

# ALGEBRA 2

## Ripasso Teoria di Gruppi

### Definizione di Gruppo

Un gruppo  $G$  è un insieme non vuoto con una operazione binaria

$$G \times G \rightarrow G \quad (g, h) \mapsto g \cdot h = gh$$

Che soddisfa tre proprietà:

1. Associatività:  $\forall g, h, k \in G, g \cdot (h \cdot k) = (g \cdot h) \cdot k$
2. Deve esistere l'elemento neutro  $e$
3. Per ogni elemento deve esistere l'inverso

Se  $gh = hg, \forall g, h \in G$ , il gruppo si dice abeliano (nei gruppi si può usare la cosiddetta notazione additiva con operazione  $+$ )

### Criterio

Sia  $H \subseteq G$  un sottoinsieme non vuoto di un gruppo  $G$ , allora  $H$  è sottogruppo se e solo se  $h \cdot k^{-1} \in H, \forall h, k \in H$

### Dimostrazione:

$\Rightarrow)$  È ovvio, segue dalla definizione di sottogruppo

$\Leftarrow)$  Mostriamo le proprietà del Sottogruppo:

- L'associatività è gratuita in quanto segue direttamente dall'associatività di  $G$
- Elemento Neutro:  $h \in H$  in quanto  $H$  è non vuoto, quindi  $h \cdot h^{-1} = e \in H$  per condizione sopra
- Inverso: Sia  $h \in H \Rightarrow e \cdot h^{-1} = h^{-1} \in H$  sempre per sopra
- Chiusura: Siano  $h_1, h_2 \in H$ , allora  $h_2^{-1} \in H$  per prima e  $h_1 \cdot (h_2^{-1})^{-1} = h_1 \cdot h_2 \in H$

□

### Definizione di Gruppo Ciclico

Un gruppo  $G$  si dice ciclico se è generato da un solo elemento  $g$ , cioè

$$\forall g' \in G, \exists n \in \mathbb{Z} : g' = g^n$$

### Teorema: Classificazione dei Gruppi Ciclici

I gruppi ciclici si suddividono in gruppi con cardinalità finita (come  $\mathbb{Z}/n, \forall n \geq 1$ ) e a cardinalità infinita  $\mathbb{Z}$

### Notazione: Alcune notazioni:

- $|G|$  = ordine di  $G$  = cardinalità di  $G$

-  $o(g) = \text{ordine di } g = \text{minimo } k > 0 \text{ tale che } g^k = e$  (si pone  $\infty$  se non esiste)

Sia quindi  $G$  un gruppo ciclico e  $|G| = n$  (quindi  $G \cong \mathbb{Z}/n$ )

$[1]_n$  è un generatore ma non è il solo, *quali sono gli altri generatori?*

Sono le classi  $[k]_n$  tali che  $\mathcal{MCD}(k, n) = 1$  e sono quindi  $\phi(n)$  dove  $\phi$  è la funzione di Eulero e dove  $\phi(n) = \{1 \leq k \leq n : \mathcal{MCD}(k, n) = 1\}$

*Quanti e quali sono i divisori di  $n$ ?*

Si utilizza il teorema di Lagrange (l'ordine di un sottogruppo è un divisore del gruppo che lo contiene)

### Proposizione

$$\forall d \mid n, \exists! \text{ sottogruppo di } \mathbb{Z}/n \text{ di ordine } d \text{ e questo sottogruppo è generato da } [\frac{n}{d}]_n$$

#### Dimostrazione:

1) Mostrare che  $[\frac{n}{d}]_n$  genera un sottogruppo di ordine  $d$  (basta fare tante somme finché non si arriva a  $d$ , cosicché si semplifichi, resta  $[n] = [0]$ , quindi l'elemento neutro)

2) Mostrare che non ci sono altri sottogruppi (è la parte meno facile)

Sia  $H \leq G$  e sia  $h > 0$  minimo tale che  $[h] \in H$

Sia  $k \in \mathbb{Z}$  tale che  $[k] \in H$ . Mostriamo che  $k$  è multiplo di  $h$ .

Si utilizza la divisione con il resto:  $k = qh + r$  con  $0 \leq r < h \Leftrightarrow [k] = q[h] + [r]$ . Poiché  $[k] \in H, [h] \in H$  per la proprietà di chiusura del sottogruppo,  $[r] \in H$ , ma per l'ipotesi di minimalità di  $[h]$  segue che necessariamente  $[r] = 0$ , quindi  $[k] = q[h]$  quindi  $q$  è multiplo di  $h$

□

Quanto fa  $\phi(1) + \phi(2) + \phi(3) + \phi(4) + \phi(6) + \phi(8) + \phi(12) + \phi(24)$ ?

Poiché si ha che  $\phi(24)$  è il numero di generatori di  $\mathbb{Z}/24$ ,  $\phi(12)$  il numero di generatori di  $\mathbb{Z}/12$  e così via, si ha che la somma precedente è uguale a 24, abbiamo quindi contatto tutti gli elementi del gruppo.

### Corollario

$$\forall n > 0 \quad \sum_{d \mid n} \phi(d) = n$$

**Notazione:** Dato un gruppo  $G$  finito con  $|G| = n$ , sia  $d \mid n$ , definiamo  $m_G(d)$  la cardinalità dell'insieme  $\{g \in G : o(g) = d\}$

Esempio di Cardinalità dei Sottogruppi

$$m_{\mathbb{Z}/n}(d) = \phi(n)$$

$m_{S_3}(d) = ?$  Abbiamo che  $m_{S_3}(1) = 1$ ,  $m_{S_3}(2) = 3$ ,  $m_{S_3}(3) = 2$  e  $m_{S_3}(6) = 0$ , quindi la somma è 6, che è esattamente il numero degli elementi di  $S_3$

**Osservazione:**  $\sum_{d \mid n} m_G(d) = n$

### Teorema: Caratterizzazione dei Gruppi Ciclici

Sia  $G$  un gruppo finito di ordine  $n$  tale che  $\forall d \mid n, \exists$  al più un sottogruppo di ordine  $d$ , allora  $G$  è ciclico

#### Dimostrazione:

Per Ipotesi abbiamo che

$$\sum_{d \mid n} m_G(d) = \sum_{d \mid n} \phi(n) = n$$

Dobbiamo dimostrare che  $m_G(n) > 0$ .

Supponiamo per assurdo che  $m_G(n) = 0 \Rightarrow \exists d \mid n : m_G(d) > \phi(d)$

Sia  $h \in G$  tale che  $o(h) = d$  e consideriamo  $\langle h \rangle$  è un sottogruppo di ordine  $d$  e quindi contiene  $\phi(n)$  elementi di ordine  $d$

Ma  $m_G(d) > \phi(d)$ , quindi esiste  $h' \in G$  tale che  $h' \notin \langle h \rangle$  e  $o(h') = d$

Quindi  $|\langle h' \rangle| = d$  e  $\langle h \rangle \neq \langle h' \rangle$ . Abbiamo quindi 2 sottogruppi distinti di ordine  $d$

□

---

# Teoria degli Anelli

Sono esempi di anelli  $\mathbb{Z}$ ,  $\mathbb{Z}[x]$  e  $M_n(\mathbb{R})$ , ma anche  $C^0(\mathbb{R})$ .

In generale sono Anelli degli insiemi con due operazioni soddisfacenti delle proprietà:

## Definizione di Anello

Si definisce un Anello  $A$  un insieme con due operazioni binarie dette rispettivamente Somma e Prodotto (indicate generalmente con  $+$  e  $\cdot$ ) tali che:

1.  $(A, +)$  sia un gruppo abeliano;
2. Il prodotto risulta associativo:  $\forall a, b, c \in A, a \cdot (b \cdot c) = (a \cdot b) \cdot c$
3. Vale la proprietà distributiva:  $\forall a, b, c \in A, a \cdot (b + c) = a \cdot b + a \cdot c$

## Proprietà di Base dell'Anello

- a)  $-(-a) = a$  dove  $-a$  è l'opposto di  $a$  rispetto alla somma
- b)  $a \cdot 0 = 0$  dove  $0$  è l'elemento neutro della rispetto alla somma
- c)  $-(a + b) = (-a) + (-b)$
- d)  $-(a \cdot b) = (-a) \cdot b = a \cdot (-b)$

### Dimostrazione:

a) Deriva direttamente da Algebra 1

b)  $a \cdot 0 = a \cdot (0 + 0) \xrightarrow{\text{P. Distributiva}} a \cdot 0 + a \cdot 0$ . Semplificando si ottiene la tesi

c) Dobbiamo mostrare che  $((-a) + (-b)) + (a + b) = 0 \xrightarrow{\text{P. Associativa}} (-a + a) + (-b + b) = 0$  Quindi abbiamo che l'opposto di  $(a + b)$  è  $(-a) + (-b)$ , ossia che  $-(a + b) = (-a) + (-b)$

d) Dobbiamo mostrare che  $(a \cdot b) + ((-a) \cdot b) = 0$ , che segue direttamente sfruttando la proprietà distributiva della moltiplicazione rispetto alla somma.

□

Verrebbe da dire anche che c'è una quinta proprietà, ossia che se  $a \cdot b = a \cdot c$  con  $a \neq 0$  allora segue che  $b = c$ . Tuttavia la cosa non è sempre vera in generale. Infatti in  $M_2(\mathbb{Z})$  se si prendono i prodotti

$$\begin{pmatrix} -1 & 1 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} -3 & 2 \\ 4 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$$

Si ha che il prodotto è lo stesso ma se si toglie la seconda matrice non sono uguali

**Notazione:** D'ora in avanti al posto di scrivere  $a + (-b)$  scriveremo  $a - b$

## Tipologie di Anelli

Un anello  $A$  si dice Compatitivo se  $a \cdot b = b \cdot a, \forall a, b \in A$

Un anello  $A$  si dice Unitario se esiste un elemento  $u \in A$  tale che  $a \cdot u = u \cdot a = a, \forall a \in A$

## Lemma

Siano  $u, u' \in A$  tali che  $a \cdot u = u \cdot a = u' \cdot a = a \cdot u' = a, \forall a \in A \Rightarrow u = u'$

### Dimostrazione:

Possiamo leggere prima  $u$  come elemento neutro, quindi  $u \cdot u' = u'$ , poi  $u'$  come elemento neutro, quindi  $u \cdot u' = u$  da cui segue che  $u = u'$

□

**Notazione:** Se abbiamo un anello unitario, chiamiamo 1 l'elemento neutro rispetto al prodotto.

In maniera analoga possiamo porre  $2 := 1 + 1$ ,  $3 := 1 + 1 + 1$  e così via

Con i numeri negativi possiamo porre  $-2$  come l'opposto di  $2$ ,  $-3$  come l'opposto di  $3$  eccetera

Bisogna però verificare che le notazioni scelte siano coerenti con le operazioni di somma e prodotto in  $\mathbb{Z}$  siano compatibili con quelle definite in  $A$ .

### Verifica Compatibilità Operazioni

Verifichiamo che  $\forall m, n \in \mathbb{Z}$  si ha che

$$\underbrace{m}_{\in A} + \underbrace{n}_{\in A} = \underbrace{m+n}_{\in A} \quad \underbrace{m}_{\in A} \cdot \underbrace{n}_{\in A} = \underbrace{m \cdot n}_{\in A}$$

**Per la Somma:**

$$\underbrace{m}_{\in A} + \underbrace{n}_{\in A} = (\underbrace{1+1+\dots+1}_{m \text{ volte}}) + (\underbrace{1+1+\dots+1}_{n \text{ volte}}) = \underbrace{1+1+\dots+1}_{m+n \text{ volte}} = \underbrace{m+n}_{\in A}$$

**Per il Prodotto:**

$$\underbrace{m}_{\in A} \cdot \underbrace{n}_{\in A} = (\underbrace{1+1+\dots+1}_{m \text{ volte}}) \cdot (\underbrace{1+1+\dots+1}_{n \text{ volte}}) = \underbrace{(1+1+\dots+1)+\dots+(1+1+\dots+1)}_{m \text{ volte}} = \underbrace{1+1+\dots+1}_{m \cdot n \text{ volte}} = \underbrace{m \cdot n}_{\in A}$$

Abbiamo inoltre che con  $m > 0$ , si ha che  $ma = \underbrace{a+a+\dots+a}_{m \text{ volte}}$ . Segue quindi che  $ma = m \cdot a$

Si può verificare facilmente come si è dimostrato precedente, ponendo  $a$  al posto di 1

Tuttavia può capitare che  $m = n$  come elementi dell'anello  $A$ , ma che siano elementi diversi visti come numeri interi

Per esempio in  $\mathbb{Z}/3$ ,  $2 = 5$

L'esempio più semplice di Anello è l'anello Banale, in cui c'è solo un elemento  $A = \{a\}$  dove  $a = 0 = 1$

**Osservazione:** L'anello banale è l'unico anello in cui  $0 = 1$ . Infatti se  $0 = 1$ , allora  $\forall a \in A, 0 = 0 \cdot a = 1 \cdot a = a$  e la cosa è vera in quanto c'è solo un elemento in  $A$

### Proposizione

Se  $A$  è un anello commutativo e unitario, allora  $\forall a, b \in A$  valgono:

- $(a+b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}$
- $a^n - b^n = (a-b) \sum_{k=0}^{n-1} a^k b^{n-1-k}$

**Dimostrazione:**

1) Procediamo per induzione su  $n$  sfruttando la formula di Stifel:

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{k-1}{n}$$

Per  $n = 0$  l'uguaglianza è banalmente verificata, infatti sostituendo  $n$  con 0 si ottiene da entrambe le parti dell'uguale 1.

Passo Induttivo: sia vero per tutti i numeri fino a  $n - 1$  e mostriamolo per  $n$ :

$$\begin{aligned} (a+b)^n &= (a+b)(a+b)^{n-1} \xrightarrow{\text{Hyp. Ind}} (a+b) \sum_{k=0}^{n-1} \binom{n-1}{k} a^k b^{n-1-k} \xrightarrow{\text{P. Dist + P. Comm}} \sum_{k=0}^{n-1} \binom{n-1}{k} a^{k+1} b^{n-1-k} + \sum_{k=0}^{n-1} \binom{n-1}{k} a^k b^{n-k} \\ &= \sum_{k=1}^n \binom{n-1}{k-1} a^k b^{n-k} + \sum_{k=0}^{n-1} a^k b^{n-k} \xrightarrow{\binom{n}{-1} = \binom{n}{n+1} = 0} \sum_{k=0}^n \left( \binom{n-1}{k-1} + \binom{n-1}{k} \right) a^k b^{n-k} = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k} \end{aligned}$$

2) Basta fare calcoli esplicativi

□

### Definizione di Sottoanello

Sia  $A$  un anello (unitario) e  $B \subseteq A$ . Si dice che  $B$  è sottoanello di  $A$  se:

1.  $B$  è un anello per le stesse operazioni di  $A$
2. Se  $A$  è unitario,  $1 \in B$

Esempio di Sottoanello ma non Sottoanello Unitario

Sia  $\mathbb{Z}/6$  un anello unitario e sia  $B = \{0, 3\} \subseteq \mathbb{Z}/6$

Da adesso in poi quando abbiamo questo tipo di anelli, consideriamo i numeri stessi come i rappresentanti di tali classi

Abbiamo che  $B$  è un sottoanello ma non è un sottoanello unitario in quanto  $1 \notin B$  nonostante  $B$  sia in sé un anello unitario

### Lemma

Sia  $A$  un anello commutativo unitario e  $B \subseteq A, B \neq \emptyset$ .  $B$  è sottoanello unitario se e solo se:

1.  $b - b' \in B, \forall b, b' \in B$
2.  $b \cdot b' \in B, \forall b, b' \in B$
3.  $1 \in B$

Esempi di Sottoanelli

1.  $\mathbb{Z}[\frac{1}{n}] = \{\frac{a}{n^k} \in \mathbb{Q} : a, k \in \mathbb{Z}\}$  è un sottoanello di  $\mathbb{Q}$ , infatti:

$$\begin{aligned} 1. \quad & \frac{a}{n^k} - \frac{b}{n^h} = \frac{an^h - bn^k}{n^{h+k}} \in \mathbb{Z}[\frac{1}{n}] \text{ perché senza perdita di generalità possiamo assumere } h, k \geq 0 \\ 2. \quad & \frac{a}{n^k} \cdot \frac{b}{n^h} = \frac{ab}{n^{k+h}} \in \mathbb{Z}[\frac{1}{n}] \\ 3. \quad & 1 = \frac{1}{n^0} \in \mathbb{Z}[\frac{1}{n}] \end{aligned}$$

2.  $\mathbb{Z}_{(p)}$  con  $p$  primo (*d'ora in avanti considereremo  $p$  sempre come numero primo*)

Abbiamo che  $\mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Q} : a, b \in \mathbb{Z}, p \nmid b\}$

Si dimostra che è sottoanello esattamente come nell'esempio appena sopra

### Definizione di Quoziente di un Anello

Siano  $A$  un anello e  $\sim$  una relazione di equivalenza. Si definisce Quoziente di un Anello rispetto alla relazione di equivalenza  $\sim$  e si indica con  $A/\sim$  l'insieme delle classi di equivalenza rispetto a  $\sim$

È possibile dare una struttura di Anello anche a  $A/\sim$  ponendo (nella maniera più naturale possibile):

$$\begin{aligned} [a] + [b] &= [a + b] \\ [a] \cdot [b] &= [a \cdot b] \end{aligned}$$

Tuttavia, sono ben poste?

Affinché siano ben poste si deve avere che la relazione di equivalenza sia compatibile con le operazioni (cioè che se  $a \sim a', b \sim b'$  allora segue che  $a + b \sim a' + b'$  e  $a \cdot b \sim a' \cdot b'$ )

**Osservazione:** Se l'equazione è compatibile, allora le due operazioni su  $A/\sim$  sono ben definite e abbiamo dato a  $A/\sim$  una struttura di anello

Esempio di Anello Quoziente

Sia  $A = \mathbb{Z}$  e  $a \sim b \Leftrightarrow a \equiv b \pmod{n}$ , cioè  $n \mid (a - b)$ . Questa è una relazione di equivalenza compatibile e quindi  $A/\sim = \mathbb{Z}/n$  è un anello. Verifichiamo la compatibilità rispetto al prodotto (rispetto alla somma è già stata vista in Algebra 1)

Siano quindi  $a = a' + kn$  e  $b = b' + hn$  con  $h, k \in \mathbb{Z}$ . Allora:

$$a \cdot b = (a' + kn)(b' + hn) = a' \cdot b' + n(khn + a'h + b'k)$$

Quindi  $a \cdot b \sim a' \cdot b'$

---

# Domini e Campi

## Definizione di Divisore dello Zero

Sia  $A$  un anello e sia  $a \in A, a \neq 0$ . Si dice che  $a$  è divisore dello 0 se  $\exists b \in A, b \neq 0$  tale che  $a \cdot b = 0$

Per esempio in  $\mathbb{Z}/8$ , 8 è un divisore dello zero, infatti  $8 \cdot 3 = 0$

## Definizione di Legge di Cancellazione

Sia  $A$  un anello e  $a \in A, a \neq 0$ .  $a$  soddisfa la legge di cancellazione se la condizione  $a \cdot b = a \cdot c$  implica  $b = c$

## Lemma

Sia  $A$  un anello e  $a \in A, a \neq 0$ .  $a$  soddisfa la legge di cancellazione se e solo se non è divisore dello zero

## Dimostrazione:

$\Rightarrow$ ) Supponiamo  $a \cdot b = 0$ , questo è uguale a  $a \cdot 0 = 0$ , da cui segue che  $b = 0$ , quindi  $a$  non è un divisore dello zero  
 $\Leftarrow$ ) Supponiamo  $a \cdot b = a \cdot c \Rightarrow a \cdot b - a \cdot c = a \cdot (b - c) = 0 \Rightarrow b = c$  in quanto  $a$  non è divisore dello zero

□

## Proposizione

$d \in \mathbb{Z}/n$  è divisore dello zero se e solo se  $\text{MCD}(d, n) > 1$

## Dimostrazione:

$\Rightarrow$ ) Sia  $\text{MCD}(d, n) > 1$ . Abbiamo che  $d \cdot \frac{m}{r}$  ( $\frac{m}{r} \in \mathbb{Z}$  in quanto  $r | m$ ), ma  $d \cdot \frac{m}{r} = \frac{d}{r} \cdot m$  (che è sempre un numero intero), quindi  $d$  è un divisore dello zero  
 $\Leftarrow$ ) Se  $\text{MCD}(d, n) = 1$  e se  $d$  fosse divisore dello zero, allora  $\exists k \in \mathbb{Z}, k \neq 0$  tale che è multiplo di  $n$ , ossia  $n | dk$ . Poiché  $\text{MCD}(d, n) = 1 \Rightarrow n | k \Rightarrow \exists h \in \mathbb{Z}, h \neq 0 : n = hk \Rightarrow k = 0$  (Qui cade l'assurdo che  $k \neq 0$ )

□

## Definizione di Dominio di Integrità

Si definisce  $A$  un Dominio di Integrità se  $A$  è un anello commutativo unitario che non ha divisori dello zero

Osservazione:  $\mathbb{Z}/n$  è un dominio se e solo se  $n$  è primo (segue dal lemma precedente)

## Definizione di Elemento Invertibile

Se  $A$  è un anello unitario,  $u \in A$  è invertibile (o è un un'unità) se  $\exists u' \in A : u \cdot u' = u' \cdot u = 1$

Osservazione: Non esistono divisori dello zero invertibili, infatti se  $u \cdot u' = 1$  e  $u \cdot a = 0$  allora  $u' \cdot u \cdot a$  ha come risultati sia 0 che  $a$

L'inverso di un elemento  $u$ , se esiste, è unico

Se  $u \cdot u' = u \cdot u'' = 1$  allora per la legge di cancellazione per  $u$ ,  $u' = u''$

Indicheremo l'inverso di  $u$  con  $u^{-1}$

L'insieme degli elementi invertibili di  $A$  si indica con  $\mathcal{U}(A)$ , in particolare

$$\mathcal{U}(A) = \{a \in A : a \text{ è invertibile}\}$$

**Osservazione**  $\mathcal{U}(A)$  è un gruppo rispetto al prodotto, infatti  $1 \in \mathcal{U}(A)$ ,  $1 \cdot 1 = 1$  e bisognerebbe dimostrare che è chiuso, ma poiché l'inverso del prodotto è il prodotto degli inversi, quindi è verificato

### Definizione di Corpo

Un Corpo è un anello unitario (non necessariamente commutativo), in cui ogni elemento diverso da 0 è invertibile

### Definizione di Campo

Un corpo commutativo si dice Campo

### Definizione di Corpo dei Quaternioni

Il corpo dei Quaternioni  $Q$  è uno spazio vettoriale di dimensione 4 su  $\mathbb{R}$  con base formale  $\{1, i, j, k\}$  dove

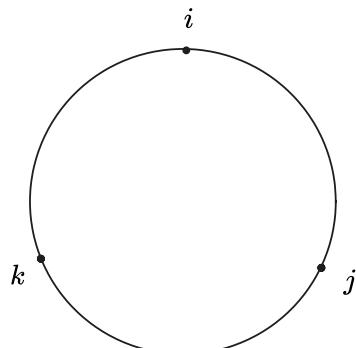
$$Q \ni \alpha = a + bi + cj + dk, \quad a, b, c, d \in \mathbb{R}$$

La somma è definita come somma normale di polinomi

1 è l'elemento neutro della moltiplicazione,  $i^2 = j^2 = k^2 = -1$  e seguono le seguenti moltiplicazioni:

$$\begin{array}{ll} i \cdot j = k & j \cdot i = -k \\ j \cdot k = 1 & k \cdot j = -i \\ k \cdot i = j & i \cdot k = -j \end{array}$$

Per ricordarsi facilmente basta ricordarsi che:



Il prodotto in senso orario è positivo

Il prodotto in senso antiorario è negativo

# Omomorfismi di Anelli

## Definizione di Omomorfismo di Anelli

Siano  $A$  e  $B$  due anelli (unitari), un omomorfismo  $\varphi$  da  $A$  a  $B$  è una funzione

$$\varphi : A \rightarrow B$$

tale che:

- 1)  $\varphi(a + a') = \varphi(a) + \varphi(a') \quad \forall a, a' \in A$
- 2)  $\varphi(a \cdot a') = \varphi(a) \cdot \varphi(a') \quad \forall a, a' \in A$

Se è unitario inoltre vale  $\varphi(1) = 1$

## Esempio Fondamentale di Omomorfismo

Sia  $A$  un anello unitario, allora  $\exists!$  omomorfismo detto fondamentale

$$\varphi : \mathbb{Z} \rightarrow A$$

definito come:

$$\varphi(n_{\in \mathbb{Z}}) = n_{\in A}$$

Le proprietà di omomorfismo sono già verificate (negli appunti precedenti)

Per l'unicità:  $\varphi(1) = 1$  è richiesta dalla definizione. Tutto il resto segue direttamente dalle proprietà dell'omomorfismo, infatti per esempio:

$$\varphi(2_{\in \mathbb{Z}}) = \varphi(1 + 1) = \varphi(1) + \varphi(1) = 1 + 1 = 2_{\in A}$$

E così per ogni elemento  $n \in \mathbb{Z}$

**Esercizio:** Dimostrare che esistono anelli unitari  $A$  e  $B$ , legati da un omomorfismo  $\varphi : A \rightarrow B$  che verificano le prime due proprietà ma non la terza.  $\varphi : \mathbb{Z}/2 \rightarrow \mathbb{Z}/6$ ,  $\varphi(1) = 3$

## Proposizione: Composizione di Omomorfismi:

Siano  $A, B, C$  anelli e siano  $\varphi, \psi$  due omomorfismi che legano gli anelli in questo modo:

$$A \xrightarrow{\varphi} B \xrightarrow{\psi} C$$

Allora  $\psi \circ \varphi : A \rightarrow C$  è un omomorfismo di anelli

## Dimostrazione:

$$\forall a, a' \in A, \psi \circ \varphi(a + a') = \psi(\varphi(a + a')) \stackrel{1)}{=} \psi(\varphi(a) + \varphi(a')) \stackrel{1)}{=} \psi(\varphi(a)) + \psi(\varphi(a')) = \psi \circ \varphi(a) + \psi \circ \varphi(a')$$

In maniera del tutto analoga per il prodotto sfruttando 2)

$$\psi \circ \varphi(1) = \psi(\varphi(1)) \stackrel{3)}{=} \psi(1) \stackrel{3)}{=} 1$$

□

## Proposizione

Sia  $\varphi : A \rightarrow B$  un omomorfismo biunivoco, allora  $\varphi^{-1} : B \rightarrow A$  è un omomorfismo di anelli

## Dimostrazione:

Sia  $* = +$  oppure  $* = \cdot$  (per indicare che sono interscambiabili).

Siano  $b_1, b_2 \in B \Rightarrow \exists! a_1, a_2 \in A$  tali che  $\varphi(a_1) = b_1$  e  $\varphi(a_2) = b_2$

Allora  $\varphi(a_1 * a_2) = \varphi(a_1) * \varphi(a_2) = b_1 * b_2$ . Ma quindi per l'identità precedente si ha che

$$\varphi^{-1}(b_1 * b_2) = \varphi^{-1}(b_1) * \varphi^{-1}(b_2) = a_1 * a_2$$

Poiché abbiamo che  $\varphi(1) = 1$  si ha che  $\varphi^{-1}(1) = 1$

□

### Definizione di Isomorfismo

Un omomorfismo biunivoco  $\varphi : A \rightarrow B$  si dice isomorfismo,  $A$  e  $B$  si dicono isomorfi e diremo anche che  $A$  e  $B$  sono lo "stesso" anello.

### Definizione di Nucleo e Immagine di un Omomorfismo

Sia  $\varphi : A \rightarrow B$  un omomorfismo, si definiscono Nucleo e Immagine rispettivamente:

$$\begin{aligned} Ker(\varphi) &= \{a \in A : \varphi(a) = 0\} \\ Im(\varphi) &= \{\varphi(a) = b, a \in A\} \end{aligned}$$

### Lemma

$Im(\varphi)$  è un sottoanello di  $B$

$Ker(\varphi)$  è un sottogruppo sulla somma e sia  $x \in Ker(\varphi)$  e  $a \in A \Rightarrow a \cdot x \in Ker(\varphi)$  Proprietà di Assorbimento

### Dimostrazione:

$Im(\varphi)$  e  $Ker(\varphi)$  sono sottogruppi additivi in quanto segue direttamente da Algebra 1 (eredita le proprietà dall'insieme che lo eredita)

Siano  $\varphi(a_1), \varphi(a_2) \in Im(\varphi) \Rightarrow \varphi(a_1) \cdot \varphi(a_2) = \varphi(a_1 \cdot a_2) \in Im(\varphi)$  inoltre  $1 = \varphi(1) \in Im(\varphi)$

Verifichiamo la proprietà di assorbimento:  $\varphi(a \cdot x) = \varphi(a) \cdot \varphi(x) = 0 \Rightarrow a \cdot x \in Ker(\varphi)$

□

### Definizione di Ideale di un Anello

Sia  $A$  un anello e  $I \subseteq A$ . Si dice che  $I$  è un ideale di  $A$  se soddisfa:

- 1)  $I$  è un sottogruppo unitario
- 2)  $I$  soddisfa la proprietà di assorbimento ( $\forall a \in A, \forall x \in I, ax \in I$ )

### Esempio di Ideale

Consideriamo gli ideali di  $\mathbb{Z}$ . Sia  $I$  un ideale, allora  $\exists m \in \mathbb{Z} : I = m\mathbb{Z}$

Sia quindi  $n \in \mathbb{Z}$  e sia  $km \in I \Rightarrow n \cdot km = m(nk) \in I$

Prendiamo  $\mathbb{Q} = A$ , abbiamo che  $\mathbb{Z}$  è un sottogruppo additivo di  $\mathbb{Q}$ , è anche ideale?

No, perché  $1 \cdot \frac{1}{2} = \frac{1}{2} \notin \mathbb{Z}$

Gli unici ideali in  $\mathbb{Q}$  sono o quello banale  $\{0\}$  oppure tutto  $\mathbb{Q}$

$\{0\}$  è banalmente verificato, in quanto soddisfa banalmente la proprietà di assorbimento

Supponiamo non sia banale, ossia  $\{0\} \neq I$ , sia quindi  $x \in I$  non nullo. Sia  $y \in \mathbb{Q}$  qualunque, allora  $y = \frac{y}{x} \cdot x$ .  $I$  è un ideale, segue che è verificata la proprietà di assorbimento, quindi  $y \in I$ . Poiché è valido per un qualsiasi  $y$  si ha che  $I = \mathbb{Q}$

Questo succede perché  $\mathbb{Q}$  è un campo, infatti vale: "Se  $\mathbb{K}$  è un campo, allora gli unici ideali sono  $\{0\}$  e  $\mathbb{K}$  stesso".

**Osservazione:** Se  $A$  è un anello e  $I$  è un ideale, allora sono equivalenti:

- 1)  $I = A$
- 2)  $I$  contiene un elemento invertibile

Segue direttamente dal ragionamento dell'esempio precedente

**Richiamo:** La relazione di equivalenza  $\sim$  è compatibile se

$$\begin{cases} a \sim a' \\ b \sim b' \end{cases} \Rightarrow \begin{cases} a + b \sim a' + b' \\ a \cdot b \sim a' \cdot b' \end{cases}$$

### Lemma

Se  $I$  è un ideale e poniamo  $a \sim_I b$  se  $a - b \in I$ . Allora  $\sim_I$  è compatibile

**Dimostrazione:**

Siccome  $I$  è un sottogruppo additivo, allora  $\sim_I$  è una relazione di equivalenza che soddisfa  $a + b \sim_I a' + b'$ .

Vediamo la compatibilità rispetto al prodotto. Siano  $a = a' + x$  e  $b = b' + y$  con  $x, y \in I$ , allora:

$$a'b' - ab = a'b' - (a' + x)(b' + y) = a'b' - a'b' + a'y - xb' - xy \in I$$

In quanto è somma di elementi nell'ideale, quindi  $a'b' \sim_I ab$

□

### Esempio di Ideale Quozientato

Sia  $A = \mathbb{Z}[x]$  e  $I = \{f \in \mathbb{K}[x] : f(0) = 0\}$ . È un ideale?

Siano  $f, g \in I \Rightarrow f + g \in I$

Siano  $f \in I$  e  $h \in \mathbb{K}[x]$ ,  $fh \in I$ ?  $f(0)h(0) = 0h(0) = 0 \Rightarrow fh \in I$

In  $A/I$ , identifichiamo i polinomi con lo stesso termine noto in quanto vogliamo che la loro differenza si annulli in 0

Per esempio  $[3x^2 + 2x + 3] \cdot [5x^{115} + 3x^{14} - 2] = [3][-2] = [-6]$

Notiamo quindi che  $A/I = \mathbb{Z}$  (cioè  $\forall n \in \mathbb{Z}$  esiste una classe in  $A/I$ )

Notiamo che non ci sono altre relazioni compatibili

### Proposizione

Sia  $\sim$  relazione di equivalenza compatibile su  $A$ . Allora esiste un ideale  $I$  tale che  $\sim = \sim_I$

**Dimostrazione:**

Poniamo  $I = \{x \in A : x \sim 0\} \Rightarrow x \in I$

Dobbiamo mostrare che  $I$  è un ideale e che  $\sim = \sim_I$

Mostriamo prima che  $I$  è un sottogruppo additivo, sia  $x \in I$ , è vero che  $-x \in I$ ?

$$-x = -x + 0 \sim -x + x = 0 \Rightarrow -x \sim 0 \Rightarrow -x \in I$$

$$\text{Se } x, y \in I \Rightarrow x + y \sim 0 + 0 = 0 \Rightarrow x + y \in I$$

Proprietà di Assorbimento:  $x \in I, a \in A \Rightarrow a \cdot x \sim a \cdot 0 = 0 \Rightarrow a \cdot x \in I$

Vediamo ora che  $\sim = \sim_I$ , cioè se  $a \sim b$  allora  $a \sim_I b$

Infatti se  $a \sim b \Rightarrow 0 \sim b - a \Rightarrow b - a \in I \Rightarrow a \sim_I b$

Leggendo poi da destra a sinistra si ottiene poi l'altra implicazione

□

### Proposizione

Sia  $A$  un anello e  $B \subseteq A$ :

- 1)  $B$  è sottoanello  $\Leftrightarrow B$  è l'immagine di un omomorfismo
- 2)  $B$  è un ideale  $\Leftrightarrow B$  è il nucleo di qualche omomorfismo

**Dimostrazione:**

- 1) Per la teoria di Algebra 1 si ha che, dato un qualsiasi omomorfismo si ha che l'immagine di tale omomorfismo è un sottoanello del codominio. Inoltre ponendo l'omomorfismo  $\varphi : B \rightarrow A$ , dove  $\varphi(b) = b$ ,  $\forall b \in B \subseteq A \Rightarrow Im(\varphi) = B$
- 2) Il nucleo di un omomorfismo è sempre un ideale. Dimostriamo il contrario. Se  $B$  è un ideale di  $A$ , allora  $\varphi : A \rightarrow A/B$ , definito come  $\varphi(a) = [a]_B$ . *Questo tipo di funzione è definito come proiezione sul quoziente.* Questo è un omomorfismo che viene dal fatto che l'operazione è fatto sui rappresentanti  $\varphi(a + a') = [a + a'] = [a] + [a'] = \varphi(a) + \varphi(a')$ . In maniera del tutto analoga viene fatta per il prodotto. Da tutto ciò si ottiene che  $Ker(\varphi) = B$

□

---

# Studio di Omomorfismi

**Osservazione:** Sia  $\varphi : A \rightarrow B$ , allora è iniettivo se e solo se  $Ker(\varphi) = \{0\}$

Infatti se è iniettivo si ha che  $\exists! a \in A : \varphi(a) = 0 \Rightarrow \varphi(0) = 0$

Se si ha che  $Ker(\varphi) = \{0\}$ , allora consideriamo  $a, a' \in A$  tali che  $\varphi(a) = \varphi(a')$ , ma allora per le proprietà dell'omomorfismo si ha che  $\varphi(a) - \varphi(a') = 0 \Rightarrow \varphi(a - a') = 0$  e poiché il nucleo è banale si ha che  $a - a' = 0 \Rightarrow a = a'$

## Primo Teorema di Omomorfismo

Siano  $A, B$  due anelli e  $\varphi : A \rightarrow B$  un omomorfismo. Allora  $\varphi$  induce un isomorfismo tra  $A/Ker(\varphi)$  e  $Im(\varphi)$

## Metateorema

Se ho un quoziente  $A/I$  e voglio mostrare che è isomorfo ad un anello  $B$ , devo trovare un omomorfismo suriettivo  $\varphi : A \rightarrow B$  con  $Ker(\varphi) = I$

### Dimostrazione del Primo Teorema di Omomorfismo:

Con "indurre" vogliamo dire che  $\exists \bar{\varphi} : A/I \rightarrow Im(\varphi)$  data da  $\bar{\varphi}([a]_I) := \varphi(a)$ .

