LE MATEMATICHE
Vol. LII (1997) – Fasc. I, pp. 127–140

STRUTTURE PSEUDO-EUCLIDEE SU CAMPI DI GALOIS

FERNANDO DI GENNARO - FRANCO EUGENI

In this paper we define an inner product in an affine plane $AG(2, q)$. The odd case, in a canonical rapresentation, is connected with a geometry studied by Tallini. The even case is very new since, the inner product cannot be commutative and we have an ordered perpendicularity. Finally we applied theese questions to construct a criptographic authentication system.

1. Introduzione.

Negli anni '70 G. Tallini presenta una sua idea per generalizzare la costruzione delle Geometrie Euclidee al caso delle geometrie affini di Galois. La costruzione di Tallini, limitata al caso di piani di Galois d'ordine dispari, può essere riassunta nel modo che segue.
Consideriamo l'anello Z_p delle classi resto modulo p (p, primo dispari) ed indichiamo con $\mathbf{F} = GF(p^n)$ una qualunque estensione algebrica d'ordine n di Z_p. Nell'insieme $\mathbf{F} \times \mathbf{F}$ introduciamo $\forall (x, y) \in \mathbf{F} \times \mathbf{F}$ la forma:

$$N(x, y) = x^2 - \theta y^2$$

ove θ è un non-quadrato di $\mathbf{F}$. La forma $N(x, y)$ si chiama la "norma" del punto. Risulta:

$$N(x, y) = 0 \Leftrightarrow x = y = 0.$$

Entrato in Redazione il 19 dicembre 1996.

Dunque la forma è a valori in $\mathbf{F}$ ed è definita non nulla (sarà intuitivamente pensata come una generalizzazione del quadrato della distanza euclidea). Si prova facilmente che gli automorfismi di $\mathbf{F} \times \mathbf{F}$, che mutano in sè la forma quadratica, formano un gruppo di trasformazioni e quindi danno luogo ad una "geometria" che diremo a "struttura pseudo-euclidea". Tale geometria "mutatis mutandis" non è molto diversa dalla classica. Il Tallini nel suo lavoro generalizza al caso molte delle idee classiche dalla nozione di bisettrice di due rette fino alla classificazione pseudo-euclidea delle coniche. Una differenza sostanziale che appare "al primo livello di esame" della struttura è la circostanza che due rette incidenti possono o non possono avere rette bisettrici, in accordo che una certa espressione sia o non sia un quadrato nel campo; di conseguenza esistono coniche senza assi, e per questo rimandiamo al lavoro originale.
Le definizioni e la teoria di Tallini per lo sviluppo di queste geometrie pseudo-euclidee non sono estensibili al caso di campi di Galois d'ordine pari in quanto ogni elemento di $GF(2^n)$ è un quadrato; in particolare la definizione di norma data sopra, punto di partenza e cardine della teoria di Tallini, non ha significato nel caso pari.
Come vedremo le difficoltà, ai fini di definire una struttura pseudoeuclidea nel caso pari, si superano ma sono in un certo qual senso di ordine più riposto.
In questo lavoro, ponendoci da un punto di vista più generale, ci preoccuperemo di introdurre assiomaticamente un prodotto interno a valori in $\mathbf{F}$, che soddisfi i seguenti requisiti:

1) Il prodotto interno sia una forma bilineare a valori in $\mathbf{F}$.
2) Il prodotto interno sia indifferentemente definito sia nel caso di campi di ordine pari sia nei casi di ordine dispari.
3) Il prodotto interno induca una "norma" intesa come forma quadratica definitivamente non nulla.
4) Esista una particolare base, da dirsi "canonica", rispetto alla quale, nel caso dispari, si ritrovi la norma di Tallini.

Si prova che un tale prodotto interno è definibile, e se ne trova l'espressione generale. Si determina anche una base speciale che viene detta pseudo-canonica, rispetto alla quale la norma nel caso dispari è quella di Tallini e quella del caso pari da luogo a "circonferenze" che di fatto coincidono con le famiglie di coniche di Denniston, con le quali furono costruiti gli oramai esempi classici di archi massimali. Per questo la norma pseudo-canonica del caso pari viene da noi chiamata "norma di Denniston". La definizione introdotta ci sembra anche essere supportata da altre analogie in quanto, nel caso pari, gli elementi di categoria zero e di categoria uno del campo giocano un ruolo analogo a quello, che nel caso dispari, giocano i quadrati e i non quadrati del campo.

