Lineární algebra 1

Martin Balko

6. přednáška

9. listopadu 2021

Algebraická tělesa

Zdroj: https://galois.com

Příklady těles

Příklady těles

1. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ s klasickými operacemi sčítání a násobení tvoří (nekonečná) tělesa,

Příklady těles

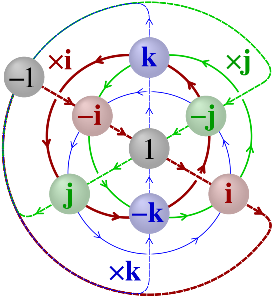
1. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ s klasickými operacemi sčítání a násobení tvoří (nekonečná) tělesa,
2. $\mathbb{Z}$ se sčítáním a násobením těleso netvoří (chybí inverzní prvky pro násobení),

Příklady těles

1. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ s klasickými operacemi sčítání a násobení tvoří (nekonečná) tělesa,
2. $\mathbb{Z}$ se sčítáním a násobením těleso netvoří (chybí inverzní prvky pro násobení),
3. $\{0, 1\}$ se sčítáním a násobením modulo 2 je nejmenší možné těleso,

Příklady těles

1. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ s klasickými operacemi sčítání a násobení tvoří (nekonečná) tělesa,
2. $\mathbb{Z}$ se sčítáním a násobením těleso netvoří (chybí inverzní prvky pro násobení),
3. $\{0, 1\}$ se sčítáním a násobením modulo 2 je nejmenší možné těleso,
4. kvaterniony (zobecnění komplexních čísel vzniklé přidáním dvou dalších imaginárních jednotek j a k, kde $j^2 = k^2 = -1$ a $ijk = -1$) tvoří nekomutativní těleso.



Zdroj: https://wikipedia.org

Příklad konečného tělesa

Příklad konečného tělesa

- Operace sčítání a násobení nad tělesem $\mathbb{Z}_5$

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Příklad konečného tělesa

- Operace sčítání a násobení nad tělesem $\mathbb{Z}_5$

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

- Inverzní prvky tělesa $\mathbb{Z}_5$

x	0	1	2	3	4
$-x$	0	4	3	2	1

x	0	1	2	3	4
x^{-1}	–	1	3	2	4

Évariste Galois

Évariste Galois

- Tělesa $GF(p^n)$ se nazývají Galoisova tělesa („Galois field“).

Évariste Galois

- Tělesa $GF(p^n)$ se nazývají Galoisova tělesa („Galois field“).
- Každé konečné těleso velikosti p^n je isomorfní tělesu $GF(p^n)$.

Évariste Galois

- Tělesa $GF(p^n)$ se nazývají Galoisova tělesa („Galois field“).
- Každé konečné těleso velikosti p^n je isomorfní tělesu $GF(p^n)$.
- Évariste Galois byl francouzský matematik, jehož práce daly vzniknout teorii grup a moderní algebře.

Évariste Galois

- Tělesa $GF(p^n)$ se nazývají Galoisova tělesa („Galois field“).
- Každé konečné těleso velikosti p^n je isomorfní tělesu $GF(p^n)$.
- Évariste Galois byl francouzský matematik, jehož práce daly vzniknout teorii grup a moderní algebře.

Obrázek: Évariste Galois (1811–1832).

Zdroj: https://galois.com

Aplikace: samoopravné kódy

Aplikace: samoopravné kódy

- Motivace: přenos dat.

Aplikace: samoopravné kódy

- Motivace: přenos dat.
- Chceme přenést data komunikačním kanálem.

Aplikace: samoopravné kódy

- Motivace: přenos dat.
- Chceme přenést data komunikačním kanálem.

Aplikace: samoopravné kódy

- Motivace: přenos dat.
- Chceme přenést data komunikačním kanálem.

"Whenever I go to my
balcony, I see a little
creek under my house."

