ALGEBRA I
ELENCO DEGLI ARGOMENTI TRATTATI DURANTE LE LEZIONI

1. MERCOLEDÌ 22 SETTEMBRE 2021

Definizione di gruppo. Significato dell'associatività. L'elemento neutro è unico. L'inverso di un fissato elemento rispetto ad un'operazione associativa è unico. Notazione moltiplicativa e additiva per un gruppo. Proprietà dell'inverso: $1^{-1} = 1, (a^{-1})^{-1} = a, (ab)^{-1} = b^{-1}a^{-1}$. Potenze di un elemento: $a^m a^n = a^{m+n}, (a^m)^n = a^{mn}$.

Esempi di operazioni associative che sono e non sono strutture di gruppo. Non sono gruppi $(\mathbb{N}, +), (\mathbb{Z}, \cdot)$, le applicazioni dell'insieme $\{1, 2\}$ in se stesso rispetto alla composizione. Sono gruppi $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{R}\setminus\{0\}, \cdot)$. Gruppi simmetrici. Il gruppo simmetrico S_n possiede $n!$ elementi. Il gruppo S_3 non è abeliano: gli assiomi di gruppo non garantiscono la commutatività dell'operazione.

2. GIOVEDÌ 23 SETTEMBRE 2021

Definizione di sottogruppo. Sottogruppi banali. Sottogruppo generato da un elemento: gruppi ciclici. Il gruppo additivo $(\mathbb{Z}, +)$ è ciclico.

Sottogruppi di $(\mathbb{Z}, +)$. Per ogni $d \geq 0$, l'insieme (d) dei multipli di d è un sottogruppo additivo di $\mathbb{Z}$. Non vi sono altri sottogruppi: ogni sottogruppo $H \neq (0)$ di $\mathbb{Z}$ è generato dal suo minimo elemento positivo. Interpretazione dei concetti di divisibilità, massimo comun divisore, minimo comune multiplo attraverso i sottogruppi additivi di $\mathbb{Z}$.

Omomorfismi di gruppi. Se $f : G \to H$ è un omomorfismo di gruppi, allora $f(1) = 1, f(x^{-1}) = f(x)^{-1}$. Esempi di omomorfismi: l'identità, l'applicazione che manda tutto in 1. Automorfismi interni di un gruppo. L'esponenziale come omomorfismo $(\mathbb{R}, +) \to (\mathbb{R}^\times, \cdot)$.

Nucleo e immagine di un omomorfismo $f : G \to H$. Il nucleo $\ker f$ è un sottogruppo di G, mentre l'immagine $\mathrm{Im}\, f$ è un sottogruppo di H.

3. LUNEDÌ 27 SETTEMBRE 2021

Un omomorfismo $f : G \to H$ è suriettivo quando $\mathrm{Im}\, f = H$ ed è iniettivo quando $\ker f = (1)$; più precisamente $f(x) = f(y)$ se e solo se $x^{-1}y \in \ker f$.

Congruenza modulo un sottogruppo: è una relazione di equivalenza. Classi di congruenza modulo H: la classe di congruenza di $x \in G$ è la classe laterale sinistra $[x] = xH = \{xh \,|\, h \in H\}$. Ogni classe laterale di H in G ha la stessa cardinalità di H; indice di un sottogruppo. Teorema di Lagrange: se G è un gruppo finito e $H < G$, allora $|G| = |H|[G : H]$. In particolare, $|H|$ divide $|G|$.

L'omomorfismo $f : (\mathbb{Z}, +) \to G$ definito da $f(n) = x^n$, dove $x \in G$. La sua immagine è il sottogruppo generato da x. Elementi di ordine infinito e finito. L'ordine di un elemento è la cardinalità del sottogruppo che genera. Se x ha ordine finito d, allora $(x) = \{1, x, \ldots, x^{d-1}\}$. Se G è un gruppo finito e $x \in G$, allora x ha ordine finito che divide $|G|$.

Sottogruppi normali. Se $f : G \to H$ è un omomorfismo di gruppi, allora $\ker f$ è un sottogruppo normale di G e si scrive $\ker f \lhd G$. Ogni sottogruppo di un gruppo abeliano è normale. Un sottogruppo non normale di S_3.

4. MARTEDÌ 28 SETTEMBRE 2021

Riassunto della lezione precedente. Che vuol dire $x^{30} = 1$? Sono affermazioni equivalenti: $x^n = 1$; l'ordine di x divide n. Insieme quoziente G/H. Che vuol dire verificare la buona definizione dell'operazione $[x][y] = [xy]$?

Aritmetica modulare. Congruenza in $\mathbb{Z}$ modulo il sottogruppo $\mathbb{Z}/(n)$. La somma ben definisce un'operazione sull'insieme $\mathbb{Z}/(n)$: è automaticamente un'operazione di gruppo. Nella verifica della buona definizione si utilizza la commutatività della somma.

Se x è un elemento del gruppo finito G, l'ordine di x divide $|G|$. Che cosa vuol dire nel gruppo $\mathbb{Z}/(n)$? Nulla di interessante: $nx \equiv 0 \mod n$.

Anche la moltiplicazione in $\mathbb{Z}$ ben definisce un'operazione (associativa, commutativa, dotata di elemento neutro) su $\mathbb{Z}/(n)$. Gruppo moltiplicativo degli invertibili di $\mathbb{Z}/(n)$. Un elemento $[a] \in \mathbb{Z}/(n)$ è moltiplicativamente invertibile esattamente quando $\mathrm{MCD}(a, n) = 1$. $\mathbb{Z}/(n)^\times = \{[a] \,|\, \mathrm{MCD}(a, n) = 1\}$ è un gruppo rispetto alla moltiplicazione. Funzione di Eulero: $\phi(n) = |\mathbb{Z}/(n)^\times|$. Se p è un numero primo, $\phi(p) = p - 1$. $\phi(6) = 2, \phi(8) = 4, \phi(15) = 8$.

Teorema di Eulero: se $\mathrm{MCD}(a, n) = 1$, allora $a^{\phi(n)} \equiv 1 \mod n$. Piccolo teorema di Fermat: se p è primo e a è intero, allora $a^p \equiv a \mod p$.

Se $N \lhd G$, allora $[x][y] = [xy]$ ben definisce un'operazione sull'insieme quoziente G/N: questa operazione costituisce una struttura di gruppo. Gruppo quoziente. Viceversa, se $H < G$ e $[x][y] = [xy]$ è ben definita, allora G/H è un gruppo, $\pi : G \to G/H$ è un omomorfismo di gruppi e quindi $H = \ker \pi$ è un sottogruppo normale di G.

