

## PROGRAMMA DI ALGEBRA 2

Corso di Laurea in Matematica A.A. 2019-2020, primo semestre

Docente: Andrea Loi

**Richiami della teoria degli insiemi.** Relazioni di preordine e di ordine; insiemi parzialmente ordinati; esempi di insiemi parzialmente ordinati; ordine totale; insiemi totalmente ordinati; esempi di insiemi totalmente ordinati; minimo e massimo di un insieme; elementi minimali e elementi massimali di un insieme parzialmente ordinato; ogni insieme parzialmente ordinato e finito ha almeno un elemento massimale e uno minimale; sottoinsiemi di insiemi parzialmente e totalmente ordinati: minoranti, maggioranti, estremo superiore e estremo inferiore; sottoinsiemi limitati superiormente e inferiormente; ordine buono; principio del buon ordinamento; lemma di Zorn (senza dimostrazione): un insieme parzialmente ordinato e induttivo ammette elementi massimali; prodotti cartesiani di insiemi finiti; prodotti cartesiani di famiglie di insiemi infiniti e legame con l'assioma di scelta; reticoli  $(X, \leq, \wedge, \vee)$ ; esempi fondamentali di reticoli:  $(\mathcal{P}(X), \cup, \emptyset)$ ,  $(\mathcal{P}(X), \cap, X)$ .

**Monoidi, semigrupp e gruppi.** Semigrupp; esempi di semigrupp; legge di cancellazione in un semigrupp; elementi idempotenti in un semigrupp; esempi di semigrupp dove tutti gli elementi sono idempotenti e esempi dove nessun elemento lo è; in un semigrupp finito esiste almeno un elemento idempotente; monoidi (semigrupp con elemento neutro  $e$ ); esempi di monoidi; un elemento  $e$  di un semigrupp dove vale la legge di cancellazione è idempotente se e solo se  $e$  è l'elemento neutro; se  $(X, \leq)$  è un reticolo (limitato) allora  $(X, \wedge)$  e  $(X, \vee)$  sono semigrupp (monoidi); 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 semigrupp dove vale la legge di cancellazione è l'elemento neutro; definizione di gruppo; un semigrupp con elemento neutro a destra (risp. sinistra) e inverso a destra (risp. sinistra) è un gruppo; esempi che mostrano che esistono semigrupp con elemento neutro a sinistra e inverso a destra che non sono gruppi; legge di cancellazione in un gruppo; un semigrupp finito dove vale la legge di cancellazione è un gruppo; esempi che mostrano che esistono semigrupp infiniti dove vale la legge di cancellazione che non sono gruppi; esempi che mostrano l'esistenza di semigrupp 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 e 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  $H \cap K = [m, n]\mathbb{Z}$ ; l'insieme  $\mathcal{L}(G)$  di tutti i sottogruppi di un gruppo  $G$  è un reticolo limitato; esistono sottogruppi  $H, K, L$  sottogruppi di un gruppo  $G$  dove non vale  $(HK) \cap L = (H \cap L)(K \cap L)$  (in generale vale  $(H \cap L)(K \cap L) \subseteq (HK) \cap L$  ma esistono gruppi (sia abeliani che non abeliani) dove non vale  $(HK) \cap L \subseteq (H \cap L)(K \cap L)$ ); legge modulare di Dedekind: siano  $H, K, L$  sottogruppi di un gruppo  $G$  e sia  $K \subseteq L$  allora  $(HK) \cap L = (H \cap L)K$ .

**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  $x \in G$ ); 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; l'insieme  $\mathcal{N}(G)$  di tutti i sottogruppi normali di un gruppo  $G$  è un reticolo limitato; 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  $SL_n(K)$  (sottogruppo normale di  $GL_n(K)$ ); il sottogruppo  $T_n^+(K)$  delle matrici triangolari superiori invertibili (non è normale in  $GL_n(K)$ , per ogni  $n \geq 2$  e per ogni campo  $K$ ); il gruppo  $D_n(K)$  delle matrici diagonali (non è un sottogruppo normale di  $GL_n(K)$  se  $|K| \geq 3$  e  $n \geq 2$ ); le matrici scalari  $Z$  sono il centro di  $GL_n(K)$ ; il gruppo ortogonale  $O_n(K)$  è un sottogruppo (non normale) di  $GL_n(K)$  per  $n \geq 2$ ; le matrici simmetriche invertibili non sono un sottogruppo di  $GL_n(K)$ ; il gruppo intersezione  $O_n(K) \cap T_n^+(K)$ ; 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; la cardinalità dei gruppi  $M_n(\mathbb{Z}_p)$  e  $GL_n(\mathbb{Z}_p)$ ,  $p$  primo.

