Anelli euclidei, PID e UFD

Gabriel Antonio Videtta

31 dicembre 2022

Indice

1 Anelli euclidei e prime proprietà

Nel corso della storia della matematica, numerosi studiosi hanno tentato di generalizzare – o meglio, accomunare a più strutture algebriche – il concetto di divisione euclidea che era stato formulato per l'anello dei numeri interi $\mathbb{Z}$ e, successivamente, per l'anello dei polinomi $\mathbb{K}[x]$. Lo sforzo di questi studiosi ad oggi è converso in un'unica definizione, quella di anello euclideo, di seguito presentata.

Definizione 1.1. Un **anello euclideo** è un dominio d'integrità D[1] sul quale è definita una funzione g detta **funzione grado** o *norma* soddisfacente le seguenti proprietà:

- $g : D \setminus \{0\} \to \mathbb{N}$,
- $\forall\, a,\, b \in D \setminus \{0\},\ g(a) \leq g(ab)$,
- $\forall\, a \in D,\, b \in D \setminus \{0\},\ \exists\, q,\, r \in D \mid a = bq + r$ e $r = 0 \vee g(r) < g(q)$.

[1] Difatti, nella letteratura inglese, si parla di *Euclidean domain* piuttosto che di anello.

Di seguito vengono presentate alcune definizioni, correlate alle proprietà immediate di un anello euclideo.

Definizione 1.2. Dato un anello euclideo E, siano $a \in E$ e $b \in E \setminus \{0\}$. Si dice che $b \mid a$, ossia che b *divide* a, se $\exists\, c \in E \mid a = bc$.

Osservazione. Si osserva che, per ogni anello euclideo E, qualsiasi $a \in E$ divide 0. Infatti, $0 = a0$.

Proposizione 1.1. Dato un anello euclideo E, $a \mid b \wedge b \nmid a \implies g(a) < g(b)$.

Dimostrazione. Poiché $b \nmid a$, esistono q, r tali che $a = bq + r$, con $g(r) < g(b)$. Dal momento però che $a \mid b$, $\exists\, c \mid b = ac$. Pertanto $a = ac + r \implies r = a(1-c)$. Dacché $1-c \neq 0$ – altrimenti $r = 0$, $\lightning$ –, così come $a \neq 0$, si deduce dalle proprietà della funzione grado che $g(a) \leq g(r)$. Combinando le due disuguaglianze, si ottiene la tesi: $g(a) < g(b)$. □

Proposizione 1.2. $g(1)$ è il minimo di $\operatorname{Imm} g$, ossia il minimo grado assumibile da un elemento di un anello euclideo E.

Dimostrazione. Sia $a \in E \setminus \{0\}$, allora, per le proprietà della funzione grado, $g(1) \leq g(1a) = g(a)$. □

Teorema 1.1. Sia $a \in E \setminus \{0\}$, allora $a \in E^* \iff g(a) = g(1)$.

Dimostrazione. Dividiamo la dimostrazione in due parti, ognuna corrispondente a una implicazione.

($\implies$) Sia $a \in E^*$, allora $\exists\, b \in E^*$ tale che $ab = 1$. Poiché sia a che b sono diversi da 0, dalle proprietà della funzione grado si desume che $g(a) \leq g(ab) = g(1)$. Poiché, dalla *Proposizione 1.2*, $g(1)$ è minimo, si conclude che $g(a) = g(1)$.

($\impliedby$) Sia $a \in E \setminus \{0\}$ con $g(a) = g(1)$. Allora esistono q, r tali che $1 = aq + r$. Vi sono due possibilità: che r sia 0, o che $g(r) < g(a)$. Tuttavia, poiché $g(a) = g(1)$, dalla *Proposizione 1.2* si desume che $g(a)$ è minimo, e quindi che r è nullo. Si conclude quindi che $aq = 1$, e dunque che $a \in E^*$. □

2 PID e UFD

2.1 Irriducibili e prime definizioni

Come accade nell'aritmetica dei numeri interi, anche in un dominio è possibile definire una nozione di *primo*. In un dominio possono essere tuttavia definiti due tipi di "primi", gli elementi *irriducibili* e gli elementi *primi*.

