Appunti di Algebra

Delle Lezioni del Prof. Brescia

2021/2022

Indice

Definizioni e Teoremi

1 Introduzione

Questi appunti di Algebra sono basate sulle lezioni del Prof. Brescia per il corso di Algebra dell'anno accademico 2021/2022. Il materiale è per lo più una trasposizione diretta di ciò che è stato scritto o detto dal Prof. Brescia, ma occasionalmente ho preso la libertà di semplificare o riformulare definizioni e teoremi. Inoltre, molti teoremi sono stati lasciati dal professore come dimostrazione, in tali situazioni ho riportato le mie soluzioni.

Questo documento sarà indubbiamente ricco di errori e sviste. Per qualsiasi segnalazione, potete inviare un'email a ra.tontaro@gmail.com, anche se uso questo account molto raramente.

2 Logica Proposizionale

2.1 Alfabeto e Sintassi

Così come usiamo il linguaggio dell'Italiano per parlare di cose comuni, utilizzeremo un linguaggio matematico per scrivere formule. Questo è il linguaggio della *logica proposizionale*.

Anche questo linguaggio è dotato di un alfabeto, che descriviamo come una terna ordinata (P, C, B) di insiemi di simboli. Tali insiemi sono:

- P è l'insieme delle variabili proposizionali, $\{a_1, a_2, a_3 \ldots\}$
- C è l'insieme dei connettivi logici, $\{\neg, \wedge, \vee, \rightarrow, \leftrightarrow\}$
- B è l'insieme delle parentesi, $\{(,)\}$

Useremo questo alfabeto per scrivere formule secondo una certa *sintassi*. La sintassi definisce quali formule sono *ben formate*, cioè valide e correttamente scritte.

La sintassi della logica proposizionale è di sole tre regole:

- Una variabile proposizionale a_n da sola costituisce una formula ben formata.
- se A e B sono due formule ben formate, allora $(\neg A), (A \wedge B), (A \vee B), (A \rightarrow B), (A \leftrightarrow B)$ sono formule ben formate.
- Le sole formule ben formate sono quelle ottenute attraverso le precedenti due regole.

In sostanza, questo vuol dire che possiamo creare formule ben formate usando connettivi logici per legare fra di loro diverse variabili proposizionali. Possiamo usare qualsiasi simboli vogliamo per le variabili proposizionali, ma in genere ci limitiamo a semplici lettere come $x, y, z, w, p, q, a, b, c, \ldots$

Le parentesi sono usate per indicare l'ordine delle operazioni, come nella notazione matematica a cui si è già abituati.

2.2 Valori di Verità

È importante notare che una formula ben formata non è necessariamente vera, così come la frase "Tutte le rose sono blu" è sintatticamente corretta ma ovviamente falsa.

Come decidiamo se una formula proposizionale è vera o falsa? Definiamo una *funzione di verità* che associa ad ogni formula proposizionale un *valore di verità*, cioè vero o falso. Per esempio:

$$f(x) = V \text{ (x è vera)} \tag{1}$$
$$f(y) = F \text{ (y è falsa)} \tag{2}$$

I connettivi logici ci permettono di "combinare" i valori di verità di formule differenti, pertanto in realtà è necessario solamente conoscere i valori di verità delle variabili proposizionali per "calcolare" il valore di verità dell'intera formula.

2.3 Connettivi Logici

I connettivi logici connettono insieme più formule creando una nuova formula (*proposizione composta*) il cui valore di verità dipende dal valore di verità delle formule di cui è formata. Immaginiamo di avere una funzione di verità f e due formule p e q, che potrebbero essere false o vere, e vediamo che valore assume la formula risultante in base al connettivo logico che usiamo:

2.3.1 Negazione Logica

Detta anche "non" o "not".

$f(\neg p) = V$ se e soltanto se $f(p) = F$.

Cioè, "non p" è vera soltanto se p è falsa. Questo è l'unico connettivo *unario*, cioè che si applica ad una singola formula invece di connetterne due separate.

2.3.2 Congiunzione Logica $\wedge$

Detta anche "e" o "and".

$f(p \wedge q) = V$ se e soltanto se $f(p) = V$ e $f(q) = V$.

Cioè, "p e q" è vera soltanto se p è vera e q è vera.

2.3.3 Disgiunzione Logica Inclusiva $\vee$

Detta anche "o", "vel", "or".

$f(p \vee q) = V$ se e soltanto se $f(p) = V$ o $f(q) = V$.

Cioè, se p o q o entrambi sono vere, allora "p o q" è vera.

2.3.4 Disgiunzione Logica Esclusiva $\veebar, \oplus$

Detta anche "xor" o "aut".

$f(p \oplus q) = V$ se e soltanto se p e q sono differenti.

Cioè, "p o q" è vera soltanto se solo una fra p e q è vera.

2.3.5 Implicazione Materiale

Detta anche "implica", "if-then".

$f(p \rightarrow q) = V$ se e soltanto se $f(p) = F$ o $f(q) = V$.

Cioè, "p implica q" è vera se p è falsa o q è vera. Pertanto, è falsa soltanto nel caso in cui p è vera e q è falsa.

Attenzione! Nel linguaggio comune, l'implicazione tende ad avere valore di implicazione causale, "p causa q". Ciò non è vero nel linguaggio logico. Stiamo solamente affermando che non si può mai avere che p è vera ma q è falsa.

Prendiamo per esempio "è notte $\rightarrow$ non vedo il sole". Se "è notte" è vera e "non vedo il sole" l"implicazione è $V \rightarrow V$ ed è quindi vera, e non c'è nulla di strano.

Se però in realtà è giorno, ma comunque non vedo il sole (magari perché è nuvoloso), l'implicazione è $F \rightarrow V$ ed è *ancora* vera, perché dalla definizione di sopra sappiamo che un'implicazione è soltanto falsa nel caso $V \rightarrow F$, nonostante non ci sia connessione fra l'ora e la mia incapacità di vedere il sole.

2.3.6 Equivalenza Materiale

Detta anche "se e solo se", "doppia implicazione".

$f(p \leftrightarrow q) = V$ se e soltanto se p e q sono entrambe false o entrambe vere (cioè sono equivalenti).

2.4 Ordine Dei Connettivi

La negazione, essendo un connettivo unario, ha sempre massima precedenza. Il resto dei connettivi, in ordine decrescente di precedenza, è come segue:

$\wedge > \vee > \leftrightarrow > \rightarrow$

2.5 Tavole di Verità

Abbiamo visto che una qualsiasi formula, per esempio $p \wedge q$, può assumere valori di verità differenti in base a quali siano i valori di verità di p e q. Ovviamente, esiste un numero finito di possibili combinazioni: o p e q sono entrambi false, o p è vera e q e falsa, o p è falsa e q è vera, o sono entrambi vere.

Dato che il numero di combinazioni possibili è finito, può spesso essere utile scrivere tutte le possibili combinazioni sotto forma di tabella, o tavola di verità.

2.6 Tautologie

Se una formula è sempre vera, indipendentemente dal valore delle sue parti, allora diciamo che essa è una *tautologia*. Allo stesso modo, se una formula è sempre falsa, allora diciamo che essa è una *contraddizione*.

Esaminiamo ora una lista di tautologie fondamentali.

2.6.1 Terzo Escluso

$p \vee \neg p$

Una formula o è vera, o è falsa.

2.6.2 Principio di Non Contraddizione

$\neg(p \wedge \neg p)$

Una formula ed il suo negato non possono essere entrambe vere.

2.6.3 Doppia Implicazione

$(p \to q \land q \to p) \leftrightarrow (p \leftrightarrow q)$
Se p implica q e viceversa, allora i due sono equivalenti.

2.6.4 Contrapposizione

$(p \to q) \leftrightarrow (\neg q \to \neg p)$
p implica q se e soltanto se non-q implica non-p.

2.6.5 Negazione di $\to$

$\neg(p \to q) \leftrightarrow (p \land \neg q)$
p non implica q se e soltanto se p è vera e non-q è falsa.

2.6.6 Involuzione

$\neg(\neg p) \leftrightarrow p$
p equivale al negato del proprio negato.

2.6.7 $\to$ espresso tramite $\land$

$(p \to q) \leftrightarrow (\neg(p \to q)) \leftrightarrow \neg(p \land \neg q)$
Segue da "Negazione di $\to$".

2.6.8 Esplicitazione dello Xor

$$p \oplus q \iff (p \land \neg q) \lor (q \land \neg p) \iff (p \lor q) \land \neg(p \land q)$$

2.6.9 Leggi di De Morgan

$$\neg(p \land q) \leftrightarrow \neg p \lor \neg q$$
$$\neg(p \lor q) \leftrightarrow \neg p \land \neg q$$

2.7 Superfluità dei Connettivi

Le Leggi di De Morgan ci permettono di usare $\lor$ per esprimere formule che usano $\land$ e viceversa. Abbiamo dunque che questi due connettivi sono *semanticamente superflui* l'uno rispetto all'altro.

Definiamo i connettivi NAND e NOR, rispettivamente come $\land$ negato e $\lor$ negato. Si verifica tramite tavola di verità che:

p NAND $p \leftrightarrow \neg p$ e p NOR $p \leftrightarrow \neg p$

Pertanto la negazione è semanticamente superflua rispetto al NAND e NOR. Chiaramente, dato che il NAND è un and negato, e il NOR è un or negato, si ha che:

$p \lor q \leftrightarrow \neg(p \text{ NOR } q)$
$p \land q \leftrightarrow \neg(p \text{ NAND } q)$

Arriviamo dunque alla conclusione che sia NOR che NAND possono essere usati per esprimere la negazione, and, e or. Di conseguenza, essi esprimono anche l'implicazione materiale e l'equivalenza materiale. Pertanto, ogni connettivo logico è semanticamente superfluo rispetto al NOR e al NAND.

2.8 Proprietà dei Connettivi

Tramite tavole di verità si dimostra che:

$\wedge, \vee, \leftrightarrow$ sono associativi, commutativi, e transitivi.

$\rightarrow$ è solamente transitivo.

$\wedge$ è distributivo su $\wedge$ e $\vee$.

$\vee$ è distributivo su $\wedge$ e $\vee$ e $\leftrightarrow$.

$\rightarrow$ è distributivo su $\wedge$, $\rightarrow$, e $\leftrightarrow$.

3 Logica del Primo Ordine

La logica proposizionale è limitata. Tratta di proposizioni a cui associamo valori di verità arbitrari, e non può agire su insiemi infiniti. Definiamo dunque un nuovo linguaggio, la *logical del primo ordine*, che ci permette di effettuare operazioni più complesse.

Una logica del primo ordine forma quindi proposizioni su oggetti di un insieme, definendo funzioni e predicati.

3.1 Alfabeto

L'alfabeto della logica del primo ordine è più complesso, e lo descriviamo come l'ennupla ordinata $(V, CON, P, F, B, CONN, Q)$, dove:

- $V = \{x_1, x_2, x_3 \ldots\}$ è l'insieme delle variabili individuali.
- $CON = \{c_1, c_2, c_3 \ldots\}$ è l'insieme delle costanti individuali.
- $P = \{p_1^{i_1}, p_2^{i_2}, p_3^{i_3}, \ldots\}$ è l'insieme delle *lettere predicativa*, ognuna con una propria *n-arietà.*
- $F = \{f_1^{j_1}, f_2^{j_2}, f_3^{j_3}, \ldots\}$ è l'insieme delle *lettere funzionali*, ognuna con una proprià n-arietà.
- $B = \{"(", ")", ","\}$ è l'insieme dei simboli accessori, cioè delle parentesi e della virgola.
- CONN è l'insieme dei connettivi logici già incontrati.
- $Q = \{\forall\}$ è l'insieme dei quantificatori.

3.1.1 Funzioni

Una funzione non fa altro che associare uno o più oggetti ad un altro oggetto. Per esempio, immaginiamo di star considerando l'insieme "Abitanti di Napoli" e di avere due costanti, "Giovanni" e "Mario". Mario è il padre di Giovanni. Una funzione potrebbe dunque essere la funzione Padre(), che ritorna il papà del suo unico argomento: Padre(Giovanni) = Mario.

3.1.2 Predicati

Mentre una funzione associa ad uno o più oggetti un altro oggetto, un predicato associa ad uno o più oggetti un valore di verità. Immaginiamo quindi di avere un predicato CapelliCastani. Giovanni è castano, ma Mario è biondo, abbiamo dunque:

CapelliCastani(Giovanni) = V
CapelliCastani(Mario) = F

3.1.3 N-Arietà

L'N-Arietà di una funzione o predicato non è nient'altro che il numero di argomenti che essa richiede. Sia Padre() che CapelliCastani() hanno N-arietà uguale ad uno.

3.2 Termini

Abbiamo fin'ora parlato intuitivamente di "oggetti" di un insieme, su cui funzioni e predicati sono definiti. Il termine tecnico è invece *termine*, e definiamo ora le regole di cosa costituisce un termine:

1. Ogni costante individuale è un termine.
2. Ogni variabile individuale è un termine.
3. se f è una funzione n-aria, e $t_1, t_2, \ldots, t_n$ sono termini, allora $f(t_1, t_2, \ldots, t_n)$ è un termine.
4. Un espressione è un termine solo se rispetta (1), (2), o (3).

Dunque, come avevamo dunque già anticipato intuitivamente, costanti, variabili, e il risultato di funzioni sono gli unici termini, o oggetti, di una logica di primo ordine.

3.3 Sintassi

Così come per la logica proposizionale, esiste un insieme di regole sintattiche che definiscono un insieme di *formule ben formate*, cioè formule valide e scritte correttamente a cui possiamo assegnare un valore di verità vero o falso. Le regole sintattiche di una logica di primo ordine sono le seguenti:

1. Se p è una lettera predicativa n-aria e $t_1, t_2, ..., t_n$ sono termini, allora $p(t_1, t_2, ..., t_n)$ è una formula ben formata.
2. se t_1, t_2 sono due termini, allora $t_1 = t_2$ è un termine.
3. se p e q sono formule ben formate, e x è una variabile individuale, allora $(\neg p), (p \wedge q), (p \vee q), (p \rightarrow q), (p \leftrightarrow q), (\forall x)(p)$ sono formule ben formate.
4. Solamente le formule ottenute tramite le regole (1), (2), (3) sono formule ben formate.

3.4 Quantificatori

3.4.1 Il Quantificatore Universale

Data una formula p ed una variabile individuale x, se $p(x)$ è vera diciamo che x *verifica* p. Per esempio, se p è "(CapelliCastani(Padre(x)) = V" allora "Giovanni" non verifica p in quanto il padre di Giovanni, Mario, è biondo.

E' semplice scrivere formule per termini specifici, ma come facciamo se stiamo cercando di fare affermazioni più generali? Per esempio, "Tutti i fenicotteri sono rosa"?

Introduciamo dunque il *quantificatore universale*, $\forall$. Data una variabile individuale x ed una formula p, allora:

$(\forall x)(p(x))$

Equivale a dire: "per ogni termine x, x verifica p". Se dunque p equivale a "ColoreRosa(x) = V" e l'insieme che stiamo considerando è quello dei fenicotteri, questo equivale dunque a dire "tutti i fenicotteri sono rosa".

3.4.2 Il Quantificatore di Esistenza

Definiamo un nuovo quantificatore a partire da quello universale:

$(\exists x)(p(x)) := \neg(\forall x(\neg p(x))$

("Esiste un x che verifica p" := "Non tutti gli x non verificano p")

Continuando l'esempio precedente, questo potrebbe dire "Esiste un fenicottero rosa".

3.4.3 Il Quantificatore Esistenziale Unico

Definiamo un terzo quantificatore a partire da quello esistenziale:

$(\exists! x)(p(x)) := (\exists x)(\forall y(p(x) \leftrightarrow x = y))$

("Esiste un unico x che verifica p" := "Esiste un x tale che, per ogni y, y verifica p se e soltanto se y è x")

3.4.4 Scopo di un Quantificatore

Dato un qualsiasi quantificatore, la formula che esso applica alla propria variabile si dice scopo. Per esempio, in $(\forall x)(p(x))$, p è lo scopo del quantificatore.

3.5 Formule Chiuse e Aperte

All'interno di una formula ben formata, diciamo che una variabile è *libera* se non compare nello scopo di nessun quantificatore della formula. Una variabile non-libera, e cioè una variabile che appare all'interno dello scopo di un quantificatore, si dice invece *vincolata*.

Una formula si dice *chiusa* se non ha variabili libere, e si dice *aperta* se ha almeno una variabile libera.

Una formula libera p con n variabili libere $x_1, x_2, ..., x_n$ si può scrivere in notazione funzionale $p(x_1, x_2, ..., x_n)$

Se abbiamo dei termini $t_1, t_2, ..., t_n$, possiamo utilizzarli come argomenti di p: $p(t_1, t_2, ..., t_n)$. Quando scriviamo in questo modo, intendiamo sostituire ogni occorrenza di x_1 con t_1, ogni occorrenza di x_2 con t_2, etc etc.

Intuitivamente, questo vuol dire che ogni formula aperta può agire da predicato.

3.6 Formule Valide

Una formula che è sempre vera, indipendentemente dall interpretazione, cioè una formula che è vera indipendentemente da quale sia la logica del primo ordine che stiamo considerando si dice *formula valida*. Segue che ogni tautologia è una formula valida.

3.7 Quantificatori Ristretti

Abbiamo definito un numero di quantificatori che ci permette di fare affermazioni su ogni elemento di un insieme, o di affermare che esiste un elemento di un insieme che verifica certe proprietà.

Questo è però ancora limitante: possiamo dire, per esempio, "Ogni uccello è rosa" se l'insieme che stiamo considerando è quello degli uccelli, ma non possiamo dire "Ogni fenicottero è rosa" o "Ogni albatro è bianco".

Introduciamo dunque il concetto di *quantificatori ristretti* che non si riferiscono ad ogni termine dell'insieme di riferimento, ma piuttosto ad una sua parte.

Definiamo dunque, data una lettera predicativa binaria p, una variabile individuale x, ed un termine t, ed una formula ben formata f:

$$\forall p(x,t)(f(x)) := \forall(p(x,t) \rightarrow f(x))$$

Per esempio, se p è il predicato "è un fenicottero", e f è "è rosa", allora abbiamo gli strumenti per dire "Ogni uccello che è un fenicottero è rosa". Un altro esempio semplice e matematico di formula ben formata che utilizza un quantificatore ristretto è il seguente:

$$(\forall x >= 0)(x = |x|)$$

(Ogni numero che è non-negativo equivale al proprio valore assoluto)

4 Teoria degli Insiemi

Un insieme è una collezione di oggetti o elementi (che sono a loro volta insiemi) per i quali esiste un criterio oggettivo che ci permette di determinare se un elemento appartiene all'insieme o meno.

Se un elemento x appartiene a un insieme s, scriveremo $s \in x$.

