Definicija: Aksiomatsko definirana afina ravnina je sestavljena iz množice točk $\mathcal{A}$ in množice premic $\mathcal{A}_1 \subseteq \mathcal{P}(\mathcal{A})$, ki zadoščata aksiomom:

A_1: Skozi poljubni različni točki poteka natanko ena premica.

A_2: Za vsako premico p in točko T, ki ne leži na p, obstaja natanko ena vzporednica q točke p skozi T.

A_3: Obstajajo 3 nekolinearne točke.

Definicija: Premici p in q sta vzporedni, če je $p = q$ ali $p \cap q = \emptyset$.

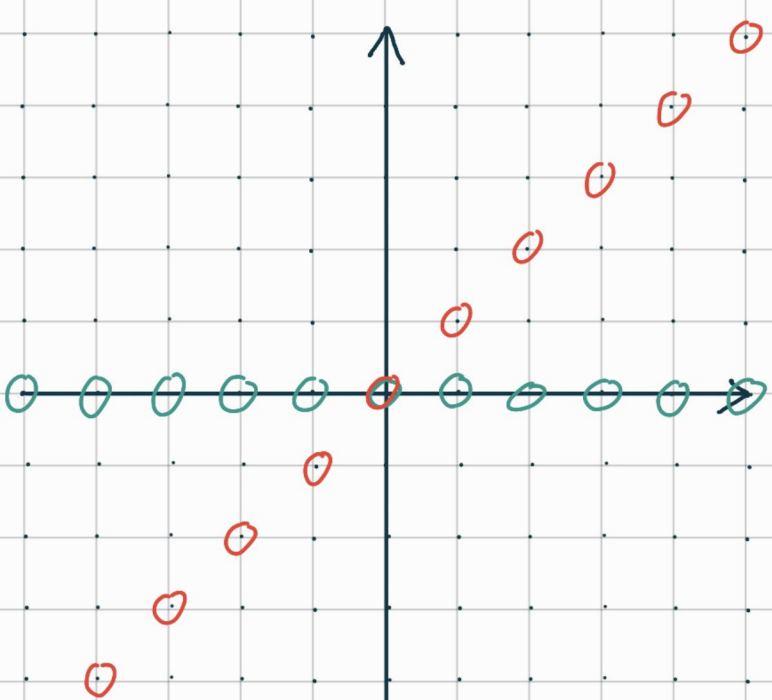
Opomba: Iz A_3 sledi, da nobena premica ne vsebuje vseh točk.

---

1) Ugotovi, ali par zadošča aksiomom za afino ravnino.

$\mathcal{A} = \mathbb{Z} \times \mathbb{Z} \subseteq \mathbb{R}^2$

$\mathcal{A}_1 = \{ p \cap \mathcal{A} ;\ p \text{ premica } ax + by = c,\ a, b, c \in \mathbb{Z} \} \setminus \{\emptyset\}$



$p_1: y = 0 \;;\; a=0, b=1, c=0$
$p_2: y = x \;;\; a=1, b=-1, c=0$

A_1: Izberimo točki $T_1(x_1, y_1), T_2(x_2, y_2) \in \mathbb{Z}^2$.

i) $x_1 = x_2$:

