Corso di ALGEBRA (1°Gruppo)
per il Corso di Laurea (triennale) in INFORMATICA
(per gli studenti i cui cognomi iniziano con lettere comprese fra **A** e **CO**)

Anno Accademico 2004-2005

(A) Docenti. Titolare: prof. Salvatore Rao. Ha collaborato allo svolgimento del corso il dr. Giovanni Cutolo.

(B) Sommario del programma.

•Elementi di logica intuitiva. Proposizioni. Principali connettivi vero-funzionali: negazione, congiunzione, disgiunzione (inclusiva, esclusiva), condizionale, bicondizionale, NAND, NOR. Tavole di verità dei connettivi. Enunciati atomici ed enunciati composti, variabili e forme proposizionali, funzioni di verità e tavole di verità di forme proposizionali. Tautologie (forme proposizionali logicamente valide) e contraddizioni, proposizioni logicamente vere o logicamente false (secondo il calcolo proposizionale); equivalenza logica. Esempi di tautologie della logica classica: legge della doppia negazione, legge del terzo escluso, legge di non contraddizione, legge dell'inferenza, legge di contrapposizione, legge del sillogismo; leggi di idempotenza, commutative, associative, distributive della congiunzione e della disgiunzione; leggi di De Morgan, relazioni fra i connettivi. Predicati e quantificatori. Quantificatori e negazione, quantificatori e congiunzione, quantificatori e disgiunzione. Inferenze corrette o non corrette, valide oppure non valide. Cenni sulla logica dei predicati con identità.

•Il linguaggio di base della teoria degli insiemi. I predicati primitivi di collezione e di appartenenza ["... è una collezione", "... appartiene a ..."]; connessione fra uguaglianza e appartenenza ["Delle collezioni coincidono se e solo se hanno gli stessi elementi"]. Inclusione e inclusione stretta. La classe **Set** di tutti gli insiemi, classi [le sottocollezioni di **Set**] e insiemi [gli elementi di **Set**]. Notazioni per rappresentare insiemi. L'insieme vuoto. Il singleton di un oggetto. L'insieme delle parti di un insieme. Intersezione di una collezione non vuota di insiemi, unione di una collezione di insiemi; differenza di una coppia di insiemi; differenza simmetrica di una coppia di insiemi. Diagrammi di Euler-Venn. Coppie non ordinate e coppie ordinate; proprietà caratteristica di una coppia ordinata; prodotto cartesiano di una coppia ordinata di insiemi.
Corrispondenze e applicazioni fra insiemi; famiglie; restrizioni e prolungamenti; immagini e controimmagini. Applicazioni iniettive, suriettive, biettive. Trasformazioni e permutazioni di un insieme. Applicazioni componibili, composizione di applicazioni; associatività del prodotto operativo, neutralità delle permutazioni identiche. Applicazioni invertibili a sinistra o a destra; retrazioni (di un'applicazione iniettiva); sezioni (di un'applicazione suriettiva) e funzioni di scelta; applicazioni invertibili, inversa di un'applicazione biettiva.
Relazioni binarie in un insieme; inversa di una relazione; prodotto relazionale; proprietà notevoli per una relazione binaria; quasiordinamenti; ordinamenti larghi e ordinamenti (stretti); ordinamenti totali; relazioni di equivalenza.
Equivalenze e partizioni; immagine e coimmagine di un'applicazione, teorema fondamentale di omomorfismo per gli insiemi, fattorizzazione canonica di un'applicazione, applicazioni e partizioni.
Insiemi ordinati, catene, diagrammi di Hasse, insiemi ordinati isomorfi; minimo, massimo, elementi minimali, elementi massimali; minoranti, maggioranti, estremo inferiore, estremo superiore. Reticoli (come particolari insiemi ordinati); insiemi ordinati inf-completi o sup-completi; reticoli completi. L'isomorfismo canonico dal reticolo delle equivalenze in un insieme al reticolo delle partizioni dell'insieme.
Cenni sui numeri naturali; principio di induzione e ragionamenti per ricorrenza. Confronto di potenze di insiemi. Insiemi finiti; insiemi numerabili; cenni sugli insiemi infiniti.

•Primi elementi di calcolo combinatorio. Ordini dell'unione e del prodotto cartesiano di una coppia di insiemi finiti. Numero delle applicazioni e numero delle applicazioni iniettive fra una coppia di insiemi finiti; numero delle trasformazioni e numero delle permutazioni di un insieme finito. Fattoriali e fattoriali discendenti. Disposizioni semplici e disposizioni con ripetizioni. k-parti di un insieme finito. Coefficienti binomiali e loro principali proprietà, triangolo di Tartaglia-Pascal. k-partizioni di un insieme finito, numeri di Stirling di seconda specie; numero delle partizioni di un insieme finito, numeri di Bell.

