

# L'Algebrario

dispense del corso di Aritmetica

GABRIEL ANTONIO VIDETTA

A.A. 2022/2023



UNIVERSITÀ DI PISA



## **Premessa**

TODO



## Indice

<b>1</b>	<b>Introduzione alla teoria degli anelli</b>	<b>8</b>
1.1	Definizione e prime proprietà	8
1.2	Omomorfismi di anelli e ideali	10
1.3	Quoziente per un ideale e primo teorema d'isomorfismo	12
<b>2</b>	<b>Anelli euclidei, PID e UFD</b>	<b>15</b>
2.1	Prime proprietà	15
2.2	Irriducibili e prime definizioni	16
2.3	PID e MCD	17
2.4	L'algoritmo di Euclide	19
2.5	UFD e fattorizzazione	21
2.6	Il teorema cinese del resto	22
<b>3</b>	<b>Esempi notevoli di anelli euclidei</b>	<b>26</b>
3.1	I numeri interi: $\mathbb{Z}$	26
3.2	I campi: $\mathbb{K}$	26
3.3	I polinomi di un campo: $\mathbb{K}[x]$	26
3.4	Gli interi di Gauss: $\mathbb{Z}[i]$	27
3.5	Gli interi di Eisenstein: $\mathbb{Z}[\omega]$	28
<b>4</b>	<b>Irriducibili e corollari di aritmetica in <math>\mathbb{Z}[i]</math></b>	<b>30</b>
4.1	Il teorema di Natale di Fermat e gli irriducibili in $\mathbb{Z}[i]$	30
4.2	L'identità di Brahmagupta-Fibonacci	32
<b>5</b>	<b>Irriducibilità in <math>\mathbb{Z}[x]</math> e in <math>\mathbb{Q}[x]</math></b>	<b>35</b>
5.1	Criterio di Eisenstein e proiezione in $\mathbb{Z}_p[x]$	35
5.2	Alcuni irriducibili di $\mathbb{Z}_2[x]$	37
5.3	Teorema delle radici razionali e lemma di Gauss	38
<b>6</b>	<b>I polinomi di un campo: <math>\mathbb{K}[x]</math></b>	<b>42</b>
6.1	Elementi preliminari	42
6.2	Sottogruppi moltiplicativi finiti di $\mathbb{K}$	43
6.3	Il quoziente $\mathbb{K}[x]/(f(x))$	44
<b>7</b>	<b>Estensioni algebriche di <math>\mathbb{K}</math></b>	<b>48</b>
7.1	Morfismi di valutazione, elementi algebrici e trascendenti	48
7.2	Teorema delle torri ed estensioni algebriche	51
7.3	Campi di spezzamento di un polinomio	56
<b>8</b>	<b>Teorema fondamentale dell'Algebra e radici reali in <math>\mathbb{Q}[x]</math></b>	<b>58</b>
<b>9</b>	<b>Introduzione alla teoria dei campi</b>	<b>60</b>
9.1	La caratteristica di un campo	60
9.2	Prime proprietà dei campi di caratteristica $p$	61
9.3	L'omomorfismo di Frobenius	61
9.4	Classificazione dei campi finiti	63
<b>10</b>	<b>Teoremi rilevanti sui campi finiti</b>	<b>65</b>
10.1	Campo di spezzamento di un irriducibile in $\mathbb{F}_p$	65
10.2	L'inclusione $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ e il polinomio $x^{p^n} - x$	66

**11 Riferimenti bibliografici**

**70**



## §1 Introduzione alla teoria degli anelli

### §1.1 Definizione e prime proprietà

**Definizione 1.1.** Si definisce **anello**<sup>a</sup> una struttura algebrica costruita su un insieme  $A$  e due operazioni binarie  $+$  e  $\cdot$ <sup>b</sup> avente le seguenti proprietà:

- $(A, +)$  è un *gruppo abeliano*, alla cui identità, detta *identità additiva*, ci si riferisce con il simbolo  $0$ ,
- $\forall a, b, c \in A, (ab)c = a(bc)$ ,
- $\forall a, b, c \in A, (a + b)c = ac + bc$ ,
- $\forall a, b, c \in A, a(b + c) = ab + ac$ ,
- $\exists 1 \in A \mid \forall a \in A, 1a = a = a1$ , e tale  $1$  viene detto *identità moltiplicativa*.

<sup>a</sup>In realtà, si parla in questo caso di anello *con unità*, in cui vale l'assioma di esistenza di un'identità moltiplicativa. In queste dispense si identificherà con "anello" solamente un anello con unità.

<sup>b</sup>D'ora in avanti il punto verrà omissso.

Come accade per i gruppi, gli anelli soddisfano alcune proprietà algebriche particolari, tra le quali si citano le più importanti:

#### Proposizione 1.2

$$\forall a \in A, 0a = 0 = a0.$$

*Dimostrazione.*  $0a = (0 + 0)a = 0a + 0a \implies 0a = 0$ . Analogamente  $a0 = a(0 + 0) = a0 + a0 \implies a0 = 0$ .  $\square$

#### Proposizione 1.3

$$\forall a \in A, -(-a) = a.$$

*Dimostrazione.*  $-(-a) - a = 0 \wedge a - a = 0 \implies -(-a) = a$ , per la proprietà di unicità dell'inverso in un gruppo<sup>1</sup>.  $\square$

#### Proposizione 1.4

$$a(-b) = (-a)b = -(ab).$$

*Dimostrazione.*  $a(-b) + ab = a(b - b) = a0 = 0 \implies a(-b) = -(ab)$ , per la proprietà di unicità dell'inverso in un gruppo. Analogamente  $(-a)b + ab = (a - a)b = 0b = 0 \implies (-a)b = -(ab)$ .  $\square$

#### Corollario 1.5

$$(-1)a = a(-1) = -a.$$

<sup>1</sup>In questo caso, il gruppo additivo dell'anello.



**Proposizione 1.6**

$$(-a)(-b) = ab.$$

*Dimostrazione.*  $(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$ , per la *Proposizione 1.4*.  $\square$

Si enuncia invece adesso la nozione di **sottoanello**, in tutto e per tutto analoga a quella di *sottogruppo*.

**Definizione 1.7.** Si definisce sottoanello rispetto all'anello  $A$  un anello  $B$  avente le seguenti proprietà:

- $B \subseteq A$ ,
- $0, 1 \in B$ ,
- $\forall a, b \in B, a + b \in B \wedge ab \in B$ .

**Definizione 1.8.** Un sottoanello  $B$  rispetto ad  $A$  si dice **proprio** se  $B \neq A$ .

**Definizione 1.9.** Un anello si dice **commutativo** se  $\forall a, b \in A, ab = ba$ .

**Esempio 1.10**

Un facile esempio di anello commutativo è  $\mathbb{Z}/n\mathbb{Z}$ .

**Definizione 1.11.** Un elemento  $a$  di un anello  $A$  si dice **invertibile** se  $\exists b \in A \mid ab = ba = 1$ .

**Definizione 1.12.** Dato un anello  $A$ , si definisce  $A^*$  come l'insieme degli elementi invertibili di  $A$ , che a sua volta forma un *gruppo moltiplicativo*.

**Definizione 1.13.** Un anello  $A$  si dice **corpo** se  $\forall a \neq 0 \in A, \exists b \in A \mid ab = ba = 1$ , ossia se  $A \setminus \{0\} = A^*$ .

**Esempio 1.14**

L'esempio più rilevante di corpo è quello dei *quaternioni*  $\mathbb{H}$ , definiti nel seguente modo:

$$\mathbb{H} = \{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \mid a, b, c, d \in \mathbb{R}\},$$

dove:

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1, \quad \mathbf{ij} = \mathbf{k}, \mathbf{jk} = \mathbf{i}, \mathbf{ki} = \mathbf{j}.$$

Infatti ogni elemento non nullo di  $\mathbb{H}$  possiede un inverso moltiplicativo:

$$(a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})^{-1} = \frac{a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}}{a^2 + b^2 + c^2 + d^2},$$

mentre la moltiplicazione non è commutativa.

**Definizione 1.15.** Un anello commutativo che è anche un corpo si dice **campo**.

### Esempio 1.16

Alcuni campi, tra i più importanti, sono  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$  e  $\mathbb{Z}/p\mathbb{Z}$  con  $p$  primo.

**Definizione 1.17.** Un elemento  $a \neq 0$  appartenente a un anello  $A$  si dice **divisore di zero** se  $\exists b \neq 0 \in A \mid ab = 0$  o  $ba = 0$ .

### Esempio 1.18

2 è un divisore di zero in  $\mathbb{Z}/6\mathbb{Z}$ , infatti  $2 \cdot 3 \equiv 0 \pmod{6}$ .

**Definizione 1.19.** Un anello commutativo in cui non sono presenti divisori di zero si dice **dominio d'integrità**, o più semplicemente *dominio*.

### Proposizione 1.20 (Legge di annullamento del prodotto)

Sia  $D$  un dominio. Allora  $ab = 0 \implies a = 0 \vee b = 0$ .

*Dimostrazione.* Siano  $a, b \in D \mid ab = 0$ . Se  $a = 0$ , la condizione è soddisfatta. Se invece  $a \neq 0$ ,  $b$  deve essere per forza nullo, altrimenti si sarebbe trovato un divisore di zero, e  $D$  non sarebbe un dominio,  $\zeta$ .  $\square$

### Esempio 1.21

L'anello dei polinomi su un campo,  $\mathbb{K}[x]$ , è un dominio.

## §1.2 Omomorfismi di anelli e ideali

**Definizione 1.22.** Un **omomorfismo di anelli**<sup>a</sup> è una mappa  $\phi : A \rightarrow B$  – con  $A$  e  $B$  anelli – soddisfacente alcune particolari proprietà:

- $\phi$  è un *omomorfismo di gruppi* rispetto all'addizione di  $A$  e di  $B$ , ossia  $\forall a, b \in A$ ,  $\phi(a + b) = \phi(a) + \phi(b)$ ,
- $\phi(ab) = \phi(a)\phi(b)$ ,
- $\phi(1_A) = 1_B$ .

<sup>a</sup>La specificazione "di anelli" è d'ora in avanti omessa.

**Definizione 1.23.** Se  $\phi : A \rightarrow B$  è un omomorfismo iniettivo, si dice che  $\phi$  è un **monomorfismo**.

**Definizione 1.24.** Se  $\phi : A \rightarrow B$  è un omomorfismo suriettivo, si dice che  $\phi$  è un **epimorfismo**.

**Definizione 1.25.** Se  $\phi : A \rightarrow B$  è un omomorfismo bigettivo<sup>a</sup>, si dice che  $\phi$  è un **isomorfismo**.

<sup>a</sup>Ovvero se è sia un monomorfismo che un epimorfismo.

Prima di enunciare l'analogo del *Primo teorema d'isomorfismo* dei gruppi in relazione agli anelli, si rifletta su un esempio di omomorfismo:

### Esempio 1.26

Sia  $\phi : \mathbb{Z} \rightarrow \mathbb{Z}, k \mapsto 2k$  un omomorfismo. Esso è un monomorfismo, infatti  $\phi(x) = \phi(y) \implies 2x = 2y \implies x = y$ . Pertanto  $\text{Ker } \phi = \{0\}$ . Sebbene  $\text{Ker } \phi < \mathbb{Z}$ , esso **non è un sottoanello**<sup>a</sup>.

<sup>a</sup>Infatti  $1 \notin \text{Ker } \phi$ .

Dunque, con lo scopo di definire meglio le proprietà di un *kernel*, così come si introdotto il concetto di *sottogruppo normale* per i gruppi, si introduce ora il concetto di **ideale**.

**Definizione 1.27.** Si definisce ideale rispetto all'anello  $A$  un insieme  $I$  avente le seguenti proprietà:

- $I \leq A$ ,
- $\forall a \in A, \forall b \in I, ab \in I$  e  $ba \in I$ .

### Esempio 1.28

Sia  $I$  l'insieme dei polinomi di  $\mathbb{R}[x]$  tali che 2 ne sia radice. Esso altro non è che un ideale, infatti  $0 \in I \wedge \forall f(x), g(x) \in I, (f + g)(2) = 0$  (i.e.  $I < \mathbb{R}[x]$ ) e  $\forall f(x) \in A, g(x) \in I, (fg)(2) = 0$ .

### Proposizione 1.29

Sia  $I$  un ideale di  $A$ .  $1 \in I \implies I = A$ .

*Dimostrazione.* Per le proprietà dell'ideale  $I, \forall a \in A, a1 = a \in I \implies A \subseteq I$ . Dal momento che anche  $I \subseteq A$ , si deduce che  $I = A$ .  $\square$

### Proposizione 1.30

Sia  $\phi : A \rightarrow B$  un omomorfismo.  $\text{Ker } \phi$  è allora un ideale di  $A$ .

*Dimostrazione.* Poiché  $\phi$  è anche un omomorfismo tra gruppi, si deduce che  $\text{Ker } \phi \leq A$ . Inoltre  $\forall a \in A, \forall b \in \text{Ker } \phi, \phi(ab) = \phi(a)\phi(b) = \phi(a)0 = 0 \implies ab \in \text{Ker } \phi$ .  $\square$

### Proposizione 1.31

Sia  $\phi : A \rightarrow B$  un omomorfismo.  $\text{Im } \phi$  è allora un sottoanello di  $B$ .

*Dimostrazione.* Chiaramente  $0, 1 \in \text{Imm } \phi$ , dal momento che  $\phi(0) = 0$ ,  $\phi(1) = 1$ . Inoltre, dalla teoria dei gruppi, si ricorda anche che  $\text{Imm } \phi \leq B$ . Infine,  $\forall \phi(a), \phi(b) \in \text{Imm } \phi$ ,  $\phi(a)\phi(b) = \phi(ab) \in \text{Imm } \phi$ .  $\square$

**Definizione 1.32.** Si definisce con la notazione  $(a)$  l'ideale *bilatero* generato da  $a$  in  $A$ , ossia:

$$(a) = \{ba \mid b \in A\} \cup \{ab \mid b \in A\}.$$

**Definizione 1.33.** Si dice che un ideale  $I$  è *principale* o **monogenerato**, quando  $\exists a \in I \mid I = (a)$ .

### Esempio 1.34

In relazione all'*Esempio 1.28*, l'ideale  $I$  è monogenerato<sup>a</sup>. In particolare,  $I = (x - 2)$ .

<sup>a</sup>Non è un caso:  $\mathbb{R}[x]$ , in quanto anello euclideo, si dimostra essere un PID (*principal ideal domain*), ossia un dominio che ammette *solo* ideali monogenerati.

## §1.3 Quoziente per un ideale e primo teorema d'isomorfismo

Si definisce invece adesso il concetto di **anello quoziente**, in modo completamente analogo a quello di *gruppo quoziente*:

**Definizione 1.35.** Sia  $A$  un anello e  $I$  un suo ideale, si definisce  $A/I$  l'anello ottenuto quozientando  $A$  per  $I$ . Gli elementi di tale anello sono le classi di equivalenza di  $\sim$  (i.e. gli elementi di  $A/\sim$ ), dove  $\forall a, b \in A$ ,  $a \sim b \iff a - b \in I$ . Tali classi di equivalenza vengono indicate come  $a + I$ , dove  $a$  è un rappresentante della classe. L'anello è così dotato di due operazioni:

- $\forall a, b \in A$ ,  $(a + I) + (b + I) = (a + b) + I$ ,
- $\forall a, b \in A$ ,  $(a + I)(b + I) = ab + I$ .

**Osservazione.** L'addizione di  $A/I$  è ben definita, dal momento che  $I \trianglelefteq A$ , in quanto sottogruppo di un gruppo abeliano.

**Osservazione.** Anche la moltiplicazione di  $A/I$  è ben definita. Siano  $a \sim a'$ ,  $b \sim b'$  quattro elementi di  $A$  tali che  $a = a' + i_1$  e  $b = b' + i_2$  con  $i_1, i_2 \in I$ . Allora  $ab = (a' + i_1)(b' + i_2) = a'b' + \underbrace{i_1b' + i_2a' + i_1i_2}_{\in I} \implies ab \sim a'b'$ .

