

• UNITÀ DI $K[x] = \text{POLINOMIO } 1_K$

• $P+Q := \sum_{n=0}^{\infty} (a_n + b_n)x^n$

• $PQ := \sum_{n=0}^{\infty} \left(\sum_{i=0}^n a_i b_{n-i} \right) x^n$

ESEMPIO: IN $\mathbb{F}_2[x]$ SIANO $P := 1+x^2+x^3$ E $Q := x+x^2$

$$P+Q = 1+x+x^2+x^2+x^3 = 1+x+x^3$$

$$+x^3+x^5$$

$$PQ = (1+x^2+x^3)(x+x^2) = x+x^2+x^3+x^4+x^4+x^5 = x+x^2+$$

PROPOSIZIONE: SIANO $P, Q \in K[x]$ POLINOMI NON NULLI. ALLORA

$\deg(PQ) = \deg(P) + \deg(Q)$. IN PARTICOLARE, $K[x]$ È UN DOMINIO DI INTEGRITÀ

DEFINIZIONE) UN POLINOMIO SI DICE MONICO SE IL COEFFICIENTE DEL

TERMINALE DI GRADO MASSIMO È UGUALE A 1.

DEFINIZIONE) SIA K UN CAMPO. UN POLINOMIO P IN $K[x]$ SI DICE IRRIDUCIBILE

SE GLI UNICI SUOI DIVISORI SONO DEL TIPO a E aP CON $a \in K \setminus \{0\}$,

ALTRIMENTI SI DICE RIDUCIBILE.

ESEMPI:

a) IN $\mathbb{F}_2[x]$ IL POLINOMIO x^2+1 È RIDUCIBILE. INFATTI $x^2+1 = (x+1)^2$

$\Rightarrow x+1$ DIVIDE x^2+1 E $x+1 \notin \mathbb{F}_2$

b) IN $\mathbb{F}_2[x]$ OGNI POLINOMIO DI GRADO 1 È IRRIDUCIBILE. INFATTI,

$\deg(P)=1 \Rightarrow P=ax+b$ con $a,b \in K$ e $a \neq 0$ E I SUOI

DIVISORI SONO c E $c^{-1}(ax+b)$, $c \in K \setminus \{0\}$

DEFINIZIONE) SIA $a \in K$. L'ELEMENTO a È DETTO RADICE DEL POLINOMIO

$$P = \sum_{n=0}^{\deg(P)} a_n x^n \in K[x] \text{ SE } \sum_{n=0}^{\deg(P)} a_n n! = 0$$

ANCHE NELL'ANELLO $K[x]$, COME IN \mathbb{Z} , ABBIANO UN ALGORITMO DI

DIVISIONE EUCLIDEA. $f(x), g(x) \in K[x]$ POLINOMI NON NULLI $\Rightarrow \exists$ UNICO QUOTIENTE RESTO

POLINOMI $q(x), r(x) \in K[x]$ I($f(x) = g(x)q(x) + r(x) \wedge r(x) = 0$)

$\checkmark (\deg(r(x)) < \deg(q(x)))$. SEGUE IL SEGUENTE...

...TEOREMA: L'ANELLO $K[x]$ È A IDEALI PRINCIPALI. $I = \langle P(x) \rangle$

$\Rightarrow \exists$ UNICO GENERATORE MONICO DI I

DEFINIAMO IL MCD $\{f \in K[x], g \in K[x]\}$ COME L'UNICO MASSIMO

COMUN DIVISORE MONICO. (COME IN \mathbb{Z} , IL MCD SI PUÒ TROVARE CON

L'ALGORITMO DELL'EQUAZIONE DI BEZOUT.

