

Capitolo 3

Valutazioni

Sia $(\Gamma, +)$ un gruppo abeliano, denotiamo con 0 il suo elemento neutro.

Definizione 3.1. Si dice che un gruppo Γ è un *gruppo ordinato* se è dato un sottoinsieme $P \subseteq \Gamma$, chiuso additivamente, tale che:

$$\Gamma = P \sqcup \{0\} \sqcup -P \quad \text{dove } -P := \{-x \mid x \in P\}$$

In tal caso, infatti, si vede facilmente che una relazione d'ordine è definita canonicamente in Γ :

$$\alpha > \beta :\iff \alpha - \beta \in P$$

In particolare: $\alpha > 0 \iff \alpha \in P$. Per tale ragione, P è chiamato *insieme degli elementi positivi del gruppo ordinato* Γ .

Osservazione 3.2. Sia (Δ, \cdot) un gruppo abeliano con notazione moltiplicativa e sia $1 \in \Delta$ il suo elemento neutro. Allora, Δ è un gruppo ordinato se esiste $P \subseteq \Delta$, chiuso moltiplicativamente, in modo tale che:

$$\Delta = P \sqcup \{1\} \sqcup P^{-1} \quad \text{dove } P^{-1} := \{x^{-1} \mid x \in P\}.$$

La relazione d'ordine in Δ viene così definita:

$$\alpha < \beta :\iff \alpha\beta^{-1} \in P \iff \alpha^{-1}\beta \in P^{-1}.$$

Esempi 3.3. 1. $(\mathbb{Z}, +)$ è un gruppo ordinato prendendo $P = \{x \in \mathbb{Z} \mid x \geq 1\}$.

Più generalmente se $(\Gamma, +)$ è un sottogruppo di $(\mathbb{R}, +)$, con $\mathbb{Z} \subseteq \Gamma \subseteq \mathbb{R}$, allora Γ è un gruppo ordinato con $P = \{\alpha \in \Gamma \mid \alpha > 0\}$.

2. $(\mathbb{R}^>, \cdot)$ con $\mathbb{R}^> := \{x \in \mathbb{R} \mid x > 0\}$ è un gruppo ordinato, prendendo: $P = \{x \in \mathbb{R} \mid 0 < x < 1\}$.

3. $(\mathbb{Z} \times \mathbb{Z}, +)$ è un gruppo ordinato prendendo

$$P = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x \geq 1 \text{ oppure } x = 0 \text{ e } y \geq 1\}.$$

$\mathbb{Z} \times \mathbb{Z}$ con tale ordinamento si dice *ordinato lessicograficamente*.

È facile estendere a $(\mathbb{Z}^n = \mathbb{Z} \times \cdots \times \mathbb{Z} \text{ (} n \text{ volte)}, +)$ l'ordine lessicografico.

Proposizione 3.4. Sia $(\Gamma, +)$ un gruppo ordinato. Valgono le seguenti proprietà:

(a) (*Proprietà di tricotomia o di ordine totale*): presi comunque $\alpha, \beta \in \Gamma$ allora vale una ed una soltanto delle seguenti tre relazioni:

$$\alpha > \beta, \quad \alpha = \beta, \quad \alpha < \beta.$$

(b) (*Compatibilità con +*): presi comunque $\alpha, \beta, \gamma \in \Gamma$ allora:

$$\alpha < \beta \implies \alpha + \gamma < \beta + \gamma.$$

(c) (*Proprietà transitiva*): presi comunque $\alpha, \beta, \gamma \in \Gamma$ allora:

$$\alpha < \beta \quad e \quad \beta < \gamma \implies \alpha < \gamma.$$

Viceversa, dato un gruppo $(\Gamma, +)$ con una relazione binaria “ $<$ ” soddisfacente alle proprietà (a), (b) e (c) allora Γ è ordinato ed ha come insieme degli elementi positivi

$$P = \{\alpha \in \Gamma \mid \alpha > 0\}.$$

Dimostrazione. Le semplici verifiche sono lasciate come esercizio. \square

Proposizione 3.5. Sia $(\Gamma, +)$ un gruppo ordinato. Preso comunque $\alpha \in \Gamma$ ed $n \in \mathbb{Z}$, $n \neq 0$, allora:

$$n\alpha = 0 \implies \alpha = 0$$

In altre parole, l'omomorfismo di gruppi:

$$\begin{array}{ccc} \Gamma & \longrightarrow & \Gamma \\ \alpha & \longmapsto & n\alpha \end{array}$$

è iniettivo, per ogni $n \neq 0$.

