Diario Lezioni
anno accademico 2025/26

1. Lezione 23/9/25. Introduzione al corso. Alcuni richiami. Relazioni di equivalenza e partizioni. Gruppi, sottogruppi e sottogruppi normali.

2. Lezione 25/9/25 (1 ora). Gruppi quoziente. Omomorfismi tra gruppi. Nucleo di un omomorfismo. Proiezione canonica. Richiamo dei teoremi di omomorfismo per gruppi.

3. Lezione 26/9/25. Divisione in $\mathbb{Z}$. Massimo comun divisore in $\mathbb{Z}$. Algoritmo di Euclide e identità di Bezout.
Anelli. Ideali in un anello. Ideale generato da un insieme. Ideali finitamente generati. Ideali principali.

4. Lezione 30/9/25. Omomorfismi di anelli. Teorema di omomorfismo di anelli. Campi. Gli anelli $\mathbb{Z}_m$. Il gruppo degli elementi invertibili di $\mathbb{Z}_m$. La funzione totiente di Eulero. Il teorema di Eulero e il piccolo teorema di Fermat.

5. Lezione 2/10/25 (1 ora). Esempi di applicazione del piccolo teorema di Fermat e del teorema di Eulero. Test di primalità con il piccolo teorema di Fermat.

6. Lezione 7/10/25. Il teorema cinese dei resti. Conseguenza del teorema: se $m_1, \dots, m_k$ sono numeri naturali a due a due coprimi, allora $\mathbb{Z}_{m_1 \cdots m_k} = \mathbb{Z}_{m_1} \times \cdots \times Z_{m_k}$. Gruppi finiti. Il teorema di Lagrange e il problema di invertirlo. Esempio: i gruppi ciclici. Il teorema di Cauchy (in un gruppo abeliano finito di ordine n esiste un elemento di ordine p se p è un primo che divide n).

7. Lezione 9/10/25 (1 ora). G è un gruppo abeliano finito di ordine n e se m divide n, allora esiste un sottogruppo di G di ordine m. I tre teoremi di Sylow (solo enunciato).

8. Lezione 10/10/25. Ancora sui tre teoremi di Sylow. Alcuni esempi. L'anello dei polinomi, il teorema di estensione (se $\phi : A \longrightarrow B$ è un omomorfismo di anelli e se $b \in B$ è fissato, allora esiste un unico omomorfismo di anelli $F : A[x] \longrightarrow B$ tale che F ristretto ad A sia ϕ e $F(x) = b$). L'omomorfismo di valutazione (Se A è un anello e $a \in A$ è fissato, l'applicazione $v : A[x] \longrightarrow A$ data da $v(f(x)) = f(a)$ è un omomorfismo di anelli.

9. Lezione 16/10/25 (1 ora) Divisione tra polinomi. Algoritmo di divisione, il teorema di Ruffini, il teorema di D'Alambert.

10. Lezione 17/10/25. Elementi primi e irriducibili in un dominio. In generale, un elemento primo è anche irriducibile. In $\mathbb{Z}$ e in $K[x]$ un elemento è primo

se e solo se è irriducibile. Ideali primi e massimali. in $\mathbb{Z}$ e in $K[x]$ gli ideali primi coincidono con i massimali (e sono generati da elementi irriducibili). Definizione di domini a fattorizzazione unica.

11. Lezione 21/10/25. L'anello degli interi $\mathbb{Z}$ e l'anello dei polinomi $K[x]$ sono UFD. I polinomi di grado 1 sono irriducibili in $K[x]$ (qualunque sia il campo K). Cenno al teorema fondamentale dell'algebra. Nell'anello dei polinomi $\mathbb{C}[x]$ (e in $K[x]$ se K è algebricamente chiuso), gli unici polinomi irriducibili sono i polinomi di grado 1. In $\mathbb{R}[x]$ i polinomi irriducibili sono i polinomi di grado 1 e i polinomi di grado 2 con il discriminante negativo.

