INSA de Rouen

STPI - SIB

Module M2:

"Elementary algebraic structures and geometry"

Lecture notes

Vladimir Salnikov,
vladimir.salnikov@insa-rouen.fr
with active participation of

Maria Bermudez, Celia Fontenelle, Morgan Ridel, Jorge Ochoa

The goal of this course is twofold. On the one hand we will discuss some basic algebraic and geometric notions that constitute some minimal knowledge necessary for continuing your studies in INSA, does not matter if you plan to do pure or applied mathematics, information technology, physics or any other science. On the other hand (and even more important) we will profit from these basic objects to understand the internal logic of mathematics: the way from definitions to general statements via proofs, the way from abstract generalizable notions to concrete examples, the way from vague analogies to well-defined similarities.

The course is mostly self-consistent and does not need any special preliminary knowledge, though we will rediscover/redefine some things that you ~~were supposed to~~ did learn in high school, but we will consider them, probably from a somewhat different angle.

Some of the topics in these lecture notes (especially in the first half) are not mandatory for the M2 module: they are given either to simplify the understanding of appropriate notions in the next semesters or for general culture. These parts will be marked in blue. Each section will be followed by a list of typical exercises that are useful to check your understanding of the material.

Contents

0 Complex Numbers

The M2 module traditionally starts with complex numbers. In this section we will construct the theory of complex numbers "from scratch". We will have to admit only one trigonometric formula that will be proven in the next section, otherwise the presentation is self consistent.

0.1 Definition of arithmetic operations

Definition 0.1 *(Formal) A* $\underline{\textit{complex number}}$ *is an ordered couple of real numbers* (x, y).
On the set of complex numbers $\mathbb{C}$ *two binary operations are defined:*
$\underline{\textit{Addition}}$ $+\colon \mathbb{C} \times \mathbb{C} \to \mathbb{C}$; *If* $z_1 = (x_1, y_1), z_2 = (x_2, y_2)$, *then* $z_1 + z_2 := (x_1 + x_2, y_1 + y_2)$
$\underline{\textit{Multiplication}}$ $\cdot\colon \mathbb{C} \times \mathbb{C} \to \mathbb{C}$; *If* $z_1 = (x_1, y_1), z_2 = (x_2, y_2)$, *then* $z_1 \cdot z_2 := (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1)$

Proposition 0.1 *Properties of these operations:* $\forall z_1, z_2, z_3 \in \mathbb{C}$

- *Commutativity of addition:* $z_1 + z_2 = z_1 + z_2$ *and multiplication:* $z_1 \cdot z_2 = z_2 \cdot z_1$
- *Associativity of addition:* $z_1 + (z_2 + z_3) = (z_1 + z_2) + z_3$ *and multiplication:* $z_1 \cdot (z_2 \cdot z_3) = (z_1 \cdot z_2) \cdot z_3$
- *Distributivity of multiplication over addition:* $z_1 \cdot (z_2 + z_3) = z_1 \cdot z_2 + z_1 \cdot z_3$

Proof. Direct computation using the definition □

Existence of zero: $\underline{\text{Zero}}$ is an identity element with respect to addition:
$\exists 0 \in \mathbb{C} : \forall z \in \mathbb{C} \quad z + 0 = 0 + z = z.$
This permits to define the additive inverse
$\forall z \in \mathbb{C} \quad \exists(-z) \in \mathbb{C} : z + (-z) = (-z) + z = 0.$ $0 = (0, 0)$. If $z = (x, y), -z = (-x, -y)$.
This permits to define the $\underline{\text{subtraction}}$ $z_1 - z_2 = z_1 + (-z_2)$

Existence of a unity: $\underline{\text{Unity}}$ is an identity element w.r.t multiplication:
$\exists 1 \in \mathbb{C} : \forall z \in \mathbb{C} \quad z \cdot 1 = 1 \cdot z = z.$
This permits to define the multiplicative inverse
$\forall z \in \mathbb{C} \quad \exists(z^{-1}) \in \mathbb{C} : z \cdot (z^{-1}) = (z^{-1}) \cdot z = 1.$
$1 = (1, 0)$. If $z = (x, y), z^{-1} = (\frac{x}{x^2 + y^2}, \frac{-y}{x^2 + y^2})$.
This permits to define the $\underline{\text{division}}$ $\frac{z_1}{z_2} = z_1 \cdot z_2^{-1} = z_2^{-1} \cdot z_1$.

Remark 0.1 *All these properties hold for* $\mathbb{Q}$ *and* $\mathbb{R}$ *as well (up to formulas).*

Two characteristic features of complex numbers:

- There is no natural order on $\mathbb{C}$, i.e $z_1 = z_2$ is defined but $z_1 > z_2$, $z_1 < z_2$ for generic $z_1, z_2 \in \mathbb{C}$ is not.
- Existence of imaginary unity: $\exists$ an element $z \in \mathbb{C}$ such that $z^2 = -1$; $z = (0, 1)$

0.2 Algebraic model of complex numbers

Denote $i = (0, 1)$ then $i^2 = -1$.
$$\mathbb{C} \ni (x, y) \leftrightarrow \underbrace{x + iy = z.}_{\text{algebraic form of complex number}}$$
The real part $\Re\mathrm{e}(z) = x$, the imaginary part $\Im\mathrm{m}(z) = y$
This is compatible with the operations $+, -, \cdot, /$ if we consider them as acting on polynomials in i modulo the relation $i^2 = -1$

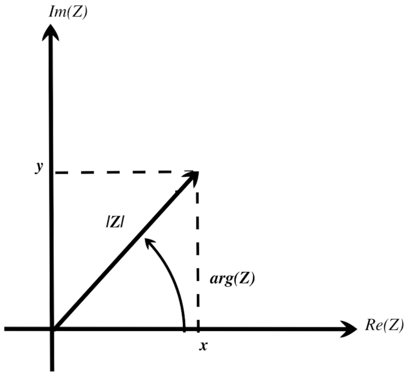
Example 0.1 *For* $z_1 = x_1 + iy_1$, $z_2 = x_2 + iy_2$
$z_1 \cdot z_2 = (x_1 + iy_1)(x_2 + iy_2) = x_1x_2 + iy_1x_2 + ix_1y_2 - y_1y_2 = x_1x_2 - y_1y_2 + i(y_1x_2 + x_1y_2)$

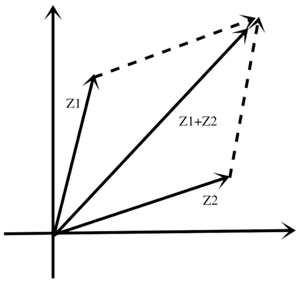
Definition 0.2 *The complex conjugate of* $z = x + iy$ *is* $\bar{z} = x - iy$

Remark 0.2 $z = \bar{z}$ *then* z *is real*

0.3 Geometric model of complex numbers

To each complex number $z = (x, y)$ we associate a vector in $\mathbb{R}^2$ with coordinates $\begin{pmatrix} x \\ y \end{pmatrix}$. The addition is just the usual addition of vectors in $\mathbb{R}^2$: $\overrightarrow{(x_1, y_1)} + \overrightarrow{(x_2, y_2)} = \overrightarrow{(x_1 + x_2, y_1 + y_2)}$





Definition 0.3 *Modulus of a complex number* $|z|$ *is the length of the corresponding vector in* $\mathbb{R}^2$

Definition 0.4 *Argument of a complex number* $arg(z)$ *is the oriented angle between the corresponding vector and the abscissa axis*

Proposition 0.2 *For* $z = x + iy$
$arg(z)$ *satisfies:*

$$\begin{cases} x &= |z|cos(arg(z)) \\ y &= |z|sin(arg(z)) \end{cases}$$

"Proof": The statement follows from the properties of the length in $\mathbb{R}^2$ and the definition of sin and cos with the trigonometric circle.

Definition 0.5 *The trigonometric form of complex numbers* $z = x + iy = r(\cos(\gamma) + i\sin(\gamma))$, *such that* $r \geq 0$,$\gamma \in [0, 2\pi[$

Proposition 0.3 $\forall z_1, z_2 \in \mathbb{C}: \quad |z_1 \cdot z_2| = |z_1||z_2|$; $arg(z_1) \cdot z_2 = arg(Z_1) + arg(z_2)$

Proof: Write z_1 and z_2 in the trigonometric form:
$z_1 = r_1(\cos(\gamma_1 + i\sin\gamma_1))$, $z_2 = r_2(\cos(\gamma_2 + i\sin\gamma_2))$.

$$\begin{aligned} z_1 \cdot z_2 &= r_1(\cos\gamma_1 + i\sin\gamma_1) \cdot r(\cos\gamma_2 + i\sin\gamma_2) \\ &= r_1r_2(\cos\gamma_1\cos\gamma_2 + i\sin\gamma_2\cos\gamma_1 + i\sin\gamma_1\cos\gamma_2 - \sin\gamma_1\sin\gamma_2) \\ &= r_1r_2(\cos(\gamma_1 + \gamma_2) + i\sin(\gamma_1 + \gamma_2)) \end{aligned}$$

Remark 0.3 $\gamma_1 + \gamma_2$ *need not belong to* $[0, 2\pi[$

Corollary 0.1 *For* $n \in \mathbb{N}$

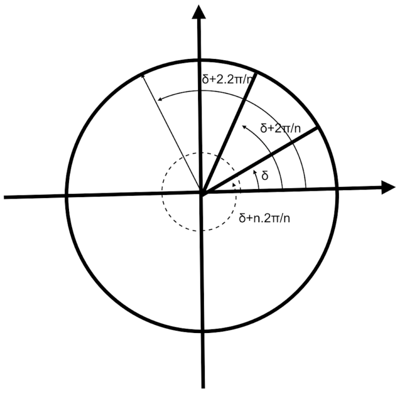
1). For $z \neq 0$ $|z^{-1}| = \frac{1}{|z|}$, $arg(z^{-1}) = -arg(z)$

2). $|z^n| = |z|^n$, $arg(z^n) = n\, arg(z)$

3). $z^n = w \neq 0$ *admits* n *distinct solutions in* $\mathbb{C}$.
By definition these solutions are called n-th roots of w.

Proof.
1). By definition $z^{-1} \cdot z = 1$
In view of the proposition $|z^{-1}||z| = |1| = 1$; $arg(z^{-1}) + arg(z) = arg(1) = 0$.
2). By induction (recurrence proof).
3). $z^n = w \Leftrightarrow \begin{cases} |z|^n = |w| \\ n\, arg(z) = arg(w) + 2\pi k, \quad k \in \mathbb{Z} \end{cases} \Leftrightarrow \begin{cases} |z| = \sqrt[n]{|w|} \\ arg(z) = \frac{arg(w)}{n} + \frac{2\pi k}{n} \end{cases}$

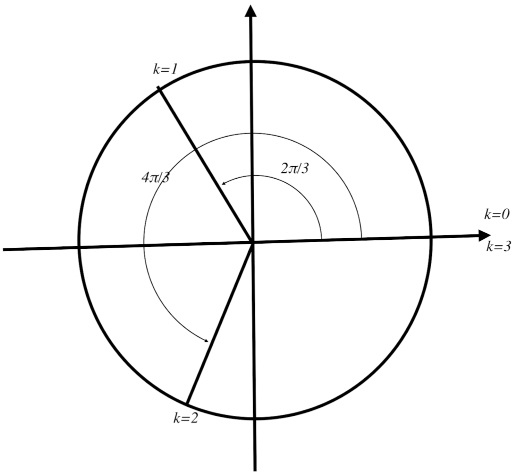
$$
\begin{aligned}
&n\delta = \omega \\
&n(\delta + \tfrac{2\pi}{n}) = n\delta + 2\pi = \omega + 2\pi \\
&n(\delta + \tfrac{2\pi \cdot 2}{n}) = \omega + 4\pi \\
&\dots \\
&n(\delta + \tfrac{2\pi n}{n}) = \omega + n2\pi
\end{aligned}
$$



Example 0.2 $z^3 = 1 \Leftrightarrow \begin{cases} |z|^3 = 1 \\ arg(z) = \frac{2\pi k}{3}, k \in \mathbb{Z} \end{cases}$

The solutions are:

$$
\begin{cases}
\omega_{3,0} = 1 \\
\omega_{3,1} = -\frac{1}{2} + i\frac{\sqrt{3}}{2} \\
\omega_{3,2} = -\frac{1}{2} - i\frac{\sqrt{3}}{2}
\end{cases}
$$



Definition 0.6 *Exponential form of complex numbers (Moivre's formula):* $e^{i\gamma} = \cos\gamma + i\sin\gamma$.
A complex number with modulus equal to 1 *and argument equal to* γ *is often denoted by* $e^{i\gamma}$.

For the moment we view it as a notation. In fact it is related to the Taylor series of exp, cos, sin.

Remark 0.4 *Because of the proposition 0.3, $e^{i\gamma}$ satisfies the usual property of exponential:* $e^a \cdot e^b = e^{a+b}$

Exercises.

1. Given a complex number in some form, cast it into algebraic/trigonometric/exponential form.
2. Choose the convenient form of a complex number to perform addition/subtraction/multiplication/division and explain the geometric meaning of the result.
3. Find *all* the solutions of the equation $z^n = w$ in $\mathbb{C}$, depict them on the complex plane.
4. Describe the set of points on the plane given by a condition on complex numbers.
5. Deduce the formulas for trigonometric functions of multiple angles.

1 Geometry of $\mathbb{R}^2$ and $\mathbb{R}^3$

In this long section we will introduce most of the geometric objects and notions that are necessary in the course. We will always give general definitions that you will review in the next semester, but the main examples will be $\mathbb{R}^2$ and $\mathbb{R}^3$.

