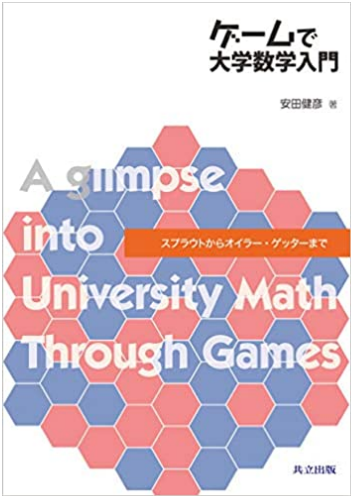
応用数学特論 II (集中講義)

Day 3 Finite Geometries & Finite Fields

盧 暁南 (山梨大学)
Xiao-Nan LU (University of Yamanashi)

Aug. 27, 2021
Kobe University

Two interesting books

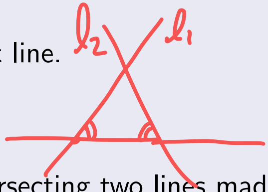


Outline

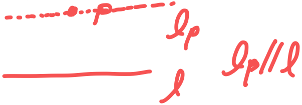
Euclidean geometry

Axiom (公理) of Euclidean geometry

1. Any two points can be connected by a straight line.
2. A line segment can be extended continuously to a straight line.
3. A circle can be produced with given center and radius.
4. All right angles are equal to one another.
5. (The parallel postulate; 平行線公準) If a straight line intersecting two lines made two interior angles on the same side less than two right angles, then the two lines will intersect on that side.



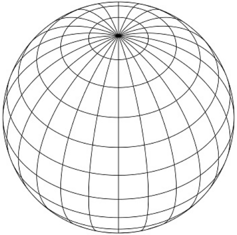
- The parallel postulate $\iff$ Given a line ℓ and a point P not lying on ℓ, there exists a unique line passing through P that is parallel to ℓ.
- The parallel postulate is independent of the first four!



Non-Euclidean geometry

- (Traditional) non-Euclidean geometries by relaxing the parallel postulate:
  - hyperbolic geometry (双曲幾何学) ($\exists$ infinite many parallel lines)
  - elliptic geometry (楕円幾何学) ($\nexists$ parallel line with Axiom 2 eliminated)

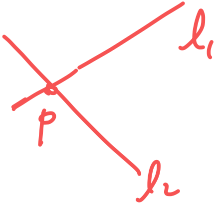
Parallel lines intersect at ∞



Lines of longitude intersects at poles

Incidence structure

$\ell_1 \not\parallel \ell_2$



$(P,\ell_1) \in \mathcal{I}$, $(P,\ell_2) \in \mathcal{I}$

- $\mathcal{P}$: set of points
- $\mathcal{L}$: set of lines
- $\mathcal{I} \subseteq \mathcal{P} \times \mathcal{L}$: incidence relation (結合関係)
- $(P, \ell) \in \mathcal{I}$ means $P \in \mathcal{P}$ is incident with $\ell \in \mathcal{L}$ (P lying on ℓ)
- $(\mathcal{P}, \mathcal{L}, \mathcal{I})$ is an incidence structure (結合構造)
- Two distinct $\ell_1, \ell_2 \in \mathcal{L}$ are parallel iff they have no point incident with both of them.

Today, we consider geometries when $|\mathcal{P}|$ (also $|\mathcal{L}|$) is a finite set.

Affine plane

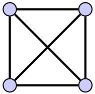
Affine plane

An affine plane (アフィン平面) is an incidence structure $(\mathcal{P}, \mathcal{L}, \mathcal{I})$ such that

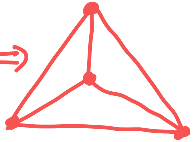
1. For any two points $p_1, p_2 \in \mathcal{P}$, there exists a unique line $\ell \in \mathcal{L}$ passing through both p_1 and p_2, i.e. $(p_1, \ell), (p_2, \ell) \in \mathcal{I}$.
2. If $p \in \mathcal{P}$ is not lying on $\ell \in \mathcal{L}$, i.e. $(p, \ell) \notin \mathcal{I}$, then there exists a unique line ℓ_P passing through P, i.e. $(P, \ell_P) \in \mathcal{I}$, and ℓ_P parallel to ℓ. $\ell /\!/ \ell$
3. There exists at least three non-collinear points.