L'omomorfismo $\mathrm{sgn} : \mathrm{S}_n \to \{\pm 1\}$. Il sottogruppo alterno $\mathrm{A}_n = \ker \mathrm{sgn}$ costituito da tutte e sole le permutazioni pari è un sottogruppo normale di S_n.

5. MERCOLEDÌ 29 SETTEMBRE 2021

Decomposizione di una permutazione nel prodotto disgiunto di permutazioni cicliche; unicità e non unicità della notazione ciclica. Trasposizioni e k-cicli. Ordine di un k-ciclo, ordine di una permutazione. Sottogruppi di S_3: quali sono normali? Classi laterali di $\langle(12)\rangle$ in S_3; classi laterali di A_3 in S_3. L'operazione di gruppo in S_3 non induce una struttura di gruppo sull'insieme quoziente $\mathrm{S}_3/\langle(12)\rangle$. Classi laterali destre e sinistre.

Alcune caratterizzazioni della normalità: un sottogruppo $H < G$ è normale esattamente quando $aH = Ha$ per ogni scelta di $a \in G$. Equivalentemente, $H < G$ è normale quando ogni suo laterale sinistro è anche un laterale destro (e viceversa).

Se $f : G \to H$ è un omomorfismo di gruppi, allora $|\mathrm{Im}\, f| = [G : \ker f]$; in particolare, se G è finito, allora $|G| = |\mathrm{Im}\, f| \cdot |\ker f|$. Descrizione degli omomorfismi additivi $\mathbb{Z}/(46) \to \mathbb{Z}/(15)$.

6. GIOVEDÌ 30 SETTEMBRE 2021

Omomorfismi, isomorfismi, automorfismi. Il gruppo $\mathrm{Aut}(G)$ degli automorfismi di un gruppo G. Gruppo moltiplicativo degli invertibili di un anello con unità. Il gruppo generale lineare $\mathrm{GL}_n(\mathbb{K})$ e il suo sottogruppo speciale $\mathrm{SL}_n(\mathbb{K})$.

Prodotto diretto di gruppi: definizione, proprietà. Finitezza e abelianità di un prodotto diretto di gruppi. Esempi: $\mathbb{Z}/(2) \times \mathbb{Z}/(2)$ è isomorfo al gruppo di Klein V; $\mathbb{Z}/(2) \times \mathbb{Z}/(3)$ è ciclico di ordine 6.

Prodotti diretti di sottogruppi: definizione. Se G è prodotto diretto di suoi sottogruppi normali $H.K$, allora è isomorfo a $H \times K$. Esempi: V è isomorfo a $\mathbb{Z}/(2) \times \mathbb{Z}/(2)$; il gruppo ciclico di ordine 6 è isomorfo a $\mathbb{Z}/(2) \times \mathbb{Z}/(3)$. Omomorfismi $G \to H_1 \times H_2$. Enunciato del teorema di omomorfismo.

7. LUNEDÌ 4 OTTOBRE 2021

Risoluzione di esercizi. Si ha l'identità $\mathrm{MCD}(a,b)\,\mathrm{mcm}(a,b) = ab$.

8. MARTEDÌ 5 OTTOBRE 2021

Teorema di omomorfismo per gruppi. Omomorfismi $\mathbb{Z}/(10) \to \mathbb{Z}/(10)$. Teorema cinese dei resti: due modi per individuare le soluzioni di un sistema di congruenze. Corrispondenza tra sottogruppi di G/N e sottogruppi di G che contengono N, quando $N \lhd G$.

9. MERCOLEDÌ 6 OTTOBRE 2021

Corrispondenza tra sottogruppi di G/N e sottogruppi di G che contengono N, quando $N \lhd G$. La normalità è preservata. Esempi: sottogruppi di $\mathbb{Z}/(10)$.

Isometrie lineari di $\mathbb{R}^n$ e matrici ortogonali. Determinante di matrici ortogonali. I gruppi $\mathrm{O}(n)$ e $\mathrm{SO}(n)$. Gli elementi di $\mathrm{O}(2)$: rotazioni e simmetrie ortogonali rispetto a rette. Composizione di due simmetrie ortogonali.

Gruppi ciclici e diedrali: definizione, ordine, elementi. Tavola moltiplicativa del gruppo diedrale.

10. GIOVEDÌ 7 OTTOBRE 2021

Azioni di gruppi su insiemi. Azioni fedeli. Gruppi di trasformazioni. Teorema di Cayley: ogni gruppo è (isomorfo a) un sottogruppo di un gruppo di permutazioni.

Ogni isometria di uno spazio vettoriale reale euclideo che manda 0 in 0 è lineare; ogni isometria di uno spazio vettoriale reale euclideo è affine. Classificazione delle isometrie del piano. Classificazione dei gruppi finiti di isometrie del piano.

11. LUNEDÌ 11 OTTOBRE 2021

Risoluzione di esercizi.

12. MARTEDÌ 12 OTTOBRE 2021

Ultimi dettagli sulla classificazione dei sottogruppi finiti di $\mathrm{O}(2)$.

Azioni di gruppi su insiemi. Definizione, esempi, orbita di un elemento, stabilizzatore di un elemento. Corrispondenza biunivoca tra G-orbita di x e classi laterali sinistre di $\mathrm{Stab}(x)$ in G.

Elementi di $\mathrm{SO}(3)$: sono tutti rotazioni attorno ad una retta passante per l'origine. Struttura dei sottogruppi finiti di $\mathrm{SO}(3)$: polo di un elemento (diverso dall'identità); l'azione di $G < \mathrm{SO}(3)$ su $\mathbb{R}^3$ stabilizza l'insieme dei poli di G. Una relazione numerica.

13. MERCOLEDÌ 13 OTTOBRE 2021

Se $G < \mathrm{SO}(3)$ è finito, la sua azione sull'insieme dei poli ha al più tre orbite. Se ha esattamente due orbite, allora $G \simeq \mathrm{C}_n$; se ha tre orbite, G è diedrale oppure ha ordine 12, 24 o 60 (ed è isomorfo, ma non l'ho dimostrato, a A_4, S_4 oppure A_5).

Ancora azioni di gruppi su insiemi. Azione di G su G/H per moltiplicazione sinistra, se $H < G$: ha una sola orbita e ogni azione di G su un insieme con una sola orbita (una tale azione si dice *transitiva*) è isomorfa ad una tale azione.