1.1 Linear spaces

Definition 1.1 *A $\underline{\text{vector space}}$ $\underline{\text{(linear space)}}$ over $\mathbb{R}$ is a non empty set V with two operations:*

$$\begin{array}{ll} +: V \times V \to V & \cdot : \mathbb{R} \times V \to V \\ \vec{v}, \vec{w} \mapsto \vec{v} + \vec{w} & \alpha, \vec{v} \mapsto \alpha \cdot \vec{v} \end{array}$$

satisfying the axioms: $\forall u, v, w \in V$, $\forall \alpha, \beta \in \mathbb{R}$
(we will omit the arrow above vectors when it does not lead to a confusion)

1. $v+w = w+v$
2. $v+(w+u)=(v+w)+u$
3. $\exists\ \vec{0} \in V : \forall v \in V \quad v + \vec{0} = \vec{v}$
4. $\exists(-v)\in V$, $v+(-v)=\vec{0}$
5. $\alpha \cdot (\beta \cdot v) = (\alpha\beta) \cdot v$
6. $\alpha(v+w) = \alpha v + \alpha w$
7. $1 \cdot v = v$
8. $(\alpha+\beta)v=\alpha v + \beta v$

Example 1.1 $\{\vec{0}\}$ *is a vector space*

Example 1.2 $\mathbb{R}^2$ *with component-wise addition and multiplication by real numbers*

Definition 1.2 *A $\underline{\text{norm}}$ is a $\underbrace{\underline{\text{mapping}}}_{v\mapsto||v||}$ $V\to\mathbb{R}$ satisfying :*

- $\forall\ v\ ||v||\geq 0$ *and* $||v|| = 0 \Rightarrow v = \vec{0}$
- $||\alpha \cdot v||=|\alpha|\ ||v||$
- $||v + w|| \leq ||v|| + ||w||$

Example 1.3 *In* $\mathbb{R}^2 = \{(x,y)\}$, $||(x,y)|| = \sqrt{x^2+y^2}$

Definition 1.3 *A real-valued scalar product is a mapping* $V\times V \to \mathbb{R}$
$v, w \mapsto (v,w)$ *(other notations:* $<v,w>$, $v \cdot w$*), which is*

- *linear* $(\alpha v+\beta w,u) = \alpha(v,u)+\beta(w,u)$
- *symmetric* $(v,w) = (w,v)$
- *positive definite* $(v,v) \geq 0$ *and if* $(v,v) = 0$ *then* $v = \vec{0}$

Proposition 1.1 *A scalar product always induces a norm* $||v|| = \sqrt{(v,v)}$.
For a real-valued scalar product $(v,w) = \frac{1}{2}(||v+w||^2 - ||v||^2 - ||w||^2)$.

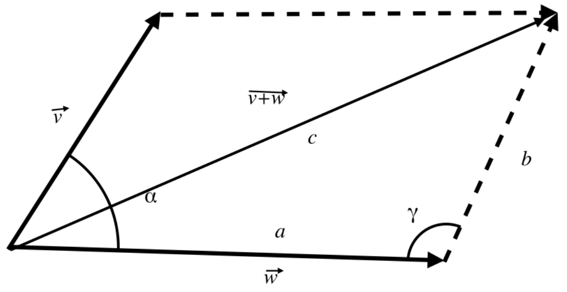
Proof. The axioms for (v,v) repeat exactly the axioms for the norm, up to the triangular inequality, that follows from isolating a perfect square. (This is true even for complex-valued scalar products). The other way around: for a real valued $(\cdot,\cdot)$ let us compute

$$\frac{1}{2}(||v+w||^2 - ||v||^2 - ||w||^2) = \frac{1}{2}\left((v+w,v+w) - (v,v) - (w,w)\right) =$$
$$= \frac{1}{2}\left((v,v) + (w,w) + (v,w) + (w,v) - (v,v) - (w,w)\right) = (v,w)$$

Example 1.4 *In* $\mathbb{R}^2$ $||v|| = \sqrt{v_x^2 + v_y^2}$

$$(v,w) = \frac{1}{2}\left[(v_x+w_x)^2 + (v_y+w_y)^2 - (v_x^2+v_y^2) + (w_x^2+w_y^2)\right] =$$
$$= \frac{1}{2}[2v_xw_x + 2v_yw_y] = v_xw_x + v_yw_y$$

Remark 1.1 *On the following picture consider the triangle formed by* $\vec{v}, \vec{w}$ *and* $\vec{v}+\vec{w}$.



If we apply the cosine law to it we obtain $c^2 = a^2 + b^2 - 2ab\cos\gamma$ *which is equivalent to* $||v+w||^2 = ||w||^2 + ||v||^2 + 2||v||\,||w||\cos\alpha$. *Compare it with the result of the proposition 1.1 – we see that the scalar product can be computed using the "high-school" formula:* $(v,w) = ||v||\,||w||\cos\alpha$ *and on the other hand with the formula that we have proven in the example 1.4:*
$(v,w) = v_xw_x + v_yw_y$. *We can use any of them depending on the problem, moreover we have now filled the gap in the proof of the formula for* $\cos(\alpha - \beta)$ *(cf. tutorial 0).*

Definition 1.4 *Let* $(V, ||.||_v)$ *be a normed vector space, them a mapping* $f\colon V \to V$ *such that* $||f(v)|| = ||v||, \forall v \in V$ *is called an isometry.*

Exercise. Describe the isometries $\mathbb{R}^2 \to \mathbb{R}^2$.

1.2 Dimension and linear subspaces

Definition 1.5 *Consider $W \subseteq V$, W is a linear subspace of V (sub-vector space) if W is non-empty and is itself a vector space with respect to the same operations as V.*
It means that $\forall \alpha_1, \alpha_2 \in \mathbb{R}$, $\forall w_1,\ w_2 \in W$, $\alpha_1 w_1 + \alpha_2 w_2 \in W$ as well.

Example 1.5 *$V = \mathbb{R}^2$ any line passing through $\vec{0}$ is a linear subspace. Any other line is not.*

Example 1.6 *$\mathbb{R}^2$ is a linear subspace of itself.*
$\left\{\vec{0}\right\}$ is a linear subspace of any linear subspace.

Definition 1.6 *Consider $v_1, ..., v_m \in V$ $\alpha_1, ..., \alpha_m \in \mathbb{R}$. A vector $v = \alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_m v_m$ is called a linear combination of $v_1 ... v_m$ with coefficients $\alpha_1 ... \alpha_m$.*

Definition 1.7 *The vectors $v_1, ..., v_m$ are called linearly independent if from $\alpha_1 v_1 + ... + \alpha_m v_m = \vec{0}$, it follows that $\alpha_1 = ... = \alpha_m = 0$*

Example 1.7 *In $\mathbb{R}^2$, two vectors are linearly independent if and only if they are not collinear.*
In $\mathbb{R}^3$, three vectors are linearly independent $\Leftrightarrow$ they are not coplanar.

Definition 1.8 *V is a linear span of $v_1, ..., v_m$ if any $v \in V$ can be expressed as a linear combination of $v_1, ..., v_m$.*

Theorem 1.1 ***(Without proof.)*** *The maximal number of linearly independent vectors in V does not depend on the choice of these vectors.*

Definition 1.9 *The number from theorem 1.1 is called the dimension of V*

Definition 1.10 *The set of linearly independent vectors that span the whole space V is called a basis. And the number of vectors in a basis is the dimension of V.*

Remark 1.2 *Theorem 1.1 + definitions above $\Rightarrow$ the dimension doesn't depend on the choice of a basis.*

Example 1.8 *In $\mathbb{R}^2 = \left\{\begin{pmatrix} x \\ y \end{pmatrix}\right\}$, the vectors $e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ are linearly independent.*
Indeed, if $\vec{0} = \alpha_1 e_1 + \alpha_2 e_2 = \alpha_1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \alpha_2 \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix}$, thus $\alpha_1 = \alpha_2 = 0$.
$\mathbb{R}^2$ is a span e_1, e_2. Indeed, any $v = \begin{pmatrix} x \\ y \end{pmatrix} = x e_1 + y e_2$. x, y are then called the coordinates of v in the basis e_1, e_2.

Exercise : Write explicitly the same thing in $\mathbb{R}^3 = \left\{\begin{pmatrix} x \\ y \\ z \end{pmatrix}\right\}$.

Example 1.9 *$\mathbb{C}$ can be viewed as a real vector space of dimension 2.*
Indeed, Take $e_1 = 1 \in \mathbb{C}$, $e_2 = i \in \mathbb{C}$, $\forall z \in \mathbb{C}$, $z = a \cdot 1 + b \cdot i$; $(a, b) \in \mathbb{R}^2$

1.3 Linear mappings

Consider V and W – vector spaces.

Definition 1.11 *A mapping* $f\colon V \to W$ *is called linear if*
$\forall v_1, v_2 \in V$, $\forall \alpha_1, \alpha_2 \in \mathbb{R}$
$f(\alpha_1 v_1 + \alpha_2 v_2) = \alpha_1 f(v_1) + \alpha_2 f(v_2)$.

Example 1.10 *(Trivial)*
V=$\mathbb{R}$, W=$\left\{\vec{0}\right\}$ *; f(v)=*$\vec{0}$ *is linear.*
V=$\mathbb{R} = \{x\}$, W=$\mathbb{R} = \{y\}$ *: any linear mapping is of the form* $y = f(x) = kx$

Example 1.11 *Interesting examples are mappings* $\mathbb{R}^2 \to \mathbb{R}^2$ *and* $\mathbb{R}^3 \to \mathbb{R}^3$

Linear mappings $\mathbb{R}^2 \to \mathbb{R}^2$

In the above definitions fix $V = \mathbb{R}^2$, $W = \mathbb{R}^2$

If $v = \alpha_1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \alpha_2 \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ then $f(v) = f\left(\alpha_1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \alpha_2 \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right)$
$= \alpha_1 f\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \alpha_2 f\begin{pmatrix} 0 \\ 1 \end{pmatrix}$

Denote $f\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} a_{11} \\ a_{21} \end{pmatrix}$ and $f\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} a_{12} \\ a_{22} \end{pmatrix}$.

Definition 1.12 $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ *is called the* <u>*matrix of the linear mapping*</u> f *in the basis* e_1, e_2.

Exercise: Let $v = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ and f be given by A. Compute $f(v)$.

Let g be given by B=$\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$. Compute $f(g(v))$

Correction. $f(v) = x_1 f\begin{pmatrix} 1 \\ 0 \end{pmatrix} + x_2 f\begin{pmatrix} 0 \\ 1 \end{pmatrix} = x_1 \begin{pmatrix} a_{11} \\ a_{21} \end{pmatrix} + x_2 \begin{pmatrix} a_{12} \\ a_{22} \end{pmatrix} = \begin{pmatrix} a_{11}x_1 + a_{12}x_2 \\ a_{21}x_1 + a_{22}x_2 \end{pmatrix} \quad (*)$

Definition 1.13 *In* $\mathbb{R}^2$ *for* $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ *and* $v = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$, *the* <u>*matrix-vector product*</u> $A \cdot \vec{v}$ *is defined by* $(*)$

Remark 1.3 *A way to remember the explicit formula* $(*)$ $A\vec{v} = \begin{pmatrix} \overrightarrow{1^{st} \textit{ line of } A} \cdot \vec{v} \\ \overrightarrow{2^{nd} \textit{ line of } A} \cdot \vec{v} \end{pmatrix}$, *where "$\cdot$" denotes the scalar product in* $\mathbb{R}^2$.

Consider now the composition of two linear mappings $f : \mathbb{R}^2 \longmapsto \mathbb{R}^2$; $g : \mathbb{R}^2 \longmapsto \mathbb{R}^2$
$f \circ g : \mathbb{R}^2 \to \mathbb{R}^2$, $v \longmapsto f(g(v))$

Proposition 1.2 $f \circ g$ *is a linear mapping.*

Proof. $(f \circ g)(\alpha v + \beta w) = f(g(\alpha v + \beta w)) = f(\alpha g(v) + \beta g(w)) = \alpha f(g(v)) + \beta f(g(w))$.

