Programma del corso di Algebra per Informtica

a.a. 2022/2023

PROF. MATTIA BRESCIA

Parte prima: Il linguaggio e la teoria di base

Introduzione alla logica e calcolo proposizionale

Il linguaggio della matematica ed il problema della formalizzazione. Paradossi. Logica proposizionale. Linguaggio: alfabeto (variabili proposizionali, parentesi, connettivi (AND, OR, implica, se e solo se)), formule ben formate e loro definizione ricorsiva. Sintassi e semantica.
Ordine di precedenza dei connettivi e delle formule tra parentesi. La semantica Definizione semantica della negazione e dei connettivi binari. Funzione di valutazione definita costruttivamente sull'insieme delle formule ben formate. Tavole di verità. Tautologie e contraddizioni. Formule logicamente equivalenti. Idempotenza e commutatività di AND e OR. Tautologia del terzo escluso, di non contraddizione, della doppia negazione. Doppia implicazione scritta a partire da implica e AND.
Tautologie varie: contrapposizione, negazione dell'implicazione, doppia implicazione, implicazione scritta a partire da NOT e OR. NAND, XOR, NOR, NAND. Formule di De Morgan. Ottenere NOT e AND a partire da NOR. Tutti i connettivi possono definirsi semanticamente a partire da NOR (o da NAND). Associatività di AND, OR e se e solo se. Distributività di AND e OR. Transitività dell'implicazione. Esplicitazione di XOR.

Logica dei predicati

Logica dei predicati. Esempio: Aritmetica del primo ordine (N con somma, prodotto, =, successore e minore o uguale). Definizione sintattica di linguaggio del primo ordine. Alfabeto (variabili, costanti, lettere predicative, lettere funzionali con i-arietà, simboli accessori, connettivi, quantificatori, identità), termini e loro definizione ricorsiva, formule atomiche, formule ben formate e loro definizione ricorsiva. Quantificatore esistenziale e quantificatore "esiste ed è unico". Interpretazione e formule valide. Variabili vincolate e libere, formule chiuse. Quantificatori multipli. Negazione dei quantificatori studiati. Quantificatori ristretti.

Teoria assiomatica degli insiemi di base

Introduzione alla teoria degli insiemi. Concetto di insieme. Appartenenza, inclusione (stretta), singleton. Come si scrive un insieme e possibili paradossi. Cenni sull'assiomatizzazione di Zermelo e Fraenkel. Assiomi: Vuoto, Separazione, Estensionalità, Parti, Coppia, Unione (unaria). Unicità dell'insieme vuoto. Unicità dell'insieme delle parti. La collezione di tutti gli insiemi che non appartengono a loro stessi non è un insieme. La collezione di tutti gli insiemi non è un insieme. Operazioni insiemistiche a partire dai connettivi logici. Intersezione e unione binarie. Differenza simmetrica. Differenza.
Utilizzo delle tautologie per ottenere formule valide in teoria degli insiemi: doppia negazione, terzo escluso, doppia inclusione; idempotenza, commutatività ed associatività di intersezione e unione. Associatività della differenza simmetrica. Distributività di intersezione rispetto ad unione e viceversa. Esplicitazione della differenza simmetrica. Leggi di De Morgan insiemistiche. Unione binaria a partire da unione unaria. Intersezione unaria.
Diagrammi di Venn e loro utilità per trovare controesempi in teoria degli insiemi. Vari esempi. Coppia ordinata e sua caratterizzazione. Terna ordinata. Proprietà caratteristica delle terne ordinate. Prodotto cartesiano.

