ALGEBRA e LOGICA

Docenti: Fabio GAVARINI & Andrea SANTI

CdL in Ingegneria Informatica 2021-2022

DIARIO del CORSO

PRIMA LEZIONE - *28 Febbraio 2022*:

Presentazione generale del corso.

Insiemi: definizione (naturale, o "ingenua"), descrizioni possibili; appartenenza e non appartenenza di elementi. Famiglie (di oggetti in un insieme): definizione "ingenua".

Sottoinsiemi, sovrainsiemi. Inclusione tra insiemi; l'uguaglianza tra insiemi come doppia inclusione. L'insieme vuoto. L'insieme delle parti di un insieme: definizione, esempi.

Operazioni tra insiemi: intersezione, unione, differenza, complementare (in un sovrainsieme), differenza simmetrica, prodotto cartesiano.

Bibliografia: [Ca] Capitolo I - [G-P] file Insiemi - [L-L] Chapter 1 - [PC] Capitolo 1
Videolezione: *Insiemi* (insiemi, sottoinsiemi, insieme delle parti, operazioni tra insiemi)
Esercizi: *Insiemi*

SECONDA LEZIONE - *3 Marzo 2022*:

Proprietà notevoli delle operazioni tra insiemi: *(1)* commutatività e associatività di intersezione, unione e differenza simmetrica; *(2)* esistenza di elementi speciali; *(3)* distributività e leggi di De Morgan.

Corrispondenze tra insiemi: definizione, notazione. Immagine - tramite una corrispondenza data - di un sottoinsieme del dominio; controimmagine - tramite una corrispondenza data - di un sottoinsieme del codominio. Esempi, casi speciali: relazioni, funzioni; la corrispondenza vuota, la corrispondenza totale; la corrispondenza identica (o "identità") su un insieme.

Costruzioni sulle corrispondenze: operazioni insiemistiche tra corrispondenze, la corrispondenza inversa.

Bibliografia: [Ca] Capitolo I - [G-P] file Insiemi - [L-L] Chapters 1-2 - [PC] Capitoli 1-2
Videolezione: *Corrispondenze* (corrispondenze tra insiemi e operazioni tra di esse)
Esercizi: *Insiemi* - *Corrispondenze*

TERZA LEZIONE - *7 Marzo 2022*:

Costruzioni sulle corrispondenze *(continua)*: composizione tra corrispondenze, e sue proprietà.

Funzioni (o "applicazioni"): definizione, esempi, controesempi. Immagine - tramite una funzione - di un elemento del dominio. La funzione canonicamente associata ad una corrispondenza. Famiglie - di oggetti in un insieme *E* - come funzioni a valori in *E*.

Funzioni iniettive (o "iniezioni"), funzioni suriettive (o "suriezioni"), funzioni biiettive (o "biiezioni").

Caratterizzazione della biiettività di una funzione tramite la corrispondenza inversa.

Bibliografia: [Ca] Capitolo I - [G-P] file Funzioni e cardinalità - [L-L] Chapter 3 - [PC] Capitolo 1

Videolezione: *Funzioni 1* (funzioni; iniettività, suriettività, biiettività)
Esercizi: *Corrispondenze - Funzioni*

QUARTA LEZIONE - *10 Marzo 2022*:

Composizione di funzioni: la composizione di due funzioni è ancora una funzione.
Funzioni invertibili; unicità dell'inversa. Caratterizzazione delle funzioni invertibili in termini intrinseci (biiettività) e in termini della corrispondenza inversa (dev'essere a sua volta una funzione).
Permutazioni in un insieme. Funzioni caratteristiche in un insieme. La funzione caratteristica di un sotto-insieme *F* in un insieme *E*.
La funzione dall'insieme delle parti di un insieme *E* all'insieme delle funzioni caratteristiche in *E* è invertibile: descrizione esplicita della funzione inversa.

Bibliografia: [Ca] Capitolo I - [G-P] file Funzioni e cardinalità - [L-L] Chapter 3 - [PC] Capitolo 1
Videolezione: *Funzioni 2* (composizione di funzioni, funzioni invertibili) - *Funzioni caratteristiche* (funzioni caratteristiche in un insieme).
Esercizi: *Funzioni*

QUINTA LEZIONE - *14 Marzo 2022*:

Relazioni (binarie) in un insieme; operazioni insiemistiche tra relazioni, composizione, inversa e potenze di relazioni (in uno stesso insieme).
Proprietà notevoli per una relazione: riflessività, transitività, simmetricità, antisimmetricità.
Relazioni di preordine; relazioni d'ordine, relazioni d'ordine totale; relazioni di equivalenza. Esempi e controesempi. In ogni insieme, la relazione identità è un ordine *e* un'equivalenza.
La divisibilità tra numeri interi è un preordine, ma non un ordine; la divisibilità tra numeri naturali è un ordine, ma non è totale. Nell'insieme delle parti (di un insieme *X* qualunque), l'inclusione è un ordine, che è totale se e soltanto se *X* ha meno di due elementi.
Ad ogni funzione *f* da *X* a *Y* è associata in modo canonico una relazione in *X* che è una equivalenza.
Partizioni in un insieme: definizione, esempi, controesempi.

