AL1 Algebra (1^0 Modulo)

A.A. 2006/2007

Prof. Stefania Gabelli

Fondamentii

1. Insiemi ed applicazioni

Nozione intuitiva di insieme. Operazioni tra insiemi (unione, intersezione, differenza, complementare, prodotto cartesiano) e loro proprietà. Insieme delle parti. Esempi.

Corrispondenze, relazioni e applicazioni. Corrispondenza inversa di una applicazione. Applicazione identica ed applicazioni costanti. Esempi. Prodotto operatorio di applicazioni e sue prime proprietà. Applicazioni iniettive, suriettive e biiettive; loro caratterizzazioni. Funzione caratteristica di un sottoinsieme. Applicazioni tra insiemi finiti. Biiezione tra l'insieme delle parti di un insieme di n elementi con l'insieme $\{0,1\}^n$. Esempi.

Relazioni d'equivalenza e partizioni associate. Insieme quoziente. Relazione di equivalenza associata ad una applicazione e biezione dell'insieme quoziente con l'immagine dell'applicazione. Esempi.

Relazioni di ordine e ordine totale. Diagrammi lineari di insiemi ordinati. Maggioranti, minoranti, elementi massimali, elementi minimali, massimi e minimi, estremi inferiori e superiori. Esempi.

2. Numeri

Assiomi di Peano; addizione, moltiplicazione e relazione d'ordine nell'insieme dei numeri naturali $\mathbb{N}$. Principio di induzione (e sua formulazione forte). Principio del Buon Ordinamento. Dimostrazioni per induzione. Coefficienti binomiali.

Costruzione di $\mathbb{Z}$ a partire da $\mathbb{N}$ e di $\mathbb{Q}$ a partire da $\mathbb{Z}$.

Costruzione dell'insieme $\mathbb{C}$ dei numeri complessi e loro rappresentazione nel piano di Gauss. Norma e modulo di un numero complesso: coniugato e inverso. Rappresentazione trigonometrica dei numeri complessi; formule di moltiplicazione. Radici n-sime di un numero complesso. Radici n-sime dell'unità e radici primitive.

3. Cenni sulle strutture algebriche

Operazioni e loro proprietà. Elementi neutri e simmetrizzabili. Notazione additiva e moltiplicativa.

Gruppi. Il gruppo delle trasformazioni di un insieme. Gruppi di permutazioni. Prime proprietà del gruppo S_n: permutazioni cicliche, trasposizioni, decomposizione in cicli, ordine e parità di una permutazione. Il gruppo delle radici complesse n-sime dell'unità.

Anelli. Anelli commutativi e unitari. Elementi invertibili e divisori dello zero. Domini di integrità. Il gruppo degli elementi invertibili di un dominio. Campi. Esempi.

4. Divisibilità in $\mathbb{Z}$. L'anello delle classi resto modulo n.

Divisione con il resto tra due interi. Esistenza di MCD e mcm; algoritmo di Euclide per la determinazione del MCD. Identità di Bézout. Lemma di Euclide.

Scrittura in base b dei numeri naturali.

Numeri primi. Teorema fondamentale dell'aritmetica. Teorema sull'infinità dei numeri primi.

Prime proprietà aritmetiche dell'anello $\mathbb{Z}_n$ delle classi resto modulo un intero $n > 1$. Criteri di divisibilità.

Elementi invertibili e zero-divisori dell'anello $\mathbb{Z}_n$. Funzione di Eulero. Il teorema di Eulero-Fermat.

Calcolo di un inverso aritmetico mod n. Congruenze lineari in una indeterminata: criterio di risolubilità, numero di soluzioni e ricerca di soluzioni. Esempi.

Sistemi di congruenze lineari. Teorema cinese dei resti. Risoluzione di sistemi di congruenze lineari. Esempi.

5. Polinomi

L'anello dei polinomi a coefficienti in un dominio di integrità. Somma e prodotto di polinomi, grado. Formula del grado. Polinomi invertibili e associati.

Polinomi a coefficienti in un campo K. Algoritmo di divisione tra polinomi. Esistenza ed unicità del MCD monico. Identità di Bézout.

Polinomi irriducibili. Teorema di fattorizzazione unica in $K[X]$.

Radici di un polinomio. Relazione tra l'esistenza di radici e la riducibilità di un polinomio. Teorema del resto. Regola di Ruffini.

Polinomio derivato. Radici multiple.

Polinomi a coefficienti numerici. Enunciato del Teorema Fondamentale dell'Algebra. Polinomi irriducibili di $\mathbb{C}[X]$ e di $\mathbb{R}[X]$.

Ricerca di radici intere e razionali di polinomi su $\mathbb{Q}$. Polinomi a coefficienti interi. Contenuto di un polinomio, polinomi primitivi. Lemma di Gauss. Teorema di fattorizzazione unica in $\mathbb{Z}[X]$.

Criterio di irriducibilità di Eisenstein. Criterio di irriducibiltà modulo un primo p.

Testi consigliati

[1] G.M. Piacentini Cattaneo, *Algebra, un approccio algoritmico*. Decibel – Zanichelli, (1996).
[2] M. Fontana – S. Gabelli, *Insiemi, numeri e polinomi. Primo ciclo di lezioni del Corso di Algebra con esercizi svolti*. CISU, (1989).
[3] M. Fontana – S. Gabelli, *Esercizi di Algebra*. Aracne, (1993).

Modalità d'esame

- valutazione in itinere ("esoneri")		■ SI	□ NO
- esame finale	scritto	■ SI	□ NO
	orale	■ SI	□ NO
- altre prove di valutazione del profitto (meglio descritte sotto)		□ SI	■ NO

L'esame consiste in una prova scritta ed un colloquio orale, volto ad accertare l'acquisizione da parte dello studente dei concetti e dei metodi illustrati nel corso.

Gli studenti che hanno superato le prove scritte di valutazione parziale (esoneri) con la media di almeno 16/30 accedono direttamente al colloquio orale, da sostenersi esclusivamente negli appelli di Gennaio/Febbraio. Per sostenere l'esame nelle sessioni di Giugno e Settembre è invece necessario ripetere la prova scritta.