Università degli Studi di Roma "Tor Vergata"

Corso di Laurea Triennale in **Matematica** - a.a. 2024/2025

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

1 - RICHIAMI SU INSIEMI, RELAZIONI, APPLICAZIONI, OPERAZIONI

Relazioni, equivalenze, partizioni; insiemi quoziente. Applicazioni (o "funzioni"); il *Teorema Fondamentale delle Applicazioni*. Operazioni (binarie) in un insieme, (omo)morfismi; il *Teorema di Cayley* per semigrupp. Relazioni compatibili con operazioni (o "congruenze"). Il *Teorema Fondamentale di Omomorfismo* per gruppi.

2 - TEORIA GENERALE DEI GRUPPI E DEGLI ANELLI

Gruppi e loro morfismi; sottogruppi, sottogruppi normali, sottogruppi caratteristici; centro di un gruppo. Il *Teorema di Cayley* per gruppi. Congruenze in un gruppo e sottogruppi normali; gruppi quoziente; sottogruppi normali come nuclei di morfismi. Sottogruppo e sottogruppo normale generati da un sottoinsieme di un gruppo. Il *Teorema Fondamentale di Omomorfismo per Gruppi*.

Corrispondenza tra sottogruppi e tra sottogruppi normali nel dominio e codominio di un morfismo di gruppi. Il *Primo Teorema di Isomorfismo* per gruppi. Prodotto di sottogruppi in un gruppo. Il *Secondo Teorema di Isomorfismo* (o *Teorema del Doppio Quoziente*) per gruppi.

Prodotto diretto di gruppi e sua caratterizzazione. Endomorfismi e automorfismi di un gruppo; automorfismi interni, coniugazione in un gruppo. Prodotto semidiretto di gruppi e sue caratterizzazioni.

Anelli e loro morfismi, sottoanelli; anelli commutativi, domini, corpi, campi; centro di un anello. Il *Teorema di Cayley* per anelli. Congruenze in un anello; ideali (sinistri, destri, bilateri); anelli quoziente; ideali (bilateri) come nuclei di morfismi. Sottoanello e ideale sinistro/destro/bilatero generati da un sottoinsieme di un anello. Il *Teorema Fondamentale di Omomorfismo per Anelli*.

Corrispondenza tra sottoanelli e tra ideali (sinistri/destri/bilateri) nel dominio e codominio di un morfismo di anelli. Il *Primo Teorema di Isomorfismo* per anelli. Somma di sottoanelli in un anello. Il *Secondo Teorema di Isomorfismo* (o *Teorema del Doppio Quoziente*) per anelli.

Prodotto diretto di anelli e sua caratterizzazione.

3 - AZIONI DI GRUPPI, G-SPAZI

Azioni/rappresentazioni di un gruppo su un insieme: G -insiemi (o " G -spazi"). G -orbite, stabilizzatori, punti fissi; azioni fedeli, azioni transitive, G -spazi omogenei. Relazione tra orbita e stabilizzatore di un punto in un G -spazio. Azioni indotte (sui sottoinsiemi, sulle partizioni, ecc.).

Azioni di un gruppo su sé stesso: azione sinistra, destra, per coniugazione. Centralizzante di un elemento in un gruppo. *Equazione delle Classi* in un gruppo finito. Il *Teorema di Burnside*.

Il gruppo simmetrico $\mathcal{S}(X)$ delle permutazioni di un insieme X ; il gruppo simmetrico $\mathcal{S}_n$ su n elementi. Permutazioni cicliche. Esistenza e unicità della scomposizione in cicli disgiunti di una permutazione. Ordine di una permutazione. Fattorizzazione di una permutazione in prodotto di trasposizioni; parità di una permutazione; il sottogruppo alterno $\mathcal{A}_n$. Il gruppo $\mathcal{S}_n$ è prodotto semidiretto di $\mathbf{Z}_2$ per $\mathcal{A}_n$.

Partizioni di n . Coniugazione nel gruppo $\mathcal{S}_n$. Classi coniugate in $\mathcal{S}_n$: biiezione con le partizioni di n .

Il gruppo diedrale $\mathcal{D}_n$ su n elementi: definizione come gruppo di automorfismi del grafo ciclico con n vertici; calcoli in $\mathcal{D}_n$, formule fondamentali. Il gruppo diedrale $\mathcal{D}_n$ è prodotto semidiretto di $\mathbf{Z}_2$ per $\mathcal{Z}_n$.

4 - ANALISI STRUTTURALE DEI GRUPPI, GRUPPI ABELIANI FINITI E GRUPPI RISOLUBILI

Teorema di Cauchy sull'esistenza di elementi di ordine primo in un gruppo finito. I p -gruppi e loro struttura; in ogni p -gruppo il centro è non banale, e ogni p -gruppo di ordine p^2 è abeliano.

