AL110 Algebra 1

A.A. 2012/2013

Prof. Florida Girolami

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. Coppie ordinate. Prodotto cartesiano di due insiemi.

Proposizioni. Principali simboli logici: $\wedge$, $\vee$, $\neg$, $\Rightarrow$, $\Leftrightarrow$, simbolo di Sheffer. Tabelle di verità. Equivalenze logiche. Tautologie. Negazione di proposizioni del tipo $P \wedge Q$ e $P \vee Q$; negazione di proposizioni contenenti i simboli quantificatore esistenziale $\exists$ e quantificatore universale $\forall$. Dimostrazione per assurdo.

Corrispondenza tra un insieme X ed un insieme Y. Esempi. Corrispondenza composta. Esempi. Corrispondenza inversa. Applicazioni o funzioni. Esempi. Corrispondenza inversa di una applicazione. Applicazione identica ed applicazioni costanti. Prodotto operatorio di applicazioni e sue prime proprietà. La composizione di applicazioni iniettive è un'applicazione iniettiva. Una applicazione è iniettiva se e solo se ha una inversa a sinistra. Una applicazione è iniettiva se e solo è cancellabile a sinistra. Famiglia di elementi di un insieme X; famiglia di sottoinsiemi di un insieme X.

La composizione di applicazioni suriettive è un'applicazione suriettiva. Una applicazione è suriettiva se e solo se è cancellabile a destra. Assioma della scelta. Una applicazione è suriettiva se e solo se ha una inversa a destra. Applicazioni biiettive. Teorema di Cantor: non esiste alcuna applicazione suriettiva da un insieme non vuoto sull'insieme delle sue parti. $f^{-1}\big(f(A)\big)$ e $f\big(f^{-1}(B)\big)$.

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

Relazioni di preordine, ordine e ordine totale su un insieme. Elementi massimali e minimali, massimi e minimi, maggioranti e minoranti, estremo superiore ed estremo inferiore in insiemi ordinati. Catene in un insieme ordinato. Diagrammi lineari (di Hasse). Ordinamenti definiti sul prodotto cartesiano: ordine lessicografico ed ordine prodotto.

Principio di Dirichlet. Non esiste alcuna applicazione iniettiva da $\{1, 2, \cdots, m+1\}$ a $\{1, 2, \cdots, m\}$ per ogni $m \in N^+$. Insiemi finiti. Un sottoinsieme di un insieme finito è finito. Intersezione e unione di un numero finito di insiemi finiti. Una applicazione

da un insieme finito in se stesso è iniettiva se e solo se è suriettiva se e solo se è biiettiva. 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. Numero delle applicazioni biiettive (permutazioni) da un insieme finito in se stesso.

Funzione caratteristica χ_A. Esistenza di una applicazione biiettiva dall'insieme $\mathcal{P}(\mathcal{X})$ nell'insieme$\{0,1)^X$. Se X è un insieme finito con n elementi, allora $\mathcal{P}(\mathcal{X})$ ha 2^n elementi (anche dimostrazione per induzione su n). Determinazione del numero dei sottoinsiemi con k elementi di un insieme con n elementi.

2. Numeri naturali

Assiomi di Peano; sistemi di Peano isomorfi (o equivalenti); principio di induzione; metodo di dimostrazione per induzione. Definizione di somma, prodotto, elevazione a potenza e fattoriale di numeri naturali. Sistemi di Peano; sistemi di Peano equivalenti. Principio di induzione ampia. Principio del Buon Ordinamento.

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

3. Insiemi numerici

Costruzione di Z (numeri interi relativi) a partire da N. Operazioni di addizione e moltiplicazione 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. Definizione di mcm; relazione tra MCD e mcm. Equazioni diofantee del tipo $aX + bY = c$: criterio di risolubilità e descrizione delle sue radici.

Numeri primi. Teorema fondamentale dell'aritmetica. Determinazione del MCD e del mcm attraverso la fattorizzazione. Teorema sulla infinità dei numeri primi. Crivello di Eratostene.