Trivial geometry

(not an affine plane)



$\Leftrightarrow$



An affine plane

Basic propositions of an affine plane (1/4)

Proposition A

Any two lines intersect at either one point or do not intersect.

背理法

Proof: Assume two lines intersect at ≥ 2 points. A contradiction to Axiom 1.

Proposition B

Parallelism is an equivalence relation on the lines of an affine plane.

- $\ell // \ell$ (Reflexivity; 反射律)
- If $\ell_1 // \ell_2$ then $\ell_2 // \ell_1$ (Symmetry; 対称律)
- If $\ell_1 // \ell_2$ and $\ell_2 // \ell_3$ then $\ell_1 // \ell_3$ (Transitivity; 推移律)

Proof: The first two are trivial by the definition of parallelism.
For the third, assume ℓ_1 intersects ℓ_3 at P. By Axiom 2, ℓ_1 should be identical with ℓ_3, as the unique parallel line of ℓ_2 passing through P.

$\ell_1 = \ell_3$

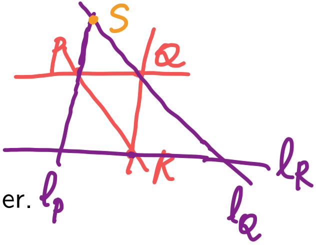
Basic propositions of an affine plane (2/4)

Proposition C

There are four points such that any three of them are not lying on a same line.

Proof: By Axiom 3, let P, Q, R be three non-collinear points. Let

- ℓ_P: the unique line passing P that is $//\overline{QR}$
- ℓ_Q: the unique line passing Q that is $//\overline{PR}$
- ℓ_R: the unique line passing R that is $//\overline{PQ}$



By transitivity of parallelism, ℓ_P, ℓ_Q, ℓ_R are not parallel to each other. Suppose ℓ_P and ℓ_Q intersect at S.

Quiz

Complete the above proof by showing that P, Q, R, S are the desired four points.

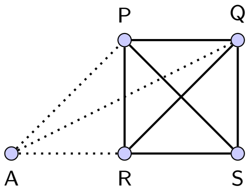
Basic propositions of an affine plane (3/4)

Proposition D

Any point is incident with at least two lines.

Proof: Use the previously defined points P, Q, R, S.

- For $A \in \{P, Q, R, S\}$, done.
- $\overline{AP}$, $\overline{AQ}$, $\overline{AR}$ cannot coincide; otherwise, P, Q, R were collinear. done.

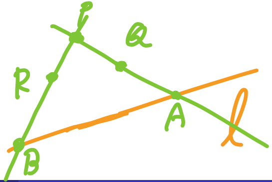


Basic propositions of an affine plane (4/4)

Proposition E

Each line contains at least two points.

Proof: Suppose ℓ contains at most one of the previously defined P, Q, R, S (w.l.o.g., suppose P, Q, R are not on ℓ). Then, at most one of $\overline{PQ}$, $\overline{PR}$, $\overline{QR}$ is parallel to ℓ.
Suppose $\overline{PQ}$, $\overline{PR}$ intersects ℓ at A, B, respectively.
If $A = B$, then $\overline{PQA} = \overline{PRB}$ by Axiom 1. However, $\overline{PQ} \neq \overline{PR}$. A contradiction.
This means ℓ contains at least two different points A and B.



The number of points and lines

Proposition F

In an affine plane, all the lines contain the same number of points.

- The order of the affine plane: # of points on a line

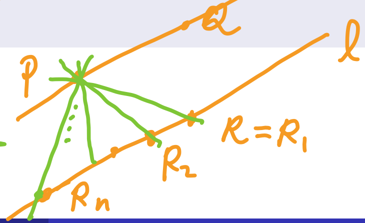
Proposition G

In an affine plane of order n,

There are exactly $n+1$ lines passing through a given point.

