Esempi notevoli di anelli euclidei

§1.1 I numeri interi: $\mathbb{Z}$

Senza ombra di dubbio l'esempio più importante di anello euclideo – nonché l'esempio da cui si è generalizzata proprio la stessa nozione di anello euclideo – è l'anello dei numeri interi.

In questo dominio la funzione grado è canonicamente il valore assoluto:

$$g : \mathbb{Z} \setminus \{0\} \to \mathbb{N},\ k \mapsto |k|\,.$$

Infatti, chiaramente $|a| \leq |ab|\ \forall\, a,\ b \in \mathbb{Z} \setminus \{0\}$. Inoltre esistono – e sono anche unici, a meno di segno – $q,\ r \in \mathbb{Z} \mid a = bq + r$, con $r = 0 \vee |r| < |q|$.

Dal momento che così si verifica che $\mathbb{Z}$ è un anello euclideo, il *Teorema fondamentale dell'aritmetica* è un corollario del teorema per cui ogni anello euclideo è un UFD.

§1.2 I campi: $\mathbb{K}$

Ogni campo $\mathbb{K}$ è un anello euclideo, seppur banalmente. Infatti, eccetto proprio per 0, ogni elemento è "divisibile" per ogni altro elemento: siano $a,\ b \in \mathbb{K}$, allora $a = ab^{-1}b$.

Si definisce quindi la funzione grado come la funzione nulla:

$$g : \mathbb{K}^* \to \mathbb{N},\ a \mapsto 0.$$

Chiaramente g soddisfa il primo assioma della funzione grado. Inoltre, poiché ogni elemento è "divisibile", il resto è sempre zero – non è pertanto necessario verificare nessun'altra proprietà.

§1.3 I polinomi di un campo: $\mathbb{K}[x]$

I polinomi di un campo $\mathbb{K}$ formano un anello euclideo rilevante nello studio dell'algebra astratta. Come suggerisce la terminologia, la funzione grado in questo dominio coincide proprio con il grado del polinomio, ossia si definisce come:

$$g : \mathbb{K}[x] \setminus \{0\} \to \mathbb{N},\ f(x) \mapsto \deg f.$$

Si verifica facilmente che $g(a(x)) \leq g(a(x)b(x))\ \forall\, a(x),\ b(x) \in \mathbb{K}[x] \setminus \{0\}$, mentre la divisione euclidea – come negli interi – ci permette di concludere che effettivamente $\mathbb{K}[x]$ soddisfa tutti gli assiomi di un anello euclideo[1].

Esempio 1.3.1

Sia $\alpha \in \mathbb{K}$ e sia $\varphi_\alpha : \mathbb{K}[x] \to \mathbb{K}$, $f(x) \mapsto f(\alpha)$ la sua valutazione polinomiale in $\mathbb{K}[x]$. φ_α è un omomorfismo, il cui nucleo è rappresentato dai polinomi in $\mathbb{K}[x]$ che hanno α come radice. Poiché $\mathbb{K}[x]$ è un PID, $\operatorname{Ker}\varphi$ deve essere monogenerato. $x - \alpha \in \operatorname{Ker}\varphi$ è irriducibile, e quindi è il generatore dell'ideale. Si deduce così che $\operatorname{Ker}\varphi = (x - \alpha)$.

§1.4 Gli interi di Gauss: $\mathbb{Z}[i]$

Un importante esempio di anello euclideo è il dominio degli interi di Gauss $\mathbb{Z}[i]$, definito come:

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}.$$

La funzione grado coincide in particolare con il quadrato del modulo di un numero complesso, ossia:

$$g(z) : \mathbb{Z}[i] \setminus \{0\} \to \mathbb{N},\ a + bi \mapsto |a + bi|^2 .$$

Il vantaggio di quest'ultima definizione è l'enfasi sul collegamento tra la funzione grado di $\mathbb{Z}$ e quella di $\mathbb{Z}[i]$. Infatti, se $a \in \mathbb{Z}$, il grado di a in $\mathbb{Z}$ e in $\mathbb{Z}[i]$ sono uno il quadrato dell'altro. In particolare, è possibile ridefinire il grado di $\mathbb{Z}$ proprio in modo tale da farlo coincidere con quello di $\mathbb{Z}[i]$.

Teorema 1.4.1

$\mathbb{Z}[i]$ è un anello euclideo.