Aplikace: samoopravné kódy

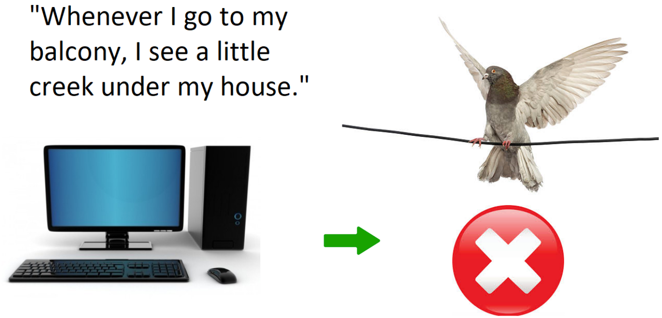
- Motivace: přenos dat.
- Chceme přenést data komunikačním kanálem.

"Whenever I go to my
balcony, I see a little
creek under my house."

- Při přenosu může dojít k chybám.

Aplikace: samoopravné kódy

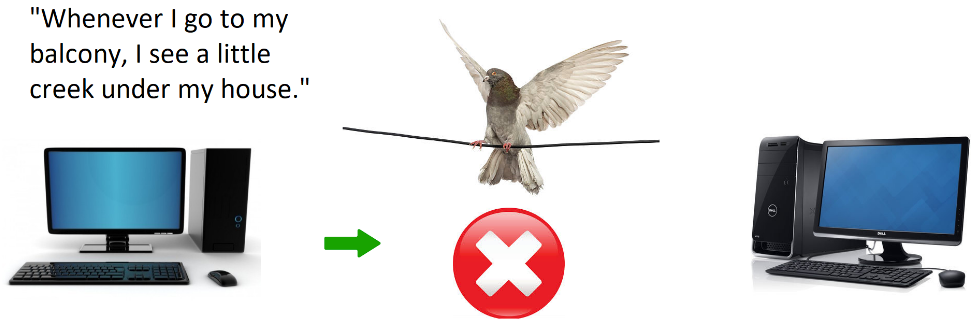
- Motivace: přenos dat.
- Chceme přenést data komunikačním kanálem.



- Při přenosu může dojít k chybám.

Aplikace: samoopravné kódy

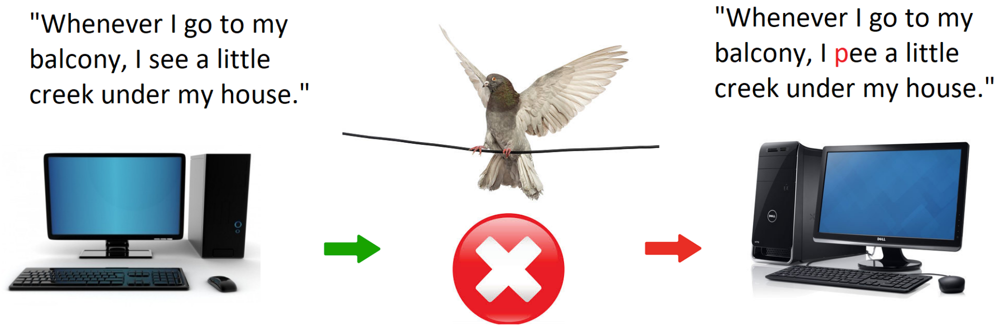
- Motivace: přenos dat.
- Chceme přenést data komunikačním kanálem.



- Při přenosu může dojít k chybám.

Aplikace: samoopravné kódy

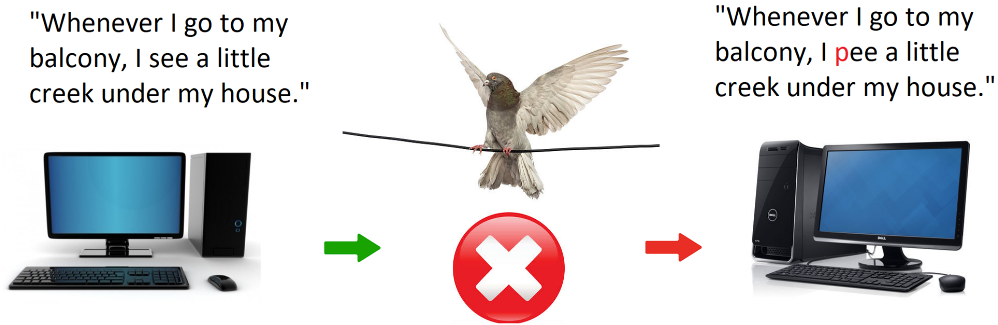
- Motivace: přenos dat.
- Chceme přenést data komunikačním kanálem.



