ALGEBRA 1
ELENCO DEGLI ARGOMENTI TRATTATI DURANTE LE LEZIONI

Primo semestre

1. MARTEDÌ 27 SETTEMBRE 2022

Presentazione del corso e chiacchiere.

Cardinalità di insiemi. Due insiemi X, Y hanno la stessa cardinalità se esiste una corrispondenza biunivoca, cioè un'applicazione invertibile, $X \to Y$; si scrive $|X| = |Y|$. Si ha: $|X| = |X|$; $|X| = |Y| \implies |Y| = |X|$; $|X| = |Y|$, $|Y| = |Z| \implies |X| = |Z|$. Nel caso di insiemi finiti, la cardinalità di un insieme è determinata dal numero dei suoi elementi; nel caso di insiemi infiniti, un sottoinsieme (proprio) può avere la stessa cardinalità dell'insieme che lo contiene.

Confronto tra cardinalità: $|X| \leq |Y|$ sse esiste un'applicazione iniettiva $X \to Y$. Si ha: $|X| \leq |X|$; $|X| \leq |Y|$, $|Y| \leq |Z| \implies |X| \leq |Z|$. Se $X \subset Y$ allora $|X| \leq |Y|$. Dire che $|X| \leq |Y|$ è equivalente a dire che X è in corrispondenza biunivoca con un sottoinsieme di Y. Definizione alternativa: esiste un'applicazione iniettiva $X \to Y$ se e solo se esiste un'applicazione suriettiva $Y \to X$ (richiede la scelta).

Esempi: insiemi numerabili. $|\mathbb{N}| = |\mathbb{N} \setminus \{0\}|; |\mathbb{Z}| = |\mathbb{N}|; |\mathbb{N}| = |\mathbb{N} \times \{0, 1\}|; |\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$. L'unione (disgiunta) di insiemi numerabili è numerabile; l'unione numerabile (disgiunta) di insiemi numerabili è numerabile (richiede la scelta).

Enunciato del Teorema di Cantor-Schröder-Bernstein(-Dedekind-Zermelo): se $|X| \leq |Y|$ e $|Y| \leq |X|$, allora $|X| = |Y|$. Preparazione della dimostrazione.

2. LUNEDÌ 3 OTTOBRE 2022

Dimostrazione del Teorema di Bernstein-Schröder-Cantor.

Ogni insieme infinito contiene un sottoinsieme numerabile; $|\mathbb{N}| \leq |X|$ vuol dire che X è infinito; $|X| \leq |\mathbb{N}|$ vuol dire che X è finito o numerabile (= al più numerabile); l'unione di due insiemi numerabili (non necessariamente disgiunti) è numerabile; l'unione di un'infinita numerabile di insiemi (non necessariamente disgiunti) è numerabile. $\mathbb{Q}$ è numerabile.

Insiemi non numerabili. Teorema di Cantor: non esistono applicazioni suriettive da un insieme al suo insieme delle parti. Confronto stretto di cardinalità: si dice che $|X| < |Y|$ se $|X| \leq |Y|$ ma $|X| \neq |Y|$, cioè se esistono applicazioni iniettive $X \to Y$ ma nessuna di esse è invertibile. Riformulazione del Teorema di Cantor: $|X| < |2^X|$. Conseguenze: non esiste una cardinalità massima, pertanto alcune cose (l'unione di tutti gli insiemi, l'insieme di tutti gli insiemi, ecc...) non si possono fare (a meno di incorrere in contraddizioni). Perché la dimostrazione del Teorema di Cantor è detta *procedimento diagonale di Cantor*.

Cardinalità di $\mathbb{R}$. Alcune precisazioni sul modo di scrivere i numeri reali (in base 10, 2, ecc...). Un'applicazione iniettiva dalle parti di $\mathbb{N}$ in $\mathbb{R}$; un'applicazione suriettiva dalle parti di $\mathbb{N}$ in $[0, 2]$. $|\mathbb{R}| = |2^{\mathbb{N}}|$. Una dimostrazione diagonale della non numerabilità di $\mathbb{R}$ (cenni).

3. MARTEDÌ 4 OTTOBRE 2022

Aggiungere o rimuovere un insieme finito a/da un insieme numerabile lo lascia numerabile. L'unione numerabile di insiemi al più numerabile è al più numerabile. $\mathbb{Z}[x]$ è numerabile. Esistenza di numeri irrazionali per cardinalità. Esistenza di numeri trascendenti per cardinalità. Aggiungere o rimuovere un numero finito di elementi a/da un insieme infinito non ne cambia la cardinalità.

E' vero che le cardinalità di due insiemi sono sempre confrontabili? Assioma della scelta e Lemma di Zorn. Spiegazione dell'enunciato. Perché è necessario il Lemma di Zorn? Esempi di ragionamenti fallaci.

Applicazioni del Lemma di Zorn: ogni spazio vettoriale ammette una base; se X, Y sono insiemi, esiste un'applicazione iniettiva $X \to Y$ o $Y \to X$.

4. LUNEDÌ 10 OTTOBRE 2022

Ogni insieme infinito è ripartibile in sottoinsiemi tutti numerabili. Se X è infinito, allora $|X| = |X \times \{0, 1\}|$. Se X, Y sono insiemi infiniti, allora $|X \cup Y| = \max(|X|, |Y|)$. Se $X \subset Y$ soddisfa $|X| < |Y|$, allora $|Y \setminus X| = |Y|$.

Se X è infinito, allora $|X \times \mathbb{N}| = |X|$. Cardinalità di $X \times X$. Se X, Y sono insiemi infiniti tali che $|X| \leq |Y|$ allora $|X \times Y| = |Y|$.

5. MARTEDÌ 11 OTTOBRE 2022

Varie formulazioni dell'assioma della scelta. Teorema di Zermelo. Lemma di Zorn. Dal Teorema di Zermelo segue l'esistenza di un'inversa destra di ogni suriezione, da cui segue la forma tradizionale dell'assioma della scelta.

Buoni ordinamenti, segmenti iniziali e dimostrazione del Teorema di Zermelo a partire dal Lemma di Zorn.

Dimostrazione del Lemma di Zorn dall'assioma della scelta. (da finire)

6. LUNEDÌ 17 OTTOBRE 2022

Fine della dimostrazione del Lemma di Zorn a partire dall'assioma della scelta.

Numeri naturali e interi. Operazioni di somma e prodotto. Gergo algebrico. Gli interi formano un anello commutativo con unità. La relazione di divisibilità; suo rapporto con la relazione d'ordine naturale. La divisione euclidea.

Algoritmo euclideo per il calcolo del Massimo Comun Divisore. Nuova definizione del MCD: il MCD è unico a meno del segno. Identità di Bézout. Lemma di Euclide: se a divide bc e $\mathrm{MCD}(a,b)=1$, allora a divide c.

7. MARTEDÌ 18 OTTOBRE 2022

Elementi invertibili in $\mathbb{N}$ e $\mathbb{Z}$. Elementi primi e irriducibili in $\mathbb{Z}$. Numeri primi. Un intero è primo se e solo se è irriducibile. Definizioni alternative di numero (naturale) primo.

Esistenza della fattorizzazione di $n \neq 0$ nel prodotto di numeri primi in $\mathbb{N}$. Unicità della fattorizzazione. Un enunciato equivalente in $\mathbb{Z}$.

Applicazioni: la divisibilità si controlla tramite la fattorizzazione in primi; il MCD si calcola attraverso la fattorizzazione in primi; $\sqrt{2}$ è irrazionale; $\sqrt[k]{N}$ è razionale se e solo se N è una k-esima potenza perfetta. Un pianoforte è impossibile da accordare perfettamente. Esistono infiniti numeri primi.