Esistono due modi per definire un insieme. Il primo è listarne tutti gli elementi.

$$s := \{1, 2, 3, 4, 5, 6\}$$

Il secondo è di utilizzare una formula ben formata:

$$\exists s \forall x(\phi(x))$$

Per esempio:

$$\exists s \forall x((x >= 1 \land x <= 6) \rightarrow x \in s)$$

("Esiste un insieme s tale che per ogni x, se x è maggiore o uguale ad 1 e minore o uguale a 6, allora x appartiene ad s")

Diciamo questo secondo metodo *definizione intrinseca* dell'insieme e definiamo per esso una notazione breve:

$$s := \{x|\phi(x)\}$$

("s è l'insieme delle x che verificano phi")

4.1 Sottoinsiemi

Dati due insiemi x ed y, dico che x è un *sottoinsieme* di y, e che y è dunque un *superinsieme* di x, se ogni elemento di x è anche elemento di y.

$$x \subseteq y \leftrightarrow (\forall z)(z \in x \rightarrow z \in y)$$

Da questo segue che ogni insieme è un proprio sottinsieme. Diciamo dunque che x è *parte propria* di y se è un sottoinsieme di y ma distinto da esso:

$$x \subset y \leftrightarrow x \subseteq y \land x \neq y$$

4.2 Singleton

Un insieme di un solo elemento si dice *singleton*. Chiamiamo tale elemento s ed esplicitiamo la definizione:

$$\{s\} := \{x|x = s\}$$

4.3 Assiomi della Teoria degli Insiemi

Inizialmente i matematici utilizzavano il concetto di insieme intuitivamente. Con il passare del tempo, però, questo ha portato alla scoperta di diversi paradossi, principalmente il "Paradosso Di Russell". A causa di ciò, la teoria degli insiemi moderna afferma che un insieme esiste effettivamente soltanto se è possibile dimostrarne l'esistenza a partire da un insieme di *assiomi della teoria degli insiemi.*

Assioma 1 (Assioma del Vuoto)**.** *Esiste un insieme, detto l'insieme vuoto* $\emptyset$*, che non contiene nulla.*

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

Assioma 2 (Assioma di Estensionalità)**.** *Due insiemi coincidono se e solo se ogni elemento del primo insieme appartiene al secondo e viceversa.*

$$\forall x\forall y(x = y \leftrightarrow \forall z(z \in x \leftrightarrow z \in y))$$

Assioma 3 (Assioma di Separazione)**.** *Per ogni insieme* s *e predicato unario* p *esiste l'insieme degli elementi di* s *che verificano* p*.*

$$\{x | x \in s \wedge p(x)\}$$

Assioma 4 (Assioma di Esistenza dell'Insieme delle Parti)**.** *Per ogni insieme* s *esiste l'insieme delle parti* $\mathcal{P}(s)$*, che è l'insieme di tutti i sottoinsiemi di* s*.*

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

Assioma 5 (Assioma della Coppia)**.** *Per ogni coppia di insiemi* x, y *esiste l'insieme coppia* $\{x, y\}$*.*

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

Assioma 6 (Assioma di Unione)**.** *Per ogni insieme di insiemi* f *esiste l'insieme unione unaria di* f*, cioè l'insieme unione di tutti gli insiemi che sono elementi di* f*.*

$$(\forall f)(\exists u)(\forall x)(\forall y)(x \in u \leftrightarrow (x \in y \wedge y \subseteq f))$$

Esempio. Facciamo un esempio di unione unaria. Prendiamo l'insieme:

$$f = \{\{a, b\}, \{c, d, e\}\}$$

L'unione unaria di questo insieme è $\bigcup f = \{a, b, c, d, e\}$.

Assioma 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.*

Assioma 8 (Assioma dell'Infinito)**.** *Esiste un insieme infinito, e tale insieme è* $\mathbb{N}$*.*

4.3.1 Teoremi Derivanti dagli Assiomi

Teorema 4.1 (Unicità dell'Insieme Vuoto)**.** *L'insieme vuoto è unico.*

Dimostrazione. Siano x ed y due insiemi vuoti. Dalla definizione segue che, per ogni elemento generico z:

$$(\forall z)(z \notin x \wedge z \notin y)$$

Le implicazioni $z \in x \rightarrow z \in y$ e $z \in y \rightarrow z \in x$ sono dunque entrambi vere. Pertanto, $z \in x \leftrightarrow z \in y$ e per l'assioma di estensionalità $x = y$, cioè esiste un singolo insieme vuoto. □

Teorema 4.2 (Ogni Insieme contiene l'Insieme Vuoto)**.**

Dimostrazione. La formula $(\forall z)(z \in \emptyset \rightarrow z \in \emptyset)$ è una formula valida perché $z \in \emptyset$ è sempre falsa (e dunque l'implicazione è sempre vera). Pertanto, $\emptyset \subseteq \emptyset$.

Similarmente, la formula $(\forall x)(\forall z)(z \in \emptyset \rightarrow z \in x)$ è una formula valida, pertanto $(\forall x)(\emptyset \subseteq x)$ □

Teorema 4.3 (Unicità dell'Insieme delle Parti)**.**

Dimostrazione. Sia x un insieme e siano u e w insiemi delle sue parti. Dall'assioma di esistenza dell'insieme delle parti abbiamo che $(\forall z)(z \in u \leftrightarrow z \subseteq x)$ e $(\forall z)(z \in u \leftrightarrow z \subseteq x)$. Da questo segue che $(\forall z)(z \in u \leftrightarrow z \in x \leftrightarrow zinw)$ e quindi $z \in u \leftrightarrow z \in w$ per ogni z. Dall'assioma di estensionalità si ha dunque che $u = w$. □

Teorema 4.4 (Paradosso di Russell)**.** *Non esiste l'insieme degli insiemi che non appartengono a se stessi.*

Dimostrazione. Ipotizziamo per assurdo che tale insieme,

$$r := \{x | (x \notin x)\}$$

esista. Esistono solo due possibilità, o $r \in r$ o $r \notin r$.

Se $r \in r$, allora per definizione non appartiene a sé stesso (dato che r è l'insieme degli insiemi che non appartengono a sé stessi), cioè $r \in r \rightarrow r \notin r$ il che è chiaramente assurdo.

Se $r \notin r$, allora è un insieme che non appartiene a sé stesso, e deve quindi appartenersi, $r \notin r \rightarrow r \in r$ il che è chiaramente assurdo. □

4.3.2 Parti del Vuoto

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

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

C'è un solo insieme tale che ogni suo elemento z appartiene anche all'insieme vuoto... l'insieme vuoto stesso! (dato che non ha elementi, "ogni suo elemento appartiene all'insieme vuoto" è un'implicazione vera).

Pertanto $\mathcal{P}(\emptyset) = \{\emptyset\}$ cioè 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 teorema essere sottoinsieme di ogni insieme) oppure se è $\{\emptyset\}$ stesso (dato che ogni insieme è proprio sottoinsieme). Da questo segue che:

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

4.4 Operazioni fra Insiemi

L'assioma di estensionalità ci permette di definire l'uguaglianza fra due insiemi, accomunando l'equivalenza logica $\leftrightarrow$ all'uguaglianza $=$.

Allo stesso modo, definiamo la relazione "essere sottoinsieme di" $\subseteq$ a partire dall'implicazione logica $\rightarrow$.

Vogliamo adesso definire altri tre operatori fra, $\cup, \cap, \triangle$ che sono operazioni fra insiemi accomunabili ai connettivi logici $\vee, \wedge, \veebar$.

Definizione 1 (Intersezione fra Insiemi)**.**

$$x \cap y = \{z | z \in x \wedge z \in y\}$$

L'intersezione fra x ed y è dunque l'insieme che contiene tutti gli elementi che appartengono sia all'uno che all'altro. Questo insieme esiste sicuramente per l'assioma di separazione.

L'intersezione è l'operazione fra insiemi corrispondente all'and logico.

Definizione 2 (Unione di Insiemi)**.**

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

L'unione di x ed y è dunque l'unione unaria del loro insieme coppia. Questo insieme esiste sicuramente per l'assioma di separazione e per l'assioma di unione.

L'unione è l'operazione fra insiemi corrispondente all'or logico.

Attenzione! Si potrebbe pensare che si può definire l'unione come:

$$x \cup y = \{z | z \in x \vee z \in y\}$$

Cioè come l'insieme degli elementi che appartengono ad uno o all'altro insieme, in modo simile a come abbiamo fatto per l'intersezione.

L'insieme unione è effettivamente uguale a tale insieme, ma se lo definissimo in tale modo non avremmo nessun assioma che ci dà la certezza che l'insieme esista! Infatti l'assioma di separazione funziona soltanto quando usiamo $\wedge$ e non $\vee$.

Dunque, non è scorretto dire che l'insieme unione è uguale a $\{z | z \in x \vee z \in y\}$, ma non possiamo usare questa dicitura come sua *definizione*.

Definizione 3 (Differenza Simmetrica fra Insiemi)**.**

$$x \triangle y = \{z \in x \cup y | z \in x \oplus z \in y\}$$

Questo insieme esiste sicuramente per l'assioma di separazione.
La differenza simmetrica è l'operazione corrispondente allo xor.

4.4.1 Differenza fra Insiemi

Esiste un solo connettivo per cui dobbiamo ancora definire un'operazione fra insiemi corrispondente, la negazione. Si potrebbe pensare di definire il negato di un insieme x come:

$$\{z | z \notin x\}$$

Cioè, semplicemente, come l'insieme degli elementi che non appartengono ad x. Sfortunatamente, tale insieme non esiste. Se tale insieme, che chiamiamo per esempio y, esistesse, allora esisterebbe l'unione $x \cup y$ che sarebbe uguale al cosiddetto "insieme universo", insieme di tutti gli insiemi. Ma dimostriamo adesso che l'insieme universo non esiste.

Teorema 4.5 (L'Insieme Universo non Esiste)**.**

Dimostrazione. Assumiamo per assurdo esista l'insieme universo v. Allora, per separazione, per ogni predicato ϕ esiste l'insieme $\{x \in v | \phi(x)\}$. Ma se scegliamo $\phi = x \notin x$, allora questo implicherebbe che esiste l'insieme $\{x | x \notin x\}$. Ma questo insieme non esiste per il Paradosso di Russell, e abbiamo l'assurdo. □

Da questo segue che non possiamo semplicemente negare un insieme da solo, e l'ultima operazione che definiamo è l'operazione *differenza di insiemi*.

Definizione 4 (Differenza di Insiemi)**.**

$$x - y = \{z \in x | z \notin y\}$$

Cioè l'insieme degli elementi che appartengono ad x ma non y.

4.5 Operazioni Insiemistiche Derivanti da Tautologie

Abbiamo visto che ogni connettivo logico è corrispondente ad un'operazione fra insiemi. Segue dunque che anche le tautologie della logica proposizionale corrispondono a proprietà degli insiemi.

Teorema 4.6 (Doppia Negazione)**.**

$$(\forall x, y)(y \subseteq x \to x - (x - y) = y)$$

Dimostrazione.

$$\begin{aligned} x-(x-y) &= \{z \in x \mid z \notin (x-y)\} && \text{(definizione di differenza)} \\ &= \{z \in x \mid \neg(z \in x \wedge z \notin y)\} \\ &= \{z \in x \mid z \notin x \vee z \in y\} && \text{(De Morgan)} \\ &= \{z \mid z \in x \wedge (z \notin x \vee z \in y)\} \\ &= \{z \mid (z \in x \wedge z \notin x) \vee (z \in x \wedge z \in y)\} && \text{(distributivita')} \\ &= \{z \mid z \in x \wedge z \in y\} = x \cap y \end{aligned}$$

Poiché $y \subseteq x \implies x \cap y = y$ abbiamo la tesi. □

Teorema 4.7 (Terzo Escluso)**.**

$$\forall x, y(y \subseteq x \to y \cup (x-y) = x)$$

Dimostrazione.

$$\begin{aligned} y \cup (x-y) &= \{z \mid (z \in y) \vee (z \in (x-y))\} \\ &= \{z \mid (z \in y) \vee (z \in x \wedge z \notin y)\} && \text{(def. di differenza)} \\ &= \{z \mid (z \in y \vee z \in x) \wedge (z \in y \vee z \notin y)\} && \text{(distributivita')} \\ &= \{z \mid z \in y \vee z \in x\} \\ &= x \cup y \end{aligned}$$

Da cui: $y \subseteq x \implies x \cup y = y$ che è la tesi. □

Teorema 4.8 (Principio di Non Contraddizione)**.**

$$(\forall x, y)(y \cap (x-y) = \emptyset)$$

Dimostrazione.

$$\begin{aligned} y \cap (x-y) &= \{z \mid (z \in y) \wedge (z \in (x-y))\} \\ &= \{z \mid (z \in y) \wedge (z \in x \wedge z \notin y)\} && \text{(def. di x - y)} \\ &= \{z \mid (z \in y \wedge z \notin y) \wedge z \in x\} && \text{(proprieta' ass. e comm. di and)} \end{aligned}$$

Essendo $(z \in y \wedge z \notin y)$ sempre falsa (principio di non contraddizione), l'insieme è vuoto. □

Teorema 4.9 (Doppia Induzione)**.**

$$(\forall x, y)(x = y \leftrightarrow x \subseteq y \wedge y \subseteq x)$$

Cioè due insiemi coincidono solo se si contengono a vicenda.

Dimostrazione. Per l'assioma di estensionalità, $x = y \leftrightarrow (\forall z)(z \in x \leftrightarrow z \in y)$.
Per la tautologia di doppia induzione, questo è equivalente a:

$$(\forall z)((z \in x \to z \in y) \land (z \in y \to z \in x))$$

Perl a definizione di $\subseteq$, questo equivale infine a:

$$(\forall z)((x \subseteq y) \land (y \subseteq x))$$

□

Teorema 4.10 (Idempotenza)**.**

$$x \cup x = x$$
$$x \cap x = x$$

Dimostrazione. Si sfruttano le proprietà di idempotenza di $\land$ e $\lor$:

$$x \cup x = \{z \mid z \in x \lor z \in x\} = \{z \mid z \in x\} = x$$
$$x \cap x = \{z \mid z \in x \land z \in x\} = \{z \mid z \in x\} = x$$

□

Teorema 4.11 (Associatività)**.**

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

Dimostrazione. Per l'unione, analoga per intersezione e differenza simmetrica:

$$\begin{aligned} a \cup (b \cup c) &= \{z \mid z \in a \lor z \in (b \cup c)\} && \text{(def. di unione)} \\ &= \{z \mid z \in a \lor (z \in b \lor z \in c)\} && \text{(def. di unione)} \\ &= \{z \mid (z \in a \lor z \in b) \lor z \in c\} && \text{(associativita' di unione)} \\ &= \{z \mid z \in (a \cup b) \lor z \in c\} = (a \cup b) \cup c \end{aligned}$$

□

Teorema 4.12 (Commutatività)**.**

$$a \cup b = b \cup a$$
$$a \cap b = b \cap a$$
$$a \triangle b = b \triangle a$$

Dimostrazione. Per l'intersezione:

$$\begin{aligned} a \cap b &= \{z \mid z \in a \wedge z \in b\} \text{ (def. di intersezione)} \\ &= \{z \mid z \in b \wedge z \in a\} \text{ (comm. dell'and)} \\ &= b \cap a \end{aligned}$$

Per l'unione: $a \cup b = \bigcup(\{a, b\}) = \bigcup(\{b, a\}) = b \cup a$ □

Teorema 4.13 (Distributività)**.**

$$\begin{aligned} a \cup (b \cap c) &= (a \cup b) \cap (a \cup c) \\ a \cap (b \cup c) &= (a \cap b) \cup (a \cap c) \end{aligned}$$

Dimostrazione. Per l'unione rispetto all'intersezione (analoga nell'altro caso):

$$\begin{aligned} a \cup (b \cap c) &= \{z \mid z \in a \vee (z \in b \wedge z \in c)\} && \text{(def. di unione e intersezione)} \\ &= \{z \mid (z \in a \vee z \in b) \wedge (z \in a \vee z \in c)\} && \text{(distributivita')} \\ &= \{z \mid z \in (a \cup b) \wedge z \in (a \cup c)\} \\ &= \{z \mid z \in ((a \cup b) \cap (a \cup c)) = (a \cup b) \cap (a \cup c) \end{aligned}$$

□

Teorema 4.14 (Esplicitazione della Differenza Simmetrica)**.**

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

Dimostrazione:

Dimostrazione.

$$\begin{aligned} a \triangle b &= \{z \in a \cup b \mid z \in a \oplus z \in b\} && \text{(def. di diff. simmetrica)} \\ &= \{z \in a \cup b \mid (z \in a \vee z \in b) \wedge \neg(z \in a \wedge z \in b)\} && \text{(esplicit. dello xor)} \\ &= \{z \in a \cup b \mid (z \in a \cup b) \wedge \neg(z \in a \cap b)\} && \text{(def. di unione ed intersez.)} \\ &= \{z \mid (z \in a \cup b) \wedge (z \in a \cup b) \wedge \neg(z \in a \cap b)\} \\ &= \{z \mid (z \in a \cup b) \wedge \neg(z \in a \cap b)\} && \text{(idempotenza di and)} \\ &= (a \cup b) - (a \cap b) && \text{(def. di diff. di insiemi)} \end{aligned}$$

□

Teorema 4.15 (Leggi di De Morgan fra Insiemi)**.**

$$\begin{aligned} (\forall a, b, c)((c - (a \cup b)) &= (c - a) \cap (c - b)) \\ (\forall a, b, c)((c - (a \cap b)) &= (c - a) \cup (c - b)) \end{aligned}$$

Dimostrazione. Dimostrazione per (1), la (2) è equivalente:

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

□

4.6 Diagrammi di Venn

TODO

4.7 Ennuple Ordinate

Dall'assioma di estensionalità, sappiamo che due insiemi sono uguali fintanto che hanno gli stessi elementi. Pertanto, non ha importanza l'ordine, l'insieme $\{a, b\}$ è equivalente all'insieme $\{b, a\}$.

Diamo ora la definizione di *coppia ordinata*, che è un insieme di due elementi in cui l'ordine ha importanza e $(a, b) \neq (b, a)$.

Definizione 5 (Coppia Ordinata)**.**

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

Da questo segue il teorema:

Teorema 4.16 (Caratterizzazione di Coppie Ordinate)**.**

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

Dimostrazione. 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:

$$\begin{aligned}
&(x, y) = \{\{x\}, \{x, y\}\} = \{\{x\}, \{x\}\} = \{\{x\}\} \\
\implies &(y, x) = \{\{y\}, \{y, x\}\} = \{\{x\}, \{x\}\} = \{\{x\}\} = (x, y)
\end{aligned}$$

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. □

Avendo definito le coppie ordinate, possiamo definire le triple ordinate:

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

E, ricorsivamente, possiamo definire una qualsiasi n-upla ordinata:

$$(x_1, x_2, \ldots, x_n) = ((x_1, x_2, \ldots, x_{n-1}), x_n)$$

L'elemento all'i-esimo posto di un'ennupla cartesiana si dice *componente i-esima* dell'ennupla.

4.8 Prodotto Cartesiano

Dati due insiemi a e b, il *prodotto cartesiano* $a \times b$ non è nient'altro che l'insieme di tutte le coppie cartesiane che hanno come prima componente un elemento di a e come secondo componente un elemento di b. La definizione formale dunque è:

Definizione 6 (Prodotto Cartesiano)**.**

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

Esempio. Siano $i = \{a, b, c\}$ e $j = \{x, y, z\}$. Il prodotto cartesiano sarà dunque $i \times j = \{(a, x), (a, y), (a, z), (b, x), (b, y), (b, z), (c, x), (c, y), (c, z)\}$

5 Corrispondenze e Applicazioni

5.1 Corrispondenze

Alice, Bob e Cathy sono allergici a certi cibi. Alice è allergica a noci e uova, Bob è allergico al pesce, e Cathy è allergica a uova e pesce. Un semplice modo per esprimere la *corrispondenza* che c'è fra ognuno e le proprie allergie è una tabella:

Soggetto	Allergia
Alice	Noci
Alice	Uova
Bob	Pesce
Cathy	Uova
Cathy	Pesce

Notiamo che in realtà la tabella così scritta non è nient'altro che la rappresentazione visuale del seguente insieme di coppie ordinate:

{(Alice, Noci), (Alice, Uova), (Bob, Pesce), (Cathy, Uova), (Cathy, Pesce)}

Questo insieme è a sua volta un sottoinsieme del prodotto cartesiano {Alice, Bob, Cathy} × {Noci, Uova, Pesce}.

Procediamo dunque col definire:

Definizione 7 (Corrispondenza fra Insiemi)**.** *Una coppia ordinata del tipo* $(a \times b, g)$ *dove* $g \subseteq a \times b$ *si dice corrispondenza fra gli insiemi* a *e* b *di grafico* g*.*

Se una coppia $(x, y) \in g$ si dice che "x è in corrispondenza o relazione con y", o che y corrisponde ad x.

Se due elementi x, y sono in corrispondenza rispetto ad una corrispondenza ρ, scriviamo allora $x \rho y$.

Definizione 8 (Relazione Binaria)**.** *Se* $a = b$*, cioè la corrispondenza è definita su un singolo insieme, essa si dice in particolare relazione binaria.*

Diciamo $\mathrm{Corr}(a, b)$ l'insieme delle corrispondenze definibili fra a e b e $\mathrm{Rel}(a)$ l'insieme delle relazioni definibili su a. Segue che $\mathrm{Rel}(a) = \mathrm{Corr}(a, a)$.

5.1.1 Rappresentazione Grafica di Corrispondenze

TODO

5.2 Applicazioni

Definizione 9 (Applicazione)**.** *Sia* $f = (a \times b, g)$ *con* $g \subseteq a \times b$*. Se si verifica che:*

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

Cioè per ogni elemento di a *esiste uno ed un solo elemento di* b *con cui è in corrispondenza, allora diciamo che* ρ *è un'applicazione o funzione.*

Scriveremo dunque $f : a \to b$. a si dice *dominio* della funzione e b suo *codominio*. Se xfy, scriveremo invece $f(x) = y$. y è *immagine* di x.

