Università degli Studi di Roma "Tor Vergata"

CdL in Matematica

ALGEBRA 2

prof. Fabio GAVARINI

a.a. 2024–2025

Esame scritto del 30 Giugno 2025 — 2° appello, sessione estiva

N.B.: compilare il compito in modo sintetico ma **esauriente**, *spiegando chiaramente quanto si fa, e scrivendo in corsivo con grafia leggibile.*

. . . . . * . . . . . .

[1] — Si consideri l'anello quoziente

$$A := \mathbb{Z}[x,y] \Big/ \left(x\,(y+6) - 3\,x^2 + x + 2\,, 4\,x - y - 7 \right)$$

(a) Dimostrare che A non è un campo.

(b) Dimostrare che A è un dominio euclideo.

[2] — Determinare il numero di anagrammi distinti della parola

"TRATTORIA"

[3] — Sia G un gruppo finito, e sia $\Gamma := \mathrm{Aut}_{\mathcal{G}}(G)$ il suo gruppo degli automorfismi. Il gruppo Γ agisce naturalmente su G; supponiamo che per tale azione esistano soltanto due Γ–orbite in G.

(a) Dimostrare che tutti gli elementi di G diversi dall'elemento neutro hanno lo stesso ordine.

(b) Dimostrare che G è un p–gruppo (per un qualche primo p).

(c) Dimostrare che G è un gruppo abeliano.

(d) Dimostrare che G è isomorfo al gruppo $\mathbb{Z}_p^n := \underbrace{\mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}_{n}$, per un certo $n \in \mathbb{N}$, con p primo come in *(b)*.

(e) Dimostrare che $\Gamma := \mathrm{Aut}_{\mathcal{G}}(G) \cong GL_n(\mathbb{Z}_p)$.

[4] — Sia G un gruppo di ordine 70.

(a) Determinare tutti i valori di $d \in \mathbb{N}_+$ per i quali esista un sottogruppo H in G che abbia ordine d.

(b) Determinare tutti i valori di $t \in \mathbb{N}_+$ per i quali esista un sottogruppo normale N in G che abbia ordine t.

[5] — Sia p un primo, $\mathbb{Z}_p$ il campo con p elementi, $\mathbb{Z}_p(y)$ il campo delle funzioni razionali in y a coefficienti in $\mathbb{Z}_p$, sia $\mathbb{Z}_p[x\,,y]$ l'anello dei polinomi in x e y a coefficienti in $\mathbb{Z}_p$, e infine sia $\mathbb{K} := \big(\mathbb{Z}_p(y)\big)[x]\Big/\big(x^p - y\big)$.

(a) Dimostrare che $\mathbb{K}$ è un campo.

(b) Determinare il grado dell'estensione $\mathbb{K}\Big/\mathbb{Z}_p(y)$.

(c) Determinare il grado dell'estensione $\mathbb{K}\Big/\mathbb{Z}_p$.

(d) Dimostrare che il gruppo di Galois dell'estensione $\mathbb{K}\Big/\mathbb{Z}_p(y)$ è banale, cioè $Gal\Big(\mathbb{K}\Big/\mathbb{Z}_p(y)\Big) = \{\mathrm{id}_{\mathbb{K}}\}$.

"ALGEBRA 2"

2024/2025 (F. GAVARINI)

— ∘ —

COMPITO SCRITTO DEL 30/06/2025

— 2° APPELLO —

— ∘ —

1 Sia $A := \dfrac{\mathbb{Z}[x,y]}{(x(y+6)-3x^2+x+2,\ 4x-y-7)}$

(a) Dimostrare che A non è un campo.

(b) Dimostrare che A è un dominio euclideo.

Soluzione: Risolviamo i due problemi posti dando una descrizione alternativa di A, tramite applicazioni ripetute dei vari Teoremi di Isomorfismo. Abbiamo

$$A := \frac{\mathbb{Z}[x,y]}{(x\cdot(y+6)-3x^2+x+2,\ 4x-y-7)} \cong$$

$$\cong \frac{\mathbb{Z}[x,y]/(4x-y-7)}{(x\cdot(y+6)-3x^2+x+2,\ 4x-y-7)/(4x-y-7)} \cong$$

$$\cong \frac{\mathbb{Z}[x]}{(x\cdot(4x-7+6)-3x^2+x+2,\ 0)} =$$

$$= \frac{\mathbb{Z}[x]}{(x^2+2)} \cong \mathbb{Z}[\sqrt{-2}]$$

$$(\bar{x} \longleftrightarrow \sqrt{-2})$$

cioè

$$\boxed{A \cong \mathbb{Z}[\sqrt{-2}]}$$

e sappiamo che:

(I) $\mathbb{Z}[\sqrt{-2}]$ è dominio euclideo, con valutazione $(\forall (a+b\sqrt{-2}) \in \mathbb{Z}[\sqrt{-2}])$

$$v(a+b\sqrt{-2}) := a^2+2b^2$$

(II) $\mathbb{Z}[\sqrt{-2}]$ non è un campo, ad esempio perché il suo gruppo degli invertibili è

$$U(\mathbb{Z}[\sqrt{-2}]) = \{+1, -1\}$$

e quindi non è $\mathbb{Z}[\sqrt{-2}] \setminus \{0\}$

QUINDI si conclude che

(a) è provata da (II),

(b) è provata da (I). □

---

2 Determinare il numero di anagrammi distinti della parola "TRATTORIA"

Soluzione:

Gli anagrammi considerati sono le parole che si ottengono da "TRATTORIA" permutandone le lettere. Tali lettere sono 9, quindi stiamo considerando l'azione del gruppo simmetrico S_9 (su 9 elementi) sull'insieme delle parole di 9 lettere nell'alfabeto $A := \{A, B, C, \dots, Z\}$, cioè l'insieme $A^{\times 9} = \underbrace{A \times A \times \cdots \times A}_{9}$. In questo

linguaggio, gli anagrammi di una parola π in A^{*g} sono esattamente tutti e soli gli elementi dell'orbita di π in A^{*g} sotto l'azione di S_g, cioè $\mathcal{O}_\pi = S_g \cdot \pi$

In particolare

$$N := \#(\text{anagrammi di } \pi) = |\mathcal{O}_\pi| = |S_g \cdot \pi| = \frac{|S_g|}{|St_\pi^{S_g}|} \quad (1)$$

dove

$$St_\pi^{S_g} := \text{stabilizzatore di } \pi \text{ in } S_g = \{\sigma \in S_g \mid \sigma \cdot \pi = \pi\}$$

Per $\pi :=$ "TRATTORIA", lo stabilizzatore è dato dalle $\sigma \in S_g$ che scambiano tra loro lettere uguali, cioè

- le 3 "T" tra loro (in posizioni 1, 4, 5)
- le 2 "R" tra loro (in posizioni 2, 7)
- le 2 "A" tra loro (in posizioni 3, 9)

QUINDI è

$$\mathcal{H}^{S_9}_{\text{TRATTORIA}} = S_{\{1,4,5\}} \cdot S_{\{2,7\}} \cdot S_{\{3,9\}} =$$

$$= S_{\{1,4,5\}} \times S_{\{2,7\}} \times S_{\{3,9\}} \cong$$

$$\cong S_3 \times S_2 \times S_2$$

Ne segue che

$$\left| \mathcal{H}^{S_9}_{\text{TRATTORIA}} \right| = \left| S_3 \times S_2 \times S_2 \right| = \tag{2}$$

$$= |S_3| \cdot |S_2| \cdot |S_2| = 3! \cdot 2! 2! = 24$$

e quindi da (1) e (2) otteniamo

$$N := \frac{|S_9|}{\left| \mathcal{H}^{S_9}_{\text{TRATTORIA}} \right|} = \frac{9!}{3!2!2!} = \binom{9}{3,2,2}$$

che è il numero richiesto. □

(CONTINUA...)

3 Sia G un gruppo finito, e $\Gamma := Aut_g(G)$, che agisce naturalmente su G. Supponiamo che per tale azione esistono soltanto due Γ-orbite in G.

(a) Dimostrare che tutti gli elementi di G diversi dall'elemento neutro 1_G hanno lo stesso ordine.

(b) Dimostrare che G è un p-gruppo, per un qualche primo p.

(c) Dimostrare che G è un gruppo abeliano.

(d) Dimostrare che G è isomorfo a $\mathbb{Z}_p^n := \underbrace{\mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}_{n}$ per un certo $n \in \mathbb{N}$ con p primo come in (b).

(e) Dimostrare che $\Gamma := Aut_g(G) \cong GL_n(\mathbb{Z}_p)$.