Definizione 2.1. In un dominio A, si dice che $a \in A \setminus A^*$ è **irriducibile** se $\exists\, b$, $c \mid a = bc \implies b \in A^*$ o $c \in A^*$.

Osservazione. Dalla definizione si escludono gli invertibili di A per permettere di definire meglio il concetto di fattorizzazione in seguito. Infatti, se li avessimo inclusi, avremmo che ogni dominio sarebbe a fattorizzazione non unica, dal momento che $a = bc$ potrebbe essere scritto anche come $a = 1bc$.

Definizione 2.2. In un dominio A, si dice che $a \in A \setminus A^*$ è **primo** se $a \mid bc \implies a \mid b \vee a \mid c$.

Proposizione 2.1. Se $a \in A$ è primo, allora a è anche irriducibile.

Dimostrazione. Si dimostra la tesi contronominalmente. Sia a non irriducibile. Se $a \in A^*$, allora a non può essere primo. Altrimenti $a = bc$ con $b, c \in A \setminus A^*$.

Chiaramente $a \mid bc$, ossia sé stesso. Senza perdità di generalità, se $a \mid b$, esiste $d \in A$ tale per cui $b = ad$. Pertanto, $a = adc \implies a(1 - dc) = 0$. Poiché A è un dominio, uno dei due fattori deve essere nullo. a non può esserlo, perché 0 non può dividere b. Tuttavia neanche $dc - 1$ può essere nullo, altrimenti si verificherebbe che $dc = 1$, e quindi che $c \in A^*$, ↯. □

Definizione 2.3. Si dice che due elementi non nulli a, b appartenenti a un anello euclideo E sono **associati** se $a \mid b$ e $b \mid a$.

Proposizione 2.2. a e b sono associati $\iff \exists\, c \in E^* \mid a = bc$ e a, b entrambi non nulli.

Dimostrazione. Si dimostrano le due implicazioni separatamente.

($\implies$) Se a e b sono associati, allora $\exists\, d$, e tali che $a = bd$ e che $b = ae$. Combinando le due relazioni si ottiene:

$$a = aed \implies a(1 - ed) = 0.$$

Poiché a è diverso da zero, si ricava che $ed = 1$, ossia che d, $e \in E^*$, e quindi la tesi.

($\impliedby$) Se a e b sono entrambi non nulli e $\exists\, c \in E^* \mid a = bc$, b chiaramente divide a. Inoltre, $a = bc \implies b = ac^{-1}$, e quindi anche a divide b. Pertanto a e b sono associati. □

Proposizione 2.3. Siano a e b due associati in E. Allora $a \mid c \implies b \mid c$.

Dimostrazione. Poiché a e b sono associati, per la *Proposizione 2.2*, $\exists\, d \in E^*$ tale che $a = db$. Dal momento che $a \mid c$, $\exists\, \alpha \in E$ tale che $c = \alpha a$, quindi:

$$c = \alpha a = \alpha db,$$

da cui la tesi. □

Proposizione 2.4. Siano a e b due associati in E. Allora $(a) = (b)$.

Dimostrazione. Poiché a e b sono associati, $\exists\, d \in E^*$ tale che $a = db$. Si dimostra l'uguaglianza dei due insiemi.

Sia $\alpha = ak \in (a)$, allora $\alpha = dbk$ appartiene anche a (b), quindi $(a) \subseteq (b)$. Sia invece $\beta = bk \in (b)$, allora $\beta = d^{-1}ak$ appartiene anche a (a), da cui $(b) \subseteq (a)$. Dalla doppia inclusione si verifica la tesi, $(a) = (b)$. □

2.2 PID e MCD

Come accade per $\mathbb{Z}$, in ogni anello euclideo è possibile definire il concetto di *massimo comun divisore*, sebbene con qualche accortezza in più. Pertanto, ancor prima di definirlo, si enuncia la definizione di PID e si dimostra un teorema fondamentale degli anelli euclidei, che si ripresenterà in seguito come ingrediente fondamentale per la fondazione del concetto di MCD.

