Definizioni:

A anello commutativo con 1
(unità, el. neutro per $\cdot$)

$\emptyset \neq I \subseteq A$ è un ideale se

- $a_1, a_2 \in I \Rightarrow a_1 - a_2 \in I$

(in particol. $0 \in I$, $a \in I \Rightarrow -a \in I$)

- $a \in I \quad b \in A \Rightarrow ab \in I$

<u>Es.</u> se $a \in A$

$(a) := \{$ gli el. "divisibili per a"
cioè della forma ab
per $b \in A\}$ è un ideale
che si dice principale generato da a

<u>Def.</u> A/I è il quoz. di A per la
r.d.e. $a_1 \sim a_2 \Leftrightarrow a_1 - a_2 \in I$.

<u>TEO 1</u> A A/I anello e

$A \xrightarrow{\pi} A/I$ omom di anelli

definendo

$$[a]+[b] := [a+b]$$

$$[a][b] := [ab].$$

<u>Dim</u>

Vediamo che il prod. è ben definito

$$a' = a + \alpha \quad b' = b + \beta$$

$$\alpha, \beta \in I \implies$$

$$a'b' = ab + \underbrace{\alpha b + a\beta + \alpha\beta}_{\in I}$$

$\in I$ per def di ideale

le altre proprietà si verificano facilmente.

Es. $\mathbb{Z}/(n)$

<u>TEO 2</u>. Ogni ideale in $\mathbb{Z}$ o $\mathbb{K}[X]$ è principale

(Es. Trovare un ideale non principale in $\mathbb{Z}[X]$)

<u>Dim</u>. per $\mathbb{K}[X]$.

I ideale consideriamo $I \setminus \{0\}$ ($0 \in I$ sempre) e sia $p \in I \setminus \{0\}$ un elemento di grado minimo.

Mostriamo che se $q \in I \Rightarrow q$ è divisibile per p

$\deg q \geq \deg p$ per come abbiamo scelto p, quindi posso dividere:

$q = a p + r$ con $\deg r < \deg p$

ma $q \in I$, $p \in I \Rightarrow r = q - ap \in I$

perciò $r = 0$ e q è divisibile per p. $\square$

($\mathbb{Z}$, $\mathbb{K}[X]$ sono quindi domini ad ideali principali PID)

Chiaramente la dim dice anche che il generatore p è unico a meno di cost. molt. quindi

Corollario $I \subseteq \mathbb{K}[x]$

$\Rightarrow$ esiste unico p MONICO

t.c. $I = (p)$.

Dalla dim segue anche che

preso $q \in \mathbb{K}[x]$

$q = ap + r$ con $\deg r < p$

cioè OGNI el di $\mathbb{K}[x]$

(se $I \neq \{0\}$) è equivalente

a un elemento di grado $< p$.

Quindi se $\deg p = d$, si può scrivere ogni el di $\mathbb{K}[X]/(p)$ come

$$\left[a_0 + a_1 X + \ldots + a_{d-1} X^{d-1}\right].$$

<u>OSS.</u> $\mathbb{K}[X]/(p)$ è uno sp. vett. su $\mathbb{K}$ e stiamo dicendo che

$[1], \ldots, [X^{d-1}]$ è una base.

(Allo stesso modo una cl. di rappr.)
per $\mathbb{Z}/(n)$ è $[1], \ldots, [n-1]$.

es. $p = X^2+1$ $\quad \mathbb{K} = \mathbb{R}$

ogni el. in $\mathbb{R}[X]/X^2+1$ si scrive
$[a + bX]$ Come si fa il prod.?

$$[a+bX][c+dX] = [(a+bX)(c+dX)]$$

$[ac + (ad+bc)X + bdX^2]$

ma $[X^2] = [X^2+1-1] = [-1] \Rightarrow$

$[(ac-bd) + (ad+bc)X]$

<u>oss</u> $[X]^2 = [X^2] = [-1]$. Cioè $[X]$ è una "radice quadrata" di -1.

<u>OSS.</u>

$$[a+bX]\left[\frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}X\right] = [1]$$

$\Rightarrow \mathbb{R}[X]/_{X^2+1}$ è un campo

($=: \mathbb{C}$ campo dei numeri complessi.
Trad. $[X]$ si indica i e
$[a+bX] =: a+ib$.)

Questo fatto non è un caso:

TEO 3. p è irriducibile in $\mathbb{K}[X] \iff \mathbb{K}[X]/(p)$ è un campo.

Dim $\Leftarrow$ Se $p = p_1 p_2$ con p_1, p_2 di grado positivo $\overset{< \deg p}{\Longrightarrow}$

$[p_1], [p_2] \neq 0$ ma

$[p_1][p_2] = [p_1 p_2] = 0$!

$\Rightarrow \mathbb{K}[X]/(p)$ è un anello.

per far vedere che è un campo devo mostrare che se $[q] \neq 0 \Rightarrow$ trovo un inverso. q è primo con p quindi (Bézout) $\exists a, b$ t.c.

$$aq + bp = 1.$$

(dim veloce di Bezout. prendo l'insieme $I = \{\alpha p + \beta q\}$ $\alpha, \beta \in \mathbb{K}[x]$ è un ideale che è principale sia r il suo gen: $(r) = I$

$p \in (r)$, $q \in (r)$ ~~ma~~ ma p q primi tra loro quindi $(r) = (1)$

$1 \in I$ quindi si scrive

$\alpha p + \beta q$.). Applicando π

all'uguaglianza $aq + bp = 1$

si ha (per la def. delle

operazioni in A/I)

$[a][q] = 1$ quindi

$$[a] = [q]^{-1}$$

$\square$