Dimostrazione. Si verifica la prima proprietà della funzione grado. Siano $a, b \in \mathbb{Z}[i] \setminus \{0\}$, allora $|a| \geq 1 \wedge |b| \geq 1$. Poiché $|ab| = |a|\,|b|$[2], si verifica facilmente che $|ab| \geq |a|$, ossia che $g(ab) \geq g(a)$.

Si verifica infine che esiste una divisione euclidea, ossia che $\forall\, a \in \mathbb{Z}[i]$, $\forall\, b \in \mathbb{Z}[i] \setminus \{0\}$, $\exists\, q,\ r \in \mathbb{Z}[i] \mid a = bq + r$ e $r = 0 \vee g(r) < g(b)$. Tutti i multipli di b formano un piano con basi b e ib, dove sicuramente esiste un certo q tale che la distanza $|r| = |a - bq|$ sia

[1] Curiosamente i polinomi di $\mathbb{K}[x]$ e i campi $\mathbb{K}$ sono gli unici anelli euclidei in cui resti e quozienti sono unici, includendo la scelta di segno (vd. [1]).

[2] Questa interessante proprietà del modulo è alla base dell'identità di Brahmagupta-Fibonacci: $(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$.

minima.

Se a è un multiplo di b, vale sicuramente che $a = bq$. Altrimenti dal momento che r è sicuramente inquadrato in uno dei tasselli del piano, vale sicuramente la seguente disuguaglianza, che lega il modulo di r alla diagonale di ogni quadrato:

$$|r| \leq \frac{|b|}{\sqrt{2}}.$$

Pertanto vale la seconda e ultima proprietà della funzione grado:

$$|r| \leq \frac{|b|}{\sqrt{2}} < |b| \implies |r|^2 < |b|^2 \implies g(r) < g(b).$$

□

§1.5 Gli interi di Eisenstein: $\mathbb{Z}[\omega]$

Sulla scia di $\mathbb{Z}[i]$ è possibile definire anche l'anello degli interi di Eisenstein, aggiungendo a $\mathbb{Z}$ la prima radice cubica primitiva dell'unità in senso antiorario, ossia:

$$\omega = e^{\frac{2\pi i}{3}} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i.$$

In particolare, ω è una delle due radici dell'equazione $z^2 + z + 1 = 0$, dove invece l'altra radice altro non è che $\omega^2 = \overline{\omega}$.

La funzione grado in $\mathbb{Z}[\omega]$ deriva da quella di $\mathbb{Z}[i]$ e coincide ancora con il quadrato del modulo del numero complesso. Si definisce quindi:

$$g : \mathbb{Z}[\omega] \setminus \{0\},\ a + b\omega \mapsto |a + b\omega|^2.$$

Sviluppando il modulo è possibile ottenere una formula più concreta:

$$|a + b\omega|^2 = \left| \left(a - \frac{b}{2}\right) + \frac{b\sqrt{3}}{2}i \right|^2 =$$

$$= \left(a - \frac{b}{2}\right)^2 + \frac{3b^2}{4} = a^2 - ab + b^2.$$

Teorema 1.5.1

$\mathbb{Z}[\omega]$ è un anello euclideo.

Dimostrazione. Sulla scia della dimostrazione presentata per $\mathbb{Z}[i]$, si verifica facilmente la prima proprietà della funzione grado. Siano a, $b \in \mathbb{Z}[\omega]$, allora $|a| \geq 1$ e $|b| \geq 1$. Poiché dalle proprietà dei numeri complessi vale ancora $|a|\,|b| \geq |a|$, la proprietà $g(ab) \geq g(a)$ è già verificata.

Si verifica infine la seconda e ultima proprietà della funzione grado. Come per $\mathbb{Z}[i]$, i multipli di $b \in \mathbb{Z}[\omega]$ sono visualizzati su un piano che ha per basi b e ωb, pertanto esiste sicuramente un q tale che la distanza $|a - bq|$ sia minima.

Se a è multiplo di b, allora chiaramente $a = bq$. Altrimenti, a è certamente inquadrato in uno dei triangoli del piano, per cui vale la seguente disuguaglianza:

$$|r| \leq \frac{\sqrt{3}}{2}\,|b|\,.$$

Dunque la tesi è verificata:

$$|r| \leq \frac{\sqrt{3}}{2}\,|b| < |b| \implies |r|^2 < |b|^2 \implies g(r) < g(b).$$

□

Riferimenti bibliografici

[1] M. A. Jodeit. ≪Uniqueness in the Division Algorithm≫. In: *The American Mathematical Monthly* 74.7 (1967), pp. 835–836. ISSN: 00029890, 19300972. URL: http://www.jstor.org/stable/2315810.