Corrispondenze e funzioni
Corrispondenze tra insiemi e loro rappresentazioni (tabelle, diagrammi, proprietà che le definiscono). Relazioni binarie. Applicazioni tra due insiemi. Dominio, codominio, immagine di un elemento, immagine di una funzione. Notazione alternativa per denotare un insieme. Descrizione esplicita di una funzione. Buona posizione di una funzione. Prodotto relazionale e sua associatività.
Composizione di funzioni e sua descrizione esplicita. Applicazioni costanti, identità, immersione, restrizione e prolungamento. Suriettività e sua caratterizzazione. Negazione della suriettività. Ridotta di un'applicazione. Iniettività e sua caratterizzazione. Negazione dell'iniettività. Restrizioni di funzioni iniettive. Biettività. Composizione di applicazioni biettive, iniettive e suriettive conserva la stessa proprietà. Se la composta è iniettiva, la seconda funzione è iniettiva; Se la composta è suriettiva, la prima funzione è suriettiva. Applicazione immagine. Applicazione antiimmagine. Caratterizzazioni di iniettività, suriettività e biettività utilizzando l'applicazione antiimmagine. Sezioni, retrazioni ed inverse di una funzione.
Caratterizzazione di iniettività, suriettività e biettività usando retrazioni, sezioni ed inverse. Unicità dell'inversa. Se f è una funzione, sono equivalenti: 1) f è biettiva; 2) f ha inversa; 3) f ha sezioni e retrazioni; 4) f ha una ed una sola sezione; 5) l'applicazione antiimmagine porta ogni singleton di elementi del codominio in singleton di elementi del codominio.

Parte seconda: Operazioni su insiemi e strutture algebriche

Semigruppi e strutture algebriche ad una operazione interna
Operazioni binarie interne su un insieme. Notazioni. Proprietà commutativa e associativa. Strutture algebriche. Semigruppi. Elementi neutri a destra e a sinistra. Elemento neutro. Se la struttura algebrica ha un elemento sinistro ed uno destro, allora essi coincidono. Unicità dell'elemento neutro. Monoidi. Notazione per i monoidi. Monoide delle parole su un alfabeto.
Operazioni opposte e cenno ai principi di dualità. L'applicazione che ad ogni operazione (su un certo insieme) associa la sua duale è l'inversa di se stessa. Parti chiuse o stabili di una struttura algebrica. Operazione indotta su una parte, struttura indotta. Sottostrutture. Sottosemigruppi, sottomonoidi. Proprietà conservate e non conservate su sottostrutture. Simmetrici destri e sinistri nei monoidi. Elementi simmetrizzabili ed elementi simmetrici. Se un elemento ha simmetrico sinistro e simmetrico destro, allora questi coincidono. Unicità del simmetrico di un elemento in un monoide.
Opposti in notazione additiva. Notazioni. L'elemento neutro è l'inverso di sé stesso. Gruppi. Cenni a gruppi di simmetrie di figure piane. Gli inversi non si conservano nelle sottostrutture. Sottostrutture generate. Caratterizzazione di sottogruppo generato da una parte (di un gruppo) e di sottomonoide generato dalla parte (di un monoide).
Sottomonoidi e sottogruppi ciclici. Gruppi abeliani. Gruppo degli invertibili in un monoide. Notazione moltiplicativa nei gruppi. L'unità di un sottogruppo è l'unità del gruppo. Traslazioni sinistra e destra in un semigruppo. Elementi cancellabili a sinistra, a destra e cancellabili. Loro caratterizzazione a partire dalle traslazioni. Simmetrizzabile (dx/sx) implica cancellabile (dx/sx). L'inverso non vale. Ogni elemento invertibile di un semigruppo determina traslazioni biettive. Tavola di Cayley di un'operazione binaria e visualizzazione, tramite questa, delle proprietà algebriche della struttura quali commutatività, esistenza di elementi neutri, elementi simmetrizzabili, cancellabili a destra o a sinistra.
L'insieme degli elementi cancellabili a destra (risp. a sinistra) è una parte stabile del monoide di partenza. Potenze (o multipli in notazione additiva) di un elemento di un semigruppo. Regole delle potenze di uno stesso elemento (dimostrate più avanti per Induzione di prima forma). Le potenze di uno stesso elemento commutano sempre. Gruppi ciclici. $m\mathbb{Z}$. I sottogruppi $m\mathbb{Z}$ di $\mathbb{Z}$ sono tutti e soli i sottogruppi di $\mathbb{Z}$ (senza dimostrazione). Omomorfismi tra strutture algebriche ad una operazione binaria. Monomorfismi, epimorfismi, isomorfismi, automorfismi. Inversa di un isomorfismo è un isomorfismo. Gli epimorfismi conservano commutatività, associatività, elementi neutri e simmetrici. Gli isomorfismi conservano anche la cancellabilità. Invarianza delle proprietà algebriche per isomorfismi.