Azione di $H < G$ su G per moltiplicazione sinistra o destra (composta con l'inverso): le orbite sono le classi laterali destre e sinistre di H in G. Azione di $H \times K$ su G data da $(h,k).g = hgk^{-1}$, dove $H, K < G$. Cardinalità di HK e dei laterali doppi HaK.

Azione di $\mathrm{GL}_m \times \mathrm{GL}_n$ sulle matrici $m \times n$ per *cambiamento di base*. Azione di G su se stesso per coniugazione. Classi di coniugio. Il numero di coniugati di x in G è uguale a $[G : Z(x)]$. Equazione delle classi (cenni).

14. Giovedì 14 ottobre 2021

Il centro di un gruppo ne è un sottogruppo normale. Se G non è abeliano, $G/Z(G)$ non è ciclico; in particolare, $[G : Z(G)]$ non è mai un numero primo. Equazione delle classi. Applicazioni: se $|G| = p^k$, dove p è primo e $k > 0$, allora $Z(G) \neq \{1\}$. Se $|G|$ è il quadrato di un numero primo, allora G è necessariamente abeliano. Se $|G|$ è il cubo di un numero primo p, allora G è abeliano oppure $|Z(G)| = p$. Esempi: il gruppo diedrale D_4 e il gruppo delle unità dei quaternioni. Gruppi di ordine 35: hanno un unico sottogruppo di ordine 7; possiedono esattamente sei elementi di ordine 7; sono abeliani; sono ciclici. Classi di coniugio di D_n quando n è dispari.

15. Lunedì 18 ottobre 2021

Risoluzione di esercizi.

16. Martedì 19 ottobre 2021

Se $H, K < G$ allora $[H : H \cap K] \leq [G : K]$. Un esempio in cui $[H : H \cap K]$ non divide $[G : K]$.

Enunciato del Teorema di Sylow. Conseguenze: il Teorema di Cauchy; un p-sottogruppo di Sylow di un gruppo finito G è normale se e solo se è l'unico p-Sylow. Lemma tecnico: se P è un p-sottogruppo di Sylow di G e $H < G$, allora $H \cap aPa^{-1}$ è un p-Sylow di G per qualche $a \in G$. Ogni gruppo finito si immerge in qualche $\mathrm{GL}_n(\mathbb{Z}/(p)$, per il quale è facile esibire esplicitazione un p-Sylow.

I p-Sylow di un gruppo finito sono tutti coniugati; ogni p-sottogruppo di un gruppo finito G è contenuto in qualche p-Sylow di G; gli elementi di G il cui ordine è una potenza di p coincidono con l'unione dei p-Sylow di G; un p-Sylow di G è normale esattamente quando è l'unico p-Sylow di G. Il numero dei p-Sylow di G divide $|G|$ ed è $\equiv 1 \mod p$.

Prodotti semidiretti di gruppi.

17. Mercoledì 20 ottobre 2021

Prodotti semidiretti di gruppi. Gruppi che sono prodotto semidiretto di un sottogruppo normale N e un sottogruppo H: rimane definito un omomorfismo di gruppi $\phi : H \to \mathrm{Aut}(N)$ definito da $\phi_h(n) = hnh^{-1}$. Prodotto semidiretto astratto di gruppi. Un gruppo che è prodotto semidiretto di $H < G$ e $N \lhd G$ è isomorfo a un prodotto semidiretto astratto di N con H. I prodotti diretti sono prodotti semidiretti.

Gruppi con 8 elementi: i gruppi abeliani $\mathrm{C}_8, \mathrm{C}_4 \times \mathrm{C}_2, \mathrm{C}_2 \times \mathrm{C}_2 \times \mathrm{C}_2$. Se $G, |G| = 8$, possiede un elemento di ordine 8 è ciclico. Se non possiede né elementi di ordine 8, né di ordine 4, allora $G \simeq \mathrm{C}_2 \times \mathrm{C}_2 \times \mathrm{C}_2$. Se G possiede un elemento x di ordine 4 e trovo in $G \setminus (x)$ elementi di ordine 2, allora $G \simeq \mathrm{C}_4 \times \mathrm{C}_2$ oppure $G \simeq \mathrm{D}_4$.

18. Giovedì 21 ottobre 2021

Se $G, |G| = 8$, possiede un solo elemento di ordine 2, allora $G \simeq \mathrm{Q}_8$.

Gruppi di ordine 12. Se il 3-Sylow di un gruppo $G, |G| = 12$, è normale, allora $G \simeq \mathrm{C}_{12}, \mathrm{C}_6 \times \mathrm{C}_2, \mathrm{D}_6$ oppure al gruppo di presentazione $x^4 = 1, y^3 = 1, xyx^{-1} = y^{-1}$. Se il 3-Sylow non è normale allora il 2-Sylow è normale e $G \simeq \mathrm{A}_4$. Il gruppo $\mathrm{S}_3 \times \mathrm{C}_2$ è isomorfo a D_6.

Classi di coniugio in S_n: due permutazioni sono coniugate in S_n se e solo se possiedono la stessa struttura ciclica. Esempi: classi di coniugio in S_3 e S_5. Un sottogruppo è normale se e solo se è unione di classi di coniugio. Sottogruppi normali di S_5 (cenni).

19. Lunedì 25 ottobre 2021

Risoluzione di esercizi.

20. Martedì 26 ottobre 2021

Risoluzione di alcuni ultimi esercizi. Anelli, anelli commutativi. Anelli con unità: si richiede che $1 \neq 0$; Se $1 = 0$ l'unico esempio è l'anello con un unico elemento. Sottoanelli, ideali (sinistri, destri, bilateri). Omomorfismi di anelli. Un omomorfismo tra anelli con unità non manda necessariamente 1 in 1, e bisogna richiederlo esplicitamente se vogliamo che lo faccia.

L'immagine di un omomorfismo $f : A \to B$ è un sottoanello di B; il suo nucleo è un ideale di A. L'anello quoziente A/I, dove $I \subsetneq A$ è un ideale. Ogni ideale $I \subsetneq A$ è nucleo di qualche omomorfismo, e più precisamente della proiezione $\pi : A \to A/I$ dove A/I è l'anello quoziente.

Ideali di $\mathbb{Z}$.

21. MERCOLEDÌ 27 OTTOBRE 2021

Richiami dalla lezione precedente. Se $I \subsetneq A$ è un ideale, allora esiste un'unica struttura di anello sul gruppo quoziente A/I che renda la proiezione $\pi : A \to A/I$ un omomorfismo di anelli.

