Algebra 1 – Matematica – A.A. 2023-24, corso annuale
Docenti: Alberto De Sole & Daniele Valeri

Diario delle lezioni

MODULO 1

Settimana 1. (*Lettura: Artin Sez. 2.1, 2.2, 2.3, 2.4*)

(26/9)-2h Presentazione del corso. Definizione di gruppo. Esempi di gruppi.
(28/9)-3h Alcune proprietà dei gruppi: l'unità di un gruppo G è unica; l'elemento inverso di $a \in G$ è unico; legge di cancellazione in un gruppo. Sottogruppi: definizione ed esempi. Classificazione dei sottogruppi del gruppo additivo $\mathbb{Z}$. Omomorfismo di gruppi: definizione ed esempi.

Settimana 2. (*Lettura: Artin Sez. 2.5, 2.6, 2.7*)

(3/10)-2h Esempio: massimo comun divisore. Sottogruppo ciclico generato da un elemento. Ordine di un gruppo e di un elemento. Nucleo ed immagine di un omomorfismo.
(5/10)-2h Classi laterali destre e sinistre di un sottogruppo. Sottogruppi normali e gruppo quoziente.

Settimana 3. (*Lettura: Artin Sez. 2.6, 2.7, 2.10*)

(10/10)-2h Teorema di Lagrange e applicazioni. L'unico gruppo di ordine primo p è il gruppo ciclico C_p. Gruppo quoziente. Primo Teorema di Isomorfismo: $G/\ker\varphi \simeq \operatorname{Im}\varphi$. Applicazioni ed esempi.
(12/10)-2h Secondo Teorema di Isomorfismo: dato un gruppo G ed un sottogruppo normale $N \subset G$, c'è una corrispondenza biunivoca tra l'insieme dei sottogruppi $H \subset G$ contenenti N e l'insieme dei sottogruppi $\bar{H} \subset G/N$; tale corrispondenza restringe ad una corrispondenza biunivoca tra i corrispondenti sottogruppi normali; dato un sottogruppo normale $L \subset G$ contenente N ed il corrispondente sottogruppo normale $\bar{L} \subset G/N$, c'è un isomorfismo canonico $(G/N)/\bar{L} \simeq G/L$. Esempi.

Settimana 4. (*Lettura: Artin Sez. 2.4, 2.8*)

(17/10)-2h Dati sottogruppi $H, K \subset G$, il prodotto $HK \subset G$ è sottogruppo se e solo se $HK = KH$. Teorema: $|HK| = |H||K|/|H \cap K|$. Gruppo $\operatorname{Aut}(G)$ degli automorfismi di un gruppo G e sottogruppo normale degli automorfismi interni. Omomorfismo $\operatorname{Ad} : G \to \operatorname{Aut}(G)$ dato dal coniugio. Prodotto diretto di gruppi.
(19/10)-2h Prodotto diretto e prodotto semidiretto tra gruppi. Teorema: (a) Se $H, K \subset G$ sono sottogruppi normali, $H \cap K = \{e\}$ e $HK = G$, allora $G \simeq H \times K$. (b) Se $H, K \subset G$ sono sottogruppi e H è normale, $H \cap K = \{e\}$ e $HK = G$, allora $G \simeq H \rtimes_\varphi K$, con $\varphi : K \to \operatorname{Aut}(H)$ data dal coniugio.

Settimana 5. (*Lettura: Artin Sez. 2.3, 2.8, 2.9*)

(24/10)-2h Applicazioni del prodotto diretto e semidiretto. Esempio: $\operatorname{Aut}(C_n) \simeq C_n^*$. Prodotti semidiretti della forma $C_n \rtimes_\varphi C_2$. Esempio: $C_8 \rtimes_\varphi C_2$.
(26/10)-2h Divisione euclidea in $\mathbb{Z}$. Divisibilità in $\mathbb{Z}$. MCD, identità di Bezout e algoritmo euclideo. Relazione di congruenza modulo n. Elementi invertibili in $\mathbb{Z}/n\mathbb{Z}$. MCD e mcm. Teorema cinese dei resti: se $MCD(m, n) = 1$, allora per ogni $a, b \in \mathbb{Z}$ esiste (unico mod mn) $x \in \mathbb{Z}$ tale che $x \equiv a\,(m), x \equiv b\,(n)$. Piccolo Teorema di Fermat: $a^p \equiv a\,(p)$.

