Inverses of the elements of a linear subspace and related problems

Bence Csajbók

University of Basilicata, Italy

Szeged, June 10-14, 2013

Inverse-closed additive subgroups in rings

Definition

For a subset S of a (unitary) ring let:

- S^* be the set of invertible elements in S,
- S^{-1} be the inverse set of S, that is $S^{-1} = \{s^{-1} : s \in S^*\}$.
- If $S^{-1} = S^*$, then S is called inverse-closed.

Theorem (Kroll, 1992)

Let V be a commutative, unitary, associative $\mathbb{K}$-algebra with $\mathrm{char}(\mathbb{K}) \neq 2$. If A is an inverse-closed $\mathbb{K}$-subspace in V and $1 \in A$, then A is a subalgebra of V.

Theorem (Goldstein, Guralnick, Small and Zelmanov, 2006)

Characterised pairs $A \subseteq D$, where A is an inverse-closed additive subgroup, D is a division ring with $\mathrm{char}(D) \neq 2$.

The field case

Definition

For a subset S of a field $\mathbb{F}$ we use the following notation:

- For $a \in \mathbb{F}$ let $aS = \{as : s \in S\}$, that is the elements of S multiplied by a,
- For an integer n, let $S^n = \{s^n : s \in S\}$, that is the set of n-th powers of the elements in S.

Lemma

Let $\mathbb{F}$ be a field of characteristic $p > 0$ and let k be a positive integer:

- *If $A \subseteq \mathbb{F}$ is subfield, then A^{p^k} is also a subfield of $\mathbb{F}$,*
- *if $A \subseteq \mathbb{F}$ is an additive subgroup, then A^{p^k} is also an additive subgroup.*

Theorem (Goldstein, Guralnick, Small and Zelmanov, 2006 and independently Mattarei, 2007)

Let A be an inverse-closed additive subgroup in a field $\mathbb{F}$, with characteristic $p \geq 0$, then:

1. *$p \neq 2$ and A is a subfield of $\mathbb{F}$ or $A = \epsilon\mathbb{K}$, where $\mathbb{K}$ is a subfield of $\mathbb{F}$, $\epsilon \notin \mathbb{K}$ and $\epsilon^2 \in \mathbb{K}$,*
2. *$p = 2$ and A is a $\mathbb{K}^2$-subspace of $\mathbb{K}$ for some subfield $\mathbb{K}$ of $\mathbb{F}$.*

These are indeed inverse-closed additive subgroups:

1. The inverse of ϵk is $\epsilon(\epsilon^2 k)^{-1}$, where $(\epsilon^2 k)^{-1}$ is in $\mathbb{K}$, so $A = \epsilon\mathbb{K}$ is inverse-closed.
2. The inverse of $a \in A$ is $a(a^2)^{-1}$, where $(a^2)^{-1} \in \mathbb{K}^2$ thus A is inverse-closed.

Hua's identity

Lemma (Hua's identity)

For invertible a, b such that $ab - 1$ is also invertible:

$$a - (a^{-1} + (b^{-1} - a)^{-1})^{-1} = aba.$$

It follows suddenly that if $1, a, b \in A$, that is an inverse-closed additive subgroup in a field $\mathbb{F}$, then $a^2, b^2, (a+b)^2 \in A$, thus also

$$(a+b)^2 - a^2 - b^2 = 2ab \in A.$$

So if $\mathrm{char}(\mathbb{F}) \neq 2$, then A is closed also to multiplication, hence it is a subfield of $\mathbb{F}$.

Theorem (BCs)

Let A be an infinite additive subgroup of the field $\mathbb{F}$, where $\mathrm{char}(\mathbb{F}) \neq 2$. If $|A \setminus A^{-1}| < |A|$, then A is inverse-closed.

Sketch of Proof.

Suppose, contrary to our claim, that there is an element $a \in A^* \setminus A^{-1}$. It can be proved that there exists an element $x \in A^*$ such that

$$x^2(2a)^{-1}, x^{-2}(2a)^{-1}, (x + x^{-1})^2(2a)^{-1} \in A.$$

Since A is an additive subgroup, this implies

$$(x + x^{-1})^2(2a)^{-1} - x^2(2a)^{-1} - x^{-2}(2a)^{-1} = a^{-1} \in A,$$

which contradicts the choice of a.

Again Hua's identity can be used:

$$a-(a^{-1}+(b^{-1}-a)^{-1})^{-1}=a^2b$$

$$\Downarrow$$

$$x-(x^{-1}+(2a-x)^{-1})^{-1}=x^2(2a)^{-1}, \tag{1}$$

$$x^{-1}-(x+(2a-x^{-1})^{-1})^{-1}=x^{-2}(2a)^{-1}, \tag{2}$$

$$(x+x^{-1})-((x+x^{-1})^{-1}+(2a-(x+x^{-1}))^{-1})^{-1}=(x+x^{-1})^2(2a)^{-1}, \tag{3}$$

hold for each $x \in \mathbb{F}$ when the elements of the set

$$\{x, x^{-1}, x+x^{-1}, (2a)^{-1}x-1, (2a)^{-1}x^{-1}-1, (2a)^{-1}(x+x^{-1})-1\}$$

are defined and non-zeros. One has to find an x such that the left-hand sides in (1), (2), (3) are in A ...

