PROGRAMMA DI ALGEBRA 2 (seconda parte)
Corso di Laurea in Matematica A.A. 2024-2025, secondo semestre, 6 crediti
Docente: Prof. Stefano Bonzio
Tutor: Dott.ssa Francesca Tolu

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; l'anello $(A^S, +, \cdot)$ dove A è un anello e S un insieme non vuoto; $(End(G), +, \circ)$ è un anello unitario per ogni gruppo abeliano G; 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 integri (anelli unitari privi di divisori dello zero), domini (anelli integri 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 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 e da due elementi permutabili; sottoanello fondamentale di un anello unitario e caratteristica di un anello; sottoanello $B[a]$ di un anello commutativo unitario A generato da $a \in A$ e da un sottoanello B di A.

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'unione di una catena di ideali è ancora un ideale; 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 (sinistro, destro e bilatero) generato da un elemento di un anello unitario; ideali (bilateri) 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); la somma di un ideale e di un sottoanello è un sottoanello; sia A un anello (commutativo) unitario allora A è un corpo (campo) se e solo se A è privo di ideali (destri o sinistri) 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; il teorema di Krull (in un anello commutativo unitario ogni ideale proprio è contenuto in un ideale massimale); controesempio al teorema di Krull nel caso di anelli non unitari ($\mathbb{Q}$ con il prodotto banale); anelli locali (anelli commutativi unitari per i quali esiste un unico ideale massimale); un anello commutativo unitario A è locale se e solo se i suoi elementi non invertibili formano un ideale di A; $\mathbb{Z}_m$ è locale se e solo se $m = p^k$, p primo; in un anello commutativo unitario l'insieme $N(A)$ degli elementi nilpotenti è un ideale che si ottiene come l'intersezione di tutti gli ideali primi di A; gli elementi nilpotenti di $\mathbb{Z}_m$; $\mathbb{Z}_m$ è privo di elementi nilpotenti non nulli se e solo se m è il prodotto di primi distinti.

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; primo teorema di isomorfismo per anelli (sia $f : A_1 \to A_2$ un omomorfismo tra due anelli A_1 e A_2 allora esiste un omomorfismo iniettivo $\tilde{f} : A_1/\ker f \to A_2$ tale che $\tilde{f} \circ \pi = f$ che risulta essere un isomorfismo se e solo se f è suriettivo); sia $f : A_1 \to A_2$ un omomorfismo allora $A_1/\ker f \cong f(A_1)$); teorema di corrispondenza per anelli e sottoanelli (sia $f : A_1 \to A_2$ 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 $f : A_1 \to A_2$ 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 $f : A_1 \to A_2$ 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 $f : A_1 \to A_2$ 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 $f : A_1 \to A_2$ 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 $f : A_1 \to A_2$ 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 masimale 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 $f : \mathbb{Z} \to \mathbb{Z}_2$, $I_1 = 3\mathbb{Z}$ 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 $f : \mathbb{Z} \to \mathbb{Q}$, $I_2 = \{0\}$ 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 $f : A \to K$ 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 $f : A \to Q(A)$ un suo campo dei quozienti, se K è un campo e $g : A \to K$ è un omomorfismo iniettivo di anelli allora esiste un unico omomorfismo iniettivo di anelli unitari $h : Q(A) \to K$ tale che $h \circ f = g$; sia A un dominio e siano $f_1 : A \to Q(A_1)$ e $f_2 : A \to Q(A_2)$ due suoi campi dei quozienti allora esiste un isomorfismo di anelli unitari $i : Q(A_1) \to Q(A_2)$ tale che $i \circ f_1 = f_2$.

Prodotto diretto di anelli. Prodotto diretto di anelli e proprietà; il prodotto di due campi non è un campo; $U(A \times B) = U(A) \times U(B)$; dato un anello R e A e B due suoi ideali bilateri tali che $A \cap B = \{0\}$ e $R = A + B$ allora R è isomorfo a $A \times B$; caratteristica del prodotto diretto di due anelli (zero se uno dei due anelli ha caratteristica zero altrimenti uguale al minimo comune multiplo delle caratteristiche dei due anelli); ideali (primi, massimali e principali) del prodotto diretto di due anelli; se A e B sono anelli commutativi unitari a ideali principali allora il loro prodotto diretto $A \times B$ è un anello commutativo unitario a ideali principali.

Reticoli. Definizione di reticolo come insieme parzialmente ordinato che ammette sup e inf per ogni coppia di elementi; definizione di reticolo come struttura algebrica con due operazioni associative, commutative, idempotenti e che soddisfano assorbimento. Teorema di equivalenza delle due definizioni. Reticoli distributivi, limitati e completi; se un reticolo L ammette sup oppure inf di sottoinsieme arbitrari allora è completo. Esempi di reticoli e reticoli completi: reticolo dei sottoinsiemi di un insieme $\mathcal{P}(X)$, aperti e chiusi di uno spazio topologico, reticolo dei sottogruppi e dei sottogruppi normali di un gruppo, reticolo dei sottoanelli di un anello; reticolo degli ideali (sinistri, destri, bilateri) di un anello. Omomorfismi di reticoli; gli omomorfismi di reticoli preservano l'ordine. Ideali e ideali primi di un reticolo; ogni ideale di un reticolo finito è principale. Teorema di rappresentazione dei reticoli distributivi limitati (come sottoreticolo di $\mathcal{P}(X)$). Cenni di algebre di Boole.

Anelli di polinomi. Esistenza ed unicità dell'anello dei polinomi $A[x]$ su un anello commutativo unitario A. Grado di un polinomio e sue proprietà: se A è un dominio allora $A[x]$ è un dominio. Algoritmo della divisione per polinomi.
Domini fattoriali. Corrispondenza tra elementi primi ed irriducibili. Unicità della fattorizzazione. Catene di ideali principali: un dominio è fattoriale sse gli elementi irriducibili sono primi e ogni catena di ideali principali si stabilizza. Massimo Comun Divisore. Domini principali: esistenza del MCD e scrittura come combinazione lineare. Ogni dominio principale è fattoriale. Domini euclidei. Ogni dominio euclideo è principale (e quindi fattoriale). Gli interi di Gauss sono un dominio euclideo.
Divisibilità nell'anello dei polinomi e radici: teorema di Ruffini e sue applicazioni. Ogni polinomio di grado n ha al più n radici distinte. Principio di identità dei polinomi. Il gruppo moltiplicativo di un campo finito è ciclico. Teorema di Wilson. L'anello dei polinomi su un campo è un dominio euclideo. L'anello dei polinomi su un dominio in generale non è euclideo. Ideali dell'anello dei polinomi su un campo.
Fattorizzazione negli anelli di polinomi. Contenuto, p-riduzioni e il lemma di Gauss (il prodotto di polinomi primitivi è primitivo).
Polinomi irriducibili. Un polinomio è irriducibile in $A[x]$ sse è primitivo e irriducibile in $K[x]$ (K il campo dei quozienti di A). L'anello dei polinomi su un dominio fattoriale è fattoriale. Il criterio di Eisenstein. Cenni sui polinomi irriducibili in $K[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$

e $\mathbb{Z}[x]$.

Esercizi: verranno caricati nel canale Teams del corso e sulla pagina web del corso.

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.

Nota. Per gli studenti che dovessero sostenere soltanto 4 CFU sugli anelli (10 CFU totali), il programma termina con l'algoritmo della divisione per polinomi.