update: 05/08/2016

http://ricerca.mat.uniroma3.it/users/valerio/hochiminh16.html

CIMPA

A joint CIMPA-ICTP research school on
Lattices and applications to cryptography and coding theory
Saigon University, Ho Chi Minh City, Vietnam.
August 1st - 12th, 2016

ICTP
The Abdus Salam
International Centre
for Theoretical Physics
50th Anniversary 1964-2014

Lattices and geometry of numbers

Exercises

Michel Waldschmidt

Exercise 1. Let x be a real number, $p_1, \dots, p_m$ distinct primes, $s_1, \dots, s_m$ positive integers, $a_1, \dots, a_m$ rational integers and ϵ a positive real number.
(a) Show that there exist two nonzero relatively prime integers u, v, such that

$$\left| x - \frac{u}{v} \right| < \epsilon \qquad \text{and} \qquad u \equiv a_i v \pmod{p_i^{s_i}} \text{ for } 1 \le i \le m.$$

(b) Show that there exist two integers $n \ge 0$ and u such that

$$\left| x - \frac{u}{p_1^n} \right| < \epsilon \qquad \text{and} \qquad u \equiv a_i p_1^n \pmod{p_i^{s_i}} \text{ for } 2 \le i \le m.$$

Exercise 2. Check

$$\{-x\} = \begin{cases} 1 - \{x\} & \text{if } x \notin \mathbb{Z}, \\ 0 & \text{if } x \in \mathbb{Z}. \end{cases}$$

$$\{x_1+x_2\} = \begin{cases} \{x_1\}+\{x_2\} & \text{if } \{x_1\}+\{x_2\}<1, \\ \{x_1\}+\{x_2\}-1 & \text{if } \{x_1\}+\{x_2\}\geq 1. \end{cases}$$

$$\{x_1-x_2\} = \begin{cases} \{x_1\}-\{x_2\} & \text{if } \{x_1\}-\{x_2\}\geq 0, \\ 1+\{x_1\}-\{x_2\} & \text{if } \{x_1\}-\{x_2\}<0. \end{cases}$$

Exercise 3. Let x_1, x_2 be two real numbers and let $\epsilon > 0$. Show that there exists integers p_1, p_2, q such that

$$|x_1 - q\sqrt{2} - p_1| < \epsilon \quad \text{and} \quad |x_2 - q\sqrt{3} - p_2| < \epsilon.$$

Exercise 4. Let R be a rectangle in the Euclidean plane; we consider a partition of R into smaller rectangles, the sides of which are parallel to those of R. Suppose that each of the smaller rectangles has at least one side, the length of which is an integer. Show that the length of at least one of the sides of R is an integer.

Exercise 5. Let G be a discrete subgroup of $\mathbb{R}^n$ and $x_1, \ldots, x_m$ elements in G. Check that $x_1, \ldots, x_m$ are linearly independent over $\mathbb{Z}$ if and only if they are linearly independent over $\mathbb{R}$.

Exercise 6. Let G be subgroup of $\mathbb{R}^n$ and H a subgroup of finite index of G. Show that G is dense in $\mathbb{R}^n$ if and only if H is dense in $\mathbb{R}^n$.

Exercise 7. Show that the subgroup of $\mathbb{R}_+^\times$ generated by 2 and 3

$$\left\{ 2^a 3^b \;\mid\; (a,b) \in \mathbb{Z}\times\mathbb{Z} \right\}$$

is dense in $\mathbb{R}_+^\times$ and that the subgroup of $\mathbb{R}^\times$ generated by -2 and 3

$$\left\{ (-2)^a 3^b \;\mid\; (a,b) \in \mathbb{Z}\times\mathbb{Z} \right\}$$

is dense in $\mathbb{R}^\times$.

Exercise 8. Let θ be a real number. Prove that the following conditions are equivalent.
(i) θ is irrational.
(ii) For any $\epsilon > 0$ there exist $p/q \in \mathbb{Q}$ such that

$$0 < |q\theta - p| < \epsilon.$$

(iii) There exist infinitely many $p/q \in \mathbb{Q}$ with $q > 0$ such that

$$\left|\theta - \frac{p}{q}\right| < \frac{1}{q^2}\cdot$$

(iv) For any $Q > 1$, there exist p and q in $\mathbb{Z}$ with $1 \leq q < Q$ and

$$0 < |q\theta - p| \leq \frac{1}{Q}\cdot$$

`Remark:` *Compare with Exercise 20.*

Exercise 9. Let R be a commutative topological group, V a closed subgroup of R and G a subgroup of R.
(a) Suppose that G is dense in R; show that $G/G \cap V$ is dense in R/V.
(b) Suppose that $G \cap V$ is dense in V and that $G/G \cap V$ is dense in R/V. Show that G is dense in R.
(c) Give an example where G is dense in R, but $G \cap V$ is not dense in V.

Exercise 10. Let R_1 and R_2 be two commutative topological groups and let R be the product $R_1 \times R_2$.
(a) If G_1 is a dense subgroup of R_1 and G_2 is a dense subgroup of R_2, show that $G_1 \times G_2$ is dense in R.
(b) Let G be a subgroup of R such that $\{x \in R_1 \mid (x, 0) \in G\}$ is dense in R_1 and $\{y \in R_2 \mid (0, y) \in G\}$ is dense in R_2. Show that G is dense in R.
(c) Give an example of a subgroup of $\mathbb{R}^2$ of finite type such that its projection onto each of $\mathbb{R} \times \{0\}$ and $\{0\} \times \mathbb{R}$ is dense, but which is not dense itself in $\mathbb{R}^2$.

Exercise 11. Let $G = \mathbb{Z}g_1 + \cdots + \mathbb{Z}g_{n+1}$ be a subgroup of $\mathbb{R}^n$ of finite type generated by $n+1$ elements $g_1, \ldots, g_{n+1}$ of $\mathbb{R}^n$. Write the g_j's in terms of the canonical basis of $\mathbb{R}^n$:

$$g_j = (g_{1j}, \ldots, g_{nj}), \qquad (1 \leq j \leq n+1).$$

Show that the following conditions are equivalent.
(i) G is dense in $\mathbb{R}^n$.
(ii) The $n+1$ real numbers

$$\Delta_h = \det\Bigl(g_{ij}\Bigr)_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n+1, j \neq h}}, \qquad (1 \leq h \leq n+1)$$

are linearly independent over $\mathbb{Q}$.
(iii) For all $(s_1, \dots, s_{n+1})$ in $\mathbb{Z}^{n+1}$ distinct from $(0, \dots, 0)$, the number

$$\det \begin{pmatrix} g_{11} & \cdots & g_{1\,n+1} \\ \vdots & \ddots & \vdots \\ g_{n1} & \cdots & g_{n\,n+1} \\ s_1 & \cdots & s_{n+1} \end{pmatrix}$$

is not zero.