- The same result holds if $\mathrm{char}(\mathbb{F})=2$ and $1 \in A$.
- I don't known the answer if $1 \notin A$.

The finite field case

Theorem (Goldstein, Guralnick, Small and Zelmanov, 2006 and independently Mattarei, 2007)

Let A be a non-trivial inverse-closed additive subgroup of $\mathrm{GF}(q)$, with $q = p^n$, p prime. Then

- *A is either a subfield of $\mathrm{GF}(q)$ or*
- *$p \neq 2$ and A consists of all elements $x \in \mathrm{GF}(q)$ such that $x^{p^d} + x = 0$ for some $1 \leq d < n$ and $2d|n$.*

Consider $\mathrm{GF}(q^n)$ as an n-dimensional vector space over $\mathrm{GF}(q)$. We can identify the k-dimensional $\mathrm{GF}(q)$-subspaces of $\mathrm{GF}(q^n)$ with the $(k-1)$-dimensional projective subspaces of $\mathrm{PG}(n-1, q)$.

- If $m+1$ divides n, then let $\mathcal{P}_m$ be the m-dimensional subspace of $\mathrm{PG}(n-1, q)$ corresponding to $\mathrm{GF}(q^{m+1})$.
- If $2m+2$ divides n, then let $\mathcal{L}_m$ be the m-dimensional subspaces of $\mathrm{PG}(n-1, q)$ corresponding to the set of roots of $x^{q^{m+1}} + x = 0$.

When the inverse set is also an additive subgroup

Corollary (BCs)

Let A be a non-trivial additive subgroup of the field $\mathbb{F}$. Suppose that $A^{-1} \cup \{0\}$ is also an additive subgroup.

1. *If $\mathrm{char}(\mathbb{F}) \neq 2$, then A is a one-dimensional subspace over a subfield of $\mathbb{F}$,*
2. *If $\mathrm{char}(\mathbb{F}) = 2$, then $A = aB$, for some $a \in \mathbb{F}$, where B is a $\mathbb{K}^2$-subspace of $\mathbb{K}$ for some subfield $\mathbb{K}$ of $\mathbb{F}$.*

Corollary (BCs)

Let A be a non-trivial additive subgroup of $\mathrm{GF}(q)$. If $A^{-1} \cup \{0\}$ is also an additive subgroup, then A is a one-dimensional subspace over a subfield of $\mathrm{GF}(q)$. (In Case 2 above the map $x \to x^2$ is a field automorphism if $\mathbb{F}$ is finite.)

The Singer group

- For an element $x \in \mathrm{GF}(q^n)^*$ denote by $\langle x \rangle$ the point of $\mathrm{PG}(n-1,q)$ identified with the $\mathrm{GF}(q)$-subspace generated by x.
- With this notation $\langle x \rangle = \langle y \rangle$ iff $x/y \in \mathrm{GF}(q)$, i.e. $x^{q-1} = y^{q-1}$.
- Let α be a primitive element of $\mathrm{GF}(q^n)$. The collineation group generated by $\langle x \rangle \to \langle \alpha x \rangle$ is a cyclic Singer group G of $\mathrm{PG}(n-1,q)$, that is a cyclic collineation group of order $(q^n-1)/(q-1)$ permuting the points in one orbit. Moreover it also permutes the hyperplanes in one orbit.

- Let θ_n denote the number of points of $\mathrm{PG}(n, q)$, that is $\frac{q^{n+1}-1}{q-1}$.
- The points of $\mathrm{PG}(n-1, q)$ can be represented by $\{\alpha^0, \alpha^1, \alpha^2, \ldots, \alpha^{v-1}\}$, where $v = \theta_{n-1}$.
- A further identification with Z_v, that is the cyclic group of order v, can be made by $\alpha^j \leftrightarrow j$.
- Let $D = \{a_1, a_2, \ldots, a_k\} \subset Z_v$ be the set of elements corresponding to a hyperplane $\mathcal{H}$, hence $k = (q^{n-1} - 1)/(q - 1)$.
- Then $D + j = \{a_1 + j, a_2 + j, \ldots, a_k + j\} \subset Z_v$ corresponds to the hyperplane $\alpha^j\mathcal{H}$. Thus the translates of D correspond exactly to the hyperplanes of $\mathrm{PG}(n-1, q)$.

Difference Sets

Definition

Let G be a finite abelian group (written additively). We say that $D \subset G$ is a (v, k, λ)-difference set of G if $|G| = v$, $|D| = k$, and for each $0 \neq g \in G$, there are exactly λ pairs $d, d' \in D$ such that $d - d' = g$. The difference set $D \subset G$ is said to be cyclic if G is cyclic.

Note that if $D \subset G$ is a difference set, then $D + j$ is also a difference set.

