Algebra

Manuel Mignogna

December 12, 2023

Contents

1 Assiomi

1.1 Assioma del Vuoto

Esiste un insieme, detto l'insieme vuoto $\emptyset$, che non contiene nulla.

$$\exists \emptyset \ (\forall x \ (x \notin \emptyset))$$

1.2 Assioma di Estensionalità

Due insiemi coincidono se e solo se ogni elemento del primo insieme appartiene al secondo e viceversa.

$$\forall x, y \ (x = y \iff \forall z \ (z \in x \iff z \in y))$$

1.3 Assioma di Separazione

Esiste sempre l'insieme degli elementi di un insieme s che verificano un predicato ρ.

$$\{x \mid x \in s \wedge \rho(x)\}$$

1.4 Assioma di Esistenza dell'insieme delle Parti

Per ogni insieme s esiste l'insieme delle parti $\mathcal{P}(s)$, ovvero l'insieme di tutti i sottoinsiemi di s.

$$\forall s \ \exists \mathcal{P}(s) \ (\forall x \ (x \in \mathcal{P}(s) \iff x \subseteq s))$$

1.5 Assioma della Coppia

Per ogni coppia si insiemi x, y esiste l'insieme coppia $\{x, y\}$.

$$\forall x, y \ \exists c \ (\forall z \ (z \in c \iff (z = x \vee z = y)))$$

1.6 Assioma di Unione

Per ogni insieme di insiemi a esiste l'insieme unione unaria di a, cioè l'insieme unione di tutti gli insiemi che sono elementi di a.

$$\forall a \; \exists u \; (\forall x \; (\exists y \; (x \in u \iff (z \in y \land y \in a))))$$

1.7 Assioma della Scelta

Data una famiglia non vuota di insiemi non vuoti esiste una funzione che ad ogni insieme della famiglia fa corrispondere un suo elemento.

1.8 Assioma dell'infinito

Esiste un insieme infinito, e tale insieme è $\mathbb{N}$.

2 Teoremi derivanti dagli assiomi

2.1 Unicità dell'insieme vuoto

Proof. Siano a e b due insiemi vuoti. Dalla definizione di insieme vuoto segue che, per ogni elemento generico x:

$$\forall x \; (x \notin a \land x \notin b)$$

Le implicazioni

$$x \in a \implies x \in b$$

$$x \in b \implies x \in a$$

sono entrambe vere perchè l'antecedente è sempre falso.
Pertanto per l'assioma di estensionalità

$$(x \in a \iff x \in b) \implies a = b$$

Quindi esiste un unico insieme vuoto. □

2.2 Ogni insieme contiene l'insieme vuoto

Proof. La formula

$$\forall z \ (z \in \emptyset \implies z \in \emptyset)$$

è una tautologia perchè $z \in \emptyset$ è sempre falso e dunque l'implicazione è vera. Pertanto $\emptyset \subseteq \emptyset$. Similarmente, la formula

$$\forall x \ \forall z \ (z \in \emptyset \implies z \in x)$$

è una tautologia, pertanto $\forall x \ (\emptyset \subseteq x)$ □

2.3 Unicità dell'insieme delle parti

Proof. Sia x un insieme e siano u e w insiemi delle sue parti. Dall'assioma di esistenza dell'insieme delle parti abbiamo che

$$\forall z \ (z \in u \iff z \subseteq x)$$

$$\forall z \ (z \in w \iff z \subseteq x)$$

Da questo segue che

$$\forall z \ (z \in u \iff z \subseteq x \iff z \in w)$$

e quindi

$$\forall z \ (z \in u \iff z \in w)$$

Dall'assioma di estensionalità si ha dunque che $u = w$. □

2.4 Paradosso di Russel

Non esiste l'insieme degli insiemi che non appartengono a se stessi.

Proof. Ipotizziamo per assurdo che tale insieme esita

$$r := \{x \mid x \notin x\}$$

Esistono solo due possibilità: $r \in r$ oppure $r \notin r$. Se $r \in r$, allora per definizione non appartiene a sé stesso

$$r \in r \implies r \notin r$$

il che è chiaramente assurdo. Se $r \notin r$, allora è un insieme che non appartiene a se stesso, e deve per definizione appartenere a se stesso

$$r \notin r \implies r \in r$$

il che è chiaramente assurdo. □

2.5 L'insieme di tutti gli insiemi non esiste

Proof. Sia $f(x) = \neg(x \in x)$ ed assumiamo per assurdo che esista I l'insieme di tutti gli insiemi. Allora, definiamo $r = \{x \in I \mid f(x)\}$, che dovrebbe esistere per l'assioma di separazione ma che non può esistere per il paradosso di Russell. Si ha quindi l'assurdo. □

2.6 Parti del Vuoto

$\emptyset$ è un insieme, quindi dall'assioma di esistenza dell'insieme delle parti segue che deve esistere $P(\emptyset)$. A cosa è uguale?

$$\mathcal{P}(\emptyset) = \{x \subseteq \emptyset \iff \forall z \ (z \in x \implies z \in \emptyset)\}$$

C'è un solo insieme tale che ogni suo elemento z appartiene anche all'insieme vuoto... l'insieme vuoto stesso!
Pertanto $\mathcal{P}(\emptyset) = \{\emptyset\}$ cioé il singleton dell'insieme vuoto. Proviamo adesso a chiederci, chi è $\mathcal{P}(\mathcal{P}(\emptyset))$, cioè $\mathcal{P}(\{\emptyset\})$.
Un insieme è sottoinsieme di $\{\emptyset\}$ soltanto se è l'insieme vuoto (abbiamo dimostrato tramite un teorema che l'insieme vuoto è sottoinsieme di ogni insieme) oppure se è $\{\emptyset\}$ stesso (dato che ogni insieme è proprio sottoinsieme). Da questo segue che:

$$\mathcal{P}(\mathcal{P}(\emptyset)) = \mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$$

3 Operazioni tra Insiemi

3.1 Leggi di De Morgan

$\forall a, b, c$

$$c - (a \cup b) = (c - a) \cap (c - b)$$
$$c - (a \cap b) = (c - a) \cup (c - b)$$

Proof.

$$\begin{aligned}
c - (a \cup b) &= \{z \in c \mid \neg(z \in (a \cup b))\} \text{ (def. di diff. di insiemi)} \\
&= \{z \in c \mid \neg(z \in a \vee z \in b)\} \text{ (def. di unione)} \\
&= \{z \in c \mid \neg(z \in a) \wedge \neg(z \in b)\} \text{ (De Morgan)} \\
&= \{z \mid (z \in c) \wedge (\neg(z \in a) \wedge \neg(z \in b))\} \text{ (ass. di separazione)} \\
&= \{z \mid ((z \in c) \wedge \neg(z \in a)) \wedge ((z \in c) \wedge \neg(z \in b))\} \\
&\text{(distrib. di and su and)} \\
&= \{z \mid (z \in (c - a)) \wedge (z \in (c - b)\} \text{ (def. di diff. di insiemi)} \\
&= (c - a) \cap (c - b) \text{ (def. di intersezione)}
\end{aligned}$$

□

3.2 Unione di Insiemi

Dati due insiemi A e B, definiamo:

$$A \cup B = \bigcup \{A, B\}$$

Questo insieme esistente sicuramente grazie agli assiomi d'unione e della coppia.

3.3 Intersezione di Insiemi

Dati due insiemi A e B, definiamo:

$$A \cap B = \{x \mid x \in A \wedge x \in B\}$$

Che è un insieme sicuramente esistente per l'assioma di separazione.

3.4 Insiemi Disgiunti

Due insiemi a e b si dicono disgiunti se e solo se $a \cap b = \emptyset$

3.5 Differenza di Insiemi

Dati due insiemi A e B, definiamo la differenza di insiemi come:

$$B - A = \{Z \in B \mid Z \notin A\}$$

Che è sicuramente un insieme grazie all'assioma di separazione.

3.6 Differenza Simmetrica di Insiemi

Definiamo la differenza simmetrica di a e b come:

$$a \triangle b = \{x \in a \cup b \mid x \in a \oplus x \in b\}$$

Che è un insieme sicuramente esistente per l'assioma di separazione.

3.7 Coppia Ordinata

Dati x, y due insiemi. Allora definiamo la coppia ordinata (x, y) come:

$$(x, y) := \{\{x\}, \{x, y\}\}$$

3.8 Caratterizzazione di Coppie Ordinate

$$x = y \iff (x, y) = (y, x)$$

Proof. Dimostriamo

$$x = y \implies (x, y) = (y, x)$$

Si ha che:

$$x = y \implies (\{x\} = \{y\}) \wedge (\{x, y\} = \{y, x\} = \{x, x\} = \{x\})$$

E dunque:

$$(x, y) = \{\{x\}, \{x, y\}\} = \{\{x\}, \{x\}\} = \{\{x\}\}$$
$$(y, x) = \{\{y\}, \{y, x\}\} = \{\{x\}, \{x\}\} = \{\{x\}\}$$

Dunque $(x, y) = (y, x)$
Dimostriamo

$$(x, y) = (y, x) \implies x = y$$

Allora

$$\{\{x\}, \{x, y\}\} = \{\{y\}, \{y, x\}\}$$

e dunque $\{x\}$ è membro sia del primo insieme che del secondo per estensionalità e allora

$$\{x\} = \{y\} \vee \{x\} = \{x, y\}$$

In entrambi i casi, ciò implica la tesi. □

3.9 Ennupla Ordinata

Iniziamo col definire la terna ordinata come:

$$(x, y, z) = ((x, y), z)$$

Dunque, dati n+1 elementi $i_1, i_2, i_3, ..., i_n, i_{n+1}$ allora definiamo la ennupla ordinata di n+1 elementi come:

$$(i_1, i_2, i_3, ..., i_n, i_{n+1}) = ((i_1, i_2, i_3, ..., i_n), i_{n+1})$$

3.10 Prodotto Cartesiano

$$a \times b := \{z \in \mathcal{P}(\mathcal{P}(a \cup b)) \mid \exists x, y \ (x \in a \wedge y \in b \wedge z = (x, y))\}$$

3.11 Corrispondenza fra Insiemi

Dati due insiemi a e b e $g \subseteq a \times b$, la coppia ordinata $(a \times b, g)$ si definisce corrispondenza fra a e b di grafico g.

Data una corrispondenza fra due insiemi a e b $\rho = (a \times b, g)$. Dati $x \in a$ e $y \in b$ scriveremo:

$$x \rho y \iff (x, y) \in g$$

e diremo che x ed y sono in corrispondenza o relazione fra loro.

$\rho = (a \times b, g)$

$$\forall x \in a$$

$$\forall y \in b$$

$$(x, y) \in g \iff \varphi(x, y)$$

Cioè stiamo definendo g in base ad una proprietà definita dalla formula binaria $\varphi(x_1, x_2)$.

3.12 Definizione di Relazione Binaria

Dato un insieme a, una corrispondenza fra a ed a stesso si definisce relazione binaria.

3.13 Insieme delle Corrispondenze

Dati due insiemi a e b, notiamo con $CORR(a, b)$ l'insieme delle corrispondenze definibili fra a e b.

3.14 Insieme delle Relazioni

Dato un insieme a, notiamo con $REL(a)$ l'insieme delle relazioni binarie definibili su a. Si nota chiaramente che $REL(a) = CORR(a, a)$.

3.15 Definizione di Applicazione/Funzione

Sia f una corrispondenza fra due insiemi a e b. La definiremo:

$$f = (a \times b, g) \text{ applicazione} : \iff \forall x \in a \; \exists! y \in b \; (xfy)$$

Che equivale a dire:

$$f = (a \times b, g) \text{ applicazione} : \iff \forall x \in a \; \exists! y \in b \; ((x, y) \in g)$$

Descrizione esplicita di una funzione

$$f : x \in a \mapsto f(x) \in b$$

Esempio: $f : x \in \mathbb{N} \mapsto (n + 1) \in \mathbb{N}$

3.16 Dominio e Codominio di un'Applicazione

Data un'applicazione $f = (a \times b, g)$, chiameremo a il dominio di f e b il codominio di f.

3.17 Immagine di un'Applicazione

Data una funzione $f = (a \times b, g)$, definiremo l'insieme immagine di f

$$Im(f) = \{y \in b \mid \exists x \in a \; (f(x) = y)\}$$

Definizione Alternativa Semplificata della Notazione di $Im(f)$

$$Im(f) = \{f(x) \mid x \in a\}$$

Chiaramente questa non è, da sola una formula ben formata, ed è per questo che utilizziamo la definizione originale di $Im(f)$.

3.18 Funzione Ben Posta

Definiremo come ben posta ogni corrispondenza che sia un'applicazione. Ovviamente, ciò è equivalente a dire che la funzione è, difatti, una funzione. E' un modo colloquiale per assicurare che una data corrispondenza che chiamiamo funzione è una funzione per davvero, dato che non è sempre ovvio se una corrispondenza sia una funzione o meno.

3.19 Definizione di Prodotto Relazionale (o tra Corrispondenze)

Siano a, b, c, d insiemi e siano $\rho = (a \times b, g_1)$ e $\sigma = (c \times d, g_2)$ due corrispondenze. Definiamo quindi il prodotto relazionale come la corrispondenza $\rho\sigma = (a \times d, g_3)$ tale che:

$$\forall x \in a$$

$$\forall y \in d$$

$$(x, y) \in g_3 \iff \exists z \ ((x, z) \in g_1 \land (z, y) \in g_2)$$

3.20 Associatività del Prodotto Relazionale

Date tre corrispondenze σ, ρ, φ, volgiamo dimostrare che:

$$\sigma(\rho\varphi) = (\sigma\rho)\varphi$$

Proof.

$$(x, y) \in g_{\sigma(\rho\varphi)} \implies \exists z : \ (x, z) \in g_\sigma \land (z, y) \in g_{\rho\varphi}$$

$$\implies \exists w : \ (z, w) \in g_\rho \land (w, y) \in g_\varphi$$

$$\implies (x, w) \in g_{\sigma\rho} \land (w, y) \in g_\varphi$$

$$\implies (x, y) \in g_{(\sigma\rho)\varphi}$$

La dimostrazione inversa è analoga. □

3.21 Composizione di Applicazioni

Date due funzioni

$$f : a \to b$$

$$g : b \to c$$

definiamo la funzione

$$g \circ f = fg$$

(cioè prodotto relazionale di f e g), e la chiamiamo "g composta f" o "composta di g e f".
Forma esplicita della composizione di funzioni

$$g \circ f : x \in a \to g(f(x)) \in c$$

3.22 Funzione Immersione

Siano due insiemi $a, b : a \subseteq b$. Allora la funzione

$$f : x \in a \to x \in b$$

si dice immersione di a in b.

3.23 Funzione Identità

La funzione

$$Id_a : x \in a \to x \in a$$

si dice identità di a.

3.24 Restrizione di una Funzione

Data una funzione $f : a \to b$, definito $s \subseteq a$, allora definiamo la restrizione di f in s la funzione:

$$f_{|s} : x \in s \mapsto f(x) \in b$$

3.25 Prolungamento di una Funzione

Data una funzione $f : a \to c$, una funzione $g : b \to c$ si dice prolungamento di f se $\exists s \subseteq b : g_{|s} = f$, cioè se esiste un sottoinsieme di b uguale ad a.

3.26 Funzione Ridotta / Riduzione di una Funzione

Dati $f : a \to b$, $s \subseteq b : Im_f \subseteq s$, la funzione

$$g : x \in a \mapsto f(x) \in s$$

si chiama ridotta di f ad s.

3.27 Applicazione Costante

Dati due insiemi a, b e $\overline{y} \in b$. La funzione

$$f : x \in a \to \overline{y} \in b$$

si dice funzione costante di valore $\overline{y}$

3.28 Funzione Immagine

$$\overrightarrow{f} : \ \overline{a} \in \mathcal{P}(a) \to \{f(z) \mid z \in \overline{a}\} \in \mathcal{P}(b)$$

3.29 Funzione Antimmagine

$$\overleftarrow{f} : \ \overline{b} \in \mathcal{P}(b) \to \{z \in a \mid f(z) \in \overline{b}\} \in \mathcal{P}(a)$$

3.30 Immagine di un Insieme

Dato un insieme a e una funzione $f : a \to b$, definiamo l'immagine di a come:

$$Im(a) = \{f(x) \mid x \in a\}$$

3.31 Antimmagine di un Insieme

Data una funzione $f : a \to b$ ed un insieme $s \subseteq b$, definiamo l'antimmagine (o controimmagine, preimmagine, immagine inversa) dell'insieme s per la funzione f come l'insieme:

$$\overleftarrow{f}(s) = \{z \in a \mid f(z) \in s\}$$

3.32 Immagine del Dominio ed Antimmagine del Codominio

Per ogni funzione $f : a \to b$ si osserva che:

$$\overrightarrow{f}(a) = Im(f)$$
$$\overleftarrow{f}(b) = a$$

3.33 Immagine ed Antimmagine dell'Insieme Vuoto

Per ogni $f : a \to b$, si ha:

$$\overrightarrow{f}(\emptyset) = \overleftarrow{f}(\emptyset) = \emptyset$$

3.34 Funzione Suriettiva

Una funzione $f : a \to b$ si dice *suriettiva* se e soltanto se:

$$Im(f) = b$$

oppure in modo più esplicito

$$\forall y \in b \ (\exists x \in a \ (f(x) = y))$$

Negazione della suriettiva

$$\exists y \in b \ (\forall x \in a \ (f(x) \neq y))$$

3.35 Funzione Iniettiva

Una funzione $f : a \to b$ si dice *iniettiva* se e soltanto se:

$$\forall x, y \in a \ (f(x) = f(y) \iff x = y)$$

oppure analogamente

$$\forall x, y \in a \ (x \neq y \implies f(x) \neq f(y))$$

Negazione dell'iniettiva

$$\exists x, y \in a \ (f(x) = f(y) \land x \neq y)$$

3.36 Funzione Biettiva

Una funzione $f : a \to b$ si dice *biettiva* se e soltanto se:

$$\forall y \in b \ (\exists! x \in a \ (f(x) = y))$$

ovvero se è iniettiva e suriettiva
Negazione della biettività

$$(\exists y \in b)(\forall x \in a)(f(x) \neq y) \lor (\exists x, y \in a)(f(x) = f(y) \land x \neq y)$$

3.37 Definizione di Iniettivà tramite Antimmagine

Una funzione è iniettiva se e soltanto se per ogni singleton sottoinsieme del suo codominio, la sua antimmagine è vuota o ha un solo elemento.

$$\forall y \in \mathcal{P}_1(b)$$

$$\overleftarrow{f}(y) = \emptyset \lor \exists! x \in a \ (\overleftarrow{f}(y) = \{x\})$$

Proof. DIM $\Rightarrow$: Sia $y \in \mathcal{P}_1(b)$ e supponiamo che $\overleftarrow{f}(y) \neq \emptyset$. Allora, dalla definizione di antimmagine $\exists x(f(x) \in y)$. Ma, essendo f iniettiva, si ha che

$$\forall z \in a \ (f(z) = y \iff z = x)$$

e dunque $\overleftarrow{f}(y) = \{x\}$
DIM $\Leftarrow$: Siano $x, y \in a$ tali che $f(x) = f(y)$. Allora

$$\overleftarrow{f}(\{f(x)\}) = \overleftarrow{f}(\{f(y)\}) = \{x\} = \{y\} \implies x = y$$

e dunque la funzione è iniettiva. □

3.38 Definizione di Suriettività tramite Antimmagine

Una funzione è suriettiva se e soltanto se per ogni singleton sottoinsieme del suo codominio, la sua antimmagine è non vuota

$$\forall y \in \mathcal{P}_1(b) \setminus \{\emptyset\} \ \overleftarrow{f}(y) \neq \emptyset$$

Proof. DIM $\Rightarrow$:

$$\text{f suriettiva} \implies (\forall y \in b)(\exists x \in a)(f(x) = y) \implies$$

$$\implies (\forall \{y\} \in \mathcal{P}_1(b))(\exists x)(x \in \overleftarrow{f}(\{y\})$$

DIM $\Leftarrow$:

$$(\forall y \in \mathcal{P}_1(b) - \{\emptyset\})(\overleftarrow{f}(y) \neq \emptyset) \implies$$

$$\implies (\forall y \in b)(\exists x \in \overleftarrow{f}(y))(f(x) = y) \implies \text{f suriettiva}$$

□

3.39 Definizione di Biettività tramite Antimmagine

Una funzione è biettiva se e soltanto se per ogni singleton sottoinsieme del suo codominio, la sua antimmagine è un singleton

$$\forall y \in \mathcal{P}_1(b) \ \overleftarrow{f}(y) = \{x\}$$

3.40 Sezione di una funzione

Date due funzioni $f : a \to b$ e $g : b \to a$, se

$$f \circ g = id_b$$

g si dice sezione di f

3.41 Retazione di una funzione

Date due funzioni $f : a \to b$ e $g : b \to a$, se

$$g \circ f = id_a$$

g si dice retrazione di f

3.42 Caratterizzazione di Iniettività tramite Retrazione

Una funzione è iniettiva se e soltanto se il suo dominio è vuoto o esiste una sua retrazione.

$$a = \emptyset \vee \exists g : b \to a \ (g \circ f = id_a)$$

Proof. Dimostrazione $\Leftarrow$: Se a è l'insieme vuoto, si verifica banalmente l'iniettività. Se

$$(\exists g : b \to a)(g \circ f = id_a)$$

allora essendo id_a iniettiva, f è iniettiva.
Questo perchè se f non fosse iniettiva allora esisterebbero $x_1, x_2 \in a$ tali che $x_1 \neq x_2$ e $f(x_1) = f(x_2)$. Ma allora

$$(g \circ f)(x_1) = g(f(x_1)) = g(f(x_2)) = (g \circ f)(x_2)$$

e dunque $g \circ f$ non sarebbe iniettiva, il che è assurdo perchè id_a è iniettiva.
Dimostrazione $\Rightarrow$: Definisco la funzione

$$g : y \in b \mapsto \begin{cases} x_y \text{ se } y \in Imf \\ \overline{x} \text{ se } y \notin Imf \end{cases}$$

Dove x_y è definito come l'unico elemento di $\overleftarrow{f}(\{y\})$ (vedi "Caratterizzazione dell'Iniettività tramite Antimmagine"). Si verifica semplicemente che g è una retrazione:

$$g \circ f(x) = g(f(x)) = g(y) = x_y$$

tale che

$$f(x_y) = f(x) \implies x_y = x$$

per iniettività di f, e quindi la funzione g è una retrazione. □

3.43 Caratterizzazione di Suriettività tramite Sezione

Una funzione è suriettiva se e soltanto se esiste una sua sezione.

$$\exists g : b \to a \ (f \circ g = id_b)$$

Proof. Dimostrazione $\Leftarrow$:

$$(\exists g : b \to a)(f \circ g = id_b)$$

implica che f sia suriettiva dato che id_b è suriettiva.
Questo perchè se f non fosse suriettiva allora esisterebbe $y \in b$ tale che $\overleftarrow{f}(\{y\}) = \emptyset$. Ma allora

$$(f \circ g)(y) = f(g(y)) = f(x)$$

per qualche $x \in a$, ma allora $x \notin \overleftarrow{f}(\{y\})$ e quindi $f(x) \neq y$, il che è assurdo perchè id_b è suriettiva.
Dimostrazione $\Rightarrow$: Dalla caratterizzazione di suriettività tramite antimmagine si ha che

$$\text{f è suriettiva} \iff \forall y \in b\ (\overleftarrow{f}(\{y\}) \neq \emptyset)$$

Per l'assioma della scelta esiste la funzione

$$\varphi : \overleftarrow{f}(\{y\}) \in \mathcal{P}(a) \mapsto (x \in a)(x \in \overleftarrow{f}(\{y\}))$$

Definiamo quindi

$$g : y \in b \mapsto \varphi(\overleftarrow{f}(\{y\})) \in a$$

che è una sezione in quanto:

$$f \circ g(y) = f(g(y)) = f(\varphi(\overleftarrow{f}(\{y\}))) = y$$

□

3.44 Inversa di una Funzione

Date due funzioni $f : a \to b$ e $g : b \to a$, se g è sia retrazione che sezione di f, allora g si dice inversa di f.

3.45 Caratterizzazione della Biettività tramite Inversa

Una funzione è biettiva se e soltanto se esiste una sua inversa.

$$\exists g : b \to a\ (f \circ g = id_b) \wedge (g \circ f = id_a)$$

3.46 Unicità dell'Inversa

Se una funzione f che ha una sezione s ed una retrazione r, allora si ha che $r = s$ ed essa è la sua unica inversa.

Proof.

$$r \circ f = id_a \wedge f \circ s = id_b$$

allora

$$(r \circ f) \circ s = id_a \circ s = s$$

$$r \circ (f \circ s) = r \circ id_b = r$$

Ma per l'associatività del prodotto relazionale

$$(r \circ f) \circ s = r \circ (f \circ s)$$

e dunque $r = s$. □

3.47 Una funzione con una sola sezione è biettiva

Se una funzione f ha una ed una sola sezione s, allora essa è una funzione biettiva ed s è la sua inversa.

Proof.

$$(\exists! g : b \to a)(f \circ g = id_b) \implies (\forall y \in b)(\exists! x \in a)(f(x) = y)$$

Supponiamo per assurdo che $\exists x_1, x_2 \in a : x_1 \neq x_2 \wedge f(x_1) = f(x_2) = y$, cioè che f non sia iniettiva. Ciò implica che possono esistere g_1, g_2 sezioni distinte (definite in basso) tali che $g_1(y) = x_1$ e $g_2(y) = x_2$, il che va contro l'ipotesi. Quindi f dev'essere iniettiva, il che implica che essa abbia una retrazione. Avendo entrambe una sezione ed una retrazione, esse coincidono e sono anche l'inversa, e dunque la funzione è biettiva.

$$g_1 : g(f(x_1)) = x_1$$

$$g_2 : y \in b \mapsto \begin{cases} g(y) \text{ se } y \neq f(x_1) \\ x_2 \text{ se } y = f(x_2) \end{cases}$$

□

3.48 Affermazioni equivalenti alla Biettività

1. f è biettiva
2. f ha inversa
3. f ha sezioni e retrazioni
4. f ha una sola sezione
5. $\forall y \in b\ (\exists! x \in a\ (f(x) = y))$

4 Strutture Algebriche

4.1 Struttura algebrica

Una ennupla ordinata del tipo:

$$(s, *_1, *_2, \ldots, *_n)$$

dove $s \neq \emptyset$ si dice insieme di sostegno, e $*_k$ sono le operazioni, si dice struttura algebrica.

4.2 Operazione Interna

Dato un insieme $s \neq \emptyset$, una funzione del tipo

$$* : s \times s \to s$$

si dice operazione interna (binaria dato che ha n-arietà uguale a due).

Se l'applicazione che stiamo usando è un'operazione, non usiamo la normale notazione di funzione, ma piuttosto poniamo il simbolo dell'operazione fra i due operandi. Scriviamo cioè

$$x * y \text{ invece di } *(x, y)$$

4.3 Commutatività

Un'operazione $*$ si dice commutativa se

$$\forall x, y \in s$$

$$(x * y = y * x)$$

4.4 Associatività

Un'operazione $*$ si dice associativa se

$$\forall x, y, z \in s$$

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

In tal caso possiamo evitare le parentesi e scrivere semplicemente

$$x * y * z$$

4.5 Operazione Duale o Opposta

Data un'operazione $* : s \times s \to s$, definiamo la sua operazione duale o opposta come $\overline{*} : s \times s \to s$ tale che:

$$\forall x, y \in s \ (x \overline{*} y \iff y * x)$$

4.6 Semigruppo

Una struttura algebrica $(s, *)$ si dice semigruppo se $*$ è un'operazione binaria interna associativa su s.

4.7 Elemento Neutro

Dato un semigruppo $(s, *)$, un elemento $e \in s$ si dice elemento neutro se

$$\forall x \in s$$

$$(e * x = x = x * e)$$

4.8 Unicità dell'elemento neutro

Dato un semigruppo $(s, *)$, se esiste un elemento neutro, questo è unico.