12. Lezione 23/10/25 (1 ora) Analogia tra gli $\mathbb{Z}$ e $K[x]$ (con K campo). Sono entrambi PID e UFD. L'anello dei polinomi $\mathbb{Z}[x]$ non è un PID: l'ideale $(2, x)$ non può essere principale. Polinomi di $\mathbb{Q}[x]$ (e di $\mathbb{Z}[x]$) primitivi. Ogni polinomio di $\mathbb{Q}[x]$ è associato ad un polinomio primitivo. Due polinomi primitivi associati o sono uguali o uno è dato da (-1) moltiplicato per l'altro. Il prodotto di due polinomi primitivi è un polinomio primitivo.

13. Lezione 24/10/2025. Il lemma di Gauss (se un polinomio f in $\mathbb{Q}[x]$ è a coefficienti interi ed è, in $\mathbb{Q}[x]$ dato dal prodotto di due polinomi a e b, allora esistono due polinomi a coefficienti interi a_1 e b_1 tali che $f = a_1 \cdot b_1$. Conseguenze del lemma di Gauss: Un polinomio primitivo di grado maggiore o uguale ad uno è irriducibile in $\mathbb{Z}[x]$ se e solo se è irriducibile in $\mathbb{Q}[x]$. Un polinomio primitivo di grado maggiore o uguale ad uno è il prodotto, essenzialmente in unico modo, di polinomi irriducibili in $\mathbb{Z}[x]$ (necessariamente primitivi). Petanto, poiché ogni polinomio in $\mathbb{Z}[x]$ è prodotto di un numero intero per un polinomio primitivo, si vede che ogni polinomio di $\mathbb{Z}[x]$ è prodotto, in modo essenzialmente unico, di polinomi irriducibili, quindi $\mathbb{Z}[x]$ è un UFD. Come trovare se un polinomio di $\mathbb{Q}[x]$ ha fattori lineari (o, equivalentementre, ha radici razionali). Il criterio di irriducibilità di Eisenstein.

14. Lezione 28/10/2025. Dimostrazione del criterio di irriducibilità di Eisenstein. La caratteristica di un anello commutativo unitario. Ogni anello commutativo unitario contiene una copia di $\mathbb{Z}$ (caratteristica 0) o contiene una copia di $\mathbb{Z}_m$ (caratteristica m). I domini d'integrità hanno caratteristica 0 o un numero primo. In particolare i campi hanno caratteristica 0 o p. In un anello di caratteristrica p vale la formula: $(a+b)^p = a^p + b^p$. Se K è un campo di caratteristica p, si può definire l'omomorfismo di Frobenius $(a \mapsto a^p)$. Se l'omomorfismo di Frobenius è suriettivo, il campo si dice perfetto. I campi finiti sono perfetti. Il derivato di un polinomio e alcune sue proprietà. Se un campo è di caratteristica 0 e f è un polinomio, il suo derivato è zero se e solo se il polinomio è una costante. Se il campo è di caratteristica p ed è perfetto, allora un polinomio f ha derivato zero se e solo se esite un polinomio g tale che $f = g^p$.

15. Lezione 30/10/2025 (1 ora). In un campo di caratteristica 0 o in un campo di caratteristica p e perfetto, un polinomio f ha fattori multipli se e solo

se il massimo com un divisore tra f e $D(f)$ è diverso da 1 (cioè non è unitario). Studio dell'anello quoziente $K[x]/(f)$ dove K è un campo.

