Università degli Studi di Roma "Tor Vergata"

Corso di Laurea Triennale in **Matematica** - a.a. 2019/2020

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, gruppoidi e loro (omo)morfismi; il *Teorema di Cayley* per semigruppi. Relazioni compatibili con operazioni (o "congruenze"). Il *Teorema Fondamentale di Omomorfismo* per gruppoidi.

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 sua caratterizzazione.

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: 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 per rotazioni e riflessioni. Teorema di struttura dei gruppi diedrali: il gruppo $\mathcal{D}_n$ è prodotto semidiretto di $\mathbf{Z}_2$ per $\mathbf{Z}_n$.

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* per un gruppo finito. Applicazioni dei Teoremi di Sylow allo studio della struttura di un gruppo finito. 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.

Commutatore tra elementi, sottogruppo derivato e serie derivata in un gruppo. Gruppi risolubili. Caratterizzazione dei gruppi risolubili tramite la serie derivata. Ogni *p*-gruppo (finito) è risolubile. Il gruppo simmetrico $\mathcal{S}_n$ è risolubile se e soltanto se $n < 5$.

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.

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

Criterio di divisibilità in un D.F.U. Espressioni esplicite per MCD(a,b) e mcm(a,b) in un D.F.U., e relazione tra loro.

Condizione della catena discendente - (ccd) - e funzioni di valutazione in un dominio. Ogni dominio in cui valga la (ccd) è un D.F. In ogni dominio in cui esista una funzione di valutazione, vale la (ccd), e quindi è un D.F. Applicazione ai domini di forma $\mathbf{Z}[\sqrt{-z}]$. In un dominio in cui ogni irriducibile sia primo, ogni fattorizzazione in irriducibili è unica. In ogni D.B. "irriducibile => primo". La funzione "altezza" in un D.F.U. Caratterizzazione dei D.F.U. in termini di (ccd) e di "irriducibile => primo".

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 $R[x_1,...,x_n]$ 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 $char(R)$ 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 $\mathbf{N}_+$, 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 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 polinomi corrispondenti. Due qualunque campi di spezzamento su F di uno stesso polinomio f(x) in $F[x]$ sono sempre isomorfi, tramite un isomorfismo che estende l'identità su F.

Elementi coniugati in un'estensione. Un'estensione K/F è chiusa per coniugati $\Leftrightarrow$ ogni polinomio irriducibile in $F[x]$ che abbia una radice in K si fattorizza in prodotti lineari in $K[x]$. Estensioni normali. Un'estensione è finita e normale se e soltanto se è campo di spezzamento di un polinomio.

Derivazione (formale) di polinomi. Radici multiple di un polinomio; polinomi separabili, polinomi inseparabili. Un polinomio $P(x)$ è inseparabile $\Leftrightarrow$ MCD(P(x),P'(x)) $\nsim 1$. In caratteristica zero, ogni polinomio è separabile. Caratterizzazione dei polinomi inseparabili in caratteristica positiva.

Il *Teorema dell'Elemento Primitivo* in caratteristica zero: Ogni estensione finita tra campi di caratteristica zero è (algebrica) semplice.

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

7 – TEORIA DI GALOIS E CAMPI FINITI

L'insieme $I(E/F)$ dei monomorfismi di un'estensione di campi E/F nella sua chiusura algebrica. Il gruppo di Galois $G(E/F)$ di un'estensione E/F. Il sottocampo E^H degli H-invarianti in E per ogni sottogruppo H del gruppo $\mathrm{Aut}_A(E)$. Le corrispondenze di Galois per un'estensione di campi qualsiasi.

Per un'estensione finita semplice E/F si ha $|G(E/F)| \leq |I(E/F)| \leq [E:F]$. Relazione tra $I(E/F)$ e i coniugati di un elemento primitivo di un'estensione algebrica semplice $E=F(\alpha)$ di F. Se char(F)=0 , allora $|I(E/F)| = [E:F]$ per $E=F(\alpha)$ algebrica semplice. Estensioni finite di Galois (o "galoisiane").

Teorema di Corrispondenza di Galois: Se char(F)=0 e K/F è estensione finita di Galois, allora le corrispondenze di Galois tra estensioni intermedie di K/F e sottogruppi di $G(K/F)$ sono inverse l'una dell'altra. Inoltre, ogni estensione intermedia L è normale (o, equivalentemente, è di Galois) su F se e soltanto se $G(K/L)$ è sottogruppo normale in $G(K/F)$; in tal caso $G(L/F)$ è isomorfo a $G(K/F)/G(K/L)$.

Il *Teorema Fondamentale dell'Algebra*: dimostrazione tramite la teoria di Galois.

Campi finiti. *Teorema di Struttura*, *Teorema di Esistenza* (costruzione di un modello esplicito) e *Teorema di Unicità* per campi finiti. Le estensioni tra campi finiti sono normali. Il gruppo moltiplicativo di un campo finito è ciclico. Il *Teorema dell'Elemento Primitivo* per campi finiti. L'automorfismo di Frobenius di un campo finito. Il gruppo degli automorfismi di un campo finito è ciclico, generato dal suo automorfismo di Frobenius; il gruppo di Galois di un'estensione tra campi finiti è ciclico, generato da un'opportuna estensione dell'automorfismo di Frobenius. Il *Teorema di Corrispondenza di Galois* per estensioni tra campi finiti.

==========