Anelli euclidei, PID e UFD

§1.1 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 1.1.1. Un **anello euclideo** è un dominio d'integrità D[a] 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 $r = 0 \vee g(r) < g(q)$.

[a] 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 1.1.2. 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 1.1.3

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 $r = 0$, ↯ –, 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 1.1.4

$g(1)$ è il minimo di $\operatorname{Im} g$, 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 1.1.5

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 1.1.4*, $g(1)$ 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 1.1.4* si desume che $g(a)$ è minimo, e quindi che r è nullo. Si conclude quindi che $aq = 1$, e dunque che $a \in E^*$. □

§1.2 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 1.2.1. 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 1.2.2. 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 1.2.3

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 1.2.4

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 1.2.3*, $\exists\, d \in E^*$ 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 1.2.5

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, $(a) = (b)$. □

Definizione 1.2.6. 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 1.2.7

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 $a \mid b$, dal momento che anche $b \mid a$, si dedurrebbe che a e b sono associati secondo la *Proposizione 1.2.3*. Tuttavia questo implicherebbe che $c \in A^*$, ↯. □

§1.3 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 1.3.1. Si dice che un dominio è un *principal ideal domain* (**PID**)[a] se ogni suo ideale è monogenerato.

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

Teorema 1.3.2

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 1.3.3. 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[a]. Quando si scriverà $\text{MCD}(a, b)$ s'intenderà quindi uno qualsiasi di questi associati.

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

Teorema 1.3.4 (*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 1.3.5
Siano $a, b \in D$. Allora vale la seguente equivalenza:

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

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*, $\exists\, \alpha, \beta$ 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 $m = \text{MCD}(a, b)$. 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 1.2.5*, $(m) = (d) = (a, b)$, da cui $d = \text{MCD}(a, b)$. □

Proposizione 1.3.6
Se $a \mid bc$ e $d = \text{MCD}(a, b) \in D^*$, allora $a \mid c$.

Dimostrazione. Per l'*Identità di Bézout* $\exists\, \alpha, \beta$ 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 1.3.7
Se a è un irriducibile di un PID D, allora $\forall\, b \in D$, $(a, b) = D \vee (a, b) = (a)$, o equivalentemente $\text{MCD}(a, b) \in D^*$ o $\text{MCD}(a, b) = a$.

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

Teorema 1.3.8
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 1.3.7*, $\text{MCD}(a, b)$ può essere solo un associato di a o essere un invertibile. Se è un associato di a, allora, per la *Proposizione 1.2.4*, poiché $\text{MCD}(a, b)$ divide b, anche a divide b. Altrimenti $\text{MCD}(a, b) \in D^*$, e quindi, per la *Proposizione 1.3.6*, $a \mid c$. □

§1.4 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[1]. L'algoritmo classico è di seguito presentato:

[1] 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[2].

Lemma 1.4.1
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 1.4.2
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 1.2.5* generano quindi lo stesso ideale, da cui la tesi. □

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

Teorema 1.4.3

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 1.4.1*, 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 1.4.1*. Per il *Lemma 1.4.2*, si ha la seguente uguaglianza:

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

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

§1.5 UFD e fattorizzazione

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

Definizione 1.5.1. Si dice che un dominio D è uno *unique factorization domain* (**UFD**)[a] se ogni $a \in D$ non nullo e non invertibile può essere scritto in forma unica come prodotto di irriducibili, a meno di associati.

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

Lemma 1.5.2

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 1.5.3

Sia E un anello euclideo. Allora E è un UFD[a].

[a] 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 queste dispense, si è preferito dimostrare il caso più familiare. Per la dimostrazione del teorema più generale si rimanda a [DM, pp. 124-126].

Dimostrazione. Innanzitutto, per il *Lemma 1.5.2*, 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.

