

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 $\mathbb{Z}_{m_1 \dots m_k} = \mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_k}$. 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'Alembert.
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). Pertanto, 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, equivalentemente, ha radici razionali). Il criterio di irriducibilità di Eisenstein.