離散数理工学 第 8 回
離散代数：有限体の応用

岡本 吉央
okamotoy@uec.ac.jp

電気通信大学

2015 年 12 月 8 日

最終更新：2015 年 12 月 9 日　08:17

スケジュール 前半 (予定)

1. 数え上げの基礎：二項係数と二項定理 (10/6)
- ⋆ 休講 (体育祭) (10/13)
2. 数え上げの基礎：漸化式の立て方 (10/20)
3. 数え上げの基礎：漸化式の解き方 (基礎) (10/27)
- ⋆ 祝日で休み (11/3)
4. 数え上げの基礎：漸化式の解き方 (発展) (11/10)
5. 離散代数：整数と有限体 (11/17)
6. 離散代数：多項式環 (11/24)
7. 離散代数：多項式環による有限体の構成 (12/1)
8. 離散代数：有限体の応用 (12/8)

注意：予定の変更もありうる

スケジュール 後半 (予定)

9	離散確率論：確率の復習と確率不等式	(12/15)
⋆	中間試験	(12/22)
10	離散確率論：確率的離散システムの解析	(1/5)
11	離散確率論：乱択データ構造とアルゴリズム (基礎)	(1/12)
12	離散確率論：乱択データ構造とアルゴリズム (発展)	(1/19)
13	離散確率論：マルコフ連鎖 (基礎)	(1/26)
14	離散確率論：マルコフ連鎖 (発展)	(2/2)
⋆	予備日	(2/9)
⋆	期末試験	(2/16?)

注意：予定の変更もありうる

今日の目標

- 有限体を用いて射影平面を構成する
- 射影平面を用いて組合せデザインの問題を解く

目次

考えたい問題の種類

7 種類のワインを 7 人のスタッフで品評したい

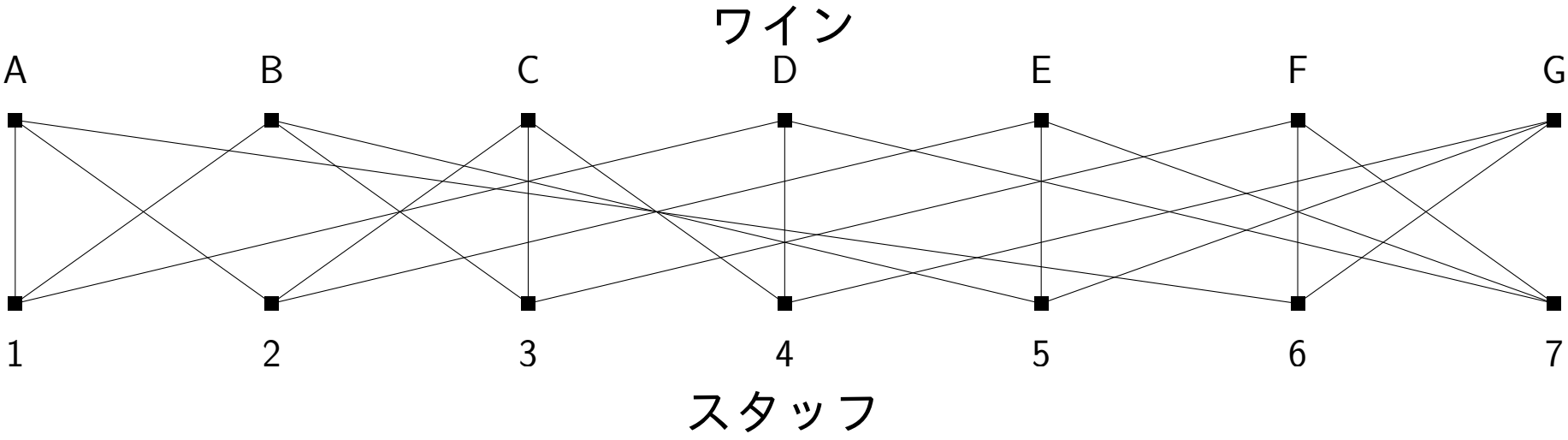
公平にするため，次を満たすようにしたい

- どのワインも，3 人のスタッフが品評する
- どの 2 つのワインも，あるスタッフが同時に品評する

問題

このような品評の仕方は可能か？

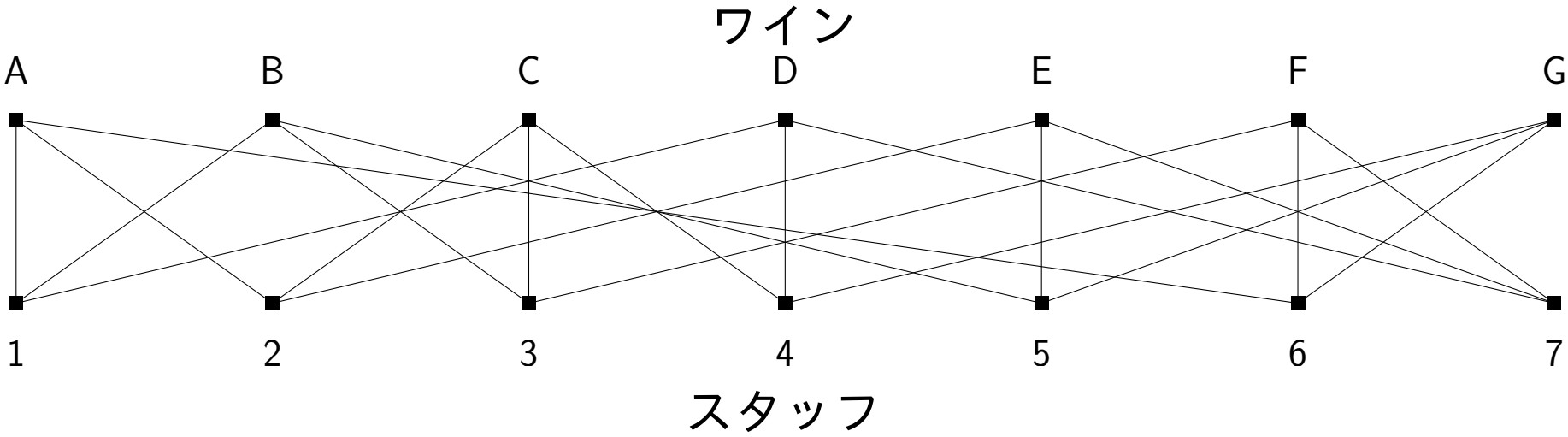
答：可能



つまり，各スタッフ 1, 2, ..., 7 は次のワインを品評する

- 1: A, B, D
- 2: A, C, E
- 3: B, C, F
- 4: C, D, G
- 5: B, E, G
- 6: A, F, G
- 7: D, E, F

疑問



次の問い

どうやって見つけるのか？

この問いに対する回答：「射影平面」を用いる

目次

射影平面：例 — 考える空間は $\mathbb{Z}_2^3$

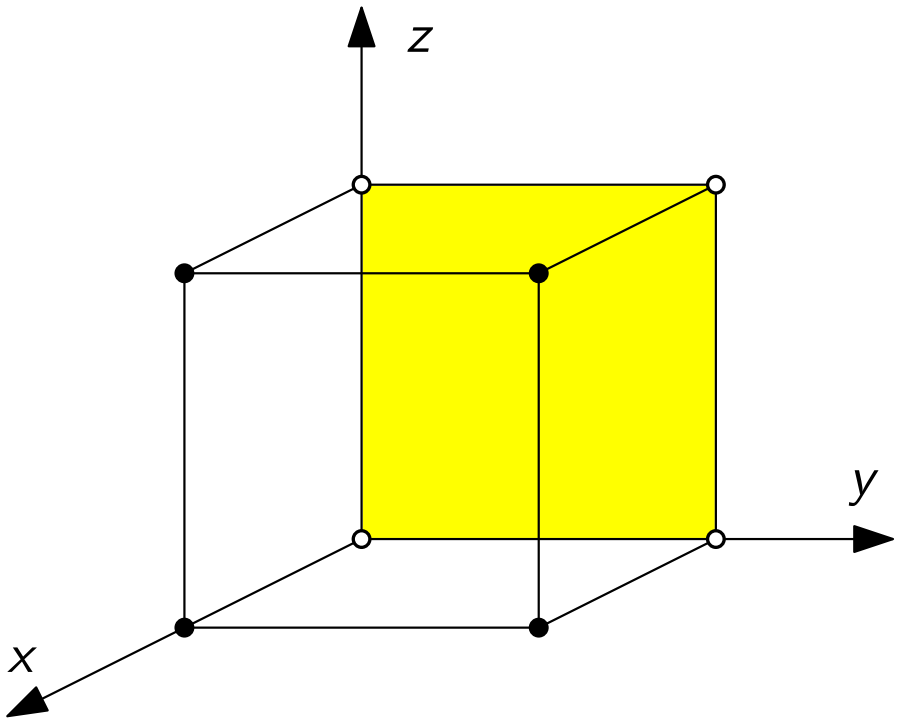
- $\mathbb{Z}_2^3$ を考える

$$\begin{aligned}\mathbb{Z}_2^3 = \{&(0,0,0),(1,0,0),(0,1,0),(0,0,1),\\ &(1,1,0),(1,0,1),(0,1,1),(1,1,1)\}\end{aligned}$$