$\ell \mathbin{/\!/} \overline{PQ}$

$(n+1)$本 $\leftarrow \overline{PQ} + n$本 $\leftarrow$



The number of lines in an affine plane of order n

Proposition H

Every parallel class has exactly n lines.

class of parallel lines (which partitions points on the plane)

Theorem

There are n^2 points. $\Longleftrightarrow$ $(n \text{ pts}/\text{line}) \times (n \text{ lines}/\text{para. class}) = n^2$

Proposition I

There are $n+1$ parallel classes.

P (n+1) lines

each line belongs to some parallel class

Theorem

There are n^2+n lines. $= \underbrace{(n+1)}_{\#PC} \cdot \underbrace{n}_{\#\text{lines}/PC}$

Affine plane of order n and $n-1$ MOLS of order n

Mutually orthogonal Latin square

Theorem

A complete set of $n-1$ MOLS of order n $\iff$ an affine plane of order n.

Cells in $LS(n)$ $\longleftrightarrow$ points in affine plane of order n

n^2 cells

n^2 pts

Outline

Group (revisit)

Group

A group (群) $(G, +)$ is a set G with an operator $+$ (addition) such that

1. If $a, b \in G$ then $a + b \in G$; (closure; basic property for any groupoid);
2. There exists $0 \in G$ such that $x + 0 = 0 + x = x$ for any $x \in G$ (identity);
3. For any $a \in G$ there exists $b \in G$ such that $a + b = b + a = 0$ (inverse; Latin property);
4. For any $a, b, c \in G$, $(a + b) + c = a + (b + c)$ (associative law) .

- A group $(G, +)$ is commutative (可換) if for any $a, b \in G$, $a + b = b + a$.

Field

(四則演算)

Field

A field (体) $(\mathbb{F}, +, \times)$ is a set $\mathbb{F}$ with two operators $+$ (addition) and $\times$ (multiplication) such that

1. $(\mathbb{F}, +)$ is a commutative group (with additive identity 0);
2. $(\mathbb{F} \setminus \{0\}, \times)$ is a commutative group (with multiplicative identity 1);
3. For any $a, b, c \in \mathbb{F}$, $a \times (b + c) = a \times b + a \times c$ and $(a + b) \times c = a \times c + b \times c$ (distributive property; 分配法則).

- For any $a \in \mathbb{F}$, $0 \times a = a \times 0 = 0$ (so that $(\mathbb{F}, \times)$ is a groupoid).
- $1 \neq 0$ (for nontrivial fields).
- Examples: $(\mathbb{C}, +, \times)$ (complex numbers), $(\mathbb{R}, +, \times)$ (real numbers), $(\mathbb{Q}, +, \times)$ (rational numbers), $(\mathbb{Z}_p, +, \times)$ (finite field of prime order)

Finite field $\mathbb{F}_p$: examples

$\mathbb{F}_p = \mathbb{Z}_p = \{0, 1, \ldots, p-1\}$.

Finite field $\mathbb{F}_2$

$+$	0	1
0	0	1
1	1	0

$\times$	1
1	1

Finite field $\mathbb{F}_5$

Cayley table

$+$	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

$\times$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Finite field $\mathbb{F}_p$

$\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$

Theorem

$\mathbb{Z}_n$ is a field iff n is a prime.

$\mathbb{Z}_4$ is not a field

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

$\times$	1	2	3
1	1	2	3
2	2	4	2
3	3	2	1

$\nexists x$, s.t.
$2 \cdot x \equiv 1 \pmod 4$

- 2 does not have a multiplicative inverse.

Irreducible polynomials over prime fields

irreducible polynomial

An irreducible polynomial (既約多項式) $f(x)$ is a polynomial that cannot be factorized into the product of two non-constant polynomials.

irreducible polynomial over $\mathbb{F}_2$

$f(0) = 1$, $f(1) = 1+1+1 = 1$.
$\neq 0$ $\neq 0$

$f(x) =$ $x^n + x + 1$ is irreducible over $\mathbb{F}_2$ for any $n \geq 2$.

irreducible polynomial over $\mathbb{F}_3$

$g(0) = 1$, $g(1) = 2$,
$g(2) = g(-1) = 1+1 = 2$.

