Università degli Studi di Roma "Tor Vergata"

Corso di Laurea Triennale in **Matematica** - a.a. 2021/2022

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

## 1 – 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* (=*Teorema del Doppio Quoziente*) per gruppi.

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* (=*Teorema del Doppio Quoziente*) per anelli. Prodotto diretto di anelli.

Prodotto diretto di anelli e sua caratterizzazione.

Prodotto diretto di gruppi e sua caratterizzazione. Endomorfismi e automorfismi di un gruppo; automorfismi interni, coniugazione in un gruppo; il centro di un gruppo, classi coniugate.

Prodotto semidiretto di (semi)gruppi e sue caratterizzazioni.

## 2 – ANALISI STRUTTURALE DEI GRUPPI, GRUPPI ABELIANI FINITI

Inversione del *Teorema di Lagrange* per gruppi ciclici.

*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. Inversione del *Teorema di Lagrange* per $p$-gruppi.

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.

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.

## 3 – ANELLI COMMUTATIVI, DIVISIBILITÀ E FATTORIZZAZIONE

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 unitari (=:$DOM_1$): campi (=: CAM), 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.) - o "domini atomici"- e domini a fattorizzazione unica (=:D.F.U.).'

*Esempi di anelli euclidei:* l'anello degli interi, l'anello degli interi di Gauss l'anello $k[x]$ con $k$ campo.

L'algoritmo euclideo per il calcolo del MCD e di un'identità per esso in un domino euclideo.

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.

Le inclusioni (strette) tra classi notevoli di domini

$$\text{CAM} \subsetneq \text{D.E.} \subsetneq \text{D.I.P.} \subsetneq \text{D.B.} \subsetneq \text{D.MCD} \subsetneq \text{DOM}_1 \quad - \quad \text{D.F.U.} \subsetneq \text{D.F.} \subsetneq \text{DOM}_1$$

Domini con la condizione della catena discendente (=:D.CCD); funzioni di valutazione, domini con valutazione (=:D.V.). Le inclusioni D.V. $\subsetneq$ D.CCD. $\subsetneq$ D.F. e D.F.U. $\subsetneq$ D.V. (per la valutazione "altezza"). Applicazione ai D.V. di forma $\mathbf{Z}[\sqrt{-z}]$. Domini in cui ogni irriducibile sia primo (=:D.I=P); in un D.I=P, ogni fattorizzazione in irriducibili è unica. L'inclusione D.B. $\subsetneq$ D.I=P (*Lemma di Euclide*).

Le inclusioni D.E. $\subsetneq$ D.V. $\subsetneq$ D.CCD $\subsetneq$ D.F. e D.I.P. $\subsetneq$ D.CCD $\subsetneq$ D.F.

*Caratterizzazioni dei D.F.U.:* D.F.U. $\Leftrightarrow$ D.V. & D.I=P $\Leftrightarrow$ D.CCD. & D.I=P $\Leftrightarrow$ D.F. & D.I=P

Le inclusioni D.E. $\subsetneq$ D.I.P. $\subsetneq$ D.F.U.

Polinomi a coefficienti in un D.F.U.: contenuto 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 Eisenstein* sull'irriducibilità di un polinomio a coefficienti in un D.F.U.

## 4 – 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 generate da un sottoinsieme. 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 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 su un campo 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 $\Leftrightarrow$ è campo di spezzamento di un polinomio.

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

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

## 5 – 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 $\mathrm{Aut}_{\mathcal{A}}(E)$. 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 $\mathrm{char}(F)=0$ , 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, e invertono l'inclusione. 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, il quoziente $G(K/F)/G(K/L)$ è isomorfo a $G(L/F)$, con un isomorfismo indotto dalla restrizione da $K$ a $L$.

Il gruppo di Galois $\mathcal{G}_f$ di un polinomio $f(x)$; il gruppo $\mathcal{G}_f$ agisce fedelmente sulle radici di $f(x)$, e tale azione è transitiva quando $f(x)$ è irriducibile. Radici dell'unità in un campo; proprietà del gruppo di Galois del polinomio $x^n - 1$ in $\mathbf{F}[x]$: l'isomorfismo con $U(\mathbf{Z}_n)$ quando $\mathbf{F} = \mathbf{Q}$ .

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* (a meno di isomorfismi) 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: ogni campo finito è estensione algebrica semplice di ogni suo sottocampo.

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 potenza dell'automorfismo di Frobenius.

Il *Teorema di Corrispondenza di Galois* per estensioni tra campi finiti *(cenni)*.

## BIBLIOGRAFIA


Giulio Campanella, "Appunti di Algebra 1 e 2" - con esercizi, ed. Nuova Cultura - La Sapienza, Roma; *disponibili in rete* agli indirizzi dispense 1 *(Campanella)* , esercizi 1 *(Campanella)* , dispense 2 - con esercizi *(Campanella)*

G. M. Piacentini Cattaneo, "Algebra", ed. Decibel-Zanichelli, Padova, 1996.

Serge Lang, "Algebra", Graduate Texts in Mathematics Vol. **211**, Springer Verlag, New York, 2002.

N. Herstein, "Algebra", ed. Editori Riuniti, Roma, 1994.


==========