Aritmetica, Tutorato 4

Rivediamo la costruzione del quoziente per gruppi.

Se G è un gruppo, $\mathcal{H} < G$ è un sottogruppo, possiamo considerare

$$G/\mathcal{H} = \{\text{laterali sinistri di } \mathcal{H} \text{ in } G\}$$
$$= \{g\mathcal{H} \mid g \in G\}.$$

Nessun problema nello scegliere laterali destri, ma "laterali" e basta è <u>ambiguo</u>: in generale, $gH \neq Hg$!

Vorremmo dare a $G/\mathcal{H}$ una "naturale" struttura di gruppo, cioè speriamo che $G/\mathcal{H}$ sia un gruppo con l'operazione "indotta" da G, vale a dire quella ottenuta ponendo

$$g_1\mathcal{H} \cdot g_2\mathcal{H} := (g_1 g_2)\mathcal{H}. \qquad (*)$$

<u>PROBLEMA</u> Poiché, preso $h \in \mathcal{H}$, vale

$$g\mathcal{H} = (gh)\mathcal{H},$$

non è detto che l'operazione scritta sopra sia ben definita (in generale, <u>non lo sarà</u>): vediamo come cambia il risultato al variare della scelta di rappresentanti per i laterali. Notiamo che, presi $g, g' \in \mathcal{H}$,

$$\begin{aligned} g\mathcal{H} = g'\mathcal{H} &\iff \mathcal{H} = g^{-1}g'\mathcal{H} \\ &\iff g^{-1}g' \in \mathcal{H} \\ &\iff \text{esiste } h \in \mathcal{H} \text{ t.c. } g^{-1}g' = h, \text{ e} \\ &\qquad g'\mathcal{H} = g(g^{-1}g')\mathcal{H} \\ &\qquad\quad = gh\mathcal{H} \end{aligned}$$

cioè due laterali $g\mathcal{H}$, $g'\mathcal{H}$ sono uguali $\iff g'\mathcal{H} = gh\mathcal{H}$ per un certo $h \in \mathcal{H}$.

Fissiamo allora $g_1, g_2 \in G$, $h_1, h_2 \in \mathcal{H}$: perché l'operazione $(*)$ sia ben def. deve valere

$$g_1\mathcal{H} \cdot g_2\mathcal{H} = g_1 h_1 \mathcal{H} \cdot g_2 h_2 \mathcal{H},$$

cioè

$$(g_1 g_2)H = (g_1 h_1 g_2 h_2) H.$$

Questo è vero se e solo se

$$\cancel{g_2^{-1}} \cancel{g_1^{-1}} \cancel{g_1} \cancel{g_2} H = g_2^{-1} g_1^{-1} g_1 h_1 g_2 h_2 H$$

$$\iff \quad H = g_2^{-1} \cancel{g_1^{-1} g_1} h_1 g_2 h_2 H$$

$$\iff \quad H = g_2^{-1} h_1 g_2 h_2 H$$

$$\iff \quad H = g_2^{-1} h_1 g_2 H, \quad \longleftarrow h_2 \in H \Rightarrow h_2 H = H.$$

cioè se e solo se

$$g_2^{-1} h_1 g_2 \in H \text{ per ogni } h_1 \in H, g_2 \in G,$$

o anche, scambiando $g_2 \leftrightarrow g_2^{-1}$ e togliendo gli indici,

$$g h g^{-1} \in H \text{ per ogni } h \in H, g \in G. \quad (\Pi)$$

Per $g \in G$, avete chiamato <u>coniugio</u> l'automorfismo di G definito da

$$\gamma_g : G \longrightarrow G, \quad x \longmapsto g x g^{-1}.$$

Isoliamo allora la classe di sgp. di G con la proprietà (Π):

<u>Def</u> Un sgp. H di un gp G è <u>normale</u> in G (scriviamo $H \triangleleft G$) se è chiuso per coniugio di elementi di G, cioè

$$g h g^{-1} \in H \text{ per ogni } h \in H, g \in G.$$

Abbiamo quindi mostrato

<u>Fatto</u> L'operazione $(*)$ indotta da G su G/H è ben definita $\iff$ H è normale in G.

