

# AL1 Algebra (1<sup>o</sup> Modulo)

A.A. 2007/2008

Prof. Francesca Tartarone

## Fondamentii

### 1. Insiemi ed applicazioni

Nozione intuitiva di insieme. Operazioni tra insiemi (unione, intersezione, differenza, differenza simmetrica, complementare, prodotto cartesiano) e loro proprietà. Diagrammi di Venn. Insieme delle parti. Famiglie di insiemi. Elementi di Logica Proposizionale: le Tavole della Verità. Esempi.

Corrispondenze, relazioni e applicazioni. Grafico di una corrispondenza. Corrispondenza inversa di una applicazione. Prodotto operatorio di applicazioni e sue prime proprietà. Applicazioni iniettive, suriettive e biiettive; loro caratterizzazioni. Applicazione inversa a destra e a sinistra. Immagine e controimmagine di un'applicazione. 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. Relazione nucleo associata ad un'applicazione e relativa decomposizione di un'applicazione. Esempi.

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

Elementi di calcolo combinatorio (coefficienti binomiali).

### 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. Equivalenza fra il Principio di induzione, il Principio di Induzione Forte ed il Principio del Buon Ordinamento. Dimostrazioni per induzione.

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. 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. Elementi primi e irriducibili, invertibili ed associati in  $\mathbb{Z}$ . Lemma di Euclide.

Scrittura in base  $b$  dei numeri naturali.

Teorema fondamentale dell'aritmetica. Teorema sull'infinità dei numeri primi. Crivello di Eratostene.

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 Piccolo Teorema di Fermat ed 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. Isomorfismo fra  $(\mathbb{Z}_{rs}, +, \cdot)$  e  $(\mathbb{Z}_r, +, \cdot) \times (\mathbb{Z}_s, +, \cdot)$ , quando  $r, s$  sono interi positivi coprimi. Esempi.

#### 4. Cenni sulle strutture algebriche

Definizione di anello e gruppo. Notazione additiva e moltiplicativa.

Gruppi. Gruppi di permutazioni. Prime proprietà del gruppo  $S_n$ : trasposizioni, decomposizione in cicli, ordine e parità di una permutazione. Il gruppo delle radici complesse  $n$ -sime dell'unità,  $(U_n, \cdot)$ . Isomorfismo fra  $(U_n, \cdot)$  e  $(\mathbb{Z}_n, +)$ .

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

Sottoanelli e sottogruppi. Omomorfismi e isomorfismi fra strutture algebriche.

#### 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. Numero delle radici di un polinomio in  $\mathbb{C}[X]$ . 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 e Teorema di Gauss. Passaggio dell'irriducibilità da  $\mathbb{Z}[X]$  a  $\mathbb{Q}[X]$  e viceversa

Criterio di irriducibilità di Eisenstein. Criterio di irriducibilità modulo un primo  $p$  e criterio di traslazione della variabile.

## 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”)		<input checked="" type="checkbox"/> SI	<input type="checkbox"/> NO
- esame finale	scritto	<input checked="" type="checkbox"/> SI	<input type="checkbox"/> NO
	orale	<input checked="" type="checkbox"/> SI	<input type="checkbox"/> NO
- altre prove di valutazione del profitto (meglio descritte sotto)		<input type="checkbox"/> SI	<input checked="" type="checkbox"/> 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 15/30 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.