- $\mathbb{Z}_2^3$ は線形空間

射影平面：例 — $\mathbb{Z}_2^3$ における平面

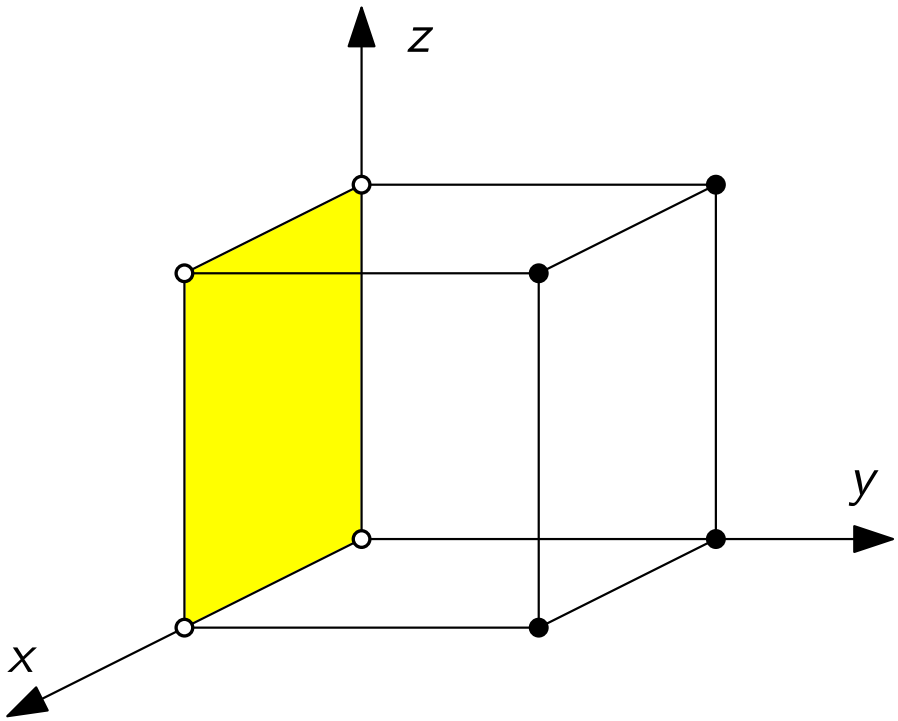
- $\mathbb{Z}_2^3$ において，原点 $(0,0,0)$ を通る平面は，$(a,b,c) \in \mathbb{Z}_2^3 - \{\mathbf{0}\}$ を使って
$$\{(x,y,z) \mid ax + by + cz = 0\}$$
と書ける
- 異なる (a,b,c) に対して，異なる平面が得られる



$$\{(x,y,z) \mid x = 0\}$$

射影平面：例 — $\mathbb{Z}_2^3$ における平面

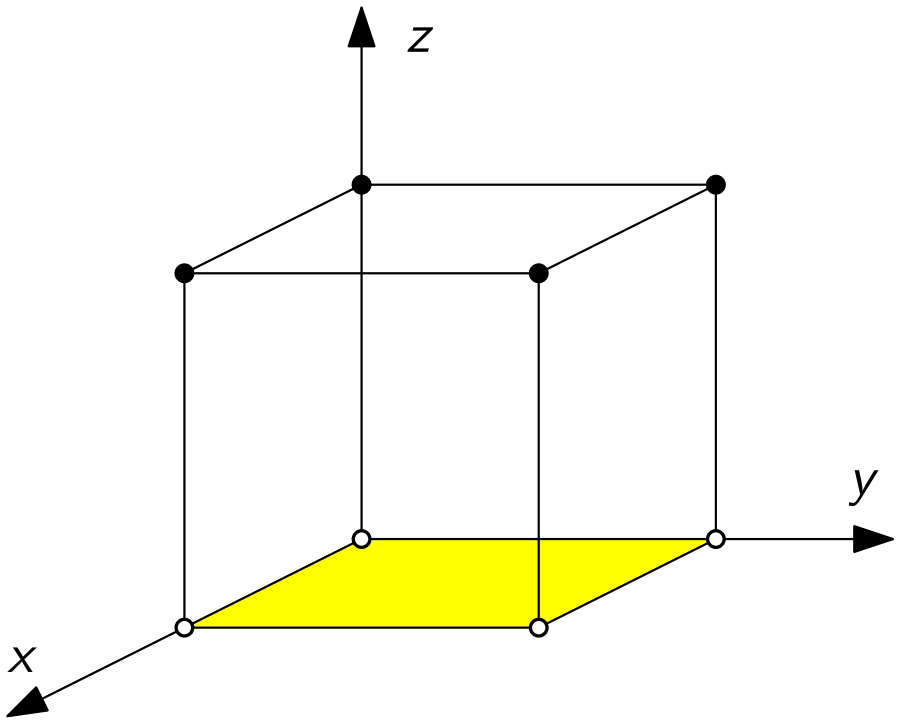
- $\mathbb{Z}_2^3$ において，原点 $(0,0,0)$ を通る平面は，$(a,b,c) \in \mathbb{Z}_2^3 - \{\mathbf{0}\}$ を使って
$$\{(x,y,z) \mid ax + by + cz = 0\}$$
と書ける
- 異なる (a,b,c) に対して，異なる平面が得られる



$$\{(x,y,z) \mid y = 0\}$$

射影平面：例 — $\mathbb{Z}_2^3$ における平面

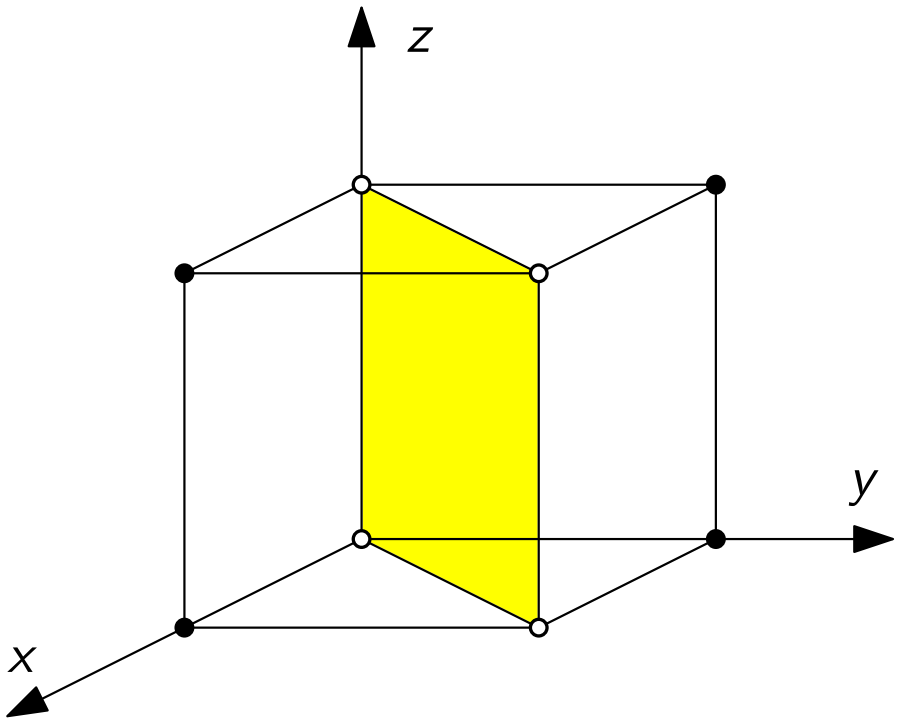
- $\mathbb{Z}_2^3$ において，原点 $(0,0,0)$ を通る平面は，$(a,b,c) \in \mathbb{Z}_2^3 - \{\mathbf{0}\}$ を使って
$$\{(x,y,z) \mid ax + by + cz = 0\}$$
と書ける
- 異なる (a,b,c) に対して，異なる平面が得られる



$$\{(x,y,z) \mid z = 0\}$$

射影平面：例 — $\mathbb{Z}_2^3$ における平面

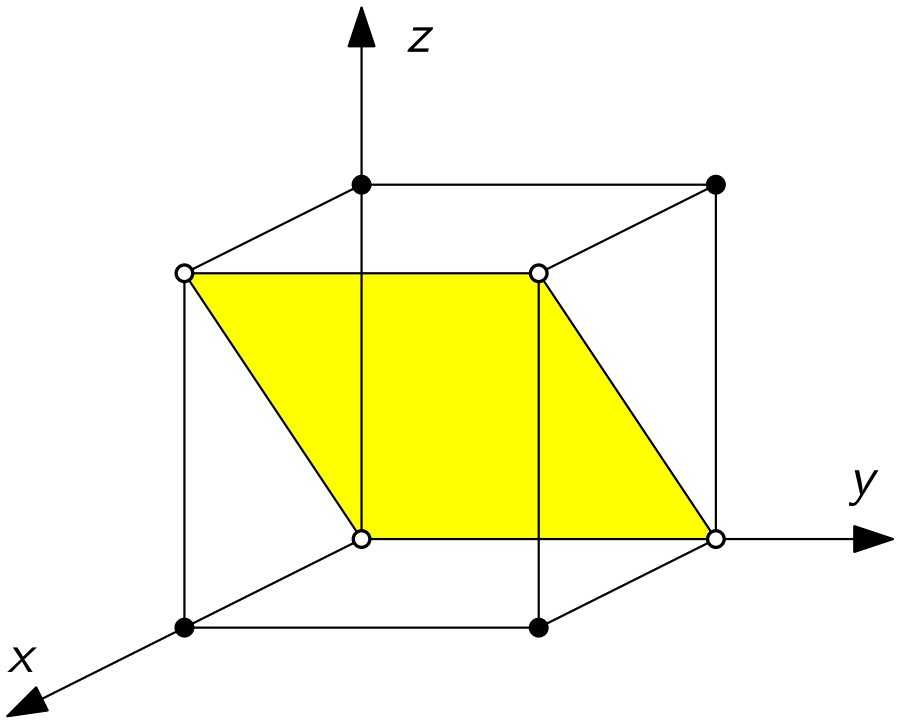
- $\mathbb{Z}_2^3$ において，原点 $(0,0,0)$ を通る平面は，$(a,b,c) \in \mathbb{Z}_2^3 - \{\mathbf{0}\}$ を使って
$$\{(x,y,z) \mid ax + by + cz = 0\}$$
と書ける
- 異なる (a,b,c) に対して，異なる平面が得られる