$g(x) =$ $x^{2n} + 1$ is irreducible over $\mathbb{F}_3$ for any $n \geq 1$.

- $x^2 + 1$ is irreducible over $\mathbb{F}_3$ but not irreducible over $\mathbb{F}_2$.

$\mathbb{F}_2$上で $x^2+1 = (x+1)^2$

- $x^2 + 1$ is irreducible over $\mathbb{R}$ but not irreducible over $\mathbb{C}$.

$x^2+1 = (x+i)(x-i) \in \mathbb{C}[x]$

Finite field $\mathbb{F}_{2^m}$: example

Construct $\mathbb{F}_4$

- Let α be a "root" of an irreducible polynomial $f(x) = x^2 + x + 1$ over $\mathbb{F}_2$.
- Clearly, $\alpha \notin \mathbb{F}_2$. Add α into $\mathbb{F}_2$ to obtain $\mathbb{F}_2[\alpha]$. = 係数が$\{0,1\} = \mathbb{F}_2$ の α の多項式全体
- The arithmetic in $\mathbb{F}_2[\alpha]$ is reduced by modulo polynomial $\alpha^2 + \alpha + 1$. In other words, since $\alpha^2 + \alpha + 1 = 0$, we can replace α^2 by $-\alpha - 1 = \alpha + 1$.

Rigorously, $\mathbb{F}_{2^2} = \underbrace{\mathbb{F}_2[\alpha]}_{\text{poly ring}} \Big/ \underbrace{\langle f(\alpha) \rangle}_{\text{ideal}}$ ← quotient ring

Finite field $\mathbb{F}_{2^m}$: example

$[1 = -1 \pmod 2]$

$\alpha^2 + \alpha + 1 = 0$

Finite field $\mathbb{F}_4 = \{0, 1, \alpha, \alpha + 1\}$

$+$	0	1	α	$\alpha + 1$
0	0	1	α	$\alpha + 1$
1	1	0	$\alpha + 1$	α
α	α	$\alpha + 1$	0	1
$\alpha + 1$	$\alpha + 1$	α	1	0

$\times$	1	α	$\alpha + 1$
1	1	α	$\alpha + 1$
α	α	$\alpha + 1$	1
$\alpha + 1$	$\alpha + 1$	1	α

$\alpha + \alpha = 2\alpha = 0$.
$\pmod 2$

$\alpha \cdot \alpha = \alpha^2 = \alpha + 1$

$\alpha(\alpha + 1) = \alpha^2 + \alpha = \alpha + 1 + \alpha = 1$.

Finite field $\mathbb{F}_{2^m}$: example

Finite field $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$

$+$	0	1	α	α^2
0	0	1	α	α^2
1	1	0	α^2	α
α	α	α^2	0	1
α^2	α^2	α	1	0

$\times$	1	α	α^2
1	1	α	α^2
α	α	α^2	1
α^2	α^2	1	α

Finite field $\mathbb{F}_{p^m}$: construction

A non-rigorous description for finite field $\mathbb{F}_{p^m}$

- Let α be a "root" of an irreducible polynomial $f(x)$ over $\mathbb{F}_p$, where $\deg f(x) = m$.
- Clearly, $\alpha \notin \mathbb{F}_p$. Add α into $\mathbb{F}_p$ to obtain $\mathbb{F}_p[\alpha]$.
- The arithmetic in $\mathbb{F}_p[\alpha]$ is reduced by modulo $f(\alpha)$ (as a polynomial).

Theorem (rigorous description for $\mathbb{F}_{p^m}$ using polynomial quotient rings)

Let $f(x)$ be an irreducible polynomial of degree m in $\mathbb{F}_p[x]$. Then $\mathbb{F}_p[x]/\langle f(x)\rangle$ is a field of order p^m.