Proof. Per definizione di elementi neutri a sinistra e a destra:

$$l = l * d = d$$

□

4.9 Monoide

Una struttura algebrica $(s, *)$ si dice monoide se $*$ è un'operazione binaria interna associativa su s e se s ha un elemento neutro rispetto a $*$.
È possibile notare l'elemento neutro esplicitamente, in tale modo:

$$(s, *, u)$$

Esempio. $(\mathbb{N}, +, 0)$ è un monoide, in quanto la somma è associativa e lo zero è elemento neutro.

4.10 Elemento invertibile

Dato un monoide $(s, *, u)$, un elemento $x \in s$ si dice invertibile se

$$\exists y \in s$$

$$(x * y = u = y * x)$$

In tal caso y si dice inverso di x.

Un elemento invertibile si dice anche simmetrizzabile.
Un elemento inverso si dice anche elemento simmetrico o elemento opposto.
Usiamo la dicitura $\mathcal{U}(s)$ per indicare l'insieme di tutti gli elementi simmetrizzabili di s.

4.11 Unicità dell'inverso

Dato un monoide $(s, *, u)$, se un elemento $x \in s$ è invertibile, il suo inverso è unico.

Proof. Siano l e d due inversi di x:

$$l = l * u = l * (x * d) = (l * x) * d = u * d = d$$

□

4.12 Gruppo

Una struttura algebrica $(s, *)$ si dice gruppo se $*$ è un'operazione binaria interna associativa su s, se s ha elemento neutro rispetto a $*$ e se ogni elemento di s è invertibile rispetto a $*$.

Un gruppo $(s, *)$ si dice abeliano se $*$ è commutativa.

Esempio. $(\mathbb{Z}, +, 0)$ è un gruppo, in quanto la somma è associativa, lo zero è elemento neutro ed ogni intero è invertibile rispetto alla somma.

4.13 Parte Stabile

Sia $(s, *)$ una struttura algebrica e sia $t \subseteq s$ non vuoto. Allora t si dice parte stabile o chiusa di s rispetto a $*$ se e soltanto se:

$$\forall x, y \in t$$

$$(x * y \in t)$$

Cioè se, effettuando un'operazione a partire da elementi di t, il risultato è ancora in t.

Esempio. Sia $(\mathbb{R}, +)$ una struttura algebrica. Allora $\mathbb{N}$ è una parte stabile di $\mathbb{R}$ rispetto alla somma. Non è parte chiusa rispetto alla differenza, dato che ad esempio sia 5 che 7 appartengono ad $\mathbb{N}$ ma $(5 - 7) = -2 \notin \mathbb{N}$

In generale, per ogni monoide $(s, *, u)$, $\{u\}$ è parte stabile in quanto $u * u = u$. Inoltre, s è sempre parte stabile di se stesso.

4.14 Operazine Indotta

Sia $(s, *)$ una struttura algebrica e $t \subseteq s$ parte stabile, allora si nota che:

$$*_{|t\times t} = ((t \times t) \times t, g)$$

$$g = \{(x, y, z) \in t \times t \times t \mid x * y = z\}$$

Cioè la ridotta è un'operazione binaria interna del tipo

$$*_{|t\times t} : t \times t \to t$$

Definiamo quindi $*_{|t\times t}$ operazione indotta da $*$ su t.

Un'operazione indotta conserva sempre le proprietà di commutatività, associatività dell'operazione originale, ma può "perdere" l'elemento neutro o gli inversi se questi non fanno parte della parte chiusa.

4.15 L'intersezione di Parti Stabili è una Parte Stabile

Sia $(s, *)$ una struttura algebrica e sia $t \subseteq \mathcal{P}(s)$ tale che

$$\forall x \in t \ (t \text{ parte stabile di } s)$$

Allora

$$\bigcap t \text{ è parte stabile di } s$$

Proof. Siano $x, y \in \bigcap t$. Allora, per la definizione di intersezione unaria

$$\forall z \in t \ (x, y \in z)$$

(questo perché x e y appartengono a tutti gli insiemi di t)

Essendo ogni z parte stabile di s, ciò implica che

$$\forall z \in t \ (x * y \in z) \iff x * y \in \bigcap t$$

E dunque $\bigcap t$ è parte stabile di s. □

4.16 Sottostruttura

Sia $(s, *)$ una struttura algebrica e sia $t \subseteq s$ parte stabile. Allora $(t, *_{|t \times t})$ è una struttura algebrica, detta sottostruttura di $(s, *)$.

Se la struttura $(s, *)$ e la sottostruttura $(t, *_{|t \times t})$ hanno le stesse proprietà allora scriveremo $t \leq s$.

4.17 Elemento Neutro di un Sottogruppo

Sia $(s, *)$ un gruppo e sia $t \leq s$. Allora l'elemento neutro di t è lo stesso di s.

Proof.

$$1_t \in t \implies 1_t \in s \implies 1_t \cdot 1_t = 1_t = 1_t \cdot 1_s$$

Il che implica che sia 1_s e 1_t siano inversi di 1_t, ma essendo l'inverso unico si ha che

$$1_t = 1_s$$

□

4.18 Sottostruttura Generata

Sia $(s, *)$ una struttura algebrica e sia $t \subseteq s$ parte stabile. Allora

$$\langle t \rangle = \bigcap \{u \leq s \mid t \subseteq u\}$$

si dice sottostruttura generata da t.

La ragione per cui la chiamiamo "generata" è che si può dimostrare che essa è in realtà l'insieme delle combinazioni lineari dell'insieme t.
Per esempio, il sottomonoide generata da 2 di $(\mathbb{N}, +)$ è l'insieme di tutti i valori che si possono ottenere sommando 2

$$\langle 2 \rangle = \{2, 4, 6, 8, 10, 12, 14, 16, 18, 20, \dots\}$$

4.19 Caratterizzazione dei Sottomonoidi Generati

Sia $(s, *)$ un monoide e sia $\emptyset \neq t \subseteq s$ parte stabile. Allora:

$$\langle t \rangle = \{x \ \in s \mid (\exists n \in \mathbb{N})(\exists x_1, x_2, ..., x_n \in t)(x = x_1 * x_2 * ... * x_n)\} \cup \{1_s\}$$

Proof. Caso $\subseteq$) chiamiamo l'insieme a destra dell'ipotesi b per brevità. Consideriamo che:

- $t \subseteq b$, perché se $x \in t$ scelgo $n = 1, x_1 = x \implies x \in b$
- Ogni elemento di b è esprimibile come composizione di elementi di t e dunque di s, ed essendo $*$ un'operazione interna allora $b \subseteq s$.
- L'elemento neutro appartiene a b per costruzione.
- Siano $x, y \in b$, allora per definizione di b

  $$(\exists n, m \in \mathbb{N})(\exists x_1, ..., x_n, y_1, ..., y_m)(x = x_1 * ... * x_n \wedge y = y_1 * ... * y_n)$$

  Questo implica che $x * y = x_1 * ... * x_n * y_1 * ... * y_n \implies x * y \in b$ e dunque l'operazione indotta è interna.

Essendo $b \leq s \wedge t \subseteq b$allora $< t > \subseteq b$ per la definizione di sottoinsieme generato come l'intersezione di tutte le sottostrutture di tale tipo.
Caso $\supseteq$) Vogliamo dimostrare che

$$(\forall x \leq s)(t \subseteq x \implies b \subseteq x)$$

poiché da questo segue che $b \subseteq < t >$, che è la tesi. Allora, siano $x \leq s \wedge t \subseteq x$. Essendo x parte chiusa, allora

$$(\forall n \in \mathbb{N})(\forall y_1, ...y_n \in t \subseteq x)(y_1 * ... * y_n \in x) \implies (\forall y \in b)(y \in x) \implies b \subseteq x$$

Quindi b è parte di ogni sottostruttura contente t, e dunque parte della loro intersezione, e quindi $b \subseteq < t >$. □

4.20 Caratterizzazione dei Gruppi Generati

Sia $(g, *, 1_s)$ un gruppo e sia $\emptyset \neq t \subseteq g$ parte stabile. Allora:

$$< t >= \{x \in g \mid (\exists n \in \mathbb{N})(\exists \varepsilon_1, \varepsilon_2, ..., \varepsilon_n \in \{-1, 1\})$$
$$(\exists x_1, x_2, ..., x_n \in t)(x = x_1^{\varepsilon_2} * x_2^{\varepsilon_2} * ... * x_n^{\varepsilon_n})\}$$

Proof. Caso $\subseteq$) chiamiamo l'insieme a destra dell'ipotesi b per brevità. Consideriamo che:

- $t \subseteq b$, perché se $x \in t$ scelgo $n = 1, \varepsilon_1 = 1, x_1 = x \implies x \in b$
- Ogni elemento di b è esprimibile come composizione di elementi di $t \subseteq s$ o dei loro inversi in s, ed essendo $*$ un'operazione interna allora $b \subseteq s$.
- Se scegliamo $n = 2, \varepsilon_1 = 1, \varepsilon_2 = -1, x_1 = x_2 = x \in t \implies$

$$(\exists y \in b)(y = x_1^{\varepsilon_1} * x_2^{\varepsilon_2} = x * x^{-1} = 1_s)$$

- Dalle due precedenti segue che ogni elemento di b è dotato di inverso.
- Siano $x, y \in b$, allora per definizione sono entrambi esprimibili come composizione di $n, m \in \mathbb{N}$ elementi di t o loro inversi. Dunque la loro composizione è esprimibile come $n + m$ elementi di t o loro inversi, quindi essa appartiene a b e l'operazione indotta è binaria interna.

Essendo $b \leq s \wedge t \subseteq b$ allora $< t > \subseteq b$ per la definizione di sottoinsieme generato come l'intersezione di tutte le sottostrutture di tale tipo.
Caso $\supseteq$) Vogliamo dimostrare che

$$(\forall x \leq s)(t \subseteq x \implies b \subseteq x)$$

poiché da questo segue che $b \subseteq < t >$, che è la tesi. Allora, siano $x \leq s \wedge t \subseteq x$. Essendo x parte chiusa dotata di inversi per ogni elemento, allora

$$(\forall n \in \mathbb{N})(\forall \varepsilon_1, ...\varepsilon_n \in \{1, -1\})(\forall y_1, ...y_n \in t \subseteq x)(y_1^{\varepsilon_1} * ... * y_n^{\varepsilon_n} \in x) \implies$$

$$\implies (\forall y \in b)(y \in x) \implies b \subseteq x$$

Quindi b è parte di ogni sottostruttura contente t, e dunque parte della loro intersezione, e quindi $b \subseteq < t >$. □

4.21 Struttura Ciclica

$(s, *)$ è una struttura ciclica $\iff \exists x \in s$ tale che $< x >= s$

4.22 Elemento Cancellabile

Sia $(s, *)$ una struttura algebrica e sia $k \in s$. Allora k si dice cancellabile se

$$\forall x, y \in s$$

$$k * x = k * y \implies x = y$$

$$x * k = y * k \implies x = y$$

Un elemento non è cancellabile quando

$$k \text{ non cancellabile a sx} \iff \exists x, y \in g \ (kx = ky \wedge x \neq y)$$

$$k \text{ non cancellabile a dx} \iff \exists x, y \in g \ (xk = yk \wedge x \neq y)$$

4.23 Invertibilità implica Cancellabilità

Dato un gruppo $(g, \cdot)$

$$\forall x \ (x \in \mathcal{U}(g) \implies x \text{ cancellabile})$$

Proof.

$$x \in \mathcal{U}(g) \implies \exists \bar{x} \in g \ (x \cdot \bar{x} = 1_g = \bar{x} \cdot x)$$

Siano allora $y, z \in g$ tali che

$$xy = xz \implies \bar{x} \cdot x \cdot y = \bar{x} \cdot x \cdot z \implies 1_g \cdot y = 1_g \cdot z \implies y = z$$

Analogamente

$$yx = zx \implies y \cdot x \cdot \bar{x} = z \cdot x \cdot \bar{x} \implies y \cdot 1_g = z \cdot 1_g \implies y = z$$

□

Attenzione. L'opposto non è necessariamente vero: cancellabilità non implica invertibilità. Per esempio, in $(\mathbb{Z}, \cdot)$ nessun elemento a parte 1 è invertibile, ma tutti sono cancellabili.

4.24 Funzione Traslazione

Sia $(s, \cdot)$ un semigruppo e sia $x \in s$.

$$\sigma_x : z \in s \mapsto x \cdot z \in s \text{ funzione traslazione a sinistra}$$

$$\delta_x : z \in s \mapsto z \cdot x \in s \text{ funzione traslazione a destra}$$

x è cancellabile a sinistra $\iff$ la funzione traslazione a sx è iniettiva.
x è cancellabile a destra $\iff$ la funzione traslazione a dx è iniettiva.

4.25 Tavola di Cayley

neutro a sx $\iff$ riga = riga elementi

neutro a dx $\iff$ colonna = colonna elementi

invertibile a sx $\iff$ riga contiene elemento neutro

invertibile a dx $\iff$ colonna contiene elemento neutro

operazione commutativa $\iff$ tavola simmetrica

cancellabile a sx $\iff$ riga con elementi tutti diversi

cancellabile a dx $\iff$ colonna con elementi tutti diversi

4.26 Omomorfismi fra Strutture Algebriche

Siano $(s, *_s)$ e $(t, *_t)$ due strutture algebriche. Una funzione $f : s \to t$ si dice omomorfismo se

$$\forall x, y \in s$$

$$f(x *_s y) = f(x) *_t f(y)$$

Un'omomorfismo è dunque una funzione che ci permette di "passare" da una struttura ad un'altra conservando però le proprietà delle operazioni.
Esempio.

$$EXP : x \in \mathbb{R} \mapsto e^x \in \mathbb{R} - \{0\}$$

Questa funzione è un'omomorfismo fra le strutture $(\mathbb{R}, +)$ e $(\mathbb{R} - \{0\}, \cdot)$ in quanto

$$(\forall x, y \in \mathbb{R})(EXP(x + y) = e^{x+y} = e^x \cdot e^y = EXP(x) \cdot EXP(y))$$

4.27 Monomorfismo

Un omomorfismo iniettivo si dice monomorfismo.

4.28 Epimorfismo

Un omomorfismo suriettivo si dice epimorfismo.

Epimorfismi conservano l'associatività, la commutatività, i neutri, e gli inversi.

4.29 Epimorfismi conservano i Neutri

Proof. Siano $(s, *)$ e $(\bar{s}, \bar{*})$ strutture algebriche, $\varphi : s \to \bar{s}$ un'epimorfismo, $1_s \in s$ elemento neutro, e sia $y \in \bar{s}$.
Essendo la funzione suriettiva

$$\exists x \in s \ (\varphi(x) = y)$$

Allora

$$y \ \bar{*} \ \varphi(1_s) = \varphi(x) \ \bar{*} \ \varphi(1_s) = \varphi(x * 1_s) = \varphi(x) = y$$

quindi $\varphi(1_s)$ è elemento neutro di $(\bar{s}, \bar{*})$ □

4.30 Epimorfismi conservano la Commutatività

Siano $(s, *)$ e $(\bar{s}, \bar{*})$ strutt. algebriche tale che $*$ è un'operazione commutativa e sia $\varphi : s \to \bar{s}$ un'epimorfismo. Vogliamo dimostrare che anche l'operazione $\bar{*}$ è commutativa.

Proof. Siano $y_1, y_2 \in \bar{s}$. Essendo la funzione suriettiva

$$\exists x_1, x_2 \in s \ (\varphi(x_1) = y_1 \wedge \varphi(x_2) = y_2)$$

Allora:

$$y_1 \bar{*} y_2 = \varphi(x_1) \bar{*} \varphi(x_2) =$$

$$= \varphi(x_1 * x_2) = \varphi(x_2 * x_1) = \varphi(x_2) \bar{*} \varphi(x_1) = y_2 \bar{*} y_1$$

E dunque l'operazione $\bar{*}$ è commutativa. □

4.31 Isomorfismo

Un omomorfismo biettivo si dice isomorfismo.

4.32 L'inversa di un isomorfismo è a sua volta un isomorfismo

Siano $(s, *)$ e $(\bar{s}, \bar{*})$ due strutture algebriche. Se $\varphi : s \to \bar{s}$ è un isomorfismo, allora $\varphi^{-1} : \bar{s} \to s$ è a sua volta un isomorfismo. Se φ è biettiva, allora esiste φ^{-1} anch'essa biettiva. Pertanto, per dimostrare che essa è un isomorfismo, basta dimostrare che è un omomorfismo.

$$(\forall x, y \in \bar{s})(\varphi^{-1}(x \bar{*} y) = \varphi^{-1}(x) * \varphi^{-1}(y))$$

Proof. Siano $x, y \in \bar{s}$. Essendo

$$\varphi \circ \varphi^{-1} = id_{\bar{s}}$$

allora abbiamo che:

$$\varphi^{-1}(x \bar{*} y) = \varphi^{-1}(\varphi(\varphi^{-1}(x)) \ \bar{*} \ \varphi(\varphi^{-1}(y))) =$$
$$= \varphi^{-1}(\varphi(\varphi^{-1}(x) * \varphi^{-1}(y))) = \varphi^{-1}(x) * \varphi^{-1}(y)$$

□

Proof. DIMOSTRAZIONE ALTERNATIVA

$$\varphi(\varphi^{-1}(x) * \varphi^{-1}(y)) = \varphi(\varphi^{-1}(x)) \bar{*} \varphi(\varphi^{-1}(y)) = x \bar{*} y$$

Poiché φ è un isomorfismo. Se applichiamo φ^{-1} ad entrambi gli estremi dell'equazione qui sopra, allora otteniamo:

$$\varphi^{-1}(\varphi(\varphi^{-1}(x) * \varphi^{-1}(y))) = \varphi^{-1}(x \bar{*} y)$$

E semplificando le funzioni inverse:

$$\varphi^{-1}(x) * \varphi^{-1}(y) = \varphi^{-1}(x \bar{*} y)$$

Che è la tesi. □

4.33 Automorfismo

Un isomorfismo di una struttura algebrica in se stessa ovvero un isomorfismo $f : a \to a$ si dice automorfismo.

4.34 Anello

Sia $a \neq \emptyset$ e siano $+, \cdot$ due operazioni binarie interne di a. La struttura algebrica $(a, +, \cdot)$ si dice anello se $(a, +)$ è un gruppo abeliano, $(a, \cdot)$ è un semigruppo, e vale la proprietà distributiva di $\cdot$ su $+$:

$$\forall x, y, z \in a$$
$$x \cdot (y + z) = x \cdot y + x \cdot z$$

Dato un anello $(a, +, \cdot)$, indichiamo con

- 0_a o 0^N l'elemento neutro rispetto all'operazione $+$
- 1_a o 1^N l'elemento neutro dell'operazione $\cdot$ (se esiste)

Dato un anello $(a, +, \cdot)$, allora definiamo:

- $\forall x, y \in a \ (x - y = x + (-y))$
- $\forall x \in a$
  $\forall n \in \mathbb{N} - \{0\}$
  $nx = x + x + ... + x \ (n \text{ volte}))$
- $\forall x \in a$
  $\forall n \in \mathbb{Z} - \mathbb{N}$
  $nx = -x - x - ... - x \ (n \text{ volte}))$
- $\forall x \in a \ (0x = 0_a)$

Stiamo dunque definendo la differenza, e i multipli.

Dato un anello $(a, +, \cdot)$, allora definiamo le proprietà del prodotto:

1. $\forall x \in a$
   $\forall n \in \mathbb{N} - \{0\}$
   $$x^n = x \cdot x \cdot ... \cdot x \ (n \text{ volte})$$

2. $\forall x \in a$
   $\forall n \in \mathbb{N} - \{0\}$
   $$x^{-n} = x^{-1} \cdot x^{-1} \cdot ... \cdot x^{-1} \ (n \text{ volte})$$

3. $\forall x \in a$
   $$x^0 = 1_a \text{ (se esiste)}$$
   Con queste prime tre proprietà stiamo dunque definendo la potenza per l'anello.

4. $\forall x, y, z \in a$
   $$x \cdot (y - z) = x \cdot (y + (-z)) = xy + x(-z) = xy - xz$$

5. Per la (4), è dunque distributivo rispetto alla differenza:
   $$\forall x, y \in a \ (x \cdot (-y) = -xy = (-x)y)$$

6. Se l'anello è unitario:
   $\forall x \in a$
   $\forall n \in \mathbb{N}$
   $$(n \cdot 1_a)x = nx$$

4.35 Anello Commutativo

Un anello $(a, +, \cdot)$ si dice commutativo se $(a, \cdot)$ è un semigruppo commutativo.

4.36 Anello Unitario

Un anello $(a, +, \cdot)$ si dice unitario se $(a, \cdot)$ è un monoide.

4.37 Il prodotto per lo zero dell'anello è sempre zero

Dato un anello $(a, +, \cdot)$ vogliamo dimostrare che

$$\forall x \in a$$

$$0_a \cdot x = 0_a = x \cdot 0_a$$

Proof.

$$\forall x \in a$$

$$0_a \cdot x = (x - x)x = xx - xx = 0_a$$

$$x \cdot 0_a = x(x - x) = xx - xx = 0_a$$

□

4.38 Legge di Annullamento del Prodotto

Dato un anello $(a, +, \cdot)$, diremo che nell'anello vale la legge di annullamento del prodotto se e solo se:

$$\forall x, y \in a$$

$$x \cdot y = 0_a \implies (x = 0_a \vee y = 0_a)$$

4.39 Anello Integro

Un anello $(a, +, \cdot)$ si dice integro se vale la legge di annullamento del prodotto.

4.40 Dominio di Integrità

Un anello $(a, +, \cdot)$ si dice dominio di integrità se è un anello integro commutativo unitario.

4.41 Divisore dello Zero

Sia $(a, +, \cdot)$ un anello. Allora:

$x \in a - \{0_a\}$ divisore sx dello zero $:\iff \exists y \in a - \{0_a\}\ (xy = 0_a)$
$x \in a - \{0_a\}$ divisore dx dello zero $:\iff \exists y \in a - \{0_a\}\ (yx = 0_a)$
$x \in a - \{0_a\}$ divisore dello zero $:\iff x$ è divisore sx e dx dello zero

4.42 Divisore dello zero $\iff$ non Cancellabile

Sia $(a, +, \cdot)$ un anello. Allora:

$x \in a - \{0_a\}$ divisore a sx dello zero $\iff$ x non cancellabile a sx
$x \in a - \{0_a\}$ divisore a dx dello zero $\iff$ x non cancellabile a dx

Proof. Dimostriamo a sinistra, dato che a destra la dimostrazione è analoga. $\Rightarrow$) Sia $x \in a$ divisore sinistro dello zero, allora

$$\exists y \in a - \{0_a\}\ (xy = 0_a)$$

Per assurdo, se x fosse cancellabile a sinistra, allora

$$x \cdot y = 0_a \implies x \cdot y = x \cdot 0_a \implies y = 0_a$$

che è assurdo, in quanto $y \in a - \{0_a\}$.
$\Leftarrow$) Per ipotesi

$$\exists y, z \in a\ (y \neq z \wedge xy = xz)$$

Quindi

$$x(y - z) = xy - xz = 0$$

nonostante $y - z \neq 0$, dunque x è divisore a sinistra dello zero in quanto esiste un valore $y - z \neq 0 : x(y - z) = 0$ □

4.43 Dominio di Integrità $\iff$ è privo di Divisori dello Zero

Proof. $\Rightarrow$) Se l'anello è dominio di integrità, vale la legge di annullamento del prodotto. Per assurdo, sia $x \in a$ un divisore dello zero. Allora

$$\exists y \in a - \{0\} \ (xy = 0)$$

e dunque per la legge di annullamento del prodotto $x = 0 \vee y = 0$ che va contro l'ipotesi che siano entrambi non zero.
$\Leftarrow$) Se nessun elemento è divisore dello zero, allora tutti gli elementi sono cancellabili. Dunque, se consideriamo

$$\forall x, y \in a \ (x \neq 0 \wedge xy = 0 \implies y = 0)$$

che è la tesi. □

4.44 Corpo

Un anello si dice corpo se $(a - \{0_a\}, \cdot)$ è un gruppo.

4.45 Campo

Un corpo commutativo si dice campo.

4.46 Ogni Campo è un Dominio di Integrità

Proof. Un campo è un corpo commutativo, ed un corpo è un anello unitario. Un anello commutativo unitario è dominio di integrità se e soltanto se è privo di divisori dello zero. Ogni elemento di un campo, eccetto lo zero, è invertibile, e dunque cancellabile. Un elemento cancellabile non può essere divisore dello zero, e quindi non esistono divisori dello zero. Dunque il campo è dominio di integrità. □

5 Relazioni binarie

Una relazione binaria è uno specifico tipo di corrispondenza che mette in relazione elementi di uno stesso insieme. Esistono molte proprietà di cui possono godere le relazioni binarie. Andiamo ora a definire le più fondamentali. Data una relazione binaria $\rho = (a \times a, g)$, diremo che:

5.1 Riflessività

$$\rho \text{ è riflessiva} \iff \forall x \in a \ (x \rho x)$$

5.2 Antiriflessività

$$\rho \text{ è antiriflessiva} \iff \forall x \in a \ (\neg(x \rho x))$$

5.3 Simmetrica

$$\rho \text{ è simmetrica} \iff \forall x, y \in a \ (x \rho y \implies y \rho x)$$

5.4 Asimmetrica

$$\rho \text{ è asimmetrica} \iff \forall x, y \in a \ (x \rho y \land y \rho x \implies x = y)$$

5.5 Transitiva

$$\rho \text{ è transitiva} \iff \forall x, y, z \in a \ (x \rho y \land y \rho z \implies x \rho z)$$

Si osserva che ogni relazione definita su un insieme di due o meno elementi è transitiva.

Dividiamo poi le relazioni binarie in diverse categorie in base a quali di queste proprietà esse verificano.

5.6 Relazione d'Equivalenza

Una relazione riflessiva, simmetrica e transitiva si dice relazione di equivalenza.

5.7 Relazione d'ordine

Una relazione asimmetrica e transitiva si dice relazione d'ordine.

5.8 Relazione di Ordine Largo

Se una relazione d'ordine è riflessiva, si dice relazione di ordine largo.

5.9 Relazione di Ordine Stretto

Se una relazione d'ordine è antiriflessiva, si dice relazione di ordine stretto.

5.10 Ordine Stretto e Asimmetria

Si osserva che in una relazione d'ordine stretto l'asimmetria è ininfluente in quanto non si può avere

$$x\rho y \wedge y\rho x$$

in tal caso per transitività si avrebbe

$$x\rho x$$

che va contro la proprietà di antiriflessività della relazione d'ordine stretto.

5.11 Relazione Duale

Data una relazione binaria ρ su un insieme a, definiamo la relazione duale:

$$\overline{\rho} : \forall x, y \in a \ (x\overline{\rho}y \iff y\rho x)$$

5.12 Diagonale di un Insieme

Dato un insieme s definiamo

$$diag(s) := \{(x, y) \in s \times s \mid x = y\}$$

5.13 Caratterizzazioni delle Proprietà delle Relazioni

Data una relazione $\rho = (s \times s, g_\rho)$ e duale ρ allora:

$$\begin{aligned}
&\rho \text{ riflessiva} &&\iff diag(s) \subseteq g_\rho \\
&\rho \text{ simmetrica} &&\iff \rho = \overline{\rho} \\
&\rho \text{ antiriflessiva} &&\iff diag(s) \cap g_\rho = \emptyset \\
&\rho \text{ asimmetrica} &&\iff g_\rho \cap g_{\bar{\rho}} \subseteq diag(s)
\end{aligned}$$

5.14 Relazione di Equivalenza Universale

Data una relazione di equivalenza

$$\rho = (s \times s, g),\ g = s \times s$$

essa si dice relazione di equivalenza universale (o totale).

