

## PROGRAMMA DI ALGEBRA 2

Corso di Laurea in Matematica A.A. 2021-2022, primo semestre, 6 crediti  
(gli altri 4 crediti saranno svolti dal Professor Stefano Bonzio)

Docente: Andrea Loi

**Monoidi, semigrupperi e gruppi.** Semigrupperi; esempi di semigrupperi; legge di cancellazione in un semigruppero; elementi idempotenti in un semigruppero; esempi di semigrupperi dove tutti gli elementi sono idempotenti e esempi dove nessun elemento lo è; in un semigruppero finito esiste almeno un elemento idempotente; monoidi (semigrupperi con elemento neutro  $e$ ); esempi di monoidi; un elemento  $e$  di un semigruppero dove vale la legge di cancellazione è idempotente se e solo se  $e$  è l'elemento neutro; elementi invertibili in un monoide; unicità dell'inverso; un elemento idempotente in un monoide dove vale la legge di cancellazione è l'elemento neutro; un elemento idempotente in un semigruppero dove vale la legge di cancellazione a sinistra (o a destra) è l'elemento neutro; definizione di gruppo; un semigruppero con elemento neutro a destra (risp. sinistra) e inverso a destra (risp. sinistra) è un gruppo; esempi che mostrano che esistono semigrupperi con elemento neutro a sinistra e inverso a destra che non sono gruppi; legge di cancellazione in un gruppo; un semigruppero finito dove vale la legge di cancellazione è un gruppo; esempi che mostrano che esistono semigrupperi infiniti dove vale la legge di cancellazione che non sono gruppi; esempi che mostrano l'esistenza di semigrupperi finiti dove vale la legge di cancellazione a destra ma che non sono gruppi; esempi di gruppi; gli elementi invertibili di un monoide formano un gruppo; proprietà elementari dei gruppi: inverso del prodotto; proprietà delle potenze in un gruppo; confronto tra la notazione addittiva e moltiplicativa; ordine di un elemento; alcune proprietà dell'ordine: se  $x$  ha ordine finito  $o(x) = m$ , (a) allora  $x^k = 1$  se e solo se  $m$  divide  $k$ , (b)  $x^n = x^k$  per  $n, k \in \mathbb{Z}$  se e solo se  $n$  è congruo a  $k$  modulo  $m$ , (c)  $o(x^k) = m/(m, k)$ , (d)  $o(x^{-1}) = m$ .

**Permutazioni.** 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; ogni permutazione  $f$  non identica con supporto finito può scriversi in modo essenzialmente unico 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  $\sigma_j$ ; 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  $\text{sgn}(f) = (-1)^{N(f)}$ ; permutazioni di classe pari e dispari; ogni permutazione  $f$  si può scrivere come prodotto di  $N(f)$  trasposizioni; il  $\text{sgn}$  è una funzione moltiplicativa  $\text{sgn}(f \circ g) = \text{sgn}(f)\text{sgn}(g)$ ; una permutazione è di classe pari se e solo se si può scrivere come prodotto di un numero pari di trasposizioni.

**Sottogruppi.** 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  $\langle X \rangle$  di un gruppo  $G$  generato da un sottoinsieme  $X \subseteq G$ ; sottogruppo  $\langle x \rangle$  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  $|\langle x \rangle| = o(x)$ ; 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  $\langle H, K \rangle = \langle H \cup K \rangle$  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  $\langle H, K \rangle = HK$ ; 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.** 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  $|G| = [G : H]|H|$ ); se  $G$  è un gruppo finito e  $H$  un sottogruppo di  $G$  allora  $[G : H]$  e  $|H|$  dividono  $|G|$ ; 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  $G$ .

**Sottogruppi normali.** Definizione di sottogruppo normale di un gruppo  $G$ :  $N$  è un sottogruppo 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 ( $N \trianglelefteq G$  se e solo se  $N^x \leq N$  se e solo se  $N^x = N$  per ogni  $x \in G$ ); il gruppo alterno  $A_n$  è un sottogruppo normale di  $S_n$ ; 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  $G$ ; l'intersezione di una famiglia di sottogruppi normali è un sottogruppo normale; il sottogruppo generato da una famiglia qualsiasi di sottogruppi normali è un sottogruppo normale; gruppi semplici (gruppi che non hanno sottogruppi normali non banali); il centro  $Z(G)$  di un gruppo  $G$  (gli elementi di  $G$  che commutano con tutti gli elementi di  $G$ ); 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  $Z(G) = \{1\}$ ; un sottogruppo  $N$  di indice due in un gruppo  $G$  è normale inoltre esistono sottogruppi  $N$  di un gruppo  $G$  di indice tre che non sono normali (per esempio il sottogruppo  $H = \langle (12) \rangle$  di  $S_3$ ).

**I gruppi lineari** 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 intersezione  $O_n(\mathbb{K}) \cap T_n^+(\mathbb{K})$ ; il gruppo  $Q_8$  dei quaternioni di ordine 8 e le sue proprietà (il più piccolo gruppo non abeliano di ordine una potenza di un primo; il più piccolo gruppo non abeliano in cui tutti i suoi sottogruppi sono normali;  $Q_8$  è unione di tre suoi sottogruppi propri ma non è il più piccolo gruppo con questa proprietà, per esempio  $\mathbb{Z}_2 \times \mathbb{Z}_2 = \langle (1, 0) \rangle \cup \langle (0, 1) \rangle \cup \langle (1, 1) \rangle$ ); il gruppo di Heisenberg e il suo centro.