Exercise 12.
(a) Let $f : \mathbb{R} \to \mathbb{C}$ be continuous homomorphisms of the additive group $\mathbb{R}$ into the additive group $\mathbb{C}$. Show that there exists a unique $\lambda \in \mathbb{R}$ such that $f(x) = \lambda x$.
(b) Verify that all continuous homomorphisms of the additive group $\mathbb{R}$ into itself are $\mathbb{R}$-linear maps, that is, of the form $x \mapsto \lambda x$ for some $\lambda \in \mathbb{R}$.
(c) Let $f : \mathbb{R} \to \mathbb{C}$ be continuous homomorphisms of the additive group $\mathbb{R}$ into the multiplicative group $\mathbb{R}^\times$. Deduce from (b) that there exists a unique $\lambda \in \mathbb{R}$ such that $f(x) = e^{\lambda x}$.
(d) Let $f : \mathbb{R} \to \mathbb{C}$ be continuous homomorphisms of the additive group $\mathbb{R}$ into the multiplicative group

$$\mathbb{U} = \{z \in \mathbb{C}^\times \ \mid \ |z| = 1\}.$$

Show that there exists a unique $\lambda \in \mathbb{R}$ such that $f(x) = e^{i\lambda x}$.
(e) Deduce that all continuous homomorphisms $\chi : \mathbb{R} \to \mathbb{R}/\mathbb{Z}$ factor as $\chi = s \circ h$:

$$\begin{tikzcd} \mathbb{R} \arrow[r, "h"] \arrow[dr, "\chi"'] & \mathbb{R} \arrow[d, "s"] \\ & \mathbb{R}/\mathbb{Z} \end{tikzcd}$$

where $s : \mathbb{R} \to \mathbb{R}/\mathbb{Z}$ is the canonical surjection and $h : \mathbb{R} \to \mathbb{R}$ is a linear map.
(f) When u is an element of $\mathbb{R}^n$, the map ψ_u of $\mathbb{R}^n$ into $\mathbb{U}$ given by $x \mapsto e^{2i\pi u \cdot x}$ (where $u \cdot x$ is the standard scalar product in $\mathbb{R}^n$) is a character of $\mathbb{R}^n$. Verify that one obtains all characters in this way. Prove that the kernel of ψ_u is $\{x \in \mathbb{R}^n \ \mid \ u \cdot x \in \mathbb{Z}\}$.
(g) Deduce that the map from $\mathrm{Hom}_{\mathbb{R}}(\mathbb{R}^n, \mathbb{R})$ into the group of characters

of $\mathbb{R}^n$ that, for a linear form φ, associates $\chi_\varphi : x \mapsto e^{2i\pi\varphi(x)}$, is a group isomorphism. Prove that the kernel of χ_φ est $\varphi^{-1}(\mathbb{Z})$.

Exercise 13. Let $k \subset K$ be a field extension and n a positive integer. For a K-vector subspace V of K^n, show that the two following properties are equivalent:
(i) There exists a basis of V which consists of elements in k^n.
(ii) There exist linear forms $L_1, \dots, L_m$ with coefficients in k such that V is the intersection of the hyperplanes $L_s = 0$, $(1 \le s \le m)$.
When there properties are satisfied, the subspace V is called *rational over* k.

Exercise 14. Let G be a subgroup of $\mathbb{R}^n$ of finite type which contains $\mathbb{Z}^n$. Show that G is dense in $\mathbb{R}^n$ if and only if for all hyperplanes H of $\mathbb{R}^n$ *rational over* $\mathbb{Q}$, the projection $G/G \cap H$ of G onto $\mathbb{R}^n/H$ has a dense image.
`Remark:` *Compare with Exercise 9.*

Exercise 15. Let G be a subgroup of $\mathbb{R}^n$. Show that the following conditions are equivalent.
(i) G contains a subgroup of finite type that is dense in $\mathbb{R}^n$.
(ii) For all subspaces V de $\mathbb{R}^n$ (considered as a vector space) distinct from $\mathbb{R}^n$, we have $\mathrm{rang}_{\mathbb{Z}}(G/G \cap V) > \dim_{\mathbb{R}}(\mathbb{R}^n/V)$.
(iii) For all hyperplanes H of $\mathbb{R}^n$, we have $\mathrm{rang}_{\mathbb{Z}}(G/G \cap H) \ge 2$.
(iv) For all nonzero linear forms $\varphi : \mathbb{R}^n \longrightarrow \mathbb{R}$, we have $\varphi(G) \not\subset \mathbb{Q}$.
(v) For all nontrivial character $\chi : \mathbb{R}^n \longrightarrow \mathbb{U}$, we have $\chi(G) \ne \{1\}$.
Further, if G is finitely generated, if $g_1, \dots, g_\ell$ are generators of G over $\mathbb{Z}$ and if the coordinates of g_j in the canonical basis of $\mathbb{R}^n$ are

$$g_j = (g_{1j}, \dots, g_{nj}), \qquad (1 \le j \le \ell),$$

then these conditions are equivalent to:
(vi) For all $(s_1, \dots, s_\ell)$ in $\mathbb{Z}^\ell$ different from $(0, \dots, 0)$, the matrix

$$\begin{pmatrix} g_{11} & \cdots & g_{1\ell} \\ \vdots & \ddots & \vdots \\ g_{n1} & \cdots & g_{n\ell} \\ s_1 & \cdots & s_\ell \end{pmatrix}$$

has rank $n+1$.

Exercise 16. Let m and n be two positive integers and let θ_{ji}, $(1 \le j \le n$, $1 \le i \le m)$ be real numbers; we put

$$\gamma_i = (\theta_{1i}, \dots, \theta_{ni}) \in \mathbb{R}^n, \qquad (1 \le i \le m)$$

and

$$\delta_j = (\theta_{j1}, \dots, \theta_{jm}) \in \mathbb{R}^m, \qquad (1 \le j \le n).$$

So

$$\Gamma = \mathbb{Z}^n + \mathbb{Z}\gamma_1 + \cdots + \mathbb{Z}\gamma_m \subset \mathbb{R}^n \quad \text{and} \quad \Delta = \mathbb{Z}^m + \mathbb{Z}\delta_1 + \cdots + \mathbb{Z}\delta_n \subset \mathbb{R}^m$$

are subgroups generated by the column vectors of the matrix

$$\begin{pmatrix} 1 & \cdots & 0 & \theta_{11} & \cdots & \theta_{1m} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 1 & \theta_{n1} & \cdots & \theta_{nm} \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & \cdots & 0 & \theta_{11} & \cdots & \theta_{n1} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 1 & \theta_{1m} & \cdots & \theta_{nm} \end{pmatrix}.$$

Show that the subgroup Γ is dense in $\mathbb{R}^n$ if and only if the subgroup Δ is of rank $n+m$ over $\mathbb{Z}$.

Exercise 17. Recall that when G is a subgroup of $\mathbb{R}^n$, we set

$$G^\star = \{\varphi \in \mathrm{Hom}_{\mathbb{R}}(\mathbb{R}^n, \mathbb{R}) \mid \varphi(G) \subset \mathbb{Z}\},$$

while when $\mathcal{G}$ is a subgroup of $\mathrm{Hom}_{\mathbb{R}}(\mathbb{R}^n, \mathbb{R})$, we set

$$\mathcal{G}^\star = \{x \in \mathbb{R}^n \mid \varphi(x) \in \mathbb{Z} \text{ for all } \varphi \in \mathcal{G}\}.$$

See [2, Chap. 7 §1 n°3].
(a) Let G_1 and G_2 be subgroups of $\mathbb{R}^n$. Verify

$$(G_1 + G_2)^\star = G_1^\star \cap G_2^\star,$$

$$G_1 \subset G_2 \Longleftrightarrow G_1^\star \supset G_2^\star$$

and

$$(\overline{G}_1 \cap \overline{G}_2)^\star = \overline{G_1^\star + G_2^\star}.$$

`Hint.` Recall $\overline{G} = (G^\star)^\star$.
(b) Let G be a lattice in $\mathbb{R}^n$. Verify that $G^\star$ is a lattice of $\mathrm{Hom}_{\mathbb{R}}(\mathbb{R}^n, \mathbb{R})$ (the lattice $G^\star$ is called the *dual* lattice of G).
What is the dual lattice $(\mathbb{Z}^n)^\star$ of $\mathbb{Z}^n$?

What is the dual lattice of $G^\star$?
(c) Let G_1 and G_2 be two lattices in $\mathbb{R}^n$ with $G_2 \subset G_1$. Verify that the two finite groups G_1/G_2 and $G_2^\star/G_1^\star$ are isomorphic.