- $\mathbb{F}_p[x]$: polynomial ring (多項式環), $\langle f(x)\rangle$: ideal (イデアル) in $\mathbb{F}_p[x]$,
- $\mathbb{F}_p[x]/\langle f(x)\rangle$: quotient ring (商環, 剰余環)

Example: finite field $\mathbb{F}_{3^2}$ (1/3)

Construct $\mathbb{F}_{3^2} = \{0, 1, 2, \alpha, \alpha+1, \alpha+2, 2\alpha, 2\alpha+1, 2\alpha+2\}$

- Let α be a "root" of an irreducible polynomial $f(x) = x^2 + 1$ over $\mathbb{F}_3$.
- The arithmetic in $\mathbb{F}_3[\alpha]$ is reduced by modulo polynomial $\alpha^2 + 1$.
  In other words, since $\alpha^2 + 1 = 0$, we can replace α^2 by $-1 = 2$.

$\alpha^2 + 1 = 0 \iff \alpha^2 = 2$

Example: finite field $\mathbb{F}_{3^2}$ (2/3)

- All the coefficients are reduced modulo 3. For example, $3\alpha = 0\alpha = 0$.

$+$	0	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$
0	0	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$
1	1	2	0	$\alpha+1$	$\alpha+2$	α	$2\alpha+1$	$2\alpha+2$	2α
2	2	0	1	$\alpha+2$	α	$\alpha+1$	$2\alpha+2$	2α	$2\alpha+1$
α	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$	0	1	2
$\alpha+1$									
$\alpha+2$									
2α									
$2\alpha+1$									
$2\alpha+2$									

Example: finite field $\mathbb{F}_{3^2}$ (3/3)

- All the coefficients are reduced modulo 3. For example, $2\alpha + 4 = 2\alpha + 1$.
- Replace α^2 by 2, since $\alpha^2 + 1 = 0$.

$\times$	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$
1	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$
2	2	1	2α	$2\alpha+2$	$2\alpha+1$	α	$\alpha+2$	$\alpha+1$
α	α	2α	2	$\alpha+2$	$2\alpha+2$	1	α	$\alpha+1$
$\alpha+1$								
$\alpha+2$								
2α								
$2\alpha+1$								
$2\alpha+2$								

Finite field $\mathbb{F}_{p^m}$: uniqueness

Theorem ①

Finite fields exist iff their order is of the form p^m where p is a prime.

Theorem ②

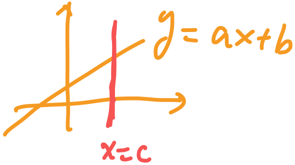
Any two finite fields of the same order are isomorphic (同型).

① $\leftrightarrow$ $\nexists\ \mathbb{F}_{p \cdot q}$ $p \neq q$

$\boxed{\deg f = \deg g = m}$

② $\leftrightarrow$ $\mathbb{F}_p$ 上で $f(x)$ or $g(x)$ を用いて、同じ $\mathbb{F}_{p^m}$ が生成される。
irr. irr.

Affine plane over $\mathbb{F}_q$



- Euclidean plane $\mathbb{R}^2$:
  - Points: $(x, y) \in \mathbb{R}^2$.
  - Lines: $y = ax + b$ and $x = c$, where $x, y \in \mathbb{R}$.
- Affine plane over $\mathbb{F}_q$ (of order q):
  - Points: $(x, y) \in \mathbb{F}_q^2$.
  - Lines: $y = ax + b$ and $x = c$, where $x, y \in \mathbb{F}_q$.

Affine plane over $\mathbb{F}_2$

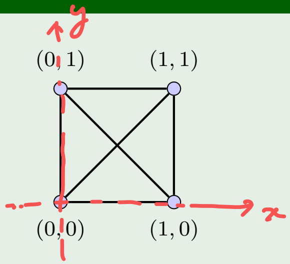
6 lines:

$y=0$ $\quad$ $x=0$

$y=1$ $\quad$ $x=1$

$y=x$

$y=x+1$



Construction of $q-1$ MOLS(q)

$\mathbb{F}_q^* := \mathbb{F}_q \setminus \{0\}$

Theorem

The set of polynomials $f_a(x,y) = ax+y$ with $a \neq 0$ gives a complete set of $q-1$ MOLS(q).