### Proposizione 1.36

$$A/\{0\} \cong A.$$

*Dimostrazione.* Sia  $\pi : A \rightarrow A/\{0\}$ ,  $a \mapsto a + \{0\}$  l'omomorfismo di proiezione al quoziente. Innanzitutto,  $a \sim a' \iff a - a' = 0 \iff a = a'$ , per cui  $\pi$  è un monomorfismo (altrimenti si troverebbero due  $a, b \mid a \neq b \wedge a \sim b$ ). Infine,  $\pi$  è un epimorfismo, dal momento che  $\forall a + \{0\} \in A/\{0\}$ ,  $\pi(a) = a + \{0\}$ . Pertanto  $\pi$  è un isomorfismo.  $\square$

Adesso è possibile enunciare il seguente fondamentale teorema:

**Teorema 1.37** (*Primo teorema d'isomorfismo*)

Sia  $\phi : A \rightarrow B$  un omomorfismo.  $A/\text{Ker } \phi \cong \text{Imm } \phi$ .

*Dimostrazione.* La dimostrazione procede in modo analogo a quanto visto per il teorema correlato in teoria dei gruppi.

Sia  $\zeta : A/\text{Ker } \phi \rightarrow \text{Imm } \phi$ ,  $a + \text{Ker } \phi \mapsto \phi(a)$ . Si verifica che  $\zeta$  è un omomorfismo: essendolo già per i gruppi, è sufficiente verificare che  $\zeta((a + I)(b + I)) = \zeta(ab + I) = \phi(ab) = \phi(a)\phi(b) = \zeta(a + I)\zeta(b + I)$ .

$\zeta$  è chiaramente anche un epimorfismo, dal momento che  $\forall \phi(a) \in \text{Imm } \phi$ ,  $\zeta(a + \text{Ker } \phi) = \phi(a)$ . Inoltre, dal momento che  $\zeta(a + \text{Ker } \phi) = 0 \iff \phi(a) = 0 \iff a + \text{Ker } \phi = \text{Ker } \phi$ , ossia l'identità di  $A/\text{Ker } \phi$ , si deduce anche che  $\zeta$  è un monomorfismo. Pertanto  $\zeta$  è un isomorfismo.  $\square$

**Corollario 1.38**

Sia  $\phi : A \rightarrow B$  un monomorfismo.  $A \cong \text{Imm } \phi$ .

*Dimostrazione.* Poiché  $\phi$  è un monomorfismo,  $\text{Ker } \phi = \{0\}$ . Allora, per il *Primo teorema di isomorfismo*,  $A/\{0\} \cong \text{Imm } \phi$ . Dalla *Proposizione 1.36*, si desume che  $A \cong A/\{0\}$ . Allora, per la proprietà transitiva degli isomorfismi,  $A \cong \text{Imm } \phi$ .  $\square$



## §2 Anelli euclidei, PID e UFD

### §2.1 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 2.1.** 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:

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

<sup>a</sup>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 2.2.** 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 2.3

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  $r = 0$ ,  $\nexists$  –, 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:  $g(a) < g(b)$ .  $\square$

#### Proposizione 2.4

$g(1)$  è il minimo di  $\text{Imm } g$ , 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,  $g(1) \leq g(1a) = g(a)$ .  $\square$

#### Teorema 2.5

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 2.4*,  $g(1)$  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 2.4* si desume che  $g(a)$  è minimo, e quindi che  $r$  è nullo. Si conclude quindi che  $aq = 1$ , e dunque che  $a \in E^*$ .  $\square$

## §2.2 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 2.6.** In un dominio  $A$ , si dice che  $a \in A \setminus A^*$  è **irriducibile** se  $\exists b, c \mid a = bc \implies b \in A^* \text{ o } c \in A^*$ .

**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 2.7.** 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 2.8

$a$  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.  $\square$

### Proposizione 2.9

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 2.8*,  $\exists d \in E^*$  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 2.10

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 2.11.** 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 2.12

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

*Dimostrazione.* Si dimostra la tesi contronominale. 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 perdita di generalità, se  $a \mid b$ , dal momento che anche  $b \mid a$ , si dedurrebbe che  $a$  e  $b$  sono associati secondo la *Proposizione 2.8*. Tuttavia questo implicherebbe che  $c \in A^*$ ,  $\neq$ . □

## §2.3 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 2.13.** Si dice che un dominio è un *principal ideal domain (PID)*<sup>a</sup> se ogni suo ideale è monogenerato.

<sup>a</sup>Ossia un dominio a soli ideali principali, quindi monogenerati, proprio come da definizione.

### Teorema 2.14

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  $r = a - mq \in I$  e  $g(m)$  è minimo, necessariamente  $r = 0$  – altrimenti  $r$  sarebbe ancor più minimo di  $m$ ,  $\neq -$ , 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  $I = (m)$ .  $\square$

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

**Definizione 2.15.** 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<sup>a</sup>. Quando si scriverà  $\text{MCD}(a, b)$  s'intenderà quindi uno qualsiasi di questi associati.

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

### Teorema 2.16 (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,  $\alpha$  e  $\beta$  tali che  $d = \alpha a + \beta b$ .  $\square$

### Proposizione 2.17

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  $\gamma$  e  $\delta$  tali che  $a = \gamma c$  e  $b = \delta c$ . Pertanto si verifica la seconda proprietà, e quindi la tesi:

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

( $\Leftarrow$ ) 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 2.10*,  $(m) = (d) = (a, b)$ , da cui  $d = \text{MCD}(a, b)$ .  $\square$

### Proposizione 2.18

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:

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

$\square$

### Lemma 2.19

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.  $\square$

### Teorema 2.20

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 2.19*,  $\text{MCD}(a, b)$  può essere solo un associato di  $a$  o essere un invertibile. Se è un associato di  $a$ , allora, per la *Proposizione 2.9*, poiché  $\text{MCD}(a, b)$  divide  $b$ , anche  $a$  divide  $b$ . Altrimenti  $\text{MCD}(a, b) \in D^*$ , e quindi, per la *Proposizione 2.18*,  $a \mid c$ .  $\square$

## §2.4 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<sup>2</sup>. L'algoritmo classico è di seguito presentato:

<sup>2</sup>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  $\bmod$  restituisce un resto della divisione euclidea<sup>3</sup>.

### Lemma 2.21

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  $\bmod$ , 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.  $\square$

### Lemma 2.22

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  $\alpha, \beta$  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 2.10* generano quindi lo stesso ideale, da cui la tesi.  $\square$

### Teorema 2.23

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 2.21*, l'algoritmo sicuramente termina. Se  $d$  è pari a 0, allora l'algoritmo termina restituendo  $e$ . Il valore è corretto, dal momento che, senza perdita di generalità, se  $b$  è nullo, allora  $\text{MCD}(a, b) = a$ : infatti  $a$  divide sia sé stesso che

<sup>3</sup>Ossia  $a \bmod b$  restituisce un  $r$  tale che  $\exists q \mid a = bq + r$  con  $r = 0$  o  $g(r) < g(q)$ .

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 2.21. Per il Lemma 2.22, 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  $(e_0, d_0) = (a, b)$ ,  $d_n = \text{MCD}(a, b)$ .  $\square$

## §2.5 UFD e fattorizzazione

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

**Definizione 2.24.** Si dice che un dominio  $D$  è uno *unique factorization domain (UFD)*<sup>a</sup> se ogni  $a \in D$  non nullo e non invertibile può essere scritto in forma unica come prodotto di irriducibili, a meno di associati.

<sup>a</sup>Ossia un dominio a fattorizzazione unica.

### Lemma 2.25

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  $A \neq \emptyset$ , 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  $g(m) \notin A$ ,  $\neq$  –, 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,  $\neq$ .

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

### Teorema 2.26

Sia  $E$  un anello euclideo. Allora  $E$  è un UFD<sup>a</sup>.

<sup>a</sup>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 2.25, 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  $\sigma$  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 2.20*,  $p_1$  è anche primo, e quindi  $p_1 \mid q_1 \circ p_1 \mid q_2 \cdots q_s$ .

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  $\sigma$  a  $S_r$  mappando  $p_1$  a  $q_1$ , verificando la tesi.  $\square$

## §2.6 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 2.27

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

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

*Dimostrazione.* Si consideri la funzione  $\pi$  definita nel seguente modo:

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

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

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

$$\pi\left((e+(a))+(k+(a))\right) = \pi(e+k+(a)) = (e+k+(b), e+k+(c)) = (e+(b), e+(c)) + (k+(b), k+(c)) = \pi(e+(a)) + \pi(k+(a)).$$

e la moltiplicatività:

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

Si studia  $\text{Ker } \pi$  per dimostrare l'iniettività di  $\pi$ . Si pone dunque  $\pi(e+(a)) = (0+(b), 0+(c))$ . 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  $\text{MCD}(a, b) \in E^*$ , per la *Proposizione 2.18*  $c$  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  $\text{Ker } \pi = (0)$ ,  $\pi$  è un monomorfismo.

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

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

Unendo le due condizioni si ottiene la seguente equazione:

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

Si consideri ora  $d = \text{MCD}(b, c)$ . 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  $\pi$  è un epimorfismo.

Poiché  $\pi$  è sia un monomorfismo che un epimorfismo, si conclude che  $\pi$  è un isomorfismo, da cui la tesi. □

**Teorema 2.28** (*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  $d = \text{MCD}(p_1^{m_1} \cdots p_{n-1}^{m_{n-1}}, p_n^{m_n})$  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 2.20*, 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,  $\zeta$ .

Allora dal *Lemma 2.27* 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:

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

□





### §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:

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

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 2.26*.

#### §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:

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

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:

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

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<sup>4</sup>.

##### Esempio 3.1

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

<sup>4</sup>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]).

### §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:

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

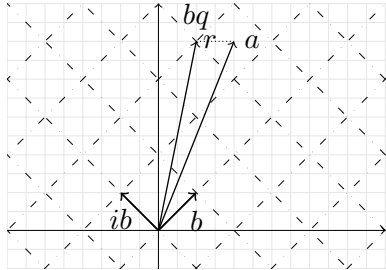


Figura 1: Visualizzazione della divisione euclidea nel piano degli interi di Gauss.

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

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

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 3.2

$\mathbb{Z}[i]$  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  $|ab| = |a||b|^5$ , 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:

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

□

<sup>5</sup>Questa interessante proprietà del modulo è alla base dell'identità di Brahmagupta-Fibonacci:  $(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$ .

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

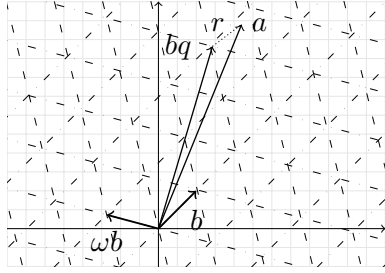


Figura 2: Visualizzazione della divisione euclidea nel piano degli interi di Eisenstein.

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:

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

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

#### Teorema 3.3

$\mathbb{Z}[\omega]$  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  $\omega b$  (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 Irriducibili e corollari di aritmetica in $\mathbb{Z}[i]$

Come già dimostrato,  $\mathbb{Z}[i]$  è un anello euclideo con la seguente funzione grado:

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

A partire da questo preconcetto è possibile dimostrare un teorema importante in aritmetica, il *Teorema di Natale di Fermat*, che discende direttamente come corollario di un teorema più generale riguardante  $\mathbb{Z}[i]$ .

### §4.1 Il teorema di Natale di Fermat e gli irriducibili in $\mathbb{Z}[i]$

#### Lemma 4.1

Sia  $p$  un numero primo riducibile in  $\mathbb{Z}[i]$ , allora  $p$  può essere scritto come somma di due quadrati in  $\mathbb{Z}$ .

*Dimostrazione.* Se  $p$  è riducibile in  $\mathbb{Z}[i]$ , allora esistono  $a + bi$  e  $c + di$  appartenenti a  $\mathbb{Z}[i] \setminus \mathbb{Z}[i]^*$  tali che  $p = (a + bi)(c + di)$ .

Impiegando le proprietà dell'operazione di coniugio si ottiene la seguente equazione:

$$\bar{p} = p = (a - bi)(c - di) \implies p^2 = p\bar{p} = (a^2 + b^2)(c^2 + d^2).$$

Dal momento che  $a + bi$  e  $c + di$  non sono invertibili, i valori della funzione grado calcolati in essi sono strettamente maggiori del valore assunto nell'unità, ovverosia:

$$a^2 + b^2 > 1, \quad c^2 + d^2 > 1.$$

Allora devono per forza valere le seguenti equazioni:

$$p = a^2 + b^2, \quad p = c^2 + d^2,$$

da cui la tesi. □

#### Lemma 4.2

Sia  $p$  un numero primo tale che  $p \equiv 1 \pmod{4}$ . Allora esiste un  $x \in \mathbb{Z}$  tale che  $p \mid x^2 + 1$ .

*Dimostrazione.* Per il *Teorema di Wilson*,  $(p - 1)! \equiv -1 \pmod{p}$ . Attraverso varie manipolazioni algebriche si ottiene:

$$\begin{aligned} -1 &\equiv 1 \cdots \frac{p-1}{2} \cdot \frac{p+1}{2} \cdots (p-1) \equiv 1 \cdots \frac{p-1}{2} \left(-\frac{p-1}{2}\right) \cdots (-1) \equiv \\ &\equiv (-1)^{\frac{p-1}{2}} \left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv \left(\left(\frac{p-1}{2}\right)!\right)^2 \pmod{p}, \end{aligned}$$

da cui con  $x = \left(\frac{p-1}{2}\right)!$  si verifica la tesi. □

**Teorema 4.3**

Sia  $p$  un numero primo tale che  $p \equiv 1 \pmod{4}$ . Allora  $p$  è riducibile in  $\mathbb{Z}[i]$ .

*Dimostrazione.* Per il *Lemma 4.2*, si ha che esiste un  $x \in \mathbb{Z}$  tale che  $p \mid x^2 + 1$ . Se  $p$  fosse irriducibile, dacché  $\mathbb{Z}[i]$  è un PID in quanto euclideo,  $p$  sarebbe anche un primo di  $\mathbb{Z}[i]$ . Dal momento che  $x^2 + 1 = (x + i)(x - i)$ ,  $p$  dovrebbe dividere almeno uno di questi due fattori.

Senza perdita di generalità, si ponga che  $p \mid (x + i)$ . Allora  $\exists a + bi \in \mathbb{Z}[i] \mid x + i = (a + bi)p$ . Uguagliando le parti immaginarie si ottiene  $bp = 1$ , che non ammette soluzioni,  $\neq$ . Pertanto  $p$  è riducibile.  $\square$

**Corollario 4.4 (Teorema di Natale di Fermat)**

Sia  $p$  un numero primo tale che  $p \equiv 1 \pmod{4}$ . Allora  $p$  è somma di due quadrati in  $\mathbb{Z}$ .

*Dimostrazione.* Per il *Teorema 4.3*,  $p$  è riducibile in  $\mathbb{Z}[i]$ . In quanto riducibile in  $\mathbb{Z}[i]$ , per il *Lemma 4.1*,  $p$  è allora somma di due quadrati.  $\square$

**Teorema 4.5**

Sia  $p$  un numero primo tale che  $p \equiv -1 \pmod{4}$ . Allora  $p$  è irriducibile in  $\mathbb{Z}[i]$ .

*Dimostrazione.* Se  $p$  fosse riducibile in  $\mathbb{Z}[i]$ , per il *Teorema di Natale di Fermat* esisterebbero  $a$  e  $b$  in  $\mathbb{Z}$  tali che  $p = a^2 + b^2$ . Dal momento che  $p$  è dispari, possiamo supporre, senza perdita di generalità, che  $a$  sia pari e che  $b$  sia dispari. Pertanto  $a^2 \equiv 0 \pmod{4}$  e  $b^2 \equiv 1 \pmod{4}$ , dacché sono uno pari e l'altro dispari<sup>6</sup>. Tuttavia la congruenza  $a^2 + b^2 \equiv 1 \equiv -1 \pmod{4}$  non è mai soddisfatta,  $\neq$ . Pertanto  $p$  può essere solo irriducibile.  $\square$

**Osservazione.** Si osserva che  $2 = (1 + i)(1 - i)$ . Dal momento che  $\|1 + i\|^2 = \|1 - i\|^2 = 2 \neq 1$ , si deduce che nessuno dei due fattori è invertibile. Pertanto 2 non è irriducibile.

