Esercizi del 23 novembre 2020

K campo $K[x]$ P.I.D. $I \subseteq K[x]$ $I \neq (0)$

$I = K[x]$. $I = (f)$ $f \in K[x]$.

Vogliamo studiare $K[x]/(f)$

- f è irrid (= primo) $K[x]/(f)$ è campo.
- Gli elem di $K[x]/(f)$

sono classi $[g] = \{ g + h \mid h \in (f) \}$

$= \{ g + \alpha f \mid \alpha \in K[x] \}$.

- $g \equiv g_1 \mod f$ significa

$[g] = [g_1]$ in $K[x]/(f)$

cioè $g - g_1$ è multiplo di f.

- Se $g \in K[x]$ $[g]$ è rappresentata

in modo unico dal resto della div di

g per f $g = qf + r$ $0 \leq \deg r < \deg f$

$[g] = [qf + r] = [r]$

r è unico.

Se $[g] = [g_1]$ $\qquad g_1 = q_1 f + r_1$

allora $r_1 = r$.

Infatti $g - g_1$ è div per f

$$\underbrace{qf + r - (q_1 f + r_1)}$$

$$\underbrace{f(q - q_1)} + \underbrace{r - r_1} \leftarrow \text{è div per } f$$

è div f

r, r_1 div per f $\quad \deg(r - r_1) < \deg f \Rightarrow r = r_1$

$\mathbb{Z}_m$ $\qquad \underline{[0], [1], \ldots, [m-1]}.$

$[m]\ [10m+1] \ldots$

$K[x]/(f)$ è K-sp vett.

$K[x]/(f)$ contiene K. $\qquad \underline{a \in K}$ $\underline{\underline{[a]}}$

$[a], [b]$ $\qquad a, b \in K$ $\qquad [a] = [b]$

$a - b \in I \Longrightarrow a = b.$

$K[x]/(f)$ è K-sp. vett.

$$K \times K[x]/(f) \longrightarrow K[x]/(f)$$

$$a, \; [g] \longmapsto [ag].$$

$K[x]/(f)$ è K-sp. vett. di dim n

dove $n = \deg f$

Una sua base è data da $[1], [x], [x^2], \dots, [x^{n-1}]$ $\; \| \; [x]^{n-1}$

Infatti

$[g] \in K[x]/(f)$ $\quad [g] = [a_0 + a_1 x + \dots + a_{n-1} x^{n-1}]$

dove $a_0, \dots, a_{n-1} \in K$ e $a_0 + a_1 x + \dots + a_{n-1} x^{n-1}$

è il resto della div di g per f.

$$[g] = [a_0] + [a_1][x] + \dots + [a_{n-1}][x^{n-1}]$$

$$= a_0 + a_1 [x] + \dots + a_{n-1}[x^{n-1}]$$

$$= \text{comb lin } [1], [x], \dots, [x^{n-1}].$$

$[1], \dots [x^{n-1}]$ sono lin indip

Esercizi Trovare tutti i div dello zero

di $\mathbb{Q}[x]/(x^2-1)$.

Gli elem di $\mathbb{Q}[x]/(x^2-1)$ sono della seguente forma:

$$[a_0+a_1x] = [a_0]+[a_1][x] = a_0+a_1[x]$$

Scriviamo x al posto di $[x]$. (forzatura).

Quindi gli el di $\mathbb{Q}[x]/(x^2-1)$ si possono scrivere

come a_0+a_1x. $a_0, a_1 \in \mathbb{Q}$

Prendo a_0+a_1x e $b_0+b_1x \in \mathbb{Q}[x]/(x^2-1)$

$(a_0+a_1x)(b_0+b_1x)=0$ vedo quando succede questo.

