October 1, 2018

QUOZIENTI

Durante lo svolgimento del corso avremo a che fare con diversi "spazi quoziente" che emergeranno naturalmente, per esempio quando studieremo gli effetti di un "cambiamento di sistema di riferimento". E' allora conveniente richiamare alcune nozioni generali sulle *relazioni di equivalenza* e gli *insiemi quoziente*. Come prime applicazioni vedremo diverse costruzioni che producono *campi* (i campi saranno un ingrediente importante dello svolgimento successivo del corso).

Sia X un insieme non vuoto. Una *relazione* su X è un sottoinsieme non vuoto R del prodotto cartesiano: $R \subset X \times X$. Diremo allora che l'elemento x di X è in relazione con l'elemento y se la coppia ordinata $(x, y) \in R$ (scriveremo anche $x \sim_R y$ e a volte ometteremo di indicare la R). $R \subset X \times X$ è una *relazione di equivalenza* se verifica le seguenti proprietà:

(1) *(Riflessiva)* Per ogni $x \in X$, $(x, x) \in R$, cioè la *diagonale* $\Delta := \{(x, x) \in X \times X\} \subset R$.
(2) *(Simmetrica)* $x \sim_R y$ se e solo se $y \sim_R x$. In altre parole, definita l'applicazione

$$j : X \times X \to X \times X,\ j(x, y) = (y, x)$$

allora R è *j-invariante*, cioè $j(R) \subset R$.
(3) *(Transitiva)* Se $x \sim y$ e $y \sim z$, allora $x \sim z$.

Due esempi basici, in un certo senso banali, di relazione di equivalenza sono dati da $R = \Delta$ (per cui $x \sim y$ se e solo se $x = y$) e da $R = X \times X$ per cui ogni x è equivalente a tutti gli altri. Relazioni di equivalenza 'intermedie' più interessanti emergono di solito quando l'insieme X è munito di qualche struttura addizionale. Capita anche spesso che il sottoinsieme R non venga dato esplicitamente ma sia definito in modo implicito.

Data una relazione di equivalenza R su X, per ogni $x \in X$, la sua *classe di equivalenza* è il sottoinsieme di X definito da:

$$[x] = [x]_R := \{y \in X;\ y \sim x\}\ .$$

Ricordiamo che una *partizione di X* è per definizione un insieme $\mathcal{U}$ di sottoinsiemi di X (cioè $\mathcal{U}$ è un sottoinsieme dell'insieme $\mathcal{P}(X)$ delle parti di X) che verifichi le seguenti proprietà:

(1) Ogni $U \in \mathcal{U}$ è non vuoto;
(2) Per ogni $x \in X$ esiste $U \in \mathcal{U}$ tale che $x \in U$ (cioè l'unione degli elementi di $\mathcal{U}$ è tutto X, si dice anche che $\mathcal{U}$ *ricopre* X);
(3) Se $U, U' \in \mathcal{U}$ sono diversi allora $U \cap U' = \emptyset$ (elementi diversi di $\mathcal{U}$ sono disgiunti).

La seguente proposizione mostra che relazioni di equivalenza e partizioni sono facce della stessa medaglia.

Proposizione 0.1. *(1) Per ogni relazione di equivalenza su X, le classi di equivalenza degli elementi di X formano una partizione di X;*

(2) Per ogni partizione $\mathcal{U}$ di X, ponendo " $x \sim y$ se e solo se esiste $U \in \mathcal{U}$ tale che $x, y \in U$ ", si definisce una relazione di equivalenza su X tale che se $x \in U \in \mathcal{U}$, allora $U = [x]$.

Dim. Dimostriamo (1): poiché ogni $x \in X$ appartiene ad $[x]$, le prime due proprietà della definizione di partizione seguono immediatamente; se esiste $z \in [x] \cap [y]$, allora (usando le proprietà simmetrica e transitiva) abbiamo che per ogni $u \sim x$, $u \sim x \sim z \sim y$, quindi $u \sim y$; cioè $[x] \subset [y]$; invertendo i ruoli di x e y si ha anche che $[y] \subset [x]$.

