UNITELMA SAPIENZA

SAPIENZA
UNIVERSITÀ DI ROMA
DIPARTIMENTO DI INFORMATICA

Algebra

Alessandro D'Andrea

4. Gruppi

Richiami

- $\mathbb{Z}/n$ è un anello
- $\overline{a}$ è invertibile in $\mathbb{Z}/n$ se e solo se MCD$(a, n) = 1$
- Alcune proprietà degli elementi invertibili di $\mathbb{Z}/n$ si comprendono meglio in un contesto più generale
- Oggi: **Concetto di gruppo e prime proprietà dei gruppi**

Definizione di gruppo

Un gruppo è un insieme G dotato di un'operazione associativa

- $G \times G \ni (a, b) \mapsto a \circ b \in G$

che deve possedere un elemento neutro $e \in G$:

$$e \circ a = a \circ e = a \quad \text{per ogni } a \in G;$$

e rispetto alla quale ogni elemento $a \in G$ possieda un inverso $a^* \in G$

$$a \circ a^* = a^* \circ a = e.$$

Si dovrebbe scrivere $(G, \circ)$, ma scriveremo G ogni volta che si sia implicitamente d'accordo sull'operazione di gruppo.

Il gruppo si dice abeliano se l'operazione di gruppo è commutativa.

Gruppi additivi

Se A è un anello, possiamo ignorare l'operazione di moltiplicazione, e considerare solo quella di somma. Allora $(A, +)$ è un gruppo.

La somma è associativa, l'elemento neutro è $e = 0$, e l'inverso di a è $a^* = -a$.

$$(a + b) + c = a + (b + c),$$
$$a + 0 = 0 + a = a;$$
$$a + (-a) = (-a) + a = 0.$$

L'operazione di somma è anche commutativa, e quindi $(A, +)$ è un gruppo abeliano.

Attenzione: quando si usa la notazione additiva per un'operazione di gruppo, si indica l'elemento neutro sempre con 0, l'inverso di a sempre con $-a$ e, a meno di esplicito riferimento contrario, si dà per scontato che il gruppo sia abeliano.

Esempi di gruppi additivi

Sono gruppi (abeliani):

- il gruppo additivo $(\mathbb{Z}, +)$ dei numeri interi;
- il gruppo additivo $(\mathbb{Q}, +)$ dei numeri razionali;
- il gruppo additivo $(\mathbb{R}, +)$ dei numeri reali;
- il gruppo additivo $(\mathbb{C}, +)$ dei numeri complessi;
- il gruppo additivo $(\mathbb{Z}/n, +)$ delle classi di congruenza mod n;

Non è un gruppo l'insieme $(\mathbb{N}, +)$ dei numeri naturali.

Gruppi moltiplicativi - I

Se A è un anello, possiamo ignorare l'operazione di somma, e considerare solo quella di moltiplicazione. Allora $(A, \cdot)$ non è un gruppo. In effetti, l'elemento neutro dell'operazione non può che essere 1, ma allora 0 non possiede un inverso, poiché $0 \cdot a = 0 \neq 1$ comunque sia scelto a.

Tuttavia, se indichiamo con $A^\times$ gli elementi di A che possiedono un inverso moltiplicativo, allora $(A^\times, \cdot)$ è un gruppo.

Attenzione: quando si usa la notazione moltiplicativa per un'operazione di gruppo, si indica l'elemento neutro sempre con 1, e l'inverso di a sempre con a^{-1}. Spesso si scrive ab invece che $a \cdot b$.

Gruppi moltiplicativi - II

$(A^\times, \cdot)$ è un gruppo. La moltiplicazione è associativa, l'elemento neutro è $e = 1$, e l'inverso di a è $a^* = a^{-1}$.

$$(a \cdot b) \cdot c = a \cdot (b \cdot c),$$
$$a \cdot 1 = 1 \cdot a = a;$$
$$a \cdot a^{-1} = a^{-1} \cdot a = 1.$$

L'operazione di prodotto non è necessariamente commutativa.

