Logica per l'Informatica

Cenni di algebra particolare: teoria dei gruppi

Claudio Sacerdoti Coen

<sacerdot@cs.unibo.it>

Universitá di Bologna

09/12/2020

Algebra particolare

L'algebra particolare studia un particolare tipo di struttura algebrica (es. i monoidi, i gruppi, gli anelli, ...).

Vediamo in questi lucidi i primissimi risultati di teoria dei gruppi

Gruppo

Un gruppo $(\mathbb{A}, \circ, e, \cdot^{-1})$ è un monoide con un'operazione aggiuntiva $\cdot^{-1}$ t.c. $\forall x \in \mathbb{A}. x \circ x^{-1} = e = x^{-1} \circ x$

a^{-1} si chiama elemento opposto di a (rispetto a $\circ$).

Teorema: l'elemento opposto di a è unico
Dimostrazione: siano $a, b \in \mathbb{A}$ t.c. $\forall x. a \circ b = e = b \circ a$. Si ha $b = b \circ e = b \circ (a \circ a^{-1}) = (b \circ a) \circ a^{-1} = e \circ a^{-1} = a^{-1}$ □

Il gruppo delle permutazioni

Permutazioni

Sia $\mathbb{A}$ un insieme. Una permutazione di $\mathbb{A}$ è semplicemente una funzione biettiva $\pi \in \mathbb{A}^{\mathbb{A}}$.

Teorema: la funzione identità $id \in \mathbb{A}^{\mathbb{A}}$ è una permutazione.
Teorema: siano π_1, π_2 permutazioni di $\mathbb{A}$. Anche $\pi_2 \circ \pi_1$ lo è.
Teorema: siano π una permutazione di $\mathbb{A}$. Anche π^{-1} (la funzione inversa di π) lo è.

Gruppo delle permutazioni

Sia $Perm(\mathbb{A})$ l'insieme di tutte le permutazioni di un insieme $\mathbb{A}$. Allora $(Perm(A), \circ, id, \cdot^{-1})$ è un gruppo, chiamato gruppo delle permutazioni di $\mathbb{A}$).

Gruppi e permutazioni

Da ora in poi sia $(\mathbb{A}, \circ, e, \cdot^{-1})$ un gruppo.

Definizione: $\pi_\cdot \in Perm(\mathbb{A})^{\mathbb{A}}$, la funzione che associa a ogni elemento di $\mathbb{A}$ una permutazione di $\mathbb{A}$, è definita come segue: $\pi_a(b) = a \circ b$. Dimostriamo che per ogni $a \in \mathbb{A}$ la funzione π_a è una permutazione:

- π_a è iniettiva: siano $b, c \in \mathbb{A}$ t.c. $\pi_a(b) = \pi_a(c)$ (H). Dimostriamo che $b = c$. Da H si ha $b = a^{-1} \circ a \circ b = a^{-1} \circ \pi_a(b) = a^{-1} \circ \pi_a(c) = a^{-1} \circ a \circ c = c$.
- π_a è suriettiva: sia $y \in \mathbb{A}$. Dimostriamo che $\exists x.\pi_a(x) = y$. Scelgo $a^{-1} \circ y$ per x e dimostro $\pi_a(a^{-1} \circ y) = a \circ a^{-1} \circ y = y$. □

Esempio: considerando il gruppo $(\mathbb{N}, +, 0, -)$, π_3 è la permutazione che somma 3 a tutti i numeri.

Teorema: $\pi_.$ è un omomorfismo di gruppi.
Dimostrazione: Considero i gruppi $(\mathbb{A}, \bullet, e, \cdot^\star)$ e $(Perm(\mathbb{A}), \circ, id, \cdot^{-1})$

