2) $\mathbb{R}^n=\left\{x=\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix} \mid x_i\in\mathbb{R}\right\} \supset \underbrace{\mathbb{Z}^n}_{x_i\in\mathbb{Z}}$, $\mathrm{Hom}_{\mathbb{R}}(\mathbb{R}^n,\mathbb{R})=(\mathbb{R}^n)^*=\{a=(a_1,\dots,a_n)\mid a_i\in\mathbb{R}\}\supset\underbrace{(\mathbb{Z}^n)^*}_{a_i\in\mathbb{Z}}$ the dual space to $\mathbb{R}^n$

$ax=(a_1,\dots,a_n)\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}=\sum\limits_1^n a_ix_i$, $\|x\|_\infty=\max\limits_{1\leq i\leq n}|x_i|$, $\|a\|_\infty=\max\limits_{1\leq i\leq n}|a_i|$ (the L^∞-norm)

$((x))=\max\limits_{1\leq i\leq n}((x_i))$, $((a))=\max\limits_{1\leq i\leq n}((a_i))$

(3) The rows $A_1,\dots,A_m\in(\mathbb{R}^n)^*$ of a matrix $A\in M_{m,n}(\mathbb{R})$ are linear forms $A_i:\mathbb{R}^n\longrightarrow\mathbb{R}$, $x\longmapsto A_ix=\sum\limits_{j=1}^n A_{ij}x_j$

Simultaneous approximations.

Thm. $\forall A\in M_{m,n}(\mathbb{R})\ \forall M\in\mathbb{Z}_{>1}\ \exists x\in\mathbb{Z}^n\setminus\{0\}$ $\|x\|_\infty\leq M^{m/n}$, $((Ax))<1/M$.

Pf. Decompose $[0,1)^m$ into M^m boxes $\prod\limits_{j=1}^m [i_j/M,(i_j+1)/M)$ $i_j=0,1,\dots,M-1$. Let $k=[M^{m/n}]$; then $k+1>M^{m/n}$, $(k+1)^n>M^m$. Consider the $(k+1)^n$ values $\{Ax\}\in[0,1)^m$ for $x\in\{0,1,\dots,k\}^n$. The Box Principle $\Rightarrow \exists\ x'\neq x''\in\{0,\dots,k\}^n$ for which $\{Ax'\}$, $\{Ax''\}$ are in the same box $\Rightarrow$ $x=x'-x''\in\mathbb{Z}^n\setminus\{0\}$ satisfies $\|x\|_\infty\leq k$, $((Ax))<1/M$.

Thm! $\forall A\in M_{m,n}(\mathbb{R})\ \forall t\in\mathbb{R}_{>1}\ \exists x\in\mathbb{Z}^n\setminus\{0\}$ $\|x\|_\infty\leq t$, $((Ax))<1/t^{n/m}$.

Ex1: ($m=1$) $\forall A=(\alpha_1,\dots,\alpha_n)\in(\mathbb{R}^n)^*\ \forall t>1\ \exists x\in\mathbb{Z}^n\setminus\{0\}$ $\|x\|_\infty\leq t$, $\left(\left(\sum\limits_{j=1}^n\alpha_jx_j\right)\right)<1/t^n$

Ex2: ($n=1$) $\forall A=\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_m\end{pmatrix}\in\mathbb{R}^m\ \forall t>1\ \exists x\in\mathbb{Z}\setminus\{0\}$ $((\alpha_1x))<1/t^{1/m},\dots,((\alpha_mx))<1/t^{1/m}$

Pf. Apply the following variant of Minkowski's thm for parallelograms to $\widetilde{A}=\begin{pmatrix}I_n & 0\\ -A & I_m\end{pmatrix}$, $\ell=m+n$, $t_1=\dots=t_n=t>1>t_{n+1}=\dots=t_{n+m}=1/t^{n/m}$; get $z=\begin{pmatrix}x\\ y\end{pmatrix}\in\mathbb{Z}^{m+n}\setminus\{0\}$, $x\in\mathbb{Z}^n$, $y\in\mathbb{Z}^m$, $\|x\|_\infty\leq t$, $\|-Ax+y\|_\infty<1/t^{n/m}$ ($\Rightarrow x\neq 0$).

Thm. $\forall \widetilde{A}=\begin{pmatrix}\widetilde{A}_1\\ \vdots\\ \widetilde{A}_\ell\end{pmatrix}\in GL_\ell(\mathbb{R})$ $\forall i_0\in\{1,\dots,\ell\}$ $\forall t_1,\dots,t_\ell>0$ such that $\prod\limits_{j=1}^\ell t_j\geq|\det(\widetilde{A})|$ $\exists z\in\mathbb{Z}^\ell\setminus\{0\}$ $\forall i\neq i_0$ $|\widetilde{A}_iz|<t_i$, $|\widetilde{A}_{i_0}z|\leq t_{i_0}$.

