

Proposizione:

Ogni dominio è sottoanello di un campo

Def. (Frazione):

Una **FRAZIONE** è una coppia $a, b \in \mathbb{Z}$ con $b \neq 0$
a meno di una relazione di equivalenza \sim t.c.:

$$\frac{a}{b} \sim \frac{c}{d} \Leftrightarrow ad = bc \quad \forall a, b \in \mathbb{Z}, b \neq 0$$

Sia $X = R \times (R \setminus \{0\})$ e definiamo \sim su X t.c.:

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc \quad \forall (a, b), (c, d) \in X$$

\sim è relazione di equivalenza:

1) Riflessività: $(a, b) \sim (a, b) \Leftrightarrow ab = ba \quad \checkmark$

2) Simmetria: \checkmark (ovvio)

3) Transitività:

$$(a, b) \sim (c, d), (c, d) \sim (e, f) \Rightarrow ad = bc \wedge c f = de$$

$$\Rightarrow adf = bcf \wedge bcf = bde \Rightarrow adf = bde \text{ con } d \neq 0$$

$$\Rightarrow \exists d^{-1} \in X \Rightarrow af = be$$

Poniamo $\mathbb{Q}(R) = X/\sim$, allora la classe di (a, b) si
indica con $\frac{a}{b}$ (o a/b) e quindi si ha:

$$\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc$$

Definiamo le seguenti operazioni su $\mathbb{Q}(R)$:

$$1) \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

$$2) \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

Va mostrato che, se $\frac{a}{b} = \frac{a'}{b'} \wedge \frac{c}{d} = \frac{c'}{d'}$, allora

$$\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'} \wedge \frac{ac}{bd} = \frac{a'c'}{b'c'}. \text{ Si ha:}$$

$$1) (ad+bc)b'd' = ab'd'd' + bb'cd' = a'bdd' + b'b'c'd' \\ = (a'd' + b'c')bd \quad \checkmark$$

2) \checkmark

$\Rightarrow +, \cdot$ sono ben definite e rendono $(\mathbb{Q}(R), +, \cdot)$ un anello con elemento neutro additivo $\frac{0}{1} = \frac{0}{b}$
 $\forall b \in R \setminus \{0\}$ ed elemento neutro moltiplicativo $1 = \frac{b}{b}$
 $\forall b \in R \setminus \{0\}$. L'opposto è invece $-\frac{a}{b}$ $\forall (a, b) \in \mathbb{Q}(R)$.

$\mathbb{Q}(R)$ è per costruzione un anello commutativo, ed ogni elemento non nullo ha inverso:

$$\frac{a}{b} = \frac{0}{1} \Leftrightarrow a = 0$$

$$\Rightarrow \text{quindi, se } a \neq 0, \text{ si ha } \frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ba} = \frac{1}{1}$$

$\Rightarrow \mathbb{Q}(R)$ è quindi un campo

Consideriamo l'omomorfismo iniettivo definito da:

$$\begin{aligned} R &\rightarrow \mathbb{Q}(R) \\ a &\mapsto \frac{a}{1} \quad \left(\frac{a}{1} = \frac{0}{1} \Leftrightarrow a = 0 \right) \end{aligned}$$

Identificando a con $\frac{a}{1}$ possiamo quindi considerare R come sottanello di $\mathbb{Q}(R)$

$\mathbb{Q}(R)$ è detto CAMPO DELLE FRAZIONI di R. Se si ha $R = F[x]$, $\mathbb{Q}(R) = F(x)$ è costituito dalle frazioni $\frac{f(x)}{g(x)}$. In $\mathbb{Q}(x)$ si ha $\frac{x^2+2x-3}{x+3} = x-1$. $F(x)$ è detto CAMPO DELLE FUNZIONI RAZIONALI (anche se NON sono funzioni !!!!)

Se R è un campo, chi è $\mathbb{Q}(R)$?

\Rightarrow l'automorfismo precedente è, in questo caso, anche suriettivo ($\frac{a}{b} = \frac{ab^{-1}}{1}$), quindi $R = \mathbb{Q}(R)$

Proposizione:

Se $x \in F(x)$, x non è un quadrato in $F(x)$

Dim.:

Se la frase, si avrebbe:

$$x = \left(\frac{f(x)}{g(x)} \right)^2 = \frac{f(x)^2}{g(x)^2} \Rightarrow x g(x)^2 = f(x)^2$$

$$\Rightarrow \underbrace{\deg(x g(x)^2)}_{\text{dispari}} = \underbrace{\deg(f(x)^2)}_{\text{pari}} \quad \leftarrow$$

q.e.d.