Definizione 2.4. Si dice che un dominio è un *principal ideal domain* (**PID**)[2] se ogni suo ideale è monogenerato.

Teorema 2.1. Sia E un anello euclideo. Allora E è un PID.

Dimostrazione. Sia I un ideale di E. Se $I = (0)$, allora I è già monogenerato. Altrimenti si consideri l'insieme $g(I \setminus \{0\})$. Poiché $g(I \setminus \{0\}) \subseteq \mathbb{N}$, esso ammette un minimo per il principio del buon ordinamento.

Sia $m \in I$ un valore che assume tale minimo e sia $a \in I$. Poiché E è euclideo, $\exists\, q,\ r \mid a = mq + r$ con $r = 0$ o $g(r) < g(m)$. Tuttavia, poiché $r = a - mg \in I$ e $g(m)$ è minimo, necessariamente $r = 0$ – altrimenti r sarebbe ancor più minimo di m, ↯ –, quindi $m \mid a,\ \forall\, a \in I$. Quindi $I \subseteq (m)$.

Dal momento che per le proprietà degli ideali $\forall\, a \in E,\ ma \in I$, si conclude che $(m) \subseteq I$. Quindi $I = (m)$. □

Adesso è possibile definire il concetto di massimo comun divisore, basandoci sul fatto che ogni anello euclideo è un PID.

Definizione 2.5. Sia D un dominio e siano $a,\ b \in D$. Si definisce *massimo comun divisore* (**MCD**) di a e b un generatore dell'ideale (a, b).

Osservazione. Questa definizione di MCD è una buona definizione dal momento che sicuramente esiste un generatore dell'ideale (a, b), dacché D è un PID.

Osservazione. Non si parla di un unico massimo comun divisore, dal momento che potrebbero esservi più generatori dell'ideale (a, b). Segue tuttavia che tutti questi generatori sono in realtà associati[3]. Quando si scriverà $\mathrm{MCD}(a, b)$ s'intenderà quindi uno qualsiasi di questi associati.

Teorema 2.2 (*Identità di Bézout*)**.** Sia d un MCD di a e b. Allora $\exists\, \alpha,\ \beta$ tali che $d = \alpha a + \beta b$.

Dimostrazione. Il teorema segue dalla definizione di MCD come generatore dell'ideale (a, b). Infatti, poiché $d \in (a, b)$, esistono sicuramente, per definizione, α e β tali che $d = \alpha a + \beta b$. □

Proposizione 2.5. Siano $a,\ b \in D$. Allora vale la seguente equivalenza:

$$d = \mathrm{MCD}(a, b) \iff \begin{cases} d \mid a \wedge d \mid b \\ \forall\, c \text{ t.c. } c \mid a \wedge c \mid b,\ c \mid d \end{cases}$$

[2] Ossia un *dominio a soli ideali principali*, quindi monogenerati, proprio come da definizione.

[3] Infatti ogni generatore divide ogni altro elemento di un ideale, e così i vari generatori si dividono tra di loro. Pertanto sono associati.

Dimostrazione. Si dimostrano le due implicazioni separatamente.

($\implies$) Poiché d è generatore dell'ideale (a, b), la prima proprietà segue banalmente.

Inoltre, per l'*Identità di Bézout*, $\exists\, \alpha$, β tali che $d = \alpha a + \beta b$. Allora, se $c \mid a$ e $c \mid b$, sicuramente esistono γ e δ tali che $a = \gamma c$ e $b = \delta c$. Pertanto si verifica la seconda proprietà, e quindi la tesi:

$$d = \alpha a + \beta b = \alpha\gamma c + \beta\delta c = c(\alpha\gamma + \beta\delta).$$

($\impliedby$) Sia $m = \mathrm{MCD}(a, b)$. Dal momento che d divide sia a che b, d deve dividere, per l'implicazione scorsa, anche m. Per la seconda proprietà, m divide d a sua volta. Allora d è un associato di m, e quindi, dalla *Proposizione 2.4*, $(m) = (d) = (a, b)$, da cui $d = \mathrm{MCD}(a, b)$. □

Proposizione 2.6. Se $a \mid bc$ e $d = \mathrm{MCD}(a, b) \in D^*$, allora $a \mid c$.

