Programma di Algebra 1

A. A. 2025/2026

Docenti: Alberto Canonaco e Filippo Favale

Richiami su insiemi e funzioni: composizione di funzioni e associatività della composizione; immagine attraverso una funzione di un sottoinsieme del dominio e controimmagine di un sottoinsieme del codominio. Funzioni iniettive, suriettive e biunivoche e loro stabilità rispetto alla composizione; funzione inversa di una funzione biunivoca. Cardinalità di un insieme; una funzione tra due insiemi finiti con la stessa cardinalità è iniettiva se e solo se è suriettiva. Cardinalità dell'insieme di tutte le funzioni e delle funzioni iniettive tra due insiemi finiti.

Richiami su relazioni di equivalenza: definizione, classe di equivalenza di un elemento, insieme quoziente e proiezione naturale al quoziente; corrispondenza tra relazioni di equivalenza su un insieme e partizioni dell'insieme; corrispondenza tra funzioni definite sull'insieme quoziente e funzioni costanti sulle classi di equivalenza.

Richiami su relazioni d'ordine; assioma della scelta e lemma di Zorn (solo enunciato).

Richiami su numeri naturali, interi, razionali, reali e complessi: proprietà delle operazioni di somma e prodotto e della relazione d'ordine. Principio del buon ordinamento dei numeri naturali e principio di induzione.

Divisibilità tra numeri interi e sue proprietà; divisione con resto. Massimo comun divisore e minimo comune multiplo di due interi e loro proprietà; per ogni $a, b \in \mathbb{Z}$ si ha $a\mathbb{Z} + b\mathbb{Z} = \mathrm{mcd}(a,b)\mathbb{Z}$ e $a\mathbb{Z} \cap b\mathbb{Z} = \mathrm{mcm}(a,b)\mathbb{Z}$. Numeri primi; un numero primo divide il prodotto di due interi se e solo se divide uno dei due fattori. Teorema fondamentale dell'aritmetica; i numeri primi sono infiniti. Espressione di $\mathrm{mcd}(a,b)$ e $\mathrm{mcm}(a,b)$ in termini delle fattorizzazioni di a e di b. Algoritmo di Euclide per il calcolo del massimo comun divisore. Soluzioni intere dell'equazione $ax + by = c$.

Congruenza modulo n (intero positivo) come relazione di equivalenza su $\mathbb{Z}$; insieme quoziente $\mathbb{Z}/n\mathbb{Z}$, definizione di somma e prodotto su $\mathbb{Z}/n\mathbb{Z}$ e loro proprietà. Soluzioni di congruenze modulo n e di equazioni in $\mathbb{Z}/n\mathbb{Z}$; sistemi di congruenze e teorema cinese del resto.

Definizione di gruppo e primi esempi: gruppi additivi $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/n\mathbb{Z}$ e gruppi moltiplicativi $\mathbb{Z}^*$, $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$, $\mathbb{Z}/n\mathbb{Z}^*$ (tutti commutativi o abeliani); gruppo delle funzioni da un insieme a un gruppo; gruppo $S(X)$ delle permutazioni di un insieme X con operazione data dalla composizione di funzioni (non abeliano se $\#X > 2$). Prime proprietà: unicità dell'elemento neutro e dell'inverso di un elemento; inverso dell'inverso di un elemento e del prodotto di due elementi; in

un gruppo la moltiplicazione a sinistra o a destra per un fissato elemento è una permutazione del gruppo; leggi di cancellazione a sinistra e a destra.

Sottogruppi: definizione ed esempi; criteri per verificare se un sottoinsieme di un gruppo è un sottogruppo. Sottogruppo generato da un elemento e gruppi ciclici; un sottogruppo di un gruppo ciclico è ciclico; classificazione dei sottogruppi di $\mathbb{Z}$ e di $\mathbb{Z}/n\mathbb{Z}$. L'intersezione di sottogruppi è un sottogruppo; sottogruppo generato da un sottoinsieme di un gruppo e insiemi di generatori di un gruppo. Sottogruppi di gruppi di permutazioni; gruppo delle isometrie del piano e suo sottogruppo $O_2(\mathbb{R})$ delle isometrie che fissano l'origine; gruppo diedrale D_n come sottogruppo di $O_2(\mathbb{R})$ costituito dagli elementi che fissano un poligono regolare di n lati centrato nell'origine; descrizione puramente algebrica di D_n. Gruppo Q delle unità dei quaternioni.

Ordine di un gruppo; l'ordine di $\mathbb{Z}/n\mathbb{Z}^*$ è dato dal valore della funzione di Eulero $\varphi(n)$. Ordine di un elemento di un gruppo; l'ordine di un elemento è uguale all'ordine del sottogruppo da esso generato; un gruppo di ordine n è ciclico se e solo se contiene un elemento di ordine n; ordine di una potenza di un elemento.

