AL1 Algebra (1^0 Modulo)
A.A. 1999/2000

Prof. Stefania Gabelli

Insiemi, numeri e polinomi

1. Insiemi ed applicazioni

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

Corrispondenze e relazioni. Ricoprimenti e partizioni. Relazioni d'equivalenza e partizioni. Insieme quoziente. Esempi.

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. Applicazioni tra insiemi finiti. Esempi.

Relazione d'equivalenza associata ad una applicazione. Teorema fondamentale di decomposizione di una applicazione. Esempi.

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

2. Cenni sulle strutture algebriche

Operazioni e loro proprietà. Elementi neutri e simmetrizzabili. Unicità dell'elemento neutro e del simmetrico di un elemento. Notazione additiva e moltiplicativa.

Semigruppi e 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. Anelli integri. Campi. Esempi.

3. 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.

L'anello dei numeri interi: costruzione di $\mathbb{Z}$ a partire da $\mathbb{N}$. Divisione con il resto. 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.

4. Polinomi

Costruzione dell'anello dei polinomi a coefficienti in un anello commutativo unitario A come successioni di elementi di A. Somma e prodotto di polinomi, grado.

Polinomi a coefficienti in un dominio di integrità. Formula del grado. Polinomi invertibili e associati.

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

Polinomi irriducibili. Teorema di fattorizzazione unica.

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

Polinomi a coefficienti numerici. Cenni sul teorema fondamentale dell'Algebra. Ricerca di radici intere e razionali di polinomi su $\mathbb{Q}$. Polinomi irriducibili di $\mathbb{C}[X]$ e di $\mathbb{R}[X]$.

Polinomi a coefficienti interi. Contenuto di un polinomio, polinomi primitivi. Lemma di Gauss. Teorema di fattorizzazione unica.

Criterio di irriducibiltà di Eisenstein.

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).
[4] R. Procesi Ciampi – R. Rota, *Algebra Moderna. Esercizi*. Veschi, (1992).

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 e 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, nel corso del semestre, le prove scritte di valutazione parziale (esoneri) accedono direttamente al colloquio orale, da sostenersi esclusivamente negli appelli di Gennaio/Febbraio e Giugno/Luglio. Per sostenere l'esame nella sessione Autunnale è invece necessario ripetere la prova scritta.

Gli studenti che non hanno superato soltanto una delle due prove di valutazione parziale, possono sostenere una prova scritta di "recupero" (per la parte di programma riguardante la prova non superata) esclusivamente nel 1^o Appello della 1^a Sessione di esame (Gennaio).