Def. 1.1 A point-line incidence structure (or incidence system) is a triple $(\mathcal{P}, \mathcal{L}, I)$, where

$\mathcal{P}, \mathcal{L}$ are sets of points and lines respectively, and incidence relation $I \subseteq \mathcal{P} \times \mathcal{L}$ is a binary relation indicating which point-line pairs are incident.

Def. 1.2. (Isomorphism)

Consider two point-line incidence structures $(\mathcal{P}, \mathcal{L})$ and $(\mathcal{P}', \mathcal{L}')$. An isom from $(\mathcal{P}, \mathcal{L})$ to $(\mathcal{P}', \mathcal{L}')$ is a bijection $\sigma: \mathcal{P} \cup \mathcal{L} \to \mathcal{P}' \cup \mathcal{L}'$ such that

(i) $\mathcal{P}^\sigma = \mathcal{P}'$ and $\mathcal{L}^\sigma = \mathcal{L}'$, and

(ii) for all $p \in \mathcal{P}$ and $l \in \mathcal{L}$, we have

$$p \in l \Leftrightarrow p^\sigma \in l^\sigma$$

Def 1.3. A proj plane is an incidence system of points and lines such that

(P1) For any two distinct points, there is exactly one line through both,

(P2) Any two distinct lines meet in exactly one point

(P3) There exist four points such that no three are collinear.

Example 1.4. The classical proj. planes are constructed as follows: V: 3-dim v.s. $/\mathbb{F}$, $\mathbb{F}$: a field

$\mathcal{P}$ = the set of 1-dim subspaces of V

$\mathcal{L}$ = the set of 2-dim subspaces of V

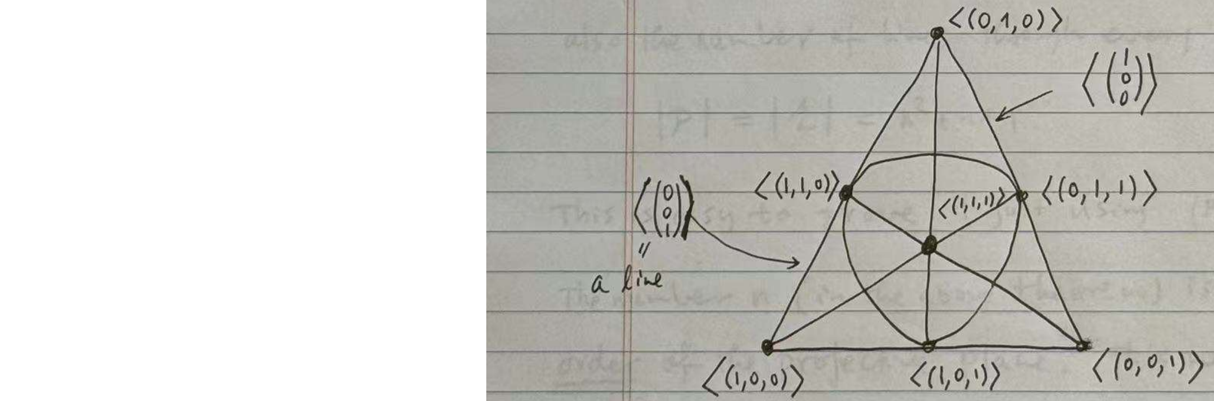
I: the natural inclusion (that is, a point P lies on a line ℓ $\Leftrightarrow$ $P \subset \ell$ as subspaces of V)

The resulting plane is denoted $\mathbb{P}^2(F)$ or $PG(2,F)$.

In the case of a finite field $F = \mathbb{F}_q$ (q a prime power), we also denote this plane $\mathbb{P}^2(q) = PG(2,q)$.

The smallest projective plane $\mathbb{P}^2(\mathbb{F}_2) = PG(2,2)$:

$$7 \text{ points} = \begin{bmatrix}3\\1\end{bmatrix}_2 = \frac{2^3-1}{2-1}, \qquad 7 \text{ lines} = \begin{bmatrix}3\\2\end{bmatrix}_2$$



We label each point as $\langle (x,y,z) \rangle$, the 1-dim subsp spanned by a nonzero vector (x,y,z); we refer to x,y,z as homogeneous coordinates for this pt.