Theorem (Singer – the classical Singer difference set)

In the cyclic group Z_{θ_n}, the set of elements D corresponding to a hyperplane of $\mathrm{PG}(n, q)$ is a $(\theta_n, \theta_{n-1}, \theta_{n-2})$-difference set.

Definition

A $2-(n,k,\lambda)$ block design is a set of v points arranged into b blocks of size k, where any 2 points are together on exactly λ blocks. A design is called symmetric (or square) if $v = b$.

Let $D \subset G$ be a (v,k,λ) difference set. We can define the points of a design as the elements of G, and the blocks as the translates of D, that are: $\{g + D : g \in G\}$. This construction gives a symmetric design with an automorphism group G acting regularly on the points (and blocks) of G.

Definition (Hall)

Let $D \subset G$ be an abelian difference set. A natural number, t is a (numerical) multiplier of D if $\gcd(t, |G|) = 1$ and $tD = D + j$ for some j.

- The function $x \to x^t$ is a permutation of the elements of $\mathrm{GF}(q^n)$ iff $\gcd(t, q^n - 1) = 1$,
- the function $\langle x \rangle \to \langle x^t \rangle$ is a permutation of the points of $\mathrm{PG}(n-1, q)$ iff $\gcd(t, \frac{q^n-1}{q-1}) = 1$.

Suppose that $x \to x^t$ permutes the elements of $\mathrm{GF}(q^n)$. If there exist two $(n-1)$-dimensional $\mathrm{GF}(q)$-subspace A and B such that $A^t = B$, then:

- t is a multiplier of the classical Singer difference set,
- the image of any $(n-1)$-dimensional $\mathrm{GF}(q)$-subspace is again an $(n-1)$-dimensional $\mathrm{GF}(q)$-subspace,
- $\langle x \rangle \to \langle x^t \rangle$ is a collineation of the associated $\mathrm{PG}(n-1, q)$.

It is widely studied when -1 is a multiplier of a difference set.

Theorem (Johnsen, 1963)

Let D be a non-trivial (v, k, λ)-difference set in an abelian group G. If -1 is a multiplier of D, then G is not cyclic. (Non-trivial means $0 < \lambda < k < v - 1$)

The proof relies on the simple fact that in the cyclic group Z_r, the map $g \to -g$ fixes one element if r is odd and two if r is even. While in the automorphism group of the associated design, if an involution fixes a point, then it fixes more than two points. This also implies that in $\mathrm{PG}(n, q)$ there is

- one inverse-closed point ($\mathcal{P}_0$) iff θ_n is odd, i.e. n is even
- and there are two ($\mathcal{P}_0$ and $\mathcal{L}_0$) iff n is odd.

Corollary

If A is an $(n-1)$-dimensional $\mathrm{GF}(q)$-subspace of $\mathrm{GF}(q^n)$, then A^{-1} is not an $(n-1)$-dimensional $\mathrm{GF}(q)$-subspace. (We have already known that since $\mathrm{GF}(q^n)$ does not contain $\mathrm{GF}(q^{n-1})$ if $n > 2$.)

Conjecture (McFarland): If -1 is a multiplier of an abelian (v, k, λ)-difference set D (assume $k < v/2$), then either $(v, k, \lambda) = (4000, 775, 150)$ or D is a Hadamard difference set, i.e. $(v, k, \lambda) = (4N^2, 2N^2 - N, N^2 - N)$.

Theorem (Pott: Finite Geometry and Character Theory)

Let D be a classical Singer difference set with parameters $(v, k, \lambda) = (\theta_n, \theta_{n-1}, \theta_{n-2})$. Then t is a multiplier of D if and only if $t \equiv p^k$ (mod v), for some k, where q is a power of the prime p.

- In $\mathrm{GF}(9^3)$ the map $x \to x^{61}$ takes 2-dimensional $\mathrm{GF}(9)$-subspaces into 2-dimensional $\mathrm{GF}(9)$-subspaces, since $61 \equiv 3^5$ (modulo $\frac{9^3-1}{9-1}$). But $61 \not\equiv 3^k$ (modulo $9^3 - 1$).

Corollary

Let A be an $(n-1)$-dimensional $\mathrm{GF}(q)$-subspace of $\mathrm{GF}(q^n)$. Then A^t is an $(n-1)$-dimensional $\mathrm{GF}(q)$-subspace if and only if $\gcd(t, q^n - 1) = 1$ and $t \equiv p^k$ (mod $\frac{q^n-1}{q-1}$) where q is a power of the prime p.

What is the inverse of a line?

Theorem (Hall, 1947)

Let $D \subset G$ be a cyclic $(n^2+n+1, n+1, 1)$-difference set. Then $\frac{1}{2}D$ and $2D$ are ovals if n is odd (and lines if n is even) in the associated design. (That is a projective plane with a Singer group, i.e. with a regular collineation group.)

- If ℓ is a line of $\mathrm{PG}(2,q)$, then ℓ^{-1} is a conic (Hall, 1974).

Theorem (Bruck, 1973 and Jungnickel, Vedder, 1984)

Let $D \subset G$ be an abelian $(n^2+n+1, n+1, 1)$-difference set. Then $-D$ is an oval, that is a set of $n+1$ points, no three of them collinear (this is maximal if n is odd).