Dimostriamo che è un omomorfismo ben posto e biunivoco.

È ben posto: siano  $a, a' \in A : [a]_I = [a']_I \Rightarrow \varphi(a - a') = 0 \Rightarrow \varphi(a) - \varphi(a') = 0 \Rightarrow \varphi(a) = \varphi(a')$

Sia adesso \* interscambiabile tra + e  $\cdot$ . Allora si ha che

$$\bar{\varphi}([a]_I * [a']_I) \xrightarrow{\text{Classi}} \bar{\varphi}([a + a']_I) \xrightarrow{\text{Def } \bar{\varphi}} \varphi(a * a') \xrightarrow{\text{P. Omomorfismo}} \varphi(a) * \varphi(a') \xrightarrow{\text{Def } \bar{\varphi}} \bar{\varphi}(a) * \bar{\varphi}(a')$$

Inoltre se  $\varphi$  è un omomorfismo di anelli unitari, allora anche  $\bar{\varphi}$  lo è, quindi  $\bar{\varphi}([1]_I) = \varphi(1) = 1$

$\bar{\varphi}$  è Suriettivo: infatti se  $\varphi(a) \in Im(\varphi) \Rightarrow \varphi(a) = \bar{\varphi}([a]_I)$

$\bar{\varphi}$  è Iniettivo:  $\bar{\varphi}([a]_I) = 0$ , ma  $\bar{\varphi}([a]_I) = \varphi(a) = 0$ , quindi  $a \in Ker(\varphi) \Rightarrow [a]_I = [0]_I$

□

**Osservazione:** Sia  $I_\alpha$  una famiglia di Ideali di  $A$  con  $\alpha \in J$  insieme di indici, allora l'intersezione di tali Ideali è ancora un ideale:

$$\bigcap_{\alpha \in J} I_\alpha \text{ è ancora un ideale}$$

Da dimostrare per esercizio

## Definizione di Ideale Generato

Se  $S$  è un sottoinsieme di un anello  $A$ , definiamo

$$(S) := \bigcap_{I \supseteq S} I$$

Almeno un ideale c'è ed è proprio  $(S)$

Cerchiamo di capire come è fatto  $(S)$

## Lemma

Se  $A$  è unitario, allora

$$(S) = \{a_1 s_1 + \dots + a_r s_r : a_i \in A, s_i \in S\}$$

### Dimostrazione:

Dimostriamo la doppia inclusione

$\supseteq$ ) ( $S$ ) è un ideale che contiene  $S$ , per assorbimento contiene  $a_i s_i, \forall i$  e per additività anche  $a_1 s_1 + \dots + a_r s_r$

$\subseteq$ ) Ci basta mostrare che  $\{a_1 s_1 + \dots + a_r s_r : a_i \in A, s_i \in S\} = J$  è un ideale che contiene  $S$ . In tal caso è uno di quelli che intersecano nella definizione di ( $S$ ).

Notiamo che  $S \subseteq J$ , infatti basta porre  $r = 1$  e  $a_1 = 1$ , quindi al variare di  $s_1$  l'inclusione è verificata

Mostriamo che  $J$  è un ideale:  $(a_1 s_1 + \dots + a_r s_r) - (b_1 s'_1 + \dots + b_m s'_m) \in J$  e  $a(a_1 s_1 + \dots + a_r s_r) = aa_1 s_1 + \dots + aa_r s_r \in S$

□

### Definizione di Ideale Principale

Un ideale  $I$  si dice principale se  $\exists s \in A : I = (\{s\}) = (s)$

Esempio di Ideale Principale

Sia  $\mathbb{Z}[x] = A$  e  $I = (\{2x, 3x\})$ . Come è fatto? È un ideale principale?

Per il lemma precedente  $I = \{f \cdot 2x + g \cdot 3x : f, g \in \mathbb{Z}[x]\}$

$I$  è principale perché  $I = (x)$ , infatti

- $I \subseteq (x)$  perché ogni elemento di  $I$  è multiplo di  $x$
- $(x) \subseteq I$  perché  $x = 3x - 2x \in I$

Siano  $I, J$  ideali di  $A$  definiamo la somma di ideali come  $I + J = \{x + y : x \in I, y \in J\}$

È sempre un ideale in quanto si ha che  $I + J = (I \cup J)$

### Secondo Teorema di Omomorfismo

Siano  $I, J$  ideali, allora vale:

$$(I + J)/I \cong I/(I \cap J)$$

#### Dimostrazione:

Usiamo il metateorema  $\varphi : J \rightarrow I + J/I$  con  $\varphi$  suriettiva e  $\text{Ker}(\varphi) = I \cap J$ . Poniamo  $\varphi(x) = [x]_I$

$\varphi$  è un omomorfismo (basta vedere i conti precedenti)

$\varphi$  è Suriettiva: Sia  $[x + y]_I \in I + J/I$  con  $x \in I$  e  $y \in J \Rightarrow [x + y] = [y] = \varphi(y)$

Quindi deduciamo che  $\text{Ker}(\varphi) = \{x \in J : [x]_I = 0\} = \{x \in J : x \in I\} = J \cap I$

□

Esempio di Utilizzo del Secondo Teorema di Omomorfismo

Siano  $J$  l'anello dei polinomi in  $\mathbb{Z}[x]$  con termine noto multiplo di 3 e  $H$  anello dei polinomi in  $J$  con tutti i coefficienti pari.

Chi è  $J/H$ ?

$J$  è un ideale di  $\mathbb{Z}[x]$  e  $K$  è un ideale di  $\mathbb{Z}[x]$  e di conseguenza anche di  $J$

Definiamo  $I$  come l'anello dei polinomi con tutti i coefficienti pari, allora si ricava che  $H = I \cap J$  Quindi:

$$J/H = J/J \cap I \cong I + J/I \xrightarrow{1 \in I \Rightarrow I = A} \mathbb{Z}[x]/I \cong \mathbb{Z}/2[x]$$

### Definizione di Prodotto di Ideali

Siano  $I, J$  sue ideali, si definisce prodotto di Ideali, l'insieme

$$IJ = \{x_1 y_1 + \dots + x_r y_t : x_i \in I, y_i \in J\}$$

Per esercizio va dimostrato che è un ideale

**Osservazione:**  $IJ \subseteq I \cap J$ . Infatti  $x_iy_i \in I \cap J$  per la proprietà di Assorbimento

Infatti per esempio si ha che in  $\mathbb{Z}$ ,  $I = (6)$  e  $J = (4)$ , allora  $I \cap J = (12)$  e  $IJ = (24)$

**Da Dimostrare:** Se  $\varphi : A \rightarrow B$ , allora la controimmagine di un ideale di  $B$  è sempre un ideale di  $A$  che contiene anche il nucleo

### Proposizione

Sia  $\varphi : A \rightarrow B$  un omomorfismo suriettivo, allora esiste una biiezione tra gli ideali di  $A$  che contengono il nucleo e gli ideali di  $B$ . Tale corrispondenza associa a  $I$  ideale di  $A$   $\varphi(I)$  ideale di  $B$  e a  $J$  ideale di  $B$  associa  $\varphi^{-1}(J)$  ideale di  $A$

**Dimostrazione:**

Mostriamo  $\varphi(I)$  ideale di  $B$ :

- $\varphi(I)$  è sottogruppo additivo perché immagine di sottogruppo
- $\varphi(x) \in \varphi(I)$  e  $b \in B$ . Sia  $a : b = \varphi(a) \Rightarrow \varphi(x) \cdot b = \varphi(x) \cdot \varphi(a) \Rightarrow \varphi(xa) \in \varphi(I)$

Quindi  $\varphi(I)$  è un ideale

Mostriamo la biunivocità, ossia se  $J$  è un ideale di  $B$ , allora  $\varphi(\varphi^{-1}(J)) = J$  e se  $I$  è un ideale di  $A$  che contiene in nucleo, allora  $\varphi^{-1}(\varphi(I)) = I$ . La prima segue dal fatto che se  $\varphi$  è suriettiva.

Per la seconda: sia  $a \in A : \varphi(a) = \varphi(x)$  per qualche  $x \in I$  allora per la proprietà di additività di  $\varphi$  si ha che  $\varphi(a - x) = 0 \Rightarrow a - x \in \text{Ker}(\varphi) \subseteq I \Rightarrow a \in I$

□

**Osservazione:** Se  $I$  è ideale di  $A$  che non contiene  $\text{Ker}(\varphi)$ , allora, posto  $J = I + \text{Ker}(\varphi)$ , si ha che  $\varphi(J) = \varphi(I)$

Consideriamo  $\pi : A \rightarrow A/I$  la proiezione al quoziente ( $\pi(a) = [a]_I$ )

Abbiamo che  $\text{Ker}(\pi) = I$  è una corrispondenza biunivoca tra gli ideali di  $A$  che contengono  $I$  e quelli di  $A/I$

Infatti se  $J$  è un ideale che contiene  $I$ , si ha che  $J \xrightarrow{\pi} \pi(J) = J/I$

A questo proposito analizziamo il quoziente di quozienti, in particolare enunciamo il terzo teorema di omomorfismo.

### Terzo Teorema di Omomorfismo:

Sia  $I \subseteq J \subseteq A$  con  $I$  e  $J$  ideali di  $A$ . Allora si ha che

$$A/I / J/I \cong A/J$$

**Dimostrazione:**

Vogliamo costruire un omomorfismo suriettivo  $\varphi : A/I \rightarrow A/J$  con  $\text{Ker}(\varphi) = J/I$

Poniamo  $\varphi([a]_I) = [a]_J$ . Notiamo che è ben posta (*i calcoli sono sempre i soliti da fare*)

Supponiamo  $[a]_I = [a']_I$ . Vogliamo verificare che  $[a]_J = [a']_J$ . Quest'uguaglianza è vera in quanto se  $a - a' \in I \subseteq J$  allora segue che  $a - a' \in J$  quindi  $[a]_J = [a']_J$

È un omomorfismo? Si, *facendo i calcoli che sono stati fatti in precedenza, in maniera del tutto analoga*

È suriettivo? Si, in quanto segue direttamente dalla definizione,  $[a]_J = \varphi([a]_I)$

Chi è il nucleo di  $\varphi$ ?  $\text{Ker}(\varphi) = \{[a]_I : [a]_J = [0]_J\} = \{[a]_I : a \in J\} = J/I$

□

### Esempio di Applicazione del Terzo Teorema di Omomorfismo

Sia  $A = \mathbb{Z}$  e siano  $I = n\mathbb{Z}$  e  $J = d\mathbb{Z}$  con  $d$  divisore di  $n$ . Allora si ha che

$$\mathbb{Z}/n\mathbb{Z} / d\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/d\mathbb{Z}$$

### Definizione di Ideali Coprimi

Sia  $A$  anello unitario e  $I, J$  ideali di  $A$ , si dicono coprimi se, equivalentemente:

1.  $I + J = A$
2.  $1 \in I + J$

**Osservazione:** In  $\mathbb{Z}$  gli ideali  $m\mathbb{Z}$  e  $n\mathbb{Z}$  sono coprimi se e solo se  $\text{MCD}(m, n) = 1$ . Infatti:

$$\text{MCD}(m, n) = 1 \Leftrightarrow \exists a, b \in \mathbb{Z} : am + bn = 1 \Leftrightarrow 1 \in m\mathbb{Z} + n\mathbb{Z}$$

Questa cosa funziona solo se  $\text{MCD}(m, n) = 1$

### Teorema Cinese del Resto per $A = \mathbb{Z}$

Dati  $m, n \in \mathbb{Z}_{>0}$ , allora si ha che

$$\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

se e solo se  $\text{MCD}(m, n) = 1$

#### Dimostrazione:

Sia  $\text{MCD}(m, n) > 1$ . Allora si ha che  $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$  non è isomorfo a  $\mathbb{Z}/nm\mathbb{Z}$  come gruppo.

Comunque sia basta dimostrare che  $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$  non è ciclico.

Mostriamo che ogni elemento di  $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$  ha ordine minore o uguale a  $\frac{mn}{d}$  con  $d = \text{MCD}(m, n)$

$$\forall (a, b) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}, \frac{mn}{d}(a, b) = \left( \frac{mna}{d}, \frac{mnb}{d} \right) = \left( n \cdot \frac{m}{d}a, m \cdot \frac{n}{d}b \right) = (0, 0)$$

Quindi non è ciclico.

Se invece si ha che  $\text{MCD}(m, n) = 1$ . Applichiamo il metateorema e cerchiamo un omomorfismo

$$\varphi : \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

tale che sia suriettivo e che  $\text{Ker}(\varphi) = nm\mathbb{Z}$

Per il primo teorema di omomorfismo si ha che  $\mathbb{Z}/nm\mathbb{Z} \cong \text{Im}(\varphi)$

Ne segue che  $\text{Im}(\varphi) = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$  perché hanno la stessa cardinalità

□

### Quarto Teorema di Omomorfismo o Teorema Cinese del Resto Generale

Sia  $A$  anello unitario e siano  $I, J$  ideali coprimi. Allora si ha che

$$IJ = I \cap J \quad \text{e} \quad A/(IJ) = A/(I \cap J) \cong A/I \times A/J$$

#### Dimostrazione:

Notiamo che  $I \cap J \supseteq IJ$  è sempre vera

Dimostriamo l'altra inclusione. Sia  $z \in I \cap J$

Poiché si ha che  $I, J$  sono coprimi, si ha che  $1 \in I + J$ , cioè  $\exists x \in I, \exists y \in J : 1 = x + y$

Se facciamo il prodotto sia a destra che a sinistra con  $z$  si ottiene che

$$z \cdot 1 = \underbrace{z \cdot x}_{\in J} + \underbrace{z \cdot y}_{\in I} \in IJ$$

Quindi abbiamo dimostrato l'uguaglianza.

Dimostriamo adesso la seconda parte del teorema applicando il metateorema.

Vogliamo una funzione suriettiva

$$\varphi : A \rightarrow A/(I \cap J) \cong A/I \times A/J$$

con  $Ker(\varphi) = IJ$

Poniamo  $\varphi(a) = ([a]_I, [a]_J)$ . Notiamo che  $\varphi$  è un omomorfismo *sempre per gli stessi calcoli precedenti*

Analizziamo per bene il nucleo di questa funzione:

$$Ker(\varphi) : \{a \in A : [a]_I = [0]_I, [a]_J = [0]_J\} = \{a \in A : a \in I, a \in J\} = IJ$$

Mostriamo ora la suriettività di  $\varphi$ , sia quindi  $([a]_I, [b]_J) \in A/I \times A/J$

Poiché si ha che  $I, J$  sono coprimi, segue che  $a = x_a + y_a$  con  $x_a \in I$  e  $y_a \in J$ , in maniera del tutto analoga per  $b = x_b + y_b$

Definiamo con  $a' = y_a + x_b$ , e calcoliamo  $[a']_I$  e  $[a']_J$

$$\begin{aligned}[a']_I &= [y_a + x_b]_I = [y_a]_I = [y_a + x_a]_I = [a]_I \\ [a']_J &= [y_a + x_b]_J = [x_b]_J = [y_b + x_b]_J = [b]_J\end{aligned}$$

Quindi si ha che  $([a]_I, [b]_J) = ([a']_I, [a']_J) = \varphi(a')$

□

### Esempio di Applicazione del Quarto Teorema di Omomorfismo

Sia  $A = \mathbb{R}[x]$  e siano  $I = (x^2 + 1), J = (x + 1)$ .  $I, J$  sono coprimi?

$$\underbrace{(x^2 + 1)}_{\in I} - x \underbrace{(x + 1)}_{\in J} = x^2 + 1 - x^2 - x = 1 - x \in I + J$$

Ma allora è anche vero che

$$\underbrace{(1 - x)}_{\in I + J} - \underbrace{(1 + x)}_{\in I + J} = 2$$

Poiché 2 è invertibile in  $\mathbb{R}[x]$  segue che  $I + J = \mathbb{R}[x]$ .

Allora per il quarto teorema di omomorfismo si ha che

$$\mathbb{R}[x]/(x+1) \times \mathbb{R}[x]/(x^2+1) \cong \mathbb{R}[x]/(1+x+x^2+x^3)$$

### Definizione di Caratteristica di un Anello

Sia  $A$  un anello unitario. Si definisce Caratteristica di  $A$  il numero  $n \in \mathbb{Z}_{>0}$  se il sottoanello fondamentale (immagine dell'omomorfismo fondamentale) è isomorfo a  $\mathbb{Z}/n\mathbb{Z}$

### Esempio di Caratteristica

Se  $n = 0$  allora si ha che  $\mathbb{Z}/0\mathbb{Z} = \mathbb{Z}$

In generale se  $A$  ha cardinalità  $m$ , allora  $m \in A$  è uguale a 0. In particolare, considerato l'omomorfismo:

$$\begin{aligned}\varphi : \mathbb{Z} &\rightarrow A \\ k &\mapsto k\end{aligned}$$

Per il primo teorema di omomorfismo si ha che  $\mathbb{Z}/Ker(\varphi) \cong Im(\varphi)$

Inoltre  $Im(\varphi)$  è l'anello fondamentale di  $A$  e  $Ker(\varphi) = (n) = n\mathbb{Z}$

**Osservazione:** L'anello  $\mathbb{Z}/n$  ha caratteristica  $n$

$\mathbb{Z}[x]$  è un anello a caratteristica 0 in quanto il sottoanello fondamentale è esattamente  $\mathbb{Z}$

**Osservazione Importante:** Se  $A$  è un dominio, allora la sua caratteristica è un numero primo oppure zero

Infatti se  $m = 0$  in  $mA$ , con  $m > 1$  e non è primo, allora  $m = ab$  con  $a < m$  e  $b < m$

Visto che è un dominio, se  $m = 0$  allora uno tra  $a$  e  $b$  è nullo, quindi  $Char(A) \leq a$  oppure  $Char(b) \leq 0$

### Conseguenza Cruciale

Se  $A$  è un anello finito di caratteristica  $p$ , allora  $\exists n \in \mathbb{Z}_{>0} : |A| = p^n$

**Osservazione:**  $A$  è uno  $\mathbb{Z}/p$  spazio vettoriale. Infatti se  $A$  ha un sottoanello isomorfo a  $\mathbb{Z}/p$ : se  $\exists c \in \mathbb{Z}/p$  e  $a \in A$ , allora posso definire il prodotto per scalari sulla base del prodotto interno all'anello:  $c \cdot a$ . Tutto questo è possibile grazie al fatto che  $\mathbb{Z}/p \subseteq A$

Tutte le altre proprietà della definizione di spazio vettoriale sono racchiuse nella definizione di anello.

In particolare se la dimensione  $\dim_{\mathbb{Z}/p}(A) = n$ , allora esiste una base  $\{b_1, \dots, b_n\}$  di  $A$  è ogni elemento di  $A$  si scrive in modo unico come loro combinazione.

---

# Estensioni Quadratiche

## Definizione di Estensione Quadratica

Sia  $A$  un anello e  $d \in A$ . Si definisce estensione quadratica di  $A$  l'insieme:

$$A[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in A, \varepsilon^2 = d\}$$

La cosa può funzionare anche se  $d$  è già un quadrato in  $A$ , infatti in, per esempio,  $\mathbb{Z}[\sqrt{4}]$  si ha che  $\varepsilon^2 = 2^2 = (-2)^2$  però sono due oggetti completamente diversi,  $\varepsilon \neq 2 \neq -2$

Le operazioni in  $A[\sqrt{d}]$  sono definite in maniera naturale:

- $[+] : (a + b\sqrt{d}) + (a' + b'\sqrt{d}) = (a + a') + (b + b')\sqrt{d}$
- $[\cdot] : (a + b\sqrt{d}) \cdot (a' + b'\sqrt{d}) = (aa' + dbb') + (ab' + ba')\sqrt{d}$

## Lemma

Sia  $A = \mathbb{Z}$  oppure  $\mathbb{Q}$  e siano  $a, b, d \in A$  tali che  $a^2 - db^2 = 0$  con  $d$  non quadrato in  $A$ . Allora  $a = b = 0$

### Dimostrazione:

Per ogni elemento  $a \in A$ , poiché siamo in  $\mathbb{Z}$  o in  $\mathbb{Q}$  si ha che si può scrivere  $a$  come scomposizione unica di fattori primi con un esponente intero, ossia:

$$a = \prod_p p^{m_p(a)}$$

In particolare, se è razionale, gli esponenti del numeratore hanno esponente positivo, mentre quelli del denominatore hanno esponente negativo, comunque sia scritti in modo unico e con esponente intero.

Osserviamo che se  $a$  è un quadrato in  $A$ , quindi per ogni primo  $p$  si ha che  $m_p(a)$  è pari.

Visto che  $d$  non è un quadrato in  $A$  si ha che esiste un primo  $\bar{p}$  tra i divisori di  $d$  tale che  $m_{\bar{p}}(d)$  è dispari.

Per ipotesi si ha che  $a^2 - db^2 = 0 \Rightarrow a^2 = db^2$ .

Se  $a \neq 0$ , visto che  $\mathbb{Z}$  e  $\mathbb{Q}$  sono domini, segue necessariamente che  $b \neq 0$

Tuttavia segue che  $m_{\bar{p}}(a)$  è pari mentre  $m_{\bar{p}}(db)$  è dispari, quindi c'è un assurdo sull'uguaglianza  $a^2 = db^2$

Quindi necessariamente si ha che  $a = b = 0$

□

## Esempio sulle Estensioni Quadratiche

Sia  $\mathbb{Z}[\sqrt{2}]$ . Questo è un dominio (non ha divisori dello zero)

Infatti, se prendiamo due elementi qualsiasi in  $\mathbb{Z}[\sqrt{2}]$  tali che  $(a + b\sqrt{2}) \cdot (a' + b'\sqrt{2}) = 0$  si ha che uno tra i due è nullo.

Infatti, sviluppando il prodotto:

$$(aa' + 2bb') + (ab' + ba')\sqrt{2} = 0 \Rightarrow \begin{cases} aa' + 2bb' = 0 \\ ab' + ba' = 0 \end{cases}$$

Supponiamo ora che  $b' \neq 0$ . Dalla seconda equazione abbiamo che  $a = \frac{-a'b}{b'}$  e sostituendolo nella prima si ha che:

$$aa' + 2dbb' = 0 \Rightarrow -\frac{a'b}{b'}a' + 2bb' = 0 \xrightarrow{\text{Moltiplicando per } bb'} -(a'b)^2 + 2(bb')^2 = 0$$

Tuttavia, poiché 2 non è un quadrato in  $\mathbb{Z}$  si ha che  $a'b = 0$  e  $bb' = 0$  ma se  $b' \neq 0$  per quanto posto prima, segue che  $a = b = 0$

Quindi  $(a + b\sqrt{2}) = 0$ , quindi  $\mathbb{Z}[\sqrt{2}]$  è un dominio.

In maniera del tutto analoga possiamo dimostrare che  $\mathbb{Q}[\sqrt{2}]$  è un campo.

Sia  $(a + b\sqrt{2}) \neq 0$ , cioè siano  $a, b$  non entrambi nulli. Allora per il lemma precedente si ha che  $a^2 - 2b^2 \neq 0$  e possiamo

verificare che:  $\frac{a}{a^2 - 2b^2} - \frac{b\varepsilon}{a^2 - 2b^2}\varepsilon$  è l'inverso di  $a + b\varepsilon$ :

$$(a + b\varepsilon) = \left( \frac{a}{a^2 - 2b^2} - \frac{b\varepsilon}{a^2 - 2b^2} \right) = \frac{1}{a^2 - 2b^2}((a + b\varepsilon) \cdot (a - b\varepsilon)) = \frac{1}{a^2 - 2b^2}(a^2 - 2b^2) = 1$$

**Osservazione:** Un sottoanello di un dominio è un sempre un dominio, quindi  $\mathbb{Q}[\sqrt{2}]$  dominio  $\Rightarrow \mathbb{Z}[\sqrt{2}]$  campo.

**Osservazione:** Se  $d$  non è un quadrato di  $A$  è lecito denotare  $\varepsilon$  con  $\sqrt{d}$ , altrimenti no. Infatti con  $\sqrt{d}$  andremmo ad indicare quell'elemento  $a \in A$  tale che  $a^2 = d$

### Definizione di Norma

Sia  $A$  un anello unitario e  $A[\sqrt{d}]$  una sua estensione. Si definisce Norma una funzione

$$N : A[\sqrt{d}] \rightarrow A$$

data da:

$$N(a + b\varepsilon) = a^2 - db^2$$

### Definizione di Coniugio

Sia  $A$  un anello unitario e  $A[\sqrt{d}]$  una sua estensione. Si definisce Coniugio una funzione da  $A[\sqrt{d}]$  in sé stessa tale che

$$\overline{a + b\varepsilon} = a - b\varepsilon$$

Notiamo subito che la Norma non è un omomorfismo di anelli, in quanto  $N(1 + 1) = N(2) = 4 \neq 2 = N(1) + N(1)$

### Lemma

Sia  $A$  un anello unitario e commutativo e  $A[\sqrt{d}]$  una sua estensione, allora:

1. Il Coniugio è un automorfismo di  $A[\sqrt{d}]$
2.  $\forall \alpha, \beta \in A[\sqrt{d}]$  si ha che  $N(\alpha\beta) = N(\alpha)N(\beta)$ . Inoltre  $N(\alpha) = \alpha\bar{\alpha}$

### Dimostrazione:

1. Il coniugio è biunivoco perché è un involuzione (l'inverso del Coniugio è il Coniugio stesso)

Inoltre se  $\alpha = a + b\varepsilon$  e  $\alpha' = a' + b'\varepsilon$  si ha che:

$$\begin{aligned} \overline{\alpha + \alpha'} &= (a + a') + (b + b')\varepsilon = \bar{a} - \bar{a}' \\ \overline{\alpha \cdot \alpha'} &= (aa' + dbb') - (ab' + ba')\varepsilon = (a - b\varepsilon) \cdot (a' - b'\varepsilon) = \bar{a} \cdot \bar{a}' \end{aligned}$$

2. Mostriamo prima che  $\alpha\bar{\alpha} = N(\alpha)$

Riprendendo l' $\alpha$  della parte precedente abbiamo che  $\alpha\bar{\alpha} = (a + b\varepsilon)(a - b\varepsilon) = a^2 - db^2 = N(\alpha)$

Allora, unendo quanto trovato dai punti precedenti otteniamo che:

$$N(\alpha\beta) \stackrel{2.}{=} \alpha\beta\bar{\alpha}\bar{\beta} \stackrel{1.}{=} \alpha\bar{\alpha}\bar{\beta}\beta = \alpha\bar{\alpha}\beta\bar{\beta} \stackrel{2.}{=} N(\alpha)N(\beta)$$

□

### Proposizione

Sia  $A$  un anello e sia  $A[\sqrt{d}]$  una sua estensione, allora  $A$  è un dominio se e solo se  $A$  è un dominio e l'unico elemento di norma nulla è 0

### Dimostrazione:

$\Rightarrow$ ) Un Sottoanello di un dominio di un dominio è sempre un dominio, quindi  $A$  è un dominio.

Sia  $\alpha \in A[\sqrt{d}]$  tale che  $N(\alpha) = 0$ , allora  $\alpha\bar{\alpha} = 0$ . Poiché  $A[\sqrt{d}]$  è un dominio segue che uno tra  $\alpha$  e  $\bar{\alpha}$  è nullo, ma poiché uno

è il coniugato dell'altro segue che  $\alpha$  è l'elemento nullo

$\Leftarrow$ ) Siano  $\alpha, \beta \in A[\sqrt{d}]$  tale che  $\alpha\beta = 0$  allora si ha che  $N(\alpha\beta) = 0$  ma per il lemma precedente si ha che  $N(\alpha)N(\beta) = 0$

Tuttavia, per come è stata definita la norma si ha che  $N(\alpha), N(\beta) \in A$  e poiché  $A$  è un dominio per ipotesi, segue che una tra  $N(\alpha)$  e  $N(\beta)$  è nullo, quindi uno tra  $\alpha$  e  $\beta$  è l'elemento nullo.

□

**Osservazione:** Se  $d$  è un quadrato in  $A$ , allora  $A[\sqrt{d}]$  non è mai un dominio.

Infatti, se  $d = a^2$  allora si ha che  $(a + \varepsilon)(a - \varepsilon) = a^2 - d = 0$ , ma abbiamo che  $(a + \varepsilon) \neq 0$  e  $(a - \varepsilon) \neq 0$ . Quindi non è un dominio.

Può accadere anche che  $d$  non è un quadrato, ma  $A[\sqrt{d}]$  non è un dominio

### Proposizione

Sia  $A$  un anello unitario e commutativo e sia  $A[\sqrt{d}]$  una sua estensione di campo.

Allora si ha che  $\alpha \in A[\sqrt{d}]$  è invertibile se e solo se  $N(\alpha)$  è invertibile in  $A$

### Dimostrazione:

Se  $\alpha$  è invertibile, allora  $\exists \beta \in A[\sqrt{d}]$  tale che  $\alpha\beta = 1$ , quindi  $N(\alpha\beta) = N(\alpha)N(\beta) = N(1) = 1$ , cioè  $N(\alpha)$  è invertibile in  $A$ . Viceversa se  $N(\alpha)$  è invertibile in  $A$ , allora  $N(\alpha)^{-1} = \bar{\alpha}$  è l'inverso di  $\alpha$

□

### Proposizione

Sia  $K$  un campo e  $d \in K$ . Allora  $d$  non è un quadrato in  $K$  se e solo se l'unico elemento di norma nulla è 0-. Inoltre  $K[\sqrt{d}]$  è un campo se e solo se  $d$  non è un quadrato

### Dimostrazione:

$\Rightarrow$ ) Sia  $\alpha \in K[\sqrt{d}]$  tale che  $N(\alpha) = 0$ . In particolare, se  $\alpha = a + b\varepsilon$ , allora  $N(\alpha) = a^2 - db^2 = 0$

Se  $a = 0$ , allora si ha che  $b = 0$  oppure  $d = 0$ , quindi  $\alpha = 0$  oppure  $d = 0$

Se  $b = 0$ , allora si ha che  $a = 0$  e per il lemma di Inizio Capitolo si ha che  $\alpha = 0$

Supponiamo ora  $a \neq 0$  e  $b \neq 0$ , allora, poiché  $K$  campo, si ha che  $d = a^2b^{-2} = (ab^{-1})^2$ , quindi  $d$  è un quadrato

$\Leftarrow$ ) Se  $d$  fosse quadrato  $d = a^2$ , allora  $N(a + \varepsilon) = 0$  per quanto visto prima

L'ultima affermazione segue dalla precedente dimostrazione e dal lemma visto ad inizio capitolo.

Se  $d$  non è un quadrato, allora ogni  $\alpha \neq 0$  ha  $N(\alpha) \neq 0$  per la prima parte e per il lemma  $\alpha$  è invertibile.

□

Sia  $K = \mathbb{Z}/p$ , se trovo  $d \in \mathbb{Z}/p$  non quadrato, allora posso considerare  $F = \mathbb{Z}/p[\sqrt{d}]$  campo che ha  $p^2$  elementi.

Ancora, se  $F$  contiene un elemento  $\delta$  non quadrato, allora posso considerare  $F[\sqrt{\delta}]$  campo con  $p^4$  elementi

**Osservazione:** Sia  $K$  un campo finito e consideriamo l'applicazione:

$$\begin{aligned} K &\rightarrow K \\ a &\mapsto a^2 \end{aligned}$$

Quando è iniettiva?  $a^2 = b^2 \Rightarrow a^2 - b^2 = 0 \Rightarrow (a + b)(a - b) = 0$ , poiché è dominio si ha che  $a = \pm b$

A questo punto entra in gioco la Caratteristica del campo:

- Se  $\text{Char}(K) = 2$ , allora si ha che  $b = -b$ , per cui ogni elemento è un quadrato

- Se  $\text{Char}(K) \neq 2$ , allora  $b \neq -b$  se  $b \neq 0$  per la legge di cancellazione (infatti può essere vista come  $b = -b = b \cdot 1 = b \cdot (-1)$ , per cui per la legge di cancellazione  $1 = -1$ , il che è assurdo in quanto questo è vero solo se la caratteristica del campo è 2). Quindi esistono elementi non quadrati

In conclusione: se  $p$  primo è dispari, allora  $\forall n$  esiste un campo con  $p^{2^n}$  elementi (continuando esattamente come visto prima di quest'osservazione).

Per quanto visto nell'Osservazione Importante alla fine del capitolo precedente un campo finito ha necessariamente  $p^n$  elementi, con  $p$  primo e  $n$  numero maggiore di 0.

Uno degli obiettivi principali del corso sarà mostrare che  $\forall p$  primo e  $\forall n > 0, \exists!$  campo (a meno di isomorfismi) con  $p^n$  elementi

Studiamo meglio  $\mathbb{Z}/p[\sqrt{-1}]$ . Quando è un campo?

- con  $p = 3$  si ha che  $-1$  non è un quadrato, quindi  $\mathbb{Z}/3[\sqrt{-1}]$  è un campo
- se  $p = 5$  si ha che  $-1 = 4 = 2^2$ , quindi non è un campo
- se  $p = 7$  allora non c'è nessun numero che al quadrato venga  $-1$ , quindi è un campo

Cerchiamo di generalizzarlo.

### Teorema

$-1$  è un quadrato in  $\mathbb{Z}/p$  se e solo se  $p \equiv 1 \pmod{4}$ , con  $p$  primo dispari

#### Dimostrazione:

$\Rightarrow$ ) Se  $-1$  è un quadrato in  $\mathbb{Z}/p$  allora esiste un numero  $a \in \mathbb{Z}/p$  tale che  $a^2 = -1$ .

Sicuramente si ha che  $a \neq \pm 1$  in quanto  $(\pm 1)^2 = 1$

Abbiamo quindi che, riprendendo il gruppo moltiplicativo  $(\mathbb{Z}^*, \cdot)$  si ha che  $o(a) = 4$

Allora per il teorema di Lagrange si ha che  $o(a) \mid |\mathcal{U}(\mathbb{Z}_p)| \Rightarrow 4 \mid p-1 \Rightarrow 4k = p-1$  da cui segue che  $p \equiv 1 \pmod{4}$

$\Leftarrow$ ) Per dimostrare l'altra implicazione sfruttiamo questo lemma:

### Lemma

Il prodotto di tutti gli elementi non nulli in  $\mathbb{Z}/p$  è  $-1$

#### Dimostrazione:

$$\prod_{x \in \mathbb{Z}/p; x \neq 0} x$$

In questo prodotto compaiono tutti i numeri in  $\mathbb{Z}/p$  tolto l'elemento nullo.

Notiamo che tutti gli elementi diversi dal proprio inverso si semplificano tra loro.