Let us compute the columns of the matrix C associated to $f \circ g$.

$$f\left(g\begin{pmatrix}1\\0\end{pmatrix}\right) = f\begin{pmatrix}b_{11}\\b_{21}\end{pmatrix} = \begin{pmatrix}a_{11}b_{11}+a_{12}b_{21}\\a_{21}b_{11}+a_{22}b_{21}\end{pmatrix},$$

$$f\left(g\begin{pmatrix}0\\1\end{pmatrix}\right) = f\begin{pmatrix}b_{12}\\b_{22}\end{pmatrix} = \begin{pmatrix}a_{11}b_{12}+a_{12}b_{22}\\a_{21}b_{12}+a_{22}b_{22}\end{pmatrix}.$$

$$C = \begin{pmatrix}a_{11}b_{11}+a_{12}b_{21} & a_{11}b_{12}+a_{12}b_{22}\\a_{21}b_{11}+a_{22}b_{21} & a_{21}b_{12}+a_{22}b_{22}\end{pmatrix}$$

Definition 1.14 *In $\mathbb{R}^2$, C is called the <u>matrix-matrix product</u> of the matrices A and B.*

Remark 1.4 *A way to remember:* $C = \begin{pmatrix}\overrightarrow{1^{st}\ line\ of\ A}\cdot\overrightarrow{1^{st}\ column\ of\ B} & \overrightarrow{1^{st}\ line\ of\ A}\cdot\overrightarrow{2^{nd}\ column\ of\ B}\\ a_{11}b_{11}+a_{12}b_{21} & a_{11}b_{12}+a_{12}b_{22}\\ a_{21}b_{11}+a_{22}b_{21} & a_{21}b_{12}+a_{22}b_{22}\\ \overrightarrow{2^{nd}\ line\ of\ A}\cdot\overrightarrow{1^{st}\ column\ of\ B} & \overrightarrow{2^{nd}\ line\ of\ A}\cdot\overrightarrow{2^{nd}\ column\ of\ B}\end{pmatrix}.$

Remark 1.5 *In the generic case:* $A \cdot B \neq B \cdot A$

Remark 1.6 *One can define linear mappings $\mathbb{R}^m \to \mathbb{R}^n$, using $\underset{\#of\,lines}{n} \times \underset{\#of\,columns}{m}$ matrices. One can compose them and define the product of the respective matrices if the sizes match.* $f \circ g : \mathbb{R}^m \xrightarrow{g} \mathbb{R}^n \xrightarrow{f} \mathbb{R}^k$

Exercise. Consider linear mapping $\mathbb{R}^3 \longmapsto \mathbb{R}^3$

1. Define the matrix $(3 * 3)$
2. Define $A \cdot \vec{v}$
3. Define $A \cdot B$

Linear mappings $\mathbb{R}^3 \to \mathbb{R}^3$

Consider a linear mapping $f\colon \mathbb{R}^3 \to \mathbb{R}^3$. Choose a basis of $\mathbb{R}^3$:

$$e_1 = \begin{pmatrix}1\\0\\0\end{pmatrix},\ e_2 = \begin{pmatrix}0\\1\\0\end{pmatrix},\ e_3 = \begin{pmatrix}0\\0\\1\end{pmatrix}.$$

Denote $\quad f(e_1) = \begin{pmatrix}a_{11}\\a_{21}\\a_{31}\end{pmatrix},\ f(e_2) = \begin{pmatrix}a_{12}\\a_{22}\\a_{32}\end{pmatrix},\ f(e_3) = \begin{pmatrix}a_{13}\\a_{23}\\a_{33}\end{pmatrix}.$

Consider $v = \begin{pmatrix}x_1\\x_2\\x_3\end{pmatrix} = x_1e_1 + x_2e_2 + x_3e_3$. By linearity,

$$f(v) = x_1f(e_1)+x_2f(e_2)+x_3f(e_3) = \begin{pmatrix}a_{11}x_1+a_{12}x_2+a_{13}x_3\\a_{21}x_1+a_{22}x_2+a_{23}x_3\\a_{31}x_1+a_{32}x_2+a_{33}x_3\end{pmatrix} =: \begin{pmatrix}a_{11}&a_{12}&a_{13}\\a_{21}&a_{22}&a_{23}\\a_{31}&a_{32}&a_{33}\end{pmatrix}\cdot\begin{pmatrix}x_1\\x_2\\x_3\end{pmatrix}$$

This defines a <u>product</u> $A \cdot v$ of a matrix $A = \begin{pmatrix}a_{11}&a_{12}&a_{13}\\a_{21}&a_{22}&a_{23}\\a_{31}&a_{32}&a_{33}\end{pmatrix}$ and a vector $v = \begin{pmatrix}x_1\\x_2\\x_3\end{pmatrix}$.

Defining a linear mapping $\mathbb{R}^3 \to \mathbb{R}^3$ is thus equivalent to fixing a basis and giving a 3×3 matrix.

Consider now another linear mapping $g\colon \mathbb{R}^3 \to \mathbb{R}^3$ given by a matrix $B = \begin{pmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{pmatrix}$.

By the same argument as in $\mathbb{R}^2$ their composition $f \circ g(\cdot) = f(g(\cdot))$ is linear.

$$f(g(v)) = A \cdot (B \cdot v) = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \cdot \begin{pmatrix} b_{11}x_1 + b_{12}x_2 + b_{13}x_3 \\ b_{21}x_1 + b_{22}x_2 + b_{23}x_3 \\ b_{31}x_1 + b_{32}x_2 + b_{33}x_3 \end{pmatrix} =$$

$$= \begin{pmatrix} a_{11}(b_{11}x_1 + b_{12}x_2 + b_{13}x_3) + a_{12}(b_{21}x_1 + b_{22}x_2 + b_{23}x_3) + a_{13}(b_{31}x_1 + b_{32}x_2 + b_{33}x_3) \\ a_{21}(b_{11}x_1 + b_{12}x_2 + b_{13}x_3) + a_{22}(b_{21}x_1 + b_{22}x_2 + b_{23}x_3) + a_{23}(b_{31}x_1 + b_{32}x_2 + b_{33}x_3) \\ a_{31}(b_{11}x_1 + b_{12}x_2 + b_{13}x_3) + a_{32}(b_{21}x_1 + b_{22}x_2 + b_{23}x_3) + a_{33}(b_{31}x_1 + b_{32}x_2 + b_{33}x_3) \end{pmatrix} =$$

$$= \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} + a_{13}b_{31} & a_{11}b_{12} + a_{12}b_{22} + a_{13}b_{32} & a_{11}b_{13} + a_{12}b_{23} + a_{13}b_{33} \\ a_{21}b_{11} + a_{22}b_{21} + a_{23}b_{31} & a_{21}b_{12} + a_{22}b_{22} + a_{23}b_{32} & a_{21}b_{13} + a_{22}b_{23} + a_{23}b_{33} \\ a_{31}b_{11} + a_{32}b_{21} + a_{33}b_{31} & a_{31}b_{12} + a_{32}b_{22} + a_{33}b_{32} & a_{31}b_{13} + a_{32}b_{23} + a_{33}b_{33} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$$

The last line is $(A \cdot B) \cdot v$ and thus provides a definition of a product $A \cdot B$ of two 3×3 matrices.

Some particular cases

Exercise. Consider $\mathbb{R}^2 \longmapsto \mathbb{R}^2$ as vector spaces.
What are linear isometries $\mathbb{R}^2 \longmapsto \mathbb{R}^2$?
Hints. Reminder. Linear $f(\alpha v + \beta w) = \alpha f(v) + \beta f(w)$. Isometry: $\|f(v)\| = \|v\|$

Remark 1.7 *Translation (parallel transport) is not linear.*
Fix $\vec{w}$; $f(\vec{v}) := \vec{v} + \vec{w}$
If linear: $f(\vec{v_1} + \vec{v_2}) = f(\vec{v_1}) + f(\vec{v_2}) = \vec{v_1} + \vec{w} + \vec{v_2} + \vec{w}$.
In reality: $f(\vec{v_1} + \vec{v_2}) = \vec{v_1} + \vec{v_2} + \vec{w} \neq \vec{v_1} + \vec{w} + \vec{v_2} + \vec{w}$.

Proposition 1.3 *For a linear mapping $f(\vec{0}) = \vec{0}$*

Proof : $\vec{0} = f(\vec{0}) = f(2 \cdot \vec{0}) = 2 \cdot f(\vec{0}) \Rightarrow 2f(\vec{0}) = f(\vec{0}) \Leftrightarrow f(\vec{0}) = \vec{0}$

Fact: A linear isometry of $\mathbb{R}^2$ (as a vector space) is either a rotation around the origin or a reflection with respect to any line passing through the origin.

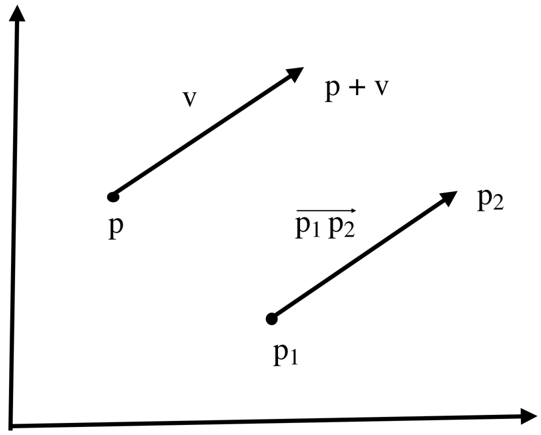
1.4 Spaces of points – affine spaces.

Definition 1.15 *An affine space is a set of points A together with an action of a vector space V on it. It means that there is an operation $+\colon A \times V \to A$,*
for $p \in A$ and $v \in V$, $\underset{point}{p}, \underset{vector}{v} \mapsto \underset{point}{p+v}$, satisfying:

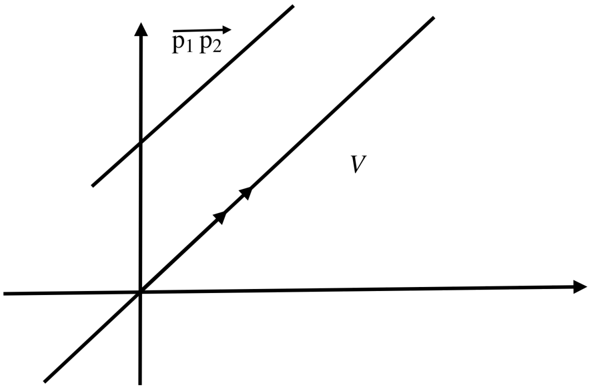
1. *$(p + v) + w = p + (v + w)$*
2. *$p + \vec{0} = p$*
3. *$\forall p_1, p_2 \in A, \exists! v \in V$ such that $p_2 = p_1 + v$. It is often denoted $\overrightarrow{p_1p_2}$.*

The dimension of the affine space A is equal to the dimension of the associated vector space V.

Example 1.12 $A = \mathbb{R}^2, V = \mathbb{R}^2$



Example 1.13 *$A =$ a line in $\mathbb{R}$, $V = 1$-dim linear subspace of $\mathbb{R}^2$ parallel to this line.*



Remark 1.8 *To define A it is sufficient to give a point in A and the vector space V. V is defined uniquely, but the choice of a point is not.*

Remark 1.9 *(Important) For a set $p_1 \dots p_m \in A$ and $\alpha_1 \dots \alpha_m \in \mathbb{R}$ the combination $\alpha_1 p_1 + \dots \alpha_m p_m$ does not have a geometric meaning in the generic case.*
But it does if $\alpha_1 + \alpha_2 + \dots \alpha_m = 1$

Definition 1.16 *For a set of points $p_1, \dots, p_m \in A$ and a set of coefficients $\alpha_1, \dots, \alpha_m \in \mathbb{R}$, such that $\alpha_1 + \alpha_2 + \dots \alpha_m = 1$, a point $p = \alpha_1 p_1 + \dots \alpha_m p_m$ is called a barycentric combination of $p_1, \dots, p_m$.*

Example 1.14 *Fix two points on a line – any point of this line can be represented as a barycentric combination of these two. Fix three non-collinear points in a plane – any point of this plane can be represented as a barycentric combination of these three. These decompositions are related to the geometric interpretation of the center of masses.*

Definition 1.17 *The points $p_1, \dots, p_m$ are called affinely independent if non of them is a barycentric combination of the others. If any point in A can be expressed as a barycentric combination of* *the points $p_1, \dots, p_m$, these points are called a barycentric basis of A; and the coefficients of the decomposition are called barycentric coordinates.*

Remark 1.10 *For an affine space of dimension n any set of $n+1$ affinely independent points in it forms its barycentric basis.*

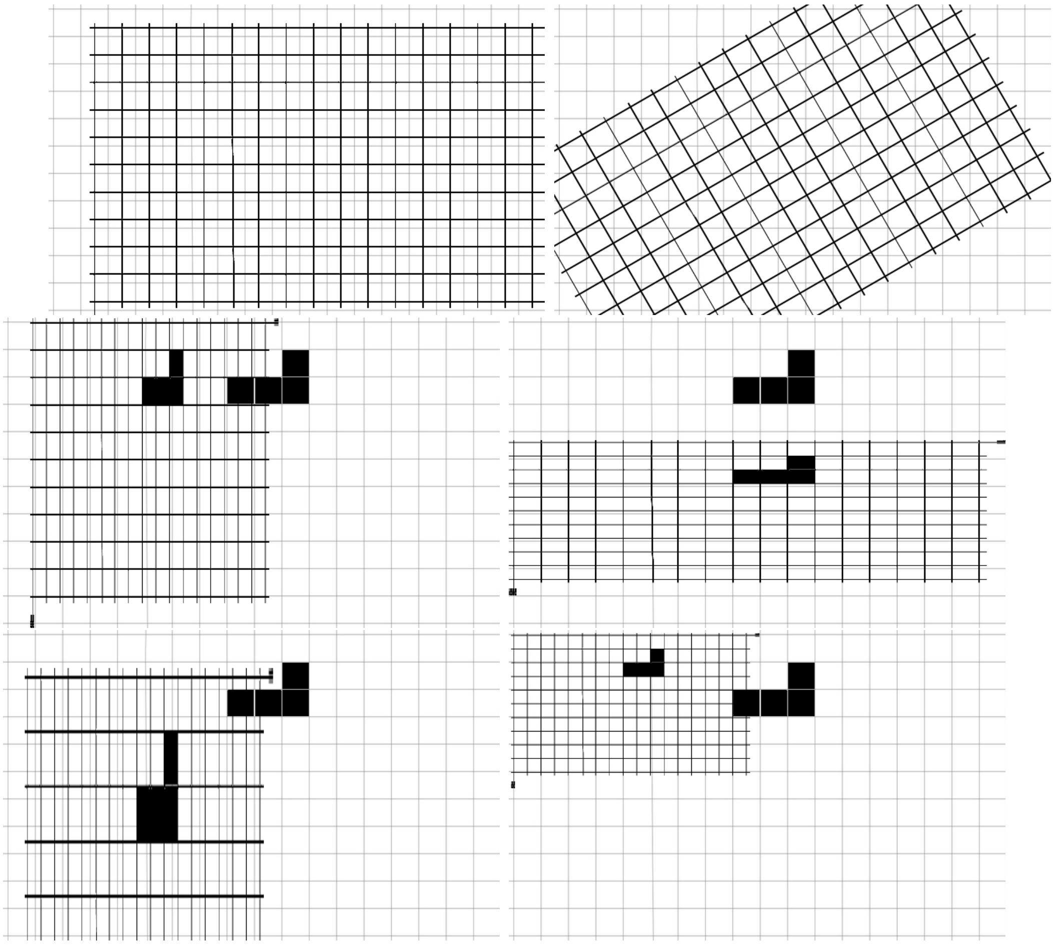
Definition 1.18 *(Formal) An affine mapping $f \colon A \to A$ is a mapping such that $\forall p_1, p_2 \in A$ $f(p_1) - f(p_2) = \varphi(p_1 - p_2)$, where φ is a linear mapping $V \to V$.*

