AL110 Algebra 1

A.A. 2009/2010

Prof. Florida Girolami

Fondamenti

1. Insiemi e applicazioni

Nozione intuitiva di insieme. Operazioni tra insiemi (unione, intersezione, differenza, complementare) e loro proprietà. Insieme delle parti di un insieme. Esempi. Famiglie di insiemi: definizione, unione e intersezione.

Coppie ordinate. Prodotto cartesiano di due insiemi. Relazioni binarie. Applicazioni o funzioni. Esempi. Relazione inversa di una applicazione. Applicazione identica ed applicazioni costanti. Esempi. Prodotto operatorio di applicazioni e sue prime proprietà. Applicazioni suriettive, iniettive e biiettive: definizioni e proprietà. Applicazione inversa di una biiezione.

Non esiste alcuna applicazione suriettiva da un insieme X sull'insieme delle sue parti. Funzione caratteristica di un sottoinsieme. Esistenza di una biiezione da $\mathbf{C}alP(X)$ a $\{0,1\}^X$. Principio di Dirichlet. Insiemi finiti.

Ricoprimenti e partizioni di un insieme X. Esempi. Assioma della scelta. Una applicazione suriettiva ha una inversa destra. Un sottoinsieme di un insieme finito è finito. Intersezione e unione di un numero finito di insiemi finiti.

Numero degli elementi del prodotto cartesiano di due insiemi finiti. Numero delle applicazioni da un insieme finito in un insieme finito. Numero delle applicazioni iniettive da un insieme finito in un insieme finito. Una applicazione da un insieme finito in se stesso è iniettiva se e solo se è suriettiva se e solo se è biiettiva.

Relazioni d'equivalenza. Classi d'equivalenza. Insieme quoziente. Esempi. Relazioni di equivalenza e partizioni. Insieme quoziente. Relazione d'equivalenza ("nucleo") associata ad una applicazione. Teorema fondamentale di decomposizione di una applicazione. Esempi.

Relazioni di ordine e preordine; elementi massimali e minimali, massimi e minimi, maggioranti e minoranti, estremo superiore ed estremo inferiore in insiemi ordinati. Relazioni di ordine totale.

2. Numeri naturali

Assiomi di Peano; sistemi di Peano isomorfi (o equivalenti); principio di induzione (prima forma o forma debole).

Definizione di somma, prodotto, elevazione a potenza e fattoriale di numeri naturali.

Proprità dell'addizione e moltiplicazione in **N**. Coefficienti binomiali; formula del binomio; triangolo di Tartaglia.

Principio del Buon Ordinamento. Principio di Induzione (seconda forma). Dimostrazione del Principio del Buon Ordinamento dal Principio di Induzione (prima forma). Equivalenza tra Principio di Induzione prima forma, Buon Ordinamento e Principio di Induzione seconda forma (senza dimostrazione).

Scrittura di numeri naturali in base $b \geq 2$.

3. Insiemi numerici

Costruzione di **Z** (numeri interi relativi) a partire da **N**. Introduzione delle operazioni di somma e prodotto e della relazione d'ordine in **Z**. Prime Proprietà.

Divisione con il resto. Definizione di MCD. Esistenza del MCD. Identità di Bézout. Lemma di Euclide. Algoritmo di Euclide per la determinazione del MCD.

Determinazione di una identità di Bézout. Esempi. Definizione ed esistenza del mcm. Numeri primi. Teorema fondamentale dell'aritmetica. Teorema sulla infinità dei numeri primi. Crivello di Eratostene.

Criteri di divisibilità per 2^t, 3, 9, 5^t,11. L'indicatore di Eulero è una funzione moltiplicativa. $\varphi(p^h)$ con p numero primo. Congruenze. Addizione e moltiplicazione nell'insieme quoziente $\mathbf{Z}/\equiv_m$ delle classi resto modulo un intero $m > 1$. Principali proprietà algebriche di $(\mathbf{Z}/\equiv_m, +, \mathbf{C}dot)$.

Elementi invertibili e "divisori dello zero" in $\mathbf{Z}/\equiv_m$.

Calcolo di un inverso aritmetico modulo m. Indicatore di Eulero. Sistemi completi di residui modulo m. Sistemi ridotti di residui modulo m. Esempi.

Equazioni diofantee lineari del tipo $aX + cY = b$: criterio di risolubilità e soluzioni. Congruenze del tipo $aX \equiv b \pmod{m}$: criterio di risolubilità, numero di soluzioni e ricerca di soluzioni. Esempi. Il Teorema cinese dei resti. Esempi. Risoluzione di sistemi di congruenze lineari. Il piccolo Teorema di Fermat. Teorema di Eulero-Fermat.

Teorema di Wilson. Caratterizzazione dei numeri primi tramite il Teorema di Wilson. Se p è un numero primo dispari, la congruenza $X^2 \equiv -1 \pmod{p}$ è risolubile se e solo se $p \equiv 1 \pmod{4}$.

Costruzione di **Q** da **Z**.

Costruzione di **C** a partire da **R**. Proprietà dei numeri complessi, inverso e coniugato. Il piano di Argand-Gauss. Scrittura di un numero complesso nella forma $a+ib$ e scrittura in forma trigonometrica. La Formula di De Moivre. Radici n-sime e loro rappresentazione nel piano di Argand-Gauss.

