

AL210 - Appunti integrativi - 1

Prof. Stefania Gabelli - a.a. 2016-2017

Funzioni tra insiemi

Ricordiamo che una *funzione* o *applicazione* di insiemi $f : A \rightarrow B$ è una corrispondenza tra A e B tale che:

- (1) f è definita su tutto A ;
- (2) per ogni $a \in A$, $f(a)$ è univocamente determinato. Ovvero, se $a = b$, allora $f(a) = f(b)$.

A si chiama il *dominio* della funzione f e B si chiama il *codominio* di f .

Due funzioni f e g sono uguali se e soltanto se hanno stesso dominio A e stesso codominio B ed inoltre $f(a) = g(a)$, per ogni $a \in A$.

Se $a \in A$, l'elemento $f(a)$ di B si chiama l'*immagine di a* e l'insieme degli elementi di B che sono immagine di qualche elemento di A si chiama l'*immagine di f* o l'*immagine di A* . L'immagine di f è un sottoinsieme di B e si denota con $\text{Im}(f)$, oppure con $f(A)$. Dunque

$$\text{Im}(f) = f(A) = \{b \in B; b = f(a), \text{ per qualche } a \in A\} \subseteq B.$$

Se $b \in B$, l'insieme degli elementi $a \in A$ tali che $f(a) = b$ si chiama la *controimmagine di b* e si denota con $f^{-1}(b)$. Dunque

$$f^{-1}(b) = \{a \in A; f(a) = b\}.$$

Ovviamente risulta $f^{-1}(b) \neq \emptyset$ se e soltanto se $b \in \text{Im}(f)$.

f è una *funzione suriettiva* se $\text{Im}(f) = B$. Cioè, per ogni $b \in B$ esiste $a \in A$ tale che $f(a) = b$.

f è una *funzione iniettiva* se per ogni $b \in \text{Im}(f)$, $f^{-1}(b)$ consiste di un solo elemento. Cioè, se $f(a) = f(a')$, allora $a = a'$.

Una funzione che è allo stesso tempo suriettiva e iniettiva si chiama *biiettiva*. Una funzione biiettiva $A \rightarrow A$ si chiama una *trasformazione*, o una *permutazione* su A .

Indichiamo con $\mathcal{F}(A, A)$ tutte le funzioni di dominio e codominio A e con $\mathcal{T}(A)$ il sottoinsieme delle funzioni biiettive, o trasformazioni, su A . Se A è un insieme finito con n elementi, si pone $\mathcal{T}(A) = S_n$

Talvolta le funzioni si possono comporre. Se $f : A \rightarrow B$ e $g : B \rightarrow C$, allora la funzione composta $g \circ f : A \rightarrow C$ è definita da $(g \circ f)(a) = g(f(a))$. In particolare, due funzioni $f, g \in \mathcal{F}(A, A)$ si possono sempre comporre.

Operazioni

Una *operazione n-aria* su un insieme X è una applicazione che ha per dominio il prodotto cartesiano di n copie di X e per codominio X , dunque associa ad una n -pla di elementi di X un altro elemento di X .

Considereremo soltanto *operazioni binarie* $f : X \times X \rightarrow X$.

Le operazioni binarie si indicano con un simbolo $*$, $+$, \times , \cdot , \circ , \dots . Ad esempio possiamo scrivere

$$* : X \times X \rightarrow X; \quad (x, y) \mapsto x * y.$$

L'elemento $x * y$ si chiama il *composto* di x e y .

Esempi: Esempi di operazioni binarie sono: addizione e moltiplicazione in \mathbb{N} , \mathbb{Z} , \mathbb{Q} , \mathbb{R} , \mathbb{C} ; addizione e moltiplicazione di polinomi in $\mathbb{Z}[X]$, $\mathbb{Q}[X]$; addizione di matrici in $\mathcal{M}_{n,m}(\mathbb{R})$; moltiplicazione (righe per colonne) di matrici in $\mathcal{M}_n(\mathbb{R})$; composizione di funzioni nell'insieme $\mathcal{F}(A, A)$ delle funzioni di dominio e codominio A ; unione e intersezione nell'insieme $\mathcal{P}(A)$ delle parti di un insieme A .