Quindi rimangono solamente quelli che coincidono con il proprio inverso, cioè quelli tali che:

$$x \cdot x = 1 \Rightarrow x^2 - 1 = 0 \Rightarrow (x+1)(x-1) = 0 \xrightarrow{\mathbb{Z}/p \text{ campo}} x = \pm 1$$

Quindi, poiché rimangono solo  $1$  e  $-1$  si ha che il prodotto precedente è uguale a  $-1$

□

Completiamo ora la dimostrazione del teorema.

$$-1 \equiv \prod_{x \in \mathbb{Z}/p; x \neq 0} x = (1)(-1) \cdot (2)(-2) \cdot (3)(-3) \cdot \dots \cdot \left(\frac{p-1}{2}\right) \left(-\frac{p-1}{2}\right) = (-1)^{\frac{p-1}{2}} \left(1 \cdot 2 \cdot 3 \cdot \dots \cdot \frac{p-1}{2}\right)^2$$

Tuttavia, poiché si ha che  $\frac{p-1}{2}$  è pari in quanto  $p \equiv 1 \pmod{4}$  per ipotesi, quindi segue la tesi in quanto

$$-1 = \left(1 \cdot 2 \cdot 3 \cdot \dots \cdot \frac{p-1}{2}\right)^2$$

□

Per esercizio estendere questa dimostrazione per mostrare che se  $K$  è un campo con  $q$  (dispari) elementi allora  $-1$  è un quadrato in  $K$  se e solo se  $q \equiv 1 \pmod{4}$

# Divisibilità

Da qui in avanti considereremo  $A$  un dominio di integrità

## Definizione di Divisore

Siano  $a, b, c \in A$ . Si dice che  $a$  è un divisore di  $b$  se  $\exists c \in A : ac = b$

## Proprietà

Siano  $a, b, c \in A$  e  $u \in A$  invertibile. Allora valgono le seguenti proprietà:

- $a | b$  e  $a | c \Rightarrow a | c$
- $u | a, \forall a \in A$
- $a | u \Leftrightarrow a$  è invertibile
- $a | 0, \forall a \in A$  infatti  $\exists 0 \in A : a \cdot 0 = 0$
- $0 | a \Leftrightarrow a = 0$
- Se  $a | b$  e  $a | c$  allora  $a$  è divisore di ogni combinazione lineare  $xb + yc, \forall x, y \in A$
- Se  $a | b$  e  $a | b + c$  allora  $a | c$

## Definizione di Elementi Associati

Due elementi  $a, b \in A$  si dicono associati se  $\exists u \in A$  invertibile tale che  $a = ub$

**Osservazione:** Essere associati è una relazione di equivalenza, infatti:

- $a = a \cdot 1$ , quindi è verificata la proprietà simmetrica
- $a = ub \Rightarrow b = u^{-1}a$ , quindi è verificata la proprietà simmetrica
- $a = bu$  e  $b = cu' \Rightarrow a = cuu'$ , quindi è verificata la proprietà transitiva.

## Lemma

Siano  $a, b \in A$ , allora sono equivalenti:

1.  $a$  e  $b$  sono associati
2.  $a | b$  e  $b | a$
3.  $(a) = (b)$

**Dimostrazione:**

$$1 \Rightarrow 2) a = bu \Rightarrow b | a \text{ ma poiché } a = bu \Leftrightarrow b = au' \Rightarrow a | b$$

$$2 \Rightarrow 3) \text{ Notiamo che } (a) \subseteq (b) \text{ in quanto } a = b \cdot u \in (b) \text{ e in maniera del tutto simmetrica si ottiene che } (b) \subseteq (a)$$

$3 \Rightarrow 1)$  Sia  $(a) = (b)$ . Si ha quindi la situazione che

$$\begin{aligned} a \in (b) &\Leftrightarrow \exists x \in A : a = bx \\ b \in (a) &\Leftrightarrow \exists y \in A : b = ay \end{aligned} \Rightarrow a = bx = ayx$$

Se  $a \neq 0$  allora per la proprietà di cancellazione si ha che  $yx = 1$  quindi  $y$  e  $x$  sono invertibili e l'uno è l'inverso dell'altro.

Se  $a = 0$  allora  $(a) = \{0\} = (b)$  quindi anche  $b = 0$ , quindi  $a$  e  $b$  sono associati

□

Come sono le classi di associazione in  $\mathbb{Z}$ ?

Sono le coppie di numeri opposti e zero da solo

Come sono le classi di associazione in  $\mathbb{R}[x]$ ?

Due polinomi sono associati se e solo se uno è multiplo dell'altro

**Osservazione:** Se  $A$  è un dominio allora si ha che:

- $\{0\}$  è una classe a se
- Gli elementi invertibili creano una classe a sé

### Definizione di Primo e Irriducibile

Sia  $a \in A, a \neq 0$ , non invertibile. allora si dice che:

- $a$  è irriducibile se  $\forall b, c \in A$  si ha che se  $a = bc \Rightarrow c$  invertibile oppure  $b$  invertibile
- $a$  è primo se  $\forall b, c \in A$  si ha che  $a | bc \Rightarrow a | b \vee a | c$

**Notazione:** Possiamo scrivere  $NINZ$  per indicare un numero non invertibile e diverso da zero, letteralmente *non invertibile non zero*.

Da Algebra 1 abbiamo che se un elemento è primo, allora è irriducibile.

Infatti se  $a = bc$  allora  $a | bc$  e poiché  $a$  è primo si ha che  $a | b$  oppure  $a | c$

Supponiamo  $a | c$  allora si ha che  $b = ax$  quindi  $a = axc$  ma poiché  $a \neq 0$  segue che  $c$  è invertibile

In maniera analoga si faceva se  $a | b$

Irriducibile non implica Primo

Prendiamo  $\mathbb{Z}[\sqrt{-5}]$ , qui si ha che  $6 = 2 \cdot 3 = (1 + \varepsilon)(1 - \varepsilon)$

Notiamo che  $2 \in \mathbb{Z}[\sqrt{-2}]$  è irriducibile, infatti  $N(2) = 4$ , cioè dovrebbero esistere due elementi  $b, c \in \mathbb{Z}[\sqrt{-5}]$  tali che  $N(bc) = 4$

Per come è stata definita la norma segue che  $N(bc) = N(b)N(c)$ , analizziamo i casi possibili:

- $N(b) = 1$ , allora  $b$  è invertibile, quindi è una fattorizzazione banale
- $N(b) = 4$ , allora  $N(c) = 1$  quindi  $c$  è invertibile, sempre una fattorizzazione banale
- $N(b) = N(c) = \pm 2$ . Notiamo che  $\forall x, y \in \mathbb{Z}, N(x + y\varepsilon) = x^2 + 5y^2$ , quindi è sempre positivo. Tuttavia  $\nexists x, y \in \mathbb{Z}$  tali che  $N(x + y\varepsilon) = x^2 + 5y^2 = 2$ . Quindi 2 è irriducibile.

Tuttavia 2 non è primo in  $\mathbb{Z}[\sqrt{-5}]$ , infatti esistono  $b, c \in \mathbb{Z}[\sqrt{-5}]$  tali che  $2 | bc$  ma  $2 \nmid b$  e  $2 \nmid c$ .

Per sopra basta prendere  $b = (1 + \varepsilon)$  e  $c = (1 - \varepsilon)$ , infatti  $2 | (1 + \varepsilon)(1 - \varepsilon)$  ma 2 non divide nessuno dei due

### Definizione di Dominio Euclideo

Un dominio  $A$  si dice Euclideo e si indica con  $ED$  se  $\exists \rho : A \rightarrow \mathbb{Z}$  tale che:

- 1)  $\rho(0) < \rho(a), \forall a \neq 0$
- 2)  $\forall a, b \in A$ , con  $b \neq 0$  si ha che  $\exists q, r \in A : a = bq + r$  con  $\rho(r) < \rho(b)$
- 3)  $\forall a, b \in A, a, b \neq 0$  si ha che  $\rho(a) \leq \rho(ab)$

Alcuni esempi di domini euclidei sono  $\mathbb{Z}$  con  $\rho(n) = |n|$  e  $K[x]$  con  $K$  campo e  $\rho(p) = \deg(p)$

### Teorema

Sia  $\mathbb{Z}[\sqrt{d}]$  con  $d \in \{-1, 2, -2\}$ . Allora  $\mathbb{Z}[\sqrt{d}]$  è un dominio con  $\rho(\alpha) = |N(\alpha)|$

**Dimostrazione:**

- 1)  $\rho(0) = 0$  e se avessi  $\alpha = a + b\varepsilon$  si ha che

$$\rho(\alpha) = |N(\alpha)| = |a^2 - db^2|$$

Ma questo è maggiore o uguale a zero se  $d \in \{-1, -2\}$  con  $\alpha \neq 0$ . Inoltre se  $d = 2$  si ha che  $N(\alpha) \neq 0$  per un lemma precedente.

3) Vogliamo mostrare che  $\rho(\alpha) \leq \rho(\alpha\beta)$ , ciò implica che  $|N(\alpha)| \leq |N(\alpha\beta)| = |N(\alpha)N(\beta)|$  il che è vero in quanto  $N(\beta) \neq 0$

2) Siano  $\alpha, \beta \in \mathbb{Z}[\sqrt{d}]$  con  $\beta \neq 0$ . Notiamo che  $\alpha, \beta \in \mathbb{Q}[\sqrt{d}]$ , che è campo perché  $-1$  e  $\pm 2$  non sono quadrati in  $\mathbb{Q}$ .

Possiamo quindi considerare  $\beta^{-1} \in \mathbb{Q}[\sqrt{d}]$ .

Prendiamo allora  $\alpha\beta^{-1} \in \mathbb{Q}[\sqrt{d}]$ ,  $\alpha\beta^{-1} = x_1 + x_2\varepsilon$  con  $x_1, x_2 \in \mathbb{Q}$ . Cerchiamo di approssimare questo numero a un valore in  $\mathbb{Z}[\sqrt{d}]$

Siano quindi  $a_1, a_2 \in \mathbb{Z}$  tali che  $|x_1 - a_1| \leq \frac{1}{2}$  e  $|x_2 - a_2| \leq \frac{1}{2}$

Poiniamo quindi  $q = a_1 + a_2\varepsilon \in \mathbb{Z}[\sqrt{d}]$ , a questo punto otterremmo che  $r = \alpha - q\beta$ .

Per costruzione abbiamo che  $\alpha = q\beta + r$ .

Dobbiamo però verificare che  $\rho(r) < \rho(\beta)$ . Allora possiamo

$$r = \alpha - q\beta \Rightarrow \beta(\alpha\beta^{-1} - q) \Rightarrow \rho(r) = |N(r)| = |N(\beta)| \cdot |N(\alpha\beta^{-1} - q)| < |N(\beta)| = \rho(\beta)$$

Ci basta mostrare a questo punto che  $|N(\alpha\beta^{-1} - q)| < 1$

$$\begin{aligned} \alpha\beta^{-1} - q &= (x_1 + x_3\varepsilon) - (a_1 + a_2\varepsilon) = (x_1 - a_1) + (x_2 - a_2)\varepsilon \Rightarrow \\ |N(\alpha\beta^{-1} - q)| &= |(x_1 - a_1)^2 - d(x_2 - a_2)^2| \leq (x_1 - a_1)^2 + 2(x_2 - a_2)^2 \leq \frac{1}{4} + 2\frac{1}{4} = \frac{3}{4} < 1 \end{aligned}$$

□

### Esempio di Divisione con Resto

Prendiamo  $A = \mathbb{Z}[\sqrt{2}]$  e prendiamo  $\alpha = 3 + 2\varepsilon$  e  $\beta = 1 + 2\varepsilon$

Per il teorema, dobbiamo prima trovare  $\beta^{-1}$  quindi

$$N(\beta) = 1^2 - 2 \cdot 2^2 = -7 \Rightarrow \beta^{-1} = \frac{\bar{\beta}}{N(\beta)} = -\frac{1}{7} + \frac{2}{7}\varepsilon$$

Da cui segue che

$$\alpha\beta^{-1} = \frac{1}{7}(3 + 2\varepsilon)(-1 + 2\varepsilon) = \frac{1}{7}(-3 + 8 + 6\varepsilon - 2\varepsilon) = \frac{5}{7} + \frac{4}{7}\varepsilon$$

Scegliamo quindi  $q = 1 + \varepsilon$ , segue quindi che

$$r = \alpha - q\beta = 3 + 2\varepsilon - (1 + \varepsilon)(1 + 2\varepsilon) = 3 + 2\varepsilon - (1 + 4 + \varepsilon + 2\varepsilon) = -2 - \varepsilon$$

Verifichiamo che sia effettivamente una soluzione:  $\rho(-2 - \varepsilon) = |4 - 2| = 2$

### Definizione di Anello di Gauss

Si definisce Anello di Gauss, l'anello  $\mathbb{Z}[i]$

**Osservazione:** Un campo  $K$  è anche un Dominio Euclideo con  $\rho(0) = 0$  e  $\rho(a) = 1$  con  $a \neq 0$ .

Infatti per verificare le tre proprietà basta notare che:

1.  $\rho(0) < \rho(a)$  per ogni  $a \in A, a \neq 0$  dalla definizione
3.  $\rho(a) = \rho(ab) = 1$  quindi è verificata  $\rho(a) \leq \rho(ab)$
2. segue dal fatto che  $q = ab^{-1}$  e  $r = 0$

Definiamo, per semplicità,  $\rho_0 = \min\{\rho(a) : a \neq 0\}$

### Lemma

Sia  $a \in A$  con  $A$  un dominio euclideo. Allora  $A$  è invertibile se e solo se  $\rho(a) = \rho_0$

### Dimostrazione:

$\Leftarrow$ ) Sia  $\rho(a) = \rho_0$ . Facciamo la divisione euclidea di 1 per  $a$ . Otteniamo quindi che  $1 = qa + r$ , con  $\rho(r) < \rho(a)$ . Tuttavia, poiché  $\rho(a) = \rho_0$ , segue necessariamente che  $\rho(r) = 0$  per la minimalità di  $a$  e per la definizione di  $\rho$  segue che  $r = 0$ .

Quindi  $1 = qa$ , quindi  $a$  è invertibile

$\Rightarrow$ ) Sia  $b$  invertibile e sia  $a \in A : \rho(a) = \rho_0$ . Per la prima parte si ha che  $a$  è invertibile, inoltre per la proprietà 3 di  $\rho$  si ha che:

$$\begin{cases} \rho(b) = \rho(ba^{-1}a) \geq \rho(a) \\ \rho(a) = \rho(ab^{-1}b) \geq \rho(b) \end{cases} \Rightarrow \rho(b) = \rho(a) \stackrel{\text{Hp}}{=} \rho_0$$

□

### Definizione di $\text{MCD}$

Sia  $A$  è un dominio e siano  $a, b, d \in A$ . Diciamo che  $d \in A$  è un Massimo Comun Divisore tra  $a$  e  $b$  e indichiamo con

$$d = \text{MCD}(a, b)$$

se:

1.  $d \mid a$  e  $d \mid b$
2. se  $\exists d' \in A : d' \mid a$  e  $d' \mid b \Rightarrow d' \mid d$

**Osservazione:** Il  $\text{MCD}$  è unico a meno di associati, cioè se  $d_1 = \text{MCD}(a, b)$  e  $d_2 \in A$ , allora  $d_2 = \text{MCD}(a, b) \Leftrightarrow d_1 \sim d_2$  sono associati. Va sottolineato che stiamo usando un abuso di notazione, infatti se  $d_1 = \text{MCD}(a, b)$  e  $d_2 = \text{MCD}(a, b) \not\Rightarrow d_1 = d_2$

Controesempio per MCD

Prendiamo  $A = \mathbb{Z}[\sqrt{-5}]$  e scegliamo  $a = 6$  e  $b = 2(1 + \varepsilon)$

Vogliamo mostrare che non esiste  $\text{MCD}(a, b)$ . Supponiamo per assurdo che esiste  $d = \text{MCD}(a, b)$

Andiamo a calcolare le norme di  $a$  e di  $b$ :

$$\begin{cases} N(a) = 36 \\ N(b) = 24 \end{cases} \Rightarrow N(d) \mid 36 \wedge N(d) \mid 24 \Rightarrow N(d) \mid 12$$

Tuttavia abbiamo che  $a = (1 + \varepsilon)(1 - \varepsilon) = 2 \cdot 3$

Se  $a = (1 + \varepsilon)(1 - \varepsilon)$ , allora abbiamo che  $(1 + \varepsilon) \mid a$  e  $(1 + \varepsilon) \mid b$ , quindi  $(1 + \varepsilon) \mid d \Leftrightarrow 6 \mid N(d)$  da cui segue che  $N(d) = 6 \vee 12$

Se  $a = 2 \cdot 3$ , allora abbiamo che  $2 \mid a$  e  $2 \mid b$ , quindi  $2 \mid d$ , da cui segue che  $4 \mid N(d)$

Da queste due affermazioni segue che  $N(d) = 12$ , tuttavia  $N(x + y\varepsilon) = x^2 + 5y^2 \neq 12, \forall x, y \in \mathbb{Z}$ , cioè non esistono elementi di norma 12 in  $\mathbb{Z}[\sqrt{-5}]$

### Proposizione

Siano  $a, b, c, d, x \in A$  con  $A$  dominio tale che  $a = bx + c$ . Allora  $d = \text{MCD}(a, b) \Leftrightarrow d = \text{MCD}(c, b)$

### Dimostrazione:

Per ipotesi (da entrambe le parti) segue che  $d \mid b$ .

Da un lato segue che, poiché  $c = a - bx$ , si ha che  $d \mid c = a - bx$

Dall'altro, poiché  $a = bx + c$  si ha che  $d \mid a = bx + c$

□

### Proposizione

Se  $A$  è un dominio euclideo,  $a, b \in A$ , allora esiste  $\text{MCD}(a, b)$

### Dimostrazione:

Procediamo per induzione su  $\min\{\rho(a), \rho(b)\} = \rho(b)$  (per simmetria la cosa è totalmente indifferente)

*Base Induttiva:* Sia  $b = 0$ , allora  $\text{MCD}(a, 0) = a$

*Passo Induttivo:* Sia  $b \neq 0$ , allora  $a = qb + r$  con  $\rho(r) < \rho(b)$ . Per induzione abbiamo che esiste  $\text{MCD}(r, b)$ , quindi per la proposizione precedente esiste  $\text{MCD}(a, b)$

□

### Proposizione

Sia  $A$  un dominio euclideo e sia  $I$  ideale di  $A$ , allora  $\exists x \in A : I = (x)$

**Dimostrazione:**

Se  $I = \{0\}$ , allora  $I = (0)$

Sceglio  $x \in I : \rho(x) = \min\{\rho(y) : y \in I, y \neq 0\}$ . Sia quindi  $y \in I$ , allora  $y = qx + r$  con  $\rho(r) < \rho(x)$

Per la scelta di  $y$  abbiamo che  $y \in I$  e  $qx \in I$ , quindi necessariamente  $r \in I$ , ma la scelta fatta di  $x$ , cioè per la minimalità di  $x$ , abbiamo che  $r = 0$ , quindi  $y = qx$

□

### Definizione di Domini a Ideali Principali

Un dominio  $A$  i cui ideali sono principali si dice Dominio a Ideali Principali (*PID*)

**Osservazione:** Se un dominio è euclideo, allora è anche un dominio a ideali principali

Per esempio,  $\mathbb{Z}[x]$  non è né un *ED* né un *PID*, basta prendere l'ideale generato da  $(2, x)$

### Lemma

Se  $A$  è un dominio qualunque e  $a, b, d \in A$  sono tali che  $(a, b) = (d) \Rightarrow d = \text{MCD}(a, b)$

*Il viceversa non vale sempre, basta vedere l'esempio precedente*

**Dimostrazione:**

$d \mid a$  e  $d \mid b$  perché  $a, b \in (d)$ , quindi  $a$  e  $b$  sono multipli di  $d$

Sia  $d' \in A$  tale che  $d' \mid a$  e  $d' \mid b$ . Sappiamo che  $\exists x, y \in A : d = xa + yb \Rightarrow d' \mid d$

□

### Corollario

In un Dominio a Ideali Principali esiste sempre il *MCD*

### Lemma

Sia  $A$  è un dominio qualunque e siano  $a, b, c \in A : a \mid bc$  e  $(a, b) = (1) = A$  allora  $a \mid c$

**Dimostrazione:**

$\exists x, y \in A : xa + by = 1$ , moltiplicando per  $c$  segue che  $xac + ybc = c$  e poiché  $a \mid xac$  (perché c'è  $a$ ) e  $a \mid ybc$  (per Ipotesi), segue che  $a \mid c$

□

### Corollario

Sia  $A$  un dominio a ideali principali. Allora  $a \in A$  è irriducibile  $\Rightarrow a \in A$  è primo

**Dimostrazione:**

Siano  $b, c \in A : a \mid bc$ . Consideriamo  $\text{MCD}(a, b)$ , che esiste perché è Dominio a Ideali Principali

Allora, poiché  $a$  è irriducibile, si ha che  $\text{MCD}(a, b) = 1 \vee a$

Se  $\text{MCD}(a, b) = a \Rightarrow a \mid b$ , quindi  $a$  è primo

Se  $\text{MCD}(a, b) = 1 \Rightarrow (a, b) = (1)$ , allora sono verificate le ipotesi del lemma precedente, quindi  $a \mid c$

□

### Esempio di Irriducibile ma non Primo

Sia  $\mathbb{Z}[\sqrt{d}]$  con  $d \leq -3$ ,  $d$  dispari, allora  $\mathbb{Z}[\sqrt{d}]$  non è né dominio euclideo, né dominio ad ideali principali.

2 è irriducibile. Infatti, studiando la norma si ha che  $N(2) = 4$ . Se 2 avesse una fattorizzazione non banale si avrebbe che  $2 = \alpha\beta$  con  $N(\alpha) = N(\beta) = \pm 2$

Quindi  $N(a + b\sqrt{d}) = a^2 - db^2 \neq 2, \forall a, b \in \mathbb{Z}$ , quindi 2 è irriducibile.

Tuttavia non è primo perché  $2 | (1 + \varepsilon)(1 - \varepsilon) = 1 - \varepsilon^2 = 1 - d$  che è un numero pari, in quanto  $d$  è dispari per ipotesi.

Tuttavia  $2 \nmid (1 + \varepsilon)$  e  $2 \nmid (1 - \varepsilon)$  perché i multipli di 2 sono della forma  $2(a + b\sqrt{d}) = 2a + 2b\sqrt{d}$ , quindi hanno entrambe le coordinate pari.

### Definizione di Fattorizzazione in Irriducibili

Una fattorizzazione in irriducibili di un elemento  $a \in A$  è una scrittura di  $a$  tale che

$$a = p_1 \cdot p_2 \cdot \dots \cdot p_n$$

con  $p_i$  irriducibili.

In  $\mathbb{Z}$  se prendiamo  $-6$  abbiamo che

$$-6 = 2 \cdot (-3) = (-2) \cdot 3 = -3 \cdot 2 = 3 \cdot (-2)$$

Però possiamo pensarle come tutte uguali

### Definizione di Fattorizzazione Unica

Un dominio  $A$  si dice a fattorizzazione unica (o dominio fattoriale) se ogni  $a \in A \setminus \{0, \text{unit}\}$  ammette una fattorizzazione in irriducibili unica a meno dell'ordine e a meno di associati.

Per esempio in  $\mathbb{Z}[\sqrt{5}]$ ,  $6 = 2 \cdot 3 = (1 + \sqrt{5})(1 - \sqrt{5})$  sono due fattorizzazioni distinte

**Osservazione:** In un dominio a ideali principali, la fattorizzazione in irriducibili, se esiste, è unica.

Infatti sia  $a \in A \setminus \{0, \text{unit}\}$ ,  $a = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$ , dove  $p_i$  e  $q_j$  sono irriducibili.

Procediamo per induzione su  $\min\{r, s\} = r$  (per simmetria è la stessa cosa)

*Base Induttiva:* Se  $r = 1$ , allora  $p_1 = q_1 \cdots q_s$ , ma poiché  $p_1$  è irriducibile, non si può scrivere come prodotto di irriducibili, quindi  $s = 1$  e  $p_1 = q_1$

*Passo Induttivo:* sia  $r \geq 2 \Rightarrow p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$ . Abbiamo che  $p_1$  è primo, in quanto  $A$  è un dominio a ideali principali, quindi  $\exists i \in \{1, \dots, s\} : p_1 = q_i$ , quindi  $p_1$  e  $q_i$  sono associati perché  $q_i$  è irriducibile.

A meno dell'ordine possiamo assumere che  $q_i = q_1$ , quindi che  $q_1 = up_1$ , con  $u$  invertibile, ma allora

$p_1 p_2 \cdots p_r = up_1 q_2 \cdots q_s$  quindi per la proprietà di cancellazione si ha che  $p_2 \cdots p_r = q_2 \cdots q_s$ , quindi per l'ipotesi induttiva segue che  $r - 1 = s - 1$ , quindi  $r = s$  e i fattori sono gli stessi a meno dell'ordine e a meno degli associati

Non sempre però è possibile trovare una fattorizzazione:

Constroesempio dell'esistenza di una fattorizzazione

Consideriamo  $A$  l'anello dei "polinomi" in infinite variabili e con monomi infiniti.

Prendiamo  $a = x_1 x_2 + x_1 x_3^2 + x_1 x_2^2 x_3^2 x_4 \cdots$

In particolare  $x_1 x_2^2 x_3^2 x_4 \cdots$  non ha una fattorizzazione, non è prodotto di irriducibili.

### Lemma

Sia  $A$  un ED e siano  $b, c \in A$  con  $b, c \in A \setminus \{0, \text{unit}\}$ , allora  $\rho(b) < \rho(bc)$

**Dimostrazione:**

Supponiamo, per assurdo, che  $\rho(b) = \rho(bc)$  e consideriamo l'ideale  $I$  generato da  $b$ , ossia  $I = (b)$

L'elemento  $bc \in I$ , in quanto è multiplo di  $b$  e siccome un ideale è generato da un qualunque elemento che minimizza la  $\rho$ , segue che  $I = (bc)$ , cioè  $bc$  è generatore di  $I$ .

Ma se  $b$  e  $bc$  generano  $I$ , allora  $b$  e  $bc$  sono associati  $\Leftrightarrow c$  è invertibile.

L'assurdo cade in quanto per ipotesi  $c$  è *NINZ*

□

**Notazione:** Se  $A$  non è un campo, definiamo  $\rho_1 = \min\{\rho(a) : a \in A, a \text{ NINZ}\}$

### Lemma

Sia  $A$  un *ED* e sia  $a \in A : \rho(a) = \rho_1$  allora  $a$  è irriducibile

### Dimostrazione:

Prendiamo  $a \in A : \rho(a) = \rho_1$ . Se  $a = bc$  con  $b, c \in A$  e  $b, c$  *NINZ*, ossia se  $a$  è riducibile, per il lemma  $\rho(b), \rho(c) < \rho(bc) = \rho(a) = \rho_1$ . Ma non ci sono *NINZ* con valutazione minore di  $\rho_1$

□

### Proposizione

Se  $A$  è un *ED* e  $a \in A$  con  $a$  *NINZ*, allora  $a$  è prodotto di irriducibili

### Dimostrazione:

Procediamo per induzione su  $\rho(a)$ .

*Base Induttiva:*  $\rho(a) = \rho_1$ , quindi per il lemma è irriducibile.

*Passo Induttivo:* Sia  $\rho(a) > \rho_1$ . Se  $a$  è irriducibile, allora è verificata.

Se  $a$  è irriducibile, allora  $\exists b, c \in A$  e  $b, c$  *NINZ* tale che  $a = bc$ , allora per il primo lemma di oggi si ha che  $\rho(b), \rho(c) < \rho(a)$ . Per Ipotesi Induttiva segue che  $b$  e  $c$  sono prodotti di irriducibili, quindi, essendo  $a = bc$ ,  $a$  lo è

□

### Proposizione

Se  $A$  è un anello *PID* (dominio a ideali principali) e sia  $d_1, d_2, \dots$  una successione di elementi di  $A$  tali che  $d_j | d_{j-1}, \forall j \geq 2$ , allora  $\exists j_0$  tale che tutti gli elementi  $d_j$  con  $j \geq j_0$  sono tutti associati tra loro.

### Dimostrazione:

Prima di procedere con la dimostrazione, riformuliamo l'enunciato con gli ideali:

*Se  $d_2 | d_1$  allora segue che  $(d_1) \subseteq (d_2)$ . Generalizzando si ottiene che  $(d_1) \subseteq (d_2) \subseteq (d_3) \subseteq \dots$  Quindi  $\exists j_0 : (d_{j_0}) = (d_{j_0+1}) = \dots$*

Definiamo  $I$  come:

$$I = \bigcup_{j \geq 1} (d_j)$$

$I$  è un'unione di ideali e in questo caso continua ad essere un ideale (perché sono contenuti uno dentro l'altro)

Infatti:

- Siano  $x, y \in I$ , allora  $x \in (d_i)$  e  $y \in (d_j)$ . Se  $i \leq j$ , allora  $x, y \in (d_j) \Rightarrow x - y \in (d_j) \Rightarrow x, y \in I$  È analogo per l'altro caso
- Banalmente  $ax \in (d_i) \subseteq I$

Quindi  $I$  è un ideale, poiché  $A$  è un *PID* segue che  $I$  è un ideale principale  $\exists d \in A : I = (d)$

$\exists j_0 : d \in (d_{j_0}) \Rightarrow d_{j_0} | d$ , ossia  $d$  è multiplo di  $d_{j_0}$ , ma  $(d_{j_0}) \subseteq I = (d) \Rightarrow d | d_{j_0}$ . Segue quindi che  $d$  e  $d_{j_0}$  sono uguali o associati.

Se  $j \geq j_0$ , l'argomento sopra, continua a funzionare, quindi è verificata  $\forall j \geq j_0$

□

### Teorema

Se  $A$  è un *PID*, allora  $A$  è un *UFD*

#### Dimostrazione:

Dobbiamo dimostrare l'esistenza della fattorizzazione.

Sia  $a \in A$ ,  $a \neq 0$ . Dimostriamo che  $a$  ammette un divisore irriducibile.

Se  $a$  è irriducibile, allora è verificata.

Se  $a$  non è irriducibile,  $a = d_1 a_1$  con  $d_1, a_1 \in A$ .

Se  $d_1$  è irriducibile è finita, altrimenti lo possiamo fattorizzare come  $d_1 = d_2 a_2$ , quindi  $a = d_2 a_1 a_2$ .

E possiamo andare avanti in questo modo. Ci possono essere due esiti:

- Troviamo, ad un certo punto, un  $d_i$  irriducibile e a quel punto è fatta;

- Procediamo all'infinito con fattorizzazioni non banali e quindi avremo  $d_1, d_2, \dots$  con  $d_i \mid d_{i-1}$  e quindi non sono mai associati, contraddicendo la proposizione.

Dimostriamo ora che è unica a meno di ordine e a meno di associati.

Riprendiamo  $a \neq 0$ . Per la prima parte  $\exists p_1$  irriducibile tale che  $p_1 \mid a$ , cioè  $a = p_1 d_1$ . Se  $d_1$  è irriducibile è fatta, altrimenti possiamo andare avanti a ridurlo seguendo lo stesso ragionamento della prima parte. Sicuramente troveremo una fattorizzazione finita, in quanto altrimenti andremmo contro la proposizione precedente.

□

Controesempio per PID ma non ED

$A \subseteq \mathbb{Q}[\sqrt{-19}]$ , con

$$A = \left\{ a + b \frac{\sqrt{-19} + 1}{2} : a, b \in \mathbb{Z} \right\}$$

È un esempio in cui  $A$  è un *PID* ma non è un *ED*

**Domanda:** Sia  $p$  per un numero primo, quando è la somma di quadrati? E se lo è, in quanti modi?

### Lemma

Sia  $p$  è un numero primo in  $\mathbb{Z}$ , allora  $p$  è un primo in  $\mathbb{Z}[i]$  se e solo se  $p$  non è somma di 2 quadrati

#### Dimostrazione:

Se  $p = a^2 + b^2 = (a + ib)(a - ib)$ . Abbiamo che  $a + ib$  e  $a - ib$  non sono invertibili, perché gli unici invertibili sono  $\pm 1$  e  $\pm i$  e il loro prodotto non è  $p$ .

Viceversa, se  $p = \alpha, \beta \in \mathbb{Z}[i]$  con  $\alpha, \beta \neq 0$ , allora  $p$  è somma di due quadrati.

Sfruttiamo le norme  $p^2 = N(p) = N(\alpha\beta) = N(\alpha)N(\beta)$

Notiamo che  $N(\alpha) \neq 1$  in quanto  $\alpha$  non è invertibile, quindi se  $N(\alpha) = p \Rightarrow \alpha = a + ib \Rightarrow N(\alpha) = a^2 + b^2$

□

### Teorema

Un numero primo  $p > 0$  è somma di due quadrati  $\Leftrightarrow p$  non è primo in  $\mathbb{Z}[i] \Leftrightarrow p = 2$  oppure  $p \equiv 1 \pmod{4}$

#### Dimostrazione:

$$\Leftarrow) 2 = 1^2 + 1^2 = (1 + i)(1 - i)$$

Sia  $p \equiv 3 \pmod{4}$ . Se per assurdo  $p = a^2 + b^2$ , allora segue che  $3 \equiv a^2 + b^2 \pmod{4}$ . Ma i quadrati in  $\mathbb{Z}/4$  sono solo 1 e 0, quindi la somma di due quadrati non può fare 3.

$\Rightarrow)$  Sia ora  $p \equiv 1 \pmod{4}$ . Sappiamo che  $-1$  è un quadrato in  $\mathbb{Z}/p$ , allora:

$$\exists n, k \in \mathbb{Z} : -1 = n^2 + kp \Leftrightarrow kp = n^2 + 1 = (n+i)(n-i) \Rightarrow p \mid (n+i) \vee p \mid (n-i)$$

Ma questo è assurdo in quanto  $p$  non divide né i coefficienti di  $n+i$ , né quelli di  $n-i$ .  
 Quindi  $p$  non è primo in  $\mathbb{Z}[i]$ . Quindi per il lemma di prima è somma di due quadrati

□

Possiamo dire qualcosa per l'unicità?

Sia  $p \equiv 1 \pmod{4}$  e supponiamo  $p = a^2 + b^2 = c^2 + d^2$ . Mostriamo l'unicità.

Abbiamo che  $p = (a+ib)(a-ib) = (c+id)(c-id)$ . Questi quattro hanno norma  $p$  e sono quindi irriducibili. Le due fattorizzazioni coincidono quindi a meno dell'ordine e a meno di associati. Quindi segue che:

$$\begin{array}{llll} a+ib = c+id & a+ib = (-1)(c+id) & a+ib = i(c+id) & a+ib = (-i)(c+id) \\ a+ib = c-id & a+ib = (-1)(c-id) & a+ib = i(c-id) & a+ib = (-i)(c-id) \end{array}$$

**Conseguenza:** Se  $p \equiv 3 \pmod{4}$ , allora  $p$  è irriducibile in  $\mathbb{Z}[i]$

Se invece  $p \equiv 1 \pmod{4}$  allora  $p = (a+ib)(a-ib)$  e  $a$  e  $b$  sono univocamente determinati se imponiamo che  $0 < a \leq b$ .

### Definizione $\pi_p$

Poniamo come  $\pi_p$  il numero gaussiano  $\alpha = a+ib \in \mathbb{Z}[i]$  tale che  $N(\alpha) = a^2 + b^2 = p$

In tal caso poniamo  $p = (a+ib)(a-ib) = \pi_p \cdot \bar{\pi}_p$

Esempi semplici di tali numeri

Alcuni esempi semplici sono

$$\begin{aligned} \pi_5 &= 1+2i \Leftrightarrow 5 = 1+4 = 1^2 + 2^2 \\ \pi_{13} &= 2+3i \Leftrightarrow 13 = 4+9 = 2^2 + 3^2 \\ \pi_{17} &= 1+4i \Leftrightarrow 17 = 1+16 = 1^2 + 4^2 \end{aligned}$$

**Osservazione:** Dobbiamo avere necessariamente che  $a \neq b$ , altrimenti avremmo che  $p = a^2 + b^2$  è pari

Gli elementi  $\pm a \pm ib$  e  $\pm b \pm ia$  sono 8 elementi distinti, che si ripartiscono in due classi di assocatura, quelli di  $\pi_p$  e quelli di  $\bar{\pi}_p$

Infatti tutti gli associati di  $\pi_p$  sono  $\pi_p$  stesso,  $-a-ib$ ,  $i\pi_p = -b+ia$  e  $b-ia$ , mentre tutti gli altri sono gli associati di  $\bar{\pi}_p$

Abbiamo quindi due elementi irriducibili di norma  $p$ , appunto  $\pi_p$  e  $\bar{\pi}_p$  a meno di assocatura

Se invece  $p = 2 \Rightarrow p = (1+i)(1-i) = \pi_2 \bar{\pi}_2$  e abbiamo 4 elementi di norma 2 che sono  $\pm 1 \pm i$ . Quindi è una sola classe di assocatura.

Ce ne sono altre?

### Teorema di Classificazione degli Irriducibili in $\mathbb{Z}[i]$

L'insieme

$$\mathcal{P} = \{i+1\} \cup \{\pi_p, \bar{\pi}_p : p \equiv 1 \pmod{4}\} \cup \{p \equiv 3 \pmod{4}\}$$

è un insieme di rappresentanti delle classi di assocatura degli elementi irriducibili di  $\mathbb{Z}[i]$

### Dimostrazione:

Prendiamo  $\alpha \in \mathbb{Z}[i]$  irriducibile.