Exercise 18. Let G be a subgroup of $\mathbb{R}^n$.
(a) Suppose that for all hyperplanes H of $\mathbb{R}^n$, $G/G\cap H$ is dense in $\mathbb{R}^n/H$. Show that G is dense in $\mathbb{R}^n$.
(b) Deduce the following statement: if $n \geq 2$ and if $G/G\cap D$ is dense in $\mathbb{R}^n/D$ for all lines D in $\mathbb{R}^n$, then G is dense in $\mathbb{R}^n$.

Exercise 19. Let $\theta_1, \dots, \theta_m$ be real numbers.
(a) For any real number $Q > 1$, show that there exist $p_1, \dots, p_m, q$ in $\mathbb{Z}$ such that $1 \leq q < Q$ and

$$\max_{1\leq i\leq m} |q\theta_i - p_i| \leq \frac{1}{Q^{1/m}}\cdot$$

(b) Show that if H a real number > 1, then there exists a tuple $(a_0, a_1, \dots, a_m)$ of rational integers such that

$$0 < \max_{1\leq i\leq m} |a_i| < H \quad \text{and} \quad |a_0 + a_1\theta_1 + \cdots + a_m\theta_m| \leq H^{-m}.$$

(c) Let θ be a real number with $|\theta| \leq 1/2$, d a positive integer and H a positive integer. Show that there exists a non–zero polynomial $P \in \mathbb{Z}[X]$ of degree $\leq d$ and coefficients in the interval $[-H, H]$ such that

$$|P(\theta)| \leq H^{-d}.$$

Exercise 20. Denote by $\|\cdot\|$ the distance to the nearest integer: for $x \in \mathbb{Z}$,

$$\|x\| = \min_{a\in\mathbb{Z}} |x - a|.$$

Let n be a positive integer and $\theta_1, \dots, \theta_n$ be real numbers.
(a) Show that the following three conditions are equivalent.
(i) $(\theta_1, \dots, \theta_n) \not\in \mathbb{Q}^n$.
(ii) There exist infinitely many integers $q > 0$ such that

$$0 < \max_{1\leq j\leq n} \|q\theta_j\| < q^{-1/n}.$$

(iii) For all $\epsilon > 0$, there exists an integer $q > 0$ such that

$$0 < \max_{1\leq j\leq n} \|q\theta_j\| < \epsilon.$$

(b) Show that the following two conditions are equivalent.
(i) The numbers $1, \theta_1, \ldots, \theta_n$ are linearly independent over $\mathbb{Q}$.
(ii) For any $\epsilon > 0$ there exist $m+1$ linearly independent elements $\mathbf{b}_0, \mathbf{b}_1, \ldots, \mathbf{b}_m$ in $\mathbb{Z}^{m+1}$, say

$$\mathbf{b}_i = (q_i, p_{1i}, \ldots, p_{mi}), \quad (0 \leq i \leq m)$$

with $q_i > 0$, such that

$$\max_{1 \leq k \leq m} \left| \theta_k - \frac{p_{ki}}{q_i} \right| \leq \frac{\epsilon}{q_i}, \quad (0 \leq i \leq m).$$

(c) Assume that, for all $\varepsilon > 0$, there exists a complete system of $m+1$ linearly independent linear forms in $m+1$ variables

$$L_i = L_i(\underline{X}) = \sum_{j=0}^{m} b_{ij} X_j, \quad i = 0, 1, \ldots, m, \quad b_{ij} \in \mathbb{Z},$$

such that

$$\max_{0 \leq i \leq m} |L_i(1, \underline{\theta})| \leq \frac{\varepsilon}{A^{m-1}} \quad \text{where} \quad A = \max_{0 \leq i,j \leq m} |b_{ij}|.$$

Show that the numbers $1, \theta_1, \ldots, \theta_m$ are linearly independent over $\mathbb{Q}$.

Exercise 21. Let $\theta_1, \ldots, \theta_m$ be real numbers. Assume that $1, \theta_1, \ldots, \theta_m$ are linearly independent over $\mathbb{Q}$. Let V be a vector subspace of $\mathbb{R}^{m+1}$ which is rational over $\mathbb{Q}$ and has dimension $\leq m$.
(a) Check that the intersection of V with the real line $\mathbb{R}(1, \theta_1, \ldots, \theta_m)$ is $\{0\}$.
(b) Deduce that

$$\|(x_0, x_1, \ldots, x_m)\| = \max_{1 \leq i \leq m} |x_0 \theta_j - x_j|$$

defines a norm on V.

Exercise 22. Let p be a prime number. Show that there exist u and v in $\mathbb{Z}$ such that $u^2 + v^2 + 1 \equiv 0 \pmod{p}$.

http://ricerca.mat.uniroma3.it/users/valerio/hochiminh16.html

Indications for the solutions

Solution of Exercise 1. The so–called *weak approximation theorem* for $\mathbb{Q}$ states that given rational numbers $x, a_1, \dots, a_m$, distinct prime numbers $p_1, \dots, p_m$ and $\epsilon > 0$, there exist $u/v \in \mathbb{Q}$ such that

$$\left| x - \frac{u}{v} \right| < \epsilon \quad \text{and} \quad \left| a_i - \frac{u}{v} \right|_{p_i} < \epsilon \quad \text{for} \quad 1 \le i \le m.$$

Exercise 1 is a special case where we assume $a_i \in \mathbb{Z}$; the assumption $x \in \mathbb{Q}$ is no loss of generality since $\mathbb{Q}$ is dense in $\mathbb{R}$.
The *strong approximation theorem* for $\mathbb{Q}$ states that the image of $\mathbb{Q}$ in the product

$$\mathbb{R} \times \mathbb{Q}_{p_1} \times \cdots \times \mathbb{Q}_{p_m}$$

is dense. These approximations theorems are valid for number fields.
`References:` [4, Chap. 2, §15 p. 67] or [7, §36 G].
The solution of Exercise 1 (a) uses the following auxiliary results. The first one expresses that, on $\mathbb{Q}$, the topologies induced by the ordinary absolute value and the p–adic ones are independent.
Lemma 1. *There exist rational numbers $z_0, z_1, \dots, z_m$ such that*

$$\begin{aligned} &|z_0| > 1, \ |z_0|_{p_i} < 1 \quad (1 \le i \le m), \\ &|z_i|_{p_i} > 1, \ |z_i| < 1, \ |z_i|_{p_j} < 1 \quad (1 \le i, j \le m, \ i \ne j). \end{aligned}$$

Proof. A solution is given as follows:

$$z_0 = p_1 \cdots p_m, \qquad z_i = \frac{p_1 \cdots p_m}{p_i^k} \quad (1 \le i \le m),$$

where k is a sufficiently large integer. □

One deduces from Lemma 1:
Lemma 2. *Let $\epsilon > 0$. There exist rational numbers $\lambda_0, \lambda_1, \dots, \lambda_m$ such that*

$$\begin{aligned} &|\lambda_0 - 1| < \epsilon, \ |\lambda_0|_{p_i} < \epsilon \quad (1 \le i \le m), \\ &|\lambda_i - 1|_{p_i} < \epsilon, \ |\lambda_i| < \epsilon, \ |\lambda_i|_{p_j} < \epsilon \quad (1 \le i, j \le m, \ i \ne j). \end{aligned}$$

Proof. Using the notations of Lemma 1, a solution is given as follows:

$$\lambda_0 = \frac{z_0^N}{1+z_0^N}, \qquad \lambda_i = \frac{z_i^N}{1+z_i^N} \quad (1 \le i \le m),$$

where N is a sufficiently large integer. □

For the solution of Exercise 1 (a), we first use the fact that the set of rational numbers with denominator prime to $p_1 \cdots p_m$ is dense in $\mathbb{R}$. Hence there exists $u_0/v_0 \in \mathbb{Q}$ with $\gcd(v_0, p_1 \cdots p_m) = 1$ and

$$\left| x - \frac{u_0}{v_0} \right| < \frac{\epsilon}{2}.$$

Without loss of generality we may assume $0 < \epsilon < 1$. Next, using Lemma 2, we deduce that there exist $\lambda_0, \lambda_1, \ldots, \lambda_m$ in $\mathbb{Q}$ such that

$$|\lambda_0 - 1| < \frac{\epsilon}{2(m+1)(|x|+1)}, \quad |\lambda_0|_{p_j} \le p_j^{-s_j} \quad (1 \le j \le m),$$

$$|\lambda_i - 1|_{p_i} \le p_i^{-s_i}, \quad |\lambda_i| < \frac{\epsilon}{2(m+1)\max\{1, |a_i|\}} \quad (1 \le i \le m)$$

and

$$|\lambda_i|_{p_j} \le p_j^{-s_j}, \quad (1 \le i, j \le m, \; i \ne j).$$

It follows that

$$\frac{u}{v} = \lambda_0 \frac{u_0}{v_0} + \lambda_1 a_1 + \cdots + \lambda_m a_m$$

satisfies the required conditions.