5.15 Congruenza di modulo m

Sia $m \in \mathbb{Z}$, allora definiamo:

$$\equiv_m := (\mathbb{Z} \times \mathbb{Z}, g)$$

$$\forall a, b \in \mathbb{Z}\ ((a, b) \in g \iff \exists k \in \mathbb{Z}\ (a - b = km))$$

5.16 La congruenza è una relazione di equivalenza

Proof. Siano $x, y, z \in \mathbb{Z}$

Riflessività:

$x - x = 0 = 0m$ quindi $x \equiv_m x$

Simmetria

$x \equiv_m y \implies \exists k \in \mathbb{Z}\ (x - y = km)$

$\implies y - x = (-k)m \implies y \equiv_m x$

Transitività

$x \equiv_m y \land y \equiv_m z$

$\implies \exists k_1, k_2 \in \mathbb{Z}\ (x - y = k_m \land y - z = k_2 m$

$\implies (x - y) + (y - z) = x - z = (k_1 + k_2)m)$

Abbiamo dimostrato che la congruenza è riflessiva, simmetrica e transitiva, quindi è una relazione di equivalenza. □

5.17 Congruenze notevoli

Relazione di uguaglianza

$$a \equiv_0 b \iff a - b = 0 \iff a = b$$

Relazione universale

$$a \equiv_1 b \text{ dato che } (a - b) = 1 \cdot (a - b)$$

5.18 Nucleo di Equivalenza di una Funzione

Data una funzione $f : a \to b$, definiamo la relazione nucleo di equivalenza:

$$KER_f := (a \times a, g)$$

$$\forall x, y \in a\ ((x, y) \in g \iff f(x) = f(y))$$

Che notiamo anche come $\sim_f$

5.19 Classe di Equivalenza

Sia s un insieme su cui è definita una relazione di equivalenza ρ. Sia $x \in s$. Allora definiamo:

$$[x]_\rho = \{y \in s \mid x \rho y\}$$

Che chiamiamo classe di equivalenza di x di modulo ρ

5.20 Rappresentante di una classe di equivalenza

Data una classe di equivalenza notata nella forma $[x]_\rho$, chiamiamo x il rappresentante della classe di equivalenza.

5.21 Calsse di Resto

Le classi di equivalenza di una congruenza si dicono classi di resto e si notano per brevità usando solamente il modulo:

$$[x]_m = [x]_{\equiv_m}$$

5.22 Insieme Quoziente

Dato un insieme s su cui è definita una relazione ρ, allora definiamo:

$$s/\rho = \{y \in P(s) \mid \exists x \in s \ (y = [x]_\rho)\} = \{[x]_\rho \mid x \in s\}$$

E lo chiamiamo insieme quoziente di s rispetto a ρ

5.23 Prima Proprietà Fondamentale: Nessuna Classe di Equivalenza è Vuota

Dato un insieme s su cui è definita una relazione di equivalenza ρ, allora:

$$(\forall y \in s/\rho)(y \neq \emptyset)$$

Proof. Per la riflessività

$$\forall x \in s \ (x \rho x \implies x \in [x]_\rho)$$

□

5.24 Seconda Proprietà Fondamentale: Le Classi di Equivalenza sono Disgiunte

Dato un insieme s su cui è definita una relazione di equivalenza ρ, allora:

$$\forall x, y \in s \ ([x]_\rho \neq [y]_\rho \iff [x]_\rho \cap [y]_\rho = \emptyset)$$

Proof. Supponiamo per assurdo l'intersezione fra le due classi sia non vuota. Allora:

$$[x]_\rho \cap [y]_\rho \neq \emptyset \implies \exists z \ (z \in [x]_\rho \wedge z \in [y]_\rho) \implies x \rho z \wedge z \rho y \implies x \rho y$$

□

5.25 Terza Proprietà Fondamentale: l'Unione Unaria dell'Insieme Quoziente è l'Insieme

Dato un insieme s su cui è definita una relazione di equivalenza ρ, allora:

$$\bigcup s/\rho = s$$

Proof.

$\subseteq$)

$y \in \bigcup s/\rho \implies \exists [x]_\rho \in s/\rho \ (y \in [x]_\rho) \implies y \in s$

$\supseteq$)

$y \in s \implies [y]_\rho \in s/\rho \wedge y \in [y]_\rho \implies y \in \bigcup s/\rho$

E dunque $\bigcup s/\rho = s$. □

5.26 Proiezione Canonica

Dato un insieme a su cui è definita una relazione di equivalenza $\sim$, definiamo:

$$\pi : x \in a \mapsto [x]_\sim \in a/\sim$$

5.27 Suriettività della Proiezione Canonica

Proof. Per le proprietà fondamentali delle classi di equivalenza, per ogni classe di equivalenza appartenente ad un insieme quoziente $a/\sim$ esiste un elemento di a contenuto in esso, in quanto nessuna classe di equivalenza è vuota. Questo implica che la proiezione canonica sia un'applicazione suriettiva. □

5.28 Partizione

Dato un insieme a, un insieme f si dice partizione di a se e solo se:

1. $\forall x \in f \ (x \neq \emptyset)$
2. $\forall x, y \in f \ (x \neq y \implies x \cap y = \emptyset)$
3. $\bigcup f = a$

5.29 Partizioni Banali

Dato un insieme a, esso è dotato delle seguenti partizioni banali:

Se stesso	$f = a$
L'insieme di tutti i singleton	$f = \{\{x\} \in P(a) \mid x \in a\}$

5.30 Insieme delle Relazioni di Equivalenza

$EQ(a)$ = insieme delle relazioni di equivalenza su a

5.31 Insieme delle Partizioni

$PART(a)$ = insieme delle partizioni di a

5.32 Insiemi Quoziente e Partizioni

Si osserva che, per le proprietà delle classi di equivalenza, ogni insieme quoziente risulta essere una partizione.

5.33 Teorema Fondamentale su Relazioni di Equivalenza e Partizioni

Per ogni insieme a, esiste una funzione biettiva

$$f :\sim\in EQ(a) \mapsto a/\sim\in PART(a)$$

Esiste dunque una corrispondenza biunivoca tra relazioni di equivalenza e partizioni: da ogni relazione di equivalenza si può definire una partizione e da ogni partizione di può definire una relazione di equivalenza.

Proof. Dimostriamo che f è iniettiva.

Prendiamo $\sim_1, \sim_2 \in EQ(a)$ tale che $f(\sim_1) = f(\sim_2)$ ovvero $a/\sim_1 = a/\sim_2$

$$\forall x, y \in a \ (x \sim_1 y \iff [x]_{\sim_1} = [y]_{\sim_1} \iff$$

$$\exists z, w \in a \ ([x]_{\sim_1} = [z]_{\sim_2} \ \wedge \ [y]_{\sim_1} = [w]_{\sim_2} \iff w \sim_2 z) \iff x \sim_2 y)$$

Quindi $\sim_1 = \sim_2$ e dunque f è iniettiva.
Dimostriamo che f è suriettiva.

$$\text{Siano } p \in PART(a)$$

$$\sim: \forall x, y \in a \ (x \sim y \iff \exists z \in p \ (x \in z \wedge y \in z))$$

Per dimostrare la suriettività dimostriamo che che $\sim$ è una relazione di equivalenza, e cioè che gode della proprietà riflessiva, simmetrica, e transitiva.

$$\forall x \in a \ \exists z \in p \ (x \in z \wedge x \in z)$$

quindi la relazione è riflessiva

$$\forall x, y \in a \ \exists z \in p \ ((x \in z \wedge y \in z) \iff (y \in z \wedge x \in z))$$

per la commutatività di $\wedge$ e dunque la relazione è simmetrica.

$$\text{Presi } x, y, z \in a \text{ tali che } x \sim y \sim z \text{ allora}$$

$$\exists w_1, w_2 \in p \ ((x \in w_1 \wedge y \in w_1) \wedge (y \in w_2 \wedge z \in w_2) \implies$$

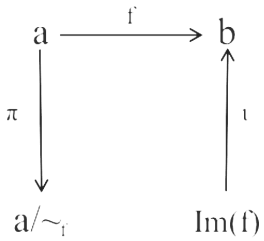
$$\implies w_1 \cap w_2 \neq \emptyset \implies w_1 = w_2)$$

in quanto p è una partizione. Pertanto x e y fanno parte dello stesso insieme e sono equivalenti, quindi la relazione è transitiva. Per ogni partizione esiste un'associata relazione di equivalenza quindi f è suriettiva e dunque biettiva.

□

6 Teorema Fondamentale di Omomorfismi per Insiemi

6.1 Premessa del Teorema Fondamentale di Omomorfismo per Insiemi



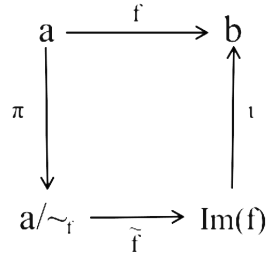
Dati due insiemi a e b ed un'applicazione $f : a \to b$, possiamo costruire il seguente diagramma, dove π è la proiezione canonica rispetto al nucleo di equivalenza di f e ι (iota) è l'immersione dell'immagine nel codominio. Vogliamo chiudere il diagramma, dunque definiamo:

$$\tilde{f} : [x]_{\sim_f} \in a/\sim_f \mapsto \ f(x) \in Im(f)$$

$\tilde{f}$ è una funzione ben posta o solo una corrispondenza? Per essere un'applicazione, per ogni classe di equivalenza deve esistere una sola immagine. Se quindi il valore $\tilde{f}([x]_{\sim_f})$ variasse in base a quale $z \in [x]_{\sim_f}$ scegliessimo, non sarebbe un'applicazione. Ma per definizione di nucleo di equivalenza:

$$\forall [x]_{\sim_f} \in a/\sim_f \ \ \forall z, w \in [x]_{\sim_f} \ (f(z) = f(w))$$

Allora si ha che tutti gli elementi della classe di equivalenza hanno la stessa immagine per f e dunque $\tilde{f}$ è un'applicazione ben posta. Possiamo quindi chiudere il diagramma:



6.2 Prima tesi del Teorema Fondamentale di Omomorfismi per Insiemi

$$\tilde{f} : [x]_{\sim_f} \in a/\sim_f \mapsto\ f(x) \in Im(f) \text{ è biettiva}$$

Proof. Definiamo

$$\alpha : f(x) \in Im(f) \mapsto [x]_{\sim_f} \in a/\sim_f$$

Questa è una funzione ben posta per la definizione di nucleo di equivalenza, in quanto tutte le x con la stessa $f(x)$ fanno parte della stessa classe di equivalenza. Sia $y \in a/\sim_f$. Per le proprietà fondamentali delle classi di equivalenza

$$\exists x \in a\ (y = [x]_{\sim_f})$$

Per tanto α è suriettiva.
Dalla definizione di nucleo di equivalenza $\tilde{f}$

$$\forall x, y \in a\ (f(x) = f(y) \iff [x]_{\sim_f} = [y]_{\sim_f})$$

Pertanto α è iniettiva.
α è biettiva, $\tilde{f}$ è la sua inversa, quindi è anch'essa biettiva. □

6.3 Seconda tesi del Teorema Fondamentale di Omomorfismi per Insiemi

$$f = \iota \circ \tilde{f} \circ \pi$$

Proof. Due funzioni coincidono se hanno stesso dominio, stesso codominio, e stesso grafico.

$$f : a \to b$$

$$\iota \circ \tilde{f} \circ \pi : a\ \to\ a/\sim_f \to Im(f)\ \to\ b$$

Hanno stesso dominio e codominio.

$$\forall x \in a\ (\iota \circ \tilde{f} \circ \pi(x) = \iota(\tilde{f}(\pi(x))) = \iota(\tilde{f}([x]_{\sim_f})) = \iota(f(x)) = f(x))$$

Anche i grafici sono identici e dunque le due funzioni sono coincidenti.
□

6.4 Ogni Funzione è Composizione di una Funzione Iniettiva e di una Funzione Suriettiva

Proof. Dalla 2^a Tesi del Teorema Fondamentale di Omomorfismo per Insiemi:

$$\forall f \ (f = \iota \circ \tilde{f} \circ \pi)$$

ι è iniettiva, $\tilde{f}$ è biettiva, e π è suriettiva. Pertanto possiamo esprimere $f = (\iota \circ \tilde{f}) \circ \pi$ oppure $f = \iota \circ (\tilde{f} \circ \pi)$. In entrambi i casi abbiamo la tesi. □

7 Teorema Fondamentale dell'Aritmetica

7.1 Lemma sui Divisori dei Primi

Se $p \in \mathbb{Z}$ è primo, allora

$$\{n \in \mathbb{Z} \mid n|p\} = \{-1, 1, p, -p\}$$

Cioè un numero primo è divisibile solo dalle unità, se stesso ed il proprio opposto.

Proof. Sia $n \in \mathbb{Z}$ tale che

$$n|p \iff (\exists k \in \mathbb{Z}\ (nk = p \implies p|n \vee p|k))$$

(questo per la definizione di primo dato che $p|nk$ perchè $p = nk$).
Nel caso

$$p|n \iff \exists h \in \mathbb{Z}\ (ph = n) \implies phk = nk \implies phk = p \implies hk = 1$$

Allora

$$(h = k = 1) \vee (h = k = -1) \implies n = \pm p$$

Nel caso

$$p|k \iff \exists h \in \mathbb{Z}\ (ph = k) \implies nph = nk \implies nph = p \implies nh = 1$$

Allora

$$(n = h = 1) \vee (n = h = -1) \implies n = \pm 1$$

□

7.2 Secondo Lemma per il Teorema Fondamentale dell'Aritmetica

Siano $a, b \in \mathbb{N} \setminus \{0\}$ e sia

$$x = \{n \in \mathbb{N} \setminus \{0\} \mid a|nb\}$$

Allora $\forall n \in x\ (min(x)|n)$

Proof. Per assurdo, sia non vuoto l'insieme degli elementi di x non divisibili per il minimo e sia z il minimo di tale insieme.
Poniamo $m = min(x)$. Essendo

$$z, m \in x \implies a|zb \wedge a|mb \implies \exists h, k \in \mathbb{N}\ (ah = zb \wedge ak = mb)$$

Dunque

$$a(h-k) = ah - ak = zb - mb = (z-m)b \implies a|(z-m)b$$

Quindi $z - m \in x$, ma $z - m < z$, e z era stato ipotizzato il minimo degli elementi non divisibili da m, il che implica che

$$m|(z-m) \iff \exists l\ (ml = z-m) \implies m(l+1) = z \implies m|z$$

che è assurdo. □

7.3 Lemma sui divisori dei non primi

$\forall m \in \mathbb{Z}$ non primo ha divisori oltre $\pm 1, \pm m$.

Proof.

$$m \in \mathbb{N} \text{ non primo } \iff \exists h, k\ (m|hk \wedge\ m \not| h \wedge m \not| k)$$

Per assurdo, ipotizziamo che

$$\{n \in \mathbb{N} \mid n|m\} = \{1, m\}$$

cioè che m sia divisibile solo dall'1 e sé stesso. Sia

$$x = \{n \in \mathbb{N} \setminus \{0\} \mid m|nk\}$$

e sia $s = min(x)$. Dato che $h, m \in x$, per il Secondo Lemma

$$s|h \wedge s|m$$

ma per ipotesi solo 1 ed m sono divisori di m, quindi

$$s = 1 \vee s = m$$

Se

$$s = 1 \implies m|1k \implies m|k$$

che va contro l'ipotesi. Se

$$s = m \implies m|h$$

(perchè per il secondo Lemma $s|h \wedge s|m$) che va contro l'ipotesi. In entrambi i casi abbiamo l'assurdo e quindi $m \in \mathbb{Z}$ ha divisori oltre $\pm 1, \pm m$.
□

7.4 2 è Primo

Proof.

$$2 \text{ è primo } \iff \forall a, b \in \mathbb{N}\ (2|ab \implies 2|a \vee 2|b)$$

Supponiamo che $2 \not| a$ dimostriamo che necessariamente $2|b$.

$2|ab \wedge 2 \not| a \implies \exists k \in \mathbb{N}\ (2k = ab) \wedge \exists h \in \mathbb{N}\ (a = 2h+1)^* \implies 2k = 2hb+b$

E dunque

$$2k - 2hb = b \implies 2(k - hb) = b \implies 2|b$$

che è la tesi.
(* perchè a non è pari, dato che $2 \not| a$). □

7.5 Prima Tesi del Teorema fondamentale dell'Aritmetica

Sia $m \in \mathbb{Z} \setminus \{-1, 0, 1\}$, allora $\exists p_1, p_2, \ldots, p_n \in \mathbb{Z}$ primi tali che $m = p_1 \cdot p_2 \cdot \cdots \cdot p_n$

Proof. Dimostriamo tramite principio di seconda forma.
Caso base: abbiamo dimostrato che 2 è primo, quindi vale per esso la tesi induttiva. Ipotizzo quindi che la tesi valga $\forall n \in \mathbb{N}\ (2 \leq n < m)$.
Se m è primo, la tesi è provata banalmente.
Se m non è primo, allora, per il Lemma sui Divisori dei non Primi

$$\exists a, b \in \mathbb{N} \setminus \{0, 1, m\}\ (m = ab)$$

e quindi si ha che $1 < a, b < m$. Quindi per ipotesi induttiva:

$$(\exists t, u \in \mathbb{N})\ (\exists p_1, \ldots, p_t, p_{t+1}, \ldots, p_{t+u} \in \mathbb{N})$$

$$(a = p_1 \cdot \ \ldots \ \cdot p_t \ \wedge \ b = p_{t+1} \cdot \cdots \cdot p_{t+u})$$

e dunque

$$m = a \cdot b = p_1 \cdot \ \ldots \ \cdot p_t \cdot p_{t+1} \cdot \ \ldots \ \cdot p_{t+u}$$

e la tesi induttiva è dimostrata, e dunque essa vale $(\forall n \in \mathbb{N})(n \geq 2)$.
Considerando $m \in \mathbb{Z} \setminus \mathbb{N}$. Allora $-m \in \mathbb{N}$ e vale per esso la tesi

$$\exists p_1, \ldots, p_r\ (-m = p_1 \cdot \ldots \cdot p_r) \implies m = -(p_1 \cdot \ldots \cdot p_r) = -p_1 \cdot \ldots \cdot -p_r$$

Dato che l'opposto di un numero primo è ancora un numero primo, allora la tesi vale in tutto $\mathbb{Z}$ □

7.6 Seconda Tesi del Teorema Fondamentale dell'Aritmetica

Se $m = q_1 \cdot \ \ldots \ \cdot q_n$ allora $r = s$ ed $\exists f : \{1, \ \ldots \ , r\} \to \{1, \ \ldots \ , r\}$ biettiva tale che $\forall i \in \{1, \ \ldots \ , r\}\ (p_i = q_{f(i)})$

Proof. Dimostriamo per Principio di Induzione di Prima Forma.
Caso base: $r = 1$. Sia

$$p_1 = m = q_1 \cdot \ \dots \ \cdot q_s$$

Quindi m è primo, e quindi

$$\forall q \in \{q_1, \ \dots \ , q_s\} \ (q|m \implies q \in \{-1, 1, -m, m\}) \implies$$

$$\implies (r = s = 1) \ \wedge \ (q_1 = p_1)$$

Ora ipotizziamo che la tesi sia vera per $r - 1$. Dimostriamo che è vera per r. Abbiamo che

$$p_1 \cdot p_2 \cdot \ \dots \ \cdot p_r = m = q_1 \cdot q_2 \cdot \ \dots \ \cdot q_r$$

Allora

$$p_1 | q_1 \cdot q_2 \cdot \ \dots \ \cdot q_r$$

e per la definizione di primo allora

$$p_1|q_1 \ \vee \ p_1|q_2 \ \cdot \ \dots \ \cdot q_r$$

Ancora una volta, per la definizione di primo

$$p_1|q_2 \vee p_1|q_3 \cdot \ \dots \ \cdot q_r$$

e così via. Dunque sia ha che

$$p_1|q_1 \ \vee \ p_1|q_2 \vee \ \dots \ \vee \ p_1|q_s$$

Suppongo senza ledere la generalità che $p_1|q_1$. Essendo q_1 primo, allora $q_1 = \pm p_1$(in quanto q_1 è divisibile solo da $\pm 1, \pm q_1$, ed essendo p_1 primo a sua volta non può essere ± 1). Abbiamo dunque che

$$p_1 \cdot p_2 \cdot \ \dots \ \cdot p_r = (\pm p_1) \cdot q_2 \cdot \ \dots \ \cdot q_s$$

E dunque cancellando p_1 da entrambi i membri:

$$p_2 \cdot \ \dots \ \cdot p_r = \pm q_2 \cdot \ \dots \ \cdot q_s$$

Siamo dunque nel caso $r - 1$ e quindi vale in esso la tesi induttiva, cioè

$$r - 1 = s - 1 \ \wedge \ (\exists \sigma : \{2, ..., r\} \to \{2, ..., r\} \text{ biettiva})$$

$$\forall i \in \{2, ..., r\} \ (p_i = \pm q_{\sigma(i)})$$

Basta quindi definire:

$$f : i \in \{2, ..., r\} \mapsto \begin{cases} \sigma(i) & i \in \{2, ..., r\} \\ 1 & i = 1 \end{cases}$$

Per avere la tesi. □

8 Insiemi Ordinati

8.1 Insieme delle Relaioni d'Ordine

Dato a, allora definiamo gli insiemi:

$OL(a) = \{\rho \in P(P(P(a \times a))) \mid \rho \text{ riflessiva, asimmetrica, transitiva}\}$
$OS(a) = \{\rho \in P(P(P(a \times a))) \mid \rho \text{ antiriflessiva, asimmetrica, transitiva}\}$

8.2 Le relazioni appartengono a $P(P(P(a \times a)))$

Proof. Consideriamo la relazione

$$\rho = (a \times a, g) = \{\{a \times a\}, \{a \times a, g\}\}$$

$$a \times a \subseteq a \times a \implies a \times a \in P(a \times a)$$
$$g \subseteq a \times a \implies g \in P(a \times a)$$

Questo implica che

$$\{a \times a\} \in P(P(a \times a))$$
$$\{a \times a, g\} \in P(P(a \times a))$$

E dunque

$$\{\{a \times a\}, \{a \times a, g\}\} \in P(P(P(a \times a)))$$

□

8.3 DA *OL* a *OS* e viceversa

Sia $\rho \in OL(a)$, definisco

$$\rho^{\wedge} :\Leftrightarrow (\forall x, y \in a)(x\rho^{\wedge}y \iff (x\rho y \wedge x \neq y))$$

Sia $\rho \in OS(a)$, definisco

$$\rho^{\vee} :\Leftrightarrow (\forall x, y \in a)(x\rho^{\vee}y \iff (x\rho y \vee x = y))$$

Si dimostra che

$$f : \rho \in OL(a) \mapsto \rho^{\wedge} \in OS(a)$$

è biettiva e la sua inversa è

$$f^{-1} : OS(a) \mapsto \rho^{\vee} \in OL(a)$$

Pertanto, per ogni relazione d'ordine stretto esiste una corrispondente relazione d'ordine largo e viceversa.

8.4 Insieme Ordinato

Sia $s \neq \emptyset$ e sia ρ una relazione d'ordine su s. La coppia (s, ρ) si dice insieme ordinato.

8.5 Relazione d'ordine Indotto

Sia (s, ρ) un insieme ordinato e sia $t \subseteq s$. Definiamo relazione d'ordine indotto da (s, ρ) su t la relazione d'ordine:

$$\rho_t = (t \times t, g_\rho \cap (t \times t))$$

8.6 Sottoinsieme Ordinato

Dato un'insieme ordinato (s, ρ) e dato $t \subseteq s$ e ρ_t la relazione d'ordine indotta da (s, ρ) su t, allora definiamo (t, ρ_t) sottoinsieme ordinato di (s, ρ).

8.7 Elementi Confrontabili

Dato un insieme ordinato (s, ρ), due elementi $x, y \in s$ si dicono confrontabili $\iff$

$$x \rho y \vee y \rho x$$

8.8 Relazione d'Ordine Totale

Data una relazione d'ordine (s, ρ), se ogni elemento di s è confrontabile, allora ρ si dice relazione d'ordine totale e (s, ρ) si dice insieme totalmente ordinato.

8.9 Minimo e Massimo di un Insieme Ordinato

Dato un insieme ordinato (s, ρ) allora:

$$m \in s \text{ massimo di } s : \iff \forall x \in s \ (x \rho m)$$

$$m \in s \text{ minimo di } s : \iff \forall x \in s (m \rho x)$$

8.10 Insieme Ben Ordinato

Un insieme ordinato (s, ρ) si dice ben ordinato se ogni suo sottoinsieme non vuoto (incluso sé stesso) è dotato di minimo.

8.11 Unicità di Minimi e Massimi di un Insieme Ordinato

Se esiste minimo e/o massimo in un insieme ordinato (s, ρ) allora essi sono unici.

Proof. Dimostriamo per il minimo, il caso del massimo è del tutto analogo.

$$Siano\ m_1, m_2 \in s\ minimi\ di\ s.$$

Per definizione di minimo:

$$\forall x \in s\ (m_1 \rho x)\ \wedge\ \forall x \in s\ (m_2 \rho x)$$

Per l'asimmetria di ρ segue:

$$(m_1 \rho m_2\ \wedge\ m_2 \rho m_1)\implies m_1 = m_2$$

□

8.12 Notazione di Minimo e Massimo di un Insieme

Essendo minimo e massimo di un insieme t unici li noteremo come $max(t)$ e $min(t)$.

8.13 Buon Ordine implica Ordine Totale

Se (s, ρ) è un insieme ben ordinato, allora esso è anche totalmente ordinato.

Proof.

$$\forall x, y \in s$$

$$\exists n \in \{x, y\}$$

$$n = min(\{x, y\})\implies n = x \vee n = y \implies x \rho y \vee y \rho x$$

□

8.14 Relazione di Copertura

Dato un insieme ordinato (s, ρ) ed $x, y \in s$ diremo che:
y COPRE $x : \iff x \rho y\ \wedge\ \nexists z \in s\ (z \neq x\ \wedge\ z \neq y\ \wedge\ x \rho z\ \wedge z \rho y)$

8.15 Predecessore/Successore Immediato

Dato un insieme ordinato (s, ρ) e $x, y \in s$ tale che y copre x, allora diremo che y è l'immediato successore x e che x è l'immediato predecessore di y.

8.16 Diagramma di Hasse

Dato un insieme ordinato (s, ρ) definiremo il suo diagramma di Hasse la coppia $(s \times s, g)$ tale che

$$\forall x, y \in s \quad (x, y) \in g \iff y \text{ COPRE } x$$

8.17 Rappresentazione Grafica del Diagramma di Hasse

Dato un insieme ordinato (s, ρ) su cui definiamo un diagramma di Hasse, lo rappresenteremo graficamente assegnando ad ogni elemento di s un vertice, connettendo due vertici con un lato solo se uno copre l'altro, con il vertice che copre piazzato più in alto rispetto a quello coperto.

8.18 Ordine Totale e Diagrammi di Hasse

Si osserva che se l'insieme è totalmente ordinato, il suo diagramma di Hasse è una linea.

8.19 Funzione Crescente fra Insiemi Ordinati

Dati due insiemi ordinati (s, ρ) e $(\bar{s}, \bar{\rho})$, diremo che la funzione $f : s \to \bar{s}$ è crescente : $\iff$

$$\forall x, y \in s \ (x \rho y \implies f(x) \ \bar{\rho} \ f(y))$$

8.20 Isomorfismo di Insiemi Ordinati

Dati due insiemi ordinati (s, ρ) e $(\bar{s}, \bar{\rho})$, diremo che la funzione $f : s \to \bar{s}$ è isomorfismo : $\iff$

$$\forall x, y \in s \ (x \rho y \iff f(x) \ \bar{\rho} \ f(y))$$

8.21 Insiemi Ordinati Finiti sono Isomorfi solo se hanno lo stesso Diagramma di Hasse

Siano (s, ρ) e $(\bar{s}, \bar{\rho})$ due insiemi ordinati finiti e sia $f : s \to \bar{s}$ un isomorfismo $\iff$ hanno lo stesso Diagramma di Hasse

8.22 Minimali e Massimali di un Insieme Ordinato

Dato un insieme ordinato (s, ρ) e un suo sottoinsieme ordinato $t \subseteq s$, diremo che:
$m \in s$ massimale di $t : \iff$

$$\forall x \in t \ (x \rho m \vee m \rho x \implies x \rho m)$$

$m \in s$ minimale di $t : \iff$

$$\forall x \in t \ (x \rho m \vee m \rho x \implies m \rho x)$$

Cioè un elemento è massimale (o minimale) solo se è più grande (o più piccolo) di ogni elemento con cui è confrontabile.