Tuttavia nel caso pari – a differenza del caso dispari – si presenta un

incoveniente non trascurabile, il prodotto che introduciamo è irrimediabilmente non-commutativo. Questa circostanza non è perfettibile in quanto, per altra via, è ben noto che in un piano affine d'ordine pari non esistono perpendicolarità (che sarebbero indotte da un prodotto commutativo). L'esistenza di un prodotto interno non commutativo implica conseguenze varie tra le quali, ad esempio, una "perpendicolarità ordinata" sulla quale è interessante indagare. Così esiste la perpendicolare da un punto verso una retta e da una retta verso il punto ed esistono due piedi di perpendicolari.
Nel paragrafo relativo alle applicazioni questa "negatività" viene utilizzata ai fini della costruzione crittografica di un complesso sistema di autenticazione, a nostro avviso "molto più sicuro" di quelli usualmente adottati.

2. Una definizione di pseudo-prodotto interno su $\mathbf{F} \times \mathbf{F}$.

Sia $\mathbf{F} = GF(q)$ un campo di Galois di ordine q qualsiasi. Distinguendo il caso pari dal caso dispari poniamo:

$$F_0 = F_0(q) = \left\{a : a \in F,\ \exists x \in F \text{ con } x^2 = a, q \text{ dispari}\right\}.$$

Analogamente, se q è pari, poniamo:

$$F_0 = F_0(q) = \left\{d : d \in F,\ \exists x \in F \text{ con } x^2 + x + d = 0, q \text{ pari}\right\}.$$

Porremo inoltre, quale che sia q

$$F_1 = F \setminus F_0.$$

Nel caso dispari gli elementi di F_0 si chiamano "i quadrati" del campo e quelli dell'insieme complementare F_1 "i non-quadrati"; analogamente se q è pari gli elementi di F_0 si diranno di "categoria zero" e quelli dell'insieme complementare F_1 di " categoria uno". Risulta inoltre:

$$|F_0| = (q+1)/2 \quad \text{se } q \text{ è dispari}$$
$$|F_0| = q/2 \quad \text{se } q \text{ è pari}$$

È ben noto che quale che sia q, l'insieme F_0 è chiuso rispetto alla moltiplicazione, anzi risulta:

$$F_0F_0 = F_1F_1 = F_0\ ,\ F_0F_1 = F_1F_0 = F_1\ .$$

Quale che sia q, prefissato $\theta \in F_1$, definiamo la *norma* (rispetto a θ) di un elemento del campo, ponendo:

$$|a| = \begin{cases} a & \text{se } a \in F_0 \\ \theta a & \text{se } a \notin F_0 \end{cases}$$

la norma essendo un elemento di F_0.

Osservazione. Forniamo due esempi di "norma" in $\mathbf{F} \times \mathbf{F}$ la prima nel caso pari, la seconda nel caso dispari. Prefissato $\theta \in F_2$, consideriamo le due forme quadratiche definite ponendo:

$$\gamma = x^2 - \theta y^2 \qquad q \text{ dispari} \quad (\text{"norma" di Tallini})$$
$$\gamma = x^2 + xy + \theta y^2 \quad q \text{ pari} \qquad (\text{"norma" di Denniston}).$$

Esse si annullano in $\mathbf{F}$, se e solo se $x = y = 0$. La seconda forma quadratica è stata da noi chiamata norma di Denniston poichè le circonferenze che ne derivano sono i più che famosi "fasci di Denniston" da lui utilizzati per la costruzione del suo omonimo arco. (cf. [1]).

Denotiamo con $\mathbf{V} = VG(2, q)$ lo spazio vettoriale di dimensione due sul campo $\mathbf{F}$ e poniamo la seguente definizione.

