ALGEBRA I
ELENCO DEGLI ARGOMENTI TRATTATI DURANTE LE LEZIONI

1. MARTEDÌ 29 SETTEMBRE 2020

Breve introduzione al corso.

Applicazioni iniettive e suriettive. Applicazioni invertibili e corrispondenze biunivoche. Ogni applicazione iniettiva $X \to Y$ descrive una corrispondenza biunivoca tra X e un sottoinsieme di Y. E' vero che *l'intero è più grande della parte*? Il caso degli insiemi infiniti. Problemi con la teoria ingenua degli insiemi: l'antinomia di Russell.

Confronto di cardinalità. L'argomento diagonale di Cantor: non esistono applicazioni suriettive tra un insieme e il suo insieme delle parti. Non esiste un insieme di cardinalità massima. L'*insieme di tutti gli insiemi* è un concetto malposto. Insiemi numerabili e più che numerabili.

Assiomi di Peano. Principio di induzione e dimostrazioni per induzione. Induzione forte. Il principio di buon ordinamento e la sua relazione con il principio di induzione. Varie tecniche dimostrative equivalenti alla dimostrazione per induzione. Struttura algebrica dei numeri naturali: somma, prodotto, ordinamento. Varie proprietà dei numeri naturali.

2. MERCOLEDÌ 30 SETTEMBRE 2020

Relazioni su insiemi. Relazioni d'ordine e di equivalenza. Ordinamenti totali, buoni ordinamenti: esempi e controesempi.

Relazioni di equivalenza: esempi. Un esempio caratterizzante: la relazione di equivalenza indotta da un'applicazione. Classi di equivalenza. Partizioni. Insieme quoziente e proiezione al quoziente. Ogni relazione di equivalenza è indotta dalla sua proiezione al quoziente. Teorema di omomorfismo per applicazioni tra insiemi. Il concetto di buona definizione di applicazioni $X/\sim \to Y$. Alcuni esempi di cattiva definizione.

Costruzione di $\mathbb{Z}$ a partire da $\mathbb{N}$.

3. GIOVEDÌ 1 OTTOBRE 2020

Costruzione di $\mathbb{Z}$ e $\mathbb{Q}$ a partire da $\mathbb{N}$. (Buona definizione delle) operazioni su $\mathbb{Z}$ e $\mathbb{Q}$. Ordinamento di $\mathbb{Z}$ e $\mathbb{Q}$.

Gergo algebrico: monoidi, semigruppi. Gruppi (finiti, abeliani); anelli (commutativi, con unità). Domini di integrità. Campi. $\mathbb{Z}$ è un dominio di integrità. $\mathbb{Q}$ è un campo. Ogni semigruppo commutativo cancellativo si immerge in un gruppo; ogni dominio d'integrità si immerge in un campo.

4. VENERDÌ 2 OTTOBRE 2020

Risoluzione di esercizi. Significato di *equipotente*, X^Y.

5. MARTEDÌ 6 OTTOBRE 2020

Domini d'integrità e regola di cancellazione nel prodotto. Gruppi: l'elemento neutro è unico; un elemento che si comporta come elemento neutro con anche solo un elemento è l'elemento neutro. L'inverso di ciascun elemento è unico; un inverso destro è automaticamente anche un inverso sinistro e viceversa.

Gruppi: l'elemento neutro coincide con il proprio inverso; l'inverso dell'inverso di un elemento è l'elemento stesso; inverso del prodotto di due elementi. Sottogruppi di un gruppo: un sottoinsieme di un gruppo è un sottogruppo quando è un gruppo rispetto all'operazione ereditata. Equivalentemente, è un sottoinsieme che contiene l'elemento neutro ed è chiuso rispetto all'operazione e all'inverso. L'intersezione di sottogruppi è sempre un sottogruppo; la somma di sottogruppi (in un gruppo abeliano con notazione additiva) è un sottogruppo.

Esempi di sottogruppi in $\mathbb{Z}$: sottogruppi generati da un elemento.

Divisione euclidea in $\mathbb{N}$ e in $\mathbb{Z}$. Classificazione dei sottogruppi di $\mathbb{Z}$: ogni sottogruppo possiede un generatore ciclico. Divisori, multipli e sottogruppi di $\mathbb{Z}$: $b \in (a)$ se e solo se $(b) \subset (a)$ se e solo se a divide b. Proprietà della relazione di divisibilità. Intersezione di sottogruppi di $\mathbb{Z}$: $(a) \cap (b)$ è generato dal minimo comune multiplo di a e b. Somma di sottogruppi di $\mathbb{Z}$: $(a) + (b)$ è generato dal massimo comun divisore di a e b. Proprietà di $\mathrm{MCD}(a, b)$. Algoritmo euclideo per il calcolo del massimo comun divisore: un esempio.

6. MERCOLEDÌ 7 OTTOBRE 2020

Elementi invertibili, associati, primi, irriducibili in $\mathbb{Z}$. Ogni primo è irriducibile. Se a divide bc e $\mathrm{MCD}(a, b) = 1$, allora a divide c. Ogni irriducibile è primo. Enunciato e dimostrazione del Teorema fondamentale dell'aritmetica. Fattorizzazione unica in $\mathbb{N}$.

Applicazioni: $\sqrt{2}$ è irrazionale; $\sqrt{n}$ è razionale se e solo se n è un quadrato perfetto; $\sqrt[m]{n}$ è razionale se e solo se n è un'm.esima potenza perfetta. Esistono infiniti numeri primi.

7. GIOVEDÌ 8 OTTOBRE 2020

Quarantena. *(Aritmetica modulare; teorema cinese dei resti; piccolo teorema di Fermat. Elementi invertibili in $\mathbb{Z}/(n)$. $\mathbb{Z}/(n)$ è un dominio d'integrità se e solo se n è primo, nel qual caso è un campo.)*

8. VENERDÌ 9 OTTOBRE 2020

Quarantena. *(Risoluzione di esercizi. Calcolo esplicito dell'identità di Bézout. Criteri di divisibilità. Crivello di Eratostene. Primi della forma $4n-1$ e $6n-1$.)*

9. MARTEDÌ 13 OTTOBRE 2020

Quarantena.