(*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 1.3.8*, 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 $q_1 = k p_1$ con $k \in E^*$. Allora $p_1 \cdots p_r = q_1 \cdots q_s = k p_1 \cdots q_s$, quindi, dal momento che $p_1 \neq 0$ ed E è un dominio:

$$p_1(p_2 \cdots p_r - k q_2 \cdots q_s) = 0 \implies p_2 \cdots p_r = k q_2 \cdots q_s.$$

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. □

§1.6 Il teorema cinese del resto

Il noto *Teorema cinese del resto* è un risultato più generale di quanto si sia visto nel contesto dell'aritmetica modulare. Difatti, esso è applicabile in forma estesa a tutti gli anelli euclidei, non solo ai numeri interi (che comunque rimangono un esempio classico di anello euclideo).

Lemma 1.6.1

Sia a un elemento riducibile di un anello euclideo E e sia $a = bc$, dove $\mathrm{MCD}(b, c) \in E^*$. Allora vale il seguente isomorfismo:

$$A/(a) \cong A/(b) \times A/(c).$$

Dimostrazione. Si consideri la funzione π definita nel seguente modo:

$$\pi : A/(a) \to A/(b) \times A/(c),\ e + (a) \mapsto (e + (b), e + (c)).$$

Si verifica che π è un omomorfismo. Infatti $\pi(1 + (a)) = (1 + (b), 1 + (c))$.

Siano e, $k \in A$. Allora π soddisfa la linearità:

$$\pi\Big(\big(e+(a)\big)+\big(k+(a)\big)\Big) = \pi\big(e+k+(a)\big) = \big(e+k+(b), e+k+(c)\big) = \big(e+(b), e+(c)\big)+ \big(k+(b), k+(c)\big) = \pi\big(e+(a)\big)+\pi\big(k+(a)\big).$$

e la moltiplicatività:

$$\pi\Big(\big(e+(a)\big)\cdot\big(k+(a)\big)\Big) = \pi\big(ek+(a)\big) = \big(ek+(b), ek+(c)\big) = \big(e+(b), e+(c)\big)\cdot \big(k+(b), k+(c)\big) = \pi\big(e+(a)\big)\cdot\pi\big(k+(a)\big).$$

Si studia $\operatorname{Ker}\pi$ per dimostrare l'iniettività di π. Si pone dunque $\pi\big(e + (a)\big) = \big(0 + (b), 0 + (c)\big)$. Questa condizione è equivalente ad asserire che sia b che c dividano e.

Sia allora $k \in E$ tale che $e = bk$. Dal momento che c divide e, si e divide bk. Allora, dacché per ipotesi $\mathrm{MCD}(a, b) \in E^*$, per la *Proposizione 1.3.6* c divide k. Quindi esiste $j \in E$ tale che $k = cj$. In particolare, unendo le due condizioni si ottiene $e = bk = bcj = aj$. Pertanto a divide e, da cui si deduce che $e + (a)$ è equivalente a $0 + (a)$. Allora, poiché $\operatorname{Ker}\pi = (0)$, π è un monomorfismo.

Si studia invece adesso la surgettività di π. Siano $\alpha, \beta \in E$. Si pone dunque $\pi\big(e+(a)\big) = \big(\alpha+(b), \beta+(c)\big)$. Questa condizione è equivalente al seguente sistema:

$$\begin{cases} e = \alpha + bk, \\ e = \beta + cj, \end{cases} \qquad \text{con } k, j \in E.$$

Unendo le due condizioni si ottiene la seguente equazione:

$$\alpha + bk = \beta + cj \iff cj - bk = \alpha - \beta.$$

Si consideri ora $d = \mathrm{MCD}(b, c)$. Per l'*Identità di Bézout* esistono x, y tali che:

$$cx + by = d,$$

da cui si ricava che:

$$(\alpha-\beta)(cx+by) = (\alpha-\beta)d \implies cxd^{-1}(\alpha-\beta) + byd^{-1}(\alpha-\beta) = \alpha - \beta,$$

ponendo allora $j = xd^{-1}(\alpha-\beta)$ e $k = -yd^{-1}(\alpha-\beta)$ si ricava una possibile soluzione per e. Quindi π è un epimorfismo.

Poiché π è sia un monomorfismo che un epimorfismo, si conclude che π è un isomorfismo, da cui la tesi.