Ideali principali di un anello. $\mathbb{Z}$ ha solo ideali principali. Somma e intersezione di ideali. Ideali finitamente generati come somme di ideali principali. Domini a ideali principali.

Se D è un dominio d'integrità, allora anche $D[x]$ è un dominio d'integrità: più precisamente, se $a(x), b(x)$ sono elementi non nulli di $D[x]$, allora il grado di $a(x)b(x)$ è la somma dei gradi di $a(x)$ e $b(x)$. Un esempio di ideale non principale: $(2, x) \subset \mathbb{Z}[x]$.

Gli ideali di un campo K sono solo quelli banali: (0) e K. Un anello i cui ideali sono solo quelli banali è necessariamente un campo. Ideali primi e massimali: due coppie di definizioni equivalenti. Ideali primi e massimali di $\mathbb{Z}$. (0) è un ideale primo di A se e solo se A è un dominio d'integrità. Se $f : A \to B$ è un omomorfismo di anelli, e $I \subsetneq B$ è un ideale primo, allora $f^{-1}(I)$ è un ideale primo di A. Ogni ideale massimale è primo; (0) è un ideale primo, ma non massimale, di $\mathbb{Z}$.

Teoremi di omomorfismo e isomorfismo per anelli. Se $f : A \to B$ è un omomorfismo di anelli, allora $\operatorname{Im} f \simeq A/\ker f$. Corrispondenza tra ideali di A/I e ideali di A che contengono I.

Per ogni scelta di un anello A, esiste un unico omomorfismo (che mandi 1 in 1) $\mathbb{Z} \to A$. Caratteristica di un dominio (cenni).

22. GIOVEDÌ 28 OTTOBRE 2021

Richiami sulle proprietà dei domini d'integrità: se D è un dominio d'integrità, anche $D[x]$ lo è; ogni sottoanello di un dominio d'integrità è un dominio d'integrità; in un dominio d'integrità D vale la proprietà di cancellazione: se $0 \neq d \in D$ e $dx = dy$, allora $x = y$. L'anello quoziente A/I è un dominio d'integrità se e solo se $I \subsetneq A$ è un ideale primo di A.

Caratteristica di un dominio. Nei domini a caratteristica 0, l'ordine (additivo) di 1 è infinito; nei domini a caratteristica $p > 0$, l'ordine di 1 è p. I domini d'integrità contengono (un sottoanello isomorfo a) $\mathbb{Z}$ se hanno caratteristica 0 e $\mathbb{Z}/(p)$ se hanno caratteristica $p > 0$.

Campo delle frazioni K_D di un dominio d'integrità D: è un campo e contiene (un sottoanello isomorfo a) D. Se $D = \mathbb{Z}$, allora $K_D = \mathbb{Q}$. Proprietà universale del campo delle frazioni: se $f : D \to A$ è un omomorfismo di anelli tale che $f(d)$ è invertibile in A per ogni $0 \neq d \in D$, allora f si estende (in modo unico) ad un omomorfismo di anelli $F : K_D \to A$. Conseguenza: un campo di caratteristica 0 contiene un sottocampo isomorfo a $\mathbb{Q}$.

Principio di sostituzione per anelli di polinomi: se A, B sono anelli, allora dare un omomorfismo di anelli $\Phi : A[x] \to B$ è equivalente a dare la sua restrizione alle costanti $\phi : A \to B$ e l'immagine $b \in B$ di x attraverso Φ. Esempi: omomorfismi di valutazione; riduzione di polinomi a coefficienti interi modulo n; l'omomorfismo $\mathbb{Z}[x] \to \mathbb{Z}/(2)$ che associa ad $f(x)$ la parità del suo termine noto.

Interpretazione dell'anello quoziente $\mathbb{R}[x]/(x^2 + 1)$ come $\mathbb{C}$. Tecnica generale per aggiungere ad un anello A un elemento che soddisfi un polinomio $q(x) \in A[x]$ considerando il quoziente $A[x]/(q(x))$.

23. MARTEDÌ 2 NOVEMBRE 2021

Risoluzione di esercizi.

24. MERCOLEDÌ 3 NOVEMBRE 2021

Domini euclidei: definizione ed esempi. Un dominio euclideo è sempre un dominio a ideali principali. In un dominio euclideo, $0 \neq I = (a)$ vale se e soltanto se $a \neq 0$ è un elemento di norma euclidea minima in I; analogamente, a è invertibile se e solo se $N(a) = N(1)$; se $0 \neq a = bc$ con b, c non invertibili, allora $N(b), N(c) < N(a)$. Divisibilità e inclusioni tra ideali principali: a divide b se e solo se $(b) \subset (a)$; $(a) = (b)$ se e solo se a e b sono associati (si ottengono cioè l'uno dall'altro moltiplicando per un invertibile); in un dominio a ideali principali, d è un MCD di a e b esattamente quando $(d) = (a) + (b)$. In particolare $MCD(a, b)$ esiste sempre ed è unico a meno di associati; vale inoltre l'identità di Bézout. L'algoritmo euclideo per il calcolo dell'MCD funziona in un dominio euclideo. Un esempio in $\mathbb{Z}[i]$.

Elementi primi e invertibili in un dominio d'integrità. Un elemento non invertibile $p \neq 0$ è primo quando (p) è un ideale primo; è massimale quando $p = ab \implies$ uno tra a e b è invertibile. In un dominio a ideali principali un elemento è irriducibile se e solo se genera un ideale massimale; in particolare, ogni elemento irriducibile è primo. In un dominio d'integrità ogni elemento primo è necessariamente irriducibile.

Enunciato del teorema di fattorizzazione unica.

25. GIOVEDÌ 4 NOVEMBRE 2021

Richiami dalla lezione precedente. Lemma di Euclide: se a divide bc e $\mathrm{MCD}(a, b) = 1$ allora a divide c. Seconda dimostrazione della primalità degli elementi irriducibili in un dominio a ideali principali. Se due elementi primi si dividono, sono allora associati.

Teorema di fattorizzazione unica: enunciato e dimostrazione. Applicazioni: irrazionalità di $\sqrt[k]{N}$ quando il naturale N non è una k-esima potenza perfetta. Teorema di Euclide: esistono infiniti numeri primi. Una variante: esistono infiniti numeri primi della forma $4n + 3$. Esistenza di infiniti numeri primi della forma $4n + 1$ attraverso l'uso del Teorema di Lagrange.

