

Contents

1	Analysis	3
1.1	Axioms	3
1.2	Suits and Limits	7
1.3	Series	11
2	Linear Algebra	15
2.1	Matrix Calculus	16
2.1.1	Special matrixes	16
2.1.2	Operations on matrixes	16
2.1.3	Trace of a Matrix	18
2.1.4	Transposition of a Matrix	19
2.1.5	Symmetric Matrixes	20
2.1.6	Inverse Matrixes	20
2.1.7	Sub Matrixes	20
2.2	Algebraic Structures	21
2.2.1	Morphisms between Groups	23
2.2.2	Rings	23
2.2.3	Matrixes of ring's coefficients	23
2.2.5	Fields or Coprs	24
2.2.6	Complex Numbers	24
2.3	Echelonnee Form	24
2.4	Vector Spaces	24
2.5	Linear Applicaiton	24
2.6	Proper Value	24
2.7	Stocastic Matrix	24
3	Algebraic Structures	25
3.1	Formal Logic	25
3.2	Sets	25
3.2.1	Zermelo-Ferkel's Axioms (1920)	26
3.2.2	Application	26
3.2.4	Equivalent Relations	27
3.3	Number Theory	29
3.4	Group Theory	29
4	Meccanics	31
4.1	Introduction	31
4.2	Elastic forces and Harmonic Oscillations	36
4.2.1	Dampded elastic oscillator	36

Chapter 1

Analysis

Introduction

Analysis 1 will be about real function in 1 real variable.

Theorem 1.0.1 (Rigorous proof exemple). $\nexists x = \frac{a}{b}, a, b \in \mathbb{Z}, b \neq 0 \mid x^2 = 2$

Proof Suppose $\exists a, b \in \mathbb{Z}$ that satisfy the condition of the theorem. We can reduce the two number so that they have no more common factors.

By these conditions a, b cannot be both even. By hypothesis, we have $\frac{a^2}{b^2} = 2 \implies a^2 = 2b^2 \implies a^2$ is even.

We use the fact that n is even $\iff n^2$ is even since:

" \implies " suppose $n = 2k \quad k \in \mathbb{N}$. Follows $n^2 = 4k^2 = 2(2k^2)$, which is even

" \Leftarrow " suppose $n = 2k + 1$ and n^2 even. Follows $n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, which is odd. The thesis follows by contradiction.

Since a^2 is even, a is even. We can then write $a = 2q, q \in \mathbb{N}$.

Follows $a^2 = 4q^2 = 2b^2 \implies 2q^2 = b^2 \implies b^2$ is even.

With the same reasoning as before, b is even.

We thus arrived to a contradiction, meaning the assumption of the existence of such numbers is false. \square

1.1 Axioms

Def: Group

A Group $(G, +)$ is a mathematical object where G is a set and $+$ a binary operation such that:

1. Stability: $\forall a, b \in G : a + b \in G$
2. Associativity: $(a + b) + c = a + (b + c)$
3. $\exists 0 \in K \mid \forall x \in K : 0 + x = x$
4. $\forall x \in K, \exists (-x) \in K \mid x + (-x) = 0$

A Group where the operation is commutative is called an abelian group.

Def: Corp

A Corp $(K, +, \cdot)$ is a mathematical object where K is a set, $(K, +), (K, \cdot)$ must be abelian groups, and there is a relation of distributivity. We can also say that the Corp is a set K with two operations, addition and multiplication $(+, \cdot)$ such that:

1. Associativity: $(a + b) + c = a + (b + c)$
2. $\exists 0 \in K \mid \forall x \in K : 0 + x = x$
3. $\forall x \in K, \exists (-x) \in K \mid x + (-x) = 0$
4. Commutativity: $\forall a, b \in K : a + b = b + a$
5. Associativity: $\forall a, b, c : a(bc) = (ab)c$
6. $\exists 1 \in K \mid \forall x \neq 0 : 1 \cdot x = x$
7. $\forall x \neq 0, \exists x^{-1} \mid xx^{-1} = 1$
8. Commutativity: $\forall a, b : ab = ba$
9. Distributivity: $\forall a, b, c : a(b + c) = ab + ac$

With those axiomatic definitions we can rigorously prove a lot of theorems regarding real numbers.

For example we can prove that $\forall x \in K, 0x = x$

Or $\forall a, b \in K, ab = 0 \implies (a = 0 \vee b = 0)$

Def: Total order

A total order is a binary relation that satisfy notet as \leq such that:

1. $\forall x, x \leq x$
2. $\forall a, b, c : a \leq b \text{ and } b \leq c \implies a \leq c$
3. $\forall a, b : a \leq b \text{ or } b \leq a \implies a = b$
4. $\forall a, b : a \leq b \vee b \leq a$

Def: Ordered Corp

An ordered corp is a corp $(K, +, \cdot)$ with a total order such that:

1. Addition invariance: $\forall x, y, z \in K ; x \leq y \iff x + z \leq y + z$
2. Multiplication invariance $\forall x, y, z \in K, z \geq 0 ; x \leq y \iff xz \leq yz$

Notations

When we write $x - y := x + (-y)$, the second half of the equations follows by axiomatic definition. This is true also for $x + y + z = (x + y) + z$, where we don't want to define a new ternary operation for addition.

Or again $x < y$ means $(x \leq y \wedge x \neq y)$, and $[x, y[= \{z \mid x \leq z < y\}$.

Absolute Value

We can now define:

$|x|$ = bo fallo a casa stronzo

Unicity of the inverse

To cnserve the coerence of our conctructed structures we want to show:

$$a + b = 0 \wedge a + c = 0 \implies b = c$$

. $a + b + c = (a + b) + c = 0 + c = c$ and $a + b + c = b + (a + c) = b + 0 = b \implies b = c$ \square We should do the same for x^{-1} and $x + a = x \iff a = 0$

Triangular identity

Prop: $|a + b| \leq |a| + |b|$, We procede in two cases:

1. $a, b \geq 0 \implies a + b \geq 0, |a + b| = a + b = |a| + |b|$ \square
2. $a, b \leq 0 \implies a + b \leq 0, |a + b| = -(a + b) = -a - b \leq |a| + |b|$
3. $a \geq 0, b \leq 0$. Agasin, by cases: if $a + b \geq 0 \implies |a + b| = a + b = |a| - |b| \leq |a| + |b|$.
For $a + b \leq 0 \implies |a + b| = -a - b = -|a| + |b| \leq |a| + |b|$ \square .

With this we can also prove the following inequality:

$$|a - b| \leq ||a| - |b||$$

Axiome of completude

Def: Majore

Let $A \subseteq \mathbb{R}$ (or any odered corp), we say that A is majoree (borne superiorment) if
 $\exists b \forall a \in A \mid a \leq b$. We say b is the majorante of A

Def: Minore

Let $A \subseteq \mathbb{R}$ (or any odered corp), we say that A is minoree (borne inferorement) if
 $\exists b \forall a \in A \mid a \geq b$. We say b is the minorante of A

Def: Supremum

Given $A \subseteq \mathbb{R}$ (or any odered corp), s is the least upper bound (*supremum*) of A (noted as $\sup(A)$) iff:

1. s is a LUB of A
2. $\forall b$ that are LUBs A , $b \geq s$

Def: Infemum

Given $A \subseteq \mathbb{R}$ (or any odered corp), i is the highest lower bound (*infemum*) of A (noted as $\inf(A)$) iff:

1. i is a LUB of A .
2. $\forall b$ that are LUBs A , $b \leq i$.

We note that $\inf(A) = -\sup(\mathbb{R} \setminus A)$. This is to say that perfect equality (meaning categoristic) between \inf and \sup .

Theorem 1.1.1 (Completeness Axiom). *If $A \in \mathbb{R}$ is majored and non-empty, then $\exists \sup(A)$.*

The same is true for the \inf . We note that that \mathbb{R} is the only complete ordered Corp.

To, again, maintain the coherence of this mathematical system, we need to show that $\sup(A)$ is unique.

Suppose $s \neq r$, both $\sup(A)$, then $s < r \vee s > r$. But by definition if $s < r$, then r is only an upper bound, not the lowest upper bound, follows r is not the $\sup(A)$. Same reasoning holds for $s > r$.

Consequences of the completeness Axiom

$\exists x \geq 0 \in \mathbb{R} : x^2 = 2$

We prove it using $A = \{y > 0 \mid y^2 < 2\} \implies A \neq \emptyset$.

-It is bounded simply by: $(y \in A \implies y < 2 \sin y^2 \geq 4)$.

-By the completeness axiom, exists $x = \sup(A)$. We prove by showing $x^2 < 2$ and $x^2 > 2$ are both false statements, which implies $x^2 = 2$. Suppose $x^2 < 2$.

Let $0 < \varepsilon < \frac{2 - x^2}{4x}$ (since $x > 0 \wedge x^2 < 2$). Let $y = x + \varepsilon$

$$\iff y^2 = x^2 + 2\varepsilon x + \varepsilon^2 < x^2 + \frac{2 - x^2}{2} + \frac{2 - x^2}{4x} < x^2 + 2 - x^2 = 2 \implies y^2 < 2$$

which is an absurdity, since we started by $y = x + \varepsilon$, $\varepsilon > 0$.

Suppose now by absurdity $x^2 > 2$. Let $0 < \varepsilon < \frac{2 - x^2}{2x}$ (since $x > 0 \wedge x^2 < 2$).