Congruenze mod n. Insieme quoziente $Z/\equiv_m$ Inverso aritmetico modulo n. Sistemi completi di residui modulo n. Sistemi ridotti di residui modulo n. Esempi. Indicatore di Eulero.

Addizione e moltiplicazione nell'insieme quoziente $Z/\equiv_n$ delle classi resto modulo un intero $m > 1$. Principali proprietà algebriche di $(Z/\equiv_n, +, \cdot)$. Elementi invertibili e zero-divisori in Z_n. Scrittura di un numero naturale in base b. Criteri di divisibilità: per 2, 4, 2^h, per 5 e le sue potenze, per 3, per 9 e per 11. Determinazione di un criterio di divisibilità per d con d numero naturale primo con 10. 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 Wilson. Caratterizzazione dei numeri primi tramite il Teorema di Wilson. Teorema di Eulero-Fermat. Moltiplicatività dell'indicatore di Eulero (due dimostrazioni) Studio della congruenza $X^2 \equiv 1 \pmod{n}$. Se p è un numero primo dispari, la congruenza $X^2 \equiv -1 \pmod{p}$ è risolubile se e solo se $p \equiv 1 \pmod{4}$. Associare a $[a]_{nm}$ la coppia $([a]_n], [a]_m)$ definisce una applicazione f da Z_{nm} a $Z_n \times Z_m$; f è biiettiva se e solo se n ed m sono coprimi.

Costruzione di Q da Z.

Costruzione di C a partire da R. Proprieta' 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

Operazione binaria in un insieme. Semigruppi e monoidi. Esempi. Gruppi. Esempi. Notazione moltiplicativa e additiva. Gruppi abeliani. Esempi. Prime proprietà. Tabelle. Potenze e multipli. Definizione dell'ordine di un elemento di un gruppo. 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 Z. Definizione di gruppo ciclico. Esempi di gruppi ciclici. Definizione di omomorfismo di gruppi.

Permutazioni su un insieme X: definizione, prime proprieta' ed esempi. Il caso X finito, cardinalita' di S_n. Scrittura matriciale di una permutazione.Permutazione ciclica o ciclo di lunghezza l in S_n. Supporto di una permutazione. Permutazioni disgiunte. Definizione di orbita di un elemento sotto l'azione di una permutazione $f \in S_n$. Partizione del supporto di f attraverso le orbite degli elementi di X. Ogni permutazione in S_n si scrive in modo unico (a meno dell'ordine) come composizione

Scrittura di permutazioni come prodotto di trasposizioni, parita' di una permutazione. L'ordine di una permutazione in S_n e' 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. Il segno di una permutazione induce un omomorfismo da S_n nel gruppo $\{1, -1\}$. Definizione di A_n.
Anelli. Esempi. Anelli di applicazioni. Anelli di endomorfismi di gruppi abeliani. 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'. Proprieta' di universalitàdel campo dei quozienti.

L'anello (booleano commutativo unitario) delle parti di un insieme non vuoto. Ma-

trici di tipo $m \times n$. Il gruppo additivo delle matrici di tipo $m \times n$ ad elementi in un anello commutativo unitario. Prodotto righe per colonne di matrici quadrate di ordine n. L'anello unitario delle matrici quadrate di ordine n a coefficienti in un anello commutativo unitario. Anelli booleani: proprietà.

5. Polinomi

Polinomi in una indeterminata a coefficienti in un anello commutativo unitario: somma e prodotto (di convoluzione). Grado: prime proprieà. Polinomi a coefficienti in un dominio d'integrità D: formula del grado e $U(D[X]) = U(D)$. Elementi associati 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 e' multipla se e solo se annulla il polinomio derivato. Teorema di fattorizzazione unica in $K[X]$ con K campo.

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

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

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

Criterio di irriducibilita' di Eisenstein. Irriducibilita' del p-esimo polinomio ciclotomico in $Q[X]$. Criterio di irriducibilita' 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] D. Dikranjan - M. S. Lucido, *Aritmetica e algebra*. Liguori Editore, (2007).
[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.