$$\{(x,y,z) \mid x + y = 0\}$$

射影平面：例 — $\mathbb{Z}_2^3$ における平面

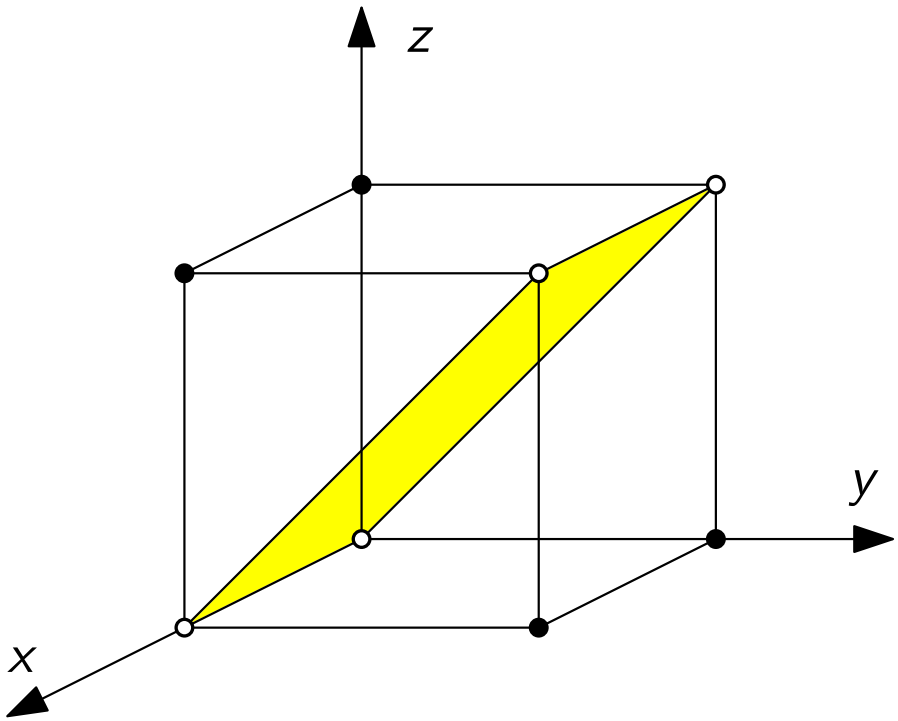
- $\mathbb{Z}_2^3$ において，原点 $(0,0,0)$ を通る平面は，$(a,b,c) \in \mathbb{Z}_2^3 - \{\mathbf{0}\}$ を使って
$$\{(x,y,z) \mid ax + by + cz = 0\}$$
と書ける
- 異なる (a,b,c) に対して，異なる平面が得られる



$$\{(x,y,z) \mid x + z = 0\}$$

射影平面：例 — $\mathbb{Z}_2^3$ における平面

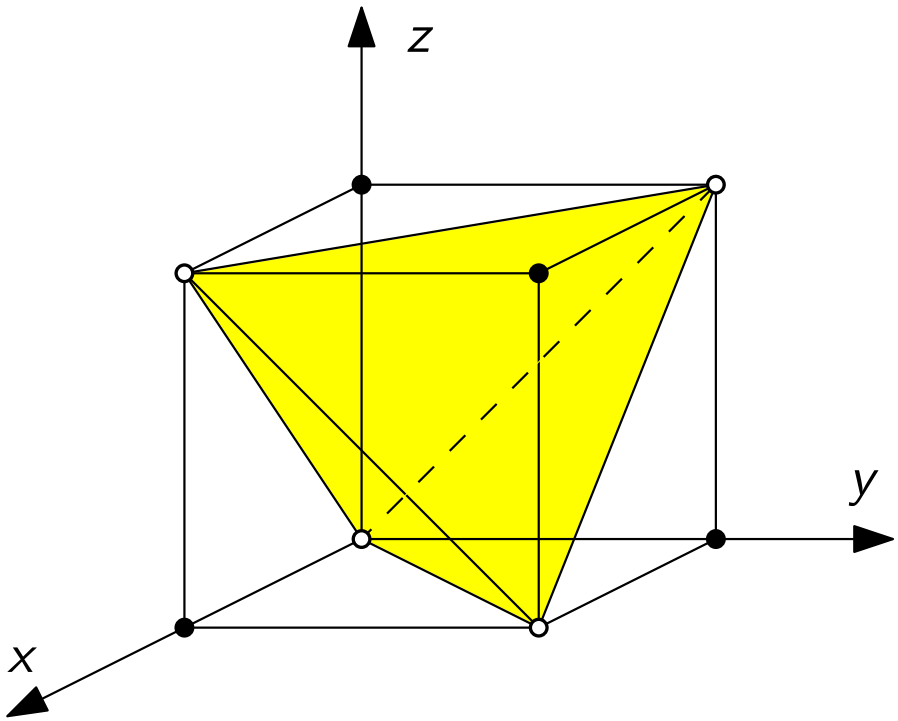
- $\mathbb{Z}_2^3$ において，原点 $(0,0,0)$ を通る平面は，$(a,b,c) \in \mathbb{Z}_2^3 - \{\mathbf{0}\}$ を使って
$$\{(x,y,z) \mid ax + by + cz = 0\}$$
と書ける
- 異なる (a,b,c) に対して，異なる平面が得られる



$$\{(x,y,z) \mid y + z = 0\}$$

射影平面：例 — $\mathbb{Z}_2^3$ における平面

- $\mathbb{Z}_2^3$ において，原点 $(0,0,0)$ を通る平面は，$(a,b,c) \in \mathbb{Z}_2^3 - \{\mathbf{0}\}$ を使って
$$\{(x,y,z) \mid ax + by + cz = 0\}$$
と書ける
- 異なる (a,b,c) に対して，異なる平面が得られる



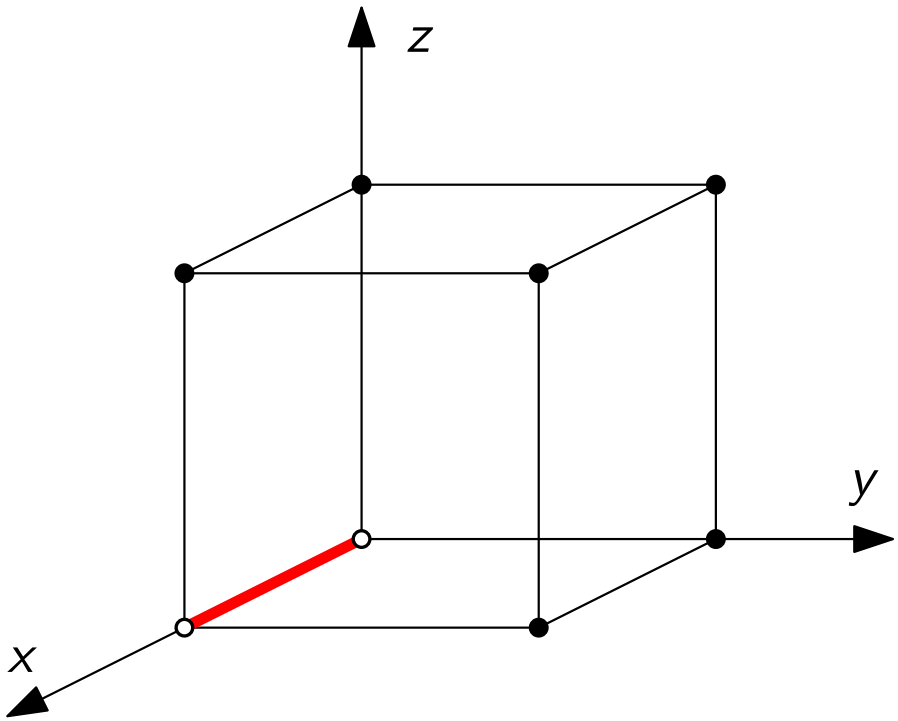
$$\{(x,y,z) \mid x + y + z = 0\}$$

射影平面：例 — $\mathbb{Z}_2^3$ における直線

- $\mathbb{Z}_2^3$ において，原点 $(0,0,0)$ を通る直線は，$(a,b,c) \in \mathbb{Z}_2^3 - \{\mathbf{0}\}$ を使って

$$\{(x,y,z) \mid \text{ある } k \in \mathbb{Z}_2 \text{ が存在して，} \ x = ka, y = kb, z = kc\}$$

と書ける
- 異なる (a,b,c) に対して，異なる直線が得られる



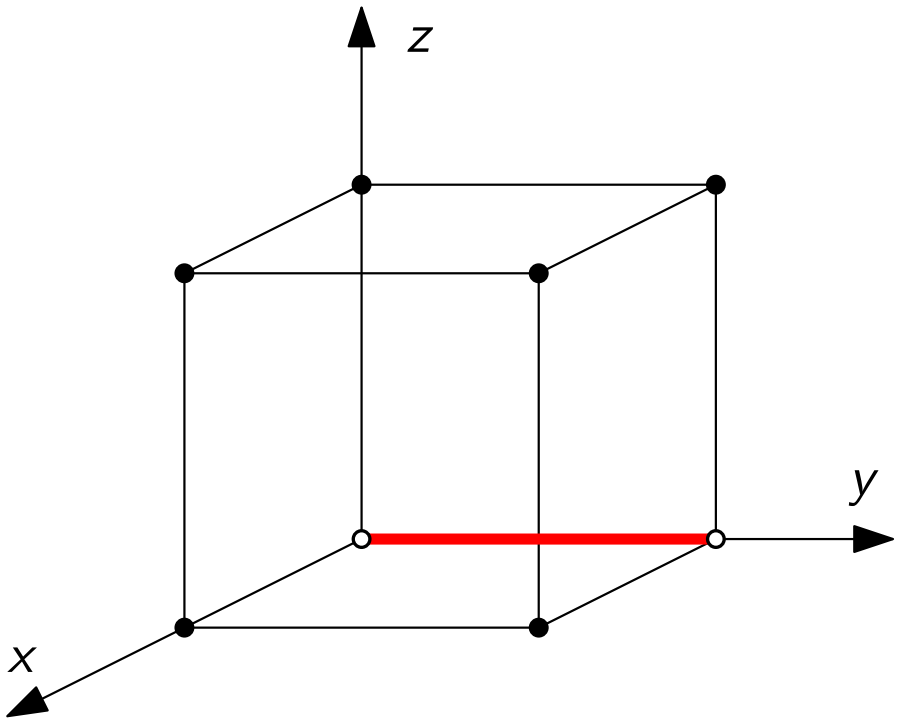
$$\{(k,0,0) \mid k \in \mathbb{Z}_2\}$$

射影平面：例 — $\mathbb{Z}_2^3$ における直線

- $\mathbb{Z}_2^3$ において，原点 $(0,0,0)$ を通る直線は，$(a,b,c) \in \mathbb{Z}_2^3 - \{\mathbf{0}\}$ を使って

$$\{(x,y,z) \mid \text{ある } k \in \mathbb{Z}_2 \text{ が存在して，} \ x = ka, y = kb, z = kc\}$$

