# AL2 Algebra 2: Gruppi, Anelli e Campi

## A.A. 2009/2010

**Prof. Francesco Pappalardi**

**1. Teoria dei Gruppi** Definizione di gruppo e prime proprietà. Proprietà delle permutazioni. La nozione di sottogruppo. Criterio per la verifica che un sottoinsieme è un sottogruppo. I sottogruppi di $S_3$. Intersezione di sottogruppi. Sottogruppo generato da un sottoinsieme di un gruppo. Gruppi finitamente generati. Gruppi ciclici. Gruppi ciclici e ordini degli elementi. Unione di sottogruppi e catene ascendenti di sottogruppi.

Classi laterali (destre e sinistre). Esempi nel gruppo $S_3$ e in $\mathbf{Z}$. Cardinalità delle classi laterali. L'indice di un sottogruppo. Il Teorema di Lagrange e sue conseguenze. Gruppi ciclici di ordine $p$. Gruppi senza sottogruppi. Esponente di un gruppo. Gruppo diedrale, definizione come gruppo delle simmetrie del quadrato e come sottogruppo di $S_4$. Tabella moltiplicativa. Prodotto diretto di gruppi. Il gruppo dei quaternioni e i suoi sottogruppi.

Sottogruppi normali. Caratterizzazioni, proprietà ed esempi. Gruppo generale lineare su un campo $\mathrm{GL}_n(K)$ e alcuni suoi sottogruppi. Il centro di un gruppo e sue proprietà. La defizione di gruppo quoziente. Omomorfismi di gruppi. Isomorfismi, proprietà degli omomorfismi. Nuclei di omomorfismi e loro relazione con l'iniettività dell'omomorfismo e con i sottogruppi normali.

Il teorema di corrispondenza e suoi corollari; il primo teorema di omomorfismo di gruppi. Il gruppo ortogonale è sottogruppo del gruppo generale lineare; descrizione esplicita del sottogruppo generato da un insieme di elementi; un gruppo in cui ogni elemento ha ordine 2 è abeliano. Il secondo e il terzo teorema di omomorfismo. Il centro del gruppo diedrale $D_n$, il centro del gruppo delle permutazioni $S_n$, il centro del gruppo generale lineare $\mathrm{GL}_n(K)$; elementi coniugati hanno lo stesso ordine; il gruppo generale lineare di ordine 2 sul campo con due elementi è isomorfo a $S_3$.

Il logaritmo come omomorfismo, applicazioni varie del primo Teorema di Omomorfismo, Il gruppo dei numeri complessi di norma 1 è isomorfo al gruppo quoziente $\mathbf{R}/\mathbf{Z}$. Il gruppo degli automorfismi di un gruppo, Il sottogruppo degli automorfismi interni. Proprietà dei gruppi ciclici e abeliani. Automorfismi dei gruppi ciclici. Il teorema di classificazione dei gruppi abeliani finiti (senza dimostrazione). Il primo teorema di Sylow (senza dimostrazione).

**2. Teoria degli Anelli** Definizione di anello e prime proprietà. Il gruppo delle unità, divisori dello zero e leggi di cancellazione. Il corpo dei Quaternioni. La nozione di sottoanello, proprietà dei sottoanelli. Sottoanello fondamentale e caratteristica. Ideali destri, sinistri e bilateri. Proprietà degli ideali.

Anelli senza ideali e campi/corpi. Definizione di Anello quoziente. Ideali Primi e Ideali massimali. Caratterizzazioni mediante i quozienti. Omomorfismi di anelli, Nucleo, priezione canonica, Teoreama di corrispondenza di sottoanelli e ideali. Il Teorema di Omomorfismo per anelli, secondo e terzo Teorema di omomorfismo per anelli (senza dimostrazione), ideali primi e massimali e omomorfismi.

Il campo dei quozienti di un dominio di integrità. Costruzione dell'anello dei polinomi $A[X]$, teorema di divisione con resto. Similarità tra $\mathbf{Z}$ e $K[X]$, con $K$ campo: entrambi sono PID, entrambi possiedono MCD e identità di Bézout. Prodotti di anelli, idempotenti centrali e ortogonali. Caratterizzazione dei prodotti diretti. Estensioni semplici e anelli di polinomi. grado. Divisioni in $A[x]$. Campi delle funzioni razionali su un dominio di integrità.

Elementi primi e irriducibili di un anello. Ogni elemento primo è irriducibile. elementi associati. Domini a fattorizzazione unica (UFD). Proprietà dei domini a fattorizzazione unica. Catene ascendenti di ideali principali. Esistenza di MCD in un UFD. Esistenza di MCD e identità in un dominio a ideali principali (PID). Dimostrazione che i domini a ideali principali sono a fattorizzazione unica. Lemma di Gauss. Ideali e elementi primi. caratterizzazione degli UFD in termini di elementi irriducibili e catenene ascendenti di ideali principali stazionarie. L'anello dei polinomi a coefficienti in un campo è un dominio Euclideo. $\mathbf{Z}[i]$ è un dominio euclideo. I primi della forma $p = 4k + 1$ sono la somma di due quadrati.

Il Teorema di Ruffini e i suoi corollari. Un polinomio di grado $n$ su un dominio ha al più $n$ radici distinte. Principio di identità per polinomi. Fattorizzazione di $X^p - X$ in $\mathbf{F}_p[X]$. Il contenuto di un polinomio. La $p$-proiezione di $A[X]$. Il lemma di Gauss sul prodotto di polinomi primitivi. Ideali del prodotto diretto di anelli, il teorema cinese dei resti in anelli commutativi unitari. Esempi di domini non a fattorizzazione unica; esempi di domini senza il MCD. Fattorizzazione negli anelli di polinomi. $A[X]$ è fattoriale se $A$ è fattoriale. Criteri di irriducipilità di Eisenstein. Irriducibilità degli anelli di polinomi.

**3. Teoria della Cardinalità** Enunciati dei Teoremi di Cantor-Bernstein e di Hertogs. Cardinalità del numerabile, cardinalità del continuo, Metodo diagonale di Cantor, proprietà fondamentali.

**4. Teoria dei Campi** Caratteristica di un campo, Teorema dei gradi, Costruzione dei campi mediante i quozienti negli anelli di polinomi, radici di polinomi, esistenza del campo di spezzamento (solo enunciato).

# Testi consigliati

[1] D. Dikranjan - M.S. Lucido, *Aritmetica e algebra*. Liguori (2007).

# Bibliografia supplementare

[2] G.M. Piacentini Cattaneo, *Algebra, un approccio algoritmico*. Decibel – Zanichelli (1996).
[3] I. N. Herstein, *Algebra*. Editori Riuniti (2003).
[4] M. Artin, *Algebra*. Bollati Boringhieri (1997).

# Modalità d'esame

| | | | |
|---|---|---|---|
| - valutazione in itinere ("esoneri") | | ■ SI | □ NO |
| - esame finale | scritto | ■ SI | □ NO |
| | orale | ■ SI | □ NO |
| - altre prove di valutazione del profitto (meglio descritte sotto) | | □ SI | ■ NO |