Centro di un gruppo e centralizzante di un elemento: sono sottogruppi; il centro è l'intersezione dei centralizzanti; un elemento appartiene al centro se e solo se il suo centralizzante è tutto il gruppo; un gruppo è abeliano se e solo se coincide con il centro.

Omomorfismi di gruppi: definizione ed esempi; un omomorfismo preserva l'elemento neutro e le potenze di un elemento; la composizione di omomorfismi è un omomorfismo. Isomorfismi di gruppi; la composizione di due isomorfismi e l'inverso di un isomorfismo sono isomorfismi; l'isomorfismo di gruppi è una relazione di equivalenza, che preserva proprietà come essere abeliano o ciclico. Endomorfismi e automorfismi di un gruppo; gruppo degli automorfismi di un gruppo. Immagine e controimmagine di sottogruppi attraverso un omomorfismo sono sottogruppi; l'immagine di un sottogruppo generato da un sottoinsieme è generata dall'immagine del sottoinsieme; immagine e nucleo di un omomorfismo; un omomorfismo è iniettivo se e solo se il nucleo contiene solo l'elemento neutro; l'immagine di un omomorfismo iniettivo è isomorfa al gruppo di partenza. Ordine dell'immagine di un elemento attraverso un omomorfismo (iniettivo). Classificazione degli omomorfismi (iniettivi e/o suriettivi) da $\mathbb{Z}$ e da $\mathbb{Z}/n\mathbb{Z}$ verso un gruppo qualunque. Un gruppo ciclico infinito è isomorfo a $\mathbb{Z}$, un gruppo ciclico di ordine n è isomorfo a $\mathbb{Z}/n\mathbb{Z}$.

Prodotto di gruppi; il prodotto di due gruppi è abeliano se e solo se entrambi i fattori sono abeliani; teorema cinese del resto (per gruppi). Ordine di un elemento in un prodotto.

Classi laterali (sinistre e destre) di un sottogruppo in un gruppo; tutte le classi laterali di un sottogruppo hanno la stessa cardinalità del sottogruppo; le classi laterali (sinistre o destre) di un sottogruppo formano una partizione del gruppo;

descrizione della corrispondente relazione di equivalenza. Corrispondenza biunivoca tra l'insieme G/H delle classi laterali sinistre e l'insieme $H\backslash G$ delle classi laterali destre di un sottogruppo H di un gruppo G; indice di un sottogruppo. Teorema di Lagrange; un gruppo di ordine un numero primo è ciclico; teorema di Eulero e (piccolo) teorema di Fermat. Classificazione (a meno di isomorfismo) dei gruppi di ordine minore di 8.

Coniugio e automorfismi interni. Sottogruppi normali: definizione ed esempi; criteri per verificare se un sottogruppo è normale. Ogni sottogruppo di indice 2 è normale; un sottogruppo contenuto nel centro è normale; l'intersezione di sottogruppi normali è normale; la controimmagine di un sottogruppo normale attraverso un omomorfismo è normale (in particolare, il nucleo di un omomorfismo è normale); l'immagine di un sottogruppo normale attraverso un omomorfismo suriettivo è normale.

Prodotto HK di due sottogruppi H e K di un gruppo G; se H e K sono finiti, allora $\#(HK) = \frac{(\#H)(\#K)}{\#(H\cap K)}$; HK è un sottogruppo di G se e solo se $HK = KH$, vero se H o K è normale; HK è normale se H e K lo sono. Se $H \cap K = \{1\}$ e $ab = ba$ per ogni $a \in H$ e per ogni $b \in K$ (vero se $H \cap K = \{1\}$ e H e K sono normali in G), allora $HK \cong H \times K$; inoltre in tal caso $HK = G$ se $\#G = (\#H)(\#K) < \infty$.

I gruppi di permutazioni di insiemi con la stessa cardinalità sono isomorfi. Gruppo simmetrico $S_n = S(\{1, \ldots, n\})$: definizione di ciclo; cicli disgiunti commutano; ogni elemento di S_n si può scrivere in modo essenzialmente unico come prodotto di cicli disgiunti; ordine di una permutazione; coniugio in S_n; S_n è generato dalle trasposizioni. Definizione del segno di una permutazione; il segno definisce un omomorfismo da S_n al gruppo moltiplicativo $\{1, -1\}$ con nucleo il gruppo alterno A_n (permutazioni pari), sottogruppo di indice 2 di S_n (se $n > 1$); le trasposizioni sono permutazioni dispari; una permutazione è pari (rispettivamente dispari) se e solo se è prodotto di un numero pari (rispettivamente dispari) di trasposizioni, se e solo se nella rappresentazione come prodotto di cicli disgiunti ci sono un numero pari (rispettivamente dispari) di cicli di lunghezza pari. Teorema di Cayley: ogni gruppo G è isomorfo a un sottogruppo di $S(G)$.