- Při přenosu může dojít k chybám.

Aplikace: samoopravné kódy

- Motivace: přenos dat.
- Chceme přenést data komunikačním kanálem.



- Při přenosu může dojít k chybám.
- Chceme být schopni chyby opravit a získat odeslanou zprávu.

Aplikace: samoopravné kódy

Aplikace: samoopravné kódy

- Obecný postup kódování: odesílatel rozdělí zprávu na bloky k bitů, které určitou metodou přetransformuje na bloky o k' bitech. Příjemce pak každý blok transformuje na původní hodnoty.

Aplikace: samoopravné kódy

- Obecný postup kódování: odesílatel rozdělí zprávu na bloky k bitů, které určitou metodou přetransformuje na bloky o k' bitech. Příjemce pak každý blok transformuje na původní hodnoty.
- Příklad: Zdvojením bitů lze 1 chybu detekovat, ale ne opravit.

Aplikace: samoopravné kódy

- Obecný postup kódování: odesílatel rozdělí zprávu na bloky k bitů, které určitou metodou přetransformuje na bloky o k' bitech. Příjemce pak každý blok transformuje na původní hodnoty.
- Příklad: Zdvojením bitů lze 1 chybu detekovat, ale ne opravit. Ztrojením bitů lze 1 chybu detekovat i opravit.

Aplikace: samoopravné kódy

- Obecný postup kódování: odesílatel rozdělí zprávu na bloky k bitů, které určitou metodou přetransformuje na bloky o k' bitech. Příjemce pak každý blok transformuje na původní hodnoty.
- Příklad: Zdvojením bitů lze 1 chybu detekovat, ale ne opravit. Ztrojením bitů lze 1 chybu detekovat i opravit.
- Hammingův kód $(7, 4, 3)$: rozdělí zprávu na bloky b s $k = 4$ bity a ty transformuje na bloky b' s $k' = 7$ bity. Umí detekovat a opravit 1 chybu.

Aplikace: samoopravné kódy

- Obecný postup kódování: odesílatel rozdělí zprávu na bloky k bitů, které určitou metodou přetransformuje na bloky o k' bitech. Příjemce pak každý blok transformuje na původní hodnoty.
- Příklad: Zdvojením bitů lze 1 chybu detekovat, ale ne opravit. Ztrojením bitů lze 1 chybu detekovat i opravit.
- Hammingův kód $(7,4,3)$: rozdělí zprávu na bloky b s $k = 4$ bity a ty transformuje na bloky b' s $k' = 7$ bity. Umí detekovat a opravit 1 chybu.
- Lze reprezentovat násobením generující maticí $H \in \mathbb{Z}_2^{7\times 4}$:

$$Hb = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = b'$$

Aplikace: samoopravné kódy

- Obecný postup kódování: odesílatel rozdělí zprávu na bloky k bitů, které určitou metodou přetransformuje na bloky o k' bitech. Příjemce pak každý blok transformuje na původní hodnoty.
- Příklad: Zdvojením bitů lze 1 chybu detekovat, ale ne opravit. Ztrojením bitů lze 1 chybu detekovat i opravit.
- Hammingův kód $(7, 4, 3)$: rozdělí zprávu na bloky b s $k = 4$ bity a ty transformuje na bloky b' s $k' = 7$ bity. Umí detekovat a opravit 1 chybu.
- Lze reprezentovat násobením generující maticí $H \in \mathbb{Z}_2^{7\times 4}$:

$$Hb = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = b'$$

- Příjemce obdrží zakódovaný blok b' zprávy, který musí dekódovat.

Aplikace: samoopravné kódy

Aplikace: samoopravné kódy

- K detekci a opravě chyb používá příjemce detekční matici $D \in \mathbb{Z}_2^{3\times 7}$.

Aplikace: samoopravné kódy

- K detekci a opravě chyb používá příjemce detekční matici $D \in \mathbb{Z}_2^{3\times 7}$.
- Pokud $Db' = 0$, pak nenastala chyba při přenosu (nebo nastaly ≥ 2).