Dimostriamo (2): $x \sim x$ perché $\mathcal{U}$ ricopre X; la relazione indotta da $\mathcal{U}$ è evidentemente simmetrica. Se $x, y \in U \in \mathcal{U}$ e $y, z \in U' \in \mathcal{U}$, allora $y \in U \cap U' \neq \emptyset$; quindi $x, z \in U = U'$.

□

Abbiamo visto che le classi di equivalenza rispetto ad una data relazione R formano una partizione di X. L' *insieme quoziente* di X rispetto ad R è per definizione l'insieme che ha per elementi le classi di equivalenza. Esso viene indicato con X/R o anche $X/\sim$. Si noti che ogni classe di equivalenza è sia

un sottoinsieme di X ($[x] \subset X$) che un elemento di X/R ($[x] \in X/R$). E' definta in modo canonico la *proiezione sul quoziente*:

$$\pi : X \to X/R,\ \pi(x) = [x]\ .$$

Chiaramente π è surgettiva e per ogni $x \in X$, $\pi^{-1}(\pi(x)) = \pi^{-1}([x]) = [x]$.

La relazione di equivalenza indotta da una funzione. Sia $f : X \to Y$ una funzione. E' facile verificare che ponendo " $a \sim_f b$ se e solo se $f(a) = f(b)$" si definisce una relazione di equivalenza su X tale che per ogni $a \in X$ $[a]_f = f^{-1}(f(a)) \subset X$. Per ogni $\alpha = [a]_f \in X/R$, definiamo $\bar{f}(\alpha) := f(a)$. Questa applicazione

$$\bar{f} : X/f \to Y$$

è *ben definita* (la scelta del rappresentante della classe α è immateriale), $f(X) = \bar{f}(X/f)$ (hanno la stessa immagine); $\bar{f} \circ \pi = f$; $\bar{f} : X/f \to f(X)$ è bigettiva. C'è quindi un modo canonico di identificare l'insieme quoziente X/f e l'immagine $f(X)$. In molti casi questo aiuta a 'visualizzare' il quoziente.

La relazione di equivalenza indotta dall'azione di un gruppo di trasformazioni. Per ogni insieme non vuoto X,

$$S(X) = \{f : X \to X;\ f \text{ bigettiva}\}$$

è l'insieme di tutte le *trasformazioni* (dette anche *simmetrie*) di X; la *composizione* è un' operazione su $S(X)$ che lo rende un gruppo detto anche il *gruppo simmetrico su* X. Se X ha almeno 3 elementi, tale gruppo non è commutativo. Un *gruppo di trasformazioni di* X è per definizione un *sottogruppo* G di $S(X)$. Questo significa che l'applicazione identità di X, id_X, appartiene a G, G è chiuso rispetto all'operazione (se $f, g \in G$ allora $f \circ g \in G$) ed è invariante per l'applicazione che associa ad ogni f l'applicazione inversa f^{-1}. Ponendo " $x \sim_G y$ se e solo se esiste $f \in G$ tale che $f(x) = y$ ", è facile verificare che si è definita una relazione di equivalenza su X. L'insieme quoziente è indicato come X/G. Di solito emergono gruppi di trasformazioni interessanti quando X è munito di strutture addizionali.

Esempi vari.

(1) Qui $X = \mathbb{R}$. Consideriamo la traslazione $\tau : \mathbb{R} \to \mathbb{R},\ \tau(x) = x + 1$; $\tau^{-1}(y) = y - 1$. Per ogni $n \in \mathbb{Z}$, poniamo τ^n la composizione di n copie di τ se $n \geq 0$ ($\tau^0 = \mathrm{id}$); la composizione di $|n|$ copie di τ^{-1} se $n < 0$. E' facile verificare che $G := \{\tau^n;\ n \in \mathbb{Z}\}$ è un gruppo di trasformazioni di $\mathbb{R}$. Inoltre $x \sim_G y$ se e solo se $x - y \in \mathbb{Z}$. Per cui indicheremo il quoziente come $\mathbb{R}/\mathbb{Z}$. Per visualizzare il quoziente consideriamo l'applicazione

