

Università degli studi di Trieste
Laurea triennale in matematica
anno accademico 2018–19

ALGEBRA 2 (6 CFU),

Programma del corso
docente: Alessandro Logar

Preliminari: Gruppi, anelli, campi. Richiami su definizione di gruppo, sottogruppo, classi laterali destre e sinistre. Sottogruppi normali, gruppi quoziente. Omomorfismi di gruppi. Nucleo di un omomorfismo. Omomorfismo canonico tra un gruppo e un suo quoziente. Teoremi di omomorfismo. Gruppi ciclici. Radici n -ime dell'unità come gruppi ciclici.

Definizione di anello, sottoanello, ideali destri, sinistri e bilateri. Ideali in anelli commutativi. Omomorfismi di anelli. Teoremi di omomorfismo per anelli. Ideale generato da un insieme, ideale finitamente generato, ideale principale. Campi. Ideali nei campi.

Approfondimenti sugli anelli e \mathbb{Z} . Domini d'integrità. Elementi invertibili (o unitari) di un anello (commutativo unitario). Elementi primi e irriducibili in un dominio di integrità. Elementi associati. In un dominio, se un elemento è primo, allora è irriducibile. Definizione di massimo comun divisore tra elementi di un anello. Unicità del massimo comun divisore (a meno di associati). La divisione tra elementi in \mathbb{Z} . Algoritmo di Euclide per la divisione e calcolo del massimo comun divisore in \mathbb{Z} per mezzo dell'algoritmo di Euclide. L'identità di Bezout. Gli ideali in \mathbb{Z} : l'anello degli interi è a ideali principali. Definizione di PID (dominio a ideali principali). Il gruppo degli elementi invertibili di \mathbb{Z}_n . La funzione di Eulero e il piccolo teorema di Fermat. Il teorema cinese dei resti per numeri interi. Conseguenze del teorema: se m_1, \dots, m_n sono numeri naturali a due a due coprimi e detto m il loro prodotto, allora \mathbb{Z}_m è un anello isomorfo a $\mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_n}$.

Approfondimenti sui gruppi finiti. Il teorema di Lagrange e suoi possibili inversi. Teorema di Cauchy per gruppi abeliani: G è gruppo finito e se m divide il suo ordine, allora G ha sottogruppo di ordine m . Definizione di p sottogruppo di Sylow di un gruppo finito G . I tre teoremi di Sylow (senza dimostrazione). Il teorema di Cauchy per gruppi non abeliani.

Anello dei polinomi. Costruzione dell'anello dei polinomi in una variabile $A[x]$ su un anello A (commutativo unitario). Grado di un polinomio, termine direttivo e coefficiente direttivo di un polinomio, termine noto, polinomio monico. Il prodotto di due polinomi di $A[x]$ i cui coefficienti direttivi hanno prodotto non nullo, è un polinomio il cui grado è la somma dei gradi dei due fattori. Se A è un dominio d'integrità, allora $A[x]$ è un dominio d'integrità. Un omomorfismo tra due anelli A e B si estende in unico modo ad un omomorfismo tra gli anelli dei polinomi $A[x]$ e $B[y]$ che estende l'omomorfismo dato e che manda x in y .

Omomorfismo di valutazione tra $A[x]$ e A (che, fissato $a \in A$, manda un polinomio $f(x)$ in $f(a)$). Dato un omomorfismo $\phi : A \rightarrow B$ di anelli e un elemento $b \in B$, esiste un unico omomorfismo $\Phi : A[x] \rightarrow B$ che estende ϕ e tale che $\Phi(x) = b$.

Divisione tra polinomi e conseguenze. Divisione tra polinomi: Dati $f, g \in A[x]$, se il coefficiente direttivo di f è invertibile, allora esistono, unici, $q, r \in A[x]$ tali che $g = qf + r$ con $\deg(r) < \deg(f)$.

Teorema di Ruffini: se $f \in K[x]$ (con K campo) e se $f(a) = 0$, allora f è divisibile per $x - a$. Teorema di D'Alambert: un polinomio di grado n a coefficienti in un campo ha al massimo n radici nel campo. Se K è un campo infinito e se $f, g \in K[x]$ allora $f = g$ se e solo se $f(a) = g(a)$ per ogni $a \in K$. Il massimo comun divisore tra polinomi in $K[x]$ (con K campo). Costruzione del massimo comun divisore tra polinomi (per mezzo della divisione) e identità di Bezout. $K[x]$ è PID.

