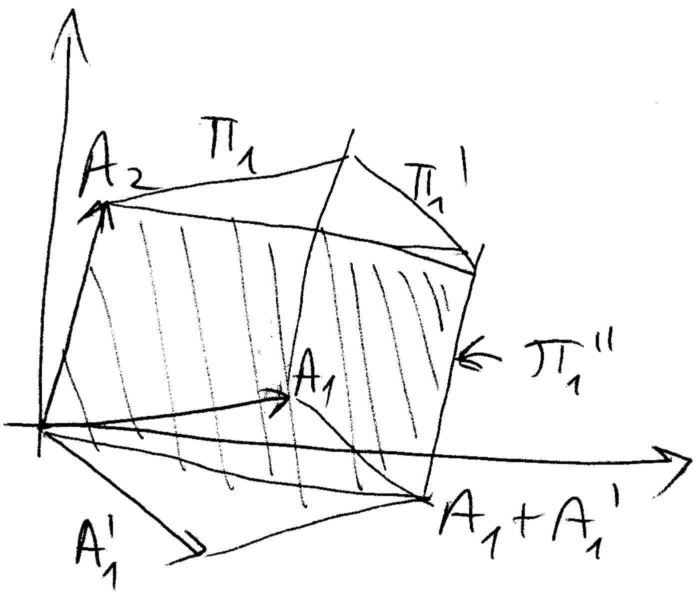
Aksjomatyczne ujście $\det(A)$.

D1. $\det(A_1,\ldots,\underbrace{A_i+A_i'}_{i},\ldots,A_n)=$

$= \det(A_1,\ldots,\underbrace{A_i}_{i},\ldots,A_n)+\det(A_1,\ldots,\underbrace{A_i'}_{i},\ldots,A_n)$



D2. Dla $t\in\mathbb{R}$

$\det(A_1,\ldots,\underbrace{tA_i}_{i},\ldots,A_n)=$

$=t\cdot\det(A_1,\ldots,\underbrace{A_i}_{i},\ldots,A_n)$

(może być ujemne, "zorientowana")

D3. Jeśli dla pewnego i, $A_i=A_{i+1}$, to

$\det(A_1,\ldots,A_n)=0$

D4. $\det(E_1,\ldots,E_n)=\det(I)=1$. $I=\begin{bmatrix}1 & & 0\\ & \ddots & \\ 0 & & 1\end{bmatrix}$

Pokażemy, że istnieje jedyna funkcja

$\det: M_{n\times n}(\mathbb{R})\longrightarrow\mathbb{R}$ spełniająca D1—D4.

Wykład 5. Wyznacznik

$$\det(\overbrace{A_1,\dots,A_n}^{A})$$

Fakt 5.8. Zał, że funkcja $\det : M_{n\times n}(\mathbb{R}) \to \mathbb{R}$ spełnia D1–D4. Wtedy

(1) Jeśli $A_i = 0$, to $\det(A_1,\dots,A_n) = 0$

(2) Dla $j \neq i$ oraz $t \in \mathbb{R}$:

$$\det(A_1,\dots,\underbrace{A_i + tA_j}_{i},\dots,A_n) = \det(A_1,\dots,\underbrace{A_i}_{i},\dots,A_n)$$

(3) dla $\sigma \in S_n$, $\det(A_{\sigma(1)},\dots,A_{\sigma(n)}) = \operatorname{sgn}(\sigma)\cdot\det(A_1,\dots,A_n)$

(4) Jeśli dla pewnych $i \neq j$, $A_i = A_j$, to $\det(A_1,\dots,A_n) = 0$.

<u>D-d</u>. (1) Gdy $A_i = 0$, to $A_i = \underset{t}{0} \cdot A_i$, więc $\boxed{\text{dla } t=0}$; z D2

$$\det(A_1,\dots,A_n) = \det(A_1,\dots,\underbrace{0\cdot A_i}_{i},\dots,A_n) \underset{D2,\, t=0}{=} 0\cdot\det(A_1,\dots,A_n) = 0,$$

(2) wynika z D1, D3 (ćw.)

(3): z D3:

$$0 = \det(A_1,\dots,\overbrace{A_i + A_{i+1}}^{i},\overbrace{A_i + A_{i+1}}^{i+1},\dots,A_n) \overset{D1}{=}$$

$$\underbrace{\det(A_1,\dots,\overset{i}{A_i},\overset{i+1}{A_i},\dots A_n)}_{=0,\ D3} + \det(A_1,\dots,\overset{i}{A_i},\overset{i+1}{A_{i+1}},\dots,A_n) +$$

$$+ \det(A_1,\dots,\overset{i}{A_{i+1}},\overset{i+1}{A_i},\dots,A_n) + \underbrace{\det(A_1,\dots,\overset{i}{A_{i+1}},\overset{i+1}{A_{i+1}},\dots,A_n)}_{=0,\ D3}$$

więc:

$$\det(A_1, \dots, \overset{i}{A_{i+1}}, \overset{i+1}{A_i}, \dots, A_n) = -\det(A_1, \dots, A_i, A_{i+1}, \dots, A_n).$$

Stąd: (3) zachodzi dla $\sigma = (i, i+1)$.