$$f : \mathbb{R} \to \mathbb{R}^2,\ f(x) = (\cos(2\pi x), \sin(2\pi x))\ .$$

Allora $x \sim_G y$ se e solo se $f(x) = f(y)$. L'immagine di f è la circonferenza unitaria

$$S^1 := \{(x, y) \in \mathbb{R}^2;\ x^2 + y^2 = 1\}$$

e sappiamo che $\mathbb{R}/\mathbb{Z}$ è in corrispondenza biunivoca canonica con S^1. L'insieme $\mathbb{R}$ è munito dell'operazione $+$ che lo rende un gruppo commutativo. La somma "passa al quoziente" in modo naturale. Infatti poniamo

$$[x] + [y] = [x + y]$$

è un facile esercizio mostrare che questa somma è ben definita su $\mathbb{R}/\mathbb{Z}$ e lo rende un gruppo commutativo, dove $[0]$ è l'elemento neutro e per ogni $\alpha = [x]$, $-\alpha = [-x]$ (essendo la scelta di un rappresentante di α immateriale). Si nota che $\pi(x+y) = \pi(x)+\pi(y)$, cioè la proiezione sul quoziente è un omomorfismo di gruppi, surgettivo e così $(\mathbb{R}/\mathbb{Z}, +)$ è un *gruppo quoziente* di $(\mathbb{R}, +)$. E' utile descrivere come questa somma agisce su S^1, identificato come sopra con $\mathbb{R}/\mathbb{Z}$. Ogni elemento $(\cos(\theta), \sin(\theta))$ di S^1 codifica la rotazione R_θ di $\mathbb{R}^2$ di angolo θ (misurato in radianti, $R_\theta = R_{\theta+2\pi}$). $R_{\theta+\beta} = R_\theta \circ R_\beta = R_\beta \circ R_\theta$. Queste rotazioni formano un gruppo di trasformazioni di $\mathbb{R}^2$ detto $SO(2)$, e S^1 è invariante per l'azione di questo gruppo. Quindi l'identificazione di $\mathbb{R}/\mathbb{Z}$ con S^1 induce una identificazione del gruppo $(\mathbb{R}/\mathbb{Z}, +)$ con $SO(2)$.

(2) L'esempio precedente può essere generalizzato come segue. Qui $X = \mathbb{R}^n$. Per $i = 1, \ldots, n$, Indichiamo con e_i l'elemento di $\mathbb{R}^n$ che ha i-esima entrata uguale a 1 e le altre uguali a 0. Consideriamo le traslazioni $\tau_i : \mathbb{R}^n \to \mathbb{R}^n,\ \tau_i(x) = x + e_i$. Poniamo $G = \{\tau_1^{n_1} \circ \cdots \circ \tau_n^{n_n};\ (n_1, \ldots, n_n) \in \mathbb{Z}^n\}$. Questo

è un gruppo di trasformazioni di $\mathbb{R}^n$. $x \sim_G y$ se e solo se $x - y \in \mathbb{Z}^n$. Il quoziente $\mathbb{R}^n/\mathbb{Z}^n$ si identifica con $(S^1)^n \subset (\mathbb{R}^2)^n$ mediante l'applicazione

$$f = (f_1, \dots, f_n) : \mathbb{R}^n \to (\mathbb{R}^2)^n;\ f(x_1, \dots, x_n) = (\cos(2\pi x_1), \sin(2\pi x_1), \dots, \cos(2\pi x_n), \sin(2\pi x_n))$$

tale che $x \sim_G y$ se e solo se $f(x) = f(y)$. Il gruppo quoziente $(\mathbb{R}^n/\mathbb{Z}^n, +)$ si identifica con il gruppo prodotto $(SO(2))^n$.

