Università degli Studi di Roma "Tor Vergata"

Corso di Laurea in **Matematica** – a.a. 2013/4

programma di **ALGEBRA 2** – prof. **Fabio Gavarini**

1 – RICHIAMI SU INSIEMI, RELAZIONI, APPLICAZIONI, OPERAZIONI

Relazioni, equivalenze, partizioni. Insiemi quoziente. Applicazioni. Teorema Fondamentale delle Applicazioni. Operazioni in un insieme, relazioni compatibili con operazioni (o "congruenze"); (omo)-morfismi; Teorema Fondamentale di Omomorfismo per gruppoidi. Prodotto diretto di gruppoidi.

2 – TEORIA GENERALE DEI GRUPPI E DEGLI ANELLI

Gruppi. Sottogruppi. Centro di un gruppo. Prodotto di sottogruppi in un gruppo. Ordine di un elemento. Equivalenze associate ad un sottogruppo; classi laterali; indice di un sottogruppo. Teorema di Lagrange. Congruenze in un gruppo, sottogruppi normali. Gruppi quoziente. Normalizzante di un sottogruppo. Sottogruppo e sottogruppo normale generati da un sottoinsieme di un gruppo.

Anelli. Sottoanelli. Anelli commutativi; domini; corpi; campi. Centro di un anello. La somma di sottoanelli in un anello. Equivalenze associate ad un sottoanello; classi laterali. Congruenze in un anello, ideali (sinistri, destri, bilateri). Anelli quoziente. Sottoanello e ideale sinistro/destro/bilatero generati da un sottoinsieme di un anello.

(Omo)morfismi tra gruppi. Immagine e nucleo di un morfismo. Teorema Fondamentale di Omomorfismo per gruppi. Corrispondenza tra sottogruppi di un gruppo G e sottogruppi dell'immagine di un morfismo di gruppi con dominio G. Primo e Secondo Teorema di Isomorfismo per gruppi.

(Omo)morfismi tra anelli. Immagine e nucleo di un morfismo di anelli. Teorema Fondamentale di Omomorfismo per anelli. Corrispondenza tra sottoanelli di un anello R e sottoanelli dell'immagine di un morfismo di anelli con dominio R. Primo e Secondo Teorema di Isomorfismo per anelli.

Endomorfismi e automorfismi di un gruppo o di un anello. Automorfismi interni e coniugazione in un gruppo. Teorema di Cayley (per gruppi e anelli); Teorema di Cayley Generalizzato per gruppi. Prodotto diretto (interno o esterno) di due o più gruppi o anelli. Prodotto semidiretto (interno o esterno) di due gruppi.

3 – AZIONI DI GRUPPI E RISULTATI STRUTTURALI

Il gruppo simmetrico $\mathcal{S}(X)$ delle permutazioni di un insieme X. Coniugazione nel gruppo simmetrico $\mathcal{S}_n$ su n elementi. Classi coniugate in $\mathcal{S}_n$: biiezione con le partizioni di n.

Azioni/rappresentazioni di un gruppo su un insieme: G-insiemi. G-orbite, stabilizzatori, punti fissi. Azioni indotte (sui sottoinsiemi, sulle partizioni, ecc.). Azioni di un gruppo su sé stesso. Centralizzante di un elemento in un gruppo. Equazione delle Classi in un gruppo finito. Teorema di Burnside.

Teorema di Cauchy. p-gruppi e loro struttura. Sottogruppi di Sylow di un gruppo finito. Teoremi di Sylow per un gruppo finito. Classificazione dei gruppi di ordine pq, con p e q primi distinti.

4 – GRUPPI RISOLUBILI E GRUPPI ABELIANI FINITI

Sottogruppo derivato, serie derivata. Gruppi risolubili. Ogni p-gruppo (finito) è risolubile. Caratterizzazione dei gruppi risolubili tramite la serie derivata. $\mathcal{S}_n$ è risolubile se e soltanto se $n < 5$.

Gruppi abeliani. Scomposizione di un gruppo abeliano finito in prodotto diretto dei suoi sottogruppi di Sylow. Classificazione dei gruppi abeliani finiti: 1° e 2° Teorema di Classificazione.

