

PROPOSIZIONE 2 : SIA A UN ANELLO COMMUTATIVO E I \subseteq A UN IDEALE

a) $I = A \Leftrightarrow I$ CONTIENE UN ELEMENTO INVERTIBILE

b) A È UN CAMPO \Leftrightarrow I SUOI UNICI IDEALI SONO $\{0\}$ E $A = \langle 1_A \rangle$

DIM

a) $\Rightarrow I = A \Rightarrow 1_A \in I$. 1_A È INVERTIBILE ✓

\Leftarrow SIA $i \in I$ INVERTIBILE. $i^{-1} \in A \Rightarrow 1_A = i \cdot i^{-1} \in I$

$\Rightarrow A = \langle 1_A \rangle \subseteq I \Rightarrow I = A$ ✓

b) \Rightarrow SIA $I \neq \{0\}$. $x \in I \wedge x \neq 0 \Rightarrow \exists x^{-1} \in A \Rightarrow I = A$

PER QUANTO VISTO IN a) ✓

\Leftarrow SIA $x \in A \setminus \{0\} \Rightarrow \langle x \rangle = \langle 1_A \rangle$, OSSIA $\exists \alpha \in A$

$\alpha x = 1_A \Rightarrow x$ È INVERTIBILE ✓

ANELLI QUOTIENTE

SIA A UN ANELLO COMMUTATIVO E I \subseteq A UN IDEALE. IN PARTICOLARE, A

CON L'OPERAZIONE "+" È UN GRUPPO ABELIANO E I È UN SOTOGRUPPO

DIA. ALLORA POSSIAMO DEFINIRE IL GRUPPO QUOTIENTE A/I . CON

L'OPERAZIONE $[x] \cdot [y] := [x \cdot y] \quad \forall [x], [y] \in A/I$ ABBIAMO CHE A/I

È UN ANELLO COMMUTATIVO CON UNITÀ $[1_A]$. MOSTRIAMO CHE L'OPERAZIONE

SIANO $x' \in [x]$ E $y' \in [y]$. ALLORA $\exists i_x, i_y \in I \mid x' = x + i_x$ E

$y' = y + i_y \Rightarrow x' + y' = x + i_x + y + i_y \in I$ PERCHÉ I È UN IDEALE DIA

$\Rightarrow [x' + y'] = [x + y]$. NOLIRE $[1_A][x] = [1_A x] = [x] \forall [x] \in A/I$

$\Rightarrow [1_A]$ È L'UNITÀ DI A/I

ESEMPIO: ABBIAMO VISTO CHE $n\mathbb{Z} = \{kn \mid k \in \mathbb{Z}\}$ È UN IDEALE DELL'

ANELLO \mathbb{Z} . QUINDI IL QUOTIENTE $\mathbb{Z}_n = \frac{\mathbb{Z}}{n\mathbb{Z}}$ HA LA STRUTTURA DI ANELLO

$$\mathbb{Z}_0 \simeq \mathbb{Z}$$

$\mathbb{Z}_1 \simeq \{0\}$ ANELLO NULLO

$$\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$$

•	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$

$$\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$$

È UN CAMPO PERCHÉ $\bar{1}$ È INVERTIBILE E $\bar{2} \cdot \bar{1} = \bar{1}$
 \Rightarrow ANCHE $\bar{2}$ È INVERTIBILE

•	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$

$$\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$$

$$\bar{2} \cdot \bar{2} = \bar{0} \Rightarrow \mathbb{Z}_4 \text{ NON È}$$

DOMINIO DI INTEGRITÀ E, IN
PARTICOLARE, NON È UN CAMPO

\cdot	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

VEDIAMO CHE, IN GENERALE, \mathbb{Z}_n È UN CAMPO $\Leftrightarrow n \in \mathbb{N} \setminus \{0, 1\}$ È

UN NUMERO PRIMO ($n=0 \Rightarrow \mathbb{Z}_0 \cong \mathbb{Z}$; $n=1 \Rightarrow$ ANELLO NULLO). UN IDEALE DI

