Algebra I

Paolo Bettelini

Contents

1 Richiami di teoria degli insiemi

Data una famiglia finita o infinite di insiemi $\{A_i\}_{i\in I}$, la loro intersection

$$\bigcap_{i\in I} A_i$$

è l'insieme degli elementi che stanno in tutti gli insiemi A_i, mentre la loro unione

$$\bigcup_{i\in I} A_i$$

è l'insieme degli elementi che stanno in almeno uno degli insiemi A_i.

2 Classi di equivalenza

Esempio insieme quoziente $\sim$ su $\mathbb{Z}$ dove $a \sim b \iff |a| = |b|$ è dato da

$$\{\{0\}, \{1, -1\}, \{2, -2\}, \cdots\}$$

L'unica relazione di equivalenza che è un ordine è l'uguaglianza.

3 Esempi di maggiorante etc.

In $\mathbb{R}$ consideriamo l'usuale ordinamento. Consideriamo i sottoinsiemi

$$A = \{x \in \mathbb{R} \,|\, x > 0\}$$

$$B = \{x \in \mathbb{R} \,|\, x \geq 0\}$$

e

$$C = \{x \in \mathbb{R} \,|\, 0 < x \leq 2\}$$

Il sottoinsieme A non ha maggioranti. Ogni numero non-positivo è minorante di A. A non ha nè massimo nè minimo.

Il sottoinsieme B non ha maggioranti. Ogni numero non-positivo è minorante di B. B ha 0 come minimo.

Il sottoinsieme C ha minoranti e maggioranti ma non minimo e ho 2 come massimo.

Consideriamo ora la relazione di divisibilità in $\mathbb{N}$. L'unico maggiorante è 0 in quanto tutti dividono zero, ed è un massimo. Il numero 1 è minorante, ed è un minimo.

Se ora prendiamo l'insieme $\{2, 3, 4, 5\}$, i maggioranti sono mulitpli del minimo comune multiplo (60), i minoranti sono i divisori comuni. Non ci sono massimo e minimo.

Proposition Il massimo è unico

Il massimo, se esiste, è unico.

Proof Il massimo è unico

Diciamo che a, b sono due massimi di A, cioè maggioranti di A che appartiene ad A. Abbiamo allora $a \geq b$ (in quanto a è un maggiorante) e $b \geq a$ (in quando b è un maggiorante). Abbiamo quindi che $a = b$.

Definizione Massimale

Un elemento $a \in A$ con A insieme partzialmente ordinato è detto massimale in A se non esiste alcun $b \in A$ tale che $a \leq b$ dove $a \neq b$.

Definizione Minimale

Un elemento $a \in A$ con A insieme partzialmente ordinato è detto minimale in A se non esiste alcun $b \in A$ tale che $a \geq b$ dove $a \neq b$.

Ogni massimo è massimale, ogni minimo è minimale.

Esempio in cui i massimali non sono massimi: in $\mathbb{N}$, rispetto alla divisibilità, consideriamo l'insieme $A = \{2, 3, 4, 5, 6\}$.

- Il numero 2 è minimale ma non massimale.
- Il numero 3 è minimale ma non massimale.
- Il numero 4 è massimale perché non divide nient'altro, ma non minimale.
- Il numero 5 è sia massimale che minimale.
- Il numero 6 è massimale ma non minimale.

In una relazione d'ordine totale un eventuale elemento massimale è massimo. Infatti, se a è massimale per A, preso un qualsiasi elemento $b \in A$, sappiamo che vale almeno una tra $a \leq b$ e $b \leq a$. Se vale la prima, per la definizione di massimalità di a, non può essere $a \neq b$. Nel secondo caso, $b \leq a$ e quindi a è un massimo. Analogamente per i minimali.

3.1 Relazioni irriflessiva

Data una relazione d'ordine $\leq$, possiamo ottenere la relazione d'ordine stretta $<$ dicendo che $a < b$ se $a \leq b$ e $a \neq b$.

Si può definire l'ordine stretto rimpiazzando la proprietà riflessiva con quella irriflessiva.

4 Funzioni

Una funzione $\phi\colon A \to B$ dove A è il dominio mentre B è il codominio, preso un elemento $a \in A$, la sua immagine viene denotata $\phi(a)$ oppure af.

Se $C \subseteq A$, la sua immagine tramite ϕ è indicata come $C\phi$ che è un sottoinsieme di B.

$$C\phi = \{c\phi \,|\, c \in C\}$$

Se D è un sottoinsieme di B, la sua immagine inversa tramite ϕ è il sottoinsieme $D\phi^{-1}$ di A degli elementi la cui immagine appartiene a D.

$$D\phi^{-1} = \{a \in A \,|\, a\phi \in D\}$$

Esempio Funzione

Sia $\phi\colon \mathbb{R} \to \mathbb{R}$ definita ponendo $\phi x \triangleq x^2$.