Theorem 1.5.

Let $(\mathcal{P}, \mathcal{L})$ be a proj plane. Then there are equally many points and lines, i.e. the sets $\mathcal{P}$ and $\mathcal{L}$ have the same cardinality. Moreover any two lines contain the same number of points, and this number equals the number of lines through any point. If $n+1$ is the number of points on every line (hence also the number of lines through every point) then

$$|\mathcal{P}| = |\mathcal{L}| = n^2+n+1.$$

This is easy to prove (just using (P1), (P2), (P3))

The number n (in the above theorem) is called the order of the projective plane. This means that the order of the classical plane $\mathbb{P}^2(F)$ is exactly $|F|$.

Remark 1.6.

When q ($q > 8$ and) is a proper prime power, i.e., $\boxed{q > 8 \quad q = p^{\alpha}, \ \alpha \geq 2 \quad p: \text{a prime}}$

there exists a proj plane of order q

that is NOT isomorphic to $\mathbb{P}^2(\mathbb{F}_q) = PG(2,q)$.

For this reason, we usually call $PG(2,q)$ the classical projective plane of order q.

The easiest (or quickest) way to construct a nonclassical plane is by constructing a translation plane (which can be constructed by spreads of $V(4,q)$)

n (the order)	no. of planes of order n up to isom.	Remarks
2	1	$\mathbb{P}^2(\mathbb{F}_2)$
3	1	$\mathbb{P}^2(\mathbb{F}_3)$
4	1	$\mathbb{P}^2(\mathbb{F}_4)$
5	1	$\mathbb{P}^2(\mathbb{F}_5)$
7	1	$\mathbb{P}^2(\mathbb{F}_7)$
8	1	$\mathbb{P}^2(\mathbb{F}_8)$
9	4	1991年 Disc. Math. paper by Lam, Kolesva, Thiel

Conjecture 1.7 (The prime power conjecture)

Let $(\mathcal{P}, \mathcal{L})$ be a finite projective plane of order n.

Then n must be a prime power.

Theorem 1.8 (Bruck – Ryser)

If there is a projective plane of order n, and

$n \equiv 1$ or $2 \pmod 4$, then n is the sum of two squares.

Corollary 1.9.

There does not exist a projective plane of order 6.

$$\left.\begin{array}{l} 6 \equiv 2 \pmod 4 \\ \text{and } 6 \neq \square + \square \end{array}\right. \xRightarrow{\text{by B-R}} \nexists \text{ a proj plane of order } 6$$

Conjecture 1.10.

Let $(\mathcal{P}, \mathcal{L})$ be a proj plane of order p (prime).

Then $(\mathcal{P}, \mathcal{L}) \stackrel{\wedge}{=} PG(2, p)$.

Conics and Ovals

Def. 2.1. A Conic in the classical plane $\mathbb{P}^2(\mathbb{F}_q)$ is the set $\mathcal{C}$ of points $\langle(x,y,z)\rangle$ satisfying a nonzero homogeneous quadratic form $Q(X,Y,Z)=0$, where

$$Q(X,Y,Z) = aX^2+bY^2+cZ^2+dXY+eXZ+fYZ,$$

$$a,b,c,d,e,f \in \mathbb{F}_q$$

Remark 2.2.

(i) Note that $Q(\lambda x,\lambda y,\lambda z) = \lambda^2 Q(x,y,z)$, $\forall \lambda \in \mathbb{F}_q^*$, we see that the above def. of conic is well-defined.

(ii) We say that $\mathcal{C}$ is nondegenerate if it doesn't contain an entire line of $\mathbb{P}^2(\mathbb{F}_q)$ (algebraically, $\mathcal{C}$ is nondeg if $Q(X,Y,Z)$ can't be factored into a product of two linear forms)

Theorem 2.3. Let $\mathcal{C}$ be a nondegenerate conic in a finite classical plane $\mathbb{P}^2(\mathbb{F}_q)$. Then $\mathcal{C}$ has $q+1$ points, of which no 3 are collinear. Moreover, $\mathcal{C}$ is equivalent, by a linear change of coordinates, to the conic defined by $Y^2 = XZ$.

Proof: Homework #1 for you.