Congruenze in $\mathbb{Z}$ modulo $n>1$. L'insieme quoziente $\mathbb{Z}/(n)$ possiede esattamente n elementi; le classi di congruenza sono classi di resto nella divisione euclidea per n. Le operazioni di somma e prodotto in $\mathbb{Z}$ ben definiscono analoghe operazioni in $\mathbb{Z}/(n)$ che lo rendono un anello commutativo con unità.

$\mathbb{Z}/(6)$ non è un dominio d'integrità. $\mathbb{Z}/(7)$ è un dominio d'integrità. $[a]$ è invertibile in $\mathbb{Z}/(n)$ se e solo se $\mathrm{MCD}(a,n)=1$. Se p è un numero primo, allora $\mathbb{Z}/(p)$ è un campo.

8. LUNEDÌ 24 OTTOBRE 2022

Alcune puntualizzazioni: ogni campo è un dominio d'integrità; non ogni dominio d'integrità è un campo; ogni dominio d'integrità finito è un campo. Un esempio di campo finito non del tipo $\mathbb{Z}/(p)$. Il piccolo teorema di Fermat. Esistono infiniti primi $\equiv 3 \mod 4$. Se $d=ha+kb$ divide sia a che b, allora $d=\mathrm{MCD}(a,b)$; in particolare $\mathrm{MCD}(ab,ac)=a\,\mathrm{MCD}(b,c)$. Se $d=\mathrm{MCD}(a,b)$, allora $\mathrm{MCD}(a/d,b/d)=1$.

Risoluzione di congruenze lineari. Se $\mathrm{MCD}(a,n)=1$, allora la congruenza $ax\equiv b \mod n$ ha un'unica soluzione intera modulo n, che si trova moltiplicando entrambi i membri per un inverso di a modulo n. Se $\mathrm{MCD}(a,n)$ non divide b, la congruenza $ax\equiv b \mod n$ non ha soluzioni intere. Se $d=\mathrm{MCD}(a,n)$ divide b, allora la congruenza $ax\equiv b \mod n$ è equivalente a $(a/d)x\equiv(b/d) \mod (n/d)$, nella quale si ha $\mathrm{MCD}(a/d,n/d)=1$.

Il Teorema Cinese dei Resti: se $\mathrm{MCD}(m,n)=1$, il sistema di congruenze

$$\begin{cases} x\equiv a \mod m \\ x\equiv b \mod n \end{cases}$$

ammette soluzioni intere per ogni scelta di $a,b\in\mathbb{Z}$. Le soluzioni sono uniche modulo mn. Tre dimostrazioni dell'enunciato.

9. MARTEDÌ 25 OTTOBRE 2022

Definire un'applicazione $F: X/\sim \to Y$ è equivalente a dare $f: X\to Y$ che soddisfi $x'\sim x'' \implies f(x')=f(x'')$. L'applicazione F è allora iniettiva se vale $x'\sim x'' \iff f(x')=f(x'')$. Se $\mathrm{MCD}(m,n)=1$, l'applicazione $\mathbb{Z}/(mn)\ni[x]\mapsto([x],[x])\in\mathbb{Z}/(m)\times\mathbb{Z}/(n)$ è ben definita, iniettiva e quindi anche suriettiva; è inoltre un omomorfismo di anelli.

Funzione toziente di Eulero. E' moltiplicativa: $\varphi(mn)=\varphi(m)\varphi(n)$ se $\mathrm{MCD}(m,n)=1$. Se p è un numero primo e $n>0$, allora $\varphi(p^n)=p^n-p^{n-1}$. Vale:

$$\varphi(N)=N\cdot\prod_{p \text{ primo divide } N}\left(1-\frac{1}{p}\right).$$

Gruppi. Definizione. Esempi. Sottogruppi. Esempi di sottogruppi. Sottogruppi ciclici. Classificazione dei sottogruppi di $\mathbb{Z}$.

Omomorfismi di gruppi. Se $f: G\to H$ è un omomorfismo di gruppi allora:

- $f(1)=1$;
- $f(x^{-1})=f(x)^{-1}$;
- l'immagine di f è un sottogruppo di H;
- il nucleo di f è un sottogruppo di G.

Congruenza modulo un sottogruppo: è una relazione di equivalenza. Se $f: G\to H$ è un omomorfismo di gruppi, allora $f(x')=f(x'') \iff x'\equiv x'' \mod \ker f$. (senza dimostrazione)

10. LUNEDÌ 7 NOVEMBRE 2022

Se $f: G\to H$ è un omomorfismo di gruppi, allora $f(x')=f(x'') \iff x'\equiv x'' \mod \ker f$; in particolare, f è iniettiva se e solo se $\ker f=(1)$.

Ordine di elementi. Definizione: un elemento $g\in G$ ha ordine finito $o(g)=d>0$ se d è il più piccolo intero positivo tale che $x^d=1$, e ha ordine infinito altrimenti. Definizione alternativa: $o(g)=|(g)|$. L'elemento neutro di G

è l'unico elemento di ordine 1. Un elemento g e il suo inverso g^{-1} hanno lo stesso ordine. In un gruppo finito, ogni elemento ha ordine finito. Se G è un gruppo abeliano finito, e $g \in G$, allora $o(g)$ divide $|G|$.

Conseguenze aritmetiche. Se $n[a] = [0]$ in $\mathbb{Z}/(n)$ (poco interessante). $[a]^p = [a]$ in $\mathbb{Z}/(p)$ se p è primo. Se $\mathrm{MCD}(a, n) = 1$, allora $a^{\varphi(n)} \equiv 1 \mod n$. Lunghezza del periodo di $1/n$ quando $\mathrm{MCD}(10, n) = 1$. Esistono infiniti numeri primi $\equiv 1 \mod 4$. Esistono infiniti numeri primi $\equiv 1 \mod 6$.

Enunciato del Teorema di Lagrange: se G è un gruppo finito e $H < G$, allora $|H|$ divide $|G|$.

11. MARTEDÌ 8 NOVEMBRE 2022

Dimostrazione del Teorema di Lagrange: le classi di congruenza modulo H sono le classi laterali sinistre aH di H in G. L'applicazione $H \ni h \mapsto ah \in aH$ è una corrispondenza biunivoca. Se $[G : H]$ indica la cardinalità dell'insieme delle classi di congruenza modulo H in G, allora $|G| = [G : H]|H|$; in particolare, se G è un gruppo finito, allora $|H|$ divide $|G|$. L'ordine di un elemento g di un gruppo finito G divide $|G|$. Un gruppo ciclico infinito è isomorfo a $(\mathbb{Z}, +)$. Un gruppo ciclico di ordine n è isomorfo a $(\mathbb{Z}/(n), +)$: cenni di dimostrazione. In particolare i gruppi ciclici sono tutti abeliani. Elenco completo dei sottogruppi di S_3. Tavola moltiplicativa di un (eventuale) gruppo non ciclico di ordine 4.

Esempi: il gruppo delle manipolazioni del cubo di Rubik: è un gruppo finito di ordine multiplo di 4. Lunghezza del periodo dell'espansione decimale di $1/n$ quando $\mathrm{MCD}(10, n) = 1$: è l'ordine moltiplicativo di $[10]$ nel gruppo moltiplicativo $\mathbb{Z}/(n)^\times$, e divide quindi $\varphi(n)$.

