August 1, 2016

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

The Abdus Salam International Centre for Theoretical Physics

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

Lattices and geometry of numbers

Michel Waldschmidt
Université Pierre et Marie Curie (Paris 6) France
http://www.imj-prg.fr/~michel.waldschmidt/

Update: 04/08/2016

Part I: August 1, 2016

- Subgroups of $\mathbb{R}^n$: discrete, closed, dense
- Topological groups
- Lattices
- Fundamental parallelepiped, covolume, determinant
- Packing, covering, tiling
- Sublattices
- Subgroup of $\mathrm{Hom}_{\mathbb{R}}(\mathbb{R}^n, \mathbb{R})$ associated with a subgroup of $\mathbb{R}^n$

Part II: August 3, 2016

- Convex sets and star bodies
- Minkowski's convex body Theorem
- Minkowski's theorems on linear forms
- Gauge functions
- Minkowsk's theorems on successive minima

Part III: August 5, 2016

Examples of lattices in number theory

- Minima of quadratic forms
- Sum of two squares
- Sum of four squares
- Primes of the form $x^2 + ny^2$
- Discriminant of a number field
- Units of a number field: Dirichlet's Theorem
- Geometry of numbers and transcendence

Subgroups of $\mathbb{R}$

Theorem 1 (Kronecker).
Let θ be an irrational number. Then $\mathbb{Z} + \mathbb{Z}\theta$ is dense in $\mathbb{R}$.

Lemma 2.
A subgroup of $\mathbb{R}$ is either discrete or dense.

Lemma 3.
The closed subgroups of $\mathbb{R}$ are $\mathbb{R}$ and the discrete subgroups generated by one element (including $\{0\}$).

Topological groups

Topological group: group G with a topology for which the maps

$$\begin{array}{ccc} G \times G & \to & G \\ (x,y) & \mapsto & xy \end{array} \quad \text{and} \quad \begin{array}{ccc} G & \to & G \\ x & \mapsto & x^{-1} \end{array}$$

are continuous ($G \times G$ is endowed with the product topology).

Examples:

$$\mathbb{R}, \;\; \mathbb{Z}, \;\; \mathbb{C}, \;\; \mathbb{R}/\mathbb{Z}, \;\; \mathbb{R}^\times, \;\; \mathbb{R}^\times_+, \;\; \mathbb{U} = \{z \in \mathbb{C}^\times \mid |z| = 1\}.$$

Isomorphisms:

$$\mathbb{R} \simeq \mathbb{R}^\times_+, \quad \mathbb{U} \simeq \mathbb{R}/\mathbb{Z}, \quad \mathbb{R}^\times_+ \simeq \mathbb{R}^\times/\{\pm 1\}, \quad \mathbb{C}^\times \simeq \mathbb{R}^\times_+ \times \mathbb{U}.$$

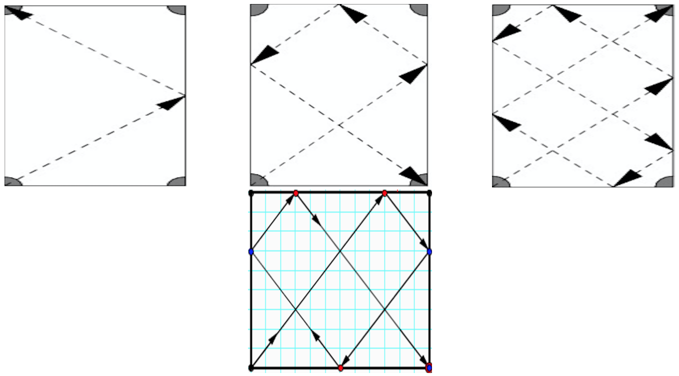
Character of a group G: continuous homomorphism $G \to \mathbb{U}$.

Subgroups of $\mathbb{R}/\mathbb{Z}$

From Lemma 2, we deduce:

Corollary 4.
A subgroup of $\mathbb{R}/\mathbb{Z}$ is either finite or dense.

Billiard problem



The orbit is either periodic or dense in the torus, depending on whether the tangent of the angle is rational or not.

The problem of the reflected ray

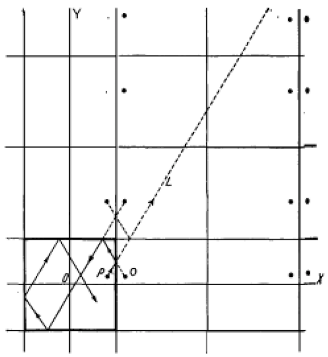


Fig. 10.

