Algebra 1 – Matematica – A.A. 2022-23 (corso annuale)
Docente: Alberto De Sole

Programma

Cardinalità. Definizioni. Teorema di Cantor Schroeder Bernstein. Insiemi numerabili ed esempi di insiemi non numerabili (in particolare $\mathbb{R}$). Assioma della scelta e Lemma di Zorn. Applicazione: $X \times X$ ha la stessa cardinalità di X, se X è infinito.

Aritmetica. L'anello $\mathbb{Z}$ dei numeri interi, come esempio di anello commutativo con unità. Divisori e multipli. Massimo comun divisore, identità di Bézout, algoritmo euclideo. Congruenza modulo n. Risoluzione di congruenze lineari e Teorema cinese dei resti. Fattorizzazione unica in $\mathbb{Z}$. Teorema: esistono infiniti numeri primi.

Gruppi. Definizione di gruppo, sottogruppo, ordine di sottogruppi ed elementi, omomorfismi, nucleo e immagine. Sottogruppi normali e quozienti. Teorema di Lagrange. Applicazione: RSA. Teorema di Cauchy (anche solo caso abeliano). Reciprocità quadratica e algoritmo di Solovay-Strassen per la primalità.

Gruppi (II parte). Azioni di gruppo. Teorema di Sylow.

Anelli. Definizioni ed esempi. Domini a ideali principali / domini Euclidei. Fattorizzazione unica in domini a ideali principali. Interi di Gauss e teorema dei due quadrati. Classificazione dei moduli f.g. su PID. Un esempio di non PID che ha fattorizzazione unica degli ideali. Lemma di Gauss. Criteri di irriducibilità.

Campi. Definizione ed esempi. Caratteristica di un campo. Campi finiti. Estensioni di campi. Elementi algebrici e trascendenti. Campi algebricamente chiusi ed esistenza della chiusura algebrica. Teorema fondamentale dell'algebra. Cenni alla teoria di Galois.