In realtà, è facile convincersi che la buona definizione era il punto cruciale: se $H \triangleleft G$, l'operazione $(*)$ su G/H rispetta gli assiomi di gruppo. Vediamo ad esempio l'esistenza di un elt. neutro: se e è l'elt. neutro di G, la scelta naturale per un elt. neutro in G/H ricade su $eH = H$, e in effetti

- $(eH)(gH) = (eg)H = gH$

- $(gH)(eH) = (ge)H = gH$

per ogni $g \in H$, in quanto e è l'identità di G. Tutte le altre verifiche sono analogamente facili, e discendono dal fatto che $(*)$ è indotta da un'op. di gruppo. Si ottiene perciò:

<u>Fatto</u> Se $H \lhd G$, G/H è un gruppo con l'operazione indotta da G, cioè quella definita ponendo

$$g_1H \cdot g_2H := g_1g_2H$$

per ogni $g_1, g_2 \in G$.

Vediamo alcune caratterizzazioni equivalenti della normalità:

<u>Esercizio</u> Per $H < G$, sono equiv:

(i) $H \lhd G$,

(ii) $gHg^{-1} \subset H$ per ogni $g \in G$,

(iii) $gHg^{-1} = H$ per ogni $g \in G$,

(iv) $gH = Hg$ per ogni $g \in G$.

<u>dim.</u> Le implicazioni sono tutte manipolazioni algebriche facili: è <u>estremamente</u> più utile che le facciate da soli. <u>Fatele</u> e, se avete dubbi, chiedete! $\square$

La (iv) dice che i sottogruppi normali sono esattamente quelli che risolvono l'ambiguità iniziale nella def. dell'<u>insieme</u> G/H, cioè quelli per cui laterali dx = laterali sx! In sostanza: se sappiamo dire senza esitazione chi deve essere l'<u>insieme</u> quoziente, allora questo è un gruppo con l'operazione indotta! Bello, no?

<u>Esercizio</u> Se G, H sono gruppi, poniamo

$$\mathrm{Hom}(G,H) := \{\varphi : G \to H \mid \varphi \text{ omomorfismo}\},$$

l'insieme degli omomorfismi $G \to H$. Descrivere $\mathrm{Hom}(G,H)$ nei casi:

(i) $G = \mathbb{Z}/n$, $n > 1$, $H = \mathbb{Z}$;

(ii) $G = \mathbb{Z}_5$, $\mathcal{H} = \mathbb{Z}_3$.

dim. Prima di affrontare l'esercizio ricordiamo le proprietà base degli omomorfismi, cioè delle funzioni $\varphi : G \to \mathcal{H}$ tali che

$$(\Delta) \quad \varphi(xy) = \varphi(x)\varphi(y) \text{ per ogni } x, y \in G.$$

Fatti Sia $\varphi : G \to \mathcal{H}$ un omomorfismo. Allora:

(I) $\varphi(e_G) = e_{\mathcal{H}}$, con e_G, $e_{\mathcal{H}}$ le identità di $G, \mathcal{H}$ risp.;

(II) $\varphi(g^{-1}) = \varphi(g)^{-1}$ per ogni $g \in G$;

(III) se $g \in G$ ha ordine finito k, $\varphi(g)$ ha ordine finito h e $h \mid k$

["l'ordine di arrivo divide l'ordine di partenza"].

(i) Sicuramente, la funzione $\varphi_0 : \mathbb{Z}/_n \to \mathbb{Z}$, $\varphi_0(x) = 0$ per ogni $x \in \mathbb{Z}/_n$ è un omomorfismo, in quanto

$$\varphi_0(x+y) = 0 = \varphi_0(x) + \varphi_0(y).$$

[Più in generale: se $G, \mathcal{H}$ sono gp., la mappa $G \to \mathcal{H}$, $x \mapsto e_{\mathcal{H}}$ è un hom, che diciamo banale].

Ce ne sono altri? Poiché ogni elemento di $\mathbb{Z}/_n$ ha ordine finito (per il teorema di Lagrange), il punto (III) sopra dice:

se $\psi : \mathbb{Z}/_n \to \mathbb{Z}$ è un hom, $\psi(x) \in \mathbb{Z}$ ha ordine finito per ogni $x \in \mathbb{Z}/_n$.