L'insieme di tutte le immagini, $Im(f) := \{y \in b | (\exists x \in a)(f(x) = y)\}$ si definisce *immagine della funzione*. Questa la possiamo anche scrivere $Im(f) := \{f(x) \mid x \in a\}$.

Dato un insieme $s \subseteq a$, allora definiamo l'*immagine dell'insieme* s $f(s) = \{y \in b \mid (\exists x \in a)(f(x) = y)\}$, cioè l'insieme di tutte le immagini degli elementi di s.

Equivalentemente, se $s \subseteq b$, definiamo l'*antimmagine o controimmagine* di s l'insieme di tutti gli elementi di a che hanno immagine in s: $f^{-1}(s) = \{x \in a | f(x) \in s\}$.

Possiamo definire totalmente una funzione attraverso una sua *descrizione esplicita* che ne definisce dominio, codominio, e la *legge* che lega gli elementi.

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

Esempio. $f : n \in \mathbb{N} \mapsto (n+1) \in \mathbb{N}$ è la funzione che associa ad ogni numero naturale il suo valore successivo: $f(1) = 2, f(2) = 3, f(3) = 4, \ldots$

Un'applicazione si può anche dire *ben posta* o *ben definita* per sottolineare che essa è effettivamente un'applicazione e non solo una corrispondenza.

Esempio. "La funzione $f : x \in \mathbb{Z} \mapsto \sqrt{x} \in \mathbb{C}$ è ben posta?"

Non lo è, in quanto ad ogni x negativa sono associate due radici in $\mathbb{C}$, ed una funzione associa ad ogni elemento una ed una sola immagine. Pertanto f non è una funzione ben posta, cioè non è affatto una funzione ma solo una corrispondenza.

5.3 Prodotto Relazionale e Applicazioni Composte

Siano $\rho = (a \times b, g_1)$ e $\sigma = (c \times d, g_2)$ due corrispondenze.

Definizione 10 (Prodotto Relazionale)**.** *Il prodotto relazionale fra la corrispondenza ρ e la corrispondenza σ è la corrispondenza $\rho\sigma = (a \times d, g_3)$ dove:*

$$(\forall x \in a)(\forall y \in d)((x, y) \in g_3 \iff (\exists z)((x, z) \in g_2 \wedge (z, y) \in g_2))$$

Esempio. Sia $x\rho y \iff x$ padre di y.
Sia $x\sigma y \iff x$ fratello di y.
Allora:

$$x\rho\rho y = x\rho^2 y \iff (\exists z)(x\rho z \wedge z\rho y)$$

Cioè x è in relazione con y soltanto se esiste z che è figlio di x e padre di y. La corrispondenza ρ^2 è quindi la corrispondenza "essere nonno di".

Similarmente, se consideriamo $x\rho\sigma y \iff (\exists z)(x\rho z \wedge z\sigma y)$, allora x è in corrispondenza con y soltanto se esiste z che è figlio di x ma fratello di y. Pertanto $\rho\sigma$ è la corrispondenza "essere zio di".

Teorema 5.1 (Associatività del Prodotto Relazionale)**.** *Date tre corrispondenze σ, ρ, φ, vogliamo dimostrare che:*

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

Per cui bisogna dimostrare che: $g_{\sigma(\rho\varphi)} = g_{(\sigma\rho)\varphi}$, e cioè che (per estensionalità) ogni punto che appartiene al primo grafico appartiene anche al secondo e viceversa. Limitiamoci al dimostrare che un punto che appartiene al primo appartiene anche al secondo, dato che la dimostrazione inversa è analoga.

$$\begin{aligned}(x,y) \in g_{\sigma(\rho\varphi)} &\implies \exists z : (x,z) \in g_\sigma \wedge (z,y) \in g_{\rho\varphi} \\ &\implies \exists w : (z,w) \in g_\rho \wedge (w,y) \in g_\varphi \\ &\implies (x,w) \in g_{\sigma\rho} \wedge (w,y) \in g_\varphi \implies (x,y) \in g_{(\sigma\rho)\varphi}\end{aligned}$$

Anche applicazioni so possono unire in *applicazioni composte.*

Definizione 11. *Date due funzioni $f : a \to b$ e $g : b \to c$, 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".*

Si osserva che $g \circ f(x) = g(f(x))$

Notiamo come sia necessario che il codominio della prima funzione sia il dominio della seconda (o un suo sottoinsieme) affinché la composizione delle due applicazioni sia possibile.

5.4 Applicazioni Particolari

La funzione $\mathrm{Id}_a : x \in a \mapsto x \in a$, cioè la funzione che associa ad ogni valore di a sé stesso, si dice *funzione identità.*

Data una funzione $f : x \in a \mapsto f(x) \in b$, e $s \subseteq a$, la funzione $f_{|s} : x \in s \mapsto f(x) \in b$ si dice *restrizione* della funzione f ad s.

Se $a \subseteq h$, Una funzione $g : h \to c$ si dice *prolungamento* di f se $g_{|a} = f$ cioè se f è una restrizione di g.

Se $s \subseteq b \wedge Im(f) \subseteq s$, la funzione $p : x \in a \mapsto f(x) \in s$ si dice *ridotta* di f ad s.

Se $y* \in b$, la funzione $f : x \in a \mapsto y* \in b$ si dice *funzione costante* in quanto associa ad ogni elemento la stessa immagine.

Per ogni funzione $f : a \to b$ possiamo definire le funzioni:

$$\begin{aligned}\overrightarrow{f} &: \overline{a} \in \mathcal{P}(a) \to \{f(z) \mid z \in \overline{a}\} \in \mathcal{P}(b) \\ \overleftarrow{f} &: \overline{b} \in \mathcal{P}(b) \to \{z \in a \mid f(z) \in \overline{b}\} \in \mathcal{P}(a)\end{aligned}$$

Cioè le funzioni immagine ed antimmagine che, rispettivamente, associano ad ogni sottoinsieme del dominio la sua immagine, e ad ogni sottoinsieme del codominio la sua antimmagine.

5.5 Applicazioni Suriettive ed Iniettive

Definizione 12. *Una funzione $f : a \to b$ si dice suriettiva se e soltanto se:*

$$Im(f) = b$$

Cioè se il codominio e l'immagine della funzione coincidono. Questo si può anche esprimere esplicitamente come:

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

Definizione 13. *Una funzione $f : a \to b$ si dice iniettiva se e soltanto se:*

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

Cioè due elementi hanno la stessa immagine se e soltanto se coincidono. Equivalentemente, usando la contrapposizione, possiamo anche dire che la funzione è iniettiva se e soltanto se:

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

Cioè ad elementi distinti corrispondono immagini distinte.

Definizione 14. *Una funzione si dice biettiva se e soltanto se è sia iniettiva che suriettiva.*

Teorema 5.2 (La composizione di funzioni suriettive è suriettiva.)**.**

Dimostrazione. Siano $f : a \to b$ e $g : b \to c$ due funzioni suriettive. Sia $y \in c$. Poiché g è suriettiva, $(\exists z \in b)(g(b) = y$. Essendo $z \in b$, $(\exists x \in a)(f(x) = z)$.

Allora si ha che $g(z) = g(f(x)) = g \circ f(x) = y$, per ogni y, e dunque $g \circ f$ è suriettive. □

Teorema 5.3 (La composizione di funzioni iniettive è iniettive)**.**

Dimostrazione. Siano $f : a \to b$ e $g : b \to c$ due funzioni iniettive. Siano $w, z \in a$ tali che $g \circ f(w) = g \circ f(z)$. Questo equivale a dire che $g(f(w)) = g(f(z))$. Essendo g iniettiva, allora $f(w) = f(z)$. Ma, essendo f iniettiva, allora $w = z$. Pertanto la funzione composta è iniettiva. □

Teorema 5.4 (La composizione di funzioni biettive è biettiva)**.**

Dimostrazione. Segue dai precedenti due teoremi. □

Teorema 5.5 (Caratterizzazione di Iniettività 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.*

$$f \in In(a, b) \iff \forall y \in \mathcal{P}_(b) : \overleftarrow{f}(y) = \emptyset \vee ((\exists! x \in a)(\overleftarrow{f}(y) = \{x\})))$$

Dimostrazione. $\Rightarrow$: Sia $y \in \mathcal{P}_(b)$ 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 $\overleftarrow{f}(y) = \{x\}$

$\Leftarrow$: 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. □

Teorema 5.6 (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.*

$$fSuriettiva(a, b) \iff (\forall y \in \mathcal{P}_1(b) - \{\emptyset\})(\overleftarrow{f}(y) \neq \emptyset)$$

Dimostrazione. $\Rightarrow$: f suriettiva $\implies (\forall y \in b)(\exists x \in a)(f(x) = y) \implies (\forall \{y\} \in \mathcal{P}_1(b))(\exists x)(x \in \overleftarrow{f}(\{y\})$

$\Leftarrow$: $(\forall y \in \mathcal{P}_1(b) - \{\emptyset\})(\overleftarrow{f}(y) \neq \emptyset) \implies (\forall y \in b)(\exists x \in \overleftarrow{f}(y) \subseteq a)(f(x) = y) \implies$ f suriettiva □

Teorema 5.7 (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.*

Dimostrazione. Segue dai precedenti due teoremi. □

5.6 Sezioni, Retrazioni, Inverse di una Funzione

Definizione 15 (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.*

Definizione 16 (Retrazione 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.*

Definizione 17 (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.*

Teorema 5.8 (Caratterizzazione di Iniettività tramite Retrazione)**.** *Una funzione è iniettiva se e soltanto se il suo dominio è vuoto o esiste una sua retrazione.*

$$f : a \to b \text{ iniettiva} \iff a = \emptyset \vee (\exists g : b \to a)(g \circ f = id_a)$$

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.

$\Rightarrow$: 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. □

Teorema 5.9 (Caratterizzazione di Suriettività tramite Sezione)**.** *Una funzione è suriettiva se e soltanto se esiste una sua sezione.*

$$f : a \to b \text{ suriettiva} \iff (\exists g : b \to a)(f \circ g = id_b)$$

Dimostrazione. $\Leftarrow$: $(\exists g : b \to a)(f \circ g = id_b)$ implica che f sia suriettiva dato che id_b è suriettiva.

$\Rightarrow$: Dalla caratterizzazione di suriettività tramite antimmagine si ha che 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: $f \circ g(y) = f(g(y)) = f(\varphi(\overleftarrow{f}(\{y\}))) = y$ □

Teorema 5.10 (Caratterizzazione di Biettività tramite Inversa)**.**

Dimostrazione. Segue dai precedenti due teoremi. □

Teorema 5.11 (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.*

Dimostrazione. $r \circ f = id_a, f \circ s = id_b$ allora $(r \circ f) \circ s = id_a \circ s = s$ e $r \circ (f \circ s) = r \circ id_b = r$. Ma per associatività del prodotto relazionale $r \circ (f \circ s) = (r \circ f) \circ s$ e dunque r = s, che è la tesi. □

Teorema 5.12 (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.*

Dimostrazione. Supponiamo per assurdo che la funzione non sia iniettiva. Devono quindi esistere x_1 e x_2 distinti tali che $f(x_1) = f(x_2)$. Ciò implica che possono esistere g_1, g_2 sezioni distinte tali che $g_1(y) = x_1$ e $g_2(y) = x_2$, il che va contro l'ipotesi.

$$g_1 : g(f(x_1)) = x_1$$
$$g_2 : y \in b \mapsto \begin{cases} g(y) \text{ se } y \neq f(x_1) \\ x_2 \text{ se } y = f(x_2) \end{cases}$$

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. □

Per concludere questa sezione, riassumiamo affermando che i precedenti teoremi ci permettono di dire che:

Teorema 5.13 (Affermazioni equivalenti alla Biettività)**.** *Sia* $f : a \to b$*. Le seguenti affermazioni sono fra di loro equivalenti:*

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

Dimostrazione. Segue dai teoremi dimostrati in questa sezione. □

6 Strutture Algebriche

Molto spesso è utile non solo parlare di insiemi, ma anche delle operazioni che sono eseguibili su di essi. Per esempio, l'insieme $\mathbb{R}$ dei numeri reali è molto più interessante se non ignoriamo tutte le operazioni che possiamo effettuare sui suoi elementi, operazioni come la somma, la sottrazione, il prodotto, e la divisione. Introduciamo dunque un concetto superiore a quello di singolo insieme, il concetto di *struttura algebrica*, cioè di insieme su cui sono definite delle operazioni.

Definizione 18 (Struttura Algebrica)**.** *Un'ennupla ordinata del tipo:*

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

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

Definizione 19 (Operazione Interna)**.** *Dato un insieme $s \neq \emptyset$, una funzione del tipo $* : s \times s \to s$ si dice operazione interna (specificamente 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 xfy o $x * y$ invece di $f(x, y)$ o $*(x, y)$.

Definizione 20 (Commutatività)**.** $*$ *è commutativa se e solo se $x * y = y * x$ per ogni $x, y \in s$.*

Definizione 21 (Associatività)**.** $*$ *è associativa se e solo se $(x * y) * z = x * (y * z)$ per ogni $x, y, z \in s$. In tal caso possiamo evitare le parentesi e scrivere semplicemente $x * y * z$.*

6.1 (Extra) Operazioni Duali

TODO

6.2 Semigruppi

Dividiamo le strutture algebriche in categorie in base al numero e alle proprietà delle operazioni di cui esse sono dotate. La tipologia più semplice di struttura che useremo è il *semigruppo*.

Definizione 22 (Semigruppo)**.** *Una struttura algebrica ad una sola operazione binaria interna*

$$(s, *)$$

si dice semigruppo se $*$ è associativa.

6.3 Monoidi

Definizione 23 (Elemento Neutro)**.** *Sia $(s, *)$ una struttura algebrica. Allora:*

$$\begin{aligned} l \in s \text{ el. neutro a sinistra} &\iff (\forall x \in s)(l * x = x) \\ d \in s \text{ el. neutro a destra} &\iff (\forall x \in s)(x * d = x) \\ e \in s \text{ el. neutro} &\iff \text{neutro a destra e a sinistra} \end{aligned}$$

Teorema 6.1 (Unicità dell'Elemento Neutro)**.** *Se un'operazione $*$ è dotata di neutro a sinistra l e neutro a destra d, allora si ha che $l = d$ ed in particolare esso è l'unico elemento neutro dell'operazione.*

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

$$l = l * d = d$$

□

Definizione 24 (Monoide)**.** *Un semigruppo $(s, *)$ dotato di elemento neutro $u \in s$ si dice monoide. E' possibile notare l'elemento neutro esplicitamente, in tale modo:*

$$(s, *, u)$$

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

6.4 Gruppi

Definizione 25 (Inverso di un Elemento)**.** *Sia $(s, *, u)$ un monoide e sia $x \in s$. Allora:*

$$\begin{aligned} (\exists d \in s)(x * d = u) &:\Leftrightarrow d \text{ inverso a destra di } x. \\ (\exists l \in s)(l * x = u) &:\Leftrightarrow l \text{ inverso a sinistra di } x. \end{aligned}$$

Un elemento inverso di x sia a destra che a sinistra si dice semplicemente inverso di x.

Definizione 26 (Elemento Invertibile)**.** *Un elemento si dice invertibile a sinistra (a destra) se è dotato di inverso a sinistra (a destra). Se è dotato di entrambi si dice semplicemente invertibile.*

Un elemento invertibile si dice anche simmetrizzabile. Un elemento inverso si dice anche elemento simmetrico o elemento opposto.

Usiamo la dicitura $U(s)$ per indicare l'insieme di tutti gli element simmetrizzabili di s

Teorema 6.2 (Unicità dell'Elemento Inverso)**.** *Sia x elemento di un monoide $(s, *, u)$ dotato di inverso a sinistra l e inverso a destra d. Allora $l = d$ e, in particolare, esso è l'unico inverso a sinistra, l'unico inverso a destra, e l'unico inverso.*

Dimostrazione. Per definizione di elemento inverso a sinistra o a destra, $l*x = u$ e $x*d = u$. Inoltre, trovandoci in un monoide, l'operazione $*$ è associative. Segue che:

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

Definizione 27 (Gruppo)**.** *Un gruppo è un monoide $(s, *)$ dove ogni elemento di s è invertibile.*

Definizione 28 (Gruppo Abeliano)**.** *Un gruppo la cui operazione è non solo associativa ma anche commutativa si dice gruppo abeliano.*

Esempio. La struttura algebrica $(\mathbb{Z}, +)$ è un gruppo abeliano.

6.5 Sottostrutture

Definizione 29 (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. $\mathbb{N}$ è parte stabile di $\mathbb{R}$ rispetto alla somma, dato che sommando due numeri naturali si ha sempre un numero naturale. Non è parte chiusa rispetto alla differenza, dato che per esempio sia 5 che 7 appartengono ad $\mathbb{N}$ ma $(5 - 7) = -2 \notin \mathbb{N}$

Esempio. $\{0\}$ è parte stabile di $\mathbb{R}$ rispetto alla somma e prodotto in quanto $0 + 0 = 0 \cdot 0 = 0$.

Esempio. In generale, per ogni monoide $(s, *, u)$, $\{u\}$ è parte stabile in quanto $u * u = u$.

Definizione 30 (Operazione Indotta)**.** *Data una struttura algebrica $(s, *)$ 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.

Teorema 6.3 (L'intersezione di Parti Stabili è una Parte Stabile)**.** *Sia $(s, *)$ una struttura algebrica e sia $t \subseteq \mathcal{P}(S)$ tale che $(\forall x \in t)(x$ parte stabile di $s)$. Allora $\bigcap t$ è anch'essa una parte stabile.*

Dimostrazione. Siano $x, y \in \bigcap t$. Allora, per la definizione di intersezione unaria, $(\forall z \in t)(x, y \in z)$. Essendo ogni z parte chiusa 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 chiusa di s. □

Avendo dato la definizione di parte stabile e di operazione indotta, possiamo finalmente definire il concetto di sottostruttura:

Definizione 31 (Sottostruttura)**.** *Data una struttura algebrica* $(s, *)$ *e sia* $t \leq s$*. Allora la struttura algebrica* $(t, *_{|t \times t})$ *si dice sottostruttura.*

Se la struttura è un semigruppo (o monoide, o gruppo) e la sottostruttura è anch'essa un semigruppo (o monoide, o gruppo), allora scriveremo $t \leq s$

Dimostriamo che l'elemento neutro di un sottogruppo è sempre lo stesso del gruppo di cui esso è sottostruttura:

Teorema 6.4 (Elemento Neutro di una Sottogruppo)**.** $h \leq g$ *sottogruppo* $, 1_h \in h, 1_g \in g \implies 1_h = 1_g$

Dimostrazione. $1_h \in h \implies 1_h \in g \implies 1_h \cdot 1_h = 1_h = 1_h \cdot 1_g$

Il che implica che sia 1_g e 1_h siano inversi di 1_h, ma essendo l'inverso unico si ha allora che $1_h = 1_g$ □

6.5.1 Sottostrutture Generate

Consideriamo il monoide $(\mathbb{N}, +)$ ed il numero 2. Qual è il più piccolo sottomonoide che contiene 2? Abbiamo dimostrato che l'intersezione di parti stabili è a sua volta una parte stabile, pertanto segue che tale sottomonoide sarà quello che avrà come insieme di sostegno l'intersezione di tutte le parti stabili di $\mathbb{N}$ che contengono 2.

Definizione 32. *Data una struttura algebrica* $(s, *)$ *e* $t \subseteq s$ *allora definiamo:*

$$< t >:= \bigcap \{x \in P(s) \mid x \leq s \wedge t \subseteq x\}$$

E diciamo che $< t >$ *è la 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 due di $(\mathbb{N}, +)$ è l'insieme di tutti i valori che si possono ottenere sommando due: $< 2 >= \{2, 4, 6, 8, 10, 12, 14, 16, 18, 20, \ldots\}$.

Procediamo a dimostrare quest'affermazione nel caso dei sottomonoidi e sottogruppi.

Teorema 6.5 (Caratterizzazione di Monoidi Generati)**.** *Dato un monoide* $(s, *, 1_s)$*, se e t suo sottoinsieme non vuoto, allora:*

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

Cioè è l'insieme di tutti gli elementi che si possono ottenere combinando gli elementi di t.

Dimostrazione. Chiamiamo l'insieme a destra b per comodità. Per l'assioma di estensionalità, dimostrare che $< t >= b$ vuol dire dimostrare che si contengono a vicenda.