For the proof of part (b), we use the fact that the set (subring of $\mathbb{Q}$) $\mathbb{Z}[1/p_1]$ of rational numbers with denominator a power of p_1 is dense in $\mathbb{R}$. We start with $u_0/v_0 \in \mathbb{Z}[1/p_1]$ and

$$\left| x - \frac{u_0}{v_0} \right| < \frac{\epsilon}{2}.$$

We set $P = p_2^{s_2} \cdots p_m^{s_m}$. Using again the density of $\mathbb{Z}[1/p_1]$ in $\mathbb{R}$, we deduce that there exists $\mu_0 \in \mathbb{Z}[1/p_1]$ such that

$$|P\mu_0 - 1| < \frac{\epsilon}{2m(|x|+1)}.$$

We set $\lambda_0 = P\mu_0$, so that $\lambda_0 \in \mathbb{Z}[1/p_1]$ satisfies

$$|\lambda_0 - 1| < \frac{\epsilon}{2m(|x|+1)} \quad \text{and} \quad |\lambda_0|_{p_i} \le p_i^{-s_i} \quad (2 \le i \le m).$$

For $i = 2, \dots, m$, define

$$q_i = \frac{P}{p_i^{s_i}} = p_2^{s_2} \cdots p_{i-1}^{s_{i-1}} p_{i+1}^{s_{i+1}} \cdots p_m^{s_m}.$$

Let N be a sufficiently large integer so that, for $2 \le i \le m$,

$$\frac{P}{p_1^N} < \frac{\epsilon}{2m \max\{1, |a_i|\}}.$$

Let $r_i \in \{1, \dots, p_i^{s_i} - 1\}$ be the solution of the congruence

$$q_i r_i \equiv p_1^N \pmod{p_i^{s_i}}.$$

Define

$$\lambda_i = \frac{q_i r_i}{p_1^N} \quad (i = 2, \dots, m).$$

Then we have

$$|\lambda_i| < \frac{\epsilon}{2m \max\{1, |a_i|\}}, \quad |\lambda_i - 1|_{p_i} \le p_i^{-s_i}, \quad |\lambda_i|_{p_j} \le p_j^{-s_j} \quad (2 \le i, j \le m, \ i \ne j).$$

One easily deduces that a solution to question (b) is given by

$$\frac{u}{p_1^n} = \lambda_0 \frac{u_0}{v_0} + \lambda_2 a_2 + \cdots + \lambda_m a_m.$$

Solution of Exercise 2. Use the fact that for x and y in $\mathbb{R}$, we have

$$\{x\} = \{y\} \iff x - y \in \mathbb{Z}$$

and

$$\{x\} = y \iff x - y \in \mathbb{Z} \quad \text{and} \quad 0 \le y < 1.$$

Solution of Exercise 3. Since $1, \sqrt{2}, \sqrt{3}$ are linearly independent over $\mathbb{Q}$, the subgroup $\mathbb{Z}^2 + \mathbb{Z}(\sqrt{2}, \sqrt{3})$ is dense in $\mathbb{R}^2$.

Solution of Exercise 4.
A rectangle $R = [0, a] \times [0, b]$ has one integer side if and only if

$$\int_0^a \int_0^b e^{2i\pi(x+y)} \mathrm{d}x \mathrm{d}y = 0.$$

Indeed, this integral has the value

$$\int_0^a\int_0^b e^{2i\pi(x+y)}\mathrm{d}x\mathrm{d}y = \int_0^a e^{2i\pi x}\mathrm{d}x\int_0^b e^{2i\pi y}\mathrm{d}y = \frac{-1}{4\pi^2}(e^{2i\pi a}-1)(e^{2i\pi b}-1),$$

and $(e^{2i\pi a}-1)(e^{2i\pi b}-1)$ is 0 if and only if one at least of a, b is an integer. If R is the disjoint union of subrectangles $R_1,\dots,R_m$, then

$$\int_R e^{2i\pi(x+y)}\mathrm{d}x\mathrm{d}y = \sum_{j=1}^m \int_{R_j} e^{2i\pi(x+y)}\mathrm{d}x\mathrm{d}y.$$

Remarks.
1. The density of $\mathbb{Z}+\mathbb{Z}\theta$ in $\mathbb{R}$ for θ irrational has been proved by Bohr using the function $e^{2i\pi x}$. See [6, §23.9]. This argument has been extended by Weyl to study the equidistribution of the points $\{n\theta\}$ on the unit circle [8], [6, S23.10, Th. 445].
2. Further solutions of Exercise 4 are given in [1, Chapter 26, *tiling rectangles*, pp.173–177]. See also [11] and [10, Problem 5.2, pp. 74–77].

Solution of Exercise 5. Clearly, if $x_1,\dots,x_m$ are linearly independent over $\mathbb{R}$, then they are linearly independent over $\mathbb{Z}$. Conversely, assume that $x_1,\dots,x_m$ are linearly independent over $\mathbb{Z}$. Let V be the subspace of $\mathbb{R}^n$ which they span. The dimension of V is $\le m$. The intersection of V with G is a discrete subgroup of V containing m elements linearly independent over $\mathbb{Z}$, hence V has dimension $\ge m$ over $\mathbb{R}$; it follows that V has dimension m : $G\cap V$ is a lattice in V.

Solution of Exercise 6. If H is dense in $\mathbb{R}^n$, then G also. Conversely, assume G is dense in $\mathbb{R}^n$. This means that the topological closure $\overline{G}$ of G in $\mathbb{R}^n$ is $\mathbb{R}^n$. Since G is the disjoint union of finitely many classes modulo H and since $\mathbb{R}^n$ is not the union of finitely many proper affine subspaces, it follows that the closure $\overline{H}$ of H in $\mathbb{R}^n$ is also $\mathbb{R}^n$.

Solution of Exercise 7.
(a) Since $\log 2$ and $\log 3$ are linearly independent over $\mathbb{Q}$, the subgroup $\mathbb{Z}\log 2+\mathbb{Z}\log 3$ is dense in $\mathbb{R}$, and its image under the continuous isomorphism

$$\begin{array}{ccc}\mathbb{R} & \to & \mathbb{R}_+^\times\\ x & \mapsto & e^x\end{array}$$

is dense.
(b) The subgroup $\big\{(-2)^a 3^b \;\mid\; (a,b) \in \mathbb{Z}\times\mathbb{Z}\big\}$ of $\mathbb{R}^\times$ is finitely generated, it has rank 2 and it contains -2, hence is dense in $\mathbb{R}^\times$.