Anelli
Anelli. Notazioni: elementi neutri rispetto alle due operazioni, opposti e inversi, multipli e potenze. Regole: moltiplicazione per lo zero dell'anello, moltiplicazione per l'opposto di un elemento, distributività della moltiplicazione rispetto alla differenza, moltiplicazione per un multiplo dell'unità (la dimostrazione, per Induzione di prima forma, è rimandata) Omomorfismo di anelli. Automorfismo di anelli. Anello delle parti con intersezione e unione. Legge di annullamento del prodotto. Anelli integri, domini di integrità, divisori (sx/dx) dello zero. Un elemento è un divisore sinistro (risp. destro) dello zero se e solo se non è cancellabile a sinistra (risp. a destra). Un anello commutativo unitario è un dominio di integrità se e solo se è privo di divisori dello zero. In un anello con almeno due elementi lo zero non è cancellabile; in particolare lo zero non è invertibile e quindi differisce dall'unità. Corpi e campi. Ogni campo è un dominio di integrità. L'inverso non vale.

Parte terza: Relazioni binarie

Concetti di base
Relazioni binarie. Proprietà riflessiva, antiriflessiva, simmetrica, asimmetrica, transitiva. Per verificare la transitività basta guardare alle terne di elementi a due a due distinti. Relazioni di equivalenza. Relazioni d'ordine. Relazione d'ordine largo e stretto. Per una relazione d'ordine stretto bastano la antiriflessività e la transitività. Relazione duale.
Diagonale di un quadrato cartesiano. Controllo delle proprietà delle relazioni binarie guardando il grafico e la relazione duale. Negazione di alcune delle proprietà elencate.

Relazioni di equivalenza
Congruenza modulo un intero. Nucleo di equivalenza di un'applicazione. Classi di equivalenza. Insieme quoziente. Proprietà fondamentali: ogni classe di equivalenza è non vuota; le classi di equivalenza sono a due a due disgiunte; l'unione (unaria) dell'insieme quoziente è l'insieme stesso. Due elementi sono in relazione di equivalenza se e solo se le classi di cui sono rappresentanti coincidono. Descrizione delle classi di equivalenza rispetto al nucleo di equivalenza di una funzione utilizzando l'applicazione antiimmagine. Teorema fondamentale di omomorfismo per insiemi. Corollario: ogni applicazione è la composta di un'applicazione iniettiva con una suriettiva. Partizioni. Teorema fondamentale su relazioni di equivalenza e partizioni. Applicazioni nel trovare tutte le relazioni di equivalenza su un dato insieme.

Relazioni d'ordine
Definizione di una relazione di ordine largo a partire da una di ordine stretto e viceversa (senza dimostrazione). Insiemi ordinati. Ordine indotto su una parte. Sottoinsiemi ordinati. Elementi confrontabili. Minimo, massimo ed unicità di questi. Buon ordine. Ordine totale ed insiemi totalmente ordinati. Buon ordine implica ordine totale. Applicazioni crescenti ed isomorfismi tra insiemi ordinati. Esistono applicazioni biettive e crescenti che non sono isomorfismi. Relazione di copertura. Diagrammi di Hasse e loro rappresentazione. Due insiemi ordinati finiti sono isomorfi se e solo se possono rappresentarsi con lo stesso diagramma di Hasse (la dimostrazione si rimanda a quando viene definita la finitezza). L'insieme delle parti ordinato mediante l'inclusione è ordinato se e solo se è le parti del vuoto o di un singleton. In un insieme ordinato, elementi minimali e massimali, minoranti e maggioranti di parti.

Principio di induzione e teorema fondamentale dell'aritmetica
Principio di induzione di prima forma. Principio di induzione di seconda forma (o Induzione completa). Teorema fondamentale dell'aritmetica.

