Corso di Laurea Triennale in **Matematica** - a.a. 2018/19

programma di **ALGEBRA 1** (8 CFU)

prof. **Fabio Gavarini**

1 – INSIEMI, RELAZIONI, APPLICAZIONI

Insiemi, sottoinsiemi; insieme delle parti di un insieme. Unione, intersezione, differenza, differenza simmetrica, prodotto cartesiano di insiemi; complementare di un sottoinsieme.

Partizioni di un insieme; insieme quoziente e proiezione canonica associati a una partizione.

Corrispondenze tra insiemi; operazioni tra corrispondenze, corrispondenza inversa, composizione.

Funzioni (o "applicazioni"); funzioni iniettive, suriettive, biiettive. Composizione di funzioni; funzioni invertibili, funzione inversa. Caratterizzazioni delle funzioni invertibili; permutazioni di un insieme. Funzioni caratteristiche su un insieme. Biiezione tra funzioni caratteristiche e insieme delle parti.

Relazioni (binarie); casi speciali. Relazioni d'ordine. Equivalenze; classi di equivalenza, rappresentanti; insieme quoziente e applicazione canonica. Biiezione tra equivalenze in X e quozienti di X. L'equivalenza associata ad una applicazione. Il *Teorema Fondamentale delle Applicazioni*.

2 – IL SISTEMA DEI NUMERI NATURALI

Il Sistema dei Numeri Naturali $\mathbf{N}$: assiomi di Peano, esistenza, unicità. Principio di Induzione Semplice, Principio di Induzione forte, Principio del minimo. Metodo di dimostrazione per induzione.

Somma, prodotto e ordinamento per i naturali. Divisione con resto tra numeri naturali.

Scrittura posizionale dei numeri naturali; numerazioni in base qualsiasi, cambiamenti di base.

Elementi di calcolo combinatorio, Coefficienti binomiali, triangolo di Pascal-Tartaglia; la funzione fattoriale; formula di Newton per la potenza di un binomio (o di un multinomio).

3 – CARDINALITÀ

Insiemi equipotenti: cardinalità di un insieme. Insiemi (o cardinalità, o numeri cardinali) finiti e infiniti; ordine tra numeri cardinali. Cardinalità del numerabile. Caratterizzazione degli insiemi infiniti.

Primo Teorema ("diagonale") di Cantor. *Secondo Teorema di Cantor* (sulla cardinalità dell'insieme delle parti). Cardinali infiniti superiori; l'ipotesi generalizzata del continuo. La distribuzione (rispetto all'ordine) dei numeri cardinali. L'insieme $\mathbf{R}$ dei numeri reali ha la cardinalità del continuo (cenni).

4 – INSIEMI CON OPERAZIONI

Insiemi con una operazione (=gruppoidi); semigruppi, monoidi, gruppi; elementi speciali. Gli invertibili in un monoide M formano un gruppo $U(M)$.

(Omo)morfismi di gruppoidi. Il *Teorema di Cayley per Semigruppi*; il caso speciale dei monoidi.

Prodotto diretto di gruppoidi; gruppoidi di funzioni (a valore in un gruppoide).

Relazioni compatibili in un gruppoide; gruppoidi quoziente. L'equivalenza associata ad un morfismo di gruppoidi è compatibile (nel gruppoide dominio), e l'applicazione canonica è un (epi)morfismo dal gruppoide al gruppoide quoziente. Il *Teorema Fondamentale di Omomorfismo per Gruppoidi*.

Gruppoidi cancellativi. Costruzione del gruppo associato ad un gruppoide commutativo cancellativo; esempi: $(\mathbf{Z};+)$ - associato a $(\mathbf{N};+)$ - $(\mathbf{Q}_+;\cdot)$ - associato a $(\mathbf{N}_+;\cdot)$ - e $(\mathbf{Q}^*;\cdot)$ - associato a $(\mathbf{Z}^*;\cdot)$.

5 – I NUMERI INTERI

Costruzione di $(\mathbf{Z};+)$ come gruppo associato al semigruppo commutativo cancellativo $(\mathbf{N};+)$. Somma, prodotto, ordinamento in $\mathbf{Z}$; definizione e proprietà fondamentali. Valore assoluto di un intero.

Divisibilità in $\mathbf{Z}$: elementi primi, elementi irriducibili. Ogni elemento primo è irriducibile. *M.C.D.* e *m.c.m.* in $\mathbf{Z}$. Divisione euclidea (con resto) in $\mathbf{Z}$. Esistenza del *M.C.D.* in $\mathbf{Z}$, e identità di Bézout; calcolo tramite l'algoritmo euclideo. Equazioni diofantee; criterio di risolubilità, algoritmo di risoluzione.

In $\mathbf{Z}$ ogni elemento irriducibile è primo. Il *Teorema Fondamentale dell'Aritmetica* ("l'anello $\mathbf{Z}$ dei numeri interi è un dominio a fattorizzazione unica"). Esistono in $\mathbf{Z}$ infiniti elementi irriducibili (=primi). Esistenza di *m.c.m.* in $\mathbf{Z}$, relazione con *M.C.D.* La funzione di Eulero.

Equazioni diofantee in $\mathbf{Z}$; semplificazioni, criterio di risolubilità, metodo risolutivo.

Congruenza modulo n in $\mathbf{Z}$; definizione, descrizione del quoziente $\mathbf{Z}_n$, compatibilità con somma e prodotto. Somma e prodotto in $\mathbf{Z}_n$; definizione, proprietà. Criteri di divisibilità tra numeri interi.