Definizione 1. Si dice *pseudo-prodotto interno* su $\mathbf{V}$, una legge:

$$f : \mathbf{V} \times \mathbf{V} \to \mathbf{F}$$

che a due vettori $u, v \in \mathbf{V}$ associa l'elemento $f(u, v)$ di $\mathbf{F}$, indicato con $u * v$, tale che:

a) la forma f è bilineare, cioè $\forall u, v, w \in \mathbf{V}$ e $\forall \lambda \in \mathbf{F}$:

$$(1) \qquad u * (v + w) = u * v + u * w$$
$$(2) \qquad (v + w) * u = v * u + w * u$$
$$(3) \qquad (\lambda u) \quad * \quad v = u * (\lambda v) = \lambda(u * v);$$

b) la forma $f(u, u) = u * u$ è nulla se e solo se u è il vettore nullo;

c) se $u \neq v$, allora $f(u, v) - f(v, u) = 0, 1$ in accordo con il fatto che q sia dispari o pari.

Come è usuale se $\{e_1, e_2\}$ è una base di $\mathbf{V}$ e se si pone

$$u = xe_1 + ye_2$$
$$v = x'e_1 + y'e_2$$
$$e_i * e_j = a_{ij}, \quad i, j = 1, 2$$

allora risulta:

$$\begin{aligned} u * v &= (xe_1 + ye_2) * v = x(e_1 * v) + y(e_2 * v) = \\ &= x\Big[e_1 * \Big(x'e_1 + y'e_2\Big)\Big] + y\Big[e_2 * \Big(x'e_1 + y'e_2\Big)\Big] = \\ &= xx'e_1 * e_1 + xy'e_1 * e_2 + yx'e_2 * e_1 + yy'e_2 * e_2 = \\ &= xx'a_{11} + xy'a_{12} + yx'a_{21} + yy'a_{22}\,. \end{aligned}$$

Definizione 2. Una base ordinata (e_1, e_2) si dice *pseudo-canonica* se

$$e_1 * e_1 = 1,\ e_2 * e_2 = -\theta,\ e_1 * e_2 = \varepsilon,\ e_2 * e_1 = 0$$

essendo $\theta \in F_1$ ed $\varepsilon = 0$ *oppure* 1 secondo che q sia dispari o pari.

Teorema. *L'espressione di uno pseudo-prodotto interno rispetto ad una base canonica è la seguente:*

$$u * v = xx' - \theta yy' \qquad \textit{se } q \textit{ è dispari}$$
$$u * v = xx' + xy' + \theta yy' \quad \textit{se } p \textit{ è pari.}$$

(Si noti che le norme associate sono quelle di Tallini e Denniston).

Dimostrazione. Sia q dispari, allora dalla espressione:

$$u * v = a_{11}xx' + a_{12}xy' + a_{21}x'y + a_{22}yy'$$

per essere

$$a_{11} = e_1 * e_1 = 1\ , \quad a_{22} = e_2 * e_2 = -\theta$$
$$a_{12} = a_{21} = 0$$

risulta

$$u * v = xx' - \theta yy'$$

Nel caso pari, procedendo in modo analogo, si ottiene:

$$u * v = xx' + xy' - \theta yy'. \qquad \square$$

Gli obiettivi posti nell'introduzione sono così raggiunti e rimane da analizzare qualche conseguenza.
La proprietà c) della Definizione 1, asserendo che $f(u, v) - f(v, u) = 1$, rimarca la non commutività dello pseudo-prodotto interno nel caso pari.
Nel seguito chiameremo *piano pseudo-euclideo* su F la coppia costituita dal piano affine $\mathbf{F} \times \mathbf{F}$ e da uno pseudo-prodotto interno definito su di esso.
Il prodotto induce una norma, cioè una funzione:

$$N : V \times V \to F$$

definita ponendo, $\forall u, v \in V$

$$N(u, v) = (u - v) * (u - v).$$

Se $u = xe_1 + ye_2$ e se $v = 0$, e la base (e_1, e_2) è una base pseudo-canonica, allora si ha:

$$N(u, 0) = \begin{cases} x^2 - \theta y^2 & \text{per } q \text{ dispari} \\ x^2 + xy + \theta y^2 & \text{per } q \text{ pari} \end{cases}$$