**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 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  $|G|$ ; 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  $\varphi(G)$ ; il secondo teorema di isomorfismo (siano  $K \leq G$  e  $N \trianglelefteq G$  allora  $N \cap K \trianglelefteq K$  e  $K/K \cap N \cong KN/N$ ); sia  $\varphi : G \rightarrow H$  un omomorfismo suriettivo di gruppi e  $\ker \varphi \leq K \leq G$  allora  $G/K \cong H/\varphi(K)$ ; il terzo teorema di isomorfismo (siano  $N \trianglelefteq G$ ,  $K \trianglelefteq G$ ,  $N \leq K$  allora  $K/N \trianglelefteq G/N$  e  $G/K \cong (G/N)/(K/N)$ ); 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 di un gruppo; il gruppo degli automorfismi interni è isomorfo al quoziente del gruppo e del suo centro; il gruppo degli automorfismi interni è un sottogruppo normale del gruppo degli automorfismi; il teorema di Cayley (ogni gruppo è isomorfo ad un sottogruppo di un gruppo di permutazioni); ogni gruppo finito è isomorfo ad un sottogruppo del gruppo lineare  $GL_n(K)$  per un opportuno  $n$  e per qualsiasi campo  $K$ ; il determinante  $\det : GL_n(K) \rightarrow K^*$  è un omomorfismo suriettivo di gruppi il cui nucleo è  $SL_n(K)$ ; la funzione  $\text{sgn} : S_n \rightarrow \{-1, 1\}$  è un omomorfismo suriettivo di gruppi il cui nucleo è  $A_n$ .

**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  $G \cong H \times K$ ; 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  $y$ .

**Gruppi abeliani finiti.** Classificazione dei gruppi ciclici (un gruppo ciclico finito è isomorfo a  $\mathbb{Z}_m$ , un gruppo ciclico infinito è isomorfo a  $\mathbb{Z}$ ); generatori di un gruppo ciclico ( $\mathbb{Z}_m$  ha  $\Phi(m)$  generatori dove  $\Phi(m)$  è la funzione di Eulero mentre  $\mathbb{Z}$  ha due generatori); siano  $m > 0$  e  $n > 0$  due numeri naturali allora  $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$  se e solo se  $(m, n) = 1$ ; il quoziente di un gruppo ciclico è ciclico; un sottogruppo 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  $d$ ; studio del gruppo  $(U(\mathbb{Z}_m), \cdot)$  degli elementi invertibili di  $(\mathbb{Z}_m, \cdot)$ ; sia  $m > 0$  un numero naturale allora  $\text{Aut}(\mathbb{Z}_m)$  è isomorfo a  $(U(\mathbb{Z}_m), \cdot)$ ; 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  $\mathbb{Z}_2 \times \mathbb{Z}_2$ ; 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 (dimostrazione solo 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); ogni gruppo abeliano di ordine 6 è isomorfo a  $\mathbb{Z}_6$  oppure a  $S_3$  (dando per buono il Lemma di Cauchy nel caso non abeliano); non esiste un sottogruppo  $H$  di  $A_4$  di ordine 6;

**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.

**Anelli.** Definizione di anello e di anello unitario; elementi invertibili di un anello; anelli commutativi e elementi permutabili; esempi di anelli: gli interi, i razionali, i reali, i complessi, gli interi modulo  $m$ , le matrici  $n \times n$  a coefficienti reali, le matrici  $n \times n$  a coefficienti in un anello  $A$ ; alcune proprietà di base sulla somma e la moltiplicazione di anelli; divisori sinistri e destri dello zero e leggi di cancellazione in un anello; elementi nilpotenti; anelli interi (anelli unitari privi di divisori dello zero), domini (anelli interi commutativi), corpi (anelli unitari dove tutti gli elementi non nulli sono invertibili), campi (corpi commutativi); gli elementi invertibili non sono divisori dello zero e quindi un corpo è integro e un campo è un dominio; un anello finito privo di divisori dello zero è un corpo (e quindi un anello commutativo finito privo di divisori dello zero è un campo); il corpo dei quaternioni.

**Sottoanelli.** Sottoanelli di un anello (unitario); sottoanelli banali; se  $C$  è un sottoanello di  $B$  e  $B$  un sottoanello di  $A$  allora  $C$  è un sottoanello di  $A$ ; l'intersezione di una famiglia qualunque di sottoanelli di un anello  $A$  è ancora un sottoanello di  $A$ ; sottoanello di un anello  $A$  generato da un sottoinsieme  $X \subset A$ ; sottoanello generato da un elemento; sottoanello fondamentale di un anello unitario e caratteristica di un anello;