Bibliografia: [Ca] Capitolo I - [G-P] file Relazioni 1 - [L-L] Chapter 2 - [PC] Capitolo 1
Videolezioni: *Relazioni (relazioni in un insieme: generalità, esempi)*
Esercizi: *Insiemi, funzioni, relazioni - Relazioni 1 - Relazioni 2*

SESTA LEZIONE - *17 Marzo 2022*:

Famiglie di sottoinsiemi in un insieme; insieme quoziente e proiezione canonica associati.
Nel caso di una partizione, la proiezione canonica associata è una funzione suriettiva (e viceversa).
L'equivalenza associata all'insieme quoziente di una partizione.
Classi di equivalenza e loro proprietà fondamentali.
Proposizione: La famiglia delle classi di equivalenza (per una equivalenza data) in *E* è una partizione di *E*.
Teorema: Le due funzioni che associano, rispettivamente, una equivalenza al quoziente di una partizione, ed un quoziente di una partizione ad una equivalenza, sono una l'inversa dell'altra *(cenni di dimostrazione)*.

Bibliografia: [Ca] Capitolo I - [G-P] Relazioni 1 - [L-L] Chapter 2 - [PC] Capitolo 1
Videolezioni: *Equivalenze 1 (equivalenze e partizioni) - Equivalenze 2 (equivalenze e funzioni)*
Esercizi: *Relazioni 1 - Relazioni 2*

SETTIMA LEZIONE - *21 Marzo 2022*:

NOTA: ogni equivalenza in un insieme *A* è l'equivalenza indotta da una qualche funzione con dominio *A*.

Sistema dei numeri naturali (=S.N.N.): definizione tramite gli *assiomi di Peano*; il Principio di Induzione Debole, o Semplice (=Pr.I.D./S.). Esistenza e unicità di un S.N.N. (cenni).

Ordinamenti *buoni*: definizione, proprietà *"buono"* implica *"totale"*.

La relazione d'ordine in un S.N.N. (definizione tramite il Pr.I.D.).

Le operazioni di somma e prodotto in un S.N.N. (definizione ricorsiva, tramite il Pr.I.D.).

Le proprietà fondamentali delle operazioni di somma e di prodotto e della relazione d'ordine standard in un S.N.N.; somma e prodotto sono compatibili con la relazione d'ordine.

Bibliografia: [AaVv] Numeri naturali *(D'Andrea)* - [Ca] Capitolo I - [PC] Capitolo 1

Videolezione: *Naturali (sistema dei numeri naturali: assiomi di Peano, ordine, operazioni)*

Esercizi: *Principio di Induzione*

OTTAVA LEZIONE - *24 Marzo 2022*:

Proprietà notevoli della relazione d'ordine in un S.N.N..

Il Principio di Induzione Forte (=Pr.I.F.), il Principio del Minimo (=Pr.M.); l'equivalenza tra il Pr.I.D., il Pr.I.F. e il Pr. M.

Il metodo di dimostrazione per induzione (*debole* o *forte* o mediante *principio del minimo*): idea, strategia - base, passo induttivo (con ipotesi induttiva), ecc.

La divisione con resto tra numeri naturali. Esistenza e unicità di quoziente e resto nella divisione: dimostrazione dell'esistenza per induzione in tre modi diversi (col Pr.I.D., col Pr.I.F. e col Pr.M.).

Bibliografia: [AaVv] Numeri naturali *(D'Andrea)* - [Ca] Capitolo II - [G-P] files Induzione e Aritmetica sugli interi, etc. (complementi) - [L-L] Chapter 1, Chapter 11 - [PC] Capitolo 1, Capitolo 2

Videolezioni: *Induzione (metodo di dimostrazione per induzione [semplice / forte / minimo])* - *Divisione (divisione con resto tra numeri naturali)*

Esercizi: *Principio di Induzione*

NONA LEZIONE - *28 Marzo 2022*:

Scrittura posizionale (di un numero naturale) in base *b* (>1) arbitraria: idee e definizioni preliminari.