Sottogruppi di Sylow di un gruppo finito. I *Teoremi di Sylow*. Applicazioni dei Teoremi di Sylow allo studio dei gruppi finiti. Classificazione dei gruppi di ordine pq , con p e q primi distinti.

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

5 - ANELLI COMMUTATIVI

Richiami su anelli commutativi unitari: divisibilità, divisori di zero, domini (di integrità), elementi invertibili, elementi associati, campi; elementi irriducibili (=atomi), elementi primi. Ogni primo è irriducibile. Caratterizzazioni alternative dei campi (tra gli anelli commutativi unitari). Ideali primi e ideali massimali in anelli commutativi unitari: definizione, caratterizzazione in termini di anelli quoziente. Massimo comun divisore (=MCD), minimo comune multiplo (=mcm); identità di Bézout per MCD.

Domini notevoli: domini di Bézout (=D.B.), domini con MCD (=D.MCD), domini euclidei (=D.E.), domini a ideali principali (=D.I.P.), domini di valutazione (=D.V.), domini a fattorizzazione (=D.F.) e domini a fattorizzazione unica (=D.F.U.). Le inclusioni tra classi notevoli di domini

CAMPI $\subsetneq$ D.E. $\subsetneq$ D.I.P. $\subsetneq$ D.B. $\subsetneq$ D.MCD e CAMPI $\subsetneq$ D.E. $\subsetneq$ D.I.P. $\subsetneq$ D.F.U. $\subsetneq$ D.V. $\subsetneq$ D.F.

Criterio di divisibilità in un D.F.U. Espressioni esplicite per $\text{MCD}(a,b)$ e $\text{mcm}(a,b)$ in un D.F.U., e relazione tra loro. In un dominio in cui ogni irriducibile sia primo, ogni fattorizzazione in irriducibili è unica; in particolare, ogni D.F. in cui ogni irriducibile sia primo è un D.F.U., e viceversa.

Polinomi a coefficienti in un D.F.U.: contenuto $c(f)$ di un polinomio, polinomi primitivi. *Lemma di Gauss*: il contenuto è moltiplicativo. Divisibilità in $R[x]$ – con R un D.F.U. – rispetto alla divisibilità in $Q_R[x]$ – con Q_R campo dei quozienti di R . Invertibilità, o (ir)riducibilità di un polinomio in $R[x]$ – con R un D.F.U. – rispetto a $Q_R[x]$. *Teorema di Trasporto*: Se R è un D.F.U., allora anche $R[x]$ è un D.F.U.; in conseguenza, anche $R[x_1, \dots, x_n]$ è un D.F.U.

Lemma: Un polinomio non nullo a coefficienti in un dominio ha al più tante radici quanto è il suo grado. *Teorema di Ruffini* sulle radici di un polinomio. *Criterio della Radice Intera* per la ricerca di radici di un polinomio a coefficienti in un D.F.U. *Criterio di Riduzione* per l'irriducibilità di un polinomio. *Criterio di Eisenstein* sull'irriducibilità di un polinomio a coefficienti in un D.F.U.

6 - ESTENSIONI DI CAMPI

La caratteristica $\text{char}(R)$ di un anello R : caso generale, caso unitario, caso di un dominio. Il sottoanello fondamentale di un anello unitario; il sottocampo fondamentale di un campo.

Ogni sottogruppo finito del gruppo moltiplicativo di un campo è ciclico; in conseguenza (a) in ogni campo finito, il gruppo moltiplicativo è ciclico; (b) per ogni campo e per ogni n in $\mathbb{N}_+$, le radici n -esime di 1 formano un sottogruppo ciclico del gruppo moltiplicativo del campo.

Estensioni di campi. Grado di un'estensione, moltiplicatività; estensioni finite, infinite, finitamente generate. Elementi algebrici, elementi trascendenti. Estensioni semplici e loro descrizione esplicita; il polinomio minimo di un elemento algebrico. Estensioni algebriche, estensioni trascendenti; ogni estensione finita è algebrica, ma non viceversa. Torri di estensioni e algebricità. Costruzione esplicita di un'estensione algebrica semplice di un campo F con polinomio minimo (e quindi grado) assegnato.

Campi algebricamente chiusi: definizione, esempi, caratterizzazioni alternative. Chiusura algebrica di un campo: esistenza e unicità, a meno di isomorfismi (*senza dimostrazione*).

Campi di spezzamento di un polinomio. Il *Teorema di Esistenza* del campo di spezzamento di un polinomio. Ogni isomorfismo tra campi si estende ad un isomorfismo tra campi di spezzamento di poli-