Ratio Mathematica 10
(1996), 43 - 52

CAMPI DI GALOIS: UNA PRESENTAZIONE DIVULGATIVA

Fernando Di Gennaro*

Il presente lavoro è dedicato alla memoria del mio Maestro prof. Bruno Rizzi, immaturamente scomparso. Il suo ricordo sarà con me per sempre.

PREMESSA

Per molto tempo il nome di Galois, come la sua opera non è entrato negli argomenti di insegnamento. Negli ultimi trent'anni è nato un notevole interesse volto a riscoprire, ad ampliare e ad approfondire alcuni aspetti delle sue ricerche. Parimenti nasce, di conseguenza, il problema della divulgazione delle parti più semplici della sua opera...

Questo articolo propone in sostanza una scelta di argomenti ed una metodologia, molto operativa, fruibile fin da una terza Liceo Scientifico, atta a permettere agli allievi di impadronirsi dei concetti basilari della Teoria dei Campi Finiti, o "Campi di Galois", e di conseguenza delle Geometrie finite che su di essi poggiano.

* Liceo Scientifico *M.Curie* di Giulianova (TE)

1. LA NOZIONE DI CAMPO

Sia Q un insieme contenente almeno due elementi distinti che formalmente indichiamo con i simboli 0 e 1. Supponiamo che in tale insieme Q siano definite due operazioni binarie interne, dette rispettivamente la prima "addizione" e denotata con il simbolo formale (+), la seconda "moltiplicazione", denotata simbolicamente con (•).

La struttura Q = (Q, +, •) si dice che è un *corpo* se verifica i seguenti assiomi:

1.- La struttura (Q, +) è un gruppo abeliano, cioè $\forall$ a, b, c $\in$ Q valgono le seguenti proprietà:

I	(a + b) + c = a + (b + c)	[proprietà associativa]
II	a + b = b + a	[proprietà commutativa]
III	$\exists$ 0 $\in$ Q , t.c. 0+a = a+0 = a	[esistenza elemento neutro]
IV	$\forall$ a $\in$ Q, $\exists$ -a $\in$ Q tale che: a+(-a) = (-a)+a = 0	[esistenza dell'opposto]

2.- La struttura (Q\0, •) è pure un gruppo, ma non necessariamente commutativo.
Cioè $\forall$ a, b, c $\in$ Q, valgono le seguenti proprietà:

I	(a • b) • c = a • (b • c)	[proprietà associativa]
II	$\exists$ 1 $\in$ Q, t.c. 1 • a = a • 1 = a	[esistenza neutro moltiplicativo]
III	$\forall$ a $\in$ Q, $\exists$ a' $\in$ Q tale che : a • a' = a' • a = 1	[esistenza elemento inverso]

3.- Infine la moltiplicazione è distributiva rispetto all'addizione, cioè $\forall$ a, b, c $\in$ Q,

$$a \bullet (b + c) = a \bullet b + a \bullet c.$$

Quando la moltiplicazione è commutativa il corpo si dice che è un *campo*, altrimenti si dice un *corpo sghembo*. Sono esempi di campi l'insieme dei numeri razionali, dei numeri reali, dei numeri complessi. Fra i campi ci sono quelli infiniti come i campi numerici sopracitati; ci sono anche quelli finiti che sono l'oggetto della presente nota.

Si chiama *campo di Galois* un campo che contiene un numero finito q di elementi. Esso si suole indicare con GF(q). Si può dimostrare il seguente notevole:

TEOREMA DI VEDDEBURN. *Ogni corpo finito è un campo.*

Il numero q, che è il numero degli elementi del campo, si chiama *ordine del campo di Galois*. Si possono dimostrare, cosa che noi non faremo, i

seguenti tre teoremi che caratterizzano in un certo qual senso i campi di Galois. Il teorema che segue fornisce tutte le condizioni, in semplici termini di cardinalità, relative alla esistenza di un campo di Galois.

