# GEOMETRY OF NUMBERS

## Slides A

## TOOL BOX

Tapani Matala-aho, Aalto University, 2022

# Abstract/Tool box

These slides form a tool box for the course Geometry of Numbers.

# References


- J.J. Rotman, Advanced Modern Algebra. Pearson 2002.
- J. Steuding, Diophantine analysis. Chapman & Hall/CRC, Boca Baton, 2005.
- Matala-aho T., A geometric face of Diophantine analysis, Diophantine Analysis, Trends in Mathematics, Springer, 2016, 129-174. Lecture notes given at Summer School for Master and PhD students in DIOPHANTINE ANALYSIS, Würzburg 2014.

# Number systems

$\mathbb{N} = \{0, 1, 2, \dots, GOOGOL^{10}, \dots\} = \{\text{non-negative integers}\}.$

$\mathbb{P} = \{2, 3, 5, 7, 11, \dots\} = \{\text{primes}\}.$

$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\} = \{\text{integers}\}.$

$\mathbb{Z}^+ = \{1, 2, 3, \dots\} = \mathbb{N}\backslash\{0\} = \{\text{positive integers}\}.$

$\mathbb{Z}^- = \{-1, -2, -3, \dots\} = \mathbb{Z}\backslash\mathbb{N} = \{\text{negative integers}\}.$

$\mathbb{Q} = \{\frac{m}{n} \mid m \in \mathbb{Z}, n \in \mathbb{Z}^+\} = \{\text{rational numbers}\}.$

# Number systems

$\mathbb{R} = \{x \mid x = \sum_{k=l}^{\infty} a_k 10^{-k},\ l \in \mathbb{Z};\ a_k \in \{0, \ldots, 9\}\} = \{\text{real numbers}\}.$

$\mathbb{C} = \mathbb{R}(i) = \{a + ib|\ a, b \in \mathbb{R}, i^2 = -1\} = \{\text{complex numbers}\}$

$\mathbb{C} \setminus \mathbb{Q} = \{\text{irrational numbers}\},\ \mathbb{R} \setminus \mathbb{Q} = \{\text{real irrational numbers}\}.$

$\mathbb{Z}_{\geq m} = \{k \in \mathbb{Z}|\ k \geq m\},\ \mathbb{R}_{<0} = \{r \in \mathbb{R}|\ r < 0\}, \ldots$

$\mathbb{Q}^* = \mathbb{Q} \setminus \{0\},\quad \mathbb{R}^* = \mathbb{R} \setminus \{0\},\quad \mathbb{C}^* = \mathbb{C} \setminus \{0\},$

# Miscellaneous notations

$\exists! \quad \Leftrightarrow \quad \exists$ exactly one.

$\#A = |A| =$ cardinality of the set $A$.

$B^t$ denotes the transpose of the matrix $B$.

$\underline{y} = (y_1, \ldots, y_n)$ denotes a row vector. While

$$\overline{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

denotes a column vector. Hence $\overline{x} = (x_1, \ldots, x_n)^t$.

# Binary relation

Let $A$ be a nonempty set. A binary operation denoted by $*$ is a mapping

$$* : A \times A \to A, \quad (a, b) \to a * b$$

meaning that $a * b \in A$, whenever $a \in A$ ja $b \in A$.

Particular cases:

multiplication denoted by $\cdot$

addition denoted by $+$

# Identity axioms

(a) $\forall\ a: \qquad a = a.$

(b) $\forall\ a_1, a_2, b_1, b_2: \quad a_1 = b_1,\ a_2 = b_2 \quad \Rightarrow \quad (a_1 = a_2 \ \Leftrightarrow\ b_1 = b_2).$

(c) $\forall\ a_1, a_2, b_1, b_2: \quad a_1 = b_1,\ a_2 = b_2 \quad \Rightarrow \quad a_1 * a_2 = b_1 * b_2.$

# Group

Let $G$ be a nonempty set with a multiplication

$$\cdot : G \times G \to G, \quad (a, b) \to a \cdot b.$$

# Group

## Definition 1

A pair $(G, \cdot)$ is a group, if the multiplication satisfies the following axioms:

# Group

## Definition 1

A pair $(G, \cdot)$ is a group, if the multiplication satisfies the following axioms:

(a) $a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad$ for all $a, b, c \in G$ (assosiativity).