**Quozienti e omomorfismi di gruppi.** Quoziente di un gruppo  $G$  tramite un sottogruppo normale  $N$ ;  $\mathbb{Z}_m$  come quoziente di  $\mathbb{Z}/m\mathbb{Z}$ ; se  $N$  è un sottogruppo normale di un gruppo finito  $G$  allora  $|G/N|$  divide  $|G|$ ; 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); 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 e solo se il suo nucleo è banale; omomorfismo canonico  $\pi : G \rightarrow G/N$  (ogni sottogruppo normale è il nucleo di un omomorfismo); il primo teorema di isomorfismo (sia  $\varphi : G \rightarrow H$  un omomorfismo di gruppi e  $\pi : G \rightarrow G/\ker \varphi$  l'omomorfismo canonico allora esiste un unico omomorfismo iniettivo  $\tilde{\varphi} : G/\ker \varphi \rightarrow H$  tale che  $\tilde{\varphi} \circ \pi = \varphi$  che risulta essere un isomorfismo se e solo se  $\varphi$  è suriettivo); sia  $\varphi : G \rightarrow H$  un omomorfismo di gruppi allora  $G/\ker \varphi \cong \text{Im}(\varphi)$ ; sia  $\varphi : G \rightarrow H$  un omomorfismo suriettivo di gruppi allora  $H \cong G/\ker \varphi$ ; sia  $\varphi : G \rightarrow H$  un omomorfismo suriettivo di gruppi se  $G$  è finito allora  $|\ker \varphi|$  e  $|H|$  dividono  $|G|$ ;  $\text{GL}_n(\mathbb{K})/SL_n(\mathbb{K}) \cong \mathbb{K}^*$ , per ogni  $n \geq 1$ , e  $S_n/A_n \cong \mathbb{Z}_2$ , per ogni  $n \geq 2$ ; sia  $\varphi : G \rightarrow H$  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  $\text{Aut}(G)$  di un gruppo  $G$ ; il gruppo  $\text{Inn}(G)$  degli automorfismi interni;  $\text{Inn}(G) \trianglelefteq \text{Aut}(G)$  e  $G/Z(G) \cong \text{Inn}(G)$ ; 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  $\mathbb{K}$ .

**Prodotto diretto di gruppi.** Prodotto diretto di un numero finito di gruppi; proprietà commutativa e associativa del prodotto diretto; 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  $G$  è un gruppo abeliano cardinalità 6 con due elementi di ordine 2 e 3 allora  $G \cong \mathbb{Z}_6$ . 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  $\mathbb{Z}_2 \times \mathbb{Z}_2$ ; a meno di isomorfismi un gruppo con 6 elementi è isomorfo a  $\mathbb{Z}_6$  oppure a  $S_3$ ; non esiste un sottogruppo  $H$  di  $A_4$  di ordine 6; l'ordine di un elemento  $z = (x, y)$  del prodotto diretto  $H \times K$  è finito se e 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  $y$ .

**Gruppi abeliani finiti.** 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; 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; il prodotto diretto  $C_1 \times C_2$  di due gruppi ciclici è ciclico se e solo se la cardinalità di  $C_1$  e  $C_2$  sono primi fra loro; il gruppo degli automorfismi di un gruppo ciclico:  $\text{Aut}(C) \cong \mathbb{Z}_2$  se  $C$  ha infiniti elementi e  $\text{Aut}(C) \cong U(\mathbb{Z}_m)$  se

$|C| = m$ ; 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)  $H = \{x \in G \mid nx = 0\}$  è un sottogruppo di  $G$  di ordine  $n$ ; (b)  $K = \{x \in G \mid mx = 0\}$  è un sottogruppo di  $G$  di ordine  $m$ , (c)  $G \cong H \times K$ ; teorema di decomposizione 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 prodotto di gruppi ciclici).

**Esercizi:** 4.9, 4.11, 4.14, 5.5, 5.6, 5.9, 5.14, 5.16, 5.19, 5.20, 5.22, 5.24, 5.25, 5.26, 5.27, 5.28, 5.33, 5.35, 5.36, 5.37, 5.38, 5.39, 5.41, 5.47, 5.48, 5.51, 5.52, 5.53, 5.54, 5.58, 6.1, 6.2, 6.3, 6.5, 6.6, 6.7, 6.8, 6.10, 6.16, 6.17, 6.18, 6.19, 6.20, 6.21, 6.22, 6.23, 6.24, 6.25, 6.27, 6.28, 6.29, 6.33, 6.34, 6.35, 6.40, 7.2, 7.3, 7.4, 7.5, 7.14, 7.16, 7.17, 7.26, 7.29, 7.32.

#### Testo di riferimento

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

#### Altri testi consigliati

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

**M. Artin**, *Algebra*, Bollati Boringhieri.