と書ける
- 異なる (a,b,c) に対して，異なる直線が得られる



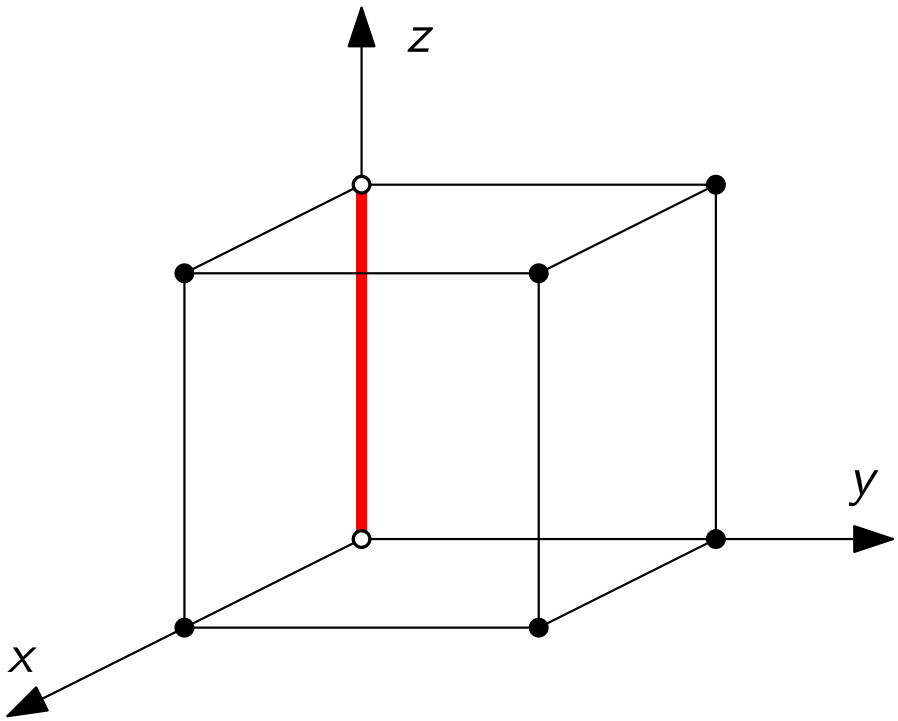
$\{(0,k,0) \mid k \in \mathbb{Z}_2\}$

射影平面：例 — $\mathbb{Z}_2^3$ における直線

- $\mathbb{Z}_2^3$ において，原点 $(0,0,0)$ を通る直線は，$(a,b,c) \in \mathbb{Z}_2^3 - \{\mathbf{0}\}$ を使って

$$\{(x,y,z) \mid \text{ある } k \in \mathbb{Z}_2 \text{ が存在して，} \ x = ka, y = kb, z = kc\}$$

と書ける
- 異なる (a,b,c) に対して，異なる直線が得られる



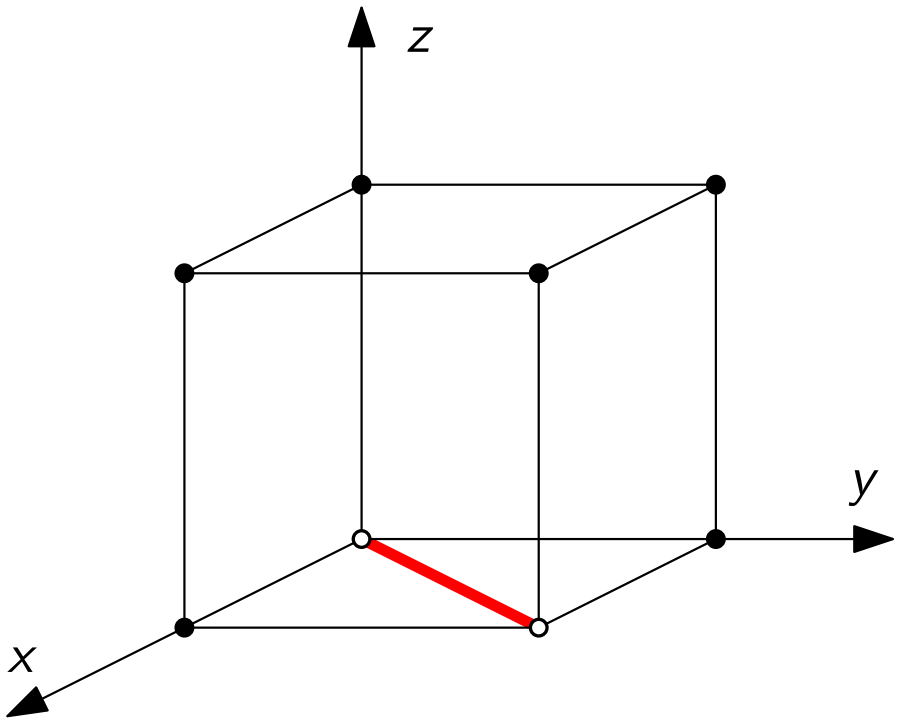
$$\{(0,0,k) \mid k \in \mathbb{Z}_2\}$$

射影平面：例 — $\mathbb{Z}_2^3$ における直線

- $\mathbb{Z}_2^3$ において，原点 $(0,0,0)$ を通る直線は，$(a,b,c) \in \mathbb{Z}_2^3 - \{\mathbf{0}\}$ を使って

$$\{(x,y,z) \mid \text{ある } k \in \mathbb{Z}_2 \text{ が存在して，} \ x = ka, y = kb, z = kc\}$$

と書ける
- 異なる (a,b,c) に対して，異なる直線が得られる



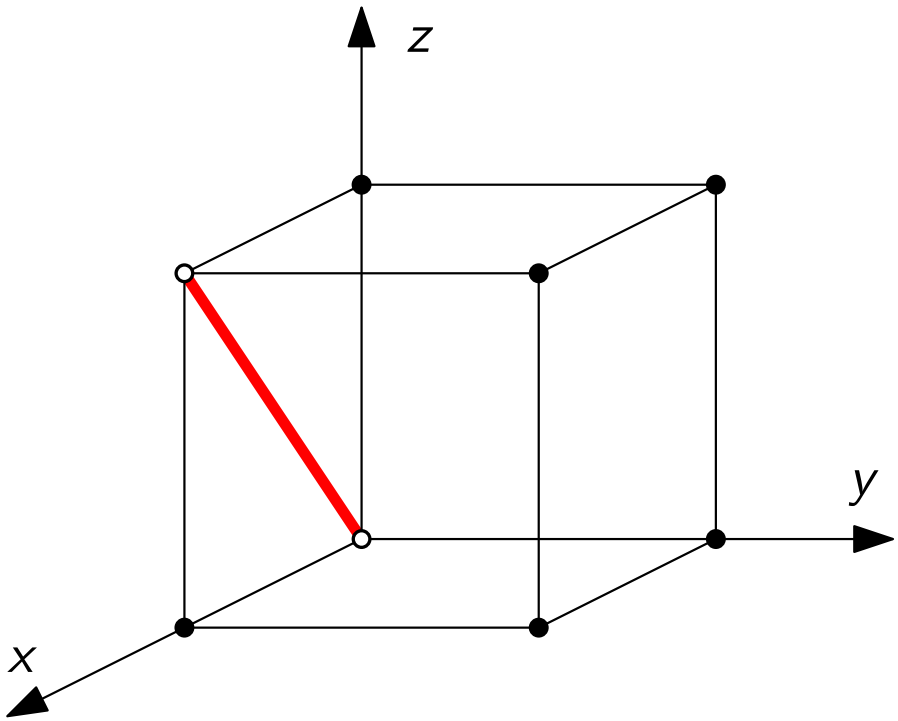
$$\{(k,k,0) \mid k \in \mathbb{Z}_2\}$$

射影平面：例 — $\mathbb{Z}_2^3$ における直線

- $\mathbb{Z}_2^3$ において，原点 $(0,0,0)$ を通る直線は，$(a,b,c) \in \mathbb{Z}_2^3 - \{\mathbf{0}\}$ を使って

$$\{(x,y,z) \mid \text{ある } k \in \mathbb{Z}_2 \text{ が存在して，} \ x = ka, y = kb, z = kc\}$$

と書ける
- 異なる (a,b,c) に対して，異なる直線が得られる



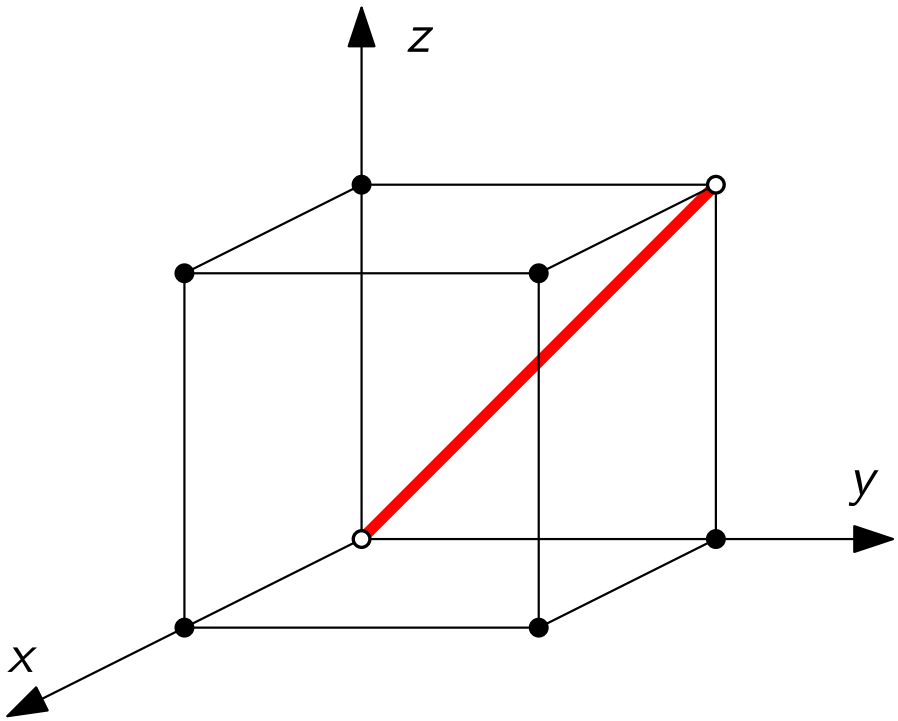
$$\{(k,0,k) \mid k \in \mathbb{Z}_2\}$$

射影平面：例 — $\mathbb{Z}_2^3$ における直線

- $\mathbb{Z}_2^3$ において，原点 $(0,0,0)$ を通る直線は，$(a,b,c) \in \mathbb{Z}_2^3 - \{\mathbf{0}\}$ を使って

$$\{(x,y,z) \mid \text{ある } k \in \mathbb{Z}_2 \text{ が存在して，} \ x = ka, y = kb, z = kc\}$$