ESEMPIO: $f(x) := x^4 - x^3 - 4x^2 + 4x + 1$; $g(x) := x^2 - x - 1$ IN

$\mathbb{Q}[x]$. ALLORA $f(x) = g(x)(x^2 - 3) + (x - 2)$ $g(x) = (x - 2)(x + 1)$

$\Rightarrow \text{MCD}(f, g) = 1$. INOLTRE $1 = g(x) - (x - 2)(x + 1) =$

$$= g(x) - [f(x) - g(x)(x^2 - 3)](x+1) = -(x+1)f(x) +$$

$$+ (x^3 + x^2 - 3x - 2)g(x)$$

PROPOSIZIONE 6a: SIA K UN CAMPO E $P(x) \in K[x]$ UN POLINOMIO

IRRIDUCIBILE. ALLORA L'ANELLO QUOTIENTE $\frac{K[x]}{(P(x))}$ È UN CAMPO.

DIM

SIA $[R] \in \frac{K[x]}{(P(x))} \setminus [0] \Rightarrow \frac{P(x)}{R(x)} \Rightarrow \text{MCD}\{f(x), P(x)\} = 1$

PERCHÉ $P(x)$ È IRRIDUCIBILE \Rightarrow IDENTITÀ DI BÉZOUT $a(x)f(x) + b(x)P(x) =$

$= 1 \Rightarrow [a(x)] = [f(x)]^{-1}$ IN $\frac{K[x]}{(P(x))}$

ESEMPI :

a) IN $\mathbb{F}_2[x]$ IL POLINOMIO $1+x+x^2$ È IRRIDUCIBILE. INFATI NON

HA RADICI IN $\mathbb{F}_2 \Rightarrow$ L'ANELLO $\frac{\mathbb{F}_2[x]}{(1+x+x^2)}$ È UN CAMPO, CHE INDIVIDIAMO

CON \mathbb{F}_4 . UN ELEMENTO DI \mathbb{F}_4 È DEL TIPO $a_0 + a_1 x$

CON $a_0, a_1 \in \mathbb{F}_2$

\cdot	0	1	x	$1+x$
0	0	0	0	0
1	0	1	x	$1+x$
x	0	x	$1+x$	1
$1+x$	0	$1+x$	1	x

$$x^{-1} = 1+x$$

b) IN $\mathbb{F}_3[x]$ IL POLINOMIO $1+x^2$ NON HA RADICI, QUINDI È IRREDUCIBILE.

INDICIAMO CON \mathbb{F}_9 IL CAMPO $\frac{\mathbb{F}_3[x]}{\langle 1+x^2 \rangle}$. I SUOI ELEMENTI SONO

DEL TIPO $a_0 + a_1x$ CON $a_1, a_3 \in \mathbb{F}_3$

.	0	1	2	x	$1+x$	$2+x$	$2x$	$1+2x$	$2+2x$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$1+x$	$2+x$	$2x$	$1+2x$	$2+2x$
2	0	2	1	$2x$	$2+2x$	$1+2x$	x	$2+x$	$1+x$
x	0	x	$2x$	2	$2+x$	$2+2x$	1	$1+x$	$1+2x$
$1+x$	0	$1+x$	$2+2x$	$2+x$	$2x$	1	$1+2x$	2	x
$2+x$	0	$2+x$	$1+2x$	$2+2x$	1	x	$1+x$	$2x$	2
$2x$	0	$2x$	x	1	$1+2x$	$1+x$	2	$2+2x$	$2+x$
$1+2x$	0	$1+2x$	$2+x$	$1+x$	2	$2x$	$2+2x$	x	1
$2+2x$	0	$2+2x$	$1+x$	$1+2x$	x	2	$2+x$	1	$2x$

TEOREMA DI RUFFINI: SIA $f(x) \in K[x]$ UN POLINOMIO NON NULLO.

