PROGRAMMA DI ALGEBRA 2 PRIMA PARTE
Corso di Laurea in Matematica A.A. 2025-2026, primo semestre 6 CFU
Docente: Andrea Loi

1. Semigruppi, monoidi e gruppi. Semigruppi; esempi di semigruppi; legge di cancellazione in un semigruppo; elementi idempotenti in un semigruppo; in un semigruppo finito esiste almeno un elemento idempotente; monoidi (semigruppi con elemento neutro); esempi di monoidi; un elemento idempotente in un monoide dove vale la legge di cancellazione a sinistra (o a destra) è l'elementto neutro; un elemento idempotente in un semigruppo dove vale la legge di cancellazione è l'elemento neutro; definizione di elemento invertibile in un monoide; unicitá dell'inverso; definizione di gruppo: monoide dove tutti gli elementi sono invertibili; un semigruppo con elemento neutro a destra (risp. sinistra) e inverso a destra (risp. sinistra) è un gruppo; alcuni esempi di gruppi: gli esempi numerici; il cerchio unitario come gruppo; il gruppo lineare $\mathrm{GL}_n(\mathbb{K})$ su un campo $\mathbb{K}$; gli elementi invertibili $U(M)$ di un monoide formano un gruppo; legge di cancellazione in un gruppo; un monoide finito dove vale la legge di cancellazione a destra (oppure a sinistra) è un gruppo; un semigruppo finito dove vale la legge di cancellazione è un gruppo; proprietà elementari dei gruppi: inverso del prodotto; proprietà delle potenze in un gruppo; confronto tra la notazione additiva e moltiplicativa; elementi permutabili in un gruppo e commutatore tra due elementi; ordine di un elemento e le sue proprietà.

2. Due gruppi importanti. Il gruppo diedrale D_n, $n \geq 3$, delle isometrie del piano che fissano un poligono regolare di n-lati; esempi nel caso $n = 3$ e $n = 4$; le permutazioni come gruppo; prodotto di permutazioni finite; supporto di una permutazione; permutazioni disgiunte; due permutazioni disgiunte commutano; cicli; ordine, supporto e inverso di un ciclo; potenze di un ciclo; il teorema fondamentale delle permutazioni: ogni permutazione f non identica con supporto finito può scriversi in modo unico (a meno dell'ordine) come prodotto di cicli disgiunti $f = \sigma_1 \cdots \sigma_t$ e l'ordine di f è uguale al minimo comune multiplo della lunghezza dei cicli σ_j; una permutazione ha ordine un primo p se e solo se si può scrivere come prodotto di cicli tutti di lunghezza p; definizione di $N(f)$; segno di una permutazione $sgn(f) = (-1)^{N(f)}$; permutazioni di classe pari e dispari; ogni permutazione f si può scrivere come prodotto di $N(f)$ trasposizioni; il sgn è una funzione moltiplicativa $sgn(f \circ g) = sgn(f)sgn(g)$; una permutazione è di classe pari se e solo se si può scrivere come prodotto di un numero pari di trasposizioni.

3. Sottogruppi e classi laterali. Sottogruppi: stabilità e inverso; esempi di sottogruppi; se un insieme finito A di un gruppo G è stabile allora A è un sottogruppo di G; il gruppo alterno A_n; criterio per riconoscere un sottogruppo (un sottoinsieme non vuoto H di un gruppo G è un sottogruppo se e solo se $x^{-1}y \in H$ per ogni $x, y \in H$); l'intersezione di una famiglia qualsiasi di sottogruppi è un sottogruppo; sottogruppo $< X >$ di un gruppo G generato da un sottoinsieme $X \subseteq G$; sottogruppo $< x >$ generato da un elemento; gruppi ciclici; i sottogruppi di $\mathbb{Z}$ sono tutti ciclici e della forma $m\mathbb{Z}$, $m \in \mathbb{N}$; se G è un gruppo e x un suo elemento allora $| < x > | = o(x)$; siano H e K sottogruppi di un gruppo G allora $H \cup K$ è un sottogruppo di G se solo se $H \subseteq K$ oppure $K \subseteq H$; un gruppo G non può essere unione di due suoi sottogruppi propri; l'unione di una catena di sottogruppi è ancora un sottogruppo; sottogruppo $\langle H, K\rangle =< H \cup K >$ generato da due sottogruppi $H, K \subseteq G$; prodotto HK di due sottogruppi H e K di un gruppo G; siano H e K sottogruppi di un gruppo G allora $HK = KH$ (ossia H e K