Anello dei polinomi sui campi $\mathbb{Q}, \mathbb{R}, \mathbb{C}$. Ancora sugli elementi primi e irriducibili in un dominio. Se in un dominio esiste il massimo comun divisore, allora un elemento è primo se e solo se è irriducibile. Polinomi di grado 1 sono irriducibili in $K[x]$. Unicità della fattorizzazione in $K[x]$. Definizione di campo algebricamente chiuso. Un campo algebricamente chiuso è necessariamente finito. Teorema fondamentale dell'algebra: \mathbb{C} è un campo algebricamente chiuso (cenno di dimostrazione). Conseguenza: gli unici polinomi irriducibili di $\mathbb{C}[x]$ sono quelli di grado 1. Fattorizzazione di polinomi in $\mathbb{R}[x]$: gli unici polinomi irriducibili o sono di grado 1 o di grado 2 con discriminante negativo. Polinomio primitivo di $\mathbb{Q}[x]$. Ogni polinomio di $\mathbb{Q}[x]$ è associato a un polinomio primitivo. Prodotto di polinomi primitivi è primitivo. Se due polinomi primitivi sono associati, allora o sono uguali o uno è l'opposto dell'altro. Lemma di Gauss. Conseguenza: un polinomio primitivo (non costante) è irriducibile in $\mathbb{Q}[x]$ se e solo se lo è in $\mathbb{Z}[x]$. Definizione di dominio a fattorizzazione unica (UFD). Esempi: gli anelli \mathbb{Z} e $K[x]$ (con K campo) sono domini a fattorizzazione unica. Ogni polinomio primitivo in $\mathbb{Z}[x]$ è prodotto di polinomi irriducibili in $\mathbb{Z}[x]$, primitivi, essenzialmente in unico modo. L'anello $\mathbb{Z}[x]$ è un UFD. Come trovare se un polinomio di $\mathbb{Z}[x]$ (o $\mathbb{Q}[x]$) ha fattori lineari (cioè se ha una radice razionale). Criterio di irriducibilità di Eisenstein. Conseguenza: ci sono infiniti polinomi irriducibili in $\mathbb{Z}[x]$ (e quindi anche in $\mathbb{Q}[x]$) in ogni grado.

Anelli e campi. Caratteristica di un anello. Ogni anello unitario contiene una copia di \mathbb{Z} (se è di caratteristica 0) o una copia di \mathbb{Z}_m (se è di caratteristica m). Un dominio d'integrità ha caratteristica 0 o p , con p numero primo. In un anello di caratteristica p vale la formula: $(a + b)^p = a^p + b^p$. L'omomorfismo di Frobenius. Definizione di un campo perfetto (di caratteristica p): un campo in cui esistono le radici p -ime di ogni elemento, cioè se l'omomorfismo di Frobenius è un isomorfismo. I campi finiti sono perfetti. Nei campi \mathbb{Z}_p ogni elemento è radice prima di sè stesso (piccolo teorema di Fermat). Il derivato $D(f)$ di un polinomio $f \in K[x]$. L'applicazione D è lineare e inoltre vale: $D(fg) = D(f)g + fD(g)$. Se un campo K è di caratteristica 0, allora se $f \in K[x]$ e $D(f) = 0$ necessariamente

$f \in K$. Se un campo è di caratteristica p ed è perfetto, allora $D(f) = 0$ comporta che f è una potenza p -ima di un altro polinomio. Se K è di caratteristica 0 o se è perfetto, allora $f \in K[x]$ ha un fattore multiplo se e solo se il massimo comun divisore tra f e $D(f)$ non è unitario. La fattorizzazione in $\mathbb{Z}_p[x]$: i tre teoremi di Berlekamp. Costruzione della matrice Q (le cui colonne sono i resti delle potenze di x divise per il polinomio f che si vuole fattorizzare).