Solution of Exercise 8.
The implication $(i) \Rightarrow (iv)$ is a basic result on the homogeneous approximation of a real number by a rational number, which can be proved either by means of Dirichlet's box principle, Farey series or continued fractions; see for instance [3, Chap. 1, Th. 1] and [9, Th. 1A]. The assumption (i) is used to obtain $q\theta - p \neq 0$.
$(iv) \Rightarrow (iii)$. Clearly, (iv) implies that there is at least one solution to (iii). Assume that $p_1/q_1, \ldots, p_m/q_m$ are solutions. Define

$$\eta = \min_{1\le i\le m} |q_i x - p_i|$$

and use (iv) with $Q > 1/\eta$.
$(iii) \Rightarrow (ii)$. Let p_1/q_1 and p_2/q_2 be two distinct approximations, given by the assumption (iii), with $q_1 > 1/\epsilon$ and $q_2 > 1/\epsilon$. Then one at least of $q_1x - p_1$, $q_2x - p_2$ is not 0.
$(ii) \Rightarrow (i)$. Assume θ is rational, say $\theta = a/b$. Let ϵ satisfy $0 < \epsilon < 1/b$. Then the condition

$$|q\theta - p| \le \epsilon$$

implies $q\theta = p$.

Solution of Exercise 9.
(a) The map $s : R \to R/V$ is continuous and surjective.
(b) Let $x \in R$ and let $\mathcal{U}$ be a neighborhood of x in R. By density of $G/G\cap V$ in R/V, there exists $y \in G$ such that $s(x-y) \in s(\mathcal{U})$. Let $t = x - y$ and let $u \in \mathcal{U}$ be such that $s(t) = s(u)$; hence $t - u \in V$. The set of $z \in V$ such that $t - z \in \mathcal{U}$ is open in V and not empty (it contains u). By density of $G \cap V$ in V, there exists $z \in G \cap V$ such that $t - z \in \mathcal{U}$. Hence $x - z - y \in \mathcal{U}$ with $y + z \in G$.
(c) The intersection of $\mathbb{Q}^2$ with the line $\{(t, t\sqrt{2}) \;\mid\; t \in \mathbb{R}\}$ of $\mathbb{R}^2$ is $\{0\}$. Another example is the intersection of $\mathbb{Z}^2 + \mathbb{Z}(\sqrt{2}, \sqrt{3})$ with the line $\mathbb{R}\times\{0\}$.

Solution of Exercise 10.
(a) is clear and (b) follows from (a).
(c) Let $D = \{(t,t) \;\mid\; t \in \mathbb{R}\}$ be the diagonal of $\mathbb{R}^2$. The projections of the subgroup

$$G = (\mathbb{Z} + \mathbb{Z}\sqrt{2})^2 \cap D = \mathbb{Z}(1,1) + \mathbb{Z}(\sqrt{2}, \sqrt{2})$$

on $\mathbb{R} \times \{0\}$ and on $\{0\} \times \mathbb{R}$ are both $\mathbb{Z} + \mathbb{Z}\sqrt{2}$.

Solution of Exercise 11. Change the basis so that $g_1, \ldots, g_n$ becomes the canonical basis while g_{n+1} becomes $(\theta_1, \ldots, \theta_n)$. Then, up to a sign ± 1, $\Delta_1, \ldots, \Delta_n, \Delta_{n+1}$ are $\theta_1, \ldots, \theta_n, 1$, while in statement (*iii*) the determinant has the value $s_1\theta_1 + \cdots + s_n\theta_n + s_{n+1}$. Then use Kronecker's Theorem (see for instance [13, Th. 4.1] or Exercise 16).

Solution of Exercise 12.
(a) Let $f : \mathbb{R} \to \mathbb{C}$ be a continuous homomorphism. Define $\lambda = f(1)$. We have $f(n) = n\lambda$ for all $n \in \mathbb{Z}$. We deduce $qf(p/q) = f(p) = \lambda p$ for all $p/q \in \mathbb{Q}$, hence $f(p/q) = \lambda p/q$ for all $p/q \in \mathbb{Q}$. Therefore, by continuity, given $x = \lim p_n/q_n$, we have

$$f(p_n/q_n) = \lambda p_n/q_n \to \lambda x \quad \text{and also} \quad f(p_n/q_n) \to f(x),$$

hence $f(x) = \lambda x$.
(b) follows from (a).
(c) The exponential map

$$\begin{array}{rccc} \exp : & \mathbb{R} & \to & \mathbb{R}_+^\times \\ & x & \mapsto & e^x \end{array}$$

is a continuous isomorphism, the inverse isomorphism is the logarithm

$$\begin{array}{rccc} \log : & \mathbb{R}_+^\times & \to & \mathbb{R} \\ & x & \mapsto & \log x. \end{array}$$

Let f be continuous homomomorphism of $\mathbb{R}$ into $\mathbb{R}^\times$. The image $f(\mathbb{R})$ of f is connected, and the connected component of 1 in $\mathbb{R}^\times$ is $\mathbb{R}_+^\times$. Hence $f(\mathbb{R}) \subset \mathbb{R}_+^\times$. The map $\log \circ f$ is a continuous homomorphism $\mathbb{R} \to \mathbb{R}$, hence, by (b), is of the form $x \mapsto \lambda x$ for some $\lambda \in \mathbb{R}$. Therefore $f(x) = e^{\lambda x}$. The unicity of λ is clear.
(d) The unicity follows from the following remark: if $e^{i\lambda x} = e^{i\lambda' x}$ for all $x \in \mathbb{R}$, then $(\lambda - \lambda')x \in 2i\pi\mathbb{Z}$ for all $x \in \mathbb{R}$, and therefore $\lambda = \lambda'$. For the existence of λ, we first use the continuity of f at the origin: there exists $r > 0$ such that $f(x)$ has a positive real part for all $x \in (-r, r)$. Let x_0 satisfy $0 < x_0 < r$. Since $f(x_0)$ is an element of $\mathbb{U}$ of positive real part, there exists $y_0 \in \mathbb{R}$ with $-\pi/2 < y_0 < \pi/2$ such that $f(x_0) = e^{iy_0}$. Define $\lambda = y_0/x_0$. Then one checks that $f(x) = e^{i\lambda x}$ for all x in $(-r, r) \cap \mathbb{Q}$, next for all x in $(-r, r)$, and finally

for all $x \in \mathbb{R}$.
(e) follows from (d): the map

$$\begin{array}{ccc} \mathbb{R} & \to & \mathbb{U} \\ x & \mapsto & e^{2i\pi x} \end{array}$$

is a continuous surjective homomorphism with kernel $\mathbb{Z}$, hence $\mathbb{U}$ is isomorphic to $\mathbb{R}/\mathbb{Z}$. .
(f) and (g) follow from (b), which implies that the continuous homomorphisms $\mathbb{R}^n \to \mathbb{R}$ are the linear maps $x \mapsto u \cdot x$.

Solution of Exercise 13. Let $e_1, \dots, e_r$ be elements of k^n, say $e_i = (a_{1i}, \dots, a_{ni})$. The K–vector space V of K^n spanned by $e_1, \dots, e_r$ is

$$\{e_1t_1 + \cdots + e_rt_r \mid (t_1, \dots, t_r) \in K^r\}.$$

Let

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1r} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nr} \end{pmatrix}.$$

Hence the subspace V is

$$\left\{ A \begin{pmatrix} t_1 \\ \vdots \\ t_r \end{pmatrix} \mid (t_1, \dots, t_r) \in K^r \right\}.$$

On the other hand, if $L_1, \dots, L_{n-r}$ are linear forms with coefficients in k, say

$$L_s(z_1, \dots, z_n) = b_{s1}z_1 + \cdots + b_{sn}z_n,$$

the vector subspace W of K^n, intersection of the kernels of $L_1, \dots, L_{n-r}$, is

$$\left\{ (z_1, \dots, z_n) \in K^n \mid \sum_{j=1}^n b_{sj}z_j = 0 \ (s = 1, \dots, n-r) \right\}.$$

Let

$$B = \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{n-r\ 1} & \cdots & a_{n-r\ r} \end{pmatrix}.$$

Hence W is nothing else than

$$\left\{ (z_1, \ldots, z_n) \in K^n \ \mid B \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} = 0 \right\}.$$

The coefficients of A and B are in k. The equivalence between the two definitions of a rational subspace follows from the fact that a $n \times r$ matrix A with coefficients in k has rank r if and only if there exists a $(n-r) \times n$ matrix B with coefficients in k of rank $n-r$ such that $BA = 0$, and a $(n-r) \times n$ matrix B with coefficients in k has rank $n-r$ if and only if there exists a $n \times r$ matrix A with coefficients in k of rank r such that $BA = 0$.

