Lezione del 14 marzo; Registro dettagliato

1. **Fattorizzazione epi-mono.**

   A livello di insiemi, ciascuna funzione $f : A \to B$ individua: (1) un sottinsieme di B, l'insieme delle immagini degli elementi di A tramite f, detto "immagine di A tramite f" ed indicato con $f(A)$, oppure "immagine di f" ed indicato con $\mathrm{Im}(f)$; (2) una relazione di equivalenza $\sim_f$ su A, nella quale due elementi di A sono in relazione se e solo se hanno la stessa immagine tramite f; questa relazione d'equivalenza individua un insieme quoziente $A/\sim_f$ di A e la funzione suriettiva proiezione $p_f : A \to A/\sim_f$. Questi oggetti sono legati dalla seguente

   Proposition 1. *(Fattorizzazione epi-mono) Sia $f : A \to B$ una funzione fra insiemi. Allora*

   (1) la posizione
   $$\hat{f}([x]_{\sim_f}) = f(x), \qquad x \in A$$
   definisce una funzione, iniettiva, $\hat{f} : A/\sim_f \to B$;

   (2) f e' composizione di una funzione suriettiva seguita da una iniettiva:
   $$f = \hat{f} \circ p_f.$$

   (3) $\hat{f} : A/\sim_f \to f(A)$ (abuso di notazione) e' una biiezione.

   La prova di questa proposizione e' immediata.

2. **Primo teorema fondamentale di omomorfismo, per anelli commutativi.**

   Le costruzioni e la proposizione di sopra hanno una versione in ogni teoria di strutture algebriche di uno stesso tipo con i corrispondenti omomorfismi. Consideriamo il caso particolare degli anelli commutativi;

   > *fino ad avviso contrario, tutti gli anelli considerati sono tacitamente assunti commutativi.*

   Sia $f : A \to B$ un omomorfismo fra anelli. Allora: (1) l'insieme immagine $f(A)$ e' un sottoanello di B; (2) la relazione di equivalenza $\sim_f$ e' una congruenza su A, alla qale corrisponde un anello quoziente $A/\sim_f$ e l'epimorfismo proiezione $p_f : A \to A/\sim_f$. Questi oggetti sono legati dalla proposizione ottenuta dalla proposizione di sopra sostituendo al termine "insieme" il termine "anello" e ai termini "funzione, ..., biiezione" i termini "omomorfismo, ..., isomorfismo" (di anelli).

   Si puo' dare, e normalmente si da', una diversa formulazione di questa proposizione. L'insieme delle preimmagini in A dello zero di B e' un ideale di A che si dice "nucleo di f" e si indica con $\mathrm{Ker}(f)$:
   $$\mathrm{Ker}(f) = \{x \in A |\ f(x) = 0\};$$

a questo ideale di A corrisponde una partizione di A in classi laterali

$$A/\mathrm{Ker}(f) = \{\mathrm{Ker}(f) + x;\ x \in A\}$$

sulla quale dunque sono ben definite le operazioni rappresentante per rappresentante che danno all'insieme $A/\mathrm{Ker}(f)$ la struttura di anello; si ha un omomorfismo suriettivo $p_f : A \to A/\mathrm{Ker}(f)$, $x \mapsto \mathrm{Ker}(f)+x$. La proposizione di fattorizzazione epi-mono viene formulata come segue e viene detta "primo teorema fondamentale di omomorfismo".

Proposition 2. *Sia $f : A \to B$ un omomorfismo da un anello A ad un anello B. Allora*

(1) la posizione

$$\hat{f}(\mathrm{Ker}(f) + x) = f(x), \qquad x \in A$$

definisce un omomorfismo, iniettivo, $\hat{f} : A/\mathrm{Ker}(f) \to B$;

(2) f e' composizione di un epimorfismo seguito da un monomorfismo:

$$f = \hat{f} \circ p_f.$$

(3) $\hat{f} : A/\mathrm{Ker}(f) \to f(A)$ (abuso di notazione) e' un isomorfismo.

3. **Caratteristica di un anello.**

Definition 1. *Sia A un anello con unita' moltiplicativa 1. Se a qualche intero positivo corrisponde un multiplo nullo di 1, allora si definisce caratteristica di A il minimo fra tali interi positivi. Se a nessun intero positivo corrisponde un multiplo nullo di 1, allora si definisce caratteristica di A l'intero 0. La caratteristica di A si indica con* $\mathrm{char}(A)$.

