Algebra 2
programma del corso
a.a. 2023–24 Alessandro Logar

Richiami e primi approfondimenti. Definizione di gruppo, sottogruppo, classi laterali (destre e sinistre), primi esempi di gruppi. Il teorema di Lagrange. Sottogruppi normali, gruppi quoziente, omomorfismi di gruppi. Il nucleo di un omomorfismo. L'omomorfismo canonico da un gruppo nel suo quoziente fatto rispetto ad un sottogruppo normale. Teoremi di omomorfismo. Gruppi ciclici. Esempi di gruppi ciclici. I gruppi ciclici delle radice n-ime dell'unità.
Definizione di anello. Anelli commutativi e unitari. Ideali in anelli commutativi. Primi esempi di anelli ($\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$). Anelli quoziente. Gli anelli $\mathbb{Z}_n$. Domini d'integrità. Omomorfismi tra anelli. Teoremi di omomorfismo per anelli. Ideali generati da un insieme. Ideali finitamente generati. Ideali principali. Definizione di PID (dominio ad ideali principali). Campi. Ideali nei campi.

Domini d'integrità e l'anello degli interi. Elementi invertibili in un anello. Definizione di dominio d'integrità. Elementi primi e irriducibili in un dominio d'integrità. In un dominio, se un elemento è primo, allora è anche irriducibile. Definizione di massimo comun divisore tra due elementi di un dominio. Elementi associati in un anello. Unicità del massimo comun divisore (a meno di associati). La divisione nell'anello degli interi $\mathbb{Z}$. Calcolo del massimo comun divisore in $\mathbb{Z}$ per mezzo dell'algoritmo di Euclide. L'identità di Bezout. Il gruppo degli elementi invertibili di $\mathbb{Z}_m$. La funzione di Eulero e il piccolo teorema di Fermat. Teorema cinese dei resti per numeri interi. Conseguenza/altra formulazione del teorema: se $m_1, \dots m_n$ sono numeri naturali a due a due coprimi, allora $\mathbb{Z}_m$ è isomorfo al prodotto $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_n}$, dove m è il prodotto degli m_i.

Gruppi finiti. Quando si può invertire il teorema di Lagrange? Se G è un gruppo ciclico finito e se m divide il suo ordine, G ha un sottogruppo di ordine m. Teorema di Cauchy per gruppi abeliani: dato un gruppo finito abeliano G di ordine m, se p è un primo che divide m, allora G ha un elemento di ordine p. Se G è un gruppo abeliano finito di ordine n e se m divide n, allora G ha un sottogruppo di ordine m. Definizione di p sottogruppo e di p sottogruppo di Sylow di un gruppo. I tre teoremi di Sylow (senza dim). Teorema di Cauchy per gruppi non abeliani.

L'anello dei polinomi. La costruzione dell'anello dei polinomi in una variabile (a coefficienti in un anello commutativo). Grado di un polinomio, termine/coefficiente direttivo di un polinomio, termine noto, polinomio monico. Dati due polinomi di $A[x]$, se i loro coefficienti direttivi non sono divisori dello zero, allora il grado del loro prodotto è la somma dei loro gradi. Se A è un dominio di integrità, allora $A[x]$ è anche un dominio. Teorema di estensione: dato un omomorfismo f tra due anelli A e B e fissato un elemento $b \in B$, esiste un unico omomorfismo di anelli tra $A[x]$ e B che estende f e che manda x in b. L'omomorfismo di valutazione (che manda un polinomio $f(x)$ di $A[x]$ nell'elemento $f(a)$ di A). Divisione tra polinomi: dati $f, g \in A[x]$, se il coefficiente direttivo di f è invertibile, allora esistono due polinomi q, r unici con grado di

r minore del grado di f tali che $g = qf + r$. Teorema di Ruffini: il resto della divisione di un polinomio di $K[x]$ (con K campo) quando viene diviso per $x - a$ vale $f(a)$; inoltre f è divisibile per $x - a$ se e solo se $f(a) = 0$. Teorema di D'Alambert: un polinomio di grado n a coefficienti in un campo ha al massimo n radici. Conseguenza: se il campo K dei coefficienti è infinito, allora $f = g$ se e solo se $f(a) = g(a)$ per ogni $a \in K$.

