$\mathbb{Z} \subset \mathbb{R}$, $\mathbb{Z}[1/p] \subset \mathbb{Q}_p \times \mathbb{R}$, $\mathbb{Q} \subset \hat{\mathbb{Q}} \times \mathbb{R} = \mathbb{A}$

We know that, for any finite set of primes $S = \{p_1, \dots, p_r\} \subset \mathcal{P}$, $\mathbb{Z}$ is dense in $\mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_r} = \prod_{p \in S} \mathbb{Z}_p$, by the Chinese Remainder Thm.

($\Rightarrow$ $\mathbb{Q}$ is dense in $\prod_{p \in S} \mathbb{Q}_p$).

$a \longmapsto (a, a, \dots, a)$

What about the subrings $\mathbb{Z}[1/p] = \left\{ \frac{a}{p^n} \mid a \in \mathbb{Z}, n \geq 0 \right\} \subset \mathbb{Q}$

$$\mathbb{Z}[1/S] := \mathbb{Z}[1/(p_1 \cdots p_r)] = \left\{ \frac{a}{p_1^{n_1} \cdots p_r^{n_r}} \;\middle|\; \begin{matrix} a \in \mathbb{Z}, \\ n_i \geq 0 \end{matrix} \right\} \subset \mathbb{Q} ?$$

It turns out that the embedding $\mathbb{Z}[1/p] \subset \mathbb{Q}_p \times \mathbb{R}$ (and, more generally, $\mathbb{Z}[1/S] \subset \prod_{p \in S} \mathbb{Q}_p \times \mathbb{R}$) behaves very much like $\mathbb{Z} \subset \mathbb{R}$.

Exercise 1. Let $p \neq q$ be primes. (1) By considering the compact subset $\mathbb{Z}_p \times [-1,1] \subset \mathbb{Q}_p \times \mathbb{R}$ and its interior $\mathbb{Z}_p \times (-1,1)$ show that the abelian group $\mathbb{Z}[1/p]$ is discrete (hence closed) in $\mathbb{Q}_p \times \mathbb{R}$ and the quotient group $(\mathbb{Q}_p \times \mathbb{R}) / \mathbb{Z}[1/p]$ (with the quotient topology) is compact (Hausdorff, and every open cover has a finite subcover).

(2) Show that: $\lim_{n \to +\infty} p^{(q-1)q^n} = (0,1) \in \mathbb{Z}_p \times \mathbb{Z}_q \subset \mathbb{Q}_p \times \mathbb{Q}_q$

$\lim_{n \to +\infty} p^{-(q-1)q^n} = (0,1) \in \mathbb{R} \times \mathbb{Z}_q \subset \mathbb{R} \times \mathbb{Q}_q$.

(3) $\mathbb{Z}[1/p]$ is dense in both $\mathbb{Q}_p$ and $\mathbb{R}$.

(4) $\mathbb{Z}_p[1/p]$ is dense in $\mathbb{Q}_p \times \mathbb{Z}_q$ and in $\mathbb{R} \times \mathbb{Z}_q$.

Exercise 2. (1) Let $S \subset \mathcal{P} = \{\text{primes}\}$, $T \subset \mathcal{P} \cup \{\infty\}$ be non-empty finite subsets. Determine the closure of $\mathbb{Z}[1/S] = \mathbb{Z}[1/\prod_{p \in S} p]$ in $\prod_{v \in T} \mathbb{Q}_v$ ($\mathbb{Q}_\infty = \mathbb{R}$).

---

(2) Show that $\mathbb{Q}$ is dense in $\prod_{v \in T} \mathbb{Q}_v$.

Exercise 3. (1) Show that the continuous map

$$\begin{array}{ccc} \mathbb{R} & \longrightarrow & (\mathbb{Q}_p \times \mathbb{R})/\mathbb{Z}[1/p] \\ \downarrow & & \downarrow \\ a & \longmapsto & (0,a) + \mathbb{Z}[1/p] \end{array}$$

is injective, with dense image. Does it induce a homeomorphism between $\mathbb{R}$ and its image?

(2) $(\mathbb{Q}_p \times \mathbb{R})/\mathbb{Z}[1/p]$ is connected.

(3) $\mathbb{Q}_p = \mathbb{Z}_p + \mathbb{Z}[1/p]$, $\mathbb{Z}_p \cap \mathbb{Z}[1/p] = \mathbb{Z}$, $\underbrace{\mathbb{Z}[1/p]/\mathbb{Z} \simeq \mathbb{Q}_p/\mathbb{Z}_p}_{\text{canonical isomorphism of abelian groups}}$.

(4) The inclusion $\mathbb{Z}_p \subset \mathbb{Q}_p$ defines an isomorphism of abelian groups

$$(\mathbb{Z}_p \times \mathbb{R})/\mathbb{Z} \xrightarrow{\sim} (\mathbb{Q}_p \times \mathbb{R})/\mathbb{Z}[1/p].$$

(5) The maps

$$(\mathbb{Z}_p \times \mathbb{R})/\mathbb{Z} = \left(\left(\varprojlim_{n\geq 0} \mathbb{Z}/p^n\mathbb{Z}\right) \times \mathbb{R}\right)/\mathbb{Z} \xrightarrow{\sim} \varprojlim_{n\geq 0} \mathbb{R}/p^n\mathbb{Z} \xrightarrow{\sim} \varprojlim_{n\geq 0} \left(\mathbb{R}/\mathbb{Z} \xleftarrow{\times p} \mathbb{R}/\mathbb{Z} \xleftarrow{\times p} \cdots\right)$$

$$\begin{array}{ccc} ((x_n), y) + \mathbb{Z} & \longmapsto & (y - x_n \ (\mathrm{mod}\ p^n\mathbb{Z})) \\ \downarrow & & \downarrow \\ (y_n)_{n\geq 0} & \longmapsto & (y_0, p^{-1}y_1, p^{-2}y_2, \cdots) \end{array}$$

are isomorphisms of abelian groups, as well as homeomorphisms.

(6) There exists a natural isomorphism of abelian groups

$$\underbrace{\mathrm{Hom}_{Ab}(\mathbb{Z}[1/p], \mathbb{R}/\mathbb{Z})}_{\{f : \mathbb{Z}[1/p] \to \mathbb{R}/\mathbb{Z} \text{ morphism of abelian gps}\}} \xrightarrow{\sim} (\mathbb{Z}_p \times \mathbb{R})/\mathbb{Z} \quad \text{that extends}$$

$$\begin{array}{ccc} \mathrm{Hom}_{Ab}(\mathbb{Z}, \mathbb{R}/\mathbb{Z}) & \xrightarrow{\sim} & \mathbb{R}/\mathbb{Z} \\ \downarrow & & \downarrow \\ f & \longmapsto & f(1). \end{array}$$

What is the topology on the left hand side that corresponds to the quotient topology on the right hand side?

Exercise 4. For a finite set $\emptyset \neq S = \{p_1, \dots, p_r\} \subset \mathcal{P}$ $(r \geq 1)$, generalise Exercise 3 by replacing $\mathbb{Z}[1/p]$ by $\mathbb{Z}[1/S]$ and $\mathbb{Q}_p$ by $\prod_{p\in S} \mathbb{Q}_p$.

Exercise 5. Pass to the limit "$S \to \mathcal{P}$": (1) let

$$\hat{\mathbb{Q}} := \bigcup_{\substack{S \subset \mathcal{P} \\ |S| < \infty}} \underbrace{\left(\prod_{p\in S} \mathbb{Q}_p\right) \times \left(\prod_{p\notin S} \mathbb{Z}_p\right)}_{\text{product topology}},$$

with $U \subset \hat{\mathbb{Q}}$ open $\Leftrightarrow$ its intersection with each is open

($\hat{\mathbb{Q}} \subset \prod_{p\in\mathcal{P}} \mathbb{Q}_p$, but its topology is not induced from the product topology on $\prod_{p\in\mathcal{P}} \mathbb{Q}_p$).

(2) Let $\widehat{\mathbb{Z}} := \prod_{p \in P} \mathbb{Z}_p \subset \widehat{\mathbb{Q}}$. Then $\widehat{\mathbb{Z}} + \mathbb{Q} = \widehat{\mathbb{Q}}$, $\widehat{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$.

(3) Let $\mathbb{A} := \widehat{\mathbb{Q}} \times \mathbb{R}$ (with the product topology). Then $\mathbb{Q}$ is discrete in $\mathbb{A}$ and $\mathbb{A}/\mathbb{Q}$ is compact.

(4) There is a natural isomorphism of abelian groups

$$\mathrm{Hom}_{Ab}(\mathbb{Q}, \mathbb{R}/\mathbb{Z}) \xrightarrow{\sim} (\widehat{\mathbb{Z}} \times \mathbb{R})/\mathbb{Z} \quad (\xrightarrow{\sim} (\widehat{\mathbb{Q}} \times \mathbb{R})/\mathbb{Q} = \mathbb{A}/\mathbb{Q}),$$

extending $\mathrm{Hom}_{Ab}(\mathbb{Z}[1/S], \mathbb{R}/\mathbb{Z}) \xrightarrow{\sim} (\prod_{p \in S} \mathbb{Z}_p \times \mathbb{R})/\mathbb{Z}$ [redacted]

$$\downarrow 2$$

$$(\prod_{p \in S} \mathbb{Q}_p \times \mathbb{R})/\mathbb{Z}[1/S]$$

from Exercise 3(6) (if $|S| = 1$) resp. Exercise 4.

Again, what is the topology on the L.H.S. corresponding to the product topology (and the quotient topology) on the R.H.S.?

---

(5) There are natural isomorphisms of abelian groups

$$\mathrm{Hom}_{Ab}(\mathbb{Z}, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z} = \widehat{\mathbb{Q}}/\widehat{\mathbb{Z}},$$

$$\mathrm{Hom}_{Ab}(\mathbb{Q}/\mathbb{Z}, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\sim} \widehat{\mathbb{Z}},$$

$$\mathrm{Hom}_{Ab}(\mathbb{Q}, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\sim} \widehat{\mathbb{Q}},$$

compatible with each other and with (4).

$x^2+y^2+z^2=m$ and geometry of numbers

Thm. An integer $m \geq 1$ is of the form $m = x^2+y^2+z^2$ $(x,y,z \in \mathbb{Z})$
$\Leftrightarrow$ $m \neq 4^a m'$, $m' \equiv -1 \pmod 8$, $a \geq 0$.

We know that $x^2 \equiv 0, 1, 4 \pmod 4$, which gives the easy implication $(\Rightarrow)$. the difficult part $(\Leftarrow)$ follows from

Thm'. If $m \geq 1$, $m \neq -1 \pmod 8$ is square free, then $\exists x,y,z \in \mathbb{Z}$ $x^2+y^2+z^2=$

Pf: (Ankeny, 1957) We use the following facts:

(a) Dirichlet's thm on primes in arithmetic progressions;

(b) Minkowski's thm for ellipsoids in $\mathbb{R}^3$;

(c) $\{n \in \mathbb{N}_+ \mid \exists u,v \in \mathbb{Z} \ u^2+v^2=n\} = \{n \in \mathbb{N}_+ \mid \exists u,v \in \mathbb{Q} \ u^2+v^2=n\} =$

$$= \left\{ \prod_{p \text{ prime}} p^{a_p} \mid a_p \equiv 0 \pmod 2 \text{ for each prime } p \equiv -1 \pmod 4 \right\}$$

Case 1: $\boxed{m \not\equiv 3 \pmod 8}$ By (a), $\exists$ prime $q \equiv -1 \pmod m$ such that

$$q \equiv \begin{cases} m-1 \pmod 8 & \text{if } 2 \mid m \\ m \pmod 4 & \text{if } 2 \nmid m \end{cases} \Rightarrow \text{QRL} \Rightarrow \left(\frac{-m}{q}\right) = 1. \quad \text{(note: } q \equiv 1 [4]\text{)}$$

Fix $b \in \mathbb{Z}$, $b^2 \equiv -m \pmod q$

the lattice $L := \{(x,y,z) \in \mathbb{Z}^3 \mid x \equiv y \pmod m, \ y \equiv bz \pmod q\} \subset \mathbb{R}^3$ satisfies

$\operatorname{vol}(\mathbb{R}^3/L) = mq$ and $\forall (x,y,z) \in L$ $qx^2+y^2+mz^2 \equiv \begin{cases} -x^2+y^2 \equiv 0 \pmod m \\ (b^2+m)z^2 \equiv 0 \pmod q \end{cases}$

$\Rightarrow qx^2+y^2+mz^2 \equiv 0 \pmod{mq}$.

the ellipsoid $K := \{qx^2+y^2+mz^2 < 2mq\}$ has volume $\frac{4\pi}{3} mq(\sqrt{2})^3 > 2^3 qm$.

By (b), $\exists (x,y,z) \in (K \cap L) \setminus \{0\} \Rightarrow \exists x,y,z \in \mathbb{Z}$ $qx^2+y^2+mz^2 = mq$.

If $p \neq 2, q$ is a prime such that $v_p(y^2+mz^2) \equiv 1 \pmod 2$, then $\left(\frac{-m}{p}\right) = 1$. On the other hand, $x^2-m \equiv 0 \pmod p \Rightarrow \left(\frac{m}{p}\right) = 1 \Rightarrow \left(\frac{-1}{p}\right) = 1 \Rightarrow p \equiv 1 [4]$

By (c), $\exists u,v \in \mathbb{Z}$ $(y^2+mz^2)/q = u^2+v^2 \Rightarrow m = x^2+u^2+v^2$.

Case 2: $\boxed{m \equiv 3 \pmod 8}$, $\exists$ prime $q \equiv 1 \pmod 4$, $q \equiv -\frac{1}{2} \pmod m \overset{\text{Jacobi symbol}}{\Rightarrow} \left(\frac{q}{m}\right) = \left(\frac{-2}{m}\right) = 1$

$\overset{\text{QRL}}{\Rightarrow} \left(\frac{m}{q}\right) = \left(\frac{-m}{q}\right) = 1$; fix $b \in \mathbb{Z}$ such that $b^2 \equiv -m \pmod q$ and repeat the previous arguments with $L := \{(x,y,z) \in \mathbb{Z}^3 \mid x \equiv y \pmod m, \ y \equiv bz \pmod{2q}\}$ and $K := \{(x,y,z) \in \mathbb{R}^3 \mid 2qx^2+y^2+mz^2 < 4mq\}$. In this case

$\operatorname{vol}(\mathbb{R}^3/L) = 2mq$, $\forall (x,y,z) \in L$ $2qx^2+y^2+mz^2 \equiv \begin{cases} -x^2+y^2 \equiv 0 \pmod m \\ y^2+mz^2 \equiv 0 \pmod{2q} \end{cases}$

$\operatorname{vol}(K) = \frac{4}{3} \frac{(2\sqrt{mq})^3}{\sqrt{2mq}} > 2^3 \cdot 2mq \overset{(b)}{\Rightarrow} \exists (x,y,z) \in (K \cap L) \setminus \{0\} \Rightarrow$

$\exists x,y,z \in \mathbb{Z}$ $2qx^2+y^2+mz^2 = 2mq$. Again, if $p \neq 2, q$ and $v_p(y^2+mz^2) \equiv 1$

$\Rightarrow p \equiv 1 \pmod 4 \overset{(c)}{\Rightarrow} \exists u,v \in \mathbb{Z}$ $(y^2+mz^2)/2q = u^2+v^2 \Rightarrow m = x^2+u^2+v^2$.

Minkowski's bounds for quadratic forms

Majorants: given a non degenerate real quadratic form of dim $= n \geq 1$

$f(x) := {}^t x Q x$, $Q = {}^tQ \in GL_n(\mathbb{R})$, choose a diagonalisation

${}^t U Q U = D = \begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_n \end{pmatrix}$, $d_j \in \mathbb{R}^\times$ $\quad (U \in GL_n(\mathbb{R}))$ and define

$D^+ := \begin{pmatrix} |d_1| & & 0 \\ & \ddots & \\ 0 & & |d_n| \end{pmatrix}$, $Q^+ := ({}^tU)^{-1} D^+ U^{-1} = {}^tQ^+$, $f^+(x) := {}^t x Q^+ x$.

$\det(Q^+) = |\det(Q)|$

Then: f^+ is positive definite and $\forall x \in \mathbb{R}^n \quad |f(x)| \leq f^+(x)$.

f^+ is called a majorant of f (obtained in this way) (f^+ is NOT unique)

Prop. For f as above, $\exists\, x \in \mathbb{Z}^n \setminus \{\begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}\}$ such that $|f(x)| \leq c(n) |\det(Q)|^{1/n}$,

where $c(n) = \frac{4}{\pi} \left((n/2)!\right)^{2/n} = \frac{4}{\pi} \Gamma\left(\frac{n}{2}+1\right)^{2/n}$.