Dimostrazione. Non è restrittivo limitarci al caso $n > 0$, essendo $(-n)\alpha = -(n\alpha)$. La conclusione è immediata conseguenza del fatto che P è chiuso additivamente. \square

Definizione 3.6. Sia $(\Gamma, +)$ un gruppo ordinato. Sia ∞ un nuovo elemento, $\infty \notin \Gamma$, che chiameremo *infinito*. Nell'insieme:

$$\Gamma_\infty := \Gamma \cup \{\infty\}$$

poniamo per definizione:

- $\alpha < \infty, \quad \forall \alpha \in \Gamma,$
- $\alpha + \infty = \infty + \alpha = \infty, \quad \forall \alpha \in \Gamma_\infty.$

Γ_∞ è chiamato *ampliamento del gruppo ordinato* $(\Gamma, +)$ con l'aggiunta di “ ∞ ”.

Osservazione 3.7. Nel caso di un gruppo ordinato con notazione moltiplicativa (Δ, \cdot) , l'analogo di Γ_∞ è $\Delta_0 := \Delta \cup \{0\}$, dove con “0” viene denotato un elemento non in Δ tale che (per definizione):

- $0 < \alpha, \quad \forall \alpha \in \Delta,$
- $\alpha \cdot 0 = 0 \cdot \alpha = 0, \quad \forall \alpha \in \Delta_0.$

Definizione 3.8. Sia K un campo. Una *valutazione di K con gruppo di valori* $(\Gamma, +)$, (risp. (Δ, \cdot)), gruppo ordinato, o semplicemente *una valutazione di K su Γ* (risp. Δ) è un'applicazione suriettiva:

$$v : K \twoheadrightarrow \Gamma_\infty \quad (\text{risp. } v : K \twoheadrightarrow \Delta_0)$$

soddisfacente alle seguenti proprietà, presi comunque $x, y \in K$:

- (a) $v(x) = \infty \iff x = 0$ (risp. $v(x) = 0 \iff x = 0$);
- (b) $v(xy) = v(x) + v(y)$ (risp. $v(xy) = v(x) \cdot v(y)$);
- (c) $v(x + y) \geq \min(v(x), v(y))$ (risp. $v(x + y) \leq \max(v(x), v(y))$).

Osservazioni 3.9. 1. Se $K^* := \{x \in K \mid x \neq 0\}$ è il gruppo moltiplicativo degli elementi invertibili di un campo K . Allora una valutazione v di K su Γ (risp. Δ) subordina un omomorfismo (suriettivo) di gruppi:

$$v|_{K^*} : K^* \twoheadrightarrow \Gamma \quad (\text{risp. } v|_{K^*} : K^* \twoheadrightarrow \Delta).$$

- 2. La condizione imposta a v di essere suriettiva non è essenziale. Infatti, se v non lo fosse, ci si potrebbe ricondurre a tale caso prendendo, al posto di Γ (o Δ), il gruppo $v(K^*)$ (che è ancora un gruppo ordinato).
- 3. Una valutazione si dice *impropria* (o *banale*) se il suo gruppo di valori $v(K^*)$ è il gruppo banale (consistente cioè del solo elemento neutro).
- 4. Se F è un sottocampo di un campo K e se v è una valutazione di K , allora v si dice una *valutazione di K banale su F* se $v(F^*)$ è il gruppo banale (essendo al solito $F^* := F \setminus \{0\}$).