Sottogruppi normali. Il nucleo di un omomorfismo di gruppi è un sottogruppo normale. Relazioni di equivalenza su un gruppo G sulle cui classi l'operazione di G ben definisce un'operazione: sono le classi di congruenza modulo un sottogruppo normale di G. Definizioni equivalenti della normalità. I sottogruppi banali sono normali. Un sottogruppo di indice 2 è sempre normale. Un sottogruppo di un gruppo abeliano è sempre normale.

Notazione ciclica nei gruppi simmetrici. Ordine di una permutazione. $\langle(12)\rangle$ è un sottogruppo non normale di S_3. $\langle(123)\rangle$ è un sottogruppo normale di S_3.

12. LUNEDÌ 14 NOVEMBRE 2022

Risoluzione di esercizi. Il *rompicapo dei cappelli* e l'assioma della scelta. Conversione approssimativa tra miglia e km attraverso i numeri di Fibonacci.

13. MARTEDÌ 15 NOVEMBRE 2022

Il concetto di isomorfismo tra gruppi. Prodotto diretto (esterno) di gruppi. $\mathbb{Z}/(2) \times \mathbb{Z}/(3)$ è ciclico di ordine 6. Teorema cinese dei resti: $\mathbb{Z}/(m) \times \mathbb{Z}/(n)$ è isomorfo a $\mathbb{Z}/(mn)$ se $\mathrm{MCD}(m, n) = 1$. Classificazione dei gruppi di ordine 4: $\mathbb{Z}/(2) \times \mathbb{Z}/(2)$ è l'unico, a meno di isomorfismi, gruppo non ciclico di ordine 4.

Un gruppo di ordine pari possiede elementi di ordine 2. Un gruppo in cui ogni elemento ha ordine 1 o 2 è necessariamente abeliano. Struttura dei gruppi di ordine 6: un gruppo non ciclico di ordine 6 possiede elementi di ordine 2 e 3 che non commutano tra loro. Ogni gruppo non ciclico di ordine 6 è isomorfo a S_3. Gruppi diedrali. $|D_n| = 2n$. $D_3 = S_3$. Gruppi alterni. Segno di una permutazione. $[S_n : A_n] = 2$ se $n > 1$.

Teorema di omomorfismo per gruppi. Dare un omomorfismo $G/N \to H$ è la stessa cosa che dare un omomorfismo $G \to H$ che abbia N nel suo nucleo. Dare un isomorfismo $G/N \to H$ è la stessa cosa che dare un omomorfismo suriettivo $G \to H$ il cui nucleo coincida con N.

Omomorfismi $(\mathbb{Z}, +) \to G$ e $(\mathbb{Z}/(n), +) \to G$. Ogni gruppo ciclico di ordine n è isomorfo a $(\mathbb{Z}/(n), +)$.

14. LUNEDÌ 21 NOVEMBRE 2022

Primo teorema di isomorfismo: se $f : G \to H$ è un omomorfismo di gruppi, allora $\mathrm{Im}\, f \simeq G/\ker f$.

Sottogruppi di G/N dove $N \lhd G$. Preliminari: se $f : G_1 \to G_2$ è un omomorfismo di gruppi, allora

- $H < G_1 \implies f(H) < G_2$
- $K < G_2 \implies f^{-1}(K) < G_1$
- $H < G_1 \implies f^{-1}(f(H)) = H \cdot \ker f$
- $K < G_2 \implies f(f^{-1}(K)) = K \cap \mathrm{Im}\, f$.

Inoltre se $K \lhd G_2$ allora $f^{-1}(K) \lhd G_1$ e se $H \lhd G_1$ allora $f(H) \lhd \mathrm{Im}\, f$; in particolare $f(H) \lhd G_2$ non appena f è suriettiva.

Esiste una corrispondenza biunivoca tra sottogruppi di G che contengono N e sottogruppi di G/N data da $H \mapsto \pi(H)$ dove $\pi : G \to G/N$ è la proiezione al quoziente. La sua inversa è $\overline{H} \mapsto \pi^{-1}(\overline{H})$. Questa corrispondenza preserva inclusioni e normalità.

Crittografia RSA.

15. MARTEDÌ 22 NOVEMBRE 2022

Preliminari: se $f : G \to H$ è un omomorfismo tra gruppi finiti, allora l'ordine di $x \in G$ divide l'ordine di $f(x) \in H$. Teorema di Cauchy (per gruppi abeliani finiti). Due omomorfismi $\phi, \psi : G \to H$ coincidono su un sottogruppo di G; pertanto due se $\phi \neq \psi$ e G è finito, differiscono su almeno la metà degli elementi di G.

Chiacchiere su complessità algoritmica: complessità della somma; complessità della moltiplicazione à la Karatsuba; difficoltà della fattorizzazione; esistenza di algoritmi polinomiali di primalità.

Residui quadratici. Simbolo di Legendre. Se p è un primo dispari e a un intero, si ha

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p.$$

Il simbolo di Legendre è moltiplicativo. Calcolo di $\left(\frac{2}{p}\right)$. Enunciato della legge di reciprocità quadratica e suo uso nel calcolo del simbolo di Legendre. Simbolo di Jacobi. Generalizzazione della reciprocità quadratica. Calcolo rapido del simbolo di Jacobi (e quindi di quello di Legendre) per mezzo di una discesa euclidea.

Teorema di Solovay-Strassen: se l'intero $N > 0$ non è primo, allora

$$\left(\frac{a}{N}\right) \not\equiv a^{\frac{N-1}{2}} \mod N$$

per almeno un valore di a primo con N. Se N non è primo, almeno la metà delle scelte di $0 \leq a < N$ contraddicono la congruenza o forniscono un simbolo di Jacobi nullo, confermando la non primalità di N. Algoritmo probabilistico di primalità di Solovay-Strassen.

16. LUNEDÌ 28 NOVEMBRE 2022

Dimostrazione (grafica) della legge di reciprocità quadratica e della sua generalizzazione al simbolo di Jacobi.

Teorema di Cauchy per gruppi finiti (anche non abeliani). Se $H, K < G$, allora $HK < G$ se e solo se $HK = KH$ (solo enunciato). In particolare, se $H < G, N \lhd G$ allora HN è un sottogruppo di G.

17. MARTEDÌ 29 NOVEMBRE 2022

Due modi per mostrare che $(p-1)! \equiv -1 \mod p$ quando p è primo. Se $H, K < G$ allora $HK < G$ se e solo se $HK = KH$. Se $H, K < G$ sono finiti, allora $|HK| = |H||K|/|H \cap K|$. Un esempio in cui $HK = KH$ ma né H, né K sono normali.

Gruppi che sono prodotto diretto di propri sottogruppi. Se G è prodotto diretto di $H, K < G$, allora G è isomorfo a $H \times K$. Classificazione dei gruppi di ordine 8. I gruppi $C_8, C_4 \times C_2, C_2 \times C_2 \times C_2, D_4, Q_8$ sono a due a due non isomorfi. Ogni gruppo di ordine 8 è isomorfo a esattamente uno di essi.

Criteri di divisibilità per $2, 3, 4, 6, 9, 11$ e anche per 7.

18. LUNEDÌ 5 DICEMBRE 2022

Automorfismi di gruppi. Gli automorfismi di un gruppo G formano un gruppo rispetto alla composizione, nel quale l'elemento neutro è id_G. L'applicazione che manda ogni elemento di G nel suo inverso è un automorfismo di G esattamente quando G è abeliano. Se G è abeliano, l'applicazione che manda ciascun x nella sua k-esima potenza è un omomorfismo $G \to G$, ed è un automorfismo se G è finito e $\mathrm{MCD}(k, |G|) = 1$. Automorfismi interni. L'applicazione $T : G \to \mathrm{Aut}(G)$ che associa a ciascun $g \in G$ l'automorfismo interno T_g indotto da g è un omomorfismo di gruppi, la cui immagine è il sottogruppo $\mathrm{Int}(G) < \mathrm{Aut}(G)$ degli automorfismi interni di G, e il cui nucleo è il sottogruppo normale $Z(G) \lhd G$ detto *centro* di G. Per il teorema di isomorfismo, $\mathrm{Int}(G) \simeq G/Z(G)$. Il sottogruppo $\mathrm{Int}(G)$ è normale in $\mathrm{Aut}(G)$.