# Group

## Definition 1

A pair $(G, \cdot)$ is a group, if the multiplication satisfies the following axioms:

(a) $a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad$ for all $a, b, c \in G$ (assosiativity).

(b) There exists an identity element $1 \in G$, satisfying

$1 \cdot a = a \cdot 1 = a \quad$ for all $a \in G$.

# Group

### Definition 1

A pair $(G, \cdot)$ is a group, if the multiplication satisfies the following axioms:

(a) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in G$ (assosiativity).

(b) There exists an identity element $1 \in G$, satisfying

$1 \cdot a = a \cdot 1 = a$ for all $a \in G$.

(c) For all $a \in G$ there exists an inverse $a^{-1} \in G$, satisfying

$a \cdot a^{-1} = a^{-1} \cdot a = 1.$

# Basics of equation manipulation

### Remark 1

*Let* $a, b \in G$*. By the identity axiom c we may multiply the identity*

$$a = b$$

*with the same element* $c \in G$*, whereupon*

$$ca = cb.$$

# Abelian group

In the case of commutative group an addition notation is widespread.

Let $A$ be a non-empty set with an addition

$$+ : A \times A \to A, \quad (a, b) \to a + b.$$

# Abelian group

## Definition 2

The couple $(A, +)$ is an Abelian group, if the addition satisfies the following axioms:

(a) $a + (b + c) = (a + b) + c \quad$ for all $a, b, c \in A$.

(b) $a + b = b + a \quad$ for all $a, b \in A$ (commutativity).

(c) There exists a zero-element $0 \in A$ satisfying

$0 + a = a \quad$ for all $a \in A$.

(d) For all $a \in A$ there exists an additive inverse $-a \in A$ satisfying

$a + (-a) = 0.$

# Basics of equation manipulation

**Remark 2**

*Let $A$ be an Abelian group and $a, b \in A$. By the indentity axiom c we may add the same element $c \in A$ to the both sides of the identity*

$$a = b$$

*whereupon*

$$a + c = b + c.$$

# Ring

Let $R$ be a non-empty set with an addition

$$+ : R \times R \to R, \quad (a, b) \to a + b,$$

and with a multiplication

$$\cdot : R \times R \to R, \quad (a, b) \to a \cdot b.$$

# Ring

## Definition 3

A triple $(R, +, \cdot)$, $\#R \geq 1$, is a ring, if the addition and multiplication satisfy the following axioms:

1. Addition axioms:

(a) $a + (b + c) = (a + b) + c$ for all $a, b, c \in R$.

(b) $a + b = b + a$ for all $a, b \in R$.

(c) There exits a zero-element $0 \in R$, satisfying

$0 + a = a$ for all $a \in R$.

(d) For all $a \in R$ there exists an additive inverse $-a \in R$ satisfying

$a + (-a) = 0.$

# Ring

2. Multiplication axioms:

(a) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in R$.

3. Distributive laws:

(a) $a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in R$.

(b) $(a + b) \cdot c = a \cdot c + b \cdot c$ for all $a, b, c \in R$.

Shortly: A ring $(R, +, \cdot)$ is an Abelian group $(R, +)$ satisfying 2. and 3.

# Ring with unity

## Definition 4

A triple $(R, +, \cdot)$, $\#R \geq 1$, is a ring with unity, if:

1. $(R, +)$ is an Abelian group.
2. 

(a) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in R$.

(b) There exists an identity element (unity) $1 \in R$ satisfying

$1 \cdot a = a \cdot 1 = a$ for all $a \in R$.

3. Distributive laws hold.

# Commutative ring with unity

## Definition 5

A triple $(R, +, \cdot)$, $\#R \geq 1$, is a commutative ring with unity, if:

1. $(R, +)$ is an Abelian group.

2.

(a) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in R$.

(b) $a \cdot b = b \cdot a$ for all $a, b \in R$.