**Ideali.** Ideali sinistri, destri e bilateri di un anello; ideali banali e ideali propri; ideali e sottoanelli; sia  $A$  un anello con unità e sia  $I$  un suo ideale (sinistro, destro o bilatero), se  $I$  contiene l'unità oppure contiene un elemento invertibile allora  $I = A$ ; l'intersezione di una famiglia qualunque di ideali (sinistri, destri, bilateri) è un ideale (sinistro, destro, bilatero); ideale (sinistro, destro e bilatero) generato da un sottoinsieme; ideale generato da un elemento di un anello commutativo e unitario; ideali principali e anelli commutativi unitari a ideali principali; gli interi sono un dominio a ideali principali (tutti i suoi ideali sono della forma  $m\mathbb{Z}$ ); la somma di due ideali (sinistri, destri, bilateri) è un ideale (sinistro, destro, bilatero); sia  $A$  un anello commutativo unitario allora  $A$  è un campo se e solo se  $A$  è privo di ideali non banali; gli anelli quoziente; gli interi modulo  $m$  come anello quoziente; ideali primi e ideali massimali; sia  $A$  un anello commutativo unitario un ideale  $I$  è primo (risp. massimale) se e solo se  $A/I$  è un dominio (risp. campo); un ideale massimale è primo; l'ideale nullo è primo in  $\mathbb{Z}$  ma non massimale; gli ideali non banali massimali e primi di  $\mathbb{Z}$  sono della forma  $p\mathbb{Z}$  dove  $p$  è primo; in un anello commutativo unitario finito un ideale primo è massimale.

**Omomorfismi di anelli.** Omomorfismi di anelli e di anelli unitari; composizione di omomorfismi è un omomorfismo; isomorfismi di anelli; nucleo di un omomorfismo come ideale bilatero; immagine di un anello tramite un omomorfismo; omomorfismo canonico; un omomorfismo unitario tra un campo e un anello è iniettivo; per ogni anello  $A$ , l'omomorfismo  $\varphi(a) : A \rightarrow A$ ,  $\varphi(a) = a^{-1}xa$  è un omomorfismo per ogni  $a \in U(A)$ ; primo teorema di isomorfismo per anelli (sia  $f : A_1 \rightarrow A_2$  un omomorfismo tra due anelli  $A_1$  e  $A_2$  allora esiste un omomorfismo iniettivo  $\tilde{f} : A_1/\ker f \rightarrow A_2$  tale che  $\tilde{f} \circ \pi = f$  che risulta essere un isomorfismo se e solo se  $f$  è suriettivo); sia  $f : A_1 \rightarrow A_2$  un omomorfismo allora  $A_1/\ker f \cong f(A_1)$ ; teorema di corrispondenza per anelli e sottoanelli (sia  $f : A_1 \rightarrow A_2$  un omomorfismo tra due anelli  $A_1$  e  $A_2$  (a) se  $B_1$  è un sottoanello di  $A_1$  allora  $f(B_1)$  è un sottoanello di  $A_2$ , (b) se  $B_2$  è un sottoanello di  $A_2$  allora  $f^{-1}(B_2)$  è un sottoanello di  $A_1$  che include  $\ker f$ , (c) sia  $f : A_1 \rightarrow A_2$  è un omomorfismo tra anelli unitari se  $B_1$  è un sottoanello di  $A_1$  allora  $f(B_1)$  è un sottoanello di  $A_2$  e se  $B_2$  è un sottoanello di  $A_2$  allora  $f^{-1}(B_2)$  è un sottoanello di  $A_1$ , (d)  $f^{-1}(f(B_1)) = B_1 + \ker f$ , (e)  $f(f^{-1}(B_2)) = B_2 \cap f(A_1)$ , (f) esiste una corrispondenza biunivoca tra i sottoanelli di  $A_1$  che contengono il  $\ker f$  e i sottoanelli di  $A_2$  contenuti in  $f(A_1)$ ); teorema di corrispondenza per anelli e ideali (sia  $f : A_1 \rightarrow A_2$  un omomorfismo tra due anelli  $A_1$  e  $A_2$  (a) se  $I_1$  è un ideale (sinistro, destro, bilatero) di  $A_1$  allora  $f(I_1)$  è un ideale (sinistro, destro, bilatero) di  $f(A_1)$ , (b) se  $I_2$  è un ideale (sinistro, destro, bilatero) di  $A_2$  allora  $f^{-1}(I_2)$  è un ideale (sinistro, destro, bilatero) di  $A_1$  che include  $\ker f$ , (c)  $f^{-1}(f(I_1)) = I_1 + \ker f$ , (d)  $f(f^{-1}(I_2)) = I_2 \cap f(A_1)$ , (e) esiste una corrispondenza biunivoca tra gli ideali (sinistri, destri, bilateri) di  $A_1$  che contengono il  $\ker f$  e gli ideali (sinistri, destri, bilateri) di  $f(A_1)$ ); l'inclusione di  $\mathbb{Z}$  in  $\mathbb{Q}$  mostra che in generale non è detto che  $f(I_1)$  sia un ideale di  $A_2$ ; secondo teorema di isomorfismo per anelli (sia  $J$  un ideale bilatero e  $B$  un sottoanello di un anello  $A$  allora  $B \cap J$  è un ideale bilatero di  $B$  e  $B/B \cap J \cong B + J/J$ ); teorema intermedio (sia  $f : A_1 \rightarrow A_2$  un omomorfismo di anelli e sia  $I_2$  un ideale di  $A_2$  tale che  $I_2 \subseteq f(A_1)$