L'unità moltiplicativa 1 è invertibile, e il suo inverso è 1, in quanto $1 \cdot 1 = 1$. Pertanto $1 \in A^\times$. Inoltre $(a^{-1})^{-1} = a$.

Se a, b sono invertibili e i loro inversi sono a^{-1}, b^{-1} allora

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aa^{-1} = 1.$$

Pertanto, se $a, b \in A^\times$, allora $ab \in A^\times$, e $(ab)^{-1} = b^{-1}a^{-1}$.

Esempi di gruppi moltiplicativi

Sono gruppi (abeliani):

- il gruppo moltiplicativo $(\mathbb{Z}^\times = \{\pm 1\}, \cdot)$ dei numeri interi;
- il gruppo moltiplicativo $(\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}, \cdot)$ dei numeri razionali;
- il gruppo moltiplicativo $(\mathbb{R}^\times = \mathbb{R} \setminus \{0\}, \cdot)$ dei numeri reali;
- il gruppo moltiplicativo $(\mathbb{C}^\times = \mathbb{C} \setminus \{0\}, \cdot)$ dei numeri complessi;
- il gruppo moltiplicativo $((\mathbb{Z}/n)^\times, \cdot)$ delle classi di congruenza mod n;
  - Se p è un numero primo, allora $(\mathbb{Z}/p)^\times = \mathbb{Z}/p \setminus \{\overline{0}\}$;
  - $(\mathbb{Z}/6)^\times = \{\overline{1}, \overline{5}\}$;
  - $(\mathbb{Z}/8)^\times = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$;
  - $(\mathbb{Z}/12)^\times = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$.

Più in là, vedremo degli anelli non commutativi, che hanno gruppo moltiplicativo non abeliano.

Gruppo delle permutazioni

Se X è un insieme, un'applicazione $f : X \to X$ si dice invertibile se esiste $f^* : X \to X$ tale che $f \circ f^* = f^* \circ f = \mathrm{Id}_X$. L'applicazione f si dice allora una permutazione di X.

L'operazione di composizione tra applicazioni è associativa e l'identità ne è l'elemento neutro:

$$(f \circ g) \circ h = f \circ (g \circ h);$$
$$f \circ \mathrm{Id}_X = \mathrm{Id}_X \circ f = f,$$

per ogni scelta di $f, g, h : X \to X$.

Se $f, g : X \to X$ sono invertibili, allora anche $f \circ g$ è invertibile. In effetti,

$$(f \circ g) \circ (g^* \circ f^*) = f \circ (g \circ g^*) \circ f^* = f \circ \mathrm{Id}_X \circ f^* = f \circ f^* = \mathrm{Id}_X .$$

L'insieme $\mathrm{S}(X)$ di tutte le permutazioni di X, con l'operazione di composizione, è un gruppo.

Gruppo simmetrico S_n

Il gruppo delle permutazioni dell'insieme $\{1, 2, 3, \ldots, n\}$ con n elementi si indica con S_n.

Contiene esattamente $n!$ elementi.

Se $n > 2$, S_n non è abeliano: ad esempio, se

$$f : \begin{cases} 1 \mapsto 2 \\ 2 \mapsto 1 \\ 3 \mapsto 3 \end{cases} \quad , \qquad g : \begin{cases} 1 \mapsto 2 \\ 2 \mapsto 3 \\ 3 \mapsto 1 \end{cases}$$

allora

$$f \circ g : \begin{cases} 1 \mapsto 1 \\ 2 \mapsto 3 \\ 3 \mapsto 2 \end{cases} \quad , \qquad g \circ f : \begin{cases} 1 \mapsto 3 \\ 2 \mapsto 2 \\ 3 \mapsto 1 \end{cases}$$

Proprietà immediate dei gruppi

Se $(G, \circ)$ è un gruppo, allora può esserci solo un elemento neutro dell'operazione:

$$e = e \circ e' = e' \circ e = e'.$$

Ogni elemento possiede un unico inverso: se $\overline{a}$ e a^* sono entrambi inversi di a, allora

$$a^* = a^* \circ (a \circ \overline{a}) = (a^* \circ a) \circ \overline{a} = \overline{a}.$$

L'inverso di ab è $b^* a^*$. Lo abbiamo già dimostrato più volte.