(3) Consideriamo $G = SO(2)$ come gruppo di trasformazioni di $\mathbb{R}^2$. Consideriamo l'applicazione

$$f : \mathbb{R}^2 \to \mathbb{R},\ f(x) = x_1^2 + x_2^2$$

allora $x \sim_G y$ se e solo se $f(x) = f(y)$. L'immagine di f è $\mathbb{R}^+ = \{a \in \mathbb{R};\ a \geq 0\}$. Per ogni $a \neq 0$, la classe di equivalenza $f^{-1}(a)$ è la circonferenza in $\mathbb{R}^2$ di centro l'origine e raggio uguale a $\sqrt{a}$; $[0] = \{0\}$.

(4) $X = \mathbb{R}^n$. Consideriamo il gruppo commutativo moltiplicativo $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$. Per ogni $\lambda \in \mathbb{R}^*$, $m_\lambda : \mathbb{R}^n \to \mathbb{R}^n$, $m_\lambda(x) := \lambda x$ è una trasformazione di $\mathbb{R}^n$. La corrispondenza $\lambda \to m_\lambda$ permette di considerare $\mathbb{R}^*$ come un gruppo di trasformazioni G di $\mathbb{R}^n$. $[0] = \{0\}$, mentre per ogni $x \neq 0$, $[x] \subset \mathbb{R}^n$ è la retta di $\mathbb{R}^n$ passante per x e per l'origine, privata dell' origine. Restringendo la relazione di equivalenza, il quoziente $\mathbb{R}^n \setminus \{0\}/G$ è in corrispondenza biunivoca con l'insieme delle rette per l'origine di $\mathbb{R}^n$.

(5) Sappiamo che $(\mathbb{Z}, +, .)$ è un anello commutativo ma non è un campo perchè ± 1 sono gli unici numeri interi non nulli che ammettono inverso rispetto al prodotto. Sappiamo inoltre che su $\mathbb{Z}$ possiamo fare la divisione euclidea ("con il resto"): per ogni intero $m > 0$, per ogni intero a, esistono unici interi q e r tali che

$$a = mq + r,\ 0 \leq r < m$$

r è detto il "resto della divisione di a per m". Fissiamo $m \geq 2$ e definiamo l'applicazione

$$r = r_m : \mathbb{Z} \to \mathbb{Z}$$

che associa ad ogni a il suo resto $r(a)$ della divisione per m. Si verifica facilmente che $r(a) = r(b)$ se e solo se $a - b \in m\mathbb{Z}$ cioè è un multiplo di m. Indichiamo con $\mathbb{Z}/m\mathbb{Z}$ il quoziente per la relazione indotta dall'applicazione r. L'immagime consiste di tutti i resti possibili, cioè è l'insieme $\{0, 1, \dots, m-1\}$. Per ogni $0 \leq s < m$, la corrispondente classe di equivalenza è $[s]$. Le operazioni passano al quoziente e si ottiene così un anello quoziente $(\mathbb{Z}/m\mathbb{Z}, +, .)$. Se $m = ab$ non è primo allora $0 = [m] = [a][b]$, quindi nonostante $[a]$ e $[b]$ siano non nulli non possono essere invertibili. Condizione necessaria affinché $(\mathbb{Z}/m\mathbb{Z}, +, .)$ sia un campo è che m sia primo. In effetti tale condizione è anche sufficiente. Questo sarà sicuramente visto in altri corsi. Per completezza ricordiamo che il $\mathrm{MCD}(a, m)$ può essere caratterizzato come il più piccolo intero positivo d tale che esistano interi p, q tali che

$$d = pm + qa\ .$$

Se m è primo e a non è un multiplo di m allora, per qualche p e q

$$1 = pm + qa$$

e quindi $[q][a] = 1$, $[q] = [a]^{-1}$. In questo modo possiamo allora costruire un'infinità di campi finiti della forma $\mathbb{Z}/m\mathbb{Z}$ con m primo.