Polinomi in più variabili. Definizione induttiva dell'anello dei polinomi $A[x_1, \dots, x_n]$ nelle variabili x_1, \dots, x_n . Monomi e termini di un polinomio. Grado di un polinomio (globale e relativo ad una variabile). Principio di identità di polinomi. Se A è dominio, anche $A[x_1, \dots, x_n]$ è un dominio. Se A è un UFD, anche $A[x_1, \dots, x_n]$ è un UFD (cenno di dimostrazione con lemma di Gauss). Se $n > 1$, allora $A[x_1, \dots, x_n]$ non è un PID. Teoremi di estensione di un omomorfismo. Se $\phi : A \rightarrow B$ è un omomorfismo, si estende in unico modo a $\Phi : A[x_1, \dots, x_n] \rightarrow B$ tale che $\Phi(x_i) = b_i$ (con $b_i \in B$ fissati). Ideali in $K[x_1, \dots, x_n]$ (con K campo). Ideali della forma $(x_1 - a_1, \dots, x_n - a_n)$ sono massimali (dove a_1, \dots, a_n sono elementi fissati di K). Se B è un anello e A è un sottoanello di B e se b_1, \dots, b_n sono elementi fissati di B , allora si può considerare il più piccolo anello che contiene A e b_1, \dots, b_n e si indica con $A[b_1, \dots, b_n]$. L'anello $A[b_1, \dots, b_n]$ è l'immagine dell'omomorfismo di valutazione $F : A[x_1, \dots, x_n] \rightarrow B$ che manda x_i in b_i .

Estensione di campi. Se L è un campo e K è un sottocampo (si indica con $L : K$) e se b_1, \dots, b_n sono elementi di L , con $K(b_1, \dots, b_n)$ si intende il più piccolo campo che contiene L e b_1, \dots, b_n . L'estensione L di K si dice semplice se $L = K(b)$. Data un'estensione $L : K$, definizione di elemento $a \in L$ algebrico e trascendente su K . Definizione di polinomio minimo di un elemento algebrico a : è il polinomio monico, di grado minimo che si annulla in a e può essere anche visto come il generatore dell'ideale $\ker(\phi)$, dove $\phi : K[x] \rightarrow L$ è l'omomorfismo di valutazione che manda x in a . Il polinomio minimo m di un elemento $a \in L$ è irriducibile. Da questo segue che $K[a]$, essendo isomorfo a $K[x]/(m)$, è un campo. In particolare, $K[a] = K(a)$. Sia $L : K$ un'estensione. Allora L è un K -spazio vettoriale. La dimensione di L su K si indica con $[L : K]$ e si dice grado dell'estensione. Sia $L : K$ un'estensione, sia $a \in L$ algebrico su K . Allora $[K[a] : K] = n$, dove n è il grado del polinomio minimo di a su K . Definizione di estensione algebrica: quando ogni elemento di L è algebrico su K . Se $[L : K] = n$ è un numero finito, allora L è un'estensione algebrica di K . Legge della torre: Se $M : L$ e $L : K$, allora $[M : K] = [M : L] \cdot [L : K]$. Dato $f \in K[x]$ esiste un campo L tale che f ammette almeno uno zero in L . Campo di spezzamento o di riducibilità completa di un polinomio $f \in K[x]$: il più piccolo campo che contiene K e tutti gli zeri di f . Esistenza del campo di riducibilità completa. Il campo \mathbb{C} visto come $\mathbb{R}[x]/(x^2 + 1)$.

Campi finiti. Se K è un campo finito allora ha caratteristica p (numero primo) e contiene p^n elementi, dove $n = [K : \mathbb{Z}_p]$. Teorema dell'elemento primitivo: Se K è finito, allora il gruppo moltiplicativo $K \setminus \{0\}$ è un gruppo ciclico (un suo generatore si chiama elemento primitivo). Ogni campo finito è

della forma $\mathbb{Z}_p[x]/(q)$, dove q è un polinomio irriducibile di $K[x]$. Dati p primo ed $n \in \mathbb{N}$, esiste sempre un campo finito con p^n elementi. Dati due campi finiti con lo stesso numero di elementi, sono isomorfi. Pertanto, per ogni primo p ed ogni n esiste uno e un solo campo finito con p^n elementi, che si indica con $\text{GF}(p, n)$ e si dice campo di Galois.

Testi consigliati

- I. N. Herstein, *Algebra*, Roma, Editori Riuniti (1992)
- Lindsay N. Childs, *A concrete introduction to higher algebra*, third edition, Springer.
- John Rose *A course on Group theory*, Cambridge University Press.
- N. Jacobson, *Basic Algebra I*, Dover Publications.