Teorema di Esistenza e Unicità per la scrittura posizionale (di un numero naturale) in base *b* (>1) arbitraria.

Algoritmo effettivo per il calcolo della scrittura posizionale di un numero naturale (in base arbitraria).

Esempi espliciti di calcolo della scrittura posizionale di un numero dato.

Esempi espliciti di calcolo di somma e prodotto con scrittura posizionale in base arbitraria (cenni).

Bibliografia: [Ca] Capitolo II - [PC] Capitolo 1, Capitolo 2

Videolezione: *Numerazione (numerazione in base arbitraria / scrittura posizionale)*

Esercizi: *Scrittura posizionale*

DECIMA LEZIONE - *31 Marzo 2022*:

La relazione di equipotenza tra insiemi. La cardinalità (o "potenza") di un insieme; numeri cardinali.

Insiemi finiti e insiemi infiniti. Insiemi numerabili. Ogni insieme numerabile è infinito.

Relazione d'ordine (buono) tra numeri cardinali; il Teorema di Schroeder-Bernstein (senza dimostrazione della transitività e dell'essere buono).

Proposizione: *(a)* Ogni insieme infinito contiene un sottoinsieme numerabile. *(b)* Ogni sottoinsieme di un insieme numerabile o è finito oppure è numerabile.

Bibliografia: [AaVv] file Cardinalità *(D'Andrea)* - [Ca] Capitolo I - [G-P] file Funzioni e cardinalità - [L-L] Chapter 3 - [PC] Capitolo 1

Videolezione: *Cardinalità 1 (insiemi equipotenti, cardinalità; Primo Teorema di Cantor)*

Esercizi: *Cardinalità (N.B.: in linea di massima, questi esercizi sono un po' più difficili della media)*

UNDICESIMA LEZIONE - *4 Aprile 2022*:

Proposizione: Ogni insieme infinito contiene un sottoinsieme numerabile; ogni sottoinsieme di un insieme numerabile o è finito oppure è numerabile.

Caratterizzazione degli insiemi infiniti: Per ogni insieme X le seguenti proprietà sono a due a due equivalenti: *(a)* X è infinito, *(b)* esiste una funzione iniettiva dall'insieme **N** dei numeri naturali ad X, *(c)* esiste un sottoinsieme proprio X' di X che è equipotente ad X stesso.

Proposizione: **N** è equipotente a **N**×**N** .

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

Applicazioni: **Z** , **Z**x**Z** e **Q** sono numerabili.

2° Teorema di Cantor: Per ogni insieme X, la cardinalità dell'insieme delle parti $\mathcal{P}(X)$ e la cardinalità dell'insieme delle funzioni caratteristiche $\mathbf{2}^X$ sono strettamente maggiori della cardinalità di X stesso.

I numeri cardinali infiniti superiori $\aleph_n$ (per ogni n in **N**).

La cardinalità del continuo: $|\mathbf{R}| = |\mathcal{P}(\mathbf{N})| =: \aleph_0$ (*senza dimostrazione*).

L'ipotesi del continuo generalizzata (cenni).

La "distribuzione" dei numeri cardinali rispetto alla relazione d'ordine (cenni).

Bibliografia: [AaVv] file Cardinalità *(D'Andrea)* - [Ca] Capitolo I - [G-P] file Funzioni e cardinalità - [L-L] Chapter 3 - [PC] Capitolo 1

Videolezione: *Cardinalità 1 (insiemi equipotenti, cardinalità; Primo Teorema di Cantor)* - *Cardinalità 2 (Secondo Teorema di Cantor)*

Esercizi: *Cardinalità (N.B.: in linea di massima, questi esercizi sono un po' più difficili della media)*

DODICESIMA LEZIONE - *7 Aprile 2022*:

L'insieme **Z** dei numeri interi: relazione coi numeri naturali, operazioni (somma e prodotto), ordinamento, valore assoluto. **Z** è un anello commutativo unitario senza divisori di zero, e la relazione d'ordine in esso è totale. Divisibilità, multipli e divisori in **Z**. Elementi unità (=invertibili) in **Z**; elementi associati.
Elementi riducibili, irriducibili, primi.
Lemma: Ogni primo è irriducibile.
Fattorizzazioni di un elemento, fattorizzazioni banali.
Teorema Fondamentale dell'Aritmetica (esistenza): Per ogni intero non nullo e non invertibile esiste una fattorizzazione in prodotto di interi irriducibili.
Teorema di Euclide: Esistono infiniti interi irriducibili.
Massimo comun divisore (=*M.C.D.*) e minimo comun multiplo (=*m.c.m.*). Interi primi tra loro (o "coprimi").