**Proposizione 4.6**

Gli unici primi  $p \in \mathbb{Z}$  irriducibili in  $\mathbb{Z}[i]$  sono i primi  $p$  tali che  $p \equiv -1 \pmod{4}$ .

*Dimostrazione.* Per l'osservazione precedente, 2 non è irriducibile in  $\mathbb{Z}[i]$ , così come i primi congrui a 1 in modulo 4, per il *Teorema 4.3*. Al contrario i primi  $p$  congrui a  $-1$  in modulo 4 sono irriducibili, per il *Teorema 4.5*, da cui la tesi.  $\square$

**Teorema 4.7**

$z \in \mathbb{Z}[i]$  è irriducibile se e solo se  $z$  è un associato di un  $k \in \mathbb{Z}$  tale che  $k \equiv -1 \pmod{4}$ , o se  $\|z\|^2$  è primo.

<sup>6</sup>Infatti,  $0^2 \equiv 0 \pmod{4}$ ,  $1^2 \equiv 1 \pmod{4}$ ,  $2^2 \equiv 4 \equiv 0 \pmod{4}$ ,  $3^2 \equiv 9 \equiv 1 \pmod{4}$ .

*Dimostrazione.* Si dimostrano le due implicazioni separatamente.

( $\implies$ ) Sia  $z \in \mathbb{Z}[i]$  irriducibile. Chiaramente  $z \mid z\bar{z} = g(z)$ . Dacché  $\mathbb{Z}$  è un UFD,  $g(z)$  può decomporre in un prodotto di primi  $q_1 q_2 \cdots q_n$ . Dal momento che  $\mathbb{Z}[i]$  è un PID, in quanto anello euclideo,  $z$  deve dividere uno dei primi della fattorizzazione di  $g(z)$ . Si assuma che tale primo sia  $q_i$ . Allora esiste un  $w \in \mathbb{Z}[i]$  tale che  $q_i = wz$ .

Se  $w \in \mathbb{Z}[i]^*$ , si deduce che  $z$  è un associato di  $q_i$ . Dal momento che  $z$  è irriducibile,  $q_i$ , che è suo associato, è a sua volta irriducibile. Allora, per la *Proposizione 4.6*,  $q_i \equiv -1 \pmod{4}$ .

Altrimenti, se  $w$  non è invertibile, si ha che  $g(w) > g(1)$ , ossia che  $\|w\|^2 > 1$ . Inoltre in quanto irriducibile, anche  $z$  non è invertibile, e quindi  $g(z) > g(1) \implies \|z\|^2 > 1$ . Dalla proprietà moltiplicativa del modulo si ricava  $q_i^2 = \|q_i\|^2 = \|w\|^2 \|z\|^2$ , da cui necessariamente consegue che:

$$\|w\|^2 = q_i, \quad \|z\|^2 = q_i,$$

attraverso cui si verifica l'implicazione.

( $\impliedby$ ) Se  $k \in \mathbb{Z}$  e  $k \equiv -1 \pmod{4}$ , per il *Teorema 4.5*,  $k$  è irriducibile. Allora in quanto suo associato, anche  $z$  è irriducibile.

Altrimenti, se  $\|z\|^2$  è un primo  $p$ , si ponga  $z = ab$  con  $a$  e  $b \in \mathbb{Z}[i]$ . Per la proprietà moltiplicativa del modulo,  $p = \|z\|^2 = \|ab\|^2 = \|a\|^2 \|b\|^2$ . Tuttavia questo implica che uno tra  $\|a\|^2$  e  $\|b\|^2$  sia pari a 1, ossia che uno tra  $a$  e  $b$  sia invertibile, dacché  $g(1) = 1$ . Pertanto  $z$  è in ogni caso irriducibile.  $\square$

Infine si enuncia un'ultima identità inerente all'aritmetica, ma strettamente collegata a  $\mathbb{Z}[i]$ .

## §4.2 L'identità di Brahmagupta-Fibonacci

### **Proposizione 4.8** (*Identità di Brahmagupta-Fibonacci*)

Il prodotto di due somme di quadrati è ancora una somma di quadrati. In particolare:

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2.$$

*Dimostrazione.* La dimostrazione altro non è che una banale verifica algebrica. Ciononostante è possibile risalire a questa identità in via alternativa mediante l'uso del modulo dei numeri complessi.

Siano  $z_1 = a + bi$ ,  $z_2 = c + di \in \mathbb{C}$ . Allora, per le proprietà del modulo dei numeri complessi:

$$\|z_1\| \|z_2\| = \|z_1 z_2\|. \tag{1}$$

Computando il prodotto tra  $z_1$  e  $z_2$  si ottiene:

$$z_1 z_2 = (ac - bd) + (ad + bc)i,$$



da cui a sua volta si ricava:

$$\|z_1 z_2\| = \sqrt{(ac - bd)^2 + (ad + bc)^2},$$

assieme a:

$$\|z_1\| = \sqrt{a^2 + b^2}, \quad \|z_2\| = \sqrt{c^2 + d^2}.$$

Infine, da (1), elevando al quadrato, si deduce l'identità presentata:

$$\sqrt{a^2 + b^2} \sqrt{c^2 + d^2} = \sqrt{(ac - bd)^2 + (ad + bc)^2} \implies (a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2.$$

□

#### Esempio 4.9

Si consideri  $65 = 5 \cdot 13$ . Dal momento che sia 5 che 13 sono congrui a 1 in modulo 4, sappiamo già si possono scrivere entrambi come somme di due quadrati. Allora, dall'*Identità di Brahmagupta-Fibonacci*, anche 65 è somma di due quadrati.

Infatti  $5 = 2^2 + 1^2$  e  $13 = 3^2 + 2^2$ . Pertanto  $65 = 5 \cdot 13 = (2 \cdot 3 - 1 \cdot 2)^2 + (2 \cdot 2 + 1 \cdot 3)^2 = 4^2 + 7^2$ .



## §5 Irriducibilità in $\mathbb{Z}[x]$ e in $\mathbb{Q}[x]$

### §5.1 Criterio di Eisenstein e proiezione in $\mathbb{Z}_p[x]$

Prima di studiare le irriducibilità in  $\mathbb{Z}$ , si guarda alle irriducibilità nei vari campi finiti  $\mathbb{Z}_p$ , con  $p$  primo. Questo metodo presenta un vantaggio da non sottovalutare: in  $\mathbb{Z}_p$  per ogni grado  $n$  esiste un numero finito di polinomi monici<sup>7</sup> – in particolare,  $p^n$  – e quindi per un polinomio di grado  $d$  è sufficiente controllare che questo non sia prodotto di tali polinomi monici per  $1 \leq n < d$ .

In modo preliminare, si definisce un omomorfismo fondamentale.

**Definizione 5.1.** Sia il seguente l'omomorfismo di proiezione da  $\mathbb{Z}$  in  $\mathbb{Z}_p$ :

$$\hat{\pi}_p : \mathbb{Z}[x] \rightarrow \mathbb{Z}_p[x], \quad a_n x^n + \dots + a_0 \mapsto [a_n]_p x^n + \dots + [a_0]_p.$$

**Osservazione.** Si dimostra facilmente che  $\hat{\pi}$  è un omomorfismo di anelli. Innanzitutto,  $\hat{\pi}(1) = [1]_p$ . Vale chiaramente la linearità:

$$\begin{aligned} \hat{\pi}_p(a_n x^n + \dots + a_0) + \hat{\pi}_p(b_n x^n + \dots + b_0) &= [a_n]_p x^n + \dots + [a_0]_p + [b_n]_p x^n + \dots + [b_0]_p = \\ &= [a_n + b_n]_p x^n + \dots = \hat{\pi}_p(a_n x^n + \dots + a_0 + b_n x^n + \dots + b_0). \end{aligned}$$

Infine vale anche la moltiplicatività:

$$\begin{aligned} \hat{\pi}_p(a_n x^n + \dots + a_0) \hat{\pi}_p(b_n x^n + \dots + b_0) &= ([a_n]_p x^n + \dots)([b_n]_p x^n + \dots) = \\ &= \sum_{i=0}^n \sum_{j+k=i} [a_j]_p [b_k]_p x^i = \sum_{i=0}^n \sum_{j+k=i} [a_j b_k]_p x^i = \hat{\pi}_p \left( \sum_{i=0}^n \sum_{j+k=i} a_j b_k x^i \right) = \\ &= \hat{\pi}_p((a_n x^n + \dots + a_0)(b_n x^n + \dots + b_0)). \end{aligned}$$

Prima di enunciare un teorema che si rivelerà importante nel determinare l'irriducibilità di un polinomio in  $\mathbb{Z}[x]$ , si enuncia una definizione che verrà ripresa anche in seguito

**Definizione 5.2.** Un polinomio  $a_n x^n + \dots + a_0 \in \mathbb{Z}[x]$  si dice **primitivo** se  $\text{MCD}(a_n, \dots, a_0) = 1$ .

#### Teorema 5.3

Sia  $p$  un primo. Sia  $f(x) = a_n x^n + \dots \in \mathbb{Z}[x]$  primitivo. Se  $p \nmid a_n$  e  $\hat{\pi}_p(f(x))$  è irriducibile in  $\mathbb{Z}_p[x]$ , allora anche  $f(x)$  lo è in  $\mathbb{Z}[x]$ .

*Dimostrazione.* Si dimostra la tesi contronominale. Sia  $f(x) = a_n x^n + \dots \in \mathbb{Z}[x]$  primitivo e riducibile, con  $p \nmid a_n$ . Dal momento che  $f(x)$  è riducibile, esistono  $g(x), h(x)$  non invertibili tali che  $f(x) = g(x)h(x)$ .

<sup>7</sup>Si prendono in considerazione solo i polinomi monici dal momento che vale l'equivalenza degli associati: se  $a$  divide  $b$ , allora tutti gli associati di  $a$  dividono  $b$ .  $\mathbb{Z}_p$  è infatti un campo, e quindi  $\mathbb{Z}_p[x]$  è un anello euclideo.

Si dimostra che  $\deg g(x) \geq 1$ . Se infatti fosse nullo,  $g(x)$  dovrebbe o essere uguale a  $\pm 1$  – assurdo, dal momento che  $g(x)$  non è invertibile,  $\neq$  – o essere una costante non invertibile. Tuttavia, nell'ultimo caso, risulterebbe che  $f(x)$  non è primitivo, poiché  $g(x)$  dividerebbe ogni coefficiente del polinomio. Analogamente anche  $\deg h(x) \geq 1$ .

Si consideri ora  $\hat{\pi}_p(f(x)) = \hat{\pi}_p(g(x))\hat{\pi}_p(h(x))$ . Dal momento che  $p \nmid a_n$ , il grado di  $f(x)$  rimane costante sotto l'operazione di omomorfismo, ossia  $\deg \hat{\pi}_p(f(x)) = \deg f(x)$ .

Inoltre, poiché nessuno dei fattori di  $f(x)$  è nullo,  $\deg f(x) = \deg g(x) + \deg h(x)$ . Da questa considerazione si deduce che anche i gradi di  $g(x)$  e  $h(x)$  non devono calare, altrimenti si avrebbe che  $\deg \hat{\pi}_p(f(x)) < \deg f(x)$ ,  $\neq$ . Allora  $\deg \hat{\pi}_p(g(x)) = \deg g(x) \geq 1$ ,  $\deg \hat{\pi}_p(h(x)) = \deg h(x) \geq 1$ .

Poiché  $\deg \hat{\pi}_p(g(x))$  e  $\deg \hat{\pi}_p(h(x))$  sono dunque entrambi non nulli,  $\hat{\pi}_p(g(x))$  e  $\hat{\pi}_p(h(x))$  non sono invertibili<sup>8</sup>. Quindi  $f(x)$  è prodotto di non invertibili, ed è dunque riducibile.  $\square$

#### **Teorema 5.4** (Criterio di Eisenstein)

Sia  $p$  un primo. Sia  $f(x) = a_n x^n + \dots + a_0 \in \mathbb{Z}[x]$  primitivo tale che:

- (1)  $p \nmid a_n$ ,
- (2)  $p \mid a_i, \forall i \neq n$ ,
- (3)  $p^2 \nmid a_0$ .

Allora  $f(x)$  è irriducibile in  $\mathbb{Z}[x]$ .

*Dimostrazione.* Si ponga  $f(x)$  riducibile e sia pertanto  $f(x) = g(x)h(x)$  con  $g(x)$  e  $h(x)$  non invertibili. Analogamente a come visto per il *Teorema 5.3*, si desume che  $\deg g(x)$ ,  $\deg h(x) \geq 1$ .

Si applica l'omomorfismo di proiezione in  $\mathbb{Z}_p[x]$ :

$$\hat{\pi}_p(f(x)) = \underbrace{[a_n]_p}_{\neq 0} x^n,$$

da cui si deduce che  $\deg \hat{\pi}_p(f(x)) = \deg f(x)$ .

Dal momento che  $\hat{\pi}_p(f(x)) = \hat{\pi}_p(g(x))\hat{\pi}_p(h(x))$  e che  $\mathbb{Z}_p[x]$ , in quanto campo, è un dominio, necessariamente sia  $\hat{\pi}_p(g(x))$  che  $\hat{\pi}_p(h(x))$  sono dei monomi.

Inoltre, sempre in modo analogo a come visto per il *Teorema 5.3*, sia  $\deg \hat{\pi}_p(g(x))$  che  $\deg \hat{\pi}_p(h(x))$  sono maggiori o uguali ad 1.

Combinando questo risultato col fatto che questi due fattori sono monomi, si desume che  $\hat{\pi}_p(g(x))$  e  $\hat{\pi}_p(h(x))$  sono monomi di grado positivo. Quindi  $p$  deve dividere entrambi i

<sup>8</sup>Si ricorda che  $\mathbb{Z}_p[x]$  è un anello euclideo. Pertanto, non avere lo stesso grado dell'unità equivale a non essere invertibili.

termini noti di  $g(x)$  e  $h(x)$ , e in particolare  $p^2$  deve dividere il loro prodotto, ossia  $a_0$ . Tuttavia questo è un assurdo,  $\neq$ .  $\square$

**Osservazione.** Si consideri  $x^k - 2$ , per  $k \geq 1$ . Per il *Criterio di Eisenstein*, considerando come primo  $p = 2$ , si verifica che  $x^k - 2$  è sempre irriducibile. Pertanto, per ogni grado di un polinomio esiste almeno un irriducibile – a differenza di come invece avviene in  $\mathbb{R}[x]$  o in  $\mathbb{C}[x]$ .

### Teorema 5.5

Sia  $f(x) \in \mathbb{Z}[x]$  primitivo e sia  $a \in \mathbb{Z}$ . Allora  $f(x)$  è irriducibile se e solo se  $f(x + a)$  è irriducibile.

*Dimostrazione.* Si dimostra una sola implicazione, dal momento che l'implicazione contraria consegue dalle stesse considerazioni poste studiando prima  $f(x + a)$  e poi  $f(x)$ .

Sia  $f(x) = a(x)b(x)$  riducibile, con  $a(x), b(x) \in \mathbb{Z}[x]$  non invertibili. Come già visto per il *Teorema 5.3*,  $\deg a(x), \deg b(x) \geq 1$ .

Allora chiaramente  $f(x + a) = g(x + a)h(x + a)$ , con  $\deg g(x + a) = \deg g(x) \geq 1$ ,  $\deg h(x + a) = \deg h(x) \geq 1$ . Pertanto  $f(x + a)$  continua a essere riducibile, da cui la tesi.  $\square$

### Esempio 5.6

Si consideri  $f(x) = x^{p-1} + \dots + x^2 + x + 1 \in \mathbb{Z}[x]$ , dove tutti i coefficienti del polinomio sono 1. Si verifica che:

$$f(x + 1) = \frac{(x + 1)^p - 1}{x} = p + \binom{p}{2}x + \dots + x^{p-1}.$$

Allora, per il *Criterio di Eisenstein* con  $p$ ,  $f(x + 1)$  è irriducibile. Pertanto anche  $f(x)$  lo è.