$$a_0b_0+(a_0b_1+a_1b_0)x+a_1b_1\underline{x^2}=0$$

$[x^2]=[1]$ cioè, scritto abbreviato, $x^2=1$

$$(a_0b_0+a_1b_1)\cdot 1+(a_0b_1+a_1b_0)\cdot x = 0 \;/\; 1$$

$\boxed{a_1 \neq 0}$

$$\begin{cases} a_0b_0+a_1b_1=0 \\ a_0b_1+a_1b_0=0 \end{cases} \qquad \begin{cases} b_1 = -\dfrac{a_0b_0}{a_1} \\ \dfrac{-a_0\cdot a_0b_0}{a_1}+a_1b_0=0 \end{cases}$$

$$\begin{cases} b_1 = -\dfrac{a_0b_0}{a_1} \\ -a_0^2b_0+a_1^2b_0=0 \end{cases} \qquad b_0(a_1^2-a_0^2)=0$$

$$\begin{cases} b_1 = -\dfrac{a_0 b_0}{a_1} \\ b_0 \cdot (a_1^2 - a_0^2) = 0 \end{cases} \qquad a_0, a_1, b_0, b_1 \in \mathbb{Q}$$

Caso 1 $b_0 = 0$ (II eq.) $\Rightarrow b_1 = 0$ (I eq.)

$(a_0 + a_1 x) \cdot 0 = 0$ non dà inform.

Caso 2 $\underline{(a_1^2 - a_0^2) = 0}$ $\underline{(a_1 - a_0)(a_1 + a_0) = 0}$

$a_1 = a_0$ oppure $a_1 = -a_0$.

Se $a_1 = a_0$ $b_1 = -b_0$

$a_0 + a_0 x$ è div. dello zero complice $b_0 - b_0 x$.

$a_0(1 + x)$ $a_0 \in \mathbb{Q}$ tutti questi sono div. 0.

Se $a_1 = -a_0$ ...... $a_0(1 - x)$ $a_0 \in \mathbb{Q}$ sono anche div. 0.

Altro procedimento.

$[f][g] = 0$ $fg \in (x^2 - 1)$. $\deg f \leq 1$
$\deg g \leq 1$

$fg = \alpha(x^2 - 1)$ $\alpha \in \mathbb{Q}$

$= \alpha(x+1)(x-1)$

$x+1$ divide f o g p.es. f. $f = u \cdot (x+1)$

$u\cancel{(x+1)} g = \alpha \cancel{(x+1)}(x-1) \Rightarrow x - 1$ divide g.

i div dello zero sono della forma $a(x+1)$ $a \in \mathbb{Q}$

oppure $b(x-1)$ $b \in \mathbb{Q}$.

$\mathbb{Q}[x]/(x^2-1)$ trovare gli el invertibili.
El. di $\mathbb{Q}$ sono invertibili.

$(a_0 b_0 + a_1 b_1) \cdot 1 + (a_0 b_1 + a_1 b_0) x = 1$

$(a_0 b_0 + a_1 b_1 - 1) \cdot \underline{1} + (a_0 b_1 + a_1 b_0) \underline{x} = 0$

$$\begin{cases} a_0 b_0 + a_1 b_1 = 1 \\ a_0 b_1 + a_1 b_0 = 0 \end{cases} \qquad a_1 \neq 0 \qquad \boxed{b_0 = -\frac{a_0 b_1}{a_1}}$$

$-\frac{a_0^2 b_1}{a_1} + a_1 b_1 = 1$ $/ -a_1$

$-a_0^2 b_1 + a_1^2 b_1 = a_1$

$$\boxed{b_1 = \frac{a_1}{a_1^2 - a_0^2}}$$

$$\boxed{b_0 = -\frac{a_0}{a_1^2 - a_0^2}}$$

Si può fare purché $\boxed{a_1^2 - a_0^2 \neq 0}$

Vale: l'inverso di $a_0 + a_1 x$ è

dato da $-\frac{a_0}{a_1^2 - a_0^2} + \frac{a_1}{a_1^2 - a_0^2} x$ $(a_0 \neq \pm a_1)$

Sia $f \in \mathbb{Q}[x]$ dato da $f = x^2+2$

f è irrid (per esempio per Eisenstein)

f è irrid perché lo è in $\mathbb{R}[x]$ $(\Delta < 0)$

f è irrid perché in $\mathbb{Z}_5[x]$.

$0, 1, 2, 3, 4$

$0 \quad 1 \quad 4 \quad 4 \quad 1 \qquad x^2$

$2 \quad 3 \quad 1 \quad 1 \quad 3 \quad \neq 0$

x^2+2 valutato in $x = 0, 1, 2, 3, 4$

è sempre $\neq 0$.

x^2+2 non ha fattori lin in $\mathbb{Z}_5[x]$.