Niech $\sigma \in S_n$ dowolne, $\sigma = \sigma_1 \dots \sigma_k$

transpozycje liczb sąsiednich

$$\operatorname{sgn}(\sigma) = \begin{cases} 1, & \text{gdy } 2 \mid k \\ -1, & \text{gdy } 2 \nmid k \end{cases}$$

stąd (3).

(4) Zał, że $A_i = A_j$ dla pewnych $i \neq j$.

Niech $\sigma \in S_n$ t. że $\sigma(1) = i$, $\sigma(2) = j$.

z (3) i D3:

$$0 = \det(A_{\sigma(1)}, A_{\sigma(2)}, \dots, A_{\sigma(n)}) = \operatorname{sgn}(\sigma) \det(A_1, \dots, A_n)$$

$$\Rightarrow \det(A_1, \dots, A_n) = 0.$$

TW. 5.9. Zał, że det spełnia D1–D4,

$A = [a_{ij}]_{n \times n}$, $B = [b_{ij}]_{n \times n}$. Wtedy

$$\det(AB) = \det(A) \cdot \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \cdot b_{\sigma(1)1} b_{\sigma(2)2} \cdots b_{\sigma(n)n}.$$

$$B = \begin{array}{c} \begin{array}{ccccc} 1 & 2 & 3 & 4 & \dots \end{array} \\ \begin{bmatrix} & & b_{\sigma(3),3} & & \\ b_{\sigma(1),1} & & & & \dots \\ & b_{\sigma(2)2} & & & \\ & & & b_{\sigma(4),4} & \end{bmatrix}_{n\times n} \end{array}$$

<u>D-d</u> $A = (A_1, \dots, A_n)$ $AB = (C_1, \dots, C_n)$

dla $t = 1, \dots, n$:

$$C_t = b_{1t} A_1 + b_{2t} A_2 + \dots + b_{nt} A_n = \sum_{j=1}^{n} b_{jt} A_j$$

bo: $c_{it} = a_{i1} b_{1t} + a_{i2} b_{2t} + \dots + a_{in} b_{nt}$.

$\det(AB) = \det(C_1, \dots, C_n) =$

D1-D3, Fakt 5.8

$$= \det\Big(\sum_{s_1=1}^{n} b_{s_1 1} A_{s_1}, \sum_{s_2=1}^{n} b_{s_2 2} A_{s_2}, \dots, \sum_{s_n=1}^{n} b_{s_n n} A_{s_n}\Big) =$$

$$= \sum_{s_1=1}^{n} b_{s_1 1} \det\Big(A_{s_1}, \sum_{s_2=1}^{n} b_{s_2 2} A_{s_2}, \dots, \sum_{s_n} b_{s_n n} A_{s_n}\Big) =$$

$$= \sum_{s_1=1}^{n} b_{s_1 1} \cdot \Big(\sum_{s_2=1}^{n} b_{s_2 2} \cdot \dots \cdot \Big(\sum_{s_n=1}^{n} b_{s_n n} \cdot \det(A_{s_1}, A_{s_2}, \dots, A_{s_n})\Big)\dots\Big)$$

(4

$$\sum_{s_1=1}^{n}\sum_{s_2=1}^{n}\dots\sum_{s_n=1}^{n} b_{s_1 1} b_{s_2 2}\dots b_{s_n n}\cdot \det(A_{s_1}, A_{s_2},\dots,A_{s_n}).$$ AlI/5

(*)

Dla $1 \leq s_1, s_2, \dots, s_n \leq n$ niech

$\sigma : \{1,\dots,n\} \longrightarrow \{1,\dots,n\}$ t. że $\sigma(i) = s_i$.

Wtedy $(A_{s_1}, A_{s_2},\dots, A_{s_n}) = (A_{\sigma(1)}, A_{\sigma(2)},\dots, A_{\sigma(n)})$.

Jeśli w ciągu $s_1,\dots,s_n$ jedna z liczb się powtarza, to w macierzy $(A_{s_1},\dots,A_{s_n})$ pewne dwie kolumny są $=$, więc z 5,8(4): $\det(A_{s_1},\dots,A_{s_n}) = 0$.