## §5.2 Alcuni irriducibili di $\mathbb{Z}_2[x]$

Tra tutti gli anelli  $\mathbb{Z}_p[x]$ ,  $\mathbb{Z}_2[x]$  ricopre sicuramente un ruolo fondamentale, dal momento che è il meno costoso computazionalmente da analizzare, dacché  $\mathbb{Z}_2$  consta di soli due elementi. Pertanto si computano adesso gli irriducibili di  $\mathbb{Z}_2[x]$  fino al quarto grado incluso, a meno di associati.

Sicuramente  $x$  e  $x + 1$  sono irriducibili, dal momento che sono di primo grado. I polinomi di secondo grado devono dunque essere prodotto di questi polinomi, e pertanto devono avere 0 o 1 come radice: si verifica quindi che  $x^2 + x + 1$  è l'unico polinomio di secondo grado irriducibile.

Per il terzo grado vale ancora lo stesso principio, per cui  $x^3 + x^2 + 1$  e  $x^3 + x + 1$  sono gli unici irriducibili di tale grado. Infine, per il quarto grado, i polinomi riducibili soddisfano una qualsiasi delle seguenti proprietà:

- 0 e 1 sono radici del polinomio,
- il polinomio è prodotto di due polinomi irriducibili di secondo grado.

Si escludono pertanto dagli irriducibili i polinomi non omogenei – che hanno sicuramente 0 come radice –, e i polinomi con 1 come radice, ossia  $x^4 + x^3 + x + 1$ ,  $x^4 + x^3 + x^2 + 1$ , e  $x^4 + x^2 + x + 1$ . Si esclude anche  $(x^2 + x + 1)^2 = x^4 + x^2 + 1$ . Pertanto gli unici irriducibili di grado quattro sono  $x^4 + x^3 + x^2 + x + 1$ ,  $x^4 + x^3 + 1$ ,  $x^4 + x + 1$ .

Tutti questi irriducibili sono raccolti nella seguente tabella:

- (grado 1)  $x$ ,  $x + 1$ ,
- (grado 2)  $x^2 + x + 1$ ,
- (grado 3)  $x^3 + x^2 + 1$ ,  $x^3 + x + 1$ ,
- (grado 4)  $x^4 + x^3 + x^2 + x + 1$ ,  $x^4 + x^3 + 1$ ,  $x^4 + x + 1$ .

### Esempio 5.7

Il polinomio  $51x^3 + 11x^2 + 1 \in \mathbb{Z}[x]$  è primitivo dal momento che  $\text{MCD}(51, 11, 1) = 1$ . Inoltre, poiché  $\hat{\pi}_2(51x^3 + 11x^2 + 1) = x^3 + x + 1$  è irriducibile, si deduce che anche  $51x^3 + 11x^2 + 1$  lo è per il *Teorema 5.3*.

## §5.3 Teorema delle radici razionali e lemma di Gauss

Si enunciano in questa sezione i teoremi più importanti per lo studio dell'irriducibilità dei polinomi in  $\mathbb{Q}[x]$  e in  $\mathbb{Z}[x]$ , a partire dai due teoremi più importanti: il classico *Teorema delle radici razionali* e il *Lemma di Gauss*, che si pone da ponte tra l'analisi dell'irriducibilità in  $\mathbb{Z}[x]$  e quella in  $\mathbb{Q}[x]$ .

### Teorema 5.8 (Teorema delle radici razionali)

Sia  $f(x) = a_n x^n + \dots + a_0 \in \mathbb{Z}[x]$ . Abbia  $f(x)$  una radice razionale. Allora, detta tale radice  $\frac{p}{q}$ , già ridotta ai minimi termini, questa è tale che:

- (i.)  $p \mid a_0$ ,
- (ii.)  $q \mid a_n$ .

*Dimostrazione.* Poiché  $\frac{p}{q}$  è radice,  $f\left(\frac{p}{q}\right) = 0$ , e quindi si ricava che:

$$a_n \left(\frac{p}{q}\right)^n + \dots + a_0 = 0 \implies a_n p^n = -q(\dots + a_0 q^{n-1}).$$

Quindi  $q \mid a_n p^n$ . Dal momento che  $\text{MCD}(p, q) = 1$ , si deduce che  $q \mid a_n$ .

Analogamente si ricava che:

$$a_0 q^n = -p(a_n p^{n-1} + \dots).$$

Pertanto, per lo stesso motivo espresso in precedenza,  $p \mid a_0$ , da cui la tesi.  $\square$

**Teorema 5.9** (*Lemma di Gauss*)

Il prodotto di due polinomi primitivi in  $\mathbb{Z}[x]$  è anch'esso primitivo.

*Dimostrazione.* Siano  $g(x) = a_mx^m + \dots + a_0$  e  $h(x) = b_nx^n + \dots + b_0$  due polinomi primitivi in  $\mathbb{Z}[x]$ . Si assuma che  $f(x) = g(x)h(x)$  non sia primitivo. Allora esiste un  $p$  primo che divide tutti i coefficienti di  $f(x)$ .

Siano  $a_s$  e  $b_t$  i più piccoli coefficienti non divisibili da  $p$  dei rispettivi polinomi. Questi sicuramente esistono, altrimenti  $p$  dividerebbe tutti i coefficienti, e quindi o  $g(x)$  o  $h(x)$  non sarebbe primitivo,  $\neq$ .

Si consideri il coefficiente di  $x^{s+t}$  di  $f(x)$ :

$$c_{s+t} = \sum_{j+k=s+t} a_j b_k = \underbrace{a_0 b_{s+t} + a_1 b_{s+t-1} + \dots + a_s b_t}_{\equiv 0 \pmod{p}} + \underbrace{a_{s+1} b_{t-1} + \dots}_{\equiv 0 \pmod{p}},$$

dal momento che  $p \mid c_{s+t}$ , si deduce che  $p$  deve dividere anche  $a_s b_t$ , ossia uno tra  $a_s$  e  $b_t$ , che è assurdo,  $\neq$ . Quindi  $f(x)$  è primitivo.  $\square$

**Teorema 5.10** (*Secondo lemma di Gauss*)

Sia  $f(x) \in \mathbb{Z}[x]$ . Allora  $f(x)$  è irriducibile in  $\mathbb{Z}[x]$  se e solo se  $f(x)$  è irriducibile in  $\mathbb{Q}[x]$  ed è primitivo.

*Dimostrazione.* Si dimostrano le due implicazioni separatamente.

( $\implies$ ) Si dimostra l'implicazione contronominale, ossia mostrando che se  $f(x)$  non è primitivo o se è riducibile in  $\mathbb{Q}[x]$ , allora  $f(x)$  è riducibile in  $\mathbb{Z}[x]$ .

Se  $f(x)$  non è primitivo, allora  $f(x)$  è riducibile in  $\mathbb{Z}[x]$ . Sia quindi  $f(x)$  primitivo e riducibile in  $\mathbb{Q}[x]$ , con  $f(x) = g(x)h(x)$ ,  $g(x), h(x) \in \mathbb{Q}[x] \setminus \mathbb{Q}[x]^*$ .

Si descrivano  $g(x)$  e  $h(x)$  nel seguente modo:

$$g(x) = \frac{p_m}{q_m} x^m + \dots + \frac{p_0}{q_0}, \quad \text{MCD}(p_i, q_i) = 1 \quad \forall 0 \leq i \leq m,$$

$$h(x) = \frac{s_n}{t_n} x^n + \dots + \frac{s_0}{t_0}, \quad \text{MCD}(s_i, t_i) = 1 \quad \forall 0 \leq i \leq n.$$

Si definiscano inoltre le seguenti costanti:

$$\alpha = \frac{\text{mcm}(q_m, \dots, q_0)}{\text{MCD}(p_m, \dots, p_0)}, \quad \beta = \frac{\text{mcm}(t_n, \dots, t_0)}{\text{MCD}(s_n, \dots, s_0)}.$$

Si verifica che sia  $\hat{g}(x) = \alpha g(x)$  che  $\hat{h}(x) = \beta h(x)$  appartengono a  $\mathbb{Z}[x]$  e che entrambi sono primitivi. Pertanto  $\hat{g}(x)\hat{h}(x) \in \mathbb{Z}[x]$ .

Si descriva  $f(x)$  nel seguente modo:

$$f(x) = a_k x^k + \dots + a_0, \quad \text{MCD}(a_k, \dots, a_0) = 1.$$

Sia  $\alpha\beta = \frac{p}{q}$  con  $\text{MCD}(p, q) = 1$ , allora:

$$\hat{g}(x)\hat{h}(x) = \alpha\beta f(x) = \frac{p}{q}(a_k x^k + \dots + a_0),$$

da cui, per far sì che  $\hat{g}(x)\hat{h}(x)$  appartenga a  $\mathbb{Z}[x]$ ,  $q$  deve necessariamente dividere tutti i coefficienti di  $f(x)$ . Tuttavia  $f(x)$  è primitivo, e quindi  $q = \pm 1$ . Pertanto  $\alpha\beta = \pm p \in \mathbb{Z}$ .

Infine, per il *Lemma di Gauss*,  $\alpha\beta f(x)$  è primitivo, da cui  $\alpha\beta = \pm 1$ . Quindi  $f(x) = \pm \hat{g}(x)\hat{h}(x)$  è riducibile.

( $\Leftarrow$ ) Se  $f(x)$  è irriducibile in  $\mathbb{Q}[x]$  ed è primitivo, sicuramente  $f(x)$  è irriducibile anche in  $\mathbb{Z}[x]$ . Infatti, se esiste una fattorizzazione in irriducibili in  $\mathbb{Z}[x]$ , essa non include alcuna costante moltiplicativa dal momento che  $f(x)$  è primitivo, e quindi esisterebbe una fattorizzazione in irriducibili anche in  $\mathbb{Q}[x]$ .  $\square$





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

### §6.1 Elementi preliminari

Prima di procedere ad enunciare le proprietà più rilevanti dell'anello dei polinomi  $\mathbb{K}[x]$ , si ricorda che esso è un **anello euclideo** in cui la funzione grado coincide con il grado del polinomio, ossia  $g = \deg$ . Si enuncia ora invece la definizione di radice.

**Definizione 6.1.** Si dice che  $\alpha \in \mathbb{K}$  è una **radice** del polinomio  $f(x) \in \mathbb{K}[x]$  se  $f(\alpha) = 0$ .

#### Proposizione 6.2

Se  $\alpha \in \mathbb{K}$  è una radice di  $f(x) \in \mathbb{K}[x]$ , allora  $(x - \alpha)$  divide  $f(x)$ .

*Dimostrazione.* Dal momento che  $\mathbb{K}[x]$  è un anello euclideo, si può eseguire la divisione euclidea tra  $f(x)$  e  $(x - \alpha)$ , ossia esistono  $q(x), r(x) \in \mathbb{K}[x]$  tali che  $f(x) = q(x)(x - \alpha) + r(x)$  con  $\deg r(x) < \deg(x - \alpha)$  o con  $r(x) = 0$ .

Se  $r(x) \neq 0$ , poiché  $\deg r(x) < \deg(x - \alpha)$ , si deduce che  $\deg r(x) = 0$ , ossia che  $r(x)$  è un invertibile. In entrambi i casi,  $r(x)$  è comunque una costante. Pertanto, valutando il polinomio in  $\alpha$ , si ricava:

$$0 = f(\alpha) = \underbrace{q(\alpha)(\alpha - \alpha)}_{=0} + r(\alpha),$$

da cui  $r(\alpha) = 0$ . Quindi  $f(x) = q(x)(x - \alpha)$ , e si verifica la tesi.  $\square$

#### Teorema 6.3

Sia  $f(x) \in \mathbb{K}[x]$  di grado  $n$ . Allora  $f(x)$  ha al più  $n$  radici.

*Dimostrazione.* Se  $n$  è nullo, allora  $f(x)$  è una costante non nulla, e quindi non ammette radici, in accordo alla tesi.

Sia allora  $n \geq 1$ . Se  $f(x)$  non ha radici in  $\mathbb{K}$ , allora la tesi è ancora soddisfatta. Altrimenti sia  $\zeta_1$  una radice di  $f(x)$ . Si divida  $f(x)$  per  $(x - \zeta_1)$  e se ne prende il quoziente  $q_1(x)$ , mentre si ignori il resto, che, per la *Proposizione 6.2*, è nullo.

Si reiteri il procedimento utilizzando  $q_1(x)$  al posto di  $f(x)$  fino a quando il grado del quoziente non è nullo o il quoziente non ammette radici in  $\mathbb{K}$ , e si chiami quest'ultimo quoziente  $\lambda(x)$ . Infatti, poiché i gradi dei quozienti diminuiscono di 1 ad ogni iterazione, è garantito che l'algoritmo termini al più dopo  $n$  iterazioni.

In questo modo, numerando le radici, si può scrivere  $f(x)$  come:

$$f(x) = \alpha(x - \zeta_1)(x - \zeta_2) \cdots (x - \zeta_k)\lambda(x). \quad (2)$$

Si osserva che  $x - \zeta_i$  è irriducibile  $\forall 1 \leq i \leq k$ . Se  $f(x)$  ammettesse un'altra fattorizzazione in cui compaia un fattore  $x - \alpha$  con  $\alpha \neq \zeta_i \forall 1 \leq i \leq k$ , allora  $f(x)$  ammetterebbe due fattorizzazioni in irriducibili, dacché  $x - \alpha$  non sarebbe un associato di nessuno dei  $x - \zeta_i$ ,

né tantomeno di un irriducibile  $\lambda(x)$ .

Se infatti  $x - \alpha$  fosse un associato di un irriducibile  $\lambda(x)$ ,  $x - \alpha$  dividerebbe  $\lambda(x)$ , e quindi  $\lambda(x)$  ammetterebbe  $\alpha$  come radice. Se  $\lambda(x)$  è una costante, questo è a priori assurdo,  $\neq$ . Se invece  $\lambda(x)$  non è una costante, il fatto che ammetta una radice contraddirebbe il funzionamento dell'algoritmo di fattorizzazione espresso in precedenza,  $\neq$ . Quindi  $x - \alpha$  non è associato di nessun irriducibile di  $\lambda(x)$ .

Allora il fatto che  $f(x)$  ammetta due fattorizzazioni in irriducibili è assurdo, dacché  $\mathbb{K}[x]$  è un anello euclideo, e quindi un UFD,  $\neq$ . Quindi le radici sono esattamente  $k \leq n$ , da cui la tesi.  $\square$

## §6.2 Sottogruppi moltiplicativi finiti di $\mathbb{K}$

Si illustra adesso un teorema che riguarda i sottogruppi moltiplicativi finiti di  $\mathbb{K}$ , da cui consegnerà, per esempio, che  $\mathbb{Z}_p^*$  è sempre ciclico, per qualsiasi  $p$  primo.

### Lemma 6.4

Per ogni  $n \in \mathbb{N}$  vale la seguente identità:

$$n = \sum_{d|n} \varphi(d).$$

*Dimostrazione.* Si consideri il gruppo ciclico  $\mathbb{Z}_n$  per  $n \in \mathbb{N}$ . Si osserva che  $|\mathbb{Z}_n| = n$ .

Si definisca  $X_d$  come l'insieme degli elementi di  $G$  di ordine  $d$ . Dal momento che ogni elemento appartiene a uno e uno solo di questi  $X_d$ , per ogni divisore  $d$  di  $n$ , allora si può partizionare  $G$  nel seguente modo:

$$G = \bigcup_{d|n} X_d.$$

Dal momento che  $\mathbb{Z}_n$  è ciclico, ogni  $X_d$  ha esattamente  $\varphi(d)$  elementi, e dunque si deduce che:

$$n = |G| = \sum_{d|n} |X_d| = \sum_{d|n} \varphi(d),$$

ossia la tesi.  $\square$

### Teorema 6.5

Un sottogruppo moltiplicativo finito di un campo  $\mathbb{K}$  è sempre ciclico.