Dimostrazione. Per l'*Identità di Bézout* $\exists\, \alpha$, β tali che $\alpha a + \beta b = d$. Allora, poiché $a \mid bc$, $\exists\, \gamma$ tale che $bc = a\gamma$. Si verifica quindi la tesi:

$$\alpha a + \beta b = d \implies \alpha ac + \beta bc = dc \implies ad^{-1}(\alpha c + \beta\gamma) = c.$$

□

Lemma 2.1. Se a è un irriducibile di un PID D, allora $\forall\, b \in D$, $(a, b) = D \vee (a, b) = (a)$, o equivalentemente $\mathrm{MCD}(a, b) \in D^*$ o $\mathrm{MCD}(a, b) = a$.

Dimostrazione. Dacché $\mathrm{MCD}(a, b) \mid a$, le uniche opzioni, dal momento che a è irriducibile, sono che $\mathrm{MCD}(a, b)$ sia un invertibile o che sia un associato di a stesso. □

Teorema 2.3. Se a è un irriducibile di un PID D, allora a è anche un primo.

Dimostrazione. Siano b e c tali che $a \mid bc$. Per il *Lemma 2.1*, $\mathrm{MCD}(a, b)$ può essere solo un associato di a o essere un invertibile. Se è un associato di a, allora, per la *Proposizione 2.3*, poiché $\mathrm{MCD}(a, b)$ divide b, anche a divide b. Altrimenti $\mathrm{MCD}(a, b) \in D^*$, e quindi, per la *Proposizione 2.6*, $a \mid c$. □

2.3 L'algoritmo di Euclide

Per algoritmo di Euclide si intende un algoritmo che è in grado di produrre in un numero finito di passi un MCD tra due elementi a e b non entrambi nulli di un anello euclideo[4]. L'algoritmo classico è di seguito presentato:

[4]Si richiede che l'anello sia euclideo e non soltanto che sia un PID, dal momento che l'algoritmo usufruisce delle proprietà della funzione grado.

$e \leftarrow \max(a, b)$;
$d \leftarrow \min(a, b)$;

while $d > 0$ **do**
    $m \leftarrow d$;
    $d \leftarrow e \bmod d$;
    $e \leftarrow m$;
end

dove e è l'MCD ricercato e l'operazione mod restituisce un resto della divisione euclidea[5].

Lemma 2.2. L'algoritmo di Euclide termina sempre in un numero finito di passi.

Dimostrazione. Se d è pari a 0, l'algoritmo termina immediatamente.

Altrimenti si può costruire una sequenza $(g(d_i))_{i\geq 1}$ dove d_i è il valore di d all'inizio di ogni i-esimo ciclo **while**. Ad ogni ciclo vi sono due casi: se d_i si annulla dopo l'operazione di mod, il ciclo si conclude al passo successivo, altrimenti, poiché d_i è un resto di una divisione euclidea, segue che $g(d_i) < g(d_{i-1})$, dove si pone $d_0 = \min(a, b)$.

Per il principio della discesa infinita, $(g(d_i))_{i\geq 1}$ non può essere una sequenza infinita, essendo strettamente decrescente. Quindi la sequenza è finita, e pertanto il ciclo **while** s'interrompe dopo un numero finito di passi. □

Lemma 2.3. Sia $r = a \bmod b$. Allora vale che $(a, b) = (b, r)$.