Parte quarta: Cenni di calcolo combinatorio

Insiemi finiti ed infiniti
Insiemi finiti. Definizione di ordine o cardinalità di un insieme finito. Cenno all'assioma dell'infinito. Definizione di equipotenza. Un insieme si dice infinito se è equipotente ad una sua parte propria. L'assioma dell'infinito equivale all'asserire l'esistenza di un insieme naturalmente ordinato e non

superiormente limitato (senza dimostrazione). Ne prendiamo uno e lo chiamiamo N, insieme dei numeri naturali. Ogni insieme finito non è infinito (senza dimostrazione). Definizione di unione di un numero finito di insiemi. Principio di inclusione-esclusione con dimostrazione solo per il caso di due e tre insiemi.
Definizione (ricorsiva) di fattoriale di un numero naturale. Numero di applicazioni tra due insiemi finiti. Condizione di esistenza di applicazioni iniettive (risp. suriettive, risp. biettive) tra insiemi finiti. Numero di applicazioni iniettive tra insiemi finiti. Numero di applicazioni biettive tra insiemi finiti. Cardinalità dell'insieme delle applicazioni biettive di un insieme finito in se stesso. Se due insiemi finiti hanno la stessa cardinalità, allora le applicazioni biettive tra i due sono tutte e sole le applicazioni iniettive e tutte e solo le applicazioni suriettive. Ciò non accade negli insiemi infiniti. Cenni sul confronto tra cardinalità di insiemi infiniti. Applicazione biettiva tra N e Z. In un monoide commutativo finito un elemento è cancellabile se e solo se è invertibile. Gli anelli unitari finiti integri sono corpi. I domini di integrità finiti sono cambi.Funzione caratteristica di una parte di un insieme. Esiste una biezione tra le parti di un insieme e l'insieme delle funzioni caratteristiche delle parti dell'insieme stesso. L'insieme delle parti di un insieme di ordine n ha ordine 2^n.

Coefficienti binomiali
Coefficienti binomiali definiti a partire dalle parti di un segmento iniziale di N. $(\forall n \in \mathbb{N})(\sum_{k=0}^{n} \binom{n}{k} = 2^n)$. $(\forall n, k \in \mathbb{N})(k \leq n \to \binom{n}{k} = \binom{n}{n-k})$. Formula ricorsiva dei coefficienti binomiali $(\forall n, k \in \mathbb{N})(k \leq n \to \binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1})$. Triangolo di Tartaglia-Pascal. $(\forall n, k \in \mathbb{N})(k \leq n \to \binom{n}{k} = \frac{n!}{k!(n-k)!})$. Cenno al Teorema Binomiale (o formula di Newton) in un anello commutativo unitario.

Parte quinta: Insiemi ordinati

Insiemi ordinati e principi di dualità
Cenni ai principi di dualità per insiemi ordinati. Relazione duale. Se un insieme ordinato ha minimo, questo è unico ed è l'unico minimale. Teorema duale per il massimo. Ogni insieme ordinato di ordine largo ha elementi massimali e minimali. Se un insieme ordinato finito ha un unico elemento massimale, questo è anche il minimo (senza dimostrazione). Risp. per massimale e massimo. Controesempio nel caso infinito. Relazione d'ordine indotta da una funzione su un insieme. Estremo inferiore e superiore.

Reticoli
Reticoli come strutture d'ordine e come strutture algebriche a due operazioni. Reticoli limitati e completi. Reticolo duale. Principio di dualità per i reticoli. In un reticolo ogni elemento minimale (risp. massimale) è minimo (risp. massimo). In un reticolo ogni parte finita ha estremo inferiore e superiore. Reticolo in un reticolo le operazioni inf e sup sono commutative, associative e per esse vale la legge di assorbimento. Equivalenza tra le nozioni di reticolo come insieme ordinato e di reticolo come struttura algebrica. Reticolo trirettangolo e reticolo pentagonale e alcune loro proprietà.
Operazioni reticolari indotte dall'inclusione nell'insieme delle parti di un insieme. Una funzione tra reticoli come strutture ordinate è un isomorfismo se e solo se lo è tra i reticoli visti come strutture algebriche a due operazioni. Sottoreticoli. Esempio di parte di un reticolo che è un reticolo ma non un sottoreticolo. Ogni intervallo chiuso non vuoto di un reticolo è un sottoreticolo. L'elemento neutro rispetto a $\wedge$ coincide con il massimo. L'elemento neutro rispetto a $\vee$ coincide con il minimo. Elementi complementati in un reticolo limitato. Reticoli complementati. In un reticolo limitato, gli unici elementi confrontabili e complementari sono il minimo ed il massimo del reticolo. Reticoli distributivi e definizioni equivalenti (senza dimostrazione). In un reticolo distributivo ogni complemento è unico. Sottoreticoli di reticoli distributivi sono distributivi. Criterio di distributività di Birkhoff (senza dimostrazione).