Caso $\subseteq$) Chiaramente ogni elemento di t è propria combinazione lineare, pertanto $t \subseteq b$. Inoltre, per ogni $x, y \in b$, per costruzione esisteranno $x_1, x_2, ..., x_n \in t$ e $y_1, y_2, \ldots, y_k \in t$ tali che $x = x_1 * x_2 * \ldots * x_n$ e $y = y_1 * y_2 * \ldots * y_n$. Pertanto b è parte stabile e $< t >$ è suo sottoinsieme, essendo l'intersezione di tutte le parti stabili.

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 $b \subseteq < t >$. □

Teorema 6.6 (Caratterizzazione di Gruppi Generati)**.** *Sia $(g, *, 1_s)$ un gruppo e sia t un suo sottoinsieme non vuoto. Allora:*

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

Cioè $< t >$ è l'insieme di tutti gli elementi che si ottengono combinando elementi di t o loro inversi.

Dimostrazione. La dimostrazione è analoga a quella per i monoidi generati. Caso $\subseteq$) Per ogni $x, y \in b$ si ha che essi sono combinazioni lineari di elementi di t o loro inversi, pertanto anche $x * y$ sarà una combinazione lineare e si avrà che $x * y$. Pertanto non solo $t \subset b$ ma b è parte chiusa, quindi $< t > \subseteq b$.

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 $(\forall n \in \mathbb{N})(\forall \varepsilon_1, ...\varepsilon_n \in \{1, -1\})(\forall y_1, ...y_n \in t \subseteq x)(y_1^{\varepsilon_1} * ... * y_n^{\varepsilon_n} \in x) \implies (\forall y \in b)(y \in x) \implies b \subseteq x$. Quindi b è parte di ogni sottostruttura contente t, e dunque parte della loro intersezione, e quindi $b \subseteq < t >$. □

In particolare, se una struttura può essere generato da un suo solo elemento, esso si dice struttura *ciclica*.

Definizione 33 (Struttura Ciclica)**.** $(s, *)$ *struttura ciclica se e soltanto se esiste $x \in s$ tale che $< x >= s$.*

6.6 Cancellabilità

Definizione 34 (Elemento Cancellabile)**.** *Sia $(g, \cdot)$ un gruppo e sia $x_0 \in g$. Allora:*

$$x_0 \text{ cancellabile a sinistra } :\Leftrightarrow (\forall y, z \in g)(xy = xz \implies y = z)$$
$$x_0 \text{ cancellabile a destra } :\Leftrightarrow (\forall y, z \in g)(yx = zx \implies y = z)$$

E si definisce cancellabile se lo è sia a sinistra che a destra.

Un elemento non è cancellabile quando:

$$x_0 \text{ non canc. a sinistra} \iff (\exists x, y \in g)(xy = xz \wedge y \neq z)$$
$$x_0 \text{ non canc. a destra} \iff (\exists x, y \in g)(yx = zx \wedge y \neq z)$$

Teorema 6.7 (Invertibilità implica Cancellabilità)**.** *Dato un gruppo* $(g, \cdot)$*:* $(\forall x)(x \in U(g) \implies x \text{ cancellabile})$

Dimostrazione. $x \in U(g) \implies (\exists \overline{x} \in g)(x \cdot \overline{x} = \overline{x} \cdot x = 1_g)$. Siano allora $(y, z \in g)(xy = xz) \implies y = 1_g \cdot y = \overline{x} \cdot x \cdot y = \overline{x} \cdot x \cdot z = 1_g \cdot z = z$.

Analogamente: $(y, z \in g)(yx = zy) \implies y = y \cdot 1_g = y \cdot x \cdot \overline{x} = z \cdot x \cdot \overline{x} = z \cdot 1_g = z$ □

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

Definizione 35 (Funzioni Traslazione)**.** *Sia* $(s, \cdot)$ *un semigruppo e sia* $x \in s$*. Allora:*

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

Affermiamo senza dimostrazione che:

Una x è cancellabile a sinistra se e solo se la funzione traslazione a sinistra è iniettiva.

Una x è cancellabile a destra se e solo se la funzione traslazione a destra è iniettiva.

6.7 Tavole di Cayley

TODO

6.8 Omomorfismi fra Strutture Algebriche

Definizione 36. *Siano* $(s, *)$ *e* $(\overline{s}, \overline{*})$ *due strutture algebriche. Allora:*

$\varphi : s \to \overline{s}$ *omomorfismo* $\iff (\forall x, y \in s)(\varphi(x * y) = \varphi(x) \overline{*} \varphi(y))$

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:

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

Definizione 37 (Monomorfismo)**.** *Un omomorfismo iniettivo si dice monomorfismo.*

Definizione 38 (Epimorfismo)**.** *Un omomorfismo suriettivo si dice epimorfismo.*

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

Teorema 6.8 (Epimorfismi conservano i Neutri)**.** *Gli epimorfismi conservano gli elementi neutri.*

Dimostrazione. Siano $(s, *)$ e $(\overline{s}, \overline{*})$ strutt. algebriche, $\varphi : s \to \overline{s}$ un'epimorfismo, sia $1_s \in s$ elemento neutro, e sia $y \in \overline{s}$. Essendo la funzione suriettiva, $(\exists x \in s)(\varphi(x) = y)$. Allora: $y\overline{*}\varphi(1_s) = \varphi(x)\overline{*}\varphi(1_s) = \varphi(x * 1_s) = \varphi(x) = y$
quindi $\varphi(1_s)$ è elemento neutro di $(\overline{s}, \overline{*})$ □

Teorema 6.9 (Epimorfismi conservano la Commutatività)**.** *Siano $(s, *)$ e $(\overline{s}, \overline{*})$ strutt. algebriche tale che $*$ è un'operazione commutativa e sia $\varphi : s \to \overline{s}$ un'epimorfismo. Vogliamo dimostrare che anche l'operazione $\overline{*}$ è commutativa.*

Dimostrazione. Siano $y_1, y_2 \in \overline{s}$. Essendo la funzione suriettiva, $(\exists x_1, x_2 \in s)(\varphi(x_1) = y_1 \wedge \varphi(x_2) = y_2)$. Allora: $y_1\overline{*}y_2 = \varphi(x_1)\overline{*}\varphi(x_2) = \varphi(x_1 * x_2) = \varphi(x_2 * x_1) = \varphi(x_2)\overline{*}\varphi(x_1) = y_2\overline{*}y_1$
E dunque l'operazione $\overline{*}$ è commutativa. □

Definizione 39 (Isomorfismo)**.** *Un omomorfismo biettivo si dice isomorfismo.*

Teorema 6.10 (L'Inversa di un Isomorfismo è un Isomorfismo)**.** *Siano $(s, *)$ e $(s', *')$ due strutture algebriche. Se $\varphi : s \to s'$ è un isomorfismo, allora $\varphi^{-1} : s' \to s$ è a sua volta un isomorfismo.*

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

Dimostrazione. Dato che la funzione è biettiva, basta dimostrare che l'inversa è un omomorfismo.
Siano $x, y \in s'$. Essendo $\varphi \circ \varphi^{-1} = id_{s'}$, allora abbiamo che:

$$\begin{aligned}\varphi^{-1}(x *' y) &= \varphi^{-1}(\varphi(\varphi^{-1}(x)) *' \varphi(\varphi^{-1}(y))) \\ &= \varphi^{-1}(\varphi(\varphi^{-1}(x) * \varphi^{-1}(y))) \\ &= \varphi^{-1}(x) * \varphi^{-1}(y)\end{aligned}$$

Che è la tesi. □

Definizione 40 (Automorfismo)**.** *Un isomorfismo il cui dominio è anche il suo codominio si dice automorfismo.*

6.9 Anelli

Fino ad ora abbiamo parlato unicamente di strutture algebriche per cui è definita una singola operazione. Iniziamo adesso a discutere insiemi su cui sono definite due operazioni, partendo dalla definizione di *anello*.

Definizione 41 (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 per $*$ su $\cdot$:*
$(\forall x, y, z \in a)(x \cdot (y + z) = x \cdot y + x \cdot z)$

Definizione 42 (Anello Commutativo)**.** *Se l'operazione $\cdot$ di un anello è commutativa, l'anello si dice anello commutativo.*

Definizione 43 (Anello Unitario)**.** *Se l'operazione $\cdot$ di un anello è dotata di elemento neutro, l'anello si dice anello unitario.*

Dato che in un anello possono esistere due elementi neutri (uno per la prima ed uno per la seconda operazione), indichiamo con 0_a o 0^N l'elemento neutro rispetto all'operazione $+$, e con 1_a o 1^N l'elemento neutro dell'operazione $\cdot$, se esiste.

Definizione 44 (Differenza in un Anello)**.** *Dati due x, y di un anello, allora diremo che $x - y = x + (-y)$*

Per ogni x, y si osserva che $x(-y) = (-x)y = -(xy)$. Da questo segue che il prodotto è distributivo rispetto alla differenza:

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

Definizione 45 (Multipli in un Anello)**.** *Sia x elemento di un anello e $n \in \mathbb{N}$.*
Se $n > 0$, definiamo $nx = n + n + \ldots + n$, n volte.
Inoltre definiamo $(-n)x = -n + (-n) + \ldots + (-n)$, $|n|$ volte.
Se $n = 0$, allora $0n = 0_a$.
Se l'anello è unitario, osserviamo che $(n1_s)x = nx$

Attenzione! In $\mathbb{R}$, per ogni $n \in \mathbb{Z}$ e per ogni x reale si ha che $nx = n \cdot x$. Questo non è vero per ogni anello! Ricordiamo che l'operazione $\cdot$ dell'anello è binaria interna, e quindi per $\mathbb{R}$ funziona in questo modo perché $n \in \mathbb{Z} \implies n \in \mathbb{R}$.

Teorema 6.11 (Prodotto per Zero è Zero)**.** *Dato un anello $(a, +, \cdot)$ vogliamo dimostrare che $\forall x \in a, 0_a \cdot x = x \cdot 0_a = 0_a$*

Dimostrazione. Sia $x \in a$. Allora $0_a \cdot x = (x - x)x = xx - xx = 0_a$.
Equivalentemente $x \cdot 0_a = x(x - x) = xx - xx = 0_a$ □

Definizione 46 (Potenze in un Anello)**.** *Sia $x \in a$ elemento di un anello e sia $n \in \mathbb{N}$.*
Se $n > 0$, definiamo $x^n = x \cdot x \cdot x \cdot \cdot x$, n volte.
Inoltre definiamo $x^{-n} = x^{-1} \cdot x^{-1} \cdot \ldots \cdot x^{-1}$, n volte.
Se $n = 0$ e l'anello è unitario, definiamo $x^0 = 1_a$.

6.9.1 Domini di Integrità e Divisori dello Zero

Definizione 47 (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:*

$$(\forall x, y \in a)(x \cdot y = 0_a \implies (x = 0_a \vee y = 0_a))$$

Definizione 48 (Anello Integro)**.** *Un anello in cui vale la legge di annullamento del prodotto si dice anello integro.*

Definizione 49 (Dominio di Integrità)**.** *Un anello unitario integro si dice dominio di integrità.*

Definizione 50 (Divisore dello Zero)**.** *Sia* $(a, +, \cdot)$ *un anello. Allora:*

$$x \in a - \{0_a\} \text{ divisore sinistro dello zero } :\Leftrightarrow (\exists y \in a - \{0_a\})(xy = 0_a)$$
$$x \in a - \{0_a\} \text{ divisore destro dello zero } :\Leftrightarrow (\exists y \in a - \{0_a\})(yx = 0_a)$$

Un elemento divisore sinistro e destro si dice semplicemente divisore dello zero.

Teorema 6.12 (Divisori sono Non-Cancellabili)**.** *Sia* $(a, +, \cdot)$ *un anello. Allora:*

$$x \in a \text{ divisore a sinistra dello zero} \iff x \text{ non cancellabile a sinistra}$$
$$x \in a \text{ divisore a destra dello zero} \iff x \text{ non cancellabile a destra}$$

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

Teorema 6.13 (Anelli Commutativi Unitari e Domini di Integrità)**.** *Sia* $(a, +, \cdot)$ *un anello commutativo unitario. Allora:*

è dominio di integrità $\iff$ *è privo di divisori dello zero.*

Dimostrazione. $\Rightarrow$) 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. □

6.9.2 Corpi e Campi

Definizione 51 (Corpo)**.** *Un anello si dice corpo se* $(a - \{0_a\}, \cdot)$ *è un gruppo, cioè esiste l'unità e ogni elemento dell'anello eccetto lo zero è dotato di inverso.*

Definizione 52 (Campo)**.** *Un corpo commutativo si dice campo.*

Teorema 6.14 (Ogni Campo è Dominio di Integrità)**.**

Dimostrazione. 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. □

7 Relazioni Binarie

Abbiamo già introdotto il concetto di *relazione binaria* nella sezione sulle corrispondenze. 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 relazioni binarie. Andiamo ora a definire le più fondamentali.

Data una relazione binaria $\rho = (a \times a, g)$, diremo che:

Definizione 53 (Riflessività)**.** ρ *riflessiva* $:\Leftrightarrow (\forall x \in a)(x\rho x)$

Definizione 54 (Antiriflessività)**.** ρ *antiriflessiva* $:\Leftrightarrow (\forall x \in a)(\neg(x\rho x))$

Definizione 55 (Simmetria)**.** ρ *simmetrica* $:\Leftrightarrow (\forall x, y \in a)(x\rho y \implies y\rho x)$

Definizione 56 (Asimmetria)**.** ρ *asimmetrica* $:\Leftrightarrow (\forall x, y \in a)(x\rho y \wedge y\rho x \implies x = y)$

Definizione 57 (Transitività)**.** ρ *transitiva* $:\Leftrightarrow (\forall x, y, z \in a)(x\rho y \wedge y\rho z \implies x\rho z)$

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

Definizione 58 (Relazione d'Equivalenza)**.** *Una relazione riflessiva, simmetrica e transitiva si dice relazione di equivalenza.*

Definizione 59 (Relazione d'Ordine)**.** *Una relazione asimmetrica e transitiva si dice relazione d'ordine.*

Definizione 60 (Relazione d'Ordine Largo)**.** *Se una relazione d'ordine è riflessiva, si dice relazione di ordine largo.*

Definizione 61 (Relazione d'Ordine Stretto)**.** *Se una relazione d'ordine è antiriflessiva, si dice relazione di ordine stretto.*

Notiamo con $EQ(x)$ l'insieme di tutte le relazioni di equivalenza definibili su un insieme x. Si osserva che la relazione che ha come grafico $g = a \times a$ (cioè la relazione che mette ogni elemento in relazione con ogni altro elemento) è una relazione d'ordine e si dice *relazione d'ordine universale.*

Infine, da ogni relazione si può definire la sua relazione "opposta", che chiamiamo *duale.*

Definizione 62 (Relazione Duale)**.** *Data una relazione binaria ρ su un insieme a, definiamo la relazione duale:*

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

7.1 Congruenze di Modulo m

Definizione 63 (Congruenza di Modulo m)**.** *Dato $m \in \mathbb{Z}$ una congruenza di modulo m è la congruenza*

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

tale che:

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

Teorema 7.1 (Congruenze sono Equivalenze)**.** *Ogni congruenza $\equiv_m$ è una relazione d'equivalenza.*

Dimostrazione. Siano $x, y, z \in \mathbb{Z}$. Allora:

Riflessività: $x - x = 0 = 0m$, quindi $x \equiv_m x$.

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

Transività: $x \equiv_m y \land y \equiv_m x \implies (\exists k_1, k_2 \in \mathbb{Z})(x - y = k_1 m \land y - z = k_2 m \implies (x - y) + (y - z) = x - z = (k_1 + k_2)m)$ $\square$

Due congruenze sono notabili:

La relazione di modulo 0 è la relazione di uguaglianza in quanto $a \equiv_0 b \iff a - b = 0 \iff a = b$.

l'equivalenza di modulo uno è la relazione universale in quanto $(a - b) = 1 \cdot (a - b)$.

7.2 Nucleo di Equivalenza

Definizione 64 (Nucleo di Equivalenza)**.** *Data una funzione $f : a \to b$, definiamo la relazione nucleo di equivalenza la relazione di equivalenza $KER_f := (a \times a, g)$ che fa equivalere elementi con la stessa immagine:*

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

Notiamo tale relazione anche $\sim_f$

Il nucleo di equivalenza è dunque la relazione che mette in

7.3 Classi di Equivalenza

Le relazioni di equivalenza godono, per definizione, della proprietà transitiva. Questo vuol dire che, dato un insieme su cui è definita una relazione di equivalenza, possiamo separare i suoi elementi in sottoinsiemi di elementi equivalenti. Chiamiamo questi sottoinsiemi *classi di equivalenza.*

Definizione 65 (Classe di Equivalenza)**.** *Sia s un insieme su cui è definita una relazione di equivalenza ρ e 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

Definizione 66 (Rappresentante di una Classe di Equivalenza)**.** *Data una classe di resto $[x]_\rho$, diciamo x il rappresentante della classe di resto.*

Definizione 67 (Classe di Resto)**.** *Le classi di equivalenza di una congruenza si dicono classi di resto e si notano per brevità usando solamente il modulo:*

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

Definizione 68 (Insieme Quoziente)**.** *Dato un insieme s ed una relazione d'equivalenza ρ, l'insieme di tutte le classi di equivalenza per ρ:*

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

si dice insieme quoziente di s rispetto a ρ.

7.3.1 Proprietà Fondamentali delle Classi Di Equivalenza

Sia s un insieme su cui è definita una classe di equivalenza ρ, allora le classi di equivalenza di ρ godono delle seguenti *proprietà fondamentali*:

Teorema 7.2 (1ˆ Proprietà Fondamentale delle Classi di Equivalenza)**.** *Una classe di equivalenza ha sempre almeno un elemento (non esistono, cioè, classi di equivalenza vuote).*

Dimostrazione. Per la riflessività $(\forall x \in s)(x\rho x \implies x \in [x]_\rho)$. □

Teorema 7.3 (2ˆ Proprietà Fondamentale delle Classi di Equivalenza)**.** *Due classi di equivalenza o coincidono o non hanno alcun elemento in comune.*

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

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

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

□

Teorema 7.4 (3ˆ Proprietà Fondamentale delle Classi di Equivalenza)**.** *L'unione di tutte le classi di equivalenza, cioè l'unione unaria dell'insieme quoziente di s, è proprio s.*

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

Dimostrazione. $\subseteq$) $y \in \bigcup s/\rho \implies (\exists [x]_\rho \in s/\rho)(y \in [x]_\rho) \implies y \in s$
$\supseteq$) $y \in s \implies [y]_\rho \in s/\rho \wedge y \in [y]_\rho \implies y \in \bigcup s/\rho$
E dunque $\bigcup s/\rho = s$. □

7.3.2 Proiezione Canonica

Definizione 69 (Proiezione Canonica)**.** *Dato un insieme s su cui è definita una relazione d'equivalenza ρ, diciamo proiezione canonica la funzione che associa ad ogni elemento la propria classe di equivalenza.*

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

Teorema 7.5 (Suriettività della Proiezione Canonica)**.**

Dimostrazione. Data una classe di equivalenza, per la prima proprietà fondamentale essa sarà non vuota. Ogni suo elemento l'avrà come immagine, e pertanto la funzione proiezione canonica è suriettiva. □

7.4 Teorema Fondamentale di Omomorfismo per Insiemi

TODO

7.5 Partizioni

Definizione 70 (Definizione di 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) $\bigcup f = a$

Segue che ogni insieme è dotato di due partizioni banali, sé stesso e l'insieme di tutti i suoi singleton. Inoltre, si può verificare che per ogni relazione d'equivalenza ρ l'insieme quoziente x/ρ è una partizione.

Notiamo con $PART(x)$ l'insieme di tutte le partizioni definibili su un insieme x.

Teorema 7.6 (Teorema Fondamentale su Relazioni di Equivalenza e Partizioni)**.** *Per ogni insieme a, esiste una 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.

Dimostrazione. Dimostriamo che f è iniettiva. Prendiamo $\sim_1, \sim_2 \in EQ(a)$ tale che $f(\sim_1) = f(\sim_2)$ ovvero $a/\sim_1 = a/\sim_2$.

Allora:

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

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

Dimostriamo che f è suriettiva. Sia $p \in PART(a)$ e la relazione $\sim$: $(\forall x, y \in a)(x \sim y \iff ((\exists z \in p)(x \in p \wedge y \in p)))$. Vogliamo dimostrare che $\sim$ è una relazione di equivalenza, e cioè che gode della proprietà riflessiva, simmetrica, e transitiva.