Dimostrazione. Poiché $r = a \bmod b$, $\exists\, q$ tale che $a = qb + r$. Siano k_1 e k_2 tali che $(k_1) = (a, b)$ e $(k_2) = (b, r)$. Dal momento che k_1 divide sia a che b, si ha che divide anche r. Siano α, β tali che $a = \alpha k_1$ e $b = \beta k_1$. Si verifica infatti che:

$$r = a - qb = \alpha k_1 - q\beta k_1 = k_1(\alpha - q\beta).$$

Poiché k_1 divide sia b che r, per le proprietà del MCD, k_1 divide anche k_2. Analogamente, k_2 divide k_1. Pertanto k_1 e k_2 sono associati, e dalla *Proposizione 2.4* generano quindi lo stesso ideale, da cui la tesi. □

Teorema 2.4. L'algoritmo di Euclide restituisce sempre correttamente un MCD tra due elementi a e b non entrambi nulli in un numero finito di passi.

Dimostrazione. Per il *Lemma 2.2*, l'algoritmo sicuramente termina. Se d è pari a 0, allora l'algoritmo termina restituendo e. Il valore è corretto, dal momento che, senza perdità di generalità, se b è nullo, allora $\mathrm{MCD}(a, b) = a$: infatti a divide sia sé stesso che 0, e ogni divisore di a è sempre un divisore di 0.

Se invece d non è pari a 0, si scelga il d_n tale che $g(d_n)$ sia l'ultimo elemento della sequenza $(g(d_i))_{i\geq 1}$ definita nel *Lemma 2.2*. Per il *Lemma 2.3*, si ha la seguente uguaglianza:

[5] Ossia $a \bmod b$ restituisce un r tale che $\exists\, q \mid a = bq + r$ con $r = 0$ o $g(r) < g(q)$.

$$(e_0, d_0) = (d_0, d_1) = \cdots = (d_n, 0) = (d_n).$$

Poiché quindi d_n è generatore di $(e_0, d_0) = (a, b)$, $d_n = \mathrm{MCD}(a, b)$. □

2.4 UFD e fattorizzazione

Si enuncia ora la definizione fondamentale di UFD, sulla quale costruiremo un teorema fondamentale per gli anelli euclidei.

Definizione 2.6. Si dice che un dominio D è uno *unique factorization domain* (**UFD**)[6] se ogni $a \in D$ non nullo e non invertibile può essere scritto in forma unica come prodotto di irriducibili, a meno di associati.

Lemma 2.4. Sia E un anello euclideo. Allora ogni elemento $a \in E$ non nullo e non invertibile può essere scritto come prodotto di irriducibili.

Dimostrazione. Si definisca A nel seguente modo:

$$A = \{g(a) \mid a \in E \setminus (E^* \cup \{0\}) \text{ non sia prodotto di irriducibili}\}.$$

Se $A \neq \varnothing$, allora, poiché $A \subseteq \mathbb{N}$, per il principio del buon ordinamento, esiste un $m \in E$ tale che $g(m)$ sia minimo. Sicuramente m non è irriducibile – altrimenti $g(m) \notin A$, ↯ –, quindi $m = ab$ con $a, b \in E \setminus E^*$.

Poiché $a \mid m$, ma $m \nmid a$ – altrimenti a e m sarebbero associati, e quindi b sarebbe invertibile –, si deduce che $g(a) < g(m)$, e quindi che $g(a) \notin A$. Allora a può scriversi come prodotto di irriducibili. Analogamente anche b può scriversi come prodotto di irriducibili, e quindi m, che è il prodotto di a e b, è prodotto di irriducibili, ↯.

Quindi $A = \varnothing$, e ogni $a \in E$ non nullo e non invertibile è prodotto di irriducibili. □

Teorema 2.5. Sia E un anello euclideo. Allora E è un UFD[7].

Dimostrazione. Innanzitutto, per il *Lemma 2.4*, ogni $a \in E$ non invertibile e non nullo ammette una fattorizzazione.

Sia allora $a \in E$ non invertibile e non nullo. Affinché E sia un UFD, deve verificarsi la seguente condizione: se $a = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s \in E$, allora $r = s$ ed esiste una permutazione $\sigma \in S_r$ tale per cui σ associ a ogni indice i di un p_i un indice j di un q_j in modo tale che p_i e q_j siano associati.

Si procede per induzione.

[6] Ossia un *dominio a fattorizzazione unica*.

