Singer's Theorem.

Example: $p(x) = x^3 + 2x + 1$ is a primitive polynomial of degree 3 over $\mathbb{F}_3$.

$\mathbb{F}_{27}$

$x^3+2x+1=0 \to x^3 = x+2$

$x^3+2x+1=0 \to 2x^3 = 2x+1$

Powers of x:-

$x^0 = 1$

$x^1 = x$

$x^2 = x^2$

$x^3 = x+2$

$x^4 = x^2+2x$

$x^5 = 2x^2+x+2$

$x^6 = x^2+x+1$

$x^7 = x^2+2x+2$

$x^8 = 2x^2+2$

$x^9 = x+1$

$x^{10} = x^2+x$

$x^{11} = x^2+x+2$

$x^{12} = x^2+2$

$x^{13} = 2$

$x^{14} = 2x$

$x^{15} = 2x^2$

$x^{16} = 2x+1$

$x^{17} = 2x^2+x$

$x^{18} = x^2+2x+1$

$x^{19} = 2x^2+2x+2$

$x^{20} = 2x^2+x+1$

$x^{21} = x^2+1$

$x^{22} = 2x+2$

$x^{23} = 2x^2+2x$

$x^{24} = 2x^2+2x+1$

$x^{25} = 2x^2+1$

The 26 non-zero elements of $\mathbb{F}_{27}$.

$\{x^0, x^1, \ldots, x^{25}\}$

$x^{26} = 1$

$\mathbb{F}_{27}^* \cong \mathbb{Z}_{26}$

Correspondence:

V: 3-dimensional vector space over $\mathbb{Z}_3$.

Vectors (a_0, a_1, a_2) where $a_0, a_1, a_2 \in \mathbb{Z}_3$

$\sim$

$\mathbb{F}_{27}$

$a_0 + a_1 x + a_2 x^2$

Coefficients $a_0, a_1, a_2 \in \mathbb{Z}_3$

points of PG(2,3) $\sim$ elements of the factor group $\mathbb{F}_{27}^* / \mathbb{F}_3^*$

1-dimensional subspaces of V.

$\mathbb{F}_3^* = \{1,2\}$

constant polynomials.

lines of PG(2,3)

2-dimensional subspaces/ hyperplanes of V

Eg: Vectors of the form $(a_0, a_1, 0)$ constitute a hyperplane. $\sim$ Polynomials of the form $a_0 + a_1 x$

$\{\{1,2\}, \{x, 2x\}, \{x+1, 2x+2\}, \{x+2, 2x+1\}\}$

$= \{x^0, x^1, x^3, x^9\}$

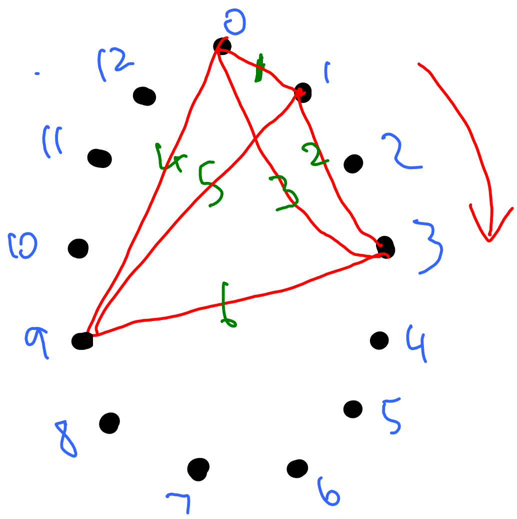
"multiplication by x" permutes hyperplanes in a single orbit.