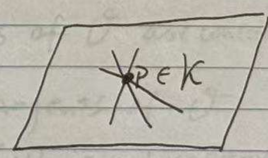
Definition 2.4.

A k-arc in a projective plane of order n is a set K of k points, no 3 of which are collinear.

Theorem 2.5. Let K be a k-arc in a proj. plane of order n. If n is odd, then $k \leq n+1$.

If n is even, then $k \leq n+2$.

Proof: Take a point $p \in K$.



$|K| \leq n+2$

If n is odd, we show that $|K| = n+2$ is impossible.

$|K| = n+2 \Rightarrow$ every line meets K in 0 or 2 points $\Rightarrow n+2 \equiv 0\ (2) \Rightarrow n$ is even

In the above theorem,

n odd & $|K| = n+1 \implies K$ is called an oval

n even & $|K| = n+2 \implies K$ is called a hyperoval

Example : In $PG(2,q) = \mathbb{P}^2(\mathbb{F}_q)$, let $\mathcal{C}$ = the conic defined by $Y^2 = XZ$. That is,

$$\mathcal{C} = \{\langle(1, t, t^2)\rangle \mid t \in \mathbb{F}_q\} \cup \{\langle(0,0,1)\rangle\}$$

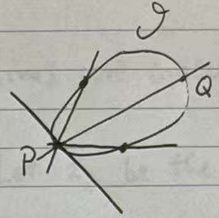
is an oval in $\mathbb{P}^2(\mathbb{F}_q)$.

Theorem 2.6. Let $\mathcal{O}$ be an oval in a proj. plane of order n. Then every point of $\mathcal{O}$ lies on a unique tangent; thus $\mathcal{O}$ has exactly $n+1$ tangents.

(i) If n is odd, then no 3 tangents of $\mathcal{O}$ are concurrent

(ii) If n is even, then all $(n+1)$ tangents of $\mathcal{O}$ meet in a point N. Now $\mathcal{O} \cup \{N\}$ is a hyperoval, the unique hyperoval containing $\mathcal{O}$.

proof:



Let $P \in \mathcal{O}$. The n points $Q \in \mathcal{O} \setminus \{P\}$ determine n distinct secants through P; So the remaining line through P is a tangent.

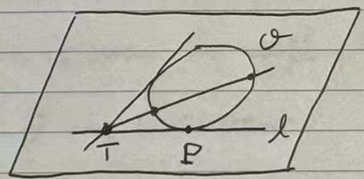
Thus we have shown that every point of $\mathcal{O}$ lies on a unique tangent

---

(i) If n is odd, then $n+1 = |\mathcal{O}|$ is even.

Claim: Any point not on $\mathcal{O}$ lies on 0 or 2 tangents

(a)



Let $T \in \ell \setminus \{P\}$.

t = the number of tangent lines through T

s = the number of secant lines through T

we have $t + 2s = n+1$ (even)

$\Rightarrow$ t is even

Since each of the n points $T \in \ell \setminus \{P\}$ lies on at least one tangent other than ℓ, the tangents of $\mathcal{O}$ other than ℓ must meet ℓ in n <u>distinct</u> points. Hence no 3 tangent lines are concurrent.

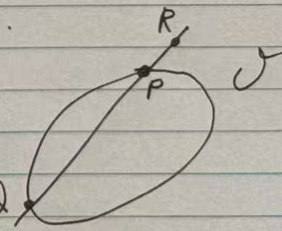
(b) Let x_i be the # of pts outside $\mathcal{O}$ which lie on exactly i tangents. We just proved that

$$x_i = 0, \text{ for } i > 2; \text{ and } x_1 = 0.$$

Hence every point not on $\mathcal{O}$ lies on 0 or 2 tangent lines. [A point not on $\mathcal{O}$ lying on 0 tangent lines is called an interior (or internal) point. A point not on $\mathcal{O}$ lying on 2 tangent lines is called an exterior point]

(ii) If n is even, we will show that the $n+1$ tangents of $\mathcal{O}$ are concurrent.

Note that if n is even, then $n+1$ is odd.