sono permutabili) se e solo se $\langle H, K\rangle = HK$; $|HK| = \frac{|H||K|}{|H\cap K|}$; se $H = m\mathbb{Z}$ e $K = n\mathbb{Z}$ sono sottogruppi $(\mathbb{Z}, +)$ allora $H + K = (m, n)\mathbb{Z}$ e $H \cap K = [m, n]\mathbb{Z}$; classi laterali di un sottogruppo; sia G un gruppo e H un suo sottogruppo allora ogni classe laterale (sinistra o destra) di H in G ha la stessa cardinalità di H; sia G un gruppo e H un suo sottogruppo allora la cardinalità delle classi laterali sinistre di H in G coincide con la cardinalità delle classi laterali destre di H in G; $[G : H]$ indice di H in G; teorema di Lagrange (sia G un gruppo finito e H un suo sottogruppo allora $|G| = [G : H]|H|$); sia G un gruppo finito e x un elemento di G allora $o(x)$ divide $|G|$ e $x^{|G|} = 1$; in un gruppo finito G di ordine p primo gli unici sottogruppi sono quelli banali, G è ciclico e tutti gli elementi non nulli di G hanno ordine p e generano G; dimostrazione del il piccolo teorema di Fermat usando la teoria dei gruppi: ordine del prodotto di due elementi: se due elementi di un gruppo commutano e hanno ordini coprimi allora l'ordine del loro prodotto é uguale al prodotto dei loro ordini.

4. Sottogruppi normali e quozienti Definizione di sottogruppo normale di un gruppo G: N è un sottoguppo normale di G ($N \trianglelefteq G$) se le classi laterali sinistre e destre coincidono xN e Nx coincidono per ogni $x \in G$; criteri per la normalità di un sottogruppo:N sottogruppo di G è normale se e solo se il coniugato di ogni elemento di N appartiene a N; il coniugato di un sottogruppo $H^x = x^{-1}Hx$; condizione di normalità ($H \trianglelefteq G$ se e solo se $H^x \leq H$ se e solo se $H^x = H$ per ogni $x \in G$); il gruppo alterno A_n è un sottogruppo normale di S_n; un sottogruppo N di indice due in un gruppo G è normale (non è vero se l'indice è tre); gruppi semplici (gruppi che non hanno sottogruppi normali non banali); il centro $Z(G)$ di un gruppo G; il centro di un gruppo G è un sottogruppo abeliano normale del gruppo G e ogni sottogruppo contenuto in $Z(G)$ è normale in G; G è abeliano se e solo se $Z(G) = G$; se G è un gruppo semplice non abeliano allora $Z(G) = \{1\}$; non vale la proprietà transitiva per sottogruppi normali: se H è normale in K e K è normale in G non è detto che H sia normale in G; operazioni con i sottogruppi normali; l'intersezione di una famiglia di sottogruppi normali è un sottogruppo normale; l'unione di una catena di sottogruppi normali è normale: il sottogruppo generato da una famiglia qualsiasi di sottogruppi normali è un sottogruppo normale sia H un sottogruppo di G e K un sottogruppo normale di G allora $HK = KH$ (e quindi HK è un sottogruppo di G) se anche H è normale allora HK è un sottogruppo normale di G; il gruppo lineare speciale $SL_n(\mathbb{K})$ (sottogruppo normale di $GL_n(\mathbb{K})$); il sottogruppo $T_n^+(\mathbb{K})$ delle matrici triangolari superiori invertibili (non è normale in $GL_n(\mathbb{K})$, per ogni $n \geq 2$ e per ogni campo $\mathbb{K}$); il gruppo $D_n(\mathbb{K})$ delle matrici diagonali (non è un sottogruppo normale di $GL_n(\mathbb{K})$ se $|\mathbb{K}| \geq 3$ e $n \geq 2$); le matrici scalari Z sono il centro di $GL_n(\mathbb{K})$; il gruppo ortogonale $O_n(\mathbb{K})$ è un sottogruppo (non normale) di $GL_n(\mathbb{K})$ per $n \geq 2$; le matrici simmetriche invertibili non sono un sottogruppo di $GL_n(\mathbb{K})$; il gruppo Q_8 dei quaternioni unitari e le sue proprietà; il gruppo quoziente di un gruppo G tramite un sottogruppo normale N; il gruppo degli interi modulo $\mathbb{Z}_m$ come quoziente: $\mathbb{Z} = \mathbb{Z}/m\mathbb{Z}$; se N è un sottogruppo normale di un gruppo finito G allora $|G| = |G/N||N|$.

