Calendario Lezioni

25 Settembre. Introduzione al corso. I numeri Naturali. Assiomi di Peano. Unicità dei numeri Naturali. Somma prodotto e ordinamento dei numeri Naturali e loro proprietà .

26 Settembre. La divisione col resto. Il principio del buon ordinamento. Definizione di Anello. L'anello dei numeri interi (costruzione a partire dai Naturali). Massimo Comun Divisore. Sua esistenza e unicità. Esempi ed esercizi.

27 Settembre. Risoluzione di semplici equazioni lineari negli interi. Definizione di numero primo. Il Teorema fondamentale dell'aritmetica. Nozione di classe resto. Esempi.

28 Settembre. L'anello $\mathbb{Z}/n\mathbb{Z}$ delle classi resto modulo n. Prime proprietà. Esempi. p è primo se e solo se $\mathbb{Z}/p\mathbb{Z}$ è un campo. Equazioni modulari lineari. Il teorema cinese del resto. Esercizi vari.

2 Ottobre. Il teorema cinese del resto. Fine della dimostrazione. Decomposizione in fattori primi. Il teorema fondamentale dell'aritmetica. Criteri di divisibiltà relativi a svariati interi. Esercizi e applicazioni varie.

4 Ottobre. Elementi invertibili in un anello. Il caso di $\mathbb{Z}$ e di $\mathbb{Z}/n$. La funzione ϕ di Eulero. Il calcolo di $\phi(n)$ in termini della fattorizzazione di n in primi. Esercizi e applicazioni varie.

5 Ottobre. Il teorema di Eulero-Fermat e sue generalizzazioni. Crittografia a chiave pubblica RSA. Criteri di primalità : il crivello di Eratostene, il criterio di Fermat e quello di WIlson. Esercizi e applicazioni varie.

9 Ottobre (Spinelli)

Presentazione della parte del Corso sulla Teoria dei Gruppi. Definizione di semigruppo, monoide, gruppo e gruppo abeliano. Esempi: l'insieme degli elementi invertibili di un monoide, l'automorfo di una struttura algebrica, il gruppo simmetrico su di un insieme X. Il gruppo delle trasformazioni di un rettangolo che non sia un quadrato: il gruppo di Klein (e sua presentazione tramite tabella di Cayley). Il gruppo delle trasformazioni di un poligono regolare con n lati: il gruppo diedrale D_{2n} e presentazione dei suoi elementi a partire da un ribaltamento ed una rotazione. Sottogruppi di un gruppo. Teorema di caratterizzazione dei sottogruppi di un gruppo. I sottogruppi banali di un gruppo. Sottogruppo generato da un sottoinsieme di un gruppo. Descrizione di tutti i sottogruppi di $(\mathbb{Z}, +)$. Condizione necessaria e sufficiente affinchè un sottoinsieme $H \subseteq G$ sia un sottogruppo: la relazione $\sim_H$. Descrizione delle classi di equivalenza rispetto a $\sim_H$. Classi laterali destre di un sottogruppo di un gruppo e suo trasversale destro.

10 Ottobre (Spinelli)
Teorema di Lagrange sull'ordine dei sottogruppi di un gruppo finito. Classi laterali sinistre di un sottogruppo di un gruppo. Indice di un sottogruppo di un gruppo. Congruenze. Sottogruppi normali e loro caratterizzazione. Esempi di sottogruppi normali di un gruppo. Il gruppo dei quaternioni Q_8 ed il reticolo dei suoi sottogruppi. Definizione di gruppi hamiltoniani (gruppi non-abeliani in cui ogni sottogruppo è normale) e alcune osservazioni su di essi. Gruppo quoziente G/H di un sottogruppo normale H in G ed epimorfismo canonico. Proprietà semplici degli omomorfismi tra gruppi. Nucleo e immagine di un omomorfismo. Teorema di fattorizzazione (dimostrazione da completare). Corollario: il Teorema di omomorfismo per gruppi.