*Dimostrazione.* Sia  $G$  un sottogruppo finito di un campo  $\mathbb{K}$  definito sulla sua operazione di moltiplicazione, e sia  $|G| = n$ .

Si definisca  $X_d$  come l'insieme degli elementi di  $G$  di ordine  $d$ . Dal momento che ogni elemento appartiene a uno e uno solo di questi  $X_d$ , per ogni divisore  $d$  di  $n$ , allora si può partizionare  $G$  nel seguente modo:

$$G = \bigcup_{d|n} X_d,$$

da cui:

$$n = |G| = \sum_{d|n} |X_d|. \quad (3)$$

Dal *Lemma 6.4* e da (3), si ricava infine la seguente equazione:

$$\sum_{d|n} |X_d| = n = \sum_{d|n} \varphi(d). \quad (4)$$

Adesso vi sono due casi: o  $|X_n| > 0$  o  $|X_n| = 0$ .

Nel primo caso si concluderebbe che esiste almeno un elemento in  $G$  di ordine  $n$ , e quindi che esiste un generatore con cui  $G$  è ciclico, ossia la tesi.

Nel secondo caso si dimostra un assurdo. Dal momento che  $|X_n| = 0$ , esiste sicuramente un divisore proprio  $d$  di  $n$  tale che  $|X_d| > \varphi(d)$ . Altrimenti, se  $|X_d| \leq \varphi(d)$  per ogni divisore  $d$ , si ricaverebbe la seguente disuguaglianza:

$$\sum_{\substack{d|n \\ d \neq n}} |X_d| \leq \sum_{\substack{d|n \\ d \neq n}} \varphi(d) \implies \sum_{d|n} |X_d| \stackrel{|X_n|=0}{=} \sum_{\substack{d|n \\ d \neq n}} |X_d| \leq \sum_{\substack{d|n \\ d \neq n}} \varphi(d) \stackrel{\varphi(n) \geq 1}{<} \sum_{d|n} \varphi(d).$$

Tuttavia questo è un assurdo, dal momento che per (4) deve valere l'uguaglianza,  $\neq$ .

Sia  $g \in X_d$  e si consideri  $\langle g \rangle$ , il sottogruppo generato da  $g$ . Vale in particolare che  $|\langle g \rangle| = d$ .

Si consideri adesso il polinomio  $f(x) = x^d - 1 \in \mathbb{K}[x]$ . Tutti e  $d$  gli elementi di  $\langle g \rangle$  sono già soluzione di  $f(x)$ . Tuttavia, poiché  $|X_d| > \varphi(d)$ , esiste sicuramente un elemento  $h$  in  $X_d$  che non appartiene a  $\langle g \rangle$ . Infatti se tutti gli elementi di  $X_d$  appartenessero a  $\langle g \rangle$  vi sarebbero più di  $\varphi(d)$  generatori,  $\neq$ .

Infine, poiché  $h \in X_d$ , anch'esso è soluzione di  $f(x)$ . Questo è però un assurdo, poiché, per il *Teorema 6.3*,  $f(x)$  ammette al più  $d$  radici, mentre così ne avrebbe almeno  $d+1$ ,  $\neq$ .

Quindi  $|X_d| > 0$ , e  $G$  è ciclico. □

### §6.3 Il quoziente $\mathbb{K}[x]/(f(x))$

Nell'ambito dello studio delle radici di un polinomio, il quoziente  $\mathbb{K}[x]/(f(x))$  gioca un ruolo fondamentale. Infatti, come vedremo in seguito, se  $f(x)$  è irriducibile, questo diventa un campo, e, soprattutto, ammette sempre una radice per  $f(x)$ .

In realtà, il quoziente  $\mathbb{K}[x]/(f(x))$  si comporta pressoché allo stesso modo dei più familiari  $\mathbb{Z}/n\mathbb{Z}$ . Infatti le principali regole dell'aritmetica modulare potrebbero essere estese anche a tale quoziente, senza particolari sacrifici.

Si enuncia adesso un teorema importante, che è equivalente – anche nella dimostrazione – all'analogo per i campi  $\mathbb{Z}/p\mathbb{Z}$ .

### Teorema 6.6

$\mathbb{K}[x]/(f(x))$  è un campo se e solo se  $f(x)$  è irriducibile.

*Dimostrazione.* Si dimostrano le due implicazioni separatamente.

( $\implies$ ) Sia  $f(x) \in \mathbb{K}[x]$  irriducibile. Affinché l'anello commutativo  $\mathbb{K}[x]/(f(x))$  sia un campo è sufficiente dimostrare che ogni suo elemento non nullo ammette un inverso moltiplicativo.

Sia  $\alpha(x) + (f(x)) \in \mathbb{K}[x]/(f(x))$  non nullo. Allora  $\alpha(x)$  non è divisibile da  $f(x)$ , e pertanto  $\text{MCD}(\alpha(x), f(x)) = 1$ <sup>9</sup>.

Allora, per l'*Identità di Bézout*, esistono  $\beta(x), \lambda(x) \in \mathbb{K}[x]$  tali che:

$$\alpha(x)\beta(x) + \lambda(x)f(x) = 1.$$

Dacché  $\alpha(x)\beta(x) - 1 \in (f(x))$ , si deduce che  $\alpha(x)\beta(x) + (f(x)) = 1 + (f(x))$ , e quindi  $\beta(x) + (f(x))$  è l'inverso moltiplicativo di  $\alpha(x) + (f(x))$ , da cui la dimostrazione dell'implicazione.

( $\impliedby$ ) Si dimostra l'implicazione contronominale. Sia  $f(x) \in \mathbb{K}[x]$  riducibile. Allora esistono  $\alpha(x)$  e  $\beta(x)$  non invertibili tali che  $f(x) = \alpha(x)\beta(x)$ , da cui si ricava che:

$$[\alpha(x) + (f(x))][\beta(x) + (f(x))] = f(x) + (f(x)) = 0 + (f(x)),$$

ossia l'identità di  $\mathbb{K}[x]/(f(x))$ .

Tuttavia, se  $\mathbb{K}[x]/(f(x))$  fosse un campo, e quindi un dominio, ciò non sarebbe ammissibile, dacché non potrebbero esservi divisori di zero. Quindi  $\mathbb{K}[x]/(f(x))$  non è un campo.  $\square$

**Osservazione.** Una notazione per indicare un elemento di  $\mathbb{K}[x]/(f(x))$  alternativa e più sintetica di  $a + (f(x))$  è  $\bar{a}$ , qualora sia noto nel contesto a quale  $f(x)$  si fa riferimento.

### Proposizione 6.7

Nell'anello  $\mathbb{K}[x]/(f(x))$  esiste sempre una radice di  $f(x)$ , convertendo opportunamente i coefficienti da  $\mathbb{K}$  a  $\mathbb{K}[x]/(f(x))$ .

*Dimostrazione.* Sia  $\bar{x} = x + (f(x)) \in \mathbb{K}[x]/(f(x))$  e si descriva  $f(x)$  come:

$$f(x) = a_n x^n + \dots + a_0.$$

<sup>9</sup>Si ricorda che in un PID la nozione di *massimo comun divisore* (MCD) è più ambigua di quella di  $\mathbb{Z}$ . Infatti  $\text{MCD}(a, b)$  comprende tutti i generatori dell'ideale  $(a, b)$ , e quindi tutti i suoi associati. Pertanto si dirà  $\text{MCD}(a, b)$  uno qualsiasi di questi associati, e nel nostro caso 1 è un buon valore, dacché l'MCD deve essere un associato di un'unità.

Allora, computando  $f(x)$  in  $\bar{x}$  e convertendone i coefficienti, si ricava che:

$$f(\bar{x}) = \overline{a_n} \bar{x}^n + \dots + \overline{a_0} = \overline{a_n x^n + \dots + a_0} = \overline{f(x)} = \bar{0}.$$

Quindi  $\bar{x}$  è una radice di  $f(x)$ , da cui la tesi.

□



## §7 Estensioni algebriche di $\mathbb{K}$

### §7.1 Morfismi di valutazione, elementi algebrici e trascendenti

Si definisce adesso il concetto di *omomorfismo di valutazione*, che impiegheremo successivamente nello studio dei quozienti  $\mathbb{K}[x]/(f(x))$  e dei cosiddetti *elementi algebrici* (o *trascendenti*).

**Definizione 7.1.** Sia  $B$  un anello commutativo, e sia  $A \subseteq B$  un suo sottoanello. Si definisce **omomorfismo di valutazione** di  $\alpha \in B$  in  $A$  l'omomorfismo:

$$\varphi_\alpha : A[x] \rightarrow B, f(x) \mapsto f(\alpha).$$

**Osservazione.** L'omomorfismo di valutazione è effettivamente un omomorfismo di anelli. Innanzitutto  $\varphi_\alpha(1) = 1$ . Inoltre vale la linearità:

$$\begin{aligned} \varphi_\alpha(f(x)) + \varphi_\alpha(g(x)) &= f(\alpha) + g(\alpha) = (f + g)(\alpha) = \varphi_\alpha((f + g)(x)) = \\ &= \varphi_\alpha(f(x) + g(x)), \end{aligned}$$

così come la moltiplicatività:

$$\varphi_\alpha(f(x))\varphi_\alpha(g(x)) = f(\alpha)g(\alpha) = (fg)(\alpha) = \varphi_\alpha((fg)(x)) = \varphi_\alpha(f(x)g(x)).$$

Si evidenziano adesso le principali proprietà di tale omomorfismo.

#### Proposizione 7.2

$$\text{Imm } \varphi_\alpha = A[\alpha]$$

*Dimostrazione.* Sicuramente  $\text{Imm } \varphi_\alpha \subseteq A[\alpha]$ , dacché ogni immagine di  $\varphi_\alpha$  è una valutazione di un polinomio a coefficienti in  $A$  in  $\alpha$ .

Sia dunque  $a = a_n\alpha^n + \dots + a_0 \in A[\alpha]$ . Allora  $\varphi_\alpha(a_nx^n + \dots + a_0) = a$ . Pertanto  $a \in \text{Imm } \varphi_\alpha$ , da cui  $A[\alpha] \subseteq \text{Imm } \varphi_\alpha$ .

Poiché vale la doppia inclusione, si desume che  $\text{Imm } \varphi_\alpha = A[\alpha]$ . □

Prima di applicare il *Primo teorema d'isomorfismo*, si distinguono due importanti casi, sui quali si baseranno le definizioni di *elemento algebrico* e di *elemento trascendente*.

**Definizione 7.3.** Sia  $\alpha \in B$ . Se  $\text{Ker } \varphi_\alpha = (0)$ , allora si dice che  $\alpha$  è un **elemento trascendente** di  $B$  su  $A$ .

**Osservazione.** Equivalentemente, se  $\alpha \in B$  è trascendente su  $A$ , significa che non vi è alcun polinomio non nullo in  $A[x]$  che ha  $\alpha$  come soluzione.



**Esempio 7.4**

Per esempio, il numero di Nepero-Eulero  $e$  è trascendente su  $\mathbb{Q}[x]$ <sup>a</sup>. Quindi  $\text{Ker } \varphi_e = (0)$ , e dunque, dal *Primo teorema di isomorfismo*, vale che:

$$\mathbb{Q}[x] \cong \mathbb{Q}[x]/(0) \cong \mathbb{Q}[e].$$

<sup>a</sup>Per una dimostrazione di questo fatto, si guardi a [H, pp. 234-237]

Possiamo generalizzare questo esempio nel seguente teorema.

**Teorema 7.5**

Sia  $B$  un campo e sia  $A \subseteq B$  un suo sottoanello. Se  $\alpha \in B$  è trascendente su  $A$ , allora vale la seguente relazione:

$$A[x] \cong A[\alpha].$$

*Dimostrazione.* Si consideri l'omomorfismo  $\varphi_\alpha$ . Dacché  $\alpha$  è trascendente,  $\text{Ker } \varphi_\alpha = (0)$ . Allora, combinando il *Primo teorema di isomorfismo* con la *Proposizione 7.2*, si ottiene proprio  $A[x] \cong A[x]/(0) \cong A[\alpha]$ , ossia la tesi.  $\square$

**Definizione 7.6.** Sia  $\alpha \in B$ . Se  $\text{Ker } \varphi_\alpha \neq (0)$ , allora si dice che  $\alpha$  è un **elemento algebrico** di  $B$  su  $A$ , mentre il generatore monico<sup>a</sup> non nullo di  $\text{Ker } \varphi_\alpha$  si dice **polinomio minimo** di  $\alpha$  su  $A$ . Il grado di tale polinomio minimo è detto **grado di  $\alpha$** .

<sup>a</sup>Vi potrebbero essere infatti più generatori di  $\text{Ker } \varphi_\alpha$ , sebbene tutti associati tra loro. L'attributo *monico* garantisce così l'unicità del polinomio minimo.

**Osservazione.** Equivalentemente, se  $\alpha \in B$  è trascendente su  $A$ , significa che esiste un polinomio non nullo in  $A[x]$  che ha  $\alpha$  come soluzione. In particolare, ogni polinomio in  $A[x]$  che ha  $\alpha$  come soluzione è un multiplo del suo polinomio minimo su  $A$ .

**Esempio 7.7**

Sia  $\alpha \in A$ . Allora  $\alpha$  è banalmente un elemento algebrico su  $A$ , il cui polinomio minimo è  $x - \alpha$ . Vale dunque che  $\text{Ker } \varphi_\alpha = (x - \alpha)$ , da cui, secondo il *Primo teorema di isomorfismo*, si ricava che:

$$A[x]/(x - \alpha) \cong A[\alpha] \cong A.$$

**Esempio 7.8**

$i \in \mathbb{C}$  è un elemento algebrico su  $\mathbb{R}$ . Infatti, si consideri  $\varphi_i$ : poiché  $i$  è soluzione di  $x^2 + 1$ , si ha che  $x^2 + 1 \in \text{Ker } \varphi_i$ , che è quindi non vuoto.

Inoltre, dal momento che  $x^2 + 1$  è irriducibile in  $\mathbb{R}[x]$ , esso è generatore di  $\text{Ker } \varphi_i$ . Inoltre, poiché monico, è anche il polinomio minimo di  $i$  su  $\mathbb{R}$ .

Allora, poiché dalla *Proposizione 7.2*  $\text{Imm } \varphi_i = \mathbb{R}[i]$ , si deduce dal *Primo teorema di isomorfismo* che:

$$\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{R}[i] \cong \mathbb{C}.$$

Ancora una volta possiamo generalizzare questo esempio con il seguente teorema.

**Teorema 7.9**

Sia  $B$  un campo e sia  $A \subseteq B$  un suo sottoanello. Se  $\alpha \in B$  è algebrico su  $A$ , allora, detto  $f(x)$  il polinomio minimo di  $\alpha$ , vale la seguente relazione:

$$A[x]/(f(x)) \cong A[\alpha].$$

*Dimostrazione.* Si consideri l'omomorfismo  $\varphi_\alpha$ . Dacché  $\text{Ker } \varphi_\alpha = (f(x))$  per definizione di polinomio minimo, combinando il *Primo teorema di isomorfismo* con la *Proposizione 7.2*, si ottiene proprio  $A[x]/(f(x)) \cong A[\alpha]$ , ossia la tesi.  $\square$

**Definizione 7.10.** Sia  $B$  un campo e sia  $A \subseteq B$  un suo sottoanello. Allora, dato  $\alpha \in B$ , si definisce con la notazione  $A(\alpha)$  il sottocampo di  $B$  che contiene  $A$  e  $\alpha$  che sia minimale rispetto all'inclusione.

**Osservazione.** Le notazioni  $\mathbb{K}(\alpha, \beta)$  e  $\mathbb{K}(\alpha)(\beta)$  sono equivalenti.

**Proposizione 7.11**

Sia  $B$  un campo e sia  $A \subseteq B$  un suo sottoanello. Se  $\alpha \in B$  è algebrico su  $A$ , allora  $A(\alpha) = A[\alpha]$ .