Aplikace: samoopravné kódy

- K detekci a opravě chyb používá příjemce detekční matici $D \in \mathbb{Z}_2^{3\times 7}$.
- Pokud $Db' = 0$, pak nenastala chyba při přenosu (nebo nastaly ≥ 2).
- Jinak nastala chyba v bitu na pozici, jejímž binárním zápisem je Db'.

Aplikace: samoopravné kódy

- K detekci a opravě chyb používá příjemce detekční matici $D \in \mathbb{Z}_2^{3\times 7}$.
- Pokud $Db' = 0$, pak nenastala chyba při přenosu (nebo nastaly ≥ 2).
- Jinak nastala chyba v bitu na pozici, jejímž binárním zápisem je Db'.
- Příklad přenosu bez chyby:

Aplikace: samoopravné kódy

- K detekci a opravě chyb používá příjemce detekční matici $D \in \mathbb{Z}_2^{3\times 7}$.
- Pokud $Db' = 0$, pak nenastala chyba při přenosu (nebo nastaly ≥ 2).
- Jinak nastala chyba v bitu na pozici, jejímž binárním zápisem je Db'.

- Příklad přenosu bez chyby:

$$Db' = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

Aplikace: samoopravné kódy

- K detekci a opravě chyb používá příjemce detekční matici $D \in \mathbb{Z}_2^{3\times 7}$.
- Pokud $Db' = 0$, pak nenastala chyba při přenosu (nebo nastaly ≥ 2).
- Jinak nastala chyba v bitu na pozici, jejímž binárním zápisem je Db'.

- Příklad přenosu s 1 chybou:

Aplikace: samoopravné kódy

- K detekci a opravě chyb používá příjemce detekční matici $D \in \mathbb{Z}_2^{3\times 7}$.
- Pokud $Db' = 0$, pak nenastala chyba při přenosu (nebo nastaly ≥ 2).
- Jinak nastala chyba v bitu na pozici, jejímž binárním zápisem je Db'.

- Příklad přenosu s 1 chybou:

$$Db' = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$$

Aplikace: samoopravné kódy

- K detekci a opravě chyb používá příjemce detekční matici $D \in \mathbb{Z}_2^{3\times 7}$.
- Pokud $Db' = 0$, pak nenastala chyba při přenosu (nebo nastaly ≥ 2).
- Jinak nastala chyba v bitu na pozici, jejímž binárním zápisem je Db'.

- Příklad přenosu s 1 chybou:

$$Db' = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \Rightarrow \text{ chyba na pozici 6}$$

Aplikace: samoopravné kódy

- K detekci a opravě chyb používá příjemce detekční matici $D \in \mathbb{Z}_2^{3\times 7}$.
- Pokud $Db' = 0$, pak nenastala chyba při přenosu (nebo nastaly ≥ 2).
- Jinak nastala chyba v bitu na pozici, jejímž binárním zápisem je Db'.

- Příklad přenosu s 1 chybou:

$$Db' = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \Rightarrow \text{ chyba na pozici 6}$$

- Více o samoopravných kódech na přednášce Kombinatorika a grafy I.

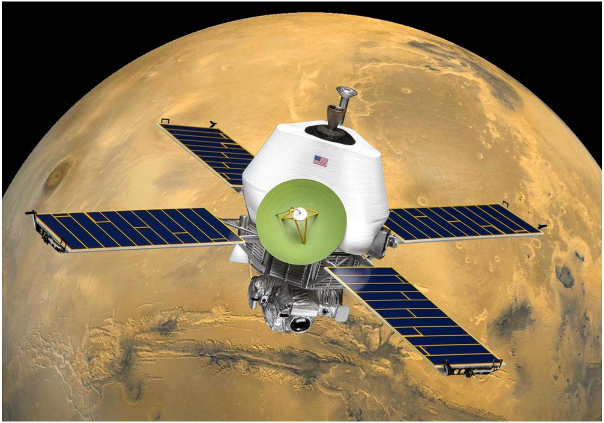
Aplikace: samoopravné kódy

Aplikace: samoopravné kódy

- Samoopravné kódy byly použity sondou Mariner 9 pro přenos prvních fotografií Marsu.