Gruppo quoziente di un gruppo per un sottogruppo normale; se H è normale in G, la proiezione naturale da G a G/H è un omomorfismo suriettivo con nucleo H. Corrispondenza biunivoca tra i sottogruppi (normali) di un gruppo G che contengono un sottogruppo normale H e i sottogruppi (normali) di G/H. Teorema di omomorfismo per gruppi; dato H normale in G, gli omomorfismi da G/H a un altro gruppo G' sono in corrispondenza biunivoca con gli omomorfismi da G a G' il cui nucleo contiene H. Primo, secondo e terzo teorema di isomorfismo per gruppi.

Definizione di anello e primi esempi: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/n\mathbb{Z}$ (commutativi), anelli di matrici, anello degli endomorfismi di un gruppo abeliano (non commutativi in generale). Prime proprietà: unicità dell'elemento neutro rispetto al prodotto e

dell'inverso di un elemento invertibile o unità; la moltiplicazione per 0 dà 0; un anello è banale se e solo se $1 = 0$. Gruppo moltiplicativo A^* delle unità di un anello A; anelli con divisione e campi; anello $\mathbb{H}$ dei quaternioni. Anello delle funzioni da un insieme a un anello; prodotto di anelli. Divisori di zero e domini (di integrità); ogni campo è un dominio (ma non viceversa); ogni dominio finito è un campo; $\mathbb{Z}/n\mathbb{Z}$ (con $n > 0$) è un dominio o un campo se e solo se n è primo.

Sottoanelli: definizione ed esempi; criteri per verificare se un sottoinsieme di un anello è un sottoanello; l'intersezione di sottoanelli è un sottoanello; un sottoanello di un dominio è un dominio.

Omomorfismi di anelli: definizione ed esempi; un omomorfismo preserva gli elementi neutri e le potenze di un elemento; la composizione di omomorfismi è un omomorfismo. Per ogni anello A esiste un unico omomorfismo di anelli da $\mathbb{Z}$ a A. Isomorfismi di anelli; la composizione di due isomorfismi e l'inverso di un isomorfismo sono isomorfismi; l'isomorfismo di anelli è una relazione di equivalenza, che preserva proprietà come essere commutativo, dominio o campo. Immagine e controimmagine di sottoanelli attraverso un omomorfismo sono sottoanelli; l'immagine di un omomorfismo iniettivo è isomorfa all'anello di partenza.

Anello $A[X]$ dei polinomi a coefficienti in un anello A; $A[X]$ è commutativo se e solo se A lo è; A come sottoanello di $A[X]$; grado di un polinomio non nullo; se $f, g \in A[X]$ sono non nulli e A è un dominio, allora $\deg(fg) = \deg(f) + \deg(g)$; $A[X]$ è un dominio se e solo se A lo è, e in questo caso $A[X]^* = A^*$.

Campo dei quozienti (o delle frazioni) di un dominio; il campo dei quozienti di $\mathbb{Z}$ è $\mathbb{Q}$; campo delle funzioni razionali $K(X)$ (su un campo K) come campo dei quozienti di $K[X]$.

Ideali sinistri, ideali destri e ideali (bilateri): definizione ed esempi; criteri per verificare se un sottoinsieme di un anello è un ideale. Un ideale (sinistro e/o destro) è tutto l'anello se e solo se contiene una unità. La controimmagine di un ideale attraverso un omomorfismo è un ideale (in particolare, il nucleo di un omomorfismo è un ideale); l'immagine di un ideale attraverso un omomorfismo suriettivo è un ideale. L'intersezione di ideali è un ideale; ideale somma e ideale prodotto di due ideali; ideali coprimi. Ideale generato da un sottoinsieme in un anello commutativo e ideali principali; l'immagine attraverso un omomorfismo suriettivo di anelli commutativi di un ideale generato da un sottoinsieme è generata dall'immagine del sottoinsieme. Un anello commutativo A con $1 \neq 0$ è un campo se e solo se gli unici suoi ideali sono $\{0\}$ e A.

Anello quoziente di un anello per un ideale; se I è un ideale di A, la proiezione naturale da A a A/I è un omomorfismo suriettivo con nucleo I. Corrispondenza biunivoca tra gli ideali di un anello A che contengono un ideale I e gli ideali di A/I. Teorema di omomorfismo per anelli; dato I ideale di A, gli omomorfismi da A/I a un altro anello B sono in corrispondenza biunivoca con gli omomorfismi da A a B il cui nucleo contiene I. Primo teorema di isomorfismo per anelli; se I è un ideale

di A, gli anelli $(A/I)[X]$ e $A[X]/I[X]$ sono isomorfi. Secondo e terzo teorema di isomorfismo per anelli. Teorema cinese del resto per anelli commutativi; formula per $\varphi(n)$ in termini della fattorizzazione di n.