Alcuni gruppi di automorfismi: l'unico automorfismo di un gruppo di ordine 2 è l'identità; gli automorfismi di $(\mathbb{Z}, +)$ sono l'identità e quello che manda ogni elemento nel suo inverso; ogni permutazione di a, b, c induce un automorfismo di $V_4 = \{1, a, b, c\}$; gli automorfismi di S_3 sono sei, e sono tutti interni; $\mathrm{Aut}(\mathbb{Z}/(n), +) \simeq \mathbb{Z}/(n)^\times$.

Prodotto semidiretto di gruppi. Se $\phi : H \ni h \mapsto \phi_h \in \mathrm{Aut}(N)$ è un omomorfismo di gruppi, l'operazione

$$(n_1, h_1) \cdot (n_2, h_2) := (n_1 \phi_{h_1}(n_2), h_1 h_2)$$

definisce una struttura di gruppo sul prodotto cartesiano $N \times H$. Questo gruppo si chiama *prodotto semidiretto di N con H tramite ϕ* e si indica con $N \rtimes_\phi H$. Quando ϕ manda ogni elemento di H in id_N, questa struttura si riduce al prodotto diretto di N con H.

Gruppi che sono prodotto semidiretto di propri sottogruppi.

19. MARTEDÌ 6 DICEMBRE 2022

Se G è prodotto semidiretto del suo sottogruppo normale N con il sottogruppo H, allora $G \simeq N \rtimes_\phi H$ dove $\phi : H \to \mathrm{Aut}(N)$ soddisfa $\phi_h(n) = hnh^{-1}$. Esempio: un gruppo non abeliano di ordine 21.

La relazione di coniugio. E' una relazione di equivalenza. Elementi coniugati hanno lo stesso ordine. Un elemento è il solo proprio coniugato esattamente quando è centrale. Classi di coniugio in S_3. Centralizzatore di un elemento. Il numero di coniugati di x in G è uguale a $[G : Z(x)]$. La cardinalità di ciascuna classe di coniugio in un gruppo finito G divide $|G|$. Equazione delle classi. Se G non è abeliano, allora $G/Z(G)$ non è ciclico; in particolare, il centro di un gruppo non ha indice primo.

Un gruppo di ordine 35 è necessariamente abeliano, e quindi ciclico. Se $p < q$ sono primi e p non divide $q - 1$, allora un gruppo di ordine pq è necessariamente abeliano, e quindi ciclico. Descrizione dei gruppi di ordine pq per mezzo del prodotto semidiretto.

Gruppi di ordine p^k, dove p è primo e $k > 1$: hanno elementi centrali diversi dall'identità. Se $|G| = p^2$ e p è primo, allora G è abeliano. Se $|G| = p^2$, allora G è isomorfo a $\mathbb{Z}/(p^2)$ oppure a $\mathbb{Z}/(p) \times \mathbb{Z}/(p)$. Gruppi di ordine < 16 e diverso da 12.

20. LUNEDÌ 12 DICEMBRE 2022

Classi di coniugio in S_n. Sottogruppi normali di S_5. Sottogruppi normali di $S_n, n \geq 5$. Classi di coniugio in A_5. Semplicità di A_5. Immersione di Cayley e gruppi di ordine $2d$, quando d è dispari.

21. MARTEDÌ 13 DICEMBRE 2022

Matrici di permutazione. Immersione di S_n in $\mathrm{GL}_n(K)$. Se K è un campo, ogni gruppo di ordine n si immerge in $\mathrm{GL}_n(K)$. Enunciato del Teorema di Sylow. Esempi: gruppi di ordine p^k; gruppi abeliani; $\mathrm{GL}_n(\mathbb{F}_p)$; p-sottogruppi di Sylow quando p non divide l'ordine del gruppo.

Laterali doppi. $|HxK| = |H| \cdot |K|/|H \cap xKx^{-1}|$. Se G possiede p-sottogruppi di Sylow, e $H < G$, allora H possiede p-sottogruppi di Sylow, e uno di tali sottogruppi è della forma $H \cap xPx^{-1}$. Conseguenze: i p-Sylow di un gruppo sono tutti coniugati; ogni sottogruppo di ordine una potenza di p è contenuto in un p-Sylow; l'unione dei p-Sylow in un gruppo contiene tutti e soli gli elementi di ordine una potenza di p.

Normalizzatore $N_G(H)$ di un sottogruppo $H < G$: è il più grande sottogruppo di G nel quale H è normale. Se $H < G$, allora $xHx^{-1} = yHy^{-1}$ esattamente quando x, y giacciono nello stesso laterale sinistro di $N(H)$. Il numero dei coniugati di H in G coincide con $[G : N(H)]$. Il numero di p-Sylow in un dato gruppo è $\equiv 1 \mod p$.

Tre esempi: 5-Sylow in S_5; 3-Sylow in A_4; un gruppo di ordine 35 ha i sottogruppi di Sylow normali e ne è quindi prodotto diretto.

22. LUNEDÌ 19 DICEMBRE 2022

Risoluzione di esercizi.

23. MARTEDÌ 20 DICEMBRE 2022

Risoluzione di esercizi.

Secondo semestre

24. MARTEDÌ 28 FEBBRAIO 2023

Breve panoramica del secondo semestre. Anelli, anelli commutativi, anelli con unità. In un anello $0 \cdot a = a \cdot 0 = 0$, $(-1) \cdot a = -a$, $-(a+b) = -a + (-b)$ per ogni scelta di a, b. Omomorfismi di anelli. Se A, B sono anelli con unità e $f : A \to B$ è un omomorfismo di anelli, $f(1) = 1$ può non valere, ma è automatico se f è suriettivo. Nel corso, tutti gli anelli saranno commutativi con unità.

Sottoanelli e ideali. L'immagine di un omomorfismo di anelli è un sottoanello; il nucleo di un omomorfismo di anelli è un ideale. Esempi di ideali: ideali banali; ideali di $\mathbb{Z}$; ideali di un campo; ideali principali. Un anello commutativo con unità i cui unici ideali sono quelli banali è necessariamente un campo.

Anello quoziente. Se $I \subsetneq A$ è un ideale proprio, allora la proiezione al quoziente $\pi : A \to A/I$ è un omomorfismo di anelli il cui nucleo coincide con I. Corrispondenza tra ideali di A/I e ideali di A che contengono I. Ideali primi e massimali. Esempi: (0) è un ideale primo di A se e solo se A è un dominio d'integrità; (2) è primo e massimale in $\mathbb{Z}$; (5) è primo e massimale in $\mathbb{Z}$. Un ideale $I \subsetneq A$ è primo se e solo se A/I è un dominio d'integrità. *3 ore.*

25. MARTEDÌ 7 MARZO 2023

Un ideale $I \subsetneq A$ è massimale se e solo se A/I è un campo ed è primo se e solo se A/I è un dominio d'integrità. In particolare, I è primo non appena sia massimale. Panoramica sugli ideali di $\mathbb{Z}$: sono della forma (d), dove $d \geq 0$; (0) è primo ma non massimale; (p) è primo e massimale se e solo se $p > 1$ è un numero primo.