Bibliografia: [Ca] Capitolo II, paragrafi 2 e 3 - [G-P] file Aritmetica sugli interi, congruenze, Teorema Cinese del Resto - [L-L] Chapter 11, sections 1-3, 5-7 - [PC] Capitolo 2, paragrafi 1-3
Esercizi: *Numeri Interi*

TREDICESIMA LEZIONE - *11 Aprile 2022*:

Divisione con resto tra numeri interi: esistenza e unicità di quoziente e resto (positivo).
Esistenza del *MCD* in **Z**, e identità di Bézout per esso: dimostrazione e calcolo mediante l'algoritmo euclideo delle divisioni successive. *Esempi* di calcolo esplicito.
Lemma di Euclide: In **Z**, ogni irriducibile è primo *(senza dimostrazione)*.
Teorema Fondamentale dell'Aritmetica: esistenza e unicità di una fattorizzazione in irriducibili per interi (non nulli) non invertibili *(cenni di dimostrazione dell'unicità)*.

Bibliografia: [AaVv] file Numeri interi *(D'Andrea)*, paragrafo 4 - [Ca] Capitolo II, paragrafi 1-3 - [G-P] file Aritmetica sugli interi, congruenze, Teorema Cinese del Resto - [L-L] Chapter 11, sections 4-7 - [PC] Capitolo 2, paragrafi 2-3
Esercizi: *MCD tra interi, Equazioni diofantee*

QUATTORDICESIMA LEZIONE - *14 Aprile 2022*:

La fattorizzazione "canonica" di un intero. La relazione tra la fattorizzazione "canonica" di un intero e quella di un suo qualunque divisore o multiplo. Forma esplicita di *MCD*(*a*,*b*) e di *mcm*(*a*,*b*) in termini di fattorizzazioni di *a* e di *b* ; la relazione *MCD*(*a*,*b*) *mcm*(*a*,*b*) = *a b.*
Calcolo di *mcm*(*a*,*b*) tramite il calcolo di *MCD*(*a*,*b*) - con l'algoritmo euclideo delle divisioni successive - e la formula *mcm*(*a*,*b*) = *a b* / *MCD*(*a*,*b*).
L'anello Z[\sqrt -5], comprensivo di esempi di suoi elementi irriducibili ma non primi.
Equazioni diofantee: definizione, criterio per l'esistenza di soluzioni, procedura per il calcolo esplicito di una soluzione. Esempi.

Bibliografia: [Ca] Capitolo II, paragrafi 2-4 - [G-P] file Aritmetica sugli interi, congruenze, Teorema Cinese del Resto - [L-L] Chapter 11, sections 6-8 - [PC] Capitolo 2, paragrafi 2-3, 6-7
Esercizi: *Scrittura posizionale, MCD, Equazioni diofantee - MCD tra interi, Equazioni diofantee*

QUINDICESIMA LEZIONE - *21 Aprile 2022*:

Congruenze ≡_*n* in **Z**. Ogni congruenza è una equivalenza; descrizione delle classi di congruenza e dell'insieme quoziente **Z**_*n* := **Z** / ≡_*n.* Compatibilità di somma e prodotto con ogni congruenza modulo *n*.
Aritmetica modulare: somma e prodotto in **Z**_*n.* Insiemi con due operazioni (binarie): anelli, anelli commutativi unitari, campi.
Teorema: **Z**_*n* è un anello commutativo unitario *(esercizio - cenni di dimostrazione)*.
Divisori dello zero, regole di cancellazione: definizioni.
Lemma: In un anello commutativo, non esistono divisori dello zero se e solo se valgono le regole di cancellazione *(esercizio -- cenni di dimostrazione)*.
Proposizione: *(a)* non esistono divisori di zero in **Z**_*n* ⇔ *n* è primo; *(b)* non esistono divisori di zero in **Z**_*n* ⇔ **Z**_*n* è un campo; *(c)* **Z**_*n* è un campo ⇔ *n* è irriducibile.
Equazioni congruenziali, equazioni modulari, equazioni diofantee: definizioni.

