

# ALGEBRA e LOGICA

( 6 CFU )

prof. **Fabio Gavarini** e **Andrea Santi**

-----

## INSIEMI, CORRISPONDENZE, RELAZIONI, OPERAZIONI

Insiemi; sottoinsiemi, sovrainsiemi, inclusione. L'insieme delle parti. Operazioni tra insiemi e loro proprietà. Corrispondenze tra insiemi; immagine o controimmagine di sottoinsiemi; corrispondenza inversa. Composizione. Funzioni. Restrizione di una funzione. Famiglie, comparazione con gli insiemi. Funzioni iniettive, suriettive o biiettive; biiettività e corrispondenza inversa. Composizione di funzioni; funzioni invertibili e loro caratterizzazioni. Permutazioni in un insieme. Funzioni caratteristiche in un insieme. Biiezione naturale tra l'insieme delle parti di un insieme  $A$  e l'insieme delle funzioni caratteristiche in  $A$ . Relazioni in un insieme. Proprietà notevoli per una relazione: riflessiva, simmetrica, antisimmetrica, transitiva. Relazioni di preordine, relazioni di ordine, relazioni di equivalenza. L'equivalenza associata a una funzione. La relazione di divisibilità tra interi e tra naturali. La congruenza modulo  $n$  tra numeri interi è una equivalenza. Classi di equivalenza, rappresentanti; insieme quoziente, proiezione canonica. Partizioni di un insieme. Biiezione naturale tra equivalenze in  $X$  e quozienti di  $X$ . Operazioni in un insieme; proprietà speciali, elementi neutri, inversi. Casi speciali: monoidi, gruppi; il gruppo degli invertibili in un monoide. Insiemi con due operazioni; anelli, campi. L'insieme delle parti di un insieme è anello commutativo unitario (non campo) per le operazioni di differenza simmetrica e intersezione.

**Bibliografia:** [Ca] [Capitolo I, paragrafi 1, 2, 3 e 4](#) - [G-P] files [Insiemi](#), [Funzioni e cardinalità](#), [Relazioni 1](#), [Gruppi, anelli, campi](#) - [L-L] Chapters 1, 2 e 3; Appendix B - [PC] Capitolo 1, paragrafi 1, 2 e 3; Capitolo 4, paragrafo 1; Capitolo 5, par. 1 e 2

**Videolezioni:** [Insiemi](#), [Corrispondenze](#), [Funzioni 1](#), [Funzioni 2](#), [Funzioni caratteristiche](#), [Relazioni](#), [Equivalenze 1](#), [Equivalenze 2](#), [Operazioni 1](#), [Operazioni 2](#)

## NUMERI NATURALI

Il Sistema dei Numeri Naturali (=S.N.N.). Il Principio di Induzione Debole (=Pr.I.D.). Ordinamento, somma e prodotto tra naturali; proprietà notevoli. Il Principio di Induzione Forte (=Pr.I.F.), il Principio del Minimo (=Pr.M.); equivalenza tra Pr.I.D., Pr.I.F. e Pr. M. (cenni). Il metodo di dimostrazione per induzione.

Divisione con resto tra numeri naturali. Numerazione in base arbitraria: scrittura posizionale (di un naturale) in base arbitraria; conversione da una base a un'altra.

**Bibliografia:** [AaVv] file [Numeri naturali \(D'Andrea\)](#) - [Ca] [Capitolo I, paragrafi 1 e 5](#); [Capitolo II, paragrafo 2](#) - [G-P] files [Induzione](#), [Aritmetica sugli interi, etc. \(complementi\)](#), paragrafo 1 - [L-L] Chapter 1, section 8; Chapter 11, section 3 - [PC] Capitolo 1, paragrafo 4; Capitolo 2, paragrafo 10

**Videolezioni:** [Naturali](#), [Induzione](#), [Divisione](#), [Numerazione](#)

## CARDINALITÀ, NUMERI CARDINALI

Equipotenza tra insiemi: riflessività, simmetria, transitività. Cardinalità di un insieme, numeri cardinali. Insiemi finiti, o numerabili o infiniti non numerabili. Ordinamento tra cardinali; Teorema di Schroeder-Bernstein (*senza dimostrazione*).

La cardinalità del numerabile è il minimo tra i cardinali infiniti. Caratterizzazione degli insiemi infiniti (per un insieme  $X$ ): (1)  $X$  è infinito, (2) esiste una funzione iniettiva dall'insieme dei numeri naturali ad  $X$ , (3) esiste un sottoinsieme proprio di  $X$  che è equipotente ad  $X$  stesso.

**1° Teorema di Cantor:** L'unione di una famiglia finita (non vuota) o numerabile di insiemi numerabili è numerabile.

**2° Teorema di Cantor:** La cardinalità dell'insieme delle parti di  $X$  è strettamente maggiore della cardinalità di  $X$ .

I numeri cardinali infiniti  $\aleph_n$ . L'ipotesi del continuo generalizzata (cenni). La cardinalità del continuo:  $|\mathbf{R}| = |\mathcal{P}(\mathbf{N})|$  (*senza dimostrazione*).

