Istituzioni di Algebra
A. A. 2016/2017
Programma svolto da Alberto Canonaco

Richiami di teoria degli anelli (con unità, non necessariamente commutativi). Esempi di anelli non commutativi: quaternioni $\mathbb{H}$ (con divisione); matrici $M_n(A)$; endomorfismi di un gruppo abeliano $\mathrm{End}(G)$. Per ogni anello A esiste un omomorfismo iniettivo naturale $A \to \mathrm{End}(A)$. Centro di un anello; $Z(\mathbb{H}) = \mathbb{R}$; $Z(M_n(A)) = Z(A)I_n$. Anello opposto A^{op} di un anello A; gli ideali destri di A sono gli ideali sinistri di A^{op}. Un anello non nullo in cui ogni elemento non nullo è invertibile a sinistra è con divisione. Ogni anello non nullo ha ideali sinistri, destri e bilateri massimali. Anelli semplici; un ideale $I \subsetneq A$ è massimale se e solo se A/I è semplice. Un anello con divisione è semplice; il viceversa vale nel caso commutativo ma non in generale. Gli ideali di $M_n(A)$ sono tutti e soli della forma $M_n(I)$ con I ideale di A (dunque $M_n(A)$ è semplice se e solo se A lo è).

Moduli (sinistri) su un anello; 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 $A = {}_AA$ sono A-moduli per ogni anello A. Moduli destri su un anello; gli A-moduli destri possono essere identificati con gli A^{op}-moduli sinistri. (A, B)-bimoduli; gli (A, B)-bimoduli possono essere identificati con i $(B^{\mathrm{op}}, A^{\mathrm{op}})$-bimoduli; A è un (A, A)-bimodulo (o A-bimodulo); ogni A-modulo è anche un $(A, \mathbb{Z})$-bimodulo; se A è commutativo, ogni A-modulo è un A-bimodulo.

Sottomoduli; 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. L'intersezione di sottomoduli, la somma di sottomoduli e il prodotto di un ideale sinistro per un sottomodulo sono sottomoduli. Sottomodulo generato da un sottoinsieme e insiemi di generatori di un modulo; moduli finitamente generati e moduli ciclici.

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. Gli omomorfismi tra due A-moduli M e N formano un gruppo abeliano $\mathrm{Hom}_A(M, N)$, che è anche un (B, C)-bimodulo se M è un (A, B)-bimodulo e N un (A, C)-bimodulo. In particolare, se A è commutativo, $\mathrm{Hom}_A(M, N)$ è un A-(bi)modulo, in ogni caso $\mathrm{Hom}_A(A, M)$ è un A-modulo (isomorfo a M), $\mathrm{End}_A({}_AA)$ e $\mathrm{End}_A(A_A)$ sono A-bimoduli (entrambi isomorfi sia a A che a A^{op}); $\mathrm{End}_A({}_AA) \cong A^{\mathrm{op}}$ e $\mathrm{End}_A(A_A) \cong A$ come anelli.

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.

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. Conucleo di un omomorfismo di moduli; il conucleo è nullo se e solo se l'omomorfismo è suriettivo. Teoremi di omomorfismo e di isomorfismo per moduli. Complessi e successioni esatte (in particolare corte) di moduli.

Prodotto e somma diretta di moduli e loro proprietà universali. Moduli liberi e basi di un modulo libero; ogni modulo è isomorfo a un quoziente di un modulo libero; un A-modulo è finitamente generato (rispettivamente ciclico) se e solo se è isomorfo a un quoziente di A^n per qualche n (rispettivamente A).

Restrizione degli scalari attraverso un omomorfismo di anelli. L'annullatore di un sottoinsieme di un modulo è un ideale sinistro, l'annullatore di un modulo è un ideale; moduli fedeli. Se $I \subseteq A$ è un ideale e M un A-modulo tale che $I \subseteq \mathrm{Ann}(M)$, M è in modo naturale un A/I-modulo (dunque M/IM è sempre un A/I-modulo).