Sappiamo che  $N(\alpha) = \alpha \cdot \bar{\alpha} \in \mathbb{Z}_{>0}$ . Sia  $p$  un primo tale che  $p \mid N(\alpha)$ , vediamo i vari casi possibili:

- se  $p \equiv 3 \pmod{4}$ , allora segue che  $p \mid \alpha \cdot \bar{\alpha}$ , per le conseguenze che abbiamo appena visto,  $p$  è irriducibile in  $\mathbb{Z}[i]$ , per i teoremi precedenti questo implica che è anche primo in  $\mathbb{Z}[i]$ , di conseguenza segue che  $p \mid \alpha$  oppure  $p \mid \bar{\alpha}$ . Poiché  $p \in \mathbb{Z}$ , segue che  $p$  divide i coefficienti di  $\alpha$ , quindi necessariamente divide sia  $\alpha$  sia  $\bar{\alpha}$ , ma poiché  $\alpha$  è irriducibile per ipotesi, segue che  $p$  e  $\alpha$  sono associati, se non addirittura uguali;
- se  $p \equiv 1 \pmod{4}$ , allora  $p \mid \alpha \cdot \bar{\alpha}$ , ma è anche vero che  $p = \pi_p \cdot \bar{\pi}_p$ . Tuttavia, per la definizione di  $\pi_p$ ,  $\pi_p$  è irriducibile in  $\mathbb{Z}[i]$ , quindi è anche primo in  $\mathbb{Z}[i]$ , segue quindi che  $\pi_p \mid \alpha$  oppure  $\pi_p \mid \bar{\alpha}$ . Nel primo caso abbiamo che  $\pi_p$  e  $\alpha$  sono associati, in quanto, come prima,  $\alpha$  è irriducibile. Nel secondo caso abbiamo che  $\pi_p \mid \bar{\alpha}$ , passando per il coniugio, otteniamo che  $\bar{\pi}_p \mid \alpha$ ,

quindi  $\bar{\pi}_p$  e  $\alpha$  sono associati.

- se  $p = 2$  allora si fa lo stesso ragionamento di prima

□

**Problema:** Sia  $n \geq 0$  con  $n \in \mathbb{Z}$ , allora esistono due interi  $a, b \in \mathbb{Z}$  tali che  $n = a^2 + b^2$

### Teorema di Fermat

Sia  $n \in \mathbb{Z}, n > 0$ . Allora  $n$  è somma di due quadrati se e solo se nella sua fattorizzazione in numeri primi, quelli congrui a 3 in modulo 4 compaiono con esponente pari.

**Dimostrazione:**

⇒) Sia  $n$  come descritto nell'enunciato del teorema:

$$n = 2^{m_2} \cdot \prod_{p : p \equiv 1 \pmod{4}} p^{m_p} \cdot \prod_{p : p \equiv 3 \pmod{4}} p^{2m_p}$$

Dobbiamo mostrare che  $n$  è somma di due quadrati oppure, equivalentemente che  $\exists \alpha \in \mathbb{Z}[i] : n = N(\alpha)$

Poniamo

$$\alpha = (1+i)^{m_2} \cdot \prod_{p \equiv 1 \pmod{4}} \pi_p^{m_p} \cdot \prod_{p \equiv 3 \pmod{4}} p^{m_p}$$

Per costruzione e per la moltiplicatività della norma si ha che:

$$N(\alpha) = N(1+i)^{m_2} \cdot \prod_{p \equiv 1 \pmod{4}} N(\pi_p)^{m_p} \cdot \prod_{p \equiv 3 \pmod{4}} N(p)^{m_p} = 2^{m_2} \cdot \prod_{p \equiv 1 \pmod{4}} p^{m_p} \cdot \prod_{p \equiv 3 \pmod{4}} p^{2m_p} = n$$

⇒) Viceversa, se  $n = a^2 + b^2 = (a+ib)(a-ib) = \alpha \cdot \bar{\alpha} = N(\alpha)$  con  $\alpha = a+ib$

Per il teorema di classificazione degli irriducibili in  $\mathbb{Z}[i]$ , segue che vale:

$$\alpha = (1+i)^{m_2} \cdot \prod_{p \equiv 1 \pmod{4}} \pi_p^{m_{p,1}} \cdot \prod_{p \equiv 1 \pmod{4}} \bar{\pi}_p^{m_{p,2}} \cdot \prod_{p \equiv 3 \pmod{4}} p^{m_p} \cdot u$$

Con  $u$  elementi invertibile, quindi  $u \in \{\pm 1, \pm i\}$

Calcolando la norma otteniamo esattamente che:

$$N(\alpha) = 2^{m_2} \cdot \prod_{p \equiv 1 \pmod{4}} p^{m_{p,1} + m_{p,2}} \cdot \prod_{p \equiv 3 \pmod{4}} p^{2m_p}$$

□

# Terne Pitagoriche

In questa piccola parte parleremo delle terne pitagoriche

## Definizione di Terna Pitagorica e di Terna Pitagorica Primitiva

Siano  $a, b, c \in \mathbb{Z}$  positivi. Si dice che  $(a, b, c)$  è una terna pitagorica se  $c^2 = a^2 + b^2$ . Si dice che è una terna pitagorica primitiva se  $\text{MCD}(a, b) = 1$

Se  $(a, b, c)$  non è primitiva, allora  $d = \text{MCD}(a, b) > 1$ , quindi  $d | c$  e  $(\frac{a}{d}, \frac{b}{d}, \frac{c}{d})$  è una terna pitagorica primitiva.

*Proprio per questo motivo possiamo limitarci a studiare quelle primitive*

Cerchiamo di studiare le terne pitagoriche primitive e in particolare le possibili ipotenuse.

## Lemma

Se  $(a, b, c)$  è una terna pitagorica primitiva, allora  $c$  è dispari

## Dimostrazione:

Sia quindi  $a^2 + b^2 = c^2$ . Se  $c$  fosse pari, allora  $a$  e  $b$  sarebbero entrambi dispari (diamo per scontato che non siano pari, altrimenti 2 sarebbe divisore di entrambi, quindi non sarebbe primitiva)

Ma ciò è comunque assurdo in quanto avremmo che  $a^2 + b^2 = c^2 \pmod{4} \Leftrightarrow 1 + 1 \equiv 0 \pmod{4}$ , in quanto in  $\mathbb{Z}/4$ , il quadrato di un numero dispari è 1 e il quadrato di un numero pari è 0.

Quindi  $c$  deve essere necessariamente dispari.

□

## Lemma

Se  $(a, b, c)$  è una terna pitagorica primitiva e  $p$  è primo tale che  $p \equiv 3 \pmod{4} \Rightarrow p \nmid c$

## Dimostrazione:

Supponiamo per assurdo che  $p | c$  e sia  $a^2 + b^2 = c^2$  una terna primitiva.

Mettendo tutto insieme abbiamo che  $p | a^2 + b^2$ , ma  $p \equiv 3 \pmod{4}$ , quindi  $p$  è irriducibile in  $\mathbb{Z}[i]$  e di conseguenza è anche primo, quindi  $p | (a^2 + b^2) \Rightarrow p | (a + ib)$  oppure  $p | (a - ib)$ .

Ma poiché  $p \in \mathbb{Z}$  segue che  $p | a \wedge p | b$ , quindi  $(a, b, c)$  non è una terna pitagorica primitiva.

□

## Teorema

Sia  $c > 0$ , allora esistono  $a, b$  tali che  $(a, b, c)$  è una terna pitagorica primitiva se e solo se  $c$  è prodotto di primi congrui a 1 in modulo 4

## Dimostrazione:

$\Rightarrow$ ) Quest'implicazione l'abbiamo già vista, dai lemmi precedenti

$\Leftarrow$ ) Sia  $c$  come descritto nella nell'enunciato del teorema, ossia:

$$c = \prod_{p \equiv 1 \pmod{4}} p^{m_p} \Rightarrow c^2 = \prod_{p \equiv 1 \pmod{4}} p^{2m_p}$$

È vero che questo prodotto è uguale alla somma di due quadrati?

Poniamo  $\alpha$  nel seguente modo:

$$\alpha = \prod_{p \equiv 1 \pmod{4}} \pi_p^{2m_p}$$

Sicuramente abbiamo in questo modo che

$$N(\alpha) = \prod_{\substack{o \equiv 1 \pmod{4}}} N(\pi_p)^{2m_p} = \prod_{\substack{p \equiv 1 \pmod{4}}} p^{2m_p} = c^2$$

Se  $\alpha = a + ib$ , allora  $(a, b, c)$  è una terna pitagorica.

Mostriamo ora che è primitiva.

Supponiamo che non sia così, quindi esiste un primo  $p$  tale che  $p \mid a$  e  $p \mid b$ , quindi  $p \mid c$ , quindi  $p \equiv 1 \pmod{4}$  per il lemma precedente, ma allora  $p \mid \alpha$ , in quanto  $\alpha = a + ib$ , ma questo è equivalente a dire che  $\pi_p, \bar{\pi}_p \mid \alpha$ , ma  $\bar{\pi}_p$  non è un divisore di  $\alpha$  in quanto non compare nella sua fattorizzazione unica in irriducibili

□

### Esempio di Terna Pitagorica

Prendiamo  $c = 65 = 5 \cdot 13$ . Il nostro

$$\alpha = \pi_5^2 \cdot \pi_{13}^2 = (1+2i)^2(2+3i)^2 = (-3+4i)(-5+12i) = -(33+56i)$$

Quindi una terna primitiva è  $(33, 56, 65)$

Avremmo potuto anche scegliere  $\alpha = \pi_5^2 \cdot \bar{\pi}_{13}^2$  e avrei ottenuto un'altra terna.

In particolare avrei ottenuto la terna  $(63, 16, 65)$

---

# Polinomi

Non sono esempi di Polinomi:  $x^{-1}$ ,  $\sin x$ ,  $e^x$

## Definizione di Polinomio

Un polinomio a coefficienti in un anello  $A$  è una scrittura formale

$$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

con  $a_i \in A, \forall i \in \{1, \dots, n\}$  e  $x$  non è altro che un simbolo in cui l'unica regola effettiva è che  $x^n \cdot x^m = x^{n+m}$

Denotiamo quest'insieme con  $A[x]$

**Osservazione:**  $A[x]$  è un anello con le usuali operazioni di somma e di prodotto.

Infatti:

$$(a_0 + a_1x + \cdots + a_nx^n) + (b_0 + b_1x + \cdots + b_mx^m) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n$$

Possiamo considerare  $m = n$  senza perdere di generalità

Per il prodotto abbiamo che:

$$(a_0 + a_1x + \cdots + a_nx^n) \cdot (b_0 + b_1x + \cdots + b_mx^m) = c_0 + c_1x + \cdots + c_{n+m}x^{n+m} \quad \text{con } c_i = \sum_{h,k:h+k=i} a_h b_k$$

**Notazione:** Indichiamo con  $f$  il polinomio

$$f = \sum a_i x^i \in A[x]$$

Per ogni  $i$ , andiamo ad indicare il coefficiente di  $x^i$  come:

$$[f]_i = a_i$$

## Definizione di Termine Noto

Definiamo termine noto il termine

$$[f]_0 = a_0$$

## Definizione di Grado del Polinomio

Sia  $f$  un polinomio. Si definisce grado di  $f$  il valore:

$$\deg(f) = \max\{i : [f]_i \neq 0\}$$

## Definizione di Coefficiente Direttore

Sia  $f$  un polinomio e sia  $n = \deg(f)$ . Si definisce coefficiente direttore il numero  $[f]_n$

## Definizione di Polinomio Monico

Sia  $f$  un polinomio, si dice che  $f$  è un polinomio monico se il coefficiente direttore di  $f$  è uguale a 1

**Notazione:** Se  $f = 0$ , allora  $\deg(f) = -\infty$

### Lemma

Sia  $A$  un anello e siano  $f, g$  due polinomi a coefficienti in  $A$ , allora valgono:

- $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$
- $\deg(f \cdot g) \leq \deg(f) + \deg(g)$
- Se  $A$  è un dominio, allora  $\deg(f \cdot g) = \deg(f) + \deg(g)$

### Dimostrazione:

La prima parte segue direttamente dalla definizione di somma e prodotto

In  $f \cdot g$  può accadere che il coefficiente di  $[f \cdot g]_{n+m}$  con  $n = \deg(f)$  e  $m = \deg(g)$  si annulli:

$$[f \cdot g]_{m+n} = \sum_{h,k:h+k=m+n} [f]_h \cdot [g]_k = [f]_n \cdot [g]_m \neq 0 \text{ se } A \text{ è dominio}$$

□

### Corollario

Se  $A$  è un dominio, allora  $A[x]$  è un dominio

### Dimostrazione:

Segue dalla condizione sui gradi

□

### Corollario

Se  $A$  è un dominio, gli elementi invertibili sono le costanti invertibili

### Dimostrazione:

$f \cdot g = 1$ , allora si ha che

$$\deg(f \cdot g) = \deg(f) + \deg(g) = 0 \Rightarrow \deg(f) + \deg(g) = 0$$

□

### Definizione di $A^A$

Sia  $A$  un anello, indichiamo con  $A^A$  l'insieme delle funzioni da  $A$  a  $A$ :

$$A^A = \{f : A \rightarrow A\}$$

### Proposizione

$A^A$  è un anello ponendo:

- $(f + g)(a) = f(a) + g(a)$
- $(fg)(a) = f(a)g(a)$

### Dimostrazione:

Tutte le proprietà seguono direttamente dal fatto che  $A$  è un anello.

□

Sia  $f \in A[x]$  definito come  $f = a_0 + a_1x + \cdots + a_nx^n$ , allora possiamo definire  $\tilde{f}$  come

$$\tilde{f}(a) = a_0 + a_1a + \cdots + a_na^n \quad a \in A$$

### Proposizione

Sia  $A$  un anello, allora

$$\begin{aligned} A[x] &\rightarrow A^A \\ f &\mapsto \tilde{f} \end{aligned}$$

è un omomorfismo

#### Dimostrazione:

Siano  $f = a_0 + a_1x + \cdots + a_nx^n$  e  $g = b_0 + b_1a + \cdots + b_ma^m$  (senza perdere generalità consideriamo  $m = n$ )

Per la somma abbiamo che:

$$\widetilde{f+g}(a) = (a_0 + b_0) + (a_1 + b_1)a + \cdots + (a_n + b_n)a^n = (a_0 + a_1a + \cdots + a_na^n) + (b_0 + b_1a + \cdots + b_na^n) = \tilde{f}(a) + \tilde{g}(a)$$

Mentre per il prodotto abbiamo che:

$$\widetilde{fg}(a) = \sum_i \left( \sum_{h,k:h+k=i} (a_h \cdot b_k) \right) a^i = \sum_i \sum_{h,k:h+k=i} a_h \cdot b_k \cdot a^h \cdot a^k = \sum_{h,k} a_h \cdot b_k \cdot a^h \cdot a^k = \left( \sum_h a_h a^h \right) \cdot \left( \sum_k b_k a^k \right) = \tilde{f}(a) \cdot \tilde{g}(a)$$

□

**Osservazione:** La funzione  $f \mapsto \tilde{f}$  generalmente non è iniettiva.

Ad esempio per  $A = \mathbb{Z}/2$ ,  $x$  e  $x^2$  sono diversi come polinomi  $\mathbb{Z}/2[x]$  ma hanno la stessa funzione polinomiale associata.

In generale se  $A$  è finito, allora  $A^A$  è finito, ma  $A[x]$  è infinito e quindi  $f \mapsto \tilde{f}$  non può essere iniettiva.

Può anche capitare che tale funzione non sia iniettiva anche se  $A$  è infinito, infatti se prendiamo  $A$  come una successione infinita di elementi in  $\mathbb{Z}/2$ , per esempio  $(a_0, a_1, a_2, \dots) \in A$ ,  $a_i \in \mathbb{Z}/2$ . Le funzioni associate a  $x$  e a  $x^2$  non coincidono.

**Osservazioni:** Se  $K$  è un campo, allora vale che:

- Gli invertibili in  $K[x]$  sono le costanti non nulle
- Due polinomi sono associati in  $K[x]$  se uno è multiplo scalare dell'altro
- In ogni classe esiste uno e un solo polinomio monico, quindi possiamo scegliere il polinomio monico come rappresentante delle classi

Vogliamo mostrare che  $K[x]$  è un dominio euclideo:

### Lemma

Sia  $A$  un anello qualsiasi, consideriamo  $f, g \in A[x]$  e sia  $g$  monico. Allora esistono  $q, r \in A[x]$  con  $\deg(r) < \deg(g)$ , oppure  $r = 0$  tali che:

$$f = q \cdot g + r$$

#### Dimostrazione:

Dimostriamolo per induzione sul grado di  $f$ .

Se  $\deg(f) = 0$ , allora  $f$  è una costante, distinguiamo i due casi:

- se  $g = 1$ , allora

$$f = c \cdot g + 0$$

- se  $\deg(g) > 1$ , allora

$$f = 0 \cdot g + c$$

Se  $\deg(f) > 0$ , riprendiamo il passo induttivo visto prima.

Se  $\deg(g) > 0$  si hanno due casi:

- se  $\deg(g) > \deg(f)$ , allora

$$q = 0 \quad \text{e} \quad r = f$$

- se  $\deg(g) \leq \deg(f)$  allora possiamo porre

$$f_1 := f - (c \cdot x^{\deg(f)-\deg(g)} \cdot g)$$

con  $c$  coefficiente direttore di  $f$ .

Questo nuovo polinomio ha grado minore di  $f$ , quindi possiamo applicare l'ipotesi induttiva su  $f_1$

Quindi  $\exists q_1, r_1 \in A[x]$  tali che

$$f_1 = q_1 \cdot g + r_1$$

Tuttavia, per come abbiamo posto  $f_1$  segue che:

$$f = f_1 + c \cdot x^{\deg(f)-\deg(g)} \cdot g \Rightarrow f = qg + r$$

□

### Corollario

Se  $K$  è un campo, allora  $K[x]$  è un dominio euclideo ponendo:

$$\rho(f) = \begin{cases} \deg(f) & f \neq 0 \\ -1 & f = 0 \end{cases}$$

### Dimostrazione:

Abbiamo subito che,  $\forall a, b \in K[x] \setminus \{0\}$ :

$$\rho(a) \leq \rho(ab)$$

Inoltre, sempre  $\forall f \in K[x] \setminus \{0\}$ :

$$\rho(0) < \rho(f)$$

Dimostriamo la proprietà due dei domini euclidei: siano  $f, g \in K[x]$  con  $g$  non nullo e non necessariamente monico.

Infatti poniamo con  $\tilde{g}$  il polinomio

$$\tilde{g} := c \cdot g$$

con  $c$  costante non nulla in modo che  $\tilde{g}$  sia monico

Allora per il lemma esistono  $q, r \in K[x]$  con  $\rho(r) < \rho(\tilde{g}) = \rho(g)$  tali che:

$$f = q \cdot \tilde{g} + r = q \cdot c^{-1} \cdot c \cdot \tilde{g} + r = q \cdot c \cdot g + r$$

□

### Proposizione

Sia  $A$  un dominio qualunque. Sono equivalenti:

- 1)  $A$  è un campo
- 2)  $A[x]$  è un dominio euclideo
- 3)  $A[x]$  è un anello ad ideali principali

### Dimostrazione:

Le dimostrazioni  $2 \Rightarrow 3$  e  $1 \Rightarrow 2$  le avevamo già fatte in precedenza.

Dimostriamo quindi che  $3 \Rightarrow 1$ . Facciamolo per assurdo.

Se  $A$  non fosse un campo, allora esisterebbe un elemento  $a \in A$  che non è invertibile, con  $a$  non nullo.

Allora l'ideale  $(a, x)$  non è principale, perché se fosse principale dovrebbe essere generato da un divisore di  $a$  e di  $x$  e ciò non è possibile. Infatti se tale elemento  $f$  esistesse, si avrebbe che:

$$f | a \Rightarrow f \text{ è costante}$$

$$f | x \Rightarrow f \text{ è invertibile come costante}$$

Allora segue che

$$(f) = A[x]$$

ma ciò è assurdo in quanto  $I = A[x]$ , in quanto in  $I$  ci sono solo polinomi che hanno  $[f]_0$  multipli di  $a$ , quindi non tutti

□

### Definizione di Radice del Polinomio

Siano  $f \in A[x]$  e  $a \in A$ . Diciamo che  $a$  è radice di  $f$  se

$$\tilde{f}(a) = 0$$

### Teorema di Ruffini

Siano  $f \in A[x]$  e  $a \in A$ , allora  $a$  è radice di  $f$  se e solo se  $(x - a) | f$ , cioè:

$$\exists g \in A[x] : f = (x - a)g$$

#### Dimostrazione:

Abbiamo quindi che

$$f = q(x - a) + r$$

dove  $r$  è una costante (cioè  $\deg(r) < 1$ )

Sia quindi

$$\tilde{f}(a) = \tilde{q}(a) \cdot 0 + r = r$$

Il risultato segue, quindi

$$\tilde{f}(a) = 0 \Leftrightarrow r = 0$$

□

**Osservazione:** In generale, non è vero che se  $a, b$  sono radici di  $f$  con  $a \neq b$ , allora  $f$  è multiplo di  $(x - a)(x - b)$ . Mancherebbe in caso la fattorizzazione unica in generale.

Esempio in cui la fattorizzazione unica è necessaria

Consideriamo

$$(x^2 - 1) \in \mathbb{Z}/8[x]$$

Abbiamo che 1 ha quattro radici in  $\mathbb{Z}/8$ , che sono proprio gli invertibili, tuttavia se facessimo

$$(x - 1)(x - 3) = x^2 - 4x + 3 \text{ che non è multiplo di } x^2 - 1$$

### Definizione di Molteplicità

Se  $a$  è radice di  $f$ , chiamiamo molteplicità di  $a$  il valore:

$$m(a) = \max\{n : (x - a)^n | f\}$$

### Corollario

Sia  $K$  un campo e sia  $f \in K[x]$ . Allora le radici di  $f$  sono finite e la somma delle molteplicità è minore di  $\deg(f)$

#### Dimostrazione:

Sia  $K[x]$  un dominio a fattorizzazione unica e  $x - a$  è irriducibile,  $\forall a \in K$ .

Quindi se  $a$  è radice di  $f$  di molteplicità  $m$ , abbiamo che  $(x - a)^m$  deve comparire nella sua unica fattorizzazione di irriducibili. Questo vale per tutte le radici.

Quindi la tesi è dimostrata

□

Sia  $K$  un campo qualunque. Sia  $G$  un sottogruppo finito di  $K^*$

Esiste un caso interessante, ossia con  $K$  campo finito e  $G = K^*$

### Teorema

$G$  è ciclico

#### Dimostrazione:

Per il teorema di caratterizzazione dei gruppi ciclici, cioè che se un gruppo non ha due sottogruppi dello stesso ordine, allora è ciclico. Supponiamo per assurdo che  $G$  abbia due sottogruppi distinti di ordine  $d$ . Chiamiamoli  $H_1$  e  $H_2$

Sia  $h \in H_1$  oppure  $h \in H_2$ . Per il teorema di Lagrange si ha che  $\exists d \in \mathbb{Z}$  tale che  $h^d = 1$ .

Quindi gli elementi di  $H_1$  e di  $H_2$  sono tanti tutti radici del polinomio  $x^d - 1$  di grado  $d$ .

Ma  $|H_1 \cup H_2| > d$  e ciò è impossibile.

Infatti se  $H_1$  ha  $d$  distinti,  $H_2$  distinto ha almeno un elemento un elemento non in  $H_1$ , dunque dovrebbe avere almeno  $d + 1$  radici di un polinomio di grado  $d$

□

### Definizione di Derivata

Sia  $f \in K[x]$ . Definiamo derivata di  $f$  ponendo

$$f' := \sum_{i=1}^n i a_i x^{i-1} \quad \text{con} \quad f = \sum_{i=0}^n a_i x^i$$

### Lemma

Siano  $f, g \in K[x]$ , allora valgono le seguenti proprietà:

- $(f + g)' = f' + g'$
- $(f \cdot g)' = f'g + fg'$

#### Dimostrazione:

Sapendo che:

$$f = \sum_{i=0}^n a_i x^i \quad g = \sum_{i=0}^n b_i x^i$$

Allora abbiamo che

$$(f + g)' = \sum_{i=1}^n i(a_i + b_i)x^{i-1} = \sum_{i=1}^n ia_i x^{i-1} + \sum_{i=1}^n ib_i x^{i-1} = f' + g'$$

Possiamo supporre che che  $f$  e  $g$  abbiano lo stesso grado senza perdere di generalità

Per la regola del prodotto, possiamo ridurci al caso  $x^n = f$  e  $x^m = g$ :

$$(f \cdot g)' = (x^{m+n})' = (m+n)x^{m+n-1} = nx^{n-1}x^m + mx^{m-1}x^n = f'g + fg'$$

□

### Proposizione

Sia  $f \in K[x]$  con  $K$  campo e  $a \in K$  tale che  $a$  è radice di  $f$ . Allora  $a$  è radice multpla di  $f$  (cioè molteplicità di  $a$  è maggiore di 1)  $\Leftrightarrow a$  è radice di  $f'$

### Dimostrazione:

Sia  $m \geq 1$  la molteplicità di  $a$  come radice di  $f$ , cioè  $f = (x - a)^m \cdot g$  con  $g$  che non ha  $a$  come radice, cioè  $\tilde{g}(a) = 0$ . Allora

$$f' = ((x - a)^m g)' = m(x - a)^{m-1} \cdot g + g'(x - a)^m$$

Se  $m \geq 2$ , allora  $\tilde{f}'(a) = 0$ , mentre se  $m = 1$ , allora  $\tilde{f}'(a) = \tilde{g}(a) \neq 0$

□

La proposizione vale se sappiamo chi è la radice di  $f$ , ovviamente

Esempio in cui un polinomio non ha radici multiple

Sia  $K$  un campo la cui cardinalità è  $n$ , allora  $f = x^n - x$  non ha radici multiple, con  $n$  intero.

Infatti, poiché

$$f' = nx^{n-1} - 1$$

Tuttavia, poiché  $n$  è multiplo di  $\text{Char}(K)$ , si ha che  $n = 0$ , quindi otteniamo che

$$f' = -1$$

Quindi  $f'$  non ha radici e  $f$  non ha radici multiple

Siano  $K \subseteq L$  due campi e siano  $f, g \in K[x]$ .

Notiamo che  $\mathcal{MCD}_{K[x]}(f, g) = \mathcal{MCD}_{L[x]}(f, g)$ , infatti il  $\mathcal{MCD}$  si calcola con l'algoritmo euclideo che non dipende dal campo.

### Proposizione

Sia  $K$  un campo e sia  $f \in K[x]$  tale che  $\mathcal{MCD}(f, f') = 1$ . Allora  $f$  non ha radici multiple, non solo in  $K$  ma neanche in una qualunque estensione  $L$  di  $K$ .

### Dimostrazione:

Se  $a$  fosse stata una radice multipla di  $f$ , allora si avrebbe avuto che

$$(x - a) \mid f \quad \text{e} \quad (x - a) \mid f'$$

Control'ipotesi che  $\mathcal{MCD}(f, f') = 1$  a meno di associati

□

### Corollario

Se  $f$  è irriducibile e  $f' \neq 0$ , allora  $f$  non ha radici multiple

### Dimostrazione:

Gli unici divisori di  $f$  sono 1 e  $f$  a meno di associati.

Inoltre  $\deg(f') < \deg(f)$ , quindi sicuramente non possiamo avere che  $f'$  sia multiplo di  $f$ .

Dunque abbiamo che  $\mathcal{MCD}(f, f') \neq f$ , quindi deve essere necessariamente 1.

Quindi per la proposizione precedente abbiamo concluso.

Tuttavia, l'ipotesi che  $f' \neq 0$ , implica che  $f$  non può essere una costante, altrimenti avremmo che  $\mathcal{MCD}(f, f') = f$

□

Esempio di Polinomio Irriducibile con derivata prima non nulla

Prendiamo  $\mathbb{Q}[x]$  e consideriamo

$$f = x^3 + 3x + 3$$

$f$  è irriducibile in  $\mathbb{Q}[x]$  ma vedremo poi il motivo

### Definizione di Campo Algebricamente Chiuso

Un campo  $K$  è algebricamente chiuso se ogni polinomio  $f \in K[x]$  di grado positivo ammette una radice in  $K$

### Lemma

Se  $\alpha \in \mathbb{C}$  e  $n \in \mathbb{N}$ , allora  $\exists \beta \in \mathbb{C} : \beta^n = \alpha$ , cioè il polinomio  $x^n - \alpha$  ammette una radice.

### Dimostrazione:

Poniamo

$$\alpha = re^{i\theta}$$

con  $r > 0$  e  $\theta \in \mathbb{R}$ . Allora possiamo prendere  $\beta$  come:

$$\beta = \sqrt[n]{r}e^{i\frac{\theta}{n}}$$

□

### Teorema Fondamentale dell'Algebra

$\mathbb{C}$  è algebricamente chiuso

### Dimostrazione:

Sia  $f \in \mathbb{C}[x]$  con  $f \neq 0$  e  $\deg(f) > 0$

Dimostriamo il teorema fondamentale dell'algebra sfruttando l'analisi e in più parti:

**1<sup>a</sup> Parte:** Mostriamo che  $|f(z)|$  ammette un minimo al variare di  $z \in \mathbb{C}$ , cioè che

$$\exists z_0 \in \mathbb{C} : |f(z_0)| \leq |f(z)|, \forall z \in \mathbb{C}$$

Poiché  $f$  è un polinomio a coefficienti complessi, segue che  $f$  sarà della forma:

$$f(z) = a_0 + a_1 z + \cdots + a_n z^n$$

Allora, sfruttando il modulo e le sue proprietà otteniamo che:

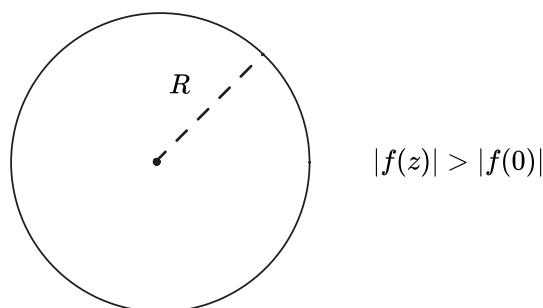
$$|f(z)| = |a_0 + a_1 z + \cdots + a_n z^n| \geq |a_n z^n| - |a_0| - |a_1 z| - \cdots - |a_{n-1} z^{n-1}| = |a_n| |z|^n - |a_0| - |a_1| |z| - \cdots - |a_{n-1}| |z|^{n-1} \in \mathbb{R}[x]$$

Notiamo che per  $z \rightarrow +\infty$ , abbiamo che  $|f(z)| \rightarrow +\infty$ , ossia, sfruttando la definizione di limite:

$$\forall M > 0, \exists R > 0 : \forall |z| > R \Rightarrow |f(z)| > M$$

Possiamo porre  $M = |f(0)|$

Graficamente



Con questa definizione di limite, abbiamo un disco chiuso centrato in 0 e con raggio  $R$ .

Visto che questo è un insieme chiuso e limitato, possiamo applicare il teorema di Weierstrass, quindi:

$$\exists z_0, |z_0| < R : |f(z_0)| < |f(z)|, \forall z : |z| < R$$

Ma da quanto affermato prima abbiamo che

$$\forall z \in \mathbb{C}, |f(z_0)| \leq |f(z)|$$

Quindi abbiamo dimostrato che esiste un minimo.

**2<sup>a</sup> Parte:** Mostriamo che tale minimo è 0

Senza perdere di generalità, possiamo assumere che il minimo della funzione sia  $|f(0)|$

Se  $|f(0)| \neq 0$ , possiamo assumere che  $|f(0)| = 1$ , in quanto basta moltiplicare il polinomio per una costante non nulla

Abbiamo quindi che il polinomio  $f$  di partenza è della forma:

$$f(x) = 1 + a_k x^k + x^{k+1} g(x) \quad \text{con } a_k \neq 0$$

Sia quindi  $w \in \mathbb{C}, w \neq 0$  tale che

$$w^k = -a_k^{-1}$$

e sappiamo che esiste per il lemma precedente.

Sia ora  $r > 0$  e calcoliamo  $f(rw)$ :

$$f(rw) = 1 + a_k r^k w^k + r^{k+1} w^{k+1} g(rw)$$

Se scegliamo  $r \in [0, 1]$ , allora otteniamo che  $g(rw) \leq c$  dove  $c$  è una costante reale positiva.

Otteniamo, sfruttando anche le proprietà del modulo, allora che:

$$|f(rw)| = |1 - r^k + r^{k+1} w^{k+1} g(rw)| \leq |1 - r^k| + |r^{k+1}| \cdot |w^{k+1}| \cdot |g(rw)|$$

Poniamo allora  $c' = |g(rw)| \cdot |w^{k+1}|$ , otteniamo quindi che:

$$|f(rw)| \leq (1 - r^k) + c' r^{k+1}$$

Se  $r$  è abbastanza piccolo, in particolare

$$r < \min \left\{ 1, \frac{1}{c'} \right\}$$

Allora segue che:

$$|f(rw)| \leq (1 - r^k) + c' r r^k < 1 - r^k + r^k = 1$$

Il che è assurdo in quanto avremmo trovato un valore che è più piccolo del minimo della funzione stessa.

□

Come sono i polinomi irriducibili in  $\mathbb{R}[x]$ ?

**Osservazione:** Se  $\deg(f) \geq 3$  dispari, allora sicuramente  $f$  ha almeno una variabile reale, quindi  $f$  è riducibile.

### Teorema

$f \in \mathbb{R}[x]$  è irriducibile se e solo se  $\deg(f) = 1$  oppure  $\deg(f) = 2$  e  $f$  non ha radici reali ( $\Delta < 0$ )

### Dimostrazione:

Se  $\deg(f) \geq 2$  e  $f$  ha una radice reale, allora  $f$  è riducibile.

Supponiamo quindi che  $f$  non abbia radici reali.

Per il teorema fondamentale dell'algebra, abbiamo che le radici sono complesse, quindi possiamo prendere  $\alpha \in \mathbb{C}$  radice di  $f$ .

Sia quindi  $\alpha \in \mathbb{C}$  una radice di  $f$

Se  $f$  è un polinomio della forma:

$$f = a_0 + a_1 x + \cdots + a_n x^n \quad \Rightarrow \quad f(\alpha) = a_0 + a_1 \alpha + \cdots + a_n \alpha^n = 0$$

E sappiamo che  $f(\alpha) = 0$  per la scelta di  $\alpha$  fatta.

Visto che il coniugio su  $\mathbb{C}$  è un automorfismo di  $\mathbb{C}$  possiamo calcolare  $\overline{f(\alpha)}$ :

$$\overline{f(\alpha)} = \bar{a}_0 + \bar{a}_1 \bar{\alpha} + \cdots + \bar{a}_n \bar{\alpha}^n = 0$$

Tuttavia, poiché per ogni  $i$  abbiamo che  $a_i \in \mathbb{R}$ , abbiamo che:

$$\overline{f(\alpha)} = a_0 + a_1 \overline{\alpha} + \cdots + a_n \overline{\alpha^n} = 0$$

Deduciamo quindi che anche  $\overline{\alpha}$  è una radice di  $f$ .

Poiché sia  $\alpha$ , sia  $\overline{\alpha}$  sono radici di  $f$ , otteniamo che  $(x - \alpha)$  e  $(x - \overline{\alpha})$  dividono  $f$ . In particolare, poiché  $\alpha$  e  $\overline{\alpha}$  non sono associati:

$$(x - \alpha)(x - \overline{\alpha}) \mid f$$

Quindi a maggior ragione, sviluppando quanto ottenuto, abbiamo che:

$$(x - \alpha)(x - \overline{\alpha}) = x^2 - \overline{\alpha}x - \alpha x + \alpha \overline{\alpha} = x^2 - (\underbrace{\alpha + \overline{\alpha}}_{\in \mathbb{R}})x + \underbrace{\alpha \overline{\alpha}}_{\in \mathbb{R}} \in \mathbb{R}[x]$$

Quindi abbiamo ottenuto che il più grande polinomio irriducibile in  $\mathbb{R}[x]$  è un polinomio di grado due e con radici complesse.