4. Cenni sulle strutture algebriche: Gruppi ed Anelli

Semigruppi e monoidi. Gruppi. Notazione moltiplicativa e additiva. Gruppi abeliani. Esempi. Prime proprietà. Leggi di cancellazione. Tabelle. Potenze e

multipli. Esempi. Ordine di un elemento di un gruppo. Esempi.

Proprietà dell'ordine di un elemento di un gruppo. Sottogruppi. Esempi. Sottogruppo generato da un sottoinsieme di un gruppo. Sottogruppo generato da un elemento di un gruppo. Esempi. Sottogruppi di $\mathbf{Z}$. Definizione di gruppo ciclico. Esempi di gruppi ciclici. Definizione di omomorfismo di gruppi.

Permutazioni su un insieme X: definizione, prime proprietà ed esempi. Il caso X finito, cardinalità di S_n. Scrittura matriciale di una permutazione. Cicli e trasposizioni, cicli di una permutazione. Ordine di una permutazione, ogni elemento di S_n ha ordine finito, l'ordine di un m-ciclo è m. Ogni permutazione in S_n si scrive in modo unico (a meno dell'ordine) come composizione dei suoi cicli.

Scrittura di permutazioni come prodotto di trasposizioni, parità di una permutazione. L'ordine di una permutazione in S_n è il m.c.m. delle lunghezze dei suoi cicli. Definizione di orbita di un elemento sotto l'azione di una permutazione $\sigma \in S(X)$. Partizione del supporto di σ attraverso le orbite degli elementi di X.

Noindent Anelli. Esempi. Prime proprietà. Anelli commutativi ed unitari. Esempi. Elementi invertibili e zero-divisori. Domini d'integrità. Corpi. Campi. Esempi.

Caratteristica di un anello commutativo unitario. Caratteristica di un dominio d'integrità. Sottoanelli. Omomorfismi di anelli.

Il campo dei quozienti di un dominio d'integrità. Proprietà di universalità del campo dei quozienti.

5. Polinomi

Polinomi in una indeterminata a coefficienti in un anello commutativo unitario: somma e prodotto (di convoluzione). Grado: prime proprietà. Polinomi a coefficienti in un dominio d'integrità. Elementi associati in un dominio d'integrità. Polinomi invertibili a coefficienti in un dominio d'integrità. Algoritmo di divisione tra polinomi. Campo dei quozienti di un anello di polinomi a coefficienti in un campo ed in un dominio integro. L'algoritmo Euclideo in $K[X]$ ed esistenza del massimo comune divisore.

Elementi primi ed irriducibili in un dominio.

Polinomi irriducibili.

Radici di un polinomio. Teorema del resto. Esistenza di radici e riducibilità. La regola di Ruffini. Polinomio derivato. Radici multiple. Una radice è multipla se e solo se annulla il polinomio derivato. Un polinomio $f(X)$ a coefficienti in un campo numerico ha una radice complessa multipla se e solo se $\mathrm{MCD}(f(x), f'(X))$ è diverso da 1.

Teorema di fattorizzazione unica in $K[X]$ con K campo.

Polinomi a coefficienti numerici. Teorema Fondamentale dell'Algebra (solo

enunciato).

Polinomi irriducibili di $\mathbf{C}[X]$. Radici complesse e reali di polinomi a coefficienti reali. Polinomi irriducibili di $\mathbf{R}[X]$.

Polinomi a coefficienti interi: contenuto di un polinomio, polinomi primitivi. Lemma di Gauss. Teorema di fattorizzazione unica in $\mathbf{Z}[X]$. Polinomi irriducibili in $\mathbf{Z}[X]$ ed in $\mathbf{Q}[X]$.

Criterio di irriducibilità di Eisenstein. Irriducibilità del p-esimo polinomio ciclotomico in $\mathbf{Q}[X]$. Criterio di irriducibilità modulo un primo p. Schema riassuntivo sullo studio dell'irriducibilità di polinomi a coefficienti razionali.

Testi consigliati

[1] D. Dikranjan - M. S. Lucido, *Aritmetica e algebra*. Liguori Editore (2007).
[2] G.M. Piacentini Cattaneo, *Algebra, un approccio algoritmico*. Decibel – Zanichelli (1996).
[3] M. Fontana – S. Gabelli, *Insiemi, numeri e polinomi. Primo ciclo di lezioni del Corso di Algebra con esercizi svolti*. CISU (1989).
[4] M. Fontana, *Algebra 1, fondamenti (appunti integrativi per il corso AL1)*.
http://www.mat.uniroma3.it/users/fontana/didattica/fontana-didattica.html
[5] S. Gabelli - F. Girolami, *Anelli di Polinomi*.
http://www.mat.uniroma3.it/users/girolami/2005_2006/AL1/AL1.html

Bibliografia supplementare

[6] R.B.J. Allenby, *Rings, fields and groups*. E. Arnold, Hodder& Staughton (1991).
[7] 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

L'esame finale consiste di una prova scritta e di un colloquio orale.

Sono previste due prove di valutazione intermedia (esoneri); gli studenti che abbiano conseguito la sufficenza in entrambe queste prove sono esonerati dal sostenere la prova di esame scritta purché accedano alla prova orale negli appelli della prima sessione utile (appelli A e B).

Soltanto in occasione della prova scritta dell'appello A si può recuperare uno dei due esoneri.