R-algebre con R anello commutativo; dare una struttura di R-algebra su un anello A equivale a dare un omomorfismo di anelli $R \to Z(A)$; ogni anello ha un'unica struttura di $\mathbb{Z}$-algebra. Omomorfismi di R-algebre; gli omomorfismi di $\mathbb{Z}$-algebre sono gli omomorfismi di anelli. Se A è una R-algebra e M un A-modulo, $\mathrm{End}_A(M)$ è una R-algebra.

Anello AG (con A anello e G gruppo o, più in generale, monoide); rappresentazioni A-lineari di un gruppo; dare un AG-modulo equivale a dare una rappresentazione A-lineare di G.

Moduli semplici; un A-modulo è semplice se e solo se è isomorfo a A/I per qualche ideale sinistro massimale I di A; ${}_AA$ è semplice se e solo se A è con divisione. Se A non è nullo e tutti gli A-moduli sono liberi, A è con divisione. Lemma di Schur: un omomorfismo non nullo tra moduli semplici è un isomorfismo, e dunque $\mathrm{End}_A(M)$ è un anello con divisione se M è un A modulo semplice; se inoltre A è una K-algebra e $\dim_K(M) < \infty$, anche $\dim_K(\mathrm{End}_A(M)) < \infty$; se poi K è algebricamente chiuso, $K \to \mathrm{End}_A(M)$ è un isomorfismo.

Somma diretta di sottomoduli e addendi diretti di un modulo; un sottomodulo $N \subseteq M$ è un addendo diretto se e solo se esiste un omomorfismo $f\colon M \to N$ tale che $f|_N = \mathrm{id}_N$. Moduli semisemplici (definiti come moduli tali che ogni sottomodulo è un addendo diretto); sottomoduli e quozienti di un modulo semisemplice sono semisemplici; un modulo è semisemplice se e solo se è somma (diretta) di sottomoduli semplici. Tutti gli A-moduli sono semisemplici se e solo se ${}_AA$ è semisemplice; su un anello con divisione tutti i moduli sono semisemplici e liberi. Ogni modulo semisemplice è in modo essenzialmente unico una somma diretta di moduli semplici. Lunghezza di un modulo semisemplice; un modulo semisemplice ha lunghezza finita se e solo se è finitamente generato; la lunghezza coincide con il rango (che quindi è ben definito) per i moduli (liberi) su un anello con divisione. Se $I \subseteq A$ è un ideale e il rango è ben definito per gli A/I-moduli liberi, lo è anche per gli A-moduli liberi (dunque il rango è ben definito per i moduli liberi su un anello commutativo non nullo).

Anelli semisemplici (a sinistra); se A è semisemplice, esistono $I_1, \dots, I_n$ ideali sinistri non nulli minimali di A tali che ${}_AA = I_1 \oplus \cdots \oplus I_n$ e ogni A-modulo semplice è isomorfo a I_i per qualche i. Se $A_1, \dots, A_r$ sono anelli semisemplici, anche $A = A_1 \times \cdots \times A_r$ lo è e le classi di isomorfismo degli A-moduli semplici si identificano all'unione disgiunta delle classi di isomorfismo degli A_i-moduli semplici. Se D è un anello con divisione, $n > 0$ e $V = D^n_D$, allora $A = M_n(D)$ è isomorfo all'anello $\mathrm{End}_D(V)$, V è un (A, D)-bimodulo, V è l'unico A-modulo semplice (a meno di isomorfismo), ${}_AA \cong V^n$ e l'anello $\mathrm{End}_A(V)$ è isomorfo a D^{op}. Teorema di Wedderburn-Artin: un anello è semisemplice se e solo se è isomorfo a un prodotto finito di anelli di matrici a coefficienti in anelli con divisione; inoltre tale scrittura come prodotto è essenzialmente unica. Conseguenze: un anello è semisemplice a sinistra se e solo se lo è a destra; un anello commutativo è semisemplice se e solo se è isomorfo a un prodotto finito di campi; un anello semisemplice è semplice se e solo se è isomorfo a $M_n(D)$ per qualche $n > 0$ e qualche anello con divisione D.

