Gypsy Akhyar
13th August 2025

Advanced Discrete Mathematics
Lecture 7

Writing advice

(1) Start thinking about the structure of the document.

(2) Start trying to explain your writing to a friend.

→ specialised version of last lecture's

Theorem Let $\mathbb{F}$ be a field. Let V be an $\mathbb{F}$-vector space. Define

$$\mathbb{G}(V) = \{\mathbb{F}\text{-subspaces of } V\},$$

partially ordered by inclusion. Then, $\mathbb{G}(V)$ is a modular lattice.

Important examples:

(1) If $\mathbb{F} = \mathbb{Z}$ and $V = \mathbb{Z}$, then $\mathbb{G}(V) = \{\text{ideals of } \mathbb{Z}\}$.

(2) If $\mathbb{F} = G$, where G is a group, and $V = G$, then $\mathbb{G}(V) = \{\text{subgroups of } V\}$.

Proposition Let $n \in \mathbb{Z}_{>0}$. Let $\mathbb{R}$ be a field. Let $\mathbb{G}(\mathbb{R}^n) = \{\mathbb{R}\text{-subspaces of } \mathbb{R}^n\}$. Let $M, N, P \in \mathbb{G}(\mathbb{R}^n)$. Then

(a) (infimums exist)

$$\inf(M,N) = M \cap N = \{v \in \mathbb{R}^n \mid v \in M \text{ and } v \in N\}$$

(b) (supremums exist)

$$\sup(M,N) = M + N = \{m + n \mid m \in M \text{ and } n \in N\}$$

(c) (modular law)

If $M \subseteq P$ then $M + (N \wedge P) = (M+N) \wedge P$

(d) (modular property)

$$\frac{M+N}{M} \simeq \frac{N}{M \wedge N}$$

The function $\dim : G(F^n) \to \{0, 1, \ldots, n\}$ given by

$\dim(M) = \#$ elements in an R-basis of M

makes $G(F^n)$ into a ranked modular lattice

Theorem Let $q \in \mathbb{Z}_{>0}$ and $\mathbb{F}_q$ be a field with q elements.
For $r \in \mathbb{Z}_{>0}$ let

$$[r] = \frac{q^r - 1}{q-1} \quad \text{and} \quad [r]! = [r][r-1] \cdots [2][1].$$

We say that $[r]$ is the q-analogue of r.

(Remark: $[r] = 1 + q + q^2 + \cdots + q^{r-1}$ and $ev_{q=1}([r]) = r$)

For $k \in \{0, 1, \ldots, n\}$ let

$$\begin{bmatrix} n \\ k \end{bmatrix} = \frac{[n]!}{[k]!\,[n-k]!}$$

Then, $G(\mathbb{F}_q^n) = \bigsqcup_{k=0}^{n} G(\mathbb{F}_q^n)_k$ and $\mathrm{Card}(G(\mathbb{F}_q^n)_k) = \begin{bmatrix} n \\ k \end{bmatrix}$

where $G(\mathbb{F}_q^n)_k = \{\mathbb{F}_q\text{-subspaces of } \mathbb{F}_q^n \text{ with } \mathbb{F}_q\text{-dimension } k\}$.

Example: $q = 8327$, $n=5$, $k=3$. Then

$$\begin{bmatrix} 5 \\ 3 \end{bmatrix} = \frac{[5][4]\cancel{[3]}\cancel{[2]}\cancel{[1]}}{\cancel{[3]}[2]\cancel{[1]}\cancel{[2]}\cancel{[1]}} = \frac{(q^4+q^3+q^2+q+1)(q^3+q^2+q+1)}{q+1}$$

$$= 192,508,205,775,287,856,337,121,848,881,660,720$$

(an integer, wow!)

(Remark: These counts over finite fields all at once were the source of the Weil conjectures.)

$$\sum_{k=0}^{n} x^k q^{\frac{k(k-1)}{2}} \begin{bmatrix} n \\ k \end{bmatrix} = \begin{bmatrix} n \\ 0 \end{bmatrix} + \begin{bmatrix} n \\ 1 \end{bmatrix} q^0 x + \begin{bmatrix} n \\ 2 \end{bmatrix} q^1 x^2 + \dots + \begin{bmatrix} n \\ n \end{bmatrix} q^{\frac{n(n-1)}{2}} x^n$$

$$= (1+x)(1+xq)\cdots(1+xq^{n-1})$$

is the q-analogue of

$$\sum_{k=0}^{n} x^k \binom{n}{k} = \binom{n}{0} + \binom{n}{1} x + \binom{n}{2} x^2 + \cdots \binom{n}{n} x^n$$

$$= (1+x)^n.$$

The crucial example is the Fano plane.
This is when $q=2$ and $\mathbb{F}_q = \mathbb{F}_2 = \{0,1\}$.
Let $n=3$ and draw the Hasse diagram of $G(\mathbb{F}_q^3)$.

Show (/observe) that this is equivalent to the Fano plane