10. MERCOLEDÌ 14 OTTOBRE 2020

Gruppi, sottogruppi, omomorfismi di gruppi. Sottogruppi normali. L'immagine di un omomorfismo $\phi : G \to H$ è un sottogruppo di H; il nucleo di ϕ è un sottogruppo (normale) di G. Congruenza modulo un sottogruppo $H < G$: è una relazione di equivalenza e le sue classi di equivalenza sono le classi laterali $[a] = aH, a \in G$. La classe dell'identità è il sottogruppo stesso; le classi laterali sono in corrispondenza biunivoca tra loro. Ordine di un gruppo, indice di un sottogruppo. Se G è un gruppo finito e $H < G$, allora $|G| = |H|[G : H]$; in particolare, l'ordine di un sottogruppo divide sempre l'ordine del gruppo (finito) che lo contiene.

Se $\phi : G \to H$ è un omomorfismo di gruppi e $x, y \in G$, allora $\phi(x) = \phi(y)$ se e solo se $x \equiv y \mod \ker \phi$; di conseguenza $|\text{Im } \phi| = [G : \ker \phi]$. ϕ è iniettivo se e solo se $\ker \phi = \{1\}$.

Ordine di un elemento. Se $d > 0$ è il minimo intero positivo tale che $g^d = 1$, allora $(g) = \{g^n \mid n \in \mathbb{Z}\}$ possiede esattamente d elementi. Elementi di ordine infinito. Se G è un gruppo finito, ogni suo elemento g ha ordine finito e $o(g)$ divide $|G|$; in particolare $g^{|G|} = 1$. Esempi: $na \equiv a \mod n$; $a^{\phi(n)} \equiv 1 \mod n$ quando $\text{MCD}(a, n) = 1$. Come calcolare la funzione ϕ di Eulero.

Relazioni di equivalenza su un gruppo G. Se $\sim$ è di equivalenza su G e $[a][b] = [ab]$ è una buona definizione, allora $G/\sim$ è un gruppo rispetto a tale operazione e la proiezione $\pi : G \to G/\sim$ è un omomorfismo di gruppi.

11. GIOVEDÌ 15 OTTOBRE 2020

Se $\sim$ è di equivalenza su G e $[a][b] = [ab]$ è una buona definizione, allora $G/\sim$ è un gruppo rispetto a tale operazione e la proiezione $\pi : G \to G/\sim$ è un omomorfismo di gruppi. In particolare, $N = [1]$ è un sottogruppo normale e $\sim$ è la congruenza modulo N. Quando N è normale, l'operazione di gruppo di G induce una ben definita operazione su G/N. Gruppo quoziente. Definizioni equivalenti di normalità. Ogni sottogruppo di un gruppo abeliano è normale; un sottogruppo centrale è sempre normale; ogni sottogruppo di indice 2 è normale.

Isomorfismi e gruppi isomorfi.

Teorema di omomorfismo: sia $N \lhd G$ e indichiamo con $\pi : G \to G/N$ la proiezione canonica. Se $f : G \to H$ è un omomorfismo di gruppi e $N \subset \ker f$, allora esiste un'unico omomorfismo di gruppi $F : G/N \to H$ tale che $f = F \circ \pi$. Esiste una corrispondenza biunivoca tra omomorfismi $F : G/N \to H$ e omomorfismi $f : G \to H$ tali che $N \subset \ker f$. F è iniettiva esattamente quando $N = \ker f$ e ha la stessa immagine di f. Conseguenze del teorema di omomorfismo: se $f : G \to H$ è un omomorfismo di gruppi, allora $\text{Im } f \simeq G/\ker f$. Gruppi ciclici: sono isomorfi a $(\mathbb{Z}, +)$ se infiniti e a $(\mathbb{Z}/(n), +)$ se di ordine finito n.

12. VENERDÌ 16 OTTOBRE 2020

Risoluzione degli esercizi del quarto foglio. Se H, K sono sottogruppi di G, allora $HK < G$ se e solo se $HK = KH$.

13. MARTEDÌ 20 OTTOBRE 2020

Esempi di gruppi. Gruppo ciclico e gruppo diedrale. Gruppo simmetrico e gruppo alterno. Decomposizione ciclica di una permutazione: suo ordine e sua parità. I gruppi di ordine primo sono ciclici; sottogruppi di S_3.

Lemmi: se $x^2 = 1$ per ogni $x \in G$, allora G è abeliano; se $|G|$ è pari, allora G possiede un elemento di ordine 2. Gruppi di ordine 4: sono isomorfi a C_4 o a V_4. Gruppi di ordine 6: sono isomorfi a C_6 o a $\mathrm{D}_3 = \mathrm{S}_3$. Quaternioni reali e il gruppo Q_8 delle unità dei quaternioni. Se $f : G \to H$ è un omomorfismo di gruppi allora:

- $K < G \implies f(K) < H$;
- $L < H \implies f^{-1}(L) < G$;
- $N \lhd H \implies f^{-1}(N) \lhd G$.

Se $N \lhd G$ e $\pi : G \to G/N$ è la proiezione al quoziente, esiste una corrispondenza biunivoca tra sottogruppi di G/N e sottogruppi di G che contengono N, data da $G/N > \overline{K} \mapsto \pi^{-1}(\overline{K}) < G$.

14. MERCOLEDÌ 21 OTTOBRE 2020

Ancora sulla corrispondenza tra sottogruppi di G e di G/N. Se $N < H$ sono sottogruppi normali di G, allora $G/H \simeq (G/N)/(H/N)$. Sottogruppi e quozienti del gruppo additivo $\mathbb{Z}/(n)$. Ordine degli elementi di $\mathbb{Z}/(n)$. Ordine dell'immagine di un elemento attraverso un omomorfismo (possibilmente iniettivo). Teorema di Cayley. I gruppi di ordine $2d$, con d dispari, possiedono un sottogruppo normale di indice 2. La relazione di coniugio: è una relazione di equivalenza.