La relazione fra caratteristica, ... e sottoanello fondamentale e' piuttosto naturale. I multipli interi relativi dell'1 di un anello A sono creati dall'unico omomorfismo $f : \mathbb{Z} \to A$; si ha $\mathrm{Ker}(f) = n\mathbb{Z}$, per un unico $n \in \mathbb{Z}^+$, il quale n e' proprio la caratteristica di A; l'anello quoziente $\mathbb{Z}/\mathrm{Ker}(f) = \mathbb{Z}_n$ per il teorema di omomorfismo e' isomorfo al sottoanello fondamentale di A. Si noti che $\mathbb{Z}_0 = \mathbb{Z}$, $\mathbb{Z}_1$ e' l'anello banale $\{0\}$, e per $n \neq 0, 1$ $\mathbb{Z}_n$ e' un anello finito, di ordine n. Riassumendo, si ha

Proposition 3. *Sia A un anello, sia $f : \mathbb{Z} \to A$ l'unico omomorfismo di anelli da $\mathbb{Z}$ ad A, e sia $n \in \mathbb{Z}^+$. Sono equivalenti: (1)* $\mathrm{char}(A) = n$; *(2)* $\mathrm{Ker}(f) = n\mathbb{Z}$; *(3)* $f(\mathbb{Z}) \cong \mathbb{Z}_n$.

4. **Primi fatti sugli anelli di classi di resti**

Consideriamo gli anelli $\mathbb{Z}_n$, $n \in \mathbb{Z}^+$ con $n \neq 0, 1$; ciascun $\mathbb{Z}_n$ e' un anello finito, di ordine n. Una parte delle proprieta' di questi anelli deriva da fatti generali su monoidi e anelli finiti.

Proposition 4. *Un monoide finito e' regolare se e solo se e' un gruppo.*

Dim. (parte non ovvia). Sia $M = (M, *, e)$ un monoide regolare finito. Ciascun $m \in M$ si puo' rappresentare come una endofunzione $t_m : M \to M$, $x \mapsto m * x$; questa endofunzione, per l'ipotesi M regolare, e' iniettiva e dunque, per l'ipotesi M finito, e' anche suriettiva; esiste allora un $m' \in M$ tale che $t_m(m') = e$, cioe' $m * m' = e$. Abbiamo cosi' provato che ciascun elemento di M posside un inverso destro; in modo analogo si prova che ciascun elemento di M possiede uninverso sinistro; cio' basta per affermare che ciascun elemento di M possiede un inverso bilatero.

Applicando questa proposizione al monoide moltiplicativo ridotto, cioe' privato dello zero, di un anello finito si ha

Proposition 5. *Un anello finito e' un dominio d'integrita' se e solo se e' un campo.*

Per gli anelli classi di resti si ha

Proposition 6. *Per un anello $\mathbb{Z}_n$, con $n \in \mathbb{Z}^+$ e $n \neq 0, 1$, sono equivalenti: (1) $\mathbb{Z}_n$ e' un dominio d'integrita'; (2) $\mathbb{Z}_n$ e' un campo; (3) n e' primo.*

Dim. (equivalenza fra (1) e (3))

Sia n non primo. Allora si ha $n = ab$, per qualche a, b interi con $1 < a, b < n$; in $\mathbb{Z}_n$ si ha dunque $[0]_n = [a]_n[b]_n$ e $[a]_n, [b]_n \neq [0]_n$; cio' significa che $\mathbb{Z}_n$ non e' un dominio di integrita'.

Sia n primo. Siano $[a]_n$ e $[b]_n$ in $\mathbb{Z}_n$ tali che $[a]_n[b]_n = [0]_n$; cio' significa che ab e' divisibile per n, e dunque, per il lemma di Euclide, almeno uno fra a e b e' divisibile per n; cio' significa che almeno una fra $[a]_n$ e $[b]_n$ e' $[0]_n$. Cio' significa che $\mathbb{Z}_n$ e' un dominio d'integrita'.

5. Dal punto precedente, per quanto riguarda caratteristica e sottoanello fondamentale si ha

   Proposition 7. *Sia A un dominio di integrita'. Allora la caratteristica di A e' 0 e dunque il sottoanello minimo di A e' $\cong \mathbb{Z}$, oppure la caratteristica di A e' un numero primo p e dunque il sottoanello minimo di A e' $\cong \mathbb{Z}_p$.*

Campo dei numeri razionali

1. Nel perscorso che stiamo seguendo, stiamo dando le costruzioni dal seminanello ordinato $\mathbb{N}$ dei numeri naturali all'anello ordinato $\mathbb{Z}$ degli interi relativi al campo ordinato $\mathbb{Q}$ dei razionali al campo ordinato completo $\mathbb{R}$ dei numeri reali. Un altro percorso potrebbe essere dal seminanello ordinato $\mathbb{N}$ dei numeri naturali al semicampo ordinato $\mathbb{Q}^+$ dei razionali non negativi al semicampo ordinato completo $\mathbb{R}^+$ dei reali non negativi al campo ordinato completo $\mathbb{R}$ dei numeri reali (si noti che questo secondo percorso, tranne l'ultimo passo, era gia' sostanzialmente presente in Euclide).