□

### Esempio di Polinomio Riducibile

Prendiamo  $f = x^4 + 1$

Allora il teorema ci assicura che  $f$  è riducibile in  $\mathbb{R}[x]$ , in quanto  $\deg(f) = 4$

Abbiamo che le radici di  $f$  come polinomio in campo complesso sono le radici quarte di  $-1$ , ossia sono

$$\frac{\sqrt{2}}{2}(\pm 1 \pm i)$$

Poniamo

$$\alpha = \frac{\sqrt{2}}{2}(1+i) \quad \text{e} \quad \beta = \frac{\sqrt{2}}{2}(-1+i)$$

Otteniamo allora che:

$$(x - \alpha)(x - \overline{\alpha}) = \left( x - \frac{\sqrt{2}}{2}(1+i) \right) \left( x - \frac{\sqrt{2}}{2}(1-i) \right) = x^2 - \sqrt{2}x + 1$$

$$(x - \beta)(x - \overline{\beta}) = \left( x - \frac{\sqrt{2}}{2}(-1-i) \right) \left( x - \frac{\sqrt{2}}{2}(-1+i) \right) = x^2 + \sqrt{2}x + 1$$

da cui si ottiene che

$$f = (x^2 - \sqrt{2}x + 1)(x^2 + \sqrt{2}x + 1)$$

Vediamo adesso come si comportano i polinomi in  $A[x]$  dove  $A$  è un dominio a fattorizzazione unica.

**Esempio Principale:** L'esempio principale da tenere a mente è  $A = \mathbb{Z}$ . In questo caso li possiamo ricollegare a polinomi in  $\mathbb{Q}[x]$

Diamo questa definizione per poter andare avanti.

## Definizione di Campo dei Quozienti o Campo delle Frazioni

Sia  $A$  un anello, definisce  $Q(A)$  il campo dei Quozienti di  $A$  o il Campo delle Frazioni di  $A$  l'insieme costituito da:

$$Q(A) = \left\{ \frac{a}{b} : a, b \in A, b \neq 0 \right\}$$

In cui vige la relazione di equivalenza

$$\frac{a}{b} \sim \frac{c}{d} \Leftrightarrow ad = bc$$

### Lemma

$\sim$  come definita nella definizione precedente è una relazione di equivalenza

**Osservazione:** Va sottolineato che se  $A$  non è un dominio, questa non è una relazione di equivalenza

### Dimostrazione:

Supponiamo quindi  $A$  un dominio e verifichiamo che  $\sim$  sia una relazione di equivalenza

- (R) Chiaramente si ha che:

$$\frac{a}{b} \sim \frac{a}{b} \Leftrightarrow ab = ba$$

Stiamo considerando  $A$  anello commutativo

- (S) Sempre passando per l'uguaglianza del prodotto si ha che:

$$\frac{a}{b} \sim \frac{c}{d} \Rightarrow \frac{c}{d} \sim \frac{a}{b} \quad \text{In quanto } ab = cd \Rightarrow cd = ab$$

- (T) Vogliamo mostrare che:

$$\frac{a}{b} \sim \frac{b}{c} \quad \text{e} \quad \frac{c}{d} \sim \frac{e}{f} \quad \Rightarrow \quad \frac{a}{b} \sim \frac{e}{f}$$

Allora per ipotesi abbiamo che  $ad = cb$  e che  $cf = de$ . Allora moltiplicando tutto per  $a$  e andando a sostituire si ha che:

$$cf = de \Rightarrow acf = (ad)e \Rightarrow acf = (bc)e$$

Allora per la proprietà di cancellazione, per  $c \neq 0$ , otteniamo che:

$$af = be \Rightarrow \frac{a}{b} \sim \frac{e}{f}$$

Se invece  $c = 0$ , allora era banalmente verificato

□

## Teorema

$Q(A)$  è un campo con le operazioni definite come:

$$[+] : \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \quad [\cdot] : \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

Inoltre l'applicazione

$$\begin{aligned} \varphi : A &\rightarrow Q(A) \\ a &\mapsto \frac{a}{1} \end{aligned}$$

è un omomorfismo iniettivo

### Dimostrazione:

Sono tutte verifiche elementari, quindi ci limiteremo a verificare che siano ben poste

- Supponiamo di avere due elementi associati  $\frac{a}{b} \sim \frac{a'}{b'}$  e mostriamo che dato un terzo elemento  $\frac{c}{d}$  si ha che

$$\frac{a}{b} + \frac{c}{d} \sim \frac{a'}{b'} \sim \frac{c}{d} \quad \Leftrightarrow \quad \frac{ad+bc}{bd} \sim \frac{a'd+b'c}{b'd}$$

Ma questo è vero in quanto:

$$\frac{ad+bc}{bd} \sim \frac{a'd+b'c}{b'd} \quad \Leftrightarrow \quad (ad+bc)b'c = (a'd+b'c)bc$$

E con opportune moltiplicazioni e opportune sostituzioni nella definizione che abbiamo appena dato è verificato.

- In maniera del tutto analoga mostriamo anche che

$$\frac{a}{b} \cdot \frac{c}{d} \sim \frac{a'}{b'} \cdot \frac{c}{d} \quad \Leftrightarrow \quad acb'd = bda'c$$

- Mostriamo che  $\varphi$  è un omomorfismo:

$$\varphi(a+b) = \frac{a}{1} + \frac{b}{1} \quad \varphi(ab) = \frac{ab}{1} = \frac{a}{1} \cdot \frac{b}{1}$$

Mostriamo ora che è iniettivo:

$$\varphi(a) = \varphi(b) \quad \Rightarrow \quad \frac{a}{1} = \frac{b}{1} \quad \Leftrightarrow \quad a = b$$

□

Supponiamo di avere  $A \subseteq L$ , con  $A$  anello e  $L$  campo. Ci chiediamo se  $L$  contiene un sottocampo  $K$  che contiene a sua volta  $A$  e che sia isomorfo a  $Q(A)$

### Proposizione

Siano  $A$  dominio e  $L$  campo tali che  $A \subseteq L$ . Siano

$K_1 =$  Intersezione di tutti i sottocampi di  $L$  che contengono  $A$

$$K_2 = \{a \cdot b^{-1} : a, b \in A, b \neq 0\}$$

Allora  $K_1 = K_2$  e  $K_2 \cong Q(A)$

### Dimostrazione:

Dimostriamo l'uguaglianza sfruttando la doppia inclusione.

-  $K_1 \subseteq K_2$ : Basta mostrare che  $K_2$  è un campo che contenga  $A$

Notiamo che  $A \subseteq K_2$  in quanto

$$a = a \cdot 1^{-1} \quad \forall a \in A$$

Inoltre  $K_2$  è un campo perché:

$$\begin{aligned} a \cdot b^{-1} - c \cdot d^{-1} &= add^{-1}b^{-1} - cbb^{-1}d^{-1} = (ad - cb)d^{-1}b^{-1} \in K_2 \\ (a \cdot b^{-1}) \cdot (c \cdot d^{-1}) &= (ac) \cdot (b^{-1}d^{-1}) \in K_2 \\ (a \cdot b^{-1})^{-1} &= b \cdot a^{-1} \in K_2 \end{aligned}$$

Quindi  $K_2$  è un campo che contiene  $A$ , quindi  $K_1 \subseteq K_2$

-  $K_2 \subseteq K_1$ : Affinché un campo che contiene  $A$  "deve" contenere tutti gli elementi  $ab^{-1} \in K_2$

Quindi l'uguaglianza è verificata.

- Mostriamo ora l'isomorfismo: definiamo

$$\varphi : Q(A) \rightarrow K_2 \quad \varphi \left( \left[ \frac{a}{b} \right] \right) = a \cdot b^{-1}$$

Questo è un omomorfismo ben definito, iniettivo e suriettivo

□

Chi è  $Q(\mathbb{Z}[\sqrt{2}])$

Prendiamo prima  $L = \mathbb{Q}[\sqrt{2}]$ . Sappiamo che è un campo che contiene  $\mathbb{Z}[\sqrt{2}]$

Per il teorema sappiamo anche che  $Q(\mathbb{Z}[\sqrt{2}])$  è il più piccolo campo di  $\mathbb{Q}[\sqrt{2}]$  contenente  $\mathbb{Z}[\sqrt{2}]$  e quindi, dovendo contenere tutto  $\mathbb{Q}$  e  $\sqrt{2}$ , abbiamo che  $Q(\mathbb{Z}[\sqrt{2}]) = \mathbb{Q}[\sqrt{2}]$

*A priori, la vera procedura da fare era considerare un elemento qualsiasi della forma*

$$\frac{a+b\sqrt{2}}{c+d\sqrt{2}}$$

*per poi razionalizzare come elemento di  $\mathbb{Q}[\sqrt{2}]$ . Il teorema in questo caso ci facilità tutto*

**Osservazione:** Sia  $A$  un dominio e sia  $f \in A[x]$ . Siccome  $f \in A[x] \subseteq Q(A[x])$ , le radici di  $f$  in  $A$  sono anche radici in  $Q(A[x])$ . Quindi la somma delle molteplicità delle radici di  $f$  in  $A$  è al più  $\deg(f)$

### Lemma

Sia  $A$  un UFD e sia  $Q = Q(A)$ . Sia  $f$  un polinomio in  $A[x]$  della forma:

$$f = a_0 + a_1x + \cdots + a_nx^n$$

dove  $a_n \neq 0$ . Allora le radici di  $f$  in  $Q(A)$  sono necessariamente della forma

$$\frac{r}{s} \quad \text{con } r \mid a_0 \quad \text{e } s \mid a_n$$

### Dimostrazione:

Sia quindi  $\frac{r}{s}$  radice con  $\text{MCD}(r, s) = 1$ . Allora, valutando  $f$  in  $\frac{r}{s}$  abbiamo che:

$$a_0 + a_1 \frac{r}{s} + \cdots + a_{n-1} \frac{r^{n-1}}{s^{n-1}} + a_n \frac{r^n}{s^n} = 0$$

Quindi moltiplicando tutto per  $s^n$  otteniamo che:

$$a_0s^n + a_1s^{n-1}r + \cdots + a_{n-1}sr^{n-1} + a_nr^n = 0$$

Allora, portando  $a_nr^n$  a destra dell'uguaglianza, notiamo che  $s \mid a_nr^n$ . Tuttavia, poiché  $\text{MCD}(r, s) = 1$  segue necessariamente che

$$s \mid a_n$$

In maniera del tutto analoga, portando  $a_0s^n$  a destra dell'uguaglianza, notiamo che  $r \mid a_0s^n$  da cui si ottiene che:

$$r \mid a_0$$

□

### Esempio del Calcolo di una Radice

Prendiamo  $f \in \mathbb{Z}[x]$ :

$$f = 3 + 5x + 5x^2 + 2x^3$$

Per il lemma, le uniche possibili radici sono:

$$\pm 1, \pm 3, \pm \frac{1}{2}, \pm \frac{3}{2}$$

Possiamo già escludere quelle positive non possono essere soluzione, in quanto sono somme di numeri interamente positivi

Facendo i conti, notiamo che:

$$f\left(-\frac{3}{2}\right) = 0$$

Quindi possibile dividere  $f$  per  $(x + \frac{3}{2})$

In particolare, usando l'algoritmo di Ruffini abbiamo che:

$$\begin{array}{c|ccc|c}
 & 2 & 5 & 5 & 3 \\
 -\frac{3}{2} & & -3 & -3 & -3 \\
 \hline
 & 2 & 2 & 2 & 0
 \end{array} \Rightarrow f = \left(x + \frac{3}{2}\right)(2x^2 + 2x + 2) = (2x + 3)(x^2 + x + 1)$$

Quindi la fattorizzazione in  $\mathbb{Q}[x]$  a meno di coefficienti è valida in  $\mathbb{Z}[x]$

### Definizione di Contenuto del Polinomio

Sia  $f \in A[x]$ . Definiamo il contenuto di  $f$  e lo indichiamo come  $c(f)$  come:

$$\mathcal{MCD}(a_0, a_1, \dots, a_n)$$

dove  $\forall i, a_i$  sono i coefficienti dei delle varie potenze di  $x$

### Definizione di Polinomio Primitivo

Sia  $f \in A[x]$ , si dice che è primitivo se  $c(f) = 1$

**Osservazione:** Possiamo scrivere  $f \in A[x]$  come

$$f = c(f) \cdot f^\#$$

**Esempio:** se  $f = 2x^2 + 4x$  allora  $c(f) = 2$ , quindi il polinomio primitivo ad esso associato è  $f^\# = x^2 + 2x$

### Teorema

Siano  $f, g \in A[x]$ , allora  $c(fg) = c(f)c(g)$

### Dimostrazione:

Per l'osservazione precedente abbiamo che

$$fg = c(f)c(g) \cdot f^\# g^\#$$

Ci resta da mostrare che  $f^\# g^\#$  è primitivo, cioè che il prodotto di primitivi è primitivo.

Supponiamo per assurdo che ogni coefficiente di  $f^\# g^\#$  sia divisibile per un elemento irriducibile  $\pi$

Allora, ponendo:

$$f^\# = a_0 + a_1x + \dots \quad g^\# = b_0 + b_1x + \dots$$

Sia  $i$  il minimo indice tale che  $\pi \nmid a_i$  e  $j$  il minimo indice tale che  $\pi \nmid b_j$

Il coefficiente di grado  $i + j$  nel prodotto è

$$\sum_{h,k : h+k=i+j} a_h \cdot b_k$$

Abbiamo che tutti gli addendi sono divisibili per  $\pi$  (in quanto per  $h < i$ ,  $\pi \mid a_i$ , mentre se  $h > i \Rightarrow k < j$ , quindi  $\pi \mid b_j$ ) tranne per  $a_i b_j$ . Quindi, poiché esiste un termine non divisibile per  $\pi$  tutta la somma non lo è

□

### Corollario

Sia  $f \in A[x]$  primitivo e sia  $g \in Q(A)[x]$  tale che  $f \cdot g \in A[x]$ . Allora  $g \in A[x]$

### Dimostrazione:

Sia  $d \in A$  tale che  $d \cdot g \in A[x]$ . In questo modo abbiamo che  $c(f \cdot dg)$  è multiplo di  $d$  perché  $fg \in A[x]$

D'altra parte abbiamo che

$$c(f \cdot dg) = c(f) \cdot c(dg) = c(dg)$$

in quanto  $f$  è primitivo

Quindi i coefficienti di  $dg$  sono multipli in  $A$  di  $d$  e quindi i coefficienti di  $g$  sono in  $A$

□

Per comodità di linguaggio diamo le seguenti definizioni:

### Definizione di Polinomio Intero

Sia  $f$  un polinomio. Si dice che  $f$  è un polinomio intero se tutti i coefficienti sono elementi in  $A$

### Definizione di Polinomio Razionale

Sia  $f$  un polinomio. Si dice che  $f$  è un polinomio razionale se tutti i coefficienti sono elementi in  $Q$

Prendiamo un polinomio  $f \in A[x] \subseteq Q[x]$ , che correlazione c'è tra la riducibilità di  $f$  come elemento di  $A[x]$  o di  $Q[x]$ ?

Verrebbe da pensare che l'implicazione da sinistra a destra ( $A[x] \Rightarrow Q[x]$ ) sia banalmente verificata.

Non è così. In particolare, quest'affermazione nella maggior parte dei casi è falsa.

Esempio di polinomio riducibile in  $A$  ma non in  $Q$

Prendiamo  $A[x] = \mathbb{Z}[x]$  e  $Q[x] = \mathbb{Q}[x]$  e prendiamo  $f = 2x$

In  $\mathbb{Z}[x]$  abbiamo che  $f$  è scrivibile come prodotto di due elementi irriducibili  $2$  e  $x$ , mentre in  $\mathbb{Q}[x]$  questo non è vero, in quanto, essendo un campo,  $2$  è invertibile, quindi  $x$  è associato ad  $2x$  quindi è irriducibile come prodotto di fattori irriducibili

### Teorema: Lemma di Gauss

Sia  $f \in A[x]$ . Allora  $f$  è riducibile in  $Q[x]$  se e solo se è prodotto di due polinomi interi di grado maggiore di 1.

Inoltre, se  $f$  è primitivo, allora  $f$  è riducibile in  $Q[x]$  se e solo se  $f$  è riducibile in  $A[x]$

### Dimostrazione:

*Dimostriamo prima la prima parte*

$\Rightarrow$ ) Sia  $f$  riducibile in  $Q[x]$ , allora esistono  $h, g \in Q[x]$  non invertibili tali che

$$f = hg$$

Segue subito allora che  $f, g$  non sono costanti.

Sia quindi  $q \in \mathbb{Q}$  tale che  $qh$  sia un polinomio intero e primitivo. È sempre possibile trovare tale  $q$  perché possiamo prima moltiplicare tutti i coefficienti affinché siano tutti interi per poi dividere per il contenuto del polinomio.

Abbiamo quindi che  $f$  si può scrivere come

$$f = (q \cdot h)(q^{-1} \cdot h)$$

con  $qh$  primitivo per costruzione e per ipotesi  $f$  è intero. Quindi per il corollario precedente abbiamo che  $q^{-1}h$  è intero

$\Leftarrow$ ) Il viceversa invece è banale

*Dimostriamo la seconda parte*

Sia quindi  $f$  primitivo. Se  $f$  è riducibile in  $Q[x]$  abbiamo allora che, per la prima parte della dimostrazione,  $f$  è riducibile in  $A[x]$ .

Viceversa supponiamo  $f$  riducibile in  $Q[x]$ . Se fosse riducibile in  $A[x]$  la fattorizzazione in  $A[x]$  deve essere banale in  $Q[x]$  e quindi uno dei due fattori è una costante e, siccome  $f$  è primitivo, segue che tale costante è 1

□

Per quanto visto in precedenza abbiamo visto che se  $A$  è un campo, allora  $A[x]$  è un dominio euclideo mentre se non è un campo  $A[x]$  non è un dominio a ideali principali.

*Cosa sappiamo dire di  $\mathbb{Z}[x]$ ? Oppure di  $\mathbb{Q}[x, y] = (\mathbb{Q}[x])[y]$ ?*

Sappiamo che non sono domini a ideali principali ma dimostreremo che sono domini a fattorizzazione unica (*UFD*)

### Criterio

Se  $A$  è un dominio in cui ogni *NINZ* è prodotto di irriducibili, allora se  $A$  è un *UFD* allora gli irriducibili sono primi

#### Dimostrazione:

$\Rightarrow$ ) Sia  $\pi$  irriducibile.

Siano  $a, b \in A$  tali che  $\pi | a \cdot b$  allora esiste un elemento  $c \in A$  tale che:

$$c \cdot \pi = a \cdot b$$

Fattorizziamo  $a, b, c$  in fattori primi, abbiamo allora che l'uguaglianza diventa:

$$\pi \cdot c_1 \cdots c_r = a_1 \cdots a_s \cdot b_1 \cdots b_t$$

Per l'unicità della fattorizzazione abbiamo che  $\pi$  è associato ad un  $a_i$  oppure  $\pi$  è associato ad un  $b_j$ .

Quindi  $\pi | a$  oppure  $\pi | b$ . In entrambi i casi otteniamo che  $\pi$  è primo

$\Leftarrow$ ) L'abbiamo già dimostrato quando abbiamo mostrato l'unicità della fattorizzazione negli *UFD*

□

### Teorema

Se  $A$  è un *UFD*, allora  $A[x]$  è un *UFD*

#### Dimostrazione:

Mostriamo che in  $A[x]$  ogni elemento è prodotto di irriducibili

Sia quindi  $f \in A[x] \subseteq Q[x]$ . Sappiamo che  $Q[x]$  è un Dominio Euclideo, quindi possiamo scrivere  $f$  come

$$f = \pi_1 \cdots \pi_r$$

dove  $\pi_i \in Q[x]$  sono irriducibili.

Siano quindi  $q_1, \dots, q_r \in \mathbb{Q}$  delle costanti razionali tali che  $q_i \pi_i \in A[x]$  e che sia primitivo.

Basta usare lo stesso meccanismo che abbiamo menzionato nelle dimostrazioni precedenti.

Allora possiamo scrivere  $f$  come:

$$f = (q_1 \pi_1) \cdots (q_r \pi_r) \cdot \frac{1}{q_1 \cdots q_r}$$

Tuttavia abbiamo che, per ogni  $i$ , ogni  $q_i \pi_i$  è intero e primitivo per costruzione

Siccome, dal corollario precedente, abbiamo che il prodotto tra un razionale e un primitivo è un intero, segue che

$$a = \frac{1}{q_1 \cdots q_r} \in A$$

Visto che  $a \in A$ , possiamo scrivere  $a$  come la sua fattorizzazione in elementi irriducibili, sia quindi  $a = a_1 \cdots a_s$  tale fattorizzazione.

Osserviamo che gli  $a_i$  sono irriducibili anche in  $A[x]$

*Se così non fosse, sarebbero allora scrivibili come prodotto di polinomi di grado maggiore di 0 ma questo è un assurdo*

Segue allora, sempre per il corollario che

$$f = a_1 \cdots a_s \cdot (q_1 \pi_1) \cdots (q_r \pi_r)$$

Abbiamo che questi ultimi termini sono irriducibili in  $A[x]$  perché primitivi e irriducibili in  $Q[x]$

Segue quindi che  $f$  è prodotto di irriducibili.

Ci resta ora da dimostrare che gli irriducibili in  $A[x]$  sono anche primi.

Sia quindi  $f \in A[x]$  irriducibile. Allora possiamo distinguere due casi a seconda di  $\deg(f)$ :

- Se  $\deg(f) > 0$ : Possiamo considerare  $f$  primitivo (per quanto fatto in precedenza) di conseguenza  $f$  irriducibile in  $Q[x]$ , ci conseguenza anche primo in  $Q[x]$

Siano  $h, g \in A[x]$  tali che

$$f \mid hg \in A[x] \subseteq Q[x]$$

Senza perdere di generalità possiamo considerare che  $f \mid h$  in  $Q[x]$ , quindi

$$\exists \ell \in Q[x] : \ell f = h$$

Tuttavia sappiamo che possiamo scrivere  $\ell$  come prodotto di una costante  $q \in \mathbb{Q}$  per un polinomio  $\tilde{\ell}$  primitivo  
Quindi otteniamo che  $h$  può essere scritto come:

$$h = \ell \cdot f = q \cdot \tilde{\ell} \cdot f$$

Notiamo però che  $\tilde{\ell} \cdot f$  è prodotto di primitivi, quindi è ancora primitivo.

Sapendo che  $\ell$  è razionale, otteniamo che, per il lemma  $f$  è intero, da cui segue che  $\ell \in A[x]$

Da cui, direttamente, segue che  $f \mid h$  in  $A[x]$

- Se  $\deg(f) = 0$ , allora  $f = \pi$  e quindi è irriducibile in  $A$  e di conseguenza anche primo.

Siano  $h, g \in A[x]$  tali che  $\pi \mid hg$ , visto che è una costante, segue che  $\pi$  divide tutti i coefficienti, quindi in particolare divide  $c(hg)$  e, visto che il contenuto dei polinomi si comporta bene rispetto al prodotto, segue che  $\pi \mid c(f) \cdot c(g)$

Ma i contenuti delle funzioni sono elementi di  $A$  segue che  $\pi \mid c(h)$  oppure  $\pi \mid c(g)$ , quindi  $\pi = f$  è primo

□

### Definizione di Valutazione in $f$

Sia  $f \in A[x]$  fissato. Definiamo Valutazione in  $f$  l'applicazione:

$$v_f : A[x] \rightarrow A[x] \quad v_f(g(x)) = g(f(x))$$

È facile verificare che  $v_f$  è un omomorfismo.

Da ciò segue direttamente che

$$g = g_1 \cdot g_2 \Rightarrow v_f(g) = v_f(g_1) \cdot v_f(g_2)$$

In particolare, se  $v_f(g)$  è irriducibile, allora anche  $g$  lo è

Caso particolare della valutazione di  $f$

Poniamo  $f = x + 1$ , dalle osservazioni appena fatte segue che  $g(x)$  è irriducibile se e solo se  $g(x + 1)$  lo è

In questo caso abbiamo anche che  $v_{x+1}$  è invertibile e  $v_{x+1}^{-1} = x_{x-1}$

Infatti per esempio:

$$v_{x+1}(x^2 + 1) = (x + 1)^2 + 1 = x^2 + 2x + 2 \Leftrightarrow v_{x-1}(x^2 + 2x + 2) = (x^2 + 2x + 1) + 2(x - 1) + 2 = x^2 + 1$$

### Teorema: Criterio di Eisenstein

Sia  $f \in A[x]$  primitivo con  $f = a_0 + a_1x + \dots + a_nx^n$  tale che esista  $\pi \in A$  irriducibile tale che:

$$1) \quad \pi \mid a_0, \dots, \pi \mid a_{n-1}$$

$$2) \quad \pi \nmid a_0^2$$

Allora  $f$  è irriducibile sia in  $A[x]$  sia in  $Q[x]$

### Dimostrazione:

Supponiamo che  $f$  sia prodotto di due polinomi di grado strettamente positivo, in particolare supponiamo che:

$$f = (b_0 + b_1x + \dots)(c_0 + c_1x + \dots)$$

Sappiamo per ipotesi che  $a_0 = b_0 \cdot c_0$  e che  $\pi \mid a_0$ , allora, poiché  $A = UFD$ ,abbiamo che, essendo  $\pi$ , irriducibile, è anche primo, quindi o si ha che  $\pi \mid b_0$  oppure  $\pi \mid c_0$ , ma non può dividere entrambi contemporaneamente.

*Se così fosse avremmo che  $\pi \mid a_0^2$  contro la prima condizione di  $\pi$*

Supponiamo quindi che  $\pi \mid b_0$  e  $\pi \nmid c_0$

Per il prodotto di polinomi, sappiamo anche che  $a_1 = b_0 \cdot c_1 + b_1 \cdot c_0$ , per ipotesi abbiamo che  $\pi \mid a_1$  e per quanto assunto abbiamo che  $\pi \mid b_0$ . Otteniamo necessariamente che  $\pi \mid b_1 \cdot c_0$ , avendo assunto che  $\pi \nmid c_0$  segue necessariamente che  $\pi \mid b_1$ . Dimostriamo ora per induzione che:

$$\forall b \in \{0, \dots, n-1\} \quad \pi \mid b_i$$

Sempre per il prodotto di polinomi di polinomi abbiamo che per ogni  $i$  il termine  $a_i$ -esimo è:

$$a_i = b_0 c_i + b_1 c_{i-1} + \dots + b_i c_0$$

Per induzione abbiamo che  $\pi$  è divisore di tutti gli addendi tranne l'ultimo, abbiamo anche, per ipotesi, che  $\pi \mid a_i$  da cui segue che  $\pi \mid b_i c_0$ , da cui segue che  $\pi \mid b_i$ . Tutto questo è assurdo in quanto se fosse così avremmo che  $\pi \mid b_i$  per ogni  $i$ , quindi avremmo che  $\pi \mid f$  contro l'ipotesi che  $f$  sia primitivo.

□

### Esempio del Criterio di Eisenstein

Sia  $f = x^3 + 6x - 2$

Allora  $f$  è irriducibile in  $\mathbb{Z}[x]$  per il teorema di Eisenstein, in quanto

$$2 \mid 6 \quad 2 \mid -2 \quad 2^2 \nmid -2$$

### Proposizione

Sia  $p$  un numero primo, allora  $f = 1 + x + x^2 + \dots + x^{p-1}$  è irriducibile in  $\mathbb{Z}[x]$

#### Dimostrazione:

Per quanto visto in precedenza abbiamo che  $f(x)$  è irriducibile se e solo se  $f(x+1)$  lo è

Notiamo che se moltiplichiamo  $f(x)(x-1) = x^p - 1$

"Calcoliamo" quest'identità in  $x+1$  e otteniamo:

$$f(x+1) \cdot x = (x+1)^p - 1$$

Ma questo è esattamente uguale a

$$f(x+1) \cdot x = \sum_{i=0}^p \binom{p}{i} x^i - 1 = \sum_{i=1}^p \binom{p}{i} x^i$$

Deduciamo quindi che

$$f(x+1) = \sum_{i=1}^p \binom{p}{i} x^{i-1} = \binom{p}{1} + \binom{p}{2} x + \binom{p}{3} x^2 + \dots + \binom{p}{p} x^{p-1}$$

Esplicitando il coefficiente binomiale otteniamo che:

$$\binom{p}{i} = \frac{p!}{i! \cdot (p-i)!}$$

Quindi ogni coefficiente binomiale (per  $0 < i < p$ ) è multiplo di  $p$ , inoltre abbiamo che  $\binom{p}{p} = 1$ , quindi  $f(x+1)$  soddisfa il criterio di Eisenstein

□

## Polinomi Ciclotomici

Prima di dare una vera definizione di cosa sia un polinomio ciclotomico, diamo prima questa definizione:

### Definizione di Radice Primitiva

Una radice  $n$ -esima  $\omega$  di 1 si dice primitiva se  $\omega^m \neq 1 \forall m < n$

Sono esempi di radici primitive 1 per la radice prima di 1,  $-1$  come radice quadrata primitiva,  $e^{\frac{2\pi i}{3}}$  e  $e^{\frac{4\pi i}{3}}$  eccetera

### Proposizione

Esiste un'unica famiglia di polinomi  $\Phi_n(x)$  per  $x \geq 1$  tali che:

- 1)  $\Phi_n(x) \in \mathbb{Z}[x]$
- 2)  $\Phi_n(x)$  ha come radici complesse le radici primitive  $n$ -esime di 1, tutte con molteplicità 1
- 3)  $\Phi_n(x)$  è monico

### Dimostrazione:

Se  $a_1, \dots, a_{\phi(n)}$  sono le radici primitive  $n$ -esime allora

$$\Phi_n(x) = (x - a_1) \cdot (x - a_2) \cdots (x - a_{\phi(n)})$$

Prima di andare avanti con la dimostrazione facciamo degli esempi concreti con dei numeri piccoli:

Se prendiamo  $n = 1$  abbiamo che l'unica radice prima di 1 è 1, da cui segue che  $\Phi_1(x) = (x - 1)$

Prendiamo  $n = 2$ , le radici quadrate di 1 sono  $\pm 1$ , ma l'unica primitiva è  $-1$ , quindi  $\Phi_2(x) = (x + 1)$

Prendiamo adesso  $n = 3$ , le radici terze di 1 sono  $1, e^{\frac{2}{3}i\pi}, e^{\frac{4}{3}i\pi}$ , ma le uniche primitive sono le ultime due quindi abbiamo che:

$$\Phi_3(x) = (x - e^{\frac{2}{3}i\pi}) \cdot (x - e^{\frac{4}{3}i\pi})$$

Complichiamoci un po' la vita e prendiamo  $n = 12$  abbiamo che le radici primitive sono esattamente  $\phi(12) = 4$ , in particolare, se pensiamo al gruppo delle rotazioni  $D_{12}$ , sono esattamente gli elementi di ordine 12, quindi le radici dodicesime primitive di 1 sono  $e^{\frac{1}{12}i\pi}, e^{\frac{5}{12}i\pi}, e^{\frac{7}{12}i\pi}, e^{\frac{11}{12}i\pi}$ , da cui otteniamo che:

$$\Phi_{12}(x) = (x - e^{\frac{1}{12}i\pi}) \cdot (x - e^{\frac{5}{12}i\pi}) \cdot (x - e^{\frac{7}{12}i\pi}) \cdot (x - e^{\frac{11}{12}i\pi})$$

Prendiamo adesso un  $n$  qualsiasi e consideriamo  $x^n - 1$ . Questo polinomio può essere scritto come:

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

In quanto tutte le radici  $n$ -esime di 1 sono l'unione delle radici primitive  $d$ -esime al variare di  $d | n$

Mostriamo ora per induzione che  $\Phi_d(x)$  è monico e sta in  $\mathbb{Z}[x]$  per ogni  $d$  positivo

*Base Induttiva:*  $\Phi_1(x) = x - 1$  che è intero e monico

*Passo Induttivo:* Sia quindi  $n \in \mathbb{Z}$  e prendiamo  $x^n - 1$ :

$$x^n - 1 = \Phi_n(x) \cdot \prod_{d|n, d < n} \Phi_d(x)$$

Per ipotesi induttiva abbiamo che

$$g = \prod_{d|n, d < n} \Phi_d(x) \in \mathbb{Z}[x] \quad \text{e per ora} \quad \Phi_n(x) \in \mathbb{C}[x]$$

Sappiamo anche che  $x^n - 1 \in \mathbb{Z}[x]$  che è un anello euclideo

Notiamo che la divisione euclidea di  $x^n$  per  $g$  in  $\mathbb{C}[x]$  e in  $\mathbb{Q}[x]$  deve dare lo stesso risultato per l'unicità del quoziente e del resto della divisione in  $K[x]$

Da tutto questo segue come minimo che  $\Phi_n(x) \in \mathbb{Q}[x]$ , tuttavia, per il lemma che abbiamo utilizzato nelle scorse dimostrazioni, abbiamo che  $x^n - 1$  è intero e  $g$  è primitivo, da cui segue che  $\Phi_n(x) \in \mathbb{Z}[x]$

□

### Lemma

La divisione euclidea è unica in  $K[x]$

### Dimostrazione:

Siano  $a, b \in K[x]$  com  $b \neq 0$  e supponiamo esistano due risultati alla divisione euclidea:

$$a = q_1 b + r_1 = q_2 b + r_2$$

con il grado di  $r_1$  e di  $r_2$  strettamente minore del grado di  $b$

Andando a fare opportuni cambi otteniamo che:

$$b(q_1 - q_2) = r_2 - r_1$$

Se  $q_1$  e  $q_2$  fossero diversi avremmo che  $\deg(r_2 - r_1) = \deg(b(q_1 - q_2)) \geq \deg(b)$  Il che è assurdo

□

Sia  $p$  un primo e sia  $\Phi_p(x)$ , allora abbiamo che:

$$x^p - 1 = (x - 1) \cdot \Phi_p(x) = (x - 1)(x^{p-1} + x^{p-2} + \dots + 1)$$

Abbiamo che  $\Phi_p(x)$  è irriducibile

**Osservazione:** L'identità

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

ci permette di calcolare ricorsivamente tutti i  $\Phi_n(x)$ , infatti abbiamo che:

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{d|n, d < n} \Phi_d(x)}$$

**Esempio:**

$$\Phi_6(x) = \frac{x^6 - 1}{\Phi_1(x) \cdot \Phi_2(x) \cdot \Phi_3(x)} = \frac{(x^3 - 1)(x^3 + 1)}{(x - 1)(x + 1)(x^2 + x + 1)} = \frac{(x - 1)(x^2 + x + 1)(x + 1)(x^2 - x + 1)}{(x - 1)(x + 1)(x^2 + x + 1)} = x^2 - x + 1$$


---

# Estensioni di un Omomorfismo agli anelli dei Polinomi

## Proposizione

Siano  $A, B$  anelli (unitari e commutativi) e sia  $\phi : A \rightarrow B$  un omomorfismo. Allora esiste un unico omomorfismo

$$\varphi : A[x] \rightarrow B[x]$$

che gode delle seguenti proprietà:

$$\varphi(a) = \phi(a) \quad \varphi(x) = x$$

## Dimostrazione:

Per le proprietà di omomorfismo di  $\phi$  abbiamo che  $\varphi(1) = \phi(1) = 1$

L'unicità di  $\varphi$  segue dalle prescrizioni, infatti:

$$\varphi(a_0 + a_1x + \cdots + a_nx^n) = \phi(a_0) + \phi(a_1)x + \cdots + \phi(a_n)x^n$$

Inoltre  $\varphi$  rispetta sia la somma sia il prodotto. *Senza scrivere le verifiche, sono sempre le stesse*

□

**Osservazione:** Sia  $a \in A$ , allora possiamo considerare l'applicazione  $v_a$  definita come:

$$v_a : A[x] \Rightarrow A \quad v_a(f) = \tilde{f}(a)$$

Notiamo che è un omomorfismo

Infatti

$$v_a(f+g) = \widetilde{f+g}(a) = (\tilde{f}+\tilde{g})(a) = \tilde{f}(a) + \tilde{g}(a) = v_a(f) + v_a(g)$$

*Se mettiamo · al posto di + otteniamo che è verificata anche per il prodotto*

Segue poi banalmente che  $v_a(1) = 1$

## Corollario

Siano  $A, B$  anelli e sia  $\phi : A \rightarrow B$  un omomorfismo e  $b \in B$ , allora esiste un unico omomorfismo

$$\psi : A[x] \rightarrow B$$

tale che goda delle seguenti proprietà:

$$\psi(a) = \phi(a) \quad \psi(x) = b$$

## Dimostrazione:

Banalmente basta porre

$$\phi = v_b \circ \varphi$$

e otteniamo un omomorfismo come desiderato

*È omomorfismo in quanto è composizione di omomorfismi*

□

Un caso particolare va fatto per l'applicazione  $\phi : \mathbb{Z} \rightarrow \mathbb{Z}/p$ , in particolare:

$$\varphi : \mathbb{Z}[x] \rightarrow \mathbb{Z}/p[x]$$

Abbiamo che  $\varphi$  è un omomorfismo detto riduzione modulo  $p$ . In particolare:

$$f = hg \in \mathbb{Z}[x] \quad \Rightarrow \quad \varphi(f) = \varphi(h)\varphi(g) \in \mathbb{Z}/p[x]$$

**Osservazione:** Andiamo a vedere come sono i polinomi irriducibili in  $\mathbb{Z}/_2[x]$ :

- *Grado 1:*  $x, x + 1$  e sono entrambi irriducibili
- *Grado 2:* Sono 4, di cui tre ( $x^2, (x + 1)^2, x^2 + x$ ) sono riducibili mentre uno no ( $x^2 + 1$ )
- *Grado 3:* Sono 8 (4 come prodotti di termini di primo grado, 2 come prodotti di un termine di primo grado e uno di secondo e 2 irriducibili)

Più in generale abbiamo che se  $K$  è un campo con  $q$  elementi, ossia  $|K| = q$ , i polinomi monici irriducibili sono:

- *Grado 1:* Sono della forma  $x + a$  con  $a \in K$ , quindi abbiamo  $q$  elementi
- *Grado 2:* Sono della forma  $x^2 + ax + b$  con  $a, b \in K$ .