Let $P, Q \in \mathcal{O}$, and $\overline{PQ}$ be the secant line of $\mathcal{O}$ through P and Q. Let $R \in \overline{PQ} \setminus \{P, Q\}$

Claim: Through R there is at least one tangent

This is clear since any line connecting R to a point of $\mathcal{O}$ contains one or two points of $\mathcal{O}$. Since $n+1$ is odd, there must be a tangent line through R.

Since through each of the $n+1$ pts of $\overline{PQ}$ there is a tangent of $\mathcal{O}$, we see that through each pt of $\overline{PQ}$ there is <u>exactly</u> one tangent. Consequently two tangents of $\mathcal{O}$ must meet in a pt N that is <u>NOT ON ANY Secant of $\mathcal{O}$</u> (if N is on a secant, then $\exists!$ tangent line through N). (In other words, every line through N must be a tangent of $\mathcal{O}$.

N: called the Knot of the oval $\mathcal{O}$

Examples of ovals and hyperovals in $PG(2,q)$

q odd, $\mathcal{C} = \{ \langle (x,y,z) \rangle \mid y^2 = xz \}$ is an oval

since it has $q+1$ pts, no 3 of which are collinear

$q = 2^d$ $\quad \mathcal{C} = \{ \langle (1,t,t^2) \rangle \mid t \in \mathbb{F}_q \} \cup \{ \langle (0,0,1) \rangle \}$

is a conic since $Y^2 = XZ$

$N = \langle (0,1,0) \rangle$ is the knot of $\mathcal{C}$

why? $\quad Y^2 - XZ = 0, \quad Q(X,Y,Z) = Y^2 - XZ$

$$\frac{\partial Q}{\partial X} = -Z, \quad \frac{\partial Q}{\partial Y} = 2Y, \quad \frac{\partial Q}{\partial Z} = -X$$

$\forall t \in \mathbb{F}_q$, 过点 $\langle (1,t,t^2) \rangle$ 的 tangent line is :

$$(-t^2)X + 2tY + (-1)Z = 0$$

$t = 0$, 过点 $\langle (0,0,1) \rangle$ 的 tangent line is :

$$(-1)X + 0 \cdot Y + 0 \cdot Z = 0$$

One can check that $\langle (0,1,0) \rangle$ is on all the above $q+1$ lines

$q = 2^d$

So $\mathcal{C} \cup \{N\} = \{(1, t, t^2) \mid t \in \mathbb{F}_q\} \cup \{(0,0,1), (0,1,0)\}$

is a hyperoval in $PG(2, 2^d)$, usually called the regular hyperoval.

Segre's Theorem 1955.

Any oval in $PG(2,q)$, q odd prime power, must be a nondeg. Conic.

Segre's theorem gives a complete classification of ovals in $PG(2,q)$, q odd.

When $q = 2^d$, the classification of hyperovals in $PG(2, 2^d)$ is open. We do Know that there are hyperovals in $PG(2, 2^d)$ which are inequivalent to the regular hyperoval. Some examples are

(i) The Segre hyperoval. Let $d \geq 3$ be odd

$$S = \{(1, t, t^6) \mid t \in \mathbb{F}_{2^d}\} \cup \{(0,0,1), (0,1,0)\}$$

(ii) The Glynn hyperovals. Let $d \geq 3$ be odd

$$G1 = \{(1, t, t^{\sigma+\gamma}) \mid t \in \mathbb{F}_{2^d}\} \cup \{(0,0,1), (0,1,0)\}$$

$$\sigma = 2^{\frac{d+1}{2}}, \quad \gamma = \begin{cases} 2^{\frac{3d+1}{4}} \\ 2^{\frac{d+1}{4}} \end{cases}$$

$$G2 = \{(1, t, t^{3\sigma+4}) \mid t \in \mathbb{F}_{2^d}\} \cup \{(0,0,1), (0,1,0)\}$$

$$\sigma = 2^{\frac{d+1}{2}}$$

(iii) The translation hyperovals. Let $d > 1$ be an integer $\forall i \geq 1$, $\gcd(i, d) = 1$.

$$T_i = \{(1, t, t^{2^i}) \mid t \in \mathbb{F}_{2^d}\} \cup \{(0,0,1), (0,1,0)\}$$

HW 2: Prove S, $G1$, $G2$ are hyperovals in $PG(2, 2^d)$.