と書ける
- 異なる (a,b,c) に対して，異なる直線が得られる



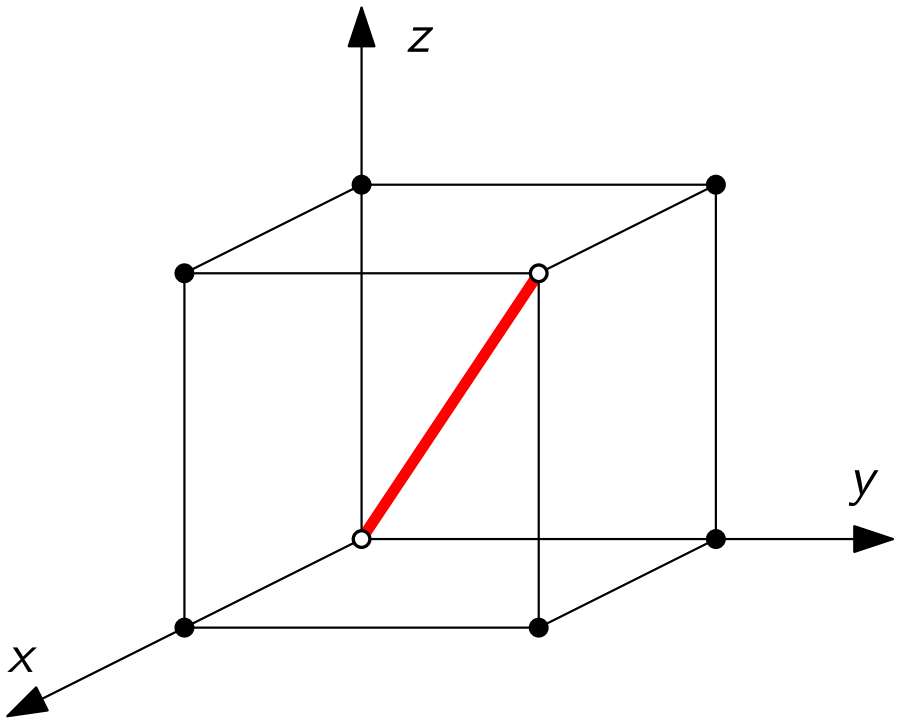
$$\{(0,k,k) \mid k \in \mathbb{Z}_2\}$$

射影平面：例 — $\mathbb{Z}_2^3$ における直線

- $\mathbb{Z}_2^3$ において，原点 $(0,0,0)$ を通る直線は，$(a,b,c) \in \mathbb{Z}_2^3 - \{\mathbf{0}\}$ を使って

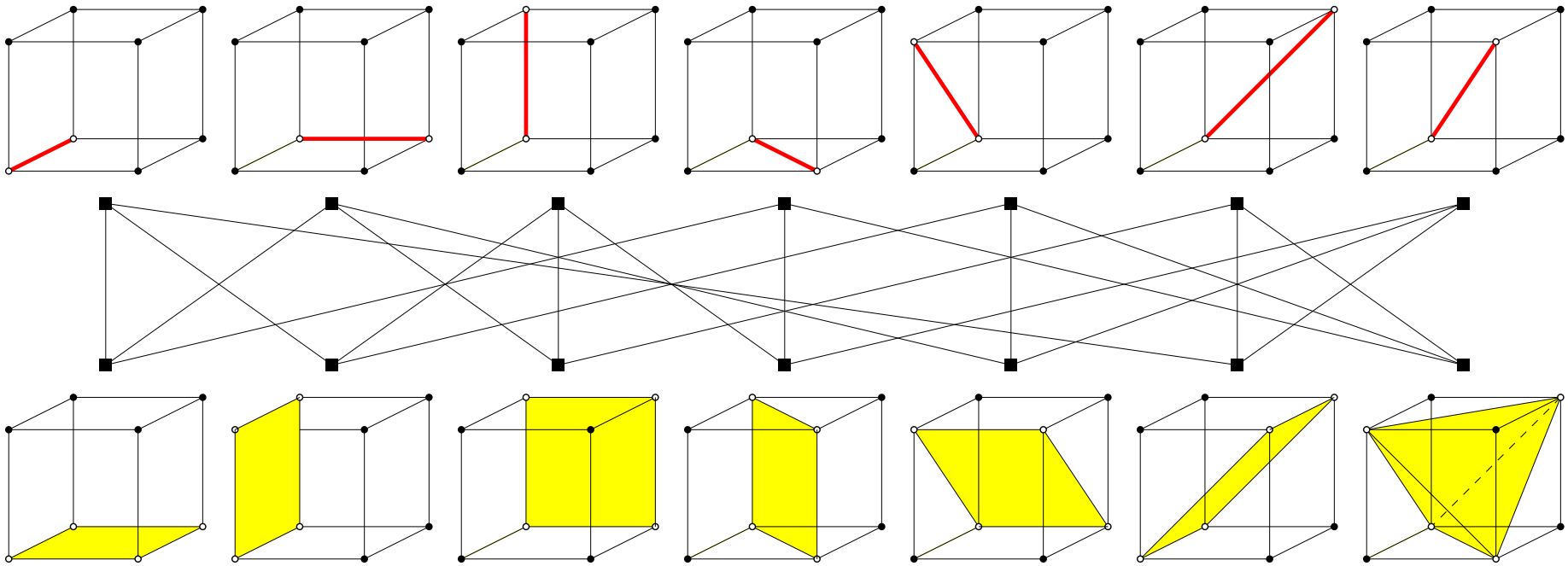
$$\{(x,y,z) \mid \text{ある } k \in \mathbb{Z}_2 \text{ が存在して，} \ x = ka, y = kb, z = kc\}$$

と書ける
- 異なる (a,b,c) に対して，異なる直線が得られる



$$\{(k,k,k) \mid k \in \mathbb{Z}_2\}$$

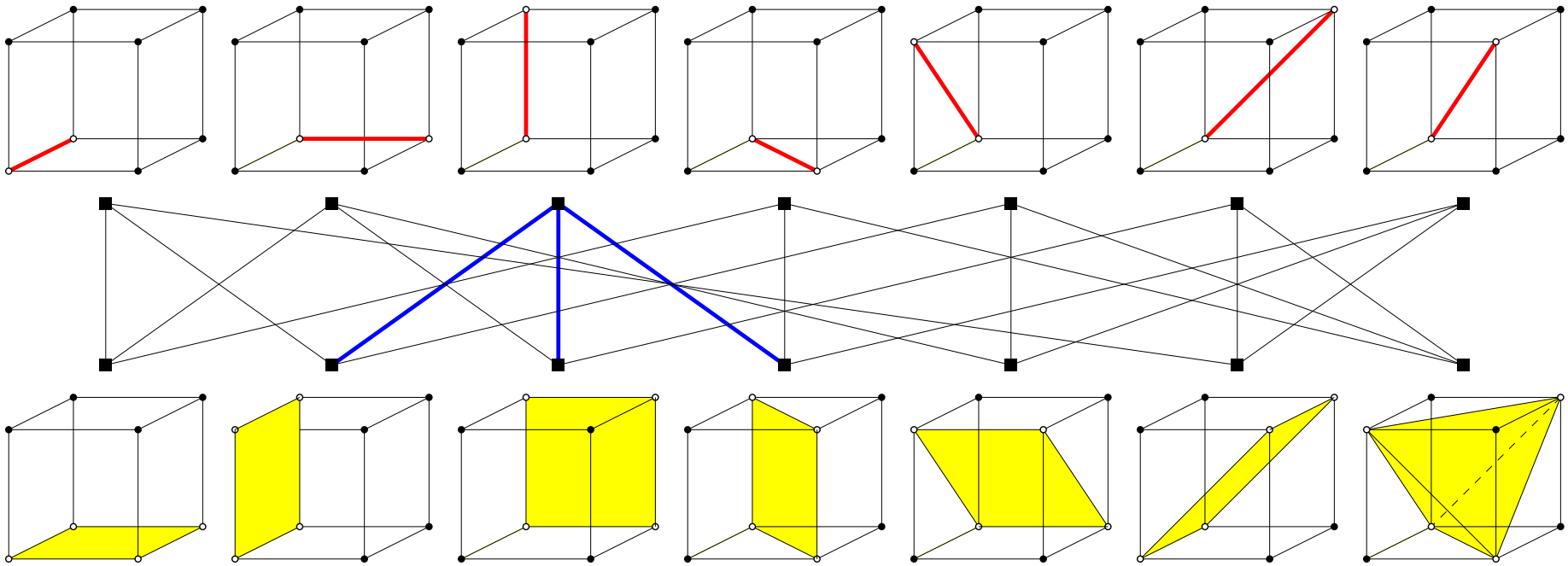
射影平面：例 — $\mathbb{Z}_2^3$ における直線と平面の接続関係



観察

- どの直線も 3 つの平面に含まれる
- どの平面も 3 つの直線を含む
- 2 つの平面に含まれる直線はちょうど 1 つ
- 2 つの直線を含む平面はちょうど 1 つ

