Programma di Algebra 2

A. A. 2018/2019

Docente: Alberto Canonaco

Moduli (sinistri) su un anello A; se K è un campo, un K-modulo è un K-spazio vettoriale. Dare una struttura di A-modulo su un gruppo abeliano M equivale a dare un omomorfismo di anelli $A \to \mathrm{End}(M)$; ogni gruppo abeliano ha un'unica struttura di $\mathbb{Z}$-modulo. $\{0\}$ e A sono A-moduli per ogni anello A.

Sottomoduli di un modulo; i K-sottomoduli sono i K-sottospazi vettoriali, gli $\mathbb{Z}$-sottomoduli sono i sottogruppi; gli A-sottomoduli di A sono gli ideali sinistri di A. Intersezione di sottomoduli, somma di sottomoduli e prodotto di un ideale sinistro per un sottoinsieme di un modulo; divisione di un sottomodulo per un sottoinsieme (in particolare un sottomodulo) e annullatore di un sottoinsieme (in particolare di un sottomodulo). Sottomodulo generato da un sottoinsieme e insiemi di generatori di un modulo; moduli finitamente generati e moduli ciclici. Moduli semplici; A è un A-modulo semplice se e solo se A è un anello con divisione; gruppi semplici; un gruppo abeliano è semplice come gruppo se e solo se lo è come $\mathbb{Z}$-modulo.

Omomorfismi e isomorfismi di moduli; gli omomorfismi di K-moduli sono le applicazioni K-lineari, gli omomorfismi di $\mathbb{Z}$-moduli sono gli omomorfismi di gruppi. Omomorfismi di A-moduli da A verso un A-modulo qualunque. Immagine e controimmagine di sottomoduli attraverso un omomorfismo di moduli sono sottomoduli (in particolare, nucleo e immagine di un omomorfismo di moduli sono sottomoduli); l'immagine del sottomodulo generato da un sottoinsieme è generata dall'immagine del sottoinsieme. Gli omomorfismi tra due A-moduli M e N formano un gruppo abeliano $\mathrm{Hom}_A(M, N)$, che è anche un A-modulo se A è commutativo. Lemma di Schur.

Quoziente M/N di un modulo M per un sottomodulo N; la proiezione naturale $M \to M/N$ è un omomorfismo suriettivo di moduli con nucleo N; i sottomoduli di M/N sono tutti e soli della forma P/N con P sottomodulo di M contenente N. Teorema di omomorfismo e primo, secondo e terzo teorema di isomorfismo per moduli. Un A-modulo è ciclico (rispettivamente semplice) se e solo se è isomorfo a A/I per qualche ideale sinistro (rispettivamente ideale sinistro massimale) I di A; se inoltre A è commutativo e I e J sono due ideali di A, allora gli A-moduli A/I e A/J sono isomorfi se e solo se $I = J$; i gruppi abeliani semplici sono tutti e soli della forma $\mathbb{Z}/p\mathbb{Z}$ con p numero primo.

Prodotto e somma diretta (o coprodotto) di moduli e loro proprietà universali; somma diretta di sottomoduli. Insiemi linearmente indipendenti e basi di un modulo su un anello non nullo; moduli liberi. Omomorfismi da un modulo libero verso un modulo qualunque. Un A-modulo è libero se e solo se è isomorfo a una

somma diretta di copie di A. Ogni modulo è isomorfo a un quoziente di un modulo libero; un A-modulo è finitamente generato se e solo se è isomorfo a un quoziente di A^n per qualche n. Tutti gli A-moduli sono liberi se e solo se A è un anello con divisione. Due somme dirette di copie di un modulo semplice sono isomorfe se e solo se sono indicizzate da insiemi della stessa cardinalità (dimostrazione solo nel caso in cui uno dei due insiemi è finito). Tutte le basi di un A-modulo libero hanno la stessa cardinalità (detta rango del modulo) se A è un anello con divisione.

Restrizione degli scalari attraverso un omomorfismo di anelli. Se $I \subseteq A$ è un ideale, dare un A/I-modulo equivale a dare un A-modulo il cui annullatore contenga I; estensione degli scalari attraverso la proiezione al quoziente $A \to A/I$. Il rango di ogni A-modulo libero è ben definito se lo è il rango di ogni A/I-modulo libero; il rango di ogni A-modulo libero è ben definito se A è commutativo e non nullo.

Moduli noetheriani; un modulo noetheriano è finitamente generato (ma non viceversa). Dato un sottomodulo M' di un modulo M, M è noetheriano se e solo se M' e M/M' lo sono; una somma diretta finita di moduli è noetheriana se e solo se tutti gli addendi lo sono. Tutti gli A-moduli finitamente generati sono noetheriani se e solo se A è un A-modulo noetheriano. Anelli commutivi noetheriani; ogni dominio a ideali principali è noetheriano; ogni quoziente di un anello commutativo noetheriano è noetheriano. Teorema della base di Hilbert (solo enunciato).