Dlatego w (*) sumowanie można ograniczyć do układów $1 \leq s_1,\dots,s_n \leq 1$ ~~t. że~~ które odpowiadają permutacjom $\sigma \in S_n$. ~~Więc:~~

~~$(*) = \sum_{\sigma\in S_n}$~~ Wtedy: $b_{s_1 1}\cdot\ldots\cdot b_{s_n n} = b_{\sigma(1)1} b_{\sigma(2)2}\dots b_{\sigma(n)n}$

i $\det(A_{s_1}, A_{s_2},\dots, A_{s_n}) =$

$$= \det(A_{\sigma(1)},\dots,A_{\sigma(n)}) \underset{5,8(3)}{=} \operatorname{sgn}(\sigma)\det(A_1,\dots,A_n),$$

więc $$(*) = \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma)\, b_{\sigma(1)1}\dots b_{\sigma(n)n}\cdot \det(A) =$$

$$= \det(A)\cdot \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma)\, b_{\sigma(1)1}\cdot\ldots\cdot b_{\sigma(n)n}.$$

D4: $\det(I) = 1$.

Wn 5,10. Jeśli det spełnia D1–D4, to:

$$(\dagger)\quad \det[b_{ij}]_{n\times n} = \sum_{\sigma\in S_n} \mathrm{sgn}(\sigma)\, b_{\sigma(1)1}\cdots b_{\sigma(n)n}.$$

<u>D-d</u> $A = I$ w 5,9, $AB = B$.

<u>TW</u>, 5.11. Istnieje dokładnie jedna funkcja $\det : M_{n\times n}(R) \longrightarrow R$ spełniająca D1–D4. Wyraża się ona wzorem $(\dagger)$.

<u>D-d</u> (idea). Sprawdzamy (rachunkowo), że $(\dagger)$ zadaje funkcję det spełniającą D1–D4. Jedyność wynika z 5.10.

Wn. 5.12 (tw. Cauchy'ego)

$$\det(AB) = \det(A)\det(B).$$

<u>Przykłady</u>

$$\det\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = \overset{id}{ad} - \overset{(1,2)}{bc}$$

Wzór Sarrusa:

$$\det\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} = \begin{array}{c|ccc|c} + & a & b & c & - \\ + & d & e & f & - \\ + & g & h & i & - \\ & a & b & c & \\ & d & e & f & \end{array} = aei + dhc + gbf - ceg - fha - ibd$$

TW. 5,13.

$\det(A) \neq 0 \Leftrightarrow$ macierz A jest odwracalna.

<u>D-d</u> $\Rightarrow$ nie wprost:

zał, że $A = (A_1, \dots, A_n)$ i kolumny $A_1, \dots, A_n \in \mathbb{R}^n$ nie są lin. niezależne.

np. $A_1 = \sum_{i=2}^{n} t_i A_i$.

D1, D2, Fakt 5.8(4)

Wtedy $\det(A_1, \dots, A_n) = \det(\sum_{i=2}^{n} t_i A_i, A_2, \dots, A_n) =$

$\sum_{i=2}^{n} t_i \det(\overset{i}{A_i}, A_2, \dots, A_i, \dots, A_n) = 0$

$\Leftarrow$. Zał, że A odwracalna. $A \cdot A^{-1} = I$

$1 = \det(I) = \det(A A^{-1}) = \det(A) \cdot \det(A^{-1}) \Rightarrow$

- $\det(A^{-1}) = \det(A)^{-1}$
- $\det(A) \neq 0$. $\square$

<u>Transpozycja macierzy</u>

transponowana

$A = [a_{ij}]_{n \times m} \longrightarrow A^* = [a^*_{ij}]_{m \times n} = A^T, \; a^*_{ij} = a_{ji}$

<u>np</u>. $A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} \quad A^* = A^T = \begin{bmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{bmatrix}$

Tw. 5.14. $A \in M_{n\times n}(\mathbb{R}) \Rightarrow \det(A) = \det(A^T)$.
$A = [a_{ij}]_{n\times n}$

D-d Niech $A^* = [a^*_{ij}]_{n\times n}$, $a^*_{ij} = a_{ji}$

$$\det A = \sum_{\sigma\in S_n} \mathrm{sgn}(\sigma) a_{\sigma(1)1} \dots a_{\sigma(n)n} =$$

$$= \sum_{\sigma\in S_n} \mathrm{sgn}(\sigma) \underbrace{a_{1\sigma^{-1}(1)} \dots a_{n\sigma^{-1}(n)}}_{\text{permutacja czynników}} =$$

$$\left[\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix} = \begin{pmatrix} \sigma^{-1}(1) & \sigma^{-1}(2) & \sigma^{-1}(3) & \dots & \sigma^{-1}(n) \\ 1 & 2 & 3 & \dots & n \end{pmatrix} \right]$$

$$\underset{\uparrow}{=} \sum_{\tau\in S_n} \mathrm{sgn}(\tau) a^*_{\tau(1)1} a^*_{\tau(2)2} \dots a^*_{\tau(n)n} = \det(A^*)$$