**Bibliografia:** [AaVv] file [Cardinalità \(D'Andrea\)](#) - [Ca] [Capitolo I, paragrafo 6](#) - [G-P] file [Funzioni e cardinalità](#), paragrafo 5 - [L-L] Chapter 3, section 7 - [PC] Capitolo 1, paragrafo 5

**Videolezioni:** [Cardinalità 1](#), [Cardinalità 2](#)

## NUMERI INTERI, CONGRUENZE, ARITMETICA MODULARE

Insiemi con due operazioni (binarie): anelli, anelli commutativi unitari, campi. L'anello commutativo unitario dei numeri interi, relazione coi numeri naturali, ordinamento, valore assoluto. Divisibilità, divisori, multipli; elementi invertibili, elementi associati. Elementi riducibili, elementi irriducibili. Fattorizzazioni banali, fattorizzazioni equivalenti. Massimo comun divisore (=MCD) e minimo comun multiplo (=mcm). Elementi coprimi.

Divisione con resto tra interi: esistenza e unicità di quoziente e resto (positivo). Esistenza di MCD in  $\mathbf{Z}$ , e identità di Bézout: algoritmo euclideo. Elementi primi; ogni primo è irriducibile; tra i numeri interi, ogni irriducibile è primo (*senza dimostrazione*). L'anello  $\mathbf{Z}_{\setminus 5}$ , comprensivo di esempi di suoi elementi irriducibili ma non primi.

Teorema Fondamentale dell'Aritmetica: esistenza e unicità di una fattorizzazione in irriducibili per interi non nulli e non invertibili. Teorema di Euclide: Esistono infiniti interi irriducibili a due a due non associati.

Forma esplicita di MCD( $a,b$ ) e di mcm( $a,b$ ); la relazione  $MCD(a,b) \cdot mcm(a,b) = a \cdot b$ .

Equazioni diofantee: criterio di esistenza di soluzioni, algoritmo per il calcolo di una soluzione.

Congruenze in  $\mathbf{Z}$  (modulo  $n$ ). Ogni congruenza è una relazione di equivalenza; descrizione delle classi di congruenza e dell'insieme quoziente  $\mathbf{Z}_n$ . Somma e prodotto in  $\mathbf{Z}_n$ . Teorema:  $\mathbf{Z}_n$  è un anello commutativo unitario (*cenni*).

Divisori dello zero, regole di cancellazione. Lemma: In un anello commutativo, non esistono divisori dello zero se e solo se valgono le regole di cancellazione (*cenni*).

Proposizione:  $\mathbf{Z}_n$  è un dominio  $\Leftrightarrow n$  è irriducibile (=primo)  $\Leftrightarrow \mathbf{Z}_n$  è un campo. Criteri di divisibilità in  $\mathbf{Z}$ .

Equazioni congruenziali in  $\mathbf{Z}$ , equazioni modulari in  $\mathbf{Z}_n$ : discussione e risoluzione. Definizione di gruppo. Elementi invertibili in  $\mathbf{Z}_n$ ; criterio di invertibilità, calcolo della classe inversa; la funzione di Eulero. Il Teorema cinese del resto: per  $r,s$  numeri naturali coprimi, gli anelli commutativi unitari  $\mathbf{Z}_{rs}$  e  $\mathbf{Z}_r \times \mathbf{Z}_s$  sono isomorfi. Calcolo di potenze in  $\mathbf{Z}_n$ : generalità, il Teorema di Eulero (*senza dimostrazione*). L'algoritmo di riduzione dell'esponente di una potenza in  $\mathbf{Z}_n$ .

Sistemi di equazioni congruenziali: discussione, risoluzione tramite il Teorema Cinese del Resto o per sostituzioni.

**Bibliografia**: [AaVv] files [Numeri interi \(D'Andrea\), paragrafo 4](#), [Congruenze, aritmetica modulare\(D'Andrea\), paragrafi 1 e 2](#) - [Ca] [Capitolo II, paragrafi da 1 a 6](#) - [G-P] files [Aritmetica sugli interi, congruenze, Teorema Cinese del Resto](#), [Aritmetica sugli interi, etc. \(complementi\)](#) - [L-L] Chapter 11, sections 1 to 9 - [PC] Capitolo 2, paragrafi da 1, 2, 3, 6, 7, 8 e 9