8.23 Maggioranti e Minoranti di un Insieme Ordinato

Dato un insieme ordinato (s, ρ) e un suo sottoinsieme ordinato $t \subseteq s$, diremo che:
$m \in s$ maggiorante di $t : \iff$

$$\forall x \in t \ (x \rho m)$$

$m \in s$ minorante di $t : \iff$

$$\forall x \in t \ (m \rho x)$$

Cioè un elemento di s è maggiorante (o minorante) solo se è più grande (o più piccolo) di ogni elemento di t.

8.24 Relazione fra Massimali/Maggioranti/Massimi e Minimali/Minoranti/Minimi

$$\text{massimo} \implies \text{maggiorante} \implies \text{massimale}$$
$$\text{minimo} \implies \text{minorante} \implies \text{minimale}$$

8.25 Notazione di Insieme dei Maggioranti e di Insieme dei Minoranti

Dato un insieme ordinato (s, ρ) e un suo sottoinsieme ordinato $t \subseteq s$. Allora noteremo:

$MAGGIOR_{(s,\rho)}(t) :=$ insieme dei maggioranti di t in s
$MINOR_{(s,\rho)}(t) :=$ insieme dei minoranti di t in s

8.26 Insieme Limitato

Sia (s, ρ) un insieme ordinato e $t \subseteq s$. Allora:

t è limitato inferiormente $: \iff MINOR_{(s,\rho)}(t) \neq \emptyset$
t è limitato superiormente $: \iff MAGGIOR_{(s,\rho)}(t) \neq \emptyset$

Cioè se è dotato di minorante e/o maggiorante.

8.27 Insieme Naturalmente Ordinato

(s, ρ) insieme ordinato è naturalmente ordinato : $\iff$ è ben ordinato e ogni sua parte non vuota superiormente limitata ha massimo.

8.28 Il buon ordine implica l'ordine largo

Proof. Sia (s, ρ) un insieme ben ordinato. Allora:

$$\forall x \in s \ (\{x\} \text{ ha minimo } \implies x \rho x)$$

□

8.29 Assioma dei Numeri Naturali

Esiste un insieme naturalmente ordinato non limitato superiormente e questo insieme è $\mathbb{N}$. Questo assioma è equivalente all'Assioma dell'Infinito.

8.30 Principio di Dualità per Insiemi Ordinati

Dato (s, ρ) e la duale $\overline{\rho}$, allora si osserva che: $max(s, \rho) = min(s, \overline{\rho})$ Cioè, ogni massimo è minimo per la duale, e ogni minimo è massimo per la duale. Quindi, se dimostriamo un teorema per il massimo, allora esso varrà anche per il minimo (cioè il massimo della duale), e viceversa.

8.31 Il Minimo (Massimo) è l'unico Minimale (Massimale)

Dato un insieme ordinato (s, ρ) con $m = min(s, \rho)$, allora esso è l'unico minimale interno ad (s, ρ) (per dualità, lo stesso vale per il massimo).

Proof. Sia $n \in s$ minimale di (s, ρ). Per definizione di minimo, si ha che $m \rho n$. Ma questo vuol dire che m, n sono confrontabili, quindi per definizione di minimale $n \rho m$. Per asimmetria, allora i due coincidono. □

8.32 Ogni Insieme Ordinato Finito Non Vuoto di Ordine Largo ha Minimali e Massimali

$$(s, \rho) \wedge \rho \in OL(s) \implies (s, \rho) \text{ ha minimali} \in s$$

Per dualità, allora ha anche massimali.

Proof. Sia $x \in s$. Per assurdo, ipotizziamo che (s, ρ) non abbia minimali, e dunque x non è un minimale. Se $s = \{x\}$, allora x sarebbe minimale, il che è assurdo. Quindi $s \neq \{x\}$. Ipotizziamo che s sia di due elementi. Allora $\exists y \in s \ (x \neq y)$. Ma y, per ipotesi di assurdo, non è minimale. Quindi si deve avere che $x \rho y$, ma ciò implicherebbe che x è minimale. Pertanto, deve $\exists z \in s \ (z \neq x \wedge z \neq y)$. Ma per ipotesi di assurdo, z non è minimale, quindi si deve avere che $x \rho z \vee y \rho z$, ma questo implicherebbe che uno di loro è minimale. Allora deve esistere un elemento w... ma chiaramente questo continua all'infinito, e s è un insieme finito. Pertanto, c'è l'assurdo e deve esistere un minimale. □

8.33 In Insiemi Finiti l'unico Minimale (Massimale) è Minimo (Massimo)

Questo non vale per gli insiemi infiniti.

8.34 Relazione d'Ordine Indotta da una Funzione

Sia $f : a \to b$ e sia $\rho \in OL(b)$. Allora definiamo la relazione ρ_f tale che:

$$\forall x, y \in a \ (x \rho_f y \iff f(x) \rho f(y))$$

la relazione d'ordine indotta da f su a.

8.35 Estremo Superiore ed Estremo Inferiore

Sia (s, ρ) un insieme ordinato e $t \subseteq s$. Definiamo l'estremo inferiore e l'estremo superiore rispettivamente:

$$SUP_{(s,\rho)}(t) = min(MAGGIOR_{(s,\rho)}(t)) \text{ (se esiste)}$$
$$INF_{(s,\rho)}(t) = max(MINOR_{(s,\rho)}(t)) \text{ (se esiste)}$$

9 Reticoli

9.1 Reticolo

Sia (s, ρ) un insieme ordinato, con $\rho \in OL(s)$. Allora: (s, ρ) è un reticolo $:\iff$

$$\forall x, y \in s$$

$$\exists z, w \in s$$

$$z = INF_{(s,\rho)}(\{x, y\}) \wedge w = SUP_{(s,\rho)}(\{x, y\})$$

Cioè l'insieme di ogni coppia di elementi di s è dotato di estremo superiore ed inferiore in s.

9.2 Operazioni in un Reticolo

Dato un reticolo (s, ρ), possiamo definire, $\forall x, y \in s$:

Intersezione reticolare

$$\wedge : (x, y) \in s \times s \mapsto INF_{(s,\rho)}(\{x, y\}) \in s$$

Unione Reticolare

$$\vee : (x, y) \in s \times s \mapsto SUP_{(s,\rho)}(\{x, y\}) \in s$$

Cioè due operazioni binarie ed interne.

9.3 Notazione di Reticolo come Struttura

Dato un reticolo (s, ρ), dato che possiamo definire in esso due operazioni binarie interne $\vee$ e $\wedge$, allora possiamo notarlo come una struttura: $(s, \wedge, \vee)$

9.4 Reticolo Limitato

Un reticolo (s, ρ) si dice limitato se è dotato di minimo e massimo.

9.5 Reticolo Completo

Un reticolo (s, ρ) si dice completo se ogni sua parte non vuota è dotata di estremi superiore ed inferiore. Ogni reticolo completo è anche un reticolo limitato.

9.6 Estremi di Coppie di Elementi Confrontabili di un Reticolo

Dato un reticolo (s, ρ) e due elementi $x, y \in s$. Siano essi confrontabili, ad esempio $x \rho y$. Allora:

$$INF_{(s,\rho)}(\{x, y\}) = (x \wedge y) = x$$
$$SUP_{(s,\rho)}(\{x, y\}) = (x \vee y) = y$$

Proof. $x \rho x$ per riflessività di ρ (che, essendo s un reticolo, deve necessariamente essere d'ordine largo). Per ipotesi, $x \rho y$. Dunque x è minimo di $\{x, y\}$, e quindi è anche estremo inferiore. Analgoamente si dimostra per l'estremo superiore. □

9.7 Enunciato Duale sui Reticoli

Sia (s, ρ) un reticolo, e $(s, \overline{\rho})$ il suo reticolo duale. Se e è un enunciato sui reticoli, dico enunciato duale $\overline{e}$ l'enunciato ottenuto:
- Rimpiazzando ogni ρ in e con $\overline{\rho}$ (e viceversa)
- Rimpiazzando ogni $\wedge$ in e con $\vee$ (e viceversa)

9.8 Principio di Dualità Per i Reticoli

Se e è una formula valida per ogni reticolo, allora anche la sua duale $\overline{e}$ lo è.

Proof. e è valida per ogni reticolo (s, ρ), ma quindi è valida anche per il suo duale $(s, \overline{\rho})$. Ma nel reticolo duale, gli estremi inferiori sono estremi superiori e viceversa. Dunque, e riferito a $(s, \overline{\rho})$ è esattamente $\overline{e}$ riferito a (s, ρ). □

9.9 In un Reticolo ogni Minimale è Minimo e ogni Massimale è Massimo

Proof. Dimostriamo per i minimali, per dualità vale anche per i massimali.
Sia (s, ρ) un reticolo e sia $m \in s$ minimale. Sia $x \in s$ un elemento generico del reticolo. Allora si ha che

$$(m \wedge x) \ \rho \ m$$

per la definizione di estremo inferiore. Ma quindi $m \wedge x$ ed m sono confrontabili, e dunque per la definizione di minimale,

$$m \ \rho \ (m \wedge x)$$

Dunque per asimmetria $m \wedge x = m$, per ogni $x \in s$, e allora m è mimimo di s. □

9.10 In un Reticolo I Minoranti (Maggioranti) dell'Unione sono l'Intersezione dei Minoranti (Maggioranti) di Parti Finite

Sia (s, ρ) un reticolo e siano $a, b \in P(s)$ finiti. Allora:

$$MINOR_{(s,\rho)}(a \cup b) = MINOR_{(s,\rho)}(a) \cap MINOR_{(s,\rho)}(b)$$

Per dualità vale l'analogo per i maggioranti.

Proof.

$$\begin{aligned}
x \in MINOR_{(s,\rho)}(a \cup b) &\iff \forall y \in a \cup b \ (x \rho y) \\
&\iff \forall y \ (y \in a \vee y \in b \implies x \rho y) \\
&\iff \forall y \ (y \in a \implies x \rho y) \wedge \forall y \ (y \in b \implies x \rho y) \\
&\iff x \in MINOR_{(s,\rho)}(a) \wedge x \in MINOR_{(s,\rho)}(b) \\
&\iff x \in MINOR_{(s,\rho)}(a) \cap MINOR_{(s,\rho)}(b)
\end{aligned}$$

□

9.11 I Minoranti (Maggioranti) di un Insieme Ordinato sono i Minoranti (Maggioranti) dell'Estremo Inferiore (Superiore)

Sia (s, ρ) un insieme ordinato e sia $a \subseteq s$. Se esiste $m = INF_{(s,\rho)}(a)$, allora:

$$MINOR_{(s,\rho)}(a) = MINOR_{(s,\rho)}(\{m\})$$

Proof. Questo deriva semplicemente dal fatto che l'estremo inferiore è il massimo dei minoranti. □

9.12 Ogni Parte Finita di un Reticolo è dotata di Estremo Inferiore e Superiore

Sia (s, ρ) un reticolo. Ogni sua parte finita è dotata di estremo inferiore e superiore.

Proof. Siano $a, b \in P(s)$ due insiemi finiti. Allora: 1) Per "I Minoranti (Maggioranti) dell'Unione sono l'Intersezione dei Minoranti (Maggioranti) degli Insiemi Finiti" e per "I Minoranti (Maggioranti) di un Insieme sono i Minoranti (Maggioranti) dell'Estremo Inferiore (Superiore)" abbiamo che:
Siano

$$m_1 = INF_{(s,\rho)}(a)$$
$$m_2 = INF_{(s,\rho)}(b)$$

$$MINOR_{(s,\rho)}(a \cup b) =$$
$$MINOR_{(s,\rho)}(a) \cap MINOR_{(s,\rho)}(b) =$$
$$MINOR_{(s,\rho)}(\{m_1\}) \cap MINOR_{(s,\rho)}(\{m_2\}) =$$
$$MINOR_{(s,\rho)}(\{m_1, m_2\})$$

2) Dimostriamo per induzione su $n = |t|$ dove t è una parte finita di s. Caso base: $n = 1$. Allora t è un singleton, ed il suo unico elemento è (per riflessività) sia estremo superiore che estremo inferiore. Assumendo adesso che la tesi induttiva sia valida per ogni $1 \leq k < n$, dimostriamo per n. Sia $x \in t$. Allora

$$t = (t - \{x\}) \cup \{x\}$$

cioè l'unione di un insieme di ordine $n - 1$ e di uno di ordine 1. Per ipotesi induttiva, allora essi sono dotati di estremi inferiori, con

$$m = INF_{(s,\rho)}(t - \{x\})$$

$$x = INF_{(s,\rho)}(\{x\})$$

Allora, per la (1):

$$MINOR(t) = MINOR((t - \{x\}) \cup x) = MINOR(\{m, x\}).$$

Dato che siamo in un reticolo, la coppia $\{m, x\}$ ha sicuramente estremo inferiore, cioè

$$max(MINOR(\{m, x\})) = max(MINOR(t))$$

da cui la tesi.
Per dualità, lo stesso vale per l'estremo superiore. □

9.13 Commutatività di $\wedge$ e $\vee$

Sia $(s, \wedge, \vee)$ un reticolo. Allora:

$$\forall x, y \in s \ ((x \wedge y = y \wedge x) \wedge (x \vee y = y \vee x))$$

Proof.

$$x \wedge y = INF_{(s,\rho)}(\{x, y\}) = INF_{(s,\rho)}(\{y, x\}) = y \wedge x$$

$$x \vee y = SUP_{(s,\rho)}(\{x, y\}) = SUP_{(s,\rho)}(\{y, x\}) = y \vee x$$

□

9.14 Associatività di $\wedge$ e $\vee$

Sia $(s, \wedge, \vee)$ un reticolo. Allora $\wedge, \vee$ sono associative.

Proof. Dimostriamo per $\vee$, la dimostrazione per $\wedge$ è analoga per dualità. Siano $x, y, z \in s$. Per definizione abbiamo che:

- $x\rho[x \vee (y \vee z)]$
- $(y \vee z)\rho[x \vee (y \vee z)]$
- $y\rho(y \vee z)$
- $z\rho(y \vee z)$

Allora per transitività:

$$y\rho[x \vee (y \vee z)]$$

$$z\rho[x \vee (y \vee z)]$$

E dunque:

$$(x \vee y)\rho[x \vee (y \vee z)]$$

Ed infine:

$$[(x \vee y) \vee z]\rho[x \vee (y \vee z)]$$

Lo stesso procedimento si può fare nel senso opposto per dimostrare che

$$[x \vee (y \vee z)]\rho[(x \vee y) \vee z]$$

Dunque, per asimmetria:

$$[(x \vee y) \vee z] = [x \vee (z \vee y)]$$

□

9.15 Proprietà di Assorbimento di un Reticolo

$$\forall x, y \in s\ ((x \vee (x \wedge y) = x) \wedge (x \wedge (x \vee y) = x))$$

9.16 Proprietà di Idempotenza/Iteratività di $\wedge$ e $\vee$

In un reticolo (s, ρ)

$$\forall x \in s\ (x = x \vee x = x \wedge x)$$

Proof. Dimostriamo per $\wedge$, analogo per $\vee$. Dalle proprietà di assorbimento, segue che:

$$\forall y \in s \ (x \wedge (x \vee y) = x)$$

Dato che $x \wedge x \in s$, allora, ponendo $y = x \wedge x$ e applicando ancora una volta l'assorbimento:

$$x = x \wedge (x \vee (x \wedge x)) = x \wedge x$$

□

9.17 Corrispondenza Biunivoca fra Reticoli e Strutture

Sia s un insieme non vuoto e sia r l'insieme delle relazioni d'ordine largo ρ per cui s è un reticolo. Sia b l'insieme delle coppie di operazioni binarie interne (α, β) tali che entrambe siano commutative, associative, e valga la legge di assorbimento in (s, α, β) Allora l'applicazione

$$f : \rho \in r \mapsto (\wedge_\rho, \vee_\rho) \in b \text{ è biettiva}$$

Cioè, da ogni reticolo si possono definire $\wedge$ e $\vee$, e ogni coppia di operazioni associative, commutative, idempotenti, e per cui vale l'assorbimento sono $\wedge$ e $\vee$ di un qualche reticolo.

Proof. Per dimostrare che f è biettiva, vogliamo trovare la sua inversa. Siano $(\wedge, \vee) \in b$ e definiamo ρ tale che

$$\forall x, y \in s \ (x \rho y \iff x = x \wedge y)$$

Nota che da questo segue che $x \vee y = (x \wedge y) \vee y = y$ per assorbimento.
1) ρ così definita è di ordine largo? Per idempotenza,

$$x \wedge x = x \implies x \rho x$$

quindi vale la riflessività. Se

$$(x = x \wedge y) \wedge (y = y \wedge x)$$

dato che $\wedge$ è ipotizzata commutativa, $x = y$ e quindi vale l'asimmetria. Se $x \rho y \wedge y \rho z$, allora

$$(x = x \wedge y) \wedge (y = y \wedge z)$$

Quindi, per associatività:

$$x = x \wedge (y \wedge z) = (x \wedge y) \wedge z = x \wedge z \implies x \rho z$$

quindi vale la transitività.
ρ è effettivamente una relazione d'ordine largo.
2) Vogliamo far vedere che

$$INF_{(s,\rho)}(\{x, y\}) = x \wedge y$$

e che

$$SUP_{(s,\rho)}(\{x, y\}) = x \vee y$$

per ogni $x, y \in s$. Per assorbimento $(x \wedge y) \vee x = x$ quindi per definizione abbiamo che $(x \wedge y) \rho x$.
Analogamente $(x \wedge y) \rho y$.
Quindi

$$x \wedge y \in MINOR_{(s,\rho)}(\{x, y)\}$$

Vogliamo far vedere che $x \wedge y$ è il massimo dell'insieme. Sia dunque z un generico minorante. Allora si ha:

$$z \rho y \wedge z \rho x \implies (z = z \wedge y) \wedge (z = z \wedge x)$$

E quindi: $z = z \wedge x = (z \wedge y) \wedge x = z \wedge (x \wedge y) \implies z \rho (x \wedge y)$ da cui la tesi che $x \wedge y$ è estremo inferiore. Lo stesso procedimento vale, analogamente, per gli estremi superiori.
Si osserva semplicemente che la funzione $(\wedge, \vee) \in b \mapsto \rho \in r$ è l'inversa di f, da cui la tesi. □

9.18 Isomorfismo fra Reticoli

Siano $(s, \wedge, \vee), (s', \wedge', \vee')$ due reticoli. Allora $f : s \to s'$ si dice isomorfismo fra i due reticoli se:
1) f è biettiva
2) $\forall x, y \in s \ ((f(x \wedge y) = f(x) \wedge' f(y)) \wedge (f(x \vee y) = f(x) \vee' f(y)))$

9.19 Equivalenza fra Isomorfismo di Reticoli e Isomorfismo di Insiemi Ordinati

Siano $(s, \wedge, \vee), (s', \wedge', \vee')$ due reticoli e sia $f : s \to s'$ una funzione biettiva fra i due. Allora: f isomorfismo fra i reticoli $\iff$ f è un isomorfismo di insiemi ordinati fra $(s, \rho_{(\wedge,\vee)})$ e $(s', \rho_{(\wedge',\vee')})$

Proof. Dimostrazione $\Leftarrow$):
Siano $(s, \rho), (s', \rho')$ due reticoli e sia f un isomorfismo di insiemi ordinati fra essi. I reticoli possono essere espressi come strutture $(s, \wedge_\rho, \vee_\rho), (s', \wedge_{\rho'}, \vee_{\rho'})$
Si ha che:

$$\forall x, y \in s$$

$$(x \wedge_\rho y) \rho x$$

$$(x \wedge_\rho y) \rho y$$

Applicando l'isomorfismo:

$$f(x \wedge_\rho y) \rho' f(x)$$

$$f(x \wedge_\rho y) \rho' f(y)$$

Quindi

$$f(x \wedge_\rho y) \in MINOR_{(s', \rho')}(\{f(x), f(y)\})$$

Sia $z \in MINOR_{(s', \rho')}(\{f(x), f(y)\})$.
Si ha che

$$z \rho' f(x)$$

$$z \rho' f(y)$$

Essendo f suriettiva, $\exists w \in s \ (f(w) = z)$. Allora, applicando l'isomorfismo in senso inverso $w \rho x \wedge w \rho y$. Quindi w è minorante di $\{x, y\}$. Allora si ha che:

$$w \rho (x \wedge_\rho y) \implies f(w) \rho' f(x \wedge_\rho y) \implies z \rho' f(x \wedge_\rho y)$$

E quindi $f(x \wedge_\rho y)$ è estremo inferiore di $\{f(x), f(y)\}$, cioè:

$$f(x \wedge_\rho y) = f(x) \wedge_{\rho'} f(y)$$

che è la tesi. Analogamente si dimostra per $\vee$.
Dimostrazione $\Rightarrow$: Sia f isomorfismo fra $(s, \wedge, \vee), (s', \wedge', \vee')$ e siano ρ, ρ' le relazioni d'ordine associate. Prendiamo $x, y \in s : x \rho y$. Per definizione $x = x \wedge y$ e quindi

$$f(x) = f(x \wedge y) = f(x) \wedge' f(y) \iff f(x) \rho' f(y)$$

Questo vale in entrambi i versi (in quanto è una catena di uguaglianze seguita da un'equivalenza materiale) e quindi abbiamo la tesi. $\square$

9.20 Sottoreticolo

Sia $(s, \wedge, \vee)$ un reticolo e sia $t \in P(s) - \{\emptyset\}$.
Se t è parte chiusa rispetto $\wedge, \vee$.
$(t, \wedge, \vee)$ si dice sottoreticolo di $(s, \wedge, \vee)$.

9.21 Intervallo e Intervallo Chiuso

Sia (s, ρ) un insieme ordinato, con $\rho \in OL(s)$.
$i \subseteq s$ intervallo $:\iff$

$$\forall x, y \in i$$

$$\forall z \in s$$

$$(x \rho z \wedge z \rho y \implies z \in i)$$

In particolare, se i è limitato, si dice intervallo chiuso.

9.22 Ogni Intervallo Chiuso di un Reticolo è un Sottoreticolo

Se (s, ρ) è un reticolo, ogni suo intervallo chiuso è un sottoreticolo.

Proof. Sia $i \in s$ un sottointervallo. Allora, dati $x, y \in i$, esiste estremo inferiore $x \wedge y \in s$.

$$min(i) \rho x \wedge min(i) \rho y \implies min(i) \rho (x \wedge y) \rho x \implies x \wedge y \in i$$

Procedimento analogo si effettua per l'estremo superiore. □

9.23 Massimo e Minimo sono Elementi Neutri di un Reticolo (e Viceversa)

Sia (s, ρ) un reticolo. Siano $m, M \in s$. Allora:
m minimo di $s \iff m$ neutro di $\vee_\rho$
M massimo di $s \iff M$ neutro di $\wedge_\rho$

Proof. $\Rightarrow$) Sia $x \in s$. Allora $x \rho M \wedge x \rho x$. Dunque $x = min(\{x, M\}) = x \wedge_\rho M$. Dunque M è neutro.
$\Leftarrow$) $\forall x \in s \ (M \wedge_\rho x = x) \implies \forall x \in s \ (x \rho M)$.
Analogamente si dimostra per il minimo. □

9.24 Reticolo Complementato

Un reticolo limitato (s, ρ) si dice complementato se:

$$\forall x \in s, \ \exists y \in s$$

$$(x \wedge y = min(s) \wedge x \vee y = max(s))$$

E si dice che x è complementato e che y è il suo complemento.

9.25 Elementi Confrontabili e Complementati di un Reticolo sono il Minimo e il Massimo

Sia (s, ρ) un reticolo complementato. Allora: Due elementi $x, y \in s$ sono confrontabili e complementati $\iff$ uno è il minimo e l'altro è il massimo.

Proof. Se i due elementi sono confrontabili, allora essi sono rispettivamente il minimo e massimo della loro coppia, e sono quindi anche estremo inferiore e superiore. Ma essendo i due elementi complementari, per ipotesi, allora si ha che il loro estremo inferiore è il minimo ed il loro estremo superiore è il massimo. Perciò essi coincidono. □

9.26 Reticolo Distributivo

Un reticolo $(s, \wedge, \vee)$ si dice distributivo se valgono entrambe le Leggi Distributive:

$$\forall a, b, c \in s \ (a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c))$$

$$\forall a, b, c \in s \ (a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c))$$

Si dimostra che se in un reticolo vale una legge di distributività, allora vale anche l'altra. Dunque, per essere un reticolo distributivo, basta che valga una delle due leggi dato che l'altra segue.

9.27 Unicità dei Complementi di Reticoli Distributivi

Sia (s, ρ) un reticolo distributivo limitato. Allora ogni complemento è unico.

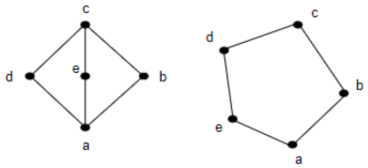
Proof. Sia $x \in s$ e siano $y, z \in s$ suoi complementi. Allora:

$$y = y \wedge max(s) = y \wedge (x \vee z) = (y \wedge x) \vee (y \wedge z) = min(s) \vee (y \wedge z) = y \wedge z$$

E cioè $y \rho z$. Effettuando il procedimento analogamente per z, otteniamo $z \rho y$. Dunque $y = z$ per asimmetria. □

9.28 Criterio di Distributività di Birkhoff

Un redicolo è distributivo $\iff$ non contiene sottoreticoli isomorfi al Reticolo Trirettangolo o al Reticolo Pentagonale.



Osservazioni:
Un reticolo totalmente ordinato è sempre distributivo.
Tutti i reticoli di ordine $n < 5$ sono distributivi.

10 Principio di Induzione

Sia $x \subseteq \mathbb{N} \setminus \{0\}$ Definiamo:

$$\mathbb{N}_{min(x)} = \{n \in \mathbb{N} \mid min(x) \leq n\}$$

Ovvero l'insieme che contiene tutti i numeri naturali $\geq$ del minimo dell'insieme x.

10.1 Prima Forma del Principio di Induzione

$$\forall x \in P(\mathbb{N}) - \{\emptyset\}$$
$$\forall n \in \mathbb{N}$$
$$((n \in x \implies n+1 \in x) \implies (x = \mathbb{N}_{min(x)}))$$

Proof. Sia $m = min(x)$. Ipotizziamo per assurdo che $x \neq \mathbb{N}_m$. Questo implica che

$$y = \mathbb{N}_m - x \neq \emptyset$$

Poniamo $min(y) = n$, che esiste sicuramente perchè $y \subseteq \mathbb{N}$.

$$m < n$$

poiché

$$x \cap y = \emptyset \wedge n \in \mathbb{N}_m$$

Quindi

$$m \leq n - 1 < n \implies (n-1) \in x$$

Per ipotesi, allora

$$(n-1) + 1 \in x \implies n \in x$$

che è assurdo. □

10.2 Seconda Forma del Principio di Induzione

$$\forall x \in P(\mathbb{N}) - \{\emptyset\}$$
$$\forall n \in \mathbb{N}$$
$$\forall k \in \mathbb{N}$$
$$((min(x) \leq k < n \implies k \in x) \implies n \in x) \implies (x = \mathbb{N}_{min(x)})$$

Proof. Sia $m = min(x)$ e supponiamo per assurdo che $x \neq \mathbb{N}_m$. Questo implica che

$$x \subset \mathbb{N}_m \implies y = \mathbb{N}_m - x \neq \emptyset$$

Allora si ha che

$$\forall k \in \mathbb{N}\ (m \leq k < min(y) \implies k \in x)$$

e quindi per ipotesi $min(y) \in x$, che è assurdo. □

11 Calcolo Combinatorio

11.1 Equipotenza

Due insiemi x, y si dicono equipotenti se esiste una funzione $f : x \to y$ biettiva.