Proprietà delle operazioni

Le proprietà più significative di una operazione $*$ su X sono:

Proprietà associativa: $(x * y) * z = x * (y * z)$, per ogni $x, y, z \in X$;

Se vale la proprietà associativa, si possono omettere le parentesi, cioè si può scrivere $(x * y) * z = x * y * z (= x * (y * z))$ e $x_1 * \dots * x_n$, per $n \geq 2$.

La composizione $x * x * \dots * x$ (n volte), si chiama la *potenza n-sima* di x .

Proprietà commutativa: $x * y = y * x$, per ogni $x, y \in X$;

Esistenza di un elemento neutro: esiste un elemento $e \in X$ tale che $e * x = x = x * e$, per ogni $x \in X$.

Se un tale elemento neutro esiste, esso è necessariamente unico. Infatti, siano e, e' due elementi neutri. Allora $e = e * e' = e'$.

Inoltre se $*$, $*'$ sono due operazioni su X ,

Proprietà distributiva destra di $$ rispetto a $*'$:* $x * (y *' z) = (x * y) *' (x * z)$, per ogni $x, y, z \in X$.

Proprietà distributiva sinistra di $$ rispetto a $*'$:* $(y *' z) * x = (y * x) *' (z * x)$, per ogni $x, y, z \in X$.

Se $*$ è commutativa, non è necessario distinguere tra proprietà distributiva destra e sinistra.

Esempi: Addizione e moltiplicazione in \mathbb{Z} , \mathbb{Q} , \mathbb{R} , \mathbb{C} sono operazioni associative e commutative. 0 è l'elemento neutro rispetto all'addizione, 1 è

l'elemento neutro rispetto alla moltiplicazione. Inoltre la moltiplicazione è distributiva rispetto alla addizione: $x(y + z) = xy + yz$.

Le stesse proprietà hanno addizione e moltiplicazione in \mathbb{Z}_n , l'insieme delle classi resto modulo n .

L'addizione di matrici in $\mathcal{M}_{n,m}(\mathbb{R})$ è associativa e commutativa, con elemento neutro la matrice nulla.

La moltiplicazione di matrici in $\mathcal{M}_n(\mathbb{R})$ è associativa ma non commutativa, con elemento neutro la matrice diagonale unitaria. La moltiplicazione è distributiva rispetto all'addizione.

La composizione di funzioni nell'insieme $\mathcal{F}(A, A)$ delle funzioni di dominio e codominio A è associativa, ma non è commutativa. La funzione identità $id_A : A \rightarrow A; a \mapsto a$ è l'elemento neutro.

Unione e intersezione di sottoinsiemi di A sono operazioni associative e commutative. Inoltre esse sono distributive l'una rispetto all'altra. L'insieme vuoto è l'elemento neutro rispetto all'unione, A è l'elemento neutro rispetto all'intersezione.

Se $*$ è un'operazione su X ed esiste l'elemento neutro $e \in X$, un elemento $x \in X$ si dice *simmetrizzabile* se esiste $y \in X$ tale che $x * y = e = y * x$. In questo caso, y si dice un *simmetrico* di x .

Chiaramente e è simmetrizzabile, perché $e * e = e$. Inoltre, segue dalla definizione che se x è simmetrizzabile, con simmetrico y , anche y è simmetrizzabile, con simmetrico x .

Sia $*$ un'operazione *associativa* su X :

(1) Se esiste un elemento simmetrico di x , esso è necessariamente unico. Infatti, se y e z sono due simmetrici di x , allora

$$y = y * e = y * (x * z) = (y * x) * z = e * z = z.$$

(2) Se x, y sono simmetrizzabili, con simmetrico x' e y' rispettivamente, allora $x * y$ è simmetrizzabile con simmetrico $y' * x'$.

Infatti si ha

$$(x * y) * (y' * x') = x * (y * y') * x' = x * e * x' = x * x' = e.$$

Analogamente $(y' * x') * (x * y) = e$.

Una funzione $f : A \rightarrow A$ è simmetrizzabile se e soltanto se essa è biiettiva. Infatti, se f è biiettiva, per ogni $b \in A$, la controimmagine $f^{-1}(b)$ è non vuota e consiste di un solo elemento. Allora, se $f^{-1}(b) = \{a\}$, la corrispondenza $g : A \rightarrow A$ definita da $g(b) = a$, per ogni $b \in A$ è una funzione ed è tale che $f \circ g = id_A = g \circ f$.