Consideriamo la costruzione dall'anello $\mathbb{Z}$ degli interi relativi al campo $\mathbb{Q}$ dei razionali. Non consideriamo il problema della sua presentazione dal punto di vista didattico. Stabiliamo solo il fatto che tale costruzione e' un caso particolare di una costruzione del campo dei quozienti di un domino di integrita' (commutativo).

Theorem 1. *Dato un dominio d'integrita' A, esiste un campo $Q(A)$ contenente un sottoanello A' isomorfo ad A tale che ogni elemento di $Q(A)$ e' del tipo $a \cdot b^{-1}$, con $a, b \in A'$.*

Il campo $Q(A)$ si dice "campo dei quozienti" dell'anello A.

Dim. (punti principali; cfr EAV 1415, Par. 3.4 p.75-77).

1- Si considera l'insieme delle coppie ordinate di elementi di A, con seconda componente $\neq 0$; ciascuna tale coppia con componenti (nell'ordine) a e b si dice "frazione" su A e si indica con $\frac{a}{b}$. Si definscono operazioni di addizione e di moltiplicazione di frazioni ponendo

$$\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1 b_2 + b_1 a_2}{b_1 b_2}, \qquad \frac{a_1}{b_1} \cdot \frac{a_2}{b_2} = \frac{a_1 a_2}{b_1 b_2};$$

si prova che queste operazioni sono ben definite, commutative, associative e possiedono elemento neutro, rispettivamente $\frac{0}{1}$ e $\frac{1}{1}$.

2- Si introduce sull'insieme delle frazioni una relazione $\sim$ ponendo

$$\frac{a_1}{b_1} \sim \frac{a_2}{b_2} \text{ sse } a_1 b_2 = b_1 a_2,$$

e si prova che e' una relazione di equivalenza, compatibile con le operazioni di addizione e moltiplicazione, cioe' e' una congruenza della struttura.

3- Si considera la struttura quoziente rispetto alla congruenza $\sim$; in essa ovviamente le operazioni di addizione e moltiplicazione continuano ad essere commutative e associative, con le classi $[\frac{0}{1}]$ e $[\frac{1}{1}]$ come elementi neutri; si prova che vale la proprieta' distributiva, e che ogni ogni classe $[\frac{a}{b}]$ possiede classe opposta e, se $[\frac{a}{b}] \neq [\frac{0}{1}]$, anche classe inversa, date da

$$-\left[\frac{a}{b}\right] = \left[\frac{-a}{b}\right], \quad \left[\frac{a}{b}\right]^{-1} = \left[\frac{b}{a}\right];$$

il campo cosi' ottenuto e' il campo $Q(A)$ dei quozienti di A.

4-Si considera la funzione $\Phi : A \to Q(A)$, $a \mapsto [\frac{a}{1}]$, si nota che e' un omomorfismo iniettivo di anelli, e si definisce $A' = \Phi(A)$. Infine si nota che ogni classe si puo' scrivere come

$$\left[\frac{a}{b}\right] = \left[\frac{a}{1}\right] \left[\frac{b}{1}\right]^{-1}.$$

Il campo dei quozienti ha la seguente proprieta' universale

Theorem 2. *Sia A un dominio di integrita', e siano $Q(A)$ il suo campo dei quozienti e $\Phi : A \to Q(A)$ il monomorfismo di anelli dati dal Th. precedente; allora per ogni campo K ed ogni monomorfismo di anelli $f : A \to K$ esiste uno ed un solo omomorfismo di campi $\hat{f} : Q(A) \to K$ tale che $f = \hat{f} \circ \Phi$.*

Dim. Sia dato un campo K ed un monomorfismo di anelli $f : A \to K$. Supponiamo che esista un omomorfismo $\hat{f} : Q(A) \to K$ con le proprieta' richieste. Ogni elemento $x \in Q(A)$ si puo' scrivere come $x = \Phi(a) \cdot \Phi(b)^{-1}$ con $a, b \in A$, e dunque si ha

$$\hat{f}(x) = \hat{f}\left(\Phi(a) \cdot \Phi(b)^{-1}\right) = \hat{f}(\Phi(a)) \left(\hat{f}(\Phi(b))\right)^{-1} = f(a)(f(b))^{-1}$$

dunque f e' univocamente determinata. Viceversa, se per ciascun $x \in Q(A)$ si considera una sua sua scrittura $x = \Phi(a)(\Phi(b))^{-1}$ con $a, b \in A$ e si considera l'elemento $f(a)(f(b))^{-1}$ in K, si prova che si ottiene effettivamente una funzione $\hat{f} : Q(A) \to K$, che questa funzione e' un omomorfismo di campi, e che $f = \hat{f} \circ \Phi$.

2. Si definsce il campo $\mathbb{Q}$ dei numeri razionali come il campo dei quozienti dell'anello $\mathbb{Z}$ degli interi relativi:
$$\mathbb{Q} = Q(\mathbb{Z}).$$