$\tau := \sigma^{-1}$

$\mathrm{sgn}\,\sigma = \mathrm{sgn}\,\tau$

$a_{ij} = a^{-1}_{ji}$

z tw. 5.14: Wszystkie własności det wyrażone w terminach kolumn macierzy są prawdziwe w terminach wierszy.

Wn. 5.15. ($A \in M_{n \times n}(\mathbb{R})$)

Kolumny A są lin. niezależne $\Leftrightarrow$ $\det A \neq 0$

$\Leftrightarrow$ wiersze —"— —"— . $\Leftrightarrow$ $\det A^T \neq 0$

Wn. 5.16. Zał., że $A \in M_{n \times n}(\mathbb{R})$ ma kolumny $A_1, \dots, A_n$ i wiersze $W_1, \dots, W_n$.

(1) Następujące operacje elementarne nie zmieniają $\det(A)$:

(a) dodanie wektora tA_j do i-tej kolumny $(i \neq j)$

(b) —"— tW_j wiersza $(i \neq j)$

(2) Zamiana wierszy (lub kolumn) miejscami zmienia znak $\det(A)$.

(3) $\det \begin{bmatrix} a_{11} & & a_{ij} \\ & a_{22} & \\ 0 & & \ddots \end{bmatrix} = a_{11} a_{22} \dots a_{nn}$. ← macierz górnotrójkątna

D-d (3) $\det[a_{ij}] = \sum_{\sigma} \operatorname{sgn} \sigma \underbrace{a_{\sigma(1)1} \dots a_{\sigma(n)n}}_{\substack{\shortparallel \\ 0,\ \text{gdy } \sigma(i) > i \\ \text{dla pewnego } i}} =$

bo:

$\left[\sigma \in S_n,\ \sigma(i) \leq i \text{ dla wszystkich } i = 1, \dots, n \right] \overset{\text{ćw.}}{\Longrightarrow} \sigma = id$

Oznaczenie: $\det[a_{ij}]_{n\times n} = |a_{ij}|_{n\times n}$

np.: $\begin{vmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{vmatrix} = \det \begin{bmatrix} 1 & 2 & 3 & 4 \\ & & \ddots & \\ 13 & 14 & 15 & 16 \end{bmatrix}$.

Ciało skalarów $\mathbb{R} = (\mathbb{R}, +, \cdot, 0, 1)$:

ciało liczb rzeczywistych.

Def. $(F, +, \cdot, 0, 1)$ <u>ciało</u>, gdy

- ~~...~~ $0, 1 \in F$, $0 \neq 1$
- $+$: przemienne, łączne, 0: el. neutralny

(tzn: $x+0 = 0+x = x$ dla wszystkich $x \in F$)

i dla każdego $x \in F$ istnieje $x' \in F$ t., że $x + x' = 0$.

(tzn: $(F, +)$: grupa abelowa.

Wtedy x': jedyny dla x, <u>przeciwny</u> do x

oznaczenie: $x' = -x$

grupa addytywna ciała F.

- $\cdot$: przemienne, łączne, 1: el. neutralny

$(\forall x \in \underbrace{F \setminus \{0\}}) (\exists x' \in F \setminus \{0\})$ $\underbrace{x' \text{ odwrotny do } x}$

$(F^*, \cdot)$: grupa multyplikatywna ciała F,

$xx' = x'x = 1$

(oznaczenie $x' = x^{-1}$)

- $\cdot$: rozdzielne względem $+$:
$$x(y+z) = xy + xz.$$

Gdy $F' \subseteq F$ t.że $0, 1 \in F'$ i
$(F', +|_{F'}, \cdot|_{F'}, 0, 1)$: ciało, to : F' : podciało ciała F.