0	1	3	9
1	2	4	10
2	3	5	11
3	4	6	12
4	5	7	0
5	6	8	1
6	7	9	2
7	8	10	3
8	9	11	4
9	10	12	5
10	11	0	6
11	12	1	7
12	0	2	8

$$\left\{ \begin{array}{cccc} x^0 & x^1 & x^3 & x^9 \\ x^1 & x^2 & x^4 & x^{10} \\ & & \vdots & \\ x^{12} & x^0 & x^2 & x^8 \end{array} \right.$$

$\{x, 2x\}$
$\{x^2, 2x^2\}$,
$\{x^2+2x, 2x^2+x\}$,
$\{x^2+x, 2x^2+2x\}$

Projective plane of order 3 (points $0, 1, \ldots, 12$)



Affine analogue of Singer's Theorem:

Example 2.7.4. Construction of an affine plane of order 5 with an automorphism that fixes one point and permutes the remaining points in a cycle of length 24. We work in $\mathbb{F}_{q^n}$ with $q = 5$ and $n = 2$. A primitive polynomial of degree $n = 2$ over $\mathbb{F}_q = \mathbb{F}_5$ is $p(x) = x^2 + x + 2$. Working modulo $p(x)$, we have $x^2 = 4x + 3$. It will also be convenient for subsequent calculations to note that $2x^2 = 3x + 1$, $3x^2 = 2x + 4$ and $4x^2 = x + 2$.

We now evaluate x^i for $i = 0, 1, 2, \ldots, 23$.

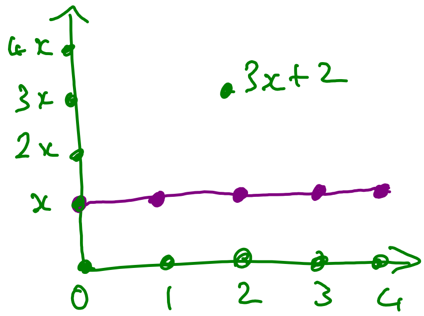
$\mathbb{F}_{5^2} = \mathbb{F}_{25}$

$x^0 = 1$	$x^6 = 2$	$x^{12} = 4$	$x^{18} = 3$
$x^1 = x$	$x^7 = 2x$	$x^{13} = 4x$	$x^{19} = 3x$
$x^2 = 4x + 3$	$x^8 = 3x + 1$	$x^{14} = x + 2$	$x^{20} = 2x + 4$
$x^3 = 4x + 2$	$x^9 = 3x + 4$	$x^{15} = x + 3$	$x^{21} = 2x + 1$
$x^4 = 3x + 2$	$x^{10} = x + 4$	$x^{16} = 2x + 3$	$x^{22} = 4x + 1$
$x^5 = 4x + 4$	$x^{11} = 3x + 3$	$x^{17} = x + 1$	$x^{23} = 2x + 2$

1-flats: $\{0, 1, 2, 3, 4\}$

translate by $+x$

$\{x, x+1, x+2, x+3, x+4\}$



$$\left.\begin{array}{l} 0, x^0, x^6, x^{12}, x^{18} \\ 0, x^1, x^7, x^{13}, x^{19} \\ 0, x^2, x^8, x^{14}, x^{20} \\ 0, x^3, x^9, x^{15}, x^{21} \\ 0, x^4, x^{10}, x^{16}, x^{22} \\ 0, x^5, x^{11}, x^{17}, x^{23} \end{array}\right\} 6$$

$$\left.\begin{array}{l} x^1, x^{17}, x^{14}, x^{15}, x^{10} \\ x^2, x^{18}, x^{15}, x^{16}, x^{11} \\ x^3, x^{19}, x^{16}, x^{17}, x^{12} \\ \vdots \\ x^0, x^{16}, x^{13}, x^{15}, x^{9} \end{array}\right\} 24$$

(The 1-subspaces are in a single orbit)

(The non-subspace 1-flats fall in a single orbit)

$\mathbb{Z}_{24} \cup \{\infty\}$

Write $0 \leftrightarrow \infty$, $x^0 \leftrightarrow 0$, $x^1 \leftrightarrow 1$, $\ldots$, $x^{23} \leftrightarrow 23$ $\Longrightarrow$

					1	10	14	15	17
					2	11	15	16	18
∞	0	6	12	18					
∞	1	7	13	19	⋮				
⋮									
∞	5	11	17	23	0	9	13	14	16

PP(5) orbits of $\{\infty, 0, 6, 12, 18\}$ and $\{1, 10, 14, 15, 17\}$ under $\mathbb{Z}_{24}$.