- $\pi_e(x) = e \bullet x = x$. Quindi, per l'assioma di estensionalità, $\pi_e = id$
- $\pi_{a \bullet b}(x) = (a \bullet b) \bullet x = a \bullet (b \bullet x) = \pi_a(\pi_b(x))$. Quindi, per l'assioma di estensionalità, $\pi_{a \bullet b} = \pi_a \circ \pi_b$
- $(\pi_a \circ \pi_{a^\star})(x) = a \bullet a^\star \bullet x = x = id(x)$. Quindi, per l'assioma di estensionalità, $\pi_a \circ pi_{a^\star} = id$. Analogamente si dimostra $\pi_{a^\star} \circ \pi_a = id$. Peranto $\pi_{a^\star}$ è un elemento opposto di π_a e, per l'unicità dell'elemento opposto, $\pi_{a^\star} = \pi_a^{-1}$. □

Teorema di Cayley: ogni gruppo $(\mathbb{A}, \bullet, e, \cdot^\star)$ è isomorfo a un sottogruppo di $(Perm(\mathbb{A}), \circ, id, \cdot^{-1})$
Dimostrazione: Abbiamo già dimostrato che $\pi.$ è un omomorfismo di gruppi. Sappiamo dalla precedente lezione che $\pi.$ è un omomorfismo suriettivo su $Imm(\pi.)$, che è un sottogruppo di $(Perm(\mathbb{A}), \circ, id, \cdot^{-1})$. Non ci resta che dimostrare che $\pi.$ è anche iniettivo: siano a, b t.c. $\pi_a = \pi_b$. Quindi si ha $a = a \bullet e = \pi_a(e) = \pi_b(e) = b \bullet e = b$. □

Esempio: consideriamo il gruppo $\mathcal{B} := (\{0,1\}, min, 0, \bar{\cdot})$ dove $\bar{b} := 1 - b$. Si ha che $\mathcal{B}$ è isomorfo al gruppo di permutazioni su $\{0,1\}$ $(\{\perp, id\}, \circ, \perp, \cdot^{-}1)$ dove $\perp(x) = 0$ e $id(x) = x$.

Gruppi e permutazioni

Quindi la teoria dei gruppi coincide con lo studio delle permutazioni e quello delle simmetrie.

- notevoli applicazioni in aritmetica, geometria, cristallografia, chimica-fisca (es. simmetrie molecolari, strutture delle proteine), fisica (tutte le leggi fisiche ubbidiscono a simmetrie), risoluzione di cubi di Rubrik, . . .
- prima dell'algebra astratta: i gruppi erano esattamente le permutazioni
- primo esempio importante di un paio di leitmotiv in matematica:
  1. si stabiliscono equivalenze fra teorie perchè certi risultati sono più facili in una teoria che nell'altra
  2. invece di studiare come certi oggetti sono fatti, conviene spesso studiare come questi oggetti possano essere manipolati

Manipolazione algebrica nei gruppi

Teorema: in un gruppo $(\mathbb{A}, \circ, e, \cdot^{-1})$

1. $\forall x, y.(x \circ y)^{-1} = y^{-1} \circ x^{-1}$
2. $\forall x, x^{-1^{-1}} = x$
3. $\forall x, y.x = y \iff x \circ y^{-1} = e \iff x^{-1} \circ y = e$

Dimostrazione:

1. $(x \circ y) \circ (y^{-1} \circ x^{-1}) = x \circ (y \circ y^{-1}) \circ x^{-1}) = x \circ x^{-1} = e$ e $(y^{-1} \circ x^{-1}) \circ (x \circ y) = y^{-1} \circ (x^{-1} \circ x) \circ y = y^{-1} \circ y = e$
2. si ha $x^{-1^{-1}} \circ x^{-1} = e$ e $x^{-1} \circ x^{-1^{-1}} = e$. Dal teorema di unicità dell'opposto si ha $x^{-1^{-1}} = x$
3. se $x = y$ allora $x \circ y^{-1} = y \circ y^{-1} = e$ e $x^{-1} \circ y = y^{-1} \circ y = e$; se $x \circ y^{-1} = e$ allora $y = e \circ y = x \circ y^{-1} \circ y = x$; se $x^{-1} \circ y = e$ allora $x = x \circ e = x \circ x^{-1} \circ y = y$.

