

**Programma del corso di Algebra 1 (prof. M. Barnabei)**  
**A.A. 2013/14**

Richiamo sugli insiemi: appartenenza, inclusione, unione, intersezione, complemento, differenza. Insieme delle parti. Leggi di De Morgan. Prodotto cartesiano. Relazioni. Funzioni. Proprietà delle relazioni in  $A \times A$ : riflessiva, simmetrica, antisimmetrica, transitiva. Funzioni: definizione, terminologia. Funzioni iniettive, suriettive, biiettive. Teorema: un insieme non può essere in biiezione con il suo insieme delle parti.

Funzione caratteristica di un sottoinsieme. Proprietà relative: principio di inclusione-esclusione. Corrispondenza tra sottoinsiemi di un insieme finito e liste in  $\{0,1\}$  e conteggi relativi. Insiemi finiti e numerabili. Gli insiemi dei numeri interi e razionali sono numerabili. L'insieme dei numeri reali non è numerabile.

Assiomi di Peano. Principio di induzione. Funzioni tra insiemi finiti: numero totale. Numero di funzioni iniettive. Principio dei cassetti. Fattoriale decrescente. Permutazioni. Fattoriale. Numeri di Fibonacci.

Coefficienti binomiali: definizione e proprietà. Formula di Stifel. Triangolo di Tartaglia. Formula del binomio di Newton. Cammini nel reticolato  $N \times N$ .

Principio di inclusione-esclusione: il caso di due e tre sottoinsiemi. Il caso generale: formule di Da Silva e Sylvester. Applicazione: il numero di funzioni suriettive tra due insiemi finiti.

Il numero di permutazioni senza punti fissi. La funzione di Eulero ed il suo calcolo.

Definizione di partizione e di relazione di equivalenza. Classi di equivalenza. Teorema: le classi di equivalenza costituiscono una partizione.

Teorema: ad ogni partizione è associata una relazione di equivalenza. Esempio: la congruenza modulo  $n$ . Insieme quoziente rispetto ad una relazione di equivalenza. La relazione di equivalenza associata ad una funzione. Teorema: ogni funzione si può scrivere come composizione di una funzione iniettiva e di una funzione suriettiva.

Costruzione dei numeri interi e dei numeri razionali come classi di equivalenza.

Numeri di Bell e numeri di Stirling di seconda specie e relative formule di ricorrenza. Legame tra i numeri di Stirling e il numero di funzioni suriettive tra due insiemi finiti.

Insiemi parzialmente ordinati: definizione ed esempi. Elementi inconfrontabili. Catene e antichatene.

Ordine lessicografico. Relazione di copertura e sue proprietà. Diagramma di Hasse. Sottoordini.

Intervalli. Morfismi e isomorfismi d'ordine. Linearizzazioni.

Duale di un poset. Principio di dualità. Elementi massimali e minimali. Massimo e minimo.

Condizione di Jordan-Dedekind e rango.

Estremo superiore ed inferiore di due elementi di un poset. Definizione di reticolo. Proprietà delle operazioni di sup ed inf. Reticolo completo. Teorema: ogni reticolo finito è completo. Reticolo astratto. Teorema: ad ogni reticolo astratto  $L$  è associata una relazione d'ordine con la quale  $L$  risulta un reticolo isomorfo a quello di partenza.

Morfismo e isomorfismo di reticoli. Sottoreticolo. Reticolo modulare e reticolo distributivo e relative caratterizzazioni (con sottoreticoli "proibiti" e attraverso il rango: senza dim.).

Divisibilità tra interi: lemma di divisione. Massimo comun divisore. Algoritmo di Euclide. Teorema di Bézout. Numeri primi. Teorema: i numeri primi sono infiniti. Crivello di Eratostene. Teorema fondamentale dell'aritmetica.

Definizione di gruppo. Gruppo abeliano. Esempi: il gruppo generale lineare e il gruppo simmetrico. Legge di cancellazione. Tavola di moltiplicazione.

Esempi di gruppo: le classi resto modulo  $n$  rispetto alla somma. Il caso del prodotto:  $Z_n^*$  è un gruppo se e solo se  $n$  è un numero primo. Definizione di semigrupp e di monoide. Teorema: un monoide è un gruppo se e solo se le equazioni  $a*x=b$  e  $x*a=b$  hanno soluzione per ogni  $a,b$ .

Sottogruppo: definizioni equivalenti. Esempi: i sottogruppi di  $(Z,+)$ . Il gruppo delle matrici triangolari superiori invertibili. Il gruppo di Heisenberg. Sottogruppi di  $S_3$ . Sottogruppo ciclico. Periodo di un elemento.

Omomorfismi di gruppi. Isomorfismi. Endomorfismi. Automorfismi. Automorfismi interni.

Il gruppo simmetrico: isomorfismo con il gruppo delle matrici di permutazione. Segno di una permutazione. Ciclo. Scomposizione di una permutazione come prodotto di cicli disgiunti. Ordine e segno di un ciclo e di una permutazione scomposta in cicli. Il gruppo alterno.

Classi laterali rispetto ad un sottogruppo (destre e sinistre). Teorema: ogni classe laterale relativa al sottogruppo  $H$  è in corrispondenza biunivoca con  $H$ . Indice di un sottogruppo. Teorema di Lagrange e sue conseguenze. Sottogruppi normali.

Quoziente di un gruppo rispetto ad un sottogruppo normale. Nucleo e immagine di un omomorfismo e loro proprietà.

Un omomorfismo di gruppi è iniettivo se e solo se il suo nucleo contiene il solo elemento neutro. Quoziente di un gruppo rispetto al nucleo di un omomorfismo. Primo teorema di isomorfismo. Intersezione di due sottogruppi. Estremo superiore di due sottogruppi.