Viceversa, sia $g : A \rightarrow A$ una funzione tale che $f \circ g = id_A = g \circ f$. Allora, se $f(a) = f(a')$, si ha $a = g(f(a)) = g(f(a')) = a'$. Dunque f è iniettiva. Inoltre, per ogni $b \in A$, $b = f(g(b))$ e perciò f è suriettiva.

Se f è biiettiva, la sua simmetrica si indica con f^{-1} e si chiama la *funzione inversa* di f .

Un elemento $x \in X$ si dice *cancellabile a destra*, rispettivamente *a sinistra*, se

$$y * x = z * x \Rightarrow y = z; \quad \text{rispettivamente,} \quad x * y = x * z \Rightarrow y = z.$$

Se x è simmetrizzabile, allora x è cancellabile a destra e a sinistra. Infatti per cancellarlo basta moltiplicare (a destra o a sinistra) per il simmetrico di x .

Notazione additiva e moltiplicativa

Considereremo sempre operazioni associative.

Se un'operazione associativa su X si indica con $+$, si dice che si usa la *notazione additiva*. L'elemento $x + y$ si chiama la *somma* di x e y . In notazione additiva, l'elemento neutro (se esiste) si chiama lo *zero* di X e si indica con 0 . Il simmetrico dell'elemento x (se esiste) si chiama l'*opposto* di x : esso si indica con $-x$. Se y ha l'opposto, si pone anche $x - y := x + (-y)$. La potenza n -sima di x si indica con nx . Notiamo che se x ha opposto, per l'associatività, anche nx ha opposto: esso è la potenza n -sima di $-x$, ovvero $-(nx) = n(-x)$.

Se un'operazione associativa su X si indica con \cdot , o semplicemente con la giustapposizione, si dice che si usa la *notazione moltiplicativa*. L'elemento xy si chiama il *prodotto* di x e y . In notazione moltiplicativa, l'elemento neutro (se esiste) si chiama l'*unità* di X e si indica con 1 . Il simmetrico di x (se esiste) si chiama l'*inverso* di x e si indica con x^{-1} . Se x ha l'inverso, x si dice *invertibile*. La potenza n -sima di x si indica con x^n . Se x è invertibile, anche x^n lo è e risulta $(x^n)^{-1} = (x^{-1})^n$.

Se sull'insieme X sono definite due operazioni associative, esse si indicano solitamente con $+$ (addizione) e \cdot (moltiplicazione). Ad esempio si parla di addizione e moltiplicazione di polinomi o matrici.

Esempi: Ogni elemento di \mathbb{Z} , \mathbb{Q} , \mathbb{R} , \mathbb{C} ha un opposto. Gli elementi di \mathbb{Z} invertibili rispetto alla moltiplicazione sono soltanto 1 e -1 . Ogni elemento non nullo di \mathbb{Q} , \mathbb{R} , \mathbb{C} è invertibile.

Ogni matrice in $\mathcal{M}_{n,m}(\mathbb{R})$ ha un opposto. Le matrici invertibili di $\mathcal{M}_n(\mathbb{R})$ sono tutte e sole quelle con determinante non nullo.

Strutture Algebriche

Una *struttura algebrica* è un insieme X su cui sono definite alcune operazioni binarie $*_1, \dots, *_n$ che soddisfano certe proprietà. Una tale struttura algebrica si indica con $(X, *_1, \dots, *_n)$.

Ricordiamo le definizioni di alcune strutture algebriche introdotte nel corso di AL110 che studieremo più a fondo.

$(S, *)$ è un *semigrupp* se $*$ è associativa.

Un semigrupp $(S, *)$ si dice *commutativo*, se $*$ è commutativa e S si dice *unitario*, o un *monoide*, se esiste l'elemento neutro.