Elementi primi in $\mathbb{Z}[i]$. Un primo di $\mathbb{Z}[i]$ divide un primo naturale. Fattorizzazioni in $\mathbb{Z}[i]$ dei primi naturali: p primo naturale è irriducibile in $\mathbb{Z}[i]$ se non è somma di due quadrati; se $p = a^2 + b^2 = (a + bi)(a - bi)$ allora $a \pm bi$ sono irriducibili in $\mathbb{Z}[i]$. I numeri primi $\equiv 3 \mod 4$ sono irriducibili in $\mathbb{Z}[i]$; $2 = (1 + i)(1 - i)$ non è irriducibile in $\mathbb{Z}[i]$. Teorema di Wilson: se p è un numero primo, $(p-1)! \equiv -1 \mod p$. Conseguenza: se $p \equiv 1 \mod 4$ è un numero primo, allora $(((p - 1)/2)!)^2 \equiv -1 \mod p$.

26. LUNEDÌ 8 NOVEMBRE 2021

Risoluzione di esercizi.

I polinomi di grado 1 a coefficienti in un campo K sono irriducibili in $K[x]$. I polinomi di grado $2, 3$ a coefficienti in un campo K sono irriducibili in $K[x]$ se e solo se non hanno radici in K. Polinomi irriducibili in $\mathbb{F}_2[x]$ di grado al più 4. Se $f(x) \in \mathbb{F}_p[x]$ è un polinomio irriducibile di grado n, allora il campo quoziente $\mathbb{F}_p[x]/(f(x))$ ha p^n elementi. Polinomi irriducibili a coefficienti reali.

Elementi primi nell'anello $\mathbb{Z}[i]$. Teorema dei due quadrati. Nuova dimostrazione dell'esistenza di infiniti numeri primi della forma $4n + 1$ attraverso l'uso del Teorema dei due quadrati.

27. MARTEDÌ 9 NOVEMBRE 2021

Domini a fattorizzazione unica. I domini a fattorizzazione unica privi di elementi primi sono esattamente i campi. Riformulazione di divisibilità e MCD in termini di fattorizzazione. In $\mathbb{Q}[x]$ le costanti (non nulle) sono invertibili; in $\mathbb{Z}[x]$ non necessariamente. Contenuto di un polinomio a coefficienti interi; polinomi primitivi. I polinomi non costanti in $\mathbb{Z}[x]$ sono tutti primitivi.

Varie forme del Lemma di Gauss: se p è primo in $\mathbb{Z}$, allora $p\mathbb{Z}[x]$ è un ideale primo di $\mathbb{Z}[x]$ e quindi p è anche primo in $\mathbb{Z}[x]$; il prodotto di polinomi primitivi è primitivo; $c(f(x)g(x)) = c(f(x))c(g(x))$; se $p(x) \in \mathbb{Z}[x]$ primitivo divide $f(x) \in \mathbb{Z}[x]$ in $\mathbb{Q}[x]$, allora lo divide anche in $\mathbb{Z}[x]$; se $p(x) \in \mathbb{Z}[x]$ non costante è irriducibile in $\mathbb{Z}[x]$ allora è irriducibile anche in $\mathbb{Q}[x]$. Gli irriducibili non costanti in $\mathbb{Z}[x]$ sono primi in $\mathbb{Z}[x]$; le costanti in $\mathbb{Z}[x]$ prime in $\mathbb{Z}$ sono prime anche in $\mathbb{Z}[x]$.

Ogni $0 \neq f(x) \in \mathbb{Z}[x]$ è prodotto di un invertibile e di elementi irriducibili in $\mathbb{Z}[x]$, che sono automaticamente tutti primi. $\mathbb{Z}[x]$ è un dominio a fattorizzazione unica.

La stessa dimostrazione fa vedere che se D è un dominio a fattorizzazione unica, allora anche $D[x]$ è un dominio a fattorizzazione unica: i suoi irriducibili sono i primi di D e i polinomi non costanti primitivi in $D[x]$ che sono irriducibili in $K[x]$, dove K è il campo delle frazioni di D. In particolare sono domini a fattorizzazione unica $\mathbb{Z}[x_1, \dots, x_n]$ e $K[x_1, \dots, x_n]$ quando K è un campo.

28. MERCOLEDÌ 10 NOVEMBRE 2021

Due esempi: nel dominio d'integrità $\mathbb{Z}[x^{1/2^n}, n \in \mathbb{N}]$ non ogni elemento (non invertibile) è prodotto di irriducibili; nel dominio d'integrità $\mathbb{Z}[\sqrt{-5}]$ non ogni elemento irriducibile è primo.

L'elemento $2x + 1$ è irriducibile (e quindi primo) nel dominio a fattorizzazione unica $\mathbb{Z}[x]$, ma l'ideale $(2x + 1)$ non è massimale: è in effetti contenuto nell'ideale proprio $(3, x - 2)$, che è invece massimale.

Calcolo del determinante di Vandermonde attraverso l'utilizzo della fattorizzazione unica in $\mathbb{Z}[x_1, \dots, x_n]$.

Irriducibilità di polinomi. Le radici razionali di un polinomio di grado n $f(x) = f_n x^n + \cdots + f_1 x + f_0 \in \mathbb{Z}[x]$ sono tutte del tipo a/b, dove $a, b \in \mathbb{Z}$ e a divide f_0, mentre b divide f_n. Allo stesso modo, quando D è un dominio a fattorizzazione unica, le radici nel campo di frazioni K_D del polinomio $f(x) = f_n x^n + \cdots + f_1 x + f_0 \in D[x]$ sono tutte della forma a/b, dove $a, b \in D$ sono tali che a divide f_0 e b divide f_n. Un polinomio $f(x) \in K[x]$ di grado ≤ 3 è irriducibile in $K[x]$ se e solo se non ha radici in K.

Criteri di irriducibilità. Riduzione modulo p: un polinomio primitivo non costante $f(x) \in \mathbb{Z}[x]$ è irriducibile quando la sua riduzione $\overline{f(x)} \in \mathbb{Z}/(p)[x]$ modulo un primo p è irriducibile in $\mathbb{Z}/(p)[x]$. Più in generale, se D è un dominio d'integrità, $\mathfrak{p}$ un suo ideale primo, $f(x) \in D[x]$ un polinomio primitivo (= i cui unici divisori costanti siano invertibili), allora $f(x)$ è irriducibile in $D[x]$ non appena la sua riduzione modulo $\mathfrak{p}$ sia irriducibile in $(D/\mathfrak{p})[x]$.