[$\forall k\in\mathbb{N}_+$ $\mathrm{vol}\left\{z\in\mathbb{R}^\ell \mid \forall i\neq i_0\ |\widetilde{A}_iz|<t_i,\ |\widetilde{A}_{i_0}z|<t_{i_0}(1+1/k)\right\}=2^\ell(1+\frac{1}{k})\prod\limits_1^\ell t_j\,|\det(\widetilde{A})|^{-1}>2^\ell$

Minkowski $\Rightarrow \exists\ 0\neq z_k\in\mathbb{Z}^\ell\cap(\text{--}\!\!\text{''}\!\!\text{--})$; $\{z_k\}$ contains some $z\in\mathbb{Z}^\ell\setminus\{0\}$ for ∞ many k.]

The exponent n/m in Thm' cannot be improved! Here is the proof if $n=1$:

Thm (Easy part of Khintchine's thm, 1926). Given functions $f_1, \dots, f_m : \mathbb{N}_+ \longrightarrow (0,1]$, let $f(q) = f_1(q) \cdots f_m(q)$. If $\sum_{q=1}^{\infty} f(q) < \infty$ (example: $f_i(q) = 1/q^{1/m+\varepsilon}$, $\varepsilon > 0$), then

$\mu\big(\{(\alpha_1, \dots, \alpha_m) \in (\mathbb{R}^m)^* \mid \exists\, \infty \text{ many } q \in \mathbb{N}_+ \text{ such that } \forall i = 1, \dots, m \ \ (\!(q\alpha_i)\!) \le f_i(q)\}\big) = 0$

(μ the Lebesgue measure).

Pf. Enough to consider $\alpha \in [0,1]^m = X$. We apply the

Borel–Cantelli Lemma: if $B_1, B_2, \dots \subset X$ are measurable subsets such that $\sum_{1}^{\infty} \mu(B_k) < \infty$, then $C = \{\alpha \in X \mid \exists\, \infty \text{ many } k \text{ such that } \alpha \in B_k\}$ $\Big(= \bigcap_{j \ge 1} C_j,\ C_j = \bigcup_{k \ge j} B_k\Big)$ satisfies $\mu(C) = 0$.

$\Big[C_1 \supset C_2 \supset \cdots \Rightarrow \forall j_0 \quad \mu(C) \le \mu(C_{j_0}) \le \underbrace{\sum_{k \ge j_0} \mu(B_k)}_{< \varepsilon \text{ if } j_0 \ge N(\varepsilon)} \Big]$

to $B_k = \{x \in X \mid \forall i = 1, \dots, m \ \ (\!(kx_i)\!) \le f_i(k)\}$. Each B_k is covered (up to translates by elements of $\mathbb{Z}^m$) by $\coprod_{0 \le N_1, \dots, N_m \le k-1} \prod_{1}^{m} \left[\frac{N_i - f_i(k)}{k}, \frac{N_i + f_i(k)}{k}\right]$,

hence $\mu(B_k) = k^m \prod_{i=1}^{m} \frac{2f_i(k)}{k} = 2^m f(k) \Longrightarrow \sum \mu(B_k) < \infty$.

The difficult part of Khintchine's Thm: if $f_1 = \cdots = f_m : [1, \infty) \longrightarrow (0, \infty)$ is continuous, $x f_1(x)^m$ is decreasing, $\lim_{x \to +\infty} x f_1(x)^m = 0$ and $\int_1^{\infty} f_1(x)^m dx = \infty$, then $\mu\big(\{(\alpha_1, \dots, \alpha_m) \in [0,1]^m \mid \exists\, \infty \text{ many } q \in \mathbb{N}_+ \text{ such that } \max_{1 \le i \le m} (\!(q\alpha_i)\!) \le f_1(q)\}\big) = 1$

Ex: $f_1(x) = \dfrac{1}{(x \ln(x))^{1/m}}$

Duality (= transference) results

Khintchine observed (1925, 1926) that there is a relation between approximation properties of $(\!(\alpha_1 x_1 + \cdots + \alpha_n x_n)\!)$ and $\max_{1\le i\le n} (\!(\alpha_i x)\!)$. Dyson (1947) generalised this to the case of approximations of $(\!(Ax)\!)$ $(x\in\mathbb{Z}^n)$ and $(\!(x^*A)\!)$ $(x^*\in(\mathbb{Z}^m)^*)$, for a given matrix $A\in M_{m,n}(\mathbb{R})$. The proofs used Dirichlet's Box Principle. Mahler (1939, 19) gave a more elegant treatment based on Minkowski's theorem for parallelograms (reproduced below) and another, more conceptual argument, relying on a variant of Minkowski's 2nd theorem (on successive minima) and its behaviour under duality.