Dato $a \in \mathbb{Z} \setminus \{0\}$, si può definire:

$$v_2(a) := \max \{ n \in \mathbb{N} \mid 2^n \mid a \}$$

$$\Rightarrow a, b = 0 \Rightarrow v_2(ab) = v_2(a) + v_2(b) \Rightarrow 2 = \frac{a^2}{b^2}$$

$$\Rightarrow 2b^2 = a^2 \Rightarrow \underbrace{v_2(2b^2)}_{\text{dispari}} = \underbrace{v_2(a^2)}_{\text{pari}} \quad \leftarrow$$

Proposizione:

Dati R dominio, F campo, $\varphi: R \rightarrow F$ automorfismo iniettivo, si ha che $\exists! \bar{\varphi}: \mathbb{Q}(R) \rightarrow F$ automorfismo t.c. $\bar{\varphi}|_R = \varphi$ ovvero $\bar{\varphi}\left(\frac{a}{b}\right) = \varphi(a)\varphi(b)^{-1}$ (la restrizione di $\bar{\varphi}$ a R è φ)

Campi:

Dato K campo e $F \subseteq K$ sottocampo, si dice che K è **ESTENSIONE** di F . Dato $b \in K$, $F[b]$ è sottosetore di K ed è l'immagine di $\ell_b : F[x] \rightarrow K$

$$\Rightarrow F[b] = \{f(b) \mid f(x) \in F[x]\}$$

Denoteremo $(f) = f(x) F[x]$

Abbiamo 2 casi:

- 1) ℓ_b è iniettivo $\Rightarrow F[b]$ non è un campo
 - 2) ℓ_b non è iniettivo ($\Leftrightarrow \text{Ker } \ell_b = (f)$ con $f \neq 0$)
- $\Rightarrow F[b] \cong F[x]/(f)$ è un dominio (sottosetore di K), quindi (f) è ideale primo
- \Rightarrow in $F[x]$ ogni ideale primo non nullo è massimale
- $\Rightarrow f$ irriducibile $\Rightarrow F[b]$ è un campo

Nel caso (1) $\nexists f(x) \in F[x]$ non nullo t.c.

$f(b) = 0$. Nel caso (2), $f(b) = 0$ dove $(f) = \text{Ker } \ell_b$

\Rightarrow nel caso (1) b si dice **TRASCENDENTE** su F ,

nel caso (2) b si dice **ALGEBRICO** su F

Algebrico: $\exists f(x) \in F[x]$ con $f(x) \neq 0$ t.c. $f(b) = 0$

Se $F = \mathbb{Q}$, $K = \mathbb{C}$, parleremo di **NUMERI TRASCENDENTI** (o **NUMERI ALGEBRICI**)

Esempi:

- 1) $\sqrt{2} \in \mathbb{C}$ è numero algebrico
- 2) $\pi \in \mathbb{C}$ è numero trascendente (Lindemann - Weierstrass)

3) Idea di Liouville:

$$\Rightarrow 0, \underbrace{01}_{1!} \underbrace{001}_{2!} \underbrace{000000}_{3!} \underbrace{10\ldots01}_{4!} \ldots$$

Proposizione:

Sia K estensione di F , $b \in K$ algebrico su F . Allora $\exists!$ $f(x)$ polinomio monico di grado minimo t.c. $f(b) = 0$

$\Rightarrow I = \{g(x) \in F[x] \mid g(b) = 0\} \neq \{0\}$ è ideale di $F[x]$. Si ha $I = (f)$ con f monico

Tale polinomio è irriducibile:

$$f(x) = f_1(x) f_2(x) \Rightarrow f(b) = f_1(b) f_2(b) = 0 \\ \Leftrightarrow f_1(b) = 0 \vee f_2(b) = 0$$

MA:

$$f_1 \in I \Rightarrow \deg f_1 \geq \deg f \Rightarrow \deg f_1 = \deg f \\ \Rightarrow f_2 \text{ invertibile}$$

Questo polinomio (monico !!!) è detto **POLINOMIO MINIMO DI b** .