11.2 Insieme Infinito

Un insieme x si dice infinito se esiste una biezione $f : x \to t \subset x$ ovvero se esiste una funzione biettiva tra se stesso ed una sua parte propria.

11.3 Insieme Finito

Si dimostra che $\forall n \in \mathbb{N}$ ($\{1, ..., n\}$ non infinito). Un insieme x equipotente ad un insieme $\{1, ..., n\} \subset \mathbb{N}$ si dice finito.

11.4 Cardinalità di un Insieme Finito

Sia x finito. Allora $\exists n \in \mathbb{N}$ (x equipotente a $\{1, 2, ..., n\} \subset \mathbb{N}$). Diciamo che n è l'ordine o cardinalità di x e lo notiamo $|x| = n$.

11.5 Cardinalità dell'Insieme delle Parti di un Insieme Finito

s insieme finito $\implies |P(s)| = 2^{|s|}$

Proof. Dimostriamo per Induzione di Prima Forma su n cardinalità dell'insieme s. Caso base:

$$n = |s| = 0 \implies s = \emptyset \implies P(s) = \{\emptyset\} \implies |P(s)| = 1 = 2^0$$

Dunque la tesi è valida nel caso base. Ipotizziamo che sia valida per $n \in \mathbb{N}$ e dimostriamo che vale per $n + 1$.

$$|s| = n + 1 \implies s \neq \emptyset \wedge \exists f : s \to \{1, 2, ..., n, n + 1\} \text{ biettiva}$$

Consideriamo un qualunque $x \in s$ e poniamo $t = s - \{x\}$. Si ha che

$$1 \leq f(x) = m \leq n + 1$$

Si osserva che la funzione ristretta e ridotta

$$f_{|t} : t \to Im_{f_{|t}} = \{1, 2, ..., m - 1, m + 1, ..., n, n + 1\} \text{ è biettiva}$$

Si può definire una biezione fra $Im_{f_{|t}}$ e $\{1, ..., n\}$ e quindi $|t| = n$.
Per ipotesi induttiva, dunque $|P(t)| = 2^n$.
Ogni sottoinsieme di s può contenere o non contenere x. I sottoinsiemi che non contengono x sono esattamente i sottoinsiemi di $s - \{x\}$, che è un insieme con un elemento in meno ad s, cioè $|s - x| = n$. Per ipotesi induttiva quindi ne esistono 2^n. Ogni sottoinsieme di s che contiene x può essere espresso come $p \cup \{x\}, p \in s - \{x\}$. Dato che esistono 2^n insiemi p, allora esisteranno 2^n insiemi che contengono x. Dunque:

$$|P(s)| = 2^n \cdot 2^n = 2^{n+1}$$

Che è la tesi induttiva. Pertanto essa vale $\forall n \in \mathbb{N}$. □

11.6 Fattoriale

Definiamo

$$0! = 1$$

Poi, ricorsivamente, definiamo:

$$n! = n \cdot (n - 1)!$$

11.7 Numero di Applicazioni fra Due Insiemi Finiti

Siano a, b due insiemi. Allora esistono $|b|^{|a|}$ applicazioni $f : a \to b$.

Proof. Poniamo $|a| = n, |b| = m$. Usiamo la Prima Forma del Principio di Induzione su n.
Consideriamo $n = 0$ come caso base, cioè $a = \emptyset$. Dato che $\emptyset \times b = \emptyset$ e il vuoto ha un solo sottonsieme $\emptyset \subseteq \emptyset \times b$ che può fare da grafico per un'applicazione, esiste una sola possibile applicazione $(\emptyset \times b, \emptyset)$ fra i due insiemi. Dato che $n^0 = 1$, la tesi è valida nel caso base.
Ipotizzando dunque che la tesi sia valida per $n > 0$, dimostriamo che vale per $n + 1$. Sia $x \in a$ e $t = a - \{x\}$. Per ipotesi induttiva, esistono m^n applicazioni da $t \to b$. Ognuna di queste funzioni potrebbe essere prolungata, associando x ad uno qualsiasi degli m elementi di b. Pertanto per ogni funzione esistono m possibili prolungamenti, e quindi il numero totale di applicazioni è $m^n \cdot m = m^{n+1}$ che è la tesi. □

11.8 Condizione di Esistenza di Applicazioni Iniettive fra due Insiemi Finiti

$$MAP_{IN}(a, b) \neq \emptyset \iff |a| \leq |b|$$

Esistono applicazioni iniettive fra due insiemi a e b se e solo se la cardinalità di a è minore o uguale di quella di b.

Proof. Poniamo $|a| = n, |b| = m$.
$\Rightarrow$) Esiste una biezione $I_n \to a$, almeno una funzione $f \in MAP_{IN}(a, b)$, e una biezione $b \to I_m$. Pertanto, la loro composizione è una funzione iniettiva da $I_n \to I_m$. Pertanto, $n \leq m$ in quanto per ognuno degli n-esimi elementi deve esistere almeno un elemento distinto in I_m.
$\Leftarrow$)Se $n \leq m$, allora $\{1, ..., n\} \subseteq \{1, ..., m\}$ ed esiste quindi la funzione immersione fra i due, che è una funzione iniettiva. Esiste dunque una biezione da $a \to \{1, ..., n\}$, una funzione iniettiva (l'immersione) da $\{1, ..., n\} \to \{1, ..., m\}$ ed una biezione da $\{1, ..., m\} \to b$ e dunque esiste una funzione iniettiva $a \to b$. □

11.9 Numero di Applicazioni Iniettive fra due Insiemi Finiti

$$MAP_{IN}(a, b) \neq \emptyset \implies |MAP_{IN}(a, b)| = \frac{|b|!}{(|b| - |a|)!}$$

Cioè, se esistono applicazioni iniettive fra due insiemi finiti, quello è il loro numero.

Proof. Poniamo $|a| = n, |b| = m$, $n \leq m$ altrimenti non esisterebbero applicazioni iniettive. Dimostriamo per Induzione di Prima Forma su n.
Caso base: $n = 0$. Quindi $a = \emptyset$. Esiste una sola funzione fra il vuoto e b, ed essa è iniettiva in quanto verifica vacuamente l'implicazione nella definizione di iniettività. Dato che $\frac{m!}{(m-0)!} = 1$ la tesi è valida.
Ipotizziamo dunque che la tesi sia valida anche per $\forall(n-1) > 0$, e dimostriamo che è valida in n. Siano $x \in a, t = a - \{x\}$. Dunque $|t| = n - 1$ ed esistono $\frac{m!}{(m-(n-1))!}$ applicazioni iniettive $t \to b$ per ipotesi induttiva. Ognuna di queste può essere prolungata ad a associando x ad uno qualsiasi degli $m - (n-1)$ elementi rimasti in b (dato che dobbiamo scegliere, per lasciare la funzione iniettiva, un'immagine distinta).
Da ciò segue che esistono $\frac{m!}{(m-(n-1))!} \cdot (m - (n-1))$ funzioni iniettive, e sviluppando:

$$\frac{m!}{(m-(n-1))!} \cdot (m-(n-1)) = \frac{m!}{\cancel{(m-n+1)!}} \cdot \cancel{(m-n+1)} = \frac{m!}{(m-n)!}$$

□

11.10 Condizione di Esistenza di Applicazioni Suriettive fra due insiemi Finiti

$$MAP_{SUR}(a,b) \neq \emptyset \iff a = b = \emptyset \vee 0 < |b| \leq |a|$$

Esistono applicazioni suriettive fra due insiemi a e b se e solo se sono entrambi vuoti o se sono entrambi non vuoti e la cardinalità di a è maggiore o uguale di quella di b.

Proof. Sia $|a| = n, |b| = m$.
$\Rightarrow$) Sia $f : a \to b$ suriettiva. Allora esiste una biezione fra $a \to \{1, ..., n\}$, una funzione suriettiva $a \to b$, ed una biezione $b \to \{1, ..., m\}$. Pertanto esiste una funzione suriettiva $\{1, ..., n\} \to \{1, ..., m\}$. Allora per ogni elemento del secondo insieme esiste un elemento distinto (dalla definizione di applicazione) del primo insieme, pertanto $m \leq n$.
$\Leftarrow$) Se sono entrambi non vuoti e $m \leq n$, allora è banale costruire una funzione suriettiva dato che per ogni possibile elemento di b si può scegliere un elemento distinto di a.
Dimostrazione nel caso particolare in cui sono vuoti: Se $b = \emptyset$, allora a dev'essere anch'esso il vuoto altrimenti non si può avere funzione ben formata fra i due, dato che per ogni elemento di a dev'esistere un elemento di b sua immagine. Se $a = \emptyset$ e b è non vuoto, allora la funzione non può essere suriettiva. Se $a = b = \emptyset$ allora la suriettività

$$\forall y \ (y \in b \implies \exists x \in a \ (y = f(x))$$

è provata vacuamente dato che $y \in b$ è sempre falso. □

11.11 Condizione di Esistenza di Applicazioni Biettive fra due Insiemi Finiti

Dalla condizione di esistenza delle funzioni iniettive e da quella per le funzioni suriettive deriva che, dati insiemi finiti a, b:

$$MAP_{BI}(a, b) \neq \emptyset \iff |a| = |b|$$

11.12 Cardinalità dell'Insieme Simmetrico di un Insieme Finito

$$|SYM(a)| = |a|!$$

Proof. L'insieme simmetrico è l'insieme delle applicazioni biettive $a \to a$. Quindi, dominio e codominio hanno stessa cardinalità e dunque ogni funzione iniettiva è biettiva. Pertanto, possiamo usare la formula per il calcolo del numero delle funzioni iniettive per calcolare le biettive:

$$|SYM(a)| = \frac{|a|!}{(|a| - |a|)!} = \frac{|a|!}{0!} = \frac{|a|!}{1} = |a|!$$

□

11.13 Relazione fra Iniettività e Suriettività di Applicazioni fra Insiemi Finiti di Uguale Cardinalità

Siano a, b insiemi e $f : a \to b$ una funzione. Allora:
$|a| = |b| \implies (f \text{ iniettiva} \iff f \text{ suriettiva} \iff f \text{ biettiva})$

Proof. Poniamo $|a| = |b| = n$. Se $f : a \to b$ è una funzione iniettiva, la sua immagine ha $|n|$ elementi. Ma

$$Imf \subseteq b \wedge |Imf| = |b| = n$$

dunque $Imf = b$ e la funzione è anche suriettiva. Se $f : a \to b$ è una funzione suriettiva, allora esiste sezione $g : b \to a$ tale che $f \circ g = Id_b$. Ma dato che Id_b è biettiva, e dunque iniettiva, allora g è iniettiva. Allora, per come mostrato sopra, essa è anche suriettiva, e dunque è biettiva, e quindi f è la sua inversa ed è biettiva a sua volta. □

11.14 Cancellabilità implica Invertibilità in un Monoide Commutativo Finito

Sia $(s, \cdot)$ un monoide commutativo finito e sia $x \in s$. Allora

$$x \text{ invertibile} \iff x \text{ cancellabile}$$

Proof. In generale, l'invertibilità implica la cancellabilità, indipendentemente che l'insieme sia finito o no. Se x è cancellabile, allora σ_x e δ_x sono iniettive, ma essendo s finito, allora esse sono anche biettive (per il teorema precedente), e quindi:

$$\exists y \in s \ (\sigma_x(y) = xy = 1_s)$$

e quindi y è inverso a destra.

$$\exists z \in s \ (\delta_x(z) = zx = 1_s)$$

e quindi z è inverso a sinistra. Allora $y = z$ e x è invertibile. □

11.15 Anelli Unitari Integri Finiti sono Corpi

Corollario di "Invertibilità e Cancellabilità in un Monoide Commutativo Finito".
Tutti gli anelli unitari integri finiti sono corpi.

Proof. Un anello unitario integro è un corpo se e solo se ogni elemento è invertibile rispetto al prodotto. Essendo integro, non esistono divisori dello zero. Pertanto ogni elemento distinto dallo zero è cancellabile. Essendo l'anello per ipotesi finito, allora, per il teorema di cui questo è corollario, ogni elemento distinto dallo zero è inverbile, e dunque l'anello è un corpo. □

11.16 Domini di Integrità Finiti sono Campi

Corollario di "Invertibilità e Cancellabilità in un Monoide Commutativo Finito"

Proof. Un dominio di integrità finito è un anello unitario integro finito, pertanto, per "Anelli Unitari Integri Finiti sono Corpi", esso è un corpo. Ma un dominio di integrità è commutativo, ed un corpo commutativo è proprio un campo. □

11.17 Funzione Caratteristica

Sia s un insieme e $t \subseteq s$. Allora l'applicazione:
$\chi_{t,s} : x \in s \mapsto \begin{cases} 0 \text{ se } x \notin t \\ 1 \text{ se } x \in t \end{cases}$
Si dice applicazione caratteristica di t in s.

11.18 Ogni sottoinsieme è dotato di funzione caratteristica

$$\varphi : t \in P(s) \mapsto \chi_{t,s} \in \{0,1\}^s \text{ è biettiva}$$

Cioè, esiste una corrispondenza biunivoca fra le parti di un insieme e le funzioni $\{0,1\}^s$. Cioè, ogni parte ha una funzione caratteristica ed ogni funzione a due immagini è funzione caratteristica di un qualche sottoinsieme di s.

Proof. Suriettività) Sia $f \in \{0,1\}^s$. Poniamo

$$t = \overleftarrow{f}(\{1\}) = \{x \in s \mid f(x) = 1\}$$

Se $x \in t \implies \chi_{t,s} = 1 = f(x)$ per costruzione di t.
Se $x \notin t \implies \chi_{t,s} = 0 = f(x)$ per costruzione di t.
Quindi $f = \chi_{t,s}$ e φ è suriettiva.
Iniettività) Sia

$$t \subseteq s \wedge v \subseteq s \wedge t \neq v$$

Senza ledere la generalità prendo $x \in t - v$. Allora

$$\chi_{t,s}(x) = 1$$

$$\chi_{v,s}(x) = 0$$

quindi le funzioni sono distinte e φ è iniettiva. □

11.19 Coefficiente Binomiale

$\forall n, k \in \mathbb{N}$ definiamo:

$$\binom{n}{k} = |P_k(I_n)|$$

Se $n < k$, allora $\binom{n}{k} = 0$

11.20 Sommatoria di Coefficienti Binomiali

$$\forall n \in \mathbb{N}$$
$$\sum_{k=0}^{n} \binom{n}{k} = 2^n$$

Proof. Si osserva che

$$P(I_n) = P_0(I_n) \cup P_1(I_n) \cup ... \cup P_n(I_n)$$

Che sono tutti insiemi disgiunti, pertanto si ha che:

$$|P(I_n)| = |P_0(I_n)| \cup |P_1(I_n)| \cup ... \cup |P_n(I_n)| = \sum_{k=0}^{n} \binom{n}{k} = 2^n$$

□

11.21 Equivalenza di Coefficienti Binomiali

$$\forall n, k \in \mathbb{N}$$
$$k \leq n \implies \binom{n}{k} = \binom{n}{n-k}$$

Proof. Sia

$$f : x \in P(I_n) \mapsto I_n \setminus x \in P(I_n)$$

f è biettiva perché la funzione differenza di insiemi è biettiva. Inoltre, ovviamente, se

$$|I_n| = n \wedge |x| = k \implies |I_n \setminus x| = n - k$$

e dunque:

$$\overrightarrow{f}(P_k(I_n)) = P_{n-k}(I_n)$$

Quindi la funzione:

$$f_{|P_k(I_n)} : x \in P_k(I_n) \mapsto I_n \setminus x \in P_{n-k}(I_n) = Imf_{|P_k(I_n)}$$

E' ancora una biezione. I due insiemi sono equipotenti e dunque:

$$\binom{n}{k} = |P_k(I_n)| = |P_{n-k}(I_n)| = \binom{n}{n-k}$$

Che è la tesi. □

11.22 Formula Ricorsiva per i Coefficienti Binomiali

$$\forall n, k \in \mathbb{N}$$

$$k \leq n \implies \binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}$$

Proof. Sia I_{n+1}. Allora definisco:

$$a = \{x \in P_{k+1}(I_{n+1}) \mid 1 \in x\}$$

$$b = \{y \in P_{k+1}(I_{n+1}) \mid 1 \notin y\}$$

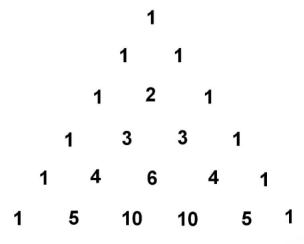
Se rimuovessimo 1 da ogni $x \in a$, questo diminuirebbe la loro cardinalità di uno, rendendola k. Non contenendo 1, sarebbero poi anche sottoinsiemi di cardinalità k dell'insieme $I_{n+1} \setminus \{1\}$, e sarebbero quindi $\binom{n}{k}$ in numero.
Similarmente, gli insiemi di b, non contenendo 1, sono gli insiemi di cardinalità $k+1$ dell'insieme $I_{n+1} \setminus \{1\}$ e quindi sono $\binom{n}{k+1}$ in numero. $\{a, b\}$ è una partizione di $P_{k+1}(I_{n+1})$, e quindi, per il Principio di Inclusione-Esclusione:

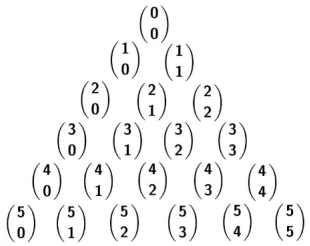
$$\binom{n+1}{k+1} = |P_{k+1}(I_{n+1})| = |a| + |b| = \binom{n}{k} + \binom{n}{k+1}$$

□

11.23 Triangolo di Tartaglia

Triangolo dei Coefficienti Binomiali, che permette di calcolare graficamente il valore di un qualsiasi coefficiente binomiale grazie alla Formula Ricorsiva dei Coefficienti Binomiali.





11.24 Formula Matematica per il Calcolo dei Coefficienti Binomiali

$$\forall n, k \in \mathbb{N}$$

$$k \leq n \implies \binom{n}{k} = \frac{n!}{(n-k)!k!}$$

Proof. Dimostriamo per induzione di seconda forma. Prima di tutto, dobbiamo organizzare i coefficienti binomiali in "linea", in modo che ad ogni coefficiente binomiale possa essere associato un intero. Utilizziamo quindi un ordine lessicografico e diciamo che:

$$\forall x, y, z, w \in \{0, ..., n\}\ ((x, y) < (z, w) \iff (x < z) \wedge (y < w))$$

Si osserva dunque che le coppie associate ai coefficienti binomiali sono così ordinate:
$(0,0) < (1,0) < (1,1) < (2,0) < (2,1) < (2,2) < (3,0) < (3,1) < (3,2) < (3,3) < (4,0) < \dots$
Ora che le coppie sono così messe in ordine, possiamo dire quale sia la zeresima, prima, seconda, n-esima coppia, etc.
Usiamo come caso base l'indice $n = 0$, cioè la zeresima coppia, $\binom{0}{0}$. Esiste un solo insieme di cardinalità zero sottoinsieme del vuoto, il vuoto stesso, quindi

$$1 = \frac{0!}{(0-0)!0!}$$

e la tesi vale nel caso base.
Estendiamo la tesi ad ogni $0 \leq i < n$ per ipotesi induttiva, e dimostriamo che essa vale in n. Ipotizziamo che la coppia di indice n sia $\binom{n}{k}$. Per la Formula Ricorsiva per i Coefficienti Binomiali, allora:

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$$

Ma per l'ordine lessicografico, questi sono minori di $\binom{n}{k}$, quindi vale per essi la tesi induttiva, e quindi:

$$\binom{n-1}{k-1} + \binom{n-1}{k} = \frac{(n-1)!}{(n-1-(k-1))!(k-1)!} + \frac{(n-1)!}{(n-1-k)!k!} =$$

$$= \frac{(n-1)!}{(n-k)!(k-1)!} + \frac{(n-1)!}{(n-k-1)!k!} =$$

$$= \frac{(n-1)!k}{(n-k)!k!} + \frac{(n-1)!(n-k)}{(n-k)!k!} = \frac{(n-1)!(k+n-k)}{(n-k)!k!} =$$

$$= \frac{(n-1)!n}{(n-k)!k!} = \frac{n!}{(n-k)!k!}$$

□

12 Strutture Booleane

12.1 Reticolo Booleano

Un reticolo si dice booleano se è distributivo e complementato

12.2 Algebra di Boole

Una struttura della forma $(s, \wedge_\rho, \vee_\rho, ')$ si dice Algebra di Boole se gode delle seguenti proprietà:

1. $\wedge_\rho, \vee_\rho$ sono commutative
2. Esse sono anche associative
3. Valgono le leggi di assorbimento
4. Vale la distributività
5. $\wedge_\rho, \vee_\rho$ hanno elementi neutri, che notiamo 0,1 rispettivamente.
6. $'$ è un operazione unaria interna (l'operazione complementazione) tale che:
$$\forall x \in s \ (x \vee_\rho x' = 1) \wedge (x \wedge_\rho x' = 0)$$

12.3 Anello Booleano

Un anello unitario $(a, +, \cdot)$ si dice booleano $\iff$

$$\forall x \in a \ (x^2 = x \cdot x = x)$$

12.4 In un Anello Booleano ogni elemento è il Proprio Opposto

$$(a, +, \cdot) \text{ booleano} \implies \forall x \in a \ (x = -x)$$

Proof.

$$\begin{aligned} x + x &= (x + x)^2 && \text{per proprietà degli anelli booleani} \\ &= x^2 + 2x^2 + x^2 && \text{per distributività dell'anello} \\ &= x + 2x^2 + x \end{aligned}$$

Quindi

$$x + x = x + 2x + x \implies 2x = 0 \implies x + x = 0 \implies x = -x$$

□

12.5 Anelli Booleani sono Commutativi

Sia $(a, +, \cdot)$ un anello booleano. Allora $(\forall x, y \in a)(xy = yx)$

Proof. Siano $x, y \in a$. Allora:

$$\begin{aligned} x + y &= (x + y)^2 && \text{prop. dell'anello booleano} \\ &= x^2 + xy + yx + y^2 && \text{prop. distributiva} \\ &= x + xy + yx + y && \text{prop. dell'anello booleano} \\ &\implies xy + yx = 0 \implies xy = -yx \end{aligned}$$

In quanto ogni elemento dell'anello è il proprio opposto $-yx = yx$ quindi abbiamo la tesi. □

12.6 Per ogni Anello Booleano esiste un corrispondente Reticolo Booleano

Dato un anello booleano $(a, +, \cdot)$ definiamo

$$\rho : \forall x, y \in a \ (x \rho y \iff xy = x)$$

Allora vogliamo dimostrare che (s, ρ) è un reticolo.

Proof. Iniziamo col dimostrare che $\rho \in OL(a)$

$$\forall x \in a \ (x \cdot x = x) \implies \forall x \ (x \rho x)$$

per la proprietà principale dell'anello booleano e quindi la relazione è riflessiva.

$$\forall x, y \in a \ (x \rho y \wedge y \rho x \implies xy = x \wedge yx = y \implies x = y)$$

per la commutatività dell'anello booleano e quindi la relazione è asimmetrica.

$$\forall x, y, z \in a$$

$$x \rho y \wedge y \rho x \implies xy = x \wedge yz = y \implies$$

$$x = xy = x(yz) = (xy)z = xz \implies x \rho z$$

la relazione è dunque transitiva. □

Proof. Dimostrazione $\wedge$ e $\vee$
Verifichiamo per ogni coppia che INF e SUP sono così definite:

$$\forall x, y \in a \ (x \vee_\rho y = x + y + xy)$$

$$\forall x, y \in a \ (x \wedge_\rho y = xy)$$

Siano $x, y \in a$. □

Proof. Dimostriamo che $x \vee_\rho y$ è maggiorante.

$$x \cdot (x \vee_\rho y) = x(x + y + xy) = x^2 + xy + x^2 y$$

Per le proprietà dell'anello booleano

$$x^2 = x \text{ e } xy + xy = 0$$

Pertanto $x \cdot (x \vee_\rho y) = x \implies x \rho (x \vee_\rho y)$ perchè $x \rho y \iff xy = x$.
Lo stesso procedimento si può effettuare per y.
Pertanto $x \vee_\rho y$ è maggiorante. □

Proof. Dimostriamo che $x \vee_\rho y$ è estremo superiore, cioè minimo dei maggioranti. Sia $z \in a$ maggiorante di $\{x, y\}$. Allora

$$\begin{aligned} & x\rho z \ \wedge \ y\rho z \\ & \implies (xz = x) \ \wedge \ (yz = y) \\ & \implies (x + y + xy)z = xz + yz + xyz = x + y + xy \\ & \implies (x + y + xy)\rho z \\ & \implies (x \vee_\rho y)\rho z \end{aligned}$$

quindi $(x \vee_\rho y)$ è sup. □

Proof. Dimostriamo che il Reticolo è limitato, distributivo e complementato.
Limitato)

$$\forall x \in a \ (0x = 0 \implies 0\rho x)$$

cioè 0 è il minimo

$$\forall x \in a \ (1x = x \implies x\rho 1)$$

cioè 1 è il massimo, quindi il reticolo è limitato.
Distributivo)

$$x \wedge (y \vee z) = x \wedge (y + z + yz) = x(y + z + yz) = xy + xz + xyz$$

pertanto il reticolo è distributivo.
Complementato) Sia $x \in a$. Allora

$$x \wedge (1 + x) = x(1 + x) = x + x^2 = x + x = 0$$

$$x \vee (1 + x) = x + (1 + x) + x(1 + x) = x + 1 + x + x + x^2 = 1$$

questo perchè ogni elemento è anche il suo opposto. □

12.7 Per ogni Reticolo Booleano esiste un corrispondente Anello Booleano

Sia (s, ρ) un reticolo booleano con almeno due elementi e definiamo:

$$x + y = (x \wedge_\rho y') \vee_\rho (x' \wedge_\rho y)$$

$$x \cdot y = (x \wedge_\rho y)$$

Dimostriamo che $(s, +, \cdot)$ è un anello booleano

Proof. Dimostrare che è un anello booleano vuol dire dimostrare che è un anello unitario dove$\forall x \in s\ (x^2 = x)$.
Associatività:

$$x(yz) = x \wedge (y \wedge y) = (x \wedge y) \wedge y = (xy)z$$

Si dimostra analogamente, ma con una LUNGA serie di calcoli, che vale lo stesso per $x + y$.
Commutatività di $+$:

$$x + y = (x \wedge y') \vee (x' \wedge y) = (y' \wedge x) \vee (y \wedge x') = (y \wedge x') \vee (y' \wedge x) = y + x$$

Definiamo

$$m = min_{(s,\rho)}(s), M = max_{(s,\rho)}(s)$$

Allora

$$x + m = (x \wedge m') \vee (x' \wedge m) = (x \wedge M) \vee (x' \wedge m) = x \vee m = x$$

$$x \cdot M = x \wedge M = x$$

Dunque $m = 0_s$ e $M = 1_s$
Si dimostra tramite calcolo che vale al distributività di $\cdot$ su $+$.
Infine:

$$x^2 = x \cdot x = x \wedge x = x$$

ed abbiamo la tesi. □

12.8 Equivalenza di Strutture Booleane

Si dimostra quindi che Algebre di Boole $\simeq$ Reticoli di Boole $\simeq$ Anelli Booleani In quanto esiste corrispondenza biunivoca fra algebre e reticoli di boole e fra reticoli e anelli booleani.

12.9 L'insieme delle Parti è un Anello Booleano

Proof. Dato che $(P(s), \subseteq)$ è un reticolo booleano, allora $(P(s), \cap, \cup, ')$ è un'algebra di boole, dove

$$\forall x \in P(s)\ (x' = s - x)$$

per la corrispondenza biunivoca fra reticoli ed algebre di boole. Allora

$$(\forall x, y \in P(s))$$

$$x \cdot y = x \cap y$$

$$x + y = (x \cap (s - y)) \cup (y \cap (s - x)) = (x - y) \cup (y - x) = x \triangle y$$

E dunque $(P(s), \triangle, \cap)$ è un anello booleano. □

12.10 Teorema di Stone

Sia $a \neq \emptyset$ e $(a, +, \cdot)$ un anello booleano. Allora

$$\exists s \neq \emptyset\ (a, +, \cdot) \overset{\text{isomorfo}}{\simeq} (P(s), \triangle, \cap).$$

Se a è finito, posso scegliere anche s finito.