Now consider $b = x - \varepsilon < x$, meaning b is not a mojarant. It is true that: $\forall y \in A : y > b \implies y^2 > b^2 = x^2 - 2\varepsilon x + \varepsilon^2 > x^2 - 2\varepsilon x > x^2 - (x^2 - 2) = 2$, which is an absurd.

Def: Maximum

We define the maxium $\max = \sup(A) \iff \max \in A$, noted as $\max(A)$.

Rem: On a separate note, $\forall x > 0 \exists! r \geq 0 : r^2 = x$, writing $\sqrt{x} = r$.

Prop: $\forall x \in \mathbb{R} \exists n \in \mathbb{N} : n > x$ **Cor**

$$1. \forall x \forall y, \exists n \in \mathbb{N} : ny > x$$

$$2. \forall \varepsilon > 0 \exists n \in \mathbb{N} : \frac{1}{n} < \varepsilon$$

Prop: (Density)

$$\forall (x, y) \in \mathbb{R}^2, x < y, \exists z \in \mathbb{Q} : x < z < y$$

Proof If $a, b \in \mathbb{R}$ satisfies $b - a > 1 \implies \exists p \in \mathbb{Z} : a < p < b$, taken as true.

For the archideian proprieties, $\exists q \in \mathbb{N} : q > \frac{1}{y - x}$

$\therefore qy - qx > 1 \implies \exists p \in \mathbb{Z} : qx < p < qy$. So $p/q \in \mathbb{Q}$ the rational we were looking for.

Prop:(Density of $\mathbb{R} \setminus \mathbb{Q}$)

$\forall x < y \exists z \notin \mathbb{Q} : x < z < y$

Proof: $\exists p/q (p \in \mathbb{Z}, q \in \mathbb{N}^*) \mid x < p/q < y$.

$\therefore x < p/q < z = p/q + \frac{\sqrt{2}}{n} < y$ if $\frac{1}{n} < \frac{y - p/q}{\sqrt{2}}$, where z is trivially out of \mathbb{Q} .

1.2 Suits and Limits

Def: Suite

A suite is a function $f : \mathbb{N} \rightarrow \mathbb{R}$, $n \mapsto x_n$. We write $(x_n)_{n=0}^\infty$ or (x_n)

However, if a suite begins with the index different than 0, we can write $(x_n)_{n=k}^\infty$.

Def: Convergence and Limit

The suite $(x_n)_{n \in \mathbb{N}}$ converges to the limit L (or ℓ) if:

$$\forall \varepsilon > 0 \exists n_0 \in \mathbb{N} \mid \forall n \geq n_0 : |x_n - L| < \varepsilon$$

We write: $\lim_{n \rightarrow \infty} x_n = L$

Lemme: If (x_n) converges, L is unique.

Proof: Otherwise $L \neq L'$. We can thus chose an arbitrary $\varepsilon = \frac{|L - L'|}{4}$.

It must hold true by definition of convergence that $\exists n_0 \forall n \geq n_0 : |x_n - L| < \varepsilon$, and that $\exists n_1 \forall n \geq n_1 : |x_n - L'| < \varepsilon$. Let $n \geq n_0, n_1$.

Then $|L - L'| = |L - x_n + x_n - L'| \leq |L - x_n| + |x_n - L'| < 2\varepsilon = \frac{|L - L'|}{2}$, which is an absurd.

As an exemple take $x_n = 2 + \frac{(-1)^n}{n}$, then $\lim_{n \rightarrow \infty} = 2$.

Than it must be that $\forall \varepsilon > 0, \exists n_0 : \forall n \geq n_0, |2 + \frac{(-1)^n}{n} - 2| < \varepsilon \iff \left| \frac{(-1)^n}{n} \right| < \varepsilon \iff \frac{1}{n} < \varepsilon$. Which is true $\forall n \geq n_0$ by archimed's relations.

Def: Limited Suite

(x_n) is borne if $\{x_n \mid n \in \mathbb{N}\}$ is borne.

Theorem 1.2.1 (Convergence implies limitation). (x_n) converges $\implies (x_n)$ is limited

Lemme:

Let $x_n = y_n \forall n \geq m$ for a given m . Then (x_n) converges $\iff (y_n)$ converges for the definition itself of limit.

Lemme: $\lim_{n \rightarrow \infty} x_{n+1} = \lim_{n \rightarrow \infty} x_n$ For $A = \lim_{n \rightarrow \infty} a_n$ and $B = \lim_{n \rightarrow \infty} b_n$

1. The suite $(a_n + b_n)$ converges to $A + B$.
2. The suite $(a_n b_n)$ converges to AB .

3. Given $B \neq 0$, the suite (a_n/b_n) converges to A/B .

Note that for $n > n_0$, the term a_n/b_n is well defined. In general we say that the structure of the limit holds true under the operation of the Corp.

We can simply prove it, starting with point 1; we need to show that (looking for n_0 for all the ε);

$$\forall \varepsilon > 0 \exists n_0 \in \mathbb{N} \mid \forall n \geq n_0 : |a_n + b_n - (A + B)| < \varepsilon$$

Assume by hypothesis;

$$\forall \varepsilon > 0 \exists n_a \in \mathbb{N} \mid \forall n \geq n_a : |a_n - A| < \varepsilon/2$$

$$\forall \varepsilon > 0 \exists n_b \in \mathbb{N} \mid \forall n \geq n_b : |b_n - B| < \varepsilon/2$$

We have $|a_n + b_n - (A + B)| \leq |a_n - A| + |b_n - B| < \varepsilon/2 + \varepsilon/2 = \varepsilon$. We can proceed similarly about the other 2 proprieties, by taking the new epsilon to be $\frac{\varepsilon}{2s}$, where s is the upper bound of the the other series.

Lemme $\lim_{n \rightarrow \infty} x_n = x$ and $x_n \geq a \in \mathbb{R} \implies x \geq a$. This proof is obvious and left as an exercise to the reader. The same olds true for \leq . As a corollary we can write, for two suits $a_n \geq b_n \forall n$, than $\lim_{n \rightarrow \infty} a_n \geq \lim_{n \rightarrow \infty} b_n$.

We now arrive at the important lemme of, given a suite x_n that is majored and monotonaly increasing, then $\lim_{n \rightarrow \infty} x_n = \sup\{x_n \mid n \in \mathbb{N}\}$

Limsup/Liminf

Def: Limsup

Given (x_n) a majored suit. The superior limit of (x_n) is

$$\limsup(x_n) = \lim_{n \rightarrow \infty} \sup\{x_k \mid k \geq n\}$$

where the lim sup always exists, and it is the infemum (the lowest) of the supremums.

We can write that for a sout (x_n) that converges to L , $\lim_{n \rightarrow \infty} |x_n| = |L|$

Cose da aggiungere

Remark We say that (x_n) tends to infinity iff $\forall t \in \mathbb{R}, \exists n_0 \mid \forall n \geq n_0; x_n > t$. This suit is still diverging, even if we say it "converges" to infinity.

D'Alembert is useless if $\rho = 1$.

Def: SubSuite

A subsuite of the suit $(x_n)_{n=1}^\infty$ is a suite $(x_{n_k})_{k=1}^\infty$ where $(n_k)_{k=1}^\infty$ is a strictly increasing suite of integers.

Theorem 1.2.2 (Bolzano-Weierstrass Theorem). *All limited suites admit a convergent subsuite.*

Lemme: If (x_n) converges, then all its subsuites converge to the same limit.

Proof

Let $L = \lim_{n \rightarrow \infty} x_n$ and $(x_{n_k})_{k=1}^\infty$ be a subsuite.

Let $\text{varepsilon} > 0$, we search for a $k_0; \forall k > k_0, |x_{n_k} - L| < \varepsilon$

We have $\exists N \forall n \geq N, |x_n - L| < \varepsilon$ and $\exists k_0 : n_k \geq N$. If $k \geq k_0, n_k \geq N \implies |x_{n_k} - L| < \varepsilon$. \square

Proof

Let $L = \lim_{n \rightarrow \infty} x_n$ and $(x_{n_k})_{k=1}^\infty$ be a subsuite with limit $L = \lim_{n \rightarrow \infty} x_{n_k}$. Note $z = \sup_{p \geq n} x_p, L = \lim_{n \rightarrow \infty} z_n$. $(n_k)_{k=0}^\infty$ by recurrence. $\exists N \forall n \geq N : |z_n - L| < 1/k$ (def of convergence for $\epsilon = 1/k$). Choose $n > N$, we have $\exists p \geq n : x_p > z_n - 1/k$, infacts $z_n - 1/k < x_p \leq z_n$. Now let $n_k = p$, then $|x_{n_k} - z_n| + |z_n - L| \geq |x_{n_k} - L| < 2/k$ So we have; $L - 2/k < x_{n_k} < L + 2/k \implies \lim_{k \rightarrow \infty} x_{n_k} = L$ \square

Def: Suite of Cauchy

A suite (x_n) is a Cauchy suite if

$$\forall \varepsilon > 0 \exists n_0 \in \mathbb{N} \forall n, m \geq n_0; |x_n - x_m| < \varepsilon$$

Alternatively we can write $\forall \varepsilon > 0 \exists n_0 : \forall n \geq n_0 \forall k \in \mathbb{N} : |x_n - x_{n+k}| < \varepsilon$

Theorem 1.2.3 (Converges of Cauchy's suites). *A suite converges \iff the suite is of Cauchy.*

Proof

1. " \Leftarrow " Suppose $L = \lim_{n \rightarrow \infty} x_n$. Let $\varepsilon > 0$.