Esempi 3.10. 1. Sia $K := k(X)$ il campo delle funzioni razionali in una indeterminata, X , a coefficienti in un campo assegnato k . Si dice che una funzione $z \in k(X)$ è definita in un punto $a \in k$ se è possibile scrivere:

$$z = \frac{f}{g} \quad \text{con } f, g \in k[X], g(a) \neq 0 \text{ (dunque, ovviamente } g \neq 0).$$

L'elemento $z(a) = \frac{f(a)}{g(a)} \in k$ è detto valore della funzione razionale z definita in a . In altri termini, in tal caso z determina una funzione $z : k \rightarrow k$ definita da $a \mapsto z(a)$, per ogni $a \in k$.

Se $z \neq 0$, $z \in K$, è definita in a , allora l'intero:

$$\text{ord}_a(z) := \text{ord}_a(f)$$

si chiama ordine della funzione razionale z (calcolata) in a . [Ricordiamo che dato un polinomio non nullo $f \in k[X]$ si definisce *ordine di f in a* , (in breve $\text{ord}_a(f)$) il più grande intero $n \geq 0$ tale che $(X - a)^n \mid f$, ma $(X - a)^{n+1} \nmid f$; in altre parole, $n = \text{ord}_a(f)$ è la molteplicità di a come zero del polinomio f (ovviamente $\text{ord}_a(f) = 0$ se e soltanto se a non è uno zero di f).]

Inoltre tale definizione è ben posta, infatti sia $z = \frac{f}{g} = \frac{f'}{g'}$, con $f, g, f', g' \in k[X]$ e con $g(a) \neq 0$ e $g'(a) \neq 0$, allora $fg' = f'g$ da cui:

$$\begin{aligned}\text{ord}_a(f) &= \text{ord}_a(f) + \text{ord}_a(g') = \text{ord}_a(fg') = \\ \text{ord}_a(f'g) &= \text{ord}_a(f') + \text{ord}_a(g) = \text{ord}_a(f').\end{aligned}$$

Se $z = 0$, $z \in K$, si pone per convenzione:

$$\text{ord}_a(0) := \infty, \quad \forall a \in k.$$

Se $z \neq 0$, $z \in K$, e z non è definita in a ciò significa che $z = \frac{f}{g}$ con $f, g \in k[X]$, $g \neq 0$ ed $\text{ord}_a(f) \leq \text{ord}_a(g)$ (in particolare, $g(a) = 0$). In tal caso, si pone $\text{ord}_a(z) = \text{ord}_a(f) - \text{ord}_a(g) (\in \mathbb{Z})$.

È subito visto che, fissato comunque $a \in k$, l'applicazione:

$$\begin{aligned}\text{ord}_a : k(X) &\longrightarrow \mathbb{Z}_\infty \\ z &\longmapsto \text{ord}_a(z)\end{aligned}$$

è una valutazione di $k(X)$ su \mathbb{Z} (che è banale su k).

2. Sia $K := k(X)$ come in 1. Denotiamo con:

$$\text{ord}_\infty : k(X) \longrightarrow \mathbb{Z}_\infty$$

l'applicazione definita come segue:

$$\text{ord}_\infty(z) := \begin{cases} \infty & \text{se } z = 0 \\ \deg(g) - \deg(f) & \text{se } z = \frac{f}{g} \neq 0, f, g \in k[X], g \neq 0 \end{cases}$$

Anche in questo caso si verifica facilmente che ord_∞ (è ben definita ed) è una valutazione di $k(X)$ su \mathbb{Z} (che è banale su k).

3. Sia k un campo e $K := k((X))$ il campo delle serie formali di Laurent in una indeterminata, X , a coefficienti su k ($k((X))$ è il campo dei quozienti dell'anello integro $k[[X]]$ delle serie formali). L'applicazione:

$$\begin{aligned}\text{ord} : k((X)) &\longrightarrow \mathbb{Z}_\infty \\ z &\longmapsto \text{ord}(z)\end{aligned}$$

è una valutazione di $k((X))$ su \mathbb{Z} (che è banale su k). [Ricordiamo che, se $0 \neq s \in k[[X]]$, l'ordine della serie formale, in breve $\text{ord}(s)$, è il più grande intero $n \geq 0$ tale che $X^n \mid s$ e $X^{n+1} \nmid s$. Se $z = \frac{s}{t} \in k((X))$ con $s, t \in k[[X]]$ e $s \neq 0, t \neq 0$, allora $\text{ord}(z) := \text{ord}(s) - \text{ord}(t)$.]