$\Longrightarrow x^2+2$ irrid in $\mathbb{Q}[x]$.

f irrid in $\mathbb{Q}[x]$.

f ha radici $\frac{p}{q}$ razionali se $p \mid$ termine noto

$q \mid$ diretto coeff dir.

$\frac{p^2}{q^2}+2=0 \qquad p^2+2q^2=0$

$p \mid 2 \quad q \mid 1 \qquad p=\pm 1,\ p=\pm 2 \qquad q=1$

$\frac{1}{1} \mid -\frac{1}{1} \mid \frac{2}{1} \mid -\frac{2}{1}$ rad di x^2+2 ?

---

f è irrid. dire com'è fatto il campo $\mathbb{Q}[x]/(f)$

dare una tabella per la moltiplicazione ....

$f = x^2+2$.

Come sp. vett. ha dim 2 su $\mathbb{Q}$.

base $1, x$

generico elem è $a_0 + a_1 x \quad a_0, a_1 \in \mathbb{Q}$.

Se $a_0 + a_1 x \neq 0$ $(a_0 \neq 0 \neq a_1)$ cerco l'inverso.

$$(a_0 + a_1 x)(b_0 + b_1 x) = 1$$

$$\begin{cases} a_0 b_0 - 2 a_1 b_1 = 1 \\ a_0 b_1 + a_1 b_0 = 0 \end{cases} \qquad \underline{b_0} = -\frac{a_0 b_1}{a_1}$$

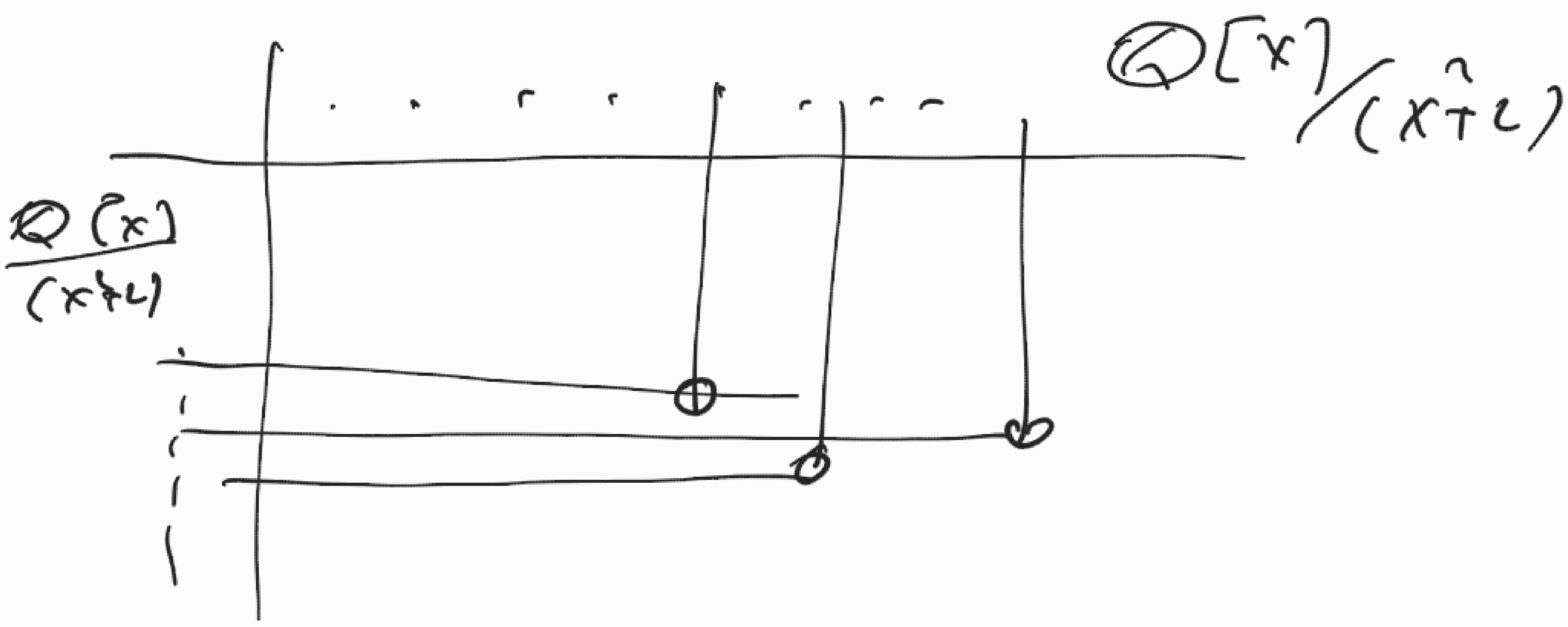
$$-\frac{a_0^2 b_1}{a_1} - 2 a_1 b_1 = 1$$

