UNITELMA SAPIENZA

SAPIENZA
Università di Roma
Dipartimento di Informatica

Algebra

Alessandro D'Andrea

15. Il concetto di campo

Richiami

- E' possibile risolvere i sistemi di equazioni lineari attraverso il procedimento di eliminazione di Gauss
- Coefficienti e soluzioni devono essere sommati e moltiplicati; per applicare il procedimento, devono anche essere divisi
- Oggi: **Campi: numeri reali, razionali. Campi finiti.**

Operazioni tra numeri

Quando risolviamo un sistema di equazioni lineari, abbiamo bisogno di sommare, moltiplicare e dividere numeri.

Di solito, questo viene fatto con i numeri reali, all'interno dei quali tutte queste operazioni sono possibili, ma nelle applicazioni è spesso necessaria una più grande generalità.

E' importante che le manipolazioni alle quali siamo abituati continuino a valere. In particolare ci aspettiamo che la somma e la moltiplicazione siano commutative e associative e che il prodotto distribuisca rispetto alla somma. Siamo interessati, in altre parole, a strutture di anello.

Dividere per un numero significa moltiplicare per il suo inverso, se esiste. L'elemento neutro della somma, cioè 0, è l'unico numero che sicuramente non possiede inverso moltiplicativo.

Definizione di campo

Un campo è un anello commutativo nel quale ogni elemento diverso da 0 **abbia un inverso moltiplicativo.** Inoltre $0 \neq 1$. (si richiede questo per evitare che esista un campo con un solo elemento, il che causerebbe molti comportamenti patologici nel resto del corso)

Sono campi

- l'anello $\mathbb{Q}$ dei numeri razionali
- l'anello $\mathbb{R}$ dei numeri reali
- l'anello $\mathbb{Z}/n$ esattamente quando n è un numero primo
- l'anello $\mathbb{C}$ dei numeri complessi.

Poiché mi aspetto che numeri razionali e reali vi siano familiari, parleremo soprattutto dei campi finiti e dei numeri complessi (nella prossima lezione).

$\mathbb{Z}/p$ è un campo $\Longleftrightarrow$ p è primo

Gli elementi invertibili di $\mathbb{Z}/p$ sono tutti e soli quelli della forma $\overline{a}$ con $\mathrm{MCD}(a, p) = 1$.

Abbiamo visto che $\mathbb{Z}/p$ possiede esattamente p elementi: $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{p-1}$. Ora, se p è un numero primo e $0 < a < p$, allora $\mathrm{MCD}(a, p) = 1$, poiché p non può dividere un numero più piccolo.

Di conseguenza, quando p è primo, ogni elemento di $\mathbb{Z}/p$ diverso da $\overline{0}$ è invertibile; pertanto, $\mathbb{Z}/p$ **è un campo.**

Attenzione: in un campo $ab = 0$ è possibile solo quando (almeno) uno dei fattori è 0. In effetti, se $a \neq 0$, allora possiamo moltiplicare per l'inverso di a e ottenere $b = a^{-1}ab = a^{-1}0 = 0$.

Se n non è primo, allora possiamo esprimerlo come prodotto $n = ab$ di numeri naturali più piccoli. Di conseguenza $\overline{a} \cdot \overline{b} = \overline{n} = \overline{0}$, e $\mathbb{Z}/n$ non può essere un campo. Ad esempio, $\mathbb{Z}/6$ non è un campo, poiché $\overline{2} \cdot \overline{3} = \overline{0}$.

Campi finiti - I

Esistono altri campi finiti oltre agli $\mathbb{Z}/p$ e sono talvolta utili nelle applicazioni crittografiche. In questo corso, non siamo interessati a studiarli a fondo; possiamo tuttavia darne qualche informazione.

Se $\mathbf{k}$ è un campo con un numero finito di elementi, allora $(\mathbf{k}, +)$ è un gruppo finito, e quindi ogni suo elemento ha ordine (additivo) finito.

Per il teorema di Cauchy, se un primo p divide $|\mathbf{k}|$, allora possiamo trovare un elemento $0 \neq x \in \mathbf{k}$ di ordine esattamente p. In altre parole sommando x a se stesso p volte si ottiene 0 come risultato, e questo è il minimo multiplo di x ad essere 0.

$$p \cdot x = \underbrace{x + x + \ldots + x}_{p \text{ addendi}} = 0.$$

Campi finiti - II

Moltiplicando per l'inverso x^{-1}, che è sicuramente contenuto nel campo $\mathbf{k}$, si ottiene

$$0 = x^{-1} \cdot 0 = x^{-1} \cdot \underbrace{(x + x + \ldots + x)}_{p \text{ addendi}} = \underbrace{1 + 1 + \ldots + 1}_{p \text{ addendi}}.$$

Di conseguenza, l'ordine (additivo) di 1 deve dividere p. Abbiamo imparato che solo l'elemento neutro 0 della struttura di gruppo ha ordine 1, e quindi 1 ha necessariamente ordine p.

Possiamo ora ripetere il ragionamento per ogni altro elemento $0 \neq y \in \mathbf{k}$. Moltiplicando per y, si ottiene:

$$0 = y \cdot 0 = y \cdot \underbrace{(1 + 1 + \ldots + 1)}_{p \text{ addendi}} = \underbrace{y + y + \ldots + y}_{p \text{ addendi}},$$

e quindi anche y deve avere ordine p. In conclusione, ogni elemento di $0 \neq y \in \mathbf{k}$ ha ordine p.