Classi laterali

Definizione: Sia $(\mathbb{A}, \circ)$ un semigruppo e siano $a \in \mathbb{A}$ e $\mathbb{B} \subseteq \mathbb{A}$.
L'insieme $a\mathbb{B} = \{z \in \mathbb{A} \mid \exists b \in \mathbb{B}.z = a \circ b\}$ si chiama classe laterale sinistra di $\mathbb{B}$ di rappresentante a.
L'insieme $\mathbb{B}a = \{z \in \mathbb{A} \mid \exists b \in \mathbb{B}.z = b \circ a\}$ si chiama classe laterale destra di $\mathbb{B}$ di rappresentante a.

Classi laterali di sottogruppi

Teorema: Sia $(\mathbb{A}, \circ, e, \cdot^{-1})$ un gruppo e $\mathbb{B}$ un suo sottogruppo. L'insieme delle classi laterali di $\mathbb{B}$ destre/sinistre forma una partizione di $\mathbb{A}$.

Dimostrazione:

1. ogni classe $a\mathbb{B}$ è non vuota in quanto $a = a \circ e \in a\mathbb{B}$ in quanto $e \in \mathbb{B}$
2. $\bigcup_{a \in \mathbb{A}} a\mathbb{B} = \mathbb{A}$ in quanto, per il punto precedente, ogni $a \in \mathbb{A}$ è contenuta in $a\mathbb{B}$
3. $a\mathbb{B} = a'\mathbb{B}$ oppure $a\mathbb{B} \cap a'\mathbb{B} = \emptyset$. Infatti, o l'intersezione è vuota, oppure supponiamo che ci sia $x \in a\mathbb{B} \cap a'\mathbb{B}$ e dimostriamo che i due insiemi sono uguali. Per l'assioma di separazione, ci sono $b, b' \in \mathbb{B}$ t.c. $x = a \circ b = a' \circ b'$ da cui $a = a' \circ b' \circ b^{-1}$. Dimostriamo che per ogni $x' \in a\mathbb{B}$, $x' \in a'\mathbb{B}$. Dall'assioma di separazione si ha che esiste $b'' \in \mathbb{B}$ t.c. $x' = a \circ b'' = a' \circ b' \circ b^{-1} \circ b''$. Poichè $\mathbb{B}$ è un sottogruppo di $\mathbb{A}$, si ha $b' \circ b^{-1} \circ b'' \in \mathbb{B}$ e quindi $x' \in a'\mathbb{B}$.

Controimmagini di funzioni

Definizione: sia $f \in \mathbb{B}^{\mathbb{A}}$. Per ogni $y \in \mathbb{B}$ si definisce $f^{-1}(y) := \{x \in \mathbb{A} \mid f(x) = y\}$ e la si chiama controimmagine di y (rispetto a f)

Esempio: sia $f(x) = |x|$. Si ha $f^{-1}(3) = \{-3, 3\}$.

Morfismi di gruppi

Teorema: sia f un morfismo dal gruppo $\mathcal{A} := (\mathbb{A}, \circ_{\mathbb{A}}, e_{\mathbb{A}}, \cdot^{-1})$ al gruppo $(\mathbb{B}, \circ_{\mathbb{B}}, e_{\mathbb{B}}, \cdot^{-1})$. Si ha $Ker(f) := f^{-1}(e_{\mathbb{B}})$ è un sottogruppo di $\mathcal{A}$ chiamato il nucleo (kernel) di f.

Dimostrazione:

- $e_{\mathbb{A}} \in f^{-1}(e_{\mathbb{B}})$ per l'assioma di separazione in quanto $f(e_{\mathbb{A}}) = e_{\mathbb{B}}$
- siano $x, y \in f^{-1}(e_{\mathbb{B}})$. Quindi per l'assioma di separazione, $f(x) = f(y) = e_{\mathbb{B}}$. Si ha $f(x \circ_{\mathbb{A}} y) = f(x) \circ_{\mathbb{B}} f(y) = e_{\mathbb{B}} \circ_{\mathbb{B}} e_{\mathbb{B}} = e_{\mathbb{B}}$. Quindi, per l'assioma di separazione, $x \circ_{\mathbb{A}} y \in f^{-1}(e_{\mathbb{B}})$
- sia $x \in f^{-1}(e_{\mathbb{B}})$. Quindi, per l'assioma di separazione, $f(x) = e_{\mathbb{B}}$. Si ha $e_{\mathbb{B}} = f(e_{\mathbb{A}}) = f(x \circ_{\mathbb{A}} x^{-1}) = f(x) \circ_{\mathbb{B}} f(x^{-1}) = e_{\mathbb{B}} \circ_{\mathbb{B}} f(x^{-1}) = f(x^{-1})$. Quindi, per l'assioma di separazione, $x^{-1} \in f^{-1}(e_{\mathbb{B}})$. □

Morfismi di gruppi

Sia f un morfismo dal gruppo $(\mathbb{A}, \circ_{\mathbb{A}}, e_{\mathbb{A}}, \cdot^{-1})$ al gruppo $(\mathbb{B}, \circ_{\mathbb{B}}, e_{\mathbb{B}}, \cdot^{-1})$. Si ha $x \sim_f y$ sse $f(x) = f(y)$ sse $e_{\mathbb{B}} = f(x) \circ_{\mathbb{B}} f(y)^{-1} = f(x \circ_{\mathbb{A}} y^{-1})$ sse $x \circ_{\mathbb{A}} y^{-1} \in Ker(f)$.

Quindi la relazione $x \sim_{Ker(f)} y := x \circ_{\mathbb{A}} y^{-1} \in Ker(f)$ coincide con $x \sim_f y$ ed è una relazione di equivalenza su $\mathbb{A}$.

Relazione di equivalenza indotta da un sottogruppo

Generalizziamo: per ogni sottogruppo $\mathbb{B}$ di un gruppo $(\mathbb{A}, \circ, e, \cdot^{-1})$ si definisce $x \sim_{\mathbb{B}} y := x \circ_{\mathbb{A}} y^{-1} \in \mathbb{B}$. La relazione $\circ_{\mathbb{B}}$ su $\mathbb{A}$ si chiama relazione di equivalenza destra indotta da $\mathbb{B}$ in quanto è una relazione di equivalenza:

- Riflessività: per ogni x, $x \sim_{\mathbb{B}} x \iff x \circ_{\mathbb{A}} x^{-1} = e \in \mathbb{B}$ in quanto $\mathbb{B}$ è un sottogruppo.
- Simmetria: per ogni x, y t.c. $x \sim_{\mathbb{B}} y$, ovvero $x \circ_{\mathbb{A}} y^{-1} \in \mathbb{B}$ (H), dobbiamo dimostrare che $y \sim_{\mathbb{B}} x$, ovvero $y \circ_{\mathbb{A}} x^{-1} \in \mathbb{B}$. Da H, poichè $\mathbb{B}$ è un sottogruppo, si ha $(x \circ_{\mathbb{A}} y^{-1})^{-1} = y^{-1^{-1}} \circ x^{-1} = y \circ x^{-1} \in \mathbb{B}$.
- Transitività: per ogni x, y, z t.c. $x \sim_{\mathbb{B}} y$, ovvero $x \circ y^{-1} \in \mathbb{B}$, e $y \sim_{\mathbb{B}} z$, ovvero $y \circ z^{-1} \in \mathbb{B}$. Quindi, poichè $\mathbb{B}$ è un sottogruppo, si ha $x \circ_{\mathbb{B}} y^{-1} \circ_{\mathbb{B}} y \circ_{\mathbb{B}} z^{-1} = x \circ_{\mathbb{B}} z^{-1} \in \mathbb{B}$. Quindi $x \sim_{\mathbb{B}} z$. □

Relazione di equivalenza indotta da un sottogruppo

Esempio: $3\mathbb{Z}$ è il sottogruppo di $(\mathbb{Z}, +, 0, -)$ formato dai multipli (positivi e negativi) di 3. Si ha $x \sim_{3\mathbb{Z}} y$ sse $x + -y \in 3\mathbb{Z}$, ovvero sse esiste un $k \in \mathbb{Z}$ t.c. $x + -y = 3k$, ovvero sse esiste un k t.c. $x = 3k + y$. Esempio: $5 \sim_{3\mathbb{Z}} 14$ in quanto $5 = 3(-3) + 14$.