Criterio di Eisenstein: se p primo divide tutti i coefficienti del polinomio primitivo $f(x) \in \mathbb{Z}[x]$ ma non il primo coefficiente, e p^2 non divide il termine noto, allora $f(x)$ è irriducibile in $\mathbb{Z}[x]$. Più in generale, sia D un dominio d'integrità e $p \in D$ un elemento primo. Se le ipotesi di sopra valgono, allora $f(x)$ è irriducibile in $D[x]$ — NB: né D, né $D[x]$ devono essere domini a fattorizzazione unica.

Irriducibilità del p-esimo polinomio ciclotomico $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$, quando p è primo.

29. LUNEDÌ 15 NOVEMBRE 2021

Il polinomio $f(x) = x^4 + 9 \in \mathbb{Z}[x] \subset \mathbb{Q}[x]$ è irriducibile in $\mathbb{Q}[x]$: per forza bruta; applicando il Criterio di Eisenstein a $f(x + 1)$ con il primo $p = 2$. Il polinomio $f(x) = x^4 + 81$ è irriducibile in $\mathbb{Q}[x]$, ma la sua irriducibilità non segue applicando il criterio di Eisenstein a $f(x + k)$ per nessuna scelta di p primo, né riducendo modulo p.

Terne pitagoriche primitive: sono tutte e sole della forma $(m^2 - n^2, 2mn, m^2 + n^2)$, dove $m > n$ hanno opposta parità. Soluzioni intere delle equazioni $y^3 = x^2 + 1, y^3 = x^2 + 2$ utilizzando la fattorizzazione unica in $\mathbb{Z}[i], \mathbb{Z}[\sqrt{-2}]$.

Fattorizzazione unica degli ideali in $\mathbb{Z}[\sqrt{-5}]$: un esempio. Se $I = (2, 1+\sqrt{-5}), J = (3, 1+\sqrt{-5}), \overline{J} = (3, 1-\sqrt{-5})$ allora $(2) = I^2, (3) = J\overline{J}, (1 + \sqrt{-5}) = IJ, (1 - \sqrt{-5}) = I\overline{J}$. Pertanto $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ si raffina a $(6) = I^2 J\overline{J}$.

30. MARTEDÌ 16 NOVEMBRE 2021

Moduli su anelli (commutativi con unità). Lineare indipendenza e insiemi di generatori. Non ogni R-modulo possiede una R-base; non ogni insieme R-linearmente indipendente si estende ad una R-base; non da ogni insieme di R-generatori si estrae una base.

Gli $\mathbb{Z}$-moduli sono i gruppi abeliani. I $K[x]$-moduli, quando K è un campo, sono i K-spazi vettoriali dotati di un endomorfismo $T(v) = x.v$.

Somma diretta di R-moduli. L'R-modulo libero R^n. Determinante di matrici a coefficienti in R: formula di Binet. Omomorfismi di R-moduli. Sottomoduli. Corrispondenza tra matrici $n \times m$ con coefficienti in R e omomorfismi $R^m \to R^n$. Una matrice $m \times n$ è invertibile se e solo se $m = n$ e ha determinante invertibile. Il gruppo $\mathrm{GL}_n(R)$.

Orbite dell'azione di $\mathrm{GL}_m(R) \times \mathrm{GL}_n(R)$ su $\mathrm{Mat}_{m\times n}(R)$ definita da $(X, Y).M = XMY^{-1}$, quando R è un campo. Cosa accade quando R è un dominio euclideo?

Alcune matrici invertibili a coefficienti in un dominio euclideo R e il loro effetto quando moltiplicano a sinistra o a destra una matrice data.

31. MERCOLEDÌ 17 NOVEMBRE 2021

Forma canonica di Smith per matrici a coefficienti in un dominio euclideo R. Descrizione di un sottomodulo di R^n, dati k suoi generatori, per mezzo di una matrice $n \times k$ a coefficienti in R. Moltiplicare tale matrice a destra per una matrice invertibile non modifica il sottomodulo; moltiplicare tale matrice a sinistra per una matrice invertibile applica un automorfismo di R^n al sottomodulo. Pertanto, se $U \subset R^n$ è un sottomodulo finitamente generato, esiste un automorfismo ϕ di R^n tale che $\phi(U)$ è generato da $d_1e_1, \dots, d_ne_n$, dove $d_i \in R$ sono elementi tali che d_i divide d_j se $i \leq j$ e gli e_i sono i vettori della base canonica di R^n.

Applicazione: se M è un R-modulo finitamente generato (e R è un dominio euclideo), allora M è isomorfo a $R/(d_1) \oplus \cdots \oplus R/(d_n)$ dove $d_i \in R$ sono elementi tali che d_i divide d_j se $i \leq j$.

Ogni gruppo abeliano finitamente generato è isomorfo a un prodotto diretto di gruppi ciclici $\mathbb{Z}/(d_i)$, dove i $d_i \in \mathbb{Z}$ sono come sopra.

32. GIOVEDÌ 18 NOVEMBRE 2021

Classificazione dei gruppi abeliani finitamente generati: alcuni esempi. I gruppi abeliani finiti sono prodotti diretti di gruppi ciclici finiti. Gruppi abeliani di ordine 8, p^5, 36.

Richiami sul teorema cinese dei resti: se $I, J \subset R$ sono ideali e $I + J = R$, allora $R/IJ \simeq R/I \oplus R/J$, anche come R-moduli. In particolare, se R è un dominio euclideo (o anche a ideali principali) e $a, b \in R$ sono primi tra loro, allora $R/(ab) \simeq R/(a) \oplus R/(b)$ come R-moduli. In particolare, quando K è un campo $K[x]/(a(x)b(x)) \simeq K[x]/(a(x)) \oplus K[x]/(b(x))$ come $K[x]$-moduli non appena $a(x), b(x)$ sono primi tra loro.

Forma canonica di Jordan. Se V è uno spazio vettoriale complesso di dimensione finita e T è un suo endomorfismo lineare, allora V è un $\mathbb{C}[x]$-modulo finitamente generato rispetto alla struttura di $\mathbb{C}[x]$-modulo definita da $x.v = T(v)$. Pertanto V è isomorfo a una somma diretta di $\mathbb{C}[x]$-moduli del tipo $\mathbb{C}[x]/(f(x))$ dove $f(x)$ è, senza perdere di generalità, un polinomio monico non costante.