$a \in K \Rightarrow$ IL RESTO DELLA DIVISIONE $f(x)/(x-a)$ È $f(a)$. IN

PARTicolARE, a È RADICE DI $f(x) \Leftrightarrow \frac{x-a}{f(x)}$ IN $K[x]$

DIM

$$f(x) = ((x-a)g(x) + r(x)) \wedge r(x)=0) \vee (\deg(r(x)) < 1)$$

$\Rightarrow r(x)$ È UN POLINOMIO COSTANTE $r(x) := c \in K$. CALCOLANDO

IN 2 SI OTTIENE $f(a) = c$

ESEMPIO: IL POLINOMIO $x^2+1 \in \mathbb{R}[x]$ NON HA RADICI IN \mathbb{R}

\Rightarrow È IRREDUCIBILE E $\frac{\mathbb{R}[x]}{\langle x^2+1 \rangle}$ È UN CAMPO, ISOMORFO A \mathbb{C} , DOVE

L'ISOMORFISMO È DATO DALL'ASSEGNAZIONE $i \mapsto i$ E $x \mapsto i$

PROPOSIZIONE: SIA K UN CAMPO. OGNI SOTTOGRUPPO FINITO DEL

GRUPPO MOLTIPLICATIVO $K \setminus \{0\}$ È CICLICO. IN PARTICOLARE, VALE CHE

K CAMPO FINITO $\Rightarrow K \setminus \{0\}$ GRUPPO CICLICO

ESEMPIO:

a) IN $\mathbb{F}_4 = \frac{\mathbb{F}_2[x]}{\langle 1+x+x^2 \rangle}$ SI HA CHE $\{x, x^2, x^3\} = \{x, 1+x, 1\} = \mathbb{F}_4 \setminus \{0\}$

$\Rightarrow x$ È UN GENERATORE DEL GRUPPO MOLTIPLICATIVO $\mathbb{F}_4 \setminus \{0\}$,

MENTRE L'ALTRO GENERATORE È $1+x$

b) IN $\mathbb{F}_9 = \frac{\mathbb{F}_3[x]}{\langle 1+x^2 \rangle}$ ABBIAMO $\langle x \rangle = \{x, x^2, x^3, x^4\} = \{x, 2, 2x, 1\}$

$\langle 1+x \rangle = \{1+x, (1+x)^2, (1+x)^3, (1+x)^4, (1+x)^5, (1+x)^6,$

$(1+x)^7, (1+x)^8\} = \mathbb{F}_9 \setminus \{0\} \Rightarrow 1+x$ GENERA IL GRUPPO

MOLTIPLICATIVO $\mathbb{F}_9 \setminus \{0\}$.

SIA $p \in \mathbb{N}$ UN NUMERO PRIMO E $n \in \mathbb{N} \setminus \{0\}$. SIA $Q(x) \in \mathbb{F}_q[x]$ UN

QUALSiasi POLINOMIO IRRIDUCIBILE DI GRADO n . DEFINIAMO IL CAMPO

$\mathbb{F}_{p^n} := \frac{\mathbb{F}_p[x]}{\langle Q(x) \rangle}$. ORA, VOGLIAMO DIMOSTRARE CHE $Q(x), Q'(x) \in \mathbb{F}_p[x]$

POLINOMI IRRIDUCIBILI DI GRADO $n \Rightarrow \frac{\mathbb{F}_p[x]}{\langle Q(x) \rangle} \cong \frac{\mathbb{F}_p[x]}{\langle Q'(x) \rangle}$ ISOMORFISMO DI CAMPI

\Rightarrow LA DEFINIZIONE DI \mathbb{F}_p È BEN POSTA A MENO DI ISOMORFISMI.

DEFINIZIONE) SIANO $F \subseteq K$ DUE CAMPI (SI DICE CHE K AMPLIA F). UN

ELEMENTO $a \in K$ SI DICE ALGEBRICO SU F SE È RADICE DI QUALCHE
SU F .

POLINOMIO NON NULLO SU F ($f(x) \in F[x]$), ALTRIMENTI SI DICE TRASCENDENTE

DATO UN AMPLIAMENTO DI CAMPI $F \subseteq K$ E $a \in K$, SI CONSIDERI IL MORFISMO

DI ANELLI $v_a: F[x] \rightarrow K$
 $f(x) \mapsto f(a)$. $\text{Ker}(v_a)$ È L'IDEALE DI $F[x]$

COSTRUITO DAI POLINOMI CHE SI ANNULLANO IN $a \Rightarrow a$ È ALGEBRICO

SU $F \Leftrightarrow \text{Ker}(v_a)$ È UN IDEALE NON NULLO DI $F[x]$ POICHÉ $F[x]$ È AD

IDEALI PRINCIPALI $\text{Ker}(v_a) = \langle m(x) \rangle$, DOVE $m(x)$ È L'UNICO POLINOMIO

MONICO DI GRADO MINIMO IN $\text{Ker}(v_a)$.

