EXISTENCE KONEČNÝCH PROJEKTIVNÍCH ROVIN:

- **VĚTA 3.1**: POKUD EXISTUJE ALGEBRAICKÉ TĚLESO O m PRVCÍCH, POTOM EXISTUJE KONEČNÁ PROJEKTIVNÍ ROVINA ŘÁDU m

  EXISTUJÍ $\Leftrightarrow$ m JE MOCNINA PRVOČÍSLA A JSOU URČENY JEDNOZNAČNĚ AŽ NA IZOMORFISMUS

- KONSTRUKCE FUNGUJE NAD KAŽDÝM TĚLESEM A NAPŘÍKLAD NAD $\mathbb{R}$ DÁVÁ REÁLNOU PROJEKTIVNÍ ROVINU

- DK:
  - MĚJME TĚLESO $\mathbb{K}$ (VELIKOSTI m), ZAVEĎME NA $\mathbb{K}^3$ EKVIVALENCI $\sim$ PŘEDPISEM $(x,y,z) \sim (\alpha x, \alpha y, \alpha z)$ PRO KAŽDÉ $(x,y,z) \in \mathbb{K}^3$ A $\alpha \in \mathbb{K} \setminus \{0\}$
  - BODY PROJEKTIVNÍ ROVINY = TŘÍDY EKVIVALENCE $\sim$ NA $\mathbb{K}^3 \setminus \{(0,0,0)\}$
    - POČET BODŮ $= \dfrac{m^3-1}{m-1} = \underline{\underline{m^2+m+1}}$

      $= $ VELIKOST $\mathbb{K}^3 \setminus \{(0,0,0)\}$, PROTOŽE $|\mathbb{K}| = m$

      $= $ VELIKOST KAŽDÉ TŘÍDY V $\sim$, PROTOŽE $\alpha \in \mathbb{K} \setminus \{0\}$ A $|\mathbb{K} \setminus \{0\}| = m-1$

  - PŘÍMKY PROJEKTIVNÍ ROVINY:
  - PRO KAŽDÉ $(a,b,c) \in \mathbb{K}^3 \setminus \{(0,0,0)\}$ DEFINUJEME PŘÍMKU $P_{a,b,c} = \{[(x,y,z)]_\sim : (x,y,z) \in \mathbb{K}^3 \setminus \{(0,0,0)\} : ax+by+cz=0\}$

    $P_{a,b,c}$ JE MNOŽINA TŘÍD EKVIVALENCE $\sim$

    - PLATÍ, ŽE $(a,b,c) \sim (a',b',c') \Leftrightarrow P_{a,b,c} = P_{a',b',c'}$

      $\Rightarrow$ MÁME m^2+m+1 PŘÍMEK

  - OVĚŘME AXIOMY (A1), (A2), (A3)
  - (A1):
    - MĚJME DVA RŮZNÉ BODY (x,y,z) A (x',y',z')
    - POTOM $\operatorname{RANK}\begin{pmatrix} x & y & z \\ x' & y' & z' \end{pmatrix} = 2$

      PROTOŽE $(x,y,z) \not\sim (x',y',z')$

      - PŘÍMKA OBSAHUJÍCÍ (x,y,z) A (x',y',z') ODPOVÍDÁ JÁDRU TÉTO MATICE

    - JÁDRO MÁ DIMENZI 1 $\Rightarrow$ EXISTENCE A JEDNOZNAČNOST PŘÍMKY

      DIM > 0 DIM < 2

  - (A2):
    - DVĚ RŮZNÉ PŘÍMKY $P_{a,b,c}$ A $P_{a',b',c'}$ URČUJÍ JEDNOZNAČNĚ BOD V JEJICH PRŮNIKU
    - ANALOGICKY Z MATICE $\begin{pmatrix} a & b & c \\ a' & b' & c' \end{pmatrix}$
  - (A3):
    - STAČÍ ZVOLIT $C := \{(0,0,1), (0,1,0), (1,0,0), (1,1,1)\}$
    - KAŽDÁ TROJICE BODŮ Z C JE PAK LINEÁRNĚ NEZÁVISLÁ A TEDY BODY Z C JSOU V OBECNÉ POLOZE ☒