5 – ANELLI COMMUTATIVI

Divisibilità, elementi invertibili, elementi associati, *M.C.D.* e *m.c.m.*, divisori di zero, elementi nilpotenti. Domini, campi. Caratterizzazione dei campi in termini di ideali. Ideali primi e ideali massimali. Elementi irriducibili (=atomi) e elementi primi in un dominio. Campo dei quozienti di un dominio unitario: definizione e costruzione. Caratteristica e sottoanello fondamentale di un anello unitario.

Condizione della catena discendente (= CCD). Funzioni “valutazione” in un dominio. Criterio: in un dominio con una funzione “valutazione” vale la CCD.

Domini euclidei (= D.E.). Esistenza dell'unità, del *M.C.D.*, e di identità di Bézout per il *M.C.D.* in un D.E.: l'algoritmo euclideo. L'anello $\mathbf{Z}[i]$ degli interi di Gauss come esempio di D.E.

Anelli (o domini) a ideali principali (= A.(D.).I.P.). Ogni D.E. è un D.I.P.

Domini di Bézout (= D.B.). Ogni D.I.P. è un D.B.

Domini con *M.C.D.* (= D.MCD). Ogni D.B. è un D.MCD.

Domini a fattorizzazione unica (= D.F.U.). Caratterizzazioni diverse di un D.F.U. Ogni D.I.P. (in particolare, ogni D.E.) è un D.F.U. Ogni D.F.U. è un D.MCD, in cui esistono sia *M.C.D.* che *m.c.m.* dati in forma esplicita.

Domini atomici (= D.A.). Ogni D.F.U. è un D.A. Criterio: un dominio in cui vale la CCD è un D.A.

Polinomi a coefficienti in un D.F.U.: contenuto di un polinomio, polinomi primitivi. Lemma di Gauss. Se R è un D.F.U., allora $R[x]$ è un D.F.U., e quindi anche $R[x_1,\dots,x_n]$ è un D.F.U.

Criterio di Eisenstein per l'irriducibilità di un polinomio in una variabile a coefficienti in un D.F.U.

6 – TEORIA GENERALE DEI CAMPI, CAMPI FINITI

Sottocampo fondamentale di un campo. Estensioni di campi. Grado di un'estensione, moltiplicatività. Estensioni finite, estensioni infinite. Elementi algebrici, elementi trascendenti. Estensioni semplici, e loro forma esplicita. Polinomio minimo di un elemento algebrico. Teorema dell'Elemento Primitivo in caratteristica zero *(senza dimostrazione)*. Estensioni algebriche, estensioni trascendenti. Campi algebricamente chiusi. Chiusura algebrica di un campo: esistenza e unicità *(senza dimostrazione)*.

Ogni sottogruppo finito del gruppo moltiplicativo di un campo è ciclico.

Campo di spezzamento di un polinomio: esistenza e unicità. Elementi coniugati. Estensioni normali.

Derivazione formale dei polinomi; criterio del *M.C.D.*(f,f') per l'esistenza di radici multiple di $f(x)$.

Campi finiti (= c.f.): Teorema di Struttura e Teorema di Esistenza e Unicità per c.f. Caratterizzazione delle estensioni tra c.f.; le estensioni tra campi finiti sono normali. Il gruppo moltiplicativo di un campo finito è ciclico. Teorema dell'Elemento Primitivo per c.f. L'automorfismo di Frobenius di un c.f.

7 – TEORIA DI GALOIS

Monomorfismi (=immersioni) di un'estensione algebrica nella sua chiusura algebrica. Gruppo di Galois di un'estensione di campi; gruppo di Galois di un polinomio. Corrispondenze di Galois per un'estensione di campi.

Caratterizzazioni della normalità per un'estensione finita in caratteristica zero. Estensioni di Galois.

Teorema di Corrispondenza di Galois per estensioni di Galois finite in caratteristica zero.

Teorema di Corrispondenza di Galois per estensioni tra campi finiti.

Dimostrazione del Teorema Fondamentale dell'Algebra tramite la teoria di Galois.

==