Università degli Studi di Bologna

C.d.L. in Matematica - C.d.L. in Matematica Informatico-Computazionale

Programma del **Corso di ALGEBRA II** A.A. **2007/2008**

Prof. Mirella Manaresi (051-2094461, manaresi@dm.unibo.it)

I parte (3 crediti)

I - Omomofismi di gruppi e guppi quoziente

Omomorfismi di gruppi; nucleo e immagine; isomorfismi. Omomorfismi da $\mathbb{Z}$ ad un gruppo, omomorfismi da $\mathbb{Z}_n$ a $\mathbb{Z}_m$.
Coniugio. Relazione di coniugio in S_n. Sottogruppi normali e gruppi quoziente. Classificazione dei gruppi di ordine minore o uguale a 7.
Teorema fondamentale di omomorfismo per gruppi. Classificazione dei gruppi ciclici. Quoziente di S_4 rispetto al gruppo di Klein.

II - Omomofismi di anelli, ideali e anelli quoziente

Omomorfismi di anelli commutativi. Omomorfismi di anelli da $\mathbb{Z}$ ad un anello commutativo. Nucleo ed immagine di omornorfismi di anelli commutativi. Omomorfismi da un campo ad un anello commutativo. Isomorfismi di anelli commutativi.
Ideali in un anello commutativo e anelli quoziente. Caratterizzazione dei campi come anelli senza ideali non banali. Ideali primi e ideali massimali e loro caratterizzazioni mediante l'anello quoziente.
Teorema fondamentale di omomorfismo per anelli. Teorema cinese del resto.
Corrispondenza biunivoca fra gli ideali di un anello A contenente un ideale I e gli ideali dell'anello quoziente A/I.
Caratteristica di un anello. Caratteristica di un dominio di integrità. L'ordine di un campo finito come potenza della caratteristica.
Campo dei quozienti di un dominio di integrità. Campo dei quozienti come il più piccolo campo che contiene un dato dominio di integrità. Ogni campo di caratteristica zero (risp. di caratteristica $p>0$) contiene un sottocampo isomorfo a $\mathbb{Q}$ (risp. a $\mathbb{Z}p$).

III - Anelli euclidei

Relazione di divisibilità tra elementi di un dominio e sue proprietà. Elementi irriducibili. Anelli euclidei. Massimo comun divisore di due elementi. Ogni ideale in un anello euclideo è principale. Il massimo comun divisore di a e b come generatore dell'ideale (a,b). Esistenza e unicità della scomposizione in fattori primi in un anello euclideo. Esempi di anelli non euclidei.
Polinomi a coefficienti in un campo. Divisibilità tra polinomi. Polinomi associati. Polinomi irriducibili. L'algoritmo euclideo per i polinomi. Scomposizione in polinomi irriducibili. Campi algebricamente chiusi. Il teorema fondamentale dell'algebra.

Irriducibilità dei polinomi razionali. Radici razionali di un polinomio razionale. Polinomi interi primitivi. Prodotto di polinomi primitivi. Lemma di Gauss. Criterio di irriducibilità di Eisenstein. Esempi di polinomi razionali irriducibili.
Esempi di polinomi irriducibili su campi finiti. Numero dei quadrati in un campo finito e polinomi irriducibili di grado 2 su un campo finito.1 polinomi irriducibili di grado basso su Z_2. La riduzione modulo un primo di un polinomio intero con applicazioni all'irriducibilità di polinomi razionali.

II parte (3 crediti)

L'anello degli interi gaussiani Z[i]. L'algoritmo euclideo nell'anello degli interi gaussiani. Caratterizzazione dei primi che rimangono irriducibili in Z[il. Primi che sono somma di due quadrati. Elementi irriducibili in Z[i]. Decomposizione in irriducibili in Z[i]. Interi che sono somma di due quadrati.

IV - Estensioni di campi

Estensioni di campi. Estensioni finite. Grado di una estensione finita. Il quoziente di un anello di polinomi K[x] per l'ideale principale (f) generato da un elemento irriducibile. Forma normale degli elementi di K[x]/(f). Nuovi esempi di campi.
Estensioni semplici. Elementi algebrici ed elementi trascendenti su un campo. Numeri algebrici e numeri trascendenti. Polinomio minimo di un elemento algebrico. Caratterizzazione delle estensioni semplici mediante un elemento algebrico. Polinomio minimo e grado dell'estensione. Isomorfismo di K[X]/(p) con K[u] se u è un numero algebrico e p e' il suo polinomio minimo. Estensione algebrica semplice di un campo mediante un polinomio irriducibile. Estensioni finite ed estensioni algebriche. Chiusura algebrica di Q. Campo di spezzamento di un polinomio: teorema di esistenza e unicità a meno di isomorfismi.
Campi finiti. Radici del polinomio $x^{pn} - x$. Il gruppo moltiplicativo di un campo finito è ciclico. Automorfismo di Frobenius di un campo finito. I campi finiti di caratteristica p come estensioni semplici di Z_p. Campi di Galois di ordine p^n. Esistenza di un campo di Galois di ordine p^n per ogni numero primo p e per ogni intero positivo n. Isomorfismo tra due qualunque campi di ordine p^n. Sottocampi di un campo di Galois di ordine p^n. Studio dei campi di Galois di ordine 8 e 16.

Testi consigliati:

A.Vistoli: *Lezioni di Algebra*. Bologna, 1993-94
A.Conte - L.Picco Botta - D.Romagnoli: *Algebra* Levrotto e Bella, Torino 1990
I.N.Herstein: *Algebra*. Editori Riuniti, Roma 1994
E. Bedocchi: *Esercizi di Algebra*. Pitagora Editrice Bologna, 1995-96.

Durante le lezioni sono stati distribuiti fogli di esercizi, che si aggiungono a quelli reperibili nei testi consigliati. Ulteriore materiale per la preparazione della prova scritta si può trovare in tutti gli eserciziari di algebra consultabili in biblioteca, in particolare:

A.Alzati - M.Bianchi: *Esercizi di Algebra per Scienze dell Informazione*. Città Studi, Milano 1991.
A.Facchini: *Sussidiario di Algebra e Matematica Discreta* Decibel - Zanichelli, Bologna 1992
M.Fontana - S.Gabelli: *Esercizi di Algebra* Aracne Editrice, Roma, 1993
S.Franciosi - F.De Giovanni: *Esercizi di Algebra*. Aracne Editrice, Roma 1993.
R. Procesi Ciampi-R.Rota: *Algebra moderna*. *Esercizi*. Editoriale Veschi. Masson, Milano 1992.
A.Rugusa - C.Sparacino: *Esercizi di Algebra*. Zanichelli Editore, Bologna 1992.