Przykłady

$\mathbb{Q} \subseteq \mathbb{R}$, $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ też.
podciało (ćwiczenie)

element odwrotny do $\overset{\neq 0}{a + b\sqrt{2}}$ w $\mathbb{Q}(\sqrt{2})$:

w $\mathbb{R}$:
$$\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{(a+b\sqrt{2})(a-b\sqrt{2})} = \frac{a-b\sqrt{2}}{a^2-2b^2} =$$
$$= \frac{a}{a^2-2b^2} + \frac{-b}{a^2-2b^2}\sqrt{2} \in \mathbb{Q}(\sqrt{2})$$

Def. $(V, +, t)_{t \in F}$: przestrzeń liniowa nad ciałem F, gdy spełnia aksjomaty przestrzeni liniowej nad $\mathbb{R}$ $\rightsquigarrow F$

Przykłady (1) F^n, $F[X]$ zbiór wielomianów nad ciałem F, $F_n(X) = \{W(X) \in F[X] : \deg W \leq n\}$,

(2) $K \subseteq L = (L, +, \cdot, 0, 1)$ ciało podciało, | np. $\mathbb{Q} \subseteq \mathbb{R}$

L : przestrzeń liniowa nad ciałem K :

$+$: z ciała L , $t\cdot$: mnożenie w L.
dla $t \in K$

Dotychczasowa algebra liniowa nad $\mathbb{R}$ w pełni przenosi się do przestrzeni liniowych nad ciałem F.

- liniowa niezależność, baza, wymiar, macierze $M_{n\times m}(F)$
- wyznacznik : $\det(A) \neq 0 \iff A$ odwracalna.

Przykład $\mathbb{R}$: przestrzeń liniowa nad $\mathbb{Q}$.

$\dim_{\mathbb{Q}} \mathbb{R} = 2^{\aleph_0}$ baza liniowa $\mathbb{R}$ nad $\mathbb{Q}$:

"baza Hamela"

istnieje (pewnik wyboru)

Nowe ciała :

$i = \sqrt{-1}$? jednostka urojona.

Zał, że $\mathbb{R} \subseteq F$: nadciało (rozszerzenie ciał) t. że $i \in F$ t. że $i^2 = -1$.

Niech $\mathbb{R}[i] = \{a + bi : a, b \in \mathbb{R}\}$.

<u>Uwaga</u> (1) $R[i]$ jest podprzestrzenią liniową ciała F (jako przestrzeni liniowej nad $\mathbb{R}$)

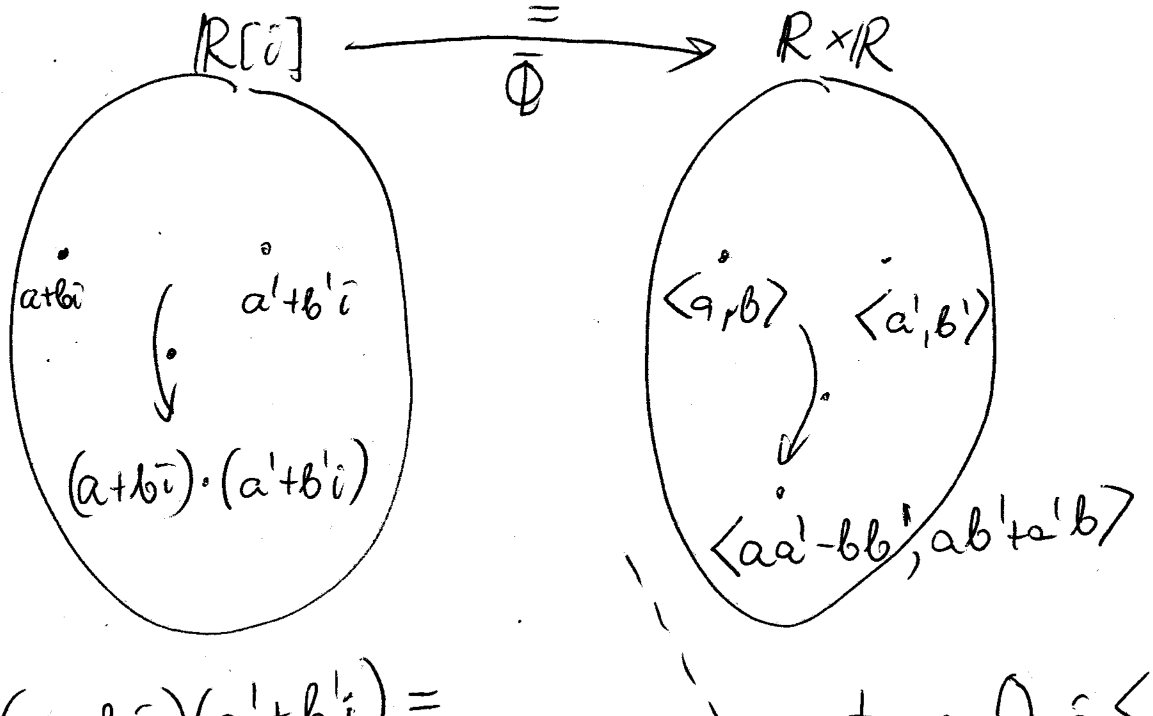
(2) $\{1, i\}$ baza $\mathbb{R}[i]$ nad $\mathbb{R}$, $\dim_{\mathbb{R}} \mathbb{R}[i] = 2$.

