AL1 Algebra: fondameni
A.A. 2008/2009

Prof. Francesco Pappalardi

1. Insiemi ed applicazioni Insiemi e appartenenza. Sottoinsiemi, l'insieme vuoto, inclusioni, operazioni tra insiemi (unione e intersezione). Leggi distributive dell'unione rispetto all'intersezione. Partizioni di insiemi. il complementare di un insieme. Leggi di de Morgan. Prodotto cartesiano di insiemi.

Relazioni. Applicazioni di insiemi. Definizione intuitiva e definizione rigorosa. Identità, immersioni, restrizioni. Dominio, codominio, immagine, controimmagine. Applicazioni iniettive, suriettive e biunivoche (o invertibili).

Applicazione biunivoca tra l'insieme delle parti di un insieme e l'insieme delle funzioni binarie. Composizione di applicazioni. Applicazioni cancellabili a destra e a sinistra. Caratterizzazione dell applicazioni cancellabili in termini di applicazioni suriettive (a DX) e iniettive (a SX).

Applicazioni invertibili. Un applicazione è invertibile se e solo è suriettiva. Permutazioni di un insieme. involuzioni.

2. Assiomi di Peano Definizione assiomatica dei numeri naturali. Gli assiomi di Peano. Indipendenza degli assiomi di Peano. Il principio di induzione. Insiemi finiti e loro proprietà. Sottoinsiemi di insiemi finiti sono finiti. Ogni suriezione da un insieme finito ha immagine finita.

Il principio di Dirichlet delle gabbie e dei piccioni. Ogni iniezione da un insieme finito in se è una suriezione.

3. Insiemi infiniti Insiemi infiniti, infiniti nel senso di Dedekind e infiniti nel senso di Cantor. I numeri naturali sono infiniti in tutti i sensi. Il Teorema di Cantor: L'esistenza di un insieme finito nel senso di Cantor implica l'esistenza dei numeri naturali.

Equivalenza tra le nozioni di infinito, infinito nel senso di Dedekind e infinito nel senso di Cantor. Numero di applicazioni iniettive tra due insiemi finiti.

4. Relazioni di equivalenza e relazioni d'ordine Definizione di relazione di equivalenza, classi di equivalenza, La partizione indotta da una relazione di equivalenza. Corrispondenza tra relazioni di equivalenza e partizioni. L'insieme quoziente e l'applicazione canonica. La relazione di equivalenza indotta da un'applicazione tra insiemi e sue proprietà.

Coefficienti binomiali. Formule ricorsive e formula per il calcolo in termini del fattoriale. Il triangolo di Tartaglia. La formula del binomio di Newton.

Relazioni di ordine parziale. Elementi confrontabili, ordini totali. Massimi, minimi, maggioranti e minoranti. La nozione di Buon ordinamento. I numeri naturali sono un insieme ben ordinato. Equivalenza tra il principio del buon ordinamento e il principio di induzione (senza dimostrazione). La seconda forma del principio di induzione come conseguenza del principio del buon ordinamento. Equivalenza tra PIN (prima forma), PBO e PIN (seconda forma) senza dimostrazioni.

5. Numeri interi, razionali, reali e complessi Costruzione assiomatica dei numeri interi relativi. Costruzione assiomatica dei numeri razionali. Cenni sulla costruzione dei numeri reali. Costruzione dei numeri complessi. Parte reale e immaginaria, coniugato, modulo (o norma). Il piano di Gauß, l'argomento di un numero complesso. Enunciato del Teorema fondamentale dell'algebra. Estrazione della radice n-esima di un numero complesso.

6. L'aritmetica dei numeri interi Divisibilità dei numeri interi. Numeri primi. Massimo comun divisore e minimo comune multiplo e loro unicità. Divisione euclidea. Esistenza di quoziente e resto. Esistenza del Massimo comun Divisore e dei coefficienti di Bezout. Algoritmo Euclideo delle divisioni successive e metodo per il calcolo dell'identità di Bezout Dimostrazione del Teorema Fondamentale dell'Aritmetica. Valutazioni p-adiche, divisibilit` MCD e mcm in termini di valutazioni p-adiche.

Operazione binarie. Semigruppi, monoidi e gruppi. Esempi sugli insiemi numerici.

7. Congruenze La relazione di congruenza è una relazione di equivalenza. Classi resto modulo m. Operazioni sulle classi resto. Le classi resto sono un gruppo abeliano rispetto alla somma e un monoide moltiplicativo rispetto al prodotto. Equazioni congruenziali lineari, esistenza e struttura della soluzioni. Applicazione al gruppo moltiplicativo delle classi resto invertibili. Funzione di Eulero. Teorema Cinese dei resti.

Moltiplicatività della funzione di Eulero. Definizione di anello e campo. L'anello delle classi resto modulo m è un campo se e solo se m è primo. Il piccolo Teorema di Fermat e il Teorema di Eulero.

8. Permutazioni Il gruppo delle permutazioni S_n. Definizioni e proprietà. La nozione di supporto e di orbita. La nozione di ciclo. Ogni permutazione si scrive in modo unico come prodotto di cicli disgiunti. Ogni permutazione si scrive come prodotto di trasposizioni. Il segno di una permutazione e sue proprietà (senza dimostrazioni)

Testi consigliati

[1] D. Dikranjan e M.S. Lucido, *Aritmetica e algebra*. Liguori, (2007).

Bibliografia supplementare

[2] M. Fontana e S. Gabelli, *Insiemi, numeri e polinomi. Primo ciclo di lezioni del Corso di Algebra con esercizi svolti*. CISU, (1989).
[3] M. Fontana e S. Gabelli, *Esercizi di Algebra*. Aracne, (1993).
[4] G.M. Piacentini Cattaneo, *Algebra, un approccio algoritmico*. Decibel, Zanichelli, (1996).
[5] R.B.J. Allenby, *Rings, fields and groups*. E. Arnold, Hodder & Staughton, (1991).
[6] M. Artin, *Algebra*. Prentice Hall, (1991).

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