PR: Minkowski's thm for $L = \mathbb{Z}^n$ and $K = \{x \in \mathbb{R}^n \mid f^+(x) \leq R\}$, where R is chosen so that

$$\frac{\pi^{n/2}}{(n/2)!} \frac{R^n}{|\det(Q)|^{1/2}} = \mathrm{vol}(K) = 2^n.$$

Ex: $c(2) = \frac{4}{\pi} < 2$, $c(3) = \left(\frac{6}{\pi}\right)^{2/3} < 2$, $c(4) = \frac{4\sqrt{2}}{\pi} < 2$, $c(5) > 2$

Quadratic forms over $\mathbb{Z}$

A real quadratic form $f(x) = {}^t x A x$, $A = {}^tA \in M_n(\mathbb{R})$ $\quad f(x) = \sum_{i,j=1}^n A_{ij} x_i x_j = \sum_1^n A_{ii} x_i^2 + \sum_{i<j} 2A_{ij} x_i x_j$

is called: (1) **matrix-integral** ("classically integral") if $A = {}^tA \in M_n(\mathbb{Z}) \iff \forall i \neq j \;\; A_{ii}, A_{ij} \in \mathbb{Z}$

$\iff \forall x, x' \in \mathbb{Z}^n \quad \frac{f(x+x') - f(x) - f(x')}{2} \in \mathbb{Z}$ $\quad (\overset{x=x'}{\Longrightarrow} f(x) \in \mathbb{Z})$

(2) **form-integral** if ~~$\forall x \in \mathbb{Z}^n$~~ $\forall i \neq j \;\; A_{ii}, 2A_{ij} \in \mathbb{Z}$ $\quad (\iff \forall x \in \mathbb{Z}^n \;\; f(x) \in \mathbb{Z})$

Change of variables by $B \in GL_n(\mathbb{Z})$ ~~$\neq$~~

$B \in M_n(\mathbb{Z})$, $\det(B) \in \mathbb{Z}^\times = \{\pm 1\}$, so $GL_n(\mathbb{Z}) = SL_n^{\pm}(\mathbb{Z})$

$f' := f|_B \quad f'(y) := f(By) = {}^t y \underbrace{{}^tBAB}_{A'} y$ $\quad \det(A') = \det(A)$

Such a form f' is called $GL_n(\mathbb{Z})$-equivalent to f. $\quad f' \underset{GL_n(\mathbb{Z})}{\sim} f$

(proper, or $SL_n(\mathbb{Z})$-) equivalent if $\det(B) = +1$.)

Note: f $\left\{\begin{matrix} \text{matrix-} \\ \text{form-} \end{matrix}\right\}$ integral $\not\Rightarrow$ so is $f|_B$, for any $B \in GL_n(\mathbb{Z})$.

Prop. If f is <u>matrix-integral</u> and $\pm 1 \in f(\mathbb{Z}^n)$, then $f \underset{Gl_n(\mathbb{Z})}{\sim} \pm x_1^2 + g(x_2, \dots, x_n)$, with g matrix-integral.

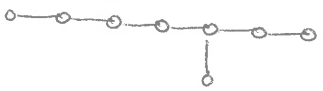
Pf: "Diagonalisation over $\mathbb{Z}$": after a $Gl_n(\mathbb{Z})$-change of basis of $\mathbb{Z}^n$, we can assume that $\pm 1 = f(e_1) = A_{11}$. In this case

$$f(x) = \pm x_1^2 + 2A_{12}x_1x_2 + \dots + 2A_{1n}x_1x_n + h(x_2, \dots, x_n) = \pm \underbrace{(x_1 \pm A_{12}x_2 \pm \dots \pm A_{1n}x_n)^2}_{x_1'^2} + g,$$

$\forall j \quad A_{1j} \in \mathbb{Z}$ $\qquad g = g(x_2, \dots, x_n)$.

Thm. If f is <u>matrix-integral</u>, <u>$|\det(f)| = 1$</u> and <u>$n \leq 4$</u>, then either $\exists x \in \mathbb{Z}^n \setminus \{0\} \quad f(x) = 0$, or $f \underset{Gl_n(\mathbb{Z})}{\sim} \pm(x_1^2 + \dots + x_n^2)$.

In fact, this is true for $n \leq 7$, but not for $n = 8$. The counterexample in dimension 8 is given by f corresponding to the Cartan matrix of the Dynkin diagram of E_8:



$$A = \begin{pmatrix} 2 & -1 & & & & & & \\ -1 & 2 & -1 & & & & & \\ & -1 & 2 & -1 & & & & \\ & & -1 & 2 & -1 & & & \\ & & & -1 & 2 & -1 & -1 & \\ & & & & -1 & 2 & & \\ & & & & -1 & & 2 & -1 \\ & & & & & & -1 & 2 \end{pmatrix}$$

$\det(f) = 1$, f is positive definite matrix-integral, $\forall x \in \mathbb{Z}^n \quad f(x) \in 2\mathbb{Z}$

Pf. This is trivially true for $n = 1$. Assume $2 \leq n \leq 4$. Minkowski's bound implies that $\exists x \in \mathbb{Z}^n \setminus \{0\} \quad |f(x)| \leq C(n)\,|\det(f)|^{1/n} = C(n) < 2$ (for $n \leq 4$), with $f(x) \in \mathbb{Z}$.

If $f(x) \neq 0$, then $f(x) = \pm 1 \overset{\text{Prop.}}{\Longrightarrow} f \underset{Gl_n(\mathbb{Z})}{\sim} \pm x_1^2 + g(x_2, \dots, x_n)$, g matrix-integral of $\dim(g) = n-1$, $|\det(g)| = 1 \overset{\text{induction}}{\Longrightarrow}$ Thm holds for g, by induction, so if f is not isotropic over $\mathbb{Q}$, then $f \underset{Gl_n(\mathbb{Z})}{\sim} \pm(x_1^2 + \dots + x_n^2)$.

Rmk: One can analyse the isotropic case more closely. The final result states that $f \underset{Gl_n(\mathbb{Z})}{\sim}$ direct sum of copies of x^2, $-x^2$, or $2x_1x_2$ (under the assumptions of the theorem).

Pf of Legendre's thm (in its original form)

(following Gauss, but replacing estimates given by reduction theory of quadratic forms in 3 variables by worse estimates coming from Minkowski's thm)

Thm (Legendre) Assume that $a_1, a_2, a_3 \in \mathbb{Z}\setminus\{0\}$, $a_1a_2a_3$ square-free, $a_1a_3 < 0$, $\exists\ t_1, t_2, t_3 \in \mathbb{Z}$ $a_1t_1^2 + a_2 \equiv 0 [a_3]$, $a_2t_2^2 + a_3 \equiv 0 [a_1]$, $a_3t_3^2 + a_1 \equiv 0 [a_2]$ then $\exists\ b_1, b_2, b_3 \in \mathbb{Z}$ (not all 0) such that $a_1b_1^2 + a_2b_2^2 + a_3b_3^2 = 0$.

Pf. the lattice $L = \left\{ x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \in \mathbb{Z}^3 \;\middle|\; x_1 \equiv t_1x_2 [a_3],\ x_2 \equiv t_2x_3 [a_1],\ x_3 \equiv t_3x_1 [a_2] \right\}$

satisfies $\mathrm{vol}(\mathbb{R}^3/L) = (\mathbb{Z}^3 : L) = |a_1a_2a_3|$ and $\left(f(x) := a_1x_1^2 + a_2x_2^2 + a_3x_3^2\right)$

$\forall\ x, x' \in L$ $\dfrac{f(x+x') - f(x) - f(x')}{2} = a_1x_1x_1' + a_2x_2x_2' + a_3x_3x_3' \equiv (a_1t_1^2 + a_2)x_2x_2' \equiv 0 [a_3]$

and similarly $\equiv 0 [a_1]$, $\equiv 0 [a_2]$, hence the quadratic form $g(y) := f(y_1e_{L,1} + y_2e_{L,2} + y_3e_{L,3})/(a_1a_2a_3)$ (for any fixed basis $\{e_{L,i}\}$ of $L = \mathbb{Z}e_{L,1} \oplus \mathbb{Z}e_{L,2} \oplus \mathbb{Z}e_{L,3}$)

satisfies $\forall\ y, y' \in \mathbb{Z}^3$ $\dfrac{g(y+y') - g(y) - g(y')}{2} \in \mathbb{Z}$, hence g is <u>matrix-integral</u>.

Moreover, $\det(g) = \dfrac{\det(f)}{(a_1a_2a_3)^{\dim(f)}} \cdot \dfrac{(\mathbb{Z}^3 : L)^2}{(a_1a_2a_3)^{\dim(f)}} = \dfrac{(a_1a_2a_3)\,|a_1a_2a_3|^2}{(a_1a_2a_3)^3} = 1$.

Thm above (for g): either g is isotropic $\Rightarrow \exists\ y \in \mathbb{Z}^3 \setminus \{\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}\}$ $g(y) = 0$

$\Rightarrow$ result,

or $g \sim \pm(y_1^2 + y_2^2 + y_3^2)$ — impossible, since f is indefinite.

Rmk. the assumptions in this theorem are equivalent (by Hensel's lemma) to the fact that the quadratic form $a_1x_1^2 + a_2x_2^2 + a_3x_3^2$ is isotropic <u>over $\mathbb{R}$</u> and <u>over $\mathbb{Q}_p$</u>, <u>for all primes $p \neq 2$</u>.

Legendre deduced from this result certain special cases of the quadratic reciprocity law (which was still a conjecture at the time).

Example : $\boxed{px^2+qy^2-z^2=0}$ $\quad p\neq q\in\mathbb{P}\setminus\{2\}$

If $\left(\frac{p}{q}\right)=\left(\frac{q}{p}\right)=1 \overset{\text{Thm}}{\Longrightarrow} \exists\, x,y,z\in\mathbb{Z}$ $\quad \gcd(x,y,z)=1$ $\quad px^2+qy^2-z^2=0$

But $px^2\equiv 0, p\ [4]$, $qy^2\equiv 0, q\ [4]$, $z^2\equiv 0,1\ [4] \Rightarrow p+q\equiv 0\ [4]$ or $p-1\equiv 0\ [4]$ or $q-1\equiv 0\ [4]$.

$\Rightarrow p\equiv 1\ [4]$ or $q\equiv 1\ [4]$.

Exercise. Apply the same argument to $px^2-qy^2-z^2=0$.

Question. Is there a reformulation of the QRL purely in terms of the solvability of suitable diophantine equations (of the form) $ax^2+by^2-z^2=0$?

Observe: the assumptions in legendre's thm in its original form (resp. in the form due to Cassels) are equivalent to the solvability of $ax^2+by^2+cz^2=0$ in $\mathbb{R}$ and in all $\mathbb{Q}_p$, $p\neq 2$ (resp. to the solvability in all $\mathbb{Q}_p$, including $p=2$). This suggests that one should analyse more closely the solvability over each $\mathbb{Q}_p$ (including $\mathbb{Q}_\infty=\mathbb{R}$). This was done by Hilbert and his reformulation of the QRL in terms of the Hilbert symbol represented an extremely important conceptual advance.

Discrete subgroups are closed

Recall: a subset Y of a topological space X is *discrete* if the topology induced on Y from X is discrete, i.e., if $\forall y \in Y \ \exists$ open $U \subset X$ $U \cap Y = \{y\}$.

Ex: $Y = \{1, \frac{1}{2}, \frac{1}{3}, \dots\}$ is discrete (but not closed) in $X = \mathbb{R}$.

Prop. A discrete subgroup $\Gamma \subset \mathbb{R}^d$ is closed.

Pf. Discreteness implies that $\exists\, U_1 \subset \mathbb{R}^d$ open, $U_1 \cap \Gamma = \{0\}$.

Continuity of $\mathbb{R}^d \times \mathbb{R}^d \longrightarrow \mathbb{R}^d$, $(x, y) \longmapsto x - y$, implies that $\exists\, U_2 \subset \mathbb{R}^d$ open, $0 \in U_2$, $\forall x, y \in U_2 \quad x - y \in U_1$.

If $a \in \mathbb{R}^d$, $a \notin \Gamma$, then $U := (a + U_2) \setminus \underbrace{((a+U_2) \cap \Gamma)}_{\text{contains at most one element } (\neq a)} \subset \mathbb{R}^d$ open, $a \in U$, $U \cap \Gamma = \emptyset$.

Therefore a does not lie in the closure of Γ $\Rightarrow$ Γ is closed.

$[x, y \in (a+U_2) \cap \Gamma \Rightarrow x - y \in U_1 \cap \Gamma = \{0\}]$

Rmk. This argument works for discrete subgroups of an arbitrary *topological group* G (by which we mean a group G equipped with a topology for which the maps $G \times G \longrightarrow G$, $g, h \longmapsto gh$ and $G \longrightarrow G$, $g \longmapsto g^{-1}$ are continuous, and the set $\{e\}$ consisting of the neutral element of G is closed). ($\Rightarrow$ the topology on G is Hausdorff). Example: $G = GL_n(\mathbb{R})$.

Cor. A subgroup $\Gamma \subset \mathbb{R}^d$ is discrete $\iff$ $\forall$ compact $K \subset \mathbb{R}^d$ $\Gamma \cap K$ is finite $\iff$ $\forall$ bounded $X \subset \mathbb{R}^d$ $\Gamma \cap X$ is finite.

Pf. Γ discrete $\Rightarrow$ Γ closed $\Rightarrow$ $\left.\begin{matrix} \Gamma \cap K \text{ compact} \\ \Gamma \cap K \text{ discrete} \end{matrix}\right\} \Rightarrow \Gamma \cap K$ finite. The rest is clear.

Prop. A subgroup $\Gamma \subset V$ in a finite-dimensional $\mathbb{R}$-vector space V is discrete if and only if $\exists$ basis $v_1, \dots, v_d \in V$ (over $\mathbb{R}$) and $0 \le m \le d$ such that

$\Gamma = \mathbb{Z}v_1 \oplus \dots \oplus \mathbb{Z}v_m$ ($\iff$ Γ is a lattice in the subspace $V' = \mathbb{R}v_1 \oplus \dots \oplus \mathbb{R}v_m \subset V$).

Pf. One can assume that Γ contains a basis $\{u_i\}$ of V (replace V by the subspace generated by Γ). Then $L = \mathbb{Z}u_1 \oplus \dots \oplus \mathbb{Z}u_d \subset V$ is a lattice in V and a subgroup of Γ. The set $F = \left\{ \sum_{i=1}^{d} t_i u_i \;\middle|\; 0 \le t_i \le 1 \right\} \subset V$ is compact and $V = \bigcup_{u \in L} (u + F) \Rightarrow \Gamma = \bigcup_{u \in F \cap L} (L + u)$. But $F \cap L$ is finite, by Cor. above

$\Rightarrow$ the index $(\Gamma : L)$ is finite $\Rightarrow$ $\Gamma = \mathbb{Z}v_1 \oplus \dots \oplus \mathbb{Z}v_d$ for some $\{v_i\} \subset V$ (necessarily a basis of V). $\underbrace{\qquad}_{L \simeq \mathbb{Z}^d}$

Exercise: A collection of elements of a discrete subgroup of $\mathbb{R}^d$ is linearly independent over $\mathbb{Z}$ $\iff$ it is linearly independent over $\mathbb{R}$.

Prop 1. If $\Gamma \subset \mathbb{R}$ is a non-zero discrete subgroup, then $\Gamma = \mathbb{Z}\alpha$ $(\alpha > 0)$ is cyclic.

Pf.

By assumption, $\alpha := \inf_{\substack{x \in \Gamma \\ x > 0}} (x) > 0$.

If $\alpha \in \Gamma$, then for each $\beta \in \Gamma$ $\exists n \in \mathbb{Z}$ $n\alpha \le \beta < (n+1)\alpha$

$\Rightarrow 0 \le \underbrace{\beta - n\alpha}_{\in \Gamma} < \alpha \Rightarrow \beta - n\alpha = 0 \Rightarrow \beta \in \mathbb{Z}\alpha$.

If $\alpha \notin \Gamma$, then $\exists x, y \in \Gamma$ $\alpha < x < y < 2\alpha$ (write $\alpha = \lim_{n\to\infty} x_n$, $\Gamma \ni x_n \downarrow$, $x_1 > x_2 > x_3 > \cdots > \alpha$)

$\Rightarrow 0 < y - x < \alpha$ — impossible.

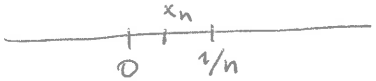
Prop 2. (1) A subgroup $\Gamma \subset \mathbb{R}$ is either discrete or dense.