Teorema di omomorfismo per anelli. Se $f : A \to B$ è un omomorfismo di anelli e $I \subset A$ è un ideale, allora esiste un omomorfismo di anelli $F : A/I \to B$ tale che $f = F \circ \pi$, dove $\pi : A \to A/I$ è la proiezione al quoziente, se e solo se $I \subset \ker f$. Inoltre F è iniettivo esattamente quando $\ker f = I$ e le immagini di F e f coincidono. In particolare, il sottoanello $\operatorname{Im} f \subset B$ è isomorfo al quoziente $A/\ker f$.

Anelli di polinomi. Se D è un dominio d'integrità, allora anche $D[x]$ lo è; il grado del prodotto di polinomi è la somma dei gradi dei fattori. $A[x]$ non è mai un campo. Alcuni ideali di $\mathbb{Z}[x]$: (0) è primo ma non massimale; $(2) = 2\mathbb{Z}[x]$ è primo ma non massimale; $(2, x)$ è un ideale massimale e non è principale.

Ideali di $\mathbb{Q}[x]$. Esistenza di una divisione euclidea in $\mathbb{Q}[x]$. *6 ore.*

26. VENERDÌ 10 MARZO 2023

Definizione di dominio euclideo. Primi esempi (motivanti): $\mathbb{Z}$; $K[x]$, quando K è un campo. In un dominio euclideo, ogni ideale non nullo è principale, ed è generato da ciascun suo elemento non nullo di norma euclidea minima. In un dominio euclideo, gli elementi invertibili sono tutti e soli quelli che hanno norma euclidea minima, cioè uguale a quella dell'unità.

Altri esempi di dominio euclideo: campi; l'anello $\mathbb{Z}[i]$ degli interi di Gauss. Definizione di $\mathbb{Z}[i]$ come sottoanello di $\mathbb{C}$: si tratta di un dominio d'integrità. Norma euclidea di $\mathbb{Z}[i]$. Divisione euclidea in $\mathbb{Z}[i]$. Elementi invertibili di $\mathbb{Z}[i]$. Serie formali: definizione e operazioni. Norma euclidea nell'anello delle serie formali a coefficienti in un campo. *8 ore.*

27. MARTEDÌ 14 MARZO 2023

Se A è un anello, $A[[x]]$ è un anello. Se D è un dominio d'integrità, $D[[x]]$ è un dominio d'integrità. Se K è un campo, $K[[x]]$ è un dominio euclideo rispetto alla norma euclidea che misura il grado del primo monomio non nullo. Invertibili di $K[[x]]$. Ideali di $K[[x]]$. $\mathbb{Z}[[x]]$ non è un dominio a ideali principali.

Serie di Laurent a coefficienti in un campo. Sono un dominio euclideo rispetto alla norma che misura la differenza tra i grado massimo e il grado minimo dei monomi non nulli.

Divisibilità in domini a ideali principali. a divide b se e solo se $(b) \subset (a)$. Riflessività e transitività della divisibilità. Se a divide b e divide a allora $(a) = (b)$ e a, b si ottengono l'uno dall'altro tramite moltiplicazione per un invertibile (sono associati).

Significato di $(a) \cap (b), (a) + (b)$ in un dominio a ideali principali. Definizione di massimo comun divisore. In un dominio d'integrità, due massimi comuni divisori di due elementi dati sono sempre associati. Il massimo comun divisore è definito a meno di moltiplicazione per un invertibile. In un dominio a ideali principali, il massimo comun divisore di a, b esiste sempre, ed è ciascun elemento d tale che $(a) + (b) = (d)$. Identità di Bézout. Un esempio di calcolo in $\mathbb{Z}[i]$: $\mathrm{MCD}(9 + 7i, 15 - i) = 1 - i$.

Elementi primi e irriducibili in un dominio d'integrità. Ogni elemento primo è automaticamente irriducibile. In un dominio a ideali principali, se $c|ab$ e $\mathrm{MCD}(c, a) = 1$, allora $c|b$. In un dominio a ideali principali, ogni elemento irriducibile è necessariamente primo.

Traduzione in ideali dei concetti di primalità e irriducibilità. In ogni dominio d'integrità, p è primo se e solo se (p) è un ideale primo, ed è irriducibile se e solo se (p) è massimale tra gli ideali principali. In particolare, in un dominio a ideali principali, p irriducibile $\implies$ (p) massimale $\implies$ (p) primo $\implies$ p primo. *11 ore.*

28. VENERDÌ 17 MARZO 2023

In un dominio d'integrità, $p \neq 0$ è irriducibile $\iff$ l'ideale (p) è massimale tra gli ideali principali. In particolare, se in un dominio d'integrità l'ideale (p) è massimale, allora $p \neq 0$ è automaticamente irriducibile; viceversa, se in un dominio a ideali principali p è irriducibile, allora (p) è automaticamente massimale. In conclusione, in un dominio a ideali principali, p è irriducibile $\iff$ (p) è un ideale massimale $\iff$ (p) è un ideale primo $\iff$ p è primo.

In un dominio d'integrità, $(a) \subsetneq (b)$ è equivalente a dire che b divide a ma $0 \neq a, b$ non sono associati; in altre parole, $a = bc$ e c non è invertibile. In un dominio euclideo, se $0 \neq a = bc$ è una fattorizzazione non banale di a, allora $N(b), N(c) < N(a)$.

Teorema di fattorizzazione unica per domini euclidei. Esistenza della fattorizzazione (fa uso della norma euclidea); unicità della fattorizzazione (non fa uso della norma euclidea e funziona in qualsiasi dominio a ideali principali).

Esempi. Fattorizzazione unica in $\mathbb{C}[x]$: gli irriducibili sono tutti e soli i polinomi di grado 1 e la fattorizzazione unica mostra l'esistenza di $0 \neq c$ e di $\alpha_1, \ldots, \alpha_k$ tali che $f(x) = c(x - \alpha_1) \ldots (x - \alpha_k)$. Fattorizzazione unica in $\mathbb{R}[x]$: gli irriducibili sono tutti e soli i polinomi di grado 1 e quelli di grado 2 privi di radici reali. Affermazioni generali: in $K[x]$, dove K è un campo, i polinomi di grado 1 sono tutti irriducibili; i polinomi di grado 2 e 3 sono irriducibili se e solo se sono privi di radici in K; i polinomi di grado più alto non sono irriducibili se hanno radici in K, ma possono essere riducibili anche quando sono privi di radici in K.

Fattorizzazione unica in $K[[x]]$. L'unico irriducibile, a meno di associati, è x. Ogni $a(x) \neq 0$ si scrive in modo unico nella forma $a(x) = u(x)x^k$ dove $u(x)$ è invertibile. *13 ore.*

29. MARTEDÌ 21 MARZO 2023

Fattorizzazione unica in domini a ideali principali. Divisibilità (propria) e inclusione (propria) di ideali. Accade $(a) + (b) = (d)$ esattamente quando d divide sia a che b e vale l'identità di Bézout per d; in tal caso d è MCD di a, b.

La condizione della catena ascendente. In un dominio a ideali principali, ogni catena ascendente infinita di inclusioni di ideali si stabilizza; equivalentemente, ogni catena ascendente di inclusioni proprie di ideali è finita. Chiacchiere brevi sulla noetherianità.

Conseguenze: ogni ideale proprio non nullo (d) di un dominio a ideali principali è contenuto in un ideale massimale; equivalentemente, ogni elemento non nullo e non invertibile possiede un divisore irriducibile. In un dominio a ideali principali, ogni elemento non nullo si scrive come prodotto di un invertibile e di un prodotto finito di primi/irriducibili.