$(G, *)$ è un *gruppo* se è un semigrupp unitario ed ogni elemento è simmetrizzabile. Dunque $(G, *)$ è un *gruppo* se:

(g1) $*$ è associativa;

(g2) esistenza dell'elemento neutro: esiste $e \in G$ tale che $e * g = g = g * e$, per ogni $g \in G$ (e è necessariamente unico);

(g3) esistenza del simmetrico: per ogni $g \in G$, esiste un elemento $g' \in G$ tale che $g * g' = e = g' * g$ (g' è necessariamente unico).

Un gruppo $(G, *)$ si dice *commutativo* se $*$ è commutativa. Un gruppo commutativo si chiama anche *abeliano*, dal matematico norvegese N. H. Abel, che per dimostrare la risolubilità per radicali di alcune equazioni polinomiali considerò certi gruppi di permutazioni commutativi (1829).

In un gruppo ogni elemento è cancellabile (a destra e sinistra), perché è simmetrizzabile.

Esempi: $(\mathbb{N}, +)$ è un semigrupp commutativo. $(\mathbb{Z} \setminus \{0\}, \cdot)$, $(\mathcal{P}(A), \cup)$, $(\mathcal{P}(A), \cap)$ sono semigruppi commutativi unitari. $(\mathcal{M}_n(\mathbb{Q}) \setminus \{0\}, \cdot)$ è un semigrupp unitario non commutativo. L'insieme $\mathcal{F}(A, A)$ delle funzioni di dominio e codominio A è un semigrupp unitario e non commutativo rispetto alla composizione di funzioni.

$(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{Z}_n, +)$, $(\mathcal{M}_{n,m}(\mathbb{R}), +)$ sono gruppi commutativi. L'insieme $(\mathcal{T}(A), \cdot)$ delle trasformazioni su A , in particolare il gruppo S_n delle permutazioni su n elementi, è un gruppo non commutativo rispetto alla composizione di funzioni.

Se sull'insieme X sono definite due operazioni associative, esse si indicano solitamente con $+$ (addizione) e \cdot (moltiplicazione).

$(A, +, \cdot)$ è un *anello* se:

(a1) $(A, +)$ è un gruppo commutativo;

(a2) (A, \cdot) è un semigrupp;

(a3) valgono le proprietà distributive della moltiplicazione rispetto alla somma.

Un anello $(A, +, \cdot)$ si dice *commutativo* se (A, \cdot) è un semigrupp commutativo e A si dice *unitario* se (A, \cdot) è un semigrupp unitario. In questo caso, l'unità di (A, \cdot) si chiama l'*unità* di A e si indica con 1_A (o semplicemente con 1 se non ci sono ambiguità). Supporremo sempre $1 \neq 0$.

Un anello commutativo unitario in cui ogni elemento non nullo è invertibile si chiama un *campo*. Dunque $(K, +, \cdot)$ è un *campo* se

(c1) $(K, +)$ è un gruppo commutativo;

(c2) $(K \setminus \{0\}, \cdot)$ è un gruppo commutativo;

(c3) valgono le proprietà distributive della moltiplicazione rispetto alla somma.

Esempi: $(\mathbb{Z}, +, \cdot)$ è un anello commutativo unitario. Se $P \subseteq \mathbb{Z}$ è l'insieme dei numeri pari, $(P, +, \cdot)$ è un anello commutativo non unitario. $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sono campi.

Se A è un anello (commutativo, unitario), l'insieme $A[X]$ dei polinomi su A è un anello (commutativo, unitario), rispetto all'addizione e moltiplicazione di polinomi. L'insieme delle matrici quadrate su A $(\mathcal{M}_n(A), +, \cdot)$ è un anello non commutativo (unitario), rispetto all'addizione di matrici e moltiplicazione righe per colonne.

Zero-divisori

Sia $(A, +, \cdot)$ un anello. Un elemento $a \in A$ si chiama uno *zero-divisore sinistro*, rispettivamente *destro*, se esiste $b \neq 0$ tale che $ab = 0$, rispettivamente $ba = 0$.

L'elemento 0 è uno zero-divisore. Infatti $0a = 0 = a0$, per ogni $a \in A$. Per vedere questo, notiamo che $0 = x - x$, per ogni $x \in A$. Allora

$$a0 = a(b - b) = ab - ab = 0.$$

Analogamente $0a = 0$.

Un anello A si dice *intero* se non ha zero-divisori non nulli. A si chiama un *dominio intero*, o semplicemente un *dominio*, se è commutativo unitario e intero.