$x = x_1$

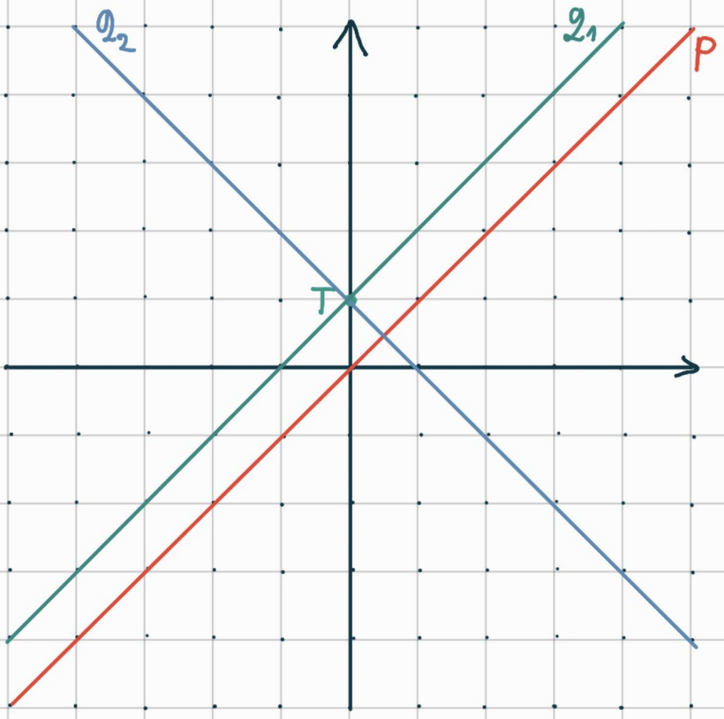
$a = 1$
$b = 0$
$c = x_1$

ii) $x_1 \neq x_2$:

$$y - y_1 = \frac{y_2 - y_1}{x_2 - x_1}(x - x_1) \quad \cdot (x_2 - x_1)$$
$$(x_2 - x_1)\cdot y - (x_2 - x_1)\cdot y_1 = (y_2 - y_1)\cdot x - (y_2 - y_1)\cdot x_1$$
$$\underbrace{-(y_2 - y_1)}_{a}\cdot x + \underbrace{(x_2 - x_1)}_{b}\cdot y = \underbrace{(x_2 - x_1)\cdot y_1 - (y_2 - y_1)\cdot x_1}_{c}$$

Enoličnost sledi iz $\mathbb{R}^2$.

A_2:



g_1 in g_2 sta različni vzporednici p skozi T, torej aksiom A_2 ne velja.

To je zato, ker se g_2 in p sekata v $\mathbb{R}^2$ izven $\mathbb{Z}^2$.

A_3: Nobena premica ne vsebuje vseh točk $\mathbb{Z}^2$.

Opomba: Za poljuben obseg $\mathcal{O}$ afina ravnina $\mathcal{O}^2$ zadošča aksiomom A1, A2, A3.

---

2) Dokaži, da v vsaki končni afini ravnini veljajo trditve:

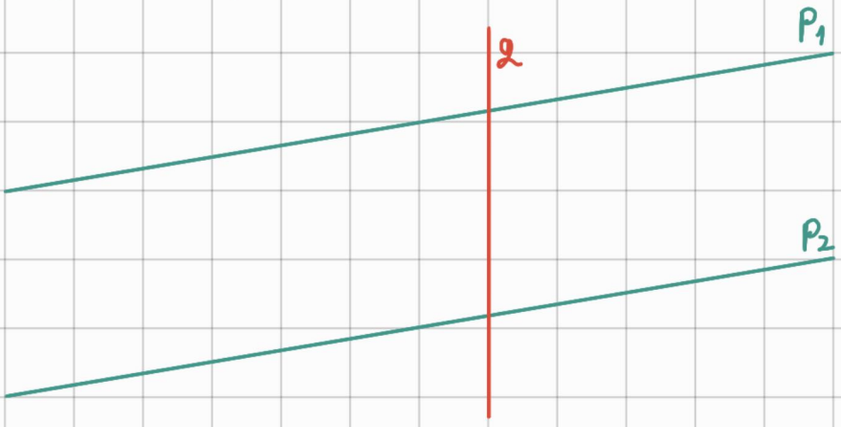
a) Naj bosta p_1 in p_2 vzporedni premici ter g poljubna od njiju različna premica. Potem g seka p_1 natanko tedaj, ko g seka p_2.

b) Na vsaki premici ležita vsaj 2 točki.

c) Vse premice imajo enako število točk.

a) Če je $p_1 = p_2$, očitno trditev velja.

