Lezione del 09.03; Registro dettagliato, parte su proprieta' universali e strutture libere

1. $\mathbb{N} = (\mathbb{N}, +, 0)$ e' un monoide commutativo regolare; queste proprieta' non lo caratterizzano, ma e' unico nel senso dato di seguito.

   Un primo fatto sulla struttura di $\mathbb{N}$. $\mathbb{N}$ e' generato da $1(= \sigma(0))$, nel senso che l'unico sottomonoide di $\mathbb{N}$ che contiene 1 e' $\mathbb{N}$ stesso. Un secondo fatto, piu' forte, sulla relazione fra $\mathbb{N}$ e gli altri monoidi, non necessariamente commutativi.

   Proposition 1. *Per ogni monoide $M = (M, *, e)$ e per ogni $x \in M$, esiste uno ed un solo omomorfismo $f : \mathbb{N} \to M$ tale che $f(1) = x$; esplicitamente:*

   $$f(0) = e, \quad f(n+1) = f(n) * x \quad \forall n \in \mathbb{N}.$$

   Commento. Certamente, se $f : \mathbb{N} \to M$ e' un omomorfismo di monoidi tale che $f(1) = x$ allora f deve soddisfare le condizioni di sopra, e per il principio di induzione queste condizioni definiscono una ed una sola funzione $f : \mathbb{N} \to M$; si prova che tale funzione e' un omomorfismo di monoidi.

   Se il monoide M e' in notazione additiva, si ottengono i multipli interi naturali di x; ad esempio questo e' il caso del monoide delle grandezze ottenuto a partire dai segmenti. Se il monoide M e' in notazione moltiplicativa, si ottengono le potenze intere naturali di x; ad esempio questo e' il caso del monoide delle endofunzioni di un insieme.

2. **Monoidi liberi**.

   Definition 1. *Sia S un insieme. Un monoide libero su S e' una coppia (M, i) costituita da un monoide M e da una funzione $i : S \to M$ con la seguente proprieta' universale*

   > *per ogni coppia (P, j) costituita da un monoide P e da una funzione $j : S \to M$ esiste uno ed un solo omomorfismo di monoidi $\hat{j} : M \to P$ tale che $j = \hat{j} \circ i$.*

La condizione si esprime graficamente rappresentando S, M, P con punti, le funzioni e l'omomorfismo con frecce, e la condizione con la richiesta che il diagramma commuti. Questa e' una istanza, espressa in linguaggio piu' grezzo, della definizione di una struttura libera mediante una proprieta' universale (cfr. ad. es Maclane e Birkhoff, Algebra, I ed. italiana del 1975).

Commento. La condizione di sopra puo' anche essere espressa dicendo che la funzione i e' iniettiva e ogni funzione dal sottinsieme $i(S)$ di M ad un monoide puo' essere estesa in uno ed un solo modo ad un omomorfismo da M a tale monoide.

Osservazione. Come caso particolare, si ha che se (M, i) e' un monoide libero su S allora l'omomorfismo id_M identita' su M e' l'unico endomorfismo di M che fissa $i(S)$.

Theorem 1. *Sia S un insieme. Allora:*

(1) esiste un monoide libero su S;

(2) se (M_1, i_1) ed (M_2, i_2) sono due monoidi liberi su S, allora esiste uno ed un solo isomorfismo di monoidi $f_{21} : M_1 \to M_2$ tale che $f_{21} \circ i_1 = i_2$.

Questo teorema permette in particolare di parlare del (e non solo di un) monoide libero su S. L'affermazione sull'esistenza verra' provata piu' avanti; l'affermazione sull'unicita' e' stata provata (cfr. appunti Lez. 09.03).

Commento. Si verifica che a insiemi equipotenti corrispondono monoidi liberi isomorfi.

3. Possiamo allora esprimere quanto stabilito al punto (1) nel modo seguente. Indicato con $\bullet$ un insieme con un solo elemento, la coppia $(\mathbb{N}, \to)$ costituita dal monoide $\mathbb{N} = (\mathbb{N}, +, 0)$ e dalla funzione $\bullet \to \mathbb{N}$, $\bullet \mapsto 1$, e' il monoide libero su un elemento.

4. $\mathbb{Z} = (\mathbb{Z}; +, 0, -)$ e' un gruppo commutativo; questa proprieta' non lo caratterizza, ma e' unico nel senso dato di seguito.