□

Teorema 1.6.2 (*Teorema cinese del resto*)
Sia a un elemento di un anello euclideo A e sia $p_1^{m_1} p_2^{m_2} \cdots p_n^{m_n}$ una sua fattorizzazione in irriducibili non associati. Allora vale il seguente isomorfismo:

$$A/(a) \cong A/(p_1^{m_1}) \times \cdots \times A/(p_n^{m_n}).$$

Dimostrazione. Si dimostra il teorema applicando il principio di induzione su n, il numero di fattori irriducibili distinti che appaiono nella fattorizzazione di a.

(*passo base*) Se a consta di un solo fattore irriducibile, allora banalmente $A/(a) \cong A/(p_1^{m_1})$.

(*passo induttivo*) Possiamo riscrivere a come il prodotto di $(p_1^{m_1} \cdots p_{n-1}^{m_{n-1}})$ e di $p_n^{m_n}$.

Si nota innanzitutto che $d = \mathrm{MCD}(p_1^{m_1} \cdots p_{n-1}^{m_{n-1}}, p_n^{m_n})$ è un invertibile. Se così non fosse, infatti, si potrebbe considerare un irriducibile q della fattorizzazione di d: tale q, in quanto primo per il *Teorema 1.3.8*, deve dividere un p_j con $1 \leq j \leq n-1$, così come deve

dividere p_n. Allora p_j e q sono associati, così come q e p_n. Dunque anche p_j e p_n sono associati. Tuttavia questo è un assurdo, dal momento che per ipotesi la fattorizzazione di a include irriducibili distinti e non associati, $\lightning$.

Allora dal *Lemma 1.6.1* si ricava che:

$$A/(a) \cong A/(p_1^{m_1} \cdots p_{n-1}^{m_{n-1}}) \times A/(p_n^{m_n}),$$

mentre dal passo induttivo si sa già che:

$$A/(p_1^{m_1} \cdots p_{n-1}^{m_{n-1}}) \cong A/(p_1^{m_1}) \times \cdots \times A/(p_{n-1}^{m_{n-1}}).$$

Pertanto, unendo le due informazioni, si verifica la tesi:

$$A/(a) \cong A/(p_1^{m_1}) \times \cdots \times A/(p_{n-1}^{m_{n-1}}) \times A/(p_n^{m_n}).$$

□

§1.7 La seminorma di $\mathbb{Z}[\sqrt{n}]$

Si definisce innanzitutto $\mathbb{Z}[\sqrt{n}]$ nel seguente modo:

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

Definizione 1.7.1. Si definisce **seminorma** di $\mathbb{Z}[\sqrt{n}]$ la seguente funzione:

$$\ell : \mathbb{Z}[\sqrt{n}] \to \mathbb{Z},\ a + b\sqrt{n} \mapsto a^2 - nb^2.$$

Proposizione 1.7.2
La seminorma di $\mathbb{Z}[\sqrt{n}]$ è una funzione moltiplicativa.

Dimostrazione. Dimostrare la tesi è equivalente al verificare la seguente identità:

$$(a^2 - nb^2)(c^2 - nd^2) = (ac + nbd)^2 - n(ad + bc)^2,$$

come si verifica nelle seguenti righe:

$$(ac + nbd)^2 - n(ad + bc)^2 = a^2c^2 + n^2b^2d^2 + \cancel{2acnbd} - na^2d^2 - nb^2c^2 - \cancel{2acnbd} = a^2(c^2 - nd^2) - nb^2(c^2 - nd^2) = (a^2 - nb^2)(c^2 - nd^2).$$

□

Teorema 1.7.3
Un elemento $a \in \mathbb{Z}[\sqrt{n}]$ è invertibile se e solo se $\ell(a) \in \{1, -1\}$.

Dimostrazione. Si dimostrano le due implicazioni separatamente.

($\implies$) Sia $a \in a \in \mathbb{Z}[\sqrt{n}]^*$. Allora esiste un $b \in \mathbb{Z}[\sqrt{n}]^*$ tale che $ab = 1$. Applicando la seminorma a entrambi i membri si ricava che:

$$\ell(ab) = 1 \implies \ell(a)\ell(b) = 1.$$

Gli unici invertibili di $\mathbb{Z}$ sono tuttavia 1 e -1, da cui la tesi.

