Corsi della laurea magistrale: Algebra

Marina Avitabile
Francesca Dalla Volta
Francesco Matucci
Andrea Previtali
Pablo Spiga
Thomas Weigel

UNIVERSITÀ DEGLI STUDI DI MILANO-BICOCCA
Dipartimento di Matematica e Applicazioni

Milano-Bicocca, 18 maggio 2020

1. Corsi
   - Teoria della Rappresentazioni
   - Teoria dei Numeri e Crittografia
   - Combinatorica Algebrica
   - Teoria geometrica dei Gruppi

2. Algebristi e argomenti di tesi

Cercate nuovi strumenti per studiare gruppi finiti?

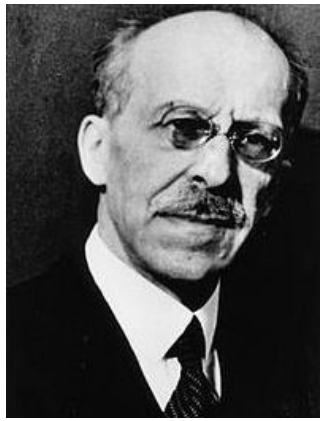
Provate ad immergerli in gruppi di matrici

Teoria delle Rappresentazioni (Prof. T. Weigel)

Anno I o II, Semestre I, 8 CFU (in inglese)

Scopo/Contenuti

- **Scopo**: *Presentare i fondamenti algebrici, i metodi, e alcune applicazioni della teoria classica*
- *Anelli e A-moduli semi-semplici;*
- *Moduli e Rappresentazioni di Gruppi e Algebre;*
- *Algebra Gruppo; Teorema di Maschke;*
- *Teoria dei Caratteri di un Gruppo finito;*
- *Prodotti tensoriali, restrizione e induzione di Rappresentazioni (teoria di Frobenius)*
- *Applicazioni: Rappresentazioni del Gruppo simmetrico; $p^a q^b$-Teorema di Burnside; Conteggio di Involuzioni, Teorema di Brauer-Fowler;*
- *Cenni alla Classificazione dei Gruppi semplici finiti;*
- *Restrizioni a un sottogruppo normale: teoria di Clifford.*



I. Schur (1875-1941)

R. Brauer (1901-1977)

Vi divertite a cifrare e decifrare messaggi?

Imparate le basi delle comunicazioni cifrate su internet

Teoria dei Numeri e Crittografia (Prof.ssa F. Dalla Volta)

Anno I o II, Semestre II, 8 CFU

Scopo/Contenuti

- **Scopo**: *Fornire alcuni argomenti (elementari e classici) di Teoria dei numeri, utili per protocolli crittografici a chiave pubblica;*
- *Sistemi crittografici; chiavi pubblici e privati;*
- *Numeri primi, il teorema di Dirichlet;*
- *Test di primalità; Algoritmi di Fattorizzazione;*
- *Funzione ζ di Riemann, Ipotesi di Riemann e Ipotesi di Riemann generalizzata;*
- *Crittosistema di Diffie-Hellman, il Logaritmo discreto;*
- *Curve ellittiche e il loro gruppo; cenno sull'ultimo teorema di Fermat;*
- *Fattorizzazione con le Curve ellittiche;*
- *Firma digitale classica e sulle Curve ellittiche.*

P. de Fermat (1601-1665)

B. Riemann (1826-1866)

Usate il telefono o comunicate col vostro satellite?