15. GIOVEDÌ 22 OTTOBRE 2020

Cardinalità dell'insieme HK: $|HK| = |H| \cdot |K|/|H \cap K|$. Il centro di un gruppo non può avere indice primo. Se un gruppo possiede un elemento di ordine n, allora possiede anche elementi di ordine d per ogni d che divide n. Teorema di Cauchy per gruppi abeliani: se l'ordine di un gruppo abeliano finito G è divisibile per un primo p, allora G possiede elementi di ordine p.

Elementi coniugati e cardinalità di una classe coniugata. Elementi coniugati hanno lo stesso ordine. Gli elementi che sono coniugati solo a se stessi sono tutti e soli quelli che giacciono nel centro. Classi coniugate in S_3. Centralizzatore $Z(x)$ di un elemento $x \in G$: è un sottogruppo di G. Il numero di coniugati di x coincide con l'indice del suo centralizzatore. Equazione delle classi. Gruppi di ordine la postenza di un primo p e loro centro; i gruppi di ordine p^2 sono abeliani. Se $|G| = pq$, dove $p < q$ sono primi, e G non è abeliano allora p divide $q - 1$.

Classi coniugate in S_n (cenni).

16. VENERDÌ 23 OTTOBRE 2020

Il quinto numero di Fermat non è primo. Esistono infiniti numeri primi della forma $4k + 1$. Esistono infiniti numeri primi della forma $6k + 1$. Enunciato del Teorema di Dirichlet.

Risoluzione del quinto foglio di esercizi.

17. MARTEDÌ 27 OTTOBRE 2020

Teorema di Cauchy: una dimostrazione attraverso l'equazione delle classi.

Classi di coniugio in S_n. Sottogruppi normali di $\mathrm{S}_3, \mathrm{S}_4, \mathrm{S}_5$. Classi di coniugio in A_n. Sottogruppi normali di A_4: il gruppo A_4 non possiede sottogruppi di ordine 6. A_5 è semplice. Parità di permutazioni: il gioco del 15.

Enunciato del Teorema di Sylow. Esempi: $\mathrm{S}_3, \mathrm{S}_4, \mathrm{GL}(n, \mathbb{F}_p)$).

18. MERCOLEDÌ 28 OTTOBRE 2020

Esempi di p-sottogruppi di Sylow: $\mathrm{GL}(n, \mathbb{F}_p)$, gruppi abeliani finiti.

Automorfismi interni e sottogruppi coniugati. Normalizzatore di un sottogruppo. Il numero dei sottogruppi coniugati ad un sottogruppo dato è l'indice del suo normalizzatore. Laterali doppi e loro cardinalità. Esempi.

Enunciato completo del Teorema di Sylow: se p è un numero primo e $|G| = p^k m$ con $\mathrm{MCD}(m, p) = 1$, allora G possiede sottogruppi di ordine p^k, che sono tutti coniugati tra loro. Inoltre il numero di tali sottogruppi divide $|G|$ ed è $\equiv 1 \mod p$. Infine, se $P < G$ ha ordine una potenza di p allora P è contenuto in un sottogruppo di ordine p^k.

Dimostrazione della prima parte del Teorema di Sylow: se il gruppo finito G possiede un p-sottogruppo di Sylow P e $H < G$, allora anche H contiene un p-sottogruppo di Sylow, che si può ottenere intersecando con H un opportuno coniugato di P in G.

Ciascun gruppo finito si immerge in $\mathrm{GL}(n, \mathbb{F}_p)$ per qualche n.

19. GIOVEDÌ 29 OTTOBRE 2020

Chiarimenti sull'immersione di S_n in $\mathrm{GL}(n, K)$. Il p-Sylow di un p-gruppo finito è il gruppo stesso. Il p-Sylow il cui ordine non è multiplo di p è il sottogruppo banale. Riformulazione del risultato della lezione precedente: se G è un gruppo finito e $P < G$ un suo p-Sylow, allora un p-Sylow di un sottogruppo $H < G$ si può ottenere come $H \cap xPx^{-1}$ per un'opportuna scelta di $x \in G$. Conseguenze: ogni p-sottogruppo di G è contenuto in qualche p-Sylow di G; i p-Sylow di G sono tutti coniugati tra loro. In particolare, un p-Sylow di G è normale se e solo se è l'unico p-Sylow.

Se P è un p-Sylow di G, allora il numero dei p-Sylow di G coincide con $[G : N(P)]$, dove $N(P)$ è il normalizzatore di P in G. Classi laterali doppie PxP: se $x \in N(P)$, allora $|PxP| = |P|$; se $x \notin N(P)$, allora $|PxP|$ è una potenza di p strettamente più grande di $|P|$. Un laterale doppio PxP o è completamente contenuto in $N(P)$ o ne è completamente fuori. $|G| = |N(P)|+$ un multiplo di p^{k+1}; di conseguenza $[G : N(P)] \equiv 1 \mod p$.

Esempi: se $|G| = 15$, allora G è ciclico. Prodotto diretto di gruppi e sottogruppi. Se $|G|$ è ciclico, è prodotto diretto del suo 3-Sylow con il suo 5-Sylow, ed è quindi isomorfo a $\mathrm{C}_3 \times \mathrm{C}_5 \simeq \mathrm{C}_{15}$. Il gruppo V_4 è isomorfo a $\mathrm{C}_2 \times \mathrm{C}_2$.

20. VENERDÌ 30 OTTOBRE 2020

Ancora sul prodotto diretto: il gruppo $H \times K$ contiene due sottogruppi normali isomorfi a H e K dei quali è prodotto diretto. Risoluzione di esercizi.

21. MARTEDÌ 3 NOVEMBRE 2020

Semplicità di $\mathrm{A}_n, n \geq 5$ con una dimostrazione per induzione che usa il principio di inclusione-esclusione. Sottogruppi normali di $\mathrm{S}_n, n \geq 5$.

Gruppi che sono prodotti semidiretti di due sottogruppi. Prodotto semidiretto astratto. Il prodotto semidiretto $N \rtimes_\phi H$ è diretto se e solo se $\phi : H \to \mathrm{Aut}(N)$ è l'omomorfismo banale. Un prodotto semidiretto $N \rtimes_\phi H$ è abeliano esattamente quando N e H sono entrambi abeliani e ϕ è banale. Un gruppo non abeliano di ordine 21.