Soluzione:

(a) Sia $\mathcal{O}_{1_G}$ la Γ-orbita in G dell'elemento neutro 1_G, cioè $\mathcal{O}_{1_G} = \{\varphi(1_G) \mid \varphi \in Aut_g(G) =: \Gamma\}$

Siccome $\varphi(1_G) = 1_G \quad \forall \varphi \in Aut_g(G)$, se

conclude che $\mathcal{O}_{1_G} = \{1_G\}$.

Detta $\mathcal{O}_+$ la seconda Γ-orbita in G, si ha

$$G = \mathcal{O}_{1_G} \amalg \mathcal{O}_+ \quad \left(\begin{array}{c}\text{unione}\\ \text{disgiunta}\end{array}\right)$$

quindi

$$\mathcal{O}_+ = G \setminus \mathcal{O}_{1_G} = G \setminus \{1_G\}$$

cioè tutti gli elementi di G diversi da 1_G formano un'unica Γ-orbita, che è appunto $\mathcal{O}_+$. In particolare,

$\forall\, g', g'' \in G \setminus \{1_G\}$ si ha

$g', g'' \in \mathcal{O}_+$, quindi

$$\exists\ \varphi \in \Gamma := Aut_g(G) : \ g'' = \varphi(g') \qquad (3)$$

MA φ è automorfismo di G, quindi preserva l'ordine degli elementi di G, cioè $\omega(\varphi(g)) = \omega(g)$ $\forall g \in G$, dove

$\omega(x) :=$ ordine di x $\quad (\forall x \in G)$

perciò dalla (3) segue che

$$\omega(g'') = \omega(\varphi(g')) = \omega(g')$$

$\forall\, g', g'' \in G \setminus \{1_G\}$, q.e.d.

(b) Se $|G|=1$, tutto l'enunciato è banale.

Se $|G|>1$, per ogni primo p che divide $|G|$ esiste un $g \in G : \omega(g)=p$, per il Teorema di Cauchy. Allora da (a) segue che $\exists!$ primo $p : p \mid |G|$, e quindi

G è un p-gruppo, q.e.d.

(c) Siccome G è un p-gruppo finito -per (b)- si ha $Z(G) \neq \{1_G\}$, in particolare $Z(G) \setminus \{1_G\} \neq \emptyset$, quindi $\exists\ z \in Z(G) \cap \mathcal{O}_+$, con $\mathcal{O}_+$ la Γ-orbita di tutti gli elementi in $G \setminus \{1_G\}$, come visto in (a). Allora

$\forall\, g \in G \setminus \{1_G\}$ si ha $g, z \in \mathcal{O}_+$, $\Rightarrow$

$\Rightarrow \exists\ \varphi \in Aut_g(G) : \quad g = \varphi(z) \qquad (4)$

MA $Z(G)$ è sottogruppo caratteristico di G, cioè $\varphi(Z(G)) = Z(G)\ \ \forall \varphi \in Aut_g(G)$

QUINDI la (4) dà $g = \varphi(z) \in Z(G)$ $\forall\, g \in G \setminus \{1_G\}$

Si conclude allora che $Z_i(G) = G$ cioè G è abeliano, q.e.d.

(ol) Dai punti (b+c) sappiamo che G è un p-gruppo abeliano finito. Ora, dal Teorema di classificazione per questo tipo di gruppi sappiamo che $\exists\ e_1 \geq \cdots \geq e_n > 0$ t.c.

$$G \cong \mathbb{Z}_{p^{e_1}} \times \cdots \times \mathbb{Z}_{p^{e_n}}$$

Se fosse $e_1 > 1$, avremmo nel gruppo ciclico $\mathbb{Z}_{p^{e_1}}$ - e quindi poi in G - un elemento di ordine p (p.es., la classe $[p^{e_1-1}]_p$) e uno di ordine p^2 (p.es., la classe $[p^{e_1-2}]_p$); ma per il punto (a) questo è impossibile, quindi dev'essere $e_1 = 1$, e allora anche $e_1 = e_2 = \cdots = e_n = 1$, così che

$$G \cong \underbrace{\mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}_{n}, \quad \text{q.e.d.}$$