Teorema di Maschke: se A è un anello non nullo e G un gruppo, allora AG è semisemplice se e solo se A è semisemplice, G è finito e l'ordine di G è invertibile in A (dimostrazione di "se", non di "solo se"). Conseguenze: se G ha ordine n e K è un campo algebricamente chiuso la cui caratteristica non divide n, tutte le rappresentazioni K-lineari di G sono completamente riducibili (cioè i KG-moduli corrispondenti sono semisemplici); esistono (a meno di isomorfismo) r rappresentazioni irriducibili (cioè corrispondenti a KG-moduli semplici), con r numero delle classi di coniugio di G; indicando con $n_1, \dots, n_r$ i gradi (cioè le dimensioni su K dei KG-moduli corrispondenti) di tali rappresentazioni, si ha $n = n_1^2 + \cdots + n_r^2$.

Categorie; esempi di categorie: Set degli insiemi, Top degli spazi topologici, Grp dei gruppi, Rng degli anelli, A-Mod (con A anello) degli A-moduli sinistri, Mod-A degli A-moduli destri, $\mathsf{Rep}_A(G)$ delle rappresentazioni A-lineari di un gruppo G e R-Alg delle R-algebre (con R anello commutativo). Categorie piccole; preordini come categorie con al più un morfismo tra due oggetti; monoidi come categorie con un solo oggetto. Morfismi invertibili a sinistra o a destra e isomorfismi; un morfismo è un isomorfismo se e solo se è invertibile a sinistra e a destra. Prodotto di categorie. Categoria opposta C^{op} di una categoria C e principio di dualità. Sottocategorie e sottocategorie piene; Ab sottocategoria piena di Grp costituita dai gruppi abeliani e CRng sottocategoria piena di Rng costituita dagli anelli commutativi. Prodotti e coprodotti in una categoria; loro unicità a meno di isomorfismo; esempi di esistenza e non esistenza; oggetti iniziali e terminali.

Funtori (covarianti) tra categorie; funtori controvarianti $\mathsf{C} \to \mathsf{D}$ come funtori $\mathsf{C}^{\mathrm{op}} \to \mathsf{D}$; funtore opposto $\mathrm{F}^{\mathrm{op}} \colon \mathsf{C}^{\mathrm{op}} \to \mathsf{D}^{\mathrm{op}}$ di un funtore $\mathrm{F} \colon \mathsf{C} \to \mathsf{D}$. Esempi di funtori: inclusioni di sottocategorie; funtori "dimenticanti"; morfismi di preordini; omomorfismi di monoidi; $\mathrm{Hom}(X, -) \colon \mathsf{C} \to \mathsf{Set}$ e $\mathrm{Hom}(-, X) \colon \mathsf{C}^{\mathrm{op}} \to \mathsf{Set}$ per ogni oggetto X di una categoria C. Ogni funtore preserva i morfismi invertibili a destra o a sinistra e gli isomorfismi. Funtori fedeli, pieni (e pienamente fedeli), essenzialmente iniettivi e essenzialmente suriettivi; un funtore pienamente fedele è essenzialmente iniettivo. Categoria Cat delle categorie (piccole); isomorfismi di categorie; un funtore è un isomorfismo se e solo se è biunivoco sugli oggetti e pienamente fedele; ci sono isomorfismi di categorie $\mathsf{Mod}\text{-}A \cong A^{\mathrm{op}}\text{-}\mathsf{Mod}$, $\mathbb{Z}\text{-}\mathsf{Mod} \cong \mathsf{Ab}$, $\mathbb{Z}\text{-}\mathsf{Alg} \cong \mathsf{Rng}$ e $AG\text{-}\mathsf{Mod} \cong \mathsf{Rep}_A(G)$.