5. Omomorfismi e isomorfismi.; Omomorfismi di gruppi; principali proprietà degli omomorfismi (l'identità va nell'identità, l'inverso va nell'inverso e le potenze si preservano); la composizione di omomorfismi è un omomorfismo; isomorfismi di gruppi (omomorfismi invertibili); ogni gruppo ciclico finito di ordine n è isomorfo a $\mathbb{Z}_n$; l'immagine di un gruppo ciclico tramite un omomorfismo è ancora ciclico; nucleo di un omomorfismo (sottogruppo normale del dominio); immagine di un omomorfismo (sottogruppo del codominio); un omomorfismo di gruppi è iniettivo se solo se il suo nucleo è banale;

omomorfismo canonico $\pi : G \to G/N$ (ogni sottogruppo normale è il nucleo di un omomorfismo); il primo teorema di isomorfismo (sia $\varphi : G \to H$ un omomorfismo di gruppi e $\pi : G \to G/\ker\varphi$ l'omomorfismo canonico allora esiste un unico omomorfismo iniettivo $\tilde{\varphi} : G/\ker\varphi \to H$ tale che $\tilde{\varphi} \circ \pi = \varphi$ che risulta essere un isomorfismo se e solo se φ è suriettivo); sia $\varphi : G \to H$ un omomorfismo di gruppi allora $G/\ker\varphi \cong Im(\varphi)$; sia $\varphi : G \to H$ un omomorfismo suriettivo di gruppi allora $H \cong G/\ker\varphi$; sia $\varphi : G \to H$ un omomorfismo suriettivo di gruppi se G è finito allora $|\ker\varphi|$ e $|H|$ dividono $|G|$; $\mathrm{GL}_n(\mathbb{K})/SL_n(\mathbb{K}) \cong \mathbb{K}^*$, per ogni $n \geq 1$, e $S_n/A_n \cong \mathbb{Z}_2$, per ogni $n \geq 2$; $\mathbb{C}^*/S^1 \cong \mathbb{R}^+$; sia $\varphi : G \to H$ un omomorfismo di gruppi allora (a) per ogni $K \leq G$ risulta $\varphi(K) \leq H$ e se $K \trianglelefteq G$ allora $\varphi(K) \trianglelefteq \varphi(G)$, (b) per ogni $L \leq H$ risulta $\ker\varphi \leq \varphi^{-1}(L) \leq G$ e inoltre $L \trianglelefteq H$ allora $\varphi^{-1}(L) \trianglelefteq G$, (c) per ogni $K \leq G$ si ha $\varphi^{-1}(\varphi(K)) = K\ker\varphi$, (d) $\varphi(\varphi^{-1}(L)) = L \cap \varphi(G)$ per ogni $L \leq H$; esiste una corrispondenza biunivoca tra l'insieme dei sottogruppi (normali) di G contenenti $\ker\varphi$ e l'insieme dei sottogruppi (normali) di H contenuti in $\varphi(G)$; sottogruppi di $\mathbb{Z}_m$ ($L \leq \mathbb{Z}_m$ se e solo se $L = \frac{n\mathbb{Z}}{m\mathbb{Z}}$ tale che $n|m$); il gruppo degli automorfismi $\mathrm{Aut}(G)$ di un gruppo G; il gruppo $Inn(G)$ degli automorfismi interni; $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$ e $G/Z(G) \cong \mathrm{Inn}(G)$; il teorema di Cayley (ogni gruppo è isomorfo ad un sottogruppo di un gruppo di permutazioni); ogni gruppo finito di cardinalità n è isomorfo ad un sottogruppo del gruppo lineare $GL_n(\mathbb{K})$ per un qualsiasi campo $\mathbb{K}$.