Aplikace: samoopravné kódy

- Samoopravné kódy byly použity sondou Mariner 9 pro přenos prvních fotografií Marsu.

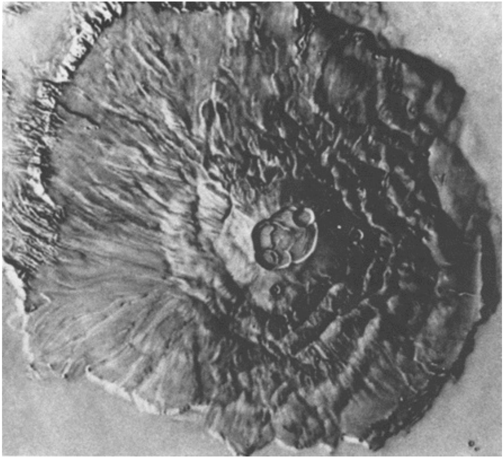


Obrázek: Sonda Mariner 9.

Zdroj: http://www.realspacemodels.com

Aplikace: samoopravné kódy

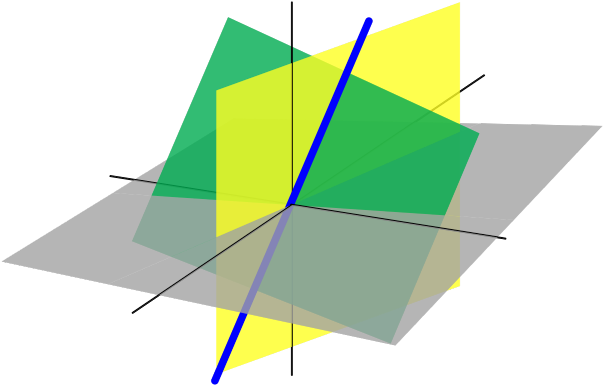
- Samoopravné kódy byly použity sondou Mariner 9 pro přenos prvních fotografií Marsu.



Obrázek: Fotografie hory Olympus Mons pořízená sondou Mariner 9.

Zdroj: https://www.khanacademy.org

Vektorové prostory



Zdroj: https://en.wikipedia.org

Příklady vektorových prostorů

Příklady vektorových prostorů

1. Aritmetický prostor $\mathbb{R}^n$ nad $\mathbb{R}$, nebo obecněji $\mathbb{T}^n$ nad tělesem $\mathbb{T}$. Vektory sčítáme a násobíme skalárem po složkách.

Příklady vektorových prostorů

1. Aritmetický prostor $\mathbb{R}^n$ nad $\mathbb{R}$, nebo obecněji $\mathbb{T}^n$ nad tělesem $\mathbb{T}$.
   Vektory sčítáme a násobíme skalárem po složkách.
2. Prostor matic $\mathbb{T}^{m \times n}$ nad tělesem $\mathbb{T}$.

Příklady vektorových prostorů

1. Aritmetický prostor $\mathbb{R}^n$ nad $\mathbb{R}$, nebo obecněji $\mathbb{T}^n$ nad tělesem $\mathbb{T}$. Vektory sčítáme a násobíme skalárem po složkách.
2. Prostor matic $\mathbb{T}^{m\times n}$ nad tělesem $\mathbb{T}$.
3. Prostor $\mathcal{P}$ všech reálných polynomů proměnné x nad tělesem $\mathbb{R}$.
   Sčítání:
   $$(a_n x^n + \cdots + a_0) + (b_n x^n + \cdots + b_0) = (a_n + b_n)x^n + \cdots + (b_0 + a_0).$$
   Násobení skalárem: $\alpha(a_n x^n + \cdots + a_0) = \alpha a_n x^n + \cdots + \alpha a_0$.