   Un primo fatto sulla struttura di $\mathbb{Z}$. $\mathbb{Z}$ e' generato da 1, nel senso che l'unico sottogruppo di $\mathbb{Z}$ che contiene 1 e' $\mathbb{Z}$ stesso (e' generato anche da -1, e non e' generato da nessun altro elemento). Un secondo fatto,

piu' forte, sulla relazione fra $\mathbb{Z}$ e gli altri gruppi, non necessariamente commutativi.

Proposition 2. *Per ogni gruppo $G = (M, *, e, ')$ e per ogni $x \in G$, esiste uno ed un solo omomorfismo $f : \mathbb{Z} \to G$ tale che $f(1) = x$; esplicitamente:*

$$f(0) = e, \quad f(n+1) = f(n) * x, \quad f(-(n+1)) = f(-n) * x', \quad \forall n > 0.$$

Se il gruppo G e' in notazione additiva, si ottengono i multipli interi relativi di x; ad esempio questo e' il caso del gruppo dei vettori del piano euclideo. Se il gruppo G e' in notazione moltiplicativa, si ottengono le potenze intere relative di x; ad esempio questo e' il caso del gruppo simmetrico di un insieme.

5. **Gruppi liberi**.

   Definition 2. *Sia S un insieme. Un gruppo libero su S e' una coppia (G, i) costituita da un gruppo G e da una funzione $i : S \to G$ con la seguente proprieta' universale*

   > *per ogni coppia (H, j) costituita da un gruppo H e da una funzione $j : S \to H$ esiste uno ed un solo omomorfismo di gruppi $\hat{j} : G \to H$ tale che $j = \hat{j} \circ i$.*

   Theorem 2. *Sia S un insieme. Allora:*

   (1) esiste un gruppo libero su S;

   (2) se (G_1, i_1) e (G_2, i_2) sono due gruppi liberi su S, allora esiste uno ed un solo isomorfismo di gruppi $f_{21} : M_1 \to M_2$ tale che $f_{21} \circ i_1 = i_2$.

   Questo teorema permette in particolare di parlare del (e non solo di un) gruppo libero su S. L'affermazione sull'esistenza verra' provata piu' avanti; l'affermazione sull'unicita' si prova esattamente come per i monoidi.

6. Possiamo allora esprimere quanto stabilito al punto (4) nel modo seguente. Indicato con $\bullet$ un insieme con un solo elemento, la coppia $(\mathbb{Z}, \to)$ costituita dal gruppo $\mathbb{Z} = (\mathbb{Z}, +, 0, -)$ e dalla funzione $\bullet \to \mathbb{Z}$, $\bullet \mapsto 1$, e' il gruppo libero su un elemento.

7. $\mathbb{Z} = (\mathbb{Z}; +, 0, -; \cdot, 1)$ e' un anello commutativo regolare, in breve un dominio di integrita'; queste proprieta' non lo caratterizzano, ma e' unico nel senso dato di seguito. Qui e in seguito consideriamo solo anelli con unita' e morfismi di anelli che preservino l'unita'.

   Un primo fatto sulla struttura di $\mathbb{Z}$. $\mathbb{Z}$ e' generato da 1, nel senso che l'unico sottoanello di $\mathbb{Z}$ che contiene 1 e' $\mathbb{Z}$ stesso. Un secondo fatto, piu' forte, sulla relazione fra $\mathbb{Z}$ e gli altri anelli, non necessariamente commutativi.

   Proposition 3. *Per ogni anello A esiste uno ed un solo omomorfismo di anelli $f : \mathbb{Z} \to A$; esplicitamente:*

$$f(n) = n \cdot 1_A \quad \forall n \in \mathbb{Z}$$

   dove $n \cdot 1_A$ indica il multiplo di 1_A secondo l'intero relativo n.

   Dim. Sia $f : \mathbb{Z} \to A$ un morfismo di anelli. Allora, in particolare $f : (\mathbb{Z}, +) \to (A, +)$ e' un morfismo di gruppi, inoltre $f(1) = 1_A$. Queste condizioni individuano uno ed un solo omomorfismo dal gruppo additivo di $\mathbb{Z}$ a quello di A, quello descritto nell'enunciato. Si verifica che questo e' anche un omomorfismo dal monoide moltiplicativo di $\mathbb{Z}$ a quello di A.

   Definition 3. *L'immagine di $\mathbb{Z}$ in un anello A, tramite l'unico omomorfismo di anelli $\mathbb{Z} \to A$ si dice "sottoanello minimo", o "sottoanello fondamentale", di A.*