Addendi diretti di un modulo; condizioni equivalenti perché un sottomodulo sia un addendo diretto; se $M' \subseteq M$ è un sottomodulo tale che M/M' è libero, allora M' è un addendo diretto di M. Moduli semisemplici; sottomoduli e quozienti di un modulo semisemplice sono semisemplici. Anelli semisemplici; ogni anello con divisione è semisemplice.

Moduli indecomponibili; un modulo è semplice se e solo se è indecomponibile e semisemplice. Ogni modulo noetheriano è somma diretta finita di moduli indecomponibili. Ogni modulo semisemplice e finitamente generato è noetheriano ed è somma diretta finita di moduli semplici in modo essenzialmente unico; se A è un A-modulo semisemplice, c'è un numero finito di classi di isomorfismo di A-moduli semplici, e ognuna compare nella decomposizione di A.

Torsione di un modulo su un dominio; moduli di torsione e moduli senza torsione. Un modulo noetheriano senza torsione è isomorfo a un sottomodulo di un modulo libero di rango finito. Un ideale non nullo di un dominio è indecomponibile.

Su un dominio a ideali principali A (che non sia un campo) ogni modulo finitamente generato è somma diretta del sottomodulo di torsione e di un sottomodulo libero di rango finito. Il sottomodulo di torsione di un modulo è somma diretta dei sottomoduli di P-torsione al variare di P tra gli ideali massimali di A. Un A-modulo finitamente generato è indecomponibile se e solo se è isomorfo a A o a A/P^n per qualche ideale massimale P e qualche $n > 0$. Teorema di struttura per gli A-moduli finitamente generati. Cenni sulla forma canonica di Jordan.

Teorema di struttura per i gruppi abeliani finitamente generati. Teorema di Sylow per gruppi abeliani. Esponente di un gruppo finito; l'esponente di un gruppo abeliano finito coincide con l'ordine se e solo se il gruppo è ciclico. Ogni sottogruppo finito del gruppo moltiplicativo di un dominio è ciclico (in particolare K^* è ciclico per ogni campo finito K).

Azioni di un gruppo G su insiemi o G-insiemi; dare un G-insieme X equivale a dare un omomorfismo di gruppi $G \to S(X)$. Azione per coniugio di G su G e azione per moltiplicazione a sinistra di G su G/H per ogni sottogruppo H di G. Sottoinsiemi G-stabili o G-invarianti di un G-insieme; morfismi e isomorfismi di G-insiemi. Orbita di un elemento in un G-insieme; le orbite formano una partizione del G-insieme e un sottoinsieme è G-stabile se e solo se è unione di orbite; azioni transitive. Stabilizzatore $\mathrm{Stab}(x)$ di un elemento x in un G-insieme; rispetto all'azione per coniugio, $\mathrm{Stab}(a)$ coincide con il centralizzatore $C(a)$ per ogni $a \in G$ e $\mathrm{Stab}(H)$ con il normalizzatore $N(H)$ per ogni H sottogruppo di G; azioni libere e azioni fedeli; $\mathrm{Stab}(gx) = g\mathrm{Stab}(x)g^{-1}$ per ogni $g \in G$.

Per ogni sottogruppo H di G il nucleo dell'omomorfismo $G \to S(G/H)$ (indotto dalla moltiplicazione a sinistra) è il più grande sottogruppo normale di G contenuto in H; tale omomorfismo non è iniettivo se G è finito e il suo ordine non divide $[G : H]!$ (dunque in questo caso G non è semplice se $H \neq G$).

Per ogni elemento x in un G-insieme c'è un isomorfismo di G-insiemi tra $G/\mathrm{Stab}(x)$ e l'orbita di x; la cardinalità della classe di coniugio di $a \in G$ coincide con $[G : C(a)]$; la cardinalità dell'insieme dei coniugati di un sottogruppo H di G coincide con $[G : N(H)]$; equazione delle classi.

p-gruppi; un p-gruppo non banale ha centro non banale; un p-gruppo ha sottogruppi normali di ogni ordine che divida l'ordine del gruppo. Se G è un gruppo non abeliano, $G/Z(G)$ non è ciclico; un gruppo di ordine p^2 è abeliano.

Sottogruppi di Sylow di un gruppo finito e prima parte del teorema di Sylow; teorema di Cauchy. Laterali doppi di due sottogruppi di un gruppo; seconda parte del teorema di Sylow. Se tutti i sottogruppi di Sylow di un gruppo finito sono normali, allora il gruppo è il prodotto di tali sottogruppi.

Se $n \geq 5$, tutti i 3-cicli sono coniugati in A_n, A_n è semplice e A_n è l'unico sottogruppo normale non banale di S_n.