*Dimostrazione.* Se  $\alpha$  è algebrico, allora  $\text{Ker } \varphi_\alpha = (f(x)) \neq (0)$ , dove  $f(x) \in A[x]$  è irriducibile. Pertanto, per il *Teorema 6.6*,  $A[x]/(f(x))$  è un campo.

Dunque dal *Teorema 7.9* si ricava che:

$$A[x]/(f(x)) \cong A[\alpha].$$

Pertanto  $A[\alpha]$  è un campo. Dacché  $A[\alpha] \subseteq A(\alpha)$  e  $A(\alpha)$  è minimale rispetto all'inclusione, si deduce che  $A[\alpha] = A(\alpha)$ , ossia la tesi.  $\square$

**Osservazione.** Il teorema che è stato appena enunciato non vale per gli elementi trascendenti. Infatti,  $A[\alpha]$  sarebbe isomorfo a  $A[x]$ , che non è un campo. Al contrario  $A(\alpha)$  è un campo, per definizione.

### Proposizione 7.12

Sia  $B$  un campo e sia  $A \subseteq B$  un suo sottoanello. Se  $\alpha, \beta \in B$  sono algebrici su  $A$  e condividono lo stesso polinomio minimo, allora  $A[\alpha] \cong A[\beta]$ .

*Dimostrazione.* Sia  $f(x)$  il polinomio minimo di  $\alpha$  e  $\beta$ . Dal *Primo teorema di isomorfismo* e dalla *Proposizione 7.2* si desume che  $A[x]/(f(x)) \cong A[\alpha]$ . Analogamente si ricava che  $A[x]/(f(x)) \cong A[\beta]$ . Pertanto  $A[\alpha] \cong A[\beta]$ .  $\square$

## §7.2 Teorema delle torri ed estensioni algebriche

**Definizione 7.13.** Siano  $A \subseteq B$  campi. Allora si denota come  $[B : A]$  la dimensione dello spazio vettoriale  $B$  costruito su  $A$ , ossia  $\dim B_A$ . Tale dimensione è detta **grado dell'estensione**.

### Teorema 7.14 (Teorema delle torri algebriche)

Siano  $A \subseteq B \subseteq C$  campi. Allora:

$$[C : A] = [C : B][B : A].$$

*Dimostrazione.* Siano  $[C : B] = m$  e  $[B : A] = n$ . Sia  $\mathcal{B}_C = (a_1, \dots, a_m)$  una base di  $C$  su  $B$ , e sia  $\mathcal{B}_B = (b_1, \dots, b_n)$  una base di  $B$  su  $A$ .

Si dimostra che la seguente è una base di  $C$  su  $A$ :

$$\mathcal{B}_A \mathcal{B}_B = \{a_1 b_1, \dots, a_1 b_n, \dots, a_m b_n\}.$$

(i)  $\mathcal{B}_C \mathcal{B}_B$  genera  $A$  su  $C$ .

Sia  $c \in C$ . Allora si può descrivere  $a$  nel seguente modo:

$$c = \sum_{i=1}^m \beta_i a_i, \quad \text{con } \beta_i \in B, \forall 1 \leq i \leq m.$$

A sua volta, allora, si può descrivere ogni  $\beta_i$  nel seguente modo:

$$\beta_i = \sum_{j=1}^n \gamma_j^{(i)} b_j, \quad \text{con } \gamma_j^{(i)} \in A, \forall 1 \leq j \leq n.$$

Combinando le due equazioni, si verifica che  $\mathcal{B}_C \mathcal{B}_B$  genera  $C$  su  $A$ :

$$c = \sum_{i=1}^m \sum_{j=1}^n \gamma_j^{(i)} b_j a_i, \quad \text{con } \gamma_j^{(i)} \in A, \forall 1 \leq i \leq m, 1 \leq j \leq n.$$

(ii)  $\mathcal{B}_C \mathcal{B}_B$  è linearmente indipendente.

Si consideri l'equazione:

$$\sum_{i=1}^m \sum_{j=1}^n \gamma_j^{(i)} b_j a_i = 0, \quad \text{con } \gamma_j^{(i)} \in A, \forall 1 \leq i \leq m, 1 \leq j \leq n.$$

Poiché  $\mathcal{B}_C$  è linearmente indipendente, si deduce che:

$$\sum_{j=1}^n \gamma_j^{(i)} b_j = 0, \quad \forall 1 \leq i \leq m.$$

Tuttavia,  $\mathcal{B}_B$  è a sua volta linearmente indipendente, e quindi  $\gamma_j^{(i)} = 0, \forall i, j$ . Dunque  $\mathcal{B}_C \mathcal{B}_B$  è linearmente indipendente.

Dal momento che  $\mathcal{B}_C \mathcal{B}_B$  è linearmente indipendente e genera  $C$  su  $A$ , consegue che essa sia una base di  $C$  su  $A$ . Quindi  $[C : A] = mn = [C : B][B : A]$ , da cui la tesi.  $\square$

**Definizione 7.15.** Siano  $A \subseteq B$  campi. Se  $[B : A] \neq \infty$ , allora si dice che  $BA$  è un'estensione finita di  $A$ . Altrimenti si dice che  $B$  è un'estensione infinita di  $A$ .

### Proposizione 7.16

Siano  $A \subseteq B \subseteq C$  campi. Allora, se  $C$  è un'estensione finita di  $A$ , anche  $B$  lo è. Inoltre  $C$  è un'estensione finita di  $B$ .

*Dimostrazione.* Dal momento che  $B$  è un sottospazio dello spazio vettoriale  $C$  costruito su  $A$ , e questo ha dimensione finita, anche  $B$  su  $A$  ha dimensione finita. Quindi  $[B : A] \neq \infty$ , e  $B$  è dunque un'estensione finita di  $A$ .

Infine, dacché una base di  $C$  su  $A$  è un generatore finito di  $C$  su  $B$ , si deduce che  $[C : B] \neq \infty$ , e quindi che  $C$  è un'estensione finita di  $B$ .  $\square$

### Teorema 7.17

Siano  $A \subseteq B$  campi. Allora  $a \in B$  è algebrico su  $A$  se e solo se  $[A(a) : A] \neq \infty$ , ossia solo se  $A(a)$  è un'estensione finita di  $A$ .

*Dimostrazione.* Si dimostrano le due implicazioni separatamente.

( $\implies$ ) Se  $a \in B$  è algebrico su  $A$ , allora dal *Teorema 7.9* si ricava che:

$$A[x]/(f(x)) \cong A[a] \cong A(a).$$

Dacché  $A[x]/(f(x))$  ha dimensione finita, anche  $A(a)$  ha dimensione finita, e quindi è un'estensione finita di  $A$ .

( $\Leftarrow$ ) Sia  $A(a)$  un'estensione finita di  $A$  e sia  $[A(a) : A] = m$ . Allora  $I = (1, a, a^2, \dots, a^m)$  è linearmente dipendente, dal momento che contiene  $m + 1$  elementi. Quindi esiste una sequenza finita non nulla  $(\alpha_i)_{i=0 \rightarrow m}$  con elementi in  $A$  tale che:

$$\alpha_m a^m + \dots + \alpha_2 a^2 + \alpha_1 a + \alpha_0 = 0.$$

Quindi  $a$  è soluzione del polinomio:

$$f(x) = \alpha_m x^m + \dots + \alpha_2 x^2 + \alpha_1 x + \alpha_0 \in A[x],$$

pertanto  $a$  è algebrico su  $A$ , da cui la tesi.  $\square$

**Definizione 7.18.** Siano  $A \subseteq B$  campi. Allora si dice che  $B$  è un'estensione algebrica di  $A$  se ogni elemento di  $B$  è algebrico su  $A$ .

### Proposizione 7.19

Siano  $A \subseteq B$  campi. Se  $B$  è un'estensione finita di  $A$ , allora  $B$  è una sua estensione algebrica.

*Dimostrazione.* Sia  $\alpha \in B$  e si consideri la catena di campi  $A \subseteq A(\alpha) \subseteq B$ . Dacché  $[B : A] \neq \infty$ , per la *Proposizione 7.16* anche  $[A(\alpha) : A] \neq \infty$ . Pertanto, dal *Teorema 7.17*,  $\alpha$  è algebrico. Così tutti gli elementi di  $B$  sono algebrici in  $A$ , e dunque, per definizione,  $B$  è un'estensione algebrica di  $A$ .  $\square$

### Teorema 7.20

Siano  $A \subseteq B$  campi e siano  $\beta_1, \beta_2, \dots, \beta_n$  elementi algebrici di  $B$  su  $A$ , con  $n \geq 1$ . Allora  $[A(\beta_1, \beta_2, \dots, \beta_n) : A] \neq \infty$ .

*Dimostrazione.* Si procede applicando il principio di induzione su  $n$ .

(*passo base*) La tesi è verificata per il *Teorema 7.17*.

(*passo induttivo*) Per l'ipotesi induttiva, si sa che  $[A(\beta_1, \beta_2, \dots, \beta_{n-1}) : A] \neq \infty$ .

Poiché  $\beta_n$  è algebrico su  $A$ , sin da subito si osserva che  $[A(\beta_n) : A] \neq \infty$  per il *Teorema 7.17*. Sia allora  $f(x)$  il polinomio minimo di  $\beta_n$  appartenente a  $A[x]$ . Esso è un polinomio che ammette  $\beta_n$  come radice anche in  $A(\beta_1, \beta_2, \dots, \beta_{n-1})[x]$ , e quindi  $\text{Ker } \varphi_{\beta_n} \neq (0)$  ammette un generatore  $p(x)$ , che divide  $f(x)$ . Si ottiene pertanto la seguente disuguaglianza:

$$[A(\beta_1, \beta_2, \dots, \beta_{n-1})(\beta_n) : A(\beta_1, \beta_2, \dots, \beta_{n-1})] = \deg p(x) \leq \deg f(x) = [A(\beta_n) : A].$$

Poiché  $[A(\beta_n) : A]$  è finito, anche  $[A(\beta_1, \beta_2, \dots, \beta_{n-1})(\beta_n) : A(\beta_1, \beta_2, \dots, \beta_{n-1})]$  lo è.

Combinando i due risultati, si ottiene con il *Teorema delle torri algebriche* che:

$$[A(\beta_1, \beta_2, \dots, \beta_n) : A] = [A(\beta_1, \beta_2, \dots, \beta_{n-1})(\beta_n) : A(\beta_1, \beta_2, \dots, \beta_{n-1})] \cdot [A(\beta_1, \beta_2, \dots, \beta_{n-1}) : A] \neq \infty,$$

da cui la tesi. □

### Corollario 7.21

Siano  $A \subseteq B$  campi e siano  $\alpha, \beta \in B$  elementi algebrici su  $A$ . Allora  $A(\alpha, \beta)$  è un'estensione algebrica.

*Dimostrazione.* Dal Teorema 7.20 si ricava che  $[A(\alpha, \beta) : A] \neq \infty$ . Quindi  $A(\alpha, \beta)$  è un'estensione finita di  $A$ , ed in quanto tale, per la Proposizione 7.19, essa è algebrica. □

**Osservazione.** Esistono estensioni algebriche che hanno grado infinito. Un esempio notevole è  $\mathcal{A}$ , l'insieme dei numeri algebrici di  $\mathbb{C}$  su  $\mathbb{Q}$ . Infatti, si ponga  $[\mathcal{A} : \mathbb{Q}] = n - 1 \in \mathbb{N}$  e si consideri  $x^n - 2$ . Dal momento che per il *Criterio di Eisenstein* tale polinomio è irriducibile, si ricava che  $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$ .

Poiché  $\sqrt[n]{2}$  è algebrico, si deduce che  $\mathbb{Q}(\sqrt[n]{2}) \subseteq \mathcal{A}$ , dal momento che per il Corollario 7.21 ogni elemento di  $\mathbb{Q}(\sqrt[n]{2})$  è algebrico su  $\mathbb{Q}$ . Tuttavia questo è un assurdo dal momento che  $\mathbb{Q}(\sqrt[n]{2})$  ha dimensione maggiore di  $\mathcal{A}$ , di cui è sottospazio vettoriale.

### Proposizione 7.22

Siano  $A \subseteq B$  campi e sia  $\alpha \in B$ . Se  $[A(\alpha) : A]$  è dispari, allora  $A(\alpha^2) = A(\alpha)$ .

*Dimostrazione.* Innanzitutto, si osserva che  $A(\alpha^2) \subseteq A(\alpha)$ , ossia che  $A(\alpha)$  è un'estensione di  $A(\alpha^2)$ . Grazie a questa osservazione è possibile considerare il grado di  $A(\alpha)$  su  $A(\alpha^2)$ , ossia  $[A(\alpha) : A(\alpha^2)]$ . Poiché  $\alpha$  è radice del polinomio  $x^2 - \alpha^2$  in  $A(\alpha^2)$ , si deduce che tale grado è al più 2.

Si applichi il *Teorema delle torri algebriche* alla catena di estensioni  $A \subseteq A(\alpha^2) \subseteq A(\alpha)$ :

$$[A(\alpha) : A] = \underbrace{[A(\alpha) : A(\alpha^2)]}_{\leq 2} [A(\alpha^2) : A].$$

Se  $[A(\alpha) : A(\alpha^2)]$  fosse 2,  $[A(\alpha) : A]$  sarebbe pari,  $\neq$ . Pertanto  $[A(\alpha) : A(\alpha^2)] = 1$ , da cui si ricava che  $[A(\alpha) : A] = [A(\alpha^2) : A]$ , ossia che  $A(\alpha^2)$  ha la stessa dimensione di  $A(\alpha)$  su  $A$ .

Dal momento che  $A(\alpha^2)$  è un sottospazio vettoriale di  $A(\alpha)$ , avere la sua stessa dimensione equivale a coincidere con lo spazio stesso. Si conclude allora che  $A(\alpha^2) = A(\alpha)$ . □

**Osservazione.** Si osserva che la *Proposizione 7.22* si può generalizzare facilmente ad un esponente  $n$  qualsiasi, finché sia data come ipotesi la non divisibilità di  $[A(\alpha) : A]$  per nessun numero primo minore o uguale di  $n$ .

Si può infatti considerare, per la dimostrazione generale, il polinomio  $x^n - \alpha^n$ , la cui esistenza implica che  $[A(\alpha) : A(\alpha^n)]$  sia minore o uguale di  $n$ .

### Teorema 7.23

Siano  $A \subseteq B \subseteq C$  campi. Se  $B$  è un'estensione algebrica di  $A$  e  $C$  è un'estensione algebrica di  $B$ , allora  $C$  è un'estensione algebrica di  $A$ .

*Dimostrazione.* Per mostrare che  $C$  è un'estensione algebrica di  $A$ , verificheremo che ogni suo elemento è algebrico in  $A$ . Sia dunque  $c \in C$ .

Poiché per ipotesi  $c$  è algebrico su  $B$ , esiste un polinomio  $f(x) \in B[x]$  tale che  $c$  ne sia radice. Sia  $f(x)$  il polinomio minimo di  $c$  su  $B$ , descritto come:

$$f(x) = b_0 + b_1x + \dots + b_nx^n, \quad n = [B(c) : B].$$

Dacché  $B$  è un'estensione algebrica di  $A$ , ogni coefficiente  $b_i$  di  $f(x)$  è algebrico su  $A$ , ossia  $[A(b_i) : A] \neq \infty$ . Allora, per il *Teorema 7.20*,  $[A(b_0, \dots, b_n) : A] \neq \infty$ .

Anche  $[A(c, b_0, \dots, b_n) : A(b_0, \dots, b_n)] \neq \infty$ , dal momento che  $c$  è soluzione di  $f(x) \in A(b_0, \dots, b_n)[x]$ .

Allora, per il *Teorema delle torri algebriche*,  $[A(c, b_0, \dots, b_n) : A] = [A(c, b_0, \dots, b_n) : A(b_0, \dots, b_n)][A(b_0, \dots, b_n) : A] \neq \infty$ . Quindi  $A(c, b_0, \dots, b_n)$  è un'estensione finita di  $A$ .