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

Subgroups of $\mathbb{R}^\times$

From Theorem 1, we deduce:

Corollary 5.

Let Γ be a finitely generated subgroup of $\mathbb{R}_+^\times$. Then the following conditions are equivalent.
(i) Γ is dense in $\mathbb{R}_+^\times$.
(ii) Γ has rank ≥ 2 over $\mathbb{Z}$.

Corollary 6.

Let Γ be a finitely generated subgroup of $\mathbb{R}^\times$. Then the following conditions are equivalent.
(i) Γ is dense in $\mathbb{R}^\times$.
(ii) Γ has rank ≥ 2 over $\mathbb{Z}$ and contains a negative real number.

Kronecker's Theorem

Theorem 7 (Kronecker).

Let θ be an irrational real number. For any $x \in \mathbb{R}$ and any $N > 0$ there exist n and k in $\mathbb{Z}$ with $n > N$ and

$$|x - k - n\theta| < \frac{3}{n}.$$

Hardy, G.H. & Wright, E.M, *An Introduction to the Theory of Numbers.* Fifth edition. The Clarendon Press, Oxford University Press, New York, 1979. See §23.2, Th. 440.

Dirichlet's Theorem

In the homogeneous case ($x = 0$), a stronger result is available.

Theorem 8 (Dirichlet).

Let θ be a real number. For any $Q \in \mathbb{R}$ with $Q > 1$ there exist p and q in $\mathbb{Z}$ with $1 \leq q < Q$ and

$$|q\theta - p| \leq \frac{1}{Q}.$$

Discrete subgroups of $\mathbb{R}^n$

Lemma 9.
A subgroup G of $\mathbb{R}^n$ is discrete in $\mathbb{R}^n$ if and only if there exists an open subset $\mathcal{U}$ of $\mathbb{R}^n$ containing 0 such that $G \cap \mathcal{U}$ is discrete.

Theorem 10.
Let $g_1, \ldots, g_\ell$ be $\mathbb{R}$–linearly independent elements in $\mathbb{R}^n$. Then the subgroup $\mathbb{Z}g_1 + \cdots + \mathbb{Z}g_\ell$ of $\mathbb{R}^n$ is discrete.
Conversely, if G is a discrete subgroup of $\mathbb{R}^n$, then there exist $\mathbb{R}$–linearly independent elements $g_1, \ldots, g_\ell$ in G such that $G = \mathbb{Z}g_1 + \cdots + \mathbb{Z}g_\ell$.

Auxiliary result

Lemma 11.
Let G be a discrete subgroup of $\mathbb{R}^n$ of real rank r. Let $e_1, \ldots, e_r$ be $\mathbb{R}$–linearly independent elements in G. Then $G' = \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_r$ is a subgroup of finite index in G.

Define

$$\overline{P} = \{x_1e_1 + \cdots + x_re_r \mid 0 \leq x_i \leq 1 \ (i = 1, \ldots, r)\}.$$

Then $G \cap \overline{P}$ is a finite set. For each $x \in G$ there exists $x' \in G'$ such that $x - x' \in G \cap \overline{P}$.

Submodules of finitely generated free $\mathbb{Z}$–modules

Proposition 12.
If G is a free finitely generated $\mathbb{Z}$–module and G' a submodule of G, then G' is free and finitely generated.

Theorem of the adapted basis

Theorem 13.
Let G be a discrete subgroup of $\mathbb{R}^n$ and G' a subgroup, $G' \neq 0$. There exists a basis $e_1, \ldots, e_r$ of G over $\mathbb{Z}$, an integer $m \geq 1$ and positive integers $a_1, \ldots, a_m$ such that
(i) $(a_1e_1, \ldots, a_me_m)$ is a basis of G' over $\mathbb{Z}$,
(ii) a_1 divides a_2, a_2 divides a_3, $\ldots$ and a_{m-1} divides a_m.

`Remark`: the a_i are called the *invariant factors*. This result is a special case of a theorem on the structure of modules over a principal ring (here: $\mathbb{Z}$).