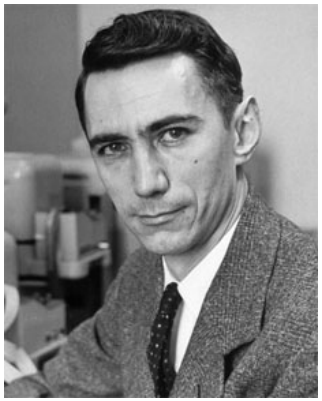
Creiamo ridondanza per difenderci da perdite di segnale

Combinatorica Algebrica:
Teoria dei Codici correttori di Errore (Prof. A. Previtali)

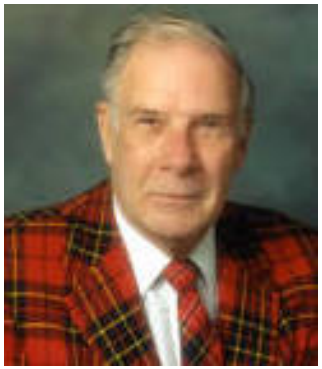
Anno I o II, Semestre II, 8 CFU

Scopo/Contenuti

- **Scopo**: *Acquisire le tecniche e gli strumenti algebrici atti a individuare e correggere errori nella trasmissione di messaggi;*
- *Informazione;*
- *Trasmissione di messaggi, Probabilità di Errore;*
- *Entropia;*
- *Teorema di Shannon;*
- *Codici correttori di errore;*
- *Campi finiti, Codici lineari;*
- *Codici di Hamming, di Reed-Salomon e di Reed-Muller;*
- *Immagini dallo spazio, CD e DVD;*
- *Teoremi di MacWilliams.*



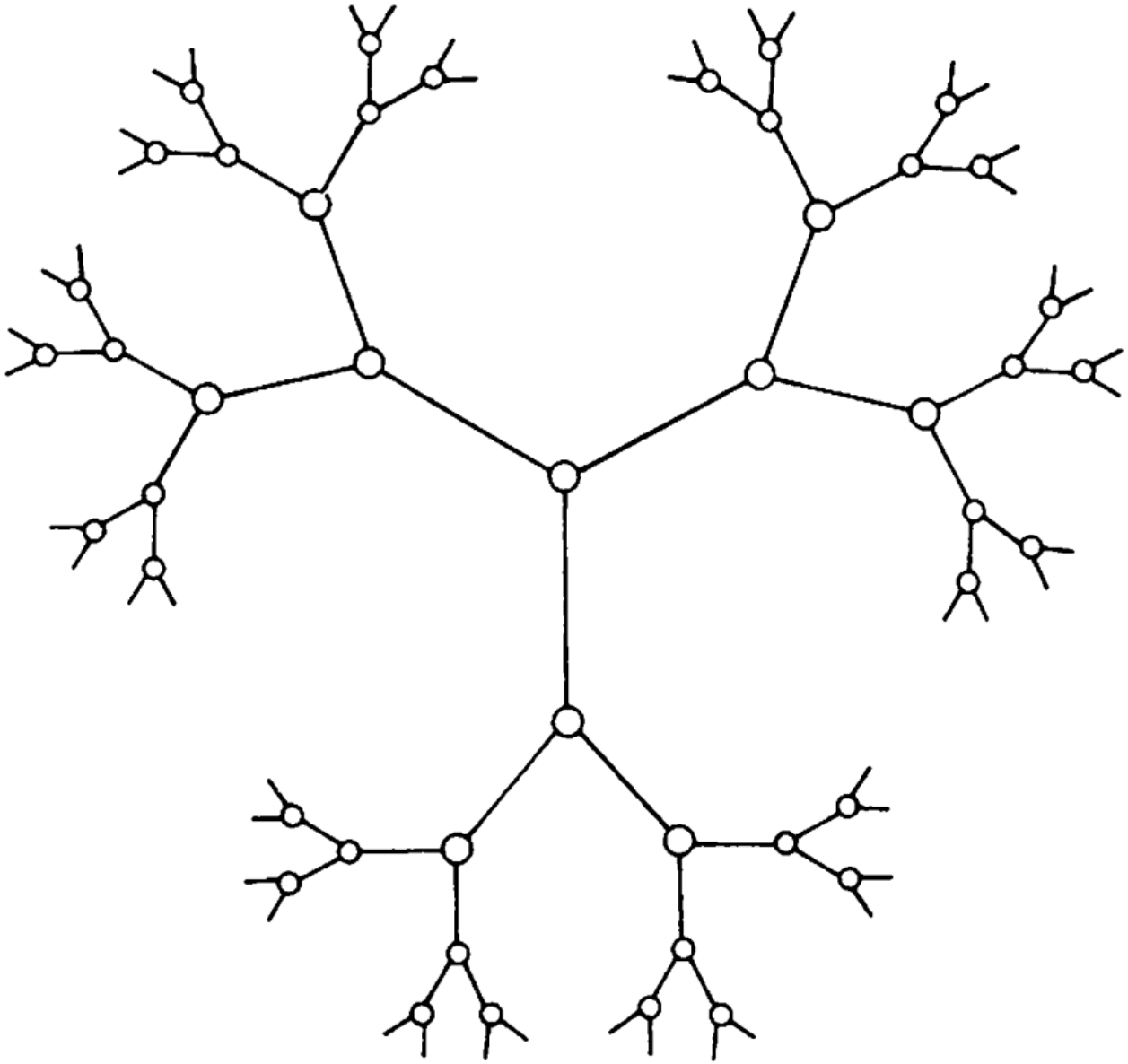
C. Shannon (1916-2001)