[7] In realtà questo teorema è un caso particolare di un teorema più generale: ogni PID è un UFD. Poiché la dimostrazione esula dalle intenzioni di questo articolo, si è preferito dimostrare il caso più familiare. Per la dimostrazione del teorema più generale si rimanda a [1, pp. 124-126].

(*passo base*) Se $r = 1$, allora a è irriducibile. Allora necessariamente $s = 1$, altrimenti a sarebbe prodotto di irriducibili, e quindi contemporaneamente anche non irriducibile. Inoltre esiste la permutazione banale $e \in S_1$ che associa p_1 a q_1.

(*passo induttivo*) Si assume che valga la tesi se a è prodotto di $r-1$ irriducibili. Si consideri p_1: poiché p_1 divide a, p_1 divide anche $q_1 q_2 \cdots q_s$. Dal momento che E, in quanto anello euclideo, è anche un dominio, dal *Teorema 2.3*, p_1 è anche primo, e quindi $p_1 \mid q_1$ o $p_1 \mid q_2 \cdots q_s$.

Se $p_1 \nmid q_1$ si reitera il procedimento su $q_2 \cdots q_s$, trovando in un numero finito di passi un q_j tale per cui $p_1 \mid q_j$. Allora si procede la dimostrazione scambiando q_1 e q_j.

Poiché q_1 è irriducibile, p_1 e q_1 sono associati, ossia $q_1 = kp_1$ con $k \in E^*$. Allora $p_1 \cdots p_r = q_1 \cdots q_s = kp_1 \cdots q_s$, quindi, dal momento che $p_1 \neq 0$ ed E è un dominio:

$$p_1(p_2 \cdots p_r - kq_2 \cdots q_s) = 0 \implies p_2 \cdots p_r = kq_2 \cdots q_s.$$

Tuttavia il primo membro è un prodotto $r-1$ irriducibili, pertanto $r = s$ ed esiste un $\sigma \in S_{r-1}$ che associa ad ogni irriducibile p_i un suo associato q_i. Allora si estende σ a S_r mappando p_1 a q_1, verificando la tesi. □

3 Esempi notevoli di anelli euclidei

3.1 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 una conseguenza del *Teorema 2.5*.

3.2 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.

3.3 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[8].

Esempio 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 desume così che $\operatorname{Ker}\varphi = (x - \alpha)$.

3.4 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:

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

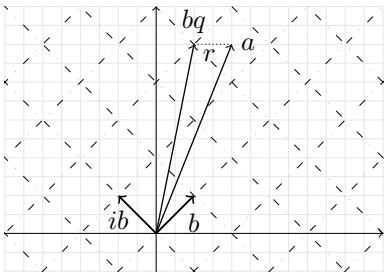

Figura 1: Visualizzazione della divisione euclidea nel piano degli interi di Gauss.

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 $\mathbb{Z}[i]$.

[8] 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. [2]).

Teorema 3.1. $\mathbb{Z}[i]$ 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 $|ab| = |a|\,|b|$[9], 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 $r = 0 \vee g(r) < g(b)$. Come si visualizza facilmente nella *Figura 1*, 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 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:

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

□

3.5 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 $\omega^2 = \overline{\omega}$.

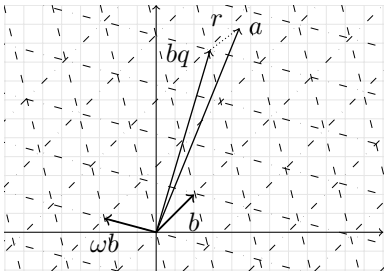

Figura 2: Visualizzazione della divisione euclidea nel piano degli interi di Eisenstein.

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:

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

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

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

Teorema 3.2. $\mathbb{Z}[\omega]$ 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 (come in *Figura 2*), 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:

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

□

4 Riferimenti bibliografici

[1] P. Di Martino e R. Dvornicich. *Algebra*. Didattica e Ricerca. Manuali. Pisa University Press, 2013. ISBN: 9788867410958.

[2] 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`.