集中講義 応用数学特論 II

Day 3 有限幾何学・有限体

担当：盧　暁南 (山梨大学)
xnlu@yamanashi.ac.jp

2021 年 8 月 27 日

本日の内容

本日は有限アフィン幾何学（平行線のある幾何学，ユークリッド幾何学の有限類似），有限射影幾何（平行線のない幾何学），有限体について紹介する．

0　記号・概念

- $\mathcal{P}$: 点の集合
- $\mathcal{L}$: 線の集合
- $\mathcal{I} \subseteq \mathcal{P} \times \mathcal{L}$: 結合関係 (incidence relation)
- $(P, \ell) \in \mathcal{I}$: 点 $P \in \mathcal{P}$ が線 $\ell \in \mathcal{L}$ にある
- $(\mathcal{P}, \mathcal{L}, \mathcal{I})$: 結合構造 (incidence structure)
- 2 本の線 $\ell_1, \ell_2 \in \mathcal{L}$ は**平行** (parallel): ℓ_1 と ℓ_2 とも結合する点がない

1　有限アフィン平面

定義 1.1. 以下の条件が満たされる $(\mathcal{P}, \mathcal{L}, \mathcal{I})$ は**アフィン平面** (affine plane) という．

(1) 任意の 2 点 $p_1, p_2 \in \mathcal{P}$ に対して，p_1 と p_2 両方を通る線 $\ell \in \mathcal{L}$ が一意に存在する．すなわち，$(p_1, \ell), (p_2, \ell) \in \mathcal{I}$ を満たす $\ell \in \mathcal{L}$ が 1 つしかない．

(2) 線 $\ell \in \mathcal{L}$ 上にない ($(p, \ell) \notin \mathcal{I}$ を満たす) 点 $p \in \mathcal{P}$ において，p を通る (すなわち，$(P, \ell_P) \in \mathcal{I}$ を満たす) ℓ に平行する線 ℓ_P が一意に存在する．

(3) 少なくとも 3 つの非共線点が存在する．

注 1.2. 各線上に点の個数はアフィン平面の**位数** (order) という．

定理 1.3. 位数 n のアフィン平面において，以下が成り立つ．

(1) 各点を通る線の数は $n + 1$.

(2) 点の数は n^2.

(3) 線の数は $n^2 + n$.

2 有限射影平面

定義 2.1. 以下の条件が満たされる $(\mathcal{P}, \mathcal{L}, \mathcal{I})$ は**射影平面** (projective plane) という．

(1) 任意の 2 点 $p_1, p_2 \in \mathcal{P}$ に対して， p_1 と p_2 両方を通る線 $\ell \in \mathcal{L}$ が一意に存在する．すなわち，$(p_1, \ell), (p_2, \ell) \in \mathcal{I}$ を満たす $\ell \in \mathcal{L}$ が 1 つしかない．

(2) 任意の 2 つの線 $\ell_1, \ell_2 \in \mathcal{L}$ は 1 点 p で交わる．すなわち，$(p, \ell_1), (p, \ell_2) \in \mathcal{I}$.

(3) 少なくとも 4 点が存在し，そのうちどの 3 点も共線しない．

注 2.2. 射影平面に平行線が存在しない．

注 2.3. 各線上に $n+1$ 点があるとき，その射影平面の**位数** (order) を n とする．

定理 2.4. 位数 n の射影平面において，以下が成り立つ．

(1) 各点を通る線の数は $n+1$.

(2) 点の数は n^2+n+1.

(3) 線の数は n^2+n+1.

注 2.5. 位数 n の射影平面は対称 $(n^2+n+1, n+1, 1)$BIB デザインと同値である．

定理 2.6. Bruck–Ryser 定理位数 $n \equiv 1, 2 \pmod 4$ の射影平面が存在するならば $n = a^2 + b^2$ を満たす整数 a, b が存在する．

3 有限体

定義 3.1. 集合 $\mathbb{F}$ と演算 $+$ (加法), $\times$(乗法) において，以下の条件が満たされる $(\mathbb{F}, +, \times)$ は**体** (field) という．

(1) $(\mathbb{F}, +)$ は可換群である．また，0 は加法における単位元とする．

(2) $(\mathbb{F} \setminus \{0\}, \times)$ は可換群である．また，1 は乗法における単位元とする．

(3) 任意の $a, b, c \in \mathbb{F}$ において分配法則 (distributive property) がある，つまり，$a \times (b+c) = a \times b + a \times c$ かつ $(a+b) \times c = a \times c + b \times c$.

定義 3.2. 要素が有限個しかない体は**有限体** (finite field) という．要素の個数を有限体の**位数** (order) という．

定理 3.3. $\mathbb{Z}_n$ が有限体 $\iff$ n が素数.

定理 3.4. 有限体の位数が素数冪である．

定理 3.5. 位数が同じの有限体は，すべて互いに同型である．

一般の有限体の構成法はスライドに参照.

レポート課題

演習課題 1. $\mathbb{F}_3$ 上の既約多項式 x^2+1 を用いて有限体 $\mathbb{F}_{3^2}$ の加法演算表と乗法演算表を完成せよ．

演習課題 2. 位数 3 のアフィン平面の点と線を列挙せよ．

レポート提出期限：9 月 6 日 (月) 23:59 まで

参考文献

[1] S. T. Dougherty. *Combinatorics and Finite Geometry*. Springer, 2020.

[2] E. H. Moore and H. S. K. Pollatsek. *Difference Sets: Connecting Algebra, Combinatorics, and Geometry*. American Mathematical Society, 2013.

[3] 安田健彦. **ゲームで大学数学入門: スプラウトからオイラー ゲッターまで**. 共立出版, 2018.

[4] 佐藤肇 and 一樂重雄. **幾何学の魔術: 魔法陣から現代数学へ** *(***第** *3* **版***)*. 日本評論社, 2012.