Se A è un anello commutativo e unitario, la proprietà di essere intero (ovvero un dominio) si esprime attraverso la:

Legge di annullamento del prodotto:

$$ab = 0 \Leftrightarrow a = 0 \text{ oppure } b = 0.$$

Gli anelli di numeri sono domini interi.

Gli zero-divisori di \mathbb{Z}_n sono le classi degli interi a tali che $MCD(a, n) \neq 1$.

Se A è un dominio, ogni elemento è cancellabile, cioè vale la

Legge di cancellazione: Se $a \neq 0$, allora

$$ba = ca \Rightarrow b = c; \quad ab = ac \Rightarrow b = c.$$

Infatti, $ba = ca \Rightarrow (b - c)a = 0$ e, per la legge di annullamento del prodotto, $b - c = 0$, cioè $b = c$.

Analogamente per la cancellazione a sinistra.

Il gruppo delle unità di un anello

Se $*$ è una operazione su X e $Y, Z \subseteq X$ sono sottoinsiemi poniamo

$$Y * Z = \{y * z; y \in Y, z \in Z\}.$$

Evidentemente $Y * Z \subseteq X * X \subseteq X$.

In particolare $Y * Y \subseteq X$, ma può essere che $Y * Y \not\subseteq Y$. Ad esempio, poiché la somma di due numeri dispari è pari, se D è l'insieme dei numeri interi relativi dispari, risulta $D + D \not\subseteq D$.

Diciamo che Y è *chiuso rispetto a ** se $Y * Y \subseteq Y$, ovvero la restrizione di $*$ al sottoinsieme Y è una operazione su Y .

Ad esempio, il sottoinsieme P dei numeri interi relativi pari è chiuso rispetto all'addizione, ma il sottoinsieme D dei numeri dispari non lo è.

Se $(S, *)$ è un semigrupp unitario, l'insieme $\mathcal{U}(S)$ degli elementi simmetrizzabili di S è un gruppo rispetto a $*$. Infatti:

(g1) $*$ è un'operazione associativa su $\mathcal{U}(S)$, ovvero $\mathcal{U}(S) * \mathcal{U}(S) \subseteq \mathcal{U}(S)$: se x, y sono simmetrizzabili, con simmetrico x' e y' rispettivamente, $x * y$ è simmetrizzabile con simmetrico $y' * x'$. Inoltre $*$ è associativa, perché lo è su X .

(g2) Esistenza dell'elemento neutro: l'elemento neutro e di S è simmetrizzabile, dunque $e \in \mathcal{U}(S)$ ed è ovviamente anche l'elemento neutro di $\mathcal{U}(S)$;

(g3) Esistenza del simmetrico: ogni $x \in \mathcal{U}(S)$ ha un simmetrico x' in S . Ma anche x' è simmetrizzabile, con simmetrico x . Dunque $x' \in \mathcal{U}(S)$.

Se $(A, +, \cdot)$ è un anello unitario, il gruppo degli elementi invertibili del semigrupp (A, \cdot) si chiama il *gruppo degli elementi invertibili di A* , o il *gruppo delle unità di A* , e si indica con $\mathcal{U}(A)$.

Esempi: $\mathcal{U}(\mathcal{F}(X, X)) = \mathcal{T}(X)$ è costituito dalle funzioni biettive sull'insieme X .

$$\mathcal{U}(\mathbb{Z}) = \{1, -1\}. \quad \mathcal{U}(\mathbb{Z}[X]) = \mathcal{U}(\mathbb{Z}) = \{1, -1\}.$$

$\mathcal{U}(\mathbb{Z}_n)$ è costituito dalle classi degli interi coprimi con n .

Se K è un campo, $\mathcal{U}(K) = K \setminus \{0\}$ e $\mathcal{U}(K[X]) = \mathcal{U}(K) = K \setminus \{0\}$.

$\mathcal{U}(\mathcal{M}_n(K))$ è costituito dalle matrici con determinante non nullo. Questo gruppo si chiama il *gruppo lineare generale di grado n su K* e si indica con $GL_n(K)$.