For $\frac{\varepsilon}{2} \implies \exists n_0 \in \mathbb{N} \mid \forall n \geq n_0 : |x_n - L| < \frac{\varepsilon}{2}$, so we have $|x_n - x_m| \leq |x_n - L| + |x_m - L| < 2 \cdot \frac{\varepsilon}{2}$.

2. " \implies " We start by showing that a suit of Cauchy (x_n) is limited. Let $\varepsilon = 1$, then j , in particular $\forall n \geq n_0 : |x_n - x_{n_0}| < 1 \implies |x_n| < |x_{n_0}| + 1$. Donc $|x_n| \leq \max(|x_0|, |x_1|, \dots, |x_{n_0}| + 1)$, which implies it is limited.

Now, since the suit is limited, we can use BWT $\implies \exists$ a subsuite (x_{n_k}) that converges to L .

We show that $\lim_{n \rightarrow \infty} x_n = L$. Let $\varepsilon > 0$.

Cauchy tells us that $\forall \varepsilon > 0 \exists n_0 \in \mathbb{N} \forall n, m \geq n_0; |x_n - x_m| < \varepsilon/2$.

And we know $\exists k_0 \forall k \geq k_0; |x_{n_k} - L| < \varepsilon/2$

Let $n \geq n_0, \exists k \geq k_0 : n_k \geq n$, then $|x_n - L| \leq |x_n - x_{n_k}| + |x_{n_k} - L| < \varepsilon$. \square

1.3 Series

The goal is to study and define infinite sums.

Def: Infinite sum

The symbol $\sum_{n=0}^{\infty} x_n$ means $\lim_{p \rightarrow \infty} \left(\sum_{n=0}^p x_n \right)$, and we have that the infinite sum converges/diverges \iff the suite of partial sums $s_p = \sum_{n=0}^p x_n$ converges/diverges.

Rem: $\sum_{n=0}^{\infty} x_n = S$ and $\sum_{n=0}^{\infty} y_n = T \implies \sum_{n=0}^{\infty} (x_n + y_n) = S + T$.

This, as many of the proprieties and characteristics we will see in this chapter, are just mere consequences of proprieties and characteristics seen in the chapter on limits and suits.

Geom. Series For $|r| < 1$, $\sum_{n=0}^{\infty} r^n = \frac{1}{1-r}$

Harm. Series $\sum_{n=0}^{\infty} \frac{1}{n}$ diverges.

Theorem 1.3.1 (Cauchy's chains theorem). *The sum $\sum_{n=0}^{\infty} x_n$ converges $\iff \forall \varepsilon > 0, \exists n_0 \forall m \geq n \geq n_0 : |x_n + \dots + x_m| < \varepsilon$*

Rem: If $\sum_{n=0}^{\infty} x_n$ converges $\implies \lim_{n \rightarrow \infty} x_n = 0$. The inverse is however not true.

Rem: If $x_n \geq 0 \forall n$, then $\sum_{n=0}^{\infty} x_n$ converges \iff the suite of partial sums (s_n) is limited.

Theorem 1.3.2 (Comparason convergence Test). *If $0 \leq x_n \leq y_n, \forall n \geq n_0$, then*

$$\sum_{n=0}^{\infty} y_n \text{ converges} \implies \sum_{n=0}^{\infty} x_n \text{ converges}$$

Exemple of Series:

$$\sum_{n=2}^{\infty} \frac{1}{n(n-1)} \text{ converges to } 1$$

Note how $\frac{1}{n(n-1)} = \frac{1}{n-1} - \frac{1}{n}$ and if we substitue on the partial sums we optain $s_n = (\frac{1}{1} - \frac{1}{2}) + (\frac{1}{2} - \frac{1}{3}) + (\frac{1}{3} - \frac{1}{4}) + \dots + (\frac{1}{n-1} - \frac{1}{n}) = 1 - \frac{1}{n}$ so $\lim_{n \rightarrow \infty} s_n = 1$

$$\sum_{n=1}^{\infty} \frac{1}{n^2} \text{ converges to } \frac{\pi^2}{6}$$

Although we cant show that converges to that abomination of a number, we can show it converges, since $\frac{1}{n^2} \leq \frac{1}{n(n-1)}$

Rem: In general, for $p \in \mathbb{Z}$ $\sum_{n=1}^{\infty} n^{-p}$ converges $\iff p > 1$

Theorem 1.3.3 (Alternate convergence theorem). *Given a series (x_n)*

with $x_n x_{n+1} \leq 0, \forall n$ and $|x_n|$ is monotone towards 0, then $\lim_{n \rightarrow \infty} x_n = 0 \implies \sum_{n=0}^{\infty} x_n$ converges.

Def: Absolute convergence

The series $\sum_{n=0}^{\infty} x_n$ *converges absolutely* if the series $\sum_{n=0}^{\infty} |x_n|$ converges.

In general the absolute convergence has no relation with the normal notion of convergence. However:

Lemme: If $\sum_{n=0}^{\infty} x_n$ converges absolutely, then $\sum_{n=0}^{\infty} x_n$ converges.

Proof: $\forall n; 0 \leq x_n + |x_n| \leq 2|x_n|$, and since $\sum_{n=0}^{\infty} |x_n|$ converges, $\sum_{n=0}^{\infty} 2|x_n|$ converges as well. We have that $x_n + |x_n| \leq 2|x_n|$ is smaller term by term and thus $\sum_{n=0}^{\infty} x_n + |x_n| \leq 2|x_n|$ converges.

Given two series that converge, their difference converges. \square

Theorem 1.3.4 (Convergence-Permutations Theorem). *If $\sum_{n=0}^{\infty} x_n$ converges absolutely, then all the permutations of the series converge to the same number.*

Let us demonstrate the following reformulation of the theorem;

Given a bijection $\phi : \mathbb{N} \rightarrow \mathbb{N}$, $\sum_{n=0}^{\infty} x_{\phi(n)}$ converges to the value $\sum_{n=0}^{\infty} x_n$.

Proof

Case 1: $x_n \geq 0 \forall n$.

Let s_n be the partial sum of the series. We call t_n the partial sum of the terms under the indexes of $\phi(n)$.

We want to show that $L = \lim_{n \rightarrow \infty} s_n \implies L = \lim_{n \rightarrow \infty} t_n$. In fact, we have that $L = \sup\{s_n \mid n \in \mathbb{N}\}$ since s_n is monotonically increasing. We also have that t_n is monotonically increasing.

We have that $\forall n \exists m : t_n \leq s_m$. In fact we need $m = \max\{\phi(0), \phi(1), \dots, \phi(n)\}$.

$\implies \forall n : t_n \leq L$

$\implies (t_n)$ converges and $\sum_{n=0}^{\infty} x_{\phi(n)} \leq L$.

But we also have that $\sum_{n=0}^{\infty} x_n$ is a permutation of $\sum_{n=0}^{\infty} x_{\phi(n)}$ for $n \mapsto \phi^{-1}(n)$, and

by the same reasoning we have $\sum_{n=0}^{\infty} x_{\phi(n)} \geq L$. Thus we have $\sum_{n=0}^{\infty} x_{\phi(n)} = L$.

Case 2: In the same way, if $\forall n, x_n \leq 0$ we have the same reasoning and the same conclusion.

Case 3: We now have the difficult case. We define $a_n := \max(x_n, 0)$ and $b_n := \min(x_n, 0)$.

And we have that $\forall n, x_n = a_n + b_n$. To use this fact, we need to have that $\sum_{n=0}^{\infty} a_n$ and

$\sum_{n=0}^{\infty} b_n$ converge.

The first one converges because by definition, $\forall n, 0 \leq a_n \leq |x_n|$.

The second one converges since, again by definition, $\forall n, -|x_n| \leq b_n \leq 0$.

Thus the limit of the sums is the sum of the limits, $\sum_{n=0}^{\infty} x_n = \sum_{n=0}^{\infty} a_n + \sum_{n=0}^{\infty} b_n$.

Now, applying the first case to the first rhs summation and the second case to the second rhs summation, we have, $\sum_{n=0}^{\infty} a_{\phi(n)} + \sum_{n=0}^{\infty} b_{\phi(n)} = \sum_{n=0}^{\infty} x_{\phi(n)} = \sum_{n=0}^{\infty} x_{\phi(n)} = \sum_{n=0}^{\infty} x_{\phi(n)} x_n$.

□

Note that the theorem requires and is sufficient to that the the seire is absolutely convergent.

Theorem 1.3.5 (d'Almenbert II). Suppose $x_n \neq 0 \forall n$ et $\rho = \lim_{n \rightarrow \infty} \frac{x_{n+1}}{x_n}$.

If $\rho < 1 \implies \sum_{n=0}^{\infty} x_n$ converges.

If $\rho > 1 \implies \sum_{n=0}^{\infty} x_n$ diverges.

Proof

If $\rho > 1 \implies (x_n)$ diverges by *d'Alembert I*.