Anello dei polinomi e domini a fattorizzazione unica. Il massimo comun divisore tra polinomi in una variabile (a coefficienti in un campo). Costruzione del massimo comun divisore tra polinomi per mezzo della divisione e identità di Bezout. L'anello dei polinomi in una variabile a coefficienti su un campo è ad ideali principali (PID). Esempi. L'anello dei polinomi in una variabile a coefficienti negli interi non è invece un PID. Elementi primi e irriducibili in un dominio. Se in un dominio esiste il massimo comun divisore, allora primo è equivalente ad irriducibile. Fattorizzazione unica in irriducibili in $K[x]$ (con K campo). Unicità della fattorizzazione. Tutti i polinomi di grado 1 sono irriducibili in $K[x]$. Teorema fondamentale dell'algebra: ogni polinomio di grado almeno 1 con coefficienti nel campo complesso ha almeno una radice (nel campo complesso). Conseguenza: gli unici polinomi irriducibili in $\mathbb{C}[x]$ sono i polinomi di grado 1; ogni polinomio di grado almeno 1 è prodotto di polinomi lineari. Cenno alla dimostrazione del teorema fondamentale dell'algebra. Fattorizzazione in $\mathbb{R}[x]$. Tutti i polinomi irriducibili sono o di grado 1 o grado 2 e con discriminante negativo. Problema della comprensione dei polinomi iriducibili in $\mathbb{Q}[x]$. Definizione di polinomio primitivo in $\mathbb{Q}[x]$ (un polinomio a coefficienti interi con i coefficienti primi tra loro). Ogni polinomio di $\mathbb{Q}[x]$ è associato ad un polinomio primitivo. Il prodotto di due polinomi primitivi è primitivo. Se due polinomi primitivi sono associati, allora o sono uguali o opposti. Lemma di Gauss. Conseguenze del lemma di Gauss: un polinomio primitivo (non constante) è irriducibile in $\mathbb{Z}[x]$ se e solo se è irriducibile in $\mathbb{Q}[x]$. Definizione di dominio a fattorizzazione unica (UFD). Esempi: gli anelli $\mathbb{Z}$ e $K[x]$ (con K campo) sono UFD. Ogni polinomio primitivo in $\mathbb{Z}[x]$ è prodotto di polinomi irriducibili in $\mathbb{Z}[x]$, primitivi, essenzialmente in unico modo. L'anello dei polinomi $\mathbb{Z}[x]$ è un dominio a fattorizzazione unica.

Fattorizzazione di polinomi: prime nozioni. Metodo per trovare se un polinomio in $\mathbb{Q}[x]$ (o in $\mathbb{Z}[x]$) ha dei fattori lineari o, equivalentemente, se ha una radice razionale p/q (basta ricercare p tra i fattori del termine noto del polinomio e q tra i fattori del coefficiente direttivo del polinomio). Criterio di irriducibiltà di Eisenstein. Conseguenze: ci sono infiniti polinomi irriducibili in $\mathbb{Q}[x]$ in ogni grado.

Caratteristica di un anello. 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 ha sempre caratteristica 0 o un numero primo p. In un anello di caratteristica p (numero primo) vale la formula $(a + b)^p = a^p + b^p$. L'omomorfismo di Frobenius. Definizione di campo perfetto: un campo di caratteristica p è perfetto se l'omomorfismo di Frobenius è un isomorfismo, cioè se ogni elemento del campo ammette una radice p-ima. I campi finiti sono perfetti. Nei campi $\mathbb{Z}_p$ ogni elemento è radice p-ima di sè stesso.

Fattorizzazione di polinomi, II parte. Definizione di derivato $D(f)$ di un polinomio $f \in K[x]$ (con K campo). L'applicazione D dell'anello dei polinomi in sè è lineare e inoltre vale: $D(fg) = D(f)g + fD(g)$. Se un campo è di caratteristica zero, allora $D(f) = 0$ comporta che $f \in K$. Se un campo è di caratteristica p ed è perfetto, allora $D(f) = 0$ comporta che f è la potenza p-ima di un polinomio. Uso del massimo comun divisore tra un polinomio e il suo derivato per scoprire se il polinomio ha fattori multipli. Vale: Se il campo K è di caratteristica zero o è un campo perfetto, allora un polinomio $f \in K[x]$ ha fattori multipli se e solo se il massimo comun divisore tra f e $D(f)$ non è unitario. Problema della fattorizzazione di polinomi in $\mathbb{Z}_p[x]$. I tre teoremi di Berlekamp: dato $f \in \mathbb{Z}_p[x]$ se esiste un polinomio g tale che $1 \leq \deg(g) < \deg(f)$ e f divide $g^p - g$, allora la scomposizione $f = \mathrm{mcd}\,(f, g) \cdot \mathrm{mcd}\,(f, g-1) \cdots \mathrm{mcd}\,(f, g-(p-1))$ dà fattori effettivi di f. Costruzione del polinomio g tramite l'algebra lineare in $\mathbb{Z}_p[x]$ (le matrici Q e $Q - I$), il numero dei fattori irriducibili corrisponde alla dimensione del nucleo della matrice $Q - I$.