22. MERCOLEDÌ 4 NOVEMBRE 2020

Azioni di gruppi su insiemi. Due definizioni equivalenti. Azioni transitive, libere, semplicemente transitive, fedeli. Orbita e stabilizzatore di un elemento. Appartenere alla stessa orbita è una relazione di equivalenza; pertanto, se G agisce su X, X è unione disgiunta di G-orbite; lo stabilizzatore di $x \in X$ è un sottogruppo di G.

$|G.x| = [G : \mathrm{Stab}(x)]$. Un'azione di G su X è transitiva se e solo se possiede una sola orbita; è libera se e solo se $\mathrm{Stab}(x) = (1)$ per ogni $x \in X$; è fedele se e solo se $\cap_{x\in X} \mathrm{Stab}(x) = (1)$.

Esempi:

- $g.x = x$ per ogni $g \in G, x \in X$ è l'azione banale di G su X.
- $g.x = gx$ è un'azione di G su $X = G$. E' semplicemente transitiva e quindi fedele.
- $g.x = xg$ è un'azione (sinistra) di G su $X = G$ solo se G è abeliano.
- $g.x = xg^{-1}$ è un'azione di G su $X = G$.
- $g.x = gxg^{-1}$ è l'azione di G su $X = G$ per coniugio. L'orbita di x è la sua classe di coniugio; lo stabilizzatore di x è il centralizzatore $Z(x)$.
- Se $H, K < G$, $(h, k).x = hxk^{-1}$ definisce un'azione di $H \times K$ su $X = G$. L'orbita di x è il laterale doppio HxK; lo stabilizzatore di x è $\{(a, x^{-1}a^{-1}x) \mid a \in H \cap xKx^{-1}\}$. Pertanto $|\mathrm{Stab}(x)| = |H \cap xKx^{-1}|$ e $|HxK| = |H||K|/|H \cap xKx^{-1}|$.
- S_n agisce transitivamente, ma non liberamente, sull'insieme $X = \{1, 2, \ldots, n\}$. Lo stabilizzatore di ciascun i è quindi un sottogruppo di S_n di indice n.

23. GIOVEDÌ 5 NOVEMBRE 2020

Se G agisce su X e $x, y \in X$ sono tali che $y = g.x$, allora $\mathrm{Stab}(y) = g\,\mathrm{Stab}(x)g^{-1}$. In altre parole gli stabilizzatori di punti nella stessa orbita sono coniugati.

Teorema di Cauchy: terza dimostrazione. Il gruppo simmetrico S_5 non possiede sottogruppi di ordine 40. Più in generale, il gruppo simmetrico $\mathrm{S}_n, n \geq 5$, non possiede sottogruppi H di indice $2 < [\mathrm{S}_n : H] < n$. Azione per coniugio di un gruppo finito sui suoi p-Sylow: è transitiva.

Gruppi semplici abeliani: sono tutti e soli quelli di ordine primo. Gruppi semplici non abeliani: hanno i p-Sylow non normali. Se K è un gruppo semplice di ordine 60, allora è isomorfo a un sottogruppo di A_6. Un sottogruppo di A_6 di indice 6 è isomorfo a A_5. In conclusione, A_5 è l'unico gruppo semplice di ordine 60, a meno di isomorfismi.

24. VENERDÌ 6 NOVEMBRE 2020

Omomorfismi (possibilmente iniettivi) da un gruppo ciclico in un gruppo. Risoluzione di esercizi.

25. MARTEDÌ 10 NOVEMBRE 2020

Ancora sugli automorfismi di un gruppo ciclico finito.

Enunciato della classificazione dei gruppi abeliani finiti. Esempi: $\mathrm{C}_5 \times \mathrm{C}_7 \simeq \mathrm{C}_{35}$; $\mathrm{C}_{12} \times \mathrm{C}_{18} \simeq \mathrm{C}_6 \times \mathrm{C}_{36}$; $\mathrm{C}_4 \times \mathrm{C}_6 \times \mathrm{C}_8 \times \mathrm{C}_{10} \times \mathrm{C}_{12} \simeq \mathrm{C}_2 \times \mathrm{C}_2 \times \mathrm{C}_4 \times \mathrm{C}_{12} \times \mathrm{C}_{120}$. Gruppi abeliani di ordine 1000 e ordine dei loro elementi.

Se un gruppo abeliano possiede elementi di ordine m, n con $\mathrm{MCD}(m, n) = 1$, allora possiede anche elementi di ordine mn. Se un gruppo abeliano possiede elementi di ordine m, n allora possiede anche elementi di ordine $\mathrm{mcm}(m, n)$. Se in un gruppo abeliano G l'elemento $x \in G$ ha ordine massimo $o(x)$, allora $o(y)$ divide $o(x)$ per ogni $y \in G$.

Prodotto diretto (astratto) di gruppi. Gruppi che sono prodotto diretto di loro sottogruppi (anche più di due!). Se G è prodotto diretto dei suoi sottogruppi $H_1, \ldots, H_n$ allora G è isomorfo al prodotto diretto $H_1 \times \cdots \times H_n$.

Risoluzione di due esercizi.

26. MERCOLEDÌ 11 NOVEMBRE 2020

Dimostrazione dei teorema di classificazione dei gruppi abeliani finiti. Sottogruppi finiti del gruppo moltiplicativo di un campo. Lunghezza del periodo dell'espansione decimale di $1/n$, quando $\mathrm{MCD}(n, 10) = 1$.

27. GIOVEDÌ 12 NOVEMBRE 2020

Invarianti per isomorfismo di gruppi abeliani finiti.

Il problema dell'estensione: se $N \lhd G$, non è detto che G sia prodotto semidiretto di N e G/N.

Ogni applicazione lineare suriettiva di spazi vettoriale ammette un'applicazione lineare inversa a destra. Non ogni omomorfismo suriettivo di gruppi ammette un inverso destro che sia un omomorfismo di gruppi.

28. VENERDÌ 13 NOVEMBRE 2020

Risoluzione di esercizi.