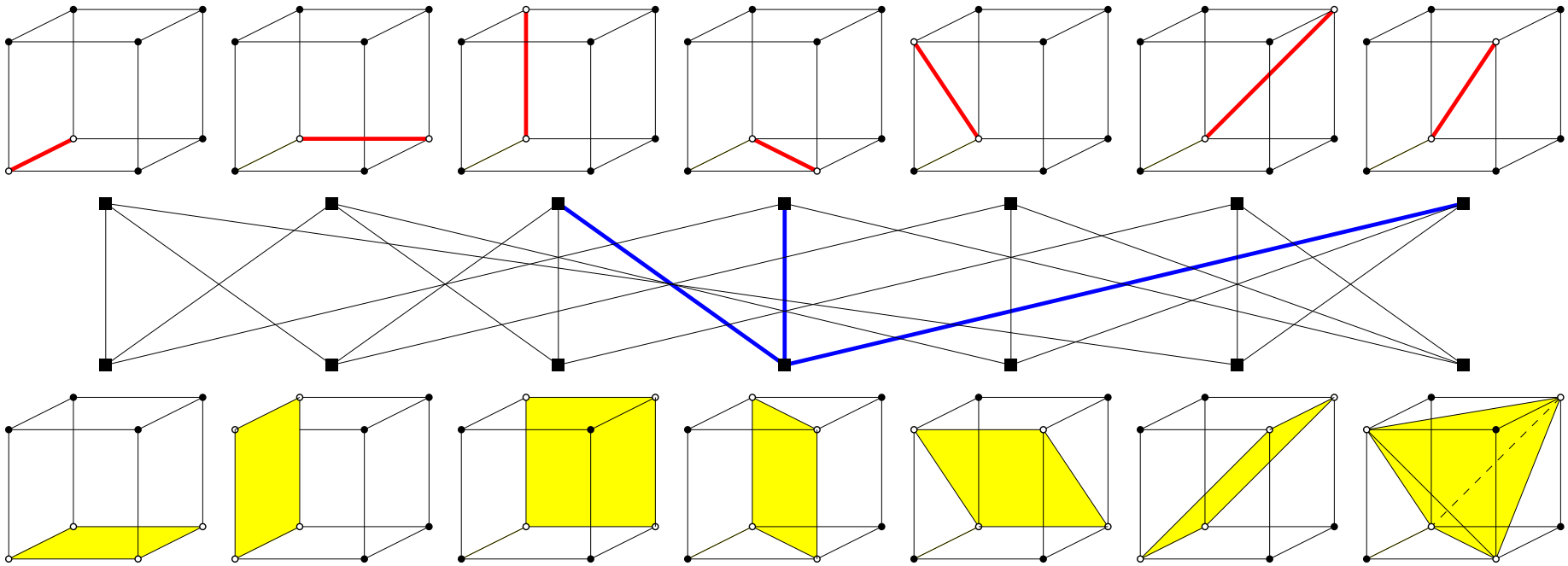
射影平面：例 — $\mathbb{Z}_2^3$ における直線と平面の接続関係



観察

- どの直線も 3 つの平面に含まれる
- どの平面も 3 つの直線を含む
- 2 つの平面に含まれる直線はちょうど 1 つ
- 2 つの直線を含む平面はちょうど 1 つ

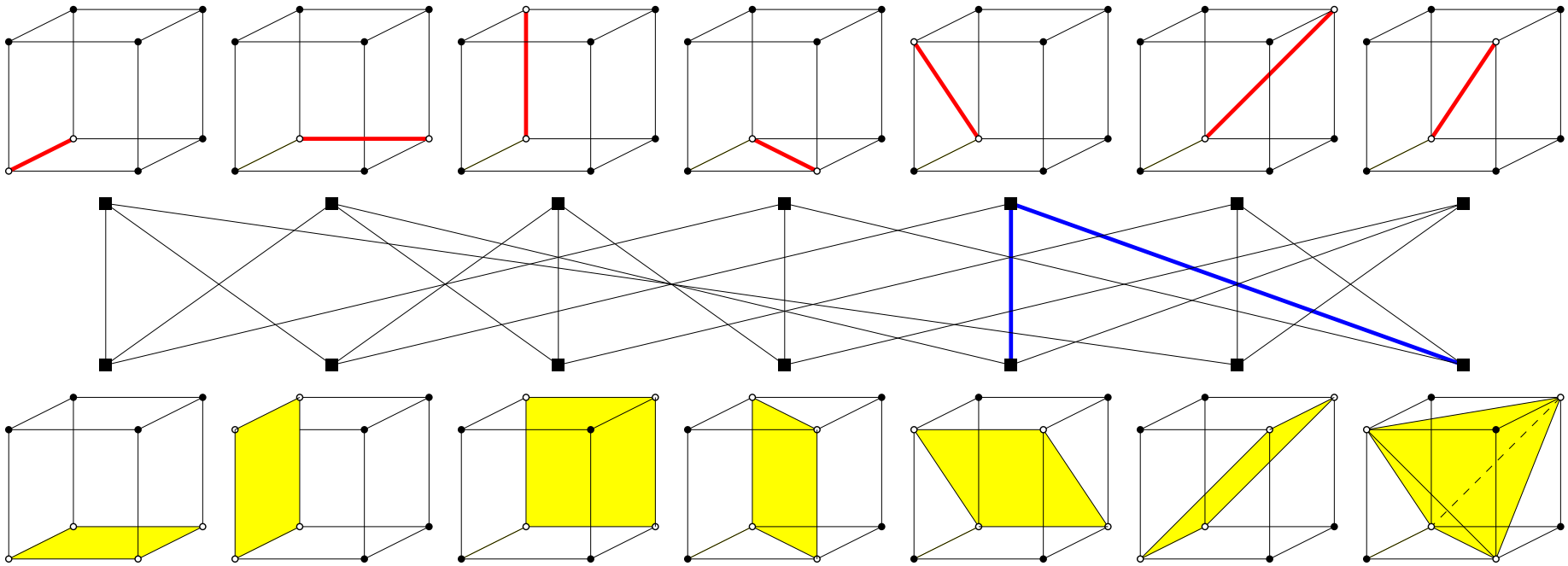
射影平面：例 — $\mathbb{Z}_2^3$ における直線と平面の接続関係



観察

- どの直線も 3 つの平面に含まれる
- どの平面も 3 つの直線を含む
- 2 つの平面に含まれる直線はちょうど 1 つ
- 2 つの直線を含む平面はちょうど 1 つ

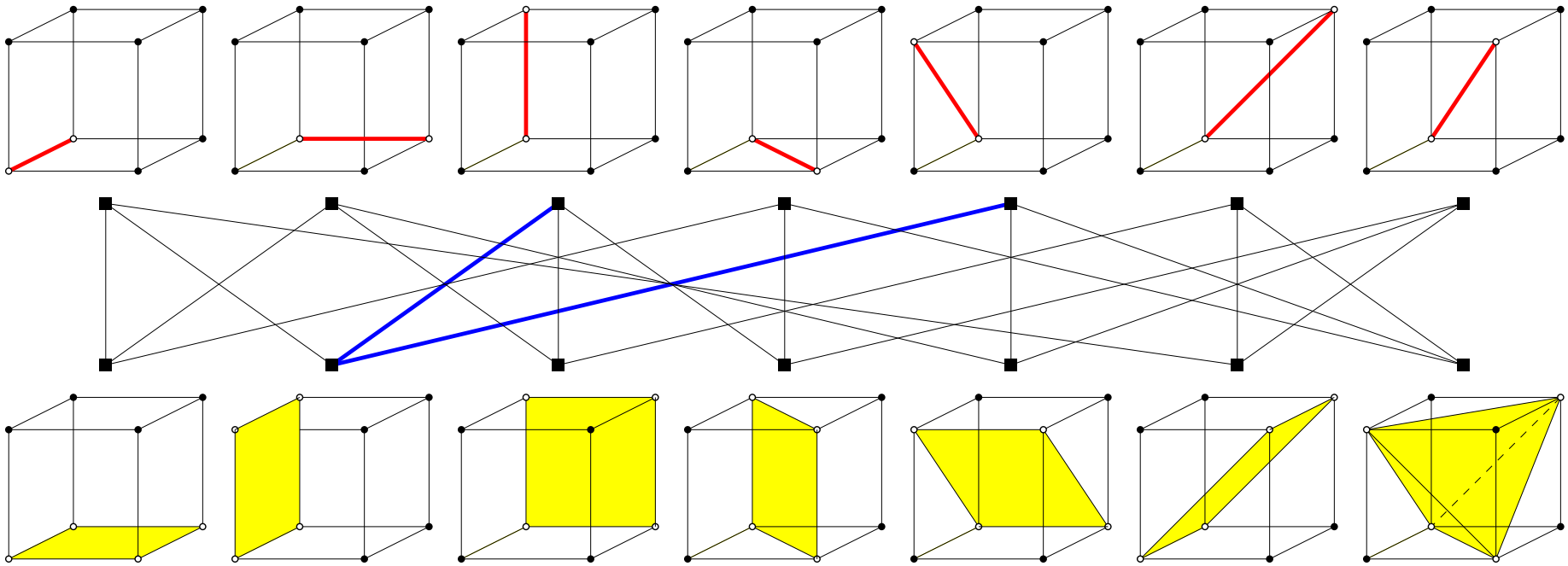
射影平面：例 — $\mathbb{Z}_2^3$ における直線と平面の接続関係



観察

- どの直線も 3 つの平面に含まれる
- どの平面も 3 つの直線を含む
- 2 つの平面に含まれる直線はちょうど 1 つ
- 2 つの直線を含む平面はちょうど 1 つ

射影平面：例 — $\mathbb{Z}_2^3$ における直線と平面の接続関係



観察

- どの直線も 3 つの平面に含まれる
- どの平面も 3 つの直線を含む
- 2 つの平面に含まれる直線はちょうど 1 つ
- 2 つの直線を含む平面はちょうど 1 つ

ワイン品評の問題との対応

ワイン品評	$\mathbb{Z}_2^3$ における対象
ワインの種類	原点を通る直線 ℓ
品評スタッフ	原点を通る平面 P
ワインを品評するスタッフ	ℓ を含む P
どのワインも 3 人が批評	どの平面も 3 つの直線を含む
どの 2 つのワインも あるスタッフが批評	どの 2 つの平面も ある直線を含む

目次

有限体：復習と記法

位数 q の有限体の構成

- q が素数べきのときのみ構成できる
  (つまり，素数 p，正整数 m を用いて，$q = p^m$ と書けるとき)
- $q = p$ のときは，$\mathbb{Z}_q$ を考えればよい
- $q = p^m$ のときは，$g(x) \in \mathbb{Z}_p[x]$ を次数 m の既約多項式として，
  $\mathbb{Z}_p[x]/(g(x))$ を考えればよい