## RETICOLI, ALGEBRE DI BOOLE, FUNZIONI BOOLEANE

Insiemi ordinati; diagramma di Hasse. Sottoinsiemi ordinati, intervalli; ordine prodotto, ordine lessicografico, ordine funzionale. Principio di Dualità per insiemi ordinati. Elementi minimali o massimali, minimo o massimo di un (sotto)insieme ordinato. Minoranti, maggioranti, estremo inferiore e estremo superiore per un sottoinsieme ordinato. Insiemi (semi)limitati. Reticoli. Definizione come insiemi ordinati e definizione come insiemi con due operazioni binarie. Il Teorema di Corrispondenza (per reticoli): Le due definizioni di reticolo sono equivalenti (*con passi principali della dimostrazione*). Principio di Dualità per reticoli. Esempi e controesempi di reticoli. Limiti, complementi, distributività in un reticolo. Proposizione: In un reticolo distributivo, il complemento - se esiste - è unico, e valgono le Leggi di De Morgan. Elementi  $v$ -riducibili o  $v$ -irriducibili; atomi. Proposizione: In un reticolo finito, (a) un elemento è  $v$ -irriducibile  $\Leftrightarrow$  copre al più un elemento, e (b) ogni atomo è  $v$ -irriducibile. Teorema di  $v$ -Fattorizzazione (in  $v$ -irriducibili) per reticoli finiti; unicità della  $v$ -fattorizzazione nel caso distributivo. Teorema di  $v$ -Fattorizzazione Unica (in atomi) per reticoli finiti distributivi complementati (=algebre di Boole finite). Isomorfismi tra reticoli, reticoli isomorfi; sottoreticoli. Criterio di distributività (*senza dimostrazione*).

Algebre di Boole; definizione come reticolo e come anello booleano unitario. Il Principio di Dualità per algebre di Boole. Isomorfismi tra algebre di Boole. Teorema (Stone - caso finito): Ogni algebra di Boole finita è isomorfa all'insieme delle parti dell'insieme dei suoi atomi. Sottoalgebre di Boole. Teorema (Stone - caso generale): Ogni algebra di Boole è isomorfa a una sottoalgebra di Boole di un insieme delle parti (*senza dimostrazione*).

Funzioni booleane, polinomi booleani, funzioni booleane polinomiali. Equivalenza tra polinomi booleani.

Prodotti, prodotti fondamentali, prodotti completi. Somme di prodotti; ridondanza e non-ridondanza. Forma Normale Disgiuntiva di un polinomio booleano: esistenza e unicità, calcolo tramite (1) tramite "tavole di verità", oppure (2) manipolazioni successive. Corollario: Ogni funzione booleana sull'algebra di Boole  $\underline{2}$  è polinomiale.

Grandezza di una somma di prodotti. Forme minimali di un polinomio booleano. Implicazione tra polinomi; implicanti primi di un polinomio booleano. Proposizione: Ogni polinomio è equivalente alla somma di tutti i suoi implicanti primi (=s.t.i.p. - *cenni della dimostrazione*). Proposizione: Ogni forma minimale di un polinomio booleano  $f$  è somma di implicanti primi di  $f$  dalla quale non si possa cancellare nessun termine. Il consenso di due prodotti. Il Metodo del Consenso per il calcolo della s.t.i.p. di un polinomio booleano (*senza dimostrazione*). Procedura di calcolo di una forma minimale di un polinomio booleano.

**Bibliografia**: [Ca] [Capitolo I, paragrafo 3\(B\)](#) - [G-P] files [Relazioni - 2](#), [Reticoli](#), [Algebre di Boole](#), [Funzioni booleane](#), [Forme minimali di una funzione polinomiale](#) - [L-L] Chapter 14, sections 1 to 5 and 7 to 11; Chapter 15, sections 1 to 9

**Videolezioni**: [Insiemi ordinati](#), [Reticoli 1](#), [Reticoli 2](#), [Reticoli 3](#), [Algebre di Boole 1](#), [Algebre di Boole 2](#)

## TESTI (libri, dispense, videolezioni, ecc.) consigliati:

- [AaVv] - Autori Vari, [Materiale vario disponibile in rete](#) (per gentile concessione degli autori) -  
- alla pagina [http://www.mat.uniroma2.it/~gavarini/page-web\\_files/mat-didat.html#Mat-Dis\\_altro-mat](http://www.mat.uniroma2.it/~gavarini/page-web_files/mat-didat.html#Mat-Dis_altro-mat)
- [Ca] - G. Campanella, [Appunti di Algebra 1](#) (per gentile concessione dell'autore) - alla pagina  
[http://www.mat.uniroma2.it/~gavarini/page-web\\_files/mat-didat\\_data/dispense-ecc/Algebra\\_1\\_-\\_dispense\\_di\\_Campanella.rar](http://www.mat.uniroma2.it/~gavarini/page-web_files/mat-didat_data/dispense-ecc/Algebra_1_-_dispense_di_Campanella.rar)
- [Ga] - F. Gavarini, [Videolezioni varie](#) - alla pagina <http://didattica.uniroma2.it/files/index/insegnamento/144372>
- [G-P] - L. Geatti, G. Pareschi, [Appunti vari](#) (per gentile concessione degli autori) - alla pagina  
[http://www.mat.uniroma2.it/~gavarini/page-web\\_files/mat-didat\\_data/Algebra-Logica\\_\(ING-INF\)/AL\\_2016-17.html#app\\_alg-log](http://www.mat.uniroma2.it/~gavarini/page-web_files/mat-didat_data/Algebra-Logica_(ING-INF)/AL_2016-17.html#app_alg-log)
- [L-L] - S. Lipschutz, M. Lipson, *Discrete Mathematics*, 3rd Edition, Schaum's Outlines, McGraw-Hill, 2007
- [PC] - G. M. Piacentini Cattaneo, *Algebra - un approccio algoritmico*, ed. Decibel/Zanichelli, Padova, 1996
- 
-