(e) Sappiamo che $\mathbb{Z}_p^n$ è gruppo abeliano

per $\underline{a} + \underline{b} := (a_1 + b_1, \dots, a_n + b_n)$

$\forall\ \underline{a} = (a_1, \dots, a_n),\ \underline{b} = (b_1, \dots, b_n) \in \mathbb{Z}_p^n$

ma $\mathbb{Z}_p^n$ è anche spazio vettoriale su $\mathbb{Z}_p$

con la somma come sopra e la

moltiplicazione per uno scalare

$$c \cdot \underline{a} := (c a_1, \dots, c a_n), \quad \forall c \in \mathbb{Z}_p,\ \forall \underline{a} \in \mathbb{Z}_p^n$$

Sia $Aut_v(\mathbb{Z}_p^n) := \left\{ \begin{array}{l} \text{automorfismi di } \mathbb{Z}_p^n \\ \text{come spazio vettoriale} \end{array} \right\}$

Ogni $\psi \in Aut_v(\mathbb{Z}_p^n)$ preserva la somma, quindi $\psi \in Aut_g(\mathbb{Z}_p^n) = \left\{ \begin{array}{l} \text{automorf.} \\ \text{di } \mathbb{Z}_p^n \\ \text{come} \\ \text{gruppo} \end{array} \right.$

e così $Aut_v(\mathbb{Z}_p^n) \leq Aut_g(\mathbb{Z}_p^n)$

MA $\forall\ c = [z]_p \in \mathbb{Z}_p$ si ha anche $(\forall z > 0)$

$$\underbrace{\underline{a} + \dots + \underline{a}}_{z} = \underline{0} = \underbrace{0_{\mathbb{Z}_p}\ \underline{a}}_{\mathbb{Z}} := \text{potenza additiva } 0\text{-esima}$$

$$c \cdot \underline{a} = [z]_p \cdot \underline{a} = z\ \underline{a} := \text{potenza additiva } z\text{-esima}$$

e ogni automorfismo di gruppo preserva le potenze, perciò si ha

$$\varphi(c.\underline{a}) = c.\varphi(\underline{a}) \qquad \forall c \in \mathbb{Z}_p,\ \forall \underline{a} \in \mathbb{Z}_p^n$$

$\forall\ \varphi \in Aut_g(\mathbb{Z}_p^n)$,

CIOÈ ogni automorfismo ("additivo") φ di $(\mathbb{Z}_p^n; +)$ è anche $\mathbb{Z}_p$-lineare, cioè $\varphi \in Aut_v(\mathbb{Z}_p^n)$

DUNQUE è $\boxed{Aut_g(\mathbb{Z}_p^n) = Aut_v(\mathbb{Z}_p^n)}$

INFINE $G \cong \mathbb{Z}_p^n \Rightarrow \Gamma := Aut_g(G) \cong Aut_g(\mathbb{Z}_p^n)$

e $\underline{Aut_v(\mathbb{Z}_p^n) \cong GL_n(\mathbb{Z}_p)}$

(fissando una base in $\mathbb{Z}_p^n$)

e quindi componendo isomorfismi e identità si ha

$\underline{\Gamma := Aut_g(G) \cong GL_n(\mathbb{Z}_p)}$, q.e.d.

(CONTINUA...)

4 Sia G un gruppo di ordine 70.

(a) Determinare tutti i $d \in \mathbb{N}_+$ t.c. $\exists\ H \leq G$ con $|H| = d$.

(b) Determinare tutti i $t \in \mathbb{N}_+$ t.c. $\exists\ N \trianglelefteq G$ con $|N| = t$.

Soluzione:

In entrambi i casi, per il Teorema di Lagrange deve essere

$$d = |H| \,\big|\, |G| = 70 \Rightarrow d \mid 70$$

& $$t = |N| \,\big|\, |G| = 70 \Rightarrow t \mid 70$$

QUINDI $d, t \in \mathrm{Div}(70) := \{\text{divisori di } 70\} =$

$$= \{1, 2, 5, 7, 10, 14, 35, 70\}$$

Analizziamo i vari casi.

$d = 1$ $\exists\ H_1 := \{1_G\} \leq G : |H_1| = 1$

& anche $H_1 \trianglelefteq G$, ovvero è anche

$$N_1 = H_1 := \{1_G\} : N_1 \trianglelefteq G \ \&\ |N_1| = 1$$

QUINDI $\underline{b = 1}$ va bene per (a)

& $\underline{b = 1}$ va bene per (b).