If $\rho < 1$ we have that $\exists n_0 \forall n \geq n_0 : |x_{n+1}| < \frac{\rho+1}{2} |x_n| \implies$, by recurrence, $\forall k, |x_{n_0+k}| < \left(\frac{\rho+1}{2}\right)^k |x_{n_0}|$. We have $\sum_{n=n_0}^{\infty} |x_n| < |x_{n_0}| \sum_{n=n_0}^{\infty} \left(\frac{\rho+1}{2}\right)^{n-n_0}$, which converges since $\frac{\rho+1}{2} < 1$. □

Theorem 1.3.6 (Teorema). Let $L = \limsup_{n \rightarrow \infty} \sqrt[n]{|x_n|}$.

If $L < 1 \implies \sum_{n=0}^{\infty} x_n$ converges absolutely.

If $L > 1 \implies \sum_{n=0}^{\infty} x_n$ diverges.

Proof

Let $L < 1$.

$\exists n_0 \forall n \geq n_0 : \sqrt[n]{|x_n|} < \frac{L+1}{2} \implies |x_n| < \left(\frac{L+1}{2}\right)^n$. So $\sum_{n=0}^{\infty} x_n$ converges by comparason.

Let $L > 1$.

Then x_n does not fall to 0 and thus $\sum_{n=0}^{\infty} x_n$ diverges. □

Chapter 2

Linear Algebra

Linear Systems (Introduction)

One variable Equations

Let $a, b \in \mathbb{R}$ The equation $ax = b$ has the following number of solutions. There are three cases:

1. $a \neq 0$ the single solution is $x = \frac{b}{a}$.
2. $a = 0, b = 0$ there are infinite solutions.
3. $a = 0, b \neq 0$ there are no solutions at all.

Two variable equation system

We can see a set of 2 equations with 2 variables as 2 lines on the plane. The coordinates of the intersection (if any, or if they are not parallel) is the solution to the system.

The case in which the second equation is a multiple of the first, infinite equations arise, since they represent the same line on the plane. Each point of the line is thus a solution, since by definition lies also on the second one.

Three variable equation system

We can see a set of 3 equations with 3 variables as 3 planes in space (as $\subset \mathbb{R}^3$ if that even means something at this point of the course)

2.1 Matrix Calculus

Def: Matrix

A Matrix $m \times n$ is a rectangular table of values arranged over m lines and n colons, where $m, n \in \mathbb{N}$

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix}$$

The elemens are noted as a_{ij} with i the line and j the colom. These elements are usually real numbers. We note all of this information with the notation $M_{n \times m}(\mathbb{R})$

We define $(A)_{ij}$ as the element on the i -th line and j -th coloumns of the matric A .

Def: Vector

In this course, we define a vector as an element of the set $M_{m \times 1}(\mathbb{R})$.

We call line vector an element of $M_{1 \times n}(\mathbb{R})$

2.1.1 Special matrixes

If $m = n$ we call the matrix a *matrice carree* .

If all the elements of the matrix are 0s, the matrix is called *matrice nulle*, written as $0_{m \times n}$.

If a matrix has all the elements not on the diagonal 0, we call the matrix *matrice diagonale*. These elements are on the diagonal of the matrix.

If the matrix is not square, the definition still holds: the diagonal are the elements of the kind a_{ii} .

If a diagonal square matrix is formed by 1s, we call the matrix *matrice identite*, written as Id_n .

2.1.2 Operations on matrixes

Scalar Multiplication

Let $A \in M_{m \times n}(\mathbb{C})$, $\lambda \in \mathbb{R}$ Element by element: $\lambda \cdot A \rightarrow (\lambda \cdot A)_{ij}$ Meaning each elemnt is multiplied by the scalar

Addition

It is element by element. $A = B + C$ But $A, B, C \in M_{m \times n}(\mathbb{C})$, meaning they have the same *tile* (the same number of lines and coloumns).

We note that, for $A, B, C \in M_{m \times n}(\mathbb{R})$, $\alpha, \beta \in \mathbb{R}$ we have:

1. $(\alpha\beta)A = \alpha(\beta A)$
2. $(\alpha + \beta)A = \alpha A + \beta A$
3. $\alpha(A + B) = \alpha A + \alpha B$
4. $A + B = B + A$
5. $A + 0_{m \times n} = A$
6. $A + (-1 \cdot A) = 0_{m \times n} \rightarrow B - A = B + (-1 \cdot A)$

Def: Matrix-Vector product

Let $A \in M_{m \times n}(\mathbb{R})$, $v \in M_{n \times 1}(\mathbb{R})$. We have:

$$w = A \cdot v \in M_{m \times 1}(\mathbb{R})$$

Where the elements of w are given by $w_i = \sum_{k=1}^n a_{ik} v_k$.

As an exemple we have equation systems written as matrix \cdot vector. In general:

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= b_m \end{aligned}$$

We take as a subsequential exemple the Fibonacci sequence: $1, 1, 2, 3, 5, 8, 13, 21, 34, 55, \dots$ where $e_0 = 1, e_1 = 1, e_n = e_{n-1} + e_{n-2}$. We can define a vector

$$\begin{aligned} b_k &= \begin{bmatrix} e_k \\ e_{k+1} \end{bmatrix} \in M_2(\mathbb{R}), \quad b_0 = \begin{bmatrix} 1 \\ 1 \end{bmatrix} \\ b_{k+1} &= \begin{bmatrix} e_{k+1} \\ e_k + e_{k+1} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} e_k \\ e_{k+1} \end{bmatrix} \end{aligned}$$

Def: Matrix product

Let $A \in M_{m \times p}(\mathbb{R})$ and $B \in M_{p \times n}(\mathbb{R})$, we have

$$AB = C \in M_{m \times n}(\mathbb{R})$$

Where $c_{ij} = \sum_{k=1}^p a_{ik} b_{kj}$. We can show the associativity of the composition of matrix multiplication in the form of

$$A(Bv) = (AB)v$$

Multiplication by Special matrixes

1. It's easy to show that $0A = A0 = 0$, $\forall A \in M_{m \times n}(\mathbb{R})$
2. We can show that $Id_n A = A Id_n = A$, $\forall A \in M_{m \times n}(\mathbb{R})$.
3. Let $D = \begin{bmatrix} d_{11} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & d_{nn} \end{bmatrix}$ be a diagonal matrix, DA is a matrix whose columns are the columns of A multiplied by the diagonal element of the corresponding line/columns in D .

Properties of the matrix-product

1. For $A \in M_{m \times n}(\mathbb{R})$, $B \in M_{n \times p}(\mathbb{R})$, $C \in M_{p \times q}(\mathbb{R})$ then, $(AB)C = A(BC)$
2. $(A + B)C = AC + BC$
3. $A(B + C) = AB + AC$

In short we can say that $(M(\mathbb{R}), +, \cdot)$ is a non-commutative Corp for the suitable dimensions of matrix multiplication.

On a last and totally related note, we can say that matrix-vector multiplication Ax is a linear combination of the columns (a_i) of A , with the coefficients of combination giving the vector x , giving $Ax = a_1x_1 + a_2x_2 + \cdots + a_nx_n$.

Vector Composition Form

We can write the matrix A with the following notation, where a_i here are the columns of A :

$$A = (a_1 | a_2 | \cdots | a_n) \quad , \quad a_i = \begin{bmatrix} a_{1i} \\ a_{2i} \\ \vdots \\ a_{ni} \end{bmatrix}$$

We can so write the identity matrix as a composition of the standard vector base of \mathbb{R}^n :

$$Id_n = (e_1 | e_2 | \cdots | e_n) \quad , \quad e_j = \begin{bmatrix} 0 \\ \vdots \\ 1_j \\ \vdots \\ 0 \end{bmatrix}$$

2.1.3 Trace of a Matrix

Given the square matrix $A \in M_{n \times n}(\mathbb{R})$, we define the trace $trace(A)$ to be the sum of the elements on its diagonal.

It's important to see that the trace is invariant of multiplication order, meaning

$\text{trace}(BC) = \text{trace}(CB)$, even if BC has a different number of lines and columns to CB . As a brief proof we consider $A = BC, \hat{A} = CB$:

$$\begin{aligned}\text{trace}(BC) = \text{trace}(A) &= \sum_{i=1}^m a_{ii} = \sum_{i=1}^m \sum_{k=1}^n b_{ik} c_{ki} \\ &= \sum_{k=1}^n \sum_{i=1}^m c_{ki} b_{ik} = \sum_{k=1}^n \hat{a}_{kk} = \text{trace}(\hat{A}) = \text{trace}(CB)\end{aligned}$$

Abstract on Summations

We define a symbol of successive addition to be:

$$\sum_{i=m}^n a_i$$

Where we call:

i the index of summation

a_i is a variable with an index

m, n are the lower and upper bound of the index

we can sometimes impose a special condition on the index i (like i is even).

We then define the empty sum $\sum_{i=1}^0 a_i = 0$ null. We note the linearity of the summation.

The summation is also invariant on index shifting:

$$\sum_{i=m-1}^{n-1} a_{i+1} = \sum_{i=m}^n a_i = \sum_{i=m+1}^{n+1} a_{i-1}$$

Considering now this example of a double summation with chained indexes:

$$\sum_{i=1}^n \sum_{j=1}^i a_{ij} = (a_{11}) + (a_{21} + a_{22}) + \cdots + (a_{n1} + a_{n2} + \cdots + a_{nn})$$

where the index j is bounded by the index i , so at every iteration of the outer sum, the inner sum gains a new term.