Indichiamo con x/y il quoziente e con $x\%y$ (pronunciato "x modulo y)" il resto della divisione intera fra x e y, che è sempre un numero non negativo più piccolo di y. Esempi: $5/3 = 1$, $5\%3 = 2$, $14/3 = 4$ e $14\%3 = 2$.

Per ogni n e x si ha $x = n * (x/n) + x\%n$. Esempi:
$14 = 3 * (14/3) + 14\%3 = 3 * 4 + 2$ e
$-14 = 3 * (-14/3) + (-14\%3) = 3 * (-5) + 1$.

Si ha $x = 3k + y$ sse $3 * (x/3) + x\%3 = 3k + 3 * (y/3) + y\%3$ sse $3 * (x/3 - y/3 + k) + x\%3 = y\%3$ sse $x/3 - y/3 + k = 0$ e $x\%3 = y\%3$. Quindi $x \sim_{3\mathbb{Z}} y$ sse $x\%3 = y\%3$!

Relazioni di equivalenza indotte e classi laterali

Teorema: Sia $(\mathbb{A}, \circ, e, \cdot^{-1})$ un gruppo $\mathbb{B}$ un suo sottogruppo. Si ha $x \sim_{\mathbb{B}} y$ sse $x \in \mathbb{B}y$, da cui $[y]_{\sim_{\mathbb{B}}} = \mathbb{B}y$
Dimostrazione: sappiamo che $x \sim_{\mathbb{B}} y$ sse $x \circ y^{-1} \in \mathbb{B}$ sse $x \circ y^{-1} \circ y \in \mathbb{B}y$ sse $x \in \mathbb{B}y$. Pertanto $[y]_{\sim_{\mathbb{B}}} = \mathbb{B}y$ per l'assioma di estensionalità: per ogni x, $x \in [y]_{\sim_{\mathbb{B}}}$ sse $x \sim_{\mathbb{B}} y$ sse $x \in \mathbb{B}y$. □

Esempio: $x \sim_{3\mathbb{Z}} y$ sse $x\%3 = y\%3$ sse $x \in 3\mathbb{Z} + y$ dove abbiamo indicato $3\mathbb{Z} + y$ la classe laterale destra di rappresentante y (al posto della notazione usata fino ad ora $3\mathbb{Z}y$).

Si ha $3\mathbb{Z}$ è l'insieme dei multipli di 3, ovvero $\{\ldots, -6, -3, 0, 3, 6, \ldots\}$, $3\mathbb{Z} + 1 = 3\mathbb{Z} + 4 = 3\mathbb{Z} + 7 = \ldots$ è l'insieme $\{\ldots, -5, -2, 1, 4, 7, \ldots\}$ e $3\mathbb{Z} + 2 = 3\mathbb{Z} + 5 = \ldots$ è l'insieme $\{\ldots, -4, -1, 2, 5, 8, \ldots\}$.
Pertanto $\mathbb{Z}_{/3\mathbb{Z}} = \{3\mathbb{Z}, 3\mathbb{Z} + 1, 3\mathbb{Z} + 2\} = \{[0]_{3\mathbb{Z}}, [1]_{3\mathbb{Z}}, [2]_{3\mathbb{Z}}\}$

Relazioni di equivalenza indotte e classi laterali

Abbiamo capito che da un morfismo f si ottiene il $Ker(f)$ t.c. $\sim_{Ker(f)} = \sim_f$. Ci chiediamo ora se a partire da un sottogruppo generico $\mathbb{B}$ si trovi sempre un morfismo g t.c. $\sim_{\mathbb{B}} = \sim_g$.