(3) $R[i]$ podciało ciała F.

<u>D-d</u> ćwiczenie.

$$\Phi : \mathbb{R}[i] \xrightarrow{\cong} \mathbb{R} \times \mathbb{R} = \mathbb{R}^2$$
$$a+bi \longmapsto \langle a, b\rangle$$

izomorfizm przestrzeni liniowych nad $\mathbb{R}$



$$(a+bi)(a'+b'i) =$$
$$= (aa' - bb') + (ab' + a'b)i$$

tu: $0 : \langle 0, 0\rangle$

$1 : \langle 1, 0\rangle$

$$\mathbb{C} = (\mathbb{R}\times\mathbb{R}, +, \cdot, 0, 1)$$

$$\langle a,b\rangle + \langle a',b'\rangle = \langle a+a', b+b'\rangle$$

$$\langle a,b\rangle \cdot \langle a',b'\rangle = \langle aa'-bb', ab'+ba'\rangle$$

$$0 = \langle 0,0\rangle \qquad 1 = \langle 1,0\rangle$$

ciało liczb zespolonych (konstrukcja Hamiltona)
XIX wiek

$\cancel{i = \langle 0,1\rangle}$

$\cancel{i^2 =}$

$$\begin{array}{ccc} \Phi : \mathbb{R} & \xrightarrow{\cong} & \mathbb{R}\times\{0\} \subseteq \mathbb{C} \\ \cap & & \text{podciało} \\ \mathbb{R}[i] & & \end{array}$$

<u>Utożsamiamy</u> $\mathbb{R}$ z $\mathbb{R}\times\{0\} \subseteq \mathbb{C}$.

$$i = \langle 0,1\rangle : \quad i^2 = \langle 0,1\rangle\langle 0,1\rangle = \langle -1,0\rangle = -1$$

$$\mathbb{C} \ni \langle a,b\rangle = \langle a,0\rangle + \langle b,0\rangle\langle 0,1\rangle = a+bi$$

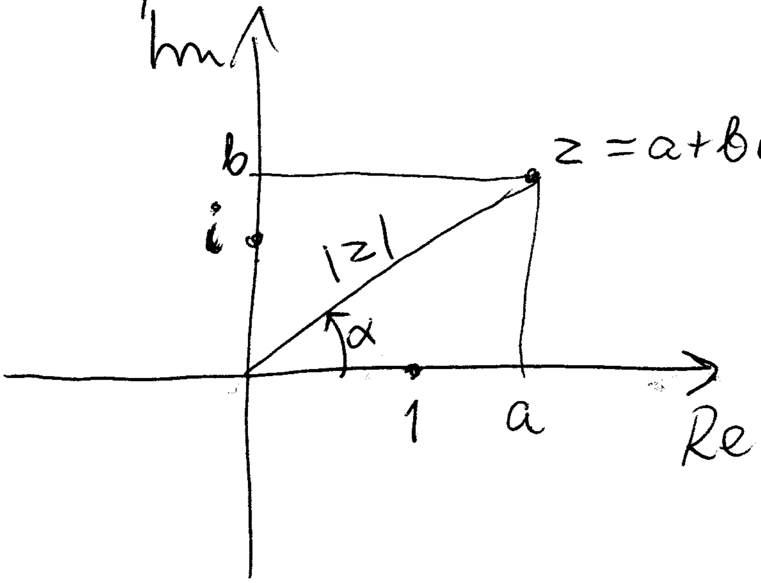
$$\mathbb{C} = \mathbb{R}[i] \ni z = a+bi, \quad a,b\in\mathbb{R}$$

postać algebraiczna liczby zespolonej z

$a = \mathrm{Re}(z)$ część rzeczywista z

$b = \mathrm{Im}(z)$: —//— urojona z. i: jednostka urojona.

· Płaszczyzna Gaussa:



$\begin{cases} 0 \leq \alpha < 2\pi \\ \text{argument główny } z \neq 0 \end{cases}$

$|z| = \sqrt{a^2+b^2}$ moduł z

· $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$ (dw.)

· $|z_1 + z_2| \leq |z_1| + |z_2|$

$a = |z| \cos\alpha$, $b = |z| \cdot \sin\alpha$

$z = |z| (\cos\alpha + i \sin\alpha) = |z| (\cos\alpha' + i \sin\alpha')$

postać trygonometryczna z $\qquad$ $\alpha' = \alpha + 2k\pi$, $k \in \mathbb{Z}$

inne argumenty z.