Proposition (Mahler) Given $\widetilde{A},\widetilde{B}\in GL_\ell(\mathbb{R})$ such that $\widetilde{B}\widetilde{A}\in M_\ell(\mathbb{Z})$, and $z\in\mathbb{Z}^\ell\smallsetminus\{0\}$ with $\|\widetilde{A}z\|_\infty\le\lambda \Rightarrow \exists\, z^*\in(\mathbb{Z}^\ell)^*\smallsetminus\{0\}$ $\|z^*\widetilde{B}\|_\infty\le(\ell-1)(\lambda|\det\widetilde{B}|)^{\frac{1}{\ell-1}}$.

Pf: let $\widetilde{A}_i$ (resp. $\widetilde{B}_i$) be the rows (resp. columns) of $\widetilde{A}$ (resp. $\widetilde{B}$):

$\widetilde{A}=\begin{pmatrix}\widetilde{A}_1\\ \vdots\\ \widetilde{A}_\ell\end{pmatrix}$, $\widetilde{B}=(\widetilde{B}_1|\cdots|\widetilde{B}_\ell)$. We can assume that $\lambda=\max_{1\le i\le\ell}|\widetilde{A}_i z|=|\widetilde{A}_\ell z|$.

the matrix $\widetilde{C}=(\widetilde{B}_1|\cdots|\widetilde{B}_{\ell-1}|\widetilde{B}\widetilde{A}z)\in M_\ell(\mathbb{R})$ satisfies $\det(\widetilde{C})=\det(\widetilde{B})(\widetilde{A}_\ell z)\neq0$

the parallelogram $\widetilde{K}=\{z^*\in(\mathbb{R}^\ell)^* \mid \forall i\neq\ell\ |z^*\widetilde{C}_i|\le|\det(\widetilde{C})|^{1/(\ell-1)},\ |z^*\widetilde{C}_\ell|<1\}$ has $\mathrm{vol}(\widetilde{K})=2^\ell \overset{\text{Minkowski}}{\underset{+\text{c}}{\Longrightarrow}} \exists\, z^*\in((\mathbb{Z}^\ell)^*\smallsetminus\{0\})\cap\widetilde{K}$. But $z^*\widetilde{C}_\ell=z^*\widetilde{B}\widetilde{A}z\in\mathbb{Z}$

$\Rightarrow 0=(z^*\widetilde{B})(\widetilde{A}z)=\sum_{i=1}^{\ell}(z^*\widetilde{B})_i(\widetilde{A}z)_i \Rightarrow |(z^*\widetilde{B})_\ell|\le(\ell-1)|\det(\widetilde{C})|^{1/(\ell-1)}$.

Cor. Let $A\in M_{m,n}(\mathbb{R})$, $0<u<1<t$. If $\exists\, x\in\mathbb{Z}^n\smallsetminus\{0\}$ $\|x\|_\infty\le t$, $(\!(Ax)\!)\le u$

$\Rightarrow \exists\, x^*\in(\mathbb{Z}^m)^*\smallsetminus\{0\}$ $\|x^*\|_\infty\le t^*=Cu^{-1}$, $(\!(x^*A)\!)\le u^*=Ct^{-1}$, $C=(\ell-1)(t^n u^m)^{1/(\ell-1)}$

$\ell=(m+n)$

Pf. Apply Prop. to $\widetilde{A}=\begin{pmatrix}t^{-1}\cdot I_n & 0\\ 0 & u^{-1}I_m\end{pmatrix}\begin{pmatrix}I_n & 0\\ -A & I_m\end{pmatrix}$, $\widetilde{B}=\widetilde{A}^{-1}=\begin{pmatrix}I_n & 0\\ A & I_m\end{pmatrix}\begin{pmatrix}t\cdot I_n & 0\\ 0 & u\cdot I_m\end{pmatrix}$, $\lambda=1$.