Categorie preadditive; A-Mod è preadditiva; l'opposta e ogni sottocategoria piena di una categoria preadditiva sono preadditive; anelli come categorie preadditive con un solo oggetto. Funtori additivi tra categorie preadditive; esempi: restrizione degli scalari $B\text{-}\mathsf{Mod} \to A\text{-}\mathsf{Mod}$ per ogni omomorfismo di anelli $A \to B$; omomorfismi di anelli; $\mathrm{Hom}(X, -) \colon \mathsf{A} \to \mathsf{Ab}$ e $\mathrm{Hom}(-, X) \colon \mathsf{A}^{\mathrm{op}} \to \mathsf{Ab}$ per ogni oggetto X di una categoria preadditiva A. Categorie e funtori R-lineari con R anello commutativo; R-Mod è R-lineare.

Oggetti nulli e biprodotti in una categoria preadditiva; un oggetto è nullo se e solo se è terminale se e solo se è iniziale; un oggetto è un biprodotto di due oggetti se e solo se ne è un prodotto se e solo se ne è un coprodotto; un funtore additivo tra categorie preadditive $\mathsf{A} \to \mathsf{B}$ preserva oggetti nulli e biprodotti, e dunque i (co)prodotti finiti che esistono in A. Categorie additive; A-Mod è additiva; l'opposta di una categoria additiva è additiva.

Monomorfismi e epimorfismi in una categoria. Nuclei e conuclei in una categoria preadditiva; ogni nucleo (conucleo) è un monomorfismo (epimorfismo); in una categoria additiva un morfismo è un monomorfismo (epimorfismo) se e solo ha nucleo (conucleo) 0. Categorie abeliane (definite come categorie additive in cui ogni morfismo ha nucleo e conucleo, ogni monomorfismo è un nucleo e ogni epimorfismo è un conucleo); A-Mod è abeliana; l'opposta di una categoria abeliana è abeliana. In una categoria abeliana ogni monomorfismo (epimorfismo) è nucleo (conucleo) del suo conucleo (nucleo); un morfismo è un isomorfismo se e solo se è un monomorfismo e un epimorfismo. Immagine e coimmagine di un morfismo in una categoria abeliana; il morfismo naturale tra coimmagine e immagine è un isomorfismo (solo enunciato). Successioni esatte in categorie abeliane; spezzamento di successioni esatte corte; categorie abeliane semisemplici (in cui cioè tutte le successioni esatte corte si spezzano); A-Mod è semisemplice se e solo se A è semisemplice.

Funtori esatti a sinistra/destra tra categorie abeliane (definiti come funtori additivi che preservano i nuclei/conuclei); F è esatto a sinistra se e solo se F^{op} è esatto a destra; un funtore additivo $\mathrm{F} \colon \mathsf{A} \to \mathsf{B}$ tra categorie abeliane è esatto a sinistra se e solo se $0 \to \mathrm{F}(X) \to \mathrm{F}(Y) \to \mathrm{F}(Z)$ è esatta in B per ogni successione esatta $0 \to X \to Y \to Z$ (o $0 \to X \to Y \to Z \to 0$) in A. Funtori esatti tra categorie abeliane (definiti come funtori esatti a sinistra e a destra); un funtore additivo tra categorie abeliane è esatto se e solo se preserva le successioni esatte se e solo se preserva le successioni esatte corte. Un funtore additivo tra categorie abeliane preserva le successioni esatte corte che si spezzano, dunque è esatto se la categoria di partenza è semisemplice. Teorema di Freyd-Mitchell (solo enunciato): per ogni categoria abeliana (piccola) A esiste un anello A e un funtore esatto e pienamente fedele $\mathsf{A} \to A\text{-}\mathsf{Mod}$. Conseguenza: le dimostrazioni di "caccia al diagramma" in A si possono fare in $A\text{-}\mathsf{Mod}$; lemma del serpente.