Theorem of the adapted basis (matrix form)

Let n and p be positive integers, A a $n \times p$ matrix with coefficients in $\mathbb{Z}$ of rank $m \geq 1$. Then there exist a unique sequence of positive integers $\alpha_1, \alpha_2, \ldots, \alpha_m$, such that α_1 divides α_2, α_2 divides α_3, ... and α_{m-1} divides α_m, and there exist regular matrices $P \in \mathrm{GL}_n(\mathbb{Z})$ and $Q \in \mathrm{GL}_p(\mathbb{Z})$ such that

$$A = P \begin{pmatrix} \alpha_1 & & & & & & \\ & \alpha_2 & & & & & \\ & & \ddots & & & & \\ & & & \alpha_m & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{pmatrix} Q.$$

Definition of a lattice in $\mathbb{R}^n$

Given a subgroup G of $\mathbb{R}^n$, the following conditions are equivalent.
(i) There exists a basis $(e_1, \ldots, e_n)$ of the $\mathbb{R}$–vector space $\mathbb{R}^n$ such that $G = \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_n$.
(ii) G is a discrete subgroup of $\mathbb{R}^n$ of rank n.
(iii) G is a discrete subgroup of $\mathbb{R}^n$ such that $\mathbb{R}^n/G$ is compact.
(iv) G is a discrete subgroup of $\mathbb{R}^n$ which contains n elements linearly independent over $\mathbb{R}$.

Lattice = discrete subgroup of $\mathbb{R}^n$ of maximal rank.

Lattices in $\mathbb{R}^n$

Let G be a lattice in $\mathbb{R}^n$ and $\mathbf{e} = (e_1, \ldots, e_n)$ a basis of G. The **fundamental parallelepiped** associated to $\mathbf{e}$ is

$$\mathcal{P}_{\mathbf{e}} = \{x_1 e_1 + \cdots + x_n e_n \mid (x_1, \ldots, x_n) \in [0,1)^n\}.$$

Proposition 14.

$\mathcal{P}_{\mathbf{e}}$ is a fundamental domain for the action of G on $\mathbb{R}^n$ by translation.

This means:
(i) $0 \in \mathcal{P}_{\mathbf{e}}$.
(ii) $\mathcal{P}_{\mathbf{e}}$ is mesurable (the characteristic function is Riemann integrable)
(iii) $\mathbb{R}^n$ is the disjoint union of the sets $\mathcal{P}_{\mathbf{e}} + g$ for $g \in G$.

Determinant, covolume

Let G be a lattice in $\mathbb{R}^n$. To a basis $\mathbf{e} = \{e_1, \ldots, e_n\}$ of G we associate the parallelepiped

$$P_{\mathbf{e}} = \{x_1 e_1 + \cdots + x_n e_n \mid 0 \leq x_i < 1 \ (1 \leq i \leq n)\}$$

A change of bases of G is obtained with a matrix of determinant ± 1 with integer coefficients, hence
• The determinant of $\mathbf{e}$ in the canonical basis of $\mathbb{R}^n$ depends only on G, not on the choice of the basis $\mathbf{e}$. It is called the determinant of G and denoted by $\det(G)$.
• The Lebesgue measure $\mu(P_{\mathbf{e}})$ of $P_{\mathbf{e}}$ does not depend on $\mathbf{e}$: this number is called the *covolume* of the lattice G and is denoted by $v(G)$.
We have $\det(G) = v(G)$.

Packing, covering, tiling

Let K_i, $i \in I$ be a family of subsets of $\mathbb{R}^n$, where each K_i is the closure of a non empty open set U_i.

The family $(K_i)_{i\in I}$ is called *a packing* of $\mathbb{R}^n$ if the U_i are pairwise disjoint.

The family $(K_i)_{i\in I}$ is called *a covering* of $\mathbb{R}^n$ if the union of the K_i is $\mathbb{R}^n$.

The family $(K_i)_{i\in I}$ is called *a tiling* of $\mathbb{R}^n$ if it is both a packing and a covering.

If P is a fundamental parallelotope of a lattice G with closure $\overline{P}$, then the family $(\overline{P}+g)_{g\in G}$ is a tiling of $\mathbb{R}^n$.

Necessary conditions for covering and packing

Let G be a lattice in $\mathbb{R}^n$ of determinant $d(G)$ and let K be the closure of a non empty open set in $\mathbb{R}^n$.

If the G–translates of K are a covering of $\mathbb{R}^n$, then $\mu(K) \ge d(G)$.

If the G–translates of K are a packing of $\mathbb{R}^n$, then $\mu(K) \le d(G)$.