Esempio

il polinomio minimo di $\sqrt{2}$ su \mathbb{Q} è $(x^2 - 2)$
 $\Rightarrow x^2 - 2$ è irriducibile in $\mathbb{Q}[x]$

Def. (Estensione Algebrica):

Diremo che K è un'ESTENSIONE ALGEBRICA di F se ogni elemento di K è algebrico su F

Esempio:

- 1) $\mathbb{Q}[\sqrt{2}]$ è un'estensione algebrica di \mathbb{Q}
 $\Rightarrow \mathbb{Q}[\sqrt{2}] = \{\alpha + b\sqrt{2} \mid \alpha, b \in \mathbb{Q}\}$
 $\Rightarrow u = \alpha + b\sqrt{2} \Rightarrow u - \alpha = b\sqrt{2} \Rightarrow u^2 - 2\alpha u + \alpha^2 = 2b^2$
 $\Rightarrow u$ è radice di $x^2 - 2\alpha x + \alpha^2 - 2b^2 \in \mathbb{Q}[x]$
- 2) π è trascendente su \mathbb{Q} \Rightarrow se F è il minimo sottocampo di \mathbb{C} contenente \mathbb{Q} e π^2 , allora π è algebrico su F dato che è radice di $x^2 - \pi^2$

Proposizione:

Se K è un'estensione di F , allora K è uno spazio vettoriale su F

Se K è finitamente generata su F , indicheremo la **DIMENSIONE** di K su F con $[K:F]$ e diremo che K è **ESTENSIONE FINITA** di F .

N.B.

\exists estensioni non finite (es. \mathbb{IR} su \mathbb{Q}):
se esistesse $\{v_1, \dots, v_n\}$ base di \mathbb{IR} come spazio vettoriale su \mathbb{Q} , avremmo $|\mathbb{IR}| = |\mathbb{Q}^n| = |\mathbb{Q}| = |\mathbb{N}| \not\rightarrow$

Esempio:

\mathbb{C} è estensione finita di \mathbb{IR} con base $\{1, i\}$

Teorema:

Ogni estensione finita è algebrica

Dim.:

Supponiamo $[K:F] = n \Rightarrow b \in K, \{1, b, b^2, \dots, b^n\}$ è lin. dip. e perciò $\exists \alpha_0, \dots, \alpha_n \in F$ non tutti nulli t.c. $\alpha_0 + \alpha_1 b + \dots + \alpha_n b^n = 0$. Dunque $\alpha_0 + \alpha_1 x + \dots + \alpha_n x^n = g(x) \in F[x]$ con $g(x) \neq 0$ e $g(b) = 0$

q.e.d.

Esempio:

$\mathbb{Q}[\sqrt[3]{2}]$ è estensione finita di \mathbb{Q} perché $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ è un insieme di generatori: $\sqrt[3]{2}$ è radice di $x^3 - 2$ \Rightarrow se $f(x) \in \mathbb{Q}[x]$, $f(x) = (x^3 - 2)q(x) + r(x)$ con $\deg r < 3 \Rightarrow f(\sqrt[3]{2}) = r(\sqrt[3]{2})$ $\Rightarrow \mathbb{Q}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$

Siano $F \subseteq K \subseteq L$ con L estensione di K , K estensione di F e L estensione di F . Se L è estensione finita di F allora è anche estensione finita di K . Inoltre K è estensione finita di F perché è sottospazio di L

Tenemo:

Dati $F \subseteq K \subseteq L$ campi, si ha:

L estensione finita di $F \Leftrightarrow \begin{cases} L \text{ estensione finita di } K \\ K \text{ estensione finita di } F \end{cases}$

Inoltre, in tal caso, si ha $[L:F] = [L:K] \cdot [K:F]$

Dim.:

(\Rightarrow): vista sopra \checkmark

(\Leftarrow): supponiamo che L estensione finita di K

\Rightarrow sia $\{u_1, \dots, u_m\}$ base di L

$\Rightarrow K$ estensione finita di K

\Rightarrow sia $\{v_1, \dots, v_n\}$ base di K

Mostriamo che $\{u_i v_s\}_{\substack{i=1, \dots, m \\ s=1, \dots, n}}$ è base di L su F

$c \in L \Rightarrow c = \sum_{i=1}^m b_i u_i$ con $b_1, \dots, b_m \in K$

$b_i \in K \Rightarrow b_i = \sum_{s=1}^n \alpha_{is} v_s$ con $\alpha_{is} \in F$

$$\Rightarrow c = \sum_{i=1}^m b_i u_i = \sum_{i=1}^m \left(\sum_{s=1}^n \alpha_{is} v_s \right) u_i = \sum_{\substack{i=1, \dots, m \\ s=1, \dots, n}} \alpha_{is} (u_i v_s)$$

$$0 = \sum_{\substack{i=1, \dots, m \\ s=1, \dots, n}} \alpha_{is} (u_i v_s) = \sum_{i=1}^m \underbrace{\left(\sum_{s=1}^n \alpha_{is} v_s \right)}_{\in K} u_i$$

Quindi $\sum_{s=1}^n \alpha_{is} v_s = 0 \quad (i = 1, \dots, m)$

$\Rightarrow \alpha_{is} = 0 \quad \forall i = 1, \dots, m, s = 1, \dots, n$

q.e.d.

