Algebra 1 – Matematica – A.A. 2022-23, corso annuale
Docente: Alberto De Sole

Diario delle lezioni

MODULO 1

Settimana 1. (*Lettura: note di D'Andrea*)

(27/9)-3h Presentazione del corso. Teoria della cardinalità. Cardinalità di un insieme: definizione di $|A| \leq |B|$, $|A| \geq |B|$, $|A| = |B|$. Insiemi numerabili ed insiemi non numerabili. Teorema: $|\mathcal{P}(S)| > |S|$. Ipotesi del continuo. Esercizio: $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$.

Settimana 2. (*Lettura: note di D'Andrea*)

(3/10)-2h Enunciato di: Assioma della Scelta (AS); Lemma di Zorn (LZ); Principio del Buon Ordinamento (BO). Relazioni d'ordine parziale e totale; buon ordinamento. Definizioni di: massimo, minimo, elemento massimale, elemento minimale, maggiorante, minorante. Applicazione del LZ: ogni spazio vettoriale ammette una base.
(4/10)-3h Dimostrazione di: BO $\Rightarrow$ AS. Dimostrazione di LZ $\Rightarrow$ BO. Dimostrazione di: AS $\Rightarrow$ LZ. Per assurdo: fissiamo una funzione di scelta f su S e supponiamo che S soddisfi le ipotesi del LZ e non abbia elementi massimali. Definizione di segmento iniziale: $I \subset A$, I " $\leq$ " $(A \backslash I)$. Lemma 1: se I, J sono segmenti iniziali di A, allora I è segmento iniziale di J o viceversa. Lemma 2: un'unione arbitraria di segmenti iniziali di A è un segmento iniziale di A. Definizione di insieme dei maggioranti $\text{Magg}(C)$ di un sottoinsieme $C \subset S$ totalmente ordinato. Lemma 3: $\text{Magg}(C) \neq \emptyset$ (usando l'ipotesi assurda).

Settimana 3. (*Lettura: note di G. Bergman*)

(10/10)-2h Definizione di insieme induttivo $A \subset S$: (i) A è ben ordinato; (ii) $\min(A) = f(S)$; (iii) per ogni segmento iniziale I di A vale $f(\text{Magg}(I)) = \min(A \backslash I)$. Lemma 4: se A è induttivo, allora $A \cup \{f(\text{Magg}(A))\}$ è induttivo. Lemma 5: se A è induttivo e I è segmento iniziale di A, allora I è induttivo. Lemma 6: se A e B sono induttivi, allora A è segmento iniziale di B o viceversa. Lemma 7: l'unione di tutti gli insiemi induttivi è un insieme induttivo. Conclusione della dimostrazione che AS $\Rightarrow$ LZ.
(11/10)-3h Teorema: (1) $|A| \leq |B|$ se e solo se $|B| \geq |A|$. (2) $|A| \leq |B|$, $|B| \leq |C| \Rightarrow |A| \leq |C|$. (3) dati A e B, vale $|A| \leq |B|$ o viceversa, (4) $|A| \leq |B|$, $|B| \leq |A| \Rightarrow |A| \leq |B|$ (Teo di Schroeder-Bernstein).

Esempi e esercizi in teoria della cardinalità. (1) Se A è numerabile e $I \subset A$ è infinito, allora I è numerabile. (2) Se A è infinito, allora esiste $I \subset A$ numerabile (usando AS). (3) Se A è numerabile, allora $A \times A$ è numerabile (e $A \times \cdots \times A$ è numerabile). (4) Se A_1, A_2, $A_3, \ldots$ è una successione di insiemi numerabili, allora $\bigcup_{i=1}^{\infty} A_i$ è numerabile. (5) Se A è un insieme infinito, esiste un ricoprimento disgiunto $\{C_\alpha\}_{\alpha \in I}$ di A costituito da insiemi numerabili (usando LZ). (6) Se A è infinito e B è numerabile o finito, allora $|A \times B| = |A|$. (7) Se $|A| \leq |B|$ e B è infinito, allora $|A \cup B| = |B|$. (8) Se A è infinito, allora $|A \times A| = |A|$ (usando LZ).