Solution of Exercise 14. If G is not dense in $\mathbb{R}^n$, there is a hyperplane H such that $G/G \cap H$ is not dense in $\mathbb{R}^n/H$ (see Exercises 15 and 18), hence is contained in a discrete subgroup $a_0\mathbb{Z}$ with $a_0 \in \mathbb{R}$, $a_0 \neq 0$. Write an equation of H as $a_1x_1 + \cdots + a_nx_n = 0$ with $a_i \in \mathbb{R}$. Since G contains $\mathbb{Z}^n$, we deduce that a_i/a_0 are integers, hence H is rational over $\mathbb{Q}$.

Solution of Exercise 15. We first prove the result when G is a group of finite type (see [13, Prop. 4.3]).
$(i) \Longrightarrow (ii)$ follows from Exercise 9 (a).
$(ii) \Longrightarrow (iii)$ is plain.
$(iii) \Longrightarrow (i)$. If G is not dense, the closure $\overline{G}$ of G in $\mathbb{R}^n$ contains a vector subspace $V \neq \mathbb{R}^n$ and $G/G \cap V$ is discrete in $\mathbb{R}^n/V$. Let H be a hyperplane containing V. Then $G/G \cap H$ is discrete in $\mathbb{R}^n/H$, hence has rank ≤ 1.
$(iii) \Longleftrightarrow (iv) \Longleftrightarrow (v)$ follow from Exercise 12.
$(v) \Longleftrightarrow (vi)$. The rank of the matrix in condition (vi) is $< n+1$ if and only if there exist real numbers $c_0, c_1, \ldots, c_n$, not all of which are zero, such that

$$c_1g_{1j} + \cdots + c_ng_{nj} = c_0s_j \qquad \text{for} \quad 1 \leq j \leq \ell.$$

The condition $(s_1, \ldots, s_\ell) \neq (0, \ldots, 0)$ implies $(c_1, \ldots, c_n) \neq (0, \ldots, 0)$. The existence of $(c_1, \ldots, c_n)$ is equivalent to say that there is a nonzero linear form $\varphi(x) = c_1x_1 + \cdots + c_nx_n$ such that $\mathrm{rang}_{\mathbb{Z}}\varphi(G) \leq 1$.
In the general case where the group G is a not of finite type, one may assume that G has rank $\geq n^2$, and one proves the result by induction on n. See [12, Lemme 3.12].

Solution of Exercise 16. We claim that a necessary and sufficient condition for Γ not to be dense in $\mathbb{R}^n$ is the existence of $a_1, \ldots, a_n$ in $\mathbb{Z}$, not all 0, such that the numbers $b_1, \dots, b_m$ defined by

$$b_i = \sum_{j=1}^{n} a_j \theta_{ji} \quad (1 \leq i \leq m)$$

are all in $\mathbb{Z}$. This is the same as to say

$$a_1\delta_1 + \cdots + a_n\delta_n + b_1e_1 + \cdots + b_me_m = 0,$$

hence our claim solves Exercise 16.
Our claim is a result due to Kronecker, it follows from Exercise 15. It also follows from $\overline{G} = (G^\star)^\star$ (see Exercise 17 and [2, TG VII.7 N°3]).

Solution of Exercise 17.
(a) If $\varphi \in G_1^\star \cap G_2^\star$, then $\varphi(G_1) \subset \mathbb{Z}$ and $\varphi(G_2) \subset \mathbb{Z}$, hence $\varphi(G_1 + G_2) \subset \mathbb{Z}$. If $\varphi \in (G_1 + G_2)^\star$, then $\varphi(G_1 + G_2) \subset \mathbb{Z}$, hence $\varphi(G_1) \subset \mathbb{Z}$ and $\varphi(G_2) \subset \mathbb{Z}$ and therefore $\varphi \in G_1^\star \cap G_2^\star$.
The equivalence

$$G_1 \subset G_2 \Longleftrightarrow G_1^\star \supset G_2^\star$$

follows from the definitions.
The subgroup $(G_1 \cap G_2)^\star$ of $\mathrm{Hom}(\mathbb{R}^n, \mathbb{R})$ is closed and contains both $G_1^\star$ and $G_2^\star$, hence it contains $\overline{G_1^\star + G_2^\star}$.
Conversely, since $\overline{G_1^\star + G_2^\star} = ((G_1^\star + G_2^\star)^\star)^\star$, to prove the inclusion

$$(\overline{G}_1 \cap \overline{G}_2)^\star \subset \overline{G_1^\star + G_2^\star},$$

it suffices to prove $(G_1^\star + G_2^\star)^\star \subset \overline{G}_1 \cap \overline{G}_2$. Let $x \in (G_1^\star + G_2^\star)^\star$ For any $\varphi \in G_1^\star + G_2^\star$, we have $\varphi(x) \in \mathbb{Z}$. Hence $x \in \overline{G_1} \cap \overline{G_2}$.
(b) If $G = \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_n$ where $(e_1, \dots, e_n)$ is a basis of $\mathbb{R}^n$ over $\mathbb{R}$, then $G^\star = \mathbb{Z}f_1 + \cdots + \mathbb{Z}f_n$ where $(f_1, \dots, f_n)$ is the dual basis of $\mathrm{Hom}(\mathbb{R}^n, \mathbb{R})$:

$$f_i(e_j) = \delta_{ij} = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases}$$

The dual lattice of $\mathbb{Z}^n$ is the group of linear forms $\mathbb{R}^n \to \mathbb{R}$ with coefficients in $\mathbb{Z}$:

$$(x_1, \dots, x_n) \to a_1x_1 + \cdots + a_nx_n$$

with $(a_1, \dots, a_n) \in \mathbb{Z}^n$.
The dual basis of $(f_1, \dots, f_n)$ is $(e_1, \dots, e_n)$, hence G is the dual lattice of

$G^\star$.

(c) Using the structure theorem on the modules over a principal ring, we can select an adapted basis $(e_1, \dots, e_n)$ of the $\mathbb{Z}$–module G_1 such that a basis of the $\mathbb{Z}$–module G_2 is $(a_1e_1, \dots, a_ne_n)$, where $a_1, \dots, a_n$ are positive integers. The quotient G_1/G_2 is isomorphic to

$$(\mathbb{Z}/a_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/a_n\mathbb{Z}).$$

As we have seen, a basis of $G_1^\star$ is given by the dual basis $(f_1, \dots, f_n)$ of $\mathrm{Hom}(\mathbb{R}^n, \mathbb{R})$. Then a basis of $G_2^\star$ is $(f_1/a_1, \dots, f_n/a_n)$. Since

$$\frac{\frac{1}{a}\mathbb{Z}}{\mathbb{Z}} \simeq \frac{\mathbb{Z}}{a\mathbb{Z}},$$

we have

$$G_2^\star/G_1^\star \simeq (\mathbb{Z}/a_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/a_n\mathbb{Z}).$$

Solution of Exercise 18.

(a) If G is not dense, the maximal subspace V of $\mathbb{R}^n$ contained in the closure $\overline{G}$ of G is not $\mathbb{R}^n$, hence is contained in a hyperplane H. The group $\mathbb{R}^n/H$ is isomorphic to $\mathbb{R}$, hence the subgroup $G/G \cap H$ is not dense in $\mathbb{R}^n/H$.