- In general what is the t-th power of a k-dimensional subspace in $\mathrm{PG}(n,q)$?

When the "power of a hyperplane" is a quadric

Theorem (Jackson, Quinn, Wild, 1996)

Let ℓ be a line of $\mathrm{PG}(2,q)$, q is a power of an odd prime p and let r be any integer. The pointset ℓ^r is a (possibly degenerate) conic if there exist integers i,j,k such that one of the following holds:

1. $rp^k(q^i+q^j) \equiv 1 \pmod{q^2+q+1}$,
2. $rp^k \equiv 2 \pmod{q^2+q+1}$.

Theorem (Jackson, Quinn, Wild, 1996)

Let $\mathcal{H}$ be hyperplane of $\mathrm{PG}(n,q)$, q is a power of a prime p and let r be any integer. The pointset $\mathcal{H}^r$ is a (possibly degenerate) quadric if there exist integers i,j,k such that:

1. $rp^k(q^i+q^j) \equiv 1 \pmod{\theta_n}$.

The converse is true if $q=2$.

Theorem (Baker, Brown, Ebert, Fisher, 1994)

Let ℓ be a line of $\mathrm{PG}(2,q)$ and let $\gcd(r, q^2+q+1) = 1$, then

- $\ell^{1/r}$ *is a curve of degree* r,
- ℓ^{-r} *is a curve of degree* $2r$,
- ℓ^{r} *is a curve of degree* r.

Lemma (Faina, Kiss, Marcugini, Pambianco, 2002)

Let $\mathcal{H}$ be a hyperplane of $\mathrm{PG}(n,q)$, then $\mathcal{H}^{-1}$ is contained in a hypersurface of degree n.

Theorem (Faina, Kiss, Marcugini, Pambianco, 2002)

Let ℓ be a line of $\mathrm{PG}(n,q)$, then ℓ^{-1} is always an arc in some $\mathcal{P}_m$, where $m+1 | n+1$. (A k-arc in $\mathrm{PG}(n,q)$ is a set of k points such that $k \geq n+1$ and there are at most n points in each hyperplane. Note that $\mathrm{PG}(1,q)$ is an arc with this definition.)

Lemma (BCs)

If $\mathcal{A}$ is a k-dimensional subspace of $\mathrm{PG}(n,q)$, where $0 < k < n$, then $\mathcal{A}^{-1} \subseteq \mathrm{PG}(n,q)$ is the intersection of $\binom{n}{k+1}$ hypersurfaces of degree $k+1$.

(The equations come from the $(k+1) \times (k+1)$ subdeterminants of an $n \times (k+1)$ matrix.)
Typical application: If a line ℓ intersects $\mathcal{A}^{-1}$ in more than $k+1$ points, then (from Bézout) ℓ is contained in $\mathcal{A}^{-1}$, hence ℓ^{-1} is contained in $\mathcal{A}$ and we can use for example the previous result.

What is the $\mathrm{GF}(q)$-subspace generated by the r-th powers of a $\mathrm{GF}(q)$-subspace?

- In $\mathrm{PG}(2, 81)$ the map $\langle x \rangle \to \langle x^{5905} \rangle$ takes lines to lines, but the map $x \to x^{5905}$ is not a bijection on $\mathrm{GF}(81^3)$.

If we ask about the generated $\mathrm{GF}(q)$-subspace, then there is no difference in the answers.

Lemma

Let $x_1, x_2, \ldots, x_r$ be elements of a field $\mathbb{F}$ and define the following:

$$s_i(x_1, x_2, \ldots, x_r) := \sum_{1 \le j_1 < j_2 < \ldots < j_i \le r} (x_{j_1} + x_{j_2} + \ldots + x_{j_i})^r.$$

Then

$$\sum_{i=0}^{r-1} (-1)^i s_{r-i}(x_1, x_2, \ldots, x_r) = r! x_1 x_2 \ldots x_r.$$

For example:

$$(a+b+c)^3 - (a+b)^3 - (a+c)^3 - (b+c)^3 + a^3 + b^3 + c^3 = 6abc.$$

Let $\overline{A^r} := \{a_1 a_2 \ldots a_r : a_i \in A, \text{ for } i = 1, 2, \ldots, r\}$.
With the previous lemma we have proved the following:

Corollary

If $\mathrm{char}(\mathbb{F}) = 0$ *or* $\mathrm{char}(\mathbb{F}) > r$, *then* $\langle \overline{A^r} \rangle = \langle \{a^r : a \in A\} \rangle$.