Un esempio di un dominio d'integrità nel quale ogni ideale finitamente generato è principale, ma non ogni ideale è principale. Nel dominio d'integrità $\mathbb{R}[x^{1/2^n}, n \in \mathbb{N}]$ la catena ascendente di ideali

$$(x) \subsetneq (x^{1/2}) \subsetneq (x^{1/4}) \subsetneq \ldots$$

non si stabilizza, ma esiste un MCD di ogni coppia di elementi e vale l'identità di Bézout. Pertanto, ogni ideale finitamente generato è principale. L'elemento non invertibile x non ammette divisori irriducibili.

Primalità tra gli interi di Gauss. Nell'anello $\mathbb{Z}[i]$, gli elementi $1 + i, 3$ sono irriducibili, mentre 2 non lo è. Vale $2 = -i(1 + i)^2$. Ogni primo di Gauss divide un naturale; ogni primo di Gauss divide un naturale primo; i primi di Gauss sono tutti e soli i divisori irriducibili dei primi naturali. Esempi: $2 = (1 + i)(1 - i); 5 = (2 + i)(2 - i)$. Un numero primo che non è somma di due quadrati interi è irriducibile in $\mathbb{Z}[i]$. I numeri primi $\equiv 3 \mod 4$ sono irriducibili in $\mathbb{Z}[i]$. Se un numero primo p soddisfa $p = a^2 + b^2$, allora $p = (a + bi)(a - bi)$ è una fattorizzazione di p in irriducibili di $\mathbb{Z}[i]$.

Identità di Wilson: quando p è un numero primo, si ha $(p - 1)! \equiv -1 \mod p$. Se $p \equiv 1 \mod 4$ è primo, allora

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv -1 \mod p.$$

Posto $\ell = ((p - 1)/2)!$, quando $p \equiv 1 \mod 4$ è primo si ha che p divide $\ell^2 + 1 = (\ell + i)(\ell - i)$ ma non divide $\ell \pm i$ in $\mathbb{Z}[i]$. Di conseguenza p non è primo, è riducibile, ed è pertanto somma di due quadrati. A meno di elementi associati, una lista completa di elementi primi di $\mathbb{Z}[i]$ è la seguente:

- $1 + i$;
- ogni numero primo $q \equiv 3 \mod 4$:
- $a \pm bi$, dove $a, b \in \mathbb{N}$ e $a^2 + b^2 = p \equiv 1 \mod 4$ è un numero primo. *16 ore.*

30. MARTEDÌ 28 MARZO 2023

Nuovi esempi. $\mathbb{Z}[\sqrt{-2}]$ è un dominio euclideo. Invece, $\mathbb{Z}[\sqrt{-3}]$ non è un dominio euclideo rispetto alla norma $N(a + b\sqrt{-3}) = a^2 + 3b^2$; in effetti, non è nemmeno un dominio a ideali principali, in quanto 2 è un elemento irriducibile ma non primo (esercizio!).

Come rendere veramente unica la fattorizzazione unica in domini a ideali principali: è sufficiente scegliere, per ciascuna classe di primi a due a due associati tra loro, un singolo rappresentante privilegiato. Esempi pratici: in $\mathbb{Z}$, si può prendere il primo positivo; in $\mathbb{Z}[i]$ si può prendere $a + bi$, con $a > |b|$ e $1 + i$ nel caso di $\pm 1 \pm i$; in $K[x]$ si può prendere l'unico polinomio monico.

Identità di Brahmagupta-Fibonacci: $(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$. Il Teorema dei due quadrati: un naturale $n \neq 0$ è somma di due quadrati perfetti esattamente quando, nella sua fattorizzazione in numeri primi, ciascuno di quelli $\equiv 3 \mod 4$ compare un numero pari di volte.

Se D è un dominio a ideali principali e $0 \neq d \in D$, allora $[a]$ è moltiplicativamente invertibile in $D/(d)$ se e solo se $\mathrm{MCD}(a, d) = 1$; in particolare, $D/(d)$ è un campo esattamente quando d è irriducibile (= primo). Un esempio in $\mathbb{Z}[i]$. L'anello quoziente $\mathbb{R}[x]/(x^2 + 1)$. E' un campo; i suoi elementi sono tutti (in modo unico) della forma $[a + bx]$, dove $a, b \in \mathbb{R}$. Somma e prodotto di tali elementi. Isomorfismo con $\mathbb{C}$.

Generalizzazione: se $f(x) = f_0 + f_1x + \ldots + f_nx^n \in K[x]$ ha grado n, allora gli elementi dell'anello quoziente $K[x]/(f(x))$ sono tutti (in modo unico) della forma $r_0 + r_1x + \ldots + r_{n-1}x^{n-1}$. Inoltre l'applicazione

$$K \ni c \mapsto [c] \in K[x]/(f(x))$$

è un omomorfismo iniettivo (= immersione) di K in $K[x]/(f(x))$ e l'elemento $[x] \in K[x]/(f(x))$ è una radice di $f(x)$. In altre parole, l'anello quoziente $K[x]/(f(x))$ *amplia* K *con una radice di* $f(x)$. *19 ore.*

31. VENERDÌ 31 MARZO 2023

L'anello quoziente $A = K[x]/(f(x))$, dove $f(x) \in K[x]$ è un polinomio di grado n: è linearmente isomorfo allo spazio vettoriale $K[x]_{<n}$ di grado minore di n; contiene una copia di K data dalle classi di congruenza dei polinomi costanti; contiene l'elemento $\alpha = [x]$ che annulla il polinomio $f(x)$; è un campo se $f(x)$ è irriducibile.

Esempi: $\mathbb{R}[x]/(x^2+1)$; $\mathbb{R}[x]/(x-c)$ è isomorfo a $\mathbb{R}$ e l'elemento $[x]$ coincide con c; l'anello $\mathbb{R}[x]/(x^2)$ dei *numeri duali reali*. Prodotto cartesiano (o somma diretta) di anelli; teorema cinese dei resti: se I, J sono ideali di A tali che $I + J = A$, allora $A/I \cap J \simeq A/I \times A/J$. L'anello quoziente $\mathbb{R}[x]/(x(x-1))$ è isomorfo a $\mathbb{R}[x]/(x) \times \mathbb{R}[x]/(x-1)$.

Fattorizzazione in $\mathbb{Z}[x]$ e Lemma di Gauss. Invertibili in $\mathbb{Z}[x]$. Confronto tra irriducibilità in $\mathbb{Z}[x]$ e in $\mathbb{Q}[x]$. $2x^2+2$ è irriducibile in $\mathbb{Q}[x]$ ma non in $\mathbb{Z}[x]$, semplicemente perché $\mathbb{Z}$ e $\mathbb{Q}$ hanno invertibili diversi.

Contenuto di un polinomio e polinomi primitivi. *21 ore.*

32. MARTEDÌ 4 APRILE 2023

Se R è un dominio a fattorizzazione unica, allora anche $R[x]$ è un dominio a fattorizzazione unica. Commenti sull'enunciato. Definizione di dominio a fattorizzazione unica: un dominio d'integrità si dice *dominio a fattorizzazione unica* se ogni elemento diverso da 0 non invertibile si scrive come prodotto (finito) di elementi irriducibili e ogni irriducibile è primo; equivalentemente, se si scrive come prodotto (finito) di elementi primi. Fatti da dimostrare in seguito: ogni dominio d'integrità si immerge nel suo campo di frazioni; in un dominio a fattorizzazione unica ogni famiglia finita di elementi non nulli ammette massimo comun divisore e $\mathrm{MCD}(ab_1, \ldots, ab_n) = a\,\mathrm{MCD}(b_1, \ldots, b_n)$.