Per contarli facilmente possiamo prendere tutti i polinomi di quella forma ( $q^2$ ) e togliere i quelli di primo grado  $q$  e quelli che sono prodotti di due polinomi di primo grado  $\frac{q(q-1)}{2}$  quindi in tutto sono:

$$q^2 - q - \frac{q(q-1)}{2} = \frac{q^2}{2} - \frac{q}{2}$$

Vediamo come la riduzione modulo  $p$  si comporta con gli omomorfismi di anelli +

### Lemma

Siano  $\phi : A \rightarrow B$  un omomorfismo di anelli e sia  $\varphi : B \rightarrow B[x]$  un'estensione di polinomi.

Se  $A$  è un dominio e  $f = f_1 f_2 \in A[x]$  allora  $\varphi(f)$  si fattorizza in  $B[x]$  in due polinomi di grado  $\deg(f_1)$  e  $\deg(f_2)$  purché  $\phi$  non si annulla sul coefficiente di  $f$

### Dimostrazione:

Abbiamo che

$$f = f_1 f_2 \quad \Rightarrow \quad \varphi(f) = \varphi(f_1) \varphi(f_2)$$

Se  $c$  è il coefficiente direttore di  $f$  e  $a, b$  sono rispettivamente i coefficienti direttori di  $f_1$  e  $f_2$ , allora, poiché  $A$  è un dominio:

$$c = ab \Rightarrow \phi(c) = \phi(a)\phi(b)$$

Inoltre, sapendo che:  $\phi(c) \neq 0$ , abbiamo che  $\phi(a), \phi(b) \neq 0$  da cui deduciamo che:

$$\deg(\phi(f_1)) = \deg(f_1) \quad \deg(\phi(f_2)) = \deg(f_2)$$

□

### Corollario

Sia  $f \in \mathbb{Z}[x]$  primitivo e siano  $p$  primo tale che  $p$  non divida il direttore coefficiente di  $f$

Indichiamo con  $f \mapsto \bar{f}$  la riduzione modulo  $p$  dei coefficienti.

Se  $\bar{f}$  è irriducibile, allora  $f$  è irriducibile

### Dimostrazione:

Basta applicare il lemma con  $A = \mathbb{Z}$  e  $B = \mathbb{Z}/_p$

□

Esempi di Polinomi Irriducibili con Riduzione modulo p

Consideriamo

$$f = 7x^2 - 5x + 3 \in \mathbb{Z}[x]$$

è riducibile in  $\mathbb{Z}[x]$ ?

Facendo la riduzione in  $\mathbb{Z}/_2$  abbiamo che

$$\bar{f} = x^2 + x + 1$$

che è irriducibile in  $\mathbb{Z}[x]/_2$ , quindi  $f$  è irriducibile

*Consideriamo*

$$g = 9x^3 + 5x^2 - 3x + 2$$

Facciamo la riduzione di  $g$  in  $\mathbb{Z}[2]/_2$ , otteniamo che

$$\bar{g} = x^3 + x^2 + x = x(x^2 + x + 1)$$

Avendo trovato una riduzione, il lemma non ci dice niente

Proviamo in  $\mathbb{Z}/5$ , allora

$$\bar{g} = -x^3 + 2x + 2$$

che in  $\mathbb{Z}/5$  non ha radici (Basta sostituire i 5 elementi)

Quindi  $\bar{g}$  è irriducibile in  $\mathbb{Z}[x]/_5$ , quindi  $g$  è irriducibile in  $\mathbb{Z}[x]$

*Consideriamo*

$$h = x^4 - 3x^3 - x^2 + 1$$

Per quanto dimostrato in precedenza abbiamo che una delle possibili radici è  $\pm 1$ , tuttavia, andando a calcolare il polinomio in  $\pm 1$  non otteniamo 0.

Abbiamo quindi che l'unica fattorizzazione possibile è quella in cui  $h$  si scrive come prodotto di due polinomi di secondo grado

Proviamo a ridurre  $h$  in  $\mathbb{Z}/2$ , otteniamo che:

$$\bar{h} = x^4 + x^3 + x^2 + 1$$

e in questo caso 1 è radice del polinomio, quindi la mera applicazione del corollario non serve a niente

Andiamo però a fare la scomposizione con Ruffini.

Con Ruffini abbiamo che  $\bar{h}$  si fattorizza come:

$$\bar{h} = (x+1)(x^3 + x + 1)$$

Possiamo concludere che  $h$  in  $\mathbb{Z}[x]$  è irriducibile perché  $\bar{h}$  in  $\mathbb{Z}/2[x]$  non è prodotto di due polinomi di grado 2

### Lemma

In un campo finito il prodotto di non quadrati è un quadrato

### Dimostrazione:

Supponiamo  $|K| = q$

Se la caratteristica del campo è  $Char(K) = 2$  allora tutti gli elementi sono quadrati

Altrimenti in  $q$  dispari abbiamo che  $K^*$  è ciclico (dove  $K^* = \{x, x^2, x^3, \dots, x^{q-1} = 1\}$ )

I non quadrati sono potenze di  $x$  con esponente dispari, quindi il prodotto di due quadrati ha esponente pari, quindi è un quadrato

□

### Proposizione

Il polinomio  $x^4 + 1$  è irriducibile in  $\mathbb{Z}[x]$  ma è riducibile in  $\mathbb{Z}/p[x]$  per ogni  $p$  primo

### Dimostrazione:

Osserviamo che per il lemma almeno uno tra  $-1, 2 - 1$  è un quadrato

Infatti, se non lo sono  $-1$  e  $2$ , allora  $-2$  lo è in quanto è prodotto di non quadrati.

Caso 1: Se  $1$  è un quadrato, allora  $a^2 = 1$  in  $\mathbb{Z}/p \Rightarrow (x^2 + a)(x^2 - a) = x^4 + 1$

Caso 2: Se  $2$  è un quadrato, allora  $a^2 = 2$  in  $\mathbb{Z}/p$

I due fattori dovranno necessariamente essere della forma

$$(x^2 + bx + a)(x^2 - bx + a)$$

Notiamo che il coefficiente di secondo grado è

$$+1 - b^2 + 1 = 0 \Rightarrow b = a$$

Allora possiamo scrivere

$$x^4 + 1 = (x^2 + ax + 1)(x^2 - ax + 1)$$

*Caso -2:* Se abbiamo che  $-2 = a^2$  in  $\mathbb{Z}/p$ , allora abbiamo che:

$$(x^2 + ax + 1)(x^2 - ax + 1) = x^4 + (-1 - a^2 - 1)x^2 + 1 = x^4 + 1$$

Mostriamo allora adesso che  $x^4 + 1$  è irriducibile in  $\mathbb{Z}[x]$

Da un esercizio precedente sappiamo che la sua fattorizzazione in  $\mathbb{R}[x]$  è:

$$x^4 + 1 = (x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1)$$

Se si fattorizzasse anche in  $\mathbb{Q}[x]$  come prodotto di due polinomi di grado 2 avremmo che

$$x^4 + 1 = fg \quad \text{con } \deg(f) = \deg(g) = 2$$

Se così fosse, avremmo che  $f$  è in qualche modo associato a  $x^2 \pm \sqrt{2}x + 1$  in  $\mathbb{R}[x]$

In particolare se  $f = x^2 + ax + b$  avremmo che  $a = \pm\sqrt{2}$ , ma  $a \notin \mathbb{Q}$

□

Con questa proposizione, possiamo dare delle dimostrazioni diverse a dei teoremi precedenti:

#### Dimostrazione Alternativa di Heisenstein:

Sia

$$f = a_0 + a_1x + a_nx^n$$

con

$$p \mid a_i \quad i \in \{0, \dots, n-1\} \quad p^2 \nmid a_0 \quad p \nmid a_n$$

Consideriamo adesso la riduzione in  $\mathbb{Z}/p$ , allora  $\bar{f}$  sarà:

$$\bar{f} = a_nx^n$$

Supponiamo di avere che

$$f = f_1f_2 \in \mathbb{Z}[x] \quad \Rightarrow \quad \bar{f} = \bar{f}_1\bar{f}_2 \in \mathbb{Z}/p[x]$$

dove  $\bar{f}_1$  e  $\bar{f}_2$  sono potenze di  $x$  e hanno termine noto nullo, allora  $f_1$  e  $f_2$  hanno termine noto multiplo di  $p$ , allora  $p \mid [f_1f_2]_0 = [f]_0 = a_0$ , il che è assurdo

□

#### Dimostrazione Alternativa del Prodotto di Primitivi:

Siano  $f, g$  primitivi, vogliamo dimostrare che  $fg$  è primitivo

Se così non fosse esisterebbe un elemento  $p$  che divide tutti i coefficienti di  $fg$ , quindi riducendo in  $\mathbb{Z}/p[x]$  avremmo che:

$$\overline{fg} = 0 \quad \Rightarrow \quad \overline{f}\overline{g} = 0 \quad \Rightarrow \quad f \text{ non primitivo} \vee g \text{ non primitivo}$$

□

#### Lemma

$$f, g \in \mathbb{Z}/p[x] \quad \Rightarrow \quad f(x)^p = f(x^p)$$

**Dimostrazione:**

Siano  $h, g \in \mathbb{Z}/p[x]$ , allora abbiamo che:

$$(h+g)^p = \sum_{k=0}^n \binom{p}{k} h^k g^{p-k} = h^p + g^p$$

Questo è vero perché

$$p \mid \binom{p}{k} \quad \forall k \in \{1, \dots, n-1\}$$

Allora prendendo  $f$  come:

$$f = a_0 + a_1 x + \dots + a_n x^n$$

Usando il piccolo teorema di Fermat abbiamo che:

$$(f(x))^p = a_0^p + (a_1 x)^p + \dots + (a_n x^n)^p = a_0 + a_1 x^p + \dots + a_n x^{pn} = f(x^p)$$

□

**Lemma**

Sia

$$S = \{\text{Radici primitive } n\text{-esime di 1}\}$$

Sia  $T \subseteq S$  non nullo tale che

$$\forall \zeta \in T \text{ e } \forall p \text{ primo tale che } p \nmid n \Rightarrow T = S$$

**Dimostrazione:**

Sia  $\zeta \in T$ . Sappiamo che  $\zeta$  genera il gruppo delle radici  $n$ -esime.

Gli altri generatori sono  $\zeta^k$  tali che  $\mathcal{MCD}(k, n) = 1$ , allora possiamo considerare

$$\zeta^{p_1 p_2 \cdots p_r} \quad \text{dove } p_i \text{ sono i primi che non dividono } n$$

Per Ipotesi abbiamo che

$$\zeta^{p_1} \in T \Rightarrow (\zeta^{p_1})^{p_2} \in T \Rightarrow \dots \Rightarrow \zeta^{p_1 p_2 \cdots p_r} \in T$$

□

**Teorema**

I polinomi ciclotomici  $\Phi_n(x)$  sono irriducibili in  $\mathbb{Z}[x]$  (e quindi anche in  $\mathbb{Q}[x]$ )

**Dimostrazione:**

Sia  $P = x^n - 1$  e sia  $f$  un fattore irriducibile di  $\Phi_n(x)$

Se  $f \neq \Phi_n(x)$  abbiamo che le radici di  $f$  non sono tutte le radici primitive di 1

Per il lemma precedente abbiamo che  $\exists \zeta$  radice di  $f$  tale che  $\zeta^p$  non è radice di  $f$  per un opportuno primo  $p \nmid n$

Abbiamo quindi che  $\zeta^p$  è radice di un altro fattore irriducibile di  $\Phi_n(x)$  che chiameremo  $g$

Segue subito quindi che:

$$fg \mid \Phi_n(x)$$

$\zeta$  è radice del polinomio  $g(x^p)$ , quindi  $g(x^p)$  è un multiplo di  $f$

Allora abbiamo che  $g(x^p) = h(x)f(x)$

Consideriamo la riduzione modulo  $p$ : otteniamo quindi che:

$$g(x^p) \mapsto \overline{g(x^p)} = \overline{g(x)^p} = \bar{g} \quad h(x) \mapsto \overline{h(x)} = \bar{h} \quad f(x) \mapsto \overline{f(x)} = \bar{f}$$

Sai  $\pi$  un fattore irriducibile di  $\bar{f}$ , allora  $\pi$  divide anche  $\bar{g}$

Abbiamo allora che  $\bar{P}$  è multiplo di  $\bar{f}\bar{g}$ , ma allora  $\pi^2$  è divisore di  $\bar{P}$ , quindi  $\pi$  è divisore di  $\bar{P}'$ .

Questo è assurdo in quanto:

$$\overline{P}' = nx^{n-1} \quad \overline{P} = x^n - 1$$

Abbiamo che gli unici divisori di  $\overline{P}'$  sono potenze di  $x$ , che non sono divisori di  $\overline{P}$ , quindi  $\text{MCD}(\overline{P}, \overline{P}') = 1$

Quindi  $\Phi_n(x)$  è necessariamente riducibile

□

**Osservazione:** Sia  $\alpha \in \mathbb{C}$  radice di due polinomi  $f, g \in \mathbb{Q}[x]$  con  $f$  irriducibile in  $\mathbb{Q}$ . Allora  $f \mid g$

Infatti, consideriamo:

$$I = \{\text{Polinomi che hanno } \alpha \text{ come radice}\}$$

Questo è un ideale, ma poiché siamo in un dominio euclideo, e in particolare in un dominio a ideali principale e abbiamo che  $f \in I$ , sapendo che è irriducibile, abbiamo che  $(f) = I$ , avendo poi che  $\alpha$  è radice anche di  $g$ ,

$$g \in I \Rightarrow g \in (f) \Rightarrow f \mid g$$


---

# Quozienti di $K[x]$

Ricordiamo che se  $K$  è un campo, allora  $K[x]$  è un dominio a ideali principali, quindi se  $I$  è un ideale di  $K[x]$ , allora esiste un  $f \in K[x]$  tale che  $(f) = I$

## Proposizione

Se  $f \in K[x]$  di grado  $n > 1$ , allora  $K[x]/(f)$  è un  $K$ -spazio vettoriale di dimensione  $n$  e con base  $\mathcal{B} = \{[1], [x], \dots, [x^{n-1}]\}$

### Dimostrazione:

Notiamo come prima cosa che  $K[x]/(f)$  contiene una "copia" di  $K$  (ossia contiene un sottoanello isomorfo a  $K$ ), infatti basta pensare alle classi delle costanti.

Se prendiamo  $[a], [b]$  con  $a, b \in K$  se sommano e si moltiplicano come in  $K$ :

$$[a] + [b] = [a + b] \quad [a] \cdot [b] = [a \cdot b]$$

Inoltre abbiamo che  $[a] = [b] \Leftrightarrow a = b$ , infatti:

$$[a] = [b] \Rightarrow [a - b] = [0] \Leftrightarrow a - b \in (f) \Rightarrow f \mid a - b \xrightarrow{\deg(f) > \deg(a-b)} a - b = 0 \Rightarrow a = b$$

Mostriamo che  $\mathcal{B}$  è effettivamente una base

Sappiamo che  $K[x]/(f)$  è generato da  $x^i$  per ogni  $i$  positivo

Infatti se  $i \geq n$ , possiamo sfruttare la relazione data da  $f$ , ossia:

$$f = x^n + g(x) \quad \text{con } \deg(g) < \deg(f)$$

Allora possiamo scrivere  $[x^n] = -[g(x)]$  e possiamo quindi diminuire il grado, quindi ripetendo questo ragionamento per un numero finito di volte, otteniamo che  $[1], [x], \dots, [x^{n-1}]$  bastano per generare  $K[x]/(f)$

Vediamo ora che questi sono effettivamente linearmente indipendenti.

Siano quindi  $a_0, a_1, \dots, a_{n-1} \in K$  tali che:

$$a_0[1] + a_1[x] + \dots + a_{n-1}[x^{n-1}] = [0] = [a_0 + a_1x + \dots + a_{n-1}x^{n-1}] = [0]$$

E questo è vero se e solo se:

$$f \mid (a_0 + a_1x + \dots + a_{n-1}x^{n-1})$$

Ma sfruttando i gradi dei polinomi, abbiamo che il grado della combinazione lineare scritta sopra è minore di  $n$  che è il grado di  $f$  e l'unico multiplo di  $f$  di grado inferiore di  $f$  stesso è il polinomio nullo, da cui:

$$a_0 + a_1x + \dots + a_{n-1}x^{n-1} = 0 \quad \Leftrightarrow \quad a_0 = a_1 = \dots = a_{n-1} = 0$$

Quindi  $\mathcal{B}$  è effettivamente una base

□

**Esempio:** Sia  $f = x^2 + x + 1$  allora:

$$[x^4] = [x^2] \cdot [x^2] = [-1 - x] \cdot [-1 - x] = [1 + 2x + x^2] = [-1 - x + 1 + 2x] = [x]$$

Quando è vero che  $K[x]/(f)$  è un campo?

In generale sappiamo che  $A/I$  è un campo se e solo se  $I$  è massimale (questo è vero per ogni anello)

## Lemma

Sia  $A$  un dominio a ideali principali  $PID$  nel nostro caso  $A = K[x]$  e sia  $f \in A$  e  $f \neq 0$ . Allora sono equivalenti:

- 1)  $A/(f)$  è un campo
- 2)  $(f)$  è massimale
- 3)  $f$  è irriducibile

### Dimostrazione:

La dimostrazione  $1 \Leftrightarrow 2$  l'avevamo già vista negli esercizi

$2 \Rightarrow 3$ ) Se  $f$  fosse invertibile, allora  $(f) = A$ , quindi  $(f)$  non è massimale

Se invece  $f$  fosse riducibile avremmo che  $f = f_1 f_2$  con  $f_1$  e  $f_2$  non invertibili, allora

$$(f) \subsetneq (f_1) \subsetneq A$$

e quindi è ancora non massimale

$3 \Rightarrow 2$ ) Se  $(f)$  non fosse massimale, avremmo che se  $(f) = A$ , allora  $f$  è invertibile, mentre se  $(f) \subsetneq (g) \subsetneq A$ , quindi  $f$  è multiplo di  $g$ , ossia esiste un fattore  $h$  tale che:

$$f = gh \quad \text{con } h \text{ non invertibile}$$

Quindi  $f$  è riducibile

□

Facciamo questo richiamo per la prossima dimostrazione:

Sia  $x^2 - d$  con  $d \in K$ . È irriducibile in se e solo se non ha radici, cioè se e solo se  $d$  non è un quadrato in  $K$  cioè se e solo se  $K[\sqrt{d}]$  è un campo

### Proposizione

$$\forall \alpha \in K, \quad K[\sqrt{d}] \cong K[x]_{(x^2-d)}$$

#### Dimostrazione:

Esistono due modi di dimostrarlo, usando il Metateorema oppure facendo i conti espliciti

Usiamo prima il Metateorema: vogliamo costruire un'applicazione  $\varphi$  tale che:

$$\varphi : K[x] \rightarrow K[\sqrt{d}] \quad \varphi(a) = a, \forall a \in K \quad \varphi(x) = \varepsilon$$

Notiamo prima di tutto che  $\varphi$  è lineare tra due spazi vettoriali, infatti:

$$\varphi(af) = \varphi(a)\varphi(f) = a\varphi(f)$$

Segue immediatamente che  $\varphi$  si comporta come l'identità sulle costanti

Vediamo subito che  $\text{Ker}(\varphi) \subseteq (x^2 - d)$ , in quanto

$$\varphi(x^2 - d) = \varepsilon^2 - d = d - d = 0$$

Siccome poi  $\varphi$  è suriettiva e  $K[x]_{(f)} \cong K[\sqrt{d}]$  e  $\dim(K[\sqrt{d}]) = 2$ , necessariamente si ha che  $\text{Ker}(\varphi)$  è generato da un polinomio di grado 2 da cui segue subito che:

$$\text{Ker}(\varphi) = (x^2 - d)$$

Vediamo ora con i conti espliciti: sia ora

$$\psi : K[\sqrt{d}] \rightarrow K[x]_{(x^2-d)} \quad a + b\varepsilon \xrightarrow{\phi} [a + bx]$$

Notiamo che  $\psi$  è l'identità su  $K$  e che  $\psi(\varepsilon) = x$  e che  $[x^2] = [d]$

Quindi  $\varepsilon$  va in un elemento che al quadrato da  $d$

□

Questo tipo di discorso può essere fatto con un qualsiasi polinomio

Esempio di Estensione di Campo con un polinomio di Terzo Grado

Sia  $f = 1 + x + x^2 + x^3 \in \mathbb{Q}[x]$

Possiamo estendere  $\mathbb{Q}$  con un elemento  $\varepsilon$  tale che:

$$1 + \varepsilon + \varepsilon^2 + \varepsilon^3 = 0$$

Chi è  $\mathbb{Q}[\varepsilon]$

$$\mathbb{Q}[\varepsilon] = \{a + b\varepsilon + c\varepsilon^2 : a, b, c \in \mathbb{Q}\} \cong \mathbb{Q}[x]_{(1+x+x^2+x^3)}$$

**Attenzione:** Se  $\alpha \in \mathbb{C}$  è radice di  $f = 1 + x + x^2 + x^3$ ,  $\mathbb{Q}[\varepsilon]$  non può essere pensato come un anello che contiene sia  $\mathbb{Q}$  e  $\alpha$ . Infatti  $\mathbb{Q}[\varepsilon]$  non è un dominio di integrità, infatti:

$$(1 + \varepsilon)(1 + \varepsilon^2) = 0$$

Quindi  $\mathbb{Q}[\varepsilon] \not\subset \mathbb{C}$

Le cose cambiano se  $f$  è irriducibile

### Definizione di $K[\alpha]$

Sia  $f \in K[x]$  e consideriamo  $K \subseteq L$  (non necessariamente campi) e  $\alpha \in L$

Sapendo che

$$v_\alpha : K[x] \rightarrow L \quad f \xrightarrow{v_\alpha} \tilde{f}(\alpha)$$

è la valutazione in  $\alpha$ , si definisce l'immagine di  $v_\alpha$ , che denoteremo con  $K[\alpha]$  come il sottoanello più piccolo che contiene sia  $K$  sia  $\alpha$

### Teorema

Siano  $K \subseteq L$  due campi e sia  $f \in K[x]$  irriducibile in  $K[x]$  e sia  $\alpha \in L$  radice di  $f$ . Allora:

$$K[x]/(f) \cong K[\alpha]$$

### Dimostrazione:

Consideriamo  $v_\alpha : K[x] \rightarrow K[\alpha]$ . Questa è suriettiva per definizione

Andiamo a vedere chi è il nucleo per  $v_\alpha$

Sicuramente abbiamo che  $f \in \text{Ker}(\alpha)$  in quanto  $f(\alpha) = 0$  Quindi sicuramente  $(f) \subseteq \text{Ker}(v_\alpha)$

In realtà possiamo già dire che vale l'uguaglianza, in quanto, visto che i polinomi di  $\text{Ker}(\alpha)$  sono quelli che si annullano in  $\alpha$ , sono tutti multipli di  $f$

Basta rivedere l'osservazione fatta precedentemente

□

### Corollario

Se  $f \in K[x]$  irriducibile e  $\alpha \in L \subseteq K$  (dove  $K$  e  $L$  sono campi) tale che  $\alpha$  è radice di  $f$ , allora  $K[\alpha]$  è uno spazio vettoriale di dimensione  $\deg(f)$

### Teorema Fondamentale di Isomorfismo delle Estensioni Semplici

Siano  $L$  e  $L'$  due estensioni di  $K$  tali che:

$$K \subseteq L \quad K \subseteq L'$$

Siano poi  $\alpha \in L$  e  $\alpha' \in L'$  entrambe radici di  $f$

Allora

$$K[\alpha] \cong K[\alpha']$$

### Dimostrazione:

Segue direttamente dalla transitività dell'isomorfismo:

$$K[\alpha] \cong K[x]/(f) \cong K[\alpha'] \quad \Rightarrow \quad K[\alpha] \cong K[\alpha']$$

□

Più in generale vale

### Teorema (lo stesso di prima ma più in generale)

Siano  $K$  e  $K'$  due campi isomorfi con

$$\phi : K \rightarrow K' \quad \text{isomorfismo che li lega}$$

Estendiamo  $\phi$  a

$$\varphi : K[x] \rightarrow K'[x]$$

Sia adesso  $f \in K[x]$  irriducibile e sia  $f' \in K'[x]$  tale che:

$$f' = \varphi(f)$$

Siano  $L \subseteq K$  un'estensione di campi e  $L' \supseteq K'$  un'altra estensione e siano  $\alpha \in L$  radice di  $f$  e  $\alpha' \in L'$  radice di  $f'$

Allora esiste un isomorfismo

$$\psi : K[\alpha] \rightarrow K'[\alpha'] \quad \text{tale che} \quad \psi(a) = \phi(a) \quad \psi(\alpha) = \alpha'$$

### Dimostrazione:

$$\begin{array}{ccccc} & \leftarrow & & \rightarrow & \\ K[\alpha] & \xleftarrow{\cong} & K[x]_{(f)} & \xrightarrow{\varphi} & K'[x]_{(f')} \xleftarrow{\cong} K'[\alpha'] \end{array}$$

□

Facciamo una piccola proposizione che potrà risultare comoda in futuro

### Definizione di Polinomio Ribaltato

Sia  $f \in A[x]$  con

$$f = a_0 + a_1x + \cdots + a_nx^n$$

Si definisce polinomio ribaltato il polinomio  $\overleftrightarrow{f} \in A[x]$

$$\overleftrightarrow{f} = a_n a_{n-1} x + \cdots + a_1 x^{n-1} + a_0 x^n$$

### Proposizione

$f$  è irriducibile se e solo se  $\overleftrightarrow{f}$  è irriducibile

### Dimostrazione:

Basta mostrare infatti che:

$$\overleftrightarrow{f} = x^{\deg(f)} f\left(\frac{1}{x}\right)$$

□

È anche vero infatti che:

$$\overleftrightarrow{f} \overleftrightarrow{g} = x^{\deg(f)} f\left(\frac{1}{x}\right) x^{\deg(g)} g\left(\frac{1}{x}\right) = x^{\deg(fg)} (fg)\left(\frac{1}{x}\right) = (\overleftarrow{f} \overrightarrow{g})$$

## Definizione di Elemento Algebrico

Sia  $\alpha \in L$  e  $L \supseteq K$  un'estensione di campo.

Si dice che  $\alpha$  è algebrico su  $K$  se:

$$\exists f \in K[x], f \neq 0 : \tilde{f}(\alpha) = 0$$

Cioè  $\alpha$  è radice di  $f$

Un numero complesso si dice algebrico se è algebrico in  $\mathbb{Q}$

### Esempio di Numero Algebrico

Prendiamo  $\alpha = \sqrt{2}$ ,  $\alpha$  è algebrico in quanto è radice del  $x^2 - 2$

Prendiamo ora  $\beta = \sqrt{2} + \sqrt{3}$ ,  $\beta$  è algebrico in quanto:

$$\beta = \sqrt{2} + \sqrt{3} \Rightarrow \beta^2 = 5 + 2\sqrt{6} \Rightarrow \beta^2 - 5 = 2\sqrt{6} \Rightarrow \beta^2 - 10\beta + 25 = 26 \Rightarrow \beta^2 - 10\beta + 1 = 0$$

Quindi è radice del polinomio

$$x^4 - 10x^2 + 1$$

## Proposizione

Se  $\alpha$  è algebrico, allora esiste un unico polinomio monico irriducibile  $f$  tale che  $\alpha$  è una radice di  $f$  e tale polinomio  $f$  genera l'ideale dei polinomi che si annullano in  $\alpha$ .

## Definizione di Polinomio Minimo

Un polinomio che ha questa caratteristica, prende il nome di polinomio minimo

### Dimostrazione:

Sia  $g \in K[x]$  che abbia  $\alpha$  come radice, allora

$$g = \pi_1 \cdot \pi_2 \cdots \pi_r$$

come fattorizzazione in irriducibili, infatti ( $\pi_i \in K[x]$  sono irriducibili)

Allora abbiamo che

$$\tilde{g}(\alpha) = \tilde{\pi}_1(\alpha) \cdot \tilde{\pi}_2(\alpha) \cdots \tilde{\pi}_r(\alpha) = 0$$

Andiamo ora a definire

$$I = \{\text{Polinomi che si annullano in } \alpha\}$$

Questo è un ideale e poiché  $K$  è un campo, allora  $K[x]$  è un PID ma anche di più, quindi è  $I = (f)$

Siccome  $I$  contiene un irriducibile, abbiamo che il polinomio minimo che genera  $I$  è proprio questo  $f$

□

**Notazione:** Indichiamo con  $K(\alpha)$  con  $\alpha \in L \supseteq K$  il campo dei quozienti di  $K[x]$ :

Notiamo subito che  $K(\alpha) \subseteq L$ , in particolare abbiamo che:

$$K(\alpha) = \left\{ \frac{\tilde{f}(\alpha)}{\tilde{g}(\alpha)} : f, g \in K[x], \tilde{g}(\alpha) \neq 0 \right\}$$

## Definizione di Estensione Finita

Diciamo che  $L \supseteq K$  è un'estensione finita di  $K$  se  $\dim_k(L) < \infty$

### Teorema

Siano  $K \subseteq L$  e  $\alpha \in L$ . Allora sono equivalenti:

- 1)  $\alpha$  è algebrico
- 2)  $K[\alpha]$  è un  $K$ -spazio vettoriale
- 3)  $K(\alpha)$  è un'estensione finita di  $K$
- 4)  $K(\alpha) = K[\alpha]$

### Dimostrazione:

1  $\Rightarrow$  2) Se  $f$  è il polinomio minimo di  $\alpha$ , allora abbiamo che  $K[x]_{/(f)} \simeq K[\alpha]$  che ha dimensione  $\deg(f)$

2  $\Rightarrow$  3) Sia  $\dim_K(K[\alpha]) = n$ , allora  $1, \alpha, \dots, \alpha^n$  sono linearmente dipendenti, allora:

$$\exists k_0, k_1, \dots, k_n \in k \text{ non tutti nulli tali che : } k_0 + k_1\alpha + \dots + k_n\alpha^n = 0$$

Quindi  $\alpha$  è una radice del polinomio  $k_0 + k_1x + \dots + k_nx^n$ , allora è vero che  $K[\alpha] \simeq K[x]_{/(f)}$  con  $f$  il polinomio minimo. Ma questo è un campo, allora  $K[\alpha] = K(\alpha)$

3  $\Rightarrow$  4) Basta ripetere i passaggi precedenti

4  $\Rightarrow$  1) Notiamo che  $\alpha^{-1} \in K[x]$ , infatti

$$\exists f \in K[x] : \alpha^{-1} = \tilde{f}(\alpha) \Rightarrow \tilde{f}(\alpha) - \alpha^{-1} = 0 \Rightarrow \alpha\tilde{f}(\alpha) - 1 = 0$$

Quindi  $\alpha$  è radice del polinomio  $xf - 1$

□

### Corollario

Se  $K \subseteq L$  è un'estensione finita, allora ogni elemento di  $L$  è algebrico in  $K$

### Dimostrazione:

Sia  $\alpha \in L, L \supseteq K$ , allora  $K[\alpha]$  è sottospazio di  $L$  e quindi ha ancora dimensione finita

□

### Definizione di Estensione Algebrica

Sia  $K \subseteq L$ .  $L$  si chiama estensione algebrica se ogni elemento di  $L$  è algebrico su  $K$

Notiamo che il fatto che un'estensione sia Finita implica che sia algebrica, ma non è vero il contrario

### Definizione di Grado dell'Estensione

Sia  $K \subseteq L$  un'estensione, allora si definisce il grado dell'estensione il valore:

$$[L : K] = \dim_K(L)$$

### Teorema (Lemma della Torre)

Siano  $K \subseteq L \subseteq M$  estensioni finite, allora  $K \subseteq M$  è un'estensione finita e

$$[M : K] = [M : L] \cdot [L : K]$$

### Dimostrazione:

Siano  $[L : K] = r$  e  $[M : L] = s$ , allora abbiamo che

$$\{\ell_1, \dots, \ell_r\} \text{ è una base di } L \text{ su } K \quad \{m_1, \dots, m_s\} \text{ è una base di } M \text{ su } L$$

L'obiettivo è mostrare che  $l_i m_j$  con  $i \in \{1, \dots, r\}$  e  $j \in \{1, \dots, s\}$  è una base di  $M$  su  $K$

*Mostriamo Prima che Generano*

Sia  $\alpha \in M$ , allora  $\exists x_1, \dots, x_s \in L : \alpha = x_1m_1 + \dots + x_sm_s$ . Ogni  $x_h \in L$  è combinazione lineare degli  $\ell_i$  con coefficienti in  $K$ , quindi  $\exists y_{h,k} \in K : x_h = y_{h,1}\ell_1 + \dots + y_{h,r}\ell_r$ . Andando poi a sostituire otteniamo che:

$$\alpha = x_1m_1 + \dots + x_sm_s = \left( \sum_k y_{1,k}\ell_k \right) m_1 + \dots + \left( \sum_k y_{s,k}\ell_k \right) m_s = \sum_{h,k} y_{h,k}\ell_k m_h$$

Da cui otteniamo che  $\alpha$  è combinazione lineare degli  $\ell_k m_h$  con coefficienti in  $K$

*Mostriamo ora che  $\ell_k m_h$  sono linearmente indipendenti*

Sia quindi

$$\sum_{h,k} z_{h,k}\ell_k m_h = 0 \quad \text{con } z_{h,k} \in K$$

Dobbiamo mostrare che  $z_{h,k} = 0, \forall h, k$ . L'uguaglianza precedente possiamo scriverla come:

$$\sum_h \underbrace{\sum_k z_{h,k}\ell_k m_h}_{\in L} = 0$$

Siccome gli  $m_h$  sono linearmente indipendenti su  $L$ , allora abbiamo che

$$\sum_k z_{h,k}\ell_k = 0 \quad \forall h$$

Ma gli  $\ell_k$  sono linearmente indipendenti su  $K$ , allora

$$z_{h,k} = 0 \quad \forall h, k$$

□

### Esempio di Estensioni Finite

*Sia  $L$  un campo con  $3^{12}$  elementi, può esistere un sottocampo di  $L$  con  $3^8$  elementi?*

La risposta è no, perché in tal caso contraddirrebbe il Lemma della Torre

Dal numero degli elementi, possiamo dedurre facilmente che  $\text{Char}(L) = 3$ , quindi  $\mathbb{Z}/3 \subseteq L$ , in particolare:

$$[L : \mathbb{Z}/3] = 12$$

Se esistesse un campo  $K$  con  $3^8$  elementi contenuto in  $L$  e contenente  $\mathbb{Z}/3$ , allora avremmo che:

$$[K : \mathbb{Z}/3] = 8$$

Tuttavia il lemma della torre ci dice che

$$\underbrace{[L : \mathbb{Z}/3]}_{=12} = \underbrace{[L : K]}_{\in \mathbb{Z}} \cdot \underbrace{[K : \mathbb{Z}/3]}_8$$

Ma la cosa è assurda perché  $8 \nmid 12$

**Osservazione:** In generale  $K \subseteq L \subseteq M \Rightarrow [L : K] \mid [M : K]$

Se  $[L : \mathbb{Z}/3] = n$ , allora abbiamo che esiste una base  $\mathcal{B} = \{\ell_1, \dots, \ell_n\}$  tale che ogni elemento  $\alpha \in L$  si scriva in modo unico come:

$$\alpha = x_1\ell_1 + \dots + x_n\ell_n$$

con  $x_i \in \mathbb{Z}/3$ . Quindi  $L$  ha  $3 \cdot 3 \cdots 3^n$  volte, quindi ha  $3^n$  elementi

Nell'esempio precedente  $n = 12$

*Ora come ora possiamo solo dimostrare che due estensioni finite sono isomorfi come Spazi Vettoriali*

*Vedremo poi in futuro che su campi finiti saranno isomorfi anche come Campi*

Sia  $K \subseteq L$  e siano  $\alpha, \beta \in L$  algebrici su  $K$ . Sappiamo che  $[K[\alpha] : K]$  è finito.