Theorem (Hou, Leung, Xiang, 2001)

Let $s_{(r,n)}$ be the maximal number such that there is an $s_{(r,n)}$-dimensional $\mathrm{GF}(q)$-subspace W in $\mathrm{GF}(q^n)$ with the property $\langle \overline{W^r} \rangle \neq \mathrm{GF}(q^n)$. Then

$$s_{(r,n)} = \max_{k|n} k \left(\left\lfloor \frac{\frac{n}{k} - 2}{r} \right\rfloor + 1 \right).$$

The above theorem is a corollary of the following vector space analogous of Kneser's Addition Theorem in abelian groups:

Theorem (Hou, Leung, Xiang, 2001)

Let $E \subset K$ be fields and let A, B be finite-dimensional E-subspaces of K such that $A \neq \{0\}$, $B \neq \{0\}$. Suppose that every algebraic element in K is separable over E. Then

$$\dim_E AB \geq \dim_E A + \dim_E B - \dim_E H(AB),$$

where $H(AB) = \{x \in K : xAB \subseteq AB\}$ is the stabilizer of AB in K.

Large inverse-closed subsets in subspaces

The classification of spatial equifocused arcs relays on a result on additive subgroups in $\mathrm{GF}(q)$, which are inverse-closed apart from at most two non-zero elements.

Lemma (Korchmáros, Lanzone, Sonnino, 2010)

If A is an additive subgroup of $\mathrm{GF}(q)$, $q = 2^n$, with $|A| \geq 16$ and $1 \in A$, then $|A^* \cap A^{-1}| \geq |A^*| - 2$ implies that $A^* = A^{-1}$ and hence A is a subfield of $\mathrm{GF}(q)$.

- Let A be a non-trivial additive subgroup of $GF(q)$. How big the positive integer ϵ depending only on $|A|$ can be chosen such that $|A^* \cap A^{-1}| \geq |A^*| - \epsilon$ implies $A^* = A^{-1}$?
- In general: Let A and B be two non-trivial $\mathrm{GF}(q)$-subspaces in $\mathrm{GF}(q^n)$ with the same size. How big the positive integer ϵ depending only on $|A| = |B|$ can be chosen such that $|B^* \cap A^{-1}| \geq |B^*| - \epsilon$ implies $B^* = A^{-1}$?

Theorem (BCs)

Let A and B be two non-trivial d-dimensional $\mathrm{GF}(q)$-subspaces in $\mathrm{GF}(q^n)$. If $|B^* \cap A^{-1}| \geq \frac{2}{q}|B| - 1$, then $B^* = A^{-1}$ and both A and B are one-dimensional $\mathrm{GF}(q^d)$-subspaces.

If $q = 2$ then $B^* = A^{-1}$ is a trivial consequence of $|B^* \cap A^{-1}| \geq \frac{2}{q}|B| - 1 = |B^*|$. In this case the following theorem gives same result under a weaker condition.

Theorem (BCs)

Let A and B be non-trivial additive subgroups of $\mathrm{GF}(2^n)$ with the same size which is greater than or equal to four. If $|B \cap A^{-1}| \geq 3|B|/4$, then $B^* = A^{-1}$ and both A and B are one-dimensional subspaces over the same subfield of $\mathrm{GF}(2^n)$.

When the bound is sharp (q odd)

Both A^* and B^{-1} are union of one-dimensional $\mathrm{GF}(q)$-subspaces, hence the same holds for $A \cap B^{-1}$ (and $A \cap B^{-1}$ is divisible by $(q-1)$). Thus we can study the problem in $\mathrm{PG}(n-1,q)$, and searching for k-dimensional subspaces $\mathcal{A}$ and $\mathcal{B}$ such that $|\mathcal{B} \cap \mathcal{A}^{-1}| = 2(q^k-1)/(q-1)$.

Example

- Let A and B be two two-dimensional $\mathrm{GF}(q)$-subspaces of $\mathrm{GF}(q^n)$, that are lines ℓ and ℓ' in $\mathrm{PG}(n-1,q)$. We have that $\ell' \cap \ell^{-1}$ contains at most $2(\frac{|A|}{q}-1)/(q-1) = 2$ points or $\ell = \ell'$ and both A and B are one-dimensional $\mathrm{GF}(q^2)$-subspaces. The latter case cannot be when n is odd.
- If $n = 3$, then $|\ell' \cap \ell^{-1}| \leq 2$ for each line ℓ'. So ℓ^{-1} is a $(q+1)$-arc in $\mathrm{PG}(2,q)$, i.e. a conic if q is odd (due to Segre).
- This proves a previous result of Hall, and shows that the previous theorem is sharp for 2-dimensional $\mathrm{GF}(q)$-subspaces.

$\mathrm{PG}(3, q)$

Theorem (Ebert, 1985)

Let G denote the cyclic Singer group of $\mathrm{PG}(n-1, q)$. If $n = 2m+2$, then there is a subgroup H of order $q^{m+1}+1$ in G. If m is odd, then the orbits of H are caps (that is a set of points of $\mathrm{PG}(n-1, q)$, no three of which are collinear).

Let $m = 1$ and $Q := \{\langle x\rangle \in \mathrm{PG}(3, q) : x^{(q^2+1)(q-1)} = 1\}$, that is the orbit of H containing $\langle 1\rangle$. Since $\{x \in \mathrm{GF}(q^4) : x^{(q^2+1)(q-1)} = 1\}$ is a subgroup of the multiplicative group of $\mathrm{GF}(q^4)$, we have $Q = Q^{-1}$. In $\mathrm{PG}(3, q)$, with q odd, Barlotti and Panella (1955) independently showed that each cap of size q^2+1 is an elliptic quadric.