Uwaga

(1) $\left.\begin{aligned} z_1 &= r_1 (\cos\alpha_1 + i \sin\alpha_1) \\ z_2 &= r_2 (\cos\alpha_2 + i \sin\alpha_2) \end{aligned}\right\} \Rightarrow z_1 z_2 = r_1 r_2 (\cos(\alpha_1+\alpha_2) + i \sin(\alpha_1+\alpha_2))$

(2) $z_1^{-1} = \frac{1}{r_1} (\cos(-\alpha_1) + i \sin(-\alpha_1)) = \frac{1}{r_1} (\cos\alpha_1 - i \sin\alpha_1)$.

gdy $z_1 \neq 0$.

(3) $z = r(\cos\alpha + i\sin\alpha) \Longrightarrow z^n = r^n(\cos n\alpha + i\sin n\alpha)$ $(n \in \mathbb{Z})$

Pierwiastkowanie:

$$z^n = \overbrace{r(\cos\alpha + i\sin\alpha)}^{w \in \mathbb{C}}$$

$$\Updownarrow$$

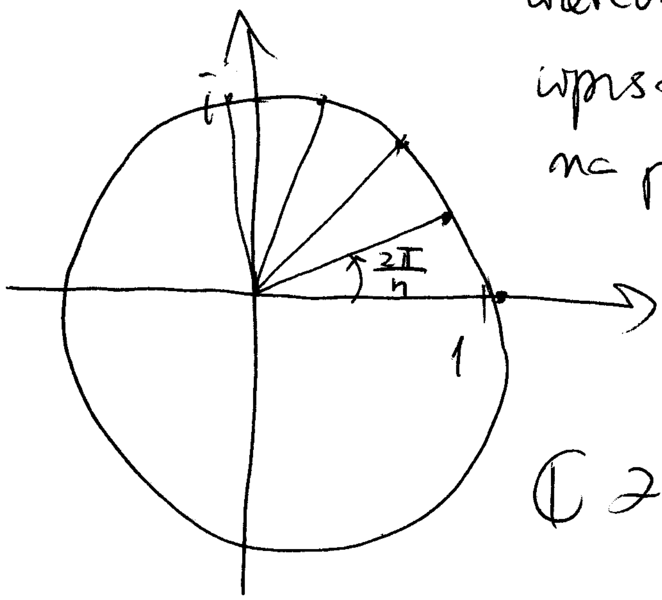
$$z = \sqrt[n]{r}(\cos\beta + i\sin\beta), \text{ gdzie } \beta = \frac{\alpha}{n} + \frac{2k\pi}{n},\ 0 \le k < n$$

gdy $\alpha \neq 0$, $r \neq 0$: n różnych pierwiastków z w w $\mathbb{C}$.

Pierwiastki stopnia n z 1:

$$z_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n},\ k = 0, 1, \dots, n-1:$$

wierzchołki n-kąta foremnego wpisanego w okrąg jednostkowy na płaszczyźnie Gaussa.



Sprzężenie:

$$\mathbb{C} \ni z = a + bi \longmapsto \bar{z} = a - bi$$

$$= r(\cos\varphi + i\sin\varphi) \to \overset{\shortparallel}{r}(\cos\varphi - i\sin\varphi)$$

$z \longmapsto \bar{z}$: automorfizm ciała $\mathbb{C} = (\mathbb{C}, +, \cdot, 0, 1)$ (ćw.)

- Ciało $\mathbb{C}$ jest algebraicznie domknięte, tzn. każdy $W(X) \in \mathbb{C}[X]$ stopnia > 0 ma pierwiastek w $\mathbb{C}$.

Ciała skończone, arytmetyka modularna

$n \geq 1 \quad r_n : \mathbb{Z} \to \mathbb{Z} \quad r_n(k) \in \{0, \dots, n-1\}$
reszta z dzielenia k przez n,

$k = l \cdot n + r_n(k) \qquad l \in \mathbb{Z}$

- $+_n$, $\cdot_n$: działania w $\mathbb{Z}$ (modulo n)

$k_1 +_n k_2 = r_n(k_1 + k_2) \qquad k_1 \cdot_n k_2 = r_n(k_1 + k_2)$

Uwaga. (1) $+_n$, $\cdot_n$ są łączne, przemienne,
$\cdot_n$: rozdzielne względem $+_n$.

(2) $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ zamknięty na $+_n$, $\cdot_n$.