- **LATINSKÝ ČTVEREC** řádu $m \in \mathbb{N}$ je tabulka $m \times m$ čísel z $\{1,\dots,m\}$, ve které se žádné číslo neopakuje v žádném řádku ani sloupci
  - dříve se latinské čtverce vyplňovaly písmeny latinky, proto se jim říká latinské
- latinské čtverce L, L' stejného řádu jsou **ORTOGONÁLNÍ**, pokud pro každé $l, l' \in \{1,\dots,m\}$ existují $i, j \in \{1,\dots,m\}$ takové, že $L_{ij} = l$, $L'_{ij} = l'$
  - zapisujeme $L \perp L'$
- motivace pochází od L. Eulera a jeho „problému 36 důstojníků": lze 6 pluků, kde každý pluk sestává z 6 členů různých hodností, uspořádat do čtverce 6×6 tak, aby v žádném sloupci ani řádku nebyli členové stejné hodnosti či stejného pluku? – neboli $\exists$ 2 ortogonální latinské čtverce řádu 6?
- PŘÍKLAD:

L

1	2	3
2	3	1
3	1	2

L'

1	2	3
3	1	2
2	3	1

$\longrightarrow$ $L \perp L'$

1, 1	2, 2	3, 3
2, 3	3, 1	1, 2
3, 2	1, 3	2, 1

dva ortogonální latinské čtverce řádu 3, každý z $3^2 = 9$ párů $(l, l') \in \{1,2,3\} \times \{1,2,3\}$ se vyskytuje na nějaké pozici (i,j) v $L \perp L'$

- **POZOROVÁNÍ 5.2**: Pro ortogonální latinské čtverce L, L' řádu m a pár $(l, l') \in \{1,\dots,m\} \times \{1,\dots,m\}$ je pozice (i,j) s $L_{ij} = l$, $L'_{ij} = l'$ určena jednoznačně. ⊠
- DK: počet párů (l, l') je m^2, stejně jako počet párů (i,j)
- **POZOROVÁNÍ 5.3**: Je-li $L = (L_{ij})_{i,j=1}^{m}$ latinský čtverec a $\pi : \{1,\dots,m\} \to \{1,\dots,m\}$ permutace, tak potom $\pi(L) := (\pi(L_{ij}))_{i,j=1}^{m}$ je latinský čtverec stejného řádu. ⊠

  $\Rightarrow$ BÚNO první řádek je vždy $1, 2, \dots, m$

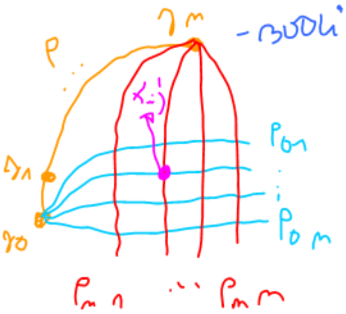
  $\Rightarrow$ je-li $L \perp L'$, pak $\pi(L) \perp L'$

- **DŮSLEDEK 5.4**: Počet navzájem ortogonálních (tedy po dvou ortogonálních) čtverců řádu $m \in \mathbb{N}$ je nanejvýš $m - 1$.
- DK:
  - BÚNO $L_1, \dots, L_m$ navzájem ortogonální latinské čtverce řádu m
  - BÚNO první řádky jsou $1, 2, \dots, m$ (podle Pozorování 5.3)
  - na pozici $(2,1)$ mohou být jen čísla $2, 3, \dots, m$ a každé z nich je v nanejvýš jednom čtverci L_k

    ↳ podle Pozorování 5.2, protože každý pár (l, l) je na pozici $(1, l)$ ⊠

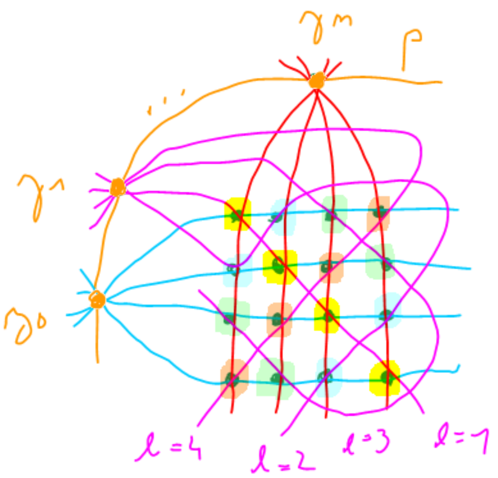
$\Rightarrow \underline{\underline{m \le m - 1}}$

