

AL1 Algebra (1^o Modulo)

A.A. 1998/1999

Prof. Florida Girolami

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 e corrispondenze. Corrispondenza inversa di una applicazione. Applicazione identica ed applicazioni costanti. Esempi. Prodotto operatorio di applicazioni e sue prime proprietà. Assioma della scelta. Applicazioni iniettive, suriettive e biiettive; loro caratterizzazioni. Applicazioni tra insiemi finiti; prime proprietà dell'insieme S_n . Esempi.

Relazione d'equivalenza ("nucleo") associata ad una applicazione. Teorema fondamentale di decomposizione di una applicazione. Esempi.

Relazioni di pre-ordine, ordine e ordine totale. Diagrammi lineari di insiemi ordinati. Maggioranti, minoranti, elementi massimali, elementi minimali, minimo e massimo, estremi inferiori e superiori. Lemma di Zorn (solo enunciato e sua equivalenza con l'assioma della scelta). Esempi.

2. Numeri

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

L'insieme dei numeri interi: costruzione di \mathbf{Z} a partire da \mathbf{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. Elementi irriducibili. Teorema fondamentale dell'aritmetica. Teorema sull'infinità dei numeri primi. Crivello di Eratostene.

Prime proprietà dell'aritmetica dell'insieme \mathbf{Z}_n delle classi resto modulo un intero $n > 1$. Criteri di divisibilità. "Prove del nove".

Sistema completo di residui mod n . Inverso aritmetico mod n : esistenza ed unicità. Sistema ridotto di residui mod n . Indicatore di Eulero. Congruenze lineari in una indeterminata. Risolubilità, numero di soluzioni e ricerca di soluzioni. Esempi. Sistemi di congruenze lineari. Teorema cinese dei resti. Risoluzione di sistemi di congruenze

lineari. Il “piccolo” teorema di Fermat. Il teorema di Eulero-Fermat. Teorema di Wilson e caratterizzazione dei numeri primi.

L’insieme dei numeri razionali: costruzione di \mathbf{Q} a partire da \mathbf{Z} . Rappresentazione in base b di un numero razionale. Frazioni continue finite semplici.

L’insieme dei numeri reali: costruzione di \mathbf{R} a partire da \mathbf{Q} attraverso le successioni di Cauchy (cenni).

L’insieme dei numeri complessi: costruzione di \mathbf{C} a partire da \mathbf{R} ; forma polare di un numero complesso; formula di de Moivre; radici n -esime dell’unità.

3. Polinomi

Assiomi di gruppo e proprietà elementari derivanti da essi. Leggi di cancellazione. Esempi. Sottogruppi. Omomorfismi. Gruppi di trasformazioni. Gruppi di permutazioni. Cicli e teorema di decomposizione. Teorema del segno (senza dimostrazione).

Definizione assiomatica di anello. Anelli commutativi e unitari. Elementi invertibili e divisori dello zero. Anelli interi. Domini, corpi, campi. Esempi. Caratteristica di un dominio di integrità.

Polinomi a coefficienti in un anello commutativo unitario: definizione, somma, prodotto, grado. Elementi invertibili e associati.

Polinomi a coefficienti in un dominio di integrità: elementi irriducibili e primi. Algoritmo di divisione per polinomi. Radici di un polinomio. Esistenza di radici e riducibilità. Teorema del resto. Regola di Ruffini. Ricerca di radici intere e razionali. MCD di due polinomi.

Polinomi a coefficienti in un campo: metodo delle divisioni successive per il MCD ed identità di Bézout; ogni polinomio irriducibile è primo; teorema di fattorizzazione unica. Cenni sul teorema fondamentale dell’Algebra. Polinomi irriducibili di $\mathbf{C}[X]$ e di $\mathbf{R}[X]$.

Polinomi a coefficienti interi: contenuto di un polinomio, polinomi primitivi. Lemma di Gauss. Teorema di fattorizzazione unica. Criterio di irriducibilità di Eisenstein. Esempi ed applicazioni (irriducibilità del p -polinomio ciclotomico).

4. Elementi di teoria della cardinalità

Insiemi equipotenti. Cardinalità di un insieme. Insiemi finiti ed infiniti. Cardinalità del numerabile e del continuo. Teorema di Cantor sull’unione numerabile di insiemi numerabili. Numerabilità di \mathbf{Z}^n , \mathbf{Q}^n ($n > 0$) e dell’insieme dei numeri algebrici. Disuguaglianza tra numeri cardinali. Secondo metodo diagonale di Cantor.

TESTI CONSIGLIATI

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

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

Gli studenti che hanno sostenuto con esito positivo, nel corso del semestre, le prove di valutazione parziale (“esoneri”) accedono direttamente al colloquio di verbalizzazione del voto proposto dal docente, da effettuarsi durante il 1° Appello della 1^a Sessione.

Per tutti gli studenti che non si avvalgono della possibilità della valutazione del profitto durante il corso, l’esame finale consiste in una prova scritta, comprendente anche domande di tipo teorico.

Soltanto la prova scritta del 1° Appello della 1^a Sessione è suddivisa in due parti distinte indipendenti, che corrispondono alle due unità didattiche in cui è suddiviso il corso. Gli studenti che hanno sostenuto con esito positivo soltanto la prova relativa ad una delle due unità didattiche in cui è suddiviso il corso, possono sostenere la prova scritta soltanto per la parte riguardante l’altra unità didattica. Si noti che, in presenza di una valutazione positiva delle prove parziali durante il corso, l’eventuale consegna da parte dello studente di una successiva prova scritta di esame comporta la rinuncia implicita al “voto di esonero”. Pertanto, in tal caso, la valutazione del profitto del corso verrà effettuata in base alla prova d’esame.