AL3 Algebra (3^0 Modulo)
A.A. 2000/2001

Prof. Florida Girolami

Gruppi, anelli e campi

1. Gruppi

Assiomi di semigruppo, monoide e gruppo e prime proprietà derivanti da essi. Esempi. Gruppi abeliani. Gruppi finiti e tavole. Gruppi di trasformazioni. Il gruppo simmetrico S_n. Cicli e teorema di decomposizione in cicli. Teorema del segno. Proprietà del segno. Il gruppo alterno A_n. Gruppi diedrali.

Sottogruppi e loro caratterizzazioni. Intersezione, unione e prodotto di sottogruppi. Sottogruppi generati da sottoinsiemi. Sottogruppi generati da un elemento. Ordine di un elemento. Esempi.

Relazioni d'equivalenza associate a sottogruppi. Classi laterali destre e sinistre. Teorema di Lagrange. Applicazioni e conseguenze: teorema di Eulero-Fermat e di Fermat.

Gruppi ciclici. Sottogruppi di gruppi ciclici. Generatori di un gruppo ciclico. Il teorema di Lagrange si inverte per i gruppi ciclici.

Omomorfismi tra gruppi. Nucleo e immagine di un omomorfismo. Composizione di omomorfismi.

Relazioni compatibili e sottogruppi normali. Gruppi quoziente. Esempi.

Il teorema fondamentale di omomorfismo tra gruppi e applicazioni. Primo e secondo teorema di omomorfismo per i gruppi.

Endomorfismi e automorfismi. Automorfismi di gruppi ciclici. Automorfismi interni. Esempi. Centro di un gruppo.

Teorema di Cayley.

Prodotti diretti di gruppi. Esempi. Azione di un gruppo su un insieme. Esempi di azioni; coniugio. Orbite; stabilizzatore e centralizzante. Equazione delle classi. Classi coniugate in S_n. Formula di Burnside. p-gruppi. Teorema di Cauchy. Applicazioni. Gruppi abeliani finiti. Teorema fondamentale sui gruppi abeliani finiti (senza dimostrazione).

2. Anelli

Definizione assiomatica di anello. Anelli commutativi e unitari. Divisori dello zero. Anelli integri. Domini, corpi, campi. Esempi: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, anelli di matrici, anelli di applicazioni, anelli di successioni, anelli di polinomi e serie formali a coefficienti in un anello qualsiasi, corpo dei quaternioni reali. Prime proprietà di un anello deducibili dagli assiomi. Prodotto diretto di anelli.

Sottoanelli. Caratterizzazione di un sottoanello di un anello. Intersezione di sottoanelli. Sottoanelli generati da sottoinsiemi. Sottoanelli di anelli unitari. Esempi.

Ideali (destri, sinistri, bilaterali). Intersezione, somma e prodotto di ideali. Ideali generati da sottoinsiemi. Ideali principali. Esempi. Ideali e relazioni d'equivalenza compatibili. Classi laterali modulo un ideale. Anello quoziente rispetto a un ideale. Esempi. Corrispondenza tra gli ideali di un anello quoziente A/I e gli ideali di A che contengono I.

Omomorfismi, epimorfismi, monomorfismi, isomorfismi, endomorfismi e automorfismi di anelli. Nucleo e immagine di un omomorfismo. Composizione di omomorfismi. Esempi. Teorema fondamentale di omomorfismo. Teorema del doppio quoziente. Applicazioni ed esempi.

Caratteristica di un anello. Esempi. Caratteristica di un dominio. Immersione di un dominio nel suo campo dei quozienti.

Ideali massimali e ideali primi. Caratterizzazioni attraverso l'anello quoziente per anelli commutativi unitari. Ideali di un campo.

Teoria della divisibilità in un dominio. Unità ed elementi associati. MCD e mcm di due elementi. Identità di Bézout. Esistenza del MCD in un dominio ad ideali principali (PID). Elementi primi e irriducibili. In un PID un elemento irriducibile è primo. Esempi di elementi irriducibili e non primi. Elementi con norma un numero primo sono irriducibili in $Z[\sqrt{d}]$.

Domini euclidei. Algoritmo euclideo delle divisioni successive. Divisione con resto in un anello di polinomi a coefficienti in un campo. Esempi di domini euclidei ($\mathbb{Z}$, $K[X]$, K campo, $Z[\sqrt{d}]$, $d = -2, -1, 2, 3$). Ogni dominio euclideo è un dominio ad ideali principali.

Domini a fattorizzazione unica (UFD). Esempi. In un UFD esiste MCD e mcm ed un elemento irriducibile primo. Ogni PID un UFD. Lemma di Gauss. Applicazioni. Criterio di irriducibilità di Eisenstein.

3. Campi

Caratteristica di un campo. Sottocampo fondamentale. Esempi.

Estensioni semplici algebriche e trascendenti.

Teorema di Kronecker (per ogni polinomio a coefficienti in un campo esiste una estensione di tale campo nella quale il polinomio ammette radici). Esempi.

Campo di spezzamento di un polinomio: teorema di esistenza e unicità (cenni). Esempi di costruzione del campo di spezzamento.

Campi finiti.

Testi consigliati

[1] G.M. Piacentini Cattaneo, *Algebra, un approccio algoritmico*. Decibel – Zanichelli, (1996).
[2] R.B.J.T. Allenby, *Rings, Fields and Groups*. Edward Arnold, (1991).
[3] M. Fontana – S. Gabelli, *Esercizi di Algebra*. Aracne, (1993).

Bibliografia supplementare

[4] M. Artin, *Algebra*. Prentice – Hall, Inc, (1991).
[5] M. Artin, *Algebra*. Bollati Boringhieri, (1997).
[6] L. Childs, *A concrete introduction to higher algegra*. Springer, (1992).
[7] I.N. Herstein, *Algebra*. Editori Riuniti, (1982).
[8] N. Jacobson, *Basic Algebra I, II*. Freeman, (1974, 1980).
[9] S. Lang, *Algebra*. Addison-Wesley, (1993).
[10] B.L. van der Waerden, *Modern Algebra*. Ungar, (1970).

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