2.1.4 Transposition of a Matrix

Given $A \in M_{m \times n}(\mathbb{R})$, we define the transpose $A^T \in M_{n \times m}(\mathbb{R})$ defined as:

$$(a)_{ij}^T = (a)_{ji}$$

As an example take:

$$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix}^T = \begin{bmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{bmatrix}$$

Properties of the transpose

1. **Linearity**: no need to write it all...
2. $(A^T)^T = A$
3. $(AB)^T = B^T A^T$ (simply by the fact that $A^T B^T$ is not always defined)

2.1.5 Symmetric Matrixes

Def: Symmetric matrix

A square matrix $A \in M_{n \times n}(\mathbb{R})$ is called symmetric iff:

$$A^T = A$$

Def: Antisymmetric Matrixes

A square matrix $A \in M_{n \times n}(\mathbb{R})$ is Antisymmetric iff:

$$A^T = -A$$

Note that the elements on the diagonal aof an antisymmetric matrix are 0s. Note that $\forall A \in M_{n \times n}(\mathbb{R})$,

$$A_s = \frac{A + A^T}{2} = \frac{A^T + A}{2} = A_s^T$$

$$A_a = \frac{A - A^T}{2} = \frac{A^T - A}{2} = -A_s^T$$

Also let $A \in M_{m \times n}(\mathbb{R})$ be symmetric and $B \in M_{m \times n}(\mathbb{R})$, then

$$BAB^T$$

is symmetric (symmetricity is invariant by similarity).

2.1.6 Inverse Matrixes

Def: Inverse Matrix

Given a square matrix $A \in M_{n \times n}(\mathbb{R})$ if there exists another matrix $X \in M_{n \times n}(\mathbb{R})$ such that:

$$AX = XA = Id_n$$

If such matrix X does not exists, the matrix A is not inversible. We sometimes call $X := A^{-1}$.

For the real numbers ($n = 1$), A is inversible $\iff A \neq 0$.

If A is invertible, it's inverse A^{-1} is unique, trivially.

Given $A, B \in M_{n \times n}(\mathbb{R})$ invertible matrixes. Then

1. $(A^{-1})^{-1} = A$
2. $(AB)^{-1} = B^{-1}A^{-1}$
3. $(A^T)^{-1} = (A^{-1})^T$

2.1.7 Sub Matrixes

Def: SubMatrix

Given a matrix $M \in M_{m \times n}(\mathbb{R})$ $I = \{i_1, \dots, i_k \mid k \leq m\}$, $J = \{j_1, \dots, j_l \mid l \leq n\}$, we define $A(I, J) \in M_{k \times l}(\mathbb{R})$ the matrix given by the elemetns of M in the intersections of the rows listens in I and the coloums listed in J .

If $I = J$ this submatrix is said to be a principal sub matrix.

2.2 Algebraic Structures

Def: Linear Operation

Given a set G and an operation $*$: $G \times G \rightarrow G$, $(a, b) \mapsto a * b$ is a linear operation on G if:

1.

Def: Group

$(G, *)$ is a group if, given a set G and a binary operation $*$: $G \times G \rightarrow G$,

1. $*$ is associative, meaning $\forall a, b, c \in G; a * (b * c) = (a * b) * c$.
2. There exists a neutral element, such that $\exists e \in G \mid \forall a \in G, a * e = e * a = a$.
3. There exists the inverse element, such that $\forall a \in G, \exists a^{-1} \mid a * a^{-1} = a^{-1} * a = e$.

We could also give the following, a little weirder, definition:

Def: Group (alternative definition)

Let $(G, *)$ be a pair (set, operation), where $*$ is associative on G .

We say that $(G, *)$ is a group \iff

1. $\exists e_y \in G \mid e_y * a = a$
2. $\forall a \in G, \exists a_y^{-1} \in G \mid a_y^{-1} * a = e_y$

Proof

" \Leftarrow " is trivial.

" \Rightarrow " is more interesting. Let $a \in G : a_y^{-1} * a = e_y, \exists \hat{a} : \hat{a} * a_y^{-1} = e_y$.

Then $a * a_y^{-1} = e_y * a * a_y^{-1} = \hat{a} * a_y^{-1} * a_y^{-1} = \hat{a} * e_y * a_y^{-1} = \hat{a} * a_y^{-1} = e_y \implies 3$.

And $a * e_y = a * a_y^{-1} * a = e_y * a = a \implies 2$.

□

Classic Properties of Groups

Given a group $(G, *)$, we have:

1. the neutral element is unique.
2. the inverse of an element is unique.
3. $(a^{-1})^{-1} = a$
4. $(a * b)^{-1} = b^{-1} * a^{-1}$

It is really important that G is stable under $*$. A group in which the operation commutes is said "abelian", or commutative, and the 4 property is not special.

Def: Monoid

$(H, *)$ is a monoid if, given a set H and a binary operation $*$: $H \times H \rightarrow H$,

1. $*$ is asociative, meaning $\forall a, b, c, \in G; a * (b * c) = (a * b) * c$.
2. There exists a neutral element, such that $\exists e \in G \mid \forall a \in G, a * e = e * a = a$.

Remark: Let $(H, *)$ be a monoid, then $(H^*, *)$ is a group, where

$$H^* = \{a \in H \mid \exists a^{-1} \in H; a^{-1} * a = e\}$$

This is obvious since we are excluding from H the elements without an inverse.

We have that $(\{1\}, \cdot)$ is the group with the smallest cardinality.

We define $GL(n) = (M_{n \times n}(\mathbb{R})^*, \cdot)$

Def: Application

Let E be a non empty set. Then

$$App(E) = \{f : E \rightarrow E \mid f \text{ is an application}\}$$

The composition $f \circ g \in App(E) \mid (f \circ g)(x) = f(g(x)) \forall x \in E$. Then $(App(E), \circ)$:

1. $App(E)$ is closed by definition of \circ .
2. Composition is associative since

$$(f \circ (g \circ h))(x) = f(g(h(x))) = ((f \circ g) \circ h)(x)$$

3. The neutral element is $Id_E : E \rightarrow E, x \mapsto x, \forall x$ since

$$Id_E(f(x)) = f(x) = f(Id_E(x))$$

It follows that $(App(E), \circ)$ is a monoid and $(App(E)^*, \circ)$ is a group, where $App(E)^* := Bij(E)$ is the set of the bijections form E to E . This group is called the symmetric group.

Note how $Bij(\{1, 2, 3, \dots, n\}) = S_n$ are the permutations of the n elements. It means S_n is the set of arbitrary one-to-one functions from a set of n elements to itself. Its cardinality is $|Bij(\{1, 2, 3, \dots, n\})| = n!$

Def: Subgroup

Let $(G, *)$ be a group and $H \subset G$, than
 $(H, *)$ is a group $\iff (H, *)$ is a subgroup of G .

We have that $(H, *)$ is non empty, closed under the operation and admits inverse to every element. As an exemple $(\{e_G\}, *)$ is the trivial subgroup of every group. The ortogonal

group $SO(2) := \left\{ G(\phi) = \begin{bmatrix} \cos \phi & \sin \phi \\ -\sin \phi & \cos \phi \end{bmatrix} \right\}$ is a subgroup of $GL_2(\mathbb{R})$.

2.2.1 Morphisms between Groups

Def:

Given $(G, *)$ and (H, \circ) groups, a group morphism is a function $f : G \rightarrow H$ such that

$$f(a * b) = f(a) \circ f(b)$$

If f is a bijection, it is called an isomorphism and the two groups are isomorphic.

Where the lhs is an image of an element in G and the rhs is an element in H given by the binary operation on the images of elements in G . **Lemme:** Let $f : G \rightarrow H$ be a morphism. Then

1. $(e_G) = e_H$
2. $(a)^{-1} = (f(a))^{-1}$

As an exemple $f(\alpha) = \alpha Id_n$ is an isomorphism.

2.2.2 Rings

Def: Ring

The mathematical object $(A, +, \cdot)$ is a ring if $(A, +)$ is an abelian group, (A, \cdot) is a monoide, and the two operation are double distributive.

If the monoid is commutative, the ring is said commutative.

$(\mathbb{R} \cup \{\infty\}, \circ, \cdot)$ where $a \circ b = \min\{a, b\}$ is not a ring.

Lemme: If $(A, +, \cdot)$ is a ring, $(A[t], +, \cdot)$ is a ring itself. The two are connectively commutative.

Lemme: Let $(A, +, \cdot)$ be a ring, then

1. $-a = (-1) \cdot a$
2. $0 \cdot a = a \cdot 0 = 0$
3. $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$
4. $(-a)(-b) = ab$

Def:

Given $(A, +, \cdot)$ and (B, \circ, \times) rings, a ring morphism is a function $f : A \rightarrow B$ such that

$$f(a + b) = f(a) \circ f(b) \wedge f(a \cdot b) = f(a) \times f(b)$$

We also need that $f(1_A) = 1_B$ If f is a bijection, it is called an isomorphism and the two rings are isomorphic.

Def: SubRing

Let $(A, +, *)$ be a ring and $B \subset A$, than
 $(B, +, *)$ is a ring $\iff (B, +, *)$ is a subring of A .

2.2.3 Matrixes of ring's coefficients

Theorem 2.2.4 (Matrix Rings). *Let $(A, +, \cdot)$ be a ring, then $(M_{n \times n}(\mathbb{A}), +, \cdot)$ is a ring as well.*

2.2.5 Fields or Corps

Def: Corp [Field]

A Corp is a commutative Ring $(K, +, \cdot)$ such that $K \neq \{0\}, \forall a \in K \setminus \{0\} \quad \exists a^{-1} \mid a \cdot a^{-1} a^{-1} \cdot a = 1$. Alternatively, $(K, +, \cdot)$ is a field if $(K, +), (K \setminus \{0\}, \cdot)$ are an abelian group and the two operations are distributive.

