PROGRAMMA DI ALGEBRA 1

A.A. 2007-2008

Prof. Elisabetta Strickland

Insiemi. Prime definizioni. Unione e intersezione di insiemi. Insieme delle parti di un insieme. Prodotto cartesiano di due insiemi.

Relazioni. Esempi. Relazioni di equivalenza. Classi di equivalenza. Partizione di un insieme. Insieme quoziente. Relazioni d'ordine. Esempi.

Funzioni. Esempi. Funzioni iniettive e funzioni suriettive. Funzioni biiettive. Composizione di applicazioni. Funzione inversa. Funzione caratteristica di un insieme.

I numeri naturali. Assiomi di Peano. Formulazioni equivalenti del principio di induzione matematica. Operazioni in N. Divisione in N.

Esempi di dimostrazione per induzione (cardinalita' dell'insieme delle parti di un insieme di cardinalita' n). Divisione con resto in N.

Insiemi equipotenti. Cardinalita' di un insieme. Insiemi numerabili. Proprieta' degli insiemi infiniti. La cardinalita' dell'insieme delle parti di un insieme numerabile A e' maggiore della cardinalita' di A.

Calcolo combinatorio. Il fattoriale n! di un intero positivo n. Permutazioni. Il gruppo simmetrico su n elementi. Calcolo del numero di funzioni da un insieme con n elementi ad un insieme con m elementi. Numero delle corrispondenze biunivoche di insieme finito in se'. Il numero di sottoinsiemi con k elementi di un insieme con n elementi. Il coefficiente binomiale. Il triangolo di Tartaglia.

Gli interi come quoziente. Proprieta' degli interi. Divisibilita' in Z. Elementi invertibili, elementi irriducibili e elementi primi. Ogni elemento primo e' irriducibile in Z. La divisione in Z. Massimo comun divisore. L'algoritmo euclideo delle divisioni successive per la determinazione del MCD. L'identita' di Bezout. Equazioni diofantee lineari. Elementi primi e irriducibili in Z e loro equivalenza. Il teorema fondamentale dell'aritmetica. Infinita' dei numeri primi.

I numeri razionali come quoziente. Loro struttura algebrica.

I numeri di Fibonacci.

Congruenze. Proprieta'. Il piccolo teorema di Fermat. L'anello delle classi resto modulo n. Criteri di divisibilita'. La prova del nove. Risoluzione di congruenze lineari. Il teorema cinese dei resti. La funzione di Eulero. Il teorema di Eulero. Elementi invertibili. Test di non primalita'. Il crivello di Eratostene per la determinazione dei primi minori di un dato intero. Il metodo di fattorizzazione di Fermat. Numerazioni in basi diverse.

Funzioni polinomiali e polinomi a coefficienti in un campo. Operazioni tra polinomi. L'anello dei polinomi in una indeterminata x a coefficienti in un campo e' un dominio di integrita'. Divisione tra polinomi. Il MCD tra due polinomi. L'algoritmo euclideo delle divisioni successive per la ricerca

del MCD tra polinomi. Polinomi associati. Polinomi irriducibili e polinomi primi: loro equivalenza in K[x] (K campo).Il teorema di fattorizzazione unica. Teorema di Ruffini. Un polinomio di grado n ammette al piu' n radici nel campo. Se il campo K ha infiniti elementi, due polinomi a coefficienti in K sono uguali come polinomi se e solo se sono uguali come funzioni polinomiali. Polinomi irriducibili sui complessi. Polinomi irriducibili sui reali. Polinomi a coefficienti razionali e polinomi a coefficienti interi. Polinomi primitivi. Ogni polinomio a coefficienti razionali e' associato in Q[x] ad un polinomio a coefficienti interi e primitivo. Il lemma di Gauss. Il contenuto del prodotto di due polinomi uguaglia il prodotto dei contenuti. Il teorema di Gauss (Un polinomio a coefficienti in Z irriducibile su Z e' irriducibile su Q). Per polinomi primitivi vale anche il viceversa. Radici razionali di polinomi a coefficienti interi. Il criterio di irriducibilita' di Eisenstein. Vari metodi per studiare la irriducibilita' di polinomi su Q. Polinomi ciclotomici, l'equazione di terzo grado e la formula di Cardano, i polinomi simmetrici.

Definizione di anello. Anelli commutativi, anelli con unita', domini di integrita', campi. Esempi vari. Ogni dominio di integrita' finito e' un campo. Sottoanelli e ideali di un anello. Relazioni di equivalenze compatibili con le operazioni e ideali: loro legame.

Definizione di gruppo. Primi esempi. Conseguenze degli assiomi (unicita' dell'elemento neutro e unicita' dell'inverso. Sottogruppi e condizione caratteristica. Sottogruppo generato da un sottoinsieme. Esempi. Periodo (o ordine) di un elemento di un gruppo. Gruppi ciclici. Ogni sottogruppo di un gruppo ciclico e' ciclico.

Il gruppo simmetrico. Scrittura ciclica di una permutazione. Permutazioni pari. Il sottogruppo alterno. Classi coniugate e partizioni dell'intero n.

Classi laterali destre e sinistre modulo un sottogruppo H di un gruppo G. Tutte le classi laterali (destre e sinistre) hanno la stessa cardinalita' (che e' la cardinalita' del sottogruppo). Il teorema di Lagrange. Conseguenze: a) un gruppo di ordine un numero primo e' ciclico; b) Se G e' finito, il periodo di ogni elemento divide l'ordine del gruppo; c) Se G e' finito, ogni elemento elevato all'ordine del gruppo e' uguale all'elemento neutro; d) dimostrazione immediata del teorema di Eulero.

Omomorfismi tra gruppi. Nucleo e immagine. Proprieta' degli omomorfismi. Un omomorfismo tra due gruppi e' un monomorfismo se e solo se Ker e' ridotto al solo elemento neutro. Relazioni compatibili con l'operazione in un gruppo. Sottogruppi normali. Gruppi quoziente. Il teorema fondamentale di omomorfismo tra gruppi e sue applicazioni. I gruppi ciclici. Il centro di un gruppo. Automorfismi e automorfismi interni.

Testo Consigliato: Gulia Maria Piacentini Cattaneo, "Algebra. Un approccio algoritmico". Ed. Decibel Zanichelli.