Settimana 6. (*Lettura: Artin Sez. 2.9, 5.1, 5.2, 5.3*)

(31/10)-2h Funzione di Eulero $\varphi(n)$. Teorema di Eulero: se $\mathrm{MCD}(a,n)=1$, allora $a^{\varphi(n)} \equiv 1\,(n)$. Numeri primi. Teorema fondamentale dell'aritmetica: per ogni $n \in \mathbb{Z}$ esiste ed è unica la fattorizzazione in fattori primi. Teorema: esistono infiniti primi $p \in \mathbb{Z}$. Teorema di Wilson: p è primo se e solo se $(p-1)! \equiv -1\,(p)$.
(02/11)-2h Gruppi di simmetria: di una figura piana; di un'insieme con una struttura algebrica. Gruppo C_n come il gruppo delle simmetrie di rotazione dell'n-gono regolare; gruppo D_n come gruppo delle simmetrie dell'n-gono regolare. Gruppo $\mathcal{M}_n$ dello spazio affine $\mathbb{A}^n$ come prodotto semidiretto $\mathcal{M}_n \simeq \mathcal{T}_n \rtimes_\varphi O_n$ del gruppo delle traslazioni $\mathcal{T}_n$ e del gruppo ortogonale O_n.

Settimana 7. (*Lettura: Artin Sez. 5.3, 5.5, 5.6, 5.7, 5.8, 5.9*)

(07/11)-2h Sottogruppi finiti del gruppo $\mathcal{M}_2$ dei movimenti rigidi del piano. Azione di un gruppo G su un insieme S. Esempio: (1) azione di $\mathcal{M}_2$ sull'insieme $\mathcal{P}(\mathbb{A}^2)$ delle figure piane.
(09/11)-2h Esempi: (2) azione di S_n su $\{1,2,\dots,n\}$; (3) azione di G su G per moltiplicazione a sinistra o destra; (3) azione di G su G/H per moltiplicazione a sinistra e su $H\backslash G$ per moltiplicazione a destra; (4) azione di G su G per coniugio. Orbita $\mathcal{O}_s = G\cdot s \subset S$ di un'azione del gruppo G sull'insieme S. Stabilizzatore $G_s = \{g \in G \,|\, g\cdot s = s\} \subset G$ di un'azione del gruppo G sull'insieme S.

Settimana 8. (*Lettura: Artin Sez. 4.5, 5.7, 5.8, 5.9, 6.1, 6.6*)

(14/11)-2h Prima formula del conteggio: $|S| = \sum |\mathcal{O}_s|$. Seconda formula del conteggio: $|G| = |G_s||\mathcal{O}_s|$. Classe di coniugio $Cl(x)$ e centralizzatore $C(x)$ di un elemento $x \in G$. Equazione delle classi di un gruppo G.
(16/11)-3h Notazione in cicli per il gruppo delle permutazioni. Teorema: ogni permutazione $\sigma \in S_n$ è prodotto di cicli disgiunti. Trasposizioni. Teorema: il gruppo S_n è generato da trasposizioni. Permutazioni pari e dispari. Teorema: la parità di una permutazione è ben definita. Solidi platonici. Classificazione dei sottogruppi finiti di SO_3.

Settimana 9. (*Lettura: Artin Sez. 6.2, 6.6*)

(21/11)-2h Classi di coniugio di S_n. Gruppo delle simmetrie di rotazione del dodecaedro.
(23/11)-2h Classi di coniugio di A_n. Un gruppo G di ordine p^n, con p primo, ha centro $Z(G)$ non banale. Classificazione dei gruppi di ordine p^2.