4. Sia p un primo fissato, $p \in \mathbb{Z}$. Preso comunque $z \in \mathbb{Q}$, $z \neq 0$ $z = \frac{p^r x'}{p^s y'} = p^{(r-s)} \frac{x'}{y'}$ con x' e y' interi non nulli e con $p \nmid x', p \nmid y'$, l'applicazione:

$$\begin{aligned}v_p : \mathbb{Q} &\longrightarrow \mathbb{Z}_\infty \\ z &\longmapsto \begin{cases} \infty & \text{se } z = 0 \\ r - s & \text{se } z = p^{(r-s)} \cdot \frac{x'}{y'} \neq 0 \end{cases}\end{aligned}$$

(che si verifica facilmente essere ben definita) è una valutazione detta *valutazione p-adica* su \mathbb{Q} .

5. Sia A un dominio a fattorizzazione unica e K il suo campo dei quozienti. Sia \mathcal{P} l'insieme degli elementi primi (o irriducibili) di A . Allora, ogni elemento $x \in A^* := A \setminus \{0\}$ si scrive in maniera unica:

$$(\bullet) \quad x = u \prod_{p \in \mathcal{P}} p^{v_p(x)}$$

dove u è un'unità di A , $v_p(x) \geq 0$, $v_p(x) \in \mathbb{Z}$ e $v_p(x)$ è quasi sempre nullo tranne al più per un numero finito di elementi $p \in \mathcal{P}$ (cioè quando $p \mid x$). Ovviamente se $x \in K^* = K \setminus \{0\}$ allora x si scrive formalmente come in (\bullet) , ma ora $v_p(x) \in \mathbb{Z}$.

L'applicazione:

$$v_p : K \longrightarrow \mathbb{Z}_\infty \\ x \longmapsto \begin{cases} \infty & \text{se } x = 0 \\ v_p(x) & \text{altrimenti} \end{cases}$$

definisce una valutazione di K su \mathbb{Z} (relativa all'elemento primo $p \in A$), detta *valutazione p -adica* sul campo K .

6. Sia $K := k(X, Y)$ il campo delle funzioni razionali in due indeterminate, X e Y , a coefficienti in un campo k (cioè, K è il campo dei quozienti dell'anello di polinomi $k[X, Y]$).

Dunque, preso comunque $f \in k[X, Y]$, $f \neq 0$, allora si può scrivere:

$$f = \sum_{i=0}^N a_i(Y)X^i = \sum_{j=0}^M b_j(X)Y^j$$

con $a_i(Y) \in k[Y]$, $0 \leq i \leq N$, $b_j(X) \in k[X]$, $0 \leq j \leq M$ (pensando $f \in (k[Y])[X]$ oppure $f \in (k[X])[Y]$).

Chiameremo *ordine di f relativamente ad X* (risp. Y) l'intero $n \leq N$ (risp. $m \leq M$) tale che:

$$a_n(Y) \neq 0 \quad \text{e} \quad a_i(Y) = 0, \quad 0 \leq i \leq n-1 \\ (\text{risp. } b_m(X) \neq 0 \quad \text{e} \quad b_j(X) = 0, \quad 0 \leq j \leq m-1).$$

In breve, scriveremo $\text{ord}^X(f) := n$ (risp. $\text{ord}^Y(f) := m$).

Se, poi, $z \in K$, $z \neq 0$, allora $z = \frac{f}{g}$ con $f, g \in k[X, Y]$, $f \neq 0$ e $g \neq 0$. Poniamo:

$$\text{ord}^X(z) := \text{ord}^X(f) - \text{ord}^X(g) \\ (\text{risp. } \text{ord}^Y(z) := \text{ord}^Y(f) - \text{ord}^Y(g)).$$

L'applicazione:

$$\text{ord} : k(X, Y) \longrightarrow (\mathbb{Z} \times \mathbb{Z})_\infty \\ z \longmapsto \begin{cases} \infty & \text{se } z = 0 \\ (\text{ord}^X(z), \text{ord}^Y(z)) & \text{se } z \neq 0 \end{cases}$$

è una valutazione di $k(X, Y)$ su $\mathbb{Z} \times \mathbb{Z}$ (ordinato lessicograficamente).