Poiché  $A \subseteq A(c) \subseteq A(c, b_0, \dots, b_n)$  è una catena di estensione di campi, per la *Proposizione 7.16*,  $A(c)$  è un'estensione finita di  $A$ , ed in quanto tale, per la *Proposizione 7.19*, è anche algebrica. Quindi  $c$  è algebrico su  $A$ , da cui la tesi.  $\square$

### Teorema 7.24

Sia  $A$  un campo, e sia  $f(x) \in A[x]$ . Allora esiste sempre un'estensione di  $A$  in cui siano contenute tutte le radici di  $f(x)$ .

*Dimostrazione.* Si dimostra il teorema applicando il principio di induzione sul grado di  $f(x)$ .

(*passo base*) Sia  $\deg f(x) = 0$ . Allora  $A$  stesso è un campo in cui sono contenute tutte le radici, dacché esse non esistono.

(*passo induttivo*) Sia  $\deg f(x) = n$ . Sia  $f_1(x)$  un irriducibile di  $f(x)$  e sia  $\gamma(x) \in A[x]$  tale che  $f(x) = f_1(x)\gamma(x)$ . Allora, per il *Teorema 6.6*  $A[x]/(f_1(x))$  è un campo, in cui, per la *Proposizione 6.7*,  $f_1(x)$  ammette radice.

Poiché  $\deg \gamma(x) < n$ , per il passo induttivo esiste un campo  $C$  che estende  $A[x]/(f_1(x))$  in cui risiedono tutte le sue radici. Dacché  $C$  contiene  $A[x]/(f_1(x))$ , sia le radici di  $f_1(x)$  che di  $\gamma(x)$  risiedono in  $C$ . Tuttavia queste sono tutte le radici di  $f(x)$ , si conclude che  $C$ , che è un'estensione di  $A[x]/(f_1(x))$ , e quindi anche di  $A$ , è il campo ricercato.  $\square$

### §7.3 Campi di spezzamento di un polinomio

Pertanto ora è possibile enunciare la definizione di *campo di spezzamento*.

**Definizione 7.25.** Si definisce **campo di spezzamento** di un polinomio  $f(x) \in A[x]$  un campo  $C$  con le seguenti caratteristiche:

- $f(x)$  si fattorizza in  $C[x]$  come prodotto di irriducibili di primo grado (i.e. in  $C[x]$  risiedono tutte le radici di  $f(x)$ ),
- Se  $B$  è un campo tale che  $A \subseteq B \subsetneq C$ , allora  $f(x)$  non si fattorizza in  $B[x]$  come prodotto di irriducibili di primo grado.

**Osservazione.** Per il *Teorema 7.24* esiste sempre un campo di spezzamento di un polinomio, dunque la definizione data è una buona definizione.

**Osservazione.** In generale i campi di spezzamento non sono uguali, sebbene siano tutti isomorfi tra loro<sup>a</sup>.

<sup>a</sup>Per la dimostrazione di questo risultato si rimanda a TODO

#### Teorema 7.26

Sia  $A$  un campo e sia  $B \supseteq A$  un campo di spezzamento di  $f(x) \in A[x]$  su  $A$ , con  $f(x)$  non costante. Sia  $\deg f(x) = n$ . Allora  $[B : A] \leq n!$ .

*Dimostrazione.* Siano  $\lambda_1, \lambda_2, \dots, \lambda_n$  le radici di  $f(x)$ . Allora  $[\mathbb{K}(\lambda_1) : \mathbb{K}] \leq n$ , dacché  $\lambda_1$  è radice di  $f(x)$ .

Sia ora  $f(x) = (x - \lambda_1)g(x)$ , con  $\deg g(x) = n - 1$ . Sicuramente  $\lambda_2$  è radice di  $g(x)$ , pertanto  $[\mathbb{K}(\lambda_1, \lambda_2) : \mathbb{K}(\lambda_1)] \leq n - 1$ . Reiterando il ragionamento si può applicare infine il *Teorema delle torri algebriche*:

$$[\mathbb{K}(\lambda_1, \dots, \lambda_n) : \mathbb{K}] = [\mathbb{K}(\lambda_1, \dots, \lambda_n) : \mathbb{K}(\lambda_1, \dots, \lambda_{n-1})] \cdots [\mathbb{K}(\lambda_1) : \mathbb{K}] \leq 1 \cdot 2 \cdots n = n!,$$

da cui la tesi.  $\square$





## §8 Teorema fondamentale dell'Algebra e radici reali in $\mathbb{Q}[x]$

Si enuncia adesso il *Teorema fondamentale dell'Algebra*, senza tuttavia fornirne una dimostrazione<sup>10</sup>.

### Teorema 8.1 (*Teorema fondamentale dell'Algebra*)

Un polinomio non costante  $f(x) \in \mathbb{C}[x]$  ammette sempre almeno una radice in  $\mathbb{C}$ .

### Corollario 8.2

Sia  $f(x) \in \mathbb{C}[x]$  di grado  $n \geq 1$ . Allora  $f(x)$  ammette esattamente  $n$  radici, contate con la giusta molteplicità.

*Dimostrazione.* Sia  $\zeta_1$  una radice complessa di  $f(x)$ , la cui esistenza è garantita dal *Teorema fondamentale dell'Algebra*. Si divida  $f(x)$  per  $(x - \zeta_1)$  e se ne prende il quoziente  $q_1(x)$ , mentre si ignori il resto, che per la *Proposizione 6.2*, è nullo.

Si reiteri il procedimento utilizzando  $q_1(x)$  al posto di  $f(x)$  fino a quando il grado del quoziente non è nullo, e si chiami infine questo quoziente di grado nullo  $\alpha$ . Infatti, poiché i gradi dei quozienti diminuiscono di 1 ad ogni iterazione, è garantito che l'algoritmo termini esattamente dopo  $n$  iterazioni. Pertanto,  $f(x)$  a priori ha almeno  $n$  radici.

In questo modo, numerando le radici, si può scrivere  $f(x)$  come:

$$f(x) = \alpha(x - \zeta_1)(x - \zeta_2) \cdots (x - \zeta_n). \quad (5)$$

Dal momento che  $x - \zeta_i$  è irriducibile  $\forall 1 \leq i \leq n$  e dacché  $\mathbb{K}[x]$ , in quanto anello euclideo, è un UFD, si dimostra che (5) è l'unica fattorizzazione di  $f(x)$ , a meno di associati. Pertanto  $f(x)$  ammette esattamente  $n$  radici.  $\square$

<sup>10</sup>Per la dimostrazione si rimanda a [DM, pp. 142-143], avvisando della sua estrema tecnicità. Una dimostrazione a tema strettamente algebrico è dovuta invece al matematico francese Laplace (1749 – 1827), per la quale si rimanda a [2, pp. 120-122].



## §9 Introduzione alla teoria dei campi

### §9.1 La caratteristica di un campo

Si consideri il seguente omomorfismo:

$$\psi : \mathbb{Z} \rightarrow \mathbb{K},$$

completamente determinato dalla condizione  $\psi(1) = 1$ , dacché  $\mathbb{Z}$  è generato da 1. Si studia innanzitutto il caso in cui  $\text{Ker } \psi = (0)$ . In questo caso,  $\psi$  è un monomorfismo, e per il *Corollario 1.38*,  $\mathbb{Z} \cong \text{Imm } \psi$ .

Pertanto,  $\mathbb{K}$  ammetterebbe come sottoanello una copia isomorfa di  $\mathbb{Z}$ . Inoltre, poiché  $\mathbb{K}$  è un campo, deve anche ammetterne gli inversi, e quindi ammetterebbe come sottocampo una copia isomorfa di  $\mathbb{Q}$ . La seguente definizione classificherà questi tipi di campo.

**Definizione 9.1.** Si dice che un campo  $\mathbb{K}$  è di **caratteristica zero** ( $\text{char } \mathbb{K} = 0$ ), quando  $\text{Ker } \psi = (0)$ .

Altrimenti, se  $\text{Ker } \psi \neq (0)$ , dacché  $\mathbb{Z}$  è un anello euclideo,  $\text{Ker } \psi$  deve essere monogenerato da un intero  $n$ , ossia  $\text{Ker } \psi = (n)$ .

Tuttavia non tutti gli interi sono ammissibili. Sia infatti  $n$  non primo, allora  $n = ab$  con  $a, b \neq \pm 1$ . Si nota innanzitutto che  $\psi(a) \neq 0$ , se infatti fosse nullo,  $n$  dovrebbe dividere  $a$ , impossibile dal momento che  $|a| < |n|$ ,  $\neq$ . Analogamente anche  $\psi(b) \neq 0$ .

Se  $n$  fosse generatore di  $\text{Ker } \psi$  si ricaverebbe allora che:

$$\underbrace{\psi(a)}_{\neq 0} \underbrace{\psi(b)}_{\neq 0} = \psi(n) = 0,$$

che è assurdo, dal momento che  $\mathbb{K}$ , in quanto campo, è anche un dominio. Quindi  $n$  deve essere un numero primo. In particolare, allora, per il *Primo teorema d'isomorfismo*,  $\mathbb{Z}_p = \mathbb{Z}/(p) \cong \text{Imm } \psi$ , ossia  $\mathbb{K}$  contiene una copia isomorfa di  $\mathbb{Z}_p$ , a cui ci riferiremo semplicemente con  $\mathbb{F}_p$ .

Allora, poiché sia  $\mathbb{K}$  che  $\mathbb{F}_p$  sono campi,  $\mathbb{K}$  è uno spazio vettoriale su  $\mathbb{F}_p$ . Si può dunque classificare quest'ultimo tipo di campi con la seguente definizione:

**Definizione 9.2.** Si dice che un campo  $\mathbb{K}$  è di **caratteristica  $p$**  ( $\text{char } \mathbb{K} = p$ ) quando  $\text{Ker } \psi = (p)$ , con  $p$  primo.

**Osservazione.** La caratteristica di un campo **non** distingue i campi finiti dai campi infiniti. Esistono infatti campi infiniti di caratteristica  $p$ , come il campo delle funzioni razionali su  $\mathbb{Z}_p$ :

$$\mathbb{Z}_p(x) = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in \mathbb{Z}_p[x], g(x) \neq 0 \right\}.$$

Infatti  $\psi(p) = p\psi(1) = 0$ .

### §9.2 Prime proprietà dei campi di caratteristica $p$

Come si è appena visto, un campo  $\mathbb{K}$  di caratteristica  $p$  contiene al suo interno un sottocampo  $\mathbb{F}_p$  isomorfo a  $\mathbb{Z}_p$ , ed è per questo uno spazio vettoriale su di esso. A partire da questa informazione si può dimostrare la seguente proposizione.

#### Proposizione 9.3

Sia  $\mathbb{K}$  un campo di caratteristica  $p$ . Allora, per ogni elemento  $v$  di  $\mathbb{K}$ ,  $pv = 0$ .

*Dimostrazione.* Considerando ogni elemento di  $\mathbb{K}$  come vettore e  $p$  come scalare, si ricava che:

$$pv = \underbrace{(1 + \dots + 1)}_{p \text{ volte}}v = \underbrace{(\psi(1) + \dots + \psi(1))}_{p \text{ volte}}v = \psi(p)v = 0v = 0.$$

□

Mentre, partendo da questa proposizione, si può dimostrare il seguente teorema.

#### Teorema 9.4 (Teorema del binomio ingenuo)

Siano  $a$  e  $b$  elementi di un campo di caratteristica  $p$ . Allora  $(a + b)^p = a^p + b^p$ .

*Dimostrazione.* Per dimostrare la tesi si applica la formula del binomio di Newton nel seguente modo:

$$(a + b)^p = \sum_{i=0}^p \binom{p}{i} a^{p-i} b^i.$$

Tuttavia, dal momento che  $p$  è un fattore di tutti i binomiali per  $1 \leq i \leq p - 1$ , tutti i termini computati con queste  $i$  sono nulli per la *Proposizione 9.3*. Si desume così l'identità della tesi. □

### §9.3 L'omomorfismo di Frobenius

**Definizione 9.5.** Dato un campo  $\mathbb{K}$  di caratteristica  $p$ , si definisce **omomorfismo di Frobenius** per il campo  $\mathbb{K}$  la funzione:

$$\mathcal{F} : \mathbb{K} \rightarrow \mathbb{K}, a \mapsto a^p.$$

**Osservazione.** In effetti, l'omomorfismo di Frobenius è un omomorfismo.

Infatti,  $\mathcal{F}(1) = 1^p = 1$ . Inoltre tale funzione rispetta la linearità per il *Teorema del binomio ingenuo*:

$$\mathcal{F}(a + b) = (a + b)^p = a^p + b^p = \mathcal{F}(a) + \mathcal{F}(b),$$

e chiaramente anche la moltiplicatività:

$$\mathcal{F}(ab) = (ab)^p = a^p b^p = \mathcal{F}(a)\mathcal{F}(b).$$

**Proposizione 9.6**

L'omomorfismo di Frobenius di un campo  $\mathbb{K}$  di caratteristica  $p$  è un monomorfismo.

*Dimostrazione.* Si prenda in considerazione  $\text{Ker } \mathcal{F}$ . Esso è sicuramente un ideale diverso da  $\mathbb{K}$ , dacché  $1 \notin \text{Ker } \mathcal{F}$ . Tuttavia, se  $\text{Ker } \mathcal{F} \neq (0)$ ,  $\text{Ker } \mathcal{F}$ , dal momento che  $\mathbb{K}$ , in quanto campo, è un anello euclideo, e quindi un PID, è monogenerato da un invertibile.

Se però così fosse,  $\text{Ker } \mathcal{F}$  coinciderebbe con il campo  $\mathbb{K}$  stesso,  $\neq$ . Quindi  $\text{Ker } \mathcal{F} = (0)$ , da cui la tesi.  $\square$

**Proposizione 9.7**

Sia  $\mathbb{K}$  un campo finito di caratteristica  $p$ . Allora l'omomorfismo di Frobenius è un automorfismo.

*Dimostrazione.* Dalla *Proposizione 9.6* è noto che  $\mathcal{F}$  sia già un monomorfismo. Dal momento che il dominio e il codominio sono lo stesso e constano entrambi dunque di un numero finito di elementi, se  $\mathcal{F}$  non fosse surgettivo, vi sarebbe un elemento di  $\mathbb{K}$  a cui non è associato nessun elemento di  $\mathbb{K}$  mediante  $\mathcal{F}$ .

Per il principio dei cassetti, allora, spartendo  $|\mathbb{K}|$  elementi in  $|\mathbb{K}| - 1$  elementi, vi sarebbe almeno un elemento dell'immagine a cui sarebbero associati due elementi del dominio. Tuttavia questo è assurdo dal momento che  $\mathcal{F}$  è un monomorfismo. Quindi  $\mathcal{F}$  è un epimorfismo.

Dacché  $\mathcal{F}$  è contemporaneamente un endomorfismo, un monomorfismo e un epimorfismo, è allora anche un automorfismo.  $\square$

**Proposizione 9.8**

Sia  $\mathbb{K}$  un campo di caratteristica  $p$  e si definisca l'insieme dei punti fissi del suo omomorfismo di Frobenius:

$$\text{Fix}(\mathcal{F}^n) = \{a \in \mathbb{K} \mid \mathcal{F}^n(a) = a\}.$$

Allora  $\text{Fix}(\mathcal{F}^n)$  è un sottocampo di  $\mathbb{K}$ .

*Dimostrazione.* Affinché  $\text{Fix}(\mathcal{F}^n)$  sia un sottocampo di  $\mathbb{K}$ , la sua somma e la sua moltiplicazione devono essere ben definite, e ogni suo elemento deve ammettere un inverso sia additivo che moltiplicativo.