R. Hamming (1915-1998)

Ogni gruppo costituisce le simmetrie di qualche spazio?

Sì e le proprietà dello spazio aiutano lo studio del gruppo



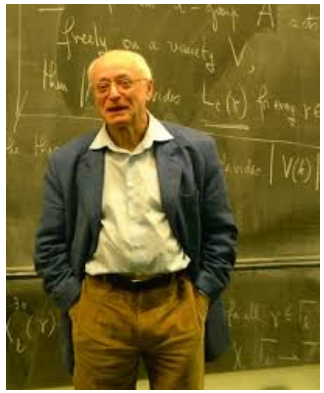
Teoria geometrica dei Gruppi (Prof. F. Matucci)

Anno I o II, Semestre I, 8 CFU

Scopo/Contenuti

- **Scopo**: *Studiare la struttura di gruppi mediante strumenti geometrici;*
- *Grafi;*
- *Cammini e connettività;*
- *Azioni di gruppi su grafi;*
- *Grafi di Cayley;*
- *Gruppi liberi;*
- *Prodotti liberi con amalgama;*
- *Grafi di gruppi;*
- *Gruppo fondamentale di un grafo di gruppi;*
- *Teorema fondamentale della teoria di Bass-Serre.*

H. Bass (1932*)



J-P. Serre (1926*)

Algebristi a Bicocca e alcuni loro interessi

- Marina Avitabile (algebre di Lie e teoria dei numeri)
- Francesca Dalla Volta (gruppi in crittografia, generazione di gruppi, curve su campi finiti)
- Francesco Matucci (teoria combinatoria e geometrica di gruppi)
- Andrea Previtali (combinatoria, teoria delle rappresentazioni)
- Pablo Spiga (combinatoria, gruppi di permutazioni)
- Thomas Weigel (gruppi profiniti, teoria delle rappresentazioni, teoria geometrica di gruppi)

Tesi di Laurea Magistrale

Argomenti

- *Applicazioni della teoria dei gruppi alla crittografia;*
- *Problemi su generazione di gruppi*
- *Argomenti classici di teoria dei gruppi finiti e profiniti;*
- *Calcolo di gruppi di automorfismi di codici;*
- *Risultati di struttura su gruppi che agiscono su alberi;*
- *Calcolo di rappresentazioni con assegnato carattere;*
- *Entropia algebrica per gruppi finitamente generati;*
- *Censimento di grafi vertice-transitivi cubici;*
- *Congettura di Isbell su giochi omogenei;*
- *Problemi di decisione, finitezza e struttura di sottogruppi in gruppi che agiscono su un insieme di Cantor;*