DEFINIZIONE) SE $a \in K$ È ALGEBRICO SU F , IL POLINOMIO $m(x)$ DEFINITO

SOPRA SI CHIAMA POLINOMIO MINIMO DI a SU F . SE $\deg(m(x)) = n$, a

SI DICE ALGEBRICO DI GRADO n .

NOTA: SIA $a \in K$ E $P(x) \in F[x] \setminus \{0\}$ P(a) = 0. ALLORA $P(x)$ È IL POLINOMIO MINIMO DI a SU $F \Leftrightarrow P(x)$ È MONICO E IRREDUCIBILE.

ESEMPIO: SI CONSIDERI L'AMPLIAMENTO $\mathbb{R} \subseteq \mathbb{C}$. ALLORA $1+x^2 \in \mathbb{R}[x]$ È IL POLINOMIO MINIMO DI $i \in \mathbb{C}$ SU \mathbb{R} .

PROPOSIZIONE: SIA $F \subseteq K$ UN AMPLIAMENTO DI CAMPI E $a \in K$. SI CONSIDERI IL MORFISMO DI ANELLI $v_a: F[x] \rightarrow K$. ALLORA $\text{Im}(v_a)$ È IL PIÙ PICCOLO SOTTOANELLO DI K CONTENENTE SIA F CHE a

DIM

SI OSSERVI CHE L'IMMAGINE DI UN MORFISMO DI ANELLI È UN SOTTOANELLO DI K . SIA $c \in F$ E SI CONSIDERI IL POLINOMIO COSTANTE $c \in F[x]$. ALLORA

$v_a(c) = c \Rightarrow F \subseteq \text{Im}(v_a)$. D'AUTRA PARTE, PER CHIUSURA ADDITIVA E

$\text{Im}(v_a)$

MOLTIPLICATIVA OGNI SOTTOANELLO DI K CONTENENTE SIA F CHE a CONTIENE

SIA $F \subseteq K$ UN AMPLIAMENTO DI CAMPI E $a \in K$. IL PIÙ PICCOLO SOTOCAMPO

DI K CONTENENTE SIA F CHE a SI CHIAMA AMPLIAMENTO DI F IN K GENERATO

DA a E SI INDICA CON $F(a)$. QUESTO È DETTO AMPLIAMENTO SEMPLICE

POICHÉ GENERATO DA UN SOLO ELEMENTO a .

COROLLAIO: SIA $F \subseteq K$ UN AMPLIAMENTO DI CAMPI E $a \in K$. ALLORA

$$F(a) = \{ f_1(a) f_2(a)^{-1} \mid f_1(x), f_2(x) \in F[x] \wedge f_2(a) \neq 0 \}$$

DIM

PER LA PROPOSIZIONE PRECEDENTE, IL PIÙ PICCOLO SOTTOANELLO DI K CONTENENTE SIA F CHE α È $\text{Im}(\psi_\alpha) = \{f(x) | f(x) \in F[x]\}$. PRENDENDO

CUI INVERSI IN K SI VERIFICA LA TESI

SE α È ALGEBRICO SU F , SI HA CHE $\text{Im}(\psi_\alpha) \cong \frac{F[x]}{\langle m(x) \rangle}$, DOVE $m(x)$

È IL POLINOMIO MINIMO DI $\alpha \Rightarrow \text{Im}(\psi_\alpha)$ È UN CAMPO E $F(\alpha) = \text{Im}(\psi_\alpha)$. SE

n È IL GRADO DI α , SI HA $F(\alpha) = \{c_0 + c_1\alpha + \dots + c_{n-1}\alpha^{n-1} \mid c_i \in F\}$