Polinomi in più variabili. I polinomi in più variabili, definiti induttivamente. Definizione di monomi e termini. Definizione di grado (globale e rispetto ad una variabile) di un polinomio. Principio di identità di polinomi. Se A è un dominio, anche $A[x_1, \ldots, x_n]$ è un dominio, se A è un UFD (dominio a fattorizzazione unica), anche $A[x_1, \ldots, x_n]$ è un UFD (cenno alla dim. riapplicando il lemma di Gauss). L'anello $A[x_1, \ldots, x_n]$, se $n > 1$, non è un PID. Teorema di estensione di un omomorfismo f tra due anelli A e B ad un omomorfismo F tra $A[x_1, ..., x_n]$ e B che estende f e che manda $x_1, \ldots, , x_n$ in n elementi di B fissati. Ideali in $K[x_1, \ldots, x_n]$ (con K campo). Esempi di ideali in $K[x, y]$ (con K campo). Ideali della forma $(x - a, y - b)$ con $a, b \in K$. Sono massimali. Per provarlo si usa il teorema di estensione di un omomorfismo (da $K[x, y]$ in K che fissa gli elementi di K e manda x in a e y in b) e si usa anche il teorema di divisione di polinomi.

Estensioni di anelli e di campi. Se B è un anello, se A è un sottoanello di B e se $b_1, \ldots, b_n$ sono n elementi di B fissati, allora con $A[b_1, \ldots, b_n]$ si indica il più piccolo sottoanello di B che contiene A e $b_1, \ldots, b_n$ (esiste sempre, basta prendere l'intersezione di tutti i sottoanelli di B che contengono A e $b_1, \ldots, b_n$). Se si definisce l'omomorfismo di anelli $F : A[x_1, \ldots, x_n] \longrightarrow B$ tale che $F(a) = a$ per ogni a elemento di A e $F(x_i) = b_i$, si vede che $A[b_1, ..., b_n]$ è l'immagine di F, pertanto è costituito da tutti i polinomi in $x_1, \ldots, x_n$ a coefficienti in A valutati in $b_1, \ldots, b_n$. Estensione di campi. Se L è un campo, K è un sottocampo e se $b_1, \ldots, b_n$ sono elementi di L, con $K(b_1, \ldots, b_n)$ si indica il più piccolo campo che contiene K e gli elementi $b_1, \ldots, b_n$. Si vede che $K(b_1, \ldots, b_n) = Q(K[b_1, \ldots, b_n])$ (cioè è il campo dei quozienti di $K[b_1, \ldots, b_n]$). L si dice un'estensione finitamente generata di K se L è della forma $K(b_1, \ldots, b_n)$ (con $b_1, \ldots, b_n$ elementi di L). In particolare, se $n = 1$, l'estensione si dice semplice.

Elementi algebrici e trascendenti. Se L è un campo e K è un sottocampo di L, allora un elemento a di L si dice algebrico su K se esiste un polinomio $f \in K[x]$ non nullo, tale che $f(a) = 0$. Se a non è algebrico, allora a si dice trascendente (su K).

Se a è un elemento di un campo L ed è algebrico su un campo K, allora il polinomio monico di grado minimo possibile a coefficienti in K che si annulla in a, si dice polinomio minimo di a (su K). Il polinomio minimo $m(x)$ di a si può vedere anche considerando l'omomorfismo di valutazione $F : K[x] \longrightarrow L$ (cioè tale che $F(u) = u$, se $u \in K$ e $F(x) = a$), infatti succede che $\ker(F)$ è un ideale di $K[x]$ generato proprio da $m(x)$. Inoltre, dal teorema di omomorfismo, si ha che $K[x]/(m)$ è isomorfo a $K[a]$. Si prova poi che il polinomio minimo m è irriducibile, quindi l'ideale (m) è primo e anche massimale, quindi $K[x]/(m)$ è un campo, pertanto $K[a] = K(a)$ è un campo.

