

# Algebra

June 19, 2017

## Syllabus

### Permutazioni, Coefficienti binomiali

- Permutazione
- Insieme di tutte le permutazioni su un insieme  $X$
- Ciclo di una permutazione,  $l$ -ciclo
- Cicli disgiunti
- Decomposizione in cicli disgiunti
- Ordine (o periodo) di un ciclo
- Ordine (o periodo) di una permutazione
- TEOREMA: Ogni permutazione si può scrivere come una composizione di cicli disgiunti in modo unico a meno dell'ordine dei cicli stessi
- Permutazione senza punti fissi, Derangement, partial derangement
- Trasposizione di una permutazione
- Segno di una permutazione
- Orbita di una permutazione
- Coefficienti binomiali: definizione e proprietà
- Principio di inclusione-esclusione

### Teoria dei Gruppi

#### Gruppi

- Gruppo
- Elemento neutro di un gruppo
- Finite Group
- Order of a group
- Ordine di un elemento di un gruppo (vedi Order of a group)

- Sottogruppo
- Gruppo abeliano
- Teorema di Lagrange e sue conseguenze
- Gruppo ciclico
- Gruppo generale lineare
- Gruppo simmetrico
- Gruppo classi resto modulo  $n$  rispetto alla somma
- Gruppo di permutazioni
- Sottogruppo ciclico del gruppo simmetrico  $S_n$  - Sottogruppo ciclico generato da una permutazione
- Omomorfismo
- Isomorfismo
- Omomorfismo/Isomorfismo tra ...
- Omomorfismo di gruppi
- Nucleo, nucleo di una funzione, nucleo di applicazione lineare
- Nucleo di omomorfismo di gruppi
- Insieme degli omomorfismo di gruppi ( dati due gruppi  $G$  e  $H$  in simboli:  $Hom(G, H)$ )

## **Anelli e Campi**

- Anelli
- Anelli commutativi: 0-divisori, elementi nilpotenti, unità.
- Domini, campi.
- Estensioni quadratiche.
- Gli interi di Gauss.
- Domini euclidei: ideali principali, esistenza del massimo comun divisore, scomposizione in fattori irriducibili.
- Morfismi di anelli; il morfismo da  $\mathbb{Z}$  ad un anello; la caratteristica.
- Ideali e anelli quozienti; ideale generato da un sottoinsieme.
- La fattorizzazione di un morfismo di anelli.
- Il campo dei quozienti di un dominio;  $\mathbb{Q}$ ,  $K(X)$ .
- Divisibilità in un anello.

- Ideali primi e massimali.
- Il campo dei numeri complessi;
- rappresentazione geometrica dei numeri complessi;
- teorema di De Moivre;
- l'insieme delle radici  $n$ -esime di un numero complesso come laterale rispetto al sottogruppo delle radici  $n$ -esime dell'unità.
- L'anello dei polinomi in una indeterminata a coefficienti in un anello,
- serie formali,
- funzioni polinomiali,
- grado di un polinomio e sue proprietà,
- se  $A$  è un dominio anche  $A[x]$  lo è.
- Polinomi a coefficienti in un campo: zeri e fattori lineari;
- il lemma di divisione e le sue conseguenze ( $K[X]$  è un dominio euclideo, a fattorizzazione unica, ad ideali principali).
- Il teorema fondamentale dell'algebra.
- La derivata di un polinomio, molteplicità di una radice.
- Polinomi reali.
- Quozienti di  $K[X]$ ; forma ridotta.
- Estensioni di campi;
- elementi algebrici e trascendenti;
- polinomio minimo;
- il sottocampo  $K(u)$  di un campo  $F$  generato dal sottocampo  $K$  di  $F$  e dall'elemento  $u$ .
- Il grado di una estensione finita;
- ogni elemento di una estensione finita è algebrico;
- il grado della composizione di due estensioni finite;
- l'insieme dei numeri algebrici è algebricamente chiuso.
- Campo di spezzamento: esistenza e unicità.
- Esistenza e unicità del campo con  $p^n$  elementi; questi sono gli unici campi finiti.

## Teoria di Galois

- Teoria di Galois
- Richiami sui polinomi e le loro radici.
- Campo di spezzamento (di un polinomio).
- Funzioni simmetriche.
- Estensioni normali di campi.
- Estensioni separabili di campi.
- Teorema dell'elemento primitivo.
- Estensioni di Galois.
- Il gruppo di Galois di un'estensione.
- La corrispondenza di Galois.
- Il gruppo di Galois di un polinomio.
- Il discriminante di un polinomio.
- Radici multiple, separabilità.
- Gruppo di Galois.
- Corrispondenza di Galois.
- Teorema 90 di Hilbert.
- Risolubilità per radicali.
- Estensioni ciclotomiche.
- Costruzioni con riga e compasso.
- Il gruppo simmetrico come gruppo di Galois.
- Chiusura algebrica.

## Teoria dei Moduli

- Anelli commutativi, ideali primi e massimali.
- Moduli: definizioni di base.
- Prodotto e somma diretta di moduli.
- Moduli liberi.
- Moduli noetheriani e artiniani.
- Anelli noetheriani.
- Teorema della base di Hilbert.

- Moduli finitamente generati e loro presentazione.
- Concetto di algebra.
- Moduli su anelli euclidei e PID.
- Decomposizione di un modulo su un anello euclideo e sue conseguenze.
- Forme canoniche di un endomorfismo.
- Prodotto tensoriale di moduli.