16. Lezione 31/10/2025. L'anello $K[x]/(f)$ è uno spazio vettoriale su K di dimensione n (dove n è il grado di f). Rappresentanti canonici di $K[x]/(f)$ (i.e. polinomi di grado $< \deg(f)$). Congruenze tra polinomi di $K[x]$. Il teorema cinese dei resti per l'anello $K[x]$. Il caso particolare in cui le congruenze sono fatte con polinomi della forma $x - \alpha_i$. Introduzione al metodo di fattorizzazione di Berlekamp. Il primo teorema di Berlekamp. Dato un polinomio f di grado d in $\mathbb{Z}_p[x]$, costruzione di un polinomio g tale che f divida $g^p - g$.

17. Lezione 4/11/2025. Introduzione all'uso di sagemath. Il metodo di Kronecker di fattorizzazione di polinomi di $\mathbb{Z}[x]$ e qualche esempio di implementazione.

18. Lezione 6/11/2025 (1 ora). Il secondo teorema di Berlekamp: la costruzione della matrice Q relativa a un polinomio $f \in \mathbb{Z}_p[x]$ (le colonne di Q sono i coefficienti dei polinomi r_j, resti della divisione di x^{jp} per f) e dimostrazione del II teorema di Berlekamp. Esempi.

19. Lezione 7/11/2025. Esempi di fattorizzazione di polinomi di $\mathbb{Z}_p[x]$ con il metodo di Berlekamp. Rappresentanti canonici di elementi di $\mathbb{Z}_p[x]/(f)$. Il terzo teorema di Berlekamp: il numero di fattori irriducibili di in polinomio $f \in \mathbb{Z}_p[x]$ coincide con la dimensione di $\ker(Q - I)$ come $\mathbb{Z}_p$-spazio vettoriale.

20. Lezione 11/11/2025. Cenno a come fattorizzare polinomi di $\mathbb{Z}[x]$ usando la fattorizzazione in $\mathbb{Z}_p[x]$. Polinomi in più variabili. Definizione dell'anello $A[x_1, \ldots, x_n]$ (anello dei polinomi in n variabili $x_1, \ldots, x_n$ a coefficienti in A). Rappresentazione di un polinomio nella forma

$$\sum_{(i_1,\ldots,i_n)\in I} a_{i1\cdots i_n} x_1^{i_1} \cdots x_n^{i_n} \quad \text{con } I \text{ insieme finito}$$

Grado di un polinomio (grado globale e grado in una singola variabile). Se A è un dominio, $A[x_1, \ldots, x_n]$ è un dominio. Cenno alla dimostrazione che se A è un UFD, allora $A[x_1, \ldots, x_n]$ è un UFD (la dimostrazione ricalca quella fatta per provare che $\mathbb{Z}[x]$ è un UFD e si basa sul lemma di Gauss). L'anello dei polinomi in più di una variabile (a coefficienti in un campo) **non** è un PID (esempio: l'ideale $(x, y) \subseteq \mathbb{Q}[x, y]$ non può essere generato da un solo polinomio).

21. Lezione 13/11/2025 (1 ora). Teorema di estensione di un omomorfismo $f : A \longrightarrow B$ tra due anelli ad un unico omomorfismo $F : A[x_1, \ldots, x_n] \longrightarrow B$ tale che $F(a) = f(a)$ per ogni $a \in A$ e $f(x_i) = b_i$ per $i = 1, \ldots, n$, dove $b_1, \ldots, b_n$ sono elementi fissati in B. Omomorfismo di valutazione. Esempi: L'ideale $(x, y) \subseteq \mathbb{Q}[x, y]$ è massimale.

22. Lezione 14/11/2025. Esempi di ideali di $K[x_1, \ldots, x_n]$. Esempi di ideali massimali di $\mathbb{Q}[x, y]$, In $K[x_1, \ldots, x_n]$ tutti gli ideali della forma $(x_1 - a_1, \ldots, x_n - a_n)$ sono massimali. Se ad esempio io campo è $\mathbb{Q}$ non è però vero che tutti gli ideali massimali sono di questa forma. Vale però: Se K è algebricamente chiuso, tutti gli ideali massimali di $K[x_1, \ldots, x_n]$ sono del tipo $(x_1 - a_1, \ldots, x_n - a_n)$ (teorema degli zeri di Hilbert, solo accennato, senza dimostrazione). La legge del doppio quoziente. Qualche esempio di ideale di $Q[x, y]$ primo ma non massimale.