11 Ottobre (Spinelli) Completamento della dimostrazione del Teorema di fattorizzazione. Soluzione di alcuni esercizi. La relazione di normalità tra sottogruppi non è transitiva. Sottogruppo degli automorfismi interni, $\mathrm{Inn}(G)$, di $\mathrm{Aut}(G)$ (che è normale) e centro, $Z(G)$, di un gruppo G: $G/Z(G)$ è isomorfo a $\mathrm{Inn}(G)$.

12 Ottobre(Spinelli) $Z(G)$ è un sottogruppo caratteristico. Immagine ed antiimmagine di un sottogruppo normale tramite un omomorfismo. Teorema di corrispondenza per i sottogruppi del gruppo quoziente. I sottogruppi di $\mathbb{Z}/\mathbb{Z}6$. Teorema del parallelogramma. Sottostruttura generata. Ancora sul sottogruppo generato da un sottoinsieme di un gruppo. Gruppi finitamente generati e gruppi ciclici. Esempi. Ordine di un elemento del gruppo.

16 Ottobre
Gruppi ciclici. Classificazione e struttura. Esistenza di un unico sottogruppo di ordine un fissato divisore dell'ordine del gruppo. Ordine di un elemento in un gruppo.
Coniugio. Il coniugio è una relazione di equivalenza. Il centro come insieme delle classi coniugate consistenti di un solo elemento. La cardinaltà di una classe coniugata divide l'ordine del gruppo.

17 Ottobre (Spinelli) Esercizi sugli ordini degli elementi di un gruppo finito e gruppi ciclici. L'automorfo di S_3 e di un gruppo ciclico.

18 Ottobre Descrizione delle classi coniugate nel gruppo dei quaternioni e nei gruppi diedrali. Il gruppo simmetrico di un insieme. Teorema di Cayley: Ogni gruppo è sottogruppo di un gruppo simmetrico. Gruppo simmetrico S_n. Nozione di permutazione ciclo. Ogni permutazione è prodotto di cicli disgiunti. Partizione associata ad una permutazione.

19 Ottobre Due permutazioni sono coniugate se e soltanto se sono hanno la stessa partizione associata. Esempio in S_4. Trasposizioni. Ogni permutazione è prodotto di trasposizioni. Segno di una permutazione. Il gruppo alterno.

Definizione di azione di un gruppo su un insieme. Nozione di orbita. Esempi.

23 Ottobre Applicazioni dell'azione di un gruppo su un insieme. Equazione delle orbite. Azioni di p-gruppi e applicazioni. Se un p gruppo finito agisce su un insieme finito X, la cardinalità dei punti fissi è congrua a quella di X modulo p. Il centro di un p-gruppo finito è non banale. Un gruppo di ordine p^2 è abeliano.

25 Ottobre Teorema di Cauchy. Primo teorema di Sylow. Normalizzatore di un sottogruppo. Secondo teorema di Sylow. Prime applicazioni.

26 Ottobre Terzo teorema di Sylow. Gruppi di ordine pq, $q^m h$ con h minore di q, di ordine qpr. Applicazioni. Non semplicità dei gruppi di ordine minore di 60. Esercizi vari sui sottogruppi di Sylow.

30 Ottobre Lezione annullata causa maltempo.

6 Novembre Classificazione dei gruppi abeliani finitamente generati. Nozione di somma diretta finita. Torsione. Parte libera. Sottogruppo di torsione, Nozione di rango di un gruppo abeliano finitamente generato. Esempi.

7 Novembre Conclusione della classificazione dei gruppi abeliani finitamente generati. Un gruppo abeliano finito è somma diretta dei suoi sottogruppi di Sylow. Un gruppo abeliano finito è somma diretta di sottogruppi ciclici di ordini $n_1, ...n_s$ con n_1 che divide n_2 che divide n_3 etc.

8 Novembre Esonero scritto sulla prima parte del corso.

9 Novembre Nozione di anello. Anelli con unità . Esempi. Anelli commutativi. Campi.Omomotfismi di anelli. Ideali. Teorema di omomorfismo per gli anelli. Ideali sinistri e destri. Algebre semplici. I quaternioni di Hamilton.