Siano allora  $a, b \in \text{Fix}(\mathcal{F}^n)$ .  $\mathcal{F}^n$  è un omomorfismo, in quanto è composizione di omomorfismi (in particolare, dello stesso omomorfismo  $\mathcal{F}$ ). Sfruttando le proprietà degli omomorfismi si dimostra dunque che  $a + b \in \text{Fix}(\mathcal{F}^n)$ :

$$\mathcal{F}^n(a + b) = \mathcal{F}^n(a) + \mathcal{F}^n(b) = a + b,$$

e che  $ab \in \text{Fix}(\mathcal{F}^n)$ :

$$\mathcal{F}^n(ab) = \mathcal{F}^n(a)\mathcal{F}^n(b) = ab.$$

Analogamente si dimostra che  $-a \in \text{Fix}(\mathcal{F}^n)$ :

$$\mathcal{F}^n(-a) = -\mathcal{F}^n(a) = -a,$$

e che  $a^{-1} \in \text{Fix}(\mathcal{F}^n)$ :

$$\mathcal{F}^n(a^{-1}) = \mathcal{F}^n(a)^{-1} = a^{-1}.$$

□

## §9.4 Classificazione dei campi finiti

### Teorema 9.9

Ogni campo finito  $\mathbb{K}$  di caratteristica  $p$  consta di  $p^n$  elementi, con  $n \in \mathbb{N}^+$ .

*Dimostrazione.* Come già detto precedentemente,  $\mathbb{K}$  è uno spazio vettoriale su una copia isomorfa di  $\mathbb{Z}_p$ ,  $\mathbb{F}_p$ .

Si consideri allora il grado  $[\mathbb{K} : \mathbb{F}_p]$ . Sicuramente questo grado non è infinito, dal momento che  $\mathbb{K}$  non ha infiniti elementi. Quindi  $[\mathbb{K} : \mathbb{F}_p] = n \in \mathbb{N}$ .

Sia dunque  $(k_1, k_2, \dots, k_n)$  una base di  $\mathbb{K}$  su  $\mathbb{F}_p$ . Ogni elemento  $a$  di  $\mathbb{K}$  si potrà dunque scrivere come:

$$a = \alpha_1 k_1 + \dots + \alpha_n k_n, \quad \alpha_1, \dots, \alpha_n \in \mathbb{F}_p,$$

e dunque vi saranno in totale  $p^n$  elementi, dove ogni  $p$  è contato dal numero di elementi che è possibile associare ad ogni coefficiente, ossia  $|\mathbb{F}_p| = p$ , per il numero di elementi appartenenti alla base, ossia  $[\mathbb{K} : \mathbb{F}_p] = n$ , da cui la tesi. □

### Teorema 9.10

Per ogni  $n \in \mathbb{N}^+$  e per ogni numero primo  $p$  esiste un campo finito con  $p^n$  elementi.

*Dimostrazione.* Si consideri il polinomio  $x^{p^n} - x$  su  $\mathbb{Z}_p$  e un suo campo di spezzamento  $A$ .  $\text{Fix}(\mathcal{F}^n)$ , per la *Proposizione 9.8*, è un sottocampo, e contiene esattamente le radici di  $x^{p^n} - x$ , che in  $A$  si spezza in fattori lineari, per definizione.

La derivata di  $x^{p^n} - x$  è  $p^n x^{p^n-1} - 1 \equiv -1$ , dacché  $A$  è uno spazio vettoriale su  $\mathbb{Z}_p$ , e pertanto vale ancora la *Proposizione 9.3*. Dal momento che  $-1$  e  $x^{p^n} - x$  non hanno fattori lineari in comune, per il *Criterio della derivata*,  $x^{p^n} - x$  non ammette radici multiple.

Allora  $\text{Fix}(\mathcal{F}^n)$  è un campo con  $p^n$  elementi, ossia tutte le radici di  $x^{p^n} - x$  (e coincide quindi con il campo di spezzamento  $A$ ), da cui la tesi. □





## §10 Teoremi rilevanti sui campi finiti

### §10.1 Campo di spezzamento di un irriducibile in $\mathbb{F}_p$

#### Teorema 10.1

Sia  $f(x)$  un polinomio irriducibile in  $\mathbb{F}_p$  e sia  $n$  il suo grado. Allora  $\mathbb{F}_{p^n}$  è il suo campo di spezzamento.

*Dimostrazione.* Dacché  $f(x)$  è irriducibile,  $\mathbb{F}_p/(f(x))$  è un campo con  $p^n$  elementi, ed è quindi isomorfo a  $\mathbb{F}_{p^n}$ .

Sia  $\alpha = x + (f(x))$  una radice di  $f(x)$  in  $\mathbb{F}_{p^n}$ . Dal momento che  $f(x)$  è irriducibile in  $\mathbb{F}_p$ , esso è il polinomio minimo di  $\alpha$ . Tuttavia, poiché  $\alpha \in \mathbb{F}_{p^n}$ ,  $\alpha$  è anche radice di  $x^{p^n} - x$ . Pertanto si deduce che  $f(x)$  divide  $x^{p^n} - x$ .

Dunque, poiché  $x^{p^n} - x$  in  $\mathbb{F}_{p^n}$  è prodotto di fattori lineari, tutte le radici di  $f(x)$  sono già in  $\mathbb{F}_{p^n}$ .

Inoltre,  $\mathbb{F}_{p^n}$  è il più piccolo sottocampo contenente  $\alpha$ , dacché  $\mathbb{F}_{p^n} \cong \mathbb{F}_p/(f(x)) \cong \mathbb{F}_p(\alpha)$ . Quindi si deduce che  $\mathbb{F}_{p^n}$  è un campo di spezzamento per  $f(x)$ , ossia la tesi.  $\square$

#### Lemma 10.2

Sia  $f(x)$  un irriducibile di grado  $n$  su  $\mathbb{F}_p[x]$  e sia  $\alpha$  una sua radice in  $\mathbb{F}_{p^n}$ . Allora  $f(\mathcal{F}^k(\alpha)) = 0, \forall k \geq 0$ .

<sup>a</sup> $\mathcal{F}$  è l'omomorfismo di Frobenius, definito come  $\mathcal{F} : \mathbb{F}_p \rightarrow \mathbb{F}_p, a \mapsto a^p$ .

*Dimostrazione.* Sia  $f(x) = a_n x^n + \dots + a_0$  a coefficienti in  $\mathbb{F}_p$ . Si dimostra la tesi applicando il principio di induzione su  $k$ .

(passo base)  $f(\mathcal{F}^0(\alpha)) = f(\alpha) = 0$ .

(passo induttivo) Per l'ipotesi induttiva,  $f(\mathcal{F}^{k-1}(\alpha)) = 0$ . Allora, si verifica algebricamente che:

$$\begin{aligned} f(\mathcal{F}^k(\alpha)) &= a_n (\mathcal{F}^k(\alpha))^n + \dots + a_0 = \mathcal{F}(a_n) \mathcal{F}((\mathcal{F}^{k-1}(\alpha))^n) + \dots + \mathcal{F}(a_0) = \\ &= \mathcal{F}(a_n (f(\mathcal{F}^{k-1}(\alpha)))) = \mathcal{F}(0) = 0, \end{aligned}$$

dove si è usato che  $\mathcal{F}(a_i) = a_i, \forall 0 \leq i \leq n$ , dacché ogni elemento di  $\mathbb{F}_p$  è radice di  $x^p - x$ .  $\square$

**Teorema 10.3**

Sia  $f(x)$  un irriducibile di grado  $n$  su  $\mathbb{F}_p[x]$  e sia  $\alpha$  una sua radice in  $\mathbb{F}_{p^n}$ . Allora vale la seguente fattorizzazione in  $\mathbb{F}_{p^n}$ :

$$f(x) = \prod_{i=0}^{n-1} (x - \alpha^{p^i}) = \prod_{i=0}^{n-1} (x - \mathcal{F}^i(\alpha)),$$

dove ogni fattore non è associato.

*Dimostrazione.* Si verifica innanzitutto che vale chiaramente che  $\alpha^{p^i} = \mathcal{F}^i(\alpha)$ . Dal momento che  $\alpha$  è radice, allora ogni  $\alpha^{p^i}$  lo è, per il *Lemma 10.2*.

Affinché tutti i fattori della moltiplicazione non siano associati è sufficiente dimostrare che  $n$  è il più piccolo esponente  $j$  per cui  $\mathcal{F}^j(\alpha) = \alpha$ . Infatti, siano  $\mathcal{F}^i(\alpha) = \mathcal{F}^j(\alpha)$  con  $0 \leq j < i < n$ , allora, applicando più volte  $\mathcal{F}$ , si ricava che:

$$\mathcal{F}^n(\alpha) = \mathcal{F}^{j+n-i}(\alpha) \implies \mathcal{F}^{j+n-i}(\alpha) = \alpha,$$

che è assurdo, dacché  $j < i < n \implies j + n - i < n$ ,  $\neq$ .

Innanzitutto, si verifica che  $\mathcal{F}^n(\alpha) = \alpha^{p^n} = \alpha$ , dacché  $\alpha \in \mathbb{F}_{p^n}$ . Infine, sia  $t$  il più piccolo esponente  $j$  per cui  $\mathcal{F}^j(\alpha) = \alpha$ . Se  $j$  fosse minore di  $n$ ,  $\alpha$  sarebbe radice di  $x^{p^t} - x$ . Tuttavia questo è assurdo, dal momento che così  $\alpha$  apparterebbe a  $\mathbb{F}_{p^t} \neq \mathbb{F}_{p^n}$ , quando invece il più piccolo campo che lo contiene è  $\mathbb{F}_p(\alpha) \cong \mathbb{F}_p[x]/(f(x)) \cong \mathbb{F}_{p^n}$ ,  $\neq$ .  $\square$

**§10.2 L'inclusione  $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$  e il polinomio  $x^{p^n} - x$** **Lemma 10.4**

Sia  $\alpha$  una radice di  $x^{p^d} - x$  con  $d \mid n$ . Allora  $\alpha$  è anche una radice di  $x^{p^n} - x$ .

*Dimostrazione.* Sia  $s \in \mathbb{N}$  tale che  $n = ds$ . Si verifica la tesi applicando il principio di induzione su  $k \in \mathbb{N}$ .

(*passo base*) Per ipotesi,  $\alpha^{p^d} = \alpha$ .

(*passo induttivo*) Per ipotesi induttiva,  $\alpha^{p^{(k-1)d}} = \alpha$ . Allora si ricava che:

$$\alpha^{p^{(k-1)d}} = \alpha \implies \alpha^{p^{kd}} = \alpha^{p^d} = \alpha.$$

In particolare,  $\alpha^{p^n} = \alpha^{p^{ds}} = \alpha$ , da cui la tesi.  $\square$

**Teorema 10.5**

$\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$  se e solo se  $m \mid n$ .

*Dimostrazione.* Si dimostrano le due implicazioni separatamente.

( $\implies$ ) Dal momento che  $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ , si ricava la seguente catena di estensioni:

$$\mathbb{F}_p \subseteq \mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n},$$

dalla quale, applicando il *Teorema delle Torri Algebriche*, si desume la seguente equazione:

$$\underbrace{[\mathbb{F}_{p^n} : \mathbb{F}_p]}_n = [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}] \underbrace{[\mathbb{F}_{p^m} : \mathbb{F}_p]}_d,$$

e quindi che  $m$  divide  $n$ .

( $\impliedby$ ) Sia  $m \mid n$ . Si consideri  $\alpha \in \mathbb{F}_{p^m}$ .  $\alpha$  è sicuramente radice di  $x^{p^m} - x$ , e poiché  $m$  divide  $n$ , è anche radice di  $x^{p^n} - x$ , per il *Lemma 10.4*. Allora  $\alpha$  appartiene al campo di spezzamento di  $x^{p^n} - x$  su  $\mathbb{F}_p$ , ossia  $\mathbb{F}_{p^n}$ . Pertanto  $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ . □

### Corollario 10.6

$\forall 1 \leq i \leq n$ . Allora, detta  $m_i$  il grado di  $g_i(x)$ , il campo di spezzamento di  $f(x)$  è  $\mathbb{F}_{p^k}$ , dove  $k = \text{mcm}(m_1, m_2, \dots, m_n)$ .

*Dimostrazione.* Il campo di spezzamento di  $f(x)$  è il più piccolo campo rispetto all'inclusione che ne contenga tutte le radici, ossia il più piccolo campo che contenga  $\mathbb{F}_{p^{m_1}}, \mathbb{F}_{p^{m_2}}, \dots, \mathbb{F}_{p^{m_n}}$ . Si dimostra che tale campo è proprio  $\mathbb{F}_{p^k}$ .

Innanzitutto  $\mathbb{F}_{p^k}$ , per il *Teorema 10.5*, contiene tutti i campi di spezzamento dei fattori irriducibili di  $f(x)$ , dacché  $m_i$  divide  $k \forall 1 \leq i \leq n$ .

Sia supponga esista adesso un altro campo  $\mathbb{F}_{p^t} \subseteq \mathbb{F}_{p^k}$  con tutte le radici. Sicuramente  $t \mid k$ , per il *Teorema 10.5*. Inoltre, dal momento che dovrebbe includere ogni campo  $\mathbb{F}_{p^{m_i}}$ , sempre per il *Teorema 10.5*,  $m_i$  divide  $t \forall 1 \leq i \leq n$ .

Allora  $t$  è un multiplo comune di tutti i  $m_i$ , e quindi  $k$ , in quanto minimo comune multiplo, lo divide. Si conclude allora che  $t = k$ , e quindi che  $\mathbb{F}_{p^k}$  è un campo di spezzamento di  $f(x)$ . □

### Teorema 10.7

$x^{p^n} - x$  è il prodotto di tutti i polinomi irriducibili in  $\mathbb{F}_p$  di grado divisore di  $n$ .

*Dimostrazione.* La proposizione è equivalente a affermare che ogni polinomio irriducibile in  $\mathbb{F}_p$  ha grado divisore di  $n$  se e solo se divide  $x^{p^n} - x$ . Si dimostrano le due implicazioni separatamente.

( $\implies$ ) Sia  $f(x)$  un polinomio irriducibile in  $\mathbb{F}_p$  di grado  $d$ , con  $d \mid n$ . Si consideri allora il campo  $\mathbb{F}_{p^d} \cong \mathbb{F}_p/(f(x))$ , e sia  $\alpha$  una radice di  $f(x)$  in tale campo.

Per il *Lemma 10.4* si verifica che  $\alpha$  è anche una radice di  $x^{p^n} - x$ . Poiché  $f(x)$  è irriducibile, esso è il polinomio minimo di  $\alpha$ , e quindi si deduce che  $f(x)$  divide  $x^{p^n} - x$ .

( $\Leftarrow$ ) Sia  $f(x)$  un polinomio irriducibile in  $\mathbb{F}_p$  di grado  $d$  che divide  $x^{p^n} - x$ . Si consideri allora il campo  $\mathbb{F}_{p^d} \cong \mathbb{F}_p/(f(x))$ , e sia  $\alpha$  una radice di  $f(x)$  in tale campo. Allora  $\mathbb{F}_{p^d} \cong \mathbb{F}_p(\alpha)$ , dacché  $f(x)$ , in quanto irriducibile, è il polinomio minimo di  $\alpha$ .

Dacché  $f(x)$  divide  $x^{p^n} - x$ ,  $\alpha$  è anche una radice di  $x^{p^n} - x$ , e quindi che  $\alpha \in \mathbb{F}_{p^n}$ . Dal momento che chiaramente anche  $\mathbb{F}_p \subseteq \mathbb{F}_{p^n}$ , si deduce che  $\mathbb{F}_{p^d} \cong \mathbb{F}_p(\alpha) \subseteq \mathbb{F}_{p^n}$ . Allora, per il *Teorema 10.5*,  $d$  divide  $n$ .  $\square$



## §11 Riferimenti bibliografici

- [DM] P. Di Martino e R. Dvornicich. *Algebra*. Didattica e Ricerca. Manuali. Pisa University Press, 2013. ISBN: 9788867410958.
- [H] I.N. Herstein. *Algebra*. Editori Riuniti University Press, 2010. ISBN: 9788864732107.
- [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>.
- [2] R. Remmert. «The Fundamental Theorem of Algebra». In: *Numbers*. New York, NY: Springer New York, 1991, pp. 97–122. ISBN: 978-1-4612-1005-4. DOI: [10.1007/978-1-4612-1005-4\\_5](https://doi.org/10.1007/978-1-4612-1005-4_5). URL: [https://doi.org/10.1007/978-1-4612-1005-4\\_5](https://doi.org/10.1007/978-1-4612-1005-4_5).