Naj bo $p_1 \cap p_2 = \emptyset$.



Recimo, da se p_1 in q sekata v točki T in da je $p_2 \cap q = \emptyset$. Torej sta p_2 in q vzporedni.

Potem bi skozi točko T potekali dve različni vzporednici premice p_2.

To je protislovje z A_2.

Opomba: Od tod sledi, da je vzporednost ekvivalenčna relacija.

b) Recimo, da premica p vsebuje eno samo točko T.

Po A_3 obstaja točka $T_1 \neq T$.

Po A_1 obstaja premica q skozi T in T_1.

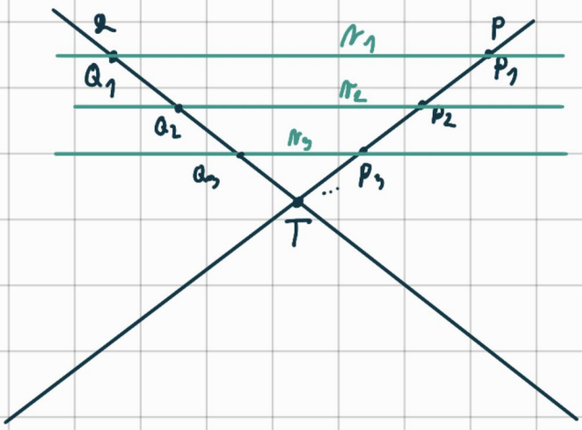
Po A_3 obstaja točka $T_2 \notin q$.

Po A_2 obstaja vzporednica l premici q skozi T_2.

Skozi točko T imamo torej vzporednici p in q premice l, kar je protislovje z A_2.

c) Pokazati želimo, da za poljubni premici p, q velja $|p| = |q|$.

i) $p \cap q = \{T\}$:



Naj bo $p = \{T, P_1, P_2, \dots, P_n\}$.

Po (b) obstaja na q točka Q_1.

Po A_1 obstaja premica r_1 skozi P_1 in Q_1.

Po A_2 za $j = 2, \dots, n$ obstaja natanko ena vzporednica r_j premice r_1 skozi P_j.

Po (a) mora q sekati vse vzporednice r_j v točkah Q_j.

Ker so r_j parama disjunktne, so Q_j različne točke.

$\Rightarrow |q| \geq |p|$

Iz simetrije $|q| \leq |p|$.

$\Rightarrow |q| = |p|$

ii) $p \parallel q$:

Izberemo premico r, ki seka p in q.

Po (i) sledi $|p| = |r| = |q|$.

Definicija: Red afine ravnine je število točk na vsaki premici.

Primer: Afina ravnina $\mathbb{Z}_p^2$ je reda p.

---

3) Naj bo $\mathcal{A}$ končna afina ravnina reda n. Pokaži trditve:

a) $\mathcal{A}$ vsebuje n^2 točk.

b) Skozi vsako točko v $\mathcal{A}$ poteka $n+1$ premic.

c) $\mathcal{A}$ vsebuje n^2+n premic.

a) Začnimo s premico $p = \{T_1, \dots, T_n\}$.

Po A_3 obstaja točka $T \notin p$.

Po A_1 obstaja premica l_1 skozi T in T_1.

Po A_2 za $j = 2, \dots, n$ obstajajo vzporednice l_j premice l_1 skozi T_j.

Premice $l_1, \dots, l_n$ so parana disjunktne in vsaka vsebuje natanko n točk.

$\Rightarrow \mathcal{A}$ ima vsaj n^2 točk.

Recimo, da obstaja točka V_1, ki ne leži na nobeni izmed $l_1, \dots, l_n$.

Po A_2 obstaja vzporednica l premice l_1 skozi V_1.

Ker p seka l_1, ki je vzporedna l, potem p seka tudi l v neki točki T_j.

Skozi T_j bi potem imeli dve vzporednici l_j in l premice l_1, kar je protislovje z A_2.