2.2.6 Complex Numbers

We all know the subject, i'm sorta not taking notes at this point. And btw why is this in the section of groups In short we can say that $(\mathbb{C}, +)$ is an abelian group. Also $(\mathbb{C} \setminus \{0\}, \cdot)$ is a group. And so $(\mathbb{C}, +, \cdot)$ is a Field with cannon standard elements (we skipped all the middle checks, but it is easy to verify that all the normal proprieties hold true).

Now, noting somethin more interesting: There exists an isomorphism

$$\varphi : \mathbb{R} \rightarrow M_2, (x + iy) \mapsto \begin{bmatrix} x & -y \\ y & x \end{bmatrix}$$

where the conjugate goes to the transpose, and the modulo to the determinant.

2.3 Echelonnee Form

2.4 Vector Spaces

2.5 Linear Applicaiton

2.6 Proper Value

2.7 Stochastic Matrix

Chapter 3

Algebraic Structures

Introduction

The subjects of the course are, at first, consequential and formal logic, with all its symbols and sign notations. We then want to begin with sets, to build up to the concept of groups. We want to study the generality of groups, and not only see examples of them, but rather study them as an overarching structure, found in all fields of mathematics. On more of an unofficial objective is to get use to abstract reasoning, and learn how to come up and write proofs.

The most important thing is to submit the starred exercises the Monday exercise section.

3.1 Formal Logic

Fuck off do it yourself

3.2 Sets

It's sort of a hard definition to give, especially if we want to maintain the rigor to which we aim in this course.

Def: Set

A Set is a collection of "things" called elements.

We note a set with a capital letter, and we can list its elements in curly brackets, or by describing those elements.

We note, $a \in A \iff a$ is an element of A , and $B \subseteq A$ meaning B is a subset of A , rigorously described as:

$$(B \subseteq A) \implies (b \in B \implies b \in A)$$

By convention a set cannot have two times the same element.

The notion of set is cloudy, but it is sort of an important aspect given the Godel/incompleteness Theorem, so that logical contradictions as *Russel's Paradox*. Take the set:

$$B = \{A \mid A \notin A\}$$

This causes no problems for the majority of sets: however considering B itself we arrive at a contradiction. If $B \in B$, by definition B cannot be in B , and at the same time if B is not in B , it satisfies the conditions to be in B .

3.2.1 Zermelo-Finkel's Axioms (1920)

Those two fellas have posed some axioms to better define the concept of axiom. We won't list them here, as they are strictly beyond the scope of this course (funny, innit), but we will list some of their remarkable consequences:

1. The empty set \emptyset is contained in every other set: $\forall A, \emptyset \subset A$
2. $A \cap B = \{e \mid e \in A \wedge e \in B\}$
3. $A \cup B = \{e \mid e \in A \vee e \in B\}$
4. $A \setminus B = \{e \mid e \in A \wedge e \notin B\}$
5. $2^A = \{B \mid B \subseteq A\}$, called the set of subsets of A .
6. $A \times B = \{(a, b) \mid a \in A, b \in B\}$, called the cartesian product of A and B

3.2.2 Application

Def: Application

An Application $\varphi : A \rightarrow B$ is a subset $\Gamma_\varphi \subseteq A \times B$ such that:

$$\forall a \in A, \exists! b \in B \mid (a, b) \in \Gamma_\varphi$$

We call A the domain of φ and B the codomain of φ .

We can write the image of φ as $\varphi(A) := \{\varphi(a) \in B \mid a \in A\}$. As an exemple, $id : A \rightarrow A$, such that

$$\forall a \in A \quad id(a) = a \iff \Gamma_\varphi = \{(a, a) \in A \times A \mid a \in A\}$$

Def: Linear Application

Let $\varphi : A \rightarrow B$.

1. φ is injective $\iff \varphi(a) = \varphi(a') \implies a = a'$.
2. φ is surjective $\iff \forall b \in B, \exists! a \in A \mid \varphi(a) = b$.
3. φ is bijective $\iff \varphi$ is both injective and surjective.

Exemples: $id : A \rightarrow A$ is a bijection.

$f : \mathbb{R} \rightarrow \mathbb{R}, f(x) = x^2$ is not injective nor surjective,

however $f : \mathbb{R} \rightarrow \mathbb{R}_+, f(x) = x^2$ is surjective and $f : \mathbb{R}_+ \rightarrow \mathbb{R}, f(x) = x^2$ is injective.

Composition of applications

Def: Composition

Given $\varphi : A \rightarrow B$ and $\xi : B \rightarrow C$. We define: $\varphi \circ \xi : A \rightarrow C$

$$\text{such that } \forall a \in A, \xi \circ \varphi(a) = \xi(\varphi(a)) \in C \text{ and} \\ \Gamma_{\xi \circ \varphi} = \{(a, c) \in A \times C \mid \exists b \in B; (a, b) \in \Gamma_{\varphi}, (b, c) \in \Gamma_{\xi}\}$$

We can now prove the lemme:

Theorem 3.2.3 (Composition-Inj-Surj relations). *Given $\varphi : A \rightarrow B$ and $\xi : B \rightarrow C$,*

1. *if φ and ξ are **injective**, $\implies \xi \circ \varphi$ is also **injective**.*
2. *if φ and ξ are **surjective**, $\implies \xi \circ \varphi$ is also **surjective**.*
3. *if $\xi \circ \varphi$ is **injective**, $\implies \varphi$ is **injective**.*
4. *if $\xi \circ \varphi$ is **surjective**, $\implies \xi$ is **surjective**.*

Def: Inverse of an Application

Let $\varphi : A \rightarrow B$ be a bijection. The inverse $\varphi^{-1} : B \rightarrow A$ is defined by

$$\forall b \in B, \exists! a \in A, \phi(a) = b \implies \varphi^{-1}(b) = a$$

Its graph deifnition is

$$\Gamma_{\varphi^{-1}} = \{(b, a) \in B \times A \mid \varphi(a) = b\}$$

Note that $\varphi \circ \varphi^{-1} = Id_B, \varphi^{-1} \circ \varphi = Id_A$

3.2.4 Equivalent Relations

Def: Equivalence Relation

Given a non empty set A , an equivalence relation on A is a subset $R \subseteq A \times A$ such that:

1. Reflexive: $\forall a \in A, (a, a) \in R$.
2. Simmteric: $\forall a, b \in A, (a, b) \in R \implies (b, a) \in R$.
3. Transitive: $\forall a, b, c \in A, (a, b) \in R \wedge (b, c) \in R \implies (a, c) \in R$

A more simple notation is to write the equivalente relation as $a =_R b \iff (a, b) \in R$.

1. Reflexive: $\forall a \in A, a = a$.
2. Simmteric: $\forall a, b \in A, a = b \implies b = a$.
3. Transitive: $\forall a, b, c \in A, a = b, b = c \implies a = c$

Given an integer $m > 0$. We define equivalence relation R on \mathbb{Z} :

$$(a, b) \in R \subseteq \mathbb{Z} \times \mathbb{Z} \iff m \mid a - b$$

meaning m devides $a - b$. In other words a and b have the same reminder when divided by m .

We need to simply show that:

1. $(a, a) \in R$, which is clear, since $m|a - a$.
2. $m|a - b \iff m|b - a$ since $a - b = -1(b - a)$.
3. $m|a - b \wedge m|b - c \implies m|(a - b) + (b - c) \implies m|a - c$, since $m|f \wedge m|g \implies m|f + g$

Working on this, we define something that will be useful later.

Def: Equivalence Class

Let $R \in A \times A$. For $a \in A$, its equivalence class is

$$R_a = \{b \in A \mid (a, b) \in R\}$$

Listing some proprieties we have:

1. $(a, b) \in R \iff R_a = R_b$
2. $(a, b) \notin R \iff R_a \cap R_b = \emptyset$

Def: Equivalence Class Modulo m

Given a set A , and a relation $(a, b) \in R \subseteq \mathbb{Z} \times \mathbb{Z} \iff m|a - b$ we have

$$R_a = \{a + cm \mid c \in \mathbb{Z}\} \text{ and we write } a \equiv b \pmod{m}$$

Def: Partition

Given a non empty set A , a set $X \in 2^A \mid \forall a \in A, \exists$

[...]

Theorem 3.2.5 (Cantor-Schroder-Bernstein Theorem). If $|A| \leq |B| \wedge |B| \leq |A| \implies |A| = |B|$

Remember that $|B| \leq |A|$ means that there is an injective application from A to B . We want to find a bijection between the two. Let $f : A \rightarrow B$, $g : B \rightarrow A$. The idea is that if $a \in g(B) \implies \exists! b \in B \mid g(a) = b$, we define $h(a) := b$ and if $a \notin g(A)$, then $h(a) = f(a)$.

Proof: Let $C_0 = A \setminus g(B)$, $C_1 = g(f(C_0))$, \dots , $C_n = g(f(C_{n-1}))$ and C is the union of those C_i . We have that $A \setminus C \subseteq A \setminus C_0 = g(B)$.

We define $h : A \rightarrow B$ for $h(a) = f(a)$ if $a \in C$, $h(a) = b \mid g(b) = a$ if $a \in A \setminus C$. We now need to prove that h constructed this way is a bijection.