Esempio:

V spazio vettoriale su $\mathbb{C} \Rightarrow V$ spazio vettoriale su \mathbb{R}

V spazio vettoriale su \mathbb{Q}

Infatti, se $\{v_1, \dots, v_n\}$ è base di V su \mathbb{C} , allora $\{v_1, iv_1, \dots, v_n, iv_n\}$ è una base di V su \mathbb{R}

N.B.

V finitamente generato su $\mathbb{Q} \Rightarrow V$ numerabile

N.B.

\mathbb{K} non è finitamente generato su \mathbb{Q} (se lo fosse, si avrebbe \mathbb{K} numerabile \mathbb{N})

Proposizione:

Dati K estensione di F e $b \in K$ algebrico su F , si ha che $F[b]$ è sottocampo di K

Sia $f(x) \in F[x]$ il polinomio minimo di b . Se $g(x) \in F[x]$, allora $g(x) = f(x)q(x) + r(x)$ con $\deg r < \deg f$. Quindi si ha:

$$r(x) = \alpha_0 + \alpha_1 x + \dots + \alpha_{n-1} x^{n-1} \text{ con } n = \deg f$$

In particolare, ogni elemento di $F[b]$ si scrive come $\alpha_0 + \alpha_1 b + \dots + \alpha_{n-1} b^{n-1}$ con $\alpha_i \in F$.

$\Rightarrow \{1, b, b^2, \dots, b^{n-1}\}$ è insieme di generatori di $F[b]$ ed è anche una base:

$$\alpha_0 + \alpha_1 b + \dots + \alpha_{n-1} b^{n-1} = 0 \Rightarrow \alpha_0 = \dots = \alpha_{n-1} = 0$$

altrimenti si avrebbe un polinomio di $\deg < n$ che ha b come radice $\frac{1}{b}$

$\Rightarrow \{1, b, b^2, \dots, b^{n-1}\}$ è base di $F[b]$ su F

Sia $c \in F[b] \setminus \{0\}$ e consideriamo la funzione

$$L_c : F[b] \longrightarrow F[b]$$
$$v \longmapsto cv$$

$\Rightarrow L_c$ è lineare su F , tuttavia:

$$L_c(v) = 0 \Rightarrow v = 0$$

$\Rightarrow L_c$ è suriettiva $\Rightarrow \exists c' \in F[b]$ t.c. $L_c(c') = 1$

$$\Leftrightarrow cc^{-1} = 1 \Leftrightarrow c^{-1} \in F[b]$$

\Rightarrow se $b \in K$ è trascendente su F , allora l'automorfismo φ_b è isomorfismo $\Rightarrow F[b]$ non è un campo $\Rightarrow F[b]$ non è sottocampo di K

$\Rightarrow b$ algebrico su $F \Leftrightarrow F[b]$ sottocampo di K

D'ora in poi scrivremo $F(b)$ se b è algebrico su F , $F(b)$ indica il minimo sottocampo di K che contiene b ed F . Scrivremo inoltre:

$$F(a)(b) = F(a, b) = F(b)(a)$$

Teorema:

Se K è estensione di F e $b, c \in K$ sono algebrici su F , allora:

- 1) $b - c$ algebrico su F
- 2) bc algebrico su F
- 3) se $b \neq 0$, b^{-1} algebrico su F

\Rightarrow l'insieme degli elementi di K algebrici su F è un sottocampo di K .

Esempio:

$3 + \sqrt[3]{7} - \sqrt[5]{2}$ è algebrico perché è somma di numeri algebrici

Dim.:

$F(b, c)$ è finitamente generato come spazio vettoriale su F , infatti:

$$[F(b,c) : F] = [F(b,c) : F(b)] \cdot [F(b) : F]$$

\Rightarrow ogni elemento di $F(b,c)$ è algebrico su F

$\Rightarrow b-c, bc, b^{-1} \in F(b,c)$ (se $b \neq 0$)

$\Rightarrow b-c, bc, b^{-1}$ algebrici su F

q.e.d.

N.B.

Non è vero in generale il inverso. Contrassempio:
l'insieme dei numeri algebrici non è estensione
finita di \mathbb{Q}

Proposizione:

Ogni polinomio NON costante a coefficienti in
 $\overline{\mathbb{Q}} \subseteq \mathbb{C}$ (insieme dei numeri algebrici) ha una
radice in $\overline{\mathbb{Q}}$.