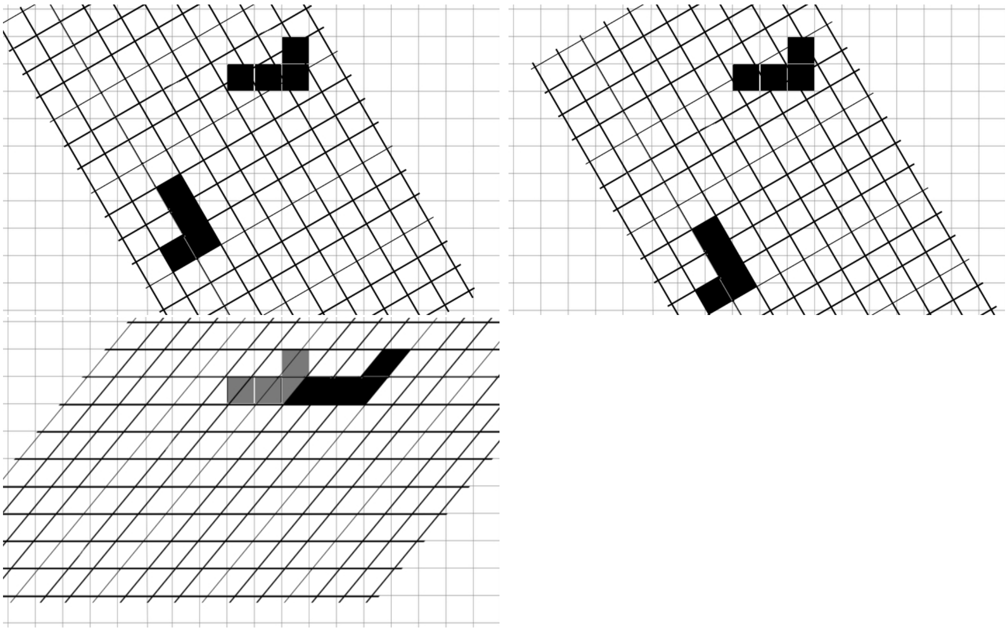
Remark 1.11 *f is affine if it maps lines to lines, planes to planes... This property is sometimes used as a definition.*

We will be interested in a subclass of affine mappings.

Definition 1.19 *A similarity transformation of A satisfies $d(f(p_1), f(p_2)) = kd(p_1, p_2)$, where $d(\cdot, \cdot)$ denotes the distance between points in A, and $k \in \mathbb{R}$.*

Example 1.15 *(Exercise) Below are the pictures of the coordinate grid after several mappings. Choose affine mappings and similarity transformations.*





Theorem 1.2 *(Chasles) Any similarity transformation in $\mathbb{R}^2$ belongs to one of the following classes:*

- *A shift (parallel transport)*
- *A rotational homothety (a composition of a rotation and homothety with the same center)*
- *A sliding symmetry (a reflection symmetry w.r.t. a line and a shift along this line) composed with a homothety with a center on the axis of symmetry.*

Idea of the proof. Consider the set of fixed points – there can be none, exactly one, a line or the whole space, moreover a line can be preserved as a set of points. Then consider the corresponding "building blocks" from tutorial 2, exercise 2.

Remark 1.12 *The similarity transformations of the first two types are orientation preserving, they are described by the mappings $\mathbb{C} \to \mathbb{C}$ of the form $z \mapsto az + b$. The similarity transformations of the third type are orientation reversing, they are described by the mappings $\mathbb{C} \to \mathbb{C}$ of the form $z \mapsto a\bar{z} + b$.*

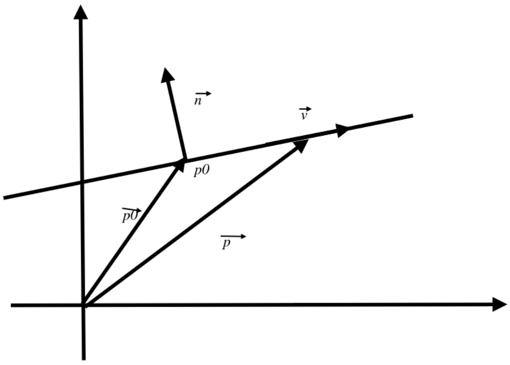
Definition 1.20 *An affine subspace of a vector space W is a couple A, V, (where A is a set of points and V is a linear subspace of W), such that any point $p \in A$ can be recovered in the form $p_0 + \vec{v}$ for a fixed point $p_0 \in A$ and some vector $v \in V$.*

Remark 1.13 *It means that A is obtained from a linear subspace $V \subseteq W$ by a shift.*

Example 1.16 $\mathbb{W} = \mathbb{R}^2$ *– any straight line is an affine subspace of $\mathbb{R}^2$.* $\mathbb{W} = \mathbb{R}^3$ *– any straight line or a plane is an affine subspace of $\mathbb{R}^3$. We will turn to these examples in more details in the following sections.*

Definition 1.21 *For an affine subspace $\mathbb{A}$ of W given by $p_0 \in A$ and $V \subseteq W$,* $\dim A = \dim V$. *If* $\dim A = \dim W - 1$ *then A is called hyperplane of W*

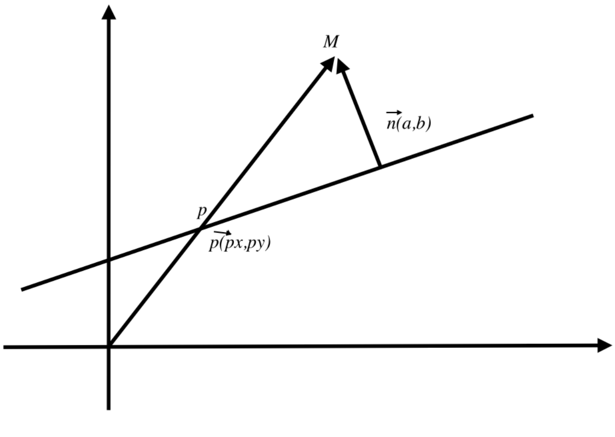
1.5 Straight lines in $\mathbb{R}^2$



Parametric description of L: $L = \{p_0 + \lambda \vec{v}\}$ where p_0 is a point on the line, $\vec{v}$ a direction vector of L and $\lambda \in \mathbb{R}$.

Consider this description in coordinates: $p = \begin{pmatrix} x \\ y \end{pmatrix}, p_0 \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$, and let $\vec{n}$ be a vector orthogonal to L: $\vec{n} \begin{pmatrix} n_x \\ n_y \end{pmatrix}$. $(\vec{p} - \vec{p_0}) \cdot \vec{n} = 0 \Rightarrow \vec{p} \cdot \vec{n} - \vec{p_0} \cdot \vec{n} = 0$, or in coordinates $xn_x + yn_y - (x_0 n_x + y_0 n_y) = 0$ – this gives the algebraic form (Cartesian form) of L: $ax + by + c = 0$

Consider now an arbitrary point $M = \begin{pmatrix} m_x \\ m_y \end{pmatrix} \in \mathbb{R}$ and compute the distance h from it to L.



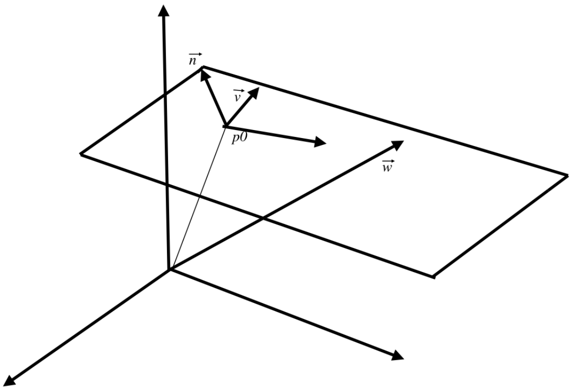
$$h = \frac{|\overrightarrow{PM} \cdot \vec{n}|}{||\vec{n}||} = \frac{\left| \begin{pmatrix} m_x - p_x \\ m_y - p_y \end{pmatrix} \cdot \begin{pmatrix} a \\ b \end{pmatrix} \right|}{\sqrt{a^2 + b^2}} = \frac{\left| \begin{pmatrix} m_x \\ m_y \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} - \begin{pmatrix} p_x \\ p_y \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} \right|}{\sqrt{a^2 + b^2}} = \frac{|am_x + bm_y + c|}{\sqrt{a^2 + b^2}}.$$

We have just proven the

Proposition 1.4 *For a line in $\mathbb{R}^2$ given by $ax + by + c = 0$ the distance from any point $M = \begin{pmatrix} m_x \\ m_y \end{pmatrix} \in \mathbb{R}^2$ to it is given by $h = \dfrac{|am_x + bm_y + c|}{\sqrt{a^2 + b^2}}$*

1.6 Planes in $\mathbb{R}^3$.

The parametric description of a plane P is given by $P = \{p_0 + \lambda\vec{v} + \mu\vec{w}\}$, $\vec{v}, \vec{w} \in \mathbb{R}^3, \lambda, \mu \in \mathbb{R}$. Following the scheme from before consider the description in coordinates:
$p = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$, $p_0 = \begin{pmatrix} x_0 \\ y_0 \\ z_0 \end{pmatrix}$ and the orthogonal vector $\vec{n} = \begin{pmatrix} a \\ b \\ c \end{pmatrix}$.
This gives: $(\vec{p} - \vec{p_0}) \cdot \vec{n} = 0 \Leftrightarrow \vec{p} \cdot \vec{n} = \vec{p_0} \cdot \vec{n}$.
Then the algebraic form (Cartesian form) of P is $ax + by + cz + d = 0$



Proposition 1.5 *For a plane in $\mathbb{R}^3$ given by $ax + by + cz + d = 0$ the distance from any point $M = \begin{pmatrix} m_x \\ m_y \\ m_z \end{pmatrix} \in \mathbb{R}^3$ to it is given by $h = \dfrac{|am_x + bm_y + cm_z + d|}{\sqrt{a^2 + b^2 + c^2}}$.*

Proof. (Exercise) The proof repeats exactly the scheme of the previous proposition about $\mathbb{R}^2$.

Remark 1.14 *Some computational hints:*
1) In $\mathbb{R}^2$ if $\vec{v} \begin{pmatrix} v_x \\ v_y \end{pmatrix}$ an orthogonal vector can be taken as $\vec{n} = \begin{pmatrix} v_y \\ -v_x \end{pmatrix}$
2) In $\mathbb{R}^3$ if $\vec{v} \begin{pmatrix} v_x \\ v_y \\ v_z \end{pmatrix}$ and $\vec{w} \begin{pmatrix} w_x \\ w_y \\ w_z \end{pmatrix}$ then an orthogonal vector $\vec{n} = \begin{pmatrix} v_y w_z - v_z w_y \\ -(v_x w_z - v_z w_x) \\ v_x w_y - v_y w_x 0 \end{pmatrix}$

Definition 1.22 *For $\vec{v}, \vec{w} \in \mathbb{R}^3$ the vector product (cross product) is given in coordinates (in a right basis) by $\vec{v} \times \vec{w} = \begin{pmatrix} v_y w_z - v_z w_y \\ -(v_x w_z - v_z w_x) \\ v_x w_y - v_y w_x \end{pmatrix}$. Other notations: $\vec{v} \wedge \vec{w}$, $[\vec{v}, \vec{w}]$.*

Proposition 1.6
1). $(\vec{v} \times \vec{w}) \perp \vec{v}$, $(\vec{v} \times \vec{w}) \perp \vec{w} = 0$
2). The direction of it is given by the right-hand rule (bottle open rule).
3). $|\vec{v} \times \vec{w}| = |\vec{v}||\vec{w}||\sin(\vec{v}; \vec{w})|$

Proof.
1). $\vec{v} \cdot \vec{v} \times \vec{w} = v_x(v_y w_z - v_z w_y) - v_y(v_x w_z - v_z w_x) + v_z(v_x w_y - v_y w_x) = v_x v_y w_z - v_x w_y v_z - v_x v_y w_z + w_x v_y v_z + v_x w_y v_z - w_x v_y v_z = 0$. Similarly for $\vec{w} \cdot \vec{v} \times \vec{w}$

2). This is more a fact about compatibility of conventions than a mathematical statement, we will however understand it in what follows talking about oriented volumes. The proof of 3). will follow from the next section as well.