$\Rightarrow \mathcal{A}$ ima natanko n^2 točk.

b) Recimo, da skozi točko T poteka premice $p_1, \dots, p_k$.

Dokazati želimo, da je $k = n+1$.

Po A_1 je $p_1 \cup \dots \cup p_k = \mathcal{A}$.

Po A_1 je $p_i \cap p_j = \{T\}$.

$p_1 \setminus \{T\}, \dots, p_k \setminus \{T\}, \{T\}$ so parama disjunktne in sestavljajo $\mathcal{A}$.

$k(n-1) + 1 = n^2$

$\Rightarrow k = n+1$

c) Točk je n^2, skozi vsako je $n+1$ premic.

Vsako premico smo šteli n-krat.

$\Rightarrow \# = \frac{n^2(n+1)}{n} = n(n+1) = n^2 + n$

Definicija: Latinski kvadrat reda n je $n \times n$ tabela znakov $\{A_1, \dots, A_n\}$, ki ima lastnost, da se vsak znak pojavi v vsaki vrstici in vsakem stolpcu natanko enkrat.

Dva latinska kvadrata lahko spojimo.

Primer:

1	2	3
2	3	1
3	1	2

A	B	C
B	C	A
C	A	B

1A	2B	3C
2B	3C	1A
3C	1A	2B

Ta dva sista ortogonalna.

Definicija: Latinska kvadrata sta ortogonalna, če se v njunem spoju pojavijo vsi možni urejeni pari.

Dobljenemu kvadratu rečemo grško-latinski kvadrat.

Primer:

1	2	3
2	3	1
3	1	2

A	B	C
C	A	B
B	C	A

1A	2B	3C
2C	3A	1B
3B	1C	2A

Ta dva sta ortogonalna.

Velja:

1) Latinski kvadrati obstajajo za vse $n \in \mathbb{N}$.

2) Grško-latinski kvadrati obstajajo za vse $n \in \mathbb{N} \setminus \{2,6\}$.

3) Pri danem n obstaja največ $n-1$ paroma ortogonalnih latinskih kvadratov reda n. Njihov obstaj je ekvivalenten obstoju afine ravnine reda n.

Primer: Geometrija $GF(4)$ $\longrightarrow$ Paroma ortogonalni latinski kvadrati reda 4:

Smeri:

$(1,0)$
$(0,1)$
$(1,1)$
$(1,x)$
$(1,1+x)$

$(1,1)$:

$\Rightarrow$

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

$(1,x)$:

$\Rightarrow$

D	B	A	C
C	A	B	D
B	D	C	A
A	C	D	B

$(1,1+x)$:

$\Rightarrow$

δ	α	γ	β
γ	β	δ	α
β	γ	α	δ
α	δ	β	γ

---

4) Konstruiraj $m-1$ paroma ortogonalnih latinskih kvadratov reda m, kjer je m praštevilo.

Vzeli bomo afino ravnino $\mathbb{Z}_m^2$, kjer je m praštevilo.

V $\mathbb{Z}_m^2$ imamo $m+1$ smeri:

- $(1,0)$ ... vodoravna
- $(0,1)$ ... navpična
- $(1,x)$ ... poševne, $x \in \{1, \dots, m-1\}$

V vsaki poševni smeri imamo n vzporednih, $p_1, \dots, p_n$.

Naredimo latinski kvadrat tako, da na mesta premice p_i napišemo znake A_i. Ker vsaka poševna premica seka vsako vodoravnico in vsako navpičnico le enkrat, je to res latinski kvadrat.

Recimo, da imamo različni poševni smeri in vzporednice $p_1, \dots, p_n$ in $q_1, \dots, q_n$, ki nam priredijo latinska kvadrata.

Ker imamo dve različni poševni smeri, se premici p_i in q_j sekata v natanko eni točki. Torej se vsak par znakov pojavi natanko enkrat.

Dobimo grško-latinski kvadrat.