*Cosa sappiamo di  $[K[\alpha][\beta] : K]$ ?, è  $\beta$  è ancora algebrico su  $K[\alpha]$*

Si perché  $K \subseteq K[\alpha] \Rightarrow [K[\alpha][\beta] : K[\alpha]]$  è ancora finito, quindi per il lemma della torre abbiamo che  $[K[\alpha][\beta] : K]$  è ancora finito.

Inoltre poiché  $\alpha, \beta \in K[\alpha][\beta]$  abbiamo che:

$$\alpha + \beta, \alpha - \beta, \alpha \cdot \beta \in K[\alpha][\beta] \quad \text{Sono ancora algebrici}$$

D'altra parte, *per quanto visto prima*, abbiamo che anche  $\alpha^{-1}$  è algebrico su  $K[\alpha]$

### Corollario

Sia  $K \subseteq L$  un'estensione finita, allora gli elementi algebrici di  $L$  su  $K$  formano un campo

**Osservazione:** Esistono numeri reali non algebrici, detti **trascendenti**, ne sono esempi  $e$  e  $\pi$

### Proposizione

Siano  $K \subseteq L$  algebrica e  $L \subseteq M$  algebrica, allora  $K \subseteq M$  è algebrica

**Dimostrazione:**

Sia  $\alpha \in M$ , allora  $\alpha$  è una radice di un polinomio in  $L[x]$ , allora:

$$\exists \ell_0, \ell_1, \dots, \ell_n \in L : \ell_0 + \ell_1\alpha + \dots + \ell_n\alpha^n = 0$$

Ogni  $\ell_i$  è radice di un polinomio a coefficienti in  $K$

Abbiamo però che  $K[\ell_0]$  è un'estensione finita di  $K$  (in quanto  $\ell_0$  è algebrico su  $K$ )

Usando il lemma della torre abbiamo che  $F = K[\ell_0][\ell_1] \dots [\ell_n]$  è ancora un'estensione algebrica di  $K$

Per costruzione abbiamo che  $\alpha$  è algebrico su  $F$ , quindi  $[F[\alpha] : F]$  è ancora finito

Sempre per il lemma della torre abbiamo che  $[F[\alpha] : F]$  è ancora finito, quindi  $\alpha$  è algebrico

□

**Notazione:** Possiamo indicare  $K[\alpha, \beta] = K[\alpha][\beta]$

Se  $\alpha \in L$ , con  $K \subseteq L$ , non è algebrico su  $K$ , allora abbiamo che

$$[K[\alpha] : K] = \infty$$

In realtà sappiamo dire di più, infatti:

$$K[\alpha] \simeq K[x]$$

Infatti se consideriamo la valutazione in  $\alpha$ ,

$$v_\alpha : K[x] \rightarrow K[\alpha]$$

Questo è un omomorfismo, *per come abbiamo definito*  $v_\alpha$ , suriettivo per la definizione che abbiamo dato di  $K[\alpha]$ , ma è anche iniettivo perché  $\text{Ker}(v_\alpha) = \{0\}$ , in quanto  $\alpha$  non è algebrico.

# Costruzioni con Riga e Compasso

Per questo capitolo, ci saranno due dimostrazioni per lemma/teorema/proposizione, una grafica e una scritta  
Prima di cominciare con l'argomento, diamo questo lemma

## Lemma

Sia  $K \subseteq L$  campi con  $[L : K] = 2$  e  $\text{Char}(K) \neq 2$ . Allora esiste  $d \in K$  e  $\alpha \in L \setminus K$  tale che:

$$L = K[\alpha] \quad \text{e} \quad \alpha^2 = d$$

## Dimostrazione:

Sia  $\beta \in L$  tale che  $\beta \notin K$ . Allora per il lemma della torre  $K[\beta] = L$ , quindi  $\beta$  è radice di un polinomio irriducibile in  $K[x]$  di grado 2:

$$f = x^2 + bx + c \quad \Rightarrow \quad \beta = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$$

Questo è il motivo per cui si richiede  $\text{Char}(K) \neq 2$ . In questo modo otteniamo che:

$$2\beta + b = \pm \sqrt{b^2 - 4c} \quad \Rightarrow \quad \alpha = 2\beta + b \quad \text{e} \quad d = b^2 - 4c$$

È quindi chiaro che  $K[\alpha] = K[\beta]$  e che  $\alpha^2 = b^2 - 4c$

□

Ora siamo pronti per iniziare la teoria delle Costruzioni con Riga e Compasso.

## Definizione di $S$ -Linea

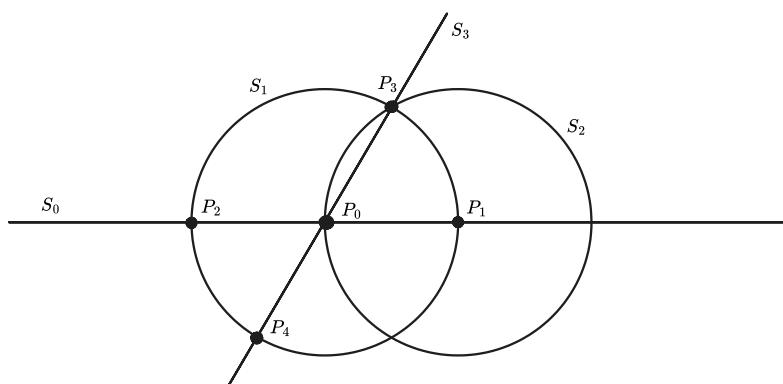
Sia  $S$  l'insieme dei punti nel piano. Si definisce una  $S$ -Linea:

1. Una retta che passa per due punti di  $S$
2. Una circonferenza con centro in  $s$  e passante per un punto di  $S$

## Definizione di Costruzione con Riga e Compasso

Dati due punti distinti  $P_0$  e  $P_1$  nel piano, una Costruzione con Riga e Compasso è una serie di punti  $(P_0, P_1, \dots, P_n)$  tali che per ogni  $i$ , il punto  $P_i$  è nell'intersezione tra due  $S_{i-1}$  linee distinte, dove  $S_{i-1}$  è una linea tra  $P_0, P_1, \dots, P_{i-1}$

Primo Esempio di Costruzione con Riga e Compasso



## Definizione di Numero Costruibile

Assumiamo la distanza tra  $P_0$  e  $P_1$  unitaria. Allora un numero  $\alpha \in \mathbb{R}$  è Costruibile (con Riga e Compasso) se riusciamo a costruire due punti con distanza  $|\alpha|$

## Proposizione

Le seguenti operazioni sono lecite in una costruzione:

1. Tracciare una retta perpendicolare ad una retta data passante per un punto
2. Tracciare una retta parallela ad una retta passante per un punto
3. Dato un segmento  $AB$  e un punto  $P$ , è possibile traslare  $AB$  in modo che abbiano un estremo in  $P$

### Dimostrazione di 1. a Parole

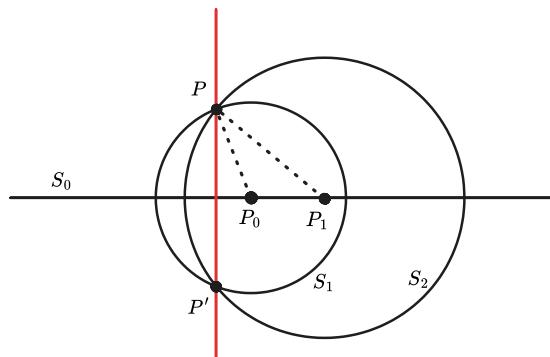
Affinché sia presente la retta, devono necessariamente essere due punti  $P_0$  e  $P_1$  che generano tale retta  $S_0$ .

Tracciamo poi le circonferenze  $S_1$  e  $S_2$  centrate in  $P_0$  e in  $P_1$  passanti per il punto  $P$

Queste due circonferenze andranno poi ad identificare un altro punto  $P'$ .

Tracciando la retta  $S_3$  passante per  $P$  e  $P'$  otteniamo la retta voluta

### Dimostrazione Grafica di 1.



### Dimostrazione di 2:

Basta applicare due volte il punto 1

### Dimostrazione di 3. a Parole

Come prima cosa, possiamo tracciare la  $S_0$  linea come prolungamento di  $AB$ .

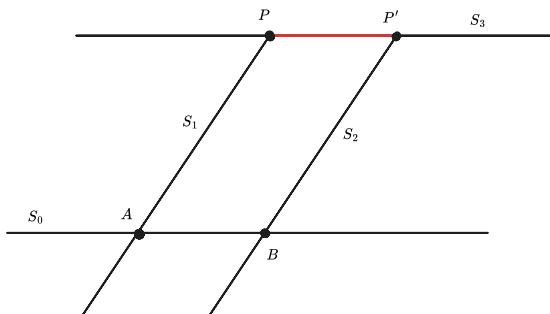
Possiamo poi tracciare la  $S_1$ -Linea  $S_1$ , la retta che congiunge  $A$  e  $P$

Per il punto 2, possiamo tracciare la parallela della retta  $S_1$  passante per  $B$ , retta che chiameremo  $S_2$

Sempre per il punto 2, possiamo tracciare la retta  $S_3$ , parallela a  $S_0$  passante per il punto  $P$  e possiamo andare a chiamare l'intersezione di  $S_2$  e  $S_3$  come  $P'$ .

Il segmento  $PP'$  è il segmento voluto

### Dimostrazione Grafica di 3.



□

## Teorema

I numeri costruibili formano un campo  $F$ . Inoltre  $\forall \alpha \in F, \alpha > 0$  allora vale che  $\sqrt{\alpha} \in F$

**Dimostrazione:**

Mostriamo prima che  $F$  è un campo, supponiamo di avere  $\alpha, \beta \in F$  mostriamo che  $\alpha \pm \beta \in F$

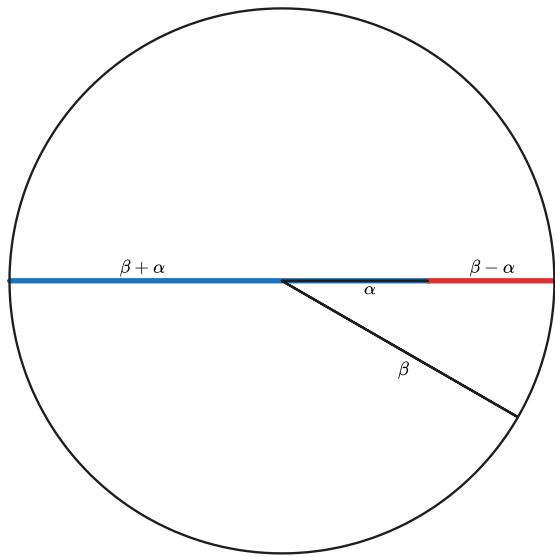
**A Parole**

Dai Teoremi/Lemmi precedenti sappiamo che se  $\alpha$  e  $\beta$  stanno in  $F$ , allora ci sono dei segmenti di tale lunghezza e per il punto 3 del lemma precedente, possiamo supporre che abbiano un vertice in comune. Senza perdere di generalità, possiamo supporre che  $\beta > \alpha$ .

Tracciamo la circonferenza  $S_1$  che punta nel vertice in comune e che ha raggio  $\beta$ .

Prolunghiamo poi il segmento passante per  $\alpha$  in modo da avere un diametro della circonferenza passante per  $\alpha$ .

In questo modo otteniamo due segmenti, uno più lungo dell'altro aventi come estremi un punto della circonferenza e l'altro estremo di  $\beta$ , rispettivamente  $\alpha + \beta$  e  $\alpha - \beta$

**Graficamente**

Mostriamo adesso che se  $\alpha, \beta \in F$ , allora  $\alpha\beta \in F$  e  $\alpha^{-1} \in F$

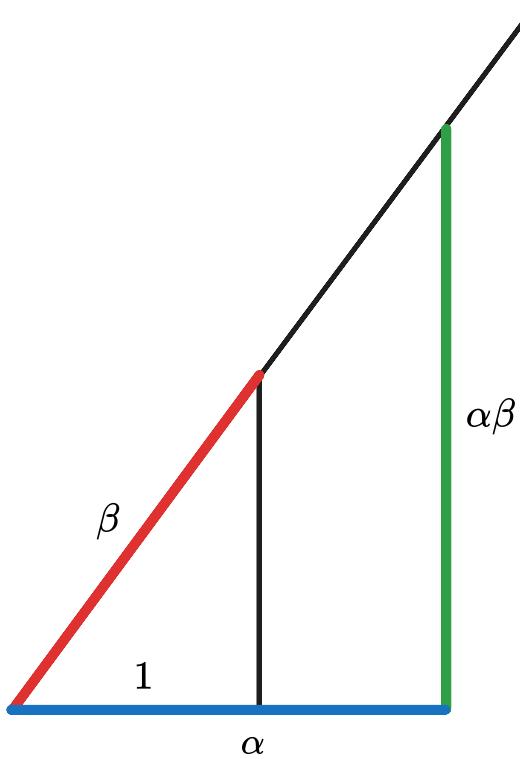
**A Parole**

Numericamente parlando sappiamo che:

$$\frac{\alpha\beta}{\alpha} = \frac{\beta}{1}$$

Se abbiamo questi due numeri, allora sicuramente da qualche parte esiste un segmento lungo  $\beta$  e uno lungo  $\alpha$ .

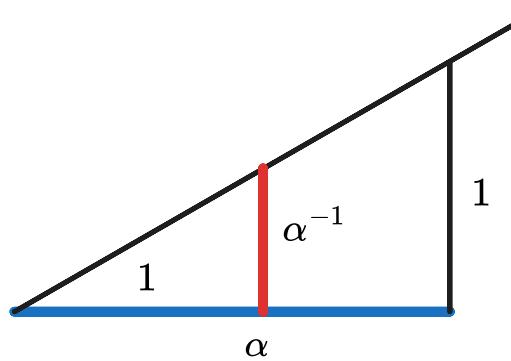
Mettiamoli come rappresentati in figura a destra, cioè con la proiezione di  $\beta$  sulla retta passante per  $\alpha$  di lunghezza unitaria. Prolunghiamo ora la retta passante per  $\beta$  e tracciamo la perpendicolare ad  $\alpha$  passante per l'estremo di  $\alpha$  non in comune con  $\beta$ , il nuovo segmento così ottenuto è lungo  $\alpha\beta$

**Graficamente**

### A Parole

Possiamo sfruttare lo stesso ragionamento di prima, solo ponendo  $\alpha\beta = 1$

### Graficamente



Mostriamo adesso che se  $\alpha \in F$  allora anche  $\alpha^{-1} \in F$

### A Parole

Se  $\alpha \in F$ , allora sicuramente esisterà un segmento lungo  $\alpha$  nel piano. Possiamo allungare tale segmento di 1 in modo da ottenere un segmento lungo  $\alpha + 1$ . Possiamo poi tracciare l'asse di tale segmento (tracciamo due circonferenze  $S_0$  e  $S_1$  in modo da ottenere due punti  $P_0$  e  $P_1$  per poi tracciare la retta  $S_2$  passante per tali punti)

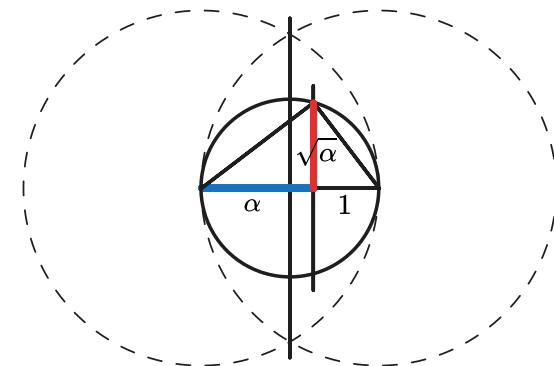
In questo modo andiamo ad individuare il punto  $P_2$ , punto medio del segmento lungo  $\alpha + 1$ .

Da  $P_2$  tracciamo la circonferenza  $S_3$  passante per gli estremi di tale segmento e tracciamo poi la retta perpendicolare allo stesso segmento passante per l'altro estremo di  $\alpha$ . In questo modo andiamo a trovare il punto  $P_3$ .

Andiamo poi a congiungere il punto  $P_3$  con gli estremi del segmento lungo  $\alpha + 1$ , in questo modo andiamo ad ottenere un triangolo rettangolo (è un triangolo inscritto in una circonferenza e con un lato coincidente con il diametro della circonferenza).

Allora vale il secondo teorema di Euclide e il segmento  $P_2P_3$  è lungo  $\sqrt{\alpha}$

### Graficamente



**Osservazione:**  $\mathbb{Q} \subseteq F$  in quanto  $F$  è un campo.

Ma allora anche  $\mathbb{Q}[\sqrt{2}] \subseteq F$  in quanto  $\sqrt{2}$  è un numero costruibile per il teorema precedente e  $\mathbb{Q} \subseteq F$

Allo stesso modo anche  $(\mathbb{Q}[\sqrt{2})[\sqrt{\sqrt{2}+1}] \subseteq F$

Introduciamo ora un sistema di riferimento ortogonale nel piano in modo da avere  $P_0 = (0, 0)$  e  $P_1 = (1, 0)$

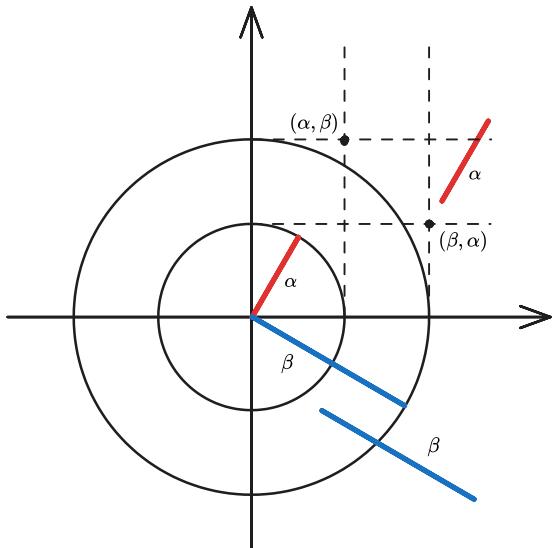
□

**Osservazione:** Il punto  $P = (\alpha, \beta)$  è costruibile se e solo se lo sono sia  $\alpha$  che  $\beta$ . Infatti:

### A Parole

Dimostriamo l'implicazione da destra a sinistra.  
 Se  $\alpha$  e  $\beta$  sono costruibili, allora abbiamo che esistono da qualche parte nel piano dei segmenti lunghi  $\alpha$  e  $\beta$ . Possiamo immaginare di traslarli in modo che abbiano un vertice nell'origine.  
 A questo punto possiamo tracciare delle circonferenze, puntando nell'origine e con raggio  $\alpha$  e  $\beta$ . Tracciamo poi le ortogonali passando per le intersezioni delle ascisse e delle ordinate e troviamo poi i punti  $(\alpha, \beta)$  e  $(\beta, \alpha)$

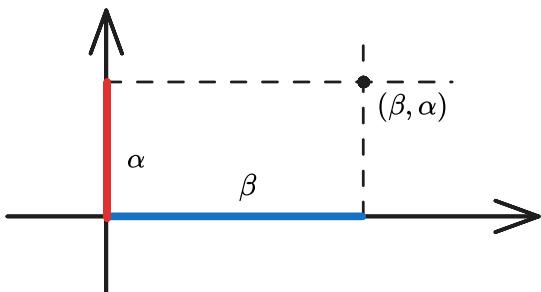
### Graficamente



### A Parole

Per l'altra implicazione, se abbiamo un punto di coordinate  $(\alpha, \beta)$ , allora ci basta tracciare le proiezioni e otteniamo dei segmenti lunghi  $\alpha$  e  $\beta$

### Graficamente



### Teorema

Sia  $\alpha \in \mathbb{R}$ .  $\alpha$  è costruibile se e solo se esiste una catena di sottocampi di  $\mathbb{R}$ :

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \dots \subseteq K_r \subseteq \mathbb{R} \quad : \quad [K_i : K_{i-1}] = 2 \quad \forall i \geq 1 \quad \alpha \in K_r$$

### Dimostrazione:

$\Leftarrow$ ) Supponiamo che esista questa catena:

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \dots \subseteq K_r$$

Supponiamo poi che goda della proprietà sopra descritta.

Allora, poiché  $[K_1 : K_0] = 2$ , esiste un elemento  $d_1 \in K_0 : K_1 = K_0[\sqrt{d_1}]$ . Sappiamo però che  $K_0 = \mathbb{Q}$  che è costruibile per ipotesi e, poiché  $d_1 \in \mathbb{Q}$ , allora si ha che anche  $\sqrt{d_1}$  è costruibile, quindi  $K_1$ , che è il più piccolo campo contenente  $\mathbb{Q}$  e  $\sqrt{d_1}$ , è costruibile.

In maniera del tutto analoga:

$$\exists d_2 \in K_1 : K_2 = K_1[\sqrt{d_2}] \quad K_1 \subseteq F \wedge \sqrt{d_2} \in F \Rightarrow K_1[\sqrt{d_2}] = K_2 \subseteq F$$

E così via fino a raggiungere  $K_r$ . Quindi  $K_r$  è costruibile e poiché  $\alpha \in K_r$ ,  $\alpha$  è costruibile-

$\Rightarrow$ ) Sia  $(P_0, P_1, \dots, P_n)$  una costruzione con riga e compasso tale che  $P_n$  abbia una coordinata uguale a  $\alpha$ . Per semplicità sia  $P_i = (\alpha_i, \beta_i)$  e sia  $S_i = \{P_0, P_1, \dots, P_n\}$ . Allora abbiamo che  $P_i$  sta nell'intersezione di due  $S_{i-1}$  linee

Andiamo ora a definire  $K_i = K_{i-1}(\alpha_i, \beta_i)$ , con  $K_0 = \mathbb{Q}$

**Osservazione:** L'equazione cartesiana di una  $S_{i-1}$  linea ha coordinate in  $K_{i-1}$

Infatti la retta che passa per i punti  $P_j$  e  $P_h$  con  $j, h < i$  ha equazione:

$$\frac{y - \beta_j}{\beta_h - \beta_j} = \frac{x - \alpha_j}{\alpha_h - \alpha_j} \quad \Leftrightarrow \quad (y - \beta_j)(\alpha_h - \alpha_j) = (x - \alpha_j)(\beta_h - \beta_j)$$

Similmente, per una circonferenza di centro  $P_j$  e passante per  $P_h$  abbiamo che:

$$(x - \alpha_j)^2 + (y - \beta_j)^2 = (\alpha_h - \alpha_j)^2 + (\beta_h - \beta_j)^2$$

In entrambi i casi hanno coefficienti in  $K_{i-1}$

Andiamo a vedere i vari casi delle varie intersezioni:

*Caso 1 - Retta con Retta:* Se  $P_i$  è intersezione di due  $S_{i-1}$  rette, allora  $\alpha_i, \beta_i$  è soluzione di un sistema lineare di due equazioni a coefficienti in  $K_{i-1}$ :

$$\begin{cases} ax + by = c \\ a'x + b'y = c' \end{cases} \quad a, b, c, a', b', c' \in K_{i-1} \quad \Rightarrow \quad \alpha_i, \beta_i \in K_{i-1}$$

Da cui deduciamo che  $K_i = K_{i-1}$

*Caso 2 - Retta con Circonferenza:* Se  $P_i$  è intersezione tra una retta e una circonferenza, allora abbiamo che  $(\alpha_i, \beta_i)$  è soluzione di:

$$\begin{cases} ax + by = c \\ x^2 + y^2 + a'x + b'y = c \end{cases} \quad a, b, c, a', b', c' \in K_{i-1}$$

Se  $a \neq 0$ , allora abbiamo che  $x = \frac{x - by}{a}$  e sostituendo nella seconda otteniamo un'equazione di secondo grado in  $y$ , quindi  $y$  è radice di un polinomio di secondo grado, ossia:

$$[K_{i-1}[\beta_i] : K_{i-1}] = 1, 2$$

Inoltre abbiamo che  $K_{i-1}[\beta_i] \ni \alpha_i$  per la soluzione di  $x$  che abbiamo trovato, da cui abbiamo che:

$$K_i = K_{i-1}[\beta_i]$$

□

## Alcune Conseguenze di Questo Teorema

- **Quadratura di un Cerchio:** *Dato un cerchio, disegnare un quadrato con la stessa area*

Supponiamo di avere un cerchio di raggio 1, allora sappiamo che l'area di un cerchio è  $\pi$ , quindi se volessimo trovare un quadrato come quello descritto, dovremmo creare un segmento di lato  $\sqrt{\pi}$ . Tuttavia, sapendo che  $\pi$  è trascendente, non può appartenere ad un campo  $K_r$  come quello del teorema, in quanto  $K_r$  è un'estensione finita di  $\mathbb{Q}$  i cui elementi sono tutti algebrici

### Osservazione Cruciale

Se  $\alpha$  è costruibile, allora abbiamo una catena

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \dots \subseteq K_r \ni \alpha$$

Allora per il lemma della torre abbiamo che  $[K_r : \mathbb{Q}] = 2^r$

Sempre per il lemma della torre abbiamo che:

$$[\mathbb{Q}[\alpha] : \mathbb{Q}] \mid [K_r : \mathbb{Q}] = 2^r$$

In particolare, abbiamo che il grado di  $\alpha$  è una potenza di 2

- **Duplicazione del Cubo:** *Sappiamo costruire un cubo di volume 2?*

Se volessimo ottenere un cubo con volume 2, dovremmo trovare il modo di costruire  $\sqrt[3]{2}$ , il suo polinomio minimo però è  $x^3 - 2$  che è di grado 3 e poiché non è una potenza di 2, allora non è possibile

## Campi di Spezzamento

Sia  $f \in K[x]$  con  $\deg(f) = n$ . Poniamoci queste domande:

*Esiste un campo  $L \subseteq K$  in cui  $f$  ha  $n$  radici contate con le loro molteplicità?*

*Esistono tali  $L$  minimali?*

*Se ne esistono diversi, sono isomorfi tra di loro?*

Cominciamo con un esempio:

Esempio di Campo di Spezzamento

Sia  $f = x^3 + 3x + 3 \in \mathbb{Q}[x]$ . Sappiamo che questo polinomio è irriducibile per Eisenstein.

Prendiamo  $\alpha \in \mathbb{R}$  una radice di  $f$  e consideriamo  $\mathbb{Q}[\alpha]$

Per costruzione abbiamo che  $\mathbb{Q}[\alpha]$  contiene una radice per costruzione, ma non sappiamo se le contiene tutte.

Facciamo quindi la divisione di  $f$  per  $(x - \alpha)$  con Ruffini:

$$\begin{array}{c}
 & | & 1 & 0 & 3 & | & 3 \\
 \alpha & | & 0 & \alpha & \alpha^2 & | & 3\alpha + \alpha^3 \\
 \hline
 & | & 1 & \alpha & 3 + \alpha^2 & | & 0
 \end{array}$$

Da cui otteniamo che:

$$f = (x - \alpha)(x^2 + \alpha x + 3 + \alpha^2)$$

*Come possiamo fare per avere anche le altre radici?*

Possiamo utilizzare la solita formula quadratica:

$$\beta_{1,2} = \frac{-\alpha \pm \sqrt{\alpha^2 - 12 - 4\alpha^2}}{2} = \frac{-\alpha \pm \sqrt{-12 - 3\alpha^2}}{2}$$

Se fosse state in  $\mathbb{Q}[\alpha]$ , avremmo avuto tutte le radici, tuttavia abbiamo che  $\sqrt{-12 - 3\alpha^2} \notin \mathbb{Q}[\alpha]$ , anzi, visto che l'argomento nella radice non è positiva, i valori  $\beta_{1,2}$  che otteniamo non sono neanche reali

Quindi possiamo aggiungere

$$\beta = \frac{-\alpha + \sqrt{-12 - 3\alpha^2}}{2} \Rightarrow [\mathbb{Q}[\alpha, \beta] : \mathbb{Q}] = 6$$

Questo per il lemma della torre, in quanto  $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 3$  e  $[\mathbb{Q}[\alpha, \beta] : \mathbb{Q}[\alpha]] = 2$

Inoltre abbiamo che  $\beta_2 = -\alpha - \beta$ , per cui otteniamo che:

$$f = x^3 + 3x + 3 = (x - \alpha)(x - \beta)(x + \alpha + \beta)$$

### Definizione di Campo di Spezzamento

Sia  $f \in K[x]$ . Un campo  $L$  contenente  $K$  si dice campo di spezzamento per  $f$  su  $K$  se:

1.  $\exists \alpha_1, \alpha_2, \dots, \alpha_n \in L, \exists c \in K : f = c(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$
2.  $L = K[\alpha_1, \dots, \alpha_n]$

### Teorema

Sia  $f \in K[x]$ , allora esiste un campo di spezzamento per  $f$  su  $K$

### Dimostrazione:

Procediamo per induzione su  $\deg(f)$

*Base Induttiva:* Se  $\deg(f) = 1$ , allora  $L = K$

*Passo Induttivo:* Se  $\deg(f) > 1$ , allora possiamo prendere un fattore  $\pi$  irriducibile di  $f$ . Poniamo  $K_1$  campo come:

$$K_1 = K[x]/(\pi)$$

Allora abbiamo che  $K_1$  è un'estensione di  $K$  e  $K_1$  contiene una radice di  $f$ .

Tale radice è  $\alpha = [x]$ , che è radice di  $\pi$  in  $K_1$  e quindi anche di  $f$ . Infatti:

$$\tilde{\pi}([x]) = [\pi] = [0]$$

Allora abbiamo che  $K_1 = K[\alpha]$ , quindi in  $K_1[x]$  abbiamo che:

$$f = (x - \alpha)f_1 \quad \text{con } f_1 \in K_1$$

Adesso possiamo usare l'ipotesi induttiva su  $f_1$  rispetto a  $K_1$

Quindi esiste  $L \supseteq K_1$  tale che

$$f_1 = c_1(x - \alpha_2) \cdots (x - \alpha_n) \quad \text{con } \alpha_2, \dots, \alpha_n \in L \text{ e } L = [\alpha_2, \dots, \alpha_n]$$

Abbiamo quindi che:

$$L = [\alpha_2, \dots, \alpha_n] \text{ e } K_1 = K[x] \Rightarrow K = [\alpha][\alpha_2, \dots, \alpha_n] = K[\alpha, \alpha_2, \dots, \alpha_n]$$

Da cui otteniamo che:

$$f = (x - \alpha)f_1 = c_1(x - \alpha)(x - \alpha_2) \cdots (x - \alpha_n)$$

In realtà possiamo anche dire che  $c_1 \in K$  in quanto  $c_1$  è anche il coefficiente direttore di  $f$

□

### Corollario della Dimostrazione

Se  $f \in K[x]$  con  $\deg(f) = n$ , allora esiste un campo di spezzamento  $L$  con grado:

$$[L : K] \leq n!$$

### Dimostrazione:

Nella dimostrazione abbiamo che:

$$[K_1 : K] = \deg(\pi) \leq n$$

Utilizzando l'ipotesi induttiva abbiamo che:

$$[L : K_1] \leq (n - 1)!$$

in quanto abbiamo che  $L$  è un campo di spezzamento di  $g$  su  $K_1$ , quindi per il lemma della torre si ha che:

$$[L : K] = [L : K_1] \cdot [K_1 : K] \leq (n - 1)! \cdot n = n!$$

□

### Teorema

Siano  $K, K'$  due campi e sia:

$$\phi : K \rightarrow K'$$

un isomorfismo di campi, sia poi:

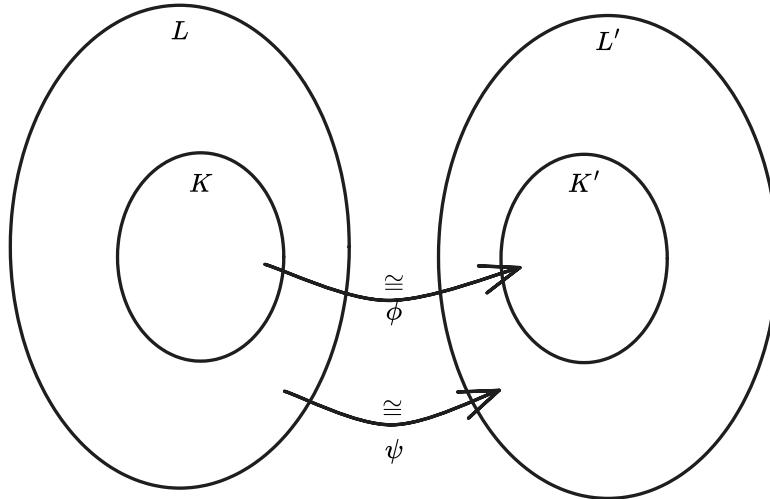
$$\varphi : K[x] \rightarrow K'[x]$$

l'estensione all'anello dei polinomi di  $\phi$ . Sia quindi  $f \in K[x]$  e sia  $f' = \varphi(f)$  e siano  $L, L'$  campi di spezzamento di  $f$  e  $f'$  su  $K$  e  $K'$  rispettivamente. Allora esiste:

$$\psi : L \rightarrow L'$$

isomorfismo che estende  $\phi$

## Rappresentazione Grafica



### Dimostrazione:

Procediamo per induzione su  $\min([L : K], [L' : K'])$ , che senza perdere di generalità possiamo supporre essere  $[L : K]$

*Caso Base:* Assumiamo che  $[L : K] = 1$ , allora abbiamo che  $L = K$ , dobbiamo quindi mostrare che  $L' = K'$

Quindi le radici  $\alpha_1, \dots, \alpha_n$  di  $f$  stanno tutte in  $K$ , quindi:

$$f' = \varphi(f) = \varphi(c(x - \alpha_1) \cdots (x - \alpha_n)) = \varphi(c)(x - \varphi(\alpha_1)) \cdots (x - \varphi(\alpha_n))$$

Quindi tutte le radici di  $f'$  stanno in  $K'$  e quindi  $L' = K'$

*Caso Induttivo:* Supponiamo di avere  $[L : K] > 1$ , allora esiste una radice  $\alpha \in L$  che non sta in  $K$

Il polinomio minimo di  $\alpha$  è il fattore irriducibile  $\pi$  di  $f$  (*se f sera irriducibile in partenza, allora  $\pi = f$* )

Consideriamo quindi una radice  $\alpha'$  di  $\pi' = \varphi(\pi)$ , che a sua volta è un fattore irriducibile di  $f'$

Da una parte abbiamo che  $K[\alpha] \subseteq L$ , dall'altra parte abbiamo che:  $K'[\alpha'] \subseteq L'$  e abbiamo che:

$$\begin{array}{ccc} K[\alpha] & \xrightarrow{\cong} & K'[\alpha'] \\ \cap | & \phi_1 & \cap | \\ L & & L' \end{array}$$

Dove abbiamo che  $\phi_1|_K = \phi$  e  $\phi_1(\alpha) = \alpha'$

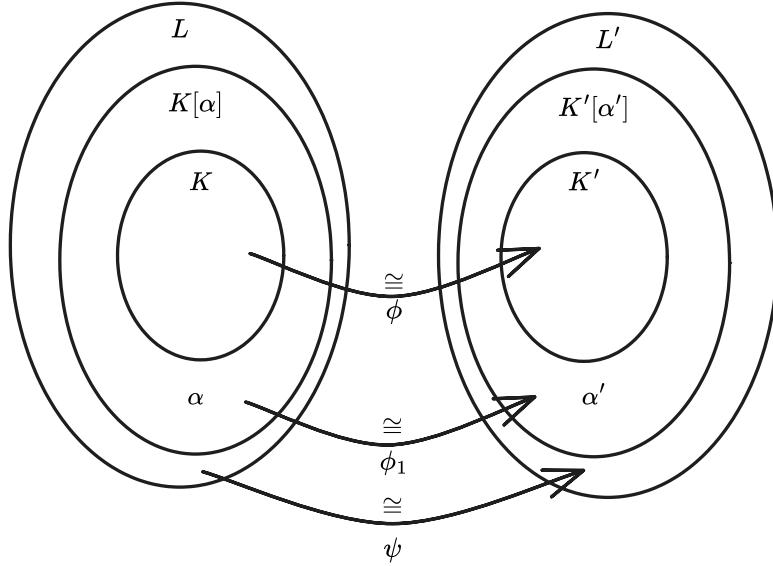
A questo punto possiamo usare l'ipotesi induttiva.

