AL1 Algebra 1, fondamenti
A.A. 2005/2006
Prof. Florida Girolami

1. Insiemi ed applicazioni

Nozione intuitiva di insieme. Operazioni tra insiemi (unione, intersezione, differenza, complementare) e loro proprietà. Differenza simmetrica di due insiemi. Insieme delle parti. Esempi.

Elementi di logica elementare. Tabelle della verità. Negazioni e quantificatori universali. Vari tipi di dimostrazione per assurdo.

Prodotto cartesiano di insiemi. 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. Applicazioni tra insiemi finiti. Biiezione tra l'insieme delle parti di un insieme X con l'insieme $\{0,1\}^X$. Esempi.

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

Cenni su: relazioni di ordine e ordine totale; insiemi ordinati; maggioranti, minoranti, elementi massimali, elementi minimali, minimo e massimo, estremi inferiori e superiori.

2. Numeri Naturali

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

Equivalenza tra il Principio del Buon Ordinamento ed il Principio di Induzione. Vari tipi di dimostrazione per induzione. Esempi.

3. Insiemi numerici

Costruzione di $\mathbb{Z}$ (numeri interi relativi) a partire da $\mathbb{N}$ e di $\mathbb{Q}$ (numeri razionali) a partire da $\mathbb{Z}$. Introduzione delle operazioni di somma e prodotto e della relazione di ordine in $\mathbb{Z}$ e $\mathbb{Q}$. Prime proprietà.

Costruzione dell'insieme $\mathbb{C}$ dei numeri complessi. Rappresentazione "geometrica" dei numeri complessi nel piano di Gauss. Rappresentazione trigonometrica di un numero complesso; formula di de Moivre; radici n-esime di un numero complesso. Radici n-esime dell'unità.

4. Divisibilità in $\mathbb{Z}$ e congruenze 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 ($b > 1$) dei numeri naturali.

Numeri primi. Elementi irriducibili. Teorema fondamentale dell'aritmetica. Teorema sull'infinità dei numeri primi. Crivello di Eratostene.

Congruenze e criteri di divisibilità. Somma e prodotto nell'insieme quoziente $\mathbb{Z}/\equiv_n$ delle classi resto modulo un intero $n > 1$. Principali proprietà algebriche ed aritmetiche di $(\mathbb{Z}/\equiv_n, +, \cdot\ )$. Elementi invertibili e "divisori dello zero" in $\mathbb{Z}/\equiv_n$. Indicatore di Eulero.

Il "piccolo" teorema di 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. Cenni sulle strutture algebriche: Gruppi ed Anelli

Operazioni e loro proprietà. Elementi neutri e invertibili. Unicità dell'elemento neutro e dell'inverso di un elemento. Notazione additiva e moltiplicativa.

Gruppi. Gruppi abeliani. Esempi. Prime proprietà. Leggi di cancellazione. Sottogruppi. Esempi. Omomorfismi di gruppi. Ordine di un elemento di un gruppo. Esempi.

Gruppi di permutazioni. Prime proprietà del gruppo S_n. Cicli e teorema di decomposizione. Trasposizioni, parità e segno di una permutazione.

Anelli. Esempi. Prime proprietà. Anelli commutativi e unitari. Esempi. Elementi invertibili e divisori dello zero. Domini d'integrità. Campi. Esempi. Omomorfismi di anelli. Caratteristica di un anello unitario. Esempi. Campo dei quozienti di un dominio d'integrità.

6. Polinomi

Polinomi in una indeterminata: somma, prodotto (di convoluzione) e grado.

Polinomi a coefficienti in un dominio d'integrità. Prime proprietà. Elementi invertibili e associati. Algoritmo della divisione tra polinomi.

Polinomi a coefficienti in un campo: esistenza ed unicità del MCD monico, identità di Bézout.

Radici di un polinomio. Teorema del resto. Regola di Ruffini. Esempi. Ricerca di radici intere e razionali di polinomi a coefficienti interi. Polinomio derivato. Radici multiple.

Polinomi irriducibili. Esistenza di radici e riducibilità. Teorema di fattorizzazione unica in $K[X]$ con K campo.

Polinomi a coefficienti numerici. Enunciato del Teorema Fondamentale dell'Algebra. Polinomi irriducibili di $\mathbb{C}[X]$ e di $\mathbb{R}[X]$.

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

Criterio di irriducibilità di Eisenstein. Esempi ed applicazioni (irriducibilità del p-polinomio ciclotomico).

Criterio di irriducibilità modulo un primo p.

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] M. Fontana, *Appunti sui primi rudimenti di teoria dei gruppi e teoria degli anelli*. http://www.mat.uniroma3.it/users/fontana/al1_04_05/al1.html,

[4] M. Fontana, *La nozione di d'insieme, prime operazioni tra insiemi, elementi basilari di logica*. http://www.mat.uniroma3.it/users/fontana/documents/al1-insiemi-log-elem-spt_000.pdf,

[5] S. Gabelli - F. Girolami, *Anelli di Polinomi*. http://www.mat.uniroma3.it/users/girolami/2005_2006/AL1/AL1.html,

[6] G.M. Piacentini Cattaneo, *Algebra, un approccio algoritmico*. Decibel – Zanichelli, (1996).

Bibliografia supplementare

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

[8] 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.