Algebre booleane, anelli booleani e reticoli
Algebre booleane. Equivalenza tra anelli booleani, algebre booleane e reticoli booleani (con almeno due elementi); come definire gli uni a partire dagli altri. Teorema di Stone (senza dimostrazione)

nel caso infinito e finito. Conseguenze: Teorema di Stone per i reticoli come strutture ordinate; ogni anello booleano finito ha ordine potenza di 2 (diversa da 1); ogni reticolo booleano finito ha ordine potenza di 2; due anelli booleani finiti sono isomorfi se e solo se hanno lo stesso ordine. Interpretazione delle funzioni caratteristiche come applicazioni a valori in $\mathbb{Z}_2$. Se $s = \{1, \ldots, n\}$, esiste un isomorfismo di anelli tra $(P(s), \Delta, \cap)$ e $(\mathbb{Z}_2^n, +, \cdot)$. Operazioni bit a bit e loro interpretazione come operazioni algebriche booleane.

Parte sesta: Divisibilità

Divisibilità nei monoidi

Divisibilità in un semigruppo commutativo. Divisori e multipli di un elemento. Elementi associati. Caratterizzazione degli elementi associati ad un elemento cancellabile in un monoide commutativo. Due elementi di un monoide commutativo sono associati se e solo se hanno gli stessi multipli e gli stessi divisori. Massimi comuni divisori e minimi comuni multipli. I massimi comuni divisori (risp. i minimi comuni multipli) sono tutti associati tra loro. Divisori banali. Elementi irriducibili in un dominio di integrità. Elementi primi, coppie di elementi coprimi tra loro. Monoidi cancellativi. Monoide fattoriale e definizioni equivalenti. Anelli fattoriali.
In un monoide fattoriale è possibile elencare esplicitamente tutti i divisori di un dato elemento, data una sua fattorizzazione. Numero di divisori di un numero naturale (risp. intero) data una sua scomposizione in fattori primi. Se a e b sono due elementi di un monoide fattoriale e m un massimo comuni divisore di a e b e n un minimo comune multiplo di a e b, allora mn è associato ad ab. In un anello commutativo unitario ogni divisore comune tra due elementi divide ogni combinazione dei due elementi all'interno dell'anello.

Divisibilità in $\mathbb{Z}$

Valore assoluto in $\mathbb{Z}$. Teorema della divisione euclidea. Algoritmo delle divisioni successive. Algoritmo delle divisioni successive esteso. Teorema di Bézout. Lemma di Euclide. In $\mathbb{Z}$ i primi sono tutti e soli gli irriducibili.

Congruenze e anelli quoziente dell'anello degli interi

Congruenze modulo un intero. Operazione (parziale) *mod*. Insieme degli interi modulo m ($m \neq 0$). Relazioni di equivalenza compatibili a destra e a sinistra con un'operazione. Congruenze. Proprietà algebriche ereditate dalla struttura quoziente su una congruenza. Quozienti di semigruppi, monoidi, gruppi, gruppi abeliani, sono strutture dello stesso tipo. Una relazione di equivalenza è una congruenza se e solo se è compatibile a destra e a sinistra con ogni operazione della struttura. Anelli quoziente dell'anello degli interi. $\mathbb{Z}_m$ è un campo se e solo se $\mathbb{Z}_m$ è un dominio di integrità se e solo se m è primo.