Settimana 10. (*Lettura: Artin Sez. 6.1, 6.4, 6.5*)

(28/11)-2h Definizione: se $|G| = p^e m$, con $e \geq 1$ e $p \not| m$, un p-Sylow in G è un sottogruppo $H \subset G$ tale che $|H| = p^e$. Primo Teorema di Sylow: se $p \big| |G|$, esiste un p-Sylow in G.
(30/11)-2h Secondo Teorema di Sylow: se $H \subset G$ è un p-Sylow e $K \subset G$ è un sottogruppo tale che $p \big| |K|$, allora esiste un p-Sylow di K della forma $K \cap gHg^{-1}$. Corollario: i p-Sylow in G sono tutti coniugati.

Settimana 11. (*Lettura: Artin Sez. 6.4, 6.5, 10.1, 10.2, 10.3, 10.4*)

(05/12)-2h Terzo Teorema di Sylow: il numero n_p di p-Sylow in G è tale che $n_p | m$ e $n_p \equiv 1$ mod p. Applicazione: classificazione dei gruppi di ordine 15, 21 e 12.
(07/12)-2h Definizione ed esempi di anelli. Esempi di anelli associativi e non, commutativi e non, con o senza unità, domini, campi. Prime proprietà. Caratteristica di un anello. Omomorfismi tra anelli. Nucleo e immagine. Ideali destri, sinistri e bilateri. Ideali principali. Anello quoziente A/I e mappa quoziente $\pi : A \to A/I$.

Settimana 12. (*Lettura: Artin Sez. 10.4, 10.6, 10.7*)

(12/12)-2h Primo teorema di isomorfismo: dato un omomorfismo di anelli $\phi : A \to B$, esiste un isomorfismo canonico $\bar{\phi} : A/\operatorname{Ker}(\phi) \simeq \operatorname{Im}(\phi)$. Teorema di corrispondenza degli ideali: dato un anello A ed un ideale $I \subset A$, esiste una corrispondenza biunivoca

$$\{\text{ideali } J \text{ di } A \text{ contenenti } I\} \xrightarrow{\sim} \{\text{ideali } \bar{J} \text{ di } A/I\}.$$

Secondo teorema di isomorfismo: $(A/I)/\bar{J} \simeq A/J$.
(14/12)-2h Costruzioni di nuovi anelli aggiungendo elementi ed imponendo relazioni: $A \to A[x]/(f(x))$. Esempi ed applicazioni. Campo dei quozienti $Q = Frac(D)$ di un dominio D. Costruzione e proprietà universale.

Settimana 13. (*Lettura: Artin Sez. 10.4, 10.5, 11.1, 11.2*)

(19/12)-2h Ideali primi $P \subset A$ e ideali massimali $\mathfrak{m} \subset A$. Lemma: (a) $P \subset A$ è primo se e solo se A/P è un dominio. (b) $\mathfrak{m} \subset A$ è massimale se e solo se $A/\mathfrak{m}$ è un campo. Teorema: se A è un anello con unità, dato un ideale $I \subsetneq A$, esiste un ideale massimale t.c. $I \subset \mathfrak{m} \subsetneq A$ (usando il Lemma di Zorn).
(21/12)-2h Domini euclidei (ED): definizione ed esempi. Anello degli interi di Gauss $\mathbb{Z}[i]$, come esempio di dominio euclideo. Domini a ideali principali (PID): definizione ed esempi. Proposizione: un dominio euclideo è ad ideali principali (ED $\Rightarrow$ PID). In un PID: divisibilità, MCD, Lemma di Bezout, elementi primi ed irriducibili. Esempio di dominio con elementi irriducibili non primi: $\mathbb{Z}[\sqrt{-5}]$.

Settimana 14.

(09/01)-2h Ripasso.
(11/01)-3h Esonero.

MODULO 2

Settimana 1. (*Lettura: Artin Sez. 11.3, 11.4, 11.5*)

(4/3)-3h Ripasso. Domini a fattorizzazione unica (UFD): definizione ed esempi. Teorema: in un PID esiste ed è unica la fattorizzazione in primi (PID $\Rightarrow$ UFD). Esistenza: un PID soddisfa la condizione della catena ascendente (ACC). Unicità: in un PID vale che p è primo se e solo se è irriducibile. Ideali primi e massimali in $\mathbb{C}[x]$, $\mathbb{R}[x]$.
(5/3)-2h *(Canale L-Z lezione cancellata)* Esempio di dominio che non soddisfa ACC: $\mathbb{Z}+x\mathbb{Q}[x]$. Contenuto e elemento primitivo associato di un polinomio $f(x)$ a coefficienti in un UFD Z. Lemma di Gauss. Teorema: se Z è un UFD, allora $Z[x]$ è un UFD.