位数 q の有限体は (本質的に) 唯一であることが知られているので，
それを $\mathbb{F}_q$ と書くことにする

- 要素 $a \in \mathbb{F}_q$ の乗算に関する逆元を a^{-1} と書くことにする
  (つまり，$\mathbb{F}_q$ において，$aa^{-1} = a^{-1}a = 1$)

$\mathbb{F}_q$ 上の射影平面：$\mathbb{F}_q^3$ における直線

- $\mathbb{F}_q^3$ において，原点 $(0,0,0)$ を通る直線は，
  $(a,b,c) \in \mathbb{F}_q^3 - \{\mathbf{0}\}$ を使って

$$\{(x,y,z) \mid \text{ある } k \in \mathbb{F}_q \text{ が存在して，} \quad x = ka, y = kb, z = kc\}$$

  と書ける (これを $L(a,b,c)$ とする)
- 異なる (a,b,c) に対して，異なる直線が得られるか？

$\mathbb{F}_q$ 上の射影平面：$\mathbb{F}_q^3$ における直線 (2)

例：$q = 3$ のとき ($\mathbb{F}_q = \mathbb{Z}_3$ と見なして考え)，$\mathbb{Z}_3$ において

$$\begin{aligned} L(2,1,1) &= \{(x,y,z) \mid \text{ある } k \in \mathbb{Z}_3 \text{ が存在して}, \quad x = 2k, y = k, z = k\} \\ &= \{(0,0,0),(2,1,1),(1,2,2)\} \\ &= \{(x,y,z) \mid \text{ある } k \in \mathbb{Z}_3 \text{ が存在して}, \quad x = k, y = 2k, z = 2k\} \end{aligned}$$

例：$q = 5$ のとき ($\mathbb{F}_q = \mathbb{Z}_5$ と見なして考え)，$\mathbb{Z}_5$ において

$$\begin{aligned} L(4,1,3) &= \{(x,y,z) \mid \text{ある } k \in \mathbb{Z}_5 \text{ が存在して}, \quad x = 4k, y = k, z = 3k\} \\ &= \{(0,0,0),(4,1,3),(3,2,1),(2,3,4),(1,4,2)\} \\ &= \{(x,y,z) \mid \text{ある } k \in \mathbb{Z}_5 \text{ が存在して}, \quad x = k, y = 4k, z = 2k\} \\ &= \{(x,y,z) \mid \text{ある } k \in \mathbb{Z}_5 \text{ が存在して}, \quad x = 2k, y = 3k, z = 4k\} \\ &= \{(x,y,z) \mid \text{ある } k \in \mathbb{Z}_5 \text{ が存在して}, \quad x = 3k, y = 2k, z = 1k\} \end{aligned}$$

つまり，同じ直線がちょうど $q - 1$ 個だけ現れる

$\mathbb{F}_q$ 上の射影平面：$\mathbb{F}_q^3$ における直線の数

$\mathbb{F}_q^3$ における原点を通る直線の数は？

$\dfrac{q^3-1}{q-1}$ (すなわち，q^2+q+1)

例

- $q=2: q^2+q+1=7$
- $q=3: q^2+q+1=13$
- $q=4: q^2+q+1=21$
- $q=5: q^2+q+1=31$

$\mathbb{F}_q$ 上の射影平面：$\mathbb{F}_q^3$ における直線の数 (補題)

まず，次の補題を証明する

補題 P

任意の $(a,b,c) \in \mathbb{F}_q^3 - \{\mathbf{0}\}$ に対して

$$|\{(a',b',c') \in \mathbb{F}_q^3 - \{\mathbf{0}\} \mid L(a,b,c) = L(a',b',c')\}| = q-1$$

補題 P の証明：左辺の集合を A とする

- 定義より，任意の $k \in \mathbb{F}_q - \{0\}$ に対して，$L(a,b,c) = L(ka,kb,kc)$
- したがって，$|A| \geq |\mathbb{F}_q - \{0\}| = q-1$
- 一方，$L(a,b,c) = L(a',b',c')$ ならば，ある $k,k' \in \mathbb{F}_q - \{0\}$ に対して

$$ka = k'a', \quad kb = k'b', \quad kc = k'c'$$

- したがって，$a = k^{-1}k'a', b = k^{-1}k'b', c = k^{-1}k'c'$
- ここで，$k^{-1}k' \in \mathbb{F}_q - \{0\}$ に注意
- $\therefore |A| \leq |\mathbb{F}_q - \{0\}| = q-1$ □

$\mathbb{F}_q$ 上の射影平面：$\mathbb{F}_q^3$ における直線 (証明)

$\mathbb{F}_q^3$ における原点を通る直線の数は？

$\dfrac{q^3-1}{q-1}$ (すなわち，q^2+q+1)

証明：$\mathbb{F}_q^3 - \{\mathbf{0}\}$ 上の同値関係 $\sim$ を以下のように定義

- $(a,b,c) \sim (a',b',c') \Leftrightarrow L(a,b,c) = L(a',b',c')$
- これは確かに同値関係である　(簡単な演習問題)
- 補題 P より，この同値関係による同値類の要素数 $= q-1$
- したがって，異なる直線の数は $|\mathbb{F}_q^3/\!\sim| = (q^3-1)/(q-1)$ □

$\mathbb{F}_q$ 上の射影平面：$\mathbb{F}_q^3$ における平面

- $\mathbb{F}_q^3$ において，原点 $(0,0,0)$ を通る平面は，
  $(a,b,c) \in \mathbb{F}_q^3 - \{\mathbf{0}\}$ を使って

$$\{(x,y,z) \mid ax + by + cz = 0\}$$

  と書ける (これを $P(a,b,c)$ をする)
- 異なる (a,b,c) に対して，異なる平面が得られるか？

$\mathbb{F}_q$ 上の射影平面：$\mathbb{F}_q^3$ における平面 (2)

例：$q = 3$ のとき ($\mathbb{F}_q = \mathbb{Z}_3$ と見なして考え)，$\mathbb{Z}_3$ において

$$\begin{aligned} 2x + y + z = 0 &\Leftrightarrow 2 \cdot (2x + y + z) = 2 \cdot 0 \\ &\Leftrightarrow x + 2y + 2z = 0 \end{aligned}$$

例：$q = 5$ のとき ($\mathbb{F}_q = \mathbb{Z}_5$ と見なして考え)，$\mathbb{Z}_5$ において

$$\begin{aligned} 4x + y + 3z = 0 &\Leftrightarrow 2 \cdot (4x + y + 3z) = 2 \cdot 0 \Leftrightarrow 3x + 2y + z = 0 \\ &\Leftrightarrow 3 \cdot (4x + y + 3z) = 3 \cdot 0 \Leftrightarrow 2x + 3y + 4z = 0 \\ &\Leftrightarrow 4 \cdot (4x + y + 3z) = 4 \cdot 0 \Leftrightarrow x + 4y + 2z = 0 \end{aligned}$$

つまり，同じ平面がちょうど $q - 1$ 個だけ現れる

$\mathbb{F}_q$ 上の射影平面：$\mathbb{F}_q^3$ における平面の数

$\mathbb{F}_q^3$ における原点を通る平面の数は？

$\dfrac{q^3-1}{q-1}$ (すなわち，q^2+q+1)

例

- $q=2: q^2+q+1=7$
- $q=3: q^2+q+1=13$
- $q=4: q^2+q+1=21$
- $q=5: q^2+q+1=31$

$\mathbb{F}_q$ 上の射影平面：$\mathbb{F}_q^3$ における平面の数 (補題 1)

まず，次の補題を証明する

補題 L1

任意の $(a, b, c) \in \mathbb{F}_q^3 - \{\mathbf{0}\}$ に対して

$$|\{(x, y, z) \mid ax + by + cz = 0\} - \{\mathbf{0}\}| = q^2 - 1$$

補題 L1 の証明：左辺の集合を B とする

- $(a, b, c) \neq \mathbf{0}$ より，a, b, c のどれかは非ゼロ
- $a \neq 0$ の場合を考える (他の場合も同様)
- このとき，$x = -a^{-1}by - a^{-1}cz$
- $\therefore$ 任意の $(y, z) \in \mathbb{F}_q^2$ に対して $ax + by + cz = 0$ を満たす $x \in \mathbb{F}_q$ が一意に定まる
- したがって，$|B| = |\mathbb{F}_q^2 - \{\mathbf{0}\}| = q^2 - 1$ □

$\mathbb{F}_q$ 上の射影平面：$\mathbb{F}_q^3$ における平面の数 (補題 2)

補題 L2

任意の $(a,b,c),(a',b',c') \in \mathbb{F}_q^3 - \{\mathbf{0}\}$ に対して，

$$L(a',b',c') \subseteq P(a,b,c) \quad \Leftrightarrow \quad (a',b',c') \in P(a,b,c)$$

証明：演習問題

$\mathbb{F}_q$ 上の射影平面：$\mathbb{F}_q^3$ における平面の数 (補題 3)

原点を通る平面は，原点を通る直線を $q+1$ 個含む

補題 L3

任意の $(a,b,c) \in \mathbb{F}_q^3 - \{\mathbf{0}\}$ に対して

$$|\{L(a',b',c') \mid (a',b',c') \in \mathbb{F}_q^3 - \{\mathbf{0}\}, L(a',b',c') \subseteq P(a,b,c)\}| = q+1$$

補題 L3 の証明：補題 L2 より，$L(a',b',c') \subseteq P(a,b,c)$ と $(a',b',c') \in P(a,b,c)$ は同値

- $P(a,b,c) - \{\mathbf{0}\}$ 上の同値関係 $\sim$ を以下のように定義

$$(a',b',c') \sim (a'',b'',c'') \Leftrightarrow L(a',b',c') = L(a'',b'',c'')$$

- これは確かに同値関係である (前と同様)
- 補題 P より，この同値関係による同値類の要素数 $= q-1$
- したがって，補題 L1 より，異なる直線の数は

$$|(P(a,b,c) - \{\mathbf{0}\})/\sim| = (q^2-1)/(q-1) = q+1 \qquad \square$$

$\mathbb{F}_q$ 上の射影平面：$\mathbb{F}_q^3$ における平面の数 (補題 4)

