

Algebra 1 – Matematica – A.A. 2023-24 (corso annuale)

DOCENTI: ALBERTO DE SOLE & DANIELE VALERI

Programma

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. 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.

Teoria di Galois. Gruppo di Galois di un'estensione di campi. Teorema fondamentale della teoria di Galois. Esempi e applicazioni.