1.7 Determinants and volumes

Definition 1.23 *In $\mathbb{R}^2$ the oriented area of a parallelogram formed by the vectors $\vec{v}$ and $\vec{w}$ is its geometric area with a sign $\pm$, where $+$ is chosen when the shortest rotation from $\vec{v}$ to $\vec{w}$ is counter clock-wise and $-$ if it is clock-wise.*
In $\mathbb{R}^3$ the oriented volume of a parallelogram formed by the vectors $\vec{u}$, $\vec{v}$ and $\vec{w}$ is its geometric volume with a sign $\pm$, where $+$ when $\vec{u}, \vec{v}, \vec{w}$ is a right triple and $-$ if it is a left one.

Definition 1.24 *The determinant of a 2×2 matrix is given by:* $\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$

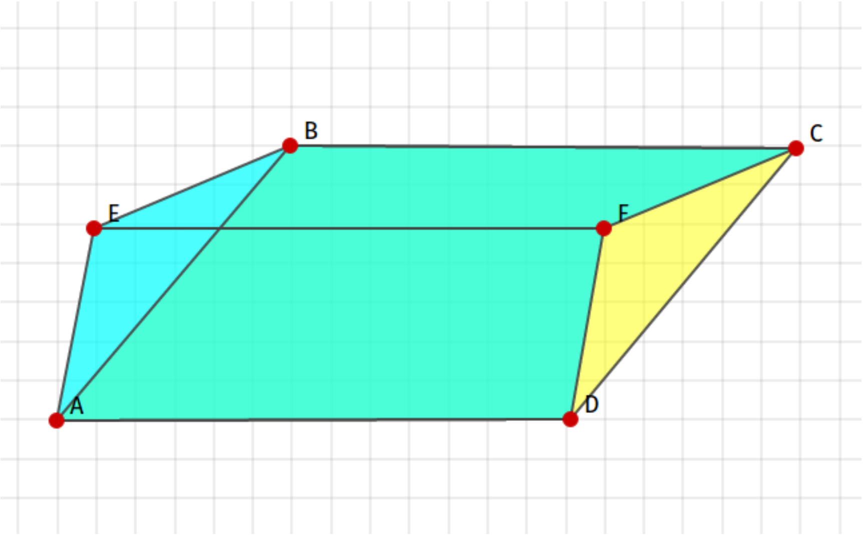
The determinant of a 3×3 matrix is given by: $\det \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = aei + bfg + dhc - ceg - bdi - afh$

These two definitions are related by the following.

Theorem 1.3
I. *Consider two vectors $\vec{v} = \begin{pmatrix} a \\ c \end{pmatrix}, \vec{w} = \begin{pmatrix} b \\ d \end{pmatrix}$. The (oriented) area of the parallelogram formed by $\vec{v}$ and $\vec{w}$ is equal to the determinant of the matrix constructed from these vectors as columns: $S(\vec{v}, \vec{w}) = \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} := ad - bc$.*

II. *Consider three vectors $\vec{u} = \begin{pmatrix} a \\ d \\ g \end{pmatrix}, \vec{v} = \begin{pmatrix} b \\ e \\ h \end{pmatrix}, \vec{w} = \begin{pmatrix} c \\ f \\ i \end{pmatrix}$. The (oriented) volume of the parallelepiped formed by $\vec{u}, \vec{v}$, and $\vec{w}$ is equal to the determinant of the matrix constructed from these vectors as columns: $V(\vec{u}, \vec{v}, \vec{w}) = \det \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} := aei + bfg + dhc - ceg - bdi - afh$.*

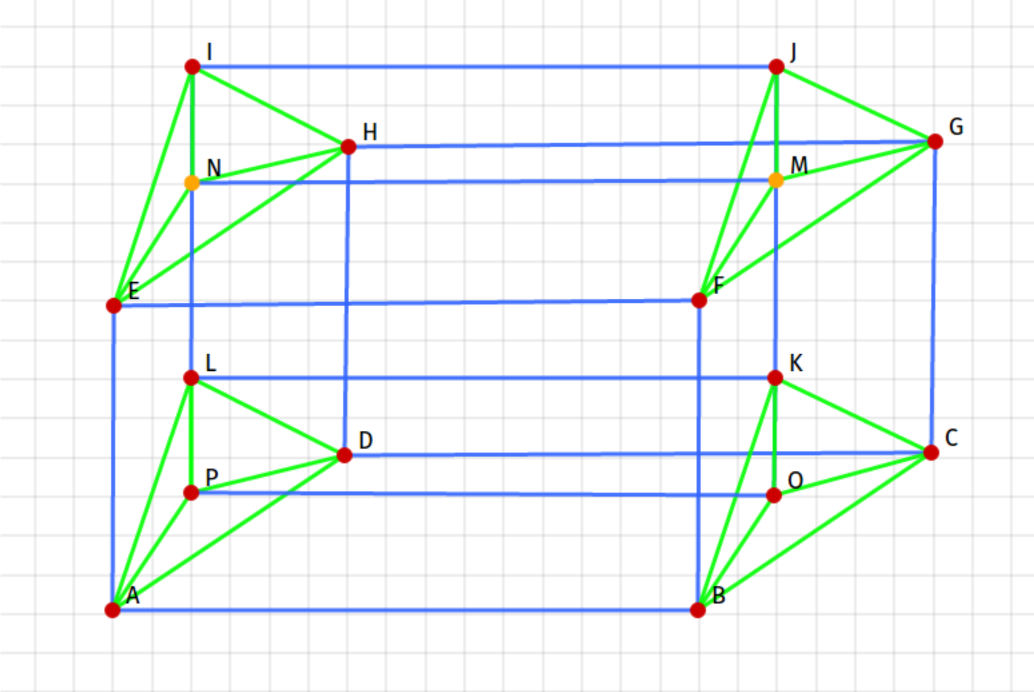
Proof of part I.
1). The (oriented) area can be viewed as a mapping $S\colon \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}$, which is bilinear, antisymmetric in its arguments, and is equal to 1 when computed on the canonical basis of $\mathbb{R}^2$. Because of antisymmetry, it is sufficient to check linearity for one argument. Clearly, $S(\alpha\vec{v}, \vec{w}) = \alpha S(\vec{v}, \vec{w})$. To prove the equality $S(\vec{u} + \vec{v}, \vec{w}) = S(\vec{u}, \vec{w}) + S(\vec{v}, \vec{w})$ consider the picture: $\vec{u} = \overrightarrow{AE}, \vec{v} = \overrightarrow{EB}, \vec{u} + \vec{v} = \overrightarrow{AB}$. The equality then means that $S_{ABCD} = S_{AEDF} + S_{EBCF}$, which is true, since $\triangle AEB = \triangle DFC$.



2). Consider now an arbitrary function S that satisfies the properties from 1). $S(v,w) = S(ae_1{+}ce_2, be_1{+}de_2) = S(ae_1, be_1{+}de_2){+}S(ce_2, be_1{+}de_2) = abS(e_1,e_1){+}adS(e_1,e_2){+}cbS(e_2,e_1){+}cdS(e_2,e_2) = ad-bc = \det\begin{pmatrix} a & b \\ c & d \end{pmatrix} := ad-bc$ □

Proof of part II.

1). The (oriented) volume can be viewed as a mapping $S\colon \mathbb{R}^3\times\mathbb{R}^3\times\mathbb{R}^3 \to \mathbb{R}$, which is trilinear, antisymmetric in its arguments, and is equal to 1 when computed on the canonical basis of $\mathbb{R}^3$. Because of antisymmetry, it is sufficient to check linearity for one argument. Clearly, $V(\alpha\vec{u},\vec{v},\vec{w}) = \alpha V(\vec{u},\vec{v},\vec{w})$. To prove the equality $V(\vec{u}_1{+}\vec{u}_2,\vec{v},\vec{w}) = V(\vec{u}_1,\vec{v},\vec{w}){+}V(\vec{u}_2,\vec{v},\vec{w})$ consider the picture: $\vec{u}_1 = \overrightarrow{AL}, \vec{u}_2 = \overrightarrow{LD}, \vec{u}_1+\vec{u}_2 = \overrightarrow{AD}$. The equality then means that $V_{ABCDEFGH} = V_{ABKLEFJI} + V_{LKCDIJGH}$. One notices immediately that the four tetrahedra ($ALDP$, $EIHN$, $FJGM$, $BKCO$) are equal. It is thus easy to see that all the parts that are added on the upper left to $ABCDEFGH$ possess equal parts that are cut out on the lower right.



2). Consider now an arbitrary function V that satisfies the properties from 1). $V(u,v,w) = V(ae_1 + de_2 + ge_3, be_1 + ee_2 + he_3, ce_1 + fe_2 + ie_3) = V(ae_1, ee_2 + he_3, fe_2 + ie_3) + V(de_2, be_1 + he_3, ce_1 + ie_3) + V(ge_3, be_1 + ee_2, ce_1 + fe_2) = aeiV(e_1,e_2,e_3) + ahfV(e_1,e_3,e_2) + dbiV(e_2,e_1,e_3) + dhcV(e_2,e_3,e_1) + gbfV(e_3,e_1,e_2) + gecV(e_3,e_2,e_1) = aei - ahf + dhc - dbi + gbf - gec =: \det \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$ □

Corollary 1.1 *Using the formula of the volume via the determinant we can prove the proposition 1.6.3)*

Proof. Consider $\vec{v} \begin{pmatrix} v_x \\ v_y \\ v_z \end{pmatrix}$ and $\vec{w} \begin{pmatrix} w_x \\ w_y \\ w_z \end{pmatrix}$ We know from the proposition 1.6.1) that the vector $\vec{v} \times \vec{w}$ is orthogonal to $\vec{v}$ and to $\vec{w}$. The area of the parallelogram formed by $\vec{v}$ and $\vec{w}$ is equal to $|\vec{v}||\vec{w}||\sin\angle(\vec{v},\vec{w})|$. Thus, the volume $|V(\vec{v},\vec{w},\vec{v}\times\vec{w})| = |\vec{v}||\vec{w}||\sin\angle(\vec{v},\vec{w})||\vec{v}\times\vec{w}|$. Let us compute it using the determinant formula: $V(\vec{v},\vec{w},\vec{v}\times\vec{w}) = \det \begin{pmatrix} v_yw_z - v_zw_y & v_x & w_x \\ -(v_xw_z - v_zw_x) & v_y & w_y \\ v_xw_y - v_yw_x & v_z & w_z \end{pmatrix} = (v_yw_z - v_zw_y)^2 + (v_xw_z - v_zw_x)^2 + (v_xw_y - v_yw_x)^2 = |\vec{v}\times\vec{w}|^2$. It means that $|\vec{v}\times\vec{w}|^2 = |\vec{v}\times\vec{w}||\vec{v}||\vec{w}||\sin\angle(\vec{v},\vec{w})| \quad \Rightarrow |\vec{v}\times\vec{w}| = |\vec{v}||\vec{w}||\sin\angle(\vec{v},\vec{w})|$. □

Exercises

1. Give an algebraic description of a given similarity transformation. Conversely, given the analytic description or some other information, situate the similarity transformation in view of the Chasles' theorem.
2. Compute the distances between points in $\mathbb{R}^2$ and $\mathbb{R}^3$, what is the relation to scalar product?
3. Given some information of a line or a plane, produce its algebraic or parametric description. Describe intersections of lines/planes.
4. Compute the distance from a point to a line/plane, compute the distance between lines/planes.
5. Compute the area of a polygon, the volume of a polyhedron.
6. Compute 2×2 and 3×3 determinant.
7. Check if given vectors are collinear/orthogonal/coplanar.

2 Abstract algebraic notions

This section is devoted to the definition of algebraic structures: groups, rings, fields, etc. We will see that a lot of familiar objects fit into some general framework. The advantage of this approach is that we can formalize the notion of objects that "look alike" (introducing morphisms) and profit from this similarity when solving concrete problems. Two important examples in this section are integer numbers and polynomial functions.

Let us start with an enigma:

Consider a set $\mathbb{E}$ and define a function $S : \mathbb{E} \mapsto \mathbb{E}$ that satisfies the following properties:

- $e \in \mathbb{E}$
- $x \in \mathbb{E} \Rightarrow S(x) \in \mathbb{E}$
- $\nexists x \in \mathbb{E} : S(x) = e$
- If $S(b) = a$ and $S(c) = a$ then $b = c$
- If $P(e)$ is true and $\forall x \; P(x) \Rightarrow P(S(x))$ then $\forall x \; P(x)$ is true.
  ($P(x)$ – some statement about elements of $\mathbb{E}$)

What can be this set $\mathbb{E}$ and the mapping S? The answer is given by the following:

Definition 2.1 *(Peano 1889) : A set of natural numbers $\mathbb{N}$ is defined by fixing the first element e, the mapping $S : \mathbb{N} \to \mathbb{N}(n \to n+1)$ with the properties :*

1. *$\nexists n \in \mathbb{N}$ such that $n + 1 = e$*
2. *If $S(n_1) = n$ and $S(n_2) = n$ then $n_1 = n_2$*
3. *The induction principle holds : if some statement P is true for $n = e$ and from $P(k)$ we can deduce $P(k+1)\forall k$, then P is true for all $n \in \mathbb{N}$*

Theorem 2.1 *(With a difficult proof using advanced mathematical analysis)*
These axioms define $\mathbb{N}$ uniquely (up to isomorphism). That is an absolutely abstract construction from the enigma above defines a very concrete object.