Settimana 4. (*Lettura: Herstein Cap 1, Artin Sez 2.9*)

(17/10)-2h Divisione euclidea in $\mathbb{Z}$. Divisibilità in $\mathbb{Z}$. MCD, identità di Bezout e algoritmo euclideo. Numeri primi. Teorema fondamentale dell'aritmetica: per ogni $n \in \mathbb{Z}$ esiste ed è unica la fattorizzazione in fattori primi. Relazione di congruenza modulo n
(18/10)-3h Anello $\mathbb{Z}/n\mathbb{Z}$. Elementi invertibili in $\mathbb{Z}/n\mathbb{Z}$. Proposizione: $\mathbb{Z}/n\mathbb{Z}$ è un campo se e solo se n è primo. MCD e mcm. Piccolo Teorema di Fermat: $a^p \equiv a\,(p)$. 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 $x \equiv a\,(m), x \equiv b\,(n)$.

Settimana 5. (*Lettura: Herstein Sez 2.1, 2.2, 2.3, Artin Sez 2.1*)

(24/10)-2h Teorema di Eulero: se $\mathrm{MCD}(m,a)=1$, allora $a^{\varphi(n)} \equiv 1\,(n)$. Funzione di Eulero $\varphi(n)$. Teorema di Wilson: p è primo se e solo se $(p-1)! \equiv -1\,(p)$. Teorema: esistono infiniti primi $p \in \mathbb{Z}$.
(25/10)-3h Definizione di gruppo. Esempi di gruppi. Gruppo delle permutazioni $\mathrm{Perm}(S)$ e gruppo simmetrico S_n. Tavola motiplicativa del gruppo S_3. Presentazione di S_3 con generatori e relazioni. Lemma 1: l'unità di un gruppo G è unica. Lemma 2: l'elemento inverso di $a \in G$ è unico. Legge di cancellazione in un gruppo.

Criteri di divisibilità per 2, 3, 5, 7, 11 in $\mathbb{Z}$.

Settimana 6. (*Lettura: Herstein Sez 2.4, 2.5, Artin Sez 2.2, 2.5, 2.6, 2.10*)

(7/11)-2h Sottogruppi: definizione ed esempi. Classificazione dei sottogruppi del gruppo additivo $\mathbb{Z}$. Sottogruppo ciclico generato da un elemento.
(8/11)-3h Ordine di un gruppo e di un elemento. Omomorfismo di gruppi: definizione ed esempi. Nucleo ed immagine di un sottogruppo. Classi laterali destre e sinistre di un sottogruppo. Sottogruppi normali e gruppo quoziente. Correzione di esercizi.

Settimana 7. (*Lettura: Herstein 2.6, 2.7, Artin Sez 2.3, 2.4, 2.7*)

(14/11)-2h Teorema di Lagrange e applicazioni. Teorema di isomorfismo: $G/\ker\varphi \simeq \mathrm{Im}\,\varphi$. Applicazioni ed esempi. L'unico gruppo di ordine primo p è il gruppo ciclico C_p.
(15/11)-3h Dati sottogruppi $H, K \subset G$, il prodotto $HK \subset G$ è sottogruppo se e solo se $HK = KH$. Teorema: $|HK| = |H||K|/|H \cap K|$. 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 $(G/N)/\bar{L} \simeq G/L$. Correzione degli esercizi.

Settimana 8. (*Lettura: Herstein Sez 2.8, 2.13, Artin Sez 2.8*)

(21/11)-2h Gruppo $\mathrm{Aut}(G)$ degli automorfismi di un gruppo G e sottogruppo normale degli automorfismi interni. Omomorfismo $\mathrm{Ad} : G \to \mathrm{Aut}(G)$ data dal coniugio. Esempio: $\mathrm{Aut}(C_n) \simeq C_n^*$. 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 $\varphi : K \to \mathrm{Aut}(H)$ data dal coniugio.
(22/11)-3h Correzione degli esercizi (a cura del Prof. Daniele Valeri).