(2) Discrete subgroups of $\mathbb{R}$ are $\{0\}$ and $\mathbb{Z}\alpha$ $(\alpha > 0)$.

(3) Closed — " — $\{0\}$, $\mathbb{Z}\alpha$ $(\alpha > 0)$ and $\mathbb{R}$.

---

(1)



If Γ is not discrete, $\forall n \in \mathbb{N}_+$ $\exists x_n \in \Gamma$, $0 < x_n < \frac{1}{n}$. Then $\mathbb{Z}x_n \subset \Gamma$ intersects every interval $[a, a+1/n]$ of length $1/n$ $\Rightarrow \bigcup_{n\ge 1} \mathbb{Z}x_n \subset \Gamma$ is dense in $\mathbb{R}$.

(2) See Prop. 1.

(3) = (1)+(2).

Cor. If $\alpha, \beta \in \mathbb{R}$ are linearly independent over $\mathbb{Q}$, then $\mathbb{Z}\alpha + \mathbb{Z}\beta$ is dense in $\mathbb{R}$.

Rmks. (a) One can show that every subgroup $\Gamma \subset \mathbb{R}^n$ $(n \ge 1)$ is of the form $\Gamma = \Gamma_0 \oplus \Gamma_1$, where Γ_0 is dense in an $\mathbb{R}$-vector subspace $V_0 \subset \mathbb{R}^n$ and Γ_1 is discrete in an — " — $V_1 \subset \mathbb{R}^n$ such that $V_0 \oplus V_1 = \mathbb{R}^n$.

(b) This implies that every closed subgroup ($\Gamma \subset \mathbb{R}^n$) decomposes as

$\Gamma = \Gamma_0 \oplus \Gamma_1 \oplus \Gamma_2$, $V_i \subset \mathbb{R}^n$ $\mathbb{R}$-vector subspace,

$\mathbb{R}^n = V_0 \oplus V_1 \oplus V_2$, $\Gamma_0 = V_0$, $\Gamma_2 = \{0\}$, $\Gamma_1 \subset V_1$ lattice in V_1.

In other words, the pair $(\Gamma \subset \mathbb{R}^n)$ is isomorphic to a direct sum of (standard) one-dimensional pairs (isomorphic to $(\mathbb{R} \subset \mathbb{R})$, $(\mathbb{Z} \subset \mathbb{R})$ or $(\{0\} \subset \mathbb{R})$, respectively).

(c) The statement (b) is equivalent to Kronecker's Thm on non-homogeneous simultaneous rational approximations.

Convex bodies, distance functions, norms

V = real vector space of dimension d, $1 \le d < \infty$

Exercise (1) If $K \subset V$ is convex, then its interior $\mathring{K}$ is either empty (in which case K is contained in an affine subspace $W \subset V$ of $\dim < d$), or convex. (2) If K is a non-empty bounded convex open set $K \subset V$, then K = the interior of its closure $\overline{K}$.

Fundamental dictionary (Minkowski):

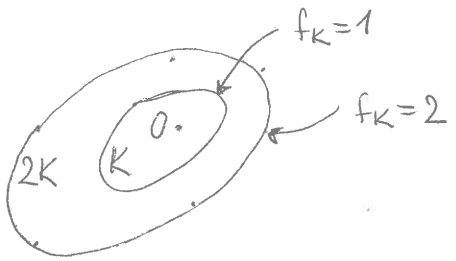
$$\left\{\begin{array}{l}\text{open bounded convex sets } K \subset V \\ \text{containing the origin } 0 \in V\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\text{functions } f: V \longrightarrow \mathbb{R}_{\ge 0} \text{ such that} \\ f(x)=0 \iff x=0 \\ \forall t \ge 0 \ \forall x \in V \quad f(tx)=t f(x) \\ \forall x,y \in V \quad f(x+y) \le f(x)+f(y)\end{array}\right\}$$

$$K = \{x \in V \mid f(x) < 1\} \longleftarrow f$$
$$\overline{K} = \{x \in V \mid f(x) \le 1\}$$
$$\partial K = \{x \in V \mid f(x) = 1\}$$

$$K \longmapsto f_K(x) := \inf\{t > 0 \mid x \in tK\}$$

"the distance function of K"
"the Minkowski functional of K"

Ex:



In general, $(x \in V \smallsetminus \{0\})$ $\quad f_K(x) = t > 0 \iff x \in t(\partial K)$

the boundary of K

Key points: (a) $x \in sK$, $y \in tK$ $(s,t>0)$ $\Rightarrow$ $x+y = (s+t)\left(\frac{s}{s+t}(s^{-1}x) + \frac{t}{s+t}(t^{-1}y)\right) \in (s+t)K$

($s^{-1}x \in K$, $t^{-1}y \in K$, so the bracketed term $\in K$)

$\Rightarrow$ $f_K(x+y) \le f_K(x) + f_K(y)$

(b) f is automatically continuous: if $V = \bigoplus_{i=1}^{d} \mathbb{R}v_i$ and $x = \sum x_i v_i = \sum \pm |x_i| v_i \in V$,

then $|f(x)| \le \left(\sum_{i=1}^{d} |x_i|\right) \max_i \left(f(\pm v_i)\right) \Rightarrow$ f is continuous at 0

$f(x) \le f(x+y) + f(-y) \Rightarrow -f(-y) \le f(x+y) - f(x) \le f(y) \xrightarrow{y \to 0} 0 \Rightarrow$ f continuous.

Special case:

K is symmetric $(x \in K \Rightarrow -x \in K)$ $\iff$ $\forall x \in V \quad f(-x) = -f(x)$

(hence $\forall t \in \mathbb{R}, \forall x \in V \quad f(tx) = |t| f(x)$; $f(x)=0 \iff x=0$; $f(x+y) \le f(x)+f(y)$)

Functions $f: V \longrightarrow \mathbb{R}_{\ge 0}$ like this are called **norms**. One often denotes f_K (for K symmetric) by $\|\cdot\|_K$.

Summary:

$$\left\{ \begin{array}{c} \text{symmetric open bounded} \\ \text{convex } K \subset V \text{ containing } 0 \end{array} \right\} \longleftrightarrow \left\{ \text{norms } \|\cdot\| : V \longrightarrow \mathbb{R}_{\geq 0} \right\}$$

$K = \{x \in V \mid \|x\| < 1\}$ open unit ball

$\overline{K} = \{x \in V \mid \|x\| \leq 1\}$ closed — " —

$\partial K = \{x \in V \mid \|x\| = 1\}$ unit sphere

for $\|\cdot\|$

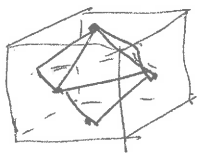
$\|x\|_K = t \iff x \in t \cdot (\partial K)$

$\|x\|_K \leq t \iff x \in t \cdot \overline{K}$

$\|x\|_K < t \iff x \in tK$

Ex: (1) The L^∞-norm on $\mathbb{R}^d$: $\|x\|_\infty = \max |x_i|$, $K = [-1,1]^d$ d-dimensional cube

(2) The L^1-norm: $\|x\|_1 = \sum_1^d |x_i|$ K = d-dimensional "octahedron"



(3) The L^2-norm: $\|x\|_2 = \left(\sum_1^d |x_i|^2\right)^{1/2}$ K = the unit ball

(the standard euclidean norm)

(4) The L^p-norm $(1 \leq p < \infty)$: $\|x\|_p = \left(\sum_1^d |x_i|^p\right)^{1/p}$

Functoriality ($\longleftrightarrow$ change of coordinates): given $V \xrightarrow{\alpha} V$ $\mathbb{R}$-linear bijection

The norm $x \longmapsto \|\alpha(x)\|_K$ corresponds to $\alpha^{-1}(K)$, since

$$\|\alpha(x)\|_K = t \iff \alpha(x) \in t \cdot (\partial K) \iff x \in t \cdot (\partial \alpha^{-1}(K)) \text{ ; so}$$

$$\|\alpha(x)\|_K = \|x\|_{\alpha^{-1}(K)}$$

Approximations of real numbers by rationals

Typical questions: (1) Given $\alpha \in \mathbb{R}$, find $\frac{p}{q} \in \mathbb{Q}$ close to α, but with $|q|$ not too large

(2) Given $\alpha_1, \dots, \alpha_m \in \mathbb{R}$, find $\frac{p_1}{q}, \dots, \frac{p_m}{q} \in \mathbb{Q}$ with the same denominator that are close to the α_i's (and $|q|$ not too large)

(3) Dual problem to (2): given $\alpha_1, \dots, \alpha_n \in \mathbb{R}$, find $q_1, \dots, q_n \in \mathbb{Z}$ with $0 < \max |q_i|$ not too large but $q_1\alpha_1 + \dots + q_n\alpha_n$ close to some integer $p \in \mathbb{Z}$.

(4) A combination of (2) and (3).

One can ask these questions for general real numbers, or for specific classes of numbers (algebraic numbers, naturally occurring constants such as π, e, $\ln(2)$ ...).

Ex (1) If $(1+\sqrt{2})^n = p_n + q_n\sqrt{2}$ $(p_n, q_n \in \mathbb{N}_+)$, then
$(1-\sqrt{2})^n = p_n - q_n\sqrt{2}$ and $(-1)^n = p_n^2 - 2q_n^2$

$$\Rightarrow \left|\sqrt{2} - \frac{p_n}{q_n}\right| = \underbrace{\frac{1}{q_n\left|\sqrt{2} + \frac{p_n}{q_n}\right|}}_{< \frac{1}{\sqrt{2}\,q_n^2}} \quad \left(> \frac{1}{2\sqrt{2}\,q_n^2} \text{ if } n = 2m+1\right)$$

If $p, q \in \mathbb{N}$, $q \neq 0 \Rightarrow |p^2 - 2q^2| \geq 1$.

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

Ex (2) For $p, q \in \mathbb{Z}$, $q \neq 0$, $\frac{1}{|q|^3} \leq \left|\frac{p^3 - 2q^3}{q^3}\right| = \left|\left(\frac{p}{q}\right)^3 - 2\right| = \left|\frac{p}{q} - \sqrt[3]{2}\right| \cdot \underbrace{\left|\left(\frac{p}{q}\right)^2 + \left(\frac{p}{q}\right)\sqrt[3]{2} + \sqrt[3]{4}\right|}_{\leq (\text{const.}) \text{ if } \left|\sqrt[3]{2} - \frac{p}{q}\right| \leq 1}$

$$\Rightarrow \left|\frac{p}{q} - \sqrt[3]{2}\right| \geq \frac{c}{|q|^3}$$

Thm (Liouville). Let $\alpha \in \mathbb{C}$ be an algebraic number of degree $d \geq 2$ (e.g., $\exists\, f(X) = a_0X^d + \dots + a_d \in \mathbb{Z}[X]$ such that $\deg(f) = d$ and $f(\alpha) = 0$, but no such polynomial exists in $\deg < d$). Then: $\forall \varepsilon > 0$ $\exists\, q_0(\varepsilon) > 0$ such that for any $\frac{p}{q} \in \mathbb{Q}$ with $|q| \geq q_0(\varepsilon)$ $\left|\alpha - \frac{p}{q}\right| \geq \left(\frac{1}{|f'(\alpha)| + \varepsilon}\right) \cdot \frac{1}{q^d}$.

Cor. If $\alpha \in \mathbb{R}$ and if $\exists$ sequence of $\frac{p_n}{q_n} \in \mathbb{Q}$ and $d_n \in \mathbb{N}_+$ such that $\lim_{n\to\infty} d_n = +\infty$ and $0 < q_n^{d_n}\left|\alpha - \frac{p_n}{q_n}\right| \leq (\text{const.})$, then α is **not algebraic**.

Ex: $\alpha = \sum_{k=0}^{\infty} (-1)^k\, 2^{-k!}$ $\left(q_n = 2^{n!},\ p_n = q_n \sum_{k=0}^{n} (-1)^k 2^{-k!},\ d_n = n+1\right)$.

Pf of Liouville's Thm. If $\alpha \notin \mathbb{R}$, $|\alpha - \frac{p}{q}| \geq \mathrm{Im}(\alpha) > 0$. Assume $\alpha \in \mathbb{R}$.

Minimality of $d \Rightarrow f'(\alpha) \neq 0$ and irreducibility of f in $\mathbb{Q}[X] \Rightarrow f(\frac{p}{q}) \neq 0$.

$q^d f(\frac{p}{q}) = a_0 p^d + \cdots + a_d q^d \in \mathbb{Z} \setminus \{0\} \Rightarrow |f(\frac{p}{q})| \geq \frac{1}{q^d}$.

Mean value thm: $\frac{1}{q^d} \leq |f(\frac{p}{q})| = |f(\frac{p}{q}) - f(\alpha)| = |(\frac{p}{q} - \alpha) f'(\theta)|$ for some $\theta \in [\frac{p}{q}, \alpha]$.

Given $\varepsilon > 0$, $\exists\, \delta(\varepsilon) > 0$ $\quad |f'(t)| \leq |f'(\alpha)| + \varepsilon$ if $|t - \alpha| \leq \delta(\varepsilon)$.

If $|\frac{p}{q} - \alpha| \leq \delta(\varepsilon) \Rightarrow q^d |\frac{p}{q} - \alpha| \geq \frac{1}{|f'(\theta)|} \geq \frac{1}{|f'(\alpha)| + \varepsilon}$.

If $|\frac{p}{q} - \alpha| > \delta(\varepsilon)$, then $q^d |\frac{p}{q} - \alpha| \geq \frac{1}{|f'(\alpha)| + \varepsilon}$ holds if $q \geq \left(\frac{1}{(|f'(\alpha)| + \varepsilon)\, \delta(\varepsilon)} \right)^{1/d}$.

Rmks: (1) $q_0(\varepsilon)$ can be easily computed in terms of ε and f.

(2) Any improvement of Liouville's Thm involving the exponent of q would prove finiteness of the number of solutions of

$$a_0 p^d + \cdots + a_d q^d = m \qquad (m \in \mathbb{Z} \setminus \{0\} \text{ fixed}; \; p, q \in \mathbb{Z} \text{ variable})$$

"Thue's equation". This can, indeed, be proved if $d \geq 3$:

Thue: $d \geq 3 \Rightarrow \forall \varepsilon > 0 \quad \forall \frac{p}{q} \in \mathbb{Q} \quad |\alpha - \frac{p}{q}| \geq \frac{c(\varepsilon)}{|q|^{d/2 + \varepsilon}}$

Further improvements of the exponents: Siegel ($\sim 2\sqrt{d}$), Gelfond, Dyson ($\sim \sqrt{2d}$), Roth (2; best possible).

Unfortunately, the constant $c(\varepsilon)$ is not effectively computable in terms of $\varepsilon > 0$.

Key principle used above: if $a \in \mathbb{Z} \setminus \{0\}$, then $|a| \geq 1$.

In Liouville's Thm, $a = q^d f(\frac{p}{q})$ is automatically non-zero, since f is irreducible in $\mathbb{Q}[X]$. However, proving the non-vanishing of a suitable analogue of this a in the proofs of Thue, ..., Roth is hard.

Repulsion of good approximations: if $\frac{p}{q} \neq \frac{p'}{q'} \in \mathbb{Q}$ are distinct rational numbers, then, for any $\alpha \in \mathbb{R}$,

$$|\alpha - \frac{p}{q}| + |\alpha - \frac{p'}{q'}| \geq |\frac{p}{q} - \frac{p'}{q'}| = \frac{|pq' - p'q|}{|qq'|} \geq \frac{1}{|qq'|}$$

So: if both $|\alpha - \frac{p}{q}|$ and $|\alpha - \frac{p'}{q'}|$ are small, $|qq'|$ is large.

This is used repeatedly in all the proofs of the thm mentioned above

Effective diophantine approximations

For general $\alpha \in \overline{\mathbb{Q}}$, the constant $c(\varepsilon)$ in the Thue/Siegel/Gelfond/Dyson/Roth thm is not effective. For special $\alpha \in \overline{\mathbb{Q}}$ one can use another method, also going back to Thue, to obtain effective results.

Ex: $\forall \frac{p}{q} \in \mathbb{Q}$, $\left|\frac{p}{q} - \sqrt[3]{2}\right| > \frac{1}{4|q|^{5/2}}$ (Bennett, building upon earlier work of Thue, Siegel, Baker, Chudnovsky)

($\Rightarrow$ explicit bound for the size of solutions of $x^3 - 2y^3 = m \in \mathbb{Z} - \{0\}$ $(x, y \in \mathbb{Z})$)

Idea: $\frac{128}{125} = 1 + \frac{3}{125}$ is close to 1 and $\sqrt[3]{\frac{128}{125}} = \frac{4}{5}\sqrt[3]{2}$.