$\boxed{d \in \{2, 5, 7\}}$ Ogni valore $d \in \{2, 5, 7\}$ è un primo che divide $720 = |G|$, quindi per il Teorema di Cauchy

$\exists\, g \in G : \omega(g) := \text{ordine di } g = d$

e allora $H_d := \langle g \rangle \cong \mathbb{Z}_d$ è un $H_d \leq G : |H_d| = d$

Perciò $d \in \{2, 5, 7\}$ sono valori di d che vanno bene per (a).

INOLTRE, dato primo d è anche la massima potenza di d (primo) che divide G, quindi $\forall\, d \in \{2, 5, 7\}$ si ha H_d è un d-Sylow di G.

Già $\nu_d := \#(d\text{-Sylow in } G)$

Dalla teoria generale abbiamo che

$$\nu_2 \in (1+2\mathbb{N}) \cap \mathrm{Div}(70/2) = \{1,5,7,35\}$$

$$\nu_5 \in (1+5\mathbb{N}) \cap \mathrm{Div}(70/5) = \{1\}$$

$$\nu_7 \in (1+7\mathbb{N}) \cap \mathrm{Div}(70/10) = \{1\}$$

QUINDI $\boxed{\nu_5 = 1}$ & $\boxed{\nu_2 = 1}$

$\Downarrow$ $\Downarrow$

$\exists!$ 5-Sylow H_5 in G, e come tale è normale, cioè $H_5 \trianglelefteq G$

$\exists!$ 7-Sylow H_7 in G, e come tale è normale, cioè $H_7 \trianglelefteq G$

PERCIÒ $t \in \{5,7\}$ sono valori di t che vanno bene per (b).

INVECE $t = 2$ non va bene per (b), in generale: ad esempio per il gruppo diedrale

$$G = D_{35} \cong \mathbb{Z}_2 \ltimes \mathbb{Z}_{35}$$

si ha $\nu_2 = 35$, cioè $\exists$ 35 diversi 2-Sylow, cioè sottogruppi H_2 di ordine 2 (ne $\exists!$ per ciascun ribaltamento in D_{35}), e nessuno di essi è normale.

$d = 35$ Sappiamo che in G

$\exists!\ H_5 \trianglelefteq G$, $\exists!\ H_7 \trianglelefteq G$ con

$|H_5| = 5$ & $|H_7| = 7$.

Allora $H_5 \cdot H_7 = H_7 \cdot H_5$ e tale sottoinsieme è sottogruppo di G; inoltre $\forall g \in G$ si ha

$$g \cdot (H_5 \cdot H_7) \cdot g^{-1} = g H_5 g^{-1} \cdot g H_7 g^{-1} = H_5 \cdot H_7$$

perché $H_5 \trianglelefteq G$ e $H_7 \trianglelefteq G$, quindi $H_5 \cdot H_7 \trianglelefteq G$, cioè $H_5 \cdot H_7$ è (anche) normale. Infine, H_5 e H_7 hanno ordine (5 e 7) primi tra loro, perciò $H_5 \cap H_7 = \{1_G\}$ - per il Teorema di Lagrange.

$$|H_5 \cdot H_7| = |H_5 \times H_7| = |H_5| \cdot |H_7| = 5 \cdot 7 = 35$$

dunque $N_{35} := H_{35} := H_5 \cdot H_7 \trianglelefteq G$

ha ordine $|N_{35}| = |H_{35}| = 35$

così $d = 35 = 5 \cdot 7$ è un valore che va bene per (a) e per (b).

$d \in \{10, 14\}$ Sia $k \in \{5, 7\}$; sappiamo allora che $\exists!\ H_k = N_k \trianglelefteq G : |N_k| = k$

Inoltre $\exists\ H_2 \leq G : |H_2| = 2$.

Allora $H_2 \cdot N_k = N_k \cdot H_2$ e tale sottoinsieme è un sottogruppo di G.

Siccome $|H_2| = 2$ e $|N_k| = k$ sono primi tra loro, il Teorema di Lagrange ci dà $H_2 \cap N_k = \{1_G\}$, da cui segue che $|H_2 \cdot N_k| = |H_2 \times N_k| = |H_2| \cdot |N_k|$

$\|$

$2 \cdot k = d$

QUINDI

$H_{2k} = H_d := H_2 \cdot N_k = H_2 \cdot N_{d/2}$

è un sottogruppo di G di ordine $2k = d$

così $d = 2k \in \{10, 14\}$ sono valori di d che vanno bene per (a)

INVECE i valori $t \in \{10, 14\}$ non vanno bene per (b), in generale.