TEOREMA DI ESISTENZA ED UNICITA' DEI CAMPI FINITI. *Un campo di Galois* K *(finito) d'ordine* q *esiste se e solo se l'intero* q *è una potenza di un numero primo* p, *cioè*

$$q = p^h$$

Inoltre due campi finiti di eguale ordine sono necessariamente isomorfi.

Il teorema sopradetto ci dice tutto tranne come costruire operativamente tali campi finiti. Questa parte costruttiva è quella che ci interessa maggiormente per accostare gli allievi alla teoria. Le prove dei due teoremi sopra enunciati sono per così dire di livello superiore alle unità didattiche che stiamo proponendo. Noi ci preoccuperemo in questo lavoro di costruire in un primo momento campi finiti di ordine primo, ovvero di introdurre l'allievo alla aritmetica modulare, in una fase successiva del lavoro ci occuperemo effettivamente della costruzione dei campi di Galois aventi come ordine una potenza di un primo. Per questi ci basterà sapere che fissato l'ordine essi sono unici, a meno di isomorfismi.

2. CAMPI DI ORDINE PRIMO

Al fine di costruire i campi aventi come ordine un numero primo, è necessario introdurre l'aritmetica modulare. Sia **Z** l'insieme dei numeri interi relativi e siano n e h due interi relativi verificanti le condizioni

$$n \in \mathbf{Z},\ n > 2 \ \text{ e } \ 0 \le h \le n-1.$$

Si indichi con [h] l'insieme dei numeri interi relativi che divisi per n danno come resto h, cioè l'insieme dei numeri del tipo kn + h. A titolo di esempio se prendiamo n = 6 allora la classe [3] è costituita da tutti i numeri della forma 6 • k + 3 cioè dai numeri che divisi per 6 danno resto 3, dunque i numeri 3, 9, 21, 27 ,ad esempio, sono tutti nella classe [3] (modulo 6), essendo:

$0 \bullet 6 + 3 = 3,\ 1 \bullet 6 + 3 = 9,\ 2 \bullet 6 + 3 = 15,\ 3 \bullet 6 + 3 = 21,\ 4 \bullet 6 + 3 = 27, \ldots$

Si ottengono, fissato n, esattamente n classi modulo n e precisamente:

$$[0],\ [1],\ [2],\ \ldots,\ [n-1].$$

Tali classi sono a due a due disgiunte ed ogni numero intero relativo appartiene ad una e una sola di tali classi. Le classi formano allora quella che si chiama una partizione di **Z**. Ciascuna classe si chiama una classe resto modulo n o un intero ridotto modulo n. L'insieme delle classi modulo n si denota con **Z**(n).

Se n = 2 l'insieme **Z**(2) ha come elementi la classe [0] che è costituita da tutti i numeri pari e la classe [1] che è costituita da tutti i numeri dispari.

Nell'insieme **Z**(2) si possono definire, $\forall$ [a], [b] $\in$ **Z**(2) due operazioni nel modo che segue:

$$[a] + [b] := [a + b]; \qquad [a] \bullet [b] := [a \bullet b]$$

La definizione nuova di addizione e moltiplicazione tra classi che appare al primo membro è definita mediante l'addizione e la moltiplicazione di elementi di **Z** .Sarebbe bene a questo punto adoperare del tempo con gli allievi sia per esemplificare, sia per mostrare loro come le operazioni siano indipendenti dai rappresentanti scelti, principalmente capire bene questa idea. Sempre nella fase di esercitazioni è poi bene dedicare il giusto tempo a verificare che quale che sia n la struttura **Z** (n) ha come zero ed uno sempre le classi [0] ed [1].

Il nostro interesse successivo è l'esame più completo della struttura **Z**(n). E' piuttosto interessante dilungarsi sulle prove dei fatti seguenti:

A) Verifica del fatto che (Z(n), +) è un gruppo commutativo, verificandone le varie proprietà.

B) Verifica per la struttura (Z(n), $\bullet$) della proprietà associativa e commutativa e verifica della distributiva.