$L$  è un campo di spezzamento di  $f$  su  $K[\alpha]$  e  $L'$  è campo di spezzamento di  $f'$  su  $K'[\alpha']$

Per Ipotesi Induttiva abbiamo che esiste un isomorfismo  $\psi : L \rightarrow L'$  che estende  $\phi_1$  e quindi anche  $\phi$

□

## Rappresentazione Grafica



### Corollario

Sia  $f \in K[x]$ ,  $L, L'$  campi di spezzamento di  $f$  su  $K$ , allora esiste un isomorfismo:

$$\psi : L \rightarrow L' \quad \text{tale che} \quad \psi|_K = id_K$$

### Dimostrazione:

Questo è un caso particolare del teorema precedente, con  $K = K'$  e  $\psi = id_K$

□

L'obiettivo di adesso è classificare i campi finiti, quali sono e quanti sono

Sappiamo che se  $K$  è un campo finito, allora:

1.  $Char(K) = p$  con  $p$  numero primo
2. Il sottocampo fondamentale è  $\mathbb{Z}/p$
3.  $K$  è uno  $\mathbb{Z}/p$ -spazio vettoriale di dimensione finita  $n$
4.  $|K| = p^n$

*Mostreremo in particolare che per ogni  $p$  primo e per ogni  $n > 0$  esiste un unico campo con  $p^n$  elementi (a meno di isomorfismi)*

Vediamo prima un caso particolare dell'unicità

#### Caso Particolare dell'Unicità

Siano  $d$  e  $d'$  due elementi in  $\mathbb{Z}/p$  non quadrati, allora

$$\mathbb{Z}/p[\sqrt{d}] \text{ e } \mathbb{Z}/p[\sqrt{d'}] \text{ hanno entrambi } p^2 \text{ elementi}$$

Vediamo ora che sono isomorfi:

Sappiamo che  $\frac{d}{d'}$  è un quadrato in  $\mathbb{Z}/p$  in quanto il prodotto (o rapporto) di due non quadrati in un campo finito è un quadrato, quindi:

$$\exists c \in \mathbb{Z}/p : \frac{d}{d'} = c^2$$

Sapendo questa cosa possiamo definire l'applicazione:

$$\varphi : \mathbb{Z}/p[\sqrt{d}] \rightarrow \mathbb{Z}/p[\sqrt{d'}] \quad \varphi(a + b\sqrt{d}) = \varphi(a) + \varphi(b)\varphi(\sqrt{d}) = a + b\varphi(\sqrt{d}) = a + b(c \cdot \sqrt{d'})$$

Infatti:

$$c \cdot \sqrt{d'} = \sqrt{\frac{d}{d'}} \sqrt{d'} = \sqrt{d}$$

Questo non solo è un omonomorfismo, ma è anche un isomorfismo. Le verifiche sono banali

**Osservazione:** Questo fatto con  $\mathbb{Q}$  al posto di  $\mathbb{Z}/p$  non è quasi mai vera, infatti:

$$\mathbb{Q}[\sqrt{2}] \not\cong \mathbb{Q}[\sqrt{3}] \text{ come campi}$$

### Teorema Fondamentale per i Campi Finiti

Per ogni primo  $p$ , per ogni  $n > 0$ , esiste un unico, a meno di isomorfismi campo con  $p^n$  elementi

**Dimostrazione:**

Dimostriamo prima l'unicità poi l'effettiva esistenza:

*Unicità:* Sappiamo che se  $|L| = p$ , allora  $\text{Char}(L) = p$  e  $\mathbb{Z}/p \subseteq L$ , in quanto la cardinalità è una potenza della caratteristica di un campo. Consideriamo il polinomio  $f = x^{p^n} - x \in \mathbb{Z}/p[x]$

Sia poi  $\alpha \in L$ . Se  $\alpha = 0$ , allora abbiamo che  $\alpha$  è radice di  $f$ , in quanto:

$$\tilde{f}(\alpha) = \tilde{f}(0) = 0^{p^n} - 0 = 0$$

Se  $\alpha \neq 0$ , allora  $\alpha \in L^*$  ma  $|L^*| = p^n - 1$  ed essendo  $L^*$  un gruppo ciclico moltiplicativo abbiamo che  $\alpha^{p^n} = 1$ , da cui segue che  $\alpha$  è radice di  $f$ :

$$\tilde{f}(\alpha) = \alpha^{p^n} - \alpha = \alpha^{p^n-1} \cdot \alpha - \alpha = \alpha - \alpha = 0$$

Quindi tutti gli elementi di  $L$  sono radici di  $f$ , quindi  $L$  è un campo di spezzamento di  $f$  su  $\mathbb{Z}/p$

*Infatti, se  $L = \{\alpha_1, \dots, \alpha_n\}$  sono le radici di  $f$ , allora*

$$f = (x - \alpha_1) \cdots (x - \alpha_n) \quad \Rightarrow \quad L = K[\alpha_1, \dots, \alpha_n]$$

*Esistenza:* Sia  $L$  il campo di spezzamento di  $f = x^{p^n} - x \in \mathbb{Z}/p[x]$

Quante sono le radici di  $f$  in  $L$ ?

Sappiamo che sono  $p^n$  contate con le loro molteplicità, ma sappiamo dire di più?

Se andiamo a calcolare la derivata di  $f$  otteniamo che  $f' = p^n x^{p^n-1} - 1 \in \mathbb{Z}/p[x] \Rightarrow f' = -1$

Abbiamo però anche che  $\mathcal{MCD}(f, f') = 1$ , quindi abbiamo la certezza che le radici sono  $p^n$  tutte distinte, cioè non c'è una radice con molteplicità maggiore di 1

Andiamo a considerare  $S \subseteq L$  l'insieme delle radici di  $f$  e sappiamo che:

$$|S| = p^n$$

Non ci resta che da dimostrare che  $S$  è un campo

Sappiamo che  $0 \in S$  in quanto abbiamo che

$$\tilde{f}(0) = 0$$

Analogamente abbiamo che  $1 \in S$  in quanto

$$\tilde{f}(1) = 1 - 1 = 0$$

Siano  $\alpha, \beta \in S$ , allora abbiamo che  $\alpha^{p^n} = \alpha$  e  $\beta^{p^n} = \beta$

*Basta sostituire calcolare  $\tilde{f}(\alpha)$  e porlo uguale a zero, poi l'uguaglianza segue portando dall'altra parte  $\alpha$*

È vero che differenza, prodotto e inverso stanno in  $S$ ?

$$(\alpha - \beta)^{p^n} = \alpha^{p^n} - \beta^{p^n} = \alpha - \beta$$

*Notiamo che se  $p = 2$  allora non ha differenza fare + o -, se è dispari allora il segno si preserva e  $(-\beta)^{p^n} = -\beta^{p^n} = -\beta$*

Quindi  $\alpha - \beta$  sta in  $S$

$$(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta \in S \quad (\alpha^{-1})^{p^n} = (\alpha^{p^n})^{-1} = \alpha^{-1} \in S$$

Quindi  $S$  è un campo e in particolare  $S = L$  con  $p^n$

□

**Notazione:** Se  $q = p^n$  allora "il" campo con  $q$  elementi si indica con

$$\mathbb{F}_q \Rightarrow \mathbb{F}_p = \mathbb{Z}/p$$

**Attenzione:** Non c'è un modello standard per questi campi

### Corollario

Siano  $f, g \in \mathbb{Z}/p[x]$  irriducibili di grado  $n$ , allora:

$$\mathbb{Z}/p[x]/(f) \cong \mathbb{Z}/p[x]/(g) \cong \mathbb{F}_{p^n}$$

### Dimostrazione:

Entrambi sono campi di grado  $n$  di  $\mathbb{Z}/p$  e quindi hanno entrambi  $p^n$  elementi

□

Per costruire quindi un campo con  $3^4$  elementi mi basta trovare un polinomio  $f \in \mathbb{Z}/3[x]$  irriducibile di grado 4 e fare il quoziente

$$\mathbb{Z}/3[x]/(f)$$

Torniamo ad un esercizio dei fogli passati, cioè:

$$x^{p^d-1} - x \mid x^{p^n-1} - x \quad \Leftrightarrow \quad d \mid n$$

Vediamo  $\Leftarrow$ ): Deriva dal fatto che se  $d \mid n$ , allora  $n = dk$  da cui:

$$a^n - 1 = (a^d - 1)(1 + a^d + a^{2d} + \cdots + a^{(k-1)d})$$

In particolare avremmo che:

$$p^d - 1 \mid p^n - 1 \quad \Leftrightarrow \quad x^{p^d-1} - 1 \mid x^{p^n-1} - 1 \quad \Leftrightarrow \quad x^{p^d} - x \mid x^{p^n} - x$$

### Corollario

Sia  $d < n$ , allora  $\mathbb{F}_{p^n}$  contiene un sottocampo con  $p^d$  elementi se e solo se  $d \mid n$ .

Inoltre, se  $d \mid n$  esiste un sottocampo con  $p^d$  elementi

### Dimostrazione:

Supponiamo che:

$$\mathbb{Z}/p \subseteq \mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$$

Per il lemma della Torre abbiamo che:

$$\underbrace{[\mathbb{F}_{p^n} : \mathbb{Z}/p]}_n = \underbrace{[\mathbb{F}_{p^d} : \mathbb{Z}/p]}_d \cdot \underbrace{[\mathbb{F}_{p^n} : \mathbb{F}_{p^d}]}_{\in \mathbb{Z}} \Rightarrow d \mid n$$

Sia ora  $d \mid n$  e mostriamo che esiste un unico sottocampo con  $p^d$  elementi

Sappiamo che gli elementi di  $\mathbb{F}_{p^n}$  sono le radici di  $x^{p^n} - x$  ma sappiamo che

$$x^{p^d} - x \mid x^{p^n} - x$$

Quindi le  $p^d$  radici di  $x^{p^d} - x$  fanno parte di un campo con  $p^d$  elementi.

Inoltre è unico perché se avessimo avuto due campi con  $p^d$  elementi, avremmo avuto più di  $p^d$  radici (che sarebbero tutti gli elementi di questi altri sottocampi) del polinomio  $x^{p^d} - x$

□

Esempio sui Campi Fondamentali dei Campi finiti

Prendiamo per esempio  $n = 12$  allora avremmo:

$$\begin{array}{ccccc}
 & & \mathbb{F}_{p^{12}} & & \\
 & \swarrow & & \searrow & \\
 \mathbb{F}_{p^6} & & & & \mathbb{F}_{p^4} \\
 \downarrow & \searrow & & \swarrow & \\
 \mathbb{F}_{p^3} & & \mathbb{F}_{p^2} & & \\
 \downarrow & & \downarrow & & \\
 \mathbb{F}_p = \mathbb{Z}/p & & & &
 \end{array}$$

### Corollario

$f = x^{p^n} - x \in \mathbb{Z}/p[x]$  è il prodotto di tutti i polinomi irriducibili monici di grado divisori di  $n$ , tutti con molteplicità 1

### Dimostrazione:

Dimostriamolo in tre momenti diversi.

*Mostriamo che i divisori irriducibili hanno molteplicità 1*

Se avesse un fattore irriducibile con molteplicità maggiore di 1, allora avremmo che avrebbe radici multiple, il che è assurdo in quanto, per prima, avevamo che in  $\mathbb{Z}/p[x]$ , si ha

$$\mathcal{MCD}(f, f') = 1$$

*Mostriamo che se  $\pi \mid f$  irriducibile, allora  $\deg(\pi) \mid n$*

Sia  $\alpha \in \mathbb{F}_{p^n}$  radice di  $\pi$ , allora  $\mathbb{Z}/p[x]$  è sottocampo di  $\mathbb{F}_{p^n}$ . È anche vero però che è estensione di  $\mathbb{Z}/p[x]$ :

$$\mathbb{Z}/p \subseteq \mathbb{Z}/p[\alpha] \subseteq \mathbb{F}_{p^n} \quad \Rightarrow \quad [\mathbb{Z}/p[x] : \mathbb{Z}/p] = \deg(\pi)$$

La tesi segue poi dal lemma della torre, in quanto abbiamo che:

$$\mathbb{Z}/p[\alpha] \cong \mathbb{F}_{p^{\deg(\pi)}} \subseteq \mathbb{F}_{p^n}$$

*Mostriamo che se  $\pi \in \mathbb{Z}/p$  irriducibile ha grado d divisore di n, allora  $\pi \mid f$*

Consideriamo il Campo di Spezzamento  $L$  di  $\pi$  su  $\mathbb{Z}/p$ . Sia  $\alpha \in L$  radice di  $\pi$ , allora:

$$\mathbb{Z}/p[\alpha] \cong \mathbb{F}_{p^{\deg(\pi)}} = \mathbb{F}_{p^d}$$

Quindi sicuramente soddisfa (cioè è radice) di  $x^{p^d} - x$ , quindi:

$$\pi \mid x^{p^d} - x \quad \Rightarrow \quad \pi \mid x^{p^n} - x$$

□

**Domanda:** Sia  $K \subseteq L$  estensione finita, esiste  $\gamma \in L$  tale che  $L = K[\gamma]$ ?

Se  $L$  è finito, e di conseguenza anche  $K$  è finito, allora la risposta è semplicemente sì:

Infatti abbiamo che  $L^*$  è un gruppo ciclico, quindi esiste un elemento  $\gamma \in L^*$  tale che:

$$L = \{\gamma, \gamma^2, \dots, \gamma^{|L|-1}\} \quad \Rightarrow \quad L = K[\gamma]$$

In generale la risposta è negativa, in particolare per i campi a caratteristica  $p$ , ad esempio  $\mathbb{Z}/p(x) = Q(\mathbb{Z}/p[x])$

Per comodità per il prossimo teorema, mettiamoci in  $\mathbb{C}$

### Teorema dell'Elemento Primitivo

Siano  $K \subseteq L \subseteq \mathbb{C}$  campi con  $[L : K] < +\infty$ , allora esiste un elemento  $\gamma \in L$  tale che  $L = K[\gamma]$

### Dimostrazione:

$L$  è generato da un numero finito di elementi,  $L = K[\alpha_1, \dots, \alpha_n]$ . Senza perdere di generalità possiamo limitarci al caso  $L = K[\alpha, \beta]$ , in quanto possiamo proseguire in maniera ricorsiva

Siano quindi  $f, g$  i polinomi minimi di  $\alpha$  e di  $\beta$  e siano

$$\alpha = \alpha_1, \dots, \alpha_n \text{ le radici di } f \quad \beta = \beta_1, \dots, \beta_n \text{ le radici di } g$$

Poniamo  $\gamma \in L$  come

$$\gamma = \alpha + c\beta \quad \text{Tale che} \quad \alpha + c\beta \neq \alpha_i + c\beta_j, \forall (i, j) \neq (1, 1)$$

Perché sappiamo che esiste  $c$ ?

Se  $j \neq 1$  allora voglio che:

$$\alpha - \alpha_i \neq c(\beta_j - \beta) \quad \Rightarrow \quad c \neq \frac{\alpha - \alpha_i}{\beta_j - \beta}$$

Quindi esiste.

Se invece  $j = 1$ , allora si ha che:

$$\alpha - c\beta \neq \alpha_i - c\beta \quad \Rightarrow \quad \alpha \neq \alpha_i \quad \Leftrightarrow \quad i \neq 1$$

Inoltre poiché  $K$  è infinito e sto escludendo un numero finito di numeri, posso trovare  $c$

Considero ora  $h(x)$  come

$$h(x) = f(\gamma - cx) \quad \Rightarrow \quad \tilde{h}(\beta) = \tilde{f}(\gamma - c\beta) = \tilde{f}(\alpha) = 0$$

Cioè,  $h$  ha  $\beta$  come radice e abbiamo che  $h \in K[\gamma][x]$

Inoltre, se  $j > 1$ , allora  $\beta_j$  non è radice di  $h$  per costruzione:

$$\tilde{(\beta_j)} = \tilde{f}(\underbrace{\gamma - c\beta_j}_{\neq \alpha})$$

Inoltre abbiamo che:

$$\mathcal{MCD}(h, g) = x - \beta \in K[\gamma][x]$$

In quanto abbiamo che  $h, g \in K[\gamma][x]$ , da cui deduciamo che  $\beta \in K[\gamma]$

Ma per costruzione, allora anche  $\alpha \in K[\gamma]$ , da cui:

$$K[\alpha, \beta] = K[\gamma]$$

□

### Esempio di Applicazione del Teorema dell'Elemento Primitivo

Sia  $L = \mathbb{Q}[\sqrt[3]{3}, i]$  (quindi  $K = \mathbb{Q}$ ) e vogliamo trovare un elemento  $\gamma$  tale che  $L = \mathbb{Q}[\gamma]$

Utilizziamo la dimostrazione del teorema:

Poniamo

$$\alpha = \sqrt[3]{3}$$

Sappiamo che il polinomio minimo di  $\alpha$  è  $f = x^3 - 3$  che è irriducibile per Eisenstein

Siano  $\alpha_2$  e  $\alpha_3$  le altre radici dello stesso polinomio e siano rispettivamente

$$\alpha_2 = \sqrt[3]{3}\omega \quad \text{e} \quad \alpha_3 = \sqrt[3]{3}\omega^2 \quad \text{con } \omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$$

Poniamo poi:

$$\beta = i$$

Abbiamo gratuitamente che il polinomio minimo di  $\beta$  è  $g = x^2 + 1$  e abbiamo che l'altra radice è:

$$\beta_2 = -i$$

Vogliamo quindi trovare una costante  $c \in \mathbb{Q}$  tale che:

$$\sqrt[3]{3} + ci \neq \alpha_i + c\beta_j \quad \text{con } (i, j) \neq (1, 1)$$

Prendiamo per esempio  $i = 2$  e  $j = 2$ , allora abbiamo che:

$$\sqrt[3]{3} + ci \neq \sqrt[3]{3}\omega - ci \quad \Rightarrow \quad 2ci \neq \sqrt[3]{3}(\omega - 1) \quad \Rightarrow \quad c \neq \frac{\sqrt[3]{3}(\omega - 1)}{2i}$$

Non mi aspetto che siano razionali, basta che ottengo un elemento  $c$  che sia diverso da tutti precedenti.

In questo caso posso scegliere  $\gamma = \sqrt[3]{3}i$ , infatti:

$$\gamma = \sqrt[3]{3}i \quad \Rightarrow \quad \gamma^3 = -3i \quad \Rightarrow \quad i \in K[\gamma]$$

Ma se  $i \in K[\gamma]$ , allora abbiamo che:

$$\sqrt[3]{3} = \frac{\gamma}{i} \in K[\gamma] \quad \Rightarrow \quad \mathbb{Q}[\gamma] = \mathbb{Q}[i, \sqrt[3]{3}]$$

*Questo funziona solamente perché  $i$  e  $\sqrt[3]{3}$  hanno gradi diversi*

---

# Teoria di Galois

## Definizioni di $K$ -Isomorfismo e Estensione Normale $L/K$

Sia  $K \subseteq L \subseteq \mathbb{C}$  con  $[L : K] < +\infty$ . Un omomorfismo:

$$\varphi : L \rightarrow \mathbb{C}$$

si dice  $K$ -Isomorfismo se

$$\varphi(c) = c \quad \forall c \in K$$

L'estensione  $L/K$  si dice normale se

$$\forall K\text{-isomorfismo } \sigma : L \rightarrow \mathbb{C} \quad \Rightarrow \quad \sigma(L) = L$$

*Ma perché  $K$  e perché isomorfismo?*

**Osservazione:** Un  $K$ -Isomorfismo è sempre iniettivo perché  $L$  è un campo. Un  $K$ -isomorfismo è quindi un isomorfismo tra  $L$  e  $\sigma(L)$

## Definizione di Gruppo di Galois dell'Estensione

Se l'estensione  $L/K$  è normale, allora i  $K$ -Isomorfismi formano un gruppo  $Gal(L/K)$ , chiamato gruppo di Galois dell'Estensione..

*Quanti sono e come sono fatti?*

**Osservazione:** Sia  $\sigma : L \rightarrow \mathbb{C}$  un  $K$ -isomorfismo e  $\alpha \in L$  e  $f \in K[x]$ , allora

$$f(\sigma(\alpha)) = \sigma(f(\alpha))$$

Infatti:

$$f = \sum c_i x^i \quad c_i \in K \quad \Rightarrow \quad \sigma(\tilde{f}(\alpha)) = \sigma\left(\sum c_i \alpha^i\right) = \sum \sigma(c_i) \sigma(\alpha)^i = \sum c_i \sigma(\alpha)^i = \tilde{f}(\sigma(\alpha))$$

Tutto questo è importante perché:

### Lemma

Sia  $\sigma : L \rightarrow \mathbb{C}$  un  $K$ -Isomorfismo e  $f \in K[x]$  e  $\alpha \in L$  radice di  $f$ . Allora  $\sigma(\alpha)$  è anche una radice di  $f$

**Dimostrazione:**

Per l'osservazione abbiamo che, visto che  $\tilde{f}(\alpha) = 0$  abbiamo che:

$$\tilde{f}(\sigma(\alpha)) = \sigma(\tilde{f}(\alpha)) = \sigma(0) = 0$$

□

Questo lemma ci permette di contare quanti sono i  $K$ -Isomorfismi

### Corollario

Se  $[L : K] = n$ , allora esistono esattamente  $n$   $K$ -Isomorfismi di  $L$

**Dimostrazione:**

Sappiamo che  $\exists \gamma \in L : L = K[\gamma]$ . Allora il polinomio minimo di  $f$  di  $\gamma$  ha grado  $n$  dunque ha esattamente  $n$  radici distinte

che chiamiamo:

$$\gamma = \gamma_1, \gamma_2, \dots, \gamma_n$$

Allora per il lemma se  $\sigma$  è un  $K$ -Isomorfismo, allora  $\sigma(\gamma) = \gamma_i$  per opportuno  $i$ ,  $\sigma$  è univocamente determinato da questa condizione.

Infatti abbiamo che:  $L = K[\gamma]$  e  $\sigma(c) = c$  per ogni  $c \in K$ . Quindi esistono al più  $n$   $K$ -Isomorfismi. Per completare dobbiamo mostrare che questi sono effettivamente  $n$ . Ma questo lo sappiamo già per il teorema fondamentale delle estensioni semplici, cioè:

$$K[\gamma] \cong K[\gamma_i] \quad \forall i$$

□

### Teorema

Un'estensione  $L/K$  è normale se e solo se  $L$  è il campo di spezzamento di un polinomio in  $K[x]$

#### Dimostrazione:

$\Leftarrow$ ) Se  $L$  è un campo di spezzamento di  $f \in K[x]$ , allora

$$L = K[\alpha_1, \dots, \alpha_r] \quad \text{con } \alpha_1, \dots, \alpha_r \text{ radici di } f$$

Per quanto detto prima, se  $\sigma$  è un  $K$ -Isomorfismo, allora  $\sigma$  permuta le radici  $\alpha_1, \dots, \alpha_r$  e quindi lascia invariato  $L$ , cioè  $\sigma(L) = L$

$\Rightarrow$ ) Viceversa, se  $L/K$  è normale, allora sia  $\gamma \in L$  tale che  $L = K[\gamma]$ . Sia  $f$  il polinomio minimo di  $\gamma$  e siano  $\gamma = \gamma_1, \gamma_2, \dots, \gamma_r$  radici di  $f$ , allora i  $K$ -Isomorfismi  $\sigma_i$  soddisfano  $\sigma_i(\gamma) = \gamma_i$  quindi  $\gamma_i \in L$  per normalità.

Allora abbiamo che:

$$L = K[\gamma] = K[\gamma_1, \dots, \gamma_r]$$

Quindi  $L$  è il campo di spezzamento per  $f$

□

## Corrispondenza di Galois

Sia  $L/K$  estensione normale e indichiamo con  $G = Gal(L/K)$ , andiamo ad indicare con:

$$\mathcal{G}(L/K) = \{H : H \leq G\} = \{\text{I sottogruppi di } G\}$$

$$\mathcal{F} = \{F : F \text{ campo}, K \subseteq F \subseteq L\} = \{\text{Campi Intermedi tra } K \text{ e } L\}$$

Consideriamo poi le applicazioni:

$$\begin{aligned} 1 : \mathcal{G}(L/K) &\rightarrow \mathcal{F}(L/K) & \text{Tale che} && H \mapsto L^H = \{\alpha \in L : h(\alpha) = \alpha, \forall h \in H\} \\ 2 : \mathcal{F}(L/K) &\rightarrow \mathcal{G}(L/K) & \text{Tale che} && F \mapsto Gal(L/F) \end{aligned}$$

Sappiamo che  $L/F$  è normale perché ogni  $F$ -Isomorfismo  $\sigma$  soddisfa  $\sigma(L) = L$ . Infatti, poiché ogni  $F$ -Isomorfismo è anche un  $K$ -Isomorfismo si ha che:

$$\sigma(F) = F \quad \text{e} \quad F \supseteq K \quad \Rightarrow \quad \sigma(K) = K$$

### Teorema di Galois

Le due applicazioni 1 e 2 sono appena descritte sono l'una l'inversa dell'altra, cioè:

$$1) L^{Gal(L/F)} = F \quad \text{e} \quad 2) Gal(L/L^H) = H$$

#### Dimostrazione:

Mostriamo prima 1

Nel dimostrare le uguaglianze mostriamo le doppie uguaglianze.

$\supseteq$ ) Per definizione gli elementi di  $F$  sono fissati dagli automorfismi di  $L$  che fissano  $F$ , quindi:

$$L^{Gal(L/F)} \supseteq F$$

$\subseteq$ ) Per dimostrare che è contenuto ci basta dimostrare che:

$$[L : F] \leq [L : L^{Gal(L/F)}]$$

Osserviamo che  $[L : F] = |Gal(L/F)|$  e ogni automorfismo che fissa  $F$  (*ogni elemento di Gal(L/F)*) fissa anche  $L^{Gal(L/F)}$  per definizione. Quindi esistono almeno  $|Gal(L/F)|$  automorfismi che fissano  $L^{Gal(L/F)}$  e quindi il risultato segue.

*Mostriamo 2*

$\supseteq$ ) Siccome gli elementi di  $Gal(L/L^H)$  fissano  $L^H$  per definizione di  $L^H$  abbiamo che

$$Gal(L/L^H) \supseteq H$$

$\subseteq$ ) Ci basta mostrare che:

$$|Gal(L/L^H)| \leq |H|$$

Ma abbiamo anche che  $|Gal(L/L^H)| = [L : K^H]$

Dobbiamo quindi dimostrare che  $[L : L^H] \leq |H|$  per ogni sottogruppo  $H \leq G$

Ma questo è il lemma di Artin, quindi:

### Lemma

$$\forall H \leq G \quad [L : L^H] \leq |H|$$

### Dimostrazione del Lemma:

Sia  $|H| = n$  e siano  $H = \{h_1, \dots, h_n\}$  con  $h_1 = id$

Dobbiamo dimostrare che  $L$  come spazio vettoriale su  $L^H$  ha dimensione minore o uguale di  $n$ , cioè:

$$\dim_{L^H}(L) \leq n$$

Per farlo mostriamo che  $n + 1$  elementi di  $L$  sono sempre linearmente dipendenti

Siano quindi  $\alpha_1, \dots, \alpha_{n+1}$  elementi di  $L$  qualunque e consideriamo il sistema lineare omogeneo di  $n$ -equazioni in  $n + 1$  incognite con coefficienti  $h_i(\alpha_j)$ :

$$\begin{cases} h_1(\alpha_1)x_1 + \dots + h_1(\alpha_{n+1})x_{n+1} = 0 \\ h_2(\alpha_1)x_1 + \dots + h_2(\alpha_{n+1})x_{n+1} = 0 \\ \vdots \\ h_n(\alpha_1)x_1 + \dots + h_n(\alpha_{n+1})x_{n+1} = 0 \end{cases} \Leftrightarrow \begin{cases} \alpha_1x_1 + \dots + \alpha_{n+1}x_{n+1} = 0 \\ h_2(\alpha_1)x_1 + \dots + h_2(\alpha_{n+1})x_{n+1} = 0 \\ \vdots \\ h_n(\alpha_1)x_1 + \dots + h_n(\alpha_{n+1})x_{n+1} = 0 \end{cases}$$

Esiste sicuramente una soluzione non banale  $(\beta_1, \dots, \beta_{n+1})$  con  $\beta_i \in L$

Scegliamo la soluzione che abbia il massimo numero di zero e a meno di permutare le  $\alpha_i$  e a meno di moltiplicare per uno scalare possiamo assumere che  $\beta_1 = 1$

Vogliamo quindi adesso mostrare che  $\beta_i \in L^H$  per ogni  $i$

Infatti, se  $\forall i$  si ha che  $\beta_i \in L^H$  allora la prima equazione del sistema lineare ci da:

$$\alpha_1\beta_1 + \alpha_2\beta_2 + \dots + \alpha_{n+1}\beta_{n+1} = 0$$

Che è una combinazione lineare degli  $\alpha_i$  con coefficienti in  $L^H$  non banale e uguale a 0

Supponiamo per assurdo quindi che esiste  $i$  tale che  $\beta_i \notin L^H$ , e senza perdere di generalità possiamo supporre che  $i = 2$

Quindi esiste  $h \in H$  tale che  $h(\beta_2) \neq \beta_2$

**Osservazione:** Notiamo che  $(h(\beta_1), h(\beta_2), \dots, h(\beta_{n+1}))$  è ancora soluzione del sistema, infatti:

$$h_i(\alpha_1)h(\beta_1) + h_i(\alpha_2)h(\beta_2) + \dots + h_i(\alpha_{n+1})h(\beta_{n+1}) = h(\underbrace{h^{-1}h_i(\alpha_1)\beta_1}_{h_j}) + h(\underbrace{h^{-1}h_i(\alpha_2)\beta_2}_{h_j}) + \dots + h(\underbrace{h^{-1}h_i(\alpha_{n+1})\beta_{n+1}}_{h_j})$$

$$h(h_k(\alpha_1)\beta_1 + h_j(\alpha_2)\beta_2 + \dots + h_j(\alpha_{n+1})\beta_{n+1}) = h_j(0) = 0$$

*L'argomento dentro a  $h_j$  è nullo in quanto era una soluzione del sistema lineare precedente*

Ma allora abbiamo che  $(\beta_1 = 1, \beta_2, \dots, \beta_{n+1})$  e  $(h(\beta_1) = 1, h(\beta_2), \dots, h(\beta_{n+1}))$  sono due soluzioni dello stesso sistema lineare, quindi necessariamente anche la differenza è ancora una soluzione di tale sistema lineare.

Facendo i conti otteniamo che  $(0, \underbrace{\beta_2 - h(\beta_2)}_{\neq 0}, \beta_3 - h(\beta_3), \dots, \beta_{n+1} - h(\beta_{n+1}))$  è ancora una soluzione del sistema lineare.

Qui cade l'assurdo, in quanto otteniamo una soluzione non nulla ( $\beta_2 - h(\beta_2) \neq 0$ ) ma con uno zero di  $(\beta_1, \dots, \beta_{n+1})$

In particolare dove c'erano prima gli zeri, sono rimasti gli zeri in quanto se  $\beta_i = 0$ , allora anche  $h(\beta_i) = 0$ , da cui si ottiene che  $\beta_i - h(\beta_i) = 0$

□

Quindi avendo dimostrato questa cosa, segue che

$$Gal(L/L^H) = H$$

□

### Dimostrazione Alternativa:

Per poter dare una dimostrazione alternativa, diamo prima questi due lemmi

#### Lemma 1

Sia  $L/K$  un'estensione normale di campi. Allora:

$$L^{Gal(L/K)} = K$$

### Dimostrazione:

⊇) Segue dalla definizione di campo fisso

⊆) Sia  $\alpha \in L^{Gal(L/K)}$  e sia  $f \in K[x]$  il polinomio minimo di  $\alpha$ .

Voglio mostrare che

$$f = x - \alpha$$

Sia quindi  $\alpha' \in L$  radice di  $f$ . Allora esiste  $\sigma \in Gal(L/K)$  tale che

$$\sigma(\alpha) = \alpha'$$

Ma  $\alpha \in L^{Gal(L/K)}$ , quindi

$$\sigma(\alpha) = \alpha \quad \Rightarrow \quad \alpha = \alpha'$$

Cioè  $f$  ha come unica radice  $\alpha$ , quindi

$$f = x - \alpha \quad \Rightarrow \quad \alpha \in K$$

□

#### Lemma 2

Sia  $L/K$  un'estensione normale e siano  $H \leq Gal(L/K)$  e  $\alpha \in L$ . Definiamo il seguente polinomio:

$$\Phi(x) = \prod_{\sigma \in H} (x - \sigma(\alpha)) \in L[x]$$

Allora  $\Phi(x) \in L^H[x]$  ed ha  $\alpha$  come radice

### Dimostrazione:

Vogliamo mostrare che  $\Phi(x) \in L^H[x]$ . Ciò è equivalente a dimostrare che:

$$\forall \varphi \in H, \varphi(\Phi) = \Phi$$

Dove  $\varphi$  indica anche l'estensione a  $L[x] \rightarrow L[x]$

Sia quindi  $\varphi \in H$ , allora:

$$\varphi(\Phi(x)) = \varphi \left( \prod_{\sigma \in H} (x - \sigma(\alpha)) \right) = \prod_{\sigma \in H} (x - (\varphi \circ \sigma)(\alpha))$$

Osserviamo che l'applicazione:  $\begin{array}{c} H \rightarrow H \\ \sigma \mapsto \varphi \circ \sigma \end{array}$  è biunivoca e quindi rappresenta una permutazione di  $H$

Dunque:

$$\prod_{\sigma \in H} (x - (\varphi \circ \sigma)(\alpha)) = \prod_{\sigma \in H} (x - \sigma(\alpha)) = \Phi(x)$$

Cioè  $\varphi(\Phi) = \Phi$ , quindi  $\Phi(x) \in L^H[x]$

Ovviamente  $id \in H$ , quindi  $x - \alpha \mid \Phi(x)$  quindi  $\alpha$  è radice di  $\Phi$

□

*Ora possiamo proseguire con la dimostrazione*

1) Sia  $F \in \mathcal{F}$ . Osserviamo che  $L/F$  è ancora un'estensione normale, infatti se  $L$  è il campo di spezzamento di un polinomio in  $K$  a maggior ragione è il campo di spezzamento dello stesso polinomio in  $F$ , quindi la tesi dal Lemma 1

2) Sia  $H \in \mathcal{G}$ . Vogliamo mostrare che  $Gal(L/L^H) = H$ .

⊇) Segue dalla definizione di  $L^H$  e dal gruppo di Galois. Quindi sappiamo che  $|H| \leq |Gal(L/L^H)|$

⊆) Per mostrare quest'inclusione dobbiamo mostrare che  $|Gal(L/L^H)| \leq |H|$ .

Sappiamo che  $|Gal(L/L^H)| = [L : L^H]$ , quindi esiste  $\alpha \in L$  tale che  $L = L^H[\alpha]$ .

Sia  $\mu \in L^H[x]$  il polinomio minimo di  $\alpha$  su  $L^H$ . Sia  $\Phi(x)$  definito come:

$$\Phi(x) = \prod_{\sigma \in H} (x - \sigma(\alpha))$$

Per il Lemma 2 abbiamo che  $\Phi(x) \in L^H[x]$  ed ha  $\alpha$  radice. Allora  $\mu(x) \mid \Phi(x)$ , quindi il grado di  $\mu$  divide il grado di  $\Phi$ .

Ma  $\deg(\mu) = [L : L^H]$  poiché  $L = L^H[\alpha]$  e  $\deg(\Phi) = |H|$  per costruzione.

Quindi  $[L : L^H] \leq |H|$ , da cui  $|Gal(L/L^H)| \leq |H|$

Dunque  $Gal(L/L^H) = H$

□