Coppel, W.A. *Number Theory. An introduction to mathematics*, Springer Verlag, 2009 . Part B, The Geometry of Numbers, pp. 327-362
`http://www.springer.com/gp/book/9780387894850`

Lattices and matrices

Let A be a regular $n\times n$ matrix with real coefficients and vector columns $a_1,\dots,a_n$. The set

$$A\mathbb{Z}^n = \{a_1x_1+\cdots+a_nx_n \mid x=(x_1,\dots,x_n)\in\mathbb{Z}^n\}$$

is a lattice in $\mathbb{R}^n$.

Let A_1 and A_2 be two non singular $n\times n$ matrices. Let $G_1 = A_1\mathbb{Z}^n$ and $G_2 = A_2\mathbb{Z}^n$. Then $G_2 \subset G_1$ if and only if there exists a regular $n\times n$ matrix with integer coefficients such that $A_2 = A_1P$.

Unimodular matrices

For a $n\times n$ matrix U with coefficients in $\mathbb{Z}$, the following conditions are equivalent:
(i) There exists a $n\times n$ matrix V with coefficients in $\mathbb{Z}$ such that $UV = VU = I_n$.
(ii) $\det U = \pm 1$.
Such a matrix is called *unimodular*. The group of unimodular matrices is denoted $\mathrm{GL}_n(\mathbb{Z})$.

If $e_1,\dots,e_n$ is a basis of the lattice G and if $f_1,\dots,f_n$ are elements in $\mathbb{R}^n$, then $f_1,\dots,f_n$ is a basis G if and only if there exists a unimodular matrix $(p_{ij})_{1\le i,j\le n}$ such that $f_i = p_{1i}e_1+\cdots+p_{ni}e_n \quad (i=1,\dots,n)$.

The two lattices $G_1 = A_1\mathbb{Z}^n$ and $G_2 = A_2\mathbb{Z}^n$ are the same if and only if $A_1^{-1}A_2$ is unimodular.

Sublattices

A sublattice of a lattice G is a subset G' of G which is also a lattice in $\mathbb{R}^n$. It is a subgroup of finite index in G.

There is a basis $e_1, \dots, e_n$ of G and positive integers $a_1, \dots, a_n$ such that $a_1 e_1, \dots, a_n e_n$ is a basis of G'.

$$(G : G') = a_1 \cdots a_n.$$

Further,

$$v(G') = (G : G')v(G).$$

Supplement

Given $v_1, \dots, v_\ell$ in $\mathbb{Z}^n$, does there exist $v_{\ell+1}, \dots, v_n$ such that $v_1, \dots, v_n$ is a basis of $\mathbb{Z}^n$ over $\mathbb{Z}$?

Proposition 15.

Let G be a discrete subgroup of $\mathbb{R}^n$ and G' a subgroup. The following conditions are equivalent.
(i) There exists a subgroup G'' of G such that $G = G' \oplus G''$.
(ii) The quotient group G/G' is torsion–free.
(iii) G' is saturated: $G' = G \cap (G' \otimes \mathbb{R})$.
(iv) The integers a_i in the Theorem of the adapted basis are all equal to 1.

Discrete subgroups of $\mathbb{R}^n$

Corollary 16.

Let $e_1, \dots, e_r$ be $\mathbb{R}$–linearly independent elements in $\mathbb{R}^n$ and $t_1, \dots, t_r$ be real numbers. Define $\theta = t_1 e_1 + \cdots + t_r e_r$. Then the subgroup $\mathbb{Z}e_1 + \cdots + \mathbb{Z}e_r + \mathbb{Z}\theta$ is discrete in $\mathbb{R}^n$ if and only if the numbers $t_1, \dots, t_r$ are all rational.

Corollary 17.

Let $t_1, \dots, t_n$ be real numbers. The following conditions are equivalent.
(i) For any $\epsilon > 0$, there exist integers $p_1, \dots, p_n, q$ with $q > 0$ such that

$$0 < \max_{1 \le i \le n} |qt_i - p_i| < \epsilon.$$

(ii) One at least of the numbers $t_1, \dots, t_n$ is irrational.
(iii) 0 is an accumulation point of $\mathbb{Z}^n + \mathbb{Z}(t_1, \dots, t_n)$.

Closed subgroups of $\mathbb{R}^n$

Theorem 18.