Consideriamo ora $A = \{-1, 0, 1, 2\}$. Abbiamo allora $A\phi = \{1, 0, 4\}$. Consideriamo poi $B = \{-1, 0, 2, 9\}$. Abbiamo allora $B\phi^{-1} = \{0, \sqrt{2}, 3, -3\}$.

L'immagine di una funzione è chiaramente l'immagine per il suo dominio come insieme considerato.

4.1 Proprietà

Proposition

Se $C \subseteq D \subseteq A$, abbiamo $C\phi \subseteq D\phi$.

Proof

Abbiamo che

$$C\phi = \{c\phi \,|\, c \in C\}$$

Dunque $x \in C\phi$ se e solo se esiste $c \in C$ tale che $x = c\phi$. Ma $C \subseteq D$, dunque $c \in D$. Quindi, $x = c\phi \in D\phi$.

Non è detto che se $C \subset D$ allora $C\phi \subset D\phi$. Mostriamo un esempio in cui $C \subset D$ ma $C\phi = D\phi$. Prendiamo $C = \{1\} \subset D = \{1, -1\}$. Se prendiamo la funzione del quadrato, in ambo caso trovo la stessa immagine per via di ambo gli insiemi.

Ciò non avviene nel caso in cui la funzione fosse iniettiva.

Proposition

Se $E \subseteq F \subseteq B$, abbiamo che $E\phi^{-1} \subseteq F\phi^{-1}$.

TODO: esercizio proof.

Anche qui la medesima proposizione ma con l'inclusione stretta non è assicurata.

Proposition
Se $C \subseteq A$, allora $C\phi\phi^{-1} \supseteq C$.

Proof
Sia $x \in C$. Bisogna mostrare $x \in C\phi\phi^{-1}$. Ricordiamo che $D\phi^{-1} = \{y \in A \mid y\phi \in D\}$. Dunque $Cy\phi = \{y \in A \mid y\phi \in C\phi\}$. Ma ora $x\phi \in C\phi$, perché $x \in C$. Dunque $x \in C\phi\phi^{-1}$.

Nel solito esempio

$$\{1, -1\}\phi\phi^{-1} = \{1, -1\}$$

e

$$\{1\}\phi\phi^{-1} = \{1, -1\}$$

Proposition
Se $D \subseteq B$ allora $D\phi^{-1}\phi \subseteq D$. L'inclusione può essere stretta.

Proof
Sia $x \in D\phi^{-1}\phi$. Ciò significa che $x = z\phi$ per qualche $z \in D\phi^{-1}$. Ma $D\phi^{-1} = \{y \mid y\phi \in D\}$. Dunque, $z \in D\phi^{-1}$, allora $z\phi \in D$, cioè $x \in D$.

Con il solito esempio

$$\{1, 2\}\phi^{-1}\phi = \{1\}$$
$$\{-1\}\phi^{-1}\phi = \emptyset$$

Proposition
Siano $\phi\colon A \to B$, $\psi\colon B \to C$ e $\theta\colon C \to D$ funzioni. allora

$$(\phi\psi)\theta = \phi(\psi\theta)$$

Proof
Notiamo che $\phi\psi\colon A \to C$ e $\theta\colon C \to D$. Dunque $\phi\psi\colon A \to D$. Analogamente $\phi\colon A \to B$, $\psi\theta\colon B \to D$ e quindi $\phi(\psi\theta)\colon A \to D$. Per mostrare l'uguaglianua devo mostrare che per ogni $x \in A$ risulta

$$a((\phi\psi)\theta) = a(\phi(\psi\theta))$$

Abbiamo infatti $a((\phi\psi)\theta) = (a(\phi\psi\theta)) = ((a\phi)\psi)\theta$ e $a(\phi(\psi\theta)) = (a\phi)(\psi\theta) = ((a\phi)\psi)\theta$.

Dunque possiamo scrivere semplicemente $\phi\psi\theta$ senza ambiguità.

Siano $\phi\colon A \to B$, $\psi\colon B \to C$ funzioni. Ci chiediamo ora che $\psi\phi = \phi\psi$. Chiaramente, non è detto che $\phi\psi$ esista. Possiamo confrontarle solo che $A = B$.

Allora guardiamo $\phi\colon A \to A$ e $\psi\colon A \to A$. Non è comunque detto che $\psi\phi = \phi\psi$ siano uguali.

Definizione Funzione identità
Dato un insieme A, la *funzione identica* di A è la funzione $\mathrm{Id}_A\colon A \to A$ definita come $a\mathrm{Id}_A \triangleq a$.

Proposition
Sia $\phi\colon A \to B$, allora $\phi\mathrm{Id}_B = \phi$ e $\mathrm{Id}_A\phi = \phi$.