Remark 2.1 *There are 2 conventions that are often used : $e = 1$ or $e = 0$.*
The second choice $e = 0$ is related to set theory: $\emptyset \mapsto 0$, $\emptyset \cup \{1 \text{ element}\} \mapsto 1 = S(0)$.
Moreover, with $e = 0$, $\mathbb{N}$ becomes a semi-group with a neutral element.
This explains also a somewhat strange numbering of sections in this document.

Combinatorics.

Before going to real algebraic construction let us recall some notions from combinatorics that deal with $E = \{1, 2, 3, ..., n\} \subset \mathbb{N}$, and that are often used in exercises in particular related to induction.

- **Permutations** : the choice of the order in E.
  Number of permutations: $P_n = n! = n(n-1)(n-2)...1$
- **Multiplets of the elements of E** : k-tuples (couples, triples) $\underbrace{(x_1, x_2....x_k)}_{x_i \in E}$ with possible repetitions of elements. $A_n^k = n^k$
- **k-permutations of n elements** : $\{x_1, x_2, ...x_k\}$, $x_i \in E, x_i \neq x_j$ if $i \neq j$

  The number of them is $A_n^k = n(n-1)(n-2)...(n-k+1) = \frac{n!}{(n-k)!}$

- **Combinations** : $\{x_1, x_2, ...x_k\}$, $x_i \in E, x_i \neq x_j$ if $i \neq j$ and the order is not important. $\binom{n}{k} = C_n^k = \frac{A_n^k}{P_k} = \frac{n!}{(n-k)!k!}$

Remark 2.2 $\binom{n}{k}$ *(or C_n^k) are often called the binomial coefficients, because of the following:*

Proposition 2.1 *(Newton's binomial formula)* $(x+y)^n = \sum\limits_{k=0}^{n} C_n^k x^{n-k} y^k$

Proof (exo) : By induction using the property $C_n^k = C_{n-1}^k + C_{n-1}^{k-1}$ (Pascal triangle)

2.1 Group theory

Definition 2.2 *A set $\mathbb{G}$ is called a group if it is non-empty and equipped with a binary operation $\star : \mathbb{G} \times \mathbb{G} \to \mathbb{G}$ with the following properties:*

1. *Associativity: $\forall a, b, c \in \mathbb{G}$, $a \star (b \star c) = (a \star b) \star c$*
2. *Existence of a neutral element: $\exists e \in \mathbb{G} : \forall a \in \mathbb{G}, a \star c = e \star a = a$*
3. *Existence of an inverse element: $\forall a \in \mathbb{G} : \exists a^{-1_\star} \in \mathbb{G}, a^{-1_\star} \star a = a \star a^{-1_\star} = e$*

The subscript $\star$ at -1 in the third property is to stress that the inverse is understood with respect to the binary operation defined by $\star$. In what follows we will drop this subscript if it does not lead to a confusion.

Definition 2.3 *If in addition to the previous definition, $\forall a, b \in \mathbb{G}, a \star b = b \star a$, the group $\mathbb{G}$ is called abelian (commutative).*

Example 2.1 $\mathbb{G} \in \mathbb{Z}, \star = +$ *is an abelian group.*
$\mathbb{G} = \mathbb{Q} > 0, \star = \times$
$\mathbb{G} = \mathbb{R}, \star = +$
$\mathbb{G} = \mathbb{R}/\left\{0\right\}, \star = \times$

Example 2.2 $\mathbb{G}$ *is set of two elements (say, a table $\sqcap$ and a chair $\mathfrak{h}$) with an operation given by:*

$\star$	$\mathfrak{h}$	$\sqcap$
$\mathfrak{h}$	$\mathfrak{h}$	$\sqcap$
$\sqcap$	$\sqcap$	$\mathfrak{h}$

The associativity can be checked explicitly by comparing the values of the expressions of the form: $\sqcap = \mathfrak{h} * (\sqcap \star \mathfrak{h}) = (\mathfrak{h} \star \sqcap) \star \mathfrak{h} = \sqcap$ for all ($A_2^3 = 8$) possible triplets of the elements of $\mathbb{G}$.
The neutral element $e = \mathfrak{h}$. The inverse elements: $\mathfrak{h}^{-1_\star} = \mathfrak{h}$, $\sqcap^{-1_\star} = \sqcap$.
This group is more familiar as $\mathbb{G} = \{0, 1\}$ with addition modulo 2.

The previous example shows that two different groups can in fact be absolutely similar. **Idea** of the mathematical construction behind this phenomenon: a morphism between two sets with similar structures is a mapping between them, which "respects" the structures.

Definition 2.4 *Consider two groups $(G_1, \star)$ and $(G_2, \circledast)$. A mapping $f \colon G_1 \to G_2$ is a homomorphism if $\forall a, b, \in G$, $f(a \star b) = f(a) \circledast f(b)$*

Example 2.3 $(\mathbb{R}, +) \overset{exp}{\to} (\mathbb{R}_{>0}, \times)$ $a \to e^a$, $b \to e^b$, $a + b \to e^{a+b} = e^a \times e^b$

Example 2.4 $(\mathbb{C},+) \overset{exp}{\to} (\mathbb{C}_*,\times)$
Define $e^{x+iy} := e^x \times e^{iy} = e^x \times (\cos y + i \sin y)$
Take $z_1 = x_1 + iy_1$ *and* $z_2 = x_2 + iy_2$
$e^{z_1+z_2} = e^{x_1+x_2+i(y_1+y_2)} = e^{x_1+x_2} \times e^{i(y_1+y_2)} = e^{x_1} \times e^{x_2} \times e^{iy_1} \times e^{iy_2} = e^{x_1+iy_1} \times e^{x_2+iy_2} = e^{z_1} \times e^{z_2}$

Remark 2.3 *Complex exponential is not bijective. It is surjective but not injective. For example because* $e^{i2\pi n} = 1\ \forall n \in \mathbb{Z}$. *All the elements of the arg* $i2\pi n \in G_1$ *go to the same element* $1 \in G_2$

Definition 2.5 *Let* $(G_1,\star)$ *and* $(G_2,\circledast)$ *be two groups, e the neutral element of* G_2
Then $\{g \in G_1, f(g) = e\}$ *is called the* *kernel* *of* f. *Notation* $\ker(f)$. *The kernel consists of all the the elements of* G_1 *that are mapped to the neutral element of* G_2.

Remark 2.4 *(exercise) The neutral element of* G_1 *is always in ker*(f).

Definition 2.6 *If a homomorphism* $(G_1,\star) \to (G_2,\circledast)$ *is bijective it is called an* *isomorphism*.

Remark 2.5 *An inverse mapping to an isomorphism is an isomorphism as well.*

Example 2.5

- $(G_1,*) = (\mathbb{R},+)$.
- $(G_2,\star) = ([0,1[,\star)$. *We can view* $[0,1[$ *as* $\mathbb{R}$ *with the identification* $a \equiv b$ *if* $(a-b) \in \mathbb{Z}$;
$\star$: $x_1, x_2 \to$ *the class of* (x_1+x_2) *that belongs to* $[0,1[$.
- $G_3 = \{z \in \mathbb{C}, |z| = 1\}$ *with complex multiplication.* $(G_3,\times)$ *is group:* $|z_1z_2| = |z_1||z_2| = 1\cdot 1 = 1$
Associativity follows from associativity of complex multiplication. $e = 1 \in G_3$, $|z^{-1}| =| \frac{1}{z} |= \frac{1}{|1|} = 1$
- $G_4 = \{$*Rotations of the plane around the origin by the angle* $\varphi \in [0;2\pi[\ \}$, *operation = composition. It is a group: The composition of two rotations is again a rotation. Associativity follows from the complex representation of similarity transformations* ($R_\varphi \leftrightarrow$ *multiplication of complex numbers by* $e^{i\varphi}$). $e = R_0, R_\varphi^{-1} = R_{-\varphi[2\pi]}$
- $G_5 = \{$*matrices of the form* $A_\varphi = \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}\}$, *with matrix multiplication.*

$$\begin{pmatrix} \cos\varphi_1 & -\sin\varphi_1 \\ \sin\varphi_1 & \cos\varphi_1 \end{pmatrix} \cdot \begin{pmatrix} \cos\varphi_2 & -\sin\varphi_2 \\ \sin\varphi_2 & \cos\varphi_2 \end{pmatrix} =$$
$$= \begin{pmatrix} \cos(\varphi_1)\cos(\varphi_2) - \sin\varphi_1 \sin\varphi_2 & -\sin\varphi_1 \sin\varphi_2 - \sin\varphi_1\cos\varphi_2 \\ \sin\varphi_1\cos\varphi_2 + \cos\varphi_1 \sin\varphi_2 & -\sin\varphi_1\sin\varphi_2 + \cos\varphi_1\cos\varphi_2 \end{pmatrix} =$$
$$= \begin{pmatrix} \cos(\varphi_1+\varphi_2) & -\sin(\varphi_1+\varphi_2) \\ \sin(\varphi_1+\varphi_2) & \cos(\varphi_1+\varphi_2) \end{pmatrix}$$

Associativity follows from associativity of addition in $\mathbb{R}$ *(or from the associativity of the matrix product, that we have not proven)*

$$e = \begin{pmatrix} \cos 0 & -\sin 0 \\ \sin 0 & \cos 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}^{-1} = \begin{pmatrix} \cos-\varphi & -\sin-\varphi \\ \sin-\varphi & \cos-\varphi \end{pmatrix}$$ *(The inverse matrix)*

The mapping $f_{12} : G_1 \to G_2, x \mapsto t = x - [x]$ *(integer part of x) is a homomorphism but not an isomorphism.*
The mapping $f_{23} : G_2 \to G_3, t \mapsto z = e^{i2\pi t}$ *is an isomorphism.*
The mapping $f_{34} : G_3 \to G_4, z \mapsto R_{arg(z)[2\pi]}$ *is an isomorphism.*
The mapping $f_{45} : G_4 \to G_5, R_\varphi \mapsto A_\varphi$ *is an isomorphism.*

A composition of two isomorphisms is an isomorphism as well, thus, the following diagram recapitulates these mappings. '$\to$' stands for homomorphisms, '$\leftrightarrow$' for isomorphisms.

$$\begin{tikzcd}
 & G_1 \arrow[dl] \arrow[dr] \arrow[ddl] \arrow[ddr] & \\
B \arrow[rr, leftrightarrow] \arrow[d, leftrightarrow] \arrow[drr, leftrightarrow] & & C \arrow[d, leftrightarrow] \arrow[dll, leftrightarrow] \\
D \arrow[rr, leftrightarrow] & & E
\end{tikzcd}$$

Remark 2.6 *Homo- and iso- morphisms can be defined for any sets with (possibly several) binary operations. The sets need not satisfy all the groups axioms, or they can satisfy some extra conditions relating different operations (like in rings or fields that we will see soon). This can be also convenient, for example, to show that some set is* not *a group/ring/field.*

Two more ways to construct groups

Remark 2.7 *When we constructed the homomorphism $G_1 \to G_2$ we identified some elements of G_1. This is a very common way to construct new groups from known ones (factor/quotient groups).*

Remark 2.8 *Another way to construct new groups is to consider a subset (a subgroup) of a known group.*

Subgroups

Definition 2.7 *Consider a group $(G, \star)$. H is a subgroup of G if: $H \subseteq G$ and H itself is a group with respect to the* same *operation $\star$.*

Example 2.6 $(G, \star) = (\mathbb{Z}, +)$

- $H_1 = \{0\}$. *The neutral element is a subgroup of any group.*
- $K = \{-1, 0\}$ *is not a subgroup (there is no inverse for -1, and $(-1) + (-1) \notin K$)*
- $\mathbb{N}$ *is not a subgroup (no inverse for any non-zero element)*
- H_2=$\{$*even numbers*$\}$ *is a subgroup*
- H_3=$\{$*odd numbers*$\}$ *is not a subgroup (7+5=12 $\notin H_3$)*

Example 2.7
– $(G, \star) = (\mathbb{C}_*, \times)$, $H = \{z \in C : |z| = 1\}$.
– $(G, \star) = \{$*Rotations of the plane*$\}$ *with composition,* $H = \{$*Rotations around the origin by a rational angle*$\}$.

Definition 2.8 *Let $(G, \star)$ be a group, $N \subseteq G$ be a subgroup of G. N is called a normal subgroup (fr: groupe distingué) if $\forall n \in N, \forall g \in G, g * n * g^{-1} \in N$.*

Remark 2.9 *If G is commutative i.e. $\forall g_1, g_2 \in G, g_1 \star g_2 = g_2 \star g_1$, then all the subgroups are normal since $g \star n \star g^{-1} = g \star g^{-1} \star n = e \star n = n$.*

Definition 2.9 *For any element $g \in G$ a class of equivalence w.r.t. a normal subgroup N is $\{g \star n, n \in N\}$ Notation: $[g]_N$ or gN, or simply $[g]$*

Let us define an operation induced by $\star$ on the set of classes: $[g_1] \star [g_2] := [g_1 \star g_2]$.