In un piano pseudo-euclideo si può definire la "norma di due punti" ponendo :

$$N(P_1, P_2) = N(P_1 P_2, 0).$$

Dall'espressione del vettore

$$P_1 P_2 = (x_2 - x_1)e_1 + (y_2 - y_1)e_2$$

si ricava

$$N(P_1, P_2) = a_{11}(x_2 - x_1)^2 + (a_{12} + a_{21})(x_2 - x_1)(y_2 - y_1) + a_{22}(y_2 - y_1)^2.$$

Nel caso dispari lo pseudo-prodotto definisce una perpendicolarità del tutto analoga alla classica. Nel caso pari si hanno cambiamenti notevoli. Diremo in generale che due vettori u e v di un piano pseudo-euclideo d'ordine pari sono *perpendicolari nel verso v verso u*, se $u * v = 0$. Si scrive:

$$u \underset{\leftarrow}{\perp} v \quad \Leftrightarrow \quad u * v = 0.$$

(Nel caso dispari questa definizione di perpendicolarità ordinata sussiste ugualmente, ma essendo simmetrica, include in se anche l'ordinamento opposto).

3. Osservazioni sulla geometria indotta nella norma.

Supponiamo di essere nel *caso q dispari*; consideriamo in $\mathbf{F} \times \mathbf{F}$ lo pseudo-prodotto interno definito da:

$$(x, y) * (x', y') = xx' - \theta yy'$$

che come noto induce la norma di Tallini definita da

$$N(x, y) = x^2 - \theta y^2.$$

Cominciamo con l'osservare che, dati due punti $Q = (a, b)$ ed $\Omega = (\alpha, \beta)$, il luogo dei punti $P = (x, y)$ tali che

$$N(P, Q) = N(P, \Omega)$$

è la retta di equazione

$$(\Lambda) \qquad 2(\alpha - a)x - 2\theta(\beta - b)y = N(\Omega, O) - N(Q, O).$$

Tale retta definisce la direzione del vettore $(\theta(\beta - b), (\alpha - a))$ che rispetto al vettore $((\alpha - a), (\beta - b))$ risulta ortogonale per essere i due vettori ortogonali. Si verifica dunque una situazione del tutto analoga al caso reale classico e la retta (Λ) ha tutto il diritto di assumere il nome di *asse del segmento* $Q\Omega$.
Inoltre la retta $Q\Omega$ è incontrata dall'asse (Λ) nel punto di coordinate

$$\left[\left(a + \alpha\right)/2, \left(b + \beta\right)/2\right],$$

dove $1/2$ è l'inverso di 2 nel campo. Tale punto, *per abuso di linguaggio*, sarà ancora detto *punto medio*.
In modo analogo si consideri la circonferenza di centro Ω e raggio R data da:

$$(x - \alpha)^2 - \theta\,(y - \beta)^2 = R^2.$$

Osserviamo ancora che se un punto Q è pensato sulla circonferenza allora la retta tangente in Q, come si prova con semplici calcoli, ha equazione:

$$(\alpha - a)\,x - \theta\,(\beta - b)\,y = \overline{\Omega O} * \overline{QO} - R^2.$$

Si prova subito, calcolando lo pseudo-prodotto interno delle direzioni, che tale retta tangente, come nel caso classico, è ortogonale alla retta ΩQ che congiunge centro e punto di tangenza.
Ben diverso è il *caso q pari*. Consideriamo per questo in $\mathbf{F} \times \mathbf{F}$ lo pseudo-prodotto interno definito da

$$(x, y) * (x', y') = xx' + xy' + \theta yy'$$

che induce la sopra definita norma di Denniston data da:

$$N(x, y) = x^2 + xy + \theta y^2.$$

Procedendo come sopra a partire da due punti dati

$$Q = (a, b),\ \Omega = (\alpha, \beta),$$

il luogo dei punti $P = (x, y)$ tali che

$$N(P, Q) = N(P, \Omega)$$

è, in tal caso, la retta di equazione

$$(b+\beta)x + (a+\alpha)y = N(\Omega, O) + N(Q, O).$$

Tale retta ha un comportamento molto differente rispetto al caso dispari visto sopra. Essa risulta parallela alla retta per Ω e Q che ha equazione (essendo $+1 = -1$)