Si noti (in relazione all'Esempio 5) che $A := k[X, Y]$ è un dominio a fattorizzazione unica (conseguenza del Lemma di Gauss) e che X ed Y sono elementi primi di A . Ebbene, in questa situazione, ord^X (risp. ord^Y) coincide con la valutazione X -adica (risp. Y -adica) v_X (risp. v_Y) di $k(X, Y)$ su \mathbb{Z} .

La semplice estensione di quanto sopra al caso del campo di funzioni razionali

$$K := k(X_1, X_2, \dots, X_n), \quad \text{con } n \geq 2,$$

è lasciata come esercizio.

7. Se K' è un sottocampo di un campo K e v è una valutazione di K , allora $v|_{K'}$ è una valutazione di K' (con gruppo dei valori opportunamente ristretto).

8. Se K è un campo finito, allora ogni valutazione di K è banale (perché ogni elemento di K^* è una radice dell'unità); v. anche la successiva Proposizione 3.12 (a, c).

9. L'applicazione:

$$\begin{aligned} \mathbb{R} &\longrightarrow (\mathbb{R}^>)_0 \\ x &\longmapsto |x| \end{aligned}$$

non è una valutazione (ad es. $|x + y| \not\leq \max(|x|, |y|)$, pur essendo $|x + y| \leq |x| + |y|$).

10. L'applicazione:

$$\begin{aligned} \mathbb{C} &\longrightarrow (\mathbb{R}^>)_0 \\ x + iy &\longmapsto \|z\| := \sqrt{x^2 + y^2} \end{aligned}$$

non è una valutazione (ad es. $\|z_1 + z_2\| \not\leq \max(\|z_1\|, \|z_2\|)$, pur essendo $\|z_1 + z_2\| \leq \|z_1\| + \|z_2\|$).

11. In questo esempio costruiamo una valutazione in cui il gruppo dei valori è assegnato a priori.

Sia $(\Gamma, +)$ un gruppo ordinato e P il suo sottomonoido degli elementi positivi. Preso comunque un campo F , sia A la F -algebra generata da P , cioè:

$$A = F[X_\alpha \mid \alpha \in P],$$

dove si pone:

$$X_\alpha X_\beta := X_{\alpha+\beta}$$

(il prodotto si estende poi in maniera ovvia su tutto A).

Preso comunque $f \in A$, $f \neq 0$, allora:

$$f := \sum_{\alpha \in P \cup \{0\}} a_\alpha X_\alpha$$

dove si pone $X_0 := 1$ e dove soltanto per un insieme finito di $\alpha \in P \cup \{0\}$ i coefficienti a_α sono non nulli.

Poniamo, per definizione,

$$\begin{aligned} v(f) &:= \inf \{ \alpha \in P \cup \{0\} \mid a_\alpha \neq 0 \}, \\ v(0) &:= \infty. \end{aligned}$$

È facile estendere v ad un'applicazione definita sul campo dei quozienti di A , che denotiamo con K :

$$v : K \rightarrow \Gamma_\infty$$

$$z \mapsto \begin{cases} \infty, & \text{se } z = 0 \\ v(f) - v(g), & \text{se } z = \frac{f}{g} \neq 0. \end{cases}$$

È facile verificare che v è una valutazione di K con gruppo di valori Γ . Per maggiori dettagli su valutazioni costruite a partire da gruppi ordinati cfr. [G-72, Ch. III, Par.18, pag. 207 e segg.].