(c) There exists an identity $1 \in R$ satisfying $1 \cdot a = a$ for all $a \in R$.

3.

(a) $a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in R$.

## Definition 6

A triple $(K, +, \cdot)$, $\#K \geq 2$, is a field, if the addition and multiplication satisfy the following axioms:

1. 1. Addition axioms:

(a) $a + (b + c) = (a + b) + c$ for all $a, b, c \in K$.

(b) $a + b = b + a$ for all $a, b \in K$.

(c) There exits a zero-element $0 \in K$, satisfying
$0 + a = a$ for all $a \in K$.

(d) For all $a \in K$ there exists an additive inverse $-a \in K$ satisfying
$a + (-a) = 0$.

2. Multiplication axioms:

(a) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in K$.

(b) $a \cdot b = b \cdot a$ for all $a, b \in K$.

(c) There exists an identity $1 \in K$ satisfying

$1 \cdot a = a$ for all $a \in K$.

(d) For all $a \in K^*$ there exists an inverse $a^{-1} \in K^*$, satisfying

$a \cdot a^{-1} = 1$.

3. Distributive law:

(a) $a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in K$.

SHORTLY: The triple $(K,+,\cdot)$, $\#K \geq 2$ is a field, if:

1. $(K,+)$ is an Abelian group (additive group),
2. $(K^*,\cdot)$ is an Abelian group (multiplicative group), $K^* = K\backslash\{0\}$.
3. $a(b+c) = ab + ac, \ \forall a, b, c \in K$.

In particular, a field is a commutative ring with unity.

Further, $0, 1 \in K$, $0 \neq 1$.

# Module

### Definition 7

Let $R$ be a commutative ring with an identity element $1 \in R$. Then

$$(M, +, \cdot)$$

is an *$R$-module*, if

1. $(M, +)$ is an Abelian group

and

# Module

the scalar product

$$\cdot : R \times M \to M$$

satisfies the following axioms

2.

(a) $1 \cdot m = m$.

(b) $(rs) \cdot m = r \cdot (s \cdot m)$.

(c) $(r + s) \cdot m = r \cdot m + s \cdot m$.

(d) $r \cdot (m + n) = r \cdot m + r \cdot n$.

for all $r, s \in R,\ m, n \in M$. The elements of $R$ are called scalars.

# Module, linear hull

Let $M$ be an $R$-module. Linear hull generated by $m_1, ..., m_k \in M$ is defined by

$$\langle m_1, ..., m_k \rangle_R := Rm_1 + ... + Rm_k = \{r_1 m_1 + \ldots + r_k m_k | \; r_1, \ldots, r_k \in R\}. \tag{1}$$

Let

$$M = \langle m_1, ..., m_n \rangle_R,$$

where $m_1, ..., m_n$ are linearly independent over $R$, then the rank of $M$ is defined by

$$\text{rank}_R \; M := n. \tag{2}$$

In this case $M$ is called finitely generated.

# Module, Cartesian product

## Example 8

Let $R$ be a ring and $n \in \mathbb{Z}^+$. In the Cartesian product

$$R^n := R \times \ldots \times R = \{\overline{x} = (x_1, \ldots, x_n) |\ x_1, \ldots, x_n \in R\}$$

we set standard identity relation, addition and scalar product by

$$\overline{x} = \overline{y} \quad \Leftrightarrow \quad x_i = y_i \quad \forall\ i = 1, ..., n;$$

$$\overline{x} + \overline{y} = (x_1 + y_1, ..., x_n + y_n);$$

$$r \cdot \overline{x} = (rx_1, ..., rx_n)$$

for $\overline{x} = (x_1, \ldots, x_n), \overline{y} = (y_1, \ldots, y_n) \in R^n$ and $r \in R$.

# Cartesian product

Then

$$(R^n, +, \cdot)$$

is an $R$-module and $\operatorname{rank}_R R^n = n$.

Example 9

Let $K$ be a field. From Example 8 we know $(K^n, +, \cdot)$ equipped with standard operations is an $K$-module and $\operatorname{rank}_K K^n = n$.