Proposition 2.2 *The result of $\star$ doesn't depend on the choice of a representative in the classes of g_1 and g_2.*

Proof. Let $\tilde{g}_1 = \mathrm{g}_1 \star n, n \in N$, so $\tilde{g}_1 \in [g_1]$. Then $[\tilde{g}_1 \star g_2] = [g_1 \star n \star g_2] = [g_1 \star g_2 \star g_2^{-1} \star n \star g_2] = [g_1 \star g_2]$

Definition 2.10 *The set H=$\{[g]\}$ of equivalence classes w.r.t a normal subgroup N with $\star$ is group itself. It is called a quotient group. Notation : G/N.*

Example 2.8 $(G, \star) = (\mathbb{Z}, +)$*, $N = 2\mathbb{Z}$ (even numbers). A class of equivalence $\{g+n\} = \{g+2k\}$. $g_1 = 1$ \{ odd numbers \}; $g_2 = 0$ \{ even numbers\}. Two equivalence classes even and odd $\mathbb{Z}/2\mathbb{Z}$. The induced operation $\star$:*

$\star$	*even*	*odd*
even	*even*	*odd*
odd	*odd*	*even*

$$\xrightarrow{isomorphism}$$

addition(mod2)	*0*	*1*
0	*0*	*1*
1	*1*	*0*

Remark 2.10 *For both types of constructions (subgroups or quotient groups) one does not have to check associativity – it follows automatically from associativity of the operation $\star$ in G.*

2.2 Rings and fields

Motivation: many sets have a richer structure than just a group ($\mathbb{R}, \mathbb{C}$, vector spaces), i.e several (compatible) operations could be defined (e.g. $(\mathbb{R}, +, \times)$)

Definition 2.11 *A ring R (anneau, m) is a set R equipped with two operations.*
$\oplus : R \otimes R \to R$ and $\otimes : R \otimes R \to R$, satisfying the following axioms:

$$\oplus \begin{cases} 1.\ \textit{Associativity of} \oplus : (a \oplus b) \oplus c = a \oplus (b \oplus c) \\ 2.\ \textit{Existence of } 0_\oplus : a \oplus 0_\oplus = a \\ 3.\ \textit{Existence of inverse } : a \oplus (-a) = 0_\oplus \\ 4.\ \textit{Commutativity } a \oplus b = b \oplus a \end{cases}$$

$$\otimes \begin{cases} 5.\ \textit{Associativity of} \otimes : (a \otimes b) \otimes c = a \otimes (b \otimes c) \\ 6.\ \textit{Distributivity: } (a \oplus b) \otimes c = a \otimes c \oplus b \otimes c \end{cases}$$

Remark 2.11 *A ring is a commutative group w.r.t. $\oplus$ with a compatible multiplication $\otimes$*

Definition 2.12 *If in a ring $a \otimes b = b \otimes a$ then a ring is called commutative.*

Example 2.9 $(\mathbb{R}, +, \times)$ *is a commutative ring.*

Definition 2.13 *If in a ring there is an element 1, such that $\forall a, 1 \otimes a = a \otimes 1 = a$, the ring is called unital or a ring with unity.*

Example 2.10 $(\mathbb{Z}, +, \times), (\mathbb{Q}, +, \times), (\mathbb{R}, +, \times)$ *– commutative rings with unity.*

Remark 2.12 *Sometimes the property 5. is not asked, then one studies* non-associative *rings.*

Definition 2.14 *A set F is called a field (corps, m) if:*
1. $(F, \oplus, \otimes)$ is a commutative ring with unity
2. $\forall a \in F$, if $a \neq 0_\oplus$, $\exists a^{-1} \in F : a \otimes a^{-1} = a^{-1} \otimes a = 1_\oplus$.

Example 2.11 *$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are fields. $\mathbb{Z}$ is not a field.*

Example 2.12 *$\mathbb{Z}/\ 3\mathbb{Z}$ $(= \mathbb{Z}_3)$*

$\oplus$	*0*	*1*	*2*
0	*0*	*1*	*2*
1	*1*	*2*	*0*
2	*2*	*0*	*1*

$\otimes$	*0*	*1*	*2*
0	*0*	*0*	*0*
1	*0*	*1*	*2*
2	*0*	*2*	*1*

$\otimes$ is commutative, $e = [1]$ is a unity; $[1]^{-1} = [1]$, $[2]^{-1} = [2]$, thus $\mathbb{Z}_3$ is a field.

Example 2.13 *(Exercise) $\{n + m\sqrt{2}, (n, m) \in \mathbb{Z}^2\}$ is a ring. $\{q + p\sqrt{2}, (q, p) \in \mathbb{Q}^2\}$ is a field.*

2.3 Modular arithmetics

Remark 2.13 ***Application** of group theory : Check digits on a credit card $a_1 ... a_n$.*
Possible mistakes: mistake at a_k (type I) or a_k and a_1 are inversed (type II).
Does a simple algorithm that finds both types of mistakes exist? No.
$w_1 a_1 + ... + w_n a_n \equiv 0(mod\ m)$, $w_k \pm 1$.
If the greatest common divisor of w_i and m is 1, then we can detect the errors of type I.
If the greatest common divisor of $(w_{i1} - w_{i2})$ and m is 1 then we can detect the errors of type II.
If m=10, $\mathbb{Z}_{10}$ has no solutions. Although a more complicated algorithm exists (using non-abelian groups).

Definition 2.15 *For a given positive integer n, two integers a and b are called congruent modulo n if $(a - b)$ is a multiple of n. Notation: $a \equiv b \mod n$ or $a \equiv b(mod\ n)$, or $a \equiv b[n]$.*

Remark 2.14 *$a \equiv b \mod n \Leftrightarrow [a] = [b]$ in $\mathbb{Z}/n\mathbb{Z}$. That is why $\mathbb{Z}_n \equiv \mathbb{Z}/n\mathbb{Z}$ is often called a residue system modulo n or a ring of remainders.*

Remark 2.15 *An interesting property of remainders is that $ab \equiv 0 \mod n \not\Leftrightarrow a \equiv 0(mod\ n)$ or $b \equiv 0(mod\ n)$. E.g. $n = 15$: $3 \times 5 \equiv 15 \equiv 0(mod\ n)$.*
This effect is called the existence of non-trivial divisors of 0.

Proposition 2.3 *If n is not a prime number then $\mathbb{Z}_n$ contains non-trivial divisors of zero.*

Proof. $n = lk$ $(l \neq 1$ and $k \neq 1)$, so $[l][k] = [lk] = [n] = [0]$
Then $l \not\equiv 0(\text{mod } n)$ and $k \not\equiv 0(\text{mod } n)$, but $lk \equiv 0(\text{mod } n)$.

Proposition 2.4 *A field never contains non-trivial divisors of zero.*

Proof. Suppose that in a field $a \neq 0$ and $b \neq 0$ but $ab = 0$. Multiply both sides by a^{-1}: $a^{-1}ab = a^{-1}0$ which implies that $b = 0$ which raises a contradiction.

Theorem 2.2 *$\mathbb{Z}$ is a field $\Leftrightarrow$ n is prime.*

Proof.

”$\Rightarrow$” follows from propositions 1 and 2.

”$\Leftarrow$” We need to show that any non-zero element in $\mathbb{Z}_n$ is invertible. Consider the class of a: $[a]$ and $[2a], [3a], [4a], ..., [(n-1)a]$. These are different non-zero classes in $\mathbb{Z}$. Indeed, if $[la] = [na]$ and $(l, k < n)$ then $la \equiv ka \mod n \Leftrightarrow (l - k)a$ is a divisor of n. This is impossible since n is prime. Thus this list contains the class [1] so a is invertible in $\mathbb{Z}_n$.

2.4 Euclidean rings

Definition 2.16 *A euclidean ring is a commutative ring without non-trivial divisors of zero and in addition there is a euclidean norm d on it.*
$d : \mathbb{R} \to \mathbb{Z}_{\geq 0} \cup \{-\infty\}$ *s.t* $d(a) = -\infty \Leftrightarrow a = 0$
It permits to define the remainder of the division $a = qb + r$ *and* $d(r) < d(b)$

Example 2.14 $\mathbb{Z} : d(a) = |a|$ *for* $a \neq 0$ $d(0) = -\infty$.

Proposition 2.5 *The euclidean algorithm of computing the greatest common divisor* $gcd(a, b)$

$$a = q_0 b + r_1$$
$$b = q_1 r_1 + r_2$$
$$\vdots$$
$$\vdots$$
$$r_{n-2} = q_n r_{n-1} + r$$
$$r_{n-1} = q_n r + 0$$

Then r is the gcd of a and b.

Proof.

1. We want to prove that the algorithm is finite.
   $r_1 > r_2 > r_3 > ... > r_{n-1} > 0$, so the process stops.
2. We want to prove that it leads to $gcd(a, b)$
   This follows from the fact that if $a = qb + r$ then $gcd(a, b) = gcd(b, r)$
   – Let $a = kl_1$ and $b = kl_2$ then $kl_1 = kl_2 + r$ and $r = k(l_1 - l_2)$ (k is a divisor of r)
   – Let k be a divisor of r and b. $r = km_1$ and $b = km_2$, then $a = k(qm_1 + m_2)$ so k is a divisor of a.
   And $gcd(r, 0) = r = gcd(a, b)$.

Proposition 2.6 *Bézout's relations/identities*
For $a, b \in \mathbb{Z}$ *there exist* $x, y \in \mathbb{Z}$ *such that* $gcd(a, b) = ax + by$.

Proof. (Exercise) Idea of the proof: Take $r_1 = a - q_0 b$, and replace r_1 in $r_2 = b - q_1 r_1$, then replace r_1 and r_2 in $r_3 = r_1 - q_2 r_2$, etc. The real proof is by induction (depending on n) and the statement is $r_k = x_k a + y_k b$

Remark 2.16 *This decomposition is not necessarily unique.*

Corollary 2.1 *: A minimal subgroup of* $\mathbb{Z}$ *that contains simultaneously two given integer numbers a and b is of the form* $k\mathbb{Z}$, *where* $k = gcd(a, b)$.
Example: $a = 15$ *and* $b = 12 \Rightarrow 3\mathbb{Z}$; $a = 15$ *and* $b = 11 \Rightarrow \mathbb{Z}$.

Remark 2.17 *This theory of remainders could have been a completely abstract science if the RSA encryption algorithm (Rivest–Shamir–Adleman public key cryptosystem) was not discovered.*

The ring $\mathbb{Z}$ is a simple example of a euclidean ring. A more interesting one will be seen in the next section, we will however observe a lot of striking similarity between them.

2.5 Polynomial functions

Definition 2.17 *A polynomial function f is a function $\mathbb{R} \to \mathbb{R}$ (or $\mathbb{C} \to \mathbb{C}$) such that it can be written in the form $f(x) = a_0 + a_1x^1 + a_2x^2... + a_nx^n$ where $a_0, a_1, ...a_n \in \mathbb{R}$ (or $\mathbb{C}$) are called coefficients of f (some of $a_0, ...a_n$, or even all can vanish).*

Remark 2.18 *A polynomial can be defined over any field (or even a ring) $\mathbb{K}$ ($f : \mathbb{K} \to \mathbb{K}$ and $a_0, ...a_n \in \mathbb{K}$) but in this course we discuss only $\mathbb{K} = \mathbb{R}$ or $\mathbb{K} = \mathbb{C}$.*

The set of polynomials over the field $\mathbb{K}$ is denoted $\mathbb{K}[x]$.

Definition 2.18 *Two polynomials $f(x) = a_0 + a_1x^1 + ... + a_nx^n$ and $g(x) = b_0 + b_1x^1 + ... + b_mx^m$ are equal if all of their non-zero coefficients coincide : $a_0 = b_0, a_1 = b_1, ..., a_n = b_n, \dots, a_m = b_m$*

Definition 2.19 *The maximal index of a non-zero coefficient of a polynomial is called its degree ($\deg(f)$). The degree of a zero polynomial (i.e $a_i = 0\ \forall i$) is $-\infty$.*

Proposition 2.7 *Consider $\mathbb{K} = \mathbb{R}$ or $\mathbb{C}$. $\mathbb{K}[x]$ is a ring with respect to usual addition and multiplication of polynomials.*

Proof.

1. Associativity and commutativity of +, as well as associativity and commutativity of × follow directly from associativity and commutativity in $\mathbb{K}$.
2. Inverse with respect to + exists: for $f(x) = a_0 + a_1x + ... + a_nx^n$, $-f(x) = -a_0 + (-a_1)x + ... + (-a_n)x^n$. neutral element with respect to $+$ – zero polynomial.
3. Distributivity of × over + :
   $f(x) = a_0 + a_1x + ... + a_nx^n$
   $g(x) = b_0 + b_1x + ... + b_mx^m$
   $h(x) = c_0 + c_1x + ... + c_lx^l$
   Let us compute the coefficients at x^k of $(f + g)h \overset{?}{=} fh + gh$
   $(a_0 + b_0)c_k + (a_1 + b_1)c_{k-1} + (a_2 + b_2)ck - 2... + (a_{k-1} + b_{k-1})c_1 + (a_k + b_k)c_0 =$
   (by distributivity in $\mathbb{R}$ or $\mathbb{C}$)=$\underbrace{a_0c_k + a_1c_{k-1} + ... + a_{k-1}c_1 + a_kc_0}_{\text{the coefficients at x}^\text{k}\text{ in fh}}+ \underbrace{b_0c_k + ... + b_kc_0}_{\text{the coefficients at x}^\text{k}\text{ in gh}}$

Proposition 2.8 $\mathbb{R}[x]$ *($\mathbb{C}[x]$) is a unital ring without non-trivial divisors of zero.*

Proof.

- The neutral element with respect to multiplication is $1 \in \mathbb{R}[x]$ ($\mathbb{C}[x]$)
- Suppose that f and g are as before and $a_n \neq 0, b_m \neq 0$ then the coefficient at x^{n+m} in fg is a_nb_m and since in $\mathbb{R}$ ($\mathbb{C}$) there are no non-trivial divisors of zero, $a_nb_m \neq 0$.