Bibliografia: [Ca] Capitolo II, paragrafi 4-5 - [G-P] file Aritmetica sugli interi, congruenze, Teorema Cinese del Resto; file Aritmetica sugli interi, etc. (complementi) - [L-L] Chapter 11, sections 8-9 - [PC] Capitolo 2, paragrafi 6-7
Esercizi: *MCD tra interi, Equazioni diofantee - Equazioni congruenziali, Equazioni modulari*

SEDICESIMA LEZIONE - *28 Aprile 2022*:

Equazioni congruenziali, *equazioni modulari*, *equazioni diofantee*: connessioni tra le une e le altre.
Criterio di esistenza di soluzioni, algoritmo per il calcolo di una soluzione, insieme completo di soluzioni per equazioni diofantee, equazioni congruenziali ed equazioni modulari. Esempi di risoluzione di equazioni modulari.
Elementi invertibili in **Z**_*n*; formula esplicita della soluzione di un'equazione modulare in caso di esistenza e unicità. Definizione di gruppo. Il gruppo *U*(**Z**_*n*) degli elementi invertibili in **Z**_*n*: criterio di invertibilità, calcolo dell'inverso mediante risoluzione di una equazione modulare (dunque congruenziale, dunque diofantea).
Corollario: **Z**_*n* è un campo ⇔ *n* è irriducibile

Bibliografia: [Ca] Capitolo II, paragrafi 4, 5 e 6 - [G-P] file Aritmetica sugli interi, congruenze, Teorema Cinese del Resto; file Aritmetica sugli interi, etc. (complementi) - [L-L] Chapter 11, sections 8 and 9 - [PC] Capitolo 2, paragrafi 6-9.
Esercizi: *MCD tra interi, Equazioni diofantee - Equazioni congruenziali, Equazioni modulari - Aritmetica modulare*

DICIASSETTESIMA LEZIONE - *2 Maggio 2022*:

La funzione φ di Eulero: definizione, proprietà, formula esplicita. Il prodotto Cartesiano di un numero finito di anelli commutativi unitari è un anello commutativo unitario. Il *Teorema cinese del resto:* per r,s numeri naturali coprimi, gli anelli commutativi unitari **Z**_{rs} e **Z**_*r* x **Z**_*s* sono isomorfi.
Ripetitività delle potenze in **Z**_*n*: generalità, caratterizzazione del caso delle potenze con base una classe invertibile. Il *Teorema di Eulero* (senza dimostrazione). L'algoritmo di riduzione dell'esponente di una potenza in **Z**_*n* . Esempi di calcolo di potenze modulari.
Criteri di divisibilità in **Z**: strategia generale (calcolo di una classe in **Z**_*n*), esempi specifici.

Bibliografia: [Ca] Capitolo II, paragrafi 4, 5 e 6 - [G-P] file Aritmetica sugli interi, congruenze, Teorema Cinese del Resto; file Aritmetica sugli interi, etc. (complementi) - [L-L] Chapter 11, sections 8 and 9 - [PC] Capitolo 2, paragrafi 6-9
Esercizi: *Aritmetica modulare - MCD tra interi, Equazioni diofantee*

DICIOTTESIMA LEZIONE - 5 *Maggio 2022*:

Sistemi di equazioni congruenziali: discussione, sistemi in forma risolta, sistemi in forma cinese (o "sistemi cinesi"). Il *Teorema Cinese del Resto* per sistemi in forma cinese. Metodo di risoluzione di un sistema tramite sostituzioni successive oppure - sotto le ipotesi del caso - tramite la procedura fornita dal *Teorema Cinese del Resto*. *Esempi* di risoluzione di un sistema di equazioni congruenziali.
Bibliografia: [Ca] Capitolo II, paragrafo 5 - [G-P] file Aritmetica sugli interi, congruenze, Teorema Cinese del Resto - [L-L] Chapter 11, section 9 - [PC] Capitolo 2, paragrafo 7
Esercizi: *Equazioni congruenziali e modulari - Aritmetica modulare - MCD tra interi, Equazioni diofantee*

DICIANNOVESIMA LEZIONE - 9 *Maggio 2022*:

Relazioni d'ordine, insiemi ordinati. Ordini totali, ordini buoni: ogni ordine buono è totale. Il *Principio di Dualità* per insiemi ordinati. Relazione di copertura e diagramma di Hasse per un insieme ordinato. Elementi minimali - risp. massimali - minimo *min*(*E'*) - risp. massimo *max*(*E'*) - per un sottoinsieme *E'* in un insieme ordinato *E*; unicità di *min*(*E'*) - risp. di *max*(*E'*) - se esiste. Minoranti - risp. maggioranti – estremo

inferiore *inf*(*E'*) - risp. estremo superiore *sup*(*E'*) – per un sottoinsieme *E'* in un insieme ordinato *E*; unicità di *inf*(*E'*) - risp. di *sup*(*E'*) - se esiste.
Sottoinsiemi (semi)limitati in un insieme ordinato. Intervalli - chiusi, aperti, semi-chiusi/aperti, limitati o illimitati - in un insieme ordinato qualsiasi.