(6) Se $\mathbf{K}$ è un campo, possiamo considerare $\mathbf{K}[X]$ l'anello dei polinomi in una indeterminata X a coefficienti in $\mathbf{K}$. Anche questo anello ha una divisione con il resto: per ogni polinomio $m(X) \neq 0$, per ogni polinomio $a(X)$, esistono unici polinomi $q(X)$ e $r(X)$ tali che

$$a(X) = m(X)q(X) + r(X),\ 0 \leq \mathrm{grado}(r(X)) < \mathrm{grado}(m(X))\ .$$

Possiamo ricalcare quanto fatto nell'esempio precedente. Fissiamo $m(X) \neq 0$. Consideriamo l'applicazione "resto per la divisione per $m(X)$":

$$r : \mathbf{K}[X] \to \mathbf{K}[X]\ .$$

$r(a(X)) = r(b(X))$ se e solo se $a(X) - b(X)$ è un multiplo di $m(X)$ in $\mathbf{K}[X]$. L'immagine di r è formata da tutti i resti possibili, cioè tutti i polinomi di grado minore del grado di $m(X)$; ogni tale polinomio rappresenta in modo biunivoco la sua classe di equivalenza. In particolare il campo $\mathbf{K}$ identificato con i polinomi di grado minore di 1 è un sottoanello dell'anello quoziente $(\mathbf{K}[X]/m(X), +, .)$. Questo è un

campo se e solo se $m(X)$ è irriducibile in $\mathbf{K}[X]$. Si noti che $\alpha = [X]$ è una radice del polinomio $m(X)$ considerato a coefficienti in $\mathbf{K}[X]/m(X)$.

Applicando tale costruzione a $\mathbb{R}[X]/(X^2+1)$ otteniamo una struttura di campo sull'insieme dei polinomi di grado minore o uguale a 1 a coefficienti reali, noto come il *campo dei numeri complessi* $\mathbb{C}$. Posto $[X] = i$, $i^2 = -1$, ogni tale polinomio è della forma $a + bi$ e le operazioni si esplicitano come

$$(a+ib) + (c+id) = (a+c) + (b+d)i,\ (a+ib).(c+id) = (ac-bd) + (bc+ad)i\ .$$

$\mathbb{R}$ è incluso in $\mathbb{C}$ identificando $a \in \mathbb{R}$ con $a + 0i$. Posto $\overline{a+bi} := a + (-b)i$, si ha che $z = a + bi \neq 0$ se e solo se $z\bar{z} = a^2 + b^2 \neq 0$, e $z^{-1} = \bar{z}/z\bar{z}$.

(7) **Costruzione di $(\mathbb{Z}, +)$ a partire da $(\mathbb{N}, +)$.** Supponiamo di conoscere $(\mathbb{N}, +)$. L'operazione è definita mediante il buon ordinamento di $\mathbb{N}$, a partire dalla definizione di $n+1$ come il minimo numero naturale maggiore di n. Le proprietà supposte note di $+$ sono che è associativa, commutativa, 0 è l'elemento neutro. $(\mathbb{N}, +)$ non è un gruppo perché ogni $n \in \mathbb{N} \setminus \{0\}$ non ha l' inverso rispetto alla somma. Inoltre $(\mathbb{N}, +)$ verifica la proprietà di *cancellazione*: se $n + p = m + p$ allora $m = n$. Si noti che questa è una proprietà intrinseca di $(\mathbb{N}, +)$, *non* si ottiene sommando $-p$ ad entrambi i membri dell' uguaglianza perchè $-p$ non c'è in $\mathbb{N}$ e, appunto, vogliamo costruire $\mathbb{Z}$ a partire dalla sola conoscenza di $\mathbb{N}$. Mettiamo sul prodotto $\mathbb{N} \times \mathbb{N}$ la relazione: " $(a, b) \sim (x, y)$ se $a + y = b + x$". E' una relazione di equivalenza; l'unica proprietà un poco piu' riposta è quella transitiva; la verifica usa la proprietà di cancellazione. Indichiamo con $[a, b]$ la classe di equivalenza di (a, b); denotiamo l' insieme quoziente come $\mathbb{Z}$. L'applicazione $j : \mathbb{N} \to \mathbb{Z},\ n \to [n, 0]$ è iniettiva e la usiamo per considerare $\mathbb{N}$ come un sottoinsieme dell'insieme quoziente $\mathbb{Z}$; con leggero abuso di notazione scriveremo n invece di $[n, 0]$. Vogliamo estendere ora anche la somma su tutto $\mathbb{Z}$. Poniamo allora $[a, b] + [x, y] = [a + x, b + y]$. E' ben definita (la verifica usa ancora, tra l'altro, la proprietà di cancellazione). Chiaramente $(\mathbb{Z}, +)$ estende $(\mathbb{N}, +)$. Inoltre $(\mathbb{Z}, +)$ è un gruppo commutativo. Infatti per ogni $\alpha = [a, b]$, $-\alpha = [b, a]$. In particolare $-n = [0, n]$ e ogni $[a, b] = a + (-b) = a - b$, a meno di un ulteriore leggero abuso di notazione. Inoltre ogni $\alpha \in \mathbb{Z}$ si può scrivere in modo unico nella forma $\alpha = n$ oppure $\alpha = -n$ per qualche $n \in \mathbb{N}$. Per estendere anche la moltiplicazione, ricaviamo formalmente