\mathbb{Z}_n È UN SOTTOGRUPPO DI \mathbb{Z}_n . Poiché \mathbb{Z}_n È CICICO, I SUOI SOTTOGRUPPI

SONO CLAICI E SONO $\{\langle \bar{m} \rangle \mid \bar{m} \in \mathbb{Z}_n\}$. INOLTRE, $\langle \bar{m} \rangle \subseteq \mathbb{Z}_n$ È UN IDEALE

$\forall m \in \mathbb{Z}_n$. INFATTI, $\bar{a} \in \mathbb{Z}_n \Rightarrow \bar{a}\bar{m} = \bar{am} = \sum_{i=1}^n \bar{m} + \bar{0} \in \langle \bar{m} \rangle$

I $\langle \bar{m} \rangle$ È L'INSIEME DEGLI ANELLI PRINCIPALI DI \mathbb{Z}_n (\mathbb{Z}_n È ANELLO AD

IDEALI PRINCIPALI).

| NOLTRÉ, $m > 1 \Rightarrow \{\langle \bar{m} \rangle \mid \bar{m} \in \mathbb{Z}_n\} = \{\langle \bar{0} \rangle, \mathbb{Z}_n\} \cup \{\langle \bar{m} \rangle \mid \text{MCD}_{m \neq 0} \{m, n\} \neq 1\}$

$\Rightarrow \mathbb{Z}_n$ È UN CAMPO $\Leftrightarrow \{\langle \bar{m} \rangle \mid \bar{m} \in \mathbb{Z}_n\} = \{\langle \bar{0} \rangle, \mathbb{Z}_n\} \Leftrightarrow n$ PRIMO

ESEMPI:

a) \mathbb{Z}_3 È UN CAMPO. $\bar{2}^{-1} = \bar{2}$ IN QUANTO $\bar{2} \cdot \bar{2} = \bar{4} = \bar{1}$

b) \mathbb{Z}_4 NON È UN CAMPO IN QUANTO $\bar{2}$ È ZERO-DIVISORE: $\bar{2} \cdot \bar{2} = \bar{4} = \bar{0}$

$\Rightarrow \bar{2}$ NON È INVERTIBILE IN \mathbb{Z}_4

ALGORITMO DI EUCLIDE E IDENTITÀ DI BÉZOUT SU Z

ESEMPIO: CALCOLARE $\text{MCD}\{1876, 3853\}$ CON L'ALGORITMO DI EUCLIDE

$$\begin{aligned} 1876 &= 365 \cdot 5 + 51 \\ 365 &= 51 \cdot 7 + 8 \\ 51 &= 8 \cdot 6 + 3 \\ 8 &= 3 \cdot 2 + 2 \\ 3 &= 2 \cdot 1 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned} \quad \Rightarrow \quad \text{MCD}\{1876, 3853\} = 1$$

A DEDDO, TROVARE DUE NUMERI $x, y \in \mathbb{Z}$ | $365x + 1876y = 1$. IN GENERALE,

UN'IDENTITÀ DEL TIPO $ax + by = \text{MCD}\{a, b\}$ È DENOMINATA IDENTITÀ DI BÉZOUT.

DALL'ALGORITMO DI EUCLIDE SI HA

$$\begin{aligned} 1 &= 3 - 2 \cdot 1 \\ 2 &= 8 - 3 \cdot 2 \\ 3 &= 51 - 8 \cdot 6 \\ 8 &= 365 - 51 \cdot 7 \\ 51 &= 1876 - 365 \cdot 5 \end{aligned} \quad \Rightarrow \quad \begin{aligned} 1 &= 3 - 2 = 3 - (8 - 3 \cdot 2) = (3 - 3) - 8 = \\ &= 3(51 - 8 \cdot 6) - 8 - 3 \cdot 51 - 8 \cdot 19 = \\ &= 3 \cdot 51 - 19 \cdot (365 - 51 \cdot 7) = 136 \cdot 51 - 19 \cdot 365 = 136(1876 - 365 \cdot 5) - \\ &\quad - 19 \cdot 365 = 136 \cdot 1876 - 699 \cdot 365 \Rightarrow x = -699 \quad y = 136. \quad \text{IN GENERALE:} \end{aligned}$$

TEOREMA: SIANO $a, b \in \mathbb{N} \setminus \{0\}$. $\frac{a}{b}$ (a DIVIDE b) $\Rightarrow a = \text{MCD}\{a, b\}$.