1) Chiaramente $(\forall x \in a)(\exists z \in p)(x \in z \wedge x \in z)$, quindi la relazione è riflessiva.

2) $(\forall x, y \in a)(\exists z \in p)((x \in z \wedge y \in z) \iff (y \in z \wedge x \in z))$ per la commutatività di $\wedge$ e dunque la relazione è simmetrica.

3) Presi $x, y, z \in a$ tale che $x \sim y \sim z$, allora $(\exists w_1, w_2 \in p)((x \in w_1 \wedge y \in w_1) \wedge (y \in w_2 \wedge z \in w_2) \implies w_1 \cap w_2 \neq \emptyset \implies w_1 = w_2)$ in quanto p è una partizione. Pertanto x e z fanno parte dello stesso insieme e sono equivalenti, quindi la relazione è transitiva.

Pertanto, per ogni partizione esiste un'associata relazione di equivalenza, e pertanto f è suriettiva e biettiva. □

7.6 Teorema Fondamentale dell'Aritmetica

Prima di dimostrare il Teorema Fondamentale dell'Aritmetica, è necessario dimostrare una serie di affermazioni i cui risultati useremo nelle dimostrazioni delle sue due testi.

Teorema 7.7 (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 è solo divisibile dalle unità, sé stesso, ed il proprio opposto.

Dimostrazione. Sia $n \in \mathbb{Z}$ tale che $n|p \iff (\exists k \in \mathbb{Z})(nk = p) \implies p|n \vee p|k$ per la definizione di primo.

Nel caso $p|n \iff (\exists h \in \mathbb{Z})(ph = n) \implies phk = p \implies hk = 1$. Allora $h = k = 1 \vee h = k = -1 \implies n = \pm p$.

Nel caso $p|k \iff (\exists h \in \mathbb{Z})(ph = k) \implies nph = p \implies nh = 1$. Allora $n = h = 1 \vee n = h = -1 \implies n = \pm 1$.

Abbiamo quindi la tesi. □

Teorema 7.8 (2° Lemma per il Teorema Fondamentale dell'Aritmetica)**.** *Siano $a, b \in \mathbb{N} - \{0\}$ e sia $x = \{n \in \mathbb{N} - \{0\} \mid a|nb\}$.*

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

Dimostrazione. 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 $m = min(x)$ per convenienza. Essendo $z, m \in x \implies a|zb \wedge a|mb \implies (\exists h, k \in \mathbb{N})(zb = ah \wedge mb = ak)$ Dunque $(z - m)b = zb - mb = ah - ak = a(h - k) \implies a|(z - m)b$

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 $m|(z - m) \iff (\exists l)(z - m = ml) \implies z = m(l + 1) \implies m|z$ che è assurdo. □

Teorema 7.9 (Lemma sui Divisori dei Non Primi)**.** *Ogni $m \in \mathbb{Z}$ non primo ha divisori oltre $\pm 1, \pm m$,*

Dimostrazione. $m \in \mathbb{N}$ non primo $\iff (\exists h, k)(m|hk \wedge m \nmid h \wedge m \nmid k)$ 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 $x = \{n \in \mathbb{N} - \{0\} \mid m|nk\}$ e sia $s = min(x)$. Dato che

$h, m \in x$, per il Secondo Lemma, $s|h \wedge s|m$, ma per ipotesi di assurdo solo 1 ed m sono divisori, quindi $s = 1 \vee s = m$. Se $s = 1 \implies m|1k$ che va contro l'ipotesi. Se $s = m \implies m|h$ che va contro l'ipotesi. In entrambi I casi abbiamo l'assurdo e quindi $m \in \mathbb{N}$ ha almeno un terzo divisore.

Quindi, se $m \in \mathbb{N}$ ha divisori oltre $1, m$ allora $m \in \mathbb{Z}$ ha divisori oltre $\pm 1, \pm m$. □

Teorema 7.10 (2 è Primo)**.**

Dimostrazione. 2 è primo se e solo se per ogni $a, b \in N, 2|ab \implies 2|a \vee 2|b$. Supponiamo che $2 \nmid a$ (2 non divide a), dimostriamo che divide b. $2|ab \wedge 2 \nmid a \implies (\exists k \in \mathbb{N})(2k = ab) \wedge (\exists h \in \mathbb{N})(a = 2h + 1) \implies 2k = 2hb + b$ E dunque $b = 2k - 2hb \implies b = 2(k - hb) \implies 2|b$ che è la tesi. □

Possiamo ora procedere con la dimostrazione di entrambe le tesi del Teorema Fondamentale dell'Aritmetica

Teorema 7.11 (1ˆ Tesi del Teorema Fondamentale dell'Aritmetica)**.** *Sia* $m \in \mathbb{Z} - \{-1, 0, 1\}$*, allora* $\exists p_1, p_2, ..., p_n \in \mathbb{Z}$ *primi tali che* $m = p_1 \cdot p_2 \cdot ... \cdot p_n$*.*

Dimostrazione. Dimostriamo tramite Principio di Induzione in Seconda forma, considerando $m \in \mathbb{N}$.

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, $(\exists a, b \in \mathbb{N} - \{0, 1, m\})(m = ab)$ e quindi si ha che $1 < a, b < m$. Quindi, per ipotesi induttiva: $(\exists t, u \in \mathbb{N})(\exists p_1, ..., p_t, p_{t+1}, ..., p_{t+u} \in \mathbb{N})(a = p_1 \cdot ... \cdot p_t \wedge b = p_{t+1} \cdot ...p_{t+u})$

E dunque $m = a \cdot b = p_1 \cdot ... \cdot p_t \cdot p_{t+1} \cdot ... \cdot p_{t+u}$ e la tesi induttiva è dimostrata, e dunque essa vale $(\forall n \in \mathbb{N})(n \geq 2)$.

Consideriamo $m \in \mathbb{Z} - \mathbb{N}$. Allora $-m \in \mathbb{N}$ e vale per esso la tesi: $(\exists p_1, ..., p_r)(-m = p_1 \cdot ... \cdot p_r) \implies m = -(p_1 \cdot ... \cdot p_r) = -p_1 \cdot ... \cdot -p_r$ Dato che l'opposto di un numero primo è ancora un numero primo, allora la tesi vale in tutto $\mathbb{Z}$. □

Teorema 7.12 (2ˆ Tesi del Teorema Fondamentale dell'Aritmetica)**.** *Se* $m = q_1 \cdot ... \cdot q_n$*, allora* $r = s$ *ed* $\exists f : \{1, .., r\} \to \{1, ..., r\}$ *biettiva tale che* $(\forall i \in \{1, ..., r\})(p_i = q_{f(i)})$

Dimostrazione. Dimostriamo per Principio di Induzione di Prima Forma.

Caso base: $r = 1$. Sia $p_1 = m = q_1 \cdot ... \cdot q_s$. Quindi m è primo, e quindi $(\forall q \in \{q_1, ..., q_s\})(q|m \implies q \in \{-1, 1, -m, m\}) \implies r = s = 1 \wedge q_1 = p_1$

Ipotizziamo ora la tesi sia vera per $r - 1$. Dimostriamo che è vera per r. Abbiamo che $p_1 \cdot p_2 \cdot ... \cdot p_r = m = q_1 \cdot q_2 \cdot ... \cdot q_r$. Allora, $p_1|q_1 \cdot q_2 \cdot ... \cdot q_r$ e per la definizione di primo allora $p_1|q_1 \vee p_1|q_2 \cdot ... \cdot q_r$. Ancora una volta, per la definizione di primo, $p_1|q_2 \vee p_1|q_3 \cdot ... \cdot q_r$ e così via. Dunque, si ha che $p_1|q_1 \vee p_1|q_2 \vee ... \vee p_1|q_s$.

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: $p_1 \cdot p_2 \cdot ... \cdot p_r = (\pm p_1) \cdot q_2 \cdot ... \cdot q_s$
E dunque, cancellando p_1 da entrambi i membri: $p_2 \cdot ... \cdot p_r = \pm q_2 \cdot ... \cdot q_s$
Siamo dunque nel caso $r-1$ e quindi vale in esso la tesi induttiva, cioè $r-1 = s-1 \wedge (\exists \sigma : \{2,...,r\} \to \{2,...,r\}$ 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. □

7.7 Relazioni d'Ordine

Sia $a \neq \emptyset$. Allora definiamo gli insiemi:

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

Potremmo chiederci perché le relazioni d'ordine appartengono all'insieme $P(P(P(a \times a)))$ (cioè l'insieme delle parti delle parti delle parti di $a \times a$).

Vediamo:

Dimostrazione. 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:
$\{\{a \times a\}, \{a \times a, g\}\} \in P(P(P(a \times a)))$ □

Se $\rho \in OL(a)$, definisco $\rho^\wedge :\Leftrightarrow (\forall x, y \in a)(x \rho^\wedge y \iff (x \rho y \wedge x \neq y))$
Se $\rho \in OS(a)$, definisco $\rho^\vee :\Leftrightarrow (\forall x, y \in a)(x \rho^\vee y \iff (x \rho y \vee x = y))$
E dichiariamo senza dimostrazione che:

Teorema 7.13 (Ordine Largo da Ordine Stretto e Viceversa)**.** *La funzione $f : \rho \in OL(a) \mapsto \rho^\wedge \in OS(a)$ 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.

Definizione 71 (Insieme Ordinato)**.** *Sia $s \neq \emptyset$ e sia ρ una relazione d'ordine su s. La coppia (s, ρ) si dice insieme ordinato.*

Definizione 72 (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:*

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

Definizione 73 (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)*.*

Definizione 74 (Elementi Confrontabili)**.** *Dato un insieme ordinato* (s, ρ)*, due elementi* $x, y \in s$ *si dicono confrontabili* $:\Leftrightarrow x\rho y \vee y\rho x$*.*

Definizione 75 (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.*

Definizione 76 (Minimo e Massimo di un Insieme Ordinato)**.** *Dato un insieme ordinato* (s, ρ) *allora:*
$m \in s$ *massimo di* $s :\Leftrightarrow (\forall x \in s)(x\rho m)$
$m \in s$ *minimo di* $s :\Leftrightarrow (\forall x \in s)(m\rho x)$

Definizione 77 (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.*

Esempio. Facciamo un esempio per contestualizzare le definizioni appena introdotte. Consideriamo l'insieme ordinato $(\mathbb{N}, \leq)$. $\leq$ è una relazione d'ordine largo e $<$ è la sua corrispondente relazione d'ordine stretto.

Tutti gli elementi di tale insieme ordinato sono a due a due confrontabili, in quanto per ogni coppia di valori $x, y \in \mathbb{N}$ si deve avere o che $x \leq y$ o che $y \leq x$, dato che per ogni coppia di numeri si può sempre dire qual è più piccolo dell'altro.

Lo 0 è chiaramente il minimo dell'insieme in quanto $(\forall x \in \mathbb{N})(0 \leq x)$.

Inoltre, non importa quale sottoinsieme non vuoto di $\mathbb{N}$ scegliamo, possiamo sempre identificare un minimo, pertanto è un insieme ben ordinato. Contrastiamo invece, l'insieme $(\mathbb{R}, \leq)$. Tale insieme non è ben ordinato in quanto, per esempio, il sottoinsieme $\{x \in \mathbb{R} \mid x > 0\}$ non è dotato di minimo (banalmente, per ogni $x > 0$, esisterà $\frac{x}{2}$ che sarà ancora parte dell'insieme, pertanto non esiste elemento "più piccolo" di tutti gli altri).

Teorema 7.14 (Unicità di Minimo e Massimo)**.** *Se esiste minimo e/o massimo in un insieme ordinato* (s, ρ) *allora essi sono unici.*

Dimostrazione. Dimostriamo per il minimo, il caso del massimo è del tutto analogo. Siano $m_1, m_2 \in s$ minimi di s. Allora per definizione:

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

Per l'asimmetria di ρ, allora $m_1 = m_2$. □

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

Teorema 7.15 (Buon Ordine implica Ordine Totale)**.** *Se* s, ρ *è un insieme ben ordinato, allora esso è anche totalmente ordinato.*

Dimostrazione.

$$(\forall x, y \in s)((\exists n \in \{x, y\})(n = min(\{x, y\})) \implies n = x \vee n = y \implies x\rho y \vee y\rho x)$$

□

7.8 Relazioni di Copertura e Diagrammi di Hasse

Definizione 78. *Dato un insieme ordinato e (s, ρ) e due elementi $x, y \in s$ diremo che:*

$$y \ COPRE \ x :\Leftrightarrow (x\rho y) \wedge ((\nexists z \in s)(z \neq x \wedge z \neq y \wedge x\rho z \wedge z\rho y))$$

Cioè se non esiste un elemento z distinto da essi che è compreso fra di essi.

Definizione 79 (Predecessore e Successore Immediato)**.** *Se x copre y, diremo che x è successore immediato di y e y è predecessore immediato di x.*

Definizione 80 (Diagramma di Hasse)**.** *Dato un insieme ordinato (s, ρ) definiremo il suo diagramma di Hasse la coppia $(s \times s, g)$ tale che $(\forall x, y \in s)((x, y) \in g \iff y \ COPRE \ x)$*

Il diagramma di Hasse è quindi la relazione duale alla copertura.

I diagrammi di Hasse sono importanti per via della loro rappresentazione grafica. Per rappresentare graficamente un diagramma di Hasse assegneremo 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.

Si nota che se un insieme è ben ordinato, il suo diagramma di Hasse è una "linea", ed è per questo che insiemi ben ordinati si dicono anche catene.

TODO

7.9 Applicazioni fra Insiemi Ordinati

Definizione 81 (Funzione Crescente)**.** *Dati due insiemi ordinati (s, ρ) e $(\overline{s}, \overline{\rho})$, diremo che la funzione $f : s \to \overline{s}$ è crescente $:\Leftrightarrow (\forall x, y \in s)(x\rho y \implies f(x)\overline{\rho}f(y))$*

Definizione 82 (Isomorfismo di Insiemi Ordinati)**.** *Dati due insiemi ordinati (s, ρ) e $(\overline{s}, \overline{\rho})$, diremo che la funzione $f : s \to \overline{s}$ è isomorfismo $:\Leftrightarrow (\forall x, y \in s)(x\rho y \iff f(x)\overline{\rho}f(y))$*

Teorema 7.16 (Insiemi Ordinati Finiti sono Isomorfi solo se hanno lo stesso Diagramma di Hasse)**.** *todo*

7.10 Minoranti e Maggioranti

Definizione 83 (Massimali e Minimali)**.** *Dato un insieme ordinato (s, ρ) e un suo sottoinsieme ordinato $t \subseteq s$, diremo che:*

$m \in s$ massimale di $t :\Leftrightarrow (\forall x \in t)((x\rho m \vee m\rho x) \implies x\rho m)$

$m \in s$ *minimale di* $t :\Leftrightarrow (\forall x \in t)((x\rho m \vee m\rho x) \implies m\rho x)$

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

Definizione 84 (Maggioranti e Minoranti)**.** *Dato un insieme ordinato* (s, ρ) *e un suo sottoinsieme ordinato* $t \subseteq s$*, diremo che:*

$m \in s$ *maggiorante di* $t :\Leftrightarrow (\forall x \in t)(x\rho m)$

$m \in s$ *minorante di* $t :\Leftrightarrow (\forall x \in t)(m\rho x)$

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

Si osserva dunque che:

Ogni massimo è un maggiorante. Ogni maggiorante è un massimale.

Ogni minimo è un minorante. Ogni minorante è un minimale.

Scriveremo come segue:

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

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

Definizione 85 (Insieme Limitato)**.** *Sia* (s, ρ) *un insieme ordinato e* $t \subseteq s$*. Allora:*

t *è limitato inferiormente* $:\Leftrightarrow MINOR_{(s,\rho)}(t) \neq \emptyset$

t *è limitato superiormente* $:\Leftrightarrow MAGGIOR_{(s,\rho)}(t) \neq \emptyset$

Cioè se è dotato di minorante e/o maggiorante.

Definizione 86 (Insieme Naturalmente Ordinato)**.** (s, ρ) *insieme ordinato naturalmente ordinato* $:\Leftrightarrow$ *è ben ordinato e ogni sua parte non vuota superiormente limitata ha massimo.*

Teorema 7.17 (Buon Ordine implica Ordine Largo)**.**

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

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

7.11 Principio d'Induzione

Sia $x \subseteq \mathbb{N} - \{\emptyset\}$. Allora:

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

Avendo introdotto tale notazione, passiamo ad esporre il Principio di Induzione.

Teorema 7.18 (Prima Forma del Principio di Induzione)**.**

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

Dimostrazione. 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 perché $y \subseteq \mathbb{N}$.

$m < n$ 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. □

Teorema 7.19 (Seconda Forma del Principio di Induzione)**.**

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

Dimostrazione. 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. □

8 Cenni di Calcolo Combinatorio

Il calcolo combinatorio è la branca della matematica che studia i modi in cui raggruppare e combinare elementi di un insieme. In particolare, ha come obiettivo quello di determinare il numero di tali combinazioni.

8.1 Insiemi Finiti e Infiniti

L'assioma dell'infinito ci assicura l'esistenza di un insieme che è, appunto, infinito, ma ci rimane di definire cosa vuol dire per ogni altro insieme essere infinito o non infinito. Diciamo dunque che:

Definizione 87 (Equipotenza)**.** *Due insiemi a e b si dicono equipotenti se esiste una biezione $f : a \to b$.*

Definizione 88 (Insieme Finito)**.** *Un insieme si dice finito se $n \in \mathbb{N}$ tale che l'insieme è equipotente all'insieme $\{1, 2, \ldots, n\} \subseteq \mathbb{N}$.*

Definizione 89 (Cardinalità di un Insieme)**.** *Sia a un insieme finito, cioè equipotente ad un certo $\{1, 2, \ldots, n\} \subseteq \mathbb{N}$. Allora diremo n la cardinalità di a e scriveremo $|a| = n$.*

Definizione 90 (Insieme Infinito)**.** *Un insieme si dice infinito se esiste una sua biezione fra sé stesso ed una sua parte propria.*

La cardinalità di un insieme è dunque i numero di elementi contenuti in esso. E' da non confondersi col valore assoluto. La notazione è la stessa, ma il valore assoluto di applica a numeri, mentre la cardinalità ad insiemi.

Teorema 8.1 (Cardinalità dell'Insieme delle Parti)**.** *s insieme finito* $\implies |P(s)| = 2^{|s|}$

Dimostrazione. 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 $n + 1$.

$|s| = n + 1 \implies s \neq \emptyset \wedge \exists f : s \to \{1, 2, ..., n, n + 1\}$ 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 $f_{|t} : t \to Im_{f_{|t}} = \{1, 2, ..., m - 1, m + 1, ..., n, n + 1\}$ 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 parti distinte. 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 $\forall n \in \mathbb{N}$. □

8.2 Numero di Applicazioni fra Insiemi Finiti

Definizione 91 (Fattoriale)**.** *Definiamo:*

$$0! = 1$$

E, ricorsivamente:

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

Cioè $1! = 1, 2! = 2, 3! = 6, 4! = 12, \ldots$

Teorema 8.2 (Numero di Applicazioni fra due Insiemi Finiti)**.** *Siano a, b due insiemi finiti. Allora esistono $|b|^{|a|}$ applicazioni $f : a \to b$.*

Dimostrazione. Poniamo $|a| = m, |b| = n$. Usiamo la Prima Forma del Principio di Induzione su m.

Consideriamo $m = 0$ 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 $m > 0$, dimostriamo che vale per $m+1$. Sia $x \in a$ e $t = a - \{x\}$. Per ipotesi induttiva, esistono n^m applicazioni da $t \to b$. Ognuna di queste funzioni potrebbe essere prolungata, associando x ad uno qualsiasi degli n elementi di b. Pertanto per ogni funzione esistono m possibili prolungamenti, e quindi il numero totale di applicazioni è $n^m \cdot n = n^{m+1}$ che è la tesi. □

Teorema 8.3 (Condizione di Esistenza di Applicazioni Iniettive fra Insiemi Finiti)**.**

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

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

Dimostrazione. Poniamo $m = |a|, n = |b|$.

$\Rightarrow$) Esiste una biezione $I_m \to a$, almeno una funzione $f \in MAP_{IN}(a, b)$, e una biezione $b \to I_n$. Pertanto, la loro composizione è una funzione iniettiva da $I_m \to I_n$. Pertanto, $m \leq n$ in quanto per ognuno degli m-esimi elementi deve esistere almeno un elemento distinto in I_n.