$$(b+\beta)(x+a) + (a+\alpha)(y+b) = 0.$$

Non è lecito dunque parlare di asse di un segmento in modo analogo al caso classico e non ha senso parlare di punto medio in accordo con la circostanza che 2 non è invertibile.
Ancora si consideri la circonferenza di centro Ω e raggio R data da:

$$(x-\alpha)^2 + (x-\alpha)(y-\beta) + \theta(y-\beta)^2 = R^2.$$

Procediamo in modo analogo al precedente caso e pensiamo Q sulla circonferenza. La retta tangente in Q, come si prova con semplici calcoli, è data da:

$$(b+\beta)(x+a) + (a+\alpha)(y+b) = 0.$$

Ma nel caso pari, in primo luogo e come è ben noto, tutte le tangenti ad una conica passano per un punto fisso Ω detto il NUCLEO della conica. Nel nostro caso si vede che il nucleo della circonferenza in esame coincide con il centro della stessa. Dunque le rette per il centro in questo caso, con differenza dal caso classico, sono tutte 1-secanti e quindi al tempo stesso raggi e tangenti. Si perde così completamente il significato della perpendicolarità tra tangente e raggio dal momento che nel caso pari non sussiste nemmeno con la perpendicolarità ordinata.
Le osservazioni fatte riguardo le due nozioni di asse di un segmento e perpendicolarità raggio-tangente in un punto di una circonferenza, ancora valide nel caso dispari e prive di senso nel caso pari sono sufficienti a mostrare la profonda differenza tra i due ambienti.

4. Norma punto-retta, perpendicolarità ordinata e piedi di una perpendicolare (ordinata).

Sia data una retta r di equazione:

$$ax + by + c = 0$$

e un punto $P_0(x_0, y_0)$ fuori di essa. Una generica retta r' per P_0, che supponiamo incidente r, ha equazioni parametriche:

$$x = lt + x_0 \qquad y = mt + y_0.$$

Il punto P' comune alle due rette ha coordinate

$$P' = [x_0 + l(B/A), y_0 + m(B/A)]$$

essendo

$$-B = ax_0 + by_0 + c; \quad A = al + bm$$

con $A \neq 0$ per essere le due rette non parallele. Risulta

$$N(P_0, r) = N(P', P_0) = N[l(B/A), m(B/A)].$$

Distinguiamo ora i due casi:

I CASO. Sia q dispari. La condizione di perpendicolarità delle due rette, condizione simmetrica nel caso dispari, è data da

$$(+b, -a) * (l, m) = bl + \theta am = 0$$

da cui: $l = \rho\theta a$, $m = -b\rho$ (essendo $\rho \neq 0$, un fattore di proporzionalità).
Definiamo la norma *punto P_0-retta r* come la norma di P_0 dal piede P' della perpendicolare, precisamente risulta:

$$N(P_0, r) = B^2/A^2(l^2 - \theta m^2) = B^2\rho^2(\theta^2 - \theta b)/\rho^2(\theta a^2 - b^2)^2 =$$

$$= B^2\theta/(\theta a^2 - b^2) = -B^2\theta/N(b, a)$$

da cui:

$$N(P_0, 0) = \theta \frac{(ax_0 + by_0 + c)^2}{N(b, a)} .$$

Discende allora che date due rette $ax + by + c = 0$, $\alpha x + \beta y + \gamma = 0$ incidenti, il luogo dei punti aventi ugual norma rispetto alle due rette è dato dalla conica:

$$(E) = \frac{(ax + by + c)^2}{a^2\theta - b^2} = \frac{(\alpha x + \beta y + \gamma)^2}{\alpha^2\theta - \beta^2}$$

che è degenere in due rette, allora e allora soltanto che l'elemento di F

$$\varphi = (\alpha^2\theta - \beta^2)/(a^2\theta - b^2)$$

sia un quadrato del campo. La precedente è dunque anche la condizione di esistenza delle "bisettrici" di due rette date. Se φ non è un quadrato la (E) è una forma quadratica nulla solo sul punto comune alle due rette date.