$$-a_0^2 b_1 - 2 a_1^2 b_1 = a_1$$

$$\boxed{\begin{aligned} b_1 &= \frac{-a_1}{a_0^2 + 2a_1^2} \\ b_0 &= \frac{a_0}{a_0^2 + 2a_1^2} \end{aligned}}$$

$$a_0^2 + 2a_1^2 \neq 0 \quad \forall a_0, a_1 \in \mathbb{Q} \quad (a_0 \neq 0 \neq a_1)$$

$$\boxed{\mathbb{Q}[x] \Big/ (x^2 + \alpha x + \beta)}$$



$v_1, \ldots, v_n$ bază de sp vect V

în V este dat un produs

$$(\lambda_1 v_1 + \ldots + \lambda_n v_n)(\mu_1 v_1 + \ldots + \mu_n v_n) =$$

$$(\ )v_1 + \ldots + (\ )v_n.$$

$$v_1 \cdot v_1, \quad v_1 \cdot v_2, \quad v_2 \cdot v_4, \quad \ldots \quad \underline{v_i \cdot v_j}$$

$$\downarrow \qquad \downarrow \qquad \downarrow$$

	v_1	v_2	$\ldots$	v_n
v_1	$\cdot$	$\cdot$		$\cdot$
$\vdots$				
v_n	$\cdot$	$\cdot$		

$1, x$ bază de $\mathbb{Q}[x]/\underline{(x^2+2)}$

	1	x
1	1	x
x	1	-2

$$(\lambda_1 1 + \lambda_2 x) \cdot (\mu_1 \cdot 1 + \mu_2 \cdot x) =$$

$$= \underline{\lambda_1 \mu_1 1 + \lambda_1 \mu_2 \cdot x + \lambda_2 x + \lambda_2 \mu_2(-2)}$$

Esercizio $\quad f = x^2 - 4 \in \mathbb{Q}[x] \quad I = (f)$

Trovare tutti gli ideali massimali che $\supseteq I$.

Sia $\mathcal{P}$ primo $\mathcal{P} \supseteq I$.

$x^2 - 4 \in \mathcal{P} \qquad (x+2)(x-2) \in \mathcal{P}$

quindi $\mathcal{P}$ è t.c.:

o $x+2 \in \mathcal{P}$ (1)

oppure $x-2 \in \mathcal{P}$ (2)

(1) $x+2$ è irrid. Quindi $(x+2)$ è primo e anche massimale $(x+2) \subseteq \mathcal{P}$

Allora $\mathcal{P} = (x+2)$

(2) $\mathcal{P} = (x-2)$

Trovare un anello (non campo) della forma $\mathbb{Q}[x]/(f)$ per f opportuno, in modo che questo anello abbia un solo ideale massimale.

$f = x^2$ Scopriamo che solamente l'ideale $\mathfrak{M} = (x)$ contiene (x^2).

Ideali di A/I sono gli id. di A che $\supseteq I$.

Esercizi: $K = \mathbb{Z}_3[x] / (x^2+x+2)$

1ª domanda Quanti el. ha K?

2ª domanda $K^* = K \setminus \{0\}$ provare che K^* è un gruppo ciclico

---

$K = \mathbb{Z}_3[x] / (x^2+1)$ K campo finito è perfetto. Ogni el. ha radice cubica $(p=3)$ trovare $\sqrt[3]{x+2}$.