$\Leftarrow$)Se $m \leq n$, allora $\{1, ..., m\} \subseteq \{1, ..., n\}$ ed esiste quindi la funzione immersione fra i due, che è una funzione iniettiva. Esiste dunque una biezione da $a \to \{1, ..., m\}$, una funzione iniettiva (l'immersione) da $\{1, ..., m\} \to \{1, ..., n\}$ ed una biezione da $\{1, ..., n\} \to b$ e dunque esiste una funzione iniettiva $a \to b$. □

Teorema 8.4 (Numero di Applicazioni Iniettive fra Insiemi Finiti)**.**

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

Cioè, se esistono applicazioni iniettive, il loro numero può essere calculato attraverso tale formula.

Dimostrazione. Poniamo $|a| = m, |b| = n$, $m \leq n$ altrimenti non esisterebbero applicazioni iniettive. Dimostriamo per Induzione di Prima Forma su m.

Caso base: $m = 0$. 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 $\frac{n!}{(n-0)!} = 1$ la tesi è valida.

Ipotizziamo dunque che la tesi sia valida anche per $\forall(m-1) > 0$, e dimostriamo che è valida in m. Siano $x \in a, t = a - \{x\}$. Dunque $|t| = m - 1$ ed esistono $\frac{n!}{(n-(m-1))!}$ applicazioni iniettive $t \to b$ per ipotesi induttiva. Ognuna di queste può essere prolungata ad a associando x ad uno qualsiasi degli $n - (m-1)$ elementi rimasti in b (dato che dobbiamo scegliere, per lasciare la funzione iniettiva, un'immagine distinta).

Da ciò segue che esistono $\frac{n!}{(n-(m-1))!} \cdot (n - (m-1))$ funzioni iniettive, e sviluppando:

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

Che è la tesi. Dunque per Principio di Induzione la tesi è valida per ogni $n \in \mathbb{N}$. □

Teorema 8.5 (Condizione di Esistenza di Applicazioni Suriettive fra 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.

Dimostrazione. Sia $|a| = m, |b| = n$.

$\Rightarrow$) Sia $f : a \to b$ suriettiva. Allora esiste una biezione fra $a \to \{1, ..., m\}$, una funzione suriettiva $a \to b$, ed una biezione $b \to \{1, ..., n\}$. Pertanto esiste una funzione suriettiva $\{1, ..., m\} \to \{1, ..., n\}$. Allora per ogni elemento del secondo insieme esiste un elemento distinto (dalla definizione di applicazione) del primo insieme, pertanto $n \leq m$.

$\Leftarrow$) Se sono entrambi non vuoti e $n \leq m \implies I_n$, 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. □

Teorema 8.6 (Condizione di Esistenza di Applicazioni Biettive fra Insiemi Finiti)**.**

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

Esistono biezioni fra due insiemi finiti se e solo se questi hanno identica cardinalità.

Dimostrazione. Segue dalle condizioni di esistenza di applicazioni iniettive e suriettive. □

Teorema 8.7. *Siano a, b insiemi e $f : a \to b$ una funzione. Allora:*

$$|a| = |b| \implies (f \text{ iniettiva} \iff f \text{ suriettiva} \iff f \text{ biettiva})$$

Dimostrazione. Poniamo $|a| = |b| = m$.

Se $f : a \to b$ è una funzione iniettiva, la sua immagine ha $|m|$ elementi. Ma $Imf \subseteq b \wedge |Imf| = |b| = m$ 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. □

Dal teorema precedente segue che:

Teorema 8.8 (Cardinalità dell'Insieme Simmetrico di un Insieme Finito)**.**

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

Dimostrazione. 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:

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

□

Teorema 8.9 (Cancellabilità e Invertibilità in un Monoide Commutativo Finito)**.** *Sia $(s, \cdot)$ un monoide commutativo finito e sia $x \in s$. Allora x è invertibile se e solo se è cancellabile.*

Dimostrazione. Abbiamo già dimostrato che l'invertibilità implica la cancellabilità, pertanto basta dimostrare l'implicazione opposta. Se x è cancellabile, allora σ_x e δ_x sono iniettive, ma essendo s finito, allora esse sono anche biettive, 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. □

Da questo teorema segue che:
Corollario. Anelli Unitari Integri finiti sono Corpi.
Corollario. Domini d'Integrità finiti sono Campi.

8.3 Funzioni Caratteristiche

Definizione 92 (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.

Abbiamo già usato la notazione $MAP(a, b)$ per indicare l'insieme di funzioni definibili fra due insiemi a e b. Per brevità, possiamo indicare tale insieme anche come b^a. Si osserva dunque che le funzioni caratteristiche formano l'insieme $\{0, 1\}^s$

Teorema 8.10 (Ogni Sottoinsieme è dotato di Funzione Caratteristica)**.** *La funzione*

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

è biettiva. Cioè, esiste una corrispondenza biunivoca fra le parti di un insieme e le funzioni $\{0, 1\}^s$. Cioè, ogni sottoinsieme è dotato di funzione caratteristica e ogni funzione del tipo $f : x \in s \to \{0, 1\}$ è funzione caratteristica di un qualche sottoinsieme di s.

Dimostrazione. 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 $\chi_{t,s}(x) = 1$ e $\chi_{v,s} = 0$ quindi le funzioni sono distinte e φ è iniettiva. □

8.4 Coefficienti Binomiali

Definizione 93 (Coefficiente Binomiale)**.** $\forall n, k \in \mathbb{N}$ *definiamo:*

$$\binom{n}{k} = |P_k(I_n)|$$

Se $n < k$, allora $\binom{n}{k} = 0$

Teorema 8.11 (Sommatoria di Coefficienti Binomiali)**.**

$$(\forall n \in \mathbb{N})(\sum_{k=0}^{n} \binom{n}{k} = 2^n)$$

Dimostrazione. 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:

$$|P(I_n)| = |P_0(I_n)| \cup |P_1(I_n)| \cup ... \cup |P_n(I_n)| = \sum_{k=0}^{n} \binom{n}{k} = 2^n$$

□

Teorema 8.12 (Equivalenza di Coefficienti Binomiali)**.**

$$(\forall n, k \in \mathbb{N})(k \leq n \implies \binom{n}{k} = \binom{n}{n-k})$$

Dimostrazione. Sia $f : x \in P(I_n) \mapsto I_n - x \in P(I_n)$. f è biettiva perché la funzione differenza di insiemi è biettiva. Inoltre, ovviamente, se $|I_n| = n, |x| = k \implies |I_n - x| = n - k$, e dunque: $\overrightarrow{f}(P_k(I_n)) = P_{n-k}(I_n)$

Quindi la funzione:

$$f_{|P_k(I_n)} : x \in P_k(I_n) \mapsto I_n - x \in P_{n-k}(I_n) = Imf_{|P_k(I_n)}$$

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. □

Teorema 8.13 (Formula Ricorsiva per i Coefficienti Binomiali)**.**

$$(\forall n, k \in \mathbb{N})(k \leq n \implies \binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1})$$

Dimostrazione. 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 $I_{n+1} - \{1\}$, 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 $I_{n+1} - \{1\}$ 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: $\binom{n+1}{k+1} = |P_{k+1}(I_{n+1})| = |a| + |b| = \binom{n}{k} + \binom{n}{k+1}$ □

Triangolo di Tartaglia: TODO

Teorema 8.14 (Formula Matematica dei Coefficienti Binomiali)**.**

$$(\forall n, k \in \mathbb{N})(k \leq n \implies \binom{n}{k} = \frac{n!}{(n-k)!k!})$$

Dimostrazione. 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:

$$(0,0) < (1,0) < (1,1) < (2,0) < (2,1) < (2,2) < (3,0) < (3,1) < (3,2) < (3,3) < (4,0) < ...$$

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 $m = 0$, 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 $0 \leq i < m$ per ipotesi induttiva, e dimostriamo che essa vale in m. Ipotizziamo che la coppia di indice m 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:

$$\begin{aligned}
\binom{n-1}{k-1} + \binom{n-1}{k} = \\
\frac{(n-1)!}{(n-1-(k-1))!(k-1)!} + \frac{(n-1)!}{(n-1-k)!k!} = \\
\frac{(n-1)!}{(n-k)!(k-1)!} + \frac{(n-1)!}{(n-k-1)!k!} = \\
\frac{(n-1)!k}{(n-k)!k!} + \frac{(n-1)!(n-k)}{(n-k)!k!} = \\
\frac{(n-1)!(k+n-k)}{(n-k)!k!} = \frac{(n-1)!n}{(n-k)!k!} = \frac{n!}{(n-k)!k!}
\end{aligned}$$

□

9 Insiemi Ordinati e Reticoli

9.1 Insiemi Ordinati II

Teorema 9.1 (Insiemi Ordinati Finiti sono Isomorfi se e soltanto se hanno lo stesso Diagramma di Hasse)**.**

Dimostrazione. TO DO □

Teorema 9.2 (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.*

Teorema 9.3 (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).*

Dimostrazione. 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. □

Teorema 9.4 (Insiemi Ordinati Larghi Finiti ha Minimali (Massimali))**.** $(s, \rho) \wedge \rho \in OL(s) \implies (s, \rho)$ *ha minimali* $\in s$ *Per dualità, allora ha anche massimali.*

Dimostrazione. 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. □

Teorema 9.5 (In Insiemi Finiti, il l'Unico Minimale (Massimale) è Minimo (Massimo))**.**

Dimostrazione. Non dimostriamo questa affermazione. Si noti bene che questo teorema non si applica ad insiemi infiniti: in insiemi infiniti è possibile avere un singolo minimale (massimale) che non è minimo (massimo). □

Definizione 94 (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.

Definizione 95 (Estremo Superiore ed Inferiore)**.** *Sia (s, ρ) un insieme ordinato e $t \subseteq s$. Definiamo l'estremo inferiore e l'estremo superiore rispettivamente:*

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

Cioè, l'estremo superiore è il minimo dei maggioranti, e l'estremo superiore è il massimo dei minoranti.

9.2 Reticoli

Avendo introdotto il concetto di estremo superiore ed inferiore, possiamo parlare di reticoli.

Definizione 96 (Reticolo)**.** *Sia (s, ρ) un insieme ordinato, con $\rho \in OL(s)$. Allora: (s, ρ) è un reticolo $:\Leftrightarrow (\forall x, y \in s)(\exists z, w \in s)(z = INF_{(s,\rho)}(\{x, y\}) \wedge w = SUP_{(s,\rho)}(\{x, y\}))$*

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

E' quindi banale definire le seguenti operazioni:

Definizione 97 (Operazioni di un Reticolo)**.** *Dato un reticolo s, ρ, possiamo definire, $\forall x, y \in s$:*

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

Cioè due operazioni binarie ed interne che chiamiamo rispettivamente wedge e vee.

Pertanto possiamo esprimere un reticolo (s, ρ) come struttura algebrica $(s, \wedge, \vee)$. Si noti bene che nonostante utilizzino lo stesso simbolo, le operazioni di un reticolo sono distinte dai connettivi logici and e or.

Definizione 98 (Reticolo Limitato)**.** *Un reticolo si dice limitato se è dotato di minimo e massimo.*

Definizione 99. *Un reticolo (s, ρ) si dice completo se ogni sua parte non vuota è dotata di estremo superiore ed estremo inferiore. Ogni reticolo completo è anche un reticolo limitato.*

9.3 Principio di Dualità per i Reticoli

Prima di procedere con la dimostrazione di vari teoremi e proprietà dei reticoli, introduciamo il concetto di *enunciato duale* ed il *Principio di Dualità per i Reticoli*.

Definizione 100. *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)*

Teorema 9.6 (Principio di Dualità per i Reticoli)**.** *Se e è una formula valida per ogni reticolo, allora anche la sua duale $\overline{e}$ lo è.*

Dimostrazione. 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). □

9.4 Teoremi sui Reticoli

Per il Principio di Dualità per i Reticoli, ogni teorema che si applica per $\wedge$ vale anche per $\vee$. Inoltre, vale comunque il Principio di Dualità per Insiemi Ordinati (dato che un reticolo è comunque un insieme ordinato) e dunque ogni teorema che vale per minimi/minimali vale equivalentemente per massimi/massimali.

Teorema 9.7 (Il Minimale (Massimale) di un Reticolo è il suo Minimo (Massimo))**.**

Dimostrazione. 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. □

Teorema 9.8 (Il Minorante (Maggiorante) dell'Unione è l'Intersezione dei Minoranti (Maggioranti))**.** *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.

Dimostrazione.

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

□

Teorema 9.9 (Minoranti (Maggioranti) sono 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:*
$MINOR_{(s,\rho)}(a) = MINOR_{(s,\rho)}(\{m\})$

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

Utilizziamo i precedenti due teoremi per dimostrare il seguente:

Teorema 9.10. *Sia (s, ρ) un reticolo. Ogni sua parte finita è dotata di estremo inferiore e superiore.*

Dimostrazione. Siano $a, b \in P(s)$ due insiemi finiti. Allora:
1) Dai due teoremi precedenti segue che:
Siano $m_1 = INF_{(s,\rho)}(a), m_2 = INF_{(s,\rho)}(b)$

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

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 massimo di $MINOR(\{m, x\}) = MINOR(t)$ da cui la tesi.

Per dualità, lo stesso vale per l'estremo superiore. □

9.5 Proprietà delle Operazioni di un Reticolo

Teorema 9.11 (Commutatività di Wedge e Vee)**.** *Sia $(s, \wedge, \vee)$ un reticolo. Allora: $(\forall x, y \in s)((x \wedge y = y \wedge x) \wedge (x \vee y = y \vee x))$*

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

Teorema 9.12 (Associatività di Wedge e Vee)**.** *Sia $(s, \wedge, \vee)$ un reticolo. Allora $\wedge, \vee$ sono associative.*

Dimostrazione. Dimostriamo per $\vee$, la dimostrazione per $\wedge$ è analoga per dualità.

Siano $x, y, z \in s$. Per definizione abbiamo che:
1) $x\rho[x \vee (y \vee z)]$
2) $(y \vee z)\rho[x \vee (y \vee z)]$
3) $y\rho(y \vee z)$
4) $z\rho(y \vee z)$.
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: $[(x \vee y) \vee z] = [x \vee (z \vee y)]$
Che è la tesi. □

Teorema 9.13 (Proprietà di Assorbimento)**.**

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

Teorema 9.14 (Proprietà di Idempotenza (o Iteratività))**.** *In un reticolo* (s, ρ)*,* $x = x \vee x = x \wedge x$ *per ogni* $x \in s$*.*

Dimostrazione. 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:
$x = x \wedge (x \vee (x \wedge x)) = x \wedge x$ □

Teorema 9.15 (Minimo e Massimo sono Elementi Neutri di un Reticolo)**.** *Sia* (s, ρ) *un reticolo. Siano* $m, M \in s$*. Allora:*

$$m \text{ minimo di } s \iff m \text{ neutro di } \vee_\rho$$
$$M \text{ massimo di } s \iff M \text{ neutro di } \wedge_\rho$$

Dimostrazione. $\Rightarrow$) 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. □

Teorema 9.16 (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 $f : \rho \in r \mapsto (\wedge_\rho, \vee_\rho) \in b$ *è biettiva. Questo vuol dire che non solo per ogni reticolo si possono definire delle operazioni, ma ogni coppia di operazioni associative, commutative, idempotenti, e per cui vale l'assorbimento forma le operazioni di un qualche reticolo.*

Dimostrazione. 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. □

9.6 Isomorfismi fra Reticoli

Definizione 101 (Isomorfismo di 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) $(\forall x, y \in s)((f(x \wedge y) = f(x) \wedge' f(y)) \wedge (f(x \vee y) = f(x) \vee' f(y)))$

Teorema 9.17 (Isomorfismi di Insiemi Ordinati e di Reticoli sono Equivalenti)**.** *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 $(s', \rho_{(\wedge',\vee')})$

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: $(\forall x, y \in s)(((x \wedge_\rho y) \rho x) \wedge ((x \wedge_\rho y) \rho y))$.

Applicando l'isomorfismo: $f(x \wedge_\rho y) \rho' f(x)$ e $f(x \wedge'_\rho y) \rho' f(y)$.

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 $z \rho' f(x)$ e $z \rho' f(y)$. 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 extremo 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. □

9.7 Sottoreticoli

TODO: grafici dei sottoreticoli

Definizione 102 (Sottoreticolo)**.** *Sia $(s, \wedge, \vee)$ un reticolo e sia $t \in P(s) - \{\emptyset\}$. Se t è parte chiusa rispetto a $\wedge, \vee$, esso si dice sottoreticolo di $(s, \wedge, \vee)$.*

Definizione 103 (Intervallo Chiuso)**.** *Sia (s, ρ) un insieme ordinato, con $\rho \in OL(s)$.*

$i \subseteq s$ intervallo $:\Leftrightarrow (\forall x, y \in i)(\forall z \in s)(x\rho z \wedge z\rho y \implies z \in i)$

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

Teorema 9.18 (Ogni Intervallo Chiuso è Sottoreticolo)**.** *Se (s, ρ) è un reticolo, ogni suo intervallo chiuso è un sottoreticolo.*

Dimostrazione. 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. □

9.8 Reticoli Complementati

Definizione 104 (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.

Teorema 9.19 (Elementi Confrontabili e Complementati sono Minimo e 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.*

Dimostrazione. 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. □

9.9 Reticoli Distributivi

Definizione 105 (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 può dimostrare che se vale una delle due legge distibutive, allora deve necessariamente valere anche l'altra. Pertanto per dimostrare che un reticolo è distributivo basta dimostrare che vale almeno una delle due leggi distributive.

Teorema 9.20 (I Complementi sono Unici in Reticoli Distributivi)**.** *Sia* (s, ρ) *un reticolo distributivo limitato. Allora ogni complemento è unico.*

Dimostrazione. 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. □

TODO: SOTTRETICOLI TRIRETTANGOLO E PENTAGONALE

Teorema 9.21 (Criterio di Distributività di Birkhoff)**.** *Un reticolo è distributivo* $\iff$ *non contiene sottoreticoli isomorfi al Reticolo Trirettangolo o al Reticolo Pentagonale.*

10 Strutture Booleane

In questa sezione esamineremo tre strutture differenti: Anelli Booleani, Reticoli Booleani, ed Algebre di Boole, e dimostreremo che sono fra di esse equivalenti e che si può trasformare ogni tipo in ogni altro tipo.

Definizione 106 (Reticolo Booleano)**.** *Un reticolo si dice booleano se è distributivo e complementato.*

Definizione 107 (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:* $(\forall x \in s)((x \vee_\rho x' = 1) \wedge (x \wedge_\rho x' = 0))$

Definizione 108 (Anello Booleano)**.** *Un anello unitario* $(a, +, \cdot)$ *si dice booleano* $:\Leftrightarrow (\forall x \in a)(x^2 = x \cdot x = x)$

Teorema 10.1 (In un Anello Booleano, Ogni Elemento è il Proprio Opposto)**.**

$$(a, +, \cdot) \text{ booleano } \implies (\forall x \in a)(x = -x)$$

Dimostrazione.

$$\begin{aligned} x + x &= (x + x)^2 && \text{per proprieta' degli anelli booleani} \\ &= x^2 + 2x^2 + x^2 && \text{per distributivita' dell'anello} \\ &= x + 2x^2 + x \end{aligned}$$

Quindi $x + x = x + 2x + x \implies 2x = 0 \implies x + x = 0 \implies x = -x$ □

Teorema 10.2 (Anelli Booleani sono Commutativi)**.** *Sia* $(a, +, \cdot)$ *un anello booleano. Allora* $(\forall x, y \in a)(xy = yx)$

Dimostrazione. 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, $-yx = yx$ ed abbiamo la tesi. □

Abbiamo già fatto vedere nella sezione sui reticoli che un reticolo può essere espresso equivalentemente come insieme ordinato o come struttura. Analogamente, esiste dunque una corrispondenza biunivoca fra reticoli ed algebre di Boole. Per dimostrare che tutte e tre le tipologie sono equivalenti ci basta allora dimostrare che ad essere equivalenti sono anelli e reticoli booleani.