II CASO. Sia ora q pari. Dobbiamo distinguere due differenti condizioni di perpendicolarità.
La prima condizione, che diremo perpendicolarità di $I^{\wedge}$ specie esprime la perpendicolarità da P_0 verso r. Tale perpendicolarità con riferimento alla coppia ordinata di rette (r', r) esprime nella coppia la perpendicolarità di r' verso r. Si ha in tal caso:

$$r' \lfloor r \qquad \Leftrightarrow \qquad bl + al + \theta am = 0$$

Calcoliamo $N(P_0, r)$ sotto la perpendicolarità $r' \lfloor r$ di $I^{\wedge}$ specie. Si ha dalla condizione di perpendicolarità scritta sopra:

$$l = -\rho\theta a \ , \ m = \rho(a + b) \ , \ \rho \neq 0.$$

Segue allora:

$$A^2 = (al + bm)^2 = \rho^2(\theta^2 a^4 + a^2 b^2 + b^4) = \rho^2 \quad N^2(b, a)$$

e quindi:

$$N\,(P_0, r) = N\,(lB/A, mB/A) = B^2\rho^2\left(l^2 - \theta m^2\right)/A^2 =$$

$$= B^2\rho^2\left(\theta^2 a^2 - \theta b^2\right)/\rho^2\left(\theta a^2 - b^2\right)^2 = B^2\theta/\left(\theta a^2 - b^2\right)$$

da cui

$$N(P_0, r) = (-\theta)\frac{(ax_0 + by_0 + c)^2}{N(b, a)}$$

$$(E) = \frac{(ax + by + c)^2}{a^2\theta - b^2} = \frac{(\alpha x + \beta y + \gamma)^2}{\alpha^2\theta - \beta^2}$$

$$N\,(P_0, r) = N[l\,(B/A)\,, m\,(B/A)] = \left(B^2/A^2\right)\left(l^2 + lm + \theta m^2\right).$$

La seconda condizione che diremo perpendicolarità di $II^{\wedge}$ specie esprime la perpendicolarità da r verso P_0. Tale perpendicolarità con riferimento alla coppia ordinata di rette (r', r) esprime nella coppia la perpendicolarità di r verso r'. Si ha in tal caso:

$$r \lfloor r' \qquad \Leftrightarrow \qquad bl + bm + \theta am = 0.$$

La condizione $r \lfloor r'$ implica $l = \rho(b - \theta a)$, $m = -\rho b$ e quindi

$$N(P_0, r) = \frac{B^2\rho^2(\theta^2 a^2 + \theta ab + \theta b^2)}{\rho^2(ab + \theta a^2 - b^2)^2} = \frac{\theta B^2}{N(b, a)}$$

e quindi ancora

$$N(P_0, r) = \frac{\theta(ax_0 + by_0 + c)^2}{N(b, a)} .$$

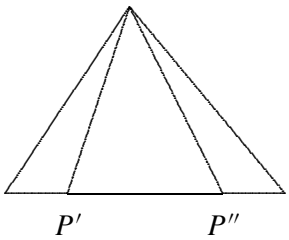
Da questa formula discende una formula per le bisettrici di $I^\wedge$ specie che sono quelle per le quali la perpendicolarità usata per il calcolo della norma punto-retta è di prima specie.
La seconda condizione esprime la perpendicolarità da r' verso r. Si ha ora:

$$r \lfloor r' \qquad \Leftrightarrow \qquad bl + bm + \theta am = 0.$$

Ripetiamo il calcolo per la perpendicolarità di $II^\wedge$ specie $r' \lfloor r$ implica $l = \rho\theta a$, $m = \rho(b - a)$ segue allora

$$N(P_0, r) = \frac{B^2\rho^2(\theta'' a^2 + \theta ab - \theta b^2)}{\rho^2(ab + \theta a^2 - b^2)^2} = \frac{\theta B^2}{N(b, a)} .$$

Ci si può porre il problema della determinazione dei due differenti piedi di perpendicolari esistenti in questo caso.