29. MARTEDÌ 17 NOVEMBRE 2020

Preliminari: gruppi finitamente generati; un quoziente di un gruppo finitamente generato è ancora finitamente generato; un addendo diretto di un gruppo finitamente generato è ancora finitamente generato; gruppi finitamente generati con generatori di ordine finito hanno un numero finito di elementi.

Se G è abeliano, $N \lhd G$ e $G/N \simeq \mathbb{Z}^r$ allora $G \simeq N \times \mathbb{Z}^r$. Un gruppo abeliano finitamente generato senza elementi di ordine finito è isomorfo a $\mathbb{Z}^d$, dove d è la minima cardinalità di un insieme di generatori per G. Se G è abeliano finitamente generato, allora esiste r tale che $G \simeq \mathbb{Z}^r \times \mathrm{Tor}(G)$, dove $\mathrm{Tor}(G)$ è il sottogruppo degli elementi di ordine finito. In particolare, G è isomorfo a $\mathbb{Z}^r \times \mathbb{Z}/(d_1) \times \cdots \times \mathbb{Z}/(d_k)$, dove i $d_i \geq 1$ soddisfano d_i divide d_j se $i < j$; i numeri r, k, d_i sono univocamente individuati dalla classe di isomorfismo del gruppo G.

Anelli, anelli commutativi, anelli con unità. Omomorfismi tra anelli e tra anelli con unità. Sottoanelli (con unità) e ideali sinistri, destri, bilateri. L'immagine di un omomorfismo di anelli è un sottoanello; il nucleo di un omomorfismo di anelli è un ideale bilatero. Ideali di $\mathbb{Z}$, ideali di un campo, ideali principali. Teorema di omomorfismo per anelli. Se $f : A \to B$ è un omomorfismo di anelli, allora $\mathrm{Im}\, f \simeq A/\ker f$. Corrispondenza biunivoca tra sottoanelli (ideali sinistri, ideali destri, ideali bilateri) di A/I e sottoanelli (ideali sinistri, destri, bilateri) di A che contengono I.

30. MERCOLEDÌ 18 NOVEMBRE 2020

Ideali primi e massimali. Un anello commutativo con unità con soli ideali banali è un campo. In un anello commutativo con unità A, un ideale $I \subset A$ è massimale se e solo se il quoziente A/I è un campo; allo stesso modo, I è primo se e solo se il quoziente A/I è un dominio d'integrità; pertanto un ideale massimale è necessariamente primo. Un anello non commutativo (con unità) che ha solo ideali (bilateri) banali ma non è né un corpo, né un dominio. Ideali primi e massimali di $\mathbb{Z}$. Operazioni tra ideali: intersezione, somma e prodotto.

Polinomi a coefficienti in un anello. Struttura additiva e moltiplicativa. $A[x]$ è un anello. Grado di un polinomio. I polinomi di grado 0 sono le costanti. Grado del polinomio nullo. Omomorfismo di valutazione. Cosa accade all'omomorfismo di valutazione se l'anello non è commutativo? (risp.: non è più un omomorfismo)

31. GIOVEDÌ 19 NOVEMBRE 2020

Precisazioni su ideali primi e massimali. $I + J$ e IJ sono ideali se I, J sono ideali. $(A/I)/(J/I) \simeq A/J$ se $I \subset J \subset A$ sono ideali. Proprietà universale dell'anello di polinomi $A[x]$, quando A è un anello commutativo con unità.

Divisione euclidea tra polinomi a coefficienti in un campo. Divisione con resto di un polinomio per un polinomio monico (a coefficienti in un anello commutativo con unità). Un'applicazione: un polinomio di grado d a coefficienti in un dominio d'integrità ha al più d radici. Ideale principale generato da un elemento; ideale generato da un numero finito di elementi. Un esempio di ideale non principale in $\mathbb{Z}[x]$.

Se K è un campo, gli ideali dell'anello $K[x]$ sono tutti principali; più precisamente, ogni ideale di $K[x]$ è generato da ciascun suo elemento non nullo di grado minimo.

32. VENERDÌ 20 NOVEMBRE 2020

Definizione ed esempi di domini euclidei:

- $D = \mathbb{Z}, N(a) = |a|$;
- $D = K[x], N(p(x)) =$ grado di $p(x)$, se K è un campo;
- $D = K, N(a) = 1$ per ogni $0 \neq a \in K$, se K è un campo;
- $D = \mathbb{Z}[i], N(a + bi) = a^2 + b^2$;
- $D = \mathbb{Z}[\sqrt{-2}], N(a + b\sqrt{-2}) = a^2 + 2b^2$,
- $D = K[[x]], N(a(x)) =$ minimo k tale che x^k ha coefficiente non nullo;

Un controesempio: $N(a+b\sqrt{-3}) = a^2+3b^2$ non è una norma euclidea per $\mathbb{Z}[\sqrt{-3}]$, che anzi non possiede nessuna norma euclidea, poiché ha ideali non principali.

33. MARTEDÌ 24 NOVEMBRE 2020

Precisazioni sull'ultima lezione. L'ideale $(2, 1 + \sqrt{-3}) \subset \mathbb{Z}[\sqrt{-3}]$ non è principale; in questo anello non vale la fattorizzazione unica. Struttura di dominio euclideo dell'anello delle serie formali a coefficienti in un campo.

Riformulazione di concetti algebrici in domini a ideali principali: elementi invertibili, primi, irriducibili; elementi associati; massimo comun divisore e identità di Bézout.

Noetherianità di domini a ideali principali. Fattorizzazione di elementi non nulli nel prodotto di elementi primi. Unicità della fattorizzazione.

34. MERCOLEDÌ 25 NOVEMBRE 2020

Elementi invertibili e primi in vari domini a ideali principali:

- In un campo, ogni elemento non nullo è invertibile e non vi sono elementi primi. Più precisamente, un dominio a ideali principali è un campo se e solo se non ha primi.
- Nell'anello $\mathbb{Z}$, gli invertibili sono ± 1 e i primi sono i numeri primi (a meno del segno).