Ancora sull'estensione di campi. La notazione $L : K$. Grado di un'estensione: se L è un'estensione del campo K, allora L è uno spazio vettoriale su K. Con $[L : K]$ si indica la dimensione di L come K-spazio vettoriale. Se $[L : K] = n$, si dice che l'estensione è di grado n. Data l'estensione $L : K$, sia a un elemento di L, algebrico su K. Allora vale: $[K[a] : K] = n$, dove n è il grado del polinomio minimo di a su K. Se in un'estensone $L : K$ ogni elemento di L è algebrico su K, l'estensione si dice algebrica. Se vale: $[L : K] = n$, allora L è un'estensione algebrica di K. Legge della torre: se $L : K$ e $M : L$ sono due estensioni, allora vale: $[M : K] = [M : L][L : K]$.

Campi di spezzamento. Dato un polinomio f irriducibile su un campo K, esiste un campo L che estende K e tale che f ammette uno zero in L (il campo L è definito da $K[x]/(f)$ e lo zero di f è la classe di equivalenza di x in $K[x]/(f)$). Campo di riducibilità completa (o di spezzamento) di un polinomio di $K[x]$: è il più piccolo campo che contiene K e in cui f si spezza in un prodotto di fattori lineari. Se f è un qualunque polinomio di $K[x]$, esiste sempre il campo di riducibilità completa per f (si prova per induzione sul grado di f: si scrive f come prodotto di fattori irriducibili; allora, per il risultato precedente, esiste un campo L dove uno dei fattori irriducibili di f ammette uno zero. Quindi in $L[x]$ il polinomio f si spezza nel prodotto di un polinomio lineare e un polinomio g di grado più piccolo del grado di f. Si procede analogamente con g).

Campi finiti. Se K è un campo finito, allora ha p^n elementi, dove p è la caratteristica ed n è un numero naturale. Questo segue dal fatto che K contiene $\mathbb{Z}_p$ ed è uno spazio vettoriale su $\mathbb{Z}_p$. Il teorema dell'elemento primitivo: Se K è un campo finito, allora il gruppo $K \setminus \{0\}$ rispetto al prodotto è un gruppo ciclico. Ogni campo finito è della forma $\mathbb{Z}_p[x]/(q)$ dove q è un polinomio irriducibile. Dati p primo ed n numero naturale, esiste sempre un campo finito con p^n elementi (si costruisce considerando il campo di riducibilità completa di $x^m - 1$, dove $m = p^n$). Due campi finiti con lo stesso numero di elementi, sono isomorfi. Pertanto per ogni p ed n esiste un unico campo finito con p^n elementi. Esso si chiama campo di Galois e si indica con $\mathrm{GF}(p, n)$.

Nota sui riferimenti bibliografici. Tutti gli argomenti trattati si possono trovare in uno o più dei testi qui di seguito elencati. In particolare [2] contiene buona parte delle nozioni su gruppi, anelli, polinomi in una o più variabili (capitoli 1 e 2) e su estensioni di anelli, estensione di campi, campi di riducibilità completa (cap. 4). Il testo [1] contiene i teoremi di Berlekamp e la trattazione dei campi finiti, altre tecniche per la fattorizzazione di polinomi, teorema cinese

dei resti, piccolo teorema di Fermat. Il libro [5] ha una trattazione esauriente degli argomenti relativi all'estensione di campi, elementi algebrici e trascendenti (capitoli 1, 2, 3, e 4). Il testo [3] è un buon riferimento per le nozioni di base di algebra, il testo [4] può essere utilizzato per approfondire tematiche relative alla teoria dei gruppi.

Riferimenti bibliografici

[1] L. Childs, *A concrete introduction to higer algebra* (III edizione) Springer, 2009.

[2] N. Jacobson, *basic algebra, I* Freeman and Company, 1974.

[3] I. N. Herstein, *Algebra*, Editori Riuniti, 1992.

[4] J. Rose *A course on Group theory*, Cambridge University Press, 1978.

[5] I. Stewart, *Galois Theory*, Champam & Hall, 2004.