Vale poi la pena dedicare tempo alla dimostrazione del seguente

TEOREMA. *La struttura* **Z**(n) *possiede divisori dello zero se e solo se* n *è composto.*

DIMOSTRAZIONE. Sia n composto, esistono allora due divisori propri di n. Dunque si ha n = a $\bullet$ b con 1 < a, b < n. Segue

$$[a] \bullet 1[b] = [n] = [0] \qquad \text{con } [a], [b] \$ [0]$$

Cioè se n è composto la struttura ha divisori dello zero.

Inversamente, se risulta [a] $\bullet$1[b] = [0] con [a], [b]$[0] allora risulta [a$\bullet$1b] = [n] con 1 < a, b < n e quindi n = a $\bullet$ b con 1 < a, b < n e quindi n è composto.

Quanto provato si completa con il seguente

TEOREMA. *Un elemento di* Z_n *è invertibile se e solo se non è un divisore dello zero.*

DIMOSTRAZIONE. Supponiamo che in un qualsiasi anello l'elemento $a\neq 0$ sia un divisore proprio dello zero (allora sia $b\neq 0$ un divisore complementare) e che l'anello abbia almeno due elementi.

Se allora si suppone che a abbia anche inverso a' segue:

$$a'ab = (a'a)b = 1\ b = b$$
$$a'ab = a'(ab) = a'\ 0 = 0$$

da cui $b = 0$ contro l'ipotesi. Dunque un divisore dello zero non può essere invertibile ed un elemento invertibile non può esser divisore dello zero essendo le due relazioni contradittorie.

Rimane da provare che ogni elemento di Z che non è un divisore dello zero è effettivamente invertibile.

Allo scopo sia a un intero che non divide n (cioè che non sia un divisore dello zero) e tale che $1 < a < n$. Considero i multipli ta di a, per $t = 1,2,...,n$; vogliamo provare che uno di essi è divisibile per n. Dividiamo con resto il generico ta-1 per n, si ha:

$$ta = r\ n + r$$

Supponiamo $t = 1, 2, ..., n$, siano t ed s due valori tra questi, risulta allora $r = r$ se e solo se $t = s$ altrimenti si avrebbe:

$$(t- s)\ a = (r - r)\ n + (r - r) = (r - r)\ n$$

con $|(t-s)\ a| < n$ e $|(r - r)\ n| > n$.

Dunque gli n resti sono tutti distinti ed uno di essi è quindi nullo.

Questa breve e semplice prova può essere fortemente istruttiva e permette per via elementare di provare l'esistenza dell'inverso. Si potrebbe anche tentare di provare ai ragazzi qualche cosa in più come ad esempio che ogni anello finito privo dı divisori dello zero è un corpo, ma questo è da sperimentare. A questo punto occorre lavorare con le tabelle e impadronirsi delle classi resto in modo realmente operativo.

La conclusione comunque del nostro paragrafo è riassunta dal seguente

TEOREMA. *La struttura Z_n avente come elementi le classi resto, munita delle operazioni di addizione e moltiplicazione, è un campo se e solo se n è primo.*

Nel seguito porremo per ogni primo p: $GF(p) = Z_p$. La costruzione dei campi di Galois di ordine primo è così completamente assegnata.

3. CAMPI DI ORDINE POTENZA DI UN PRIMO

Partiamo con dei crudi esempi costruttivi.

Si costruisca GF(9). Partiamo da $Z_3 = Z(3)$ formato dalle classi 0, 1, 2 (nel seguito ometteremo le parentesi quadra per semplicità) con

$$0 + 0 = 2 + 2 = [0],\ 1 + 0 = 2 + 2 = [1],\ 1 + 1 = 2 + 0 = [2]$$
$$1 * 2 = 2 \quad 2 * 2 = 1 * 1 = 1$$

Consideriamo l'equazione

$$x^2 + 1 = 0$$

Tale equazione in Z(3) è priva di soluzioni poiché i tre numeri

$$0 * 0 + 1 = 1$$
$$1 * 1 + 1 = 2$$
$$2 * 2 + 1 = 2$$

non sono mai nulli.