Se A è commutativo e unitario, il gruppo $\mathcal{U}(A)$ degli elementi invertibili di A è disgiunto dall'insieme degli zero-divisori di A .

Infatti, sia $a \in A$. Se $ab = 1 = ba$, necessariamente $a \neq 0$. Se $ac = 0$, si ha $c = (ba)c = b(ac) = b0 = 0$.

Sottostrutture

Sono interessanti i sottoinsiemi Y di una struttura algebrica $(X, *_1, \dots, *_n)$ che hanno la stessa struttura algebrica di X rispetto a tutte le operazioni $*_i$. In questo caso si dice che $(Y, *_1, \dots, *_n)$ è una *sottostruttura algebrica* di X . Perché Y sia una sottostruttura algebrica di X , la prima condizione è che Y sia chiuso rispetto alle operazioni $*_1, \dots, *_n$.

Notiamo che se le proprietà associativa, commutativa, distributiva valgono su X , esse valgono anche su Y .

Se $(S, *)$ è un semigruppato, un sottoinsieme di S è un *sottosemigruppato* di S se e soltanto se è chiuso rispetto a $*$.

Se $(G, *)$ è un semigruppato unitario, in particolare un gruppo, un sottoinsieme H di G è un *sottogruppo* se e soltanto se:

(sg0) $H * H \subseteq H$, cioè H è chiuso rispetto ad $*$;

(sg1) $e \in H$;

(sg2) se $g \in H$, g è simmetrizzabile e il simmetrico di g appartiene ad H .

Se $(A, +, \cdot)$ è un anello, in particolare un campo, un sottoinsieme B di A è un *sottoanello* se e soltanto se:

(sa1) $(B, +)$ è un sottogruppo di $(A, +)$;

(sa2) (B, \cdot) è un sottosemigruppato di (A, \cdot) (cioè B è chiuso rispetto alla moltiplicazione).

Inoltre, un sottoinsieme F di A è un *sottocampo* se e soltanto se:

(sc1) $(F, +)$ è un sottogruppo di $(A, +)$;

(sa2) $(F \setminus \{0\}, \cdot)$ è un sottogruppo commutativo del semigruppato $(A \setminus \{0\}, \cdot)$.

È facile verificare che:

(a) Se G è un gruppo, un suo sottoinsieme H è un sottogruppo se e soltanto se, per ogni $x, y \in H$, risulta $x * y^{-1} \in H$.

(b) Se A è un anello, un suo sottoinsieme B è un sottoanello se e soltanto se, per ogni $x, y \in B$, risulta $x - y \in B, xy \in B$.

(b) Se K è campo, un suo sottoinsieme F è un sottocampo se e soltanto se, per ogni $x, y \in F, y \neq 0$, risulta $x - y \in F, xy^{-1} \in F$.

Esempi:

$(\mathbb{N}, +)$ è un sottosemigruppo di $(\mathbb{Z}, +)$.

$(\mathbb{Z}, +, \cdot)$ è un sottoanello del campo $(\mathbb{Q}, +, \cdot)$. $(P, +, \cdot)$ è un sottoanello di $(\mathbb{Z}, +, \cdot)$. Le matrici diagonali costanti costituiscono un sottocampo dell'anello (non commutativo) delle matrici reali $(\mathcal{M}_n(\mathbb{R}), +, \cdot)$.

Se $(A, +, \cdot)$ è un anello, il gruppo delle unità di A è un sottogruppo del semigruppato moltiplicativo (A, \cdot) .

Se $S \subseteq X$ è un sottoinsieme, la più piccola sottostruttura di X contenente S si chiama la *sottostruttura generata da S* e si indica con $\langle S \rangle$. Ad esempio parleremo di sottogruppi o sottoanelli generati da un sottoinsieme S .

L'insieme delle sottostrutture di una struttura algebrica X è parzialmente ordinato rispetto all'inclusione ed inoltre è un reticolo. Precisamente, se Y_1 e Y_2 sono sottostrutture di X , allora $Y_1 \cap Y_2$ è ancora una sottostruttura e $\inf(Y_1, Y_2) = Y_1 \cap Y_2$. Inoltre $\sup(Y_1, Y_2) = \langle Y_1 \cup Y_2 \rangle$.

Questo reticolo ha un massimo, dato da X