- NYNÍ DÁME DO SOUVISLOSTI ORTOGONÁLNÍ ČTVERCE A KONEČNÉ PROJEKTIVNÍ ROVINY
- **VĚTA 5.5**: KONEČNÁ PROJEKTIVNÍ ROVINA ŘÁDU $m \geq 2$ EXISTUJE $\iff$ EXISTUJE $m-1$ NAVZÁJEM ORTOGONÁLNÍCH LATINSKÝCH ČTVERCŮ ŘÁDU m
- DK:
  - (⇒):
    - DÁNA KONEČNÁ PROJEKTIVNÍ ROVINA $(X, \mathcal{P})$ ŘÁDU $m \geq 2$
    - CHCEME SESTROJIT NAVZÁJEM ORTOGONÁLNÍ LATINSKÉ ČTVERCE $L_1, \dots, L_{m-1}$ ŘÁDU m
    - UVAŽME LIBOVOLNOU PŘÍMKU $P = \{y_0, \dots, y_m\} \in \mathcal{P}$
    - KAŽDÝM BODEM y_i PROCHÁZÍ m DALŠÍCH PŘÍMEK $P_{i1}, \dots, P_{im}$
    - PRO KAŽDÉ $i, j \in \{1, \dots, m\}$ OZNAČME JAKO X_{ij} PRŮNIK P_{0i} A P_{mj}
    - BODŮ X_{ij} JE m^2, BODŮ $y_0, \dots, y_m$ JE $m+1$ ⇒ MÁME VŠECH m^2+m+1 BODŮ Z X
      - PŘÍMKY OBSAHUJÍCÍ BODY y_0 A y_m SLOUŽÍ K „URČENÍ SOUŘADNIC"
      - PŘÍMKY OBSAHUJÍCÍ BODY $y_1, \dots, y_{m-1}$ BUDOU ODPOVÍDAT LATINSKÝM ČTVERCŮM $L_1, \dots, L_{m-1}$



- PRO $k \in \{1, \dots, m-1\}$ A $l \in \{1, \dots, m\}$ SE PŘÍMKA $P_{k,l}$ MUSÍ PROPLÉST MŘÍŽKOU $m \times m$ URČENOU PŘÍMKAMI Z y_0 A y_m – TÍMTO PROPLÉTÁNÍM URČÍ POZICE PRVKU l VE ČTVERCI L_k
- FORMÁLNĚ – NASTAVÍME $(L_k)_{ij} = l \iff X_{ij} \in P_{kl}$ PRO $\forall i = 1, \dots, m$, $\forall j = 1, \dots, m$
- PŘÍKLAD:

–



L_1

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

- ukážeme, že $L_1, \dots, L_{m-1}$ jsou navzájem ortogonální latinské čtverce řádu m
- mějme $k \in \{1, \dots, m-1\}$, na každé pozici (i,j) je v L_k číslo $\ell \in \{1, \dots, m\}$, podle (A1)
- v řádcích L_k se nic neopakuje (tedy $(L_k)_{i,j} \neq (L_k)_{i,j'}$ pro $\forall i = 1, \dots, m$, $\forall j = 1, \dots, m$, $\forall j' = 1, \dots, m$, $j \neq j'$):
  - spor: $\exists i, j, j' \in \{1, \dots, m\}$, $j \neq j'$: $(L_k)_{i,j} = (L_k)_{i,j'} = \ell$
  - potom $|P_{k\ell} \cap P_{0i}| \geq 2 \Rightarrow$ spor s (A2)

nelze podle (A2)

- analogicky se nic neopakuje ve sloupcích L_k
  - kdyby $\exists i, i', j \in \{1, \dots, m\}$: $(L_k)_{i,j} = (L_k)_{i',j} = \ell$, pak $|P_{k\ell} \cap P_{mj}| \geq 2$, $i \neq i'$
- pro $k, k' \in \{1, \dots, m-1\}$ s $k \neq k'$ ukážeme, že $L_k \perp L_{k'}$:
  - chceme $\forall \ell, \ell' \in \{1, \dots, m\}$ $\exists i, j \in \{1, \dots, m\}$: $(L_k)_{i,j} = \ell$ & $(L_{k'})_{i,j} = \ell'$
  - přímky $P_{k\ell}$ a $P_{k'\ell'}$ se podle (A2) protínají v nějakém bodě x_{ij}
  - z konstrukce pak platí $(L_k)_{i,j} = \ell$ & $(L_{k'})_{i,j} = \ell'$ a tedy $L_k \perp L_{k'}$