Chi sono gli elt. di ordine finito in $\mathbb{Z}$? Solo 0: se $n \neq 0$,

$$\underbrace{n + n + \cdots + n}_{k \text{ volte}} = kn \neq 0 \text{ per ogni } k \neq 0,$$

quindi necessariamente $\psi(x) = 0$ per ogni $x \in \mathbb{Z}/_n$, cioè $\psi = \varphi_0$.

In conclusione, c'è un unico hom $\mathbb{Z}/_n \to \mathbb{Z}$, quello banale.

(ii) Notiamo che, siccome $\mathbb{Z}$ è ciclico, generato da 1 (o -1), ogni omomorfismo $\psi : \mathbb{Z} \to \mathcal{H}$, con $\mathcal{H}$ un gruppo, è univocamente determinato da $\psi(1)$. Infatti:

Lemma Sia G un gruppo, e sia $x \in G$. Per $k \in \mathbb{Z}$, indichiamo con

$$x^k := \begin{cases} x \cdot x \cdots x & k \text{ volte, se } k > 0 \\ e_G, & \text{se } k = 0 \\ x^{-1} \cdot x^{-1} \cdots x^{-1} & |k| \text{ volte, se } k < 0 \end{cases}$$

Se H è un gruppo e $\varphi : G \to H$ è un hom, vale

$$\varphi(x^k) = \varphi(x)^k; \quad k \in \mathbb{Z}$$

<u>dim.</u> Se $k = 0$, è la proprietà (I) sopra.

Se $k > 0$, la dimostrazione è per induzione usando (Δ): il caso base è immediato; quello induttivo è

$$\begin{aligned} \varphi(x^k) &= \varphi(x \cdot x^{k-1}) \overset{(\Delta)}{=} \varphi(x)\varphi(x^{k-1}) \\ \text{hp. ind} \longrightarrow &= \varphi(x)\varphi(x)^{k-1} \\ &= \varphi(x)^k. \end{aligned}$$

Se $k < 0$, si ha $x^k = (x^{-1})^{|k|}$: quindi,

$$\begin{aligned} \varphi(x^k) &= \varphi((x^{-1})^{|k|}) \\ |k| > 0 \longrightarrow &= \varphi(x^{-1})^{|k|} \\ (\mathrm{II}) \longrightarrow &= ((\varphi(x))^{-1})^{|k|} \\ &= \varphi(x)^k \end{aligned}$$

□

<u>Notazione</u> Se G è abeliano, e usiamo $+$ per indicare l'operazione, usiamo tipicamente anche $-x$ per indicare x^{-1} e kx per x^k, con $k \in \mathbb{Z}$, $x \in G$. Notate che, se $G = \mathbb{Z}$, la notazione è coerente col fatto che

$$kx = \underbrace{x + \cdots + x}_{k \text{ volte}} = k \cdot x. \quad \text{moltiplicazione usuale in } \mathbb{Z}$$

Se quindi $\varphi : \mathbb{Z} \to H$ è un omomorfismo, e $n \in \mathbb{Z}$,

$$\begin{aligned} \varphi(n) &= \varphi(n\,1) \\ \text{Lemma} \longrightarrow &= \varphi(1)^n \end{aligned}$$

Quindi, fissata l'immagine di 1 via φ, l'intero φ è totalmente determinato.

Rimane da capire, per $H = \mathbb{Z}$, per quali scelte di $\varphi(1)$ la funzione φ così ottenuta è effettivamente un omomorfismo.

Fissiamo quindi $n \in \mathbb{Z}$, e supponiamo che $\varphi: \mathbb{Z} \to \mathbb{Z}$ sia un hom tale che $\varphi(1) = n$. Allora, per $m \in \mathbb{Z}$,

$$\varphi(m) = \varphi(m1) = m\varphi(1)$$
$$= m \cdot n,$$

cioè φ è la moltiplicazione per n. È un omomorfismo? Sì: per $s, t \in \mathbb{Z}$,

$$\varphi(s+t) = n \cdot (s+t)$$
$$\varphi(s) + \varphi(t) = ns + nt.$$

In conclusione, gli elementi di $\mathrm{Hom}(\mathbb{Z}, \mathbb{Z})$ sono gli omomorfismi di moltiplicazione per elementi di $\mathbb{Z}$. $\square$