Equazioni congruenziali lineari (in $\mathbf{Z}$), equazioni modulari (in $\mathbf{Z}_n$); semplificazioni, criterio di risolubilità, metodi di soluzione. Il gruppo $U(\mathbf{Z}_n)$ degli invertibili in $\mathbf{Z}_n$, criterio di invertibilità. Calcolo di potenze in $\mathbf{Z}_n$: generalità, il *Piccolo Teorema di Fermat*, il *Teorema di Eulero*.

Sistemi di equazioni congruenziali (lineari); sistemi in forma cinese. Il *Teorema Cinese del Resto*.

6 – GRUPPI

Gruppi e loro (omo)morfismi. Ordine di un gruppo. Il *Teorema di Cayley per Gruppi*: ogni gruppo G si immerge nel gruppo delle permutazioni su G.

Sottogruppi; criteri perché un sottoinsieme di un gruppo sia un sottogruppo. Intersezione e unione di una famiglia di sottogruppi. Il sottogruppo generato da un sottoinsieme (esistenza e descrizione).

Gruppi e sottogruppi ciclici. L'ordine di un elemento in un gruppo. Il *Teorema di Struttura dei Gruppi Ciclic*i (isomorfismo con $\mathbf{Z}$ o con $\mathbf{Z}_n$); classificazione dei gruppi ciclici. Biiezione tra i sottogruppi di un gruppo ciclico finito e i divisori del suo ordine. I generatori di un gruppo ciclico.

Equivalenza (destra e sinistra) in un gruppo associata ad un sottogruppo. Classi laterali di un sottogruppo; cardinalità delle classi laterali; indice di un sottogruppo. Il *Teorema di Lagrange* per gruppi finiti, e conseguenze: il *Teorema di Eulero*, il *Piccolo Teorema di Fermat*. Il sottogruppo associato ad una equivalenza compatibile in un gruppo; sottogruppi normali. Biiezione tra equivalenze compatibili e sottogruppi normali. Gruppi quoziente (rispetto a equivalenze compatibili).

Immagine e nucleo di un morfismo di gruppi. Un morfismo tra gruppi è iniettivo, risp. suriettivo, $\Leftrightarrow$ ha nucleo banale, risp. ha immagine totale. I sottogruppi normali di un gruppo G sono tutti e soli i nuclei dei morfismi di gruppo con dominio G. Il *Teorema Fondamentale di Omomorfismo per Gruppi*. Le corrispondenze tra sottogruppi del dominio e del codominio tramite un morfismo di gruppi.

Il gruppo simmetrico delle permutazioni di un insieme X. Notazioni standard per le permutazioni di n elementi. Permutazioni cicliche; decomposizione di una permutazione in cicli disgiunti.

7 – ANELLI

Anelli; casi speciali: commutativi, unitari, integri; corpi, campi. Anelli numerici, quaternioni; anelli di matrici; anelli di polinomi (o di serie), o di polinomi (o serie) di Laurent in una o più variabili. Anelli di funzioni; l'anello degli endomorfismi di un gruppo abeliano.

Sottoanelli di un anello; criteri per riconoscere un sottoanello. Unione e intersezione di sottoanelli. Sottoanelli generati da un sottoinsieme: esistenza e descrizione. Gli interi di Gauss.

(Omo)morfismi tra anelli. Immagine e nucleo di un morfismo tra anelli. Un morfismo tra anelli è iniettivo, risp. suriettivo, ⇔ ha nucleo banale, risp. ha immagine totale. Il *Teorema di Cayley per Anelli*: il caso speciale degli anelli unitari.

Relazioni compatibili in un anello; anelli quoziente (rispetto a equivalenze compatibili). Ideali sinistri/destri/bilateri. Biiezione tra equivalenze compatibili e ideali (bilateri). Il radicale nilpotente. Gli ideali (bilateri) di un anello A sono tutti e soli i nuclei dei morfismi di anello con dominio A. Ideali generati da un sottoinsieme; ideali principali. Il *Teorema Fondamentale di Omomorfismo per Anelli*. Le corrispondenze tra sottoanelli o idealii del dominio e del codominio tramite un morfismo di anelli.

Il campo dei quozienti di un dominio: definizione, unicità, costruzione, esempi.

Divisibilità in un dominio unitario; elementi associati; *M.C.D.*, *m.c.m.*, elementi irriducibili ed elementi primi. Ogni primo è irriducibile.

Anelli (a ideali) principali. Esistenza di *M.C.D.*, di identità di Bézout e di *m.c.m.* in anelli principali. In un dominio unitario a ideali principali, ogni elemento irriducibile è primo.

Anelli euclidei; definizione, esempi: $\boldsymbol{k}$, $\mathbf{Z}$, $\mathbf{Z}[i]$, $\boldsymbol{k}[x]$ (con $\boldsymbol{k}$ campo), $\mathbf{Z}_{(p)}$. Ogni anello euclideo è un dominio. Ogni anello euclideo è unitario e a ideali principali. Calcolo di *M.C.D.* e di identità di Bézout nei domini euclidei; risoluzione di equazioni diofantee, di equazioni congruenziali, di equazioni modulari, di sistemi di equazioni congruenziali (*Teorema Cinese del Resto*) per anelli euclidei.

Domini a fattorizzazione (o "domini atomici"), domini a fattorizzazione unica (=DFU): definizione, esempi, controesempi. Ogni anello euclideo è un DFU. Ogni dominio a ideali principali è un DFU.

Teorema di Euclide: in $\mathbf{Z}$, in $\mathbf{Z}[i]$ e in $\boldsymbol{k}[x]$ - con $\boldsymbol{k}$ campo - esistono infiniti irriducibili (=primi).

BIBLIOGRAFIA

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

Campanella G., "Appunti di Algebra 1" - "Appunti di Algebra 2"

Herstein I. N., "Algebra", Editori Riuniti University Press, Roma, 2010

==========