Ciascun $\mathbb{C}[x]/(f(x))$ è isomorfo, per il Teorema Fondamentale dell'Algebra, ad una somma diretta di addendi, ciascuno isomorfo a $\mathbb{C}[x]/((x-a)^n)$ per un'opportuna scelta di $a \in \mathbb{C}, n > 0$. Su un tale $\mathbb{C}[x]$-modulo, la matrice associata alla moltiplicazione per x nella base $[1], [x-a], \dots, [(x-a)^{n-1}]$ è un blocco di Jordan $n \times n$ di autovalore a.

33. LUNEDÌ 22 NOVEMBRE 2021

Risoluzione di esercizi.

34. MARTEDÌ 23 NOVEMBRE 2021

Esempi di (non) diagonalizzabilità di endomorfismi di spazi vettoriali complessi di dimensione finita. Polinomio minimo e polinomio caratteristico: loro proprietà. Forma canonica razionale.

35. MERCOLEDÌ 24 NOVEMBRE 2021

Come ricavare gli invarianti $d_1|d_2|\dots|d_n$ da un modulo finitamente generato M su un dominio euclideo (ma basta a ideali principali) R. Il numero n coincide con la minima cardinalità di un insieme di generatori di M come R-modulo. L'elemento $d_1 \in R$ è il generatore dell'ideale $\{a \in R \mid aM \text{ è generabile da meno di } n \text{ elementi}\}$, ed è quindi individuato a meno di moltiplicazione per un invertibile. Il numero k di elementi d_i associati a d_1 si ottiene togliendo da n il numero minimo di generatori dell'$R-$modulo d_1M. Gli elementi $d_{k+1}, \dots, d_n$ si ottengono dagli invarianti di d_1M moltiplicandoli per d_1.

Estensioni di campi. Grado di un estensione. Estensioni finite e infinite. Elementi algebrici e trascendenti. Riformulazioni dell'algebricità: se $K \subset L$ è un'estensione di campi e $\alpha \in L$, allora α è algebrico su $K \iff K[\alpha] = K(\alpha)$. Il polinomio minimo su K di un algebrico α è irriducibile e ogni polinomio $q(x) \in K[x]$ che annulla α è suo multiplo. In particolare, un polinomio irriducibile in $K[x]$ che annulla α è sicuramente il suo polinomio minimo (sempre a meno di una costante moltiplicativa non nulla).

36. GIOVEDÌ 25 NOVEMBRE 2021

Estensione finita di estensione finita è finita e se $F \subset K \subset L$, allora $[L : F] = [L : K][K : F]$. Estensione algebrica di estensione algebrica è algebrica. Chiusura algebrica di $\mathbb{Q}$ dentro $\mathbb{C}$. Un esempio: $\sqrt{2} + \sqrt[3]{2}$ è un algebrico su $\mathbb{Q}$ di grado 6; calcolo del suo polinomio caratteristico.

37. LUNEDÌ 29 NOVEMBRE 2021

Risoluzione di esercizi.

38. MARTEDÌ 30 NOVEMBRE 2021

Un sottogruppo finito del gruppo moltiplicativo di un campo è necessariamente ciclico. Sottogruppi finiti di $\mathbb{R}^\times$ e $\mathbb{C}^\times$.

Radici complesse (primitive e non) dell'unità. Estensioni ciclotomiche, polinomi ciclotomici. L'n-esimo polinomio ciclotomico $\Phi_n(x)$ è monico a coefficienti interi di grado $\varphi(n)$. E' irriducibile quando n è primo (anche quando n non è primo, ma non sappiamo una dimostrazione). L'n-esima estensione ciclotomica di $\mathbb{Q}$ contiene $\cos(2\pi/n)$ e $[\mathbb{Q}(\exp(2\pi i/n) : \mathbb{Q}(\cos(2\pi/n))] = 2$. In particolare, quando p è primo, $[\mathbb{Q}(\cos(2\pi/p)) : \mathbb{Q}] = (p-1)/2$.

Costruzioni con riga e compasso. Un numero reale è costruibile con riga e compasso solo se è algebrico su $\mathbb{Q}$ e il suo grado è una potenza di 2. Impossibilità della rettificazione della circonferenza, della quadratura del cerchio e della duplicazione del cubo. Non costruibilità del p-agono regolare, quando p è primo ma non è un primo di Fermat.

39. MERCOLEDÌ 1 DICEMBRE 2021

Se l'intero $n > 0$ ha un fattore primo dispari, allora $2^n + 1$ non è primo, ma non è detto che $2^{2^k} + 1$ sia primo per ogni $k \geq 0$. Ad esempio, $2^{2^5} + 1 = 641 \cdot 6700417$ non è primo. Trisezione dell'angolo: l'angolo di 120 gradi non è trisecabile con riga e compasso.

Campi di spezzamento. Se L è campo di spezzamento di $f(x) \in K[x]$ su K, allora è campo di spezzamento di $f(x)$ su K' per ogni campo $K \subset K' \subset L$. Un campo di spezzamento L di $f(x)$ su K è un'estensione finita di K. Se L è un'estensione di K su cui $f(x) \in K[x]$ si spezza nella forma $f(x) = f_n(x - \alpha_1) \cdot \ldots \cdot (x - \alpha_n)$, allora $K(\alpha_1, \ldots, \alpha_n)$ è un campo di spezzamento di $f(x)$ su K.

Esistenza dei campi di spezamento: se $f(x) \in K[x]$ è un polinomio di grado $n > 0$, allora esiste un'estensione $K \subset L$ di grado $\leq n!$ su cui $f(x)$ si spezza. In particolare, esiste un campo di spezzamento di $f(x)$ su K di grado $\leq n!$

Unicità del campo di spezzamento: sia $\phi : K \to K'$ un isomorfismo di campi, $f(x) \in K[x]$ un polinomio non costante e $f'(x) \in K'[x]$ il polinomio ottenuto da $f(x)$ applicando ϕ sui suoi coefficienti. Se L (rispettivamente L') è un campo di spezzamento di $f(x)$ (risp. $f'(x)$) su K (risp. K'), allora esiste un isomorfiamo $\Phi : L \to L'$ tale che $\Phi|_K = \phi$. In particolare, due campi di spezzamento L, L' dello stesso polinomio $f(x) \in K[x]$ sullo stesso campo K sono isomorfi con un isomorfismo che è l'identità sugli elementi di K.

40. GIOVEDÌ 2 DICEMBRE 2021

Campi finiti. Un campo finito ha p^n elementi, dove $p = \operatorname{char} K$ e $n > 0$. Un campo K con p^n elementi è campo di spezzamento di $x^{p^n} - x$ su $\mathbb{F}_p$. Due campi con p^n sono necessariamente isomorfi.