Esercizio Descrivere $\mathrm{Hom}(\mathbb{Z}/_{12}, \mathbb{Z}/_{20})$.

dim. Poiché $\mathbb{Z}/_{12}$ è ciclico e generato da $[1]_{12}$, ogni omomorfismo

$$\varphi: \mathbb{Z}/_{12} \longrightarrow \mathbb{Z}/_{20}$$

è univoc. det. da $\varphi([1]_{12})$ [per lo stesso ragionamento fatto su $\mathbb{Z}$ sopra!], e più precisamente

$$\varphi([k]_{12}) = \varphi(k[1]_{12})$$
$$= k\varphi([1]_{12}) \in \mathbb{Z}/_{20}.$$

Per (III) sopra, e siccome $[1]_{12}$ ha ordine 12, $\varphi([1]_{12})$ deve avere ordine un divisore di 12; d'altra parte, l'ordine di $\varphi([1])_{12} \in \mathbb{Z}/_{20}$ divide 20 per Lagrange, perciò divide $(12, 20) = 4$. In sostanza, un omomorfismo $\varphi: \mathbb{Z}/_{12} \to \mathbb{Z}/_{20}$ deve mandare $[1]_{12}$ in un elemento di ordine 1, 2, 4 in $\mathbb{Z}/_{20}$.

Tali elementi sono $[0]_{20}$, $[10]_{20}$, $[\pm 5]_{20}$ rispettivamente (non ce ne sono altri perché il loro numero è $\varphi(1)$, $\varphi(2)$, $\varphi(4)$, cioè 1, 1, 2 risp.).

Verifichiamo ora che le assegnazioni proposte si estendono effettivamente a ben definiti omomorfismi $\mathbb{Z}/_{12} \to \mathbb{Z}/_{20}$:

- se $\phi([1]_{12}) = [0]_{20}$, si ottiene l'hom banale ✓
- se $\phi([1]_{12}) = [10]_{20}$, vale, per $k \in \mathbb{Z}$,

$$\phi([k]_{12}) = k[10]_{20} = [10k]_{20}.$$

Controlliamo allora che la funzione $\phi([k]_{12}) := [10k]_{20}$ sia ben def e un hom:

  - ϕ è bd $\iff \phi([k]_{12}) = \phi([k+12m]_{12})$ per ogni $m \in \mathbb{Z}$.

  Ma

$$\begin{aligned}\phi([k+12m]_{12}) &= [10k+120m]_{20} \qquad (\star)\\ &= [10k]_{20} + [120m]_{20}\\ \xrightarrow{20 \mid 120} &= [10k]_{20}\\ &= \phi([k]_{12}). \checkmark\end{aligned}$$

  - ϕ è hom? Per $k, h \in \mathbb{Z}$,

$$\begin{aligned}\phi([k+h]_{12}) &= [10(k+h)]_{20}\\ &= [10k]_{20} + [10h]_{20}\\ &= \phi([k]_{12}) + \phi([h]_{12}). \checkmark\end{aligned}$$

- Se $\phi([1]_{12}) = [\pm 5]_{20}$, si ottiene

$$\phi([k]_{12}) = [\pm 5k]_{20}.$$

La verifica che ϕ sia un omomorfismo è identica; quella della buona definizione è analoga, ma 120 in $(\star)$ è sostituito da $\pm 5 \cdot 12 = \pm 60$, e poiché $20 \mid \pm 60$ si conclude allo stesso modo che ϕ è ben definito.

Si ottiene quindi che $\mathrm{Hom}(\mathbb{Z}/12, \mathbb{Z}/20)$ ha 4 elementi, che sono

$$\phi([k]_{12}) = [nk]_{20}$$

con $n \in \{0, 10, 5, -5\}$. $\square$

Es. per voi Adattando gli argomenti appena usati, provate a descrivere

(iii) $\mathrm{Hom}(\mathbb{Z}, \mathbb{Z}/n)$, $n > 1$,

(iv) $\operatorname{Hom}(\mathbb{Z}/m, \mathbb{Z}/n)$, $m, n \geq 1$.