Definizione: Sia $(\mathbb{A}, \circ, e, \cdot^{-1})$ un gruppo e $\mathbb{B}$ un suo sottogruppo. Definiamo $f_{\mathbb{B}}(x) := \mathbb{B}y$ dove $\mathbb{B}y$ è l'unica classe laterale destra t.c. $x \in \mathbb{B}y$.

Teorema: Sia $(\mathbb{A}, \circ, e, \cdot^{-1})$ un gruppo $\mathbb{B}$. Si ha $\sim_{f_{\mathbb{B}}} = \sim_{\mathbb{B}}$ e $\mathbb{B} = f_{\mathbb{B}}^{-1}(e)$.

Dimostrazione: Procediamo ricorrendo all'assioma di estensionalità. Si ha $x \sim_{f_{\mathbb{B}}} y$ sse $f_{\mathbb{B}}(x) = f_{\mathbb{B}}(y)$ sse ci sono z, z' t.c. $x \in \mathbb{B}z$ (Hx) e $y \in \mathbb{B}z'$ (Hy) e $[z]_{\sim_{\mathbb{B}}} = \mathbb{B}z = \mathbb{B}z' = [z']_{\sim_{\mathbb{B}}}$. Quindi $z \sim_{\mathbb{B}} z'$ per il teorema visto nella prima parte del corso e da (Hx) si ha $x \sim_{\mathbb{B}} z$ e da (Hy) si ha $y \sim_{\mathbb{B}} z'$. Quindi $x \sim_{\mathbb{B}} z \sim_{\mathbb{B}} z' \sim_{\mathbb{B}} y$ e perciò $\sim_{f_{\mathbb{B}}} = \sim_{\mathbb{B}}$. □

Relazioni di equivalenza indotte e classi laterali

Fino a qui tutto bene: abbiamo appena dimostrato che dato un sottogruppo generico $\mathbb{B}$ si trova sempre una funzione g t.c. $\sim_{\mathbb{B}} = \sim_g$.

Ci chiediamo ora se g sia un morfismo, che avrebbe come conseguenza del primo teorema di omomorfismo fra gruppi che $[\cdot]$ sarebbe anch'esso un morfismo e che l'insieme delle classi laterali destre indotte da g avesse una struttura di gruppo $(\mathbb{A}_{/\sim_{\mathbb{B}}}, \oplus, \mathbb{B}, \cdot^{-1})$.

La risposta è NEGATIVA nel caso generale. Infatti non è possibile definire $\oplus$ che dovrebbe mappare due classi laterali destre $\mathbb{B}x$ e $\mathbb{B}y$ nella classe laterale destra $\mathbb{B}(x \circ y)$. Vediamo infatti un controesempio nella prossima slide.

L'insieme delle classi laterali destre non forma un gruppo

Consideriamo l'insieme $\mathbf{X} = \{a, b, c\}$, il gruppo non abeliano delle permutazioni $(Perm(\mathbf{X}), \circ, 1, \cdot^{-1})$ e un suo sottogruppo $\mathbb{B} := \{id, f\}$ dove $f(a) = a, f(b) = c, f(c) = b$. $\mathbb{B}$ è effettivamente un sottogruppo in quanto $f \circ f = id$ e quindi $\circ$ e $\cdot^{-1}$ sono entrambe chiuse rispetto a $\mathbb{B}$ osservando che $f^{-1} = f$.

Siano $g(a) = b, g(b) = c, g(c) = a$ e $h(a) = c, h(b) = b, h(c) = a$ e $k(a) = b, k(b) = c, k(c) = a$, $l(a) = b, l(b) = a, l(c) = c$ permutazioni di $\mathbb{A}$. Si ha $\mathbb{B}g = \{g, h\}$ (in quanto $h = f \circ g$), $\mathbb{B}h = \{h, k\}$ (in quanto $k = f \circ h$) e $g \circ h = f$ e dunque $\mathbb{B}f = \mathbb{B}$. Quindi $h \in \mathbb{B}g$ e $k \in \mathbb{B}h$, ma $h \circ k = l \notin \mathbb{B}(g \circ h) = \mathbb{B}$.