Trasformazioni naturali e isomorfismi di funtori. Categoria $\mathsf{Fun}(\mathsf{C}, \mathsf{D})$ dei funtori tra due categorie C e D (con C piccola); categorie di prefasci su uno spazio topologico; $\mathsf{Rep}_A(G) \cong \mathsf{Fun}(G, A\text{-}\mathsf{Mod})$. Se D è (pre)additiva o abeliana, anche $\mathsf{Fun}(\mathsf{C}, \mathsf{D})$ lo è, e lo stesso vale per la sottocategoria piena $\mathsf{Add}(\mathsf{C}, \mathsf{D})$ dei funtori additivi se C è preadditiva; $A\text{-}\mathsf{Mod} \cong \mathsf{Add}(A, \mathsf{Ab})$.

Per ogni oggetto X di una categoria abeliana A i funtori $\mathrm{Hom}(X, -)\colon \mathsf{A} \to \mathsf{Ab}$ e $\mathrm{Hom}(-, X)\colon \mathsf{A}^{\mathrm{op}} \to \mathsf{Ab}$ sono esatti a sinistra. Oggetti proiettivi e oggetti iniettivi in una categoria abeliana; categorie abeliane con abbastanza proiettivi/iniettivi; se A ha abbastanza proiettivi/iniettivi, ogni oggetto di A ha risoluzioni proiettive/iniettive. Un coprodotto (prodotto) è proiettivo (iniettivo) se e solo se ogni termine è proiettivo (iniettivo); in $A\text{-}\mathsf{Mod}$ i proiettivi sono gli addendi diretti dei moduli liberi, quindi $A\text{-}\mathsf{Mod}$ ha abbastanza proiettivi; $A\text{-}\mathsf{Mod}$ ha abbastanza iniettivi (solo enunciato).

Categoria abeliana $\mathrm{C}(\mathsf{A})$ dei complessi di una categoria abeliana A; funtori di coomologia $\mathrm{H}^i\colon \mathrm{C}(\mathsf{A}) \to \mathsf{A}$ (additivi); successione esatta lunga di coomologia indotta da una successione esatta corta in $\mathrm{C}(\mathsf{A})$. Omotopia tra morfismi di complessi e categoria omotopa $\mathrm{K}(\mathsf{A})$ (additiva); gli H^i inducono funtori additivi $\mathrm{H}^i\colon \mathrm{K}(\mathsf{A}) \to \mathsf{A}$. Se A ha abbastanza iniettivi, la scelta di una risoluzione iniettiva di ogni oggetto di A si estende in modo unico a un funtore additivo $\mathrm{I}\colon \mathsf{A} \to \mathrm{K}(\mathsf{A})$ (e scelte diverse inducono funtori isomorfi).

Un funtore additivo tra categorie abeliane $\mathrm{F}\colon \mathsf{A} \to \mathsf{B}$ induce funtori additivi $\mathrm{F}\colon \mathrm{C}(\mathsf{A}) \to \mathrm{C}(\mathsf{B})$ e $\mathrm{F}\colon \mathrm{K}(\mathsf{A}) \to \mathrm{K}(\mathsf{B})$. Se A ha abbastanza iniettivi, l'i-esimo funtore derivato destro $\mathrm{R}^i\mathrm{F}\colon \mathsf{A} \to \mathsf{B}$ è il funtore additivo (ben definito a meno di isomorfismo) ottenuto come composizione $\mathsf{A} \xrightarrow{\mathrm{I}} \mathrm{K}(\mathsf{A}) \xrightarrow{\mathrm{F}} \mathrm{K}(\mathsf{B}) \xrightarrow{\mathrm{H}^i} \mathsf{B}$. Successione esatta lunga dei funtori derivati indotta da una successione esatta corta in A; F è esatto a sinistra se e solo se $\mathrm{R}^0\mathrm{F} \cong \mathrm{F}$; F è esatto se e solo se $\mathrm{R}^0\mathrm{F} \cong \mathrm{F}$ e $\mathrm{R}^i\mathrm{F} \cong 0$ per $i > 0$ (basta $i = 1$). Funtori derivati sinistri (se A ha abbastanza proiettivi) $\mathrm{L}_i\mathrm{F} := (\mathrm{R}^i\mathrm{F}^{\mathrm{op}})^{\mathrm{op}}$.