- Nell'anello $K[x]$, dove K è un campo, gli invertibili sono i polinomi costanti non nulli. Gli elementi primi sono i polinomi irriducibili; ogni polinomio di grado 1 è irriducibile, e i polinomi di grado 2 e 3 sono irriducibili se e solo se non hanno radici in K. Inoltre, i polinomi irriducibili di grado maggiore di 1 sono sicuramente privi di radici in K. Polinomi irriducibili in $\mathbb{F}_2[x], \mathbb{C}[x], \mathbb{R}[x]$.
- Nell'anello $K[[x]]$, dove K è un campo, gli invertibili sono le serie formali di termine costante non nullo, e l'unico primo, a meno di prendere associati, è x. La fattorizzazione unica dice che una serie formale di norma k si ottiene moltiplicando x^k per un invertibile.
- Nell'anello $\mathbb{Z}[i]$, gli invertibili sono $\pm 1, \pm i$ e ogni elemento primo (alias *primo di Gauss*) divide un numero primo naturale. I primi naturali $\equiv 3 \mod 4$ sono primi in $\mathbb{Z}[i]$. Si hanno le fattorizzazioni $2 = (1+i)(1-i), 5 = (2+i)(2-i)$.

35. GIOVEDÌ 26 NOVEMBRE 2020

Classificazione dei primi di Gauss. Teorema dei due quadrati. Terne pitagoriche primitive.

36. VENERDÌ 27 NOVEMBRE 2020

Fine della classificazione delle terne pitagoriche primitive. Struttura dei sottoanelli di $\mathbb{Q}$.
Risoluzione di esercizi.

37. MARTEDÌ 1 DICEMBRE 2020

Se ci fosse una quantità finita di primi $\equiv 1 \mod 4$, allora esisterebbero due quadrati positivi consecutivi. Calcolo del numero di soluzioni intere dell'equazione $a^2 + b^2 = n$, dove n è un numero naturale dato. Struttura di $K[x]/(x-a)$, dove K è un campo. $\mathbb{R}[x]/(x^2+1)$ è isomorfo al campo dei numeri complessi. $\mathbb{F}_2[x]/(x^2+x+1)$ è un campo con quattro elementi. $\mathbb{F}_2[x]/(x^3+x+1)$ è un campo con 8 elementi.

Se $f(x) \in \mathbb{K}[x]$ è un polinomio irriducibile di grado d, allora $\mathbb{F} = \mathbb{K}[x]/(f(x))$ è un campo che estende $\mathbb{K}$, e l'elemento $\alpha = [x]$ soddisfa $f(\alpha) = 0$. Il campo $\mathbb{F}$ è un $\mathbb{K}$-spazio vettoriale una cui base è data da $1, \alpha, \dots, \alpha^{d-1}$.

Una razionalizzazione inusuale:

$$\frac{1}{\sqrt[3]{4} - \sqrt[3]{2} - 1} = \frac{1}{\sqrt[3]{4} - \sqrt[3]{2} - 1} \cdot \frac{2\sqrt[3]{4} + \sqrt[3]{2} + 3}{2\sqrt[3]{4} + \sqrt[3]{2} + 3} = -\frac{2\sqrt[3]{4} + \sqrt[3]{2} + 3}{5}.$$

38. MERCOLEDÌ 2 DICEMBRE 2020

Costruzione del campo delle frazioni di un dominio d'integrità. Ogni dominio d'integrità si immerge nel suo campo delle frazioni. Concetto di dominio a fattorizzazione unica. In un dominio d'integrità noetheriano ogni elemento non nullo è prodotto di elementi irriducibili.

Se $f(x)$ è un polinomio non costante a coefficienti interi (o in un dominio a fattorizzazione unica) allora le sue radici razionali (o nel campo delle frazioni del dominio) si ottengono dividendo un divisore del termine noto di f per un divisore del coefficiente direttore di f.

Lemma di Gauss: il prodotto di polinomi primitivi (a coefficienti in un dominio a fattorizzazione unica) è un polinomio primitivo. Se D è un dominio a fattorizzazione unica e $p \in D$ è un elemento primo di D, allora p è un elemento primo anche in $D[x]$. Il contenuto del prodotto di due polinomi è il prodotto dei contenuti dei due fattori. Se un polinomio primitivo non costante $f(x) \in D[x]$ ammette una fattorizzazione non banale in $K[x]$, dove D è un dominio a fattorizzazione unica e K è il suo campo delle frazioni, allora $f(x)$ ammette una fattorizzazione non banale anche in $D[x]$. Se D è un dominio a fattorizzazione unica, allora anche $D[x]$ è un dominio a fattorizzazione unica, e i suoi elementi irriducibili sono le costanti irriducibili in D e i polinomi primitivi che sono irriducibili in $K[x]$, dove K è il campo delle frazioni di D.

Gli anelli $\mathbb{Z}[x_1, \dots, x_n]$ e $K[x_1, \dots, x_n]$, dove K è un campo, sono domini a fattorizzazione unica. Determinante di Vandermonde.

39. GIOVEDÌ 3 DICEMBRE 2020

Alcuni criteri di irriducibilità per polinomi a coefficienti interi: riduzione modulo un primo; criterio di Eisenstein; forza bruta. Il polinomio $x^4 + 4$ è riducibile in $\mathbb{Q}[x]$. Il polinomio $x^4 + 9$ è irriducibile in $\mathbb{Q}[x]$. Il polinomio $x^4 + 1$ è irriducibili in $\mathbb{Z}[x]$ ma ogni sua riduzione modulo p è riducibile.

Caratteristica di un dominio d'integrità e di un campo. Campo primo. Morfismo di Frobenius per campi di caratteristica prima. Il morfismo di Frobenius di un campo finito è un automorfismo.

Estensioni di campo e grado di un'estensione. Estensioni finite. Estensione finita di estensione finita è finita. Se $K \subset L \subset F$ sono estensioni finite, allora $[F : K] \leq [F : L][L : K]$.

40. VENERDÌ 4 DICEMBRE 2020

Se $K \subset L \subset F$ sono estensioni finite, allora $[F : K] \leq [F : L][L : K]$. Proprietà universale del campo delle frazioni di un dominio d'integrità.

Risoluzione di esercizi.