Varie forme del Lemma di Gauss. Se $p \in \mathbb{Z}$ è primo, allora p è anche primo in $\mathbb{Z}[x]$. Il prodotto di polinomi primitivi è primitivo. Il contenuto del prodotto di polinomi è il prodotto dei contenuti dei polinomi. Ogni elemento non nullo di $\mathbb{Z}[x]$ si scrive come prodotto di elementi primi in $\mathbb{Z}$ e di polinomi primitivi non costanti irriducibili in $\mathbb{Z}[x]$.

Se un polinomio primitivo $f(x) \in \mathbb{Z}[x]$ divide $a(x) \in \mathbb{Z}[x]$ in $\mathbb{Q}[x]$, allora lo divide anche in $\mathbb{Z}[x]$. Un polinomio primitivo $f(x) \in \mathbb{Z}[x]$ è irriducibile in $\mathbb{Z}[x]$ se e solo se è irriducibile in $\mathbb{Q}[x]$. Un polinomio primitivo, non costante, irriducibile in $\mathbb{Z}[x]$ è anche primo in $\mathbb{Z}[x]$. Campo delle frazioni di un dominio d'integrità. Se D è un dominio d'integrità, e K_D è il suo campo delle frazioni, allora esiste un omomorfismo iniettivo $D \to K_D$. Divisibilità e fattorizzazione in un dominio a fattorizzazione unica. *24 ore.*

33. VENERDÌ 14 APRILE 2023

Se A è un dominio a ideali principali oppure un campo, allora $A[x_1, \ldots, x_n]$ è un dominio a fattorizzazione unica. Un'applicazione: il determinante di Vandermonde. Se A, B sono anelli, dare un omomorfismo di anelli $A[x] \to B$ è equivalente a dare un omomorfismo $A \to B$ e a scegliere in B l'immagine di x; esempi.

Criteri di irriducibilità. Radici razionali di polinomi a coefficienti interi. Riduzione modulo un primo p. Criterio di irriducibilità di Eisenstein: inizio della dimostrazione. *26 ore.*

34. MARTEDÌ 18 APRILE 2023

Se in $D[x]$, dove D è un dominio d'integrità, il prodotto di due polinomi è un monomio, allora i due polinomi sono entrambi monomi. Fine della dimostrazione del Criterio di irriducibilità di Eisenstein. Applicazioni: $x^5 - 2$ è irriducibile in $\mathbb{Z}[x]$; il p-esimo polinomio ciclotomico, dove p è primo, è irriducibile. I polinomi $x^4 + 2, x^4 + 9$ sono irriducibili, mentre $x^4 + 4$ non lo è. Il polinomio $x^4 + 16$ è irriducibile, ma la sua riduzione modulo p è riducibile per ogni scelta di p primo, e il Criterio di Eisenstein non è applicabile nemmeno dopo una traslazione.

Moduli su anelli. Definizione. Sottomoduli. Il concetto di $\mathbb{Z}$-modulo è equivalente a quello di gruppo abeliano; il concetto di $K[x]$-modulo è equivalente a quello di K-spazio vettoriale dotato di un endomorfismo K-lineare. Gli A-sottomoduli dell'A-modulo A sono tutti e soli gli ideali di A. Somma diretta di moduli; somma diretta di sottomoduli; non tutti i sottomoduli di $M_1 \oplus M_2$ sono della forma $N_1 \oplus N_2$ dove $N_i \subset M_i$ è un sottomodulo. Non ogni A-modulo è isomorfo ad un A-modulo della forma A^n. Somma e intersezione di sottomoduli.

Omomorfismi di A-moduli. Immagine e nucleo di un omomorfismo. Teoremi di omomorfismo e isomorfismo per A-moduli. *29 ore.*

35. VENERDÌ 21 APRILE 2023

Generatori di A-moduli e sottomoduli generati da un sottoinsieme. Gli elementi $m_1, \ldots, m_k \in M$ sono generatori di M esattamente quando l'applicazione indotta $f : A^k \to M$ è suriettiva; tale omomorfismo di A-moduli è iniettivo se e solo se gli elementi sono A-linearmente indipendenti. Patologie dell'indipendenza lineare quando A non è un campo: vari esempi e controesempi. Struttura degli A-moduli ciclici. Descrizione degli A-moduli finitamente generati come quozienti di A^k per un suo sottomodulo.

Omomorfismi di A-moduli $A^m \to A^n$ e loro rappresentazione matriciale. Significato delle colonne della matrice. Omomorfismi invertibili $A^m \to A^n$: ne esistono solamente quando $m = n$. Matrici quadrate invertibili a coefficienti in A: sono tutte e sole quelle di determinante invertibile.

31 ore.

36. VENERDÌ 28 APRILE 2023

Calcolo della matrice inversa con il metodo dei cofattori. Riassunto delle ultime lezioni. $\mathbb{Z}^2/\langle(4,6)\rangle \simeq \mathbb{Z}/(2) \oplus \mathbb{Z}$.

Enunciato da dimostrare: se D è un dominio a ideali principali e $U \subset D^n$ è un D-sottomodulo, allora esistono elementi $d_1, \dots, d_n \in D$ e un automorfismo ϕ del modulo D^n tali che $d_i | d_j$ se $i \leq j$ e $\phi(U) = (d_1) \oplus \cdots \oplus (d_n)$.

Idea della dimostrazione. Un esempio.

33 ore.

37. MARTEDÌ 2 MAGGIO 2023

Dimostrazione del teorema. Struttura dei moduli finitamente generati su domini a ideali principali. Cigolii nella dimostrazione: ogni sottomodulo di D^n è finitamente generato. Perché non serve, perché si ricava, perché è comunque facilmente dimostrabile. Unicità degli invarianti $d_1, \dots, d_n$ a meno di associati.

Un esempio: se U è il sottomodulo di $\mathbb{Z}^3$ generato da $(2,3,5), (7,11,13), (17,19,23), (29,31,37)$, allora $b_1 = (1,2,-2), b_2 = (0,1,-9), b_3 = (0,0,1)$ è una $\mathbb{Z}$-base di $\mathbb{Z}^3$ tale che $U = \langle b_1, b_2, 2b_3 \rangle$.

Classificazione dei gruppi abeliani finitamente generati (e finiti). Gruppi abeliani di ordine 8, 32, 243, 72. Partizioni di un numero naturale. La forma canonica di $\mathbb{Z}/(12) \times \mathbb{Z}/(20) \times \mathbb{Z}/(30)$ è $\mathbb{Z}/(2) \times \mathbb{Z}/(60) \times \mathbb{Z}/(60)$.

Forme canoniche di endomorfismi lineari. Se V è un K-spazio vettoriale di dimensione finita, e $X : V \to V$ è un endomorfismo lineare, allora V è isomorfo, come $K[x]$-modulo, ad una somma diretta finita di moduli del tipo $K[x]/(d(x)$, dove $d(x)$, senza perdere di generalità, è una potenza di un polinomio irriducibile. Chiacchiere sul caso $K = \mathbb{C}$.

36 ore.

38. MARTEDÌ 16 MAGGIO 2023

Richiami: l'enunciato del Teorema di classificazione dei moduli finitamente generati su domini a ideali principali D; suo significato quando $D = \mathbb{Z}$ e quando D è un campo; un omomorfismo di $K[x]$-moduli è un'applicazione K-lineare che commuta con la moltiplicazione per x; dare un isomorfismo di $K[x]$-moduli tra V e una somma diretta è la stessa cosa che dare una decomposizione di V come somma diretta di K-sottospazi vettoriali invarianti rispetto alla moltiplicazione per x; dare una decomposizione di V come somma diretta di sottospazi invarianti rispetto ad un endomorfismo $T \in \mathrm{End}(V)$ significa fornire una base di V rispetto alla quale la matrice associata a T è diagonale a blocchi.