Dim.:

$$f(x) = a_0 + a_1 x + \dots + a_n x^n \text{ con } a_i \in \overline{\mathbb{Q}}, a_n \neq 0$$

\Rightarrow sia $b \in \mathbb{C}$ radice di $f(x)$. Allora b è algebrico
su $\mathbb{Q}(a_0, \dots, a_n)$ che è estensione finita di \mathbb{Q}

$$\Rightarrow [\mathbb{Q}(a_0, \dots, a_n, b) : \mathbb{Q}] < +\infty$$

\Rightarrow anche $[\mathbb{Q}(b) : \mathbb{Q}] < +\infty \Rightarrow b$ algebrico su \mathbb{Q}

$$\Rightarrow b \in \overline{\mathbb{Q}}$$

q.e.d.

Esempio:

$\sqrt{2}, \sqrt{3}$ sono algebrici su \mathbb{Q} , infatti $\sqrt{2}$ è radice

di $x^2 - 2 \in \mathbb{Q}[x]$, $\sqrt{3}$ è radice di $x^2 - 3 \in \mathbb{Q}[x]$
 $\Rightarrow \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$, infatti:

$$1) \sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3}) \Rightarrow \mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

$$2) (\sqrt{2} + \sqrt{3})^{-1} = \sqrt{3} - \sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3}), \text{ quindi:}$$

$$(\sqrt{2} + \sqrt{3}) + (\sqrt{3} - \sqrt{2}) \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$$

$$\Leftrightarrow 2\sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$$

$$\Leftrightarrow \sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$$

$$\Leftrightarrow \sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$$

$$\Leftrightarrow \mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2} + \sqrt{3})$$

Qual è il polinomio minimo di $\sqrt{2} + \sqrt{3} = b$?

$$\sqrt{2} + \sqrt{3} = b \Rightarrow b^2 = 2 + 2\sqrt{6} + 3$$

$$\Leftrightarrow b^2 - 5 = 2\sqrt{6} \Leftrightarrow b^4 - 10b^2 + 25 = 24$$

$\Rightarrow b$ è radice di $x^4 - 10x^2 + 1$

$$\Rightarrow \mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

$$\Rightarrow \underbrace{[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}]}_{\substack{\text{deg del polinomio minimo} \\ 1}} = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}]$$

$$\stackrel{1}{=} [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$$

$\Rightarrow x^2 - 3 \in \mathbb{Q}(\sqrt{2})[x]$ è irriducibile:

$$(\alpha + b\sqrt{2})^2 = 3 \text{ con } \alpha, b \in \mathbb{Q}$$

$$\Leftrightarrow \alpha^2 + 2b^2 + 2ab\sqrt{2} = 3 \text{ con}$$

$\{1, \sqrt{2}\}$ base di $\mathbb{Q}(\sqrt{2})$ su \mathbb{Q}

$$\Rightarrow \begin{cases} \alpha^2 + 2b^2 - 3 = 0 \\ 2ab = 0 \end{cases} \quad \begin{matrix} \frac{1}{1} \\ \frac{2}{2} \end{matrix}$$

$$\Rightarrow [\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = 2 \cdot 2 = 4$$

\Rightarrow Il polinomio minimo di $\sqrt{2} + \sqrt{3}$ è $x^4 - 10x^2 + 1$ che

è quindi irriducibile.

N.B.

In \mathbb{R} si ha:

$$\begin{aligned}x^4 - 10x^2 + 1 &= x^4 - 2x^2 + 1 - 8x^2 \\&\stackrel{|}{=} (x^2 - 1)^2 - (\times\sqrt{8})^2 \\&\stackrel{|}{=} (x^2 - \times\sqrt{8} - 1)(x^2 + \times\sqrt{8} - 1)\end{aligned}$$

$$\begin{aligned}&(\Rightarrow x^2 \pm 2\times\sqrt{2} - 1 \text{ ha radici } \pm\sqrt{2} \pm\sqrt{3}) \\&= (x - \sqrt{2} - \sqrt{3})(x - \sqrt{2} + \sqrt{3})(x + \sqrt{2} - \sqrt{3})(x + \sqrt{2} + \sqrt{3})\end{aligned}$$

\Rightarrow se esistessero $x^4 - 10x^2 - 1 = g(x)h(x)$ in $\mathbb{Q}[x]$,
 g, h dovrebbero avere $\deg = 2$.

Non c'è modo di accoppiare tali fattori di $\deg = 2$
per ottenere polinomi in $\mathbb{Q}[x]$