1. Injection: Suppose $a, b \in A : h(a) = h(b)$ $a, b \in C \implies f(a) = h(a) = h(b) = f(b) \implies a = b$.
2. Injection: If $a, b \in A \setminus C$ we have $c = h(a) = h(b) = d$ where $c, d \in B : g(c) = a, g(d) = b$ this implies $a = b$
3. Injection: $a \in C, b \in A \setminus C$ we have $f(a) = c$ where $c \in B : g(c) = b \implies b = g(c) = g(f(a)) \in C$, but $\exists n \geq 0; a \in C_n \implies g(f(a)) \in C_{n+1} \subset C \implies b \notin C$.
4. Surjection: $\forall c \in B, g(b) \in C \implies b \in h(C) : g(b) \in C \implies \exists n \geq 0 \mid g(b) \in C_n$. If $n = 0$, $g(b) \in A \setminus g(B)$, again, a contradiction. So $n \geq 1$ and $g(b) \in g(f(C_{n-1})) \implies b \in f(C_{n-1}) \subset f(C) = h(C)$.

Now, choosing an element $b \in B$, we have two cases. If $b \in f(C) = h(C) \implies \exists a \in C \mid h(a) = b \checkmark$.

Else $b \notin f(C) = h(C) \implies g(b) \notin C$, since $g(b) \in C \implies b \in h(C)$. So $h(g(b)) = b$.

3.3 Number Theory

Def: Greatest Common Division

Given $(a, b) \in \mathbb{Z}^2 \neq (0, 0)$ we define the greatest common divisor to be

$$\gcd(a, b) = \max\{m \in \mathbb{N} \mid m|a \wedge m|b\}$$

We have the following proprieties:

1. $\gcd(a, b) = \gcd(b, a)$
2. $\gcd(-a, b) = \gcd(a, b)$
3. $\forall r \in \mathbb{Z}, \gcd(a, b) = \gcd(a, b + r \cdot a)$

Whilst the first two arise trivially, for the third will suffice to say that $\forall r \in \mathbb{Z} m|a \implies m|a + r \cdot a$.

3.4 Group Theory

Def: Gruppi

A group is a mathematical object (G, \cdot) , as a pair of a set and a closed binary application on the set $\cdot : G \times G \rightarrow G$, that has the following proprieties.

1. The binary operation is associative.
2. There exist a lefthand nutral element.
3. There exist a lefthand inverse.

Those characteristics of a group are equivalent to the classic one we saw in LinAlg.

We note that $f \cdot g$ is a binary operation called multiplication and we often omit the dot. Moreover for associativity we can write fgh as a well define notation. The inverse $g \mapsto g^{-1}$ is a stronger operation (and thus has priority) over the normal multiplication.

The order of a group is noted as $|G|$ if it is finite. We will study finite groups.

As examples, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Q} \setminus \{0\}, +)$ are all groups.

To maintain coherence we need to have, for all groups, that

1. The lefthand inverse is also a righthand inverse. For $hg = e$

$$gh = egh = h^{-1}hgh = h^{-1}eh = e$$

2. The lefthand neutral element e is also the righthand neutral element.

$$g = ge = g(g^{-1})g = (gg^{-1})g = eg$$

3. The neutral element is unique.

$$e = e\rho = \rho \implies e = \rho$$

4. The inverse element is unique. For $hg = e$

$$hgg^{-1} = eg^{-1} \implies he = eg^{-1}$$

5. The inverse: $(fg)^{-1} = g^{-1}f^{-1}$.

Notation: Given $n \in \mathbb{Z}$ et $g \in G$, we have: $x^n := \begin{cases} e & \text{if } n = 0 \\ g \cdots g & \text{if } n > 0 \\ g^{-1} \cdots g^{-1} & \text{if } n < 0 \end{cases}$

Def: Order of a Group

For a group (G, \cdot) and an element $g \in G$ the order $o(g)$ is the smallest $n \in \mathbb{N} \mid g^n = e$. If $\forall n > 0, g^n \neq e$ we write $o(g) = \infty$.

Given a set X , the set

$$Bij(X) := \{f : X \rightarrow X \mid f \text{ is a bijection}\}$$

forms a group with the function Composition $\circ : f \circ g(x) \mapsto f(g(x))$ (with $x \in X$).

The proprieties are easy to demonstrate, and we already did this in the course of linear algebra.

Chapter 4

Meccanics

4.1 Introduction

Differential Calculus

Def: Velocity

We define Velocity as the derivative of the position, where the derivative is written as

$$v(t) = \dot{x}(t) = \frac{dx}{dt} = \lim_{h \rightarrow 0} \frac{x(t+h) - x(t)}{h}$$

Using differential notation we can write: $dx = v \cdot dt$

Def: Acceleration

We define Acceleration as the derivative of the velocity, where the derivative is written as

$$a(t) = \ddot{x}(t) = \frac{d\dot{x}}{dt} = \lim_{h \rightarrow 0} \frac{\dot{x}(t+h) - \dot{x}(t)}{h}$$

Using differential notation we can write: $d\dot{x} = a \cdot dt$

Now consider the following derivatives:

1. $\frac{d}{dt}g(t) = \frac{g(t+dt) - g(t)}{dt} \implies g(t+dt) = g(t) + dg$
2. $\frac{df}{dg} \frac{f(g+dg) - f(g)}{dg} \implies f(g+dg) = f(g) + df$
3. $\frac{d}{dt}f(g(t)) = \dots = \frac{df}{dg} \frac{dg}{dt}$

The derivative of the following functions are:

1. $x(t) = A \cos(\omega t + \varphi)$
 $\implies \frac{dx}{dt} = \frac{dA \cos(\omega t + \varphi)}{d(\omega t + \varphi)} \cdot \frac{\omega t + \varphi}{dt}$
2. $T(t) = \frac{1}{2}m\dot{x}^2$
 $\implies \frac{dT}{dt} = \frac{d(\frac{1}{2}m\dot{x}^2)}{d\dot{x}} \cdot \frac{\dot{x}}{dt}$

Def: Infinitesim Identity

$$f(x + dx) = f(x) + \frac{df}{dx}dx$$

This identity becomes an approximation for $\Delta x \ll x$. This form arises from the Taylor expansion of the function $f(x + \Delta x)$ truncated to the first order.

Vector Calculus**Def: Vector**

We will define vectors as segment with an orientation, forgetting about vector classes.

Def: Repere vectoriel

A Repere is a geometrical entity formed by three linearly independent vectors attached to the same point, called origin.

A Repere is called ortonorme iff the 3 vectors are perpendicular to each other. A repere direct (repgdir or rd) is the one formed by ordering the vectors on your right hand, the one formed with your left hand is called Repere indirect. The first vector goes on the pointing finger, the second on the middle and the third on the thumb.

Def: Scalar Product

Let $(\hat{x}_1, \hat{x}_2, \hat{x}_3)$ be a repere direct (rd). Let $\vec{a} = a_1\hat{x}_1 + a_2\hat{x}_2 + a_3\hat{x}_3$. The scalar product is defined as

$$scal(\vec{a}, \vec{b}) : V \times V \rightarrow \mathbb{R}$$

$$(\vec{a}, \vec{b}) \rightarrow \vec{a} \cdot \vec{b} = a_1b_1 + a_2b_2 + a_3b_3$$

Note that this product is commutative.

We note $|\vec{a}|$ as the length of the vector \vec{a}

Def: Vector Projection

Let \vec{a} be a vector, its projection on a vector \vec{v} with which it forms an angle θ is given by

$$|\vec{a}| \cos \theta \hat{v}$$

In general we can write the following identity:

$$\vec{a} \cdot \vec{b} = |\vec{a}| |\vec{b}| \cos \theta$$

Def: Vector product

Let $(\hat{x}_1, \hat{x}_2, \hat{x}_3)$ be a repere direct (rd). Let $\vec{a} = a_1\hat{x}_1 + a_2\hat{x}_2 + a_3\hat{x}_3$. The vector product is defined as

$$vect(\vec{a}, \vec{b}) : V \times V \rightarrow V$$

$$(\vec{a}, \vec{b}) \rightarrow \vec{a} \times \vec{b} = (a_2b_3 - a_3b_2)\hat{x}_1 + (a_3b_1 - a_1b_3)\hat{x}_2 + (a_1b_2 - a_2b_1)\hat{x}_3$$

In general, the vector product of two products gives a vector perpendicular to both vectors, with length representing the area of the parallelogram formed by those two vectors, and direction given by the right hand rule. Note the following characteristics of the vector product.

The main property is the anticommutativity, meaning:

$$\vec{a} \times \vec{b} = -\vec{b} \times \vec{a}$$

Note that this product is not associative, meaning

$$(\vec{a} \times \vec{b}) \times \vec{c} \neq \vec{a} \times (\vec{b} \times \vec{c})$$

There is also a mixed product, but who cares ... We finally arrive at the following, very slightly useful, vector identity:

$$\vec{a} \times (\vec{b} \times \vec{c}) = (\vec{a} \cdot \vec{c})\vec{b} - (\vec{a} \cdot \vec{b})\vec{c}$$

Because we like to be coherent, let's write the following vectors in cinematic and dynamic:

- Position Vector: $\vec{r}(t)$
- Velocity Vector: $\vec{v}(t)$
- Acceleration Vector: $\vec{a}(t)$
- Force vector: $\vec{F}(t)$
- Quantity of motion vector: $\vec{p}(t)$
- Kinetic Momentum vector: $\vec{L}(t)$

Cinematic

For the material point approximation, we sacrifice the proper rotation of the object. However we can still bring forward this approximation because, at normal scale, all the forces can be considered to be applied on the center of mass of the object, which will be the material point. With those approximations we also incur in errors caused by the moment of inertia of the object, which is totally ignored here.