ESEMPIO: SI CONSIDERI L'AMPLIAMENTO $\mathbb{Q} \subseteq \mathbb{R}$. L'ELEMENTO $\sqrt{2} \in \mathbb{R} \setminus \mathbb{Q}$

È ALGEBRICO SU \mathbb{Q} CON POLINOMIO MINIMO $x^2 - 2 \Rightarrow \sqrt{2}$ HA GRADO 2 SU

\mathbb{Q} E $\mathbb{Q}(\sqrt{2}) = \{c_0 + c_1\sqrt{2} \mid c_0, c_1 \in \mathbb{Q}\}$

ADESSO MOSTRIAMO CHE IL CAMPO \mathbb{F}_{p^n} È UN AMPLIAMENTO SEMPLICE

DEL CAMPO \mathbb{F}_p

PROPOSIZIONE: SIA $\alpha \in \mathbb{F}_{p^n}$ UN GENERATORE DEL GRUPPO MOLTIPLICATIVO

$\mathbb{F}_{p^n} \setminus \{0\}$. ALLORA $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$

DIM

$\mathbb{F}_p(\alpha)$ È IL PIÙ PICCOLO SOTOCAMPO DI \mathbb{F}_{p^n} CONTENENTE SIA \mathbb{F}_p CHE

$\alpha \Rightarrow \mathbb{F}_p(\alpha) \subseteq \mathbb{F}_{p^n}$. POICHÉ α GENERA IL GRUPPO MOLTIPLICATIVO

$\mathbb{F}_{p^n} \setminus \{0\}$, SI HA CHE $\mathbb{F}_{p^n} \subseteq \mathbb{F}_p(\alpha)$

ADESSO, SE $P(x)$, $Q(x)$ SIFP $[x]$ SONO DUE POLINOMI IRREDUCIBILI DI GRADO n , VOGLIAMO COSTRUIRE UN ISOMORFISMO $\rho: \frac{F_P[x]}{\langle P(x) \rangle} \rightarrow \frac{F_Q[x]}{\langle Q(x) \rangle}$

PROPOSIZIONE: SIANO $F \subseteq K$ E $F' \subseteq K'$ AMPIAMENTI DI CAMPI. SE $\alpha \in K$

È ALGEBRICO DI GRADO n SU F , CON POLINOMIO MINIMO $m(x)$, ESISTE

UN MORFISMO DI CAMPI $\varphi: F(\alpha) \rightarrow K'$ CHE FISSA $F \Leftrightarrow m(x)$ HA UNA

RADICE IN K' . IN QUESTO CASO I MORFISMI φ SONO TANTI QUANTI LE RADICI

DISTINTE β_1, \dots, β_s DI $m(x)$ IN K' E SONO TUTTI E SOLI QUELLI DEFINITI DA

$$c_0 + c_1 \alpha + \dots + c_{n-1} \alpha^{n-1} \mapsto c_0 + c_1 \beta_i + \dots + c_{n-1} \beta_i^{n-1}$$

DIM

SE α È ALGEBRICO DI GRADO n SU F , CON POLINOMIO MINIMO $m(x)$ E

$\varphi: F(\alpha) \rightarrow K'$ È UN MORFISMO ALLORA $0 = \varphi(0) = \varphi(m(\alpha)) = m(\varphi(\alpha))$

$\Rightarrow \varphi(\alpha)$ DEVE ESSERE RADICE DI $m(x)$ IN K' . VICEVERSA, SIA β UNA

RADICE DI $m(x)$ IN K' E CONSIDERANO IL MORFISMO DI ANELLI $\pi_B: \frac{F[x]}{\langle m(x) \rangle} \xrightarrow{\varphi} K'$