Pertanto non posso definire l'operazione $\mathbb{B}a \oplus \mathbb{B}b := \mathbb{B}(a \circ b)$.

Sottogruppi normali

Nota: quanto visto fino ad ora usando classi laterali destre si può riproporre usando le classi laterali sinistre, partendo dalla definizione di $\sim_{\mathbb{B}}$ non più come $x \sim_{\mathbb{B}} y := x \circ y^{-1} \in \mathbb{B}$, bensì come $x \sim_{\mathbb{B}} y := x^{-1} \circ y \in \mathbb{B}$.

Definizione: $\mathbb{B}x$ è una classe laterale di $\mathbb{B}$ di rappresentante x sse $\mathbb{B}x = x\mathbb{B}$, ovvero se le classi laterali destre e sinistre di rappresentante x coincidono.

Definizione: $\mathbb{B}$ è un sottogruppo normale di un gruppo $\mathcal{A}$ sse tutte le sue classi laterali destre sono classi laterali.

Sottogruppi di gruppi abeliani

Teorema: tutti i sottogruppi di un gruppo abeliano sono normali.

Dimostrazione: dobbiamo dimostrare che per ogni x si ha $\mathbb{B}x = x\mathbb{B}$. Il che è ovvio poichè se il gruppo è abeliano si ha $\mathbb{B}x = \{a \circ x \mid a \in \mathbb{B}\} = \{x \circ a \mid a \in \mathbb{B}\} = x\mathbb{B}$ $\square$.

Kernel e normalità

Teorema: per ogni morfismo f da $\mathcal{A} := (\mathbb{A}, \circ_{\mathbb{A}}, e_{\mathbb{A}}, \cdot^{-}1)$ a $(\mathbb{B}, \circ_{\mathbb{B}}, e_{\mathbb{B}}, \cdot^{-}1)$, $Ker(f)$ è un sottogruppo normale.
Dimostrazione: sappiamo già che $Ker(f)$ è un sottogruppo di $\mathcal{A}$. Dimostriamo che è normale, ovvero che per ogni x si ha $Ker(f)x = xKer(f)$ o, equivalentemente, che $Ker(f)x \subseteq xKer(f)$ e $Ker(f)x \supseteq xKer(f)$. Dimostriamo la seconda parte; la prima si ottiene procedendo in maniera analoga. Applichiamo la permutazione $\cdot \circ x^{-1}$ ad ambo gli insiemi, riducendoci a dimostrare $Ker(f) \supseteq xKer(f)x^{-1}$. Sia $y \in xKer(f)x^{-1}$. Quindi, per separazione, c'è uno $z \in Ker(f)$ t.c. $y = x \circ_{\mathbb{A}} z \circ_{\mathbb{A}} x^{-1}$. Ma questo implica $y \in Ker(f)$ in quanto $f(y) = f(x \circ_{\mathbb{A}} z \circ_{\mathbb{A}} x^{-1}) = f(x) \circ_{\mathbb{B}} f(z) \circ_{\mathbb{B}} f(x)^{-1} = f(x) \circ_{\mathbb{B}} e_{\mathbb{B}} \circ_{\mathbb{B}} f(x)^{-1} = e_{\mathbb{B}}$. □

Normalità e quozientamento

Se $\mathbb{B}$ è un sottogruppo normale di un gruppo, allora la definizione $\mathbb{B}a \oplus \mathbb{B}b := \mathbb{B}(a \circ b)$ funziona, in quanto $\mathbb{B}a \oplus \mathbb{B}b = a\mathbb{B} \oplus \mathbb{B}b = \{a \circ z_1 \circ z_2 \circ b \mid z_1, z_2 \in \mathbb{B}\} = \{a \circ z_3 \circ b \mid z_3 \in \mathbb{B}\} = \{z_4 \circ a \circ b \mid z_4 \in \mathbb{B}\} = \mathbb{B}(a \circ b)$.

Possiamo concludere quindi con il seguente teorema:

Teorema: i sottogruppi normali di un gruppo dato sono tutti e soli i nuclei di morfismi dal gruppo verso altri gruppi.
Dimostrazione (cenni): se $\mathbb{B}$ è sottogruppo normale allora $f_{\mathbb{B}}$ è un morfismo. Il teorema segue come corollario dai precedenti.