41. MERCOLEDÌ 9 DICEMBRE 2020

Elementi algebrici e trascendenti. Polinomio minimo e grado di un elemento algebrico. Proprietà del polinomio minimo. Le estensioni finite di campi sono algebriche. Somma, prodotto e inverso di elementi algebrici (non nulli) sono algebrici. Non ogni estensione algebrica è finita.

Il problema classico della costruibilità con riga e compasso. Duplicazione del cubo, rettificazione della circonferenza, quadratura del cerchio, costruzione del poligono regolare con n lati. Se α è la lunghezza di un segmento costruibile con riga e compasso, allora α è un reale algebrico su $\mathbb{Q}$ il cui grado è una potenza di 2.

42. GIOVEDÌ 10 DICEMBRE 2020

Precisazioni sulle costruzioni con riga e compasso. I reali costruibili con riga e compasso formano un sottocampo di $\mathbb{R}$ chiuso rispetto all'operazione di radice quadrata (dei suoi elementi positivi). Estensioni ciclotomiche e polinomi ciclotomici. Il p-esimo polinomio ciclotomico è irriducibile in $\mathbb{Q}[x]$. Il grado della p-esima estensione ciclotomica è $p-1$, se p è un numero primo. Il numero reale $2\cos(2\pi/n)$ giace nella n-esima estensione ciclotomica, ed è quindi un numero algebrico. Il grado di $2\cos(2\pi/p)$ è $(p-1)/2$, se p è un numero primo dispari.

Se l'n-agono regolare inscritto nella circonferenza unitaria è costruibile con riga e compasso, allora il grado dell'algebrico $2\cos(2\pi/n)$ è una potenza di 2. Pertanto, quando p è un numero primo dispari, il p-agono regolare è costruibile con riga e compasso solo se p è un primo di Fermat.

43. VENERDÌ 11 DICEMBRE 2020

Esercizi.

44. MARTEDÌ 15 DICEMBRE 2020

Campi finiti. In un campo finito con p^n elementi il polinomio $x^{p^n}-x$ si spezza nel prodotto di fattori lineari.

Campi di spezzamento. Due campi di spezzamento dello stesso polinomio sono isomorfi. Esistenza e unicità, a meno di isomorfismo, del campo con p^n elementi.

45. MERCOLEDÌ 16 DICEMBRE 2020

Se p è primo e $n>0$, allora esistono polinomi irriducibili di grado n in $\mathbb{F}_p[x]$. Se $q(x)\in\mathbb{F}_p[x]$ è irriducibile di grado d che divide n, allora $q(x)$ divide $x^{p^n}-x$ in $\mathbb{F}_p[x]$. Se $q(x)\in\mathbb{F}_p[x]$ è un irriducibile che divide $x^{p^n}-x$ in $\mathbb{F}_p[x]$, allora il grado di $q(x)$ divide n. Fattorizzazione di $x^{p^n}-x$ in $\mathbb{F}_p[x]$. Esempi.

Se $F\subset K$ sono campi finiti, allora $|K|$ è una potenza di $|F|$. Se $|K|=p^n$, allora il campo K possiede esattamente un sottocampo con p^d elementi per ciascun d che divide n. Se K è un campo finito di caratteristica p, gli elementi fissati dall'automorfismo di Frobenius $F(x):=x^p$ sono esattamente i p elementi del sottocampo primo $\mathbb{F}_p$. Se $\alpha\in K$ è una radice del polinomio $q(x)$ irriducibile in $\mathbb{F}_p[x]$, allora $F(\alpha)=\alpha^p$ è ancora radice di $q(x)$. Se $q(x)\in\mathbb{F}_p[x]$ è un irriducibile di grado d e α è una radice di $q(x)$ in un campo di spezzamento, allora le radici di $q(x)$ sono $\alpha,\alpha^p,\alpha^{p^2},\dots,\alpha^{p^{d-1}}$.

Chiacchiere vaghe sulle costruzioni infinite e sul Lemma di Zorn.

46. GIOVEDÌ 17 DICEMBRE 2020

Enunciato del Lemma di Zorn. Alcune applicazioni: ogni anello commutativo con unità possiede ideali massimali; ogni spazio vettoriale ammette una base; se X,Y sono insiemi, allora esiste un'applicazione iniettiva da X a Y o da Y a X. Ogni campo ammette una chiusura algebrica.

47. VENERDÌ 18 DICEMBRE 2020

Risoluzione di esercizi. Il campo $\mathbb{F}_9$.

48. MARTEDÌ 22 DICEMBRE 2020

Un esempio di corrispondenza di Galois. L'estensione $\mathbb{F}_p\subset\mathbb{F}_{p^{12}}$: sue estensioni intermedie e inclusioni non banali; suo gruppo di Galois; sottogruppi del gruppo di Galois e inclusioni non banali. Corrispondenza esplicita tra sottogruppi del gruppo di Galois ed estensioni intermedie. Campo fisso di un automorfismo e di un gruppo di automorfismi.

Enunciato del Teorema fondamentale della Teoria di Galois. Che cos'è un'estensione di Galois? Normalità e separabilità. Definizione di estensione normale. Esempi: $\mathbb{Q}\subset\mathbb{Q}(\sqrt{2})$ è normale, come ogni estensione di grado 2; $\mathbb{Q}\subset\mathbb{Q}(\sqrt[3]{2})$ non è normale. Normalità di estensioni ciclotomiche di $\mathbb{Q}$. Definizione di separabilità di polinomi ed estensioni.

49. GIOVEDÌ 7 GENNAIO 2021

Ancora sulla separabilità. Un polinomio a coefficienti in un campo di caratteristica 0 è sempre separabile: le estensioni di campi di caratteristica 0 sono separabili. Un polinomio a coefficienti in $\mathbb{F}_p$ è sempre separabile: le estensioni tra campi finiti sono separabili. Ogni estensione di Galois finita è un campo di spezzamento (di un polinomio separabile). Ogni campo di spezzamento (di un polinomio separabile) è un'estensione di Galois finita (per il momento senza dimostrazione). Se $F \subset K$ è un'estensione finita, allora esiste un'estensione finita $K \subset L$ tale che $F \subset L$ è di Galois; in altre parole, ogni estensione finita di campi si amplia ad un'estensione finita di Galois.