(3) $(n \geq 2)$ $(\mathbb{Z}_n, +_n, \cdot_n, 0, 1)$ ciało $\iff$ n : l. pierwsza.

D-d (1), (2) : ćwiczenie.

(3): element przeciwny do $k \in \mathbb{Z}_n$: $n - k \in \mathbb{Z}_n$.

1°. Zał., że n : złożona.

$n = k \cdot l \qquad 1 \leq k, l < n$

$$\Downarrow$$

$k \cdot_n l = r_n(k \cdot l) = 0 \implies \mathbb{Z}_n$ nie jest ciałem
(bo : k nie jest odwracalny)

2°. Zał., że n : pierwsza.

$k \in \mathbb{Z}_n \setminus \{0\}$. Pok., że k odwracalny, tzn.
istnieje $l \in \mathbb{Z}_n \setminus \{0\}$ t., że $k \cdot_n l = 1$.

- $k \cdot_n 1, k \cdot_n 2, \ldots, k \cdot_n (n-1) \in \mathbb{Z}_n \setminus \{0\}$
- parami $\neq$: $k \cdot_n i \overset{?}{=} k \cdot_n j \quad 1 \leq j < i < n$

$$\Updownarrow$$

$$n \mid (k \cdot i - kj)$$

$$\Updownarrow$$

$$n \mid k \cdot (i-j) \quad 1 \leq k, i-j < n \quad ⚡.$$

- stąd $k \cdot_n l = 1$ dla pewnego $l \in \mathbb{Z}_n \setminus \{0\}$.

<u>Przykłady</u> . $\mathbb{Z}_2 = \{0,1\}$ ciało 2-elementowe, $+_2, \cdot_2$

. $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ p-elementowe, $+_p, \cdot_p$.

<u>Uwaga</u> Jeśli ciało F jest skończone, to $|F| = p^n$ dla pewnej l. pierwszej p i $n \geq 1$.

- algebra liniowa nad ciałem skończonym F
  - matematyka dyskretna, grafika komputerowa,
  - kody korygujące błędy.

Z powrotem do wyznaczników:

Przykład 1. $\det A$

$$A = \begin{bmatrix} 1 & 2 & 3 & 1 \\ 2 & 1 & 3 & 1 \\ 1 & 3 & 2 & 1 \\ 2 & 1 & 3 & 0 \end{bmatrix} \begin{matrix} \\ -2\cdot[1] \\ -1\cdot[1] \\ +2[1] \end{matrix} \rightarrow \begin{bmatrix} 1 & 2 & 3 & 1 \\ 0 & -3 & -3 & -1 \\ 0 & 1 & -1 & 0 \\ 0 & -3 & -3 & -2 \end{bmatrix} \begin{matrix} \\ \\ +\frac{1}{3}[2] \\ -[2] \end{matrix} \rightarrow \begin{bmatrix} 1 & 2 & 3 & 1 \\ 0 & -3 & -3 & -1 \\ 0 & 0 & -2 & -\frac{1}{2} \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

$$\det = 1 \cdot (-3) \cdot (-2) \cdot (-1) = -6.$$

$\Rightarrow \begin{pmatrix}1\\2\\1\\2\end{pmatrix}, \begin{pmatrix}2\\1\\3\\1\end{pmatrix}, \begin{pmatrix}3\\3\\2\\3\end{pmatrix}, \begin{pmatrix}1\\1\\1\\0\end{pmatrix} \in \mathbb{R}^2$ są liniowo niezależne.

2. Załóżmy, że $\mathcal{B} = \{b_1, b_2, b_3, b_4\} \subseteq V$ baza.

$v_1 = b_1 + 2b_2 + b_3 + 2b_4$

$v_2 = 2b_1 + b_2 + 3b_3 + b_4$

$v_3 = 3b_1 + 3b_2 + 2b_3 + 3b_4$

$v_4 = b_1 + b_2 + b_3$

Czy v_1, v_2, v_3, v_4 są liniowo niezależne?

$\Updownarrow$

$F : V \xrightarrow{\cong} \mathbb{R}^4$

$v \longmapsto [v]_{\mathcal{B}}$

$\left[F(v_1) = \begin{bmatrix}1\\2\\1\\2\end{bmatrix}, F(v_2) = \begin{bmatrix}2\\1\\3\\1\end{bmatrix}, F(v_3) = \begin{bmatrix}3\\3\\2\\3\end{bmatrix}, F(v_4) = \begin{bmatrix}1\\1\\1\\0\end{bmatrix} \right.$

$\left.\text{są lin. niezależne w } \mathbb{R}^4\right]$

$\Updownarrow$

$\det A \neq 0$