Bibliografia: [Ca] Capitolo 1, paragrafo 3(B) - [G-P] file Relazioni - 2 - [L-L] Chapter 14, sections 1, 2, 3, 5 e 7
Videolezione: *Insiemi ordinati (generalità, esempi, elementi speciali)*
Esercizi*: Insiemi ordinati, Reticoli*

VENTESIMA LEZIONE - 11 *Maggio 2022*:

L'ordine indotto in un sottoinsieme *E'* di un insieme ordinato *E*. L'ordine indotto nell'insieme *E^S* da un insieme qualsiasi *S* a un insieme ordinato *E*. L'*ordine prodotto* e l'*ordine lessicografico* in un prodotto cartesiano di insiemi ordinati.
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)*.
Il *Principio di Dualità* per reticoli (in termini di relazione d'ordine e in termini di operazioni).
Esempi di reticoli: gli insiemi con ordinamento totale, l'insieme delle parti di un insieme, **N** e **N_**+ con la divisibilità, ogni intervallo in un reticolo, il reticolo dei divisori di *n*. Prodotti diretti di reticoli; reticoli di funzioni. *Controesempi:* insiemi ordinati che *non* sono reticoli.

Bibliografia: [G-P] file Relazioni - 2; file Reticoli, paragrafi 1 e 2 - [L-L] Chapter 14, section 8
Videolezioni: *Reticoli 1 (generalità, esempi; complementi in un reticolo; distributività)*
Esercizi*: Reticoli, Algebre di Boole - Insiemi ordinati, Reticoli*

VENTUNESIMA LEZIONE - 12 *Maggio 2022*:

Proposizione: Ogni reticolo finito è limitato. - *Controesempi* alla proposizione.
Complementi in un reticolo limitato; *reticoli complementati*. Questioni di esistenza e unicità del complemento, esempi e controesempi. I reticoli N_*5* e M_*5* sono complementati.
Reticoli distributivi. Esempi e controesempi: *P*(*X*) e ***D_n*** sono distributivi, N_*5* e M_*5* non sono distributivi.
Proposizione: In un reticolo distributivo, il complemento - se esiste - è unico, e valgono le *Leggi di De Morgan* per il complemento di $x \vee y$ e di $x \wedge y$.
$\vee$-*Fattorizzazione* in un reticolo; elementi $\vee$-riducibili o $\vee$-irriducibili. Atomi (in un reticolo limitato inferiormente). Esempi e controesempi di $\vee$-riducibili, di $\vee$-irriducibili e di atomi.
Proposizione: In un reticolo finito, *(a)* un elemento è $\vee$-irriducibile $\Leftrightarrow$ copre al più un elemento, e *(b)* ogni atomo è $\vee$-irriducibile.

Bibliografia: [G-P] file Reticoli, paragrafi 3 e 4 - [L-L] Chapter 14, sections from 8 to 11
Videolezioni: *Reticoli 1 (generalità, esempi; complementi in un reticolo; distributività) - Reticoli 2 (*$\vee$*-fattorizzazione:* $\vee$*-irriducibili, atomi, esistenza/unicità di* $\vee$*-fattorizzazioni)*
Esercizi: *Reticoli, Algebre di Boole*

VENTIDUESIMA LEZIONE - *16 Maggio 2022*:

Teorema: In un reticolo finito, ogni elemento ha una $\vee$-fattorizzazione in fattori $\vee$-irriducibili non ridondante (cioè i fattori sono a due a due non comparabili).
Proposizione: In un reticolo distributivo, una $\vee$-fattorizzazione non ridondante in fattori

V-irriducibili - se esiste - è unica, a meno dell'ordine dei fattori.
Teorema di V*-Fattorizzazione Unica (in* V*-irriducibili, non ridondante)* per reticoli finiti distributivi.
Proposizione: In un reticolo finito unicamente complementato, ogni elemento V-irriducibile (diverso dal minimo) è un atomo.
Teorema di V*-Fattorizzazione Unica (in atomi a due a due distinti)* per reticoli finiti distributivi complementati.