Si considerino i binomi del tipo a + ib dove a, b variano in Z(3) ed i è una "soluzione formale" dell'equazione fissata.

Operando poi sui binomi con la somma e il prodotto, si ha:

$$(2 + i) + (2 + 2i) = (1 + i) * (1 + 2i) = 1 + 4 = 2$$
$$i * (1 + i) = 2 + i$$

L'insieme di questi binomi con le operazioni è una descrizione di GF(9). Cambiando l'equazione cambia la descrizione, ma si ha sempre GF(9) a meno di isomorfismi.

Data l'equazione in Z(2)

$$x^2 + x + 1 = 0$$

possiamo costruire gli elementi di GF(4) dati da: 0, 1, i, 1+i.

Per essi si ha $i = i + 1$.

Con l'equazione

$$x^2 + 2x + 1 = 0$$

si può costruire GF(27) i cui elementi sono trinomi del tipo ai + bi + c con a, b, c e Z(3) e dove la somma dei trinomi è quella usuale con la sola sostituzione $i = -2i - 1 = i + 2$.

Con l'equazione

$$x^2 = x + 1$$

si costruisce GF(16) che ha come elementi dei polinomi di 3° ordine.

4. LA DIVISIONE IN UN CAMPO DI GALOIS

Il punto di partenza ovvio, ma da rimarcare con i ragazzi, è far capire che dividere è moltiplicare un elemento per il suo inverso. Questo ha senso essenzialmente per il fatto che la struttura moltiplicativa è commutativa. In altri ambienti come quello dell'algebra delle matrici non ha senso fare un quoziente, ma si può fare un quoziente destro ed uno sinistro...

Ad esempio, a che cosa deve corrispondere 1 diviso 2, cioè 1/2, in questo campo finito? Deve essere necessariamente uno dei numeri 0, 1, 2, 3, 4. Ma quale? In altre parole, qual è quel numero che moltiplicato per 2 dà 1?

Possiamo procedere per tentativi:

$$2 \times 0 = 0 \neq 1$$
$$2 \times 1 = 2 \neq 1$$
$$2 \times 2 = 4 \neq 1$$
$$2 \times 3 = 6 = 1$$

Allora possiamo identificare 1/2 con 3. Però non è possibile procedere sempre per tentativi per trovare l'inverso di un numero: c'è una legge generale che in questo caso è:

$$1/a = a^3$$

Infatti

$$1/2 = 2^3 = 8 = 3$$
$$1/4 = 4^3 = 64 = 4$$

Quindi 4 è il reciproco di se stesso.

Più in generale, per trovare il reciproco di un numero si può considerare la congruenza

$$a^{\Phi(m)} \equiv 1 \bmod m$$

che possiamo scrivere nella forma

$$a \bullet a^{\Phi(m)-1} = 1$$

da cui

$$1/a = a^{\Phi(m)-1}$$

dove $\Phi(m)$ è l'indicatore di Eulero.

I campi finiti si sono assicurati un posto in algebra per merito di Galois che li usò per mostrare le condizioni sotto cui le equazioni algebriche hanno soluzioni per radicali.

5. L'EQUAZIONE DI SECONDO GRADO IN UN CAMPO DI GALOIS

Ci interessiamo ora della risoluzione delle equazioni di 2° grado in un campo di Galois GF(q). Per semplicità d'ora in poi scriveremo gli elementi di GF(q) omettendo le parentesi quadre. Quindi a al posto di [a].

Sia ora

$$x^2 = a \qquad (1)$$

Proviamo che un'equazione di 2° grado pura ha al più due soluzioni tra loro opposte.

Iniziamo con il notare che la (1) non ha soluzioni quando a non è un quadrato. Ha inoltre una sola soluzione se a = 0, come è ovvio (altrimenti ci sarebbero divisori dello zero).