•Primi elementi di teoria dei grafi. Nozioni di grafo e di multigrafo, vertici, lati, adiacenza, incidenza, grado (valenza) di un vertice, vertici pari o dispari, grafi regolari. Relazioni aritmetiche fra numero dei lati, numero e grado dei vertici. Sottografi. Isomorfismi tra grafi. Cammini, circuiti, connessione, componenti

connesse. Cammini e circuiti euleriani. Alberi, foreste e loro caratterizzazioni. Sottoalbero massimale di un grafo connesso (albero di supporto). Grafi planari (piani): formula di Eulero e teorema di Kuratowski (senza dimostrazioni).

•Nozioni fondamentali sulle strutture algebriche. Operazioni interne binarie, unarie, nullarie; nozione di struttura algebrica. Omomorfismi, isomorfismi. Gruppoidi, tavole di Cayley e proprietà notevoli di operazioni binarie interne; elementi neutri a destra o a sinistra, elemento neutro; coppie di elementi permutabili o non permutabili, elementi centrali, proprietà commutativa; terne non associative e terne associative, proprietà associativa, enunciato del teorema di associatività, semigruppi; elementi simmetrizzabili, simmetrico del simmetrico di un elemento, simmetrico del composto di una coppia di elementi simmetrizzabili di un semigruppo; semigruppi cancellativi; proprietà distributive per una coppia di operazioni binarie. Traslazioni interne (sinistra e destra) di un semigruppo indotte da un elemento, simmetrizzabilità e cancellabilità in un semigruppo, il caso particolare dei semigruppi finiti.
Definizioni, esempi, morfismi e regole di calcolo per vari tipi di strutture algebriche: semigruppi, monoidi, gruppi; anelli, corpi, campi; reticoli (come particolari strutture algebriche), reticoli distributivi, reticoli complementati, reticoli booleani, algebre di Boole.
Parti stabili, strutture indotte; sottoalgebre generate. Sottosemigruppi, sottomonoidi, sottogruppi; sottoanelli, sottocorpi, sottocampi; ideali sinistri, ideali destri, ideali bilateri di un anello; sottoreticoli.
Omomorfismi fra reticoli. Reticoli pentagonali, reticoli trirettangoli ed enunciato, per un reticolo, del criterio di distributività di Birkhoff. Enunciato del teorema di Stone sui reticoli booleani. Connessioni fra reticoli booleani, algebre di Boole e anelli booleani.
Il monoide delle trasformazioni di un insieme, il gruppo degli elementi simmetrizzabili di un monoide, il gruppo simmetrico su un insieme. Il gruppo simmetrico S_n di grado n; permutazioni disgiunte; permutazioni cicliche, trasposizioni; decomposizione standard di una permutazione non identica in prodotto di cicli disgiunti; periodo; rappresentazioni di una permutazione come prodotto di scambi, permutazioni di classe pari e permutazioni di classe dispari; il gruppo alterno A_n di grado n.
Equivalenze compatibili (ed equivalenze compatibili a sinistra o a destra) con un'operazione binaria, operazione quoziente di un'operazione binaria. Equivalenze in un gruppo compatibili a sinistra o a destra, laterali di un sottogruppo, teorema di Lagrange, periodo di un elemento. Congruenze e sottogruppi normali di un gruppo, congruenze e ideali di un anello. Gruppo quoziente, anello quoziente. Ideali di un anello quoziente, quozienti di un anello rispetto a ideali massimali. Cenni sui campi finiti.

•Alcuni problemi di fattorizzazione. Elementi di aritmetica nell'anello Z degli interi, algoritmo della divisione aritmetica, congruenze (e ideali) di Z, anello degli interi mod m, equazioni congruenziali. Il gruppo degli interi mod m invertibili, funzione di Euler-Gauss, teorema di Fermat-Euler e "piccolo teorema" di Fermat.
Anello dei polinomi in una indeterminata. Divisibilità, elementi associati, elementi irriducibili, elementi primi in domini di integrità unitari. Mcd e mcm. Algoritmo euclideo e teorema di Bezout nell'anello degli interi e nell'anello dei polinomi in una indeterminata su un campo. Polinomi irriducibili su un campo, criterio di Eisenstein. Polinomi su un campo e applicazioni polinomiali; radici, teorema di Ruffini; principio di identità dei polinomi.

(C) Testi di riferimento.

[F00] Alberto FACCHINI, *Algebra e matematica discreta,* Decibel, Padova, 2000.
(oppure:
[F91] Alberto FACCHINI, *Algebra per Informatica*, Decibel, Padova, 1991.
[F92] Alberto FACCHINI, *Sussidiario di Algebra e Matematica Discreta*, Decibel, Padova, 1992.)

[GKP92] Ronald L. GRAHAM - Donald E. KNUTH - Oren PATASHNIK, *Matematica Discreta: Principi matematici per l'informatica*, Hoepli, Milano, 1992
[cfr. 3.4, 4.1, 4.2, 4.3, 4.6, 4.9, 5.1, 6.1].

***