- This means that if q is odd, then Q is an inverse-closed elliptic quadric.

- If q is a prime power and $d+1$ divides n, then $\mathcal{P}_d = \{\langle x\rangle \in \mathrm{PG}(n-1,q) : x^{q^{d+1}} = x\}$.
- Similarly if q is odd and $2d+2$ divides n, then $\mathcal{L}_d = \{\langle x\rangle \in \mathrm{PG}(n-1,q) : x^{q^{d+1}} = -x\}$.

Let $\mathcal{A}$ be a d-dimensional subspace of $\mathrm{PG}(n-1,q)$. Then $\mathcal{A}^{-1}$ is a d-dimensional subspace iff $\mathcal{A}$ corresponds to a one-dimensional $\mathrm{GF}(q^{d+1})$-subspace of $\mathrm{GF}(q^n)$. We call these subspaces the cosets of $\mathcal{P}_d$. The one-dimensional $\mathrm{GF}(q^{d+1})$-subspaces of $\mathrm{GF}(q^n)$ are pairwise disjoint, so the cosets of $\mathcal{P}_d$ form a spread of $\mathrm{PG}(n-1,q)$ by d-spaces.

Lemma

For a point $\langle x \rangle \in \mathrm{PG}(3,q)$ we have $\langle x \rangle \in Q$ if and only if $\langle x^{q^2} \rangle = \langle x^{-1} \rangle$.

Proof. The point $\langle x \rangle$ is an element of Q if and only if $1 = x^{(q^2+1)(q-1)} = (x^{q^2})^{q-1} x^{q-1}$ or equivalently $(x^{-1})^{q-1} = (x^{q^2})^{q-1}$.

Lemma

If q is odd, then $Q \cap \mathcal{P}_1 = \{\mathcal{P}_0, \mathcal{L}_0\}$ and $Q \cap \mathcal{L}_1 = \emptyset$.

Proof. We have $\langle x \rangle \in \mathcal{P}_1 \cup \mathcal{L}_1$ if and only if $x^{2(q^2-1)} = 1$. On the other hand $\langle x \rangle \in Q$ if and only if $1 = x^{(q^2+1)(q-1)} = x^{2(q^2-1)(q-1)/2} x^{2(q-1)}$. This implies that $\langle x \rangle \in Q \cap (\mathcal{L}_1 \cup \mathcal{P}_1)$ if and only if $x^{2(q-1)} = 1$ and hence $x^{q-1} = 1$ and $\langle x \rangle = \mathcal{P}_0$ or $x^{q-1} = -1$ and $\langle x \rangle = \mathcal{L}_0$. If $x^{2(q-1)} = 1$, then $x^{2(q-1)(q+1)/2} = x^{q^2-1} = 1$ and hence $\mathcal{P}_0, \mathcal{L}_0 \in \mathcal{P}_1$.

Example (BCs)

If q is odd and $\mathcal{H}$ is a plane of $\mathrm{PG}(3,q)$, that contains $\mathcal{L}_1$, then $\mathcal{H} \cap \mathcal{H}^{-1} = (Q \cap \mathcal{H}) \cup \mathcal{L}_1$. If $\mathcal{H}$ contains $\mathcal{P}_0$ or $\mathcal{L}_0$, then $|\mathcal{H} \cap \mathcal{H}^{-1}| = q+2$, otherwise we have $|\mathcal{H} \cap \mathcal{H}^{-1}| = 2q+2$.

Proof. Since $\mathcal{P}_1 \cap \mathcal{L}_1 = \emptyset$, the line $\mathcal{P}_1$ cannot be contained in $\mathcal{H}$. Let $\mathcal{H} \cap \mathcal{P}_1 = \langle p_{\mathcal{H}} \rangle$ and for each $\langle x \rangle \in \mathcal{H} \setminus \{\mathcal{L}_1 \cup \langle p_{\mathcal{H}} \rangle\}$ let $\langle l_x \rangle := \mathcal{L}_1 \cap \langle x, p_{\mathcal{H}} \rangle$. There exist $a, b \in \mathrm{GF}(q)$, not both zero, such that $a l_x + b p_{\mathcal{H}} = x$. Taking q^2-th powers on both sides yields $-a l_x + b p_{\mathcal{H}} = x^{q^2}$ and hence $\langle x^{q^2} \rangle$ is a point of $\langle l_x, p_{\mathcal{H}} \rangle \subset \mathcal{H}$. Adding the first equation to the second yields $2b p_{\mathcal{H}} = x^{q^2} + x$. Here $b \neq 0$ since $\langle x \rangle \notin \mathcal{L}_1$, thus we have:

$$\langle p_{\mathcal{H}} \rangle = \langle x^{q^2} + x \rangle. \tag{4}$$

Since (4) holds also for $\langle x \rangle = \langle p_{\mathcal{H}} \rangle$ we have that it holds for each $\langle x \rangle \in \mathcal{H} \setminus \mathcal{L}_1$.