Settimana 9. (*Lettura: Herstein Sez 2.9, Artin Sez 5.1, 5.2, 5.5, 5.6*)

(28/11)-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 $\mathcal{M}_n \simeq \mathcal{T}_n \rtimes O_n$ del gruppo delle traslazioni $\mathcal{T}_n$ e del gruppo ortogonale O_n. Teorema di Cayley: un gruppo G finito è isomorfo ad un sottogruppo di S_n.
(29/11)-3h Omomorfismo $G \to \mathrm{Perm}(G/H)$; il nucleo è il più grande sottogruppo di H normale in G. Applicazione: non esistono gruppi semplici di ordine 36. Classificazione dei gruppi G di ordine 6: G è isomorfo a C_6 o a S_3. Correzione di esercizi.

Settimana 10. (*Lettura: Herstein Sez 2.10, 2.11, Artin Sez 5.6, 5.7, 6.1, 6.2, 6.6*)

(5/12)-2h 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.
(6/12)-3h Azione di un gruppo G su un insieme S. Esempi: (1) azione di $\mathcal{M}_2$ sull'insieme $\mathcal{P}(\mathbb{A}^2)$ delle figure piane; (2) azione di S_n su $\{1, 2, \ldots, n\}$; (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 $G_s = \{g \in G \,|\, g \cdot s = g\} \subset G$ di un'azione del gruppo G sull'insieme S. 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. Applicazione: un gruppo G di ordine p^n, con p primo, ha centro $Z(G)$ non banale.

Settimana 11. (*Lettura: Herstein Sez 2.12, 2.14, Artin Sez 6.3*)

(12/12)-2h Definizione: se $|G| = p^e m$, con $e \geq 1$ e $p \nmid m$, 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.
(13/12)-3h 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. Terzo Teorema di Sylow: il numero n_p di p-Sylow in G è tale che $n_p | m$ e $n_p \equiv 1 \bmod p$. Applicazione: classificazione dei gruppi di ordine 15 e 21.

Settimana 12. (*Lettura: Artin Sez 5.9*)

(19/12)-2h Solidi platonici. Classificazione dei sottogruppi finiti di SO_3.
(20/12)-3h Correzione esercizi. Classi di coniugio di S_n e A_n. Classificazione dei gruppi di ordine 18.

MODULO 2

Settimana 1. (*Lettura: Herstein Sez 3.1 – 3.4, Artin Sez 10.1 – 10.3*)

(28/2)-3h 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.
(3/3)-2h 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 2. (*Lettura: Herstein Sez 3.5, 3.6, Artin Sez 10.4, 10.6*)

(7/3)-3h 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: $(A/I)/\bar{J} \simeq A/J$. 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 domonio. (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).
(10/3)-2h Campo dei quozienti $Q = \operatorname{Frac}(D)$ di un dominio D. Costruzione e proprietà universale.

Settimana 3. (*Lettura: Herstein Sez 3.7 – 3.9, Artin Sez 10.4, 10.5, 11.1, 11.2*)

(14/3)-3h Domini euclidei: 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. Teorema: in un PID esiste ed è unica la fattorizzazione in primi (PID $\Rightarrow$ UFD). Esistenza: proprietà di Noetherianità di un PID. Unicità: in un PID vale che p è primo se e solo se è irriducibile. Esempio di dominio NON Noetheriano: $\mathbb{K}[x_1, x_2, x_3, \dots]$. Esempio di dominio con elementi irriducibili non primi: $\mathbb{Z}[\sqrt{-5}]$. Anello degli interi di Gauss $\mathbb{Z}[i]$, come esempio di dominio euclideo.
(17/3)-2h Riassunto delle principali famiglie di anelli, con vari esempi e controesempi: anelli commutativi con unità, domini, PID, ED, UFD, anelli Noetheriani. Costruzioni di nuovi anelli aggiungendo elementi ed imponendo relazioni: $A \to A[x]/(f(x))$. Esempi ed applicazioni.