$a \in \mathbb{F}_q^*$

3 MOLS(4) over $\mathbb{F}_4 = \{0,1,\alpha,\alpha+1\}$

$L_a(x,y) = f_a(x,y)$

$a=1$

0	1	α	$\alpha+1$
1	0	$\alpha+1$	α
α	$\alpha+1$	0	1
$\alpha+1$	α	1	0

$a=\alpha$

0	1	α	$\alpha+1$
α	$\alpha+1$	0	1
$\alpha+1$	α	1	0
1	0	$\alpha+1$	α

$a=\alpha^2$

0	1	α	$\alpha+1$
$\alpha+1$	α	1	0
1	0	$\alpha+1$	α
α	$\alpha+1$	0	1

$$\begin{bmatrix} x+y \\ \alpha x+y \\ \alpha^2 x+y \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ \alpha & 1 \\ \alpha^2 & 1 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \end{bmatrix}$$

(rank $=2$)

Outline

Projective plane

Projective plane

An projective plane (射影平面) is an incidence structure $(\mathcal{P}, \mathcal{L}, \mathcal{I})$ such that

1. For any two points $p_1, p_2 \in \mathcal{P}$, there exists a unique line $\ell \in \mathcal{L}$ passing through both p_1 and p_2, i.e. $(p_1, \ell), (p_2, \ell) \in \mathcal{I}$. 2 pts → 1 line
2. Any two lines $\ell_1, \ell_2 \in \mathcal{L}$ intersect in a unique point p, i.e., $(p, \ell_1), (p, \ell_2) \in \mathcal{I}$.
3. There exists at least four points, no three of which are collinear. 2 line → 1 pt

- On a projective plane, there are no parallel lines. 双对
- The incidence structure $(\mathcal{L}, \mathcal{P}, \mathcal{I})$ is called the dual plane of $(\mathcal{P}, \mathcal{L}, \mathcal{I})$.
- A projective plane is said to have order n, if there are $n + 1$ points on a line.

affine order n " n pts on a line

Projective plane of order 2: Fano plane

(7,3,1)-BIBD

$\ell_0 \leftrightarrow \{p_0, p_1, p_3\}$

$\ell_1 \leftrightarrow \{p_1, p_2, p_4\}$

$\ell_2 \leftrightarrow \{p_2, p_3, p_5\}$

$\ell_3 \leftrightarrow \{p_3, p_4, p_6\}$

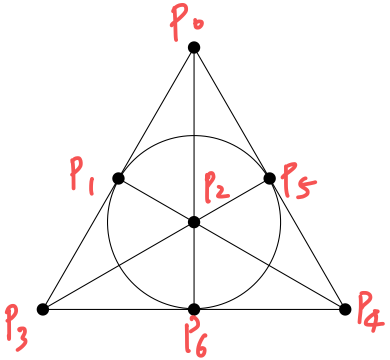
$\ell_4 \leftrightarrow \{p_4, p_5, p_0\}$

$\ell_5 \leftrightarrow \{p_5, p_6, p_1\}$

$\ell_6 \leftrightarrow \{p_6, p_0, p_2\}$

incident matrix

$$
\begin{array}{c c}
 & \begin{array}{ccccccc} p_0 & p_1 & & \cdots & & & p_6 \end{array} \\
\begin{array}{c} \ell_0 \\ \ell_1 \\ \vdots \\ \\ \\ \\ \ell_6 \end{array} &
\begin{bmatrix}
1 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 1 & 0 & 1 \\
1 & 0 & 0 & 0 & 1 & 1 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 1 \\
1 & 0 & 1 & 0 & 0 & 0 & 1
\end{bmatrix}
\end{array}
$$



$n=2 \Rightarrow \#\text{lines} = \#\text{pts} = 7 = n^2+n+1$

Propositions of projective plane of order n

Proposition

On a projective plane of order n there are $n+1$ points on each line and $n+1$ lines passing through each point.