Cardinalità delle classi laterali

Teorema: sia $\mathbb{B}$ un sottogruppo di un gruppo $(\mathbb{A}, \circ, e, \cdot^{-1})$. Tutte le classi laterali sinistre/destre di $\mathbb{B}$ hanno la stessa cardinalità.
Dimostrazione: Siano $x, y \in \mathbb{A}$. Dimostriamo che la permutazione $\pi_{y \circ x^{-1}}$ è una biezione fra $x\mathbb{B}$ e $y\mathbb{B}$. Infatti per ogni $b \in \mathbb{B}$ la permutazione mappa $z := x \circ b$ in $y \circ x^{-1} \circ z = y \circ x^{-1} \circ x \circ b = y \circ b$. □

Corollario: se $\mathbb{B}$ è sottogruppo normale del gruppo $(\mathbb{A}, \circ, e, \cdot^{-1})$ il cui sostegno è un insieme finito di cardinalità $|\mathbb{A}| = m$, allora $|\mathbb{A}| = |\mathbb{B}| * |\mathbb{A}_{/\mathbb{B}}|$.
Dimostrazione: l'insieme $\mathbb{A}$ viene partizionato in $|\mathbb{A}_{/\mathbb{B}}|$ classi di equivalenza, ognuna delle quali è una classe laterale di $\mathbb{B}$ e pertanto ha la stessa cardinalità di $\mathbb{B} = \mathbb{B}e$. □

Cardinalità delle classi laterali

Esempio: consideriamo il gruppo $(\mathbb{Z}_{/6\mathbb{Z}}, \oplus, [0]_{6\mathbb{Z}}, \cdot^{-1})$ espresso equivalentemente come $(\{0, 1, \ldots, 5\}, +_6, 0, -_6)$ dove la somma e il cambio di segno si ottengono prendendo il resto dell'operazione algebrica diviso 6. Esempio: $3 +_6 7 = 4$ in quanto $(3 + 7)\%6 = 10\%6 = 4$ e $-_6 2 = -2\%6 = 4$ in quanto $-2/6 = -1$ e $-1 * 6 + 4 = -2$.

Poichè $|\{0, \ldots, 5\}| = 6$, il gruppo può avere come sottogruppi normali solamente gruppi di cardinalità $1, 2, 3$ e 6 aventi rispettivamente $6, 3, 2$ e 1 classi laterali.

Esempio: $\{0, 2, 4\}$ (i numeri pari) formano un sottogruppo normale ($+_6$ è commutativa!) di cardinalità 3. Le due classi laterali (2 * 3 = 6) sono $\mathbb{B}0 = \{0, 2, 4\}$ e $\mathbb{B}1 = \{1, 3, 5\}$. Il loro insieme forma il gruppo abeliano $(\{\mathbb{B}0, \mathbb{B}1\}, \oplus, \mathbb{B}0, \cdot^{-1})$ dove $\mathbb{B}0 \oplus X = X$ e $\mathbb{B}1 \oplus \mathbb{B}1 = \mathbb{B}0$. Tale gruppo è isomorfo a $\mathbb{Z}_{/2\mathbb{Z}}$.

Conclusioni

- L'algebra particolare studia le proprietà caratteristiche di un singolo tipo di struttura algebrica (es. monoidi, gruppi, anelli, ...)
- Nonostante una struttura algebrica possa avere pochissime operazioni e assiomi su di essa (3 operazioni e 3 assiomi per i gruppi), la teoria generata può essere ricchissima
- Una parte rilevante della teoria studia
  1. gli isomorfismi fra strutture algebriche, ovvero il cambio di rappresentazione
  2. come ottenere nuove strutture algebriche a partire da quelle date
  3. come decomporre strutture algebriche (p.e. quozientando un gruppo rispetto a un sottogruppo normale) per studiare le proprietà delle componenti e ricavare da queste le proprietà della struttura composta