- First we show $\mathcal{H} \cap \mathcal{H}^{-1} \supseteq (Q \cap \mathcal{H}) \cup \mathcal{L}_1$.

If $\langle x \rangle \in \mathcal{L}_1$, then $\langle x^{-1} \rangle \in \mathcal{L}_1$ since $\mathcal{L}_1$ is inverse-closed. If $\langle x \rangle \in Q \cap \mathcal{H}$, then $\langle x^{q^2} \rangle \in \mathcal{H}$ and $\langle x^{-1} \rangle \in Q$ but since $\langle x \rangle \in Q$ we have $\langle x^{q^2} \rangle = \langle x^{-1} \rangle$ and hence $\langle x^{-1} \rangle \in Q \cap \mathcal{H}$, i.e. $Q \cap \mathcal{H}$ is inverse-closed.

- What are the tangent planes of Q on $\mathcal{L}_1$?

The only inverse-closed points of $\mathrm{PG}(3, q)$ are $\mathcal{P}_0$ and $\mathcal{L}_0$ thus if S is an inverse-closed pointset of $\mathrm{PG}(3, q)$, then $|S \setminus \{\mathcal{P}_0, \mathcal{L}_0\}|$ has to be even. Since q is odd, this implies that if $Q \cap \mathcal{H}$ is a non-singular conic, i.e. it has $q + 1$ points, then it cannot contain exactly one inverse-closed point. On the other hand we have $\langle \mathcal{P}_0, \mathcal{L}_0 \rangle = \mathcal{P}_1$ and $\mathcal{P}_1 \cap \mathcal{L}_1 = \emptyset$, hence $\mathcal{H}$ contains at most one of the inverse-closed points. It follows now that $\mathcal{H}$ is a tangent plane of Q if and only if it contains $\mathcal{P}_0$ or $\mathcal{L}_0$.

- Now we prove $\mathcal{H} \cap \mathcal{H}^{-1} \subseteq (Q \cap \mathcal{H}) \cup \mathcal{L}_1$.

Suppose that there is a point $\langle y \rangle \in (\mathcal{H} \cap \mathcal{H}^{-1}) \setminus \mathcal{L}_1$, this implies $\langle y^{-1} \rangle \in (\mathcal{H} \cap \mathcal{H}^{-1}) \setminus \mathcal{L}_1$. Applying (4) to $\langle y \rangle$ and $\langle y^{-1} \rangle$ yields $\langle y^{q^2} + y \rangle = \langle y^{-q^2} + y^{-1} \rangle$, or equivalently:

$$(y^{q^2} + y)^{q-1} = (y^{-q^2} + y^{-1})^{q-1}.$$

Multiply both sides by $(y^{q^2} + y)(y^{-q^2} + y^{-1})y^{q^3+q} \neq 0$ to obtain:

$$(y^{q^2}+y)^q(y^{-q^2}+y^{-1})y^{q^2+1}y^{q^3-q^2+q-1} = (y^{-q^2}+y^{-1})^q(y^{q^2}+y)y^{q(q^2+1)},$$

$$(y^{q^2} + y)^q(y + y^{q^2})y^{q^3-q^2+q-1} = (y + y^{q^2})^q(y^{q^2} + y),$$

$$(y^{q^2} + y)^{q+1}(y^{(q^2+1)(q-1)} - 1) = 0.$$

The first factor of the last equation cannot be zero since $\langle y \rangle \notin \mathcal{L}_1$ and this implies $\langle y \rangle \in Q$.
The size of $(Q \cap \mathcal{H}) \cup \mathcal{L}_1$ is $q + 2$ if $\mathcal{H}$ is a tangent of Q and $2q + 2$ otherwise, thus the same hold for $|\mathcal{H} \cap \mathcal{H}^{-1}|$. □

The same ideas work to prove the following:

Proposition (BCs)

If q is odd and $\mathcal{H}$ is a plane of $\mathrm{PG}(3,q)$ that contains $\mathcal{P}_1$, then $\mathcal{H} \cap \mathcal{H}^{-1} = (Q \cap \mathcal{H}) \cup \mathcal{P}_1$ and $|\mathcal{H} \cap \mathcal{H}^{-1}| = 2q$.

Lemma (BCs)

If $\mathcal{A}$ is a k-dimensional subspace of $\mathrm{PG}(n,q)$, where $0 < k < n$, then $\mathcal{A}^{-1} \subseteq \mathrm{PG}(n,q)$ is the intersection of $\binom{n}{k+1}$ hypersurfaces of degree $k+1$.

Theorem (Faina, Kiss, Marcugini, Pambianco, 2002)

Let ℓ be a line of $\mathrm{PG}(n,q)$, then ℓ^{-1} is always an arc in some $\mathcal{P}_m$, where $m+1 | n+1$. (A k-arc in $\mathrm{PG}(n,q)$ is a set of k points such that $k \geq n+1$ and there are at most n points in each hyperplane. So $\mathcal{P}_1$ is also an arc with this definition.)