Proposition

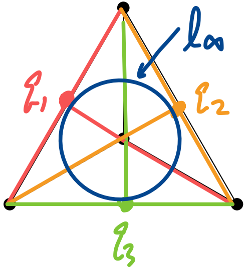
On a projective plane of order n there are totally n^2+n+1 points and n^2+n+1 lines.

Projective plane obtained from affine plane

Theorem

- $\Pi_A = (\mathcal{P}_A, \mathcal{L}_A, \mathcal{I}_A)$: *an affine plane of order n*
- q_i: *new point corresponding to the ith parallel class of Π_A*
- *Let* $\mathcal{P} = \mathcal{P}_A \cup \{q_i : i \in [n+1]\}$
- *Let* $\mathcal{L} = \{\ell_A \cup \{q_i\} : \ell_A$ *in the ith parallel class in* $\mathcal{L}_A\} \cup \{\ell_\infty\}$
- ℓ_∞ *is incident with each* q_i.
- q_i *is incident with each line in the ith parallel class in* $\mathcal{L}_A$.

Then, $\Pi = (\mathcal{P}, \mathcal{L}, \mathcal{I})$ *is a projective plane of order n.*



Fano plane

Affine plane obtained from projective plane

Theorem

- $\Pi = (\mathcal{P}, \mathcal{L}, \mathcal{I})$ *is a projective plane of order* n.
- *Removing any line* ℓ, *i.e.*, $\mathcal{L}_A = \mathcal{L} \setminus \{\ell\}$.
- *Removing all the points incident with* ℓ, *i.e.*, $\mathcal{P}_A = \mathcal{P} \setminus \{p : (p, \ell) \in \mathcal{I}\}$.
- $\mathcal{I}_A$ *is induced by* $\mathcal{I}$.

Then, $\Pi_A = (\mathcal{P}_A, \mathcal{L}_A, \mathcal{I}_A)$ *is an affine plane of order* n.

Projective plane $\iff$ Symmetric BIBD with $\lambda = 1$

$\Updownarrow$ # pts = # lines

$\Updownarrow$ $\forall$ pts x, y, x, y を通る $\exists!\ \ell$.

Theorem

Let $\Pi = (\mathcal{P}, \mathcal{L}, \mathcal{I})$ be a projective plane of order n. Regarding $\mathcal{P}$ and $\mathcal{L}$ as point set and block set of designs, respectively, Π is a symmetric $(n^2+n+1, n+1, 1)$ BIBD.

Theorem

The residual design of a projective plane of order n is an $(n^2, n^2+n, n+1, n, 1)$ BIBD, which is equivalent to an affine plane of order n.

(v, b, r, k, λ)

- remove block (= line) ℓ
- remove all pts on ℓ

Projective plane over $\mathbb{F}_q$ (1/3)

- Two points $(a,b,c),(a',b',c') \in \mathbb{F}_q^3$ (3-dimensional vector space) are equivalent, say

$$(a,b,c) \sim (a',b',c')$$

共方向のベクトルは同値.

  iff $(a',b',c') = (ta,tb,tc)$ for some $t \in \mathbb{F}_q^*$, i.e., they are linear dependent (線型従属).

- We use $[a:b:c]$ for the equivalent class of (a,b,c), which is essentially a 1-dimensional subspace of $\mathbb{F}_q^3$.

Equivalent class of $(1,2,3)$ in $\mathbb{F}_5^3$

$$[1:2:3] = \{(1,2,3),(2,4,1),(3,1,4),(4,3,2)\}$$

Projective plane over $\mathbb{F}_q$ (2/3)

- Both point set $\mathcal{P}$ and line set $\mathcal{L}$ are $\left(\mathbb{F}_q^3 \setminus \{(0,0,0)\}\right) / \sim$: equivalent classes w.r.t. $\sim$.
- To distinguish points and lines, we use row vectors $[a:b:c]$ for points and column vectors $\begin{bmatrix} d \\ e \\ f \end{bmatrix}$ for lines. The point $[a:b:c]$ is incident to a line $\begin{bmatrix} d \\ e \\ f \end{bmatrix}$ iff $ad+be+cf=0$.

