Programma di Algebra 1

Richiami su numeri naturali, interi, razionali e reali: proprietà delle operazioni di somma e prodotto e della relazione d'ordine.

Principio del buon ordinamento dei numeri naturali; principio di induzione (varie formulazioni) dimostrato usando il principio del buon ordinamento. Definizione di numero primo; ogni intero positivo è prodotto di numeri primi; i numeri primi sono infiniti.

Divisione con resto tra numeri interi. Massimo comun divisore di due interi. Definizione dell'insieme $n\mathbb{Z}$ dei multipli di un intero n; se $a, b \in \mathbb{Z}$, allora l'insieme dei numeri della forma $an + bm$ con $n, m \in \mathbb{Z}$ coincide con $\mathrm{mcd}(a, b)\mathbb{Z}$; a e b sono coprimi se e solo se esistono $n, m \in \mathbb{Z}$ tali che $an + bm = 1$. Un numero primo divide il prodotto di due interi se e solo se divide uno dei due fattori. Teorema fondamentale dell'aritmetica: ogni intero positivo è prodotto di numeri primi in modo unico a meno dell'ordine. Minimo comune multiplo di due interi e sua relazione con il massimo comun divisore; 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.

Richiami su insiemi e funzioni: intersezione, unione, unione disgiunta e prodotto di insiemi; 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; la cardinalità dell'insieme dei sottoinsiemi con m elementi in un insieme con n elementi è data dal coefficiente binomiale $\binom{n}{m}$.

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. 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; definizione dell'insieme degli elementi invertibili $\mathbb{Z}/n\mathbb{Z}^*$ e della funzione φ di Eulero. 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 $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$, $\mathbb{Z}/n\mathbb{Z}^*$ (tutti commutativi o abeliani); gruppo $S(A)$ delle permutazioni di un insieme A con operazione data dalla composizione di funzioni (non abeliano se $\#A > 2$). 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; 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 insieme di generatori per un gruppo. Centro di un gruppo; un gruppo è abeliano se e solo se coincide con il suo centro. 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.

Ordine di un gruppo e 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.

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. Immagine e controimmagine di sottogruppi attraverso un omomorfismo sono sottogruppi; immagine e nucleo di un omomorfismo; un omomorfismo è iniettivo se e solo se il nucleo è banale; 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) 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; ordine di un elemento in un prodotto; il prodotto di due gruppi è abeliano se e solo se entrambi i fattori sono abeliani; il prodotto di due gruppi finiti è ciclico se e solo se entrambi i fattori sono ciclici e i loro ordini sono coprimi; teorema cinese del resto (per gruppi).

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 delle classi laterali sinistre e l'insieme delle classi laterali destre di un sottogruppo; indice di un sottogruppo. Teorema di Lagrange; teorema di Eulero e (piccolo) teorema di Fermat. Un gruppo di ordine un numero primo è ciclico. Classificazione (a meno di isomorfismo) dei gruppi di ordine minore di 8.

Sottogruppi normali: definizione ed esempi; criteri per verificare se un sottogruppo è normale; coniugio e automorfismi interni; ogni sottogruppo di indice 2 è normale; il centro è un sottogruppo 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. 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.

Teorema di Cayley: ogni gruppo G è isomorfo a un sottogruppo di $S(G)$. I gruppi di permutazioni di insiemi con la stessa cardinalità sono isomorfi. Gruppo $S_n = S(\{1, \ldots, n\})$: 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. Definizione del segno di una permutazione; il segno definisce un omomorfismo da S_n al gruppo moltiplicativo $\{1, -1\}$ con nucleo A_n (permutazioni pari), sottogruppo normale di indice 2 (se $n > 1$); le trasposizioni sono permutazioni dispari; ogni elemento di S_n è prodotto di trasposizioni e ogni elemento di A_n è prodotto di 3-cicli; 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 omomorfismo e primo teorema di isomorfismo per gruppi; corrispondenza biunivoca tra i sottogruppi (normali) di un gruppo G che contengono un sottogruppo normale K e i sottogruppi (normali) di G/K; 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. Prodotto di anelli; anello delle funzioni da un insieme a un anello. Divisori di zero e domini (di integrità); ogni campo è un dominio; campo delle frazioni di un dominio.

Sottoanelli: definizione ed esempi; criteri per verificare se un sottoinsieme di un anello 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. 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, con divisione, campo o dominio. Immagine e controimmagine di sottoanelli attraverso un omomorfismo

sono sottoanelli; l'immagine di un omomorfismo iniettivo è isomorfa all'anello di partenza. Per ogni anello A esiste un unico omomorfismo da $\mathbb{Z}$ ad A.

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, $\deg(fg) = \deg(f) + \deg(g)$; $A[X]$ è un dominio se e solo se A lo è, e in questo caso $A[X]^* = A^*$.

Ideali (sinistri, destri e bilateri): definizione ed esempi; criteri per verificare se un sottoinsieme di un anello è un ideale; un ideale (sinistro 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; un anello commutativo A con $1 \neq 0$ è un campo se e solo se ha solo gli ideali banali $\{0\}$ 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.

Teorema di omomorfismo e 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; corrispondenza biunivoca tra gli ideali di un anello A che contengono un ideale I e gli ideali di A/I; terzo teorema di isomorfismo per anelli. Teorema cinese del resto per $\mathbb{Z}$ e per un anello commutativo.

Divisione con resto tra polinomi. Domini euclidei e domini a ideali principali; ogni dominio euclideo è a ideali principali; $\mathbb{Z}$, K, $K[X]$ (con K campo) sono domini a ideali principali; 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 $A[X]$.

Se A è un sottoanello di un anello commutativo B e $b \in B$, l'applicazione $A[X] \to B$, $f \mapsto f(b)$ è un omomorfismo di anelli con immagine il sottoanello $A[b]$ di B. Radici di polinomi; $a \in A$ è radice di $f \in A[X]$ se e solo se $X - a$ divide f, 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 $f \neq 0$). Principio di identità dei polinomi: due polinomi a coefficienti in un dominio infinito A sono uguali se e solo se definiscono funzioni uguali da A in A.

Ideali primi e ideali massimali in un anello commutativo; un ideale è primo (rispettivamente massimale) se e solo se l'anello quoziente è un dominio (rispettivamente un campo), quindi ogni ideale massimale è primo (ma non viceversa); ideali primi e massimali di $\mathbb{Z}$. Elementi irriducibili; un elemento non nullo a in un dominio A è irriducibile se (a) è primo; se inoltre A è a ideali principali, a è irriducibile se e solo se (a) è primo se e solo se (a) è massimale.