It follows now that $\mathcal{B} \cap \mathcal{A}^{-1}$ cannot contain two different lines since their inverses would be contained in $\mathcal{A}$, hence they could not be arcs of $\mathrm{PG}(3, q) = \mathcal{P}_3$, thus they would be arcs in a coset of $\mathcal{P}_m$ for some m, where $m+1$ divides $n = 4$ and $m < 3$. This could happen only if $m = 1$ but this would be a contradiction since two cosets of $\mathcal{P}_1$ cannot have a common point and hence they cannot be contained in the same plane.

Theorem (BCs)

Let $\mathcal{A}$ and $\mathcal{B}$ be two planes of $\mathrm{PG}(3, q)$.

1. *If $|\mathcal{B} \cap \mathcal{A}^{-1}| > q + 1 + \lfloor 2\sqrt{q} \rfloor$, then $|\mathcal{B} \cap \mathcal{A}^{-1}| \in \{2q, 2q+1, 2q+2\}$.*
2. *We have $|\mathcal{A} \cap \mathcal{A}^{-1}| = 2q$ if and only if $\mathcal{P}_1 \subset \mathcal{A}$.*
3. *We have $|\mathcal{A} \cap \mathcal{A}^{-1}| = 2q+2$ if and only if $\mathcal{L}_1 \subset \mathcal{A}$ and $\mathcal{P}_0, \mathcal{L}_0 \notin \mathcal{A}$.*
4. *There are no planes $\mathcal{A}, \mathcal{B}$ that satisfies $|\mathcal{B} \cap \mathcal{A}^{-1}| = 2q+1$. (We prove only for $\mathcal{A} = \mathcal{B}$.)*

Proof. Denote the cubic curve $\mathcal{B} \cap \mathcal{A}^{-1}$ by $\mathcal{F}$. The condition in 1 implies $N_q(\mathcal{F}) > q + 1 + \lfloor 2\sqrt{q} \rfloor$, where $N_q(\mathcal{F})$ is the number of rational points of the curve $\mathcal{F}$. This means that the Hasse-Weil bound does not hold and hence $\mathcal{F}$ is reducible over some extension of $\mathrm{GF}(q)$. $\mathcal{F}$ cannot contain more than one rational line and hence it has to be the union of a line ℓ and a non-degenerate conic $\mathcal{C}$. Depending on the mutual position of ℓ and $\mathcal{C}$, this implies $|\mathcal{B} \cap \mathcal{A}^{-1}| \in \{2q, 2q+1, 2q+2\}$.
If $|\mathcal{A} \cap \mathcal{A}^{-1}| \in \{2q, 2q+1, 2q+2\}$, then $\mathcal{A}$ and $\mathcal{A}^{-1}$ contain the same line denoted by ℓ. The inverse of this line ℓ^{-1} is not an arc of $\mathrm{PG}(3, q)$, hence it is a coset of $\mathcal{P}_1$. Now $\mathcal{A}^{-1}$ contains both lines ℓ and ℓ^{-1} and hence $\ell = \ell^{-1}$. This implies that ℓ is inverse-closed and hence it is $\mathcal{P}_1$ or $\mathcal{L}_1$.
Our previous results describe the cubic curve $\mathcal{A} \cap \mathcal{A}^{-1}$, when $\mathcal{A}$ contains an inverse-closed line and hence the remaining statements follow. □

The Lang-Weil bound

A projective algebraic set $X \subseteq \mathrm{PG}(n, q)$ is said to be geometrically irreducible (or projective variety) if there is no decomposition $X = X_1 \cup X_2$, with X_1 and X_2 projective algebraic sets defined over the algebraic closure of $\mathrm{GF}(q)$ such that $X_i \neq X$ for $i = 1, 2$. Let X be a projective algebraic set and denote with $N_q(X)$ the number of rational points of X, then the Lang-Weil inequailty says that if X is a projective variety of dimension r and degree d, then:

$$|N_q(X) - q^r| \leq (d-1)(d-2)q^{r-1/2} + C(n, r, d)q^{r-1}, \tag{5}$$

where $C(n, r, d)$ depends only on n, r, d and not on the field $\mathrm{GF}(q)$.

Let $\mathcal{A}$ and $\mathcal{B}$ be k-dimensional subspaces of $\mathrm{PG}(n,q)$ with $k \geq 3$ such that $B^* \neq A^{-1}$. It follows now from the Lang-Weil inequailty and from one of our previous Lemma that if $\mathcal{B} \cap \mathcal{A}^{-1}$ is geometrically irreducible and q is large enough with respect to n and k, then $|\mathcal{B} \cap \mathcal{A}^{-1}|$ cannot reach the bound $2(q^k-1)/(q-1)$ in our theorem.

- Sandro Mattarei told me that he has a proof for that the bound arising from the Lang-Weil inequality holds for $|\mathcal{B} \cap \mathcal{A}^{-1}|$ when $k > 3$ (and q is large enough) and $|\mathcal{B} \cap \mathcal{A}^{-1}| = 2(q^k-1)/(q-1)$ only if $k \leq 3$. (I have not seen the whole proof yet.)

THANK YOU

THANK YOU FOR YOUR ATTENTION