12.11 Corollari del Teorema di Stone

1. Il Teorema di Stone si applica anche fra reticoli booleani e $(P(s), \subseteq)$.
2. Se $(a, +, \cdot)$ è un anello booleano e $|a| = m \in \mathbb{N}_2$, allora
$$(\exists n \in \mathbb{N} - \{0\})(m = 2^n)$$
3. Se (a, ρ) è un reticolo booleano e $|a| = m \in \mathbb{N}_1$, allora
$$(\exists n \in \mathbb{N} - \{0\})(m = 2^n)$$
cioè la cardinalità dell'insieme sostegno di un anello booleano è sempre una potenza di due.
4. Due anelli booleani finiti sono isomorfi $\iff$ hanno la stessa cardinalità.

13 Stringhe

13.1 Insieme delle Stringhe

Scriviamo: $\mathbb{Z}_2 = \mathbb{Z}/\equiv_2 = \{[0]_2, [1]_2\}$. Allora, dato $n \in \mathbb{N}$, definiamo $a = \mathbb{Z}_2 \times ... \times \mathbb{Z}_2$ (n volte) l'insieme delle stringhe di 0 ed 1 di lunghezza n.

13.2 Somma e Prodotto Puntuali di Stringhe

Sia $a = \mathbb{Z}_2 \times ... \times \mathbb{Z}_2$, $n \in \mathbb{N}$ volte. Allora, presi $x, y \in a$ tali che $x = (x_1, ..., x_n), y = (y_1, ..., y_n), x_i, y_i \in \{0, 1\} \forall i \in I_n$, allora definiamo la somma puntuale:

$$x + y = ([x_1 + y_1], [x_2 + y_2], ..., [x_n + y_n])$$

Analogamente, definiamo il prodotto puntuale:

$$x \cdot y = ([x_1 \cdot y_1], ..., [x_n \cdot y_n])$$

13.3 Stringhe e Funzioni Caratteristiche

Dato un insieme $s : |s| = n > 0$ e $t \subseteq s$, allora la funzione caratteristica $\chi_{t,s}$ può essere vista analoga ad una stringa, dato che associa ad ogni elemento di t o 0 o 1.

13.4 L'Anello delle Parti e l'Anello delle Stringhe sono Isomorfi

Sia $n \in \mathbb{N} - \{0\}$ e $s = \{1, 2, ..., n\}$. Allora la funzione

$$\varphi : x \in P(s) \mapsto \chi_{t,s} \in \mathbb{Z}_2 \times ...\mathbb{Z}_2$$

(n volte) è un'isomorfismo fra

$$(P(s), \triangle, \cap)$$

e

$$(\mathbb{Z}_2 \times ... \times \mathbb{Z}_2 \text{ (n volte)}, +, \cdot)$$

(dove $+, \cdot$ sono la somma e prodotto puntuali).

14 Divisibilità

14.1 Divisori e Multipli

Sia $(s, \cdot)$ un semigruppo commutativo. Allora, $\forall x, y \in s$, diremo che:

$$\begin{matrix} x|y \\ x \text{ divide } y \\ y \text{ e' multiplo di } x \end{matrix} :\iff \exists z \in s \ (xz = y)$$

$$DIV_s(x) = \{y \in s \mid y|x\}$$

$$MULT_s(x) = \{z \in s \mid x|z\}$$

14.2 Elementi Associati

Sia $(s, \cdot)$ un semigruppo commutativo. Allora diremo che due elementi x, y sono associati se si dividono a vicenda.

$$x, y \text{ associati } :\iff x \in DIV_s(y) \wedge y \in DIV_s(x)$$

14.3 Insieme degli Associati

Sia $(s, \cdot)$ un semigruppo commutativo. Allora, $\forall x \in s$, definiamo l'insieme degli associati di x:

$$ASSOC_s(x) = \{y \in s \mid x|y \wedge y|x\}$$

14.4 Associati di un Elemento Cancellabile

Sia $(s, \cdot)$ un monoide commutativo. Se $x \in s$ è un elemento cancellabile, allora:

$$ASSOC_s(x) = \{xu \in s \mid u \in U(s)\}$$

Cioè tutti gli associati di un elemento cancellabile sono il prodotto di x per un elemento invertibile di s.

Proof. $\supseteq$) Sia $u \in U(s)$. Allora

$$x|xu$$

ma

$$(xu)u^{-1} = x$$

quindi

$$xu|x$$

Pertanto

$$xu \in ASSOC_s(x)$$

$\subseteq$) Sia $y \in ASSOC_s(x)$. Allora

$$\exists w, z \in s \text{ tali che } y = xw \text{ e } x = yz$$

Allora, usando la cancellabilità di x:

$$x = xwz \implies wz = 1 \implies w, z \text{ invertibili} \implies$$

$$\implies w \in U(s) \implies y \in \{xu \mid u \in U(s)\}$$

Da cui la tesi. □

14.5 Associati hanno stessi Divisori e Multipli

Sia $(s, \cdot)$ un monoide commutativo. Allora, $\forall x, y \in s$:

$$y \in ASSOC_s(x) \overset{(1)}{\iff} DIV_s(x) = DIV_s(y) \overset{(2)}{\iff} MULT_s(x) = MULT_s(y)$$

Proof. $1 \Rightarrow$) Segue dalla transitività della divisione $|$.
$1 \Leftarrow$) $y \in DIV(y) \implies y \in DIV(x) \implies y|x$.
Lo stesso vale per x, quindi $y \in ASSOC(x)$.
$2 \Leftrightarrow$) Segue immediatamente dalla definizione di insieme dei divisori e dei multiplil. □

14.6 Massimi Comuni Divisori e Minimi Comuni Multipli

Sia $(s, \cdot)$ un monoide commutativo e sia $t \subseteq s$. Allora definiamo:

$$MCD_s(t) = \{d \in \bigcap_{x \in t} DIV_s(X) \mid (\forall z \in \bigcap_{x \in t} DIV_s(x))(z|d)\}$$

$$mcm_s(t) = \{d \in \bigcap_{x \in t} MULT_s(X) \mid (\forall z \in \bigcap_{x \in t} MULT_s(x))(d|z)\}$$

Bisogna fare attenzione che nonostante si utilizzino i termini "massimo" e "minimo" questi non vanno intesi come terminologia delle relazioni d'ordine, in quanto la divisione non è necessariamente una relazione d'ordine. Il massimo e i minimi di un insieme sono sempre unici, mentre l'MCD e gli mcm, come si può vedere dalla definizione, sono un insieme e pertanto ne possono esistere molteplici.

14.7 Divisori Banali

Sia $(s, \cdot)$ un monoide commutativo e sia $x \in s$. Allora definiamo l'insieme dei divisori banali:

$$BDIV_s(x) = U(s) \cup ASSOC_s(x)$$

14.8 Elemento Irriducibile (in un Dominio di Integrità)

Sia $(s, +, \cdot)$ un dominio di integrità e sia $x \in s$. Allora x si dice:

$$x \text{ irriducibile } :\iff x \notin U(s) \wedge DIV_s(x) = BDIV_s(x)$$

14.9 Primo

Sia $(s, \cdot)$ un monoide commutativo.

$$p \in s \text{ primo } :\iff \forall a, b \in s \ (p|ab \implies p|a \vee p|b)$$

14.10 Coprimo

Sia $(s, \cdot, 1_s)$ un monoide commutativo. Allora:

$$x, y \in s \text{ coprimi } :\iff 1_s \in MCD(\{x, y\})$$

Cioè se l'unità è un loro MCD.

14.11 Monoide Cancellativo

Un monoide commutativo si dice cancellativo se ogni suo elemento è cancellabile.

14.12 Monoide Fattoriale

Un monoide commutativo $(m, \cdot)$ si dice fattoriale se vale una delle seguenti proprietà:

1. Ogni $x \in m - U(m)$ è un prodotto di primi.
2. Ogni $x \in m - U(m)$ è prodotto di irriducibili, ed ogni irriducibile è primo.
3. Ogni $x \in m - U(m)$ è prodotto di irriducibili, ed ogni fattorizzazione è unica a meno dell'ordine dei fattori e del prodotto per invertibili.

NO DIM: si dimostra che queste tre condizioni sono fra di loro equivalenti.

14.13 Anello Fattoriale

Un anello commutativo unitario $(a, +, \cdot)$ si dice anello fattoriale se $(a - \{0_a\}, \cdot)$ è un monoide fattoriale.

14.14 Caratterizzazione di MCD e mcm per Associati

Sia $(s, \cdot)$ un monoide commutativo, siano $x, y \in s$. allora:

$$m \in MCD(x,y) \iff ASSOC(m) = MCD(x,y)$$

$$m \in mcm(x,y) \iff ASSOC(m) = mcm(x,y)$$

Proof. $\rightarrow$)

$$m|x \wedge m|y \ \wedge \ \forall z \in s \ (z|x \wedge z|y \implies z|m)$$

poiché esso è MCD. Sia

$$n \in ASSOC(m) \implies n|m \wedge m|n \implies n|x \wedge n|y \wedge \forall z \in s \ (z|m \implies z|n)$$

$$\implies n|x \wedge n|y \ \wedge \ \forall z \in s \ (z|x \wedge z|y \implies z|n) \implies n \in MCD(x,y)$$

Quindi

$$ASSOC(m) \subseteq MCD(x,y)$$

Se invece

$$n \in MCD(x,y) \implies m|n \wedge n|m \implies n \in ASSOC(m)$$

Pertanto

$$MCD(x,y) \subseteq ASSOC(m) \implies ASSOC(m) = MCD(x,y)$$

$\leftarrow$) $m \in ASSOC(m)$ in quanto $(s, \cdot)$ è un monoide.

$$ASSOC(m) = MCD(x,y) \implies m \in MCD(x,y)$$

□

14.15 Fattorizzazione in Primi in un Monoide Fattoriale

Sia $(m, \cdot)$ un monoide fattoriale. Sia $a \in m - U(m)$, allora

$$a = p_1^{k_1} \cdot p_2^{k_2} \cdot ... \cdot p_n^{k_n}$$

I divisori di a sono tutti e soli gli elementi associati ad elementi del tipo

$$p_1^{l_1} \cdot ... \cdot p_n^{l_n} \text{ con } 0 \leq l_i \leq k_i, \ \forall i \in I_n$$

14.16 Numero di Divisori in $\mathbb{N}$

Corollario di "Fattorizzazione in Primi in un Monoide Fattoriale"
Sia

$$a = p_1^{k_1} \cdot p_2^{k_2} \cdot ... \cdot p_n^{k_n} \in \mathbb{N}$$

allora a ha esattamente

$$\prod_{i=1}^{n}(k_i + 1)$$

divisori.

14.17 Numero di Divisori in $\mathbb{Z}$

Corollario di "Fattorizzazione in Primi in un Monoide Fattoriale"
Sia

$$a = p_1^{k_1} \cdot p_2^{k_2} \cdot ... \cdot p_n^{k_n} \in \mathbb{Z}$$

allora a ha esattamente

$$2 \cdot \prod_{i=1}^{n}(k_i + 1)$$

divisori.

14.18 MCD e mcm dalle Fattorizzazioni

Sia $(m, \cdot)$ un monoide fattoriale e siano:

$$a = p_1^{k_1} \cdot ... \cdot p_n^{k_n}$$

$$b = p_1^{l_1} \cdot ... \cdot p_n^{l_n}$$

Dove $p_1, ..., p_n$ comprende tutti i primi che compaiano nelle fattorizzazioni di a o b. Nel caso un primo appaia nella fattorizzazione di a, ma non di b (o viceversa), allora esso può essere considerato come elevato allo zero nella fattorizzazione in cui non compare.
Poniamo inoltre

$$\forall i \in \mathbb{N}\ (1 \leq i \leq n \implies \alpha_i = MAX(k_i, l_i) \wedge \beta_i = MIN(k_i, l_i))$$

Allora, abbiamo che:

$$m = p_1^{\alpha_1} \cdot ... \cdot p_n^{\alpha_n} \in mcm(a, b)$$

$$M = p_1^{\beta_1} \cdot ... \cdot p_n^{\beta_n} \in MCD(a, b)$$

ESEMPIO:

$$a = 2 \cdot 3^2 \cdot 5 \qquad = 90 = 2 \cdot 3^2 \cdot 5 \cdot 11^0 \cdot 13^0$$
$$b = 3 \cdot 5^2 \cdot 11 \cdot 13 \qquad = 10725 = 2^0 \cdot 3 \cdot 5^2 \cdot 11 \cdot 13$$

Pertanto:

$$m = 2 \cdot 3^2 \cdot 5^2 \cdot 11 \cdot 13 \qquad = 64350$$
$$M = 2^0 \cdot 3 \cdot 5 \cdot 11^0 \cdot 13^0 \qquad = 15$$

14.19 Associati da MCD e mcm

Corollario di "Teorema: MCD e mcm dalle Fattorizzazioni"
Se

$$m \in mcm(a, b) \wedge M \in MCD(a, b)$$

allora

$$m \cdot M \in ASSOC(a, b)$$

14.20 Proprietà di Divisione Lineare dei Divisori Comuni

Sia $(s, +, \cdot)$ un anello commutativo unitario e siano $a, b \in s$. Se

$$d \in DIV_{(s,\cdot)}(a) \cap DIV_{(s,\cdot)}(b)$$

allora

$$\forall x, y \in s \ (d|(xa + yb))$$

Cioè i divisori comuni dividono ogni combinazione lineare degli elementi.

Proof.

$$d|a \wedge d|b \implies (\exists h, k \in \mathbb{Z})(a = dk \wedge b = dh)$$

E quindi:

$$\forall x, y \in Z \ (ax + by = dkx + dhy = d(kx + hy) \implies d|(ax + by))$$

□

14.21 Valore Assoluto

Sia $n \in \mathbb{Z}$. Allora definiamo la funzione valore assoluto come:

$$|n| : n \in \mathbb{Z} \mapsto \begin{cases} n & \text{se } n \in \mathbb{N} \\ -n & \text{se } n \in \mathbb{Z} - \mathbb{N} \end{cases}$$

14.22 Teorema della Divisione Euclidea (o con Resto)

$$\forall m, n \in \mathbb{Z} \ (m \neq 0 \implies (\exists!(q, r) \in \mathbb{Z} \times \mathbb{N})(n = mq + r \wedge 0 \leq r < |m|))$$

Proof. (Caso $n \in \mathbb{N}$)
Dimostriamo per induzione di seconda forma su n.
Allora se $n = 0$, scelgo $q = 0 = r$.
Se $0 < n < |m|$, allora $q = 0, r = n$.
Se $n = |m|$, allora ci sono due possibilità:

$$n = m \text{ e } q = 1, r = 0$$

oppure

$$n = -m \text{ e } q = -1, r = 0$$

Se $n > |m|$. Consideriamo vero $\forall i \in \mathbb{N}\ |m| \leq i < n$. Allora prendiamo $n - |m| < n$, e quindi per ipotesi induttiva

$$\exists q_1, r_1\ (n - |m| = mq_1 + r_1 \wedge 0 \leq r_1 \leq |m|)$$

Quindi $n = mq_1 + |m| + r_1$.
Quindi, se $m > 0$, allora $(q, r) = (q_1 + 1, r_1)$.
Se $m < 0$, allora $(q, r) = (q_1 - 1, r_1)$.
Allora per induzione la tesi vale $\forall n \in \mathbb{N}$.
(Caso $n \in \mathbb{Z} - \mathbb{N}$) sappiamo che la tesi vale $\forall n \in \mathbb{N}$. Supponiamo invece che $n \in \mathbb{Z} - \mathbb{N}$. Allora

$$-n \in \mathbb{N} \implies -n = mq_1 + r_1$$

con

$$0 \leq r < |m| \implies n = m(-q_1) - r_1 = m(-q_1) - r_1 + |m| - |m|$$

(aggiungo $+|m| - |m|$ cosi che $0 \leq r < |m|$)
Consideriamo i due casi possibili:

$$m > 0 \implies n = m(-q_1 - 1) + m - r \implies (q, r) = (-q_1 - 1, m - r)$$

$$m < 0 \implies n = m(-q_1 + 1) - m - r \implies (q, r) = (-q_1 + 1, -m - r)$$

Pertanto la tesi è valida anche in $\mathbb{Z}$.
Dimostrazione che (q, r) è unico: Siano $(q_1, r_2), (q_2, r_2) \in \mathbb{Z} \times \mathbb{N}$. Ipotizziamo WLOG che $0 \leq r_1 \leq r_2 < |m|$ e che $n = mq_1 + r_1 = mq_2 + r_2$.
Allora

$$m(q_1 - q_2) = r_2 - r_1$$

e quindi

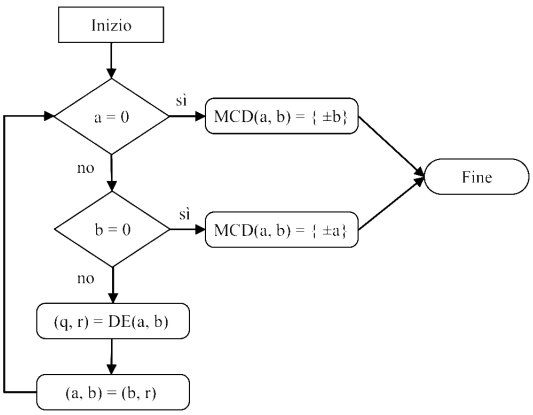
$$|m||q_1 - q_2| = |m(q_1 - q_2)| = |r_2 - r_1| \text{ e } 0 \leq |r_2 - r_1| < |m|$$

Segue che $|m||q_1 - q_2| < |m|$ che può succedere solo, dato che $m \neq 0$ per ipotesi, se $|q_1 - q_2| = 0 \implies q_1 = q_2$.
E quindi

$$n = mq_1 + r_1 = mq_1 + r_2 \implies r_1 = r_2$$

da cui la tesi. □

14.23 Algoritmo delle Divisioni Successive



Siamo sicuri che l'algoritmo abbia fine perché la successione dei resti è crescente limitata inferiormente dallo zero.

$$
\begin{aligned}
a &= bq_1 + r_1 \\
b &= r_1 q_2 + r_2 \\
r_1 &= r_2 q_3 + r_3 \\
&\dots \\
r_{t-4} &= r_{t-3} q_{t-2} + r_{t-2} \\
r_{t-3} &= r_{t-2} q_{t-1} + r_{t-1} \\
r_{t-2} &= r_{t-1} q_t + r_t
\end{aligned}
$$

con $r_t = 0$
$MCD(a, b) = \pm r_{t-1}$
Con i resti: $0 = r_t < r_{t-1} < \dots < r_1 < b$

14.24 Teorema di Bézout

$$\forall (a, b) \in \mathbb{Z} \times \mathbb{Z} - \{(0, 0)\}$$
$$\forall d \in MCD(a, b)$$
$$\exists u, v \in \mathbb{Z}$$
$$(d = au + bv)$$

Cioè, per ogni MCD di una coppia di valori a, b, esiste una combinazione lineare dei due che lo esprime.

Proof. Si consideri l'Algoritmo delle Divisioni Successive, per equazioni. Sia t il minimo numero di passi tali che $r_t = 0$. Se $t = 1$, allora $r_1 = 0$ e $a = bq_1 \implies b \in MCD(a, b)$ e $b = a \cdot 0 + b \cdot 1$. Quindi $(u, v) = (0, 1)$.
Se $t = 2$, allora $r_1 \neq 0 \wedge r_2 = 0$. Quindi $r_1 \in MCD(a, b)$ e $r_1 = a \cdot 1 + b \cdot (-q_1)$. Quindi $(u, v) = (1, -q_1)$.
Supponiamo vero l'asserto per ogni $r_i : 1 \leq i < t$. Dato che

$$r_t = 0 \implies r_{t-1} \in MCD(a, b)$$

$$r_{t-1} = r_{t-3} + r_{t-2}(-q_{t-1})$$

perchè $r_{t-3} = r_{t_2} q_{t-1} + r_{t-1}$
Ma per l'ipotesi induttiva, allora

$$\exists u, v, w, x \in \mathbb{Z} \ (r_{t-3} = au + bv \wedge r_{t-2} = aw + bx)$$

Quindi

$$r_{t-1} = (au + bv) + (aw + bx)(-q_{t-1}) =$$

$$= aw + bw - awq_{t-1} - bxq_{t-1} = a(w - wq_{t-1}) + b(v - xq_{t-1})$$

Da cui la tesi. □

14.25 Lemma di Euclide

Siano $a, b, c \in \mathbb{Z}$. Se a, b sono coprimi, allora $a|bc \implies a|c$.

Proof. $1 \in MCD(a, b)$ perché sono coprimi. Per il Teorema di Bézout,

$$\exists u, v \in \mathbb{Z} \ (au + bv = 1)$$

Quindi $c = acu + bcv$. Dato che $a|ac$ (banalmente) e $a|bc$ (per ipotesi), allora

$$\exists h, k \in \mathbb{Z} \ (c = acu + bcv = ahu + akv \implies c = a(hu + kv) \implies a|c)$$

($ac = ah$ perchè $a|ac$ quindi $\exists h \in \mathbb{Z}(ah = ac)$)
($bc = ak$ perchè $a|bc$ per ipotesi quindi $\exists k \in \mathbb{Z}(ak = bc)$) □

14.26 In $\mathbb{Z}$ i primi sono tutti e soli gli irriducibili

In $\mathbb{Z}$, i primi sono tutti e soli gli irriducibili. Cioè, $p \in \mathbb{Z}$ primo $\iff p$ irriducibile.

Proof. $\Rightarrow$) Sia $p \in \mathbb{Z}$ primo e siano $a, b \in \mathbb{Z}$ tali che $p = ab$.
p è primo $\implies p|a \vee p|b$.
Ipotizziamo senza ledere la generallità che $p|a$.
Quindi

$$p|a \wedge a|p^* \implies p \in ASSOC(a) = \{a, -a\}$$

Quindi

$$p = \pm a \implies b = \pm 1$$

Dunque, p ha solo divisori banali ed è dunque irriducibile.
$\Leftarrow$) Sia $p \in \mathbb{Z}$ irriducibile, cioè $DIV(p) = BDIV(p) = \{-1, 1, p, -p\}$.
Siano $a, b \in \mathbb{Z}$ tali che $p|ab$.
Supponendo che $p \nmid a$, bisogna dimostrare che necessariamente $p|b$.
Si ha che

$$MCD(p, a) \subseteq DIV(p) = \{-1, 1, -p, p\}^{**}$$

ma dato che $p \nmid a$, allora $MCD = \{-1, 1\}$ e quindi i due sono coprimi.
Per il Lemma di Euclide, $p|b$.

(*) $a|p$ perchè $p = ab$ per ipotesi quindi $\exists b \in \mathbb{Z}$ $(ab = p)$.
(**) dato che l'$MCD \subseteq DIV(p) \cap DIV(a)$. □

14.27 Caratterizzazione Lineare di Classe di Resto

$$[a]_m = \{b \in \mathbb{Z} \mid m|(a - b)\} = \{a + km \mid k \in \mathbb{Z}\}$$

Questo perchè sommando e sottraendo più volte m al rappresentante della classe possiamo ottenere tutti gli elementi della classe.

14.28 Operazione Parziale: Modulo

$$\forall(a,m) \in (Z \times (\mathbb{Z} - \{0\}))\ (a \bmod m = MIN([a]_m \cap \mathbb{N}))$$

Il modulo è un'operazione "parziale" perché non è definita in $\mathbb{Z} \times \mathbb{Z}$, ma in $\mathbb{Z} \times (\mathbb{Z} - \{0\})$, cioè non è possibile effettuare $a \bmod 0$.

Proprietà del Modulo

- $a \bmod m < |m|$
- $a \bmod m =$ resto di $DE(a,m)$

Notazioni del Modulo

Le seguenti notazioni sono equivalenti:

- $a \bmod m$
- $a \ \% \ m$
- $REST(a,m)$

14.29 Caratterizzazione di $\mathbb{Z}_m$

Sia $m \in \mathbb{N} - \{0\}$. Allora $\mathbb{Z}_m = \{[0]_m, [1]_m, \ldots, [m-1]_m\}$ e in particolare si ha che $|\mathbb{Z}_m| = m$

Proof. L'insieme $\{[0]_m, [1]_m, \ldots, [m-1]_m\}$ è un insieme di classi di equivalenza di elementi di $\mathbb{Z}$, quindi per definizione dev'essere sottoinsieme del suo insieme delle classi di resto. Sia $a \in \mathbb{Z}$.

$$DE(a,m) = (q,r) \land a = qm + r \land 0 \leq r < |m|$$

Quindi

$$qm = a - r \implies m|a - r \implies [a]_m = [r]_m$$

Quindi

$$\mathbb{Z}_m \subseteq \{[0]_m, [1]_m, \ldots, [m-1]_m\}$$

Quindi, dato che si contengono a vicenda, per estensionalità

$$\mathbb{Z}_m = \{[0]_m, [1]_m, \ldots, [m-1]_m\}$$

Vogliamo adesso dimostrare che le classi di resto in $\mathbb{Z}_m$ sono a due a due distinte, e sono quindi m in numero. Siano

$$i, j \in \mathbb{Z} : 0 \leq i \leq j < m \land [i]_m = [j]_m$$

Allora

$$0 \leq j - i < m \land (\exists k \in \mathbb{Z})(j = i + km) \implies j - i = km \implies j - i = 0$$

in quanto esso è strettamente minore di m. □

14.30 Relazione di Equivalenza Compatibile

Sia $s \neq \emptyset$ e $*$ un'operazione binaria interna ad esso, e $\sim$ una relazione di equivalenza su esso. Allora:

$\sim$ compatibile a sx in $(s,*) : \iff \forall a, b, c \in s \ (a \sim b \implies c * a \sim c * b)$

$\sim$ compatibile a dx in $(s,*) : \iff \forall a, b, c \in s \ (a \sim b \implies a * c \sim b * c)$

14.31 Congruenza

Sia $s \neq \emptyset$ e siano $*_1, \ldots, *_n$ operazioni binarie interne ad esso, e sia $\sim$ una relazione di equivalenza.

$$\sim \text{ congruenza in } (s, *_1, \ldots, *_n) : \iff$$

$$\forall a, b, c, d \in s$$

$$\forall i \in \mathbb{N}$$

$$0 \leq i \leq n \implies (a \sim b \wedge c \sim d \implies a *_i c \sim b *_i d)$$

14.32 Epimorfismo fra Strutture e Strutture Quoziente

Se $\sim$ è una congruenza in $(s, *_1, \ldots, *_n)$, allora sono ben poste le operazioni

$$\forall i : 0 \leq i \leq n :$$

$$(*_i)_\sim : ([x]_\sim, [y]_\sim) \in s/\sim \times s/\sim \mapsto [x *_i y]_\sim \in s/\sim$$

E la proiezione canonica $\pi : x \in s \mapsto [x]_s \in s/\sim$ è epimorfismo tra le strutture $(s, *_1, \ldots, *_n)$ e $(s/\sim, (*_1)_\sim, \ldots, (*_n)_\sim)$

14.33 Congruenza equivale a Compatibilità

Una relazione di equivalenza su una struttura $(s, *_1, \ldots, *_n)$ è una congruenza $\iff$ è compatibile con ogni operazione della struttura.

Proof. Posso supporre un'unica operazione in $(s, *)$.
$\Rightarrow$) Se ipotizziamo

$$a, b \in s : a \sim b$$

$$c \in s : c \sim c$$

abbiamo

$$(c * a \sim c * b) \wedge (a * c \sim b * c)$$

$\Leftarrow$) Supponiamo che $a \sim b \wedge c \sim d$.
Per ipotesi di compatibilità a destra

$$a * c \sim b * c$$

per compatibilità a sinistra

$$b * c \sim b * d$$

abbiamo

$$a * c \sim b * c \sim b * d$$

quindi

$$a * c \sim b * d$$

□

14.34 Anello Quoziente di $\mathbb{Z}$

Sia $\equiv_m$ una congruenza in $(\mathbb{Z}, +, \cdot)$. Allora essa è epimorfa all'anello quoziente $(\mathbb{Z}_m, +_m, \cdot_m)$.