From linear algebra we know $(K^n, +, \cdot)$ is a $K$-vector space and $\dim_K K^n = n$.

## $R$-map

### Definition 10

Let $M$ and $N$ be $R$-modules. A mapping $f : M \to N$ satisfying

$$\begin{aligned} f(a \cdot m) &= a \cdot f(m), \quad \forall\, a \in R, m \in M; \\ f(m+n) &= f(m) + f(n), \quad \forall\, m, n \in M, \end{aligned} \tag{3}$$

is called an $R$-map or an $R$-homomorphism.

### Example 11

Let $K$ be a field and $M$ and $N$ be linear spaces over $K$. Then a $K$-homomorphism $f : M \to N$ is called a linear map.

# Isomorphism

## Definition 12

Let $M$ and $N$ be $R$-modules. A bijective $R$-map $f : M \to N$ is called an isomorphism. If there exists an isomorphism $f : M \to N$, then $M$ and $N$ are isomorphic denoted by $M \cong N$.

## Definition 13

Let $M$ be a finitely generated $R$-module. If there exist a $k \in \mathbb{Z}_{\geq 1}$ such that

$$M \cong R^k, \tag{4}$$

then $M$ is a free module.

# Linear form

Let $R$ be a ring. A linear form is a first degree homogeneous polynomial

$$L\overline{x} = L(x_1, \ldots, x_n) = \alpha_1 x_1 + \ldots + \alpha_n x_n$$

in $n$ variables $x_1, \ldots, x_n$, where the coefficients $\alpha_1, \ldots, \alpha_n \in R$.

The linear forms

$$L_i\overline{x} = \alpha_{i,1} x_1 + \ldots + \alpha_{i,n} x_n, \quad i = 1, \ldots, k,$$

are called linearly independent over $R$, if the vectors

$(\alpha_{1,1}, \ldots, \alpha_{1,n})^t, \ldots, (\alpha_{k,1}, \ldots, \alpha_{k,n})^t$ are linearly independent over $R$.

# Vector $p$-norms

Let $p \in \mathbb{R}^+$. The $p$-norm or the $\ell_p$-norm is defined by

$$\|\overline{x}\|_p := \left( \sum_{k=1}^{n} |x_k|^p \right)^{1/p},$$

where $\overline{x} = (x_1, ..., x_n)^t \in \mathbb{C}^n$.

# Vector norms

For the different norms of the vector $\overline{x} = (x_1, ..., x_n)^t \in \mathbb{C}^n$ we shall use the notations

$$\|\overline{x}\|_\infty = \max_{k=1,\dots,n} |x_k|,$$
$$\|\overline{x}\|_1 = \sum_{k=1}^{n} |x_k|,$$
$$\|\overline{x}\|_2 = \|\overline{x}\| = \left(\sum_{k=1}^{n} |x_k|^2\right)^{1/2},$$

where the first is the maximum norm, the middle is the taxicap or sum norm and the last is the usual Euclidean norm.

# Matrix norms

Let $A = (a_{ij}) \in M_{m\times h}(\mathbb{C})$. we shall use the notations

$$\|A\|_\infty = \max_{i=1,\ldots,m;j=1,\ldots,h} |a_{ij}|,$$
$$\|A\|_1 = \sum_{i=1,\ldots,m;j=1,\ldots,h} |a_{ij}|,$$
$$\|A\|_2 = \left( \sum_{i=1,\ldots,m;j=1,\ldots,h} |a_{ij}|^2 \right)^{1/2},$$

where the first is maximum norm, the middle is the sum norm and the last is the Frobenius norm (or Euclidean norm).

# Matrix norms

Let $A = (a_{ij}) \in M_{m\times h}(\mathbb{C})$ and $B = (b_{ij}) \in M_{h\times n}(\mathbb{C})$. Then the sum norm and the Frobenius norm are compatible with the usual matrix product, meaning

$$\begin{aligned} \|A\cdot B\|_1 &\le \|A\|_1 \cdot \|B\|_1, \\ \|A\cdot B\|_2 &\le \|A\|_2 \cdot \|B\|_2. \end{aligned} \tag{5}$$