Teorema 10.3 (Per ogni Anello Booleano esiste un corrispondente Reticolo Booleano)**.** *Dato un anello* $(a, +, \cdot)$*, definiamo* $\rho : (\forall x, y \in a)(x\rho y \iff xy = x)$*. Allora vogliamo dimostrare che* (s, ρ) *è un reticolo booleano.*

Dimostrazione. (1) $\rho \in OL(a)$:

- $(\forall x \in a)(x \cdot x = x) \implies (\forall x)(x\rho x)$ per la proprietà principale dell'anello booleano. La relazione è dunque 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. La relazione è dunque 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. □

Dimostrazione. $\wedge$ e $\vee$:

Verifichiamo per ogni coppia, INF e SUP sono così definiti:

$$(\forall x, y \in a)(x \vee_\rho y = x + y + xy)$$
$$(\forall x, y \in a)(x \wedge_\rho y = xy)$$

Siano $x, y \in a$. Dimostriamo che $x \vee_\rho y$ è maggiorante. $x \cdot (x \vee_\rho y) = x(x + y + xy) = x^2 + xy + x^2y$ Per le proprietà dell'anello booleano, $x^2 = x$ e $xy + xy = 0$.

Pertanto $x \cdot (x \vee_\rho y) = x \implies x\rho(x \vee_\rho y)$.

Lo stesso procedimento si può effettuare per y. Pertanto $x \vee_\rho y$ è maggiorante.

Dimostriamo che $x \vee_\rho y$ è estremo superiore, cioè minimo dei maggioranti. Sia $z \in a$ maggiorante di $\{x, y\}$. Allora:

$$\begin{aligned} x\rho z \wedge y\rho z &\implies xz = x \wedge yz = y \\ &\implies (x + y + xy)z = xz + yz + xyz = x + y + xy \\ &\implies (x + y + xy)\rho z \\ &\implies (x \vee_\rho y)\rho z \end{aligned}$$

□

Dimostrazione. Esso è limitato, distributivo e complementato.

Limitato) $(\forall x \in a)(0x = 0 \implies 0\rho x)$ cioè 0 è minimo.

Analogamente, $(\forall x \in a)(1x = x \implies x\rho 1)$ e quindi 1 è massimo. Il reticolo è dunque limitato.

Distributivo) $x \wedge (y \vee z) = x \wedge (y + z + yz) = x(y + z + yz) = xy + xz + xyz$

$(x \wedge y) \vee (x \wedge z) = (xy) \vee (xz) = xy + xz + xyxz = xy + xz + xyz$

Pertanto il reticolo è distributivo.

Complementato) Sia $x \in a$. Allora:

$x \wedge (1 + x) = x(1 + x) = x + x^2 = x + x = 0$

$x \vee (1 + x) = x + (1 + x) + x(1 + x) = x + 1 + x + x + x^2 = 1$ □

Avendo dimostrato che da ogni anello booleano si può definire un corrispettivo reticolo booleano, si può dimostrare che da ogni reticolo booleano si può definire un anello booleano in questo modo:

Teorema 10.4 (Per ogni Reticolo Booleano esiste un corrispondente Anello Booleano)**.** *Sia* (s, ρ) *reticolo booleano con almeno due elementi e definiamo:* $x + y = (x \wedge_\rho y') \vee_\rho (x' \wedge_\rho y)$ $x \cdot y = (x \wedge_\rho y)$ *Allora si dimostra che* $(s, +, \cdot)$ *è un anello booleano.*

Teorema 10.5 (L'Insieme delle Parti è un Anello Booleano)**.**

Dimostrazione. 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. □

Teorema 10.6 (Teorema di Stone)**.** *Sia* $a \neq \emptyset$ *e* $(a, +, \cdot)$ *un anello booleano. Allora:* $(\exists s \neq \emptyset)((a, +, \cdot) \overset{isomorfo}{\simeq} (P(s), \triangle, \cap))$*. Se* a *è finito, posso scegliere anche* s *finito.*

Teorema 10.7 (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 del due.*

4) Due anelli booleani finiti sono isomorfi $\iff$ *hanno la stessa cardinalità.*

10.1 Stringhe

Definizione 109 (Insieme delle Stringhe Binarie)**.** *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*.*

Definizione 110 (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:

$$x \cdot y = ([x_1 \cdot y_1], ..., [x_n \cdot y_n])$$

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.

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 $(\mathbb{Z}_2 \times ... \times \mathbb{Z}_2$ (n volte), $+, \cdot)$ (dove $+, \cdot$ sono la somma e prodotto puntuali).

11 Divisibilità

Sia $(s, \cdot)$ un semigruppo commutativo, allora definiremo:

Definizione 111 (Divisori e Multipli)**.** *$\forall x, y \in s$, diremo che:*

$$\begin{matrix} x|y \\ x \text{ divide } y \\ y \text{ e' multiplo di } x \end{matrix} :\Leftrightarrow (\exists z \in s)(xz = y)$$

E noteremo gli insiemi dei divisori e dei multipli di x in s nel modo seguente:

$$DIV_s(x) = \{y \in s \mid y|x\}$$
$$MULT_s(x) = \{z \in s \mid x|z\}$$

Teorema 11.1. *Due elementi $x, y \in s$ si dicono associati se si dividono a vicenda.*

$$x, y \text{ associati } :\Leftrightarrow x \in DIV_s(y) \wedge y \in DIV_s(x)$$

Noteremo l'insieme degli associati di x in s come:

$$ASSOC_s(x) = \{y \in s \mid x|y \wedge y|x\}$$

Teorema 11.2 (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.

Dimostrazione. $\supseteq$) 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 ci sono w e z in s tali che $y = xw$ e $x = yz$. Allora, usando la cancellabilità di x:

$x = xwz \implies wz = 1 \implies w, z$ invertibili $\implies w \in U(s) \implies y \in \{xu \mid u \in U(s)\}$

Da cui la tesi. □

Teorema 11.3 (Associati hanno stessi Divisori e Multipli)**.** *Sia $(s, \cdot)$ un monoide commutativo. Allora, $\forall x, y \in s$:*

$$y \in ASSOC_s(x) \overset{(1)}{\iff} DIV_s(x) = DIV_s(y) \overset{(2)}{\iff} MULT_s(x) = MULT_s(y)$$

Dimostrazione. $1 \Rightarrow$) 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. □

Definizione 112 (Massimi Comun Divisori e Minimi Comune Multipli)**.** *Sia $(s, \cdot)$ un monoide commutativo e sia $t \subseteq s$. Allora definiamo:*

$$MCD_s(t) = \{d \in \bigcap_{x \in t} DIV_s(X) \mid (\forall z \in \bigcap_{x \in t} DIV_s(x))(z|d)\}$$
$$mcm_s(t) = \{d \in \bigcap_{x \in t} MULT_s(X) \mid (\forall z \in \bigcap_{x \in t} MULT_s(x))(d|z)\}$$

Attenzione! 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 il minimo di un insieme ordinato sono sempre unici, mentre l'MCD e gli mcm, come si può vedere dalla definizione, sono insiemi di potenzialmente molteplici elementi.

Definizione 113. *Sia $(s, \cdot)$ un monoide commutativo e sia $x \in s$. Diremo che gli elementi invertibili del monoide e gli associati di x divisori banali di x.*

$$BDIV_s(x) = U(s) \cup ASSOC_s(x)$$

Definizione 114 (Elementi Irriducibili)**.** *Sia $(s, +, \cdot)$ un dominio di integrità e sia $x \in s$.*

$$x \text{ irriducibile } :\Leftrightarrow x \notin U(s) \wedge DIV_s(x) = BDIV_s(x)$$

Definizione 115 (Elementi Primi)**.** *Sia $(s, \cdot)$ un monoide commutativo.*

$$p \in s \text{ primo } :\Leftrightarrow (\forall a, b \in s)(p|ab \implies p|a \vee p|b)$$

Definizione 116 (Elementi Coprimi)**.** *Sia $(s, \cdot, 1_s)$ un monoide commutativo. Allora:*

$$x, y \in s \text{ coprimi } :\Leftrightarrow 1_s \in MCD(\{x, y\})$$

Cioè se l'unità è un loro MCD.

Definizione 117 (Monoide Cancellativo)**.** *Un monoide commutativo si dice cancellativo se ogni suo elemento è cancellabile.*

Definizione 118 (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.

Si può dimostrare che queste tre condizioni sono fra di loro equivalenti.

Definizione 119 (Anello Fattoriale)**.** *Un anello commutativo unitario $(a, +, \cdot)$ si dice anello fattoriale se $(a - \{0_a\}, \cdot)$ è un monoide fattoriale.*

Teorema 11.4 (Caratterizzazione di MCD e mcm per Associati)**.** *Sia* $(s, \cdot)$ *un monoide commutativo, siano* $x, y \in s$*. allora:*

$$m \in MCD(x,y) \iff ASSOC(m) = MCD(x,y)$$
$$m \in mcm(x,y) \iff ASSOC(m) = mcm(x,y)$$

Dimostrazione. $\rightarrow$) $m|x \wedge m|y \wedge (\forall z \in s)(z|x \wedge z|y \implies z|m)$ 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.

$ASSOC(m) = MCD(x,y) \implies m \in MCD(x,y)$. □

Definizione 120 (Fattorizzazione in Primi)**.** *Sia* $(m, \cdot)$ *un monoide fattoriale. Sia* $a \in m - U(m)$*, allora* $a = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_n^{k_n}$*. I divisori di a sono tutti e soli gli elementi associati ad elementi del tipo* $p_1^{l_1} \cdot \ldots \cdot p_n^{l_n}$ *con* $0 \leq l_i \leq k_i, \forall i \in I_n$*.*

Se $a = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_n^{k_n} \in \mathbb{N}$, allora a ha esattamente $\prod_{i=1}^{n}(k_i + 1)$ divisori. Se $a = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_n^{k_n} \in \mathbb{Z}$, allora a ha esattamente $2 \cdot \prod_{i=1}^{n}(k_i + 1)$ divisori.

Immaginiamo di avere un secondo elemento $b = p_1^{l_1} \cdot \ldots \cdot p_n^{l_n}$. Per ogni $1 \leq i$ n definiamo $\alpha_i = MAX(k_i, l_i)$ e $\beta_i = MIN(k_i, l_i)$. Allora avremo che:

$$m = p_1^{\alpha_1} \cdot \ldots \cdot p_n^{\alpha_n} \in mcm(a,b)$$
$$M = p_1^{\beta_1} \cdot \ldots \cdot p_n^{\beta_n} \in MCD(a,b)$$
$$m \cdot M \in ASSOC(a \cdot b)$$

11.1 Fattorizzazione in Primi

Cioè, se scegliamo gli esponenti massimi, allora otteniamo un mcm, se scegliamo esponenti minimi troviamo un MCD, ed il loro prodotto è un associato di $a \cdot b$.

Si noti che non è necessario che i due valori a e b abbiano la stessa fattorizzazione, si può fare l'assunzione che ogni primo che appare nella fattorizzazione di uno ma non dell'altro abbia esponente zero.

Esempio.

$$a = 2 \cdot 3^2 \cdot 5 \qquad = 2 \cdot 3^2 \cdot 5 \cdot 11^0 \cdot 13^0 \qquad = 90$$
$$b = 3 \cdot 5^2 \cdot 11 \cdot 13 \qquad = 2^0 \cdot 3 \cdot 5^2 \cdot 11 \cdot 13 \qquad = 10725$$

Pertanto, scegliendo gli esponenti massimi e minimi otteniamo:

$$m = 2 \cdot 3^2 \cdot 5^2 \cdot 11 \cdot 13 = 64350$$
$$M = 2^0 \cdot 3 \cdot 5 \cdot 11^0 \cdot 13^0 = 15$$

E si ha che $m \in mcm(a,b)$ $M \in MCD(a,b)$.

11.2 Divisibilità in $\mathbb{Z}$

Teorema 11.5 (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.*

Dimostrazione.

$$d|a \wedge d|b \implies (\exists h, k \in \mathbb{Z})(a = dk \wedge b = dh)$$

E quindi:

$$(\forall x, y \in Z)(ax + by = dkx + dhy = d(kx + hy) \implies d|(ax + by))$$

□

Definizione 121 (Valore Assoluto)**.** *Sia $n \in \mathbb{Z}$. Allora definiamo la funzione valore assoluto come:*

$$|n| : n \in \mathbb{Z} \mapsto \begin{cases} n \text{ se } n \in \mathbb{N} \\ -n \text{ se } n \in \mathbb{Z} - \mathbb{N} \end{cases}$$

Teorema 11.6 (Teorema della Divisione Euclidea)**.**

$$(\forall m, n \in \mathbb{Z})(m \neq 0 \implies (\exists!(q, r) \in \mathbb{Z} \times \mathbb{N})(n = mq + r \wedge 0 \leq r < |m|))$$

Cioè, per ogni coppia di valori m, n con m non nullo, esistono e sono unici due valori q (quoziente) e r (resto) tali che $n = mq + r$. Inoltre, r è compreso fra lo zero e il valore assoluto di m.

Dividiamo la dimostrazione in tre sezioni:

Prima dimostriamo che esiste una coppia quoziente/resto se $n \in \mathbb{N}$.

Poi dimostriamo che esiste anche se $n \in \mathbb{Z} - \mathbb{N}$, cioè se n è un numero negativo.

Infine, avendo dimostrato che quoziente e resto esistono per ogni numero intero relativo, dimostriamo che essi sono inoltre unici.

Dimostrazione. (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: $n = m$ e $q = 1, r = 0$, oppure $n = -m$ e $q = -1, r = 0$.

Se $n > |m|$. Allora $n - |m| < n$, 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 $\forall n \in \mathbb{N}$. □

Dimostrazione. (Caso $n \in \mathbb{Z} - \mathbb{N}$)

Dalla prima parte della dimostrazione 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 $0 \leq r < |m| \implies n = m(-q_1) - r_1 = m(-q_1) - r_1 + |m| - |m|$. 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 per ogni valore di $\mathbb{Z}$. □

Dimostrazione. ((q, r) sono unici)

Siano $(q_1, r_2), (q_2, r_2) \in \mathbb{Z} \times \mathbb{N}$.

Ipotizziamo WLOG che $0 \leq r_1 \leq r_2 \leq |m|$ e che $n = mq_1 + r_1 = mq_2 + r_2$.

Allora $n(q_1 - q_2) = r_2 - r_1$ e quindi $|m||q_1 - q_2| = |m(q_1 - q_2)| = |r_2 - r_1|$ e $0 \leq |r_2 - r_1| < |m|$.

Segue che $|m||q_2 - q_1| < |m|$ che può succedere solo, dato che $m \neq 0$ per ipotesi, se $|q_2 - q_1| = 0 \implies q_2 = q_1$.

E quindi $n = mq_1 + r_1 = mq_1 + r_2 \implies r_1 = r_2$, da cui la tesi. □

ALGORITMO DELLE DIVISIONI SUCCESSIVE: TODO

Teorema 11.7 (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.

Dimostrazione. 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 $r_t = 0 \implies r_{t-1} \in MCD(a, b)$.

$r_{t-1} = r_{t-3} + r_{t-2}(-q_{t-1})$. 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. □

Teorema 11.8 (Lemma di Euclide)**.** *Siano $a, b, c \in \mathbb{Z}$. Se a, b sono coprimi, allora $a|bc \implies a|c$.*

Dimostrazione. $1 \in MCD(a, b)$ 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 $(\exists h, k \in \mathbb{Z})(c = acu + bcv = ahu + akv \implies c = a(hu + kv) \implies a|c$ □

Teorema 11.9 (In $\mathbb{Z}$, i primi sono tutti e soli gli irriducibili)**.** $p \in \mathbb{Z}$ *primo* $\iff$ p *irriducibile.*

Dimostrazione. $\Rightarrow$) Sia $p \in \mathbb{Z}$ primo e siano $a, b \in \mathbb{Z}$ tali che $p = ab$. p è primo, quindi $p|a \vee p|b$. 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 $a|b$.

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, $p|b$. □

11.3 Congruenze

Definizione 122 (Operazione Parziale: Modulo)**.**

$$(\forall (a, m) \in \mathbb{Z} \times (\mathbb{Z} - \{0\})(a \bmod m = MIN([a]_m \cap \mathbb{N}))$$

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* $a \bmod 0$*.*

Indichiamo il modulo con le seguenti notazioni equivalenti:$a \bmod m$, $a \ \% \ m$, $REST(a, m)$.

Si osserva che $a \bmod m < |m|$ e che $a \bmod m =$ resto di $DE(a, m)$.

Teorema 11.10 (Caratterizzazione di $\mathbb{Z}$)**.** *Sia* $m \in \mathbb{N} - \{0\}$*. Allora* $\mathbb{Z}_m = \{[0]_m, [1]_m, \ldots, [m-1]_m\}$ *e in particolare si ha che* $|\mathbb{Z}_m| = m$

Dimostrazione: 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* $a \in \mathbb{Z}$*.* $DE(a, m) = (q, r) \wedge a = qm + r \wedge 0 \leq r < |m|$.

Quindi $qm = a - r$*, cioè* $[a]_m = [r]_m$*. 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 Z_m *sono a due a due distinte, e sono quindi* m *in numero.*

Siano $i, j \in \mathbb{Z} : 0 \leq i \leq j < m \wedge [i]_m = [j]_m$*. Allora* $0 \leq j - i < m \wedge (\exists k \in \mathbb{Z})(j = i + km) \implies j - i = km \implies j - i = 0$ *in quanto esso è strettamente minore di* m*.*

Definizione 123 (Relazione d'Equivalenza Compatibile)**.** *Sia* $s \neq \emptyset$ *e* $*$ *una sua operazione binaria interna, e* $\sim$ *una sua relazione di equivalenza.*

Allora:

$\sim$ *compatibile a sx in* $(s, *) :\Leftrightarrow (\forall a, b, c \in s)(a \sim b \implies c * a \sim c * b)$

$\sim$ *compatibile a dx in* $(s, *) :\Leftrightarrow (\forall a, b, c \in s)(a \sim b \implies a * c \sim b * c)$

Definizione 124 (Congruenza)**.** *Sia $s \neq \emptyset$ e siano $*_1, \ldots, *_n$ sue operazioni binarie interne, e sia $\sim$ una sua relazione di equivalenza.*

Allora $\sim$ è congruenza in $(s, *_1, \ldots, *_n)$ se e soltanto se:

$$(\forall a, b, c, d \in s)((\forall i \in \mathbb{N})(0 \leq i \leq n \implies (a \sim b \wedge c \sim d \implies a *_i c \sim b *_i d)))$$

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 $(s/\sim, (*_1)_\sim, \ldots, (*_n)_\sim)$

Teorema 11.11 (Congruenza equivale a Compatibilità)**.** *Una relazione di equivalenza su una struttura $(s, *_1, \ldots, *_n)$ è una congruenza se e solo se è compatibile sia a destra che a sinistra $(\forall i)(0 \leq i \leq n)$.*

Dimostrazione. Possiamo supporre un'unica operazione in $(s, *)$.

$\Rightarrow$) Se ipotizziamo $a, b \in s : a \sim b$, allora $a \sim b \wedge c \sim c$ per riflessività e $c * a \sim c * b$. Uguale per la compatibilità a destra.

$\Leftarrow$) Supponiamo che $a \sim b \wedge c \sim d$. Per ipotesi di compatibilità a destra, allora $a*c \sim b*c$. Per compatibilità a sinistra, $b*c \sim b*d$. Quindi $a*c \sim b*d$. $\square$

Definizione 125 (Anello Quoziente)**.** *Sia $\equiv_m$ una congruenza in $(\mathbb{Z}, +, \cdot)$. Allora essa è epimorfa all'anello quoziente $(\mathbb{Z}_m, +_m, \cdot_m)$.*

Teorema 11.12 (Asserti Equivalenti sugli Anelli Quoziente)**.** *Sia $m \in \mathbb{Z} - \{0\}$. Sono equivalenti le seguenti affermazioni:*

1) $(\mathbb{Z}_m, +, \cdot)$ è un campo.

2) $(\mathbb{Z}_m, +, \cdot)$ è un dominio di integrità.

3) m è primo

Dimostrazione. $1 \to 2$) 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 $[a]_m \cdot [b]_m = [0]_m \iff [a]_m = 0 \vee [b]_m = 0$. 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. $\square$

11.4 Equazioni Diofantee

Definizione 126 (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.

