Lezione del 11 marzo; Registro dettagliato

Si e' mostrato come alle prime nozioni e costruzioni sugli insiemi corrispondano le prime nozioni e costruzioni sulle strutture algebriche; in particolare si sono considerati gruppi abeliani e anelli commutativi, e piu' in particolare il gruppo additivo e l'anello degli interi relativi $\mathbb{Z}$, e si e' mostrata un'applicazione all'aritmetica elementare.

Per ciascun insieme A si possono considerare: i sottinsiemi di A, le relazioni d'equivalenza su A e le partizioni di A; associando a ciascuna relazione d'equivalenza su A l'insieme delle classi di equivalenza si ottiene una partizione di A, associando a ciascuna partizione di A la relazione "appartenere ad uno stesso blocco" si ottiene una relazione d'equivalenza su A, e componendo le due costruzioni si torna al dato di partenza; la partizione di A associata ad una relazione d'equivalenza $\sim$ su A viene detta "insieme quoziente di A su $\sim$" e viene indicata con $A/\sim$, si pone cioe' $\{[x]_\sim;\ x \in A\} = A/\sim$; si ha infine una funzione suriettiva, la "proiezione canonica" associata a $\sim$:

$$\pi_\sim : A \to A/\sim; \quad x \mapsto [x]_\sim.$$

Gruppi

Sia $G = (G; +, 0, -)$ un gruppo in notazione additiva. Ricordiamo che un sottinsieme H di G si dice sottogruppo di G se e solo se H e' chiuso rispetto all'operazione binaria $+$, contiene 0, ed e' chiuso rispetto all'operazione unaria $-$ (leggermente informale: un sottogruppo di un gruppo non e' solo un insieme ...).

Proposition 1. *I sottogruppi di $\mathbb{Z} = (\mathbb{Z}; +, 0, -)$ sono tutti e soli i sottinsiemi di $\mathbb{Z}$ costituiti dai multipli interi relativi di un fissato intero (non-negativo, per semplicita'), cioe' i sottinsiemi del tipo*

$$n\mathbb{Z} = \{m \cdot n |\ m \in \mathbb{Z}\}, \quad n \in \mathbb{Z}^+$$

La dimostrazione si basa sulla operazione di divisione con resto. Questa operazione si esprime usualmente nei termini di addizione e moltiplicazione, ma e' esprimibile nei termni della sola operazione di addizione, in fondo perche' in $\mathbb{N}$ la moltiplicazione e' definita a partire dall'addizione.

Sia $G = (G; +, 0, -)$ un gruppo in notazione additiva; supponiamo che G sia abeliano (grande limitazione, ma per il momento e' cio' che ci interessa).

Ricordiamo che una realzione d'equivalenza $\sim$ su G si dice congruenza su G se e solo se $\sim$ e' compatibile con l'operazione binaria $+$ (e dunque compatibile anche con l'operazione unaria $-$):

$$g_1 \sim h_1 \text{ e } g_2 \sim h_2 \text{ implica } g_1 + g_2 \sim h_1 + h_2 \qquad \forall \dots .$$

In tal caso sull'insieme quoziente $G/\sim = \{[x]_\sim |\ x \in G\}$ e' ben definita l'operazione

$$[x]_\sim + [y]_\sim = [x+y]_\sim, \qquad \forall [x]_\sim, [y]_\sim \in G/\sim;$$

la struttura cosi' ottenuta e' un gruppo abeliano, ... il gruppo quoziente di G rispetto a $\sim$; la proiezione canonica

$$\pi_\sim : G \mapsto G/\sim, \quad x \mapsto [x]_\sim$$

e' un epimorfismo di gruppi (omomorfismo suriettivo).

Per ciascuna congruenza $\sim$ su G si ha: (1) la classe $[0]_\sim$ e' un sottogruppo di G, detto nucleo della congruenza; (2) ciascuna classe $[x]_\sim$ si puo' scrivere come "laterale" del nucleo di G :

$$[x]_\sim = [0]_\sim + x = \{y + x |\ y \in [0]_\sim\}.$$

Per ciascun sottogruppo H di G, si ha che: (1) i laterali $H + x = \{y + x |\ y \in H\}$ di H in G costituiscono una partizione di G; (2) la relazione di equivalenza $\sim_H$ associata a questa partizione, data da

$$x \sim_H y \text{ sse } H + x = H + y \text{ sse } x - y \in H$$

e' una congruenza di G (grazie alla commutativita' ...).

