

AL1 Algebra (1^o Modulo)

A.A. 2000/2001

Prof. Stefania Gabelli

Insiemi, numeri e polinomi

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. Biezione tra l'insieme delle parti di un insieme di n elementi con l'insieme $\{0, 1\}^n$. Esempi.

Nozione di cardinalità. Caratterizzazione degli insiemi infiniti come gli insiemi equipotenti a un (opportuno) sottoinsieme proprio. Cardinalità del numerabile e del continuo. Esempi.

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

I numeri reali come numeri decimali. Numeri decimali finiti e periodici e loro conversione in forma di frazione. Numeri reali algebrici e trascendenti.

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. Unicità dell'elemento neutro e del simmetrico di un elemento. Notazione additiva e moltiplicativa.

Semigrupperi 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. Domini di integrità. Campi. Esempi.

4. Divisibilità in \mathbb{Z} . L'anello delle classi resto modulo 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. 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. Irriducibilità del p -esimo polinomio ciclotomico.

Criterio di irriducibilità 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).
 [4] R. PROCESI CIAMPI – R. ROTA, *Algebra Moderna. Esercizi*. Veschi, (1992).

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 type="checkbox"/> SI	<input checked="" 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 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 le prove scritte di valutazione parziale (esoneri) con la media di almeno 18/30 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, riportando nell'altra la votazione di almeno 18/30, possono sostenere una prova scritta di "recupero" (per la parte di programma riguardante la prova non superata) esclusivamente nel 1° Appello della 1^a Sessione di esame (Gennaio).