È semplice utilizzando le formule in questione che il punto P' piede della perpendicolare di $I^\wedge$ specie è

$$P' = [x_0 + l\,(B/A)\,,\, y_0 + m\,(B/A)]$$

con $l(B/A) = [(b - \theta a)B]/N(b, a), m(B/A) = bB/N(b, a)$ e ponendo $t_0 = B/N(b, a)$

$$P' = [x_0 + (b - \theta a)t_0,\ y_0 + bt_0]\,.$$

Il punto P'' piede della perpendicolare di $II^{\wedge}$ specie è

$$P'' = [x_0 + l(B/A),\ y_0 + m(B/A)]$$

con $l(B/A) = [\theta aB]/N(b, a), m(B/A) = (b - a)B/N(b, a)$ e ponendo $t_0 = B/N(b, a)$

$$P'' = [x_0 + \theta at_0,\ y_0 + (b - a)t_0]\,.$$

È interessante valutare la norma dei due piedi, e verificare che essa è proporzionale alla norma di P_0 verso r. Infatti si ha:

$$N(P', P'') = (bt_0, at_0) = b^2t_0^2 + abt_0^2 + \theta a^2t_0^2 = t_0^2N(b, a) = B^2/N(b, a)$$

e quindi:

$$\theta N(P', P'') = N(P_0, r)$$

che esprime il legame con la norma punto-retta.

5. Applicazioni.

È ben noto il procedimento con cui si può costruire un metodo di autenticazione geometrico.
Consideriamo un piano affine di Galois $AG(r, q)$ con $q = 2^n$ pari. Identifichiamo i messaggi con i punti impropri del tipo: $m_1(0, 1, m)$ e fissata come chiave un punto $P_0(x_0, y_0)$ prendiamo come autenticatore la retta

$$y - y_0 = m(x - x_0)$$

cioè inviamo la coppia

$$(\textit{messaggio-autenticatore}) = (m,\ y_0 - mx_0).$$

Un utente che non conosca la chiave e vuole modificare di colpo sia m che $y_0 - mx_0$ può soltanto cercare di scegliere un punto tra i 2^n punti affini della retta

$$y = mx + (y_0 - mx_0)$$

e per questo ha probabilità di riuscita $1/2^n$. Quindi il metodo è sicuro a meno di non disporre di due autenticatori fatti con la stessa chiave perchè allora dati

$$(m, y_0 - mx_0) \quad (m', y_0 - m'x_0)$$

dall'intersezione delle due rette

$$y = mx + (y_0 - mx_0) \quad y = m'x + (y_0 - m'x_0)$$

si determina la chiave.
Se si aggiunge in $AG(r, 2^n)$ la struttura pseudo-euclidea si può eliminare l'inconveniente nella maniera che segue.
Dato il messaggio $(m) = (0, 1, m)$ fissiamo con la chiave $K = (x_0, y_0)$ una seconda chiave $K' = (x_0, y_0')$ e prendiamo come autenticatore la retta K' che sia perpendicolare di $I^\wedge$ specie alla $\lfloor$ retta (m, k) cioè si prenda la retta

$$y = m'(x - x_0) + y_0'$$

dove $m' = b/(b + \theta a)$.
Volendo si potrebbe alternare $\times$ con la perpendicolarità di $II^\wedge$ specie assumendo $m'' = (a + b)/\theta a$.
Da notare che si può complicare la vita all'intruso sia variando la scelta dell'elemento di $II^\wedge$ categoria θ e quindi variando la struttura pseudo-euclidea.
Sarà compito di un successivo lavoro la simulazione del sistema di autentificazione. La probabilità di indovinare θ è $1/2^{n-1}$ e la probabilità della scelta della perpendicolarità è $1/2$.

BIBLIOGRAFIA

[1] M. Cerasoli - F. Eugeni - M. Protasi, *Elementi di Matematica Discreta,* Zanichelli, Bologna 1988.

[2] J.W.P. Hirshfeld, *Projective Geometries over Finite Fields,* Clarendon Press, Oxford, 1976.

[3] G. Tallini, *Introduzione alle Geometrie di Galois,* Testo di una conferenza tenuta all'IAC, 1972 (non pubblicata).

Fernando Di Gennaro,
Dipartimento di Matematica,
Università della Basilicata,
Via N. Sauro 85,
85100 Potenza (ITALY)

Franco Eugeni,
Dipartimento di Teoria dei Sistemi,
Università di Teramo,
64100 Teramo (ITALY),
e-mail: eugenif@tin.it