AL1 Algebra 1
A.A. 2001/2002
Prof. Florida Girolami

Fondamenti

1. Insiemi ed applicazioni

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, 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.

Relazioni di ordine e ordine totale. Diagrammi lineari di insiemi ordinati. Maggioranti, minoranti, elementi massimali, elementi minimali, minimo e massimo, estremi inferiori e superiori. Esempi.

Cenni sulla nozione di cardinalità. Caratterizzazione degli insiemi infiniti come gli insiemi equipotenti ad un (opportuno) sottoinsieme proprio. Cardinalità del numerabile e del continuo.

2. Numeri

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

Costruzione di $\mathbb{Z}$ a partire da $\mathbb{N}$ e di $\mathbb{Q}$ a partire da $\mathbb{Z}$.

Costruzione dell'insieme $\mathbb{C}$ dei numeri complessi e loro rappresentazione 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 e radici primitive.

3. Cenni sulle strutture algebriche

Operazioni e loro proprietà. Elementi neutri e invertibili. Unicità dell'elemento neutro e dell'inverso di un elemento. Notazione additiva e moltiplicativa. Semigruppi e gruppi. Leggi di cancellazione. Esempi. Sottogruppi. Omomorfismi. Il gruppo delle trasformazioni di un insieme. Gruppi di permutazioni. Prime proprietà del gruppo

S_n. Cicli e teorema di decomposizione. Trasposizioni, parità di una permutazione. Anelli. Anelli commutativi e unitari. Elementi invertibili e divisori dello zero. Domini d'integrità. Campi. Esempi. Caratteristica di un dominio di integrità.

4. Divisibilità in $\mathbb{Z}$. L'anello delle classi resto 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 dei numeri naturali.

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

Prime proprietà aritmetiche dell'anello $\mathbb{Z}_n$ delle classi resto modulo un intero $n > 1$. Criteri di divisibilità.

Elementi invertibili e zero-divisori dell'anello $\mathbb{Z}_n$. Indicatore di Eulero. Il teorema di Eulero-Fermat. Teorema di Wilson e caratterizzazione dei numeri primi.

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.

5. Polinomi

Polinomi a coefficienti in un dominio d'integrità: definizione, somma, prodotto, grado. Elementi invertibili e associati.

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

Polinomi irriducibili; teorema di fattorizzazione unica in $K[X]$.

Radici di un polinomio. Esistenza di radici e riducibilità. Teorema del resto. Regola di Ruffini.

Polinomio derivato. Radici multiple.

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

Ricerca di radici intere e razionali di polinomi a coefficienti interi. Polinomi a coefficienti interi: contenuto di un polinomio, polinomi primitivi. Lemma di Gauss. Teorema di fattorizzazione unica.

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

Criterio di irriducibilità 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] M. Fontana – S. Gabelli, *Esercizi di Algebra*. Aracne, (1993).
[4] R. Procesi Ciampi –R. Rota , *Algebra moderna. Esercizi*. Veschi, (1992).

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 consiste di una prova scritta e di un colloquio, allo scopo di accertare l'acquisizione da parte dello studente dei concetti e dei metodi illustrati nel corso.

Gli studenti che hanno sostenuto con esito positivo, nel corso del semestre, le prove di valutazione parziale ("esoneri") accedono direttamente al colloquio da sostenersi esclusivamente negli appelli di Gennaio e Febbraio.

Gli studenti che hanno sostenuto con esito positivo soltanto una delle due prove di valutazione parziale possono, soltanto in occasione della prova scritta dell'appello di gennaio, sostenere la prova scritta 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.