$\frac{a}{b} \wedge r$ ULTIMO RESTO DELL'ALGORITMO $\Rightarrow r = \text{MCD}\{a, b\}$. INOLTRE,

$$\exists x, y \in \mathbb{Z} \mid ax + by = \text{MCD}\{a, b\}$$

EQUAZIONE DIOFANTEA LINEARE

UN'EQUAZIONE DEL TIPO $ax + by = c$, CON $a, b, c \in \mathbb{Z}$, PRENDE
IL NOME DI EQUAZIONE DIOFANTEA LINEARE.

PROPOSIZIONE: SIANO $a, b, c \in \mathbb{Z}$. $\exists x, y \in \mathbb{Z} \mid ax + by = c \Leftrightarrow \frac{\text{MCD}\{a, b\}}{c}$

DIM

$$\Rightarrow ax + by = c \Rightarrow \frac{\text{MCD}\{a, b\}}{c} \quad \checkmark$$

$$\Leftarrow d = \text{MCD}\{a, b\} \Rightarrow \text{IDENTITÀ DI BÉZOUT } ax + by = d, x, y \in \mathbb{Z}$$

$$\frac{d}{c} \left(\exists k \in \mathbb{Z} \mid c = kd \right) \Rightarrow a(kx) + b(ky) = kd = c \quad \checkmark$$



ESEMPI:

a) L'EQUAZIONE DIOFANTEA $365x - 1876y = 24$ HA SOLUZIONE PERCHÉ

$\text{MCD}\{365, 1876\} = 1 \in \frac{1}{24}$. ABBIANO L'IDENTITÀ DI BÉZOUT

$$365(-699) - 1876(136) = -1 \Rightarrow 365(-699 \cdot 24) - 1876(136 \cdot 24)$$

$$= 24 \Rightarrow x = -699 \cdot 24, y = -136 \cdot 24$$

b) IN \mathbb{Z}_{1876} CALCOLARE, SE ESISTE, L'INVERSO MOLTIPLICATIVO DI $\overline{365}$.

$$\text{IN } \mathbb{Z}_{1876}, \overline{365} \cdot \overline{a} = \overline{1} \Leftrightarrow \exists a, b \in \mathbb{Z} \mid 365a = 1 + 1876b \Leftrightarrow$$

$365a - 1876b = 1$. UNICA SOLUZIONE $a = -699, b = -136$

$$\Rightarrow \overline{365}^{-1} = \overline{-699} = \overline{1177}$$

SE P È NUMERO PRIMO, SCRIVIAMO $\mathbb{F}_P := \mathbb{Z}_P$. IL CAMPO \mathbb{F}_P HA ELEMENTI

MORFISMI DI ANELLI

SI ANNO A, B DUE ANELLI. $f: A \rightarrow B$ È UN MORFISMO DI ANELLI SE

$f: (A, +) \rightarrow (B, +)$ È UN MORFISMO DI GRUPPI E $f: (A, \cdot) \rightarrow (B, \cdot)$ È UN

MORFISMO DI MONOIDI.

$$\text{Ker}(f) := \{\alpha \in A \mid f(\alpha) = 0\}$$

DEFINIZIONE) IL NUCLÉO DI UN MORFISMO DI ANELLI $f: A \rightarrow B$ È L'INSIEME

SI OSSERVI CHE IL NUCLÉO DI UN MORFISMO DI ANELLI $f: A \rightarrow B$ È UN

IDEALE DELL'ANELLO COMMUTATIVO A .