6. Prodotto diretto di gruppi. Prodotto diretto di un numero finito di gruppi; proprietà commutativa e associativa del prodotto diretto; l'ordine di un elemento $z = (x, y)$ del prodotto diretto $H \times K$ è finito se solo se sono finiti gli ordini di $x \in H$ e $y \in K$ e in tal caso l'ordine di z è il minimo comune multiplo degli ordini di x e y; sia $G = H \times K$ allora esistono due sottogruppi normali $\tilde{H}$ e $\tilde{K}$ isomorfi a H e K tali che $\tilde{H} \cap \tilde{K} = \{1\}$ e $G = \tilde{H}\tilde{K}$; sia G un gruppo e H e K due sottogruppi normali di G tali che $H \cap K = \{1\}$ e $G = HK$ allora $G \cong H \times K$; sia G un gruppo abeliano e H e K due sottogruppi di G tali che $H \cap K = \{1\}$ e $G = H + K$ allora $G \cong H \times K$; sia G un gruppo finito e H e K due sottogruppi normali di G tali che $|H| = m$ e $|K| = n$, $(m, n) = 1$ e $|G| = mn$ allora $G \cong H \times K$; se in un gruppo G tutti gli elementi hanno ordine 2 allora G è abeliano; se G ha ordine 4 allora è isomorfo a $\mathbb{Z}_4$ oppure a $\mathbb{Z}_2 \times \mathbb{Z}_2$; se G è un gruppo abeliano cardinalità 6 con due elementi di ordine 2 e 3 allora $G \cong \mathbb{Z}_6$; a meno di isomorfismi un gruppo con 6 elementi è isomorfo a Z_6 oppure a S_3; se H e K sono gruppi finiti con cardinalità prime fra loro allora $\mathrm{Aut}(H \times K) \cong \mathrm{Aut}(H) \times \mathrm{Aut}(K)$ (solo enunciato senza dimostrazione).

7. Gruppi abeliani finiti. classificazione dei gruppi ciclici: un gruppo ciclico finito è isomorfo a $\mathbb{Z}_m$ mentre un gruppo ciclico infinito è isomorfo a $\mathbb{Z}$; generatori di un gruppo ciclico: un gruppo ciclico finito ha $\phi(m)$ generatori dove $\phi(m)$ è la funzione di Eulero mentre un gruppo ciclico infinito ha due generatori; un sottogruppo di un gruppo ciclico è ciclico; il quoziente di un gruppo ciclico è ciclico; se C è un gruppo ciclico finito allora per ogni divisore d di $|C|$ esiste un unico sottogruppo di C di ordine d; esiste una corrispondenza biunivoca tra i divisori positivi della cardinalità di un gruppo ciclico finito e i suoi sottogruppi; se K è ciclico e normale in G e H è un sottogruppo di K allora H è normale in G; se tutti i sottogruppi di un gruppo G sono solo quelli banali, allora G è ciclico di ordine p; il prodotto diretto $C_1 \times C_2$ di due gruppi ciclici (non banali) è ciclico se e solo C_1 e C_2 hanno cardinalità finite prime fra loro (quindi $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ se e solo se $((m, n) = 1)$; il gruppo degli automorfismi di un gruppo ciclico: $\mathrm{Aut}(C) \cong \mathbb{Z}_2$ se C ha infiniti elementi e $\mathrm{Aut}(C) \cong U(\mathbb{Z}_m)$ se $|C| = m$; il Teorema di Gauss: il gruppo degli automorfismi di un gruppo ciclico finito C è ciclico se e solo se $|C| = 1, 2, 4, p^m, 2p^m$ con p primo dispari (solo enunciato senza dimostrazione); sia G un gruppo abeliano, H un sottogruppo di G e $a \in G$ siano m e n interi primi tra loro tali che $ma \in H$ e $na \in K$ allora $a \in H$; lemma di Cauchy nel caso abeliano): sia p un numero primo e G un gruppo abeliano finito tale che p divide $|G|$ allora G ha elementi di ordine p; sia G un gruppo abeliano finito e m un intero positivo tale che $mx = 0$ per ogni $x \in G$ allora $|G|$ divide qualche potenza di m; siano m e n due interi positivi primi tra loro e G un gruppo abeliano di ordine mn allora: (a) $H = \{x \in G \mid mx = 0\}$ è un sottogruppo di G di ordine m; (b) $K = \{x \in G \mid nx = 0\}$ è un sottogruppo di G di ordine n, (c) $G \cong H \times K$; lemma di scomposizione primaria; sia p un numero primo e G un gruppo abeliano di ordine p^n allora G è isomorfo ad un prodotto diretto di gruppi ciclici; teorema di Frobenius–Stickelberger (ogni gruppo abeliano finito è isomorfo al prodotto di gruppi ciclici).

Testo di riferimento

D. Dikranjan, M. L. Lucido, *Aritmetica e Algebra*, Liguori Editore 2007.

Altri testi consigliati

C.C. Pinter, *A book of abstract algebra*, Dover Publications Inc.

I.N. Herstein, *Algebra*, Editori Riuniti.

M. Artin, *Algebra*, Bollati Boringhieri.