14.35 Asserti Equivalenti su Anelli Quoziente di $\mathbb{Z}$

Sia $m \in \mathbb{Z} - \{0\}$. Sono equivalenti le seguenti affermazioni:

1. $(\mathbb{Z}_m, +_m, \cdot_m)$ è un campo.
2. $(\mathbb{Z}_m, +_m, \cdot_m)$ è un dominio di integrità.
3. m è primo.

Proof. $1 \to 2$) Ovvio perché ogni campo è dominio di integrità.
$2 \to 3$) Siano $a, b \in \mathbb{Z} : m = ab$. Allora

$$[m]_m = [0]_m = [ab]_m = [a]_m \cdot [b]_m$$

Trovandoci in un dominio di integrità, vale la Legge di Annullamento del Prodotto e

$$[a]_m \cdot [b]_m = [0]_m \iff [a]_m = [0]_m \vee [b]_m = [0]_m$$

Suppongo senza ledere la generalità che $[a]_m = [0]_m$, cioè

$$a \equiv_m 0 \iff (\exists k \in \mathbb{Z})(a = km)$$

Allora

$$m = ab = kmb \implies kb = 1 \implies b = \pm 1 \wedge a = \pm m$$

Allora m è irriducibile in $\mathbb{Z}$, ed è quindi anche primo.
$3 \to 1$) Sia $[a]_m \neq [0]_m$. Posso scegliere $0 < a < |m|$. m è irriducibile, cioè i suoi divisori sono $\{\pm 1, \pm m\}$ quindi $MCD(a, m) = \{\pm 1\}$ e per il Teorema di Bézout

$$\exists u, v \in \mathbb{Z}\ (1 = au + mv)$$

Allora si ha che

$$[1]_m = [au + mv]_m = [au]_m + [0]_m = [au]_m = [a]_m \cdot [u]_m$$

quindi $[a]_m$ è invertibile.
Dato che ogni elemento è invertibile ci troviamo in un Campo. □

14.36 Equazione Diofantea

Siano $a, b, c \in \mathbb{Z}$. La funzione:

$$e[a, b, c] : (x, y) \in \mathbb{Z} \times \mathbb{Z} \mapsto ax + by - c \in \mathbb{Z}$$

si dice equazione diofantea di 1° grado, a due incognite, con termini a, b, e c.

14.37 Notazione Sintetica di Equazione Diofantea

Un'equazione diofantea della forma $e[a, b, c](x, y)$ si può esprimere sinteticamente $ax + by = c$

14.38 Soluzione dell'Equazione Diofantea

Data un'equazione diofantea $e[a, b, c](m, n)$, la coppia (x, y) per cui

$$e[a, b, c](x, y) = 0 \iff ax + by = c$$

si dice, se esiste, soluzione dell'equazione diofantea.

14.39 Asserti Equivalenti al Teorema di Bézout

Siano $a, b \in \mathbb{Z}, d \in MCD(a, b)$. Allora sono equivalenti i seguenti:

1. Il Teorema di Bézout
2. a, b coprimi $\iff (\exists u, v \in \mathbb{Z})(1 = au + bv)$
3. $< a, b >= d\mathbb{Z}$
4. L'equazione diofantea $ax + by = c$ ha soluzioni $\iff d|c$

Proof. $1 \to 2)$ $\to$) Per Bézout, se a, b sono coprimi, allora esistono

$$u, v : 1 = au + bv$$

$\leftarrow$) Se $\exists u, v : 1 = au + bv \implies d|1$, ma $d \in MCD(a, b)$, quindi $1 \in MCD(a, b)$ e dunque essi sono coprimi.
$2 \to 3)$ $a, b \in d\mathbb{Z}$ e $d\mathbb{Z}$ sottogruppo, quindi $< a, b > \subseteq d\mathbb{Z}$. Scrivo

$$a = a_1 d \wedge b = b_1 d$$

Poiché $d \in MCD(a, b)$, a_1, b_1 sono coprimi. Allora, per (2), trovo

$$u, v \in \mathbb{Z} : 1 = a_1 u + b_1 v \implies d = a_1 du + b_1 dv = au + bv \in < a, b >$$

Per asimmetria dunque $d\mathbb{Z} =< a, b >$.
$3 \to 4)$ $\to$) Ci sono

$$m, n \in \mathbb{Z} : am + bn = c$$

$$d|a \wedge d|b \implies d|c$$

$\leftarrow$) Sia $d|c$, allora $c \in d\mathbb{Z} =< a, b >$ per (3). Ma allora

$$\exists m, n \in \mathbb{Z} \ (am + bn = c)$$

$4 \to 1)$ Se prendo $d = c$, ha soluzioni $ax + by = d$, cioè

$$\exists m, n \in \mathbb{Z} \ (am + bn = d)$$

che è esattamente Bézout. □

14.40 Caratterizzazione dell'Insieme delle Soluzioni di Equazioni Diofantee

Sia $ax + by = c$ un'equazione diofantea con soluzione (x_0, y_0). Allora se $d \in MCD(a, b)$, l'insieme delle soluzioni dell'equazione è

$$\{(x_0 + \frac{b}{d}k, y_0 - \frac{a}{d}k) \mid k \in \mathbb{Z}\}$$

Proof. Chiamiamo l'insieme delle soluzioni s, e l'insieme che vogliamo dimostrare equivalente m, per comodità. Vogliamo dunque dimostrare che $m = s$.
$\subseteq$)Sostituendo si vede che

$$m \subseteq s : a(x_0 + \frac{b}{d}k) + b(y_0 - \frac{a}{d}k) = ax_0 + by_0 + \frac{\cancel{ab}}{\cancel{d}}k - \frac{\cancel{ab}}{\cancel{d}}k = c$$

$\supseteq$) Sia $(x, y) \in s$. Cioè, $ax + by = c = ax_0 + by_0$. Allora

$$a(x - x_0) = b(y_0 - y) \implies \frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y)$$

dato che $d \in MCD(a, b)$
$\frac{a}{d}, \frac{b}{d}$ sono coprimi, quindi per il lemma di Euclide:

$$\exists h, k \in \mathbb{Z} : \begin{cases} h\frac{a}{d} = y_0 - y \\ k\frac{b}{d} = x - x_0 \end{cases}$$

E quindi, sostituendo:

$$\frac{a}{d}(k\frac{b}{d}) = \frac{b}{d}(h\frac{a}{d}) \implies h = k \implies x = x_0 + k\frac{b}{d} \wedge y = y_0 - k\frac{a}{d}$$

Da cui la tesi. □

14.41 Equazione Congruenziale

$m \in \mathbb{Z} - \{0\}, a, b \in \mathbb{Z}$. Allora la funzione:

$$ec[a, b, m] : [n]_m \in \mathbb{Z}_m \mapsto [an - b]_m \in \mathbb{Z}_m$$

Si dice equazione congruenziale di 1° grado, con una incognita, di termini a e b e modulo m.

14.42 Soluzione dell'Equazione Congruenziale

$n \in \mathbb{Z}$ si dice soluzione di un'equazione congruenziale $ec[a, b, m]$ se $ec[a, b, m](n) = [0]_m$, ovvero se $an \equiv_m b$. Chiaramente, dalla definizione di classi di resto, si ottiene che ogni valore congruente ad n, cioè appartenente a $[n]_m$, è a sua volta soluzione.

14.43 Criterio per l'Esistenza di Soluzioni di un'Equazione Congruenziale

Siano $a, b \in \mathbb{Z}, m \in \mathbb{Z} - \{0\}, d \in MCD(a, m)$. Allora $ax \equiv_m b$ ha soluzioni $\iff d|b$.

Proof. L'equazione congruenziale $ax \equiv_m b$ può essere espressa come equazione diofantea $ax + my = b$. Per la 4^a Tesi di "Teorema sugli Asserti Equivalenti al Teorema di Bézout", allora l'equazione diofantea ha soluzioni solo se $d \in MCD(a, m)$ divide b. □

14.44 Primo Corollario del Teorema sull'Esistenza di Soluzioni di un'Equazione Congruenziale

Siano $a, b \in \mathbb{Z}, m \in \mathbb{Z} - \{0\}, d \in MCD(a, m)$. Allora:

$$[a]_m \in U(\mathbb{Z}_m) \iff a, m \text{ coprimi}$$

Proof. $\rightarrow$) Esiste $[u]_m$ tale che $[a]_m \cdot [u]_m = [1]_m$. Ma quindi l'equazione congruenziale $ax \equiv_m 1$ ha soluzione u, e questo implica (per il Teorema sull'Esistenza di Soluzioni) che $d|1$. Ma $1|d$ quindi i due sono associati e 1 è MCD, quindi a e m sono coprimi.
$\leftarrow$ Se a, m sono coprimi, allora 1 è MCD e ovviamente $1|1$ quindi per il Teorema sull'Esistenza delle Soluzioni, l'equazione congruenziale $ax \equiv_m 1$ ha soluzioni e quindi esiste un $[a]_m$ è invertibile. □

14.45 Secondo Corollario del Teorema sull'Esistenza di Soluzioni di un'Equazione Congruenziale

Siano $a, b \in \mathbb{Z}, m \in \mathbb{Z} - \{0\}, d \in MCD(a, m)$. Allora:

$$[a]_m \in U(\mathbb{Z}_m) \iff [a]_m \text{ non è divisore dello zero}$$

Proof. $\rightarrow$)Per assurdo, sia $[a]_m$ divisore dello zero. Allora

$$\exists [b]_m \in \mathbb{Z}_m - \{[0]_m\} : [a]_m[b]_m = [0]_m$$

Ma invertibilità implica cancellabilità, e quindi si avrebbe $[b]_m = [0]_m$ il che è assurdo.
$\leftarrow$) Per assurdo, sia $[a]_m$ non invertibile. Allora per il 1° Corollario, a, m non sono coprimi. Allora prendo $d \in \mathbb{Z}$ con $d \neq 1$ tale che

$$\exists k \in \mathbb{Z} \ (ad = km)$$

Quindi:

$$[a]_m[d]_m = [ad]_m = [km]_m = [0]_m$$

che è assurdo. □

14.46 Risoluzione di Eq. Congruenziali: Termini Congruenti

$a, b \in \mathbb{Z}, m \in \mathbb{Z} - \{0\}$.
L'equazione congruenziale $ax \equiv_m b$ ha lo stesso insieme di soluzioni dell'equazione congruenziale $a'x \equiv_m b'$, per ogni $a' \in [a]_m, b' \in [b]_m$.

Proof. Dato che $[a']_m = [a]_m \wedge [b']_m = [b]_m$ per ipotesi:

$$ax \equiv_m b \iff [a]_m[x]_m = [b]_m \iff a'x \equiv_m b'x$$

□

14.47 Equazione Congruenziale come Equazione Diofantea

Un'equazione congruenziale $ax \equiv_m b$ si può esprimere nella forma:

$$ax + my = b$$

Cioè come equazione diofantea.

Proof.

$$ax \equiv_m b \implies m|(ax-b) \implies \exists k \in z\ (mk = ax - b)$$

E quindi:

$$ax - mk = b$$

Ponendo $y = -k$ abbiamo la tesi. □

14.48 Risoluzione di Eq. Congruenziali: Equazione "Multiplo"

$a, b \in \mathbb{Z}, m \in \mathbb{Z} - \{0\}$.
Osserviamo che, nel risolvere $ax \equiv_m b$, allora $\forall k \in \mathbb{Z} - \{0\}$ si ha che l'equazione $akx \equiv_{mk} bk$ ha lo stesso insieme di equazioni.

Proof. Questo deriva semplicemente dal fatto che:

$$ax + my = b \iff akx + mky = bk$$

E da questo segue che se abbiamo che

$$\exists k \in \mathbb{Z}\ (a = a'k \wedge b = b'k \wedge m = m'k)$$

allora l'equazione $a'x \equiv_{m'} b'$ ha lo stesso insieme di soluzioni di $ax \equiv_m b$. □

14.49 Risoluzione di Eq. Congruenziali: Coprimi del Modulo

$a, b \in \mathbb{Z}, m \in \mathbb{Z} - \{0\}$.
Per ogni k coprimo ad m, l'equazione $akx \equiv_m bk$ ha lo stesso insieme di soluzioni di $ax \equiv_m b$.

Proof. Sia x soluzione dell'equazione congruenziale $akx \equiv_m bk$. Quindi

$$[a]_m[k]_m[x]_m = [b]_m[k]_m$$

Dato che k è coprimo ad m, $[k]_m$ è invertibile e dunque cancellabile. □

14.50 Algoritmo per la Soluzione di Equazioni Congruenziali

Data $ax \equiv_m b$, allora per risolverla seguiamo i seguenti step:

1. Ridurre a, b in modo tale che $0 \leq a, b \leq m-1$.
2. Prendere $d \in MCD(a, m)$. Se $d \nmid b$, non ho soluzioni. Se $d|b$, continuo.
3. Scrivo $a = a'd, b = b'd, m = m'd$. Passo all'equazione equivalente $a'x \equiv_{m'} b'$.
4. Trovo l'inverso (in $(\mathbb{Z}_{m'}, \cdot)$) di $[a']_{m'}$, tramite l'algoritmo delle divisioni successive esteso, e lo dico $[k]_{m'}$.
5. L'insieme delle soluzioni è $[b'k]_{m'}$, poiché è una classe di resto di modulo m/d con $d \in MCD(a, m)$

14.51 Elemento Periodico di un Gruppo

Sia $(g, \cdot)$ un gruppo, $x \in g$. x si dice periodico se:

$$\exists n \in \mathbb{N} - \{0\} \ (x^n = 1_g)$$

14.52 Periodo di un Elemento Periodico

Siano $(g, \cdot)$ un gruppo ed $x \in g$ un suo elemento periodico.

$$\text{Il minimo } n \in \mathbb{N} - \{0\} : x^n = 1_g$$

si dice periodo di x e si indica $|x|$.

14.53 Relazione fra Periodo e Cardinalità del Sottogruppo Generato

Siano $(g, \cdot), x \in g$ un gruppo ed un suo elemento periodico. Allora:
$|x| = n \iff | < x > | = n$
Cioè il periodo di x è uguale alla cardinalità del sottogruppo generato da x.

14.54 Teorema su Esponenti di Elementi Periodici e Congruenza

Siano $(g, \cdot), x \in g$ un gruppo ed un suo elemento periodico, tale che $|x| = m \in \mathbb{N} - \{0\}$. Allora:

$$\forall a, b \in \mathbb{Z}\ (x^a = x^b \iff a \equiv_m b)$$

Proof. Sia $x^a = x^b$. Moltiplichiamo ambo i membri per l'inverso di x^b e abbiamo quindi che

$$x^a = x^b \iff x^a \cdot x^{-b} = x^b \cdot x^{-b} = x^{b-b} = 1_g \iff x^{a-b} = 1_g = x^0$$

Prendiamo $DE(a-b, m) = (q, r)$. Quindi

$$1_g = x^{a-b} = x^{qm+r} = (x^m)^q \cdot x^r = (1_g)^q \cdot x^r = x^r$$

Dato che $0 \leq r < m$, allora $r = 0$ e quindi $a \equiv_m b$. □

15 Polinomi

15.1 Definizione di Successione di Elementi

Sia $(a, +, \cdot)$ un anello unitario commutativo. Allora una funzione del tipo $n \in \mathbb{N} \mapsto x \in a$ si dice successione di elementi di a.

15.2 Notazione di Successione di Elementi

Sia $(a, +, \cdot)$ un anello commutativo unitario. Sia $f : n \in \mathbb{N} \mapsto x \in a$ una successione di elementi di a. Allora:

$$(a_n)_{n\in\mathbb{N}} := f$$
$$a_n = f(n)$$

15.3 Polinomio

Sia $(a, +, \cdot)$ un anello commutativo unitario e sia $(a_n)_{n\in\mathbb{N}}$ una successione di elementi di a. Allora:

$$(a_n)_{n\in\mathbb{N}} \text{ poliniomio a coefficienti in } a \iff \exists k \in \mathbb{N}\ (\forall n \geq k\ (a_n = 0))$$

15.4 Coefficienti di un Polinomio

I termini di successione a_n di un polinomio $(a_n)_{n\in\mathbb{N}}$ si dicono coefficienti del polinomio.

15.5 Notazione di Insieme dei Polinomi

Sia $(A, +, \cdot)$ un anello commutativo unitario. Allora l'insieme dei polinomi a coefficienti in A si scrive $A[x]$

15.6 Polinomio Zero o Nullo

Sia $(a, +, \cdot)$ un anello commutativo unitario. Allora definiamo il polinimio nullo o polinomio zero:

$$0 := (0_a)_{n\in\mathbb{N}}$$

Dove

$$(0_a)_{n\in\mathbb{N}} = (a_n)_{n\in\mathbb{N}}$$
$$\forall n \in \mathbb{N}\ (a_n = 0_a)$$

15.7 Coefficiente Direttore di un Polinomio

Se $f \in A[x] - \{0\}$, $a_{gr(f)}$ si dice coefficiente direttore del polinomio e si indica $cd(f)$

15.8 Termine Noto di un Polinomio

Dato un polinomio $f \in A[x]$, allora a_0 si dice termine noto di f.

15.9 Grado e Coefficiente Direttore del Polinomio Zero

Poniamo:

$$cd(0) = 0$$
$$gr(0) = -\infty$$

Cioè il grado di 0 è l'ordinamento di $(N \cup \{-\infty\}, \leq)$

15.10 Polinomio Monico

$f \in A[x]$ si dice polinomio monico se $cd(f) = a_{gr(f)} = 1_a$

15.11 Somma e Prodotto di Polinomi

Siano $(a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}} \in A[x]$ due polinomi. Allora definiamo:

$$(a_n + b_n)_{n\in\mathbb{N}} = (a_n)_{n\in\mathbb{N}} + (b_n)_{n\in\mathbb{N}}$$
$$(\sum_{i+j=n} a_i b_j)_{n\in\mathbb{N}} = (a_n)_{n\in\mathbb{N}} \cdot (b_n)_{n\in\mathbb{N}}$$

15.12 Anello dei Polinomi

Avendo definito somma e prodotto per i polinomi, possiamo affermare che $(A[x], +, \cdot)$ è un anello commutativo unitario.

- Il neutro rispetto a $\cdot$ è $(1, 0, 0, 0, ...)$
- Il neutro rispetto a $+$ è $(0, 0, 0, 0, ...)$

15.13 Polinomio Costante

Sia $(A, +, \cdot)$ un anello commutativo unitario e sia $a \in A$. Allora il polinomio del tipo $(a, 0, 0, 0, 0, ...)$ si dice polinomio costante.

15.14 Notazione di Polinomio Costante

Facendo abuso di notazione, $\forall a \in A$, definiamo $a := (a, 0, 0, 0, 0, ...)$ Cioè indichiamo il polinomio costante con il suo unico coefficiente non nullo.

15.15 Monomorfismo dei Polinomi Costanti

Sia $(A, +, \cdot)$ un anello commutativo unitario. Si osserva allora che:

$$\mu : a \in A \mapsto (a, 0, 0, 0, ...) \in A[x]$$

è un monomorfismo di anelli fra $(A, +, \cdot)$ e $(A[x], +, \cdot)$.
In particolare,

$$a \overset{isomorfo}{\simeq} Im(\mu)$$

15.16 Polinomio incognita

Definiamo il polinomio $x := (0, 1_A, 0, 0, 0, 0, ...)$ Cioè il polinomio $x \in A[x]$ tale che il suo unico coefficiente non nullo è l'unità dell'anello $(A, +, \cdot)$ nella seconda posizione.

15.17 Potenze del Polinomio incognita

Si può provare per induzione che:

$$\begin{aligned} x &= (0, 1, 0, 0, 0...) \\ x^2 &= (0, 0, 1, 0, 0, ...) \\ x^3 &= (0, 0, 0, 1, 0, ...) \\ &\dots \\ x^n &= (0, \dots, 0 \text{ (n volte)}, 1, 0, ...) \end{aligned}$$

15.18 Monomio

Dato una anello $(A, +, \cdot)$, sia $a \in A$, e sia $x = (0, 1_A, 0, ...)$. Allora abbiamo che:

$$ax^n = (a, 0, 0, 0, ...) \cdot (0, \cdots, 0 \text{ (n volte)}, 1_a, 0, 0...) =$$

$$= (0, ..., 0 \text{ (n volte)}, a, 0, 0, ...)$$

Il monomio ax^n dunque non è nient'altro che il polinomio a coefficienti tutti nulli, eccetto quello in posizione n+1-esima, che ha valore a. (n+1 perchè la prima posizione è x^0).

15.19 Polinomio come Somma di Monomi

Sia f un polinomio tale che $m \in \mathbb{N} \wedge gr(f) = m$ della forma

$$f = (a_0, a_1, a_2, a_3, ..., a_m, 0, , ...)$$

Allora è facile verificare che esso si può esprimere nella forma:

$$f = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + ... + a_m x^m$$

15.20 Proprietà della Somma e Prodotto di Polinomi

Dalla distributività in $(A[x], +, \cdot)$ seguono le seguenti proprietà di somma e prodotto. Siano $f, g \in A[x], m = gr(f), n = gr(g), M = max\{n, m\}$, allora:

$$f + g = \sum_{i=0}^{M} (a_i + b_i)x^i$$

$$f \cdot g = \sum_{i=0}^{n+m} (\sum_{j=0}^{i} a_j b_{i-j})x^i$$

15.21 Proprietà del Grado della Somma di Polinomi

Siano $f, g \in A[x] - \{0\}$. Allora:

$$[gr(f) = gr(g)] \wedge [cd(f) = -cd(g)] \implies gr(f + g) < [gr(f) = gr(g)]$$

$$[gr(f) \neq gr(g)] \vee [cd(f) \neq cd(g)] \implies gr(f + g) = max\{gr(f), gr(g)\}$$

15.22 Proprietà del Grado di Prodotto di Polinomi

Siano $f, g \in A[x] - \{0\}$. Allora:

$$cd(f) \cdot cd(g) = 0 \implies gr(f \cdot g) < gr(f) + gr(g)$$

$$cd(f) \cdot cd(g) \neq 0 \implies gr(f \cdot g) = gr(f) + gr(g) \wedge cd(f \cdot g) =$$

$$= cd(f) \cdot cd(g) \text{ [FORMULA DI ADDIZIONE DEI GRADI]}$$

Se

$$f = 0, gr(f \cdot g) = gr(0) = -\infty = -\infty + gr(g)$$

e

$$cd(f \cdot g) = 0 = cd(f) \cdot cd(g)$$

si osserva che la Formula di Addizione dei Gradi vale anche con il polinomio zero.

15.23 Coefficiente Direttore Cancellabile implica Polinomio Cancellabile

Sia $f \in A[x] - \{0\}$. Se $cd(f)$ è cancellabile, allora anche f lo è. In particolare, per f vale la Formula di Addizione dei Gradi.

$cd(f)$ cancellabile vuol dire che esso non è divisore dello zero. Per la Formula di Addizione dei Gradi segue che:

$$\forall g \in A[x]$$

$$g \neq 0 \implies gr(f \cdot g) = gr(f) + gr(g) \neq -\infty \implies f \cdot g \neq 0 \implies f$$

non è divisore dello zero, cioè f è cancellabile.

15.24 Condizione Sufficiente e Necessaria per Dominio di Integrità dei Polinomi

$A[x]$ è dominio di integrità $\iff$ A è dominio di integrità.

15.25 Condizione di Non Invertibilità di un Polinomio

Sia $f \in A[x]$. Se f è cancellabile e $gr(f) > 0$, allora f non è invertibile.

Proof. Per assurdo, sia f invertibile e sia $g = f^{-1}$. Allora per la Formula di Addizione dei Gradi,

$$gr(f) + gr(g) = gr(fg) = gr(1) = 0 \implies gr(f) = 0$$

che è assurdo. □

15.26 Invertibilità del Polinomio Incognita

Il polinomio x non è mai invertibile

Proof. Dato che $cd(x) = 1$ per definizione, e l'unità dell'anello è sempre cancellabile ("Invertibillità Implica Cancellabilità"). In particolare, $A[x]$ non è mai un campo. □

15.27 Teorema della Divisione Lunga tra Polinomi

Sia $(A, +, \cdot)$ un anello commutativo unitario e siano $f, g \in A[x]$. Se

$$cd(g) \in U(A) \implies (\exists!(q, r) \in A[x] \times A[x])(f = gq + r \wedge gr(r) < gr(g))$$

Proof. Esistenza della Coppia)
Poniamo $m = gr(g), n = gr(f)$. Se $n < m$, la tesi è ovvia: $(q, r) = (0, f)$. Se $n \geq m$ ($m \neq 0$ per ipotesi su $cd(g)$), pongo $a = cd(f), b = cd(g)$ Dimostriamo per Induzione di 2^a Forma su n. Sia

$$k = ab^{-1}x^{n-m}g$$

Tra

$$ab^{-1}x^{n-m} \text{ e } g$$

vale la Formula di Addizione dei Gradi, quindi

$$gr(k) = gr(ab^{-1}x^{n-m}) + gr(g) = n - m + m = n$$

e

$$cd(k) = a$$

e dico

$$h = f - k$$

Dunque $gr(h) < n$. Allora, per induzione

$$\exists(q_1, r_1)\ (f - k = gq_1 + r_1)$$

con $gr(r_1) < gr(g)$. Allora:

$$f = gq_1 + r_1 + k = gq_1 + r_1 + ab^{-1}x^{n-m}g = g(q_1 + ab^{-1}x^{n-m}) + r_1$$

Unicita' della Coppia)
Siano $(q_1, r_1), (q_2, r_2)$ due coppie come da ipotesi. Quindi $g(q_1 - q_2) = r_2 - r_1$. $gr(r_2 - r_1) < gr(g) = m$. Vale la Formula di Addizione dei Gradi e quindi

$$gr(r_2 - r_1) = gr(g \cdot (q_1 - q_2)) = gr(g) + gr(q_1 - q_2) = m + gr(q_1 - q_2) < m$$

Ma questo è possibile solo se $gr(q_1 - q_2) = -\infty$, cioè $q_1 - q_2 = 0$. Allora

$$q_1 = q_2 \wedge r_1 = r_2$$

□

15.28 Condizione per l'Anello dei Polinomi Fattoriale

A anello fattoriale $\implies A[x]$ anello fattoriale.

15.29 Notazione Funzionale di Polinomio

Sia $f \in A[x], f = a_0 + a_1 x + ... + a_n x^n \, c \in A$, con $a_n \neq 0$.
Sia $c \in A$. Allora definisco:

$$f(c) := a_0 + a_1 c + ... + a_n c^n \in A$$

15.30 Omomorfismo di Sostituzione dei Polinomi

Sia $c \in A$, anello commutativo unitario. Allora:

$$f \in A[x] \mapsto f(c) \in A$$

è un omomorfismo di anelli.

15.31 Applicazione Polinomiale

Sia $f \in A[x]$. Definiamo l'applicazione polinomiale di f la funzione:

$$\overline{f} : c \in A \mapsto f(c) \in A$$

15.32 Applicazione Polinomiale Costante

Si osserva che se $f = a_0$, cioè è un polinomio costante, allora

$$\forall c \in A \ (\overline{f}(c) = a_0)$$

e quindi anche l'applicazione polinomiale è costante.

15.33 Radice di un Polinomio

Se $f \in A[x], c \in A, f(c) = 0_a$, allora c si dice radice (o soluzione) del polinomio.

15.34 Applicazioni Polinomiali di Somme e Prodotti

Siano $f, g \in A[x]$. Allora si verifica facilmente che:

$$\overline{f+g}(c) = \overline{f}(c) + \overline{g}(c)$$
$$\overline{f \cdot g}(c) = \overline{f}(c) \cdot \overline{g}(c)$$

Da questo deriva che, se c è radice di f, allora è anche radice di fg e gf

15.35 Teorema del Resto

Sia A un anello commutativo unitario, $f \in A[x], c \in A$. Allora $f(c)$ è il resto della divisione lunga tra f e $(x-c)$.