ESEMPIO:

a) SIA $I \subseteq A$ UN IDEALE DI UN ANELLO COMMUTATIVO A . ALLORA
LA PROIEZIONE CANONICA $\pi: A \xrightarrow{\quad} A/I$ $a \mapsto [a]$ È UN MORFISMO DI ANELLI

IL CUI NUCLÉO È I

b) SI CONSIDERI L'ANELLO DI NUMERI COMPLESSI \mathbb{C} . ALLORA IL

CONIUGIO $\bar{z} = \overline{a+bi} = a-bi$ È UN MORFISMO DI ANELLI DA \mathbb{C} IN \mathbb{C}

$$1 = \bar{1} \quad \overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2 \quad \overline{z_1 \cdot z_2} = \bar{z}_1 \cdot \bar{z}_2$$

TEOREMA DI ISOMORFISMO PER ANELLI COMMUTATIVI 3b: SIA $f: A \rightarrow B$

UN MORFISMO DI ANELLI COMMUTATIVI. ALLORA ESISTE UN MORFISMO

INIETTIVO DI ANELLI $\psi: \frac{A}{\ker(f)} \rightarrow B$ | IL SEGUENTE DIAGRAMMA È

COMMUTATIVO. IN PARTICOLARE, SE

f È SURIESSIVO, ψ È UN ISOMORFISMO

DI ANELLI

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow \pi & & \\ \frac{A}{\ker(f)} & & \end{array}$$

ψ

TEOREMA CINESE DEI RESTI 5

NOTAZIONE: SIA $x \in \mathbb{Z}_n$. LA CLASSE DI EQUIVALENZA \bar{x}

SARÀ SCRITA ANCHE COME $x \bmod n$

TEOREMA: SIANO $n_1, \dots, n_k \in \mathbb{N} \setminus \{0, 1\}$ | $\text{MCD}\{n_i, n_j\} = 1 \quad \forall 1 \leq i, j, k,$

$i \neq j$. SIA $n := \prod_{i=1}^k n_i$. Allora $\psi: \mathbb{Z}_n \rightarrow \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \dots \times \mathbb{Z}_{n_k}$ È

UN ISOMORFISMO DI ANELLI

DIM

VEDIAMO, PRIMA DI TUTTO, CHE LA FUNZIONE f È UN MORFISMO DI ANELLI

DOVE $f: \mathbb{Z} \rightarrow \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}$ È DEFINITA DA $f(x) = (x \bmod n_1, \dots, x \bmod n_k)$

$\forall x \in \mathbb{Z}$

$$f(a+b) = ((a+b) \bmod n_1, \dots, (a+b) \bmod n_k) = (a \bmod n_1 + b \bmod n_1, \dots, a \bmod n_k + b \bmod n_k)$$

$$\dots, a \bmod n_k + b \bmod n_k) = (a \bmod n_1, \dots, a \bmod n_k) + (b \bmod n_1, \dots, b \bmod n_k)$$

$$= f(a) + f(b) \quad \forall a, b \in \mathbb{Z}$$

• $f(1) = (1 \bmod n_1, \dots, 1 \bmod n_k)$, UN'UNITÀ DEL PRODOTTO DIRETTO DI

ANELLI $\mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}$

$$\bullet f(ab) = ((ab) \bmod x_1, \dots, (ab) \bmod x_k) = (a \bmod x_1 \cdot b \bmod x_1, \dots,$$

$$a \bmod x_k \cdot b \bmod x_k) = (a \bmod x_1, \dots, a \bmod x_k) \cdot (b \bmod x_1, \dots, b \bmod x_k)$$

$$= f(a) \cdot f(b) \quad \forall a, b \in \mathbb{Z}$$

ADESSO MOSTRIAMO CHE f È SURIEITIVO. SIA $(a_1 \bmod n_1, \dots, a_k \bmod n_k)$

$\in \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}$. OSSERVIAMO CHE $\text{MCD}\{n_1, n_2, \dots, n_{i-1}, n_{i+1}, \dots, n_k\}$

$= 1 \quad \forall 1 \leq i \leq k \Rightarrow$ ABBIAMO L'IDENTITÀ DI BÉZOUT $c_i n_i + b_i \frac{n}{n_i} = 1$.