Příklady vektorových prostorů

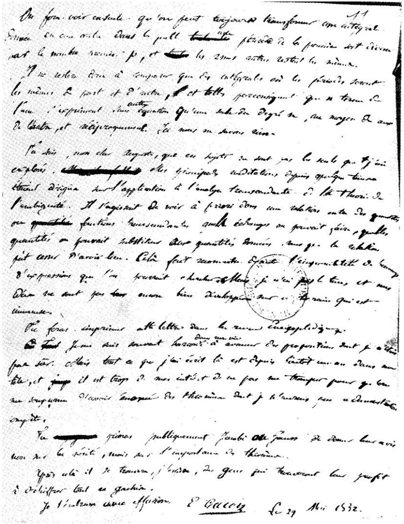
1. Aritmetický prostor $\mathbb{R}^n$ nad $\mathbb{R}$, nebo obecněji $\mathbb{T}^n$ nad tělesem $\mathbb{T}$. Vektory sčítáme a násobíme skalárem po složkách.
2. Prostor matic $\mathbb{T}^{m \times n}$ nad tělesem $\mathbb{T}$.
3. Prostor $\mathcal{P}$ všech reálných polynomů proměnné x nad tělesem $\mathbb{R}$.
   Sčítání:
   $$(a_n x^n + \cdots + a_0) + (b_n x^n + \cdots + b_0) = (a_n + b_n)x^n + \cdots + (b_0 + a_0).$$
   Násobení skalárem: $\alpha(a_n x^n + \cdots + a_0) = \alpha a_n x^n + \cdots + \alpha a_0$.
4. Prostor $\mathcal{P}^n$ všech reálných polynomů proměnné x stupně $\leq n$ nad tělesem $\mathbb{R}$.
5. Prostor $\mathcal{F}$ všech reálných funkcí $f : \mathbb{R} \to \mathbb{R}$.
   Sčítání: $(f + g)(x) = f(x) + g(x)$.
   Násobení skalárem: $(\alpha f)(x) = \alpha f(x)$.

Příklady vektorových prostorů

1. Aritmetický prostor $\mathbb{R}^n$ nad $\mathbb{R}$, nebo obecněji $\mathbb{T}^n$ nad tělesem $\mathbb{T}$. Vektory sčítáme a násobíme skalárem po složkách.
2. Prostor matic $\mathbb{T}^{m\times n}$ nad tělesem $\mathbb{T}$.
3. Prostor $\mathcal{P}$ všech reálných polynomů proměnné x nad tělesem $\mathbb{R}$.
   Sčítání:
   $$(a_n x^n + \cdots + a_0) + (b_n x^n + \cdots + b_0) = (a_n + b_n)x^n + \cdots + (b_0 + a_0).$$
   Násobení skalárem: $\alpha(a_n x^n + \cdots + a_0) = \alpha a_n x^n + \cdots + \alpha a_0$.
4. Prostor $\mathcal{P}^n$ všech reálných polynomů proměnné x stupně $\leq n$ nad tělesem $\mathbb{R}$.
5. Prostor $\mathcal{F}$ všech reálných funkcí $f : \mathbb{R} \to \mathbb{R}$.
   Sčítání: $(f+g)(x) = f(x) + g(x)$.
   Násobení skalárem: $(\alpha f)(x) = \alpha f(x)$.
6. Prostor $\mathcal{C}$ všech spojitých reálných funkcí $f : \mathbb{R} \to \mathbb{R}$.

Příklady vektorových prostorů

1. Aritmetický prostor $\mathbb{R}^n$ nad $\mathbb{R}$, nebo obecněji $\mathbb{T}^n$ nad tělesem $\mathbb{T}$. Vektory sčítáme a násobíme skalárem po složkách.
2. Prostor matic $\mathbb{T}^{m \times n}$ nad tělesem $\mathbb{T}$.
3. Prostor $\mathcal{P}$ všech reálných polynomů proměnné x nad tělesem $\mathbb{R}$.
   Sčítání:
   $$(a_n x^n + \cdots + a_0) + (b_n x^n + \cdots + b_0) = (a_n + b_n) x^n + \cdots + (b_0 + a_0).$$
   Násobení skalárem: $\alpha(a_n x^n + \cdots + a_0) = \alpha a_n x^n + \cdots + \alpha a_0$.
4. Prostor $\mathcal{P}^n$ všech reálných polynomů proměnné x stupně $\leq n$ nad tělesem $\mathbb{R}$.
5. Prostor $\mathcal{F}$ všech reálných funkcí $f : \mathbb{R} \to \mathbb{R}$.
   Sčítání: $(f + g)(x) = f(x) + g(x)$.
   Násobení skalárem: $(\alpha f)(x) = \alpha f(x)$.
6. Prostor $\mathcal{C}$ všech spojitých reálných funkcí $f : \mathbb{R} \to \mathbb{R}$.
7. Prostor $\mathcal{C}_{a,b}$ všech spojitých reálných funkcí $f : [a, b] \to \mathbb{R}$.