Proof. $cd(x-c) = 1$, che è invertibile, pertanto la divisione lunga è effettuabile fra i due. Abbiamo dunque che:

$$f = (x-c)q + r \wedge gr(r) < gr(x-c)$$

ma $gr(x-c) = 1 \implies gr(r) = 0$, cioè che r sia un polinomio costante del tipo $r = a_0$. Allora, applicando l'Omomorfismo di Sostituzione:

$$f(c) = (c-c)q(c) + r(c) = 0 \cdot q(c) + a_0 = a_0$$

□

15.36 Teorema di Ruffini

Sia A un anello commutativo unitario, $f \in A[x], c \in A$. Allora:

$$c \text{ radice di f} \iff (x-c)|f$$

Proof. c radice $\implies f(c) = 0_A \implies$ per il Teorema del Resto, il resto della divisione lunga è $0_A \implies (x-c)|f$ □

15.37 Teorema di Ruffini Generalizzato

Sia A un dominio di integrità. Sia $f \in A[x], c_1, ..., c_n \in A$ a due a due distinti. Allora:

$$c_1, ..., c_n \text{ radici di } f \iff \prod_{i=1}^{n}(x - c_i)|f$$

Proof. $\rightarrow$) Dimostriamo per induzione su n, numero delle radici. Se $n = 1$, la tesi è valida per Ruffini. Supponiamo dunque che $n > 1$ e che la tesi sia valida per $n - 1$.
$f(c_n) = 0$ per ipotesi. Allora per Ruffini

$$(x - c_n)|f \implies f = (x - c_n)g$$

Se prendo

$$i : 1 \leq i < n \implies f(c_i) = (c_i - c_n)g(c_i)$$

per l'Omomorfismo di Sostituzione. Dato che ci troviamo in un dominio di integrità, sapendo che

$$f(c_i) = 0$$

e

$$c_i - c_n \neq 0$$

dunque per la Legge di Annullamento del Prodotto

$$g(c_i) = 0$$

Ma, quindi, tutti i

$$c_i : 1 \leq i < n$$

sono radici di g, quindi vale per g la tesi induttiva e

$$g = h \cdot \prod_{i=1}^{n-1}(x - c_i)$$

Allora:

$$f = (x - c_n)g = (x - c_n) \cdot \prod_{i=1}^{n-1}(x - c_i) \cdot h = \prod_{i=1}^{n}(x - c_i) \cdot h$$

Che implica che:

$$\prod_{i=1}^{n}(x - c_i)|f$$

che è la tesi.
$\leftarrow$) Se

$$\prod_{i=1}^{n}(x - c_i)|f \implies (\exists h \in A[x])(f = h \cdot \prod_{i=1}^{n}(x - c))$$

Allora

$$\forall i : 1 \leq i < n :$$

$$f(c_i) = h \cdot [(c_i - c_1) \cdot (c_i - c_2) \cdot ... \cdot (c_i - c_i) \cdot ... \cdot (c_i - c_n)] = 0$$

Che è la tesi. □

15.38 Teorema sul Numero di Radici di Polinomio in un Dominio di Integrità

A dominio di integrita' , $f \in A[x] - \{0\}, c_1, ...c_n$ radici di f allora:
$n \leq gr(f)$
Cioè il numero delle radici è minore o uguale del grado del polinomio.

Proof. Sia

$$g = \prod_{i=1}^{n}(x - c_i)$$

Per ruffini generalizzato,

$$\exists h \in A[x] \ (f = hg)$$

Ma A è dominio di integrità e $g \neq 0$, quindi vale la Formula di Addizione dei Gradi.

$$gr(f) = gr(g) + gr(h) \geq gr(g) = n$$

perché g è il prodotto di n polinomi di grado 1. □

15.39 Controesempio del "Teorema sul Numero di Radici di Polinomio in un Dominio di Integrità"

Il "Teorema sul Numero di Radici di Polinomio in un Dominio di Integrità" ha come ipotesi che A sia dominio di integrità. Forniamo un controesempio nel caso in cui A non è dominio di integrità e mostriamo che il teorema non è valido.
Consideriamo il polinomio:

$$f = [2]_4 x \in \mathbb{Z}_4[x]$$

Dato che $[2] \cdot [2] = [4] = [0] \implies Z_4[x]$ non è dominio di integrità. Il polinomio ha grado uno, ma almeno due radici, infatti:

$$f([0]_4) = [2]_4 \cdot [0]_4 = [0]_4$$
$$f([2]_4) = [2]_4 \cdot [2]_4 = [4]_4 = [0]_4$$

Pertanto il teorema non vale quando l'anello dei polinomi non è dominio di integrità.

15.40 Principio di Identità dei Polinomi

Sia A un dominio di integrità infinito. Allora:

$$\forall f, g \in A[x] \ (f = g \iff \overline{f} = \overline{g})$$

Proof. $\rightarrow$) Se $f = g$, allora ovviamente $\overline{f} = \overline{g}$. $\leftarrow$) Definisco $h = f - g$, e dato che $\overline{f} = \overline{g}$, si ha allora che

$$\forall c \in A \ (h(c) = \overline{h}(c) = \overline{f - g}(c) = \overline{f}(c) - \overline{g}(c) = 0)$$

Poiché A è infinito, h ha infinite radici distinte, e per il Teorema sul Numero di Radici, allora $h = 0$ perché altrimenti avrebbe grado maggiore dell'infinito, il che è assurdo. Infine: $h = 0 \implies f = g$ □

15.41 Controesempio del "Principio di Identità dei Polinomi"

Proof. Consideriamo il polinomio

$$f \in x^3 - x \in \mathbb{Z}_3[x]$$

Che appartiene ad un anello finito. Allora abbiamo che:

$$\overline{f}([0]_3) = [0]_3^3 - [0]_3 = [0]_3$$
$$\overline{f}([1]_3) = [1]_3^3 - [1]_3 = [0]_3$$
$$\overline{f}([2]_3) = [2]_3^3 - [2]_3 = [8]_3 - [2]_3 = [2]_3 - [2]_3 = [0]_3$$

Quindi $\overline{f} = \overline{0}$, ma $f \neq 0$. □

15.42 Rappresentante Monico di un Polinomio

Sia A un campo e $f \in A[x] - \{0\}$. Allora

$$ASSOC(f) = \{uf \mid u \in A - \{0\}\}$$

poiché in un campo tutti gli elementi sono invertibili, eccetto lo zero. Allora, per ogni f non nullo in $A[x]$ campo, esiste ed è unico un polinomio monico associato ad f, e tale polinomio si dice rappresentante monico della classe di f.

15.43 Fattorizzazione di Polinomi in un Campo

Sia A un campo e sia $f \in A[x]$. Allora esiste $c \in A$ e $g_1, ..., g_n \in A[x]$ tali che

$$f = c \cdot g_1 \cdot ... \cdot g_n$$

$$g_1, ..., g_n$$

sono monici ed irriducibili e la decomposizione è unica a meno dell'ordine dei fattori.

Proof. A è fattoriale perché è un campo, allora $A[x]$ è fattoriale. Quindi l'unicità della decomposizione deriva dell'unicità della decomposizione negli anelli fattoriali, più l'unicità del polinomio monico associato. Rimane da dimostrare l'esistenza della decomposizione per Induzione di 1^a Forma su $gr(f)$.
Se $gr(f) = 0$, allora f è costante e vale la tesi. Suppongo $gr(f) > 1$ e ipotizzo la tesi sia valida per $gr(f) - 1$. $A[x]$ è fattoriale, allora prendo una decomposizione irriducibile di f, ovvero $f = h_1 \cdot ... \cdot h_n$ polinomi irriducibili e pongo:

$$g_i = cd(h_i)^{-1} \cdot h_i$$

$$c = \prod_{i=1}^{n} cd(h_i)$$

Cioè mettiamo in evidenza i coefficienti direttore rendendo i g_i monici e si ha che $f = c \cdot g_1 \cdot ... \cdot g_n$ che è la tesi. □

15.44 Criterio di Irriducibilità di Polinomi su un Campo

Sia A un campo, e sia $f \in A[x] - \{0\}$ e poniamo $n = gr(f)$.
Allora, f è irriducibile se e soltanto se (equivalentemente):

1. $(\forall g, h \in A[x])(f = gh \implies gr(g) = n \oplus g(h) = n)$
2. $(\forall g, h \in A[x])(f = gh \implies gr(g) = 0 \oplus g(h) = 0)$

Proof. $\leftarrow$) Gli invertibili di $A[x]$ sono gli invertibili di A, cioè i polinomi costanti. Se

$$n = gr(f) > 0$$

allora non è costante e quindi

$$f \notin U(A[x])$$

Se

$$f = gh$$

per la (1) posso supporre che

$$gr(g) = n$$

e per la Formula di Addizione dei Gradi

$$gr(h) = 0 \implies h \in U(A[x]) \implies f$$

ha solo divisori banali.
$\rightarrow$) f è irriducibile, quindi

$$f \notin U(A[x]) = U(A)$$

e

$$DIV(f) = BDIV(f)$$

A è campo, allora

$$U(A) = A - \{0\}$$

quindi

$$gr(f) > 0$$

f ha solo divisori banali ed, essendo ogni valore di A invertibile, allora ogni valore è anche cancellabile, e quindi f ha coefficiente direttore cancellabile ed è cancellabile a sua volta, e quindi

$$BDIV = \{uf \mid u \in A - \{0\}\} \cup (A - \{0\})$$

Allora

$$f = gh$$

necessariamente

$$gr(g) = 0 \vee gr(h) = 0$$

perché uno dei due è invertibile (e dunque costante) e per la Formula di Addizione dei gradi l'altro deve avere grado n, da cui la tesi. $\square$

15.45 Criterio di Esistenza di Radici di un Polinomio in un Campo

Sia A un campo e $f \in A[x]$. Allora f ha radici in $A \iff$ ha almeno un divisore di primo grado in $A[x]$.

$\rightarrow$) Per Ruffini. $\leftarrow$) Tutti i polinomi di grado 1 hanno radici in un campo.

$$kx + h \implies c = -hk^{-1}$$

è radice.

Quindi, se

$$f = g(kx + h) \implies -hk^{-1}$$

è radice di f.

15.46 Condizione di Irriducibillità di un Polinomio in un Dominio

Sia A un dominio di integrità e sia $f \in A[x]$. Se $gr(f) > 1$ e f ha radici, allora f non è irriducibile.

Proof. Segue da Ruffini e dalla Formula di Addizione dei Gradi. □

15.47 Criterio di Irriducibilità per Polinomi di Grado 2/3 su un Campo

Un polinomio di grado 2 o 3 su un campo A è irriducibile se e soltanto se non ha radici in A.

$$\text{irrducibile} \iff \text{no radici}$$

Proof. Segue da Ruffini e dalla Formula di Addizione dei Gradi. □

15.48 Condizione di Esistenza delle Radici per un Polinomio di Grado Maggiore di 3 su un Campo

Se un polinomio di grado > 3 su un campo A è irriducibile, allora non ha radici in A.

$$\text{irrducibile} \implies \text{no radici}$$

Proof. Segue da Ruffini e dalla Formula di Addizione dei Gradi. □

15.49 Teorema Fondamentale dell'Algebra

Ogni polinomio non costante di $\mathbb{C}[x]$ ha radici. Corollario: in $\mathbb{C}$ gli unici irriducibili sono polinomi di grado 1.

15.50 Criterio di Irriducibilità in $\mathbb{R}[x]$

Ogni polinomio irriducibile di $\mathbb{R}[x]$ ha grado minore di 3.

15.51 Corollario del Criterio di Irriducibilità in $\mathbb{R}$

I polinomi irriducibili in $\mathbb{R}[x]$ sono esattamente quelli di di grado 1 o quelli di grado 2 senza radici.

15.52 Teorema di Bolzano

Ogni polinomio su $\mathbb{R}[x]$ di grado dispari ha una radice in $\mathbb{R}$.

15.53 Regola del Discriminante

I polinomi di grado due su $\mathbb{R}$ hanno radici se e solo se il discriminante $\Delta \geq 0$

$$ax^2 + bx + c$$

$$\Delta = b^2 - 4ac$$

Se $\Delta \geq 0$ allora le radici sono

$$x_{1,2} = \frac{-b \pm \sqrt{\Delta}}{2a}$$

15.54 Ogni Polinomio in $\mathbb{Q}[x]$ ha un Polinomio associato in $\mathbb{Z}[x]$

Esempio: Moltiplicando e dividendo per l'MCM otteniamo che:

$$3x^4 + \frac{1}{90}x + \frac{3}{4} = \frac{1}{180}(540x^4 + 2x + 135)$$

$$540x^4 + 2x + 135 \in \mathbb{Z}[x]$$

15.55 Criterio di Irriducibilità di Eisenstein

Sia

$$f = a_0 + a_1x + ... + a_nx^n \in \mathbb{Z}[x]$$

con $a_n \neq 0$. Allora, se esiste un numero primo p tale che

$$p|a_0, p|a_1, ...p|a_{n-1}$$

ma

$$p \nmid a_n$$

e

$$p^2 \nmid a_0$$

allora f è irriducibile in $\mathbb{Q}[x]$.

15.56 Conseguenze di Eisenstein

Per Eisenstein, polinomi del tipo $x^n \pm p$ sono tutti irriducibili in $\mathbb{Q}[x]$. Dunque, in $\mathbb{Q}[x]$ ci sono polinomi irriducibili di ogni grado, a differenza di $\mathbb{R}[x]$, dove esistono polinomi irriducibili solo di grado minore di 3.

15.57 Radici Razionali di un Polinomio in $\mathbb{Z}[x]$

Sia $f \in \mathbb{Z}[x]$, con $cd(f) = a_n$ e $f(0) = a_0$. Sia $c \in \mathbb{Q}$ e $f(c) = 0$, cioè sia c una radice razionale del polinomio.
Allora $c = \frac{u}{v}$ dove $v|a_n$ e $u|a_0$. Inoltre a_n e a_0 sono coprimi.

15.58 Corollario del Teorema su Radici Razionali di un Polinomio in $\mathbb{Z}[x]$

Se $f \in \mathbb{Z}[x]$ è un polinomio monico, allora tutte le sue radici razionali sono in realtà intere.

Proof. Sia $c \in \mathbb{Q}$ radice razionale di f. Allora per il Teorema sulle Radici Razionali $c = \frac{u}{v}$ dove $u|a_0$ e $v|a_n$. Ma dato che per ipotesi f è monico, allora $a_n = 1$ e $v|1$, quindi $v = \pm 1$. Allora, la radice $c = \pm u \in \mathbb{Z}$ che è la tesi. □

16 Grafi

16.1 Grafo Semplice

Sia $v \neq 0$ e sia ρ una relazione binaria simmetrica e antiriflessiva su v. Allora la coppia (v, ρ) si dice grafo semplice.

16.2 Vertici di un Grafo

Sia (v, ρ) un grafo semplice. Allora gli elementi di v si dicono vertici del grafo.

16.3 Archi (o Lati) di un Grafo

Sia (v, ρ) un grafo semplice. Allora le coppie $\{x, y\} \in P_2(v) : x\rho y$ si dicono archi o lati del grafo.

16.4 Grafo Semplice (via Insieme dei Lati)

Sia (v, ρ) un grafo semplice. Allora esso sarà notabile equivalentemente come (v, l), dove l'insieme l è definito come:

$$l := \{\{x, y\} \in P_2(v) \mid x\rho y\}$$

16.5 Multigrafo

Una terna di insiemi non vuoti (v, l, σ) si dice multigrafo se la funzione sigma è una funzione del tipo

$$\sigma : l \mapsto P_2(v)$$

16.6 Estremi di un Arco

Sia (v, l) un vertice. Sia $a \in l$. Allora, i due vertici $x, y \in v : \{x, y\} = a$ si dicono estremi dell'arco a.

16.7 Vertici Adiacenti

Sia (v, l) un grafo, e siano $x, y \in v$. I due vertici si dicono adiacenti se

$$\exists a \in l \ (\{x, y\} = a)$$

cioè se esiste un arco di cui essi sono vertici, o equivalentemente, se esiste un arco che li connette.

16.8 Archi Incidenti

Sia (v, l) un grafo, e siano $l_1, l_2 \in l$. Allora i due lati si dicono incidenti se $l_1 \cap l_2 \neq \emptyset$, cioè se hanno vertici in comune.

16.9 Grado di un Vertice

Sia (v, l) un grafo e sia $x \in v$. Allora definiamo:

$$d(x) = |\{y \in l \mid x \in y\}|$$

Cioè il numero di archi che contengono x come vertice.

16.10 Vertici Pari o Dispari

Se il grado di un vertice è non-nullo e pari, il vertice si dice pari.
Se il grado di un vertice è dispari, il vertice si dice dispari.

16.11 Vertice Isolato

Se il grado di un vertice è zero, il vertice si dice isolato.

16.12 Grafo Completo

Un grafo (v, l) si dice completo se tutti i suoi vertici sono a due a due adiacenti, e cioè se:

$$l = P_2(v)$$

16.13 Grafo Complementare

Dato un grafo (v, l), definiamo il suo complementare il grafo

$$(v, P_2(v) - l)$$

16.14 Sottografo

Sia (v, l) un grafo, e siano $v' \subseteq v \wedge l' \subseteq l$. Allora il grafo (v', l') si dice sottografo di (v, l)

16.15 (Multi)Grafo Finito

Se l'insieme v dei vertici è finito, il (multi)grafo si dice finito. Si nota che un multigrafo è finito anche se ha un numero infiniti di lati. L'elemento importante è la finitezza dei vertici.

16.16 Isomorfismo tra Grafi

Siano (v, l) e (v', l') due grafi, e sia $f : v \to v'$ una funzione biettiva. Allora f si dice isomorfismo tra grafi se e solo se:

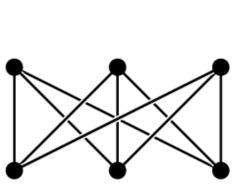
$$\forall x, y \in v \ (\{x, y\} \in l \iff \{f(x), f(y)\} \in l')$$

16.17 Grafo Planare

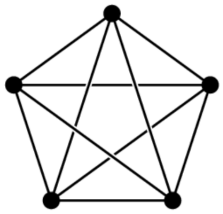
Un grafo si dice planare se è rappresentabile su un piano senza archi che si intersecano.

16.18 Teorema di Kuratowski

Un grafo finito è planare se e soltanto se non ha sottografi isomorfi a K_5 e $K_{3,3}$



$K_{3,3}$



K_5

16.19 Teorema su Lati e Gradi

Sia (v, l) un grafo finito. Allora

$$2|l| = \sum_{x \in v} d(x)$$

Proof. Sia t il numero di estremi dei lati del grafo. Allora $t = 2|l|$, in quanto ogni lato ha due estremi. Allo stesso tempo, ogni vertice x è estremo di $d(x)$ lati. Dunque $\sum_{x \in v} d(x) = t$.
Dunque

$$2|l| = \sum_{x \in v} d(x)$$

□

16.20 Cammino fra due Vertici

Sia (v, l) un grafo e siano $v_1, ..., v_n$ vertici del grafo tali che

$$\forall i \in \mathbb{N} \left((1 \leq i < n) \implies (\{v_i, v_{i+1}\} \in l) \right)$$

Se l'insieme $\{\{v_1, v_2\}, ..., \{v_{n-1}, v_n\}\}$ ha ordine n (cioè non ci sono archi che si ripetono), allora la ennupla ordinata $(\{v_1, v_2\}, ..., \{v_{n-1}, v_n\})$ si dice cammino fra v_1 e v_n di lunghezza n.

16.21 Cammino Nullo

Dato un grafo (v, l), per ogni $x \in v$ definiamo il cammino nullo c_x da x ad x, di lunghezza 0.

16.22 Componente Connessa

La relazione definita su un grafo (v, l) nel seguente modo:

$$\gamma = (v \times v, g), g \subseteq v \times v : (v_1, v_2) \in g \iff \exists \text{ cammino fra } v_1, v_2$$

E' una relazione di equivalenza e diciamo le sue classi di equivalenza le componenti connesse del grafo.

16.23 Grafo Connesso

Un grafo si dice connesso se esso ha una sola componente connessa, con cui esso coincide.

16.24 Cammino (di un Multigrafo)

Sia (v, l, σ) un multigrafo, e siano $v_1, ..., v_{n+1} \in v$ suoi vertici e siano $l_1, ..., l_n$ archi a due a due distinti tali che:

$$\sigma(l_i) = \{v_i, v_{i+1}\}, \forall i \in \mathbb{N} : 1 \leq i \leq n$$

Allora le ennupla ordinata $(l_1, ..., l_n)$ si dice cammino.

16.25 Cammino Euleriano

Un cammino $(l_1, ..., l_n)$ di un multigrafo (v, l, σ) si dice euleriano se $l = \{l_1, ..., l_n\}$, cioè se il cammino "passa" per tutti i lati del grafo.

16.26 Circuito Euleriano

Un cammino euleriano fra due vertici v_1, v_{n+1} si dice circuito euleriano se $v_1 = v_{n+1}$

16.27 Teorema di Eulero

Sia g un multigrafo finito privo di vertici isolati. Allora g ha un circuito euleriano se e solo se tutti i suoi vertici sono pari.

16.28 Foresta

Un grafo si dice foresta se non ha circuiti.

16.29 Albero

Una foresta connessa si dice albero.

16.30 Teorema di Caratterizzazione delle Foreste

Un grafo finito $g = (v, l)$ si dice foresta $\iff$ per ogni coppia $(x, y) \in v \times v : x \neq y$ esiste al più un singolo cammino da x ad y.

Proof. $\rightarrow$) Siano $(\{u_1, u_2\}, ..., \{u_{m-1}, u_m\})$ e $(\{v_1, v_2\}, ..., \{v_{n-1}, v_n\})$ due cammini distinti fra x ed y, cioè

$$u_1 = v_1 = x$$

$$u_n = v_n = y$$

Sia

$$i = \{h \in \mathbb{N} \mid \exists k \in \mathbb{N}\ (u_h = v_k \wedge \{u_h, u_{h+1}\} \neq \{v_k, v_{k+1}\})\}$$

Sia $r = min(i)$ e sia k_r il relativo k. Definiamo dunque:

$$j = \{h \in \mathbb{N}_r \mid (\exists k \in \mathbb{N})(u_{h+1} \neq v_{k+1})\}$$

$j \neq \emptyset$ e poniamo $s = min(j)$, con k_s il suo relativo k. Certamente, $k_r \neq k_s$, e possiamo quindi supporre senza ledere la generalità che $k_r < k_s$. Allora il circuito è il seguente:

$$(\{u_r, u_{r+1}\}, \{u_{r+1}, u_{r+2}\}, ..., \{u_s, u_{s+1}\}, \{v_{k_s+1}, v_{k_s}\}, ...$$

$$..., \{v_{k_r+2}, v_{k_r+1}\}, \{v_{k_r+1}, v_{k_r}\})$$

$\leftarrow$) Per assurdo, esista un circuito $(\{v_1, v_2\}, ..., \{v_{n-1}, v_n\})$ dove $v_1 = v_n$. Allora, sicuramente, $n > 1$, e quindi $(\{v_1, v_2\})$ e $(\{v_2, v_3\}, ..., \{v_{n-1}, v_n\}, \{v_1, v_2\})$ sono due cammini distinti da v_1 e v_2, che è assurdo in quanto va contro l'ipotesi che esista al più un singolo cammino fra ogni coppia di punti. □

16.31 Corollario di Caratterizzazione degli Alberi

Corollario del "Teorema di Caratterizzazione delle Foreste"
Un grafo finito g è un albero $\iff$ per ogni coppia (x, y) di vertici distinti di g esiste ed è unico il cammino da x a y.

16.32 Planarità delle Foreste

Corollario del "Teorema di Caratterizzazione delle Foreste"
Ogni foresta finita è un grafo planare.

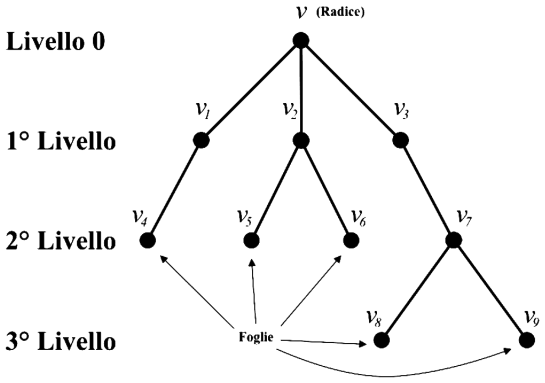
Proof. Segue dal Teorema di Kuratowski. □

16.33 Foglia di un Albero

Un vertice di primo grado di un albero si dice foglia.

16.34 Rappresentazione Radicale di un Albero

Si sceglie un vertice dell'albero, detto radice, e si rappresenta poi il grafico in maniera gerarchica a partire dalla radice.



16.35 Un Albero Finito ha almeno Una Foglia

Ogni albero finito g con almeno due vertici ha una foglia.

Proof. Assumiamo per assurdo che non esistano foglie. Consideriamo l'insieme dei vertici di g, $v = \{v_1, ..., v_n\}$ con $|v| = n$. Sia $l = \{v_1, v_2\}$, ma $d(v_2) \geq 2$ per ipotesi, e quindi troviamo un $v_3 : v_3 \notin \{v_1, v_2\}$ e sia $l_2 = \{v_2, v_3\}$. Ancora una volta, $d(v_3) \geq 2$ per ipotesi, quindi deve esistere un v_4 e così via. Troviamo quindi una successione $l_1, ..., l_n$ di lati distinti fra $n+1$ vertici distinti, ma per ipotesi $|v| = n$, e quindi assurdo. □

16.36 Numero di Lati di un Albero

Un albero $g = (v, l)$ di n vertici ha $n - 1$ lati.

Proof. Per Induzione di Prima Forma. Nel caso base, $n = 1$, la tesi è ovvia. Poniamo quindi $n > 1$ e ipotizziamo la tesi valida per $n - 1$. Allora, per il "Un Albero Finito ha Almeno una Foglia", deve esistere una foglia x. Consideriamo il sottografo s di vertici $v - x$, che ha un vertice ed un lato in meno, in quanto per definizione una foglia ha un solo lato. Quindi s ha $n - 1$ vertici e $|l| - 1$ lati. Vale per esso l'ipotesi induttiva e quindi:

$$|l| - 1 = (n - 1) - 1 = n - 2$$

Da cui segue:

$$|l| = n - 1$$

Che è la tesi. □

16.37 Un Albero Finito ha Almeno Due Foglie

Abbiamo già dimostrato che un albero finito ad almeno due vertici ha almeno UNA foglia. Adesso affermiamo che: Un albero finito con almeno due vertici ha almeno due foglie.

Proof. Sia $g = (v, l)$ un albero finito e sia $|v| = n$. Allora, per il Teorema sul Numero di Lati di un Albero, $|l| = n - 1$ e per il Teorema su Lati e Gradi,

$$2|l| = \sum_{x \in v} d(x) \implies 2(n - 1) = \sum_{x \in v} d(x)$$

Ipotizziamo per assurdo che esistano < 2 foglie. Allora, abbiamo almeno $n - 1$ vertici che non sono foglie, cioè hanno grado maggiore di uno. Pertanto si deve avere che:

$$2(n - 1) = \sum_{x \in v} d(x) \geq 2(n - 1) + 1$$

Il che è assurdo. □

16.38 Caratterizzazione di Foreste di Multigrafi

Se $g = (v, l, \sigma)$ è un multigrafo finito con esattamente k componenti connesse, allora $|l| \geq |v| - k$ e vale che $|l| = |v| - k$ se e solo se g è una foresta.

16.39 Corollario del Teorema di Caratterizzazione di Foreste di Multigrafi

Dato $g = (v, l, \sigma)$ multigrafo, equivalgono i seguenti:

1. g è un albero
2. g è un grafo connesso e $|v| = |l| + 1$
3. g è una foresta e $|v| = |l| + 1$