Hermite–Padé approximations of the series $\sqrt[3]{1+z} = \sum_{k \geq 0} \binom{1/3}{k} z^k$ by quotients of polynomials, when evaluated at $z = 3/125$, give a series of good approximations $\frac{p_n}{q_n}$ to $\frac{4}{5}\sqrt[3]{2}$. One needs to estimate the size of the denominators $|q_n|$ (not so easy) and the size of the error terms $\left|\frac{p_n}{q_n} - \frac{4}{5}\sqrt[3]{2}\right|$ (easier), and then apply a quantitative version of the principle of repulsion of good approximations. Here is a typical statement one may use.

Prop. Assume that $\alpha \in \mathbb{R}$ and that there exists a sequence of approximations $\frac{p_n}{q_n} \in \mathbb{Q}$ of α with the following properties:

$\forall n \geq 1$ $\frac{p_n}{q_n} \neq \frac{p_{n+1}}{q_{n+1}}$, $|q_n| \leq k_0 Q^n$, $|q_n \alpha - p_n| \leq l_0 Q^{-n/\mu}$

(for suitable constants $k_0, l_0, Q, \mu > 0$). Then $\forall \frac{p}{q} \in \mathbb{Q}$ $|q\alpha - p| \geq \frac{c}{|q|^\mu}$

$c = \frac{1}{(2k_0)(2l_0)^\mu Q^2}$.

Rational approximations and irrationality

Notation: rational numbers will be written as $\frac{p}{q}$ $(p,q\in\mathbb{Z},\ q\neq 0)$. It will not be assumed that $\gcd(p,q)=1$.

Basic fact: if $\boxed{x\in\mathbb{Z} \text{ and } x\neq 0, \text{ then } |x|\geq 1.}$

Cor 1. If $\alpha=\frac{p'}{q'}\in\mathbb{Q}$, then we have, for each $\frac{p}{q}\in\mathbb{Q}$, $\frac{p}{q}\neq\alpha$,

$$|q\alpha-p| = \left|\frac{qp'-pq'}{q'}\right| \geq \frac{1}{|q'|}.$$

Cor 2. (Basic criterion of irrationality) Let $\alpha\in\mathbb{R}$. If there exists a sequence $\frac{p_n}{q_n}\in\mathbb{Q}$ $(n\geq 1)$ such that $\frac{p_n}{q_n}\neq\alpha$ and $\lim_{n\to\infty}|q_n\alpha-p_n|=0$, then $\alpha\notin\mathbb{Q}$.

Irrationality of e^{-1}

$$\alpha=e^{-1}=\sum_{k\geq 0}\frac{(-1)^k}{k!}=\sum_{k\leq n}+\sum_{k>n}=\underbrace{\frac{1}{n!}}_{\frac{1}{q_n}}\underbrace{\sum_{k=0}^{n}(-1)^k\frac{n!}{k!}}_{p_n\in\mathbb{Z}}+(-1)^{n+1}\left(\overbrace{\frac{1}{(n+1)!}}^{>0}-\underbrace{\frac{1}{(n+2)!}}_{<0}+\overbrace{\frac{1}{(n+3)!}}^{>0}-\cdots\right)$$

$$\Rightarrow \exists\ \frac{p_n}{q_n}\in\mathbb{Q} \text{ with } q_n=n! \text{ and } 0<|q_n\alpha-p_n|<\frac{q_n}{(n+1)!}=\frac{1}{n+1}\Rightarrow e^{-1}\notin\mathbb{Q}.$$

Exercise. Apply the same argument to $\alpha=e$ and to $\alpha=ae+be^{-1}$ $(a,b\in\mathbb{Q}\setminus\{0\})$.

What about $\alpha=e^{-m}=\sum_{k\geq 0}\frac{(-1)^k m^k}{k!}$? $(m\in\mathbb{N}_+,\ m>2)$ (the case $m=2$ is covered by)

$$\alpha=\sum_{k\leq n}+\sum_{k>n}=\underbrace{\frac{1}{n!}}_{\frac{1}{q_n}}\underbrace{\sum_{k=0}^{n}\frac{(-1)^k m^k n!}{k!}}_{p_n}+(-1)^{n+1}m^{n+1}\underbrace{\left(\frac{1}{(n+1)!}-\frac{m}{(n+2)!}+\cdots\right)}_{\text{lies in } \left(0,\frac{1}{(n+1)!}\right)}$$

$(n>m)$

$$\Rightarrow \text{get } \frac{p_n}{q_n}\in\mathbb{Q} \text{ with } q_n=n! \text{ and } 0<|q_n e^{-m}-p_n|<\frac{m^{n+1}}{n+1}, \text{ but } \lim_{n\to\infty}\frac{m^{n+1}}{n+1}=+\infty$$

We need better rational approximations to e^{-m} in order to be able to apply Cor 2.

Key idea (Hermite): do not approximate $e^z = \sum_{k\geq 0} \frac{z^k}{k!}$ by polynomials $\sum_{k=0}^{n} \frac{z^k}{k!}$, but by suitable rational functions (quotients of polynomials).

General problem of **Hermite – Padé approximations:**

given a power series $f(z) = \sum_{k\geq 0} c_k z^k$ and integers $m, n \geq 0$,

find polynomials $A(z), B(z) \in \mathbb{C}[z]$ such that

$\deg A(z) \leq m$

$\deg B(z) \leq n$

$\operatorname{ord}_{z=0}\big(A(z) - B(z) f(z)\big) \geq m+n+1$

(i.e., $A(z) - B(z) f(z) = \sum_{k \geq m+n+1} d_k z^k$)

Key always exist:

$\Updownarrow$

$(A, B) \in \operatorname{Ker}(\phi)$, but $\dim \operatorname{Ker}(\phi) \geq \underbrace{(m+n+2) - (m+n+1)}_{1}$

$$\underbrace{\mathbb{C}[z]_{\deg \leq m} \oplus \mathbb{C}[z]_{\deg \leq n}}_{\dim = m+n+2} \xrightarrow{\ \phi\ } \underbrace{\mathbb{C}[[z]]/(z^{m+n+1})}_{\dim = m+n+1}$$

$$\downarrow \qquad\qquad \downarrow$$

$$(A, B) \longmapsto A - Bf \pmod{z^{m+n+1}}$$

---

the most satisfactory case: $\dim \operatorname{Ker}(\phi) = 1$ ($\Leftrightarrow$ (A, B) is unique up to a constant multiple)

"perfect approximation"

Hermite – Padé approximations to e^z

Use $(e^z)' = e^z$ and integration by parts:

① $$\int F^{(m)}(x) e^{zx}\, dx = F^{(m-1)}(x) e^{zx} - z \int F^{(m-1)}(x) e^{zx} dx + \cdots =$$

$$= \left(\sum_{k=0}^{m-1} (-1)^k F^{(m-k-1)}(x) z^k \right) e^{zx} + (-1)^m z^m \int F(x) e^{zx} dx$$

Cor: if $x^m (1-x)^m$ divides $F(x)$, then $\forall j < m \quad F^{(j)}(0) = F^{(j)}(1) = 0$

$$\Rightarrow \int_0^1 F^{(m)}(x) e^{zx} dx = (-1)^m z^m \int_0^1 F(x) e^{zx} dx \in z^m \mathbb{C}[[z]]$$

② If $f \in \mathbb{C}[x]$, $\deg(f) \leq n$, then

$$\int f(x) e^{zx} dx = f(x) \frac{e^{zx}}{z} - \frac{1}{z} \int f'(x) e^{zx} dx = \cdots = \left(\sum_{j=0}^{n} (-1)^j f^{(j)}(x) z^{-j-1} \right) e^{zx}$$

$$\Rightarrow \quad z^{n+1} \int f(x) e^{zx} dx = \left(\sum_{j=0}^{n} (-1)^j f^{(j)}(x) z^{n-j} \right) e^{zx}$$

③ Combine ① and ②: if $m \le n$, $F \in \mathbb{C}[x]$, $\deg(F) \le m+n$, $x^m(1-x)^m \mid F(x)$,

then

$$\underbrace{z^{n+1}\int_0^1 \underbrace{F^{(m)}(x)}_{\deg \le n} e^{zx}\,dx}_{\in z^{m+n+1}\mathbb{C}[[z]]} \overset{②}{=} \underbrace{\left(\sum_{j=0}^{n}(-1)^j F^{(m+j)}(1) z^{n-j}\right)}_{B(z)} e^z - \underbrace{\left(\sum_{j=0}^{n}(-1)^j F^{(m+j)}(0) z^{n-j}\right)}_{A(z)}$$

$A, B \in \mathbb{C}[z]_{\deg \le n}$

---

④ Optimal choice of $F(x)$ of $\deg(F) = m+n$ $(m \le n)$

(a) $F(x) = (\text{const})\, x^m(1-x)^n$: $\deg B(z) \le m$, $\deg A(z) \le n$

(b) $F(x) = (\text{const})\, x^n(1-x)^m$: $\deg B(z) \le n$, $\deg A(z) \le m$

In either case, $\operatorname{ord}_{z=0}\left(B(z)e^z - A(z)\right) \ge m+n+1$.

The diagonal approximation $(m=n)$

Take $m=n$ and $F(x) = \frac{1}{n!}x^n(1-x)^n$. We obtain

$B_n(z), A_n(z) \in \mathbb{Z}[x]$ (since $F^{(n)}(x) \in \mathbb{Z}[x]$)

with $\deg(A_n) = \deg(B_n) = n$ (since $F^{(n)}(0) \neq 0 \neq F^{(n)}(1)$) and

$$B_n(z)e^z - A_n(z) = \underbrace{(-1)^n \frac{z^{2n+1}}{n!}\int_0^1 x^n(1-x)^n e^{zx}\,dx}_{R_n(z)}$$

Note (a) $F^{(n)}(x)$ is closely related to the Legendre polynomial

$$P_n(x) = \frac{1}{2^n n!}\left((x^2-1)^n\right)^{(n)}$$

(b) letting $x \longleftrightarrow 1-x$, we obtain $R_n(z) = -e^z R_n(-z) \Rightarrow A_n(-z) = B_n(z)$

(c) $\forall z \in \mathbb{C}$ $\quad |R_n(z)| \le \frac{|z|^{2n+1}}{n!} e^{\operatorname{Re}(z)}$

(d) If $z \in \mathbb{R}_{>0}$, then $(-1)^n R_n(z) > 0$

Irrationality of e^z for $z \in \mathbb{Q} \setminus \{0\}$

Assume that $a, b \in \mathbb{N}_+$. In the identity

$$B_n\left(\tfrac{a}{b}\right) e^{a/b} - A_n\left(\tfrac{a}{b}\right) = R_n\left(\tfrac{a}{b}\right)$$

$A_n\left(\frac{a}{b}\right),\ B_n\left(\frac{a}{b}\right) \in b^{-n}\mathbb{Z}$ and $0 < \left|R_n\left(\frac{a}{b}\right)\right| \le \frac{(a/b)^{2n+1}}{n!} e^{a/b}$

let $p_n := b^n A_n\left(\frac{a}{b}\right),\ q_n := b^n B_n\left(\frac{a}{b}\right) \in \mathbb{Z}$. Then

$$0 < |q_n e^{a/b} - p_n| = b^n \left|R_n\left(\tfrac{a}{b}\right)\right| \le \underbrace{\frac{a^{2n+1} b^{-n-1}}{n!}}_{\to 0 \text{ as } n \to +\infty} e^{a/b}$$

$\Rightarrow e^{a/b} \notin \mathbb{Q}$ ($\Rightarrow e^{-a/b} = 1/e^{a/b} \notin \mathbb{Q}$).

Irrationality of π^2

Taking $z = \pm i\lambda$ ($\lambda \in \mathbb{R}$), we obtain

$$\underbrace{B_n(i\lambda)}_{A_n(-i\lambda)} e^{i\lambda} - A_n(i\lambda) = \frac{i\lambda^{2n+1}}{n!} \int_0^1 x^n (1-x)^n e^{i\lambda x}\, dx$$

$$\underbrace{B_n(-i\lambda)}_{A_n(i\lambda)} e^{-i\lambda} - \underbrace{A_n(-i\lambda)}_{B_n(i\lambda)} = \frac{-i\lambda^{2n+1}}{n!} \int_0^1 x^n (1-x)^n e^{-i\lambda x}\, dx$$

$$\Rightarrow \frac{\lambda^{2n+1}}{n!} \int_0^1 x^n (1-x)^n \sin(\lambda x)\, dx = -\frac{1}{2}\left(A_n(i\lambda)(e^{-i\lambda} - 1) + A_n(-i\lambda)(e^{i\lambda} - 1)\right)$$

$\lambda = \pi$: $\quad \frac{\pi^{2n+1}}{n!} \int_0^1 x^n (1-x)^n \sin(\pi x)\, dx = A_n(\pi i) + A_n(-\pi i)$

But $A_n(z) + A_n(-z) \in \mathbb{Z}[z^2]$ is a polynomial in z^2 of deg $\le \left[\frac{n}{2}\right]$ (with coefficients in $\mathbb{Z}$)

and $\underbrace{0 < \int_0^1 x^n (1-x)^n \sin(\pi x) < 1}$.

If $\pi^2 = \frac{p}{q} \in \mathbb{Q}$, then $A_n(\pi i) + A_n(-\pi i) \in q^{-\left[\frac{n}{2}\right]}\mathbb{Z}$

and at the same time $0 < (\text{---} \text{ " } \text{---}) < \frac{\pi^{2n+1}}{n!}$

$\Rightarrow \forall n \ge 1 \quad 1 \le \underbrace{\frac{q^{\left[\frac{n}{2}\right]} \pi^{2n+1}}{n!}}_{\to 0 \text{ as } n \to \infty}$ $\Rightarrow$ contradiction $\Rightarrow \boxed{\pi^2 \notin \mathbb{Q}}$.

Rmks. (1) In order to prove transcendence of e ($\Leftrightarrow$ the fact that $1, e, \dots, e^m$ are linearly independent over $\mathbb{Q}$) by this method one needs to construct simultaneous Hermite–Padé approximations of $e^z, e^{2z}, \dots, e^{mz}$; either of

Type I : $\operatorname{ord}_{z=0}\left(A(z) + \sum_{j=1}^{m} B_j(z)\, e^{jz}\right) \geq \deg(A) + \sum_{j=1}^{m} \deg(B_j) + m$

or of Type II : $\forall j=1,\dots,m \quad \operatorname{ord}_{z=0}\left(A_j(z) - B(z)\, e^{jz}\right) \geq$ (sth.)

---

the difficult point is then to show that an appropriate analogue of $R_n(1)$ does not vanish.

---

(2) Integrals such as $\int \frac{F^{(n)}(x)\,dx}{1-zx}$ resp. $\int \frac{F^{(n)}(x)\,dx}{(1-zx)^{\alpha+1}}$ lead to Padé approximatics of $\ln(1-z)$ resp. $(1-z)^{-\alpha}$ and non-trivial (quantitative) irrationality results when $z \in \mathbb{Q}$ close to 1 (and $\alpha = 1/n$).

Exercise. The polynomials $\underbrace{A_{m,n}(z)}_{\deg \leq n}$, $\underbrace{B_{m,n}(z)}_{\deg \leq m}$ satisfying

$\operatorname{ord}_{z=0}\left(B_{m,n}(z)e^z - A_{m,n}(z)\right) \geq m+n+1$ constructed above

are given explicitly as follows.

(1) If $m \leq n$: $A_{m,n}(z) = \sum_{j=0}^{n} \underbrace{\left[(-1)^j \binom{m+j}{j} \left(\frac{d}{dx}\right)^{m+j} \frac{x^m}{m!}(1-x)^n\right]_{x=0}}_{\frac{n!}{(n-j)!}} z^{n-j} = z^n + \dots + \frac{(m+n)!}{m!}$

$B_{m,n}(z) = \sum_{j=n-m}^{n} \left[(-1)^j \left(\frac{d}{dx}\right)^{m+j} \frac{x^m}{m!}(1-x)^n\right]_{x=1} z^{n-j} \qquad (j = n-m+k)$

$= \sum_{k=0}^{m} (-1)^{m-k} \underbrace{\left[\left(\frac{d}{dx}\right)^{n+k} \frac{x^m}{m!}(x-1)^n\right]_{x=1}}_{\binom{n+k}{k}\frac{n!}{(m-k)!}} z^{m-k} = (-1)^m \frac{n!}{m!} z^m + \dots + \frac{(m+n)!}{m!}$

(2) If $m \geq n$: $A_{m,n}(z) = B_{n,m}(-z)$, $\quad B_{m,n}(z) = A_{n,m}(-z)$

(3) If $m = n$: $\underbrace{A_{n,n}(z)}_{A_n(z)} = \underbrace{B_{n,n}(-z)}_{B_n(-z)} = z^n + \dots + \frac{(2n)!}{n!}$

Irrationality measure of $e^{\frac{a}{b}}$ $(\frac{a}{b} \in \mathbb{Q} \setminus \{0\})$

We are going to prove a quantitative version of irrationality of $e^{a/b}$ $(a, b \in \mathbb{N}_+)$, using the following version of the principle of repulsion of good approximations.