$U_i := c_i n_i \in \langle n_i \rangle$, $V_i := b_i \frac{n}{n_i} \in \langle \frac{n}{n_i} \rangle \Rightarrow U_i + V_i = 1$. DEFINIAMO

$X := a_1 U_1 + \dots + a_k U_k$. ALLORA ABBIAMO $f(X) = (a_1 \bmod x_1, \dots, a_k \bmod x_k)$.

INFATTI, $V_i \bmod n_j = \begin{cases} 0 \bmod n_j & i \neq j \\ 1 \bmod n_j & i = j \end{cases}$. DAL TEOREMA DI ISOMORFISMO,

$\frac{\mathbb{Z}}{\ker(f)} \cong \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}$. ESSENDO n_i, n_j COPRIMI $\forall i \neq j$,

$$\ker(f) = \langle n_1 \rangle \cap \langle n_2 \rangle \cap \dots \cap \langle n_k \rangle = \langle \text{lcm}\{n_1, \dots, n_k\} \rangle = \langle \bigcap_{i=1}^k n_i \rangle$$

$\Rightarrow \frac{\mathbb{Z}}{\ker(f)} = \frac{\mathbb{Z}}{\langle n \rangle} = \mathbb{Z}_n$ È L'ISOMORFISMO $\Psi: \mathbb{Z}_n \rightarrow \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \dots \times \mathbb{Z}_{n_k}$ ■

ESEMPIO: SIANO $n_1 = 3, n_2 = 7, n_3 = 10$. ALLORA $n := n_1 n_2 n_3 = 210$

\Rightarrow ISOMORFISMO DI ANELLI $\mathbb{Z}_{210} \cong \mathbb{Z}_3 \times \mathbb{Z}_7 \times \mathbb{Z}_{10}$. SIA $(2 \bmod 3, 5 \bmod 7, 4 \bmod 10)$
 $\in \mathbb{Z}_3 \times \mathbb{Z}_7 \times \mathbb{Z}_{10}$

QUESTA Terna CORRISPONDE AD UN ELEMENTO $x \bmod 210 \in \mathbb{Z}_{210}$ CHE
SODDISFA IL SISTEMA $\begin{cases} x \bmod 3 = 2 \bmod 3 \\ x \bmod 7 = 5 \bmod 7 \\ x \bmod 10 = 4 \bmod 10 \end{cases}$. LA DEMOSTRAZIONE DEL

TEOREMA CHINSESE DEI RESTI CI DICE COME TROVARE x .

$$x = 2v_1 + 5v_2 + 4v_3 \quad \left\{ \begin{array}{l} 3a + 70b = 1 \\ 7a + 30b = 1 \\ 10a + 21b = 1 \end{array} \right. \text{ IDENTITÀ DI BÉZOUT}$$

$$\Rightarrow v_1 = 70b, v_2 = 30b, v_3 = 21b$$

$$3a + 70b = 1 \Rightarrow a = -23, b = 1 \Rightarrow v_1 = 70$$

$$7a + 30b = 1 \Rightarrow 30 = 4 \cdot 7 + 2 \quad 7 = 3 \cdot 2 + 1$$

$$\Rightarrow 1 = 7 - 3 \cdot 2 = 7 - 3(30 - 4 \cdot 7) = 13 \cdot 7 - 3 \cdot 30$$

$$\Rightarrow a = 13, b = -3 \Rightarrow v_2 = -3 \cdot 30$$

$$10a + 21b = 1 \Rightarrow a = -2, b = 1 \Rightarrow v_3 = 21$$

$$\Rightarrow x = 2 \cdot 70 - 5 \cdot 3 \cdot 30 + 4 \cdot 21 = 194 \bmod 210$$

COROLARIO: SIA $U(\mathbb{Z}_n)$ IL GRUPPO DEGLI ELEMENTI INVERTIBILI

DELL'ANELLO \mathbb{Z}_n . SIA $n := \prod_{i=1}^k n_i$ DOVE $\text{MCD}\{n_i, n_j\} = 1 \quad \forall 1 \leq i, j, k, \dots \times U(\mathbb{Z}_{n_k})$
 $i \neq j, n_i \in \mathbb{N} \setminus \{0, 1\} \quad \forall 1 \leq i \leq k$. ALLORA COME GRUPPI $U(\mathbb{Z}_n) = U(\mathbb{Z}_{n_1}) \times \dots$

DIM

L'ISOMORFISMO ψ DEL TEOREMA CHINSESE DEI RESTI, RISTRETTO A $U(\mathbb{Z}_n)$,

DÀ UN ISOMORFISMO DI GRUPPO.