23. Lezione 18/11/2025. Sapendo fattorizzare polinomi in $K[x]$, come fattorizzare polinomi in $K[x, y]$. Sia $d \in \mathbb{N}$ e sia $E : K[x, y] \longrightarrow K[x]$ data da: $E(a) = a$ per ogni $a \in K$, $E(x) = x$ e $E(y) = x^d$. Se $f, g \in K[x, y]$ sono due polinomi tali che $\deg_x f < d$ e $\deg_x g < d$ e se $E(f) = E(g)$, allora $f = g$. In questo modo si vede che E, ristretta ai polinomi di grado in x inferiore a d è iniettiva. Sia allora $f \in K[x, y]$, si supponga che sia di grado inferiore a d in x e supponiamo che f sia riducibile in $K[x, y]$, cioè $f = g_1 g_2$. Allora $E(g_1)$ è un fattore di $E(f)$. Se sappiamo fattorizzare in $K[x]$, siamo in grado di trovare $E_(g_1)$ e quindi ricostruire g_1. Con un metodo simile si possono fattorizzare polinomi di $K[x_1, \ldots, x_n]$ (si usa l'omomorfismo $E : K[x_1, \ldots, x_n] \longrightarrow K[x]$ dato da $E(a) = a$ per ogni $a \in K$, $E(x_i) = x^{d^{i-1}}$).

    Dati due anelli A e B con A sottoanello di B e dati $b_1, \ldots, b_n \in B$, il più piccolo sottoanello di B che contiene A e $b_1, \ldots, b_n$ esiste (è dato dall'intersezione di tutti i sottoanelli di B che contengono A e $b_1, \ldots, b_n$) ed è l'immagine dell'omomorfismo $\phi : A[x_1, \ldots, x_n] \longrightarrow B$ dato da $\phi(a) = a$ per ogni $a \in A$ e $\phi(x_i) = b_i$. Tale anello si indica con $A[b_1, \ldots, b_n]$. Se K ed L sono campi, con K sottocampo di L, il più piccolo sottocampo di L che contiene K e $b_1, \ldots, b_n$ esiste e si indica con $K(b_1, \ldots, b_n)$. Si vede che è il campo dei quozienti $Q(K[b_1, \ldots, b_n])$.

24. Lezione 20/11/2025 (1 ora). Estrensione di campi. Esempi di estensioni. Grado di un'estensione. Elementi algebrici e trascendenti. Polinomio minimo. Unicità del polinomio minimo. Il polinomio minimo è irriducibile.

25. Lezione 21/11/2025. Un polinomio monico irriducibile di $K[x]$ che si annulla in un elemento $a \in L$ con L estensione di K è il polinomio minimo di a su K. Se a è algebrico su K, $K[a]$ è isomorfo a $K[x]/(m(x))$, dove $m(x)$ è il polinomio minimo di a su K e quindi $K[a]$ è un campo (in particolare $K[a] = K(a)$). Esempi di costruzione di campi. Il campo dei numeri complessi ottenuto come $\mathbb{R}[i]$. Esempi di numeri algebrici (su $\mathbb{Q}$). Un esempio di estensione di anelli: $\mathbb{Q}[\sqrt{2}, \sqrt{3}] = \mathbb{Q}[\sqrt{2} + \sqrt{3}]$. In particolare, essendo $\sqrt{2} + \sqrt{3}$ algebrico su $\mathbb{Q}$, allora $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ è un campo. Il teorema della torre.