L'automorfismo di Frobenius di un campo finito. Il campo di spezzamento di $x^{p^n} - x$ su $\mathbb{F}_p$ contiene esattamente p^n elementi; pertanto esiste un campo con p^n elementi per ogni p primo, $n > 0$ intero. Radici in $\mathbb{F}_{p^n}$ di un polinomio irriducibile $q(x) \in \mathbb{F}_p[x]$ di grado n.

Il polinomio $x^{p^n} - x$ coincide con il prodotto, in $\mathbb{F}_p[x]$, di tutti e soli i polinomi irriducibili di grado che divide n.

41. LUNEDÌ 6 DICEMBRE 2021

Risoluzione di esercizi.

42. MARTEDÌ 7 DICEMBRE 2021

Inclusioni tra campi finiti. Se $|L| = p^l$, con p primo, e k divide l, allora esiste un unico sottocampo di L con p^k elementi; se k non divide l, invece, non ne esiste alcuno. Cenni di corrispondenza di Galois per estensioni tra campi finiti. Irriducibilità dei polinomi ciclotomici su $\mathbb{Q}$.

Insiemi equipotenti. Proprietà delle corrispondenze biunivoche. Insiemi che hanno la stessa cardinalità: $\mathbb{N}$ può essere messo in corrispondenza biunivoca con $\mathbb{Z}, \mathbb{N} \times \{0, 1\}, \mathbb{N} \times \mathbb{N}, \mathbb{N}^n$. Non esistono applicazioni suriettive da $\mathbb{N}$ nel suo insieme delle parti, quindi $\mathbb{N}$ non ha la stessa cardinalità di $P(\mathbb{N})$. Più in generale, non esistono applicazioni suriettive da un insieme X nel suo insieme delle parti $P(X)$.

Confronto tra cardinalità. $|X| \leq |Y|$ vuol dire che esiste $f : X \to Y$ iniettiva. Riflessività, simmetria del confronto tra cardinalità. Enunciato del Teorema di Bernstein.

43. GIOVEDÌ 9 DICEMBRE 2021

Si scrive $|X| < |Y|$ quando esistono applicazioni iniettive da X a Y, ma nessuna di queste è invertibile. Per ogni insieme X si ha $|X| < |P(X)|$; pertanto, non esiste una cardinalità massima.

Dimostrazione del Teorema di Cantor-Bernstein-Schröder. Applicazioni: $\mathbb{Q}$ è numerabile; l'unione di due insiemi numerabili è numerabile; l'unione di un numero finito di insiemi numerabili è numerabile.

L'unione di una quantità numerabile di insiemi numerabili è numerabile? Funzioni di scelta e assioma della scelta. Ogni applicazione iniettiva tra insiemi ha un'inversa sinistra (che è suriettiva). Assioma della scelta: ogni applicazione suriettiva tra insiemi ha un'inversa destra (che è iniettiva). L'esistenza dell'inversa destra non ha bisogno dell'assioma della scelta se l'insieme di partenza è bene ordinato (ad esempio, se è $\mathbb{N}$) o bene ordinabile. Teorema di Zermelo: ogni insieme è bene ordinabile.

Enunciato del Lemma di Zorn: un insieme parzialmente ordinato non vuoto in cui ogni catena possiede un maggiorante contiene elementi massimali. Un esempio di utilizzo: ogni anello (commutativo con unità) possiede ideali massimali.

44. LUNEDÌ 13 DICEMBRE 2021

Risoluzione di esercizi.

45. MARTEDÌ 14 DICEMBRE 2021

Comunque siano presi due insiemi, uno dei due si inietta dentro l'altro. Aggiungere o togliere un numero finito di elementi ad un insieme numerabile lo mantiene numerabile. Ogni insieme infinito contiene un sottoinsieme numerabile. Aggiungere o togliere un numero finito di elementi ad un insieme infinito non ne cambia la cardinalità. La cardinalità di $\mathbb{R}$ coincide con quella dell'insieme delle parti di $\mathbb{N}$.

Ogni insieme infinito possiede una partizione in sottoinsiemi numerabili. Se X è infinito, $X \times \{0,1\}$ e $X \times \mathbb{N}$ possono essere messi in corrispondenza biunivoca con X. La cardinalità di un'unione finita di insiemi infiniti coincide con la massima cardinalità degli insiemi che si sono uniti.

Ogni insieme infinito è in corrispondenza biunivoca con il suo quadrato cartesiano: inizio della dimostrazione.

46. MERCOLEDÌ 15 DICEMBRE 2021

Se $X \subset Y$ e $|X| < |Y|$, allora $|Y \setminus X| = |Y|$. Ogni insieme infinito è in corrispondenza biunivoca con il suo quadrato cartesiano: fine della dimostrazione. L'insieme delle parti finite di un insieme infinito X ha la stessa cardinalità di X. Se K è un campo infinito, allora $K[x_1, \ldots, x_n]$ ha la stessa cardinalità di K. Un'estensione algebrica di un campo infinito K ha la stessa cardinalità di K.

Esistenza di numeri reali algebrici su $\mathbb{Q}$. Esistenza (e unicità) della chiusura algebrica di un campo dato.

47. GIOVEDÌ 16 DICEMBRE 2021

Cenni di Teoria di Galois. Enunciato della corrispondenza di Galois. Esempi: $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ non è di Galois. L'estensione $\mathbb{Q} \subset \mathbb{Q}(e^{2\pi i/3}, \sqrt[3]{2})$ è di Galois: sue sottoestensioni (di Galois e non di Galois su $\mathbb{Q}$). Estensioni ciclotomiche: sono tutte di Galois su $\mathbb{Q}$. $\mathrm{Gal}(\mathbb{Q}(e^{2\pi i/n})/\mathbb{Q}) \simeq \mathbb{Z}/(n)^\times$.

Applicazioni: costruibilità del p-agono regolare con riga e compasso, quando p è un primo di Fermat; teorema fondamentale dell'algebra; risolubilità per radicali di un'equazione algebrica in un incognita. Teorema di Abel-Ruffini.

48. LUNEDÌ 20 DICEMBRE 2021

Risoluzione di esercizi. (Forse: esistenza di un'inversa destra di ogni suriezione $\implies$ assioma della scelta $\implies$ lemma di Zorn $\implies$ teorema di Zermelo $\implies$ esistenza di un'inversa destra di ogni suriezione)

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