By assumption, $\exists\, 0\neq z=\begin{pmatrix}x\\ y\end{pmatrix}\in\mathbb{Z}^{m+n}$ $(0\neq x\in\mathbb{Z}^n,\ y\in\mathbb{Z}^m)$, $\|t^{-1}x\|_\infty\le1$, $\|u^{-1}(-Ax+y)\|_\infty\le1$

$\Longleftrightarrow \|\widetilde{A}z\|_\infty\le1 \overset{\text{Prop.}}{\Longrightarrow} \exists\, 0\neq z^*=(-y^*,x^*)\in(\mathbb{Z}^n)^*\oplus(\mathbb{Z}^m)^*$, $\|z^*\widetilde{B}\|_\infty\le(\ell-1)(t^n u^m)^{1/(\ell-1)}=C$

$\Rightarrow \|ux^*\|_\infty,\ \|t(x^*A-y^*)\|_\infty\le C \Rightarrow \|x^*\|_\infty\le t^*,\ (\!(x^*A)\!)\le u^*$.

If $x^*\neq0$, we are done. If $x^*=0 \Rightarrow y^*\neq0 \Rightarrow 1\le\|y^*\|_\infty\le u^*$.

As $t^*=(\ell-1)t^{n/(\ell-1)}u^{(1-n)/(\ell-1)}>1$, we can take $x^*=(1,0,\dots,0)$.

Def $A \in M_{m,n}(\mathbb{R})$ is badly approximable if $\exists\ c(A)>0$ such that
$\forall x \in \mathbb{Z}^n \setminus \{0\}$ $\quad \langle\!\langle Ax \rangle\!\rangle \geq c(A) / \|x\|_\infty^{n/m}$.

Ex: $(m=n=1)$ $\alpha = \sqrt{2}$

Exercise: $\forall \ell \geq 2$ $\left(\sqrt[\ell]{2}, (\sqrt[\ell]{2})^2, \dots, (\sqrt[\ell]{2})^{\ell-1}\right) \in M_{1,\ell-1}(\mathbb{R})$ is badly approximable:
$\forall\, {}^t(q_1, \dots, q_{\ell-1}) \in \mathbb{Z}^{\ell-1} \setminus \{0\}$ $\quad \left\langle\!\!\left\langle \sum_{j=1}^{\ell-1} q_j (\sqrt[\ell]{2})^j \right\rangle\!\!\right\rangle \geq \text{const}(\ell) \cdot \max(|q_1|, \dots, |q_{\ell-1}|)^{-(\ell-1)}$

Thm A is badly approximable $\iff {}^tA \in M_{n,m}(\mathbb{R})$ is badly approximable.

Pf: If ${}^tA$ is badly approximable $\Rightarrow \exists\ c>0$ such that t^*, u^* in Cor. above satisfy $t^{*m} u^{*n} \geq c$; but $(t^{*m} u^{*n})^{m+n-1} = (\text{const.})(t^n u^m)$
$\Rightarrow$ taking $t = \|x\|_\infty$, $u = \langle\!\langle Ax \rangle\!\rangle$ we obtain $\langle\!\langle Ax \rangle\!\rangle \geq (\text{const}) / \|x\|_\infty^{n/m}$.

Thm. (Chinčin ($m=1$ or $n=1$), 1925, 1926; Dyson in general, 1947).
For each $A \in M_{m,n}(\mathbb{R})$, the numbers

$\omega = \sup\{\eta \geq 0 \mid \exists\ \infty \text{ many } x \in \mathbb{Z}^n \setminus \{0\} \text{ such that } \langle\!\langle Ax \rangle\!\rangle < 1 / \|x\|_\infty^{\frac{n}{m}(1+\eta)}\}$

$\omega^* = \sup\{\eta^* \geq 0 \mid$ —" $x^* \in (\mathbb{Z}^m)^* \setminus \{0\}$ —" $\langle\!\langle x^* A \rangle\!\rangle < 1 / \|x^*\|_\infty^{\frac{m}{n}(1+\eta^*)}\}$

satisfy $\omega^* \geq \dfrac{\omega}{(n-1)\omega + (m+n-1)}$, $\omega \geq \dfrac{\omega^*}{(m-1)\omega^* + (m+n-1)}$.

Pf. Exercise (using Cor. above).

Def: A is very well approximable if $\omega > 0$. $\omega^* > 0$

Cor. —" $\iff$ ${}^tA$ is very well approximable.

Rmk: As in the case $n=1$, the set of very well approximable matrices has measure zero (with respect to the Lebesgue measure on $M_{m,n}(\mathbb{R}) \simeq \mathbb{R}^{mn}$).

References:

J. W. S. Cassels, An Introduction to Diophantine Approximation, CUP, 1957, ch. V

W. Schmidt, Diophantine Approximation, Lecture Notes in Maths. 785, Springer 1980, ch. II, IV.

Existence of approximations $\Longrightarrow$ non-existence of very good approximations

Prop. Let $\alpha \in \mathbb{R}$. Assume that there exist integers $p_n, q_n \in \mathbb{Z}$ $(n \geq 1)$ such that $q_n \neq 0$, $\alpha \neq p_n/q_n$, $\limsup_{n \to +\infty} \frac{\log |q_n|}{n} \leq a$, $\lim_{n \to +\infty} \frac{\log |q_n \alpha - p_n|}{n} = -b$ $(a, b > 0)$.

Then: $\alpha \notin \mathbb{Q}$ and $\forall \mu > \frac{a}{b}$ $\exists\, c(\mu), q_0(\mu) > 0$ $\forall p, q \in \mathbb{Z}$ with $|q| \geq q_0(\mu)$ $|q\alpha - p| \geq \frac{c(\mu)}{|q|^\mu}$.

Rmk: existence of p_n, q_n $(n \geq 1)$ with $|q_n| \to +\infty$, $|q_n \alpha - p_n| \leq |q_n|^{-1} \Longrightarrow a \geq b$.

Pf. Fix $\varepsilon > 0$ such that $\frac{1+\varepsilon}{1-\varepsilon}\left(\frac{a}{b} + 1\right) \leq \mu + 1$ $\left(\Longrightarrow \frac{1+\varepsilon}{1-\varepsilon}\frac{a}{b} < \mu\right)$ and define $f(x) = e^{(1-\varepsilon)bx}$ $(x \geq 0)$. By definition of a and b, $\exists\, N_0(\varepsilon)$ $\forall n \geq N_0(\varepsilon)$

(1) $|q_n| \leq e^{(1+\varepsilon)an} = f(n)^{\frac{1+\varepsilon}{1-\varepsilon}\frac{a}{b}} < f(n)^\mu$

(2) $f(n) = e^{(1-\varepsilon)bn} \leq \frac{1}{|q_n\alpha - p_n|} \leq e^{(1+\varepsilon)bn} = f(n)^{\frac{1+\varepsilon}{1-\varepsilon}}$

$\Longrightarrow \frac{|q_n|}{|q_n\alpha - p_n|} \leq f(n)^{\frac{1+\varepsilon}{1-\varepsilon}\left(\frac{a}{b}+1\right)} \leq f(n)^{\mu+1}$

Assume that $p, q \in \mathbb{Z}$, $|q| \geq \frac{1}{2} f(N_0(\varepsilon))$. Let $n > N_0(\varepsilon)$ be such that

$$\frac{1}{2} f(n-1) \leq |q| \leq \frac{1}{2} f(n).$$

Case 1. $\left(\frac{p}{q} = \frac{p_n}{q_n}\right)$ $|q\alpha - p| = \frac{|q|}{|q_n|}|q_n\alpha - p_n| \geq \frac{f(n-1)/2}{f(n)^{\mu+1}} = \frac{1}{2e^{(1-\varepsilon)b(\mu+1)}} \frac{1}{f(n-1)^\mu} \geq$

$$\geq \left(2e^{(1-\varepsilon)b}\right)^{-\mu-1} |q|^{-\mu}$$

Case 2. $\left(\frac{p}{q} \neq \frac{p_n}{q_n}\right)$ $1 \leq |p_n q - q_n p| = |q_n(q\alpha - p) - q(q_n\alpha - p_n)|$

$$|q| \cdot |q_n\alpha - p_n| \leq \frac{1}{2} f(n) |q_n\alpha - p_n| \leq \frac{1}{2}$$

$\Longrightarrow |q\alpha - p| \geq \frac{1}{2|q_n|}$

$$|q\alpha - p| \geq \frac{1}{2|q_n|} \geq \frac{1}{2f(n)^\mu} = \frac{1}{2e^{(1-\varepsilon)b\mu} f(n-1)^\mu} \geq \frac{1}{2}\left(2e^{(1-\varepsilon)b}\right)^{-\mu} |q|^{-\mu}$$

Note: an effective upper bound on $N_0(\varepsilon)$

$\Downarrow$

_____ " _____ on $q_0(\mu)$

Closed subgroups of $\mathbb{R}^m$ and Kronecker's Theorem

See C.L. Siegel, Lectures on the Geometry of Numbers, Springer, 1989, lect. VI.

Thm (The special case $n=1$ of Kronecker's thm). If $\alpha_1, \dots, \alpha_m \in \mathbb{R}$ are such that $1, \alpha_1, \dots, \alpha_m$ are linearly independent over $\mathbb{Z}$, then

$\forall \beta_1, \dots, \beta_m \in \mathbb{R}$ $\forall \varepsilon > 0$ $\exists q \in \mathbb{Z}$ $\exists p_1, \dots, p_m \in \mathbb{Z}$ $\forall i = 1, \dots, m$ $|q\alpha_i - \beta_i - p_i| < \varepsilon$

$\Leftrightarrow$ ——— " ——— $\forall i = 1, \dots, m$ $(\!(q\alpha_i - \beta_i)\!) < \varepsilon$).

Rmks: (1) If there exists a non-trivial relation $\sum_{i=1}^{m} t_i \alpha_i \in \mathbb{Z}$ $(t_i \in \mathbb{Z})$, then the condition $\forall i$ $(\!(q\alpha_i - \beta_i)\!) < \varepsilon$ implies that $(\!(\sum_1^m t_i \beta_i)\!) < \varepsilon \sum_1^m |t_i|$, hence any m-tuple $\beta_1, \dots, \beta_m$ with the property $\forall \varepsilon > 0$ $\exists q \in \mathbb{Z}$ $\forall i$ $(\!(q\alpha_i - \beta_i)\!) < \varepsilon$ must satisfy $\sum_1^m t_i \beta_i \in \mathbb{Z}$.

(2) A more general version of Kronecker's thm (see below) implies that the necessary condition on $\beta_1, \dots, \beta_m$ given in (1) is also sufficient.

(3) Exercise: Thm above is equivalent to

thm'. If $\alpha_1, \dots, \alpha_m \in \mathbb{R}$ are linearly independent over $\mathbb{Z}$, then

$\forall \beta_1, \dots, \beta_m \in \mathbb{R}$ $\forall \varepsilon > 0$ $\exists t \in \mathbb{R}$ $(\!(t\alpha_i - \beta_i)\!) < \varepsilon$.

(4) Notation: for a subset $X \subset \mathbb{R}^m$, denote by $\overline{X}$ its closure (the intersection of all closed subsets of $\mathbb{R}^m$ containing X).

A subset $X \subset \mathbb{R}^m$ is dense if $\overline{X} = \mathbb{R}^m$ ($\Leftrightarrow$ $\forall$ non-empty open $U \subset \mathbb{R}^m$ we have $U \cap X \neq \emptyset \Leftrightarrow \forall \beta \in \mathbb{R}^m$ $\forall \varepsilon > 0$ $\exists x \in X$ $\|x - \beta\|_\infty < \varepsilon$).

More generally, $\beta \in \overline{X} \Leftrightarrow \forall \varepsilon > 0$ $\exists x \in X$ $\|x - \beta\|_\infty < \varepsilon$.

(5) As a result, the conclusion of thm above amounts to saying that the subgroup $\mathbb{Z}^m + \mathbb{Z}\begin{pmatrix}\alpha_1\\ \vdots \\ \alpha_m\end{pmatrix}$ is dense in $\mathbb{R}^m$.

(6) One can also consider the quotient space $\mathbb{R}^m/\mathbb{Z}^m$ with the quotient topology: a subset $U \subset \mathbb{R}^m/\mathbb{Z}^m$ is open $\Leftrightarrow$ its inverse image $pr^{-1}(U) \subset \mathbb{R}^m$ (under the projection $pr: \mathbb{R}^m \longrightarrow \mathbb{R}^m/\mathbb{Z}^m$) is open. These are also the open sets given by the metric $d(pr(x), pr(x')) = (\!(x - x')\!)$. Under the bijective map $E: \mathbb{R}^m/\mathbb{Z}^m \longrightarrow U(1)^m = \{(z_1, \dots, z_m) \mid z_j \in \mathbb{C},\ |z_j| = 1\}$

$x \longmapsto (e^{2\pi i x_1}, \dots, e^{2\pi i x_m})$

the open subsets of $\mathbb{R}^m/\mathbb{Z}^m$ correspond to the open subsets of the torus $U(1)^m = (S^1)^m \subset \mathbb{C}^m$ (intersections of $U(1)^m$ with open subsets of $\mathbb{C}^m$).

(7) The conclusion of Thm above then says that $\mathrm{pr}\left(\mathbb{Z}\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_m\end{pmatrix}\right)$ is dense in $\mathbb{R}^m/\mathbb{Z}^m$.

Auxiliary Thm. Let V be an $\mathbb{R}$-vector space, $\dim_{\mathbb{R}}(V)<\infty$. If $H\subset(V,+)$ is an additive subgroup of V, then there exist direct sum decompositions

$$\begin{array}{ccccc} H & = & H_0 & \oplus & H_1 \oplus \{0\} \\ \cap & & \cap & & \cap \quad \cap \\ V & = & V_0 & \oplus & V_1 \oplus V_2 \end{array}$$

where (1) $V_i\subset V$ is an $\mathbb{R}$-vector subspace,
(2) H_0 is dense in V_0
(3) H_1 is a lattice in V_1

Cor. Closed subgroups $H\subset(V,+)$ are of the form $H=V_0\oplus H_1\oplus\{0\}$, where $V=V_0\oplus V_1\oplus V_2$ as above and $H_1\subset V_1$ is a lattice.
(in concrete terms, $\exists$ $\mathbb{R}$-basis $e_1,\dots,e_m$ of V such that $H=\mathbb{R}e_1\oplus\cdots\oplus\mathbb{R}e_s\oplus\mathbb{Z}e_{s+1}\oplus\cdots\oplus\mathbb{Z}e_r$, for some $0\le s\le r\le m=\dim(V)$.

Prop.–Def. For a subgroup $H\subset(V,+)$ $(\dim_{\mathbb{R}}(V)<\infty)$, let $F(H)=\{f\in V^*=\mathrm{Hom}_{\mathbb{R}}(V,\mathbb{R}) \mid f(H)\subset\mathbb{Z}\}$; then the closure $\overline{H}$ of H is equal to $\{v\in V \mid \forall f\in F(H)\ \ f(v)\in\mathbb{Z}\}=:H'$.

Pf: $\overline{H}$ is again a subgroup of V: if $v,v'\in\overline{H}\Rightarrow\exists\{v_k\},\{v_k'\}\subset H$ with $\lim_{k\to\infty}v_k=v$, $\lim_{k\to\infty}v_k'=v'\Rightarrow\lim_{k\to\infty}(v_k-v_k')=v-v'\Rightarrow v-v'\in\overline{H}$.

By definition, $H\subset H'$ and H' is a closed subgroup of V $\Rightarrow\overline{H}\subset H'$. If $v\in V$, $v\notin\overline{H}$, write $\overline{H}$ as in Cor. above:

$H\not\ni v=\sum_1^m t_ie_i$, with either • $t_i\neq0$ for some $i>r\Rightarrow e_i^*\cdot\frac{\sqrt{2}}{t_i}=f\in F(H)$, $f(v)=\sqrt{2}\notin\mathbb{Z}\Rightarrow v\notin H'$

or • $t_i\notin\mathbb{Z}$ for some $i\in\{s+1,\dots,r\}\Rightarrow f=e_i^*\in F(H)$, $f(v)=t_i\notin\mathbb{Z}\Rightarrow v\notin H'$.

Therefore $v\notin\overline{H}\Rightarrow v\notin H'$, hence $H'\subset\overline{H}$.

Thm (Kronecker) Let $A\in M_{m,n}(\mathbb{R})=\mathrm{Hom}_{\mathbb{R}}(\mathbb{R}^n,\mathbb{R}^m)$, let $A(\mathbb{Z}^n)\subset\mathbb{R}^m$ be the subgroup generated by the columns of A. Then:

(1) the closure of $\mathbb{Z}^m+A(\mathbb{Z}^n)$ (in $\mathbb{R}^m$) is equal to
$\{y\in\mathbb{R}^m \mid \forall x^*\in(\mathbb{Z}^m)^* \text{ such that } x^*A\in(\mathbb{Z}^n)^* \text{ we have } x^*y\in\mathbb{Z}\}$.

(2) $\mathbb{Z}^m+A(\mathbb{Z}^n)$ is dense in $\mathbb{R}^m$ $(\Leftrightarrow\mathrm{pr}(A(\mathbb{Z}^n))$ is dense in $\mathbb{R}^m/\mathbb{Z}^m)$

$\Updownarrow$

$\{x^*\in(\mathbb{Z}^m)^* \mid x^*A\in(\mathbb{Z}^n)^*\}=\{(0,\dots,0)\}\Leftrightarrow\forall x^*\in(\mathbb{Z}^m)^*\setminus\{0\}\ \ x^*A\notin(\mathbb{Z}^n)^*$.

Ex: if $n=1$, then $A=\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_m\end{pmatrix}$ and $\left[\mathbb{Z}^m+\mathbb{Z}\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_m\end{pmatrix}\right.$ is dense in $\mathbb{R}^m\Leftrightarrow\forall x^*=(x_1,\dots,x_m)\in(\mathbb{Z}^m)^*$, $\left.\sum_1^m x_i\alpha_i\notin\mathbb{Z}\right]$

R: (1) $F(\mathbb{Z}^m) = (\mathbb{Z}^m)^*$, $F(A(\mathbb{Z}^n)) = \{x^* \in (\mathbb{R}^m)^* \mid x^* A \in (\mathbb{Z}^n)^*\} \Rightarrow$
$F(\mathbb{Z}^m + A(\mathbb{Z}^n)) = F(\mathbb{Z}^m) \cap F(A(\mathbb{Z}^n)) = \{x^* \in (\mathbb{Z}^m)^* \mid$ — " — $\}$; apply Prop. for $H = \mathbb{Z}^m + A(\mathbb{Z}^n)$. the statement (2) follows from (1).

It remains to prove the Auxiliary Thm above (in fact, its Corollary would suffice). So, let $H \subset (V, +)$ be a subgroup, $m = \dim_{\mathbb{R}}(V) < \infty$.
For $\varepsilon > 0$, let $H(\varepsilon)$ = the subgroup of H generated by $H \cap \{v \in V \mid \|v\| < \varepsilon\}$
$V(\varepsilon)$ = the $\mathbb{R}$-vectorspace " ",

$V_0 := \bigcap_{\varepsilon>0} V(\varepsilon)$, $W := \bigcup_{\varepsilon>0} V(\varepsilon) \supset H = \bigcup_{\varepsilon>0} H(\varepsilon)$, $s = \dim_{\mathbb{R}}(V_0)$, $r = \dim_{\mathbb{R}}(W)$.

If $s = 0 \Rightarrow$ H is a discrete subgroup of W containing a basis $\Rightarrow$ H is a lattice in $W \Rightarrow$ result.

If $s > 0$: Claim1: $H \cap V_0$ is dense in V_0: indeed, $\forall \varepsilon > 0$ $\exists \varepsilon' > 0$ such that $s\varepsilon' < \varepsilon$ and $V(\varepsilon') = V_0 \Rightarrow$ $\exists v_1, \dots, v_s \in H(\varepsilon')$ such that $V_0 = \bigoplus_1^s \mathbb{R} v_i$.
$\forall v \in V_0$ $v = \sum_1^s \lambda_i v_i = \underbrace{\sum_1^s [\lambda_i] v_i}_{w} + \underbrace{\sum_1^s \{\lambda_i\} v_i}_{v-w}$, $w \in H \cap V_0$, $\|v - w\| \le s\varepsilon' < \varepsilon$
$\Rightarrow$ $v \in \overline{H \cap V_0}$.

If $s = r$: H is dense in $V_0 \Rightarrow$ result.

If $0 < r - s = q$: $\exists w_1, \dots, w_q \in H$ such that $v_1, \dots, v_s$ (as above), $w_1, \dots, w_q$ is an $\mathbb{R}$-basis of $W = V_0 \oplus W_1$, $W_1 = \bigoplus_1^q \mathbb{R} w_j$. Let $p_0 : W \to V_0$, $p_1 : W \to W_1$ be the corresponding projections.

Claim2: $p_1(H) \subset W_1$ is a discrete subgroup ($\Rightarrow$ a lattice in W_1).
Indeed, if not, then $\forall \varepsilon > 0$ $\exists h \in H$ $0 < \|p_1(h)\| < \frac{\varepsilon}{2}$. But $\overline{H \cap V_0} = V_0 \Rightarrow$
$\exists h' \in H \cap V_0$ $\|p_0(h) - h'\| < \frac{\varepsilon}{2} \Rightarrow$ $\left.\begin{matrix} \|h - h'\| < \varepsilon \\ h \notin V_0 \end{matrix}\right\} \Rightarrow$ $h - h' \in H$, $h - h' \notin V_0$ impossible for small $\varepsilon > 0$.

So $\exists H_1 \subset H$, $H_1 \simeq \mathbb{Z}^q$ such that $p_1(H) = p_1(H_1) \simeq \mathbb{Z}^q \subset W_1$ lattice,
$p_1|_{H_1} : H_1 \xrightarrow{\sim} p_1(H_1)$.
$\Rightarrow$ $H = (H \cap V_0) \oplus H_1$, as claimed.

Rmks: (1) H. Weyl (1916) proved an equidistribution result for $pr(A(\mathbb{Z}^n)) \subset pr(\overline{\mathbb{Z}^m + A(\mathbb{Z}^n)})$, using Fourier series.

(2) H. Bohr gave three closely related analytic proofs of Thm' above. the most elegant one involves an analysis of $\limsup_{T \to +\infty} \frac{1}{T} \int_0^T \left| 1 + \sum_{j=1}^m e^{2\pi i (t\alpha_j - \beta_j)} \right|^p$ for $p \in \mathbb{N}_+$, $p \gg 0$.
See K. Chandrasekharan, Introduction to Analytic Number Theory, Springer, 1968 ch. VIII.

(3) Thms above are closely related to Pontryagin duality.