Forma canonica di Jordan: se K è un campo algebricamente chiuso, V è un K-spazio vettoriale di dimensione finita e $X \in \mathrm{End}(V)$, allora V è isomorfo, come $K[x]$-modulo, ad una somma diretta di $K[x]$-moduli della forma $K[x]/((x-\lambda)^k)$, dove $\lambda \in K$ e $k > 0$. La matrice associata all'azione di X su tale modulo nella base $[(x-\lambda)^{k-1}], \dots, [x-\lambda], [1]$ è un blocco di Jordan $k \times k$ di autovalore λ.

Forma canonica razionale (o di Frobenius): matrice compagna di un polinomio a coefficienti in K. Ogni endomorfismo X di un K-spazio vettoriale di dimensione finita può essere messo in una forma diagonale a blocchi nella quale i blocchi sono matrici compagne di polinomi monici $d_i(x)$ tali che $d_i(x) | d_j(x)$ se $i < j$.

Forma canonica di Jordan generalizzata, o razionale primaria: blocco di Jordan generalizzato associato all'azione della moltiplicazione per x sul quoziente $K[x]/(q(x)^k)$, dove $q(x) \in K[x]$ è irriducibile e $k > 0$.

Come trovo la forma canonica associata ad un endomorfismo del K-spazio vettoriale di dimensione finita V, del quale conosco la matrice $A = (a_{ij})$ in una fissata base $v_1, \dots, v_n$? Il $K[x]$-sottomodulo di $K[x]^n$ generato dalle colonne della matrice $A - x\,\mathrm{Id}$ coincide con il nucleo dell'omomorfismo di $K[x]$-moduli

$$f : K[x]^n \ni (f_1(x), \dots, f_n(x)) \mapsto f_1(x)v_1 + \cdots + f_n(x)v_n \in V.$$

Un esercizio da svolgere a casa.

39 ore.

39. VENERDÌ 19 MAGGIO 2023

Due esempi dettagliati di calcolo della forma canonica (razionale e di Jordan) di un endomorfismo lineare e della base in cui questa viene raggiunta.

Teorema di Cayley-Hamilton: il polinomio minimo di un endomorfismo divide il suo polinomio caratteristico. Unicità dei fattori invarianti di un modulo finitamente generato su un dominio a ideali principali: cenni.

41 ore.

40. MARTEDÌ 23 MAGGIO 2023

Due applicazioni: cardinalità dell'anello quoziente $\mathbb{Z}[i]/(a+bi)$; ogni sottogruppo finito del gruppo moltiplicativo di un campo è ciclico.

Caratteristica di un campo e sottocampo primo; un campo di caratteristica 0 contiene un sottocampo isomorfo a $\mathbb{Q}$, mentre un campo di caratteristica $p > 0$ contiene un sottocampo isomorfo a $\mathbb{Z}/(p)$. Un campo di caratteristica 0 è necessariamente infinito, mentre un campo di caratteristica $p > 0$ può essere finito o infinito.

Estensioni di campi. Se $K \subset L$ è un'estensione di campi, allora K ed L hanno la stessa caratteristica. Grado di un'estensione; estensioni finite e infinite. Elementi algebrici e trascendenti; polinomio minimo di un algebrico α: è un polinomio irriducibile che divide ogni altro polinomio che annulla α. In particolare, ogni polinomio irriducibile che annulla α è suo polinomio minimo. Esempi.

Estensioni finite. Ogni estensione finita è algebrica. Esempi di estensioni non algebriche. Se $F \subset K \subset L$ sono campi e le estensioni $F \subset K$ e $K \subset L$ sono finite, allora $F \subset L$ è finita; in particolare $[L : F] = [L : K][K : F]$. Estensioni di grado 1.

44 ore.

41. VENERDÌ 26 MAGGIO 2023

Richiami. Grado di un elemento algebrico. K-base di $K(\alpha)$ quando α è algebrico su K. Un campo finito di caratteristica p possiede p^n elementi per qualche $n \geq 1$. Somma e prodotto di elementi algebrici sono algebrici. Se $K \subset L$ è un'estensione di campi, e X è l'insieme di tutti gli elementi di L che sono algebrici su K, allora X è un sottocampo di L che contiene K (in altre parole: è un'estensione intermedia). Il campo $\overline{\mathbb{Q}}$ di tutti e soli i numeri complessi che sono algebrici su $\mathbb{Q}$ è un'estensione algebrica ma non finita di $\mathbb{Q}$.

Calcolo dell'inverso di $3 + 2\sqrt[3]{2} + \sqrt[3]{4}$ in $\mathbb{Q}[\sqrt[3]{2}]$. Polinomio minimo di $\sqrt{2} + \sqrt{3}$ e grado delle estensioni $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2} + \sqrt{3}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Chiacchiere sulle costruzioni con riga e compasso.

46 ore.

42. MARTEDÌ 30 MAGGIO 2023

Costruzioni con riga e compasso: le regole del gioco. Le quantità costruibili per riga e compasso formano un sottocampo di $\mathbb{R}$. Un numero reale ℓ è costruibile con riga e compasso solo se è algebrico su $\mathbb{Q}$ di grado una potenza di 2. Impossibilità della rettificazione della circonferenza, della quadratura del cerchio, della duplicazione del cubo. La costruibilità dell'n-agono regolare è equivalente alla costruibilità di $\cos(2\pi/n)$. Quando p è un primo dispari, $[\mathbb{Q}(\cos(2\pi/p)) : \mathbb{Q}] = (p-1)/2$; in particolare, il p-agono regolare è costruibile con riga e compasso solo se p è un primo di Fermat. Elenco dei primi di Fermat noti.

Campi finiti. Un campo finito di caratteristica p possiede p^n elementi per qualche $n > 0$. Gli elementi di un campo di cardinalità p^n sono tutti radici del polinomio $x^{p^n} - x \in \mathbb{F}_p[x]$. Campi di spezzamento. Un campo di cardinalità p^n è campo di spezzamento, su $\mathbb{F}_p$, del polinomio $x^{p^n} - x$.

Il polinomio $f(x) \in K[x]$ ha una radice multipla $a \in K$ se e solo se $x - a$ divide $\mathrm{MCD}(f(x), f'(x))$; Quando $\mathrm{MCD}(f(x), f'(x)) = 1$, il polinomio $f(x)$ non ha radici multiple. Se a, b appartengono ad un campo di caratteristica p, allora $(a+b)^p = a^p + b^p$.

Teorema di esistenza e unicità dei campi di spezzamento (solo enunciato). Il campo di spezzamento di $x^{p^n} - x$ su $\mathbb{F}_p$ possiede p^n elementi. Due campi finiti della stessa cardinalità sono isomorfi. Se α è il generatore ciclico del gruppo moltiplicativo di un campo finito K di caratteristica p, allora $K = \mathbb{F}_p(\alpha)$; in particolare il suo polinomio minimo è un polinomio irriducibile di grado n in $\mathbb{F}_p[x]$.

49 ore.

43. MARTEDÌ 6 GIUGNO 2023

Esistenza e unicità dei campi di spezzamento.

Esercizi.

52 ore.

44. VENERDÌ 9 GIUGNO 2023

Seconda prova in itinere.

54 ore.

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