1 - INSIEMI, RELAZIONI, APPLICAZIONI

Insiemi, sottoinsiemi. Insieme delle parti. Unione, intersezione, differenza, differenza simmetrica, prodotto cartesiano di insiemi. Complementare di un sottoinsieme. Partizioni.

Corrispondenze tra insiemi; applicazioni. Applicazioni iniettive, suriettive, biiettive. Composizione di applicazioni; applicazione identità, applicazioni invertibili, l'applicazione inversa. Funzioni caratteristiche su un insieme. Biiezione tra funzioni caratteristiche e insieme delle parti.

Relazioni. Ordini. Equivalenze; classi di equivalenza; insieme quoziente e applicazione canonica. L'equivalenza associata ad una applicazione. Il Teorema Fondamentale delle Applicazioni.

2 - IL SISTEMA DEI NUMERI NATURALI

Il sistema dei numeri naturali **N**: assiomi di Peano, esistenza, unicità. Induzione semplice, induzione forte, principio del minimo. Dimostrazioni per induzione.

Somma, prodotto e ordinamento per i naturali. Notazione posizionale; numerazioni in base qualsiasi.

3 - CARDINALITÀ

Insiemi equipotenti: cardinalità di un insieme. Insiemi (o cardinalità, o numeri cardinali) finiti e infiniti; ordinamento tra numeri cardinali. Cardinalità del numerabile. Primo Teorema ("diagonale") di Cantor. Secondo Teorema di Cantor (sulla cardinalità dell'insieme delle parti). Cardinali infiniti superiori; l'ipotesi generalizzata del continuo. L'insieme dei numeri reali ha la cardinalità del continuo.

4 - INSIEMI CON OPERAZIONI

Insiemi con una operazione (=gruppidi); semigruppoidi, monoidi, gruppi. (Omo)morfismi di gruppidi. Relazioni compatibili in un gruppoide; gruppidi quoziente. L'equivalenza associata ad un morfismo di gruppidi è compatibile (nel gruppoide dominio), e l'applicazione canonica è un (epi)morfismo.

Il Teorema Fondamentale di Omomorfismo per Gruppidi.

Gruppidi cancellativi. Il gruppo associato ad un gruppoide cancellativo commutativo.

5 - I NUMERI INTERI

Costruzione del gruppo additivo **Z** dei numeri interi a partire dal monoide additivo dei naturali. Somma, prodotto, ordinamento in **Z**. Il monoide moltiplicativo degli interi non nulli è cancellativo: costruzione dei razionali non nulli come gruppo moltiplicativo associato al monoide degli interi non nulli.

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

In **Z** ogni elemento irriducibile è primo. Il Teorema Fondamentale dell'Aritmetica. Esistono in **Z** infiniti elementi irriducibili (=primi). Esistenza del *m.c.m.* in **Z**. La funzione di Eulero.

La congruenza modulo n in **Z** è compatibile con somma e prodotto; descrizione del quoziente $\mathbf{Z}_n$.

Congruenze lineari (tra interi): criterio per la risolubilità, algoritmo risolutivo. Sistemi di congruenze lineari; il Teorema Cinese del Resto. Criteri di divisibilità tra interi.

6 – GRUPPI

Gruppi; (omo)morfismi di gruppi. Ordine di un gruppo finito. Il Teorema di Cayley: per ogni gruppo G esiste un monomorfismo da G al 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.

Gruppi e sottogruppi ciclici. L'ordine di un elemento in un gruppo. Teorema di struttura dei gruppi ciclici: l'isomorfismo con $\mathbf{Z}$ o con $\mathbf{Z}_n$, biiezione tra i sottogruppi di un gruppo ciclico finito e i divisori del suo ordine. Classificazione dei gruppi ciclici. Calcolo dei generatori di un gruppo ciclico.

Equivalenza (destra e sinistra) in un gruppo associata ad un sottogruppo. Classi laterali; cardinalità delle classi laterali; indice di un sottogruppo. Il Teorema di Lagrange per gruppi finiti, e conseguenze: il Teorema di Eulero-Fermat, il Piccolo Teorema di Eulero. 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 se e soltanto se ha nucleo banale. 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.

Il gruppo simmetrico di tutte le permutazioni di un insieme X . Notazioni per le permutazioni di n elementi: tramite matrici $2 \times n$ oppure tramite fattorizzazione in cicli disgiunti. Coniugazione nei gruppi simmetrici. Permutazioni pari, permutazioni dispari.

7 – ANELLI

Anelli (in generale). Anelli commutativi, unitari, integri; corpi, campi. Anelli numerici, anello delle matrici quadrate a coefficienti in un anello, anelli di polinomi in una o più variabili, i quaternioni.

Sottoanelli di un anello; criteri perché un sottoinsieme di un anello sia un sottoanello. Gli interi di Gauss. Sottoanelli generati da un sottoinsieme (cenni).

Relazioni compatibili in un anello. Ideali sinistri/destri/bilateri. Ideali generati da un sottoinsieme (cenni); ideali principali. Anelli quoziente (rispetto a equivalenze compatibili).

Il campo dei quozienti di un dominio unitario. Esempio: i numeri razionali, le funzioni razionali.

(Omo)morfismi tra anelli Immagine e nucleo di un morfismo di anelli. Un morfismo tra anelli è iniettivo se e soltanto se ha nucleo banale. Gli ideali (bilateri) di un anello A sono tutti e soli i nuclei dei morfismi di anello con dominio A . Immagini e controimmagini di sottoanelli e di ideali rispetto ai morfismi di anelli. Il Teorema Fondamentale di Omomorfismo per Anelli.

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

Domini euclidei; definizione, esempi: k , $\mathbf{Z}$, $\mathbf{Z}[i]$, $k[x]$ (con k campo), $\mathbf{Z}_{(p)}$. Anelli (a ideali) principali. Ogni dominio euclideo è (unitario) a ideali principali. Esistenza di $M.C.D.$ e identità di Bézout in anelli principali. Calcolo di $M.C.D.$ e di identità di Bézout nei domini euclidei; risoluzione di equazioni diofantee, di congruenze, di sistemi di congruenze (Teorema Cinese del Resto). Ogni dominio euclideo è a fattorizzazione unica. Esistenza di infiniti polinomi irriducibili (=primi) in $k[x]$, con k campo; analogamente (cenni) in $\mathbf{Z}[i]$. Esistenza di $m.c.m.$, e calcolo di $M.C.D.$ e $m.c.m.$, in domini euclidei (cenni).

BIBLIOGRAFIA

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

G. Campanella, “Appunti di Algebra 1” - “Appunti di Algebra 2”.