Estensioni quadratiche: (in caratteristica diversa da 2) si ottengono tutte aggiungendo la radice quadrata di un non quadrato perfetto. Esempi: $\mathbb{C}$ non ha estensioni quadratiche; l'unica (a meno di isomorfismo) estensione quadratica di $\mathbb{R}$ è $\mathbb{C}$. $\mathbb{R}$ non ha estensioni quadratiche non banali di grado dispari.

Enunciato del Teorema Fondamentale dell'Algebra. Idea della dimostrazione.

50. VENERDÌ 8 GENNAIO 2021

Dimostrazione del Teorema Fondamentale dell'Algebra: ogni 2-gruppo finito possiede un sottogruppo di indice 2. Se $\mathbb{R} \subset L$ è un'estensione finita di Galois, allora $[L : \mathbb{R}] \leq 2$.

Estensioni ciclotomiche. Se p è un primo dispari e $\zeta = e^{2\pi/p}$ allora $\mathbb{Q}(\zeta)$ è un'estensione di Galois di $\mathbb{Q}$ di grado $p-1$ e $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \simeq \mathbb{Z}/(p)^\times$.

51. MARTEDÌ 12 GENNAIO 2021

Costruibilità del p-agono regolare quando p è un primo di Fermat. I casi $p = 3, 5, 17$. L'N-agono regolare si costruisce con riga e compasso se e solo se N si ottiene moltiplicando per una potenza di 2 un prodotto di primi di Fermat distinti.

Esempi: $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$ è un'estensione di Galois di grado 2; $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ è un'estensione di grado 3 che non è di Galois; $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$ è un'estensione di Galois di grado 6, il cui gruppo di Galois è isomorfo a S_3; $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$ è un'estensione di Galois di grado 4 e il suo gruppo di Galois è isomorfo a V_4. Calcolo delle estensioni intermedie in tutti questi casi.

52. MERCOLEDÌ 13 GENNAIO 2021

Altri esempi: l'estensione $\mathbb{Q} \subset \mathbb{Q}(\sqrt{1+\sqrt{2}})$ non è di Galois; ha grado 4 e il suo gruppo di Galois ha solo due elementi. L'estensione $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2+\sqrt{2}})$ è di Galois; ha grado 4 e il suo gruppo di Galois, che permuta le quattro radici del polinomio minimo, è generato da un 4-ciclo.

Cenni sul discriminante. L'estensione, sotto mentite spoglie, $\mathbb{Q} \subset \mathbb{Q}(\cos(2\pi/7))$.

53. GIOVEDÌ 14 GENNAIO 2021

Caratterizzazione delle estensioni di Galois finite in caratteristica 0 (o comunque in regime di separabilità). Per un'estensione finita $K \subset L$ le seguenti affermazioni sono equivalenti:

(1) L è campo di spezzamento su K di un polinomio $f(x) \in K[x]$;
(2) $|\mathrm{Gal}(L/K)| = [L : K]$;
(3) $L^{\mathrm{Gal}(L/K)} = K$;
(4) $K \subset L$ è di Galois.

Abbiamo già visto che (4) $\implies$ (1).

Se $K \subset L$ è un'estensione finita, allora $|\mathrm{Gal}(L/K)| \leq [L : K]$. Se L è il campo di spezzamento su K di un polinomio (separabile) $f(x) \in K[x]$, allora $|\mathrm{Gal}(L/K)| = [L : K]$. Pertanto (1) $\implies$ (2). Se G è un gruppo finito di automorfismi del campo L e $K = L^G$, allora $[L : K] \leq |G|$.

54. VENERDÌ 15 GENNAIO 2021

Se G è un gruppo finito di automorfismi del campo L e $K = L^G$, allora $[L : K] = |G|$ e $\mathrm{Gal}(L/K) = G$. Di conseguenza (2) $\implies$ (3). Se G è un gruppo finito di automorfismi del campo L e $K = L^G$, allora il polinomio minimo su K di $\alpha \in L$ si spezza in L (e ha radici distinte!). Di conseguenza, l'estensione $K \subset L$ è normale. Scegliendo $G = \mathrm{Gal}(L/K)$, si vede che (3) $\implies$ (4).

Enunciato e dimostrazione della corrispondenza di Galois. Dimostrare che se $K \subset L$ è di Galois e $K \subset F \subset L$, allora $L^{\mathrm{Gal}(L/F)} = F$, è equivalente a dimostrare che $F \subset L$ è di Galois. Se L è campo di spezzamento su K del polinomio $f(x) \in K[x]$, allora è anche campo di spezzamento su F dello stesso polinomio.

Ultimi dettagli: se $K \subset L$ è un'estensione finita di Galois e $H_1 \subset H_2$ sono sottogruppi di $\mathrm{Gal}(L/K)$, allora $L^{H_1} \supset L^{H_2}$. Viceversa, se $K \subset F_1 \subset F_2 \subset L$, allora $\mathrm{Gal}(L/F_1) \supset \mathrm{Gal}(L/F_2)$. Se $H < \mathrm{Gal}(L/K) = G$, allora $[G : H] = [L^H : K]$. Di conseguenza, se $H_1 < H_2 < \mathrm{Gal}(L/K)$, allora $[H_2 : H_1] = [L^{H_1} : L^{H_2}]$. Non dimostro la corrispondenza tra sottogruppi normali e sottoestensioni normali.

Ancora sull'estensione $\mathbb{Q} \subset \mathbb{Q}(\cos(2\pi/7))$. Se $f(x)$ è il polinomio minimo su $\mathbb{Q}$ di $\alpha = 2\cos(2\pi/7)$, allora anche $\alpha^2 - 2 = 2\cos(4\pi/7)$ è radice di $f(x)$. In particolare $\mathbb{Q} \subset \mathbb{Q}(\alpha)$ è un'estensione di Galois.

DIPARTIMENTO DI MATEMATICA, UNIVERSITÀ DEGLI STUDI DI ROMA – "LA SAPIENZA"
E-mail address: dandrea@mat.uniroma1.it