As for discussing motion, we will need a *repere* and a *referential*. The latter is a physical object in respect to which we describe the motion of the other objects. For a referential, at least 4 distinct, respectively fixed, non-complanar objects are needed. The first one is a geometric entity formed by 3 non-complanar vectors that describe a grid in the three-dimensional space.

Let now $\vec{r}(t)$ be the position vector of an object. With respect to a repere $(\hat{x}, \hat{y}, \hat{z})$, we can write it as

$$\vec{OP}(t) = \vec{r}(t) = x(t)\hat{x} + y(t)\hat{y} + z(t)\hat{z}$$

Note that the direction vectors are a-dimensional, and that the coordinates in function of time carry the dimensional information.

We now arrive at the notion of *trajectory*. Using the previous notation we write.

$$\Gamma = \{P \mid \vec{OP} = \vec{r}(t), \forall t\}$$

to mean that it is the set of points P that the object touches in its evolution through time.

Now, let's describe the velocity vector. Simply by derivating the position vector:

$$\vec{v}(t) = \dot{\vec{r}}(t) = \dot{x}(t)\hat{x} + \dot{y}(t)\hat{y} + \dot{z}(t)\hat{z}$$

The direction of the vector $\vec{v}(t)$ is always tangent to the trajectory.
The SI unit of the velocity vector is $[ms^{-1}]$.

The same holds true for the acceleration, given by:

$$\vec{a}(t) = \ddot{\vec{r}}(t) = \ddot{x}(t)\hat{x} + \ddot{y}(t)\hat{y} + \ddot{z}(t)\hat{z}$$

And it's SI units are $[ms^{-2}]$. note however how tis direction is normally not tangent to the graph Γ .

Dynamics

Let's now move on to dynamic. Mass is an extensive, scalar, conserved, physic grandeur. If the system is closed, the mass is costant in the system. If the system is opened the mass can change (enter and exit the system).

When we come to the quantity of movement, we mathematically define it as a general function, but we do not need to explicity write it out, that will come out later.

$$\vec{p} = \vec{f}(m, \vec{v})$$

Theorem 4.1.1 (First law of Newton). *Every Object in a state of linear motion or hold, remains in it state if no other object or force interferes with it.*

Noteth that this law only holds for inertial referes, and inertial refers are the one in which this law holds true. In generale, for the scope of giving a better definition, all the inertial referentiel move at constant or null speed relative to each other.

We simply define the Force to be an action of an object or fielt on another object. Forces are vectors, and thus behave as vector. Their SI unit is $[kg \cdot ms^{-2}]$

Theorem 4.1.2 (Second Law of Newton). *The variation of the quantity of motion of an object in time is the sum of the exterior forces on the object.*

$$\sum \vec{F} = \dot{\vec{p}}$$

Now, consider k material points of mass m and speed \vec{v} . The quantity of motion of this system is, by extensivity of mass and intensivity of velocity:

$$\vec{f}(km, \vec{v}) = k\vec{f}(m, \vec{v})$$

Assuming continuity of the objects, we derive the previous equation

$$\begin{aligned} \frac{d\vec{f}(km, \vec{v})}{d(km)} \frac{d(km)}{dk} &= \frac{dk}{dk} \vec{f}(km, \vec{v}) \iff \\ \frac{d\vec{f}(km, \vec{v})}{dkm} m &= \vec{f}(km, \vec{v}) \end{aligned}$$

With $k = 1$

$$\frac{d\vec{f}(m, \vec{v})}{dm} = \frac{\vec{f}(m, \vec{v})}{m} \iff$$

$$\vec{p} = f(m, \vec{v}) = m\vec{f}(\vec{v})$$

Now, noting, with experiments, $\gamma = \frac{\vec{f}(\vec{v})}{\vec{v}}$ that:

$$m\vec{f}(\vec{v}) = 2m\vec{f}(\vec{v}/2) \implies \vec{f}(\vec{v}) = \gamma\vec{v} \iff \vec{p} = m\vec{f}(\vec{v}) = \gamma m\vec{v}$$

So, with $\gamma = 1$ we have:

$$\vec{p} = m\vec{v} \implies \sum \vec{F} = \dot{m}\vec{v} + m\dot{\vec{v}}$$

Application 2

$$x_v(t_1) = d' = v_v \cdot (t_1 - t_0), \quad x_m(t_1) = v_m \cdot (t_1 - t_0)$$

$$\text{We have: } x_v(t_2) = d = v_v \cdot (t_2 - t_1) + x_v(t_1) = v_v \cdot (t_2 - t_1) + d', \quad x_m(t_2) = 1/2a \cdot (t_2 - t_1)^2 + v_m(t_2 - t_1) + x_m(t_1) = 1/2a \cdot (t_2 - t_1)^2 + v_m(t_2 - t_0) + x_m(t_1)$$

$$\text{We arrive at parity after } x_m(t_2) = x_v(t_1) = d \text{ implying } a = \frac{2d - 2v_m(t_2 - t_0)}{(t_2 - t_1)^2} \text{ and we}$$

$$\text{have } t_2 - t_1 = \frac{d - d'}{v_v}, t_2 - t_0 = \frac{d}{v_v} \implies a_0 = \frac{2dv_v(v_v - v_m)}{(d - d')^2} \frac{[m][ms^{-1}][ms^{-1}]}{[m]^2}$$

4.2 Elastic forces and Harmonic Oscillations

We will only see this model applied to elastic deformations, the one in which the object returns to the initial conditions after being stretched. The law that describes the relation between stretch and elastic force is given by the Hook's Law on elastic regimes:

$$\vec{F}_{el} = -k \cdot \vec{d}$$

where d is the displacement. This means the force is proportional to the displacement, and a constant k which depends on the object stretched. The direction of the force is opposing the stretch.

To study the motion of an object affected by elastic forces, we consider a mass attached to a spring. With absence of friction, under Newton's second law, we pose $\vec{d} = \vec{r}$, translating our reference to counter the gravitational force. We thus have:

$$\vec{F}_{tot} = m\vec{a} = -k\vec{r} \implies \vec{a}(t) = -\frac{k}{m}\vec{r}(t)$$

which, duh, is a differential equation of the position and its second derivative.

We define

$$\omega = \sqrt{\frac{k}{m}} \implies \ddot{x} = -\omega^2 x$$

Note that $\dot{x} = \sqrt{-\omega^2 x}$ and thus we get an ansatz of

$$x(t) = \exp(\sqrt{-\omega^2}t) = \exp(\pm i\omega t) = \cos(\omega t) \pm i \sin(\omega t)$$

But those are mathematical complex solutions of a specific case. To get the complete solution we need to take a linear combination of the two mathematical solutions:

$$x(t) = A \cos(\omega t) + B \sin(\omega t)$$

We do a change of variable from $(A, B) \rightarrow (C, \varphi)$ given as

$$A = C \cos \varphi, B = -C \sin \varphi \implies x(t) = C(\cos \varphi \cos(\omega t) - \sin \varphi \sin(\omega t))$$

which is the addition formula for two variables ωt and φ :

$$x(t) = C \cos(\omega t + \varphi)$$

We can make the following considerations on this formula. We define the physical concept of period to be $\omega T = 2\pi$ and the frequency to be $f = 1/T \implies \omega = 2\pi f$.

We now have to consider the initial conditions $x(0) = x_0$, $\dot{x}(0) = v_0$. We have:

$$\begin{cases} x(0) = A = x_0 \\ \dot{x}(0) = \omega B = v_0 \implies B = \frac{v_0}{\omega} \\ x(0) = C \cos(\varphi) \end{cases}$$

4.2.1 Damped elastic oscillator

We have that the sum of the forces:

$$ma = -bv - km \implies \ddot{x} + \frac{b}{m}\dot{x} + \frac{k}{m}x = 0$$

With an ansatz of $x(t) = \exp(\lambda t) \implies \lambda^2 + 2\gamma\lambda + \omega_0^2 = 0$ with solutions:

$$\lambda = -\gamma \pm \sqrt{\gamma^2 - \omega_0^2} \implies x(t) = A \exp(\lambda_1 t) + B \exp(\lambda_2 t)$$

We now have to distinguish 3 cases, which are coincidental, imaginary and real solutions. For the imaginary solutions we have that:

$$x(t) = C \exp(-\gamma t) \cos(\omega t + \varphi)$$

Where $\varphi = -\arctan\left(\frac{\gamma}{\omega}\right)$, $C = x_0 \sqrt{1 + \frac{\gamma^2}{\omega^2}}$

For real solutions we have:

$$x(t) = A \exp((- \gamma + \omega)t) + B \exp((- \gamma - \omega)t)$$

Where $A = \frac{x_0 \tau_1}{\tau_1 - \tau_2}$, $B = -\frac{x_0 \tau_1}{\tau_1 - \tau_2}$.

And for the critical case, using some differential linear algebra:

$$x(t) = (A + Bt) \exp(-\omega_0 t)$$

Where $A = x_0$, $B = x_0 \omega_0$