Cenni sulle serie di composizione e sul teorema di Jordan-Hölder (solo enunciato). Gruppi risolubili e serie derivata di un gruppo; sottogruppi e quozienti di gruppi risolubili sono risolubili; se H è un sottogruppo normale di G tale che H e G/H sono risolubili, anche G lo è; un gruppo semplice non abeliano non è risolubile; S_n e A_n sono risolubili se e solo se $n \leq 4$.

Prodotti semidiretti di gruppi; se $G = K \rtimes H$ (con K sottogruppo normale e H sottogruppo di G), la restrizione dell'azione per coniugio definisce un omomorfismo di gruppi $H \to \mathrm{Aut}(K)$. Dati due gruppi H e K e dato un omomorfismo di gruppi $\theta\colon H \to \mathrm{Aut}(K)$, costruzione del prodotto semidiretto $K \rtimes_\theta H$ (che coincide con

$K \times H$ se θ è banale); $K \rtimes_\theta H$ è abeliano se e solo se θ è banale e H e K sono abeliani. Condizione sufficiente perché $K \rtimes_\theta H \cong K \rtimes_{\theta'} H$ è che esista $\alpha \in \mathrm{Aut}(H)$ tale che $\theta = \theta' \circ \alpha$; classificazione dei gruppi di ordine pq con p e q primi distinti; classificazione dei gruppi di ordine minore di 16.

Algebre su un anello commutativo; ogni anello ha un'unica struttura di $\mathbb{Z}$-algebra; se B è una A-algebra e M un A-modulo, $\mathrm{End}_B(M)$ è una A-algebra. Elementi algebrici e elementi trascendenti in una K-algebra B (con K campo); polinomio minimo m_b di $b \in B$ algebrico; b è algebrico se e solo se $\dim_K(K[b])$ è finita, e in questo caso $K[b] \cong K[X]/(\mathrm{m}_b)$ e $\dim_K(K[b]) = \deg(\mathrm{m}_b)$; inoltre m_b è irriducibile se B è un anello con divisione (in particolare un campo). Se M è un B-modulo tale che $\dim_K(M)$ è finita, anche $\dim_K(\mathrm{End}_B(M))$ è finita, e vale 1 se M è semplice e K è algebricamente chiuso.

Caratteristica di un anello; la caratteristica di un dominio è 0 o un numero primo. Anello di gruppo AG di un gruppo G su un anello A; teorema di Maschke. Rappresentazioni (K-lineari con K campo) di G; morfismi e isomorfismi di rappresentazioni; le rappresentazioni di G possono essere identificate con i KG-moduli. Rappresentazioni irriducibili, rappresentazioni completamente riducibili e rappresentazione regolare; grado di una rappresentazione. Le rappresentazioni di grado 1 sono irriducibili e sono classificate (a meno di isomorfismo) dagli omomorfismi di gruppi dall'abelianizzato di G a K^*. Se G ha ordine n e la caratteristica di K non divide n, ogni rappresentazione è completamente riducibile; ogni rappresentazione di grado finito è somma diretta finita di rappresentazioni irriducibili in modo essenzialmente unico; c'è un numero finito di classi di isomorfismo di rappresentazioni irriducibili e ognuna di esse compare nella decomposizione della rappresentazione regolare (un numero di volte pari al suo grado se K è algebricamente chiuso, nel qual caso tutte le rappresentazioni hanno grado 1 se e solo se G è abeliano).

Sottocampi e estensioni di campi; l'intersezione di sottocampi è un sottocampo; sottocampo primo di un campo; il sottocampo primo è isomorfo a $\mathbb{Q}$ (se la caratteristica è 0) o a $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ (se la caratteristica è p). Grado di un'estensione e estensioni finite; se $F \subseteq K \subseteq L$ sono estensioni, $[L : F] = [L : K][K : F]$.

Se $K \subseteq L$ è un'estensione e $U \subseteq L$ è un sottoinsieme, il più piccolo sottocampo $K(U)$ contenente K e U contiene il più piccolo sottoanello $K[U]$ contenente K e U, e vale l'uguaglianza se ogni elemento di U è algebrico su K; estensioni finitamente generate e estensioni semplici. Estensioni algebriche; un'estensione è finita se e solo se è algebrica e finitamente generata; un'estensione generata da elementi algebrici è algebrica; se $K \subseteq L$ è un'estensione, gli elementi di L algebrici su K formano un sottocampo di L contenente K; se $F \subseteq K \subseteq L$ sono estensioni, $F \subseteq L$ è algebrica se e solo se $F \subseteq K$ e $K \subseteq L$ lo sono.