12. L'applicazione:

$$\begin{aligned} \mathbb{C}[X, Y] &\longrightarrow \mathbb{C}[[T]] \\ f(X, Y) &\longmapsto f(T, e^T) \end{aligned}$$

è iniettiva (cfr. [B-51, Ch. IV, Par. 2, Proposizione 9]) dunque si prolunga in un omomorfismo (iniettivo) di campi:

$$\mathbb{C}(X, Y) \hookrightarrow \mathbb{C}((T)).$$

La restrizione della valutazione ord : $\mathbb{C}((T)) \rightarrow \mathbb{Z}_\infty$ al campo $\mathbb{C}(X, Y)$ è una valutazione di $\mathbb{C}(X, Y)$ banale su \mathbb{C} , con gruppo di valori \mathbb{Z} .

Definizione 3.11. Date due valutazioni di uno stesso campo:

$$v : K \longrightarrow \Gamma_\infty, \quad v' : K \longrightarrow \Gamma'_\infty$$

diremo che v è *equivalente* a v' , in breve $v \sim v'$, se esiste un isomorfismo di gruppi ordinati:

$$\sigma : \Gamma \longrightarrow \Gamma' \quad (\text{quindi con } x < y \iff \sigma(x) < \sigma(y))$$

in modo tale che $\sigma \circ v(x) = v'(x)$, $\forall x \in K^*$.

È facile assicurarsi che “ \sim ” è effettivamente una relazione d'equivalenza nell'insieme delle valutazioni definite sul campo K .

Proposizione 3.12. Sia $v : K \longrightarrow \Gamma_\infty$ una valutazione. Allora, valgono le seguenti proprietà:

- (a) $v(1) = 0$ (dunque $v(x^{-1}) = -v(x)$, $\forall x \in K^* = K \setminus \{0\}$);
- (b) $v(x) = v(-x)$, $\forall x \in K$;
- (c) $v(x^n) = nv(x)$, $\forall x \in K \setminus \{0\}$, $\forall n \in \mathbb{Z}$;
- (d) $v(x) > v(y) \implies v(x + y) = v(y)$, $\forall x, y \in K$;
- (e) se $v(x_1 + \dots + x_n) = \infty$ (cioè, se $x_1 + \dots + x_n = 0$), con $n \geq 2$ e $x_i \neq 0$, $1 \leq i \leq n$, allora devono esistere (almeno) due indici $1 \leq i \neq j \leq n$ in modo tale che:

$$v(x_i) = v(x_j) = \min \{v(x_k) \mid 1 \leq k \leq n\};$$

- (f) Presi comunque $x_1, \dots, x_n \in K$, $n \geq 2$, con $x_i \neq 0$, $1 \leq i \leq n$, se esiste un indice i_0 , $1 \leq i_0 \leq n$ in modo tale che:

$$v(x_{i_0}) \leq v(x_k) \quad \forall k \neq i_0, 1 \leq k \leq n$$

allora necessariamente:

$$x_1 + \dots + x_n \neq 0.$$

Dimostrazione.

- (a) $v(1) = v(1 \cdot 1) = v(1) + v(1) \implies v(1) = 0$.
- (b) $v(-1) = v((-1)(-1)(-1)) = v(-1) + v(-1) + v(-1) \implies v(-1) = 0$. Quindi
 $v(-x) = v((-1) \cdot x) = v(-1) + v(x) = v(x)$.
- (c) Per induzione su $n \geq 0$, (per $n < 0$ cfr. (a)), visto che $v(x^2) = 2v(x)$.
- (d) $v(y+x) = v(x+y) \geq v(y) = v(y+x-x) \geq \min(v(y+x), v(-x)) = v(y+x)$
(perché altrimenti risulterebbe:
 $\min(v(y+x), v(-x)) = v(-x) = v(x) \implies v(y) \geq v(x)$.)
- (e) Se esistesse i_0 , $1 \leq i_0 \leq n$, in modo tale che:

$$v(x_{i_0}) = \min \{v(x_k) \mid 1 \leq k \leq n\}, \text{ e}$$

$$v(x_k) > v(x_{i_0}) \text{ con } k \neq i_0, 1 \leq k \leq n$$

allora:

$$\infty = v(x_1 + \dots + x_n) = v(x_{i_0})$$

per il punto (d). Dunque $x_{i_0} = 0$ (ed, inoltre, $v(x_k) = \infty$ ovvero $x_k = 0$ per ogni k).

- (f) È equivalente ad (e). □