Campi finiti - III

Ogni elemento di **k** ha ordine p — con l'eccezione dell'elemento neutro 0, che ha chiaramente ordine 1.

Sicuramente, non possono esserci altri primi che dividono $|\mathbf{k}|$, perché nessun elemento di **k** può avere ordine diverso da $1, p$. Pertanto $|\mathbf{k}|$ deve essere una potenza di p.

In conclusione, il numero di elementi di ciascun campo finito deve essere potenza di un numero primo. Si può dimostrare che per ogni scelta di un primo p e di $n \geq 1$, si può costruire un campo con p^n elementi (unico, a meno di isomorfismi).

Un campo con 4 elementi - I

Vediamo come è fatto l'unico campo **k** con 4 elementi.

Ne conosciamo già 2 elementi: l'elemento neutro 0 della somma e l'elemento neutro 1 della moltiplicazione. Poiché l'unico numero primo che divide $|\mathbf{k}| = 4$ è 2, abbiamo già visto che l'ordine additivo di 1, così come di ogni elemento diverso da 0, è 2.

Questo ci permette di calcolare rapidamente la parte della tabella additiva e moltiplicativa che riguarda gli elementi $0, 1$.

+	0	1	α	β
0	0	1	α	β
1	1	0		
α	α		0	
β	β			0

$\cdot$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α		
β	0	β		

Cosa possiamo dire di $\alpha + 1$?

Un campo con 4 elementi - II

L'operazione di somma definisce una struttura di gruppo su **k**. Sappiamo già che $\alpha + 0 = \alpha$, $\alpha + \alpha = 0$.

- Se $\alpha + 1 = \alpha = \alpha + 0$, allora $1 = 0$. Assurdo.
- Se $\alpha + 1 = 0 = \alpha + \alpha$, allora $1 = \alpha$. Assurdo.
- Se $\alpha + 1 = 1$, allora $\alpha = 0$. Assurdo.

In conclusione, l'unica possibilità che non conduce a contraddizioni è che $\alpha + 1 = \beta$, e allo stesso modo $\beta + 1 = \alpha$.

A questo punto, $\alpha + \beta = \alpha + (\alpha + 1) = (\alpha + \alpha) + 1 = 0 + 1 = 1$.

$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

$\cdot$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α		
β	0	β		

Un campo con 4 elementi - III

Occupiamoci ora della tavola moltiplicativa. Sappiamo che $\alpha \neq 0$ deve possedere un inverso moltiplicativo, poiché **k** è un campo, e ogni elemento non nullo ha un inverso. Questo inverso non può essere né 0, né 1, dal momento che $\alpha \cdot 0 = 0$ e $\alpha \cdot 1 = \alpha$. Pertanto l'inverso di α è uno tra α e β. Tuttavia neanche α può essere l'inverso di α. Infatti, se $\alpha^2 = 1$, allora

$$\beta^2 = (\alpha + 1)(\alpha + 1) = \alpha^2 + \alpha + \alpha + 1 = \alpha^2 + (\alpha + \alpha) + 1 = 1 + 1 = 0.$$

Ricordando come il prodotto di elementi non nulli in un campo debba essere necessariamente $\neq 0$, concludiamo che l'inverso di α è β.

+	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

$\cdot$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α		1
β	0	β	1	

Un campo con 4 elementi - IV

Abbiamo ormai terminato. Rimane solo da calcolare $\alpha \cdot \alpha$, ma sappiamo che $\alpha = \beta + 1$ e che $\alpha \cdot \beta = 1$. Allora

$$\alpha \cdot \alpha = \alpha \cdot (\beta + 1) = \alpha\beta + \alpha = 1 + \alpha = \beta.$$

Allo stesso modo, si ottiene $\beta \cdot \beta = \alpha$.

Le tavole additiva e moltiplicativa di **k** devono quindi essere:

+	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

$\cdot$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

Un campo con 4 elementi - V

E' importante fare un'osservazione: i conti che abbiamo effettuato mostrano che se un campo con 4 elementi esiste, le sue operazioni non possono che essere quelle indicate nelle nostre tavole additiva e moltiplicativa. Ma questo non vuol necessariamente dire che la somma e il prodotto che abbiamo calcolato forniscano una struttura di campo.

In effetti, magari le operazioni che abbiamo calcolato non sono associative (lo sono!) o non sono commutative (lo sono!). O magari la moltiplicazione non distribuisce rispetto alla somma (lo fa!).

Insomma: gli assiomi di campo vanno verificati tutti!! (è noioso, ma può essere istruttivo farlo)

Un campo con 4 elementi - VI

E' solo dopo la verifica che le operazioni descritte soddisfanno tutte gli assiomi per una struttura di campo che possiamo concludere che un campo con 4 elementi esiste, ed è essenzialmente unico.

Il campo con p^n elementi si indica con $\mathbb{F}_{p^n}$, e quindi quello che abbiamo costruito è $\mathbb{F}_4$. Le classi di resto $\mathbb{Z}/p$ modulo un numero primo p si indicano anche con $\mathbb{F}_p$.

Tenete sempre in mente che $\mathbb{F}_p$ coincide con $\mathbb{Z}/p$ solo quando p è primo. Il campo $\mathbb{F}_4$ che abbiamo costruito non somiglia affatto all'anello $\mathbb{Z}/4$, che **non è un campo**.

La teoria dei campi finiti è molto elegante e molto semplice, e può essere affrontata con solo un minimo di bagaglio matematico. Se vi ha incuriosito, studiatela pure!