Per ogni polinomio monico $f \in K[X]$ esiste un'estensione semplice $K \subseteq K(\alpha)$ tale che $f = \mathrm{m}_\alpha$. Campo di spezzamento di $f \in K[X]$; se $\deg(f) = n$, esiste $K \subseteq L$ campo di spezzamento di f e $[L : K]$ divide $n!$; inoltre n divide $[L : K]$ se

f è irriducibile. Morfismi e isomorfismi di estensioni; se α è algebrico su K, esiste (unico) un morfismo di estensioni da $K \subseteq K(\alpha)$ a un'altra estensione $K \to L$ che manda α in $\beta \in L$ se e solo se $\mathrm{m}_\alpha(\beta) = 0$; esite un morfismo di estensioni da $K \subseteq K'$ campo di spezzamento di $f \in K[X]$ a un'altra estensione $K \to L$ se e solo se f si spezza su L; unicità a meno di isomorfismo di estensioni del campo di spezzamento. Chiusura algebrica di un campo e sua esistenza e unicità a meno di isomorfismo di estensioni.

Campo di spezzamento di un insieme di polinomi; estensioni normali; un'estensione è normale se e solo se è il campo di spezzamento di un insieme di polinomi; un'estensione è finita e normale se e solo se è il campo di spezzamento di un polinomio. Se $F \subseteq K \subseteq L$ sono estensioni e $F \subseteq L$ è normale, anche $K \subseteq L$ lo è; se inoltre $F \subseteq L$ è finita, allora $F \subseteq K$ è normale se e solo se K è stabile per l'azione del gruppo di Galois $\mathrm{Gal}_F(L)$ di $F \subseteq L$.

Polinomi irriducibili separabili; un polinomio irriducibile è separabile se e solo se la sua derivata non è nulla. Elementi separabili in un'estensione e estensioni separabili; se $F \subseteq K \subseteq L$ sono estensioni e $F \subseteq L$ è separabile, anche $F \subseteq K$ e $K \subseteq L$ lo sono. Omomorfismo di Frobenius e campi perfetti; i campi finiti sono perfetti; un campo K è perfetto se e solo tutti i polinomi irriducibili sono separabili su K se e solo se tutte le estensioni algebriche di K sono separabili.

Estensioni di Galois; se $K \subseteq L$ è un'estensione finita, $\#\mathrm{Gal}_K(L) \leq [L : K]$ e vale l'uguaglianza se e solo se l'estensione è di Galois. Sottocampo fisso L^G di un campo L rispetto a un sottogruppo G del gruppo degli automorfismi di L; $G \subseteq \mathrm{Gal}_{L^G}(L)$ e vale l'uguaglianza se G è finito (nel qual caso $L^G \subseteq L$ è di Galois); per ogni estensione $K \subseteq L$ si ha $K \subseteq L^{\mathrm{Gal}_K(L)}$ e, se $[L : K] < \infty$, vale l'uguaglianza se e solo se $K \subseteq L$ è di Galois. Teorema fondamentale della teoria di Galois; se $K \subseteq L$ è un'estensione finita, $\#\mathrm{Gal}_K(L)$ divide $[L : K]$.

L'ordine di un campo finito è una potenza di un numero primo; per ogni p primo e per ogni $n > 0$ esiste unico a meno di isomorfismo un campo $\mathbb{F}_{p^n}$ di ordine p^n (e di caratteristica p), che è campo di spezzamento di $X^{p^n} - X$ su $\mathbb{F}_p$; ogni estensione tra campi finiti è di Galois con gruppo di Galois ciclico generato da una potenza dell'automorfismo di Frobenius.

Gruppo di Galois $\mathrm{Gal}_K(f)$ di $f \in K[X]$; $\mathrm{Gal}_K(f)$ può essere identificato con un sottogruppo di S_n se f ha n radici (in un campo di spezzamento). Se la caratteristica di K non divide n, $\mathrm{Gal}_K(X^n - 1)$ è isomorfo a un sottogruppo di $\mathbb{Z}/n\mathbb{Z}^*$; $\mathrm{Gal}_{\mathbb{Q}}(X^n - 1) \cong \mathbb{Z}/n\mathbb{Z}^*$ (dimostrazione solo per n primo).

Elementi radicali in un'estensione e estensioni per radicali; polinomi risolubili (per radicali); se K è di caratteristica 0, $f \in K[X]$ è risolubile se e solo se $\mathrm{Gal}_K(f)$ è un gruppo risolubile (solo enunciato); cenni sulla formula risolutiva dei polinomi di terzo grado. Discriminante $\Delta(f)$ di $f \in K[X]$; se la caratteristica di K non è 2, $\deg(f) = n$ e f non ha radici multiple, allora $\mathrm{Gal}_K(f) \subseteq A_n$ se e solo $\Delta(f)$ è un quadrato in K; $\Delta(X^3 + aX + b) = -4a^3 - 27b^2$ (solo enunciato).