Equazioni diofantee ed equazioni congruenziali

Equazioni diofantee di primo grado a due incognite. Equivalenza tra Teorema di Bézout e le seguenti affermazioni: "gli interi a e b sono coprimi se e solo se 1 può scriversi come combinazione di a e di b"; "se d è un massimo comun divisore di a e b, $\langle a, b\rangle = \langle d\rangle$ (come sottogruppi di $(\mathbb{Z}, +)$)"; " se d è un massimo comun divisore tra a e b, l'equazione diofantea $ax + by = c$ ammette soluzioni se e solo se $d|c$". Descrizione dell'insieme delle soluzioni di un'equazione diofantea. Equazioni congruenziali ed equivalenza con equazioni diofantee di primo grado a due incognite. Condizione necessaria e sufficiente perché un'equazione congruenziale di primo grado ad una incognita abbia soluzione. Due caratterizzazioni degli invertibili in $\mathbb{Z}_m$. Metodo risolutivo per equazioni congruenziali di primo grado in una incognita. Periodo di un elemento di un gruppo. Criterio per decidere se due potenze di un elemento di un gruppo sono lo stesso elemento.

Parte settima: Polinomi

Costruzione dell'anello dei polinomi e proprietà elementari

Definizione di polinomio a coefficienti in un anello commutativo unitario come successioni definitivamente nulle di elementi dell'anello stesso. Anello dei polinomi su un anello commutativo unitario e sue

proprietà. Se due polinomi hanno lo stesso grado e coefficienti direttori opposti, allora la somma dei due polinomi avrà grado minore del grado di entrambi, altrimenti il grado della somma è uguale al massimo tra i gradi dei due polinomi. Formula di addizione dei gradi. Se il coefficiente direttore di un polinomio è cancellabile, anche il polinomio è cancellabile. $A[x]$ è un dominio di integrità se e solo se A lo è. Ogni polinomio cancellabile di grado positivo non è invertibile; in particolare nessun anello dei polinomi su un qualche anello è mai un campo. Teorema della divisione lunga. Se A è un anello fattoriale, $A[x]$ è un anello fattoriale.

Radici e divisibilità nell'anello dei polinomi
Omomorfismo di sostituzione. Applicazioni polinomiali. Radici di un polinomio. Teorema del resto. Teorema di Ruffini. Teorema di Ruffini generalizzato. In un dominio di integrità, un polinomio non nullo ha sempre grado maggiore del numero di radici che ha. Principio di identità dei polinomi. L'inverso di questo non vale per nessun anello finito.
Ogni polinomio non nullo su di un campo è associato ad uno e un solo polinomio monico. Rappresentante monico della classe di un polinomio. Esistenza ed unicità (a meno dell'ordine) della decomposizione in fattori monici irriducibili per i polinomi non nulli su di un campo. Criterio di irriducibilità per polinomi su un campo. Un polinomio su un campo A ha radici in questo se e solo se ha almeno un divisore di primo grado in $A[x]$. Se un polinomio di grado > 1 su un dominio di integrità ammette radici, allora non è irriducibile. Un polinomio di grado 2 o 3 su un campo A è irrid. sse non ha radici in A. Teorema fondamentale dell'Algebra e conseguenze (senza dimostrazioni). Ogni polinomio irriducibile di $\mathbb{R}[x]$ ha grado < 3 (senza dimostrazione); in particolare, i polinomi irriducibili di $\mathbb{R}[x]$ sono tutti e soli quelli di grado 1 e quelli di grado 2 che non hanno radici. Ogni polinomio di grado dispari in $\mathbb{R}[x]$ ha una radice (senza dimostrazione). Regola per trovare le radici di polinomi di secondo grado su $\mathbb{R}$ (senza dimostrazione). Criterio di irriducibilità di Eisenstein (senza dimostrazione). In $\mathbb{Q}[x]$ ci sono polinomi irriducibili di qualunque grado positivo. Le radici razionali di un polinomio su $\mathbb{Z}$ si possono trovare tra i numeri che hanno a numeratore un divisore del termine noto e a denominatore un divisore del coefficiente direttore del polinomio (senza dimostrazione). Ogni radice razionale di un polinomio monico su $\mathbb{Z}$ è intera.