← 2-dim. subspace $dx+ey+fz=0$

平面

Example

In ~~affine~~ projective space of order 3, the point $[1,2,2]$ is incident to lines

$\mathbb{F}_3$ で

$$\begin{bmatrix} 0 \\ 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \\ 2 \end{bmatrix}.$$

Projective plane over $\mathbb{F}_q$ (3/3)

Theorem

If $\Pi = (\mathcal{P}, \mathcal{L}, \mathcal{I})$ *is defined by*

$$\mathcal{P} = \mathcal{L} = \left(\mathbb{F}_q^3 \setminus \{(0,0,0)\}\right) \Big/ \sim$$

and the point $[a : b : c]$ *is incident to a line* $\begin{bmatrix} d \\ e \\ f \end{bmatrix}$ *iff* $ad + be + cf = 0$, *then* Π *is a projective plane.*

A brief summary for projective planes

- Finite field construction is one construction of finite projective planes.
- All the known finite projective planes have orders that are prime powers.
- Projective planes of orders 6, 14 do not exist. (by Bruck–Ryser theorem) Chowla
- Projective plane of order 10 does not exist. (by computer search)

Table: Number of finite projective planes of order n

n	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
#	1	1	1	1	0	1	1	4	0	≥ 1	??	≥ 1	0	??	≥ 22	≥ 1	??	≥ 1	??

Theorem (Bruck–Ryser theorem)

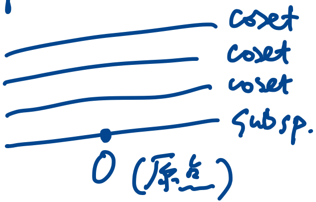
Let $n \equiv 1, 2 \pmod 4$. If there exists a projective plane of order n then $n = a^2 + b^2$ for some $a, b \in \mathbb{Z}$.

Higher dimensional finite geometries

base field

- The affine plane over $\mathbb{F}_q$ is denoted by $\mathrm{AG}(2, \mathbb{F}_q)$.
- The projective plane over $\mathbb{F}_q$ is denoted by $\mathrm{PG}(2, \mathbb{F}_q)$.
- The affine geometry $\mathrm{AG}(n, \mathbb{F}_q)$
  - points: $\mathbb{F}_q^n$
  - lines (1-flats): 1-dim subspaces of $\mathbb{F}_q^n$ and their cosets
  - planes (2-flats): 2-dim subspaces of $\mathbb{F}_q^n$ and their cosets
  - k-flats: k-dim subspaces of $\mathbb{F}_q^n$ and their cosets
  - hyperplanes ($(n-1)$-flats): $(n-1)$-dim subspaces of $\mathbb{F}_q^n$ and their cosets

parallel class



- The projective geometry $\mathrm{PG}(n, \mathbb{F}_q)$
  - points: 1-dim subspaces of $\mathbb{F}_q^{n+1}$ ← base space
  - lines: 2-dim subspaces of $\mathbb{F}_q^{n+1}$
  - planes: 3-dim subspaces of $\mathbb{F}_q^{n+1}$
  - hyperplanes: n-dim subspaces of $\mathbb{F}_q^{n+1}$

Homework assignments (レポート課題) for 3rd day

Exercise 1

Complete the addition and multiplication tables of $\mathbb{F}_{3^2}$ by using irreducible polynomial x^2+1.

Exercise 2

List the points and lines in the affine plane of order 3.

- Deadline: 6th Sept., 23:59:59

Hint: there are many ways.

(i) by definition.

(ii) using $\mathbb{F}_3^2$

(iii) using 2 MOLS(3)

- No lectures in the afternoon,
- Next lect: Next Mon. 9:00 ~
- Happy weekend!