13 Novembre Ideali primi e massimali in anelli commutativi. Domini di integrità . Campo dei quozienti di un dominio di integrità .

14 Novembre L'ideale preimmagine di un ideale primo e' primo. Anello di polinomi a coefficienti in un anello commutativo A. esempi A campo e A interi. Divisione fra polinomi.

15 Novembre Massimo comunque divisore fra polinomi. algoritmo euclideo per polinomi a coefficienti in un campo. Polinomi irriducibili e ideali primi.

16 Novembre Polinomi a coefficienti interi. Contenuto. Plonami Primitivi. Il Lamma di Gauss. I polinomi primitivi irriducibili su sono irriducibili su Q? Criterio di Eisenstein.

20 Novembre Esercizi sulla divisibilità dei polinomi e applicazioni dei criteri di irriducibilità . Gruppo moltiplicativo di un campo finito. Esempio di un polinomio irriducibile in Q[x] ma riducibile modulo p per ogni p.

22 Novembre Definizione di dominio euclideo. Elementi invartibili in anelli euclidei. In un dominio euclideo ogni ideale è principale. MCD in domini euclidei. Elementi primi ed irriducibili. In un dominio euclideo un elemento è primo se e solo se è irriducibili.

23 Novembre Fattorizzazione unica in anelli euclidei. Dimostrazione della fattorizzazione unica in aneli euclidei.

27 Novembre L'anello degli interi di Gauss. Dimostrazione che tale anello è Euclideo. Primi in $\mathbb{Z}[i]$. Applicazioni. Primi che sono somma di 2 quadrati. Classificazione degli ideali primi in $\mathbb{Z}[i]$.

29 Novembre Esercizi sugli interi di Gauss. Calcolo di MCD fra interi di Gauss. Congruenze in $\mathbb{Z}[i]$con esempi ed esercizi. Elementi irriducibili in domini che non sono sono primi.

30 Novembre Definizione di dominio a fattorizzazione unica. $\mathbb{Z}[x]$ è un dominio a fattorizzazione unica. Cenni della dimostrazione del fatto che se A è a fattorizzazione unica anche A[x] lo è.

4 Dicembre Nozione di estensione di campi. Estensioni semplici trascendenti e algebriche. Estensioni algebriche finite e finitamente generate. Formula del prodotto dei grati di una catena di estensioni. Nozione di campo di spezzamento di un polinomio.

6 Dicembre Esistenza di una campo di spezzamento di un polinomio. Caratteristica di un campo. Esistenza di campi finiti. Unicità a meno di isomorfismi di una campo di spezzamento di un polinomio. Unicità a meno di isomorfismo di un campo finito di dato ordine.

7 Dicembre I numeri complessi sono un campo algebricamente hchiuso. Funzioni simmetriche elementari. Teorema di Newton sulle funzioni simmetriche.

11 Dicembre Teorema di Newton sulle funzioni simmetriche. Dettagli della dimostrazione. Polinomi irriducibile in Rx] e C[x]. Ordine del gruppo di Galois di un polinomio. Qualche esempio.

12 Dicembre Esercizi sul decomposizione di polinomi. Irriducibilità . Calcolo del gruppo di Galois di un polinomio di grado 2 o 3.

13 Dicembre Esempi di calcolo del gruppo di Galois per polinomi di grado 3. Lemma di Artin. Applicazione: la corrispondenza di Galois. Teorema dell'elemento primitivo.

14 Dicembre Costruzioni con riga e compasso. Campo dei numeri costruibili. Duplicazione del cubo. Trisezione dell'angolo.

18 Dicembre Costruzione di poligoni regolari. Numeri di Fermat. Equazioni polinomiali di grado terzo. Formula risolutiva di Cardano.

20 Dicembre Esercizi su campi, estensioni, elementi primitivi.

21 Dicembre Esercizi su calcolo di gruppi di Galois. Elementi primitivi.

15 Gennaio Esercizi di riepilogo su aspetti della seconda parte del corso.

16 Gennaio Esercizi di riepilogo su aspetti della seconda parte del corso.

17 Gennaio Esonero scritto sulla seconda parte del corso.