Inoltre, se $gx = g$, allora $x = e$: basta moltiplicare a sinistra per l'inverso di g. Se un elemento si comporta come l'identità rispetto ad anche solo un elemento $x \in G$, allora è l'identità.

Nei gruppi, useremo sempre una notazione moltiplicativa: l'inverso di a è a^{-1} e 1 indica l'elemento neutro a meno che non abbia un nome più appropriato.

Sottogruppi

Se G è un gruppo, un sottoinsieme $H \subset G$ si dice sottogruppo se è un gruppo rispetto all'operazione di G. Equivalentemente:

- $1 \in H$;
- $h \in H \implies h^{-1} \in H$;
- $h_1, h_2 \in H \implies h_1 h_2 \in H$.

H è un sottogruppo di G si scrive $H < G$.

G e $\{1\}$ sono sempre sottogruppi di G. In genere, ce ne sono molti altri.

Se $g \in G$, indichiamo con g^n il prodotto di n copie di g, e con g^{-n} il suo inverso. Ad esempio $g^3 = g \cdot g \cdot g$. Si ha $g^m \cdot g^n = g^{m+n}$.

L'insieme $(g) = \{g^n, n \in \mathbb{Z}\}$ di tutte le potenze di g è un sottogruppo di G. E' il sottogruppo ciclico generato da g.

Sottogruppi di $(\mathbb{Z}, +)$ - I

Come sono fatti i sottogruppi di $\mathbb{Z}$?

Se $H < \mathbb{Z}$, allora H contiene sicuramente l'elemento neutro 0. Se non contiene altri elementi, allora $H = \{0\}$.

Se contiene altri elementi, allora contiene sicuramente sia elementi positivi che negativi.

In effetti, se $h \in H$, allora $-h \in H$. Indichiamo con d il minimo elemento positivo di H.

Sottogruppi di $(\mathbb{Z}, +)$ - II

$\{0\} \neq H < \mathbb{Z}$. Il minimo elemento positivo di H è d.

Se $d \in H$, allora $2d = d + d \in H$; ma allora $3d = 2d + d \in H$. Insomma, tutti i multipli di d sono elementi di H.

Se $h \in H$, allora possiamo eseguire la divisione euclidea tra h e d:

$$h = qd + r.$$

Ora, $r = h + (-qd)$. Ma se $h \in H, -qd \in H$, allora $r \in H$. Tuttavia $0 \leq r < d$. Ricordando che d è il minimo elemento positivo di H, si ottiene $r = 0$ e quindi $h = qd$.

In conclusione, ogni elemento di H è multiplo di d: H è l'insieme di tutti e soli i multipli di d. Si scrive anche $H = (d)$ oppure $H = d\mathbb{Z}$.

Omomorfismi di gruppi

Se G, H sono gruppi, un'applicazione $f : G \to H$ si dice omomorfismo di gruppi se

$$f(a \circ b) = f(a) \circ f(b)$$

per ogni scelta di $a, b \in G$.

Conseguenze: $f(e_G) = e_H$, $f(a^*) = f(a)^*$. Meglio scrivere:
$f(1) = 1, f(a^{-1}) = f(a)^{-1}$ in notazione moltiplicativa, oppure
$f(0) = 0, f(-a) = -f(a)$ in notazione additiva.

Attenzione: sono possibili anche situazioni miste. Ad esempio

$$\exp : (\mathbb{R}, +) \to (\mathbb{R}^\times, \cdot)$$

è un omomorfismo di gruppi, poiché $\exp(x + y) = \exp(x) \exp(y)$.

In effetti, $\exp(0) = 1$, $\exp(-a) = \exp(a)^{-1}$.