Corollary 2.2 *$deg(fg) = deg(f) + deg(g)$*

In what follows we will show that $\mathbb{R}[x]$ ($\mathbb{C}[x]$) is an Euclidian ring.

Proposition 2.9 *Consider a polynomial $f(x) = a_0 + a_1x^1 + a_nx^n$ and a polynomial $(x - x_0)$ for some fixed $x_0 \in \mathbb{K}$, then there is a unique decomposition of f in the form $f = (x - x_0)q + r$ where $q \in \mathbb{K}[x]$ (partial quotient), and $r \in \mathbb{K}$ (remainder).*

Proof : If $f \equiv a_0$ then $q = 0$ and $r = a_0$.
If $deg(f) = n > 0$ then $deg(q) = n - 1, q = b_0 + b_1 x + ... + b_{n-1}x^{n-1}$
$(x - x_0)q + r = (r - x_0 b_0) + (b_0 - x_0 b_1)x + (b_1 - x_0 b_2)x^2 + ... + (b_{n-2} - x_0 b_{n-1})x^{n-1} + (b_{n-1})x^n$
By identification :

$$\begin{aligned} a_n &= b_{n-1} \\ a_{n-1} &= b_{n-2} - x_0 b_{n-1} \\ a_2 &= b_1 - x_0 b_2 \\ a_1 &= b_0 - x_0 b_1 \\ a_0 &= r - x_0 b_0 \end{aligned}$$

This gives a unique way to compute b_i.

Corollary 2.3 *(Horner's scheme) It is convenient to compute b_i starting from b_{n-1}*

	a_n	a_{n-1}	a_{n-2}	...	a_2	a_1	a_0
x_0	b_{n-1}	b_{n-2}	b_{n-3}		b_1	b_0	r

Remark 2.19 *The Horner's scheme allows to compute $r = f(x_0)$ about twice faster than the direct computation.*

Corollary 2.4 *(Bézout's theorem) $f(x) \vdots (x - x_0) \Leftrightarrow x_0$ is a root of f ($\Leftrightarrow (x - x_0)|f(x)$)*

Theorem 2.3 *The number of roots of any polynomial f is $\leq deg(f)$*

Proof. Induction by the degree

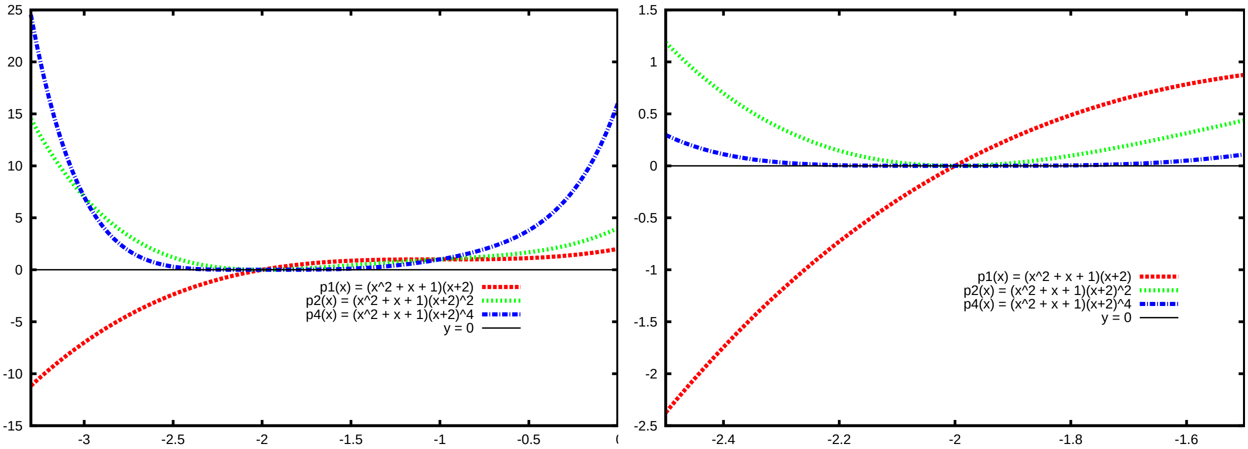
- Base : $deg = 0, f(x) = a \neq 0$. Number of roots is 0.
- Step : Suppose that the statement is true for $k = 0, ..., n-1$. Take $f(x), deg(f) = n$, suppose that $x_1, ..., x_m$ are roots, and $m > n$ Bézout $\Rightarrow f(x) = (x - x_1)g(x)$, $deg(g) = n - 1$ and $g(x_i) = 0$, $i = 2, ..., m$ impossible by the induction hypothesis.

Definition 2.20 *The multiplicity of a root x_0 for a polynomial $f(x)$ is the maximal integer k such that $f(x) = (x - x_0)^k g(x)$ and $g(x_0) \neq 0$*

Remark 2.20 *To find m the Horner's scheme is useful.*

Remark 2.21 *Analytically in the neighborhood of a root x_0 of multiplicity k the polynomial $f(x)$ behaves as $c(x - x_0)^k$. Indeed $f(x) = g(x)(x - x_0)^k$, where $g(x_0) = c \neq 0$.
More precisely, $f(x) = c(x - x_0)^k + \bar{o}((x - x_0)^k) \Leftrightarrow \lim\limits_{x \to x_0} \frac{f(x) - c(x - x_0)^k}{(x - x_0)^k} = 0$.*

*In particular, if $k = 1$ the graph of f is tangent to $y = c(x - x_0)$,
otherwise if $k > 1$ the graph is tangent to the abscissa axis with the order of tangency $k - 1$.*



Remark 2.22 *If x_0 is a root of multiplicity $k > 1$ of a polynomial $f(x)$ of degree n, then $f(x_0) = f'(x_0) = f''(x_0) = \ldots = f^{(k-1)}(x_0) = 0$.*
Thus, the Taylor series of $f(x)$ at x_0 contains at most $n - k$ terms.

Theorem 2.4 *The sum of multiplicities of all the roots of a polynomial f is $\leq$ deg(f).*
The sum is equal to deg(f) $\Leftrightarrow$ f can be decomposed to linear factors over $\mathbb{K}$.

Proof. By Bézout's theorem and induction $f(x) = (x - x_1)^{k_1}(x - x_2)^{k_2} \cdot \ldots \cdot (x - x_s)^{k_s} g(x)$, where $x_1, \ldots, x_s$ are the roots with the multiplicities $k_1, \ldots, k_s$ respectively, and $g(x) \neq 0$ in $\mathbb{K}$.
$\deg(f) = k_1 + k_2 + \ldots + k_s + \deg(g) \geq k_1 + k_2 + \ldots + k_s$.
$\deg(f) = k_1 + k_2 + \ldots + k_s \Leftrightarrow \deg(g) = 0 \Leftrightarrow g \equiv const$ and $f(x) = c(x - x_1)^{k_1}(x - x_2)^{k_2} \cdot \ldots \cdot (x - x_s)^{k_s}$.

Corollary 2.5 *(Viète's formulas) If a polynomial $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ admits exactly n roots $x_1, \ldots, x_n$ (counting multiplicities), then*
$a_{n-1} = -a_n(x_1 + \ldots + x_n)$,
$a_{n-2} = a_n(x_1x_2 + x_1x_3 + \ldots + x_{n-1}x_n)$
$\ldots$
$a_0 = (-1)^n a_n(x_1x_2 \ldots x_n)$

Proof. Expand $f(x) = a_n(x - x_1)(x - x_2) \cdot \ldots \cdot (x - x_n)$.

Theorem 2.5 *For all $f, g \in \mathbb{K}[x]$ if $g \neq 0$ $\exists!$ couple $q, r \in \mathbb{K}[x]$, such that $f = qg + r$, deg$(r) <$ deg(g).*

Proof. Consider $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, $g(x) = b_m x^m + b_{m-1}x^{m-1} + \ldots + b_1 x + b_0$.
If $m > n$ $q := 0$, $r := f$.
If $m \leq n$, $f_1 := f - c_0 x^{n-m} g$, where $c_0 = a_n/b_m$, then $\deg(f_1)$ is at most $n - 1$, $f_1 = a^{(1)}_{n-1}x^{n-1} + \ldots$
$f_2 := f_1 - c_1 x^{n-m-1} g$, where $c_1 = a^{(1)}_{n-1}/b_m$, then $\deg(f_2)$ is at most $n - 2$, $f_2 = a^{(2)}_{n-2}x^{n-2} + \ldots$
$\ldots$
$f_k := f_{k-1} - c_k x^{n-m-k} g$, where $c_k = a^{(k-1)}_n/b_m$, then $\deg(f_k)$ is at most $n - k$, $f_1 = a^{(1)}_{n-1}x^{n-1} + \ldots$.
Then $f(x) = (c_0 x^{n-m} + c_1 x^{n-m-1} + \ldots + c_{n-m-1}x + x_{n-m})g(x) + f_{n-(m-1)}$,
where $\deg(f_{n-(m-1)}) \leq m - 1 < \deg(g)$. This proves the existence.
To prove the uniqueness, suppose $f = q_1 g + r_1 = q_2 g + r_2$, then $(q_1 - q_2)g = r_2 - r_1$. $\deg((q_1 - q_2)g) \geq \deg(g)$, $\deg(r_2 - r_1) < g$, thus, $r_2 - r_1 = q_1 - q_2 \equiv 0$.

Remark 2.23 *This means that $\mathbb{K}[x]$ is a* Euclidean *ring with the Euclidean norm deg(f).*

Corollary 2.6 *The Euclidean algorithm as well as the Bézout's identities are valid in $\mathbb{K}[x]$.*

Remark 2.24 *Euclidean algorithm can be used in practice to find gcd(f, g), but for the Bézout's relations are easier to reconstruct using the 'undetermined coefficients'.*

Factorization and irreducible polynomials.

Definition 2.21 *A polynomial f is irreducible over $\mathbb{K}$ if it can not be factorized as $f = gh$ for $0 <$ deg$(g) <$ deg(f), $0 <$ deg$(h) <$ deg(f).*

Remark 2.25 *This is an analogue of the definition of prime numbers in the Euclidean ring $\mathbb{Z}$.*

Theorem 2.6 *(Fundamental theorem of algebra). Any polynomial with real or complex coefficients admits a complex root in $\mathbb{C}$.*

Remark 2.26 *We admit this theorem without proof, since none of the known proofs is purely algebraic. The name 'fundamental' here is more historic than scientific.*

Corollary 2.7 *Any $f \in \mathbb{C}[x]$ can be decomposed to linear factors over $\mathbb{C}$, i.e. a polynomial is irreducible over $\mathbb{C} \Leftrightarrow$ it is of degree 1.*

Proof. Induction by $\deg(f)$ using the Bézout's theorem.

Proposition 2.10 *If $z_0 \in \mathbb{C}$ is a root of a polynomial f with real coefficients then $\bar{z}_0$ is a root of f as well.*

Proof. $f(\bar{z}_0) = a_n(\bar{z}_0)^n + a_{n-1}(\bar{z}_0)^{n-1} + \ldots + a_1(\bar{z}_0) + a_0 = \overline{f(z_0)} = 0$

Corollary 2.8 *Any irreducible polynomial in $\mathbb{R}[x]$ is of degree at most 2.*

Corollary 2.9 *Any polynomial f in $\mathbb{R}[x]$ can be factorized as*

$$f(x) = a(x-x_1)^{k_1}(x-x_2)^{k_2} \cdot \ldots \cdot (x-x_s)^{k_s}(x^2+p_1x+q_1)^{l_1}(x^2+p_2x+q_2)^{l_2} \cdot \ldots \cdot (x^2+p_tx+q_t)^{l_t},$$

where $x^2 + p_ix + q_i$ do not admit real roots.
In particular, any polynomial in $\mathbb{R}[x]$ of degree three admits a real root.

Corollary 2.10 *(Partial fractions decomposition)*
Consider a polynomial $g(x)$ and a factorization of $f(x)$ to irreducible polynomials:
$f(x) = (x-x_1)^{k_1} \cdot \ldots \cdot (x-x_s)^{k_s}(x^2+p_1x+q_1)^{l_1} \cdot \ldots \cdot (x^2+p_tx+q_t)^{l_t}$, then

$$\frac{g(x)}{f(x)} = G(x) + \frac{A_{1,1}}{(x-x_1)} + \frac{A_{1,2}}{(x-x_1)^2} + \ldots + \frac{A_{1,k_1}}{(x-x_1)^{k_1}} + \ldots + \frac{A_{s,1}}{(x-x_s)} + \frac{A_{s,2}}{(x-x_s)^2} + \ldots + \frac{A_{s,k_s}}{(x-x_s)^{k_s}} +$$

$$+ \frac{B_{1,1}x + C_{1,1}}{(x^2+p_1x+q_1)} + \ldots + \frac{B_{1,l_1}x + C_{1,l_1}}{(x^2+p_1x+q_1)^{l_1}} + \ldots + + \frac{B_{t,1}x + C_{t,1}}{(x^2+p_tx+q_t)} + \ldots + \frac{B_{t,l_t}x + C_{t,l_t}}{(x^2+p_tx+q_t)^{l_t}}$$

Remark 2.27 *This decomposition is useful to integrate rational functions.*

Exercises

1. Given a set with operations on it, check it is a group/ring/field.
2. For a given group find subgroups satisfying some property. For a finite group find all the subgroups.
3. Given a couple of groups/rings/fields check if there is some morphism between them, identify the kernel of it.
4. Perform arithmetic operations in $\mathbb{Z}_n \Leftrightarrow$ manipulate with congruence relations.
5. Analyze the roots of polynomials (including multiplicities).
6. Decompose a polynomial to irreducible factors (with various applications).