11

On pourra voir ensuite qu'on peut toujours transformer une intégrale donnée en une autre dans laquelle telle période de la première soit divisée par le nombre premier p, et les $2n-1$ autres restent les mêmes.

Il ne restera donc à comparer que des intégrales où les périodes seront les mêmes de part et d'autre, et telles par conséquent que n termes de l'une s'expriment sans autre équation qu'une seule du degré n, au moyen de ceux de l'autre, et réciproquement. Ici nous ne savons rien.

Tu sais, mon cher Auguste, que ces sujets ne sont pas les seuls que j'ai explorés. Mes principales méditations depuis quelque temps étaient dirigées sur l'application à l'analyse transcendante de la théorie de l'ambiguïté. Il s'agissait de voir a priori dans une relation entre des quantités ou fonctions transcendantes quels échanges on pouvait faire, quelles quantités on pouvait substituer aux quantités données sans que la relation pût cesser d'avoir lieu. Cela fait reconnaître tout de suite l'impossibilité de beaucoup d'expressions que l'on pourrait chercher. Mais je n'ai pas le temps et mes idées ne sont pas encore bien développées sur ce terrain qui est immense.

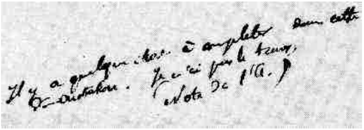
Tu feras imprimer cette lettre dans la Revue encyclopédique.

Je me suis souvent hasardé dans ma vie à avancer des propositions dont je n'étais pas sûr. Mais tout ce que j'ai écrit là est depuis bientôt un an dans ma tête, et il est trop de mon intérêt de ne pas me tromper pour qu'on me soupçonne d'avoir énoncé des théorèmes dont je n'aurais pas la démonstration complète.

Tu prieras publiquement Jacobi ou Gauss de donner leur avis non sur la vérité, mais sur l'importance des théorèmes.

Après cela il se trouvera, j'espère, des gens qui trouveront leur profit à déchiffrer tout ce gâchis.

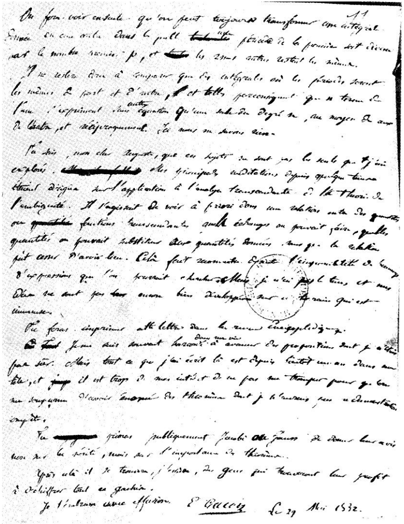
Je t'embrasse avec effusion. E. Galois. Le 29 Mai 1832.



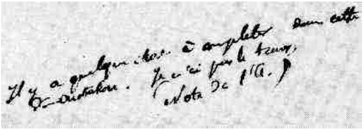
Il y a quelque chose à compléter dans cette démonstration. Je n'ai pas le temps. (Note de l'A.)

Obrázek: Dopis, který Galois sepsal noc před svou smrtí v duelu a ve kterém zachytil své matematické myšlenky. Poznámka vpravo říká „... Nemám čas.“.

Zdroje: https://conquermaths.com a https://mathshistory.st-andrews.ac.uk



Je t'embrasse avec effusion. E. Galois. Le 29 Mai 1832.



Obrázek: Dopis, který Galois sepsal noc před svou smrtí v duelu a ve kterém zachytil své matematické myšlenky. Poznámka vpravo říká „... Nemám čas.“.

Zdroje: https://conquermaths.com a https://mathshistory.st-andrews.ac.uk

Děkuji za pozornost.