Let G be a closed subgroup of $\mathbb{R}^n$ of real rank r. There exists a maximal vector subspace V of $\mathbb{R}^n$ contained in G. If W is a vector subspace of $\mathbb{R}^n$ with $V \oplus W = \mathbb{R}^n$, then $\Gamma = W \cap G$ is a discrete subgroup of $\mathbb{R}^n$ and

$$G = V \oplus \Gamma.$$

Hence $G \simeq \mathbb{R}^r \times \mathbb{Z}^{\ell - r}$.

Lemma 19.

A closed subgroup of $\mathbb{R}^n$ which is not discrete contains a real line.

Kronecker's Theorem

Theorem 20 (Kronecker).

Let $\theta_1, \ldots, \theta_n$ be real numbers. The subgroup

$$\mathbb{Z}^n + \mathbb{Z}(\theta_1, \ldots, \theta_n) = \{(s_1 + s_0\theta_1, \ldots, s_n + s_0\theta_n) \mid (s_0, s_1, \ldots, s_n) \in \mathbb{Z}^{n+1}\}$$

of $\mathbb{R}^n$ is dense in $\mathbb{R}^n$ if and only if the $n+1$ numbers $1, \theta_1, \ldots, \theta_n$ are $\mathbb{Q}$–linearly independent.

Dense subgroups of $\mathbb{R}^n$

Proposition 21.

Let G be a finitely generated subgroup of $\mathbb{R}^n$. The following conditions are equivalent.
(i) G is dense in $\mathbb{R}^n$.
(ii) For any vector subspace V of $\mathbb{R}^n$ distinct from $\mathbb{R}^n$, we have

$$\mathrm{rank}_{\mathbb{Z}}(G/G \cap V) > \dim_{\mathbb{R}}(\mathbb{R}^n/V).$$

(iii) For any hyperplane H of $\mathbb{R}^n$, we have

$$\mathrm{rank}_{\mathbb{Z}}(G/G \cap H) \geq 2.$$

(iv) For any non–zero linear form $\varphi : \mathbb{R}^n \to \mathbb{R}$, we have $\varphi(G) \not\subset \mathbb{Z}$.
(v) For any non–trivial character $\chi : \mathbb{R}^n \to \mathbb{U}$, we have $\chi(G) \neq \{1\}$.

Dense subgroups of $\mathbb{R}^n$ (continued)

(vi) Let $g_1, \ldots, g_\ell$ be a set of generators of G as a $\mathbb{Z}$–module. Write the coordinates of g_j in the canonical basis of $\mathbb{R}^n$:

$$g_j = (g_{1,j}, \ldots, g_{n,j}) \quad (1 \leq j \leq \ell).$$

For any $(s_1, \ldots, s_\ell)$ in $\mathbb{Z}^\ell \setminus \{0\}$, the matrix

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

has rank $n+1$.

Subgroup of $\mathrm{Hom}_{\mathbb{R}}(\mathbb{R}^n, \mathbb{R})$ associated with a subgroup of $\mathbb{R}^n$

When G is a subgroup of $\mathbb{R}^n$, we set

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

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

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

Proposition 22.

Let G be a subgroup of $\mathbb{R}^n$. Let $\overline{G}$ be the topological closure of G in $\mathbb{R}^n$. Then

$$\overline{G} = (G^\star)^\star.$$

Subgroup of $\mathrm{Hom}_{\mathbb{R}}(\mathbb{R}^n, \mathbb{R})$ associated with a subgroup of $\mathbb{R}^n$

Lemma 23.
If G is a subgroup of $\mathbb{R}^n$, then $G^\star$ is a closed subgroup of $\mathrm{Hom}_{\mathbb{R}}(\mathbb{R}^n, \mathbb{R})$ and $(\overline{G})^\star = G^\star$.

Lemma 24.
Let G be a closed subgroup of $\mathbb{R}^n$. Let $e_1, \ldots, e_n$ be a basis of $\mathbb{R}^n$ such that

$$G = \mathbb{R}e_1 + \cdots + \mathbb{R}e_r + \mathbb{Z}e_{r+1} + \cdots + \mathbb{Z}e_\ell.$$

Let $f_1, \ldots, f_n$ be the dual basis of $e_1, \ldots, e_n$. Then

$$G^\star = \mathbb{Z}f_{r+1} + \cdots + \mathbb{Z}f_\ell + \mathbb{R}f_{\ell+1} + \cdots + \mathbb{R}f_n.$$