($\impliedby$) Si consideri $a + b\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$. Sia $d = \ell(a) \in \{1, -1\}$ si ricava che:

$$a^2 - nb^2 = d \implies (a + b\sqrt{n})(a - b\sqrt{n}) = d \implies (a + b\sqrt{n})d^{-1}(a - b\sqrt{n}) = 1,$$

da cui la tesi. □

Esempio 1.7.4 ($\mathbb{Z}[\sqrt{10}]$ non è un UFD)
Il numero 6 ammette due fattorizzazioni in irriducibili completamente distinte in $\mathbb{Z}[\sqrt{10}]$. Dunque $\mathbb{Z}[\sqrt{10}]$ non è un UFD. Conseguentemente non è né un anello euclideo[a], né un PID[b].

[a] Violerebbe altrimenti il *Teorema 1.5.3*.
[b] Si usa ancora la proposizione, non dimostrata in queste dispense, secondo cui un PID è sempre un UFD. Per tale dimostrazione si rimanda ancora a [DM, pp. 124-126].

Dimostrazione. Dal momento che $6 = 16 - 10$, possiamo fattorizzare 6 come il prodotto di $4 + \sqrt{10}$ e $4 - \sqrt{10}$. Tuttavia, dalla fattorizzazione in $\mathbb{Z}$, sappiamo anche che $6 = 2 \cdot 3$.

Dimostriamo che sia 2 che 3 sono irriducibili in $\mathbb{Z}[\sqrt{10}]$. Se 2 fosse riducibile, si potrebbe scrivere come prodotto di due fattori non invertibili:

$$2 = (a + b\sqrt{10})(c + d\sqrt{10}) \implies 4 = (a^2 - 10b^2)(c^2 - 10d^2). \tag{1.1}$$

Poiché nessun fattore di 2 è invertibile per ipotesi, per il *Teorema 1.7.3* nessuno dei due fattori in (1.1) può essere uguale a 1 o -1. Allora l'unica possibilità è che $a^2 - 10b^2$ sia uguale a 2 o -2. Se però così fosse, $a^2 \equiv \pm 2 \ (10)$, che non ammette soluzione.

Reiterando lo stesso ragionamento per 3, si ottiene $a^2 \equiv \pm 3 \ (10)$, che anche stavolta non ammette soluzione. Quindi sia 2 che 3 sono irriducibili in $\mathbb{Z}[\sqrt{10}]$.

Analogamente dimostriamo che sia $4+\sqrt{10}$ che $4-\sqrt{10}$ sono irriducibili. Si assuma che $4+\sqrt{10}$ sia riducibile, allora si ricava che:

$$4+\sqrt{10} = (a+b\sqrt{10})(c+d\sqrt{10}),$$

da cui, passando alle seminorme si ottiene che:

$$6 = (a^2-10b^2)(c^2-10d^2).$$

Poiché entrambi i fattori sono non invertibili per ipotesi, per il *Teorema 1.7.3* ognuno di essi è diverso da 1 e -1, come visto prima. Quindi l'unica possibilità è che a^2-10b^2 sia uguale a ± 2 o ± 3. Tuttavia, da prima sappiamo che nessuna di queste equazioni ammette soluzione. Quindi $4+\sqrt{10}$ è irriducibile, e allo stesso modo si dimostra che anche $4-\sqrt{10}$ lo è.

Ora si dimostra che 2 non è associato né a $4+\sqrt{10}$ né a $4-\sqrt{10}$. Se fossero associati, esisterebbe un invertibile a tale che $2 = (4\pm\sqrt{10})a$.

Passando alle norme, si ricava che:

$$4 = 6\,\ell(a),$$

dove, ricordando che $\ell(a) = \pm 1$ per il *Teorema 1.7.3*, si ottiene:

$$4 = \pm 6,$$

ossia un assurdo, $\lightning$.

Poiché 2 non è associato né a né a $4+\sqrt{10}$ né a $4-\sqrt{10}$, le due fattorizzazioni sono due fattorizzazioni in irriducibili completamente distinte. Quindi $\mathbb{Z}[\sqrt{10}]$ non può essere un UFD. □

Riferimenti bibliografici

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