Ad esempio, per il gruppo diedrale

$$G := D_{35} \cong \mathbb{Z}_2 \ltimes \mathbb{Z}_{35}$$

sia $k := d/2 \in \{5, 7\}$; prendiamo una rotazione in D_n di ordine k, che sarà $\rho^{35/k}$, se ρ è una "rotazione elementare", cioè di ordine $\omega(\rho) = 35$ e sia σ un ribaltamento in D_n (così $\omega(\sigma) = 2$) - N.B.: nell'isomorfismo $D_n \cong \mathbb{Z}_2 \ltimes \mathbb{Z}_{35}$ si avrà

$\rho^{35/k} \longleftrightarrow ([0]_2, [35/k]_{35})$ e $\sigma \longleftrightarrow ([1]_2, [0]_{35})$

ALLORA $H_{d=2k} := \langle \rho^{35/k}, \sigma \rangle$ è un sottogruppo di D_{35} ordine $d = 2k$, realizzato come sopra - è proprio $H_{35} = H_k \cdot H_2$, con $H_k = \langle \rho^{35/k} \rangle$ e $H_2 = \langle \sigma \rangle$ - e da $H_2 \not\subseteq D_{35}$ segue che $H_{d=2k} \not\subseteq D_{35}$.

d = 70 Ovviamente $H_{70} := G =: N_{70}$

è sottogruppo normale di G di ordine 70,

quindi $d = 70$ va bene per (a)

& $t = 70$ va bene per (b). □

---

5 Sia p un primo, e sia

$$\mathbb{K} := \frac{(\mathbb{Z}_p(y))[x]}{(x^p - y)}$$

(a) Dimostrare che $\mathbb{K}$ è un campo.

(b) Determinare il grado $[\mathbb{K} : \mathbb{Z}_p(y)]$

(c) Determinare il grado $[\mathbb{K} : \mathbb{Z}_p]$

(d) Dimostrare che il gruppo di Galois di $\mathbb{K} / \mathbb{Z}_p(y)$ è banale.

Soluzione:

(a) Siccome $\mathbb{Z}_p$ è un campo, l'anello di polinomi $\mathbb{D} := \mathbb{Z}_p[y]$ è un dominio a fattorizzazione unica (=: D.F.U.), e $\mathbb{F}_{\mathbb{D}} := \mathbb{Z}_p(y)$ è il suo campo dei quozienti, cioè $\mathbb{F}_{\mathbb{D}} := \mathbb{Z}_p(y) = Q(\mathbb{Z}_p[y]) = Q(\mathbb{D})$.

In generale, se $\mathbb{F}$ è un campo e $A := \mathbb{F}[x]$ è l'anello dei polinomi in x a coefficienti in $\mathbb{F}$, allora $\forall f(x) \in \mathbb{F}[x]$ si ha che

$$\frac{\mathbb{F}[x]}{(f(x))} \text{ è campo} \iff f(x) \text{ è irriducibile in } \mathbb{F}[x]$$

Applicando questa osservazione a $\mathbb{F} := \mathbb{F}_{\mathbb{D}} = \mathbb{Z}_p(y)$ troviamo che

$$K := \frac{(\mathbb{Z}_p(y))[x]}{(x^p - y)} = \frac{\mathbb{F}_{\mathbb{D}}[x]}{(x^p - y)}$$

è un campo $\iff f(x) := x^p - y$ è irriducibile in $\mathbb{F}_{\mathbb{D}}[x]$

QUINDI ci basta dimostrare che

$f(x) := x^p - y$ è irriducibile in $\mathbb{F}_{\mathbb{D}}[x]$

ORA, osserviamo che $\mathbb{F}_{\mathbb{D}} := \mathbb{Z}_p(y) = Q(\mathbb{D})$, con $\mathbb{D} := \mathbb{Z}_p[y]$. Allora ricordiamo questo risultato

$\forall\ P(x) \in \mathbb{D}[x]$ con $P(x)$ primitivo, si ha

$P(x)$ è irriducibile in $Q(\mathbb{D})[y]$ $\iff$ $P(x)$ è irriducibile in $\mathbb{D}[x]$

PERCIÒ ci basta dimostrare che

$$P(x) := f(x) = x^p - y$$

è irriducibile in $\mathbb{D}[x] = (\mathbb{Z}_p[y])[x]$

perché $P(x) := x^p - y$ è effettivamente primitivo!