Poiché un ELEMENTO $\bar{x} \in \mathbb{Z}_n$ È INVERTIBILE $\Leftrightarrow \exists$ IDENTITÀ DI BÉZOUT

$\alpha x + bn = 1$. ABBIAMO CHE \bar{x} INVERTIBILE $\Leftrightarrow \text{MCD}\{x, n\} = 1$

$\Rightarrow |U(\mathbb{Z}_n)| = \varphi(n)$ FUNZIONE DI EULERO

COROLARIO: SIA $\varphi: \mathbb{N} \setminus \{0\} \rightarrow \mathbb{N} \setminus \{0\}$ LA FUNZIONE DI EULER. SIANO $x, y \in \mathbb{N} \setminus \{0\}$ | NCDG $x, y \geq 1$. ALLORA $\varphi(xy) = \varphi(x)\varphi(y)$

DIM

DAL COROLARIO PRECEDENTE, $|U(xy)| \approx |U(\mathbb{Z}_x) \times U(\mathbb{Z}_y)| = |\varphi(x)| \cdot |\varphi(y)|$

$$\Rightarrow \varphi(xy) = |U(\mathbb{Z}_{xy})| = |U(\mathbb{Z}_x) \times U(\mathbb{Z}_y)| = |\varphi(x)| \cdot |\varphi(y)|$$

QUESTO COROLARIO FORNISCE UNA FORMULA PER CALCOLARE LA

FUNZIONE φ DI EULER. SE p È UN NUMERO PRIMO, CI SONO p^k

NUMERI NATURALI ≥ 1 E $\leq p^k$. DI QUESTI I NUMERI $p, 2p, \dots, p^{k-1}p$ HANNO

FATTORI COMUNI CON $p^k \Rightarrow \varphi(p^k) = p^k - p^{k-1}$. SE $n = p_1^{k_1} \cdots p_s^{k_s}$, DAL

COROLARIO ($n > 1$) $\varphi(n) = \varphi(p_1^{k_1}) \cdots \varphi(p_s^{k_s}) = (p_1^{k_1} - p_1^{k_1-1}) \cdots$

$$\cdot (p_s^{k_s} - p_s^{k_s-1}) = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s} \prod_{p|n} \left(1 - \frac{1}{p}\right) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

TEOREMA DI EULER: SIA $n \in \mathbb{N} \setminus \{0\}$ E $a \in \mathbb{N} \setminus \{0\}$ | NCDG $a, n \geq 1$.

ALLORA $\overline{a}^{\varphi(n)} = 1$ IN \mathbb{Z}_n (DIA MO ANCHE CHE $a^{\varphi(n)} \equiv 1 \pmod{n}$)

DIM

SAPPIAMO CHE LA CARDINALITÀ DEL GRUPPO DI ELEMENTI INVERIBILI DI

\mathbb{Z}_n È $|U(\mathbb{Z}_n)| = \varphi(n)$. SIA $\langle \bar{a} \rangle \subseteq U(\mathbb{Z}_n)$ IL SOTTOGRUPPO GENERATO

DA \bar{a} IN $U(\mathbb{Z}_n)$. ALLORA $\exists k \in \mathbb{N} \mid \varphi(n) = k \mid \langle \bar{a} \rangle \mid$. SIA $C := |\langle \bar{a} \rangle|$

$$\Rightarrow 1 = \overline{a^c} = (\overline{a^c})^k = \overline{a^{ck}} = \overline{a^{\varphi(n)}}$$