Prop 1. Let $\alpha \in \mathbb{R}$. Assume that there exist constants $c_1, c_2 > 0$ and a sequence $\frac{p_n}{q_n} \in \mathbb{Q}$ of rational numbers satisfying

$$\forall n \in \mathbb{N}_+ \quad \frac{p_n}{q_n} \neq \frac{p_{n+1}}{q_{n+1}}, \quad |q_n \alpha - p_n| < \frac{c_1^n}{n!}, \quad |q_n| \leq c_2^n \cdot n!.$$

Then $\alpha \notin \mathbb{Q}$ and for each $\varepsilon > 0$ there exists $q_0(\varepsilon) > 0$ such that

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{1}{|q|^{2+\varepsilon}} \quad \text{for all } p, q \in \mathbb{Z} \text{ with } |q| \geq q_0(\varepsilon).$$

Pf. For each $n \in \mathbb{N}_+$ at least one of $|q_n \alpha - p_n|$, $|q_{n+1}\alpha - p_n|$ is $\neq 0$.

As $\lim_{n\to\infty} c_1^n/n! = 0$, irrationality of α follows.

Fix $\varepsilon > 0$ and let $p, q \in \mathbb{Z}$, with $|q|$ large. Let $n \in \mathbb{N}_+$ be the minimal value for which $(\forall k \geq n)$ $\frac{k!}{2c_1^k} \geq |q|$. We have $|q| > \frac{2(n-1)!}{c_1^{n-1}}$ and

$$\underbrace{\left|\alpha - \frac{p}{q}\right|}_{} + \underbrace{\left|\alpha - \frac{p_m}{q_m}\right|}_{< \frac{1}{|q_m|} \cdot \frac{c_1^m}{m!}} \geq \underbrace{\left|\frac{p}{q} - \frac{p_m}{q_m}\right|}_{\neq 0}$$

for some $m \in \{n, n+1\}$.

So for some $m \in \{n, n+1\}$ we have

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{1}{|qq_m|} - \frac{1}{|q_m|}\frac{c_1^m}{m!} = \frac{1}{|q_m||q|}\underbrace{\left(1 - \frac{|q|c_1^m}{m!}\right)}_{\geq \frac{1}{2}} = \frac{1}{2|q||q_m|}.$$

But $|q_n| \leq c_2^n \cdot n! \leq \underbrace{\left(\frac{2((n-1)!)}{c_1^{n-1}}\right)^{1+\varepsilon}}_{\left(< \frac{|q|^{1+\varepsilon}}{2} \text{ as long as } n \geq n_0(\varepsilon)\right)}$

(and similarly for $|q_{n+1}| \leq c_2^{n+1} \cdot (n+1)!$) $\Rightarrow$ result.

In order to verify the assumption $\frac{p_n}{q_n} \neq \frac{p_{n+1}}{q_{n+1}}$, we use the following useful fact about diagonal Padé approximations (those of bidegree (n, n)).

Prop 2. Let $f(z) = \sum_{n=0}^{\infty} c_n z^n \in \mathbb{C}[[z]]$ be a power series with $c_0 = f(0) \neq 0$.

Assume that $n \in \mathbb{N}$ and that we are given, for $m \in \{n, n+1\}$, polynomials $A_m(z), B_m(z) \in \mathbb{C}[z]$ such that $\deg(A_m), \deg(B_m) \leq m$ and

$$B_m(z) f(z) - A_m(z) = z^{2n+1} S_m(z) \quad \text{for some } S_m(z) \in \mathbb{C}[[z]].$$

Then $\exists\ u_n \in \mathbb{C}$ such that

$$\Delta_n(z) := \begin{vmatrix} A_n(z) & B_n(z) \\ A_{n+1}(z) & B_{n+1}(z) \end{vmatrix} = u_n z^{2n+1}, \qquad \begin{aligned} u_n f(0) &= -S_n(0) A_{n+1}(0) \\ u_n &= -S_n(0) B_{n+1}(0). \end{aligned}$$

Cor. If $S_n(0) \neq 0$ and not both $A_{n+1}(0), B_{n+1}(0)$ are zero, then

$$\begin{vmatrix} A_n(z) & B_n(z) \\ A_{n+1}(z) & B_{n+1}(z) \end{vmatrix} = u_n z^{2n+1} \quad \text{with } u_n \in \mathbb{C} \setminus \{0\}.$$

Pf of Prop: $\Delta_n(z) = z^{2n+1} \begin{vmatrix} B_n(z) & S_n(z) \\ B_{n+1}(z) & z^2 S_{n+1}(z) \end{vmatrix}$ ($\deg \leq 2n+1$)

$$\Rightarrow \underbrace{\begin{vmatrix} B_n(z) & S_n(z) \\ B_{n+1}(z) & z^2 S_{n+1}(z) \end{vmatrix}}_{\text{const. } u_n \in \mathbb{C}} \overset{z=0}{\Longrightarrow} u_n = -S_n(0) B_{n+1}(0)$$

Similarly, $\Delta_n(z) f(z) = z^{2n+1} \begin{vmatrix} A_n(z) & S_n(z) \\ A_{n+1}(z) & z^2 S_{n+1}(z) \end{vmatrix} \overset{z=0}{\Longrightarrow} u_n f(0) = -S_n(0) A_{n+1}(0)$.

Thm. Let $a, b \in \mathbb{N}_+$. Then, for each $\varepsilon > 0$ there exists $q_0(\varepsilon) > 0$ such that

$$\forall p, q \in \mathbb{Z} \text{ with } |q| \geq q_0(\varepsilon) \qquad \left| e^{a/b} - \frac{p}{q} \right| \geq \frac{1}{|q|^{2+\varepsilon}}.$$

Pf. Recall the Padé approximants $B_n(z), A_n(z) \in \mathbb{Z}[z]$ such that

$$B_n(z) e^z - A_n(z) = z^{2n+1} S_n(z), \qquad S_n(z) = \frac{(-1)^n}{n!} \int_0^1 x^n (1-x)^n e^{zx} dx \in \mathbb{C}[[z]].$$

As before, let $p_n = b^n A_n\left(\frac{a}{b}\right) \in \mathbb{Z}$, $q_n \in b^n B_n\left(\frac{a}{b}\right) \in \mathbb{Z}$.

In this case $(-1)^n S_n(0) = \frac{1}{n!} \int_0^1 x^n (1-x)^n dx > 0$ and

$A_n(0) = B_n(0) = \frac{(2n)!}{n!} \neq 0$ $(\forall n \in \mathbb{N}) \overset{\text{Cor.}}{\Longrightarrow} |p_n q_{n+1} - p_{n+1} q_n| \neq 0$

We know that $|q_n e^{a/b} - p_n| \leq \frac{a^{2n+1} b^{-n-1}}{n!} e^{a/b}$.

As $B_n(z) = \sum_{k=0}^{n} (-1)^{n-k} \underbrace{\frac{(n+k)!}{k!(n-k)!}}_{\leq (1+1+1)^{n+k} \cdot k!} z^{n-k}$, $|q_n| \leq b^n \cdot (n+1) \cdot 3^{2n} \cdot n! \cdot (e^{a/b})^n$.

We can, therefore, apply Prop. 1 to conclude.

Comparison to Lambert's proof of irrationality of π

The quantities $$I_n := \frac{1}{2}\cdot\frac{1}{n!}\int_0^{\pi} x^n(\pi-x)^n \sin(x)\,dx = \frac{\pi^{2n+1}}{2n!}\int_0^1 x^n(1-x)^n\sin(\pi x)\,dx$$
appearing in the above proof of $\pi^2\notin\mathbb{Q}$ also make appearance in Lambert's classical proof of the same assertion (in 1773).

Lambert used the continued fraction expansion

$$\operatorname{ctg}\left(\frac{1}{x}\right) = x - \cfrac{1}{3x - \cfrac{1}{5x - \cfrac{1}{7x - \cdots}}}\,, \quad \text{valid for each } x\in\mathbb{R}-\{0\}$$

in the sense that the sequence of approximants

$$(*)\qquad x\,,\quad x-\frac{1}{3x}\,,\quad x-\cfrac{1}{3x-\cfrac{1}{5x}}\,,\ \ldots \qquad \text{converges to } \operatorname{ctg}\left(\frac{1}{x}\right).$$

Infact, an analysis of the approximants to $\frac{1}{x}\operatorname{ctg}\left(\frac{1}{x}\right) = 1 - \cfrac{1}{3x^2 - \cfrac{1}{5 - \cfrac{1}{7x^2 - \cdots}}}$ and of their rate of convergence shows that

$\frac{1}{x}\operatorname{ctg}\left(\frac{1}{x}\right)\notin\mathbb{Q}$ if $x^2=\frac{a}{b}\in\mathbb{Q}-\{0\}$. For $x=\frac{2}{\pi}$, $\operatorname{ctg}\left(\frac{1}{x}\right)=0\Rightarrow\pi^2\notin\mathbb{Q}$.

In concrete terms, the approximants $(*)$ for $x=\frac{2}{\pi}$ are equal to

$$\frac{2}{\pi}-\frac{1}{\frac{6}{\pi}} = \frac{12-\pi^2}{6\pi}\,,\quad \frac{2}{\pi}-\cfrac{1}{\frac{6}{\pi}-\cfrac{1}{\frac{10}{\pi}}} = \frac{120-12\pi^2}{60\pi-\pi^3}\,,$$

$$\frac{2}{\pi}-\cfrac{1}{\frac{6}{\pi}-\cfrac{1}{\frac{10}{\pi}-\cfrac{1}{\frac{14}{\pi}}}} = \frac{1680-180\pi^2+\pi^4}{840\pi-20\pi^3}\,,$$

$$\frac{2}{\pi}-\cfrac{1}{\frac{6}{\pi}-\cfrac{1}{\frac{10}{\pi}-\cfrac{1}{\frac{14}{\pi}-\cfrac{1}{\frac{18}{\pi}}}}} = \frac{30240-3360\pi^2+30\pi^4}{15120\pi-420\pi^3+\pi^5}\,,$$

while the integrals I_n are given by

$$I_2 = 12-\pi^2\,,\quad I_3 = 120-12\pi^2\,,\quad I_4 = 1680-180\pi^2+\pi^4\,,$$
$$I_5 = 30240-3360\pi^2+30\pi^4\,.$$

What an amazing coincidence!

Is there a scientific explanation? Yes. the short answer is that the even and odd parts of the polynomials $A_n(z)$ become Padé approximants of $\frac{\operatorname{tgh}(z/2)}{z/2}$, and there is a general result relating Padé approximants to suitable continued fractions.

The continued fraction $\alpha+\cfrac{z}{\alpha+1+\cfrac{z}{\alpha+2+\cfrac{z}{\ddots}}}$

---

the Hypergeometric differential equation: $F={}_pF_q(\underline{a},\underline{b};z)=\sum_{n\geq 0}\frac{(a_1)_n\cdots(a_p)_n}{(b_1)_n\cdots(b_q)_n}\frac{z^n}{n!}$

$(a)_n=a(a+1)\cdots(a+n-1)$, $D=\frac{d}{dz}$

$$\prod_{i=1}^{p}(zD+a_i)F=\sum_{n\geq 0}\frac{(a_1)_{n+1}\cdots(a_p)_{n+1}}{(b_1)_n\cdots(b_q)_n}\frac{z^n}{n!}=\sum_{n\geq 1}\frac{(a_1)_n\cdots(a_p)_n}{(b_1)_{n-1}\cdots(b_q)_{n-1}}\frac{z^{n-1}}{(n-1)!}=D\prod_{j=1}^{q}(zD+b_j-1)F$$

$$\Rightarrow\left(\prod_{i=1}^{p}(zD+a_i)-D\prod_{j=1}^{q}(zD+b_j-1)\right){}_pF_q(\underline{a},\underline{b};z)=0.$$

Special case: $f_\alpha(z):={}_0F_1(\alpha;z)=\sum_{n\geq 0}\frac{z^n}{(\alpha)_n\,n!}$ $\quad(p=0,\ q=1,\ b_1=\alpha)$

$$\underbrace{\left(D(zD+\alpha-1)-1\right)}_{zD^2+\alpha D-1}f_\alpha=0\,,\qquad Df_\alpha=\sum_{n\geq 1}\frac{z^{n-1}}{(\alpha)_n(n-1)!}=\sum_{n\geq 0}\frac{z^n}{(\alpha)_{n+1}\,n!}=\alpha^{-1}f_{\alpha+1}$$

So $y=f_\alpha$ is a solution of $zy''+\alpha y'=y$

$\Downarrow$

$y^{(n)}=(\alpha)_n^{-1}f_{\alpha+n}$ is a solution of $z(y^{(n)})''+(\alpha+n)(y^{(n)})'=y^{(n)}$

$$\Rightarrow\ \frac{y}{y'}=\alpha+\cfrac{z}{\frac{y'}{y''}}=\alpha+\cfrac{z}{\alpha+1+\cfrac{z}{\frac{y''}{y^{(3)}}}}=\alpha+\cfrac{z}{\alpha+1+\cfrac{z}{\alpha+2+\cfrac{z}{\ddots}}}$$

---

for $\alpha=\frac{1}{2}$: $\left(\frac{1}{2}\right)_n=\frac{1\cdot 2\cdots(2n-1)}{2^n\cdot}=\frac{(2n)!}{2^{2n}(n!)}$

$$f_{\frac{1}{2}}(z)=\sum_{n\geq 0}\frac{(2\sqrt{z})^{2n}}{(2n)!}=\operatorname{ch}(2\sqrt{z})\,,\quad f'_{\frac{1}{2}}(z)=\frac{1}{\sqrt{z}}\operatorname{sh}(2\sqrt{z})$$

$$\Rightarrow\ \frac{\sqrt{z}}{\operatorname{th}(2\sqrt{z})}=\frac{1}{2}+\cfrac{z}{\frac{3}{2}+\cfrac{z}{\frac{5}{2}+\cdots}}$$

$z:=\frac{x}{4}$:

$$\frac{\sqrt{x}}{\operatorname{th}(\sqrt{x})}=1+\cfrac{x}{3+\cfrac{x}{5+\cfrac{x}{7+\cdots}}}\qquad\Rightarrow\ \frac{\sqrt{x}}{\operatorname{tg}(\sqrt{x})}=1-\cfrac{x}{3-\cfrac{x}{5-\cfrac{x}{7-\cdots}}}$$

Irrationality of π^2 revisited and generalised

A more conceptual method for proving $\pi \notin \mathbb{Q}$: show that $e^{iz} \notin \mathbb{Q}$ if $z \in \mathbb{Q} \setminus \{0\}$ (note: $e^{\pi i} = -1$). More precisely, one should decompose e^{iz} into its real and imaginary parts $\cos(z)$ and $\sin(z)$ (equivalently, decompose e^z into its even and odd parts $\mathrm{ch}(z) = \frac{e^z + e^{-z}}{2}$ and $\mathrm{sh}(z) = \frac{e^z - e^{-z}}{2}$). In order to do that, let us write the Padé approximation ($\deg A_n = \deg B_n = n$)

$$B_n(z)e^z - A_n(z) = R_n(z) = \frac{(-1)^n}{n!} z^{2n+1} \int_0^1 x^n (1-x)^n e^{zx}\, dx$$

in a more symmetric form, using the fact that $B_n(z) = A_n(-z)$:

$$A_n(-z)e^{z/2} - A_n(z)e^{-z/2} = e^{-z/2} R_n(z) = \frac{(-1)^n}{n!} z^{2n+1} \underbrace{\int_0^1 x^n (1-x)^n e^{z(x-\frac{1}{2})}\, dx}_{\text{even function of } z} =$$

$$= \frac{(-1)^n}{n!} z^{2n+1} \int_0^1 x^n (1-x)^n \,\mathrm{ch}\left(z\left(x-\tfrac{1}{2}\right)\right) dx$$

Write $\boxed{\begin{aligned} A_n(z) - A_n(-z) &= 2z\, C_n(z^2), \\ A_n(z) + A_n(-z) &= 2 D_n(z^2) \end{aligned}}$ $\quad C_n(t), D_n(t) \in \mathbb{Z}[t]$ $\quad (t = z^2)$

$\deg_t C_n(t) \le \left[\frac{n-1}{2}\right]$, $\deg_t D_n(t) \le \left[\frac{n}{2}\right]$

Then

$$\frac{1}{2} e^{-z/2} R_n(z) = \frac{D_n(z^2) - z C_n(z^2)}{2} e^{z/2} - \frac{D_n(z^2) + z C_n(z^2)}{2} e^{-z/2} = D_n(z^2)\,\mathrm{sh}\left(\tfrac{z}{2}\right) - z\, C_n(z^2)\,\mathrm{ch}\left(\tfrac{z}{2}\right)$$

$$\boxed{D_n(z^2)\,\frac{\mathrm{th}\left(\frac{z}{2}\right)}{z} - C_n(z^2) = \frac{e^{-z/2}}{2\,\mathrm{ch}\left(\frac{z}{2}\right)} \frac{R_n(z)}{z} = S_n(z^2)} \qquad \left(\text{if } z \notin (2\mathbb{Z}+1)\pi i \text{, i.e. } \mathrm{ch}\left(\tfrac{z}{2}\right) \neq 0\right)$$

$$\frac{S_n(z^2)}{(z^2)^n} = \frac{(-1)^n}{2\,n!} \cdot \frac{1}{\mathrm{ch}(z)} \int_0^1 x^n (1-x)^n \,\mathrm{ch}\left(z\left(x-\tfrac{1}{2}\right)\right) dx$$

In particular, $(C_n(t),\ D_n(t))$ is a Padé approximation of $\dfrac{\mathrm{th}\left(\frac{\sqrt{t}}{2}\right)}{\sqrt{t}}$ of bidegree $\left[\frac{n-1}{2}\right], \left[\frac{n}{2}\right]$

(since $\deg(C_n) + \deg(D_n) \le \left[\frac{n-1}{2}\right] + \left[\frac{n}{2}\right] = n-1 < n = \mathrm{ord}_{t=0} S_n(t)$).

Note: all coefficients of A_n (in degrees $0, 1, \dots, n$) are non-zero $\Rightarrow$ the same holds for C_n and D_n, and $\deg(C_n) = \left[\frac{n-1}{2}\right]$, $\deg(D_n) = \left[\frac{n}{2}\right]$.

Further properties: (a) if $z \in \mathbb{R}$ or if $-\pi \le z/i \le \pi$, then

$$\int_0^1 x^n (1-x)^n \,\mathrm{ch}\left(z\left(x-\tfrac{1}{2}\right)\right) dx > 0$$

(b) $\forall z \in \mathbb{C}$ $\quad |R_n(z)| \le \dfrac{|z|^{2n+1}}{n!}\, e^{|\mathrm{Re}(z)|}$

(c) $\Delta_n(t) = \begin{vmatrix} C_n(t) & D_n(t) \\ C_{n+1}(t) & D_{n+1}(t) \end{vmatrix} \in \mathbb{Z}[t]$ satisfies $\left.\begin{array}{l} \deg_t(\Delta_n) \le n \\ \operatorname{ord}_{t=0}(\Delta_n) \ge n \end{array}\right\} \Rightarrow \Delta_n(t) = c_n t^n$

for some $c_n \in \mathbb{Z}$. However,

$$\Delta_n(t) = \begin{vmatrix} C_n(t) - \frac{\operatorname{th}(\frac{\sqrt{t}}{2})}{\sqrt{t}} D_n(t) & D_n(t) \\ C_{n+1}(t) - \frac{\operatorname{th}(\frac{\sqrt{t}}{2})}{\sqrt{t}} D_{n+1}(t) & D_{n+1}(t) \end{vmatrix} = t^n \underbrace{\begin{vmatrix} S_n(t)/t^n & D_n(t) \\ S_{n+1}(t)/t^n & D_{n+1}(t) \end{vmatrix}}_{c_n}$$

Taking $t=0 \Rightarrow c_n = D_{n+1}(0) \left(\frac{S_n(t)}{t^n}\right)(0) \neq 0$.

Prop. If $z \in \mathbb{C} \setminus \{0\}$, $z \notin (2\mathbb{Z}+1)\pi i$ and $z^2 \in \mathbb{Q}$, then $\alpha := \frac{\operatorname{th}(\frac{z}{2})}{z} \notin \mathbb{Q}$.

Pf. Write $z^2 = \frac{a}{b}$, $a \in \mathbb{Z} \setminus \{0\}$, $b \in \mathbb{N}_+$. Then

$$\underbrace{D_n\left(\tfrac{a}{b}\right)}_{\in b^{-[n/2]}\mathbb{Z}} \frac{\operatorname{th}(\frac{z}{2})}{z} - \underbrace{C_n\left(\tfrac{a}{b}\right)}_{\in b^{-[n/2]}\mathbb{Z}} = S_n\left(\tfrac{a}{b}\right),$$

$$p_n := b^{[n/2]} C_n\left(\tfrac{a}{b}\right) \in \mathbb{Z}$$

$$\left|S_n\left(\tfrac{a}{b}\right)\right| \le \left|\frac{e^{|z|/2}}{\operatorname{ch}(z)}\right| \cdot \frac{|z|^{2n+1}}{n!}, \text{ so } q_n := b^{[n/2]} D_n\left(\tfrac{a}{b}\right) \in \mathbb{Z}$$

satisfy $|q_n \alpha - p_n| < \frac{(\text{const})^n}{n!} \to 0$ as $n \to +\infty$ ($\Rightarrow q_n \neq 0$).

If $\frac{a}{b} > 0$ or if $-\pi^2 \le \frac{a}{b} < 0$, then $(-1)^n S_n\left(\frac{a}{b}\right) > 0$ $\forall n$ (a)

$\Rightarrow \alpha \neq \frac{p_n}{q_n} \Rightarrow \alpha \notin \mathbb{Q}$.

If $\frac{a}{b} < -\pi^2$, then (c) implies that $\forall n$ $p_n q_{n+1} \neq p_{n+1} q_n$,

hence $\frac{p_n}{q_n} \neq \frac{p_{n+1}}{q_{n+1}}$, and so $\alpha \neq \frac{p_n}{q_n}$ or $\alpha \neq \frac{p_{n+1}}{q_{n+1}} \Rightarrow \alpha \notin \mathbb{Q}$.

Rmk. If $0 > z^2$, then $z = i\lambda$ ($\lambda \in \mathbb{R}$) and $\frac{\operatorname{th}(\frac{z}{2})}{z} = \frac{\operatorname{tg}(\frac{\lambda}{2})}{\lambda}$.

So the above result says the following:

(1) If $t \in \mathbb{Q}$ and $t > 0$, then $\operatorname{th}\left(\frac{\sqrt{t}}{2}\right)/\sqrt{t} \notin \mathbb{Q}$.

(2) For $z = 2\pi i$, $\operatorname{th}\left(\frac{z}{2}\right)/z = 0 \in \mathbb{Q}$, therefore $-4\pi^2 = (2\pi i)^2 \notin \mathbb{Q}$.

(3) If $t \in \mathbb{Q}$ and $t > 0$, then $\operatorname{tg}\left(\frac{\sqrt{t}}{2}\right)/\sqrt{t} \in \mathbb{R} \setminus \mathbb{Q}$.

($\sqrt{t} \notin (2\mathbb{Z}+1)\pi$, by (2)).

Comparison of two Padé approximations

If $f(z) = \sum_{n\geq 0} c_n z^n$ $(c_n \neq 0)$ and if (B, A) and $(\widetilde{B}, \widetilde{A})$ are two Padé approximations of bidegree (m,n) of f (i.e., $A, B, \widetilde{A}, \widetilde{B}$ are non-zero polynomials, $\deg(A), \deg(\widetilde{A}) \leq m$, $\deg(B), \deg(\widetilde{B}) \leq n$, $\operatorname{ord}_{z=0}(Bf - A), \operatorname{ord}_{z=0}(\widetilde{B}f - \widetilde{A}) \geq m+n+1$),

then $\begin{vmatrix} A & B \\ \widetilde{A} & \widetilde{B} \end{vmatrix}$ is a polynomial of degree $\leq m+n$ and $\operatorname{ord}_{z=0} \geq m+n+1$,

and therefore is equal to zero. The rational function

$\frac{A}{B} = \frac{\widetilde{A}}{\widetilde{B}}$ is then uniquely determined by f and (m,n).

Special case:

$$D_n(z^2)\,\mathrm{sh}\left(\tfrac{z}{2}\right) - z\,C_n(z^2)\,\mathrm{ch}\left(\tfrac{z}{2}\right) = \frac{1}{2}\,e^{-z/2}\,R_n(z) = \frac{(-1)^n}{2\cdot n!}\,z^{2n+1}\int_0^1 x^n(1-x)^n \mathrm{ch}\left(z\left(x-\tfrac{1}{2}\right)\right)dx$$

$\deg C_n(x) \leq \left[\frac{n-1}{2}\right]$

$\deg D_n(x) \leq \left[\frac{n}{2}\right]$

If $g(x) = g_{1/2}(x) = \sum_{n\geq 0} \frac{x^n}{\left(\frac{1}{2}\right)_n \cdot n!} = \mathrm{ch}(2\sqrt{x})$, then

$g'(x) = 2\,g_{3/2}(x) = \frac{\mathrm{sh}(2\sqrt{x})}{\sqrt{x}}$ and

$$g/g' = \frac{\sqrt{x}}{\mathrm{th}(2\sqrt{x})} = \frac{1}{2} + \cfrac{x}{\frac{3}{2} + \cfrac{x}{\frac{5}{2} + \cfrac{x}{\ddots}}} = \frac{1}{2}\cdot\left(1 + \cfrac{x}{3 + \cfrac{x}{5 + \cfrac{x}{7 - \ddots}}}\right)$$

The convergents $\frac{p_n}{q_n} = \frac{1}{2} + \cfrac{x}{\frac{3}{2} + \cfrac{x}{\ddots + \frac{x}{2n+1}}}$ also give a Padé

approximations of the same bidegrees: $\deg(p_n(x)) \leq \left[\frac{n+1}{2}\right]$, $\deg(q_n(x)) \leq \left[\frac{n}{2}\right]$

$$\operatorname{ord}_x\left(q_n(x)\,\mathrm{ch}(2\sqrt{x}) - p_n(x)\,\frac{\mathrm{sh}(2\sqrt{x})}{\sqrt{x}}\right) \geq n+1$$

$\Rightarrow$ if $2\sqrt{x} = \frac{z}{2}$, then $\forall n \geq 0$ $\quad \frac{p_n(x)}{q_n(x)} = \frac{D_{n+1}(z^2)}{4C_{n+1}(z^2)}$

(in fact, $p_n(x) = \alpha_n D_{n+1}(z^2)$, $q_n(x) = 4\alpha_n C_{n+1}(z^2)$ for some $\alpha_n \in \mathbb{Q}\setminus\{0\}$, for reasons of degree).

$(z^2 = (4\sqrt{x})^2 = 16x)$

Take $z = \pi i$ $(\Rightarrow 16x = z^2 = -\pi^2)$; then $\mathrm{ch}(z/2) = 0$, $\mathrm{sh}(z/2) = i$, $e^{-z/2} = -i$

$$D_n(-\pi^2) = \frac{\pi^{2n+1}}{2\cdot n!}\int_0^1 x^n(1-x)^n \sin(\pi x)\,dx = \frac{1}{2\cdot n!}\int_0^\pi t^n(\pi - t)^n \sin(t)\,dt = I_n$$

$$D_n(-\pi^2)/C_n(-\pi^2) = 2 - \cfrac{\pi^2}{6 - \cfrac{\pi^2}{10 - \ddots - \cfrac{\pi^2}{2(2n-1)}}}$$

$c_1 = 1$

$c_2 = 6$

$c_3 = x + 60$, $c_4 = 20x + 840$

$D_1 = 2$

$D_2 = 2x + 12$

$D_3 = 12x + 120$

$D_4 = x^2 + 180x + 1680$

Back to general questions on approximations of reals by rationals

(1) Given $\alpha \in \mathbb{R}$, find $p, q \in \mathbb{Z}$ with
$|q\alpha - p| < \frac{1}{r}$, $\quad 0 < |q| < t$

> ($r > 0$ large; t controlled in terms of r)

(2) Given $\alpha_1, \dots, \alpha_m \in \mathbb{R}$, find $p_1, \dots, p_m, q \in \mathbb{Z}$ with
$\forall i \le m \; |q\alpha_i - p_i| < \frac{1}{r}$, $\quad 0 < |q| < t$

(3) Given $\alpha_1, \dots, \alpha_n \in \mathbb{R}$, find $q_1, \dots, q_n, p \in \mathbb{Z}$ with
$|q_1\alpha_1 + \dots + q_n\alpha_n - p| < \frac{1}{r}$, $\quad 0 < \max |q_j| < t$

(4) $\alpha_{ij} \in \mathbb{R}$ $(1 \le i \le m,\ 1 \le j \le n)$ find $q_1, \dots, q_n, p_1, \dots, p_m \in \mathbb{Z}$ with
$\forall i = 1, \dots, m \quad \left| \sum_{j=1}^{n} \alpha_{ij} q_j - p_i \right| < \frac{1}{r}$, $\quad 0 < \max |q_j| < t$.

Matrix notation: (a) $\mathbb{R}^n = \left\{ x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \right\}$, $\quad \|x\|_\infty = \max |x_i|$

(b) dual space $(\mathbb{R}^n)^* = \{ x^* = (x_1^*, \dots, x_n^*) \}$, $\|x^*\|_\infty = \max |x_i^*|$
duality pairing = the matrix product $x^* x = x_1^* x_1 + \dots + x_n^* x_n$

(c) for $x \in \mathbb{R}$, $\quad \langle\langle x \rangle\rangle := \inf_{a \in \mathbb{Z}} |x - a| = \min_{a \in \mathbb{Z}} |x - a| \quad (\le \frac{1}{2})$.
$\langle\langle x \rangle\rangle = 0 \iff x \in \mathbb{Z}$

(d) for $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{R}^n$, $\quad \langle\langle x \rangle\rangle := \max_{1 \le i \le n} \langle\langle x_i \rangle\rangle$; $\quad \langle\langle x \rangle\rangle = 0 \iff x \in \mathbb{Z}^n$

for $x^* = (x_1^*, \dots, x_n^*) \in (\mathbb{R}^n)^*$, $\quad \langle\langle x^* \rangle\rangle := \max \langle\langle x_i^* \rangle\rangle$; $\quad \langle\langle x^* \rangle\rangle = 0 \iff x^* \in (\mathbb{Z}^n)^*$.

Reformulation of the problems above: (1) $\langle\langle q\alpha \rangle\rangle < \frac{1}{r}$, $|q| < t$, $q \in \mathbb{Z} \setminus \{0\}$

$$\begin{pmatrix} p - q\alpha \\ q \end{pmatrix} = \begin{pmatrix} 1 & -\alpha \\ 0 & 1 \end{pmatrix} \begin{pmatrix} p \\ q \end{pmatrix}, \quad \begin{pmatrix} r(p - q\alpha) \\ t^{-1} q \end{pmatrix} = \underbrace{\begin{pmatrix} r & 0 \\ 0 & t^{-1} \end{pmatrix} \begin{pmatrix} 1 & -\alpha \\ 0 & 1 \end{pmatrix}}_{M} \underbrace{\begin{pmatrix} p \\ q \end{pmatrix}}_{z \in \mathbb{Z}^2 \setminus \{0\}}$$

$|q\alpha - p| < \frac{1}{r}$, $|q| < t \iff \|Mz\|_\infty < 1$

(4) The same with $p = \begin{pmatrix} p_1 \\ \vdots \\ p_m \end{pmatrix} \in \mathbb{Z}^m$, $q = \begin{pmatrix} q_1 \\ \vdots \\ q_n \end{pmatrix} \in \mathbb{Z}^n$, $A = (\alpha_{ij}) \in M_{m,n}(\mathbb{R})$

$z = \begin{pmatrix} p \\ q \end{pmatrix} \in \mathbb{Z}^{m+n}$

$(Aq)_i = \sum_{j=1}^{n} \alpha_{ij} q_j$

$$\begin{pmatrix} p - Aq \\ q \end{pmatrix} = \begin{pmatrix} I_m & -A \\ 0 & I_n \end{pmatrix} \begin{pmatrix} p \\ q \end{pmatrix}$$

$$\underbrace{\begin{pmatrix} r \cdot I_m & 0 \\ 0 & t^{-1} I_n \end{pmatrix} \begin{pmatrix} I_m & -A \\ 0 & I_n \end{pmatrix}}_{M} \underbrace{\begin{pmatrix} p \\ q \end{pmatrix}}_{z} = \begin{pmatrix} r(p - Aq) \\ t^{-1} q \end{pmatrix}$$

Inequalities in (4) $\iff$ $\|Mz\|_\infty < 1$

(2) $\Leftrightarrow$ ($n=1$ in (4)), $A = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix}$, $z = \begin{pmatrix} p_1 \\ \vdots \\ p_m \\ q \end{pmatrix}$

(3) $\Leftrightarrow$ ($m=1$ in (4)), $A = (\alpha_1, \cdots, \alpha_n)$, $z = \begin{pmatrix} p \\ q_1 \\ \vdots \\ q_n \end{pmatrix}$

Duality: interchange $m \longleftrightarrow n$

$A \longleftrightarrow$ the transpose matrix ${}^tA$

Non homogeneous approximations

Given additional $\beta_i \in \mathbb{R}$, replace the approximation conditions by

(1') $|q\alpha - \beta - p| < \frac{1}{r}$

(2') $|q\alpha_i - \beta_i - p_i| < \frac{1}{r}$

(3') $|q_1\alpha_1 + \cdots + q_n\alpha_n - \beta - p| < \frac{1}{r}$

(4') $\left| \sum_{j=1}^{n} \alpha_{ij} q_j - \beta_i - p_i \right| < \frac{1}{r}$

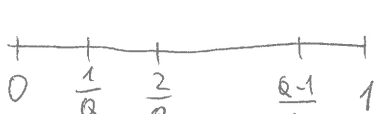
Dirichlet's approach to the homogeneous problem

(used the pigeon-hole principle)

Prop 1. Let $\alpha \in \mathbb{R}$. For any $1 < Q \in \mathbb{N}_+$ $\exists\, p, q \in \mathbb{Z}$, $1 \le q < Q$ $|p - q\alpha| < \frac{1}{Q}$.

($\Rightarrow |p - q\alpha| < \frac{1}{|q|}$).

Pf. For $q = 0, \cdots, Q$, the $Q+1$ fractional parts $\{q\alpha\} \in [0,1) = \bigsqcup_{j=0}^{Q-1} \left[\frac{j}{Q}, \frac{j+1}{Q}\right)$ fall into some of the Q intervals of length $\frac{1}{Q}$. Therefore $\exists\, 0 \le q_1 < q_2 \le Q$ such that



$\{q_1\alpha\}, \{q_2\alpha\}$ belong to the same $\left[\frac{j}{Q}, \frac{j+1}{Q}\right) \Rightarrow q := q_2 - q_1$ satisfies $1 \le q < Q$, $0 \le q\alpha - \underbrace{[q\alpha]}_{p} < \frac{1}{Q}$.

Cor. If $\alpha \notin \mathbb{Q}$, then $\exists_\infty\, p_n, q_n \in \mathbb{Z}$ $0 < |p_n - q_n\alpha| < \frac{1}{|q_n|}$.

Exercise. Deduce from Prop. 1 the following: if $\alpha \in \mathbb{R}$, $\alpha \notin \mathbb{Q}$, then

(1) $\mathbb{Z}\alpha + \mathbb{Z}$ is dense in $\mathbb{R}$: $\forall \beta \in \mathbb{R}$ $\forall \varepsilon > 0$ $\exists\, p, q \in \mathbb{Z}$ $|q\alpha - \beta - p| < \varepsilon$

(2) $\mathbb{R}\begin{pmatrix}\alpha \\ 1\end{pmatrix} + \mathbb{Z}^2$ is dense in $\mathbb{R}^2$: $\forall \begin{pmatrix}\beta_1 \\ \beta_2\end{pmatrix} \in \mathbb{R}^2$ $\forall \varepsilon > 0$ $\exists\, r \in \mathbb{R}$ $\exists \begin{pmatrix}p_1 \\ p_2\end{pmatrix} \in \mathbb{Z}^2$ $\begin{cases} |r\alpha - \beta_1 - p_1| < \varepsilon \\ |r - \beta_2 - p_2| < \varepsilon \end{cases}$

(3) Show directly, for $\alpha \in \mathbb{R}$, that ($\mathbb{Z}\alpha + \mathbb{Z}$ is dense in $\mathbb{R}$) is equivalent to ($\mathbb{R}\begin{pmatrix}\alpha \\ 1\end{pmatrix} + \mathbb{Z}^2$ is dense in $\mathbb{R}^2$).

These statements can be restated in terms of the quotients

$\mathbb{R}/\mathbb{Z} \xrightarrow{\sim}$ the circle $U(1) = S^1$

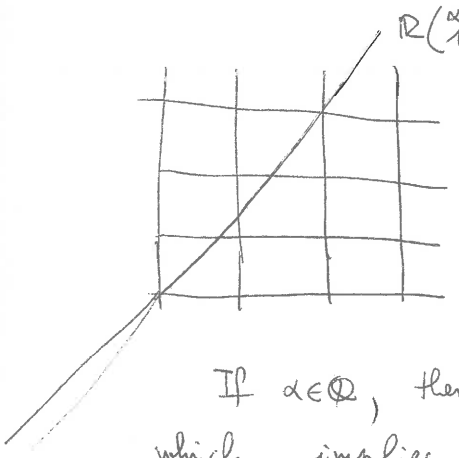
$\Psi \qquad\qquad \Psi$

$x \pmod{\mathbb{Z}} \xrightarrow{\sim} e^{2\pi i x}$

, $(\mathbb{R}/\mathbb{Z})^2 \xrightarrow{\sim}$ product of two circles

2-dim torus

and the projections $\mathbb{R} \twoheadrightarrow \mathbb{R}/\mathbb{Z} \xrightarrow{\sim} U(1)$



$\mathrm{pr}: (\mathbb{R}/\mathbb{Z})^2 \xrightarrow{\sim} U(1) \times U(1)$

Geometrically, $(\mathbb{R}/\mathbb{Z})^2$ is obtained from the unit square  by glueing together the pairs of opposite sides.

If $\alpha \in \mathbb{Q}$, then the line $\mathbb{R}\binom{\alpha}{1} \subset \mathbb{R}^2$ intersects non trivially $\mathbb{Z}^2$, which implies that its image on the torus $\mathrm{pr}\left(\mathbb{R}\binom{\alpha}{1}\right) \subset U(1)^2$ will be a closed curve:

If $\alpha \notin \mathbb{Q}$, then $\mathrm{pr}\left(\mathbb{R}\binom{\alpha}{1}\right)$ will be a dense curve on the torus, without self-intersections.

A more general result is the following:

Thm (a special case of Kronecker's Thm). Let $\alpha_1, \dots, \alpha_m \in \mathbb{R}$.

(1) If $1, \alpha_1, \dots, \alpha_m$ are linearly independent over $\mathbb{Z}$, then $\mathbb{Z}\begin{pmatrix}\alpha_1\\ \vdots \\ \alpha_m\end{pmatrix} + \mathbb{Z}^m$ is dense in $\mathbb{R}^m$ $\left(\Leftrightarrow \mathrm{pr}\left(\mathbb{Z}\begin{pmatrix}\alpha_1\\ \vdots \\ \alpha_m\end{pmatrix}\right)\right.$ is dense in $\underbrace{\mathbb{R}^m/\mathbb{Z}^m}$

m-dimensional torus

(2) If $\alpha_1, \dots, \alpha_m$ are linearly independent over $\mathbb{Z}$, then $\mathbb{R}\begin{pmatrix}\alpha_1\\ \vdots \\ \alpha_m\end{pmatrix} + \mathbb{Z}^m$ is dense in $\mathbb{R}^m$ $\left(\Leftrightarrow \mathrm{pr}\left(\mathbb{R}\begin{pmatrix}\alpha_1\\ \vdots \\ \alpha_m\end{pmatrix}\right)\right.$ is dense in $\mathbb{R}^m/\mathbb{Z}^m$)

Exercise: (a) Show that the assumptions in (1), (2) are necessarily

(b) Show that the statement (1) (for all m and all $\{\alpha_i\}$) is equivalent to the statement (2) (—— " ——).

For simultaneous approximations, Dirichlet's argument goes as follows.

Prop. 2. Given $\alpha_{ij} \in \mathbb{R}$ $(1 \le i \le m,\ 1 \le j \le n)$ and $1 < Q \in \mathbb{N}_+$, then there exist integers $p_1, \dots, p_m,\ q_1, \dots, q_n$ such that

$$\forall i = 1, \dots, m \qquad \left| \sum_{j=1}^{n} \alpha_{ij} q_j - p_i \right| < \frac{1}{Q}, \qquad 0 < \max_{j=1,\dots,n} |q_j| < Q^{m/n}.$$

Pf. Let $t := Q^{m/n}$ and consider the fractional parts

$$P(x) := \left(\left\{ \sum_{j=1}^{n} \alpha_{ij} x_j \right\} \right)_{1 \le i \le m} \in [0,1)^m \quad \text{for all } x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{Z}^n$$

with $x_j \in \{0, 1, \dots, [t]\}$. There are $([t]+1)^n > t^n = Q^m$ of them

$\Rightarrow \exists$ two distinct $x = (x_j),\ x' = (x_j') \in \{0, \dots, [t]\}^n$, for which the points $P(x)$ and $P(x')$ belong to the same cube $\left[\frac{k_1}{Q}, \frac{k_1+1}{Q}\right) \times \cdots \left[\frac{k_m}{Q}, \frac{k_m+1}{Q}\right)^m$ $(0 \le k_i < Q)$ (there are Q^m such cubes inside $[0,1)^m$).

Taking $q_j = x_j' - x_j$, we obtain the result.

Reformulation: Given $A \in M_{m,n}(\mathbb{R})$ and $1 < Q \in \mathbb{N}$, there exists $q \in \mathbb{Z}^n \setminus \{0\}$ such that $\|Aq\| \le \frac{1}{Q}$ and $\|q\|_\infty < Q^{m/n}$

$$\left(\Rightarrow \quad \|Aq\| < \frac{1}{\|q\|_\infty^{n/m}} \right).$$

Question: Is it true that there exist <u>infinitely many</u> $q \in \mathbb{Z}^n \setminus \{0\}$ satisfying $0 < \|Aq\| < \dfrac{1}{\|q\|_\infty^{n/m}}$?

Answer: No! Already for $m = n = 1$: if $\alpha = \frac{p'}{q'} \in \mathbb{Q}$, then

$$|\alpha q - p| = \left| \frac{p'q - pq'}{q'} \right| \ge \frac{1}{|q'|}$$ whenever $p, q \in \mathbb{Z}$, $q \neq 0$ and $\alpha q - p \neq 0$.

So one needs a suitable irrationality assumption on the entries of A.

Main drawback of Prop. 2: Q is assumed to be an <u>integer</u>.

As we are going to see, this assumption can be dropped if one uses geometry of numbers instead of the pigeon-hole principle.

Rational approximation and geometry of numbers

Minkowski's 1st Thm for parallelopipeds :

Let $N = \begin{pmatrix} N_1 \\ \vdots \\ N_d \end{pmatrix} \in GL_d(\mathbb{R})$, let $t_1, \dots, t_d > 0$. The rows N_i of N are linearly independent linear forms $N_i : \mathbb{R}^d \longrightarrow \mathbb{R}$, $x \longmapsto N_i x = \sum_{j=1}^{d} N_{ij} x_j$,

and the set $K := \{ x \in \mathbb{R}^d \mid \forall i \ \ |N_i x| \le t_i \}$ is a parallelopiped (compact) of volume $\mathrm{vol}(K) = 2^d |\det(N)|^{-1} \prod_{i=1}^{d} t_i$.

Prop. If $|\det(N)| \le \prod_{i=1}^{d} t_i$, then $\exists\, x \in \mathbb{Z}^d \setminus \{0\}$ $\forall i = 1, \dots, d \ \ |N_i x| \le t_i$.

Exercise. — " — , then $\forall i_0 \in \{1, \dots, d\}$ $\exists\, x \in \mathbb{Z}^d \setminus \{0\}$
$\forall i \neq i_0 \ \ |N_i x| < t_i$, $|N_{i_0} x| \le t_{i_0}$.

Hint : replace each t_i $(i \neq i_0)$ & $t_i(1 + \frac{1}{k})$ for $k \in \mathbb{N}_+$, and let $k \to \infty$.

Equivalent formulation : write $T = \begin{pmatrix} t_1 & & 0 \\ & \ddots & \\ 0 & & t_d \end{pmatrix}$, $M := T^{-1} N \in GL_d(\mathbb{R})$.

Then $K = \{ x \in \mathbb{R}^d \mid \|Mx\|_\infty \le 1 \}$, $\mathrm{vol}(K) = 2^d |\det(M)|^{-1}$.

Back to the approximation problem attached to $A \in M_{m,n}(\mathbb{R})$:

Work in $\mathbb{R}^{m+n}$ with elements $z = \begin{pmatrix} x \\ y \end{pmatrix}$, $x \in \mathbb{R}^m$, $y \in \mathbb{R}^n$
and lattice points $\begin{pmatrix} p \\ q \end{pmatrix} \in \mathbb{Z}^{m+n}$, $p \in \mathbb{Z}^m$, $q \in \mathbb{Z}^n$.

Approximation conditions $\|p - Aq\|_\infty \le r^{-1}$, $\|q\|_\infty \le t$ — (*)
are equivalent to $\left\| \begin{pmatrix} r(p - Aq) \\ t^{-1} q \end{pmatrix} \right\|_\infty \le 1$, but

$$\begin{pmatrix} r(p - Aq) \\ t^{-1} q \end{pmatrix} = \underbrace{\begin{pmatrix} r \cdot I_m & 0 \\ 0 & t^{-1} \cdot I_n \end{pmatrix}}_{T^{-1}} \underbrace{\begin{pmatrix} I_m & -A \\ 0 & I_n \end{pmatrix}}_{N} \begin{pmatrix} p \\ q \end{pmatrix}$$

$$\det(M) = r^m \cdot t^{-n}$$

$$M = \begin{pmatrix} r \cdot I_m & -rA \\ 0 & t^{-1} I_n \end{pmatrix}$$

$$\mathrm{vol} = 2^d r^{-m} t^n$$

Conclusion : (1) $(*) \iff \begin{pmatrix} p \\ q \end{pmatrix} \in \mathbb{Z}^{m+n} \cap K$, $K = \{ z \in \mathbb{R}^{m+n} \mid \|Mz\|_\infty \le 1 \}$

(2) If $r > 1$ and $(*)$ holds, then $q = 0 \in \mathbb{Z}^n \Rightarrow p = 0 \in \mathbb{Z}^m$.

Prop. Let $A \in M_{m,n}(\mathbb{R})$, $\mathbb{R} \ni r, t > 1$, $r^m t^{-n} \leq 1$. Then

$\exists\, q \in \mathbb{Z}^n \setminus \{0\}$ $\quad \|Aq\| < r^{-1}$, $\quad \|q\|_\infty \leq t$.

(Best bound for fixed t: $r = t^{n/m}$)

Cor 1. $\forall\, r > 1$, $r \in \mathbb{R}$ $\quad \exists\, q \in \mathbb{Z}^n \setminus \{0\}$ $\quad (\|Aq\|)^m \|q\|_\infty^n < 1$, $\quad \|Aq\| < r^{-1}$.

Pf. Take $t = r^{m/n}$ in Prop.

Cor 2. If $A \in M_{m,n}(\mathbb{R})$ is irrational in the sense that $\forall\, q \in \mathbb{Z}^n \setminus \{0\}$ $\quad Aq \notin \mathbb{Z}^m$, then there are infinitely many $q \in \mathbb{Z}^n \setminus \{0\}$ such that $\|Aq\| < \|q\|_\infty^{-n/m}$.

Pf of Prop. Apply Minkowski's 1st Thm to $M = T^{-1} N \in GL_d(\mathbb{R})$ ($d = m+n$) defined above and $K = \{z \in \mathbb{R}^d \mid \|Mz\|_\infty \leq 1\} \Rightarrow$ $\exists \binom{p}{q} \in \mathbb{Z}^{m+n} \setminus \{0\}$, $\|p - Aq\|_\infty < r^{-1}$, $\|q\|_\infty \leq t$. If $q = 0 \Rightarrow$ $\|p\|_\infty < r^{-1} < 1 \Rightarrow p = 0$ – impossible; so $q \neq 0$.

Special case $m = 1$: given $\alpha_1, \dots, \alpha_n \in \mathbb{R}$ and $t > 1$, $\exists\, p, q_1, \dots, q_n \in \mathbb{Z}$

$A = (\alpha_1, \dots, \alpha_n)$ such that $\begin{cases} 0 < \max |q_j| \leq t \\ |q_1\alpha_1 + \cdots + q_n\alpha_n - p| < \frac{1}{t^n} \quad \left(< \frac{1}{(\max |q_j|)^n} \right) \end{cases}$.

Special case $n = 1$: given $\alpha_1, \dots, \alpha_m \in \mathbb{R}$ and $t > 1$, $\exists\, q, p_1, \dots, p_m \in \mathbb{Z}$

$A = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix} = {}^t(\alpha_1, \dots, \alpha_m)$ such that $0 < |q| \leq t$

$\forall\, i = 1, \dots, m \quad |q\alpha_i - p_i| < \frac{1}{t^{1/m}} \left(\leq \frac{1}{|q|^{1/m}} \right)$.

Rmks: (1) For "generic" A, the exponent $\frac{n}{m}$ cannot be improved.

(2) Khinchine proved in the 1920's a duality ("transference") result relating the approximation properties of the row vector $(\alpha_1, \dots, \alpha_n)$ and the column vector ${}^t(\alpha_1, \dots, \alpha_n)$ (as in the two special cases above). This was reproved in the 1930's by Mahler, who discovered a general duality ("transference") result in geometry of numbers, based on Minkowski's 2nd Thm.

(3) Dyson generalised Khinchine's result to a general case involving a matrix $A \in M_{m,n}(\mathbb{R})$ and its transpose ${}^tA \in M_{n,m}(\mathbb{R})$.

Remarks on Kronecker's Thm

Kronecker's theorem answers the fundamental question about the existence of non homogeneous rational approximations.

Question. Given real numbers $\alpha_{ij} \in \mathbb{R}$ $(1 \le i \le m,\ 1 \le j \le n)$, describe the set of all m-tuples of real numbers $\beta_1, \dots, \beta_m \in \mathbb{R}$ having the following approximation property:

$$\forall\, \varepsilon > 0 \ \exists\, q_1, \dots, q_n, p_1, \dots, p_m \in \mathbb{Z} \quad \forall i = 1, \dots, m \quad \left| \sum_{j=1}^{n} \alpha_{ij} q_j - p_i - \beta_i \right| < \varepsilon .$$

The approximation property is equivalent to saying that the vector $b = \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_m \end{pmatrix} \in \mathbb{R}^m$ lies in the closure $\overline{X}$ of the additive subgroup $X = \mathbb{Z}^m + A\mathbb{Z}^n \subset \mathbb{R}^m$ generated by all vectors with integer entries and by the columns of the matrix $A = (\alpha_{ij})_{\substack{1 \le i \le m \\ 1 \le j \le n}} \in M_{m,n}(\mathbb{R})$.

In terms of the projection $pr : \mathbb{R}^m \longrightarrow \mathbb{R}^m/\mathbb{Z}^m = (\mathbb{R}/\mathbb{Z})^m$ on the m-dimensional real torus, one is asking for a description of the closure in $\mathbb{R}^m/\mathbb{Z}^m$ of the subgroup $pr(A\mathbb{Z}^n) \subset \mathbb{R}^m/\mathbb{Z}^m$ generated by the images under pr of the columns of A (indeed, $\overline{X} = pr^{-1}(\overline{pr(X)})$, since $X = X + \mathbb{Z}^m$, and $pr(X) = pr(A\mathbb{Z}^n)$).

This question is non-trivial already for $n = 1$, when $A = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix}$ and when the aim is to describe the closure in $\mathbb{R}^m/\mathbb{Z}^m$ of the cyclic group $\mathbb{Z} \cdot pr\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix}$ generated by a given element of $\mathbb{R}^m/\mathbb{Z}^m$.

We know the answer in the simplest case $m = n = 1$; $A = \alpha \in \mathbb{R}$:

$$\overline{\mathbb{Z} + \mathbb{Z}\alpha} = \begin{cases} \mathbb{R} & \text{if } \alpha \notin \mathbb{Q} \\ \underbrace{\frac{1}{q}\mathbb{Z}}_{\mathbb{Z} + \mathbb{Z}\alpha} & \text{if } \alpha = \frac{p}{q} \in \mathbb{Q}, \quad p, q \in \mathbb{Z} \setminus \{0\}, \quad \gcd(p, q) = 1. \end{cases}$$

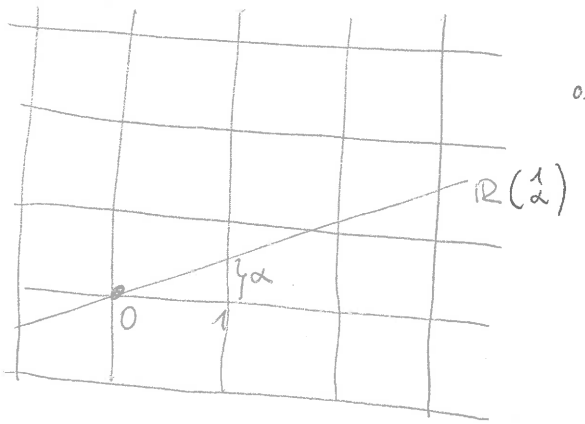
Relation to other approximation problems:

Prop. the following properties of $\alpha_1, \dots, \alpha_m \in \mathbb{R}$ are equivalent:

$\mathrm{pr}\left(\mathbb{R}\cdot\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_m\\ 1\end{pmatrix}\right)$ is dense in $\mathbb{R}^{m+1}/\mathbb{Z}^{m+1}$ $\iff$ $\mathrm{pr}\left(\mathbb{Z}\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_m\end{pmatrix}\right)$ is dense in $\mathbb{R}^m/\mathbb{Z}^m$.

Sketch proof if $m=1$: for some $t \in \mathbb{R}$, $t\cdot\begin{pmatrix}\alpha\\ 1\end{pmatrix}$ is close to $\begin{pmatrix}\beta_1\\ \beta_2\end{pmatrix}+\begin{pmatrix}p_1\\ p_2\end{pmatrix} \in \mathbb{R}^2$ $(p_i \in \mathbb{Z})$ $\iff$ αp_2 is close to $\beta_1 - \alpha\beta_2 + p_1$, and vice versa.

Cor. $(m=1)$ $\mathrm{pr}\left(\mathbb{R}\begin{pmatrix}\alpha\\ 1\end{pmatrix}\right)$ is dense in $\mathbb{R}^2/\mathbb{Z}^2 \iff \alpha \notin \mathbb{Q}$.



In other words, the image in $\mathbb{R}^2/\mathbb{Z}^2$ of a line of **irrational slope** passing through 0 will be a dense (but not self-intersecting) curve on the torus.

$\Downarrow$

any translate $\mathrm{pr}\left(\begin{pmatrix}\beta_1\\ \beta_2\end{pmatrix}+\mathbb{R}\begin{pmatrix}\alpha\\ 1\end{pmatrix}\right)$ will be dense in $\mathbb{R}^2/\mathbb{Z}^2$.

As we shall see, a special case of Kronecker's thm states that $\mathrm{pr}\left(\mathbb{Z}\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_m\end{pmatrix}\right)$ is dense in $\mathbb{R}^m/\mathbb{Z}^m \iff \alpha_1, \dots, \alpha_m, 1$ are linearly independent over $\mathbb{Q}$.

By Prop. above, this is equivalent to

$\mathrm{pr}\left(\mathbb{R}\begin{pmatrix}\alpha_0\\ \vdots\\ \alpha_m\end{pmatrix}\right)$ is dense in $\mathbb{R}^{m+1}/\mathbb{Z}^{m+1} \iff \alpha_0, \dots, \alpha_m$ are linearly independent over $\mathbb{Q}$.

It will be useful to reformulate Kronecker's thm (and the approximation question it answers) in more abstract terms.

(and more general)

Abstract question. Given a finite-dimensional $\mathbb{R}$-vector space V, describe the closure $\overline{X}$ in V of a given additive subgroup $X \subset V$.

The closure $\overline{X}$ is again a subgroup of V (exercise!).
One can study its structure by considering projections $V \to W$ to vector spaces of smaller dimension. It turns out that the case of one-dimensional W is sufficient.

Basic constraint.

(*) For every linear form $\ell : V \to \mathbb{R}$ (i.e., an element of the dual space $V^* = \mathrm{Hom}_{\mathbb{R}}(V, \mathbb{R})$), $\ell(\overline{X}) \in \overline{\ell(X)} \subset \mathbb{R}$

($\ell(\overline{X})$: closure in V; $\overline{\ell(X)}$: closure in $\mathbb{R}$)

(since ℓ is continuous).

This constraint is non-vacuous only for those $\ell \in V^*$ for which $\ell(X)$ is not dense in $\mathbb{R}$. We know that this is equivalent to $\overline{\ell(X)} \subset \mathbb{Z}\alpha$ for some $\alpha \in \mathbb{R} - \{0\}$. The condition $\ell(\overline{X}) \subset \overline{\ell(X)}$ does not change if we replace ℓ by $\alpha^{-1}\ell$. As a result, the constraint (*) is equivalent to

(*') For every $\ell \in V^*$ satisfying $\ell(X) \subset \mathbb{Z}$ we have $\ell(\overline{X}) \subset \mathbb{Z}$.

Kronecker's Thm in its abstract form asserts that there are no other constraints on $\overline{X}$ apart from (*') ($\Leftrightarrow$ (*)).

Thm. The closure $\overline{X}$ of a subgroup $X \subset V$ of a finite-dimensional real vector space is equal to $\{ v \in V \mid \ell(v) \in \mathbb{Z}$ for all $\ell \in V^*$ satisfying $\ell(X) \subset \mathbb{Z} \}$.

Cor (Kronecker's Thm in its original form) For $A \in M_{m,n}(\mathbb{R})$, the closure in $\mathbb{R}^m$ of $\mathbb{Z}^m + A\mathbb{Z}^n$ is equal to

$$\{ b \in \mathbb{R}^m \mid u^* b \in \mathbb{Z} \text{ for all } u^* \in (\mathbb{Z}^m)^* \text{ satisfying } u^* A \in (\mathbb{Z}^n)^* \}$$

Special cases: (1) $\mathbb{Z}^m + A\mathbb{Z}^n$ is dense in $\mathbb{R}^m$

$\Updownarrow$

there is no $u^* \in (\mathbb{Z}^m)^* - \{0\}$ such that $u^* A \in (\mathbb{Z}^n)^*$.

(2) $\mathbb{Z}^m + \mathbb{Z}\begin{pmatrix}\alpha_1\\ \vdots \\ \alpha_m\end{pmatrix}$ is dense in $\mathbb{R}^m \iff 1, \alpha_1, \dots, \alpha_m$ are linearly independent over $\mathbb{Z}$.

(3) $\mathbb{Z}^m + \mathbb{R}\begin{pmatrix}\alpha_1\\ \vdots \\ \alpha_m\end{pmatrix}$ is dense in $\mathbb{R}^m \iff \alpha_1, \dots, \alpha_m$ are linearly independent over $\mathbb{Z}$.

Reformulation of Thm: Def. For a subgroup $X \subset V$ (resp. $Y \subset V^*$) let

$${}^{\perp}X := \{ \ell \in V^* \mid \ell(x) \in \mathbb{Z} \text{ for all } x \in X \} \subset V^*$$

$$Y^{\perp} := \{ v \in V \mid \ell(v) \in \mathbb{Z} \text{ for all } \ell \in Y \} \subset V.$$

There are closed subgroups satisfying

$X \subset ({}^{\perp}X)^{\perp}$, $Y \subset {}^{\perp}(Y^{\perp})$. Moreover,

$X_1 \subset X_2 \Rightarrow {}^{\perp}X_1 \supset {}^{\perp}X_2$, $Y_1 \subset Y_2 \Rightarrow Y_1^{\perp} \supset Y_2^{\perp}$

Abstract form of Kronecker's Thm: the closure $\overline{X}$ of any subgroup $X \subset V$ is equal to $({}^{\perp}X)^{\perp}$.

Equivalent formulations: (1) If $X \subset V$ is a closed subgroup, then $({}^{\perp}X)^{\perp} = X$.

(2) Any closed subgroup $X \subset V$ is of the form $Y^{\perp}$, for some subgroup $Y \subset V^*$.

("X is defined by a system of linear equations with coefficients in $\mathbb{R}/\mathbb{Z}$", namely, $\ell(x) \pmod{\mathbb{Z}} = 0 \in \mathbb{R}/\mathbb{Z}$, $\ell \in Y$)

Indeed, if $X = Y^{\perp}$, then ${}^{\perp}X = {}^{\perp}(Y^{\perp}) \supset Y$ and

$X \subset ({}^{\perp}X)^{\perp} \subset Y^{\perp} = X \Rightarrow X = ({}^{\perp}X)^{\perp}$.

Similarly, if $X \subset V$ is any subgroup and if we know that $({}^{\perp}\overline{X})^{\perp} = \overline{X}$, then $X \subset \overline{X}$ implies ${}^{\perp}X \supset {}^{\perp}\overline{X}$ and

$X \subset \underbrace{({}^{\perp}X)^{\perp}}_{\text{closed}} \subset ({}^{\perp}\overline{X})^{\perp} = \overline{X} \Rightarrow ({}^{\perp}X)^{\perp} = \overline{X}$.

Structure Thm for closed subgroups of V: any pair $(X \subset V)$ (V finite dimensional $\mathbb{R}$-vector space, $X \subset V$ closed subgroup) is isomorphic to a direct sum of one-dimensional pairs $(0 \subset \mathbb{R})$, $(\mathbb{Z} \subset \mathbb{R})$ or $(\mathbb{R} \subset \mathbb{R})$.

(2) holds in these cases $\Rightarrow$ (2) holds for $(X \subset V)$.

Relation to Pontryagin duality

The exponential morphism $e: (\mathbb{R}, +) \longrightarrow U(1) = \{z \in \mathbb{C} \mid |z|=1\}$

$$x \longmapsto e^{2\pi i x}$$

has $\ker(e) = \mathbb{Z}$ (and induces an isomorphism $\mathbb{R}/\mathbb{Z} \xrightarrow{\sim} U(1)$ of topological groups). Every linear form $l: V \longrightarrow \mathbb{R}$ can be composed with e, defining a (unitary) character

$$\chi_l : \begin{array}{ccc} V & \longrightarrow & U(1) \\ \downarrow & & \downarrow \\ x & \longmapsto & e^{2\pi i l(x)} \end{array}.$$

Def. A (unitary) character of a topological abelian group G is a continuous morphism of abelian groups $\chi: G \longrightarrow U(1)$.

They form a group $\widehat{G}$ under multiplication.

Exercise: the map $\begin{array}{ccc} V^* & \longrightarrow & \widehat{V} \\ \downarrow & & \downarrow \\ (l: V \to \mathbb{R}) & \longmapsto & e^{2\pi i l} \end{array}$ is bijective.

This defines a topology on $\widehat{V}$, by transport of structure from V^*.

In this language, we define, for any subgroup $X \subset V$ (resp. $Y \subset \widehat{V}$)

$$^{\perp}X = \{\chi \in \widehat{V} \mid \forall x \in X \quad \chi(x) = 1\}$$

$$Y^{\perp} = \{v \in V \mid \forall \chi \in Y \quad \chi(v) = 1\}$$

The abstract form of Kronecker's Thm is then equivalent to the fact that $(^{\perp}X)^{\perp} = X$ holds for all closed subgroups $X \subset V$.

This is an important part of Pontryagin duality (for $G = V$), which asserts that, for any locally compact abelian group G and its closed subgroup H,

(1) $\widehat{G}$ has a natural topology under which it is locally compact

(2) the canonical map $G \longrightarrow \widehat{\widehat{G}}$ is an isomorphism of topological groups.

(3) $\widehat{G/H} = {}^{\perp}H = \{\chi \in \widehat{G} \mid \chi(H) = \{1\}\}$

(4) $\widehat{H} = \widehat{G}/{}^{\perp}H$

($\Rightarrow$ $H \overset{(2)}{=} \widehat{\widehat{H}} \overset{(4)}{=} \widehat{\widehat{G}/{}^{\perp}H} \overset{(3)}{=} ({}^{\perp}H)^{\perp}$).

(5) G is compact $\Longleftrightarrow$ $\widehat{G}$ is discrete.

Ex: $G = \mathbb{Z}$	$\widehat{G} = U(1)$
$G = \mathbb{Z}/n\mathbb{Z}$	$\widehat{G} = \mu_n(\mathbb{C})$
$G = \mathbb{Z}_p$	$\widehat{G} = \bigcup_{n \geq 1} \mu_{p^n}(\mathbb{C})$
$G = \prod_p \mathbb{Z}_p$	$\widehat{G} = \bigcup_{n \geq 1} \mu_n(\mathbb{C})$