Esempi di omomorfismi

- L'identità $\mathrm{Id}_G : G \to G$ è ovviamente un omomorfismo.
  - Poiché $\mathrm{Id}_G(g) = g$ per ogni $g \in G$, allora $\mathrm{Id}_G(ab) = ab = \mathrm{Id}_G(a)\,\mathrm{Id}_G(b)$.
- Se $f : G \to H$ manda ogni elemento di G nell'elemento neutro di H, allora f è un omomorfismo.
  - Poiché $f(g) = 1$ per ogni $g \in G$, allora $f(ab) = 1 = 1 \cdot 1 = f(a)f(b)$.
- Una volta scelto $g \in G$, l'applicazione $\phi : n \mapsto g^n$ è un omomorfismo $\mathbb{Z} \to G$.
  - Abbiamo già visto che $g^{m+n} = g^m g^n$, quindi $\phi(m+n) = \phi(m)\phi(n)$.

Nucleo e immagine

Se $\phi : G \to H$ è un omomorfismo di gruppi, allora

- $\ker \phi = \{g \in G \mid \phi(g) = 1\}$ è il nucleo di ϕ;
- $\operatorname{im} \phi = \{\phi(g) \in H \mid g \in G\}$ è l'immagine di ϕ.

Allora

- $\ker \phi < G$.
  - $\phi(1) = 1$;
  - se $\phi(a) = \phi(b) = 1$, allora $\phi(ab) = \phi(a)\phi(b) = 1 \cdot 1 = 1$;
  - se $\phi(a) = 1$, allora $\phi(a^{-1}) = \phi(a)^{-1} = 1^{-1} = 1$.
- $\operatorname{im} \phi < H$.
  - $1 = \phi(1)$;
  - se $h = \phi(a), k = \phi(b)$, allora $hk = \phi(a)\phi(b) = \phi(ab)$;
  - se $h = \phi(a)$, allora $h^{-1} = \phi(a)^{-1} = \phi(a^{-1})$.
- ϕ è iniettiva se e solo se $\ker \phi = \{1\}$.
  - Se $\phi(a) = \phi(b)$, allora $\phi(ab^{-1}) = \phi(a)\phi(b)^{-1} = 1$. Poiché $\ker \phi = \{1\}$, deve essere $ab^{-1} = 1$ e quindi $a = b$.

Ordine di un elemento

Prendiamo $g \in G$. Se $\phi : (\mathbb{Z}, +) \to G$ è l'omomorfismo $\phi(n) = g^n$, allora

- $\operatorname{im} \phi = (g)$ è il sottogruppo generato da g.
- $\ker \phi$ è un sottogruppo di $\mathbb{Z}$, ed è quindi della forma $(d) = d\mathbb{Z}$ con $d \geq 0$.

Si ha $g^m = g^n$ se e solo se $m - n \in \ker \phi = (d)$.

Se $d > 0$, allora d è il più piccolo esponente positivo da dare a g per ottenere 1 come risultato. L'intero d è detto ordine di g. Si ha $g^m = g^n$ se e solo se $m \equiv n \mod d$, quindi g possiede esattamente d potenze distinte.

Se $d = 0$, allora $g^m = g^n$ se e solo se $m = n$. In questo caso, tutte le potenze di g sono distinte, e g ha ordine infinito.

Sottogruppi normali

Un'ultima osservazione: se $f : G \to H$ è un omomorfismo di gruppi, il sottogruppo $\ker f < G$ ha una proprietà aggiuntiva.

- Se $x \in \ker f$, allora $gxg^{-1} \in \ker f$ per ogni $g \in G$.
  - Infatti
    $f(gxg^{-1}) = f(g)f(x)f(g^{-1}) = f(g) \cdot 1 \cdot f(g)^{-1} = f(g)f(g)^{-1} = 1.$

I sottogruppi con questa proprietà si chiamano sottogruppi normali.

In un gruppo abeliano, ogni sottogruppo è normale, poiché $gxg^{-1} = xgg^{-1} = x$.