Infine, proviamo che $P(x) := x^p - y$ è irriducibile in $\mathbb{D}[x] = (\mathbb{Z}_p[y])[x]$ applicando il criterio di Eisenstein per il D.F.U. $\mathbb{D} := \mathbb{Z}_p[y]$ e per l'elemento $q := y$ che è irriducibile (= primo) in $\mathbb{D} := \mathbb{Z}_p[y]$. Infatti, $q := y$ non divide il coefficiente direttivo di $P(x)$ - che è 1 - divide tutti gli altri coefficienti - che sono

o oppure $-q = -y$ (che è il termine noto) e infine $q^2 = y^2$ non divide il termine noto (che è $-q = -y$).

Pertanto le ipotesi del Criterio di Eisenstein sono soddisfatte e si può concludere che $P(x) := x^p - y$ è un polinomio irriducibile in $\mathbb{D}[x] = (\mathbb{Z}_p[y])[x]$.

(b) Siccome $\mathbb{K} := \dfrac{(\mathbb{Z}_p(y))[x]}{(x^p - y)}$

con $(x^p - y)$ irriducibile in $(\mathbb{Z}_p(y))[x]$, il grado richiesto è il grado di $(x^p - y)$, cioè

$$[\mathbb{K} : \mathbb{Z}_p(y)] = \partial(x^p - y) = p$$

(c) Abbiamo una torre di estensioni

$$\mathbb{Z}_p \subseteq \mathbb{Z}_p(y) \subseteq \mathbb{K} \qquad (5)$$

e chiaramente si ha

$$[\mathbb{Z}_p(y) : \mathbb{Z}] := \dim_{\mathbb{Z}_p}(\mathbb{Z}_p(y)) = \infty \qquad (6)$$

– per esempio, perché in $\mathbb{Z}_p(y)$ c'è il sottospazio vettoriale $\mathbb{Z}_p[y]$ e

$$\dim_{\mathbb{Z}_p}(\mathbb{Z}_p[y]) = \infty$$ – e QUINDI

da (5) e (6) insieme deduciamo che

$$[\mathbb{K} : \mathbb{Z}_p] := \dim_{\mathbb{Z}_p}(\mathbb{K}) = \infty$$

(d) Indicando con $Gal(\mathbb{K}/\mathbb{Z}_p(y))$ il gruppo di Galois di $\mathbb{K}/\mathbb{Z}_p(y)$, sia $\sigma \in Gal(\mathbb{K}/\mathbb{Z}_p(y))$.

Sia $\alpha \in \mathbb{K}$ una radice di $f(x) := x^p - y$ ((ad es., nella realizzazione $\mathbb{K} := \dfrac{(\mathbb{Z}_p(y))[x]}{(x^p-y)}$ può essere $\alpha = [x]_{(x^p-y)} = x \pmod{(x^p-y)}$)); allora $\alpha^p - y = 0$ in $\mathbb{K}$, cioè $\alpha^p = y$, cioè "$\alpha = y^{1/p}$ = radice p-esima di y"

Sappiamo ora che $\forall \sigma \in Gal(\mathbb{K}/\mathbb{Z}_p(y))$

da $f(\alpha) = 0$ segue che

$f(\sigma(\alpha)) = 0$, cioè

$\sigma(\alpha)$ è anch'essa radice p-esima di y (in $\mathbb{K}$).

MA in $\mathbb{K}[X]$ vale la fattorizzazione

$$f(X) = X^p - y = X^p - \alpha^p = (X-\alpha)^p \quad (7)$$

((N.B.: qui si sfrutta il fatto che la caratteristica di $\mathbb{K}[X]$ è p, perché il suo sottoanello fondamentale è $\mathbb{Z}_p$, e allora dalla formula del binomio di Newton e da $p = 0$ (in $\mathbb{Z}_p \leq \mathbb{K}[X]$) segue che $(a+b)^p = a^p + b^p$, $\forall a, b \in \mathbb{K}[X]$))

QUINDI da (7) $X^p - y = (X-\alpha)^p$

vediamo che $f(X) := X^p - y$ ha 1! radice in $\mathbb{K}$ (con molteplicità p), che è α; allora $\sigma(\alpha) = \alpha$, onde $\sigma = id_{\mathbb{K}}$, q.e.d. □