Settimana 4. (*Lettura: Artin Sez. 12.5, 11.3, 11.4*)

(21/3)-3h Anelli Noetheriani. Un quoziente di un anello Noetheriano è Noetheriano. Teorema della base di Hilbert: se A è Noetheriano, allora $A[x]$ è Noetheriano. Correzione esercizi.
(24/3)-2h 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 5. (*Lettura: Artin Sez. 11.5*)

(28/3)-3h Ideali primi e massimali in $\mathbb{C}[x]$, $\mathbb{R}[x]$. Criteri di irriducibilità in $\mathbb{Q}[x]$ e $\mathbb{Z}[x]$: polinomi di grado ≤ 3; riduzione modulo p. Correzione esercizi.
(31/3)-2h Criterio di Eisenstein. Polinomi ciclotomici. L'anello delle serie formali $\mathbb{K}[[x]]$: esempio di anello locale. Fattorizzazione in $\mathbb{Z}[i]$.

Settimana 6. (*Lettura: Artin Sez. 11.5, 12.1*)

(4/4)-3h Primi di Gauss. Teorema dei due quadrati. Correzione esercizi.
(7/4)-(11/4) *VACANZE PASQUALI*
(14/4)-2h Definizione di modulo su un anello, esempi. Definizioni categorighe: sottomodulo, omomorfismo, nucleo e immagine, modulo quoziente.

Settimana 7. (*Lettura: Artin Sez. 12.2, 12.3, 12.4*)

(18/4)-3h Teoremi di isomorfismo. Vettori linearmente indipendenti, generatori, base di un modulo. Moduli liberi. 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.
(21/4)-2h Eliminazione di Gauss su un dominio Euclideo Z. Formulazioni equivalenti: orbite dell'azione di $GL_m(Z) \times GL_m(Z)$ 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.

Settimana 8. (*Lettura: Artin 12.5, 12.6*)

(25/4) *FESTA DELLA LIBERAZIONE*
(28/4)-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 9. (*Lettura: Artin 12.7, 12.8*)

(2/5)-3h Applicazioni del teorema di struttura dei moduli finitamente generati su un dominio euclideo. Classificazione dei gruppi abeliani finiti. Teorema di Jordan.
(5/5)-2h Applicazioni ed esercizi sul Teorema di Jordan. Teorema di Cayley-Hamilton. Polinomio caratteristico e polinomio minimo di un endomorfismo.

Settimana 10. (*Lettura: Artin 13.1, 13.2, 13.3*)

(9/5)-3h Campi: definizioni ed esempi. Estensioni di campi. Grado di un'estensione. Elementi algebrici e trascendenti. Polinomio irriducibile di un elemento algebrico. Proposizione: esiste un isomorfismo $\mathbb{F}[\alpha] \to \mathbb{F}[\beta]$ se e solo se α e β hanno lo stesso polinomio irriducibile su $\mathbb{F}$.
(12/5) *LEZIONE CANCELLATA*

Settimana 11. (*Lettura: Artin 13.4, 13.5*)

(16/5)-3h Cosrtuzioni con riga e compasso. Campo dei numeri costruibili.
(19/5)-2h Teorema: un numero a è costruibile se e solo se esiste una catena di estensioni di grado due $\mathbb{Q} = \mathbb{F}_0 \subset \mathbb{F}_1 \subset \cdots \subset \mathbb{F}_n$ tale che $a \in \mathbb{F}_n$. Applicazione alla costruibilità di alcune figure geometriche.

Settimana 12. (*Lettura: Artin 13.6*)

(23/5) *LEZIONE CANCELLATA*
(26/5)-2h Campi in caratteristica p e campi finiti. Teorema di classificazione e struttura dei campi finiti.

Settimana 13. (*Lettura: Artin 13.9*)

(30/5)-3h Fine della dimostrazione deil Teorema di classificazione e struttura dei campi finiti. Campi algebricamente chiusi e chiusura algebrica di un cmapo. Teorema di esistenza ed unicità della chiusura algebrica.
(2/6) *FESTA DELLA REPUBBLICA*

Settimana 14. (*Lettura:*)

(6/6)-3h Ripasso ed esercizi.
(9/6)-2h SECONDO ESONERO