(b) Assume $n \geq 2$ and G not dense in $\mathbb{R}^n$. By (a), there exists a subspace H of $\mathbb{R}^n$ of positive dimension such that $G/G \cap H$ is not dense in $\mathbb{R}^n/H$. Let D be such a subspace of minimal dimension. By induction, using (a), we deduce that D has dimension 1.

Solution of Exercise 19.

(a) This result is due to Dirichlet [9, Th. 1E]. The determinant of the matrix

$$\begin{pmatrix} -1 & 0 & \cdots & 0 & \theta_1 \\ 0 & -1 & \cdots & 0 & \theta_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & -1 & \theta_m \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$$

is (-1^m), hence the result follows from Minkowski's theorem on linear forms for ([3, Appendix B, Th. III], [9, Th. 2C]) with

$$A_1 = \cdots = A_m = Q^{-1/m}, \quad A_{m+1} = Q$$

(the product $A_1A_2\cdots A_mA_{m+1}$ is 1).
(b) This result is due to Dirichlet [9, Th. 1C]. The determinant of the matrix

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ \theta_1 & \theta_2 & \cdots & \theta_m & 1 \end{pmatrix}$$

is 1, hence the result follows from Minkowski's theorem on linear forms ([3, Appendix B, Th. III], [9, Th. 2C]) with

$$A_1 = \cdots = A_m = H, \quad A_{m+1} = H^{-m}$$

(the product $A_1A_2\cdots A_mA_{m+1}$ is 1).
(c) From (b) with $m = d$ and $\theta_i = \theta^i$ we deduce that there exists $a_0, a_1, \dots, a_d$ in $\mathbb{Z}$, not all zero, such that

$$|a_0 + a_1\theta + \cdots + a_d\theta^d| \le H^{-d}$$

and

$$\max_{1\le i\le d} |a_i| < H.$$

It remains to bound $|a_0|$. From the hypothesis on $|\theta|$ and the upper bounds on $|a_1|, \dots, |a_d|$ we deduce

$$|a_0| \le |a_1||\theta| + \cdots + |a_d||\theta|^d + H^{-d} \le H\left(\frac{1}{2} + \frac{1}{4} + \cdots + \frac{1}{2^d} + \frac{1}{H^{d+1}}\right).$$

Since H is a positive integer, the result follows from

$$\frac{1}{2} + \frac{1}{4} + \cdots + \frac{1}{2^d} + \frac{1}{H^{d+1}} = 1 - \frac{1}{2^d} + \frac{1}{H^{d+1}} < 1 + \frac{1}{H}\cdot$$

Solution of Exercise 20.
$(i) \Longrightarrow (ii)$. Assume $\theta \not\in \mathbb{Q}^n$. Then we have

$$0 < \max_{1\le j\le n} \|\theta_j\| < 1,$$

hence there is at least one solution to (ii) (namely with $q = 1$). Assume $q_1, \ldots, q_m$ are solutions to (ii). Define

$$\eta = \min_{1\le i\le m} \max_{1\le j\le n} \|q_i\theta_j\|.$$

By assumption (i)we have $\eta > 0$. Let Q be a real number satisfying $Q > \eta^{-n}$. From Dirichlet's Theorem (see (a) in the preceding Exercise), it follows that there exists $q \in \mathbb{Z}$ with $1 \le q < Q$ and

$$\max_{1\le j\le n} \|q\theta_j\| < Q^{-1/n}.$$

From the definition of η and the choice of Q, we deduce $q \notin \{q_1, \ldots, q_m\}$. From (i) we deduce $\max_{1\le j\le n} \|q\theta_j\| \ne 0$. Finally from $q < Q$ we deduce

$$0 < \max_{1\le j\le n} \|q\theta_j\| < q^{-1/n}.$$

The implication $(ii) \Longrightarrow (iii)$ is plain.
Finally, if $\theta \in \mathbb{Q}^n$, let $b > 0$ be a common denominator to $\theta_1, \ldots, \theta_n$. Then for any integer $q > 0$ for which $\max_{1\le j\le n} \|q\theta_j\| \ne 0$ we have

$$\max_{1\le j\le n} \|q\theta_j\| > \frac{1}{b}\cdot$$

Hence $(iii) \Longrightarrow (i)$.
(b) This result is due to M. Laurent. The proof of $(ii) \Rightarrow (i)$ rests on the following auxiliary result.
Lemma 3. *Let $\theta_1, \ldots, \theta_m$ be real numbers. Assume that the numbers $1, \theta_1, \ldots, \theta_m$ are linearly dependent over $\mathbb{Q}$: let $a, b_1, \ldots, b_m$ be rational integers, not all of which are zero, satisfying*

$$a + b_1\theta_1 + \cdots + b_m\theta_m = 0.$$

Let $\epsilon > 0$ satisfy $\sum_{k=1}^m |b_k| < 1/\epsilon$. Assume further that $(q, p_1, \ldots, p_m) \in \mathbb{Z}^{m+1}$ satisfies $q > 0$ and

$$\max_{1\le k\le m} |q\theta_k - p_k| \le \epsilon.$$

Then

$$aq + b_1p_1 + \cdots + b_mp_m = 0.$$

Proof of Lemma 3. In the relation

$$qa + \sum_{k=1}^{m} b_k p_k = -\sum_{k=1}^{m} b_k(q\theta_k - p_k),$$

the right hand side has absolute value less than 1 and the left hand side is a rational integer, so it is 0. □

Proof of $(ii) \Rightarrow (i)$. By assumption (ii) we have $m+1$ linearly independent elements $\mathbf{b}_i \in \mathbb{Z}^{m+1}$ such that the corresponding rational approximations satisfy the assumptions of Lemma 3. Since $\mathbf{b}_0, \mathbf{b}_1, \ldots, \mathbf{b}_m$ are linearly independent, for each nonzero linear form

$$aX_0 + b_1X_1 + \cdots + b_mX_m = 0,$$

one at least of the $L(\mathbf{b}_i)$ is not 0. Hence Lemma 3 implies

$$a + b_1\theta_1 + \cdots + b_m\theta_m \neq 0.$$

Proof of $(i) \Rightarrow (ii)$. Let $\epsilon > 0$. Assume (i) holds. By Dirichlet's box principle, there exists $\mathbf{b} = (q, p_1, \ldots, p_m) \in \mathbb{Z}^{m+1}$ with $q > 0$ such that

$$\max_{1 \le k \le m} \left| \theta_k - \frac{p_k}{q} \right| \le \frac{\epsilon}{q}\cdot$$

Consider the subset $E_\epsilon \subset \mathbb{Z}^{m+1}$ of these tuples. We are going to show that the $\mathbb{Q}$-vector subspace V_ϵ of $\mathbb{Q}^{m+1}$ spanned by E_ϵ is $\mathbb{Q}^{m+1}$. It will follow that there are $m+1$ linearly independent elements in E_ϵ.
If $V_\epsilon \neq \mathbb{Q}^{m+1}$, then there is a hyperplane $a_0z_0 + a_1z_1 + \cdots + a_mz_m = 0$ containing E_ϵ. Any $\mathbf{b} = (q, p_1, \ldots, p_m)$ in E_ϵ has

$$a_0q + a_1p_1 + \cdots + a_mp_m = 0.$$

For each $n \ge 1/\epsilon$, let $\mathbf{b} = (q_n, p_{1n}, \ldots, p_{mn}) \in E_\epsilon$ satisfy

$$\max_{1 \le k \le m} \left| \theta_k - \frac{p_{kn}}{q_n} \right| \le \frac{1}{nq_n}\cdot$$

Then

$$-a_0 + a_1\theta_1 + \cdots + a_m\theta_m = \sum_{k=1}^{m} a_k \left(\theta_k - \frac{p_{kn}}{q_n} \right).$$