26. Lezione 25/11/2025. Ancora sul teorema della torre. Estensioni algebriche. Un'estensione finita è sempre un'estensione algebrica. Vi sono

estensioni algebriche che non sono finite. Utilizzo del teorema della torre per provare che, se $a, b \in L$ sono algebrici su un campo K, sottocampo di L, allora $K[a, b]$ è un campo, estensione finita di K e quindi è un'estensione algebrica. Più in generale, se $a_1, \ldots, a_n \in L$ sono n elementi algebrici su K, allora $K[a_1, \ldots, a_n]$ è un campo ed è un'estensione finita (e quindi algebrica) di K. Dato un polinomio $f(x) \in K[x]$ irriducibile, esiste un campo L, estensione di K tale che in L c'è una radice di $f(x)$ (il campo L è semplicemente il campo $K[x]/(f(x))$ e lo zero di $f(x)$ è $[x]$).

27. Lezione 27/11/2025 (1 ora). Campo di riducibilità completa di un polinomio. Dato un polinomio $f \in K[x]$ non costante, esiste sempre un campo L, estensione di K, tale che f ha tutte le radici in L (se f è irriducibile, un campo che contiene una radice di f è il campo $K[x]/(f)$; il risultato si prova poi per induzione sul grado di f). Esempi di costruzione di campi di riducibilità completa.

28. Lezione 2/12/2025. Campi finiti. Un campo finito è di caratteristica p con p primo. Quindi contiene $\mathbb{Z}_p$ e quindi è uno spazio vettoriale (di dimensione finita n) sul campo $\mathbb{Z}_p$. Da questo segue che un campo finito ha p^n elementi. Teorema dell'elemento primitivo: se K è un campo finito, allora il gruppo moltiplicativo $K \setminus \{0\}$ è un gruppo ciclico. Un suo generatore si chiama elemento primitivo. Una conseguenza di questo risultato è che se K è un campo finito di caratteristica p, allora esiste un polinomio q, irriducibile di grado n in $\mathbb{Z}_p[x]$, tale che K è isomorfo a $\mathbb{Z}_p[x]/(q)$.

29. Lezione 4/12/2025 (1 ora). Ancora proprietà dei campi finiti. Dati p numero primo ed $n \geq 1$, esiste un campo finito con p^n elementi (la sua costruzione si fa considerando un campo F di riducibilità completa del polinomio $x^{p^n} - x \in \mathbb{Z}[x]$ e prendendo tutti gli elementi di F che sono radici di tale polinomio.

30. Lezione 5/12/2025. Se $q \in \mathbb{Z}_p[x]$ è un polinomio irriducibile di grado n, allora q divide il polinomio $x^{p^n} - x$. (infatti $[x^{p^n} - x] = [0]$ in $\mathbb{Z}_p[x]/(q)$). Se F_1 e F_2 sono due campi finiti con lo stesso numero di elementi (p^n), allora sono isomorfi. Poiché si sa che ogni campo finito è della forma $\mathbb{Z}[x]/(q)$ con q polinomio irriducibile e poiché si conosce un esempio di campo finito K con p^n elementi (è dato, come visto, dalle soluzioni di $x^{p^n} - x$), basta provare che $\mathbb{Z}_p[x]/(q)$ è isomorfo a K. Poiché q divide $x^{p^n} - x$ e K è campo di riducibilità completa di quest'ultimo, c'è un elemento $\beta \in K$ che è radice di q. Da questo segue che $\mathbb{Z}_p[x]/(q)$ è isomorfo a K. Se $n \in \mathbb{N} \setminus \{0\}$ e p è un numero primo, si è dunque provato che esiste un unico campo finito con p^n elementi. Tale campo si chiama Campo di Galois e si indica con $G(n, p)$ o $G(p^n)$.

31. Lezione 9/12/2025. Alcuni esempi di utilizzo del programma di calcolo simbolico Sage.
Discussione esercizi.

32. Lezione 11/12/2025 (1 ora). Discussione esercizi.
33. Lezione 12/12/2025. Discussione esercizi.