Divisibilità tra elementi di un anello commutativo; divisione con resto tra polinomi a coefficienti in un anello commutativo. Se A è un sottoanello di un anello commutativo B e $b \in B$, la funzione $A[X] \to B$, $f \mapsto f(b)$ è un omomorfismo di anelli con immagine $A[b]$, che è il più piccolo sottoanello di B contenente A e b. Radici (o zeri) di polinomi; $a \in A$ è radice di $f \in A[X]$ se e solo se $X - a$ divide f (teorema di Ruffini), quindi $A[X]/(X - a) \cong A$; $\mathbb{R}[X]/(X^2 + 1) \cong \mathbb{C}$. Se A è un dominio e $a_1, \ldots, a_n$ sono radici distinte di $f \in A[X]$, allora $\prod_{i=1}^{n}(X - a_i)$ divide f (quindi $\deg(f) \geq n$ se $f \neq 0$); se A è un dominio infinito, l'omomorfismo naturale di anelli $A[X] \to A^A$ è iniettivo.

Domini euclidei e domini a ideali principali; ogni dominio euclideo è a ideali principali; $\mathbb{Z}$, K e $K[X]$ (con K campo) sono domini euclidei. Se A è un dominio ma non un campo e $a \in A$ è un elemento non nullo e non invertibile, l'ideale (a, X) non è principale in $A[X]$; $A[X]$ è un dominio a ideali principali se e solo se $A[X]$ è un dominio euclideo se e solo se A è un campo.

Ideali primi e ideali massimali in un anello commutativo; un ideale I di A è primo (rispettivamente massimale) se e solo se A/I è un dominio (rispettivamente un campo), quindi ogni ideale massimale è primo (ma non viceversa); ideali primi e massimali di $\mathbb{Z}$. Ogni ideale $\neq A$ di un anello commutativo A è contenuto in un ideale massimale (quindi A ha almeno un ideale massimale se $1 \neq 0$).

Elementi associati in un anello commutativo; due elementi associati generano lo stesso ideale, e il viceversa è vero in un dominio. Elementi irriducibili in un dominio; un elemento $a \neq 0$ è irriducibile se (a) è primo; se inoltre il dominio è a ideali principali, a è irriducibile se e solo se (a) è primo se e solo se (a) è massimale. Se K è un campo, $f \in K[X]$ è irriducibile se e solo se $\deg(f) > 0$ e non esiste $g \in K[X]$ che divide f con $0 < \deg(g) \leq \frac{1}{2}\deg(f)$ (in particolare, se $\deg(f) = 1$ allora f è irriducibile; se f è irriducibile e $\deg(f) > 1$ allora f non ha radici; se f non ha radici e $\deg(f) = 2$ o $\deg(f) = 3$ allora f è irriducibile).

Domini a fattorizzazione unica; un dominio è a fattorizzazione unica se e solo se ogni successione crescente di ideali principali è stazionaria e ogni elemento irriducibile genera un ideale primo. Ogni dominio a ideali principali è a fattorizzazione unica. Massimo comun divisore di due elementi in un anello commutativo; se esiste, $\mathrm{mcd}(a, b)$ genera il più piccolo ideale principale contenente l'ideale (a, b) (quindi in un dominio a ideali principali $\mathrm{mcd}(a, b)$ esiste e genera l'ideale (a, b)); esistenza di $\mathrm{mcd}(a, b)$ in un dominio a fattorizzazione unica e sua espressione in termini delle fattorizzazioni di a e di b. Contenuto di un polinomio a coefficienti in un dominio a fattorizzazione unica e polinomi primitivi; il prodotto di polinomi primitivi è primitivo. Se A è un dominio a fattorizzazione unica, gli elementi irriducibili di $A[X]$ sono i polinomi costanti che sono irriducibili in A e i polinomi

primitivi che sono irriducibili in $K[X]$ (con K campo dei quozienti di A). Se A è un dominio a fattorizzazione unica, anche $A[X]$ lo è.

Campi algebricamente chiusi; un campo è algebricamente chiuso se e solo se gli unici polinomi irriducibili sono quelli di primo grado; teorema fondamentale dell'algebra (solo enunciato); fattorizzazione in $\mathbb{R}[X]$. Criterio della radice razionale per cercare le radici di un polinomio a coefficienti in un dominio a fattorizzazione unica. Un polinomio primitivo in $\mathbb{Z}[X]$ è irriducibile se esiste un numero primo p che non divide il coefficiente del termine di grado massimo e tale che il polinomio ridotto modulo p è irriducibile in $\mathbb{Z}/p\mathbb{Z}[X]$. Criterio di Eisenstein.