Supponiamo a quadrato, cioè supponiamo che esista $b \in GF(q)$ tale che $a=b^2$. Allora la (1) ha almeno due soluzioni $x_1 = b$, $x_2 = -b$ tra loro opposte.

Proviamo che non ce ne sono altre.

Sia per questo x_3 una eventuale ulteriore soluzione con $x_3 \neq x_1$ ed $x_3 \neq x_2 = -x_1$. Risulta cioè $x_3 - x_1 \neq 0$ ed $x_3 + x_1 \neq 0$. Avendosi allora

$$x_1^2 + x_3^2 = \Delta$$

segue:

$$0 = x_3^2 - x_1^2 = (x_3 - x_1)(x_3 + x_1)$$

Cioè l'esistenza di una terza radice implicherebbe l'esistenza di divisori dello zero.2

Siamo ora in grado di trattare il caso generale:

$$ax^2 + bx + c = 0.$$

Si può scrivere

$$ax^2 + bx + c = a\left[\left(x + \frac{b}{2a}\right)^2 - \frac{\Delta}{4a^2}\right]$$

essendo $\Delta = b^2 - 4ac$.

Dunque il problema è ricondotto alla equazione:

$$\left(x + \frac{b}{2a}\right)^2 = \frac{\Delta}{4a^2}$$

Denotiamo, nell'ipotesi che Δ sia un quadrato, con:

$$\sqrt{\Delta} = \{r : r \in GF(q), r^2 = \Delta\}.$$

Segue allora la "formula risolutiva":

$$x = \frac{-b + \sqrt{\Delta}}{2a}$$

avendo $\sqrt{\Delta}$ due determinazioni.

Quando $\Delta = 0$ l'equazione ha la "radice doppia" espressa sempre dalla formula, mentre nel caso "Δ non quadrato" non ci sono soluzioni.

Il procedimento indicato cade in difetto per il caso di q pari.

Supponiamo ora che q sia pari. Si prova subito che $\forall\ a \in GF(q)$ è:

$$a^2 = b^2 \Leftrightarrow a = b$$

Infatti da $a^2 - b^2 = 0$ risulta $a^2 + b^2 = 0$ per essere $x = -x$. Inoltre essendo $2 = 0$ e quindi $2ab = 0$ è:

$$a^2 + b^2 = a^2 - 2ab + b^2 = (a - b)^2 = 0$$

da cui l'asserto.

Segue allora che i quadrati degli elementi di GF(q) sono a due a due distinti e quindi

ogni elemento di GF(q) è un quadrato.

Segue allora che una equazione della forma

$$ax^2 + bx + c = 0.$$

con $b = 0$ ha sempre una ed una sola soluzione.

Proviamo ora che una equazione del tipo

$$ax^2 + bx + c = 0.$$

con $b \neq 0$ equivale ad una equazione del tipo $y^2 + y = d$.

Infatti, posto $x = hy$ l'equazione diventa:

$$ah^2y^2 + bhy + c = 0.$$

con la condizione che sia $ah^2 = bh$ allora $ah = b$. Dividendo tutti i termini per ah si ottiene appunto l'equazione richiesta.

Si dimostra che gli elementi di GF(q), q pari, si dividono in due categorie. Gli elementi di I categoria sono gli elementi d che si possono scrivere nella forma:

$$d = y^2 + y$$

Per questi l'equazione associata ha due soluzioni che sono y ed y + 1. Risulta infatti:

$$(y + 1)^2 + (y+1) = y^2 + 1 + y + 1 = y^2 + y = d$$

Gli altri elementi detti di II categoria sono quelli che non ammettono la suddetta decomposizione. Per questi l'equazione associata non ha soluzione.

BIBLIOGRAFIA

1. M. CERASOLI, F. EUGENI e M. PROTASI, *Elementi di Matematica Discreta*, Zanichelli, Bologna, 1988.