Bibliografia: [G-P] file Reticoli, paragrafi da 4 a 6 - [L-L] Chapter 14, sections 8 to 11; Chapter 15, sections 1, 2, 4 and 5
Videolezioni: *Reticoli 2 (*V*-fattorizzazione:* V*-irriducibili, atomi, esistenza/unicità di* V*-fattorizzazioni)*
Esercizi: *Reticoli, Algebre di Boole*

VENTITREESIMA LEZIONE - *19 Maggio 2022*:

Sottoreticoli in un reticolo; ogni sottoreticolo è a sua volta un reticolo. Isomorfismi tra reticoli, proprietà fondamentali. Reticoli isomorfi; l'essere isomorfi è una relazione di equivalenza tra reticoli.
La "forma" di un reticolo ***D_n*** (*n* > 0). Criterio di isomorfismo tra un reticolo ***D_r*** e un reticolo ***D_s*** .
Teorema (caratterizzazione dei reticoli distributivi): Un reticolo è distributivo se e soltanto se non contiene sottoreticoli isomorfi a N*_5* oppure a M*_5 (cenni)*.
Algebre di Boole: definizione come reticoli, definizione come insiemi con due operazioni; equivalenza delle due definizioni *(idea della dimostrazione)*. Il *Principio di Dualità* per algebre di Boole.
Esempi di algebre di Boole: l'insieme delle parti *P*(*X*); le funzioni a valori in un'algebra di Boole; Prodotti di algebre di Boole; i prodotti {0,1}^n**;** Il caso degli insiemi totalmente ordinati.
Anelli booleani. *Teorema di Equivalenza (Stone):* Ogni algebra di Boole corrisponde a un anello booleano unitario, e viceversa *(forma esplicita della corrispondenza e idea della dimostrazione)*. L'esempio fondamentale: *P*(*X*) come anello booleano unitario con la "differenza simmetrica" come somma.
Isomorfismi tra algebre di Boole, algebre di Boole isomorfe; la relazione di "essere isomorfe" tra algebre di Boole è un'equivalenza.

Bibliografia: [G-P] file Reticoli, paragrafi da 5 a 6; file Algebre di Boole - [L-L] Chapter 14, section 8; Chapter 15, sections 1 to 6
Videolezioni: *Reticoli 3 (sottoreticoli; isomorfismi di reticoli, reticoli isomorfi), Algebre di Boole 1 (definizioni; esempi, controesempi; Teorema di Equivalenza [con anelli booleani unitari]) - Algebre di Boole 2 (isomorfismi tra algebre di Boole, sottoalgebre di Boole; Teorema di Rappresentazione di Stone [caso finito, caso generale])*
Esercizi: *Reticoli, Algebre di Boole*

VENTIQUATTRESIMA LEZIONE - *23 Maggio 2022*:

Esempio: la biiezione canonica da *P*(*X*) a 2^*X* - per ogni insieme *X* - è un isomorfismo di algebre di Boole.
Teorema di Rappresentazione (Stone - caso finito): Ogni algebra di Boole finita è isomorfa all'insieme delle parti dell'insieme dei suoi atomi, tramite un isomorfismo canonico esplicito.
Corollario: Ogni algebra di Boole finita è isomorfa all'insieme delle funzioni caratteristiche dell'insieme dei suoi atomi. In particolare, la cardinalità di un'algebra di Boole è sempre una potenza di 2.
Dimostrazione del *Teorema di Rappresentazione (Stone - caso finito)*.
Sottoalgebre di Boole di un'algebra di Boole; esempi, controesempi. *Controesempio* al Teorema di Stone: l'algebra di Boole dei sottoinsiemi finiti o cofiniti di **N** *non* è isomorfa a nessuna algebra di Boole *P*(*X*).
Teorema di Rappresentazione (Stone - caso generale): Ogni algebra di Boole è isomorfa ad una sottoalgebra di Boole dell'insieme delle parti di un opportuno insieme *(senza dimostrazione)*.

L'insieme *F_n*(*B*) delle funzioni booleane in *n* variabili su un'algebra di Boole *B*; struttura di algebra di Boole.
L'insieme *P_n* dei polinomi booleani in *n* variabili; funzioni booleane indotte da un polinomio booleano.
L'insieme *P_n*(*B*) delle funzioni polinomiali su *B*; *P_n*(*B*) è sottoalgebra di Boole di *F_n*(*B*).
Equivalenza tra polinomi booleani (quando inducono la stessa funzione booleana su **2**:={0,1}).
Teorema: Due polinomi booleani sono equivalenti se e soltanto se inducono la stessa funzione booleana su qualsiasi algebra di Boole.