Parte ottava: Grafi

Introduzione ai grafi
Due definizioni equivalenti di grafo. Multigrafo. Rappresentazione grafica di grafi e multigrafi. Estremi di un arco (o lato), vertici adiacenti archi incidenti, grado di un vertice e sua parità, grafi completi e grafi completi su un numero finito di vertici, grafo complementare, sottografo, (multi)grafi finiti. Isomorfismi ed automorfismi tra grafi e proprietà conservate. Grafi piani (o planari). Grafi bipartiti. Teorema di Kuratowski (senza dimostrazione). Formula che lega il numero dei vertici a quello degli archi in un grafo finito.

Cammini e circuiti, foreste e alberi
Cammini e loro lunghezza, circuiti, componenti connesse, grafi connessi. Cammini su multigrafi, cammini euleriani e circuiti euleriani. Teorema di Eulero: Un multigrafo finito privo di vertici isolati ha un circuito euleriano se e solo se è connesso e tutti i suoi vertici sono pari. Foreste e alberi. Un grafo finito è una foresta se e solo se esiste al più un cammino tra ogni coppia di vertici. Un grafo finito è un albero se e solo se esiste uno ed un solo cammino tra ogni coppia di vertici. Foglie di un albero. Ogni albero finito con almeno due vertici ha una foglia. Un albero di n vertici ha $n-1$ archi. Un albero finito con almeno due vertici ha almeno due foglie. Formule che legano numero di vertici, di archi e di componenti connesse in un multigrafo e in una foresta (no dim.). Se g è un grafo finito con n archi, le seguenti sono equivalenti: g è un albero; g è connesso e i vertici di g sono $n+1$; g è una foresta e i vertici di g sono $n+1$.

Testi consigliati

Il corso non si basa su nessun libro di testo specifico, quindi il consiglio è quello di studiare seguendo le lezioni registrate (se disponibili) o prendendo appunti in classe. Per chi volesse trovare materiale da cui studiare, consiglio i seguenti da cui trarre esercizi e spunti:

E. Mendelson, *Introduction to Mathematical Logic*, Springer, New York, 2005.

Alberto Facchini, *Algebra e matematica discreta*, Decibel, Padova, 2000

G. Cutolo, *Note al corso di Algebra*.

Un paio di consigli

Per quanto riguarda gli esami.

- Se non avete seguito il corso (o vi siete iscritti da poco al team) cercate gli argomenti in uno dei libri di testo o degli appunti consigliati (o da appunti di qualche compagno di corso diligente e generoso) e integrate da lì.
- Cercate di svolgere tutti gli esercizi che sono presenti come materiale didattico (ad esempio nel team) e confrontatevi sui risultati, in modo da poter migliorare la vostra consapevolezza.
- Consultate il sito del prof. Cutolo. Lì troverete tante prove d'esame passate (sullo stile di quelle che faremo in futuro) e anche interessanti appunti su temi che abbiamo trattato.
- Studiate bene le definizioni, comprendendole, perché senza queste è molto difficile passare anche solo l'esame scritto.
- Studiate bene le dimostrazioni, ovviamente capendone il significato, perché senza queste è molto difficile che si passi l'orale.
- Tralasciare del tutto (o in buona parte) interi capitoli del programma risulterà in una bocciatura. Se tentate l'orale senza aver studiato per niente i grafi, ad esempio, ed io capisco che è un capitolo che avete del tutto tralasciato, l'esame non potrà procedere.
- Non tutto è richiesto essere impeccabile o può essere perfetto, ma il programma dev'essere affrontato integralmente e con metodo.
- Siate consapevoli che nell'esame scritto di Algebra (uguale per tutti e tre i canali) non ci sono automatismi ed è pensato a posta per testare la vostra comprensione della materia. Quindi la sola strada è studiare bene e con cognizione di causa.
- Non esitate a farmi domande su esercizi, definizioni e teoremi. A volte una mano può essere molto utile e chiedere non costa niente.
- Confrontatevi con gli altri anche sulla teoria. È sempre utile scambiarsi opinioni e correggere i propri errori in gruppo.
- L'esame è monolitico e non esiste una distinzione formale tra "scritto" e "orale", che verranno spesso affrontati lo stesso giorno (quando possibile). Allo stesso modo, lo studio da riservare alla prova scritta non può prescindere da quello da riservare alla prova orale e viceversa.