(ii) $\Leftarrow$:
- mějme navzájem ortogonální latinské čtverce $L_1, \dots, L_{m-1}$ řádu $m \geq 2$
- zkonstruujeme konečnou projektivní rovinu (X, P) řádu m
- zvolme $X = \{y_0, \dots, y_m\} \cup \{x_{ij} : i, j = 1, \dots, m\}$
- do množiny P přidejme přímky $P = \{y_0, \dots, y_m\}$, $P_{0i} = \{y_0, x_{i1}, \dots, x_{im}\}$, $P_{mj} = \{y_m, x_{1j}, \dots, x_{mj}\}$, $P_{k\ell} = \{y_k\} \cup \{x_{ij} : (L_k)_{ij} = \ell\}$ pro $k = 1, \dots, m-1$, $i, j, \ell = 1, \dots, m$
- potom (X, P) je konečná projektivní rovina řádu m:
  - stačí ověřit axiomy (A1), (A2), (A3)

- (A3) ($\exists$ 4 body v obecné poloze):
  - stačí vzít $C = \{y_0, y_m, x_{11}, x_{22}\}$ $\Rightarrow$ (A3) platí

existuje, protože $m \geq 2$

- (A2) (každé 2 přímky se protínají v ≤ 1 bodě):
  - ověřit rozborem případů
  - máme nevlastní přímku P, vodorovné P_{0i}, svislé P_{mj} a šikmé $P_{k\ell}$, $k = 1, \dots, m-1$, $\ell = 1, \dots, m$
  - a) nevlastní přímka (A2) splňuje z definice
  - b) vodorovná $\cap$ vodorovná $= \{y_0\}$, svislá $\cap$ svislá $= \{y_m\}$
  - c) vodorovná $P_{0i} \cap$ svislá $P_{mj} = \{x_{ij}\}$
  - d) $|\text{vodorovná } P_{0i} \cap \text{šikmá } P_{k\ell}| = |\{x_{ij} : (L_k)_{ij} = \ell\}| = 1$

na řádku i má L_k prvek ℓ jednou

  - e) $|\text{svislá } P_{mj} \cap \text{šikmá } P_{k\ell}| = |\{x_{ij} : (L_k)_{ij} = \ell\}| = 1$

ve sloupci j má L_k prvek ℓ jednou

– 1) šikmá P_{kl} ∩ šikmá $P_{k'l'}$:

- pokud $k = k'$, pak $P_{kl} \cap P_{k'l'} = \{\gamma_k\}$
- jinak $|P_{kl} \cap P_{k'l'}| = |\{x_{ij} : (L_k)_{ij} = l \ \& \ (L_{k'})_{ij} = l'\}| = 1$

protože $L_k \perp L_{k'}$

⇒ (A2) platí

– (A1) (každé 2 body určují přímku):

- máme m^2+m+1 bodů a m^2+m+1 přímek
- spočítejme 2 způsoby počet $z := |\{(\{a,b\}, P) : a,b \in X, a \neq b, P \in \mathcal{P}, a,b \in P\}|$
- $z = (m^2+m+1)\binom{m+1}{2}$, protože $\forall P \in \mathcal{P}$ přispěje $\binom{m+1}{2}$ páry $\{a,b\}$
- na druhou stranu každými 2 body prochází podle (A2) ≤ 1 přímka

  a tedy $\binom{m^2+m+1}{2} \geq z$
- protože $\binom{m^2+m+1}{2} = \binom{m+1}{2}(m^2+m+1)$, tak musí procházet právě 1 přímka každými dvěma body z X ⇒ (A1) platí ☒

– ∄ konečná projektivní rovina řádu 6, protože ∄ 5 navzájem ortogonálních latinských čtverců řádu 6

- ∄ dokonce ani 2 takové čtverce (Tarry, 1900)

  ⇒ záporná odpověď na Eulerův problém 36 důstojníků