POLCHE' $m(x) \in \text{Ker}(\pi_B)$, DAL TEOREMA DI ISOMORFISMO PER ANELLI

ABBIAMO IL DIAGRAMMA COMMUTATIVO

INFATTI $\text{Ker}(\pi_B) = \langle m(x) \rangle$, ESSEMPO

$$\begin{array}{ccc} F[x] & \xrightarrow{\varphi_B} & K' \\ \pi \downarrow & \nearrow \varphi & \\ F(\alpha) \cong \frac{F[x]}{\langle m(x) \rangle} & & \end{array}$$

$m(x)$ IRREDUCIBILE \Rightarrow ABBIAMO UN MORFISMO INIETTIVO $\varphi: F(\alpha) \rightarrow K'$ CHE

SODDISFA LE PROPRIETÀ DELL'ENUNCIATO



SIA F UN CAMPO E $f(x) \in F[x]$ UN POLINOMIO DI GRADO $n \geq 1$. UN

CAMPO K , AMPLIAMENTO DI F , SI DICE CAMPO DI SPEZZAMENTO DI $f(x)$ SU

F SE $f(x)$ FATTORIZZA IN POLINOMI DI GRADO ≤ 1 SU $K[x]$ E NON CI

SONO CAMPI INTERMEDI $F \subseteq L \subseteq K$ CON QUESTA PROPRIETÀ

ESEMPI:

- $(\mathbb{Q}(\sqrt{2}))$ È UN CAMPO DI SPEZZAMENTO DI $x^2 - 2 \in \mathbb{Q}[x]$
- \mathbb{C} È UN CAMPO DI SPEZZAMENTO DI $x^2 + 1 \in \mathbb{R}[x]$

ADESSO VOGLIAMO MOSTRARE CHE UN CAMPO DI CARDINALITÀ p^n È UN

CAMPO DI SPEZZAMENTO DEL POLINOMIO $x^{p^n} - x \in \mathbb{F}_p[x]$.

INFATI, SE K È UN CAMPO DI CARDINALITÀ p^n , ALLORA IL SUO GRUPPO

MOLTIPLICATIVO K^\times HA CARDINALITÀ $p^n - 1 \Rightarrow d^{p^n} - 1$ DA K^\times

\Rightarrow OGNI ELEMENTO DI K È RADICE DEL POLINOMIO $x^{p^n} - x$. PER IL

TEOREMA DI RUFFINI, K È UN CAMPO DI SPEZZAMENTO DEL POLINOMIO

$x^{p^n} - x$. ADESSO MOSTRIAMO CHE OGNI POLINOMIO DI GRADO n IRREDUCIBILE

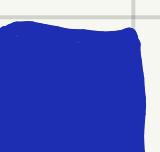
IN $\mathbb{F}_p[x]$ DIVIDE $x^{p^n} - x \in \mathbb{F}_p[x]$

PROPOSIZIONE 7: TUTTI E SOLI I POLINOMI IRREDUCIBILI SU \mathbb{F}_p DI GRADO n

SONO I FATTORI IRREDUCIBILI DI GRADO n DI $x^{p^n} - x \in \mathbb{F}_p[x]$

DIM

SIA $P(x) \in F_p[x]$ IRREDUCIBILE DI GRADON $\in K := \frac{IF_p[x]}{\langle P(x) \rangle}$. ALLORA K HA p^n ELEMENTI CHE SONO LE RADICI DI $x^{p^n} - x \in K[x]$. POICHÉ $y \in K$ È UNA RADICE $P(x) \in K[x]$, $P(x) \in x^{p^n} - x$ HANNO UNA RADICE COMUNE IN $K \Rightarrow$ PER IL TEOREMA DI RUFFINI HANNO UN FATTORE COMUNE $x - y$ IN $K[x]$ \Rightarrow POICHÉ $IF_p \subseteq K$ E IL MCD IN $IF_p[x]$ È LO STESSO CHE IN $K[x]$, $P(x) \in x^{p^n} - x$ HANNO UN MCD $\neq 1$ IN $IF_p[x]$. POICHÉ $P(x)$ È IRREDUCIBILE IN $IF_p[x]$, $P(x)$ DIVIDE $x^{p^n} - x$