allora  $f^{-1}(I_2)$  è un ideale di  $A_1$  e  $A_1/f^{-1}(I_2) \cong f(A_1)/I_2$ , in particolare se  $f$  è suriettiva  $A_1/f^{-1}(I_2) \cong A_2/I_2$ ; dimostrazione alternativa del fatto che il quoziente  $A/I$  di un anello commutativo unitario è un campo se e solo se  $I$  è massimale; terzo teorema di isomorfismo per anelli (siano  $I$  e  $J$  due ideali bilateri di un anello  $A$ ,  $I \subseteq J$  allora  $J/I$  è un ideale bilatero di  $A/I$  e  $A/J \cong (A/I)/(J/I)$ ); teorema di corrispondenza per ideali primi (sia  $f : A_1 \rightarrow A_2$  un omomorfismo tra due anelli commutativi unitari  $A_1$  e  $A_2$  (a) se  $I_1$  è un ideale primo di  $A_1$  tale che  $\ker f \subseteq I_1$  allora  $f(I_1)$  è un ideale primo di  $f(A_1)$ , (b) se  $I_2$  è un ideale primo di  $A_2$  allora  $f^{-1}(I_2)$  è un ideale primo di  $A_1$ , (c) esiste una corrispondenza biunivoca tra gli ideali primi di  $A_1$  che contengono il  $\ker f$  e gli ideali primi di  $f(A_1)$ ); teorema di corrispondenza per ideali massimali (sia  $f : A_1 \rightarrow A_2$  un omomorfismo tra due anelli commutativi unitari  $A_1$  e  $A_2$  (a) se  $I_1$  è un ideale massimale di  $A_1$  tale che  $\ker f \subseteq I_1$  allora  $f(I_1)$  è un ideale massimale di  $f(A_1)$ , (b) se  $I_2$  è un ideale massimale di  $f(A_1)$  allora  $f^{-1}(I_2)$  è un ideale massimale di  $A_1$ , (c) esiste una corrispondenza biunivoca tra gli ideali massimali di  $A_1$  che contengono il  $\ker f$  e gli ideali massimali di  $f(A_1)$ ); l'ipotesi che  $\ker f \subseteq I_1$  nei due punti (a) precedenti non è superflua (per esempio  $f : \mathbb{Z} \rightarrow \mathbb{Z}_2$ ,  $I_1 = 3\mathbb{Z}$  allora  $f(I_1) = \mathbb{Z}_2$  che non è primo); l'ipotesi che  $I_2$  sia massimale in  $f(A_1)$  nel punto (b) è necessaria (per esempio considerata l'inclusione  $f : \mathbb{Z} \rightarrow \mathbb{Q}$ ,  $I_2 = \{0\}$  è massimale in  $\mathbb{Q}$  ma  $f^{-1}(I_2) = \{0\}$  che non è massimale in  $\mathbb{Z}$ ); sottoanelli e ideali (primi e massimali) di  $\mathbb{Z}_m$ .

**Campo dei quozienti di un dominio** campo dei quozienti di un dominio  $A$  (campo  $K$  per il quale esiste un omomorfismo iniettivo  $f : A \rightarrow K$  tale che per ogni  $k \in K$  esiste  $b \in A^*$  e  $a \in A$  tale che  $k = f(a)f(b)^{-1}$ ); esistenza del campo dei quozienti  $Q(A)$  di un dominio  $A$ ; sia  $A$  un dominio e sia  $f : A \rightarrow Q(A)$  un suo campo dei quozienti, se  $K$  è un campo e  $g : A \rightarrow K$  è un omomorfismo iniettivo di anelli allora esiste un unico omomorfismo iniettivo di anelli unitari  $h : Q(A) \rightarrow K$  tale che  $h \circ f = g$ ; sia  $A$  un dominio e siano  $f_1 : A \rightarrow Q(A_1)$  e  $f_2 : A \rightarrow Q(A_2)$  due suoi campi dei quozienti allora esiste un isomorfismo di anelli unitari  $i : Q(A_1) \rightarrow Q(A_2)$  tale che  $i \circ f_1 = f_2$ .

#### 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.