$$(a-b)(x-y) = (ax+by) - (bx+ay)$$

si verifica poi che questa formula ben definisce la moltiplicazione così che $(\mathbb{Z}, +, .)$ estende $(\mathbb{N}, +, .)$.

(8) **Costruzione del campo $\mathbb{Q}$ a partire dall'anello $\mathbb{Z}$.** Procediamo in modo analogo al punto precedente. Sia $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$. Sul prodotto $\mathbb{Z} \times \mathbb{Z}^*$ mettiamo la relazione " $(a, b) \sim (x, y)$ se $ay = bx$ " . E' una relazione di equivalenza; indichiamo $\dfrac{a}{b}$ la classe di equivalenza di (a, b); $\mathbb{Q}$ denota l'insieme quoziente. $\mathbb{Z}$ si inietta in $\mathbb{Q}$ mediante l'applicazione $m \to \dfrac{m}{1}$. Estendiamo le operazioni nel modo seguente

$$\frac{a}{b} + \frac{p}{q} = \frac{aq+bp}{bq},\ \frac{a}{b}\frac{p}{q} = \frac{ap}{bq}\ .$$

Sono ben definite ed estendono $(\mathbb{Z}, +, .)$. $(\mathbb{Q}, +, .)$ è un campo; $\alpha = \dfrac{a}{b} \neq 0$ se e solo se $a \neq 0$; allora $\alpha^{-1} = \dfrac{b}{a}$. Ogni classe di equivalenza $\alpha \in \mathbb{Q}$ si rappresenta in modo unico nella forma $\dfrac{p}{q}$ dove $p \in \mathbb{Z}$, $q \in \mathbb{N} \setminus \{0\}$, $\mathrm{MCD}(p, q) = 1$.

(9) **Campi di funzioni razionali.** Sia $\mathbf{K}[X]$ come sopra l'anello dei polinomi a coefficienti nel campo $\mathbf{K}$. Possiamo formalmente ricalcare la costruzione fatta sopra (da $\mathbb{Z}$ a $\mathbb{Q}$) a partire da $\mathbf{K}[X]$. Si ottiene allora un campo che estende l'anello dei polinomi, si indica con il simbolo $\mathbf{K}(X)$ ed è chiamato il *campo delle funzioni razionali a coefficienti in* $\mathbf{K}$. Ogni elemento di $\mathbf{K}(X)$ è una classe di equivalenza $\dfrac{p(X)}{q(X)}$ dove $p(X)$ e $q(X)$ appartengono a $\mathbf{K}[X]$ e $q(X)$ è non nullo.