Bibliografia: [G-P] file Algebre di Boole; file Funzioni booleane - [L-L] Chapter 15, sections 6 to 8
Videolezioni: *Algebre di Boole 2 (isomorfismi tra algebre di Boole, sottoalgebre di Boole; Teorema di Rappresentazione di Stone [caso finito, caso generale])*
Esercizi: *Algebre di Boole - Reticoli, Algebre di Boole*

VENTICINQUESIMA LEZIONE - *26 Maggio 2022*:

Prodotti, prodotti fondamentali, prodotti completi in *P_n*.
Lemma: Ogni prodotto in *P_n* è equivalente a un prodotto fondamentale oppure a 0, 1.
Somme di prodotti; somme di prodotti fondamentali, complete, ridondanti / non ridondanti.
Lemma: Ogni somma di prodotti è equivalente ad una somma di prodotti fondamentali completi non ridondante.
La *Forma Normale Disgiuntiva* di un polinomio booleano (=F.N.D.). Esistenza e unicità della F.N.D., metodi operativi per il calcolo (tramite manipolazioni successive o tramite "tavole di verità"). *Esempi* di calcolo della F.N.D. di un polinomio booleano.

Bibliografia: [G-P] file Funzioni booleane - [L-L] Chapter 15, sections 7, 8 and 11
Esercizi: *Polinomi booleani - Algebre di Boole*

VENTISEIESIMA LEZIONE - *30 Maggio 2022*:

Esercizi vari sul calcolo della forma normale disgiuntiva (*=F.N.D.*) di un polinomio booleano.
Lemma: F_n(**2**) = *P_n*(**2**), cioè ogni funzione booleana su **2** è polinomiale.
Misura della "grandezza" di una somma di prodotti; la relazione di "maggior semplicità" tra somme di prodotti. *Forme minimali* di un polinomio booleano: definizione, esistenza e (in generale) non unicità. La relazione di "implicazione" tra polinomi booleani; il legame tra la relazione di *implicazione* e quella di *equivalenza*.

Bibliografia: [G-P] file Funzioni booleane; file Forme minimali di una funzione polinomiale - [L-L] Chapter 15, sections 8, 9 and 11
Esercizi: *Polinomi booleani*

VENTISETTESIMA LEZIONE – *1 Giugno 2022*:

Gli implicanti primi di un polinomio booleano.
Proposizione: Ogni polinomio booleano è equivalente alla somma di tutti i suoi implicanti primi *(soltanto l'idea della dimostrazione)*.
Proposizione: Ogni forma minimale di un polinomio booleano *f* è una somma di (alcuni) implicanti primi di *f* dalla quale non si può cancellare nessun termine.
La nozione di *consenso* tra due prodotti (fondamentali).
Lemma: La somma di due polinomi in consenso tra loro è equivalente alla loro somma con il loro consenso.
Il *Metodo del Consenso*: algoritmo di calcolo della somma di tutti gli implicanti primi di un polinomio booleano. Algoritmo di selezione di una forma minimale di un polinomio booleano a partire dalla somma di tutti gli implicanti primi del polinomio stesso.

Esempi espliciti di calcolo della somma di tutti gli implicanti primi (*=s.t.i.p.*) e di una forma minimale (*=f.m.*) per un polinomio booleano. Esempi espliciti di polinomi booleani che hanno diverse forme minimali.

Bibliografia: [G-P] file Forme minimali di una funzione polinomiale - [L-L] Chapter 15, section 9
Esercizi: *Polinomi booleani*

VENTOTTESIMA LEZIONE (1 Ora) – *6 Giugno 2022*:

Esercizi vari sul calcolo della somma di tutti gli implicanti primi (*=s.t.i.p.*) e di una forma minimale (*=f.m.*) per un polinomio booleano.

Bibliografia: [G-P] file Forme minimali di una funzione polinomiale - [L-L] Chapter 15, section 9
Esercizi: *Polinomi booleani*

BIBLIOGRAFIA:

[AaVv] Autori Varî, *Materiale vario disponibile in rete* (per gentile concessione degli autori)
scaricabile da
https://www.mat.uniroma2.it/~gavarini/page-web_files/mat-didat_data/Algebra-Logica_%28ING-INF%29/AL_2020-21.html#altro-mat

[Ca] G. Campanella, *Appunti di Algebra 1* (per gentile concessione dell'autore)
scaricabile da
https://www.mat.uniroma2.it/~gavarini/page-web_files/mat-didat_data/dispense-ecc/Algebra_1_-_dispense_di_Campanella.rar

[G-P] L. Geatti, G. Pareschi, *Dispense varie* (per gentile concessione degli autori)
scaricabile da
https://www.mat.uniroma2.it/~gavarini/page-web_files/mat-didat_data/Algebra-Logica_%28ING-INF%29/AL_2016-17.html#app_alg-log

[L-L] S. Lipschutz, M. Lipson, *Discrete Mathematics*, Third Edition, Schaum's Outlines, McGraw-Hill, 2007

[PC] G. M. Piacentini Cattaneo, *Algebra - un approccio algoritmico*, ed. Decibel/Zanichelli, Padova, 1996

==========