Un'equazione diofantea della forma $e[a,b,c](x,y)$ si può esprimere sinteticamente $ax + by = c$

Definizione 127 (Soluzione di un'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.*

Teorema 11.13 (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 $\iff d|c$

Dimostrazione. $1 \to 2)$ $\to$) 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. □

Teorema 11.14 (Caratterizzazione dell'Insieme delle Soluzioni di un'Equazione Diofantea)**.** *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:*

$$\{(x_0 + \frac{b}{d}k, y_0 - \frac{a}{d}k) \mid k \in \mathbb{Z}\}$$

Dimostrazione. 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. □

11.5 Equazioni Congruenziali

Definizione 128 (Equazione Congruenziale)**.** *Siano $m \in \mathbb{Z} - \{0\}, a, b \in \mathbb{Z}$. 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 ad una incognita di termini a e b e modulo m.

Definizione 129 (Soluzione di un'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.

Teorema 11.15 (Criterio per l'Esistenza di Soluzioni Congruenziali)**.** *Siano $a, b \in \mathbb{Z}, m \in \mathbb{Z} - \{0\}, d \in MCD(a, m)$. Allora $ax \equiv_m b$ ha soluzioni $\iff d|b$.*

Dimostrazione. L'equazione congruenziale $ax \equiv_m b$ può essere espressa come equazione diofantea $ax + my = b$. Per la 4^ tesi del teorema sugli Asserti Equivalenti al Teorema di Bézout, allora l'equazione diofantea ha soluzioni solo se $d \in MCD(a, m)$ divide b. □

Teorema 11.16 (Primo Corollario del Criterio d'Esistenza di Soluzioni Congruenziali)**.** *Siano $a, b \in \mathbb{Z}, m \in \mathbb{Z} - \{0\}, d \in MCD(a, m)$. Allora:*

$$[a]_m \in U(\mathbb{Z}_m) \iff a, m \text{ coprimi}$$

Dimostrazione. $\rightarrow$)) 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 Criterio) 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 Criterio, l'equazione congruenziale $ax \equiv_m 1$ ha soluzioni e quindi esiste un $[a]_m$ è invertibile. □

Teorema 11.17 (Secondo Corollario del Criterio d'Esistenza di Soluzioni Congruenziali)**.** *Siano $a, b \in \mathbb{Z}, m \in \mathbb{Z} - \{0\}, d \in MCD(a, m)$. Allora:*

$$[a]_m \in U(\mathbb{Z}_m) \iff [a]_m \textit{non è divisore dello zero.}$$

Teorema 11.18. *$\rightarrow$)) 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 Primo 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.

Teorema 11.19 (Equazioni Congruenziali si possono esprimere come Equazioni Diofantee)**.** *Un'equazione congruenziale $ax \equiv_m b$ si può esprimere nella forma:*

$$ax + my = b$$

Cioè come equazione diofantea.

Dimostrazione. $ax \equiv_m b \implies m|(ax - b) \implies (\exists k \in z)(mk = ax - b$ E quindi: $ax - mk = b$ Ponendo $y = -k$ abbiamo la tesi. □

11.5.1 Risoluzione di Equazioni Congruenziali

Siano $a, b \in \mathbb{Z}, m \in \mathbb{Z} - \{0\}$. Allora:

Teorema 11.20 (Primo Criterio per la Risoluzione di Equazioni Congruenziali)**.** *L'equazione congruenziale $ax \equiv_m b$ ha lo stesso insieme di soluzioni dell'equazione congruenziale $a'x \equiv_m b'$, per ogni $a' \in [a]_m, b' \in [b]_m$.*

Dimostrazione. Dato che $[a']_m = [a]_m \wedge [b']_m = [b]_m$ per ipotesi:

$$ax \equiv_m b \iff [a]_m[x]_m = [b]_m \iff a'x \equiv_m b'x$$

□

Teorema 11.21 (Secondo Criterio per la Risoluzione di Equazioni Congruenziali)**.** *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.*

Dimostrazione. Si ha 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 $ax \equiv_m b$. □

Teorema 11.22 (Terzo Criterio per la Risoluzione di Equazioni Congruenziali)**.** *Per ogni k coprimo ad m, l'equazione $akx \equiv_m bk$ ha lo stesso insieme di soluzioni di $ax \equiv_m b$.*

Dimostrazione. 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. □

Partendo dai precedenti tre criteri, possiamo dunque seguire il seguente algoritmo per risolvere una qualsiasi equazione congruenziale $ax \equiv_m b$:

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 $d \in MCD(a, m)$

11.6 Elementi Periodici

Definizione 130 (Elemento Periodico)**.** *Sia $(g, \cdot)$ un gruppo. $x \in g$ si dice periodico se:*

$$(\exists n \in \mathbb{N} - \{0\})(x^n = 1_g)$$

E tale n si dice periodo dell'elemento x e si indica $|x|$.

Osserviamo, senza dimostrarlo, che se x è un elemento di periodo n di un gruppo $(g, \cdot)$ allora n è uguale alla cardinalità del sottogruppo generato da x, cioè:

$$|x| = n \iff |\langle x \rangle| = n$$

Teorema 11.23 (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:*

$$(\forall a, b \in \mathbb{Z})(x^a = x^b \iff a \equiv_m b)$$

Dimostrazione. 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 $a \equiv_m b$. □

12 Polinomi

12.1 L'Anello dei Polinomi

Definizione 131 (Successione di Elementi)**.** *Sia $(a, +, \cdot)$ un anello unitario commutativo. Allora una funzione del tipo $f : n \in \mathbb{N} \mapsto x \in a$ si dice successione di elementi di a. Noteremo la successione f con la notazione:*

$$(a_n)_{n\in\mathbb{N}} := f$$

E noteremo l'elemento n-esimo della successione con la notazione:

$$a_n = f(n)$$

Definizione 132 (Polinomio)**.** *Sia $(a, +, \cdot)$ un anello commutativo unitario e sia $(a_n)_{n\in\mathbb{N}}$ una successione di suoi elementi. Allora:*

$$(a_n)_{n\in\mathbb{N}} \text{ poliniomio a coefficienti in } a \iff (\exists k \in \mathbb{N})((\forall n \geq k)(a_n = 0))$$

Un polinomio è quindi una successione che si annulla dopo un certo numero k di termini. Noteremo l'insieme di tutti i polinomi definibili su un anello a come $a[x]$.

Definizione 133 (Coefficienti di un Polinomio)**.** *Diremo coefficienti del polinomio $(a_n)_{n\in\mathbb{N}}$ i suoi termini a_n con $n < k$.*

Definizione 134 (Polinomio Nullo)**.** *Sia $(a, +, \cdot)$ un anello commutativo unitario. Allora definiamo il polinimio nullo o polinomio zero:*

$$0 := (0_a)_{n\in\mathbb{N}}$$

Dove $(0_a)_{n\in\mathbb{N}}$ è una successione $(a_n)_{n\in\mathbb{N}}$ tale che $(\forall n \in \mathbb{N})(a_n = 0_a)$

Definizione 135 (Grado di un Polinomio)**.** *Sia $f \in A[x] - \{0\}$ (cioè un polinomio non nullo). Il minimo $k \in \mathbb{N} : (\forall n > k)(a_n = 0)$ si dice grado di f e si nota $gr(f)$.*

Definizione 136 (Coefficiente Direttore di un Polinomio)**.** *Se $f \in A[x] - \{0\}$, $a_{gr(f)}$ si dice coefficiente direttore del polinomio e si indica $cd(f)$*

Definizione 137 (Grado e Coefficiente Direttore del Polinomio Nullo)**.**

$$cd(0) = 0$$
$$gr(0) = -\infty$$

Definizione 138 (Polinomio Monico)**.** *$f \in A[x]$ si dice polinomio monico se $cd(f) = 1_a$, cioè se il suo coefficiente direttore è l'unità dell'anello.*

Definizione 139 (Somma e Prodotto di Polinomi)**.** *Definiamo le operazioni si somma e prodotto di polinomi nel modo seguente:*

Siano $(a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}} \in A[x]$ *due polinomi. Allora definiamo:*

$$(a_n + b_n)_{n\in\mathbb{N}} = (a_n)_{n\in\mathbb{N}} + (b_n)_{n\in\mathbb{N}}$$
$$\left(\sum_{i+j=n} a_i b_j\right)_{n\in\mathbb{N}} = (a_n)_{n\in\mathbb{N}} \cdot (b_n)_{n\in\mathbb{N}}$$

Cioè la somma dei polinomi è il polinomio che si ottiene sommando i termini, mentre il prodotto fra polinomi è il polinomio che si ottiene moltiplicando ogni termine per ogni altro termine.

Definizione 140 (Anello dei Polinomi)**.** *Avendo definito somma e prodotto di polinomi, possiamo dunque affermare che l'insieme* $A[x]$ *definibile su un anello commutativo unitario* A *è a sua volta un anello, l'Anello dei Polinomi di* A*.*

L'elemento neutro rispetto alla somma è il polinomio nullo, $(0, 0, 0, 0, \dots)$*.*

L'elemento neutro rispetto alla somma è il polinomio monico di grado 1, $(1, 0, 0, 0, \dots)$*.*

Definizione 141 (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.*

Facendo abuso di notazione, noteremo $a := (a, 0, 0, 0, 0, ...)$

Cioè indicheremo il polinomio costante con il suo unico coefficiente non nullo.

Definizione 142 (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, $a \overset{isomorfo}{\simeq} Im(\mu)$

Definizione 143 (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.*

Teorema 12.1 (Potenze del Polinomio Incognita)**.** *Si può provare per induzione che:*

$$x = (0, 1, 0, 0, 0...)$$
$$x^2 = (0, 0, 1, 0, 0, ...)$$
$$x^3 = (0, 0, 0, 1, 0, ...)$$
$$\dots$$
$$x^n = (0, \dots, 0 \text{ } (n \text{ volte}), 1, 0, ...)$$

Definizione 144 (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.

Teorema 12.2 (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:

$$f = a_0 + a_1x + a_2x^2 + a_3x^3 + ... + a_mx^m$$

Teorema 12.3 (Proprietà di 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:

$$f + g = \sum_{i=0}^{M} (a_i + b_i)x^i$$

$$f \cdot g = \sum_{i=0}^{n+m} (\sum_{j=0}^{i} a_j b_{i-j})x^i$$

Teorema 12.4 (Proprietà del Grado della Somma di Polinomi)**.** *Siano $f, g \in A[x] - \{0\}$. Allora:*

$$\begin{aligned} gr(f) = gr(g) \wedge cd(f) = -cd(g) &\implies gr(f+g) < gr(f) = gr(g) \\ gr(f) \neq gr(g) \vee cd(f) \neq cd(g) &\implies gr(f+g) = max\{gr(f), gr(g)\} \end{aligned}$$

Teorema 12.5 (Proprietà del Grado del Prodotto di Polinomi)**.** *Siano $f, g \in A[x] - \{0\}$. Allora:*

$$\begin{aligned} cd(f) \cdot cd(g) = 0 &\implies gr(f \cdot g) < gr(f) + gr(g) \\ cd(f) \cdot cd(g) \neq 0 &\implies gr(f \cdot g) = gr(f) + gr(g) \wedge cd(f \cdot g) = cd(f) \cdot cd(g) \end{aligned}$$

Diciamo la seconda proprietà di sopra la "Formula di Addizione dei Gradi". Se $f = 0, gr(f \cdot g) = gr(0) = -\infty = -\infty + gr(g)$ e $cd(f \cdot g) = 0 = cd(f) \cdot cd(g)$ quindi si osserva che la Formula di Addizione dei Gradi vale anche con il polinomio zero.

Teorema 12.6 (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.*

Dimostrazione. $cd(f)$ 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. □

Teorema 12.7 (Condizione Sufficiente e Necessaria per Dominio di Integrità dei Polinomi)**.** *Dal teorema precedente segue che $A[x]$ è dominio di integrità $\iff$ A è dominio di integrità*

Teorema 12.8 (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.*

Dimostrazione. 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. □

Teorema 12.9 (Invertibilità del Polinomio Incognita)**.** *Il polinomio x non è mai invertibile.*

Dimostrazione. Dato che $cd(x) = 1$ per definizione, e l'unità dell'anello è sempre cancellabile. Da questo segue che $A[x]$ non è mai un campo. □

Teorema 12.10 (Teorema della Divisione Lunga fra Polinomi)**.** *Sia $(A, +, \cdot)$ un anello commutativo unitario e siano $f, g \in A[x]$.*

Allora:

$$cd(g) \in U(A) \implies (\exists!(q, r) \in A[x] \times A[x])(f = gq + r \wedge gr(r) < gr(g))$$

Cioè, dati due polinomi f e g e il coefficiente direttore di g è invertibile, allora esistono e sono unici due polinomi g (quoziente) ed r (resto) tali che $f = gq + r$. Inoltre, il grado del resto è strettamente minore di quello del quoziente.

Dimostrazione. 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^ Forma su n.

Sia $k = ab^{-1}x^{n-m}g$. Tra $ab^{-1}x^{n-m}$ 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 $q_1 = q_2 \wedge r_1 = r_2$. □

Teorema 12.11 (Condizione per l'Anello dei Polinomi Fattoriale)**.** *A anello fattoriale $\implies$ $A[x]$ anello fattoriale.*

12.2 Radici e Divisiblità nell'Anello dei Polinomi

Sia $f \in A[x], f = a_0 + a_1x + ... + a_nx^n$, con $a_n \neq 0$. Allora definisco:

$$f(c) := a_0 + a_1c + ... + a_nc^n \in A$$

Teorema 12.12 (Omomorfismo di Sostituzione)**.** *Sia $c \in A$, anello commutativo unitario. Allora la funzione:*

$$f \in A[x] \mapsto f(c) \in A$$

è un omomorfismo di anelli detto Omomorfismo di Sostituzione.

Definizione 145 (Applicazione Polinomiale)**.** *Sia $f \in A[x]$. Definiamo l'applicazione polinomiale di f la funzione:*

$$\overline{f} : c \in A \mapsto f(c) \in A$$

Si osserva che se $f = a_0$, cioè f è un polinomio costante, allora $(\forall c \in A)(\overline{f}(c) = a_0)$ e quindi anche l'applicazione polinomiale è costante.

Definizione 146 (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.*

Teorema 12.13 (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

Teorema 12.14 (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 $(x - c)$.*

Dimostrazione. $cd(x - c) = 1$, 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:

$$f(c) = (c - c)q(c) + r(c) = 0 \cdot q(c) + a_0 = a_0$$

□

Teorema 12.15 (Teorema di Ruffini)**.** *Sia A un anello commutativo unitario, $f \in A[x], c \in A$. Allora:*

$$c \text{ radice di } f \iff (x - c)|f$$

Dimostrazione. c radice $\implies f(c) = 0_A \implies$ per il Teorema del Resto, il resto della divisione lunga è $0_A \implies (x-c)|f$ □

Teorema 12.16 (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:*

$$c_1, ..., c_n \text{ radici di } f \iff \prod_{i=1}^{n}(x-c_i)|f$$

Dimostrazione. $\rightarrow$) 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:

$$f = (x-c_n)g = (x-c_n) \cdot \prod_{i=1}^{n-1}(x-c_i) \cdot h = \prod_{i=1}^{n}(x-c_i) \cdot h$$

Ciò 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. □

Teorema 12.17 (Numero di Radici in un Dominio d'Integrità)**.** *Sia A dominio di integrità, $f \in A[x] - \{0\}$, e siano $c_1, ..., c_n$ radici di f. Allora:*

$$n \leq gr(f)$$

Cioè il numero delle radici è minore o uguale del grado del polinomio.

Dimostrazione. 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. □

Controesempio. Forniamo un controesempio nel caso in cui A non è dominio di integrità e mostriamo che il teorema non è valido in tale caso.

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.

Teorema 12.18 (Principio di Identità dei Polinomi)**.** *Sia A un dominio di integrità infinito. Allora:*

$$(\forall f, g \in A[x])(f = g \iff \overline{f} = \overline{g})$$

Dimostrazione. $\rightarrow$) 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:

$$h = 0 \implies f = g$$

□

Controesempio. Forniamo un controesempio per dimostrare che il teorema precedente non è valido in un anello finito.

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 $f \neq 0$.

Definizione 147 (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.

Teorema 12.19 (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*

$$f = c \cdot g_1 \cdot ... \cdot g_n$$

e $g_1, ..., g_n$ sono monici ed irriducibili e la decomposizione è unica a meno dell'ordine dei fattori.

Dimostrazione. 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 Prima 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. □

Teorema 12.20 (Criterio di Irriducibilità di Polinomi sun 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) $(\forall g, h \in A[x])(f = gh \implies (gr(g) = 0 \oplus g(h) = 0))$

Dimostrazione. $\leftarrow$) 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. □

Teorema 12.21 (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 $A[x]$.*

Dimostrazione. $\rightarrow$) Per Ruffini. $\leftarrow$) Tutti i polinomi di grado 1 hanno radici in un campo.

$$kx + h \implies c = -hk^{-1} \text{ radice}$$

Quindi, $f = g(kx + h) \implies -hk^{-1}$ è radice di f. □

Da Ruffini e dalla Formula di Addizione dei Gradi seguono le seguenti tre conclusioni:

Teorema 12.22 (Irriducibilità di Polinomi in un Dominio di Integrità)**.** *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.*

Teorema 12.23 (Irriducibilità di 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.*

Teorema 12.24 (Radici di 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.*

Procediamo dunque ad enunciare il:

Teorema 12.25 (Teorema Fondamentale)**.** *Ogni polinomio non costante di $\mathbb{C}[x]$ ha radici.*

Corollario: *in $\mathbb{C}$ gli unici irriducibili sono polinomi di grado 1.*

Teorema 12.26 (Irriducibilità di Polinomi Reali)**.** *Ogni polinomio irriducibile di $\mathbb{R}[x]$ ha grado minore di 3.*

Corollario: *I polinomi irriducibili in $\mathbb{R}[x]$ sono esattamente quelli di di grado 1 o quelli di grado 2 senza radici.*

Teorema 12.27 (Teorema di Bolzano)**.** *Ogni polinomio su $\mathbb{R}[x]$ di grado dispari ha una radice in $\mathbb{R}$.*

Teorema 12.28 (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 $x_{1,2} = \frac{-b \pm \sqrt{\Delta}}{2a}$

Teorema 12.29 (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* $\mathbb{Q}[x]$*.*

Eisenstein si può in realtà applicare ad ogni polinomio razionale, dato che ogni polinomio in $Q[x]$ ha un polinomio associato in $Z[x]$.

Esempio: Moltiplicando e dividendo per l'MCM otteniamo che:

$$3x^4 + \frac{1}{90}x + \frac{3}{4} = \frac{1}{180}(540x^4 + 2x + 135)$$

E $540x^4 + 2x + 135 \in Z[x]$.

Inoltre, da Eisenstein segue che 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.

Teorema 12.30 (Radici Razionali di Polinomi in $\mathbb{Z}$)**.** *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.*

Corollario. Se $f \in \mathbb{Z}[x]$ è un polinomio monico, allora tutte le sue radici razionali sono in realtà intere.

Dimostrazione. 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. □

13 Grafi

Definizione 148 (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. Gli elementi di v si dicono vertici del grafo, mentre le coppie $\{x, y\} \in P_2(v) : x\rho y$ si dicono archi o lati del grafo.*

Equivalentemente, un grafo semplice si può esprimere come coppia di insiemi (v, l) dove l è un insieme del tipo:

$$l \subseteq P_2(v) = \{\{x, y\} \subseteq P(v) | x \neq y\}$$

Graficamente, un grafo semplice si rappresenta come punti (rappresentati i vertici) uniti da linee o curve (rappresentanti gli archi o lati). Notiamo che il grafo è semplice perché fra due vertici è presente al più una singola connessione, e tale connessione è a senso doppio (in quanto la relazione è simmetrica). Inoltre, non è possibile che un arco parta e finisca nello stesso punto (in quanto la relazione è antiriflessiva). Caratteristiche differenti sono trovate invece nei *multigrafi*.

Definizione 149 (Multigrafo)**.** *Una terna di insiemi non vuoti (v, l, σ) si dice multigrafo se la funzione sigma è una funzione del tipo $\sigma : l \mapsto P_2(v)$.*

Un multigrafo è quindi composto un insieme di vertici v e da un insieme di lati l. La funzione σ è la funzione che associa ad ogni grafo l'effettiva coppia ordinata di vertici che esso connette. Questo implica che possono esistere più lati che connettono gli stessi vertici (potremmo avere per esempio due lati l_1 e l_2 tali che $\sigma(l_1) = \sigma(l_2)$). Inoltre, dato che ai lati vengono associate coppie ordinate, gli archi sono "a senso unico" in quanto, dati due vertici a e b, ci è dovuto specificare se un lato va da a a b o da b ad a.