Settimana 2. (*Lettura: Artin Sez. 11.3, 11.4, 11.5, 12.5*)

(11/3)-3h Criteri di irriducibilità in $\mathbb{Q}[x]$ e $\mathbb{Z}[x]$: polinomi di grado ≤ 3; riduzione modulo p; criterio di Eisenstein. Polinomi ciclotomici.
(12/3)-2h *(Canale L-Z lezione cancellata)* Fattorizzazione in $\mathbb{Z}[i]$: primi di Gauss e teorema dei due quadrati. Anelli Noetheriani: definizione ed esempi. Un quoziente di un anello Noetheriano è Noetheriano.

Settimana 3. (*Lettura: Artin Sez. 11.3, 11.4, 11.5, 12.5*)

(18/3)-3h Teorema della base di Hilbert: se A è Noetheriano, allora $A[x]$ è Noetheriano. L'anello delle serie formali $\mathbb{F}[[x]]$: esempio di anello locale. Correzione esercizi.
(19/3)-2h *(Canale A-K lezione cancellata)* Riassunto delle principali famiglie di anelli, con vari esempi e controesempi: anelli commutativi con unità, domini, PID, ED, UFD, anelli Noetheriani.

Settimana 4. (*Lettura: Artin Sez. 12.1, 12.2, 12.3, 12.4*)

(25/3)-3h Definizione di modulo su un anello, esempi. Definizioni categorighe: sottomodulo, omomorfismo, nucleo e immagine, modulo quoziente. Teoremi di isomorfismo. Vettori linearmente indipendenti, generatori, base di un modulo. Moduli liberi.
(26/3)-2h Esempio: su un anello non commutativo il rango non e' unicamente definito. Teorema: il rango di un modulo libero (su un anello commutativo con unità) è ben definito. Teorema di Binet. Richiami di algebra lineare: eliminazione di Gauss; teorema del rango.

Settimana 5. (*Lettura: Artin Sez. 12.1, 12.2, 12.3, 12.4*)

(25/3)-3h Definizione di modulo su un anello, esempi. Definizioni categorighe: sottomodulo, omomorfismo, nucleo e immagine, modulo quoziente. Teoremi di isomorfismo. Vettori linearmente indipendenti, generatori, base di un modulo. Moduli liberi.
(26/3)-2h Esempio: su un anello non commutativo il rango non è unicamente definito. Teorema: il rango di un modulo libero (su un anello commutativo con unità) è ben definito. Teorema di Binet. Richiami di algebra lineare: eliminazione di Gauss; teorema del rango.

Settimana 6. (*Lettura: Artin Sez. 12.4, 12.5, 12.6*)

(8/4)-3h Eliminazione di Gauss su un dominio Euclideo Z. Formulazioni equivalenti: orbite dell'azione di $GL_m(Z) \times GL_n(Z)$ su $Mat_{m \times n}(Z)$; classificazione degli omomorfismi di moduli tra moduli liberi di rango finito. Enunciato del Teorema di struttura dei moduli finitamente generati su ED. Per $Z = \mathbb{Z}$: classificazione dei gruppi abeliani finiti.
(9/4)-2h Teorema: per un anello Noetheriano, un sottomodulo di un modulo finitamente generato è finitamente generato. Sottomoduli di un modulo libero su un dominio Euclideo. Dimostrazione del Teorema di struttura dei moduli finitamente generati su un dominio Euclideo.

Settimana 7. (*Lettura: Artin Sez. 12.7, 12.8*)

(15/4)-3h Applicazioni del teorema di struttura dei moduli finitamente generati su un dominio euclideo. Classificazione dei gruppi abeliani finiti. Teorema di Jordan. Applicazioni ed esercizi sul Teorema di Jordan. Teorema di Cayley-Hamilton. Polinomio caratteristico e polinomio minimo di un endomorfismo.
(16/4)-2h