Dalla caratterizzazione dei sottogruppi di $\mathbb{Z}$ segue direttamente la caratterizzazione delle congruenze su $\mathbb{Z}$:

Proposition 2. *Le congruenze sul gruppo $\mathbb{Z} = (\mathbb{Z}; +, 0, -)$ sono tutte e sole le congruenze modulo un intero non-negativo, cioe' le relazioni del tipo*

$$x \equiv_n y \text{ sse } x - y \text{ divisibile per } n, \qquad n \in \mathbb{Z}^+.$$

Le classi d'equivalenza si dicono classi di resti modulo n. Per $n > 0$ il gruppo quoziente e' dato da

$$\mathbb{Z}/n\mathbb{Z} = \{[0]_n, [1]_n, \dots, [n-1]_n\},$$

con l'operazione

$$[x]_n + [y]_n = [x+y]_n = [z]_n,$$

dove z e' il resto della divisione di $x+y$ su n.

Anelli

Sia $A = (A; +, 0, -; \cdot, 1)$ un anello; supponiamo che A sia commutativo (significativa limitazione, ma per il momento e' cio' che ci interessa). Ricordiamo che un sottinsieme H di A si dice ideale di A se e solo se H e' un sottogruppo del gruppo additivo $A = (A; +, 0, -)$ ed e' chiuso rispetto alla moltiplicazione esterna per elementi di A, cioe'

$$x \cdot y \in A, \qquad \forall x \in H,\ y \in A.$$

Proposition 3. *Per ciascun sottinsieme H dell'anello $\mathbb{Z} = (\mathbb{Z}; +, 0, -; \cdot, 1)$ le seguenti condizioni sono equivalenti: (1) H e' un sottogruppo del gruppo additivo di $\mathbb{Z}$; (2) H e' un ideale dell'anello $\mathbb{Z}$; (3) $H = n\mathbb{Z}$, per qualche $n \in \mathbb{Z}^+$.*

Sia $A = (A; +, 0, -; \cdot, 1)$ un anello; supponiamo che A sia commutativo. Ricordiamo che una relazione d'equivalenza $\sim$ su A si dice congruenza su A se e solo se $\sim$ e' compatibile con le operazione binarie $+$ e $\cdot$. In tal caso sull'insieme quoziente $A/\sim = \{[x]_\sim |\ x \in A\}$ sono ben definite sulle classi di equivalenza le operazioni date sui rappresentanti; la struttura cosi' ottenuta e' un anello commutativo, ... l'anello quoziente di A rispetto a $\sim$; la proiezione canonica

$$\pi_\sim : A \mapsto A/\sim, \quad x \mapsto [x]_\sim$$

e' un epimorfismo di anelli (omomorfismo suriettivo).

Per ciascuna congruenza $\sim$ su A si ha: (1) la classe $[0]_\sim$ e' un ideale di A, detto nucleo della congruenza; (2) ciascuna classe $[x]_\sim$ si puo' scrivere come "laterale" del nucleo di A :

$$[x]_\sim = [0]_\sim + x = \{y + x |\ y \in [0]_\sim\}.$$

Per ciascun ideale H di A, si ha che: (1) i laterali $H + x = \{y + x |\ y \in H\}$ di H in A costituiscono una partizione di A; (2) la relazione di equivalenza $\sim_H$ associata a questa partizione, data da

$$x \sim_H y \text{ sse } H + x = H + y \text{ sse } x - y \in H$$

e' una congruenza di A (grazie alla commutativita' ...).

Le congruenze sulll'anello $\mathbb{Z} = (\mathbb{Z}; +, 0, -; \cdot, 1)$ sono tutte e sole le congruenze del gruppo additivo di $\mathbb{Z}$, cioe' le congruenze modulo un intero non-negativo. Per $n > 0$ l'anello quoziente e' dato da

$$\mathbb{Z}/n\mathbb{Z} = \{[0]_n, [1]_n, \ldots, [n-1]_n\},$$

con le operazioni

$$[x]_n + [y]_n = [x+y]_n = [z]_n, \qquad [x]_n \cdot [y]_n = [x \cdot y]_n = [t]_n,$$

dove z e' il resto della divisione di $x + y$ su n e t e' il resto della divisione di $x \cdot y$ su n.

Applicazione

Consideriamo per gli elementi l'anello $\mathbb{Z}$ degli interi relativi la rappresentazione in base 10 e l'omomorfismo di anelli dato dalla proiezione $p_9 : \mathbb{Z} \to \mathbb{Z}_9$ dell'anello $\mathbb{Z}$ sull'anello $\mathbb{Z}_9$ delle classi di resti modulo 9. Per ogni scrittura decimale di un intero $c_r \cdots c_1 c_0 = c_r 10^r + \cdots + c_1 10 + c_0$ (positivo, per semplicita') si ha

$$p_9(c_r \cdots c_1 c_0) = [c_r + \cdots + c_1 + c_0]_9$$

... da cio' deriva la nota "regola del nove" per la verifica di calcoli sugli interi.