Hence

$$|-a_0+a_1\theta_1+\cdots+a_m\theta_m|\le\frac{1}{nq_n}\sum_{k=1}^m|a_k|.$$

The right hand side tends to 0 as n tends to infinity, hence the left hand side vanishes, and $1,\theta_1,\dots,\theta_m$ are $\mathbb{Q}$–linearly dependent, which contradicts (i).
(c) This result is due to C.L. Siegel (1929); see for instance [5]. Let

$$L(\underline{X})=a_0X_0+\cdots+a_mX_m,\quad a_j\in\mathbb{Z},$$

be a non–zero linear form with integer coefficients in $m+1$ variables. The aim is to prove, under the assumptions of (c), $L(1,\underline{\vartheta})\neq 0$. Set

$$H=\max_{0\le j\le m}|a_j|.$$

Let ε be a positive real number $<1/(m!\cdot mH)$. Among the forms $\{L_0,\dots,L_m\}$ satisfying the assumptions of (c) for this value of ε, there exist m of them, say $L_{k_1},\dots,L_{k_m}$, which along with L make up a complete system of linearly independent forms. Denote by Δ the determinant of the coefficient matrix of the system of linear forms $L,L_{k_1},\dots,L_{k_m}$ and, for $0\le i,j\le m$, by $\Delta_{i,j}$ the (i,j)-minor of this matrix. Then

$$\Delta=L(1,\underline{\vartheta})\cdot\Delta_{0,0}+\sum_{i=1}^m L_{k_i}(1,\underline{\vartheta})\cdot\Delta_{i,0}.$$

Since $\Delta\in\mathbb{Z}$ and $\Delta\neq 0$, we have $|\Delta|\ge 1$. One easily estimates, for $0\le j\le m$,

$$|\Delta_{0,j}|\le m!A^m\qquad\text{and}\qquad\max_{1\le i\le m}|\Delta_{i,j}|\le m!HA^{m-1}.$$

It follows that

$$\begin{aligned}(m!)^{-1}&\le|L(1,\underline{\vartheta})|\cdot A^m+\sum_{i=1}^m|L_{k_i}(1,\underline{\vartheta})|\cdot HA^{m-1}\\&\le|L(1,\underline{\vartheta})|\cdot A^m+\varepsilon\cdot mH\\&<|L(1,\underline{\vartheta})|\cdot A^m+(m!)^{-1}.\end{aligned}$$

Thus $L(1,\underline{\vartheta})\neq 0$.

Solution of Exercise 21.

(a) Since the vector space V is rational over $\mathbb{Q}$ and has dimension $\leq m$, it is contained in a hyperplane rational over $\mathbb{Q}$, say $a_0z_0 + a_1z_1 + \cdots + a_mz_m = 0$. An element of the real line $\mathbb{R}(1, \theta_1, \ldots, \theta_m)$ can be written $(x, x\theta_1, \ldots, x\theta_m)$ with $x \in \mathbb{R}$. If it belong to V, then $x(a_0 + a_1\theta_1 + \cdots + a_m\theta_m) = 0$, hence $x = 0$ since $1, \theta_1, \ldots, \theta_m$ are $\mathbb{Q}$–linearly independent.

(b) From (a) we deduce that for $(x_0, x_1, \ldots, x_m) \in V$, we have

$$\max_{1\leq i\leq m} |x_0\theta_j - x_j| = 0 \Longleftrightarrow (x_0, x_1, \ldots, x_m) = 0.$$

The properties

$$\|x\| \geq 0 \quad \text{for all} \quad x \in V,$$

$$\|x + y\| \leq \|x\| + \|y\| \quad \text{for all} \quad x \in V \quad \text{and } y \in V,$$

and

$$\|\lambda x\| = |\lambda|\|x\| \quad \text{for all} \quad \lambda \in \mathbb{R} \quad \text{and } x \in V,$$

are plain.

Solution of Exercise 22.

For $p = 2$, a solution is $u = 1$, $v = 0$.

Assume p is odd. Each of the two sets

$$\{u^2 \mid 0 \leq u \leq p/2\} \quad \text{and} \quad \{-1 - v^2 \mid 0 \leq u \leq p/2\}$$

consists of $(p+1)/2$ integers which are in different classes modulo p. By Dirichlet's box principle, there is an integer w congruent modulo p to a u^2 in the first set and to a $-1 - v^2$ in the second set. Now

$$w \equiv u^2 \equiv -1 - v^2 \pmod{p},$$

hence $1 + u^2 + v^2 \equiv 0 \pmod{p}$.

References

[1] Aigner, M. & Ziegler, G. M. *Proofs from THE BOOK.* 4th ed., Springer-Verlag, 2010.

[2] Bourbaki, N., *Eléments de mathématiques.* Livre III, Topologie générale; chapitre V: *Groupes à un paramètre.* chapitre VII: *Les groupes additifs* $\mathbb{R}^n$. Actualités Sci. Ind. **1029**, Hermann, Paris, 1947 et 1974.
General topology. Chapters 5–10. Translated from the French. Reprint of the 1966 edition. Elements of Mathematics. Springer-Verlag, Berlin-New York, 1989.

[3] Cassels, J.W.S., *An Introduction to Diophantine Approximation.* Cambridge Tracts in Mathematics and Mathematical Physics, No. **45**, Cambridge University Press, New York, 1957. x+166 pp.
Reprint of the 1957 edition. Hafner Publishing Co., New York, 1972.

[4] Cassels, J.W.S & Fröhlich, J., *Algebraic Number Theory.* Lecture notes from an instructional conference held in Brighton in 1965. London Mathematical Society (2010).

[5] Chantanasiri, A., *On the criteria for linear independence of Nesterenko, Fischler and Zudilin*, Chamchuri Journal of Mathematics, **2** (1) 31–46, 2010.

[6] Hardy, G.H. & Wright, E.M, *An Introduction to the Theory of Numbers.* Fifth edition. The Clarendon Press, Oxford University Press, New York, 1979.

[7] O'Meara, O.T., *Introduction to Quadratic Forms.* Reprint of the 1973 edition. Classics in Mathematics. Springer-Verlag, Berlin, 2000.

[8] Rauzy, G., *Propriétés statistiques de suites arithmétiques.* Le Mathématicien, No. **15**. Collection SUP. Presses Universitaires de France, Paris, 1976.

[9] Schmidt, W.M., *Diophantine Approximation.* Lecture Notes in Math. **785**. Springer, Berlin, 1980.

[10] Tao, T., *Solving Mathematical Problems: A Personal Perspective.* Oxford University Press, Oxford, 2006.

[11] WAGON, S., *Fourteen Proofs of a Result About Tiling a Rectangle.* The American Mathematical Monthly, 94, No. 7 (1987), pp. 601-617.
http://www.jstor.org/stable/2322213

[12] WALDSCHMIDT, M., *Quelques aspects transcendants de la théorie des nombres algébriques.* Cours de Troisième Cycle 1986/87, Publ. Math. Univ. P. et M. Curie (Paris VI), **89** 1989.
https://webusers.imj-prg.fr/~michel.waldschmidt/articles/pdf/QQATNT.pdf

[13] WALDSCHMIDT, M., *Topologie des points rationnels.* Cours de Troisième Cycle 1994/95, Preprint Univ. P. et M. Curie, 175 p.
https://webusers.imj-prg.fr/~michel.waldschmidt/articles/pdf/TPR.pdf

Michel WALDSCHMIDT
Sorbonne Universités
UPMC Univ Paris 06
UMR 7586 IMJ-PRG
Institut de Mathématiques de Jussieu-Paris Rive Gauche
F – 75005 Paris, France
michel.waldschmidt@imj-prg.fr
http://webusers.imj-prg.fr/~michel.waldschmidt

http://ricerca.mat.uniroma3.it/users/valerio/hochiminh16.html