原点を通る直線は，原点を通る $q+1$ 個の平面に含まれる

補題 L4

任意の $(a', b', c') \in \mathbb{F}_q^3 - \{\mathbf{0}\}$ に対して

$$|\{P(a,b,c) \mid (a,b,c) \in \mathbb{F}_q^3 - \{\mathbf{0}\}, L(a',b',c') \subseteq P(a,b,c)\}| = q+1$$

補題 L4 の証明：任意の (a', b', c') を考える

- 原点を通る直線で $L(a', b', c')$ と異なるものの数 $= q^2 + q$
- 補題 L3 より，原点を通り $L(a', b', c')$ を含む平面は $L(a', b', c')$ の他に q 個の直線を含む
- そのような 2 つの平面の共通部分は $L(a', b', c')$
- $\therefore$ $L(a', b', c')$ を含む平面の数 $= (q^2 + q)/q = q + 1$ □

$\mathbb{F}_q$ 上の射影平面：$\mathbb{F}_q^3$ における平面の数

$\mathbb{F}_q^3$ における原点を通る平面の数は？

$\dfrac{q^3-1}{q-1}$ (すなわち，q^2+q+1)

証明：原点を通る異なる平面の数を m として，次を計算する

$$M = \left| \left\{ (P(a,b,c), L(a',b',c')) \;\middle|\; \begin{array}{l} (a,b,c),(a',b',c') \in \mathbb{F}_q^3 - \{\mathbf{0}\}, \\ L(a',b',c') \subseteq P(a,b,c) \end{array} \right\} \right|$$

つまり，M は包含関係を持つ平面と直線の 2 個組の総数

- 補題 L3 より，$M = m \cdot (q+1)$
- 補題 L4 より，$M = (q^2+q+1) \cdot (q+1)$
- したがって，$m = q^2+q+1$ □

$\mathbb{F}_q$ 上の射影平面：まとめ

$\mathbb{F}_q^3$ において

- 原点を通る直線の数 $= q^2 + q + 1$
- 原点を通る平面の数 $= q^2 + q + 1$
- 原点を通る 1 直線を含む，原点を通る平面の数 $= q + 1$
- 原点を通る 1 平面が含む，原点を通る直線の数 $= q + 1$
- 原点を通る 2 平面が含む，原点を通る直線の数 $= 1$

ここで作った直線と平面の集合を $\mathbb{F}_q$ 上の射影平面と呼ぶ

考えたい問題の種類：変種

q^2+q+1 種類のワインを q^2+q+1 人のスタッフで品評したい

公平にするため，次を満たすようにしたい

- どのワインも，$q+1$ 人のスタッフが品評する
- どの 2 つのワインも，あるスタッフが同時に品評する

問題

このような品評の仕方は可能か？

解：$\mathbb{F}_q$ 上の射影平面を考えればよい

目次

有限射影平面：定義

有限射影平面は，有限個の「点」と「直線」の集合として定義される

有限射影平面とは？

正整数 q に対して，位数 q の射影平面とは，次のような 2 個組 $(X, \mathcal{L})$

- X は有限集合で，$|X| = q^2 + q + 1$
- $\mathcal{L} \subseteq 2^X$ は X の部分集合の集合で次を満たす
  1. 任意の $\ell \in \mathcal{L}$ に対して，$|\ell| = q + 1$
  2. 任意の異なる $x, y \in X$ に対して，
     $x, y \in \ell$ となる $\ell \in \mathcal{L}$ がただ 1 つ存在する

有限射影平面：いままでの議論の帰結

有限射影平面は，有限個の「点」と「直線」の集合として定義される

有限射影平面とは？

正整数 q に対して，位数 q の射影平面とは，次のような 2 個組 $(X, \mathcal{L})$

- X は有限集合で，$|X| = q^2 + q + 1$
- $\mathcal{L} \subseteq 2^X$ は X の部分集合の集合で次を満たす
  1. 任意の $\ell \in \mathcal{L}$ に対して，$|\ell| = q + 1$
  2. 任意の異なる $x, y \in X$ に対して，
     $x, y \in \ell$ となる $\ell \in \mathcal{L}$ がただ 1 つ存在する

いままでの議論の帰結

q が素数べきのとき，位数 q の射影平面は存在する

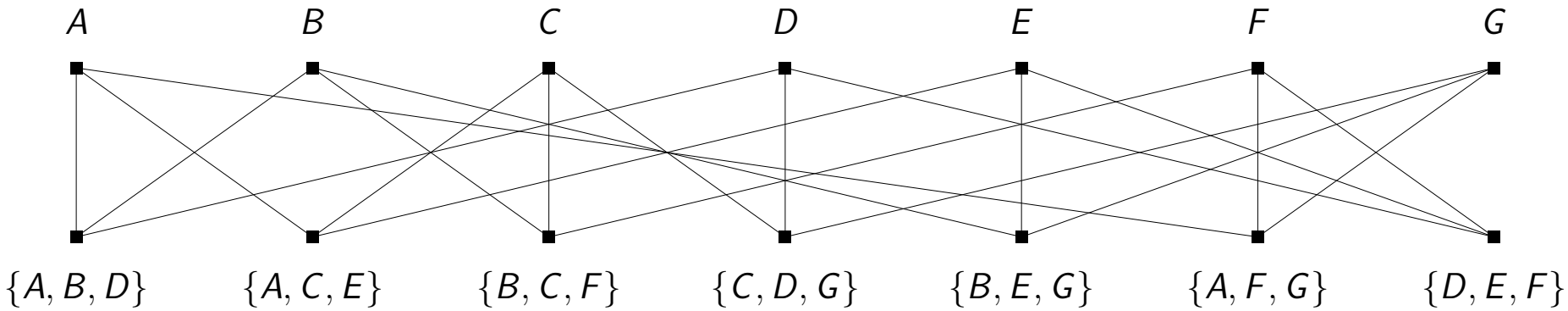
証明：X を $\mathbb{F}_q^3$ において原点を通る直線の集合として，
$\mathcal{L}$ を $\mathbb{F}_q^3$ において原点を通る平面が含む直線の集合の集合とすればよい

□

有限射影平面：いままでの議論の帰結 (例)

$q = 2$ のとき：X と $\mathcal{L}$ を次のように置く

$$
\begin{aligned}
X &= \{A, B, C, D, E, F, G\} \\
\mathcal{L} &= \{\{A, B, D\}, \{A, C, E\}, \{B, C, F\}, \{C, D, G\}, \\
&\quad \{B, E, G\}, \{A, F, G\}, \{D, E, F\}\}
\end{aligned}
$$

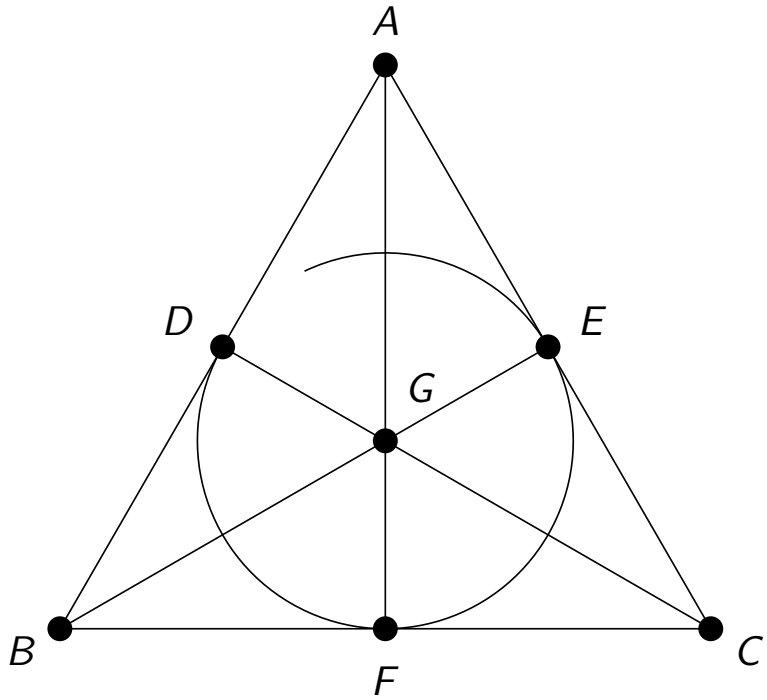


位数 2 の射影平面はファノ平面と呼ばれることが多い

有限射影平面：いままでの議論の帰結 (例：別の表現)

$q = 2$ のとき：X と $\mathcal{L}$ を次のように置く

$$
\begin{aligned}
X &= \{A, B, C, D, E, F, G\} \\
\mathcal{L} &= \{\{A, B, D\}, \{A, C, E\}, \{B, C, F\}, \{C, D, G\}, \\
&\quad \{B, E, G\}, \{A, F, G\}, \{D, E, F\}\}
\end{aligned}
$$



位数 2 の射影平面はファノ平面と呼ばれることが多い

有限射影平面：知られていること

- 位数 q の有限射影平面が存在 $\Rightarrow$「ワイン品評の問題」に解がある
- q が素数べきのとき，位数 q の有限射影平面は存在する
- $q = 6$ のとき，位数 q の有限射影平面は存在しない
  - 注：これは位数 6 の有限体が存在しないこととは別のはなし
- $q = 9$ のとき，先の構成法によらない有限射影平面が (3 つ) 存在する
- $q = 10$ のとき，位数 q の有限射影平面は存在しない
  - 注：これも位数 10 の有限体が存在しないこととは別のはなし

未解決問題

位数が素数べきでない有限射影平面は存在するか？

「存在しない」と予想されている

目次

今日のまとめ

今日のまとめ

- 有限体を用いて射影平面を構成する
- 射影平面を用いて組合せデザインの問題を解く

今日の内容に関するキーワード

有限幾何，組合せデザイン，デザイン理論

これらはどれも大きな分野

残った時間の使い方

- 演習問題をやる
  - 相談推奨 (ひとりでやらない)
- 質問をする
  - 教員と TA は巡回
- 退室時，小さな紙に感想など書いて提出する ← 重要
  - 内容は何でも OK
  - 匿名で OK

目次