PROPOSIZIONE 6b: COSTRUZIONE DI UN ISOMORFISMO DI CAMPI

$f: \frac{IF_p[x]}{\langle P(x) \rangle} \rightarrow \frac{IF_p[x]}{\langle Q(x) \rangle}$ DOVE $P(x), Q(x) \in IF_p[x]$ SONO MONICI IRREDUCIBILI DI GRADO n

BASTA COSTRUIRE UN MORFISMO DI ANELLI. INFATI, UN MORFISMO DI ANELLI

CHE SONO CAMPI È INIEZIONE. INFATI, $|\frac{IF_p[x]}{\langle P(x) \rangle}| = |\frac{IF_p[x]}{\langle Q(x) \rangle}| = p^n \Rightarrow$ IL

MORFISMO È BIUNIVOCO, OSSIA È UN ISOMORFISMO.

SI HA CHE $y \in \frac{IF_p[x]}{\langle P(x) \rangle} \Rightarrow P(x) \in IF_p[x]$ È IL POLINOMIO MINIMO DI y SU IF_p

\Rightarrow SE $P(x)$ HA UNA RADICE IN $\frac{IF_p[x]}{\langle Q(x) \rangle}$ POSSIAMO USARE LA PROPOSIZIONE

SULL'ESTENSIONE DI MORFISMI DI CAMPI PER DEFINIRE IL MORFISMO \bar{f} , CHE

SARÀ UN ISOMORFISMO. INFATI, $IF_p \subseteq \frac{IF_p[x]}{\langle P(x) \rangle}$ E $IF_p \subseteq \frac{IF_p[x]}{\langle Q(x) \rangle}$. INFATI

$\frac{IF_p[x]}{\langle P(x) \rangle} = IF_p[[x]]$, DOVE $[x]$ È LA CLASSE DI x IN $\frac{IF_p[x]}{\langle P(x) \rangle}$.

Poiché $\frac{\text{IFP}[x]}{\text{LQ}[x]}$ è un campo di spezzamento di $x^{p^n} - x \in \text{P}[x]$

DIVIDE $x^{p^n} - x \Rightarrow \text{P}[x]$ si fattorizza in fattori di grado 1 sul campo

IFP. SIA $\beta \in \frac{\text{IFP}[x]}{\text{LQ}[x]} \mid \text{P}(\beta) = 0$. ALLORA L'ASSEGNAZIONE

$c_0 + c_1 x + \dots + c_{n-1} x^{n-1} \mapsto c_0 + c_1 \beta + \dots + c_{n-1} \beta^{n-1}$ DEFINISCE UN

MORFISMO DI ANELLI $f: \frac{\text{IFP}[x]}{\text{LQ}[x]} \rightarrow \frac{\text{IFP}[x]}{\text{LQ}[x]}$

ESEMPIO: IN $\text{IF}_3[x]$ SI CONSIDERINO I POLINOMI IRREDUCIBILI $x^2 + 1$ E

$x^2 + x + 2$. IL POLINOMIO MINIMO DI $x \in \frac{\text{IF}_3[x]}{\text{LQ}[x]} =: K$ SU IF_3 È $x^2 + 1$.

IN $K':= \frac{\text{IF}_3[y]}{\text{LQ}[y+2]}$ SI HA CHE $x^2 + 1 = (x+y+2)(x+y+1) \Rightarrow$ IN $K'[x]$,

$x^2 + 1$ HA LE DUE RADICI $-y-2 = 2y+1$ E $y+2 = -2y-1$. ABBIAMO,

QUINDI, DUE ISOMORFISMI $f: \begin{array}{c} K \\ \longrightarrow \\ a_0 + a_1 x \end{array} \mapsto \begin{array}{c} K' \\ \longrightarrow \\ a_0 + a_1(2y+1) \end{array}$ E

$g: \begin{array}{c} K \\ \longrightarrow \\ a_0 + a_1 x \end{array} \mapsto \begin{array}{c} K' \\ \longrightarrow \\ a_0 + a_1(y+2) \end{array}$