COROLLAARIO (PICCOLO TEOREMA DI FERMAT): SIA P UN NUMERO PRIMO E $a \in \mathbb{N}$. ALLORA, IN \mathbb{Z}_P , $\bar{a} = \bar{a}^P$ ($a^P \equiv a \pmod{P}$)

DIM

SE P È PRIMO $\varphi(P) = P - 1$. ALLORA, DAL TEOREMA DI EULERO SEGUE

CHE $a \neq 0 \wedge \frac{P}{a} \Rightarrow a^{\varphi(P)} \equiv 1 \pmod{P} \Rightarrow a^{P-1} \equiv 1 \pmod{P} \Rightarrow a^P \equiv a \pmod{P}$

SE $a = 0 \vee \frac{P}{a} \Rightarrow$ L'UGUAGLIANZA SI RIDUCE A $0 = 0$



CARATTERISTICA DI UN ANELLO

SIA A UN ANELLO. IL SOTTOGRUPPO $\langle 1_A \rangle \subseteq (A, +)$ È UN GRUPPO

CIClico $\Rightarrow \exists n \in \mathbb{N} | \langle 1_A \rangle \cong \mathbb{Z}_n$. QUESTO È DETTO CARATTERISTICA
DELL'ANELLO A (char(A)).

ESEMPI:

a) LA CARATTERISTICA DI \mathbb{Z} È 0. INFATTI $\langle 1 \rangle = \mathbb{Z} \cong \mathbb{Z}_0$.

b) LA CARATTERISTICA DI \mathbb{Q}, \mathbb{R} E \mathbb{C} È 0 $\langle 1 \rangle = \mathbb{Z} \cong \mathbb{Z}_0$.

c) LA CARATTERISTICA DI \mathbb{Z}_n È n ($n \in \mathbb{N}$) $\langle 1 \rangle = \mathbb{Z}$ RISPETTO A "+"

DEFINIZIONE) SIA K UN CAMPO. L'INTERSEZIONE DI TUTTI I SOTOCAMPO

DI K CONTENENTI IL GRUPPO $\langle 1_K \rangle \subseteq (K, +)$ SI CHIAMA SOTOCAMPO

FONDAMENTALE DI K

ESEMPI:

- a) IL SOTOCAMPO FONDAMENTALE DI $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ È \mathbb{Q}
b) SE $p \in \mathbb{N}$ È UN NUMERO PRIMO, IL SOTOCAMPO FONDAMENTALE

DI \mathbb{F}_p È \mathbb{F}_p PERCHÉ $\langle \bar{1} \rangle = \mathbb{F}_p$

ANELLO DEI POLINOMI IN UNA
INDETERMINATA A COEFFICIENTI IN \mathbb{F}_p
UN CAMPO

SIA K UN CAMPO. UNA FUNZIONE $f: \mathbb{N} \rightarrow K$ È DETTA

SUCCESSIONE A VALORI IN K . AD UNA SUCCESSIONE A VALORI IN K

CORRISPONDE UNA SERIE FORMALE NELL'INDETERMINATA x SU K $\sum_{n=0}^{+\infty} f(n)x^n$.

SE L'INSIEME $\{n \in \mathbb{N} | f(n) \neq 0\}$ È FINITO, DICHIAMO CHE LA SERIE

FORMALE $\sum_{n=0}^{+\infty} f(n)x^n$ È UN POLINOMIO P NELL'INDETERMINATA x DI GRADO

$\deg(P) := \max\{n \in \mathbb{N} | f(n) \neq 0\}$. IL GRADO DEL POLINOMIO 0 NON È

DEFINITO. L'INSIEME DEI POLINOMI NELL'INDETERMINATA x A COEFFICIENTI IN

K LO INDICHIAMO CON $K[x]$. L'INSIEME $K[x]$ HA UNA STRUTTURA DI ANELLO

COMMUTATIVO CON LE SEGUENTI OPERAZIONI DATI $P := \sum_{n=0}^{+\infty} a_n x^n$ E

$Q := \sum_{n=0}^{+\infty} b_n x^n$: