

## RICHIAMI

- def: sia  $X$  un insieme,  $R \subseteq X \times X$  è una **RELAZIONE D'EQUIVALENZA** se valgono:
  - RIFLESSIVITÀ**:  $(a,a) \in R \forall a \in X \quad [aRa]$
  - SIMMETRIA**:  $(a,b) \in R \Rightarrow (b,a) \in R \quad \forall a, b \in X$
  - TRANSITIVITÀ**:  $(a,b) \in R \wedge (b,c) \in R \Rightarrow (a,c) \in R \quad \forall a, b, c \in X$

- def: sia  $a \in X$ ,  $R$  relazione d'equivalenza  $[a] := \{b \in X / aRb\}$  si dice **CLASSE DI EQUIVALENZA**

- def: sia  $G$  insieme non vuoto,  $\cdot : G \times G \rightarrow G$  un'OPERAZIONE INTERNA  
t.c.:
  - ASSOCIAZIONE**:  $a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \forall a, b, c \in G$ .
  - esiste l'ELEMENTO NEUTRO**:  $\exists e \in G$  t.c.  $a \cdot e = e \cdot a = a \quad \forall a \in G$ .
  - esiste l'INVERSO**:  $\forall a \in G \exists b \in G : a \cdot b = b \cdot a = e$ .

$G$  si dice, se sono rispettati 1-3., **GRUPPO**.

- NOTA: l'**elemento neutro** di  $G$  lo indichiamo con **1** o  **$1_G$** .  
l'**elem. inverso** di  $a$  con  **$a^{-1}$** .

- def: sia  $G$  gruppo, se vale **COMMUTATIVITÀ**:  $a \cdot b = b \cdot a \quad \forall a, b \in G$ , allora  $G$  si dice **COMMUTATIVO** o **ABELIANO**.

- NOTA: se il  $G$  è ABELIANO, l'oper. interna viene spesso indicata con " $+$ ", il NEUTRO con  $0$ , e l'INVERSO di  $a \in G$  con " $-a$ ".

- def: sia  $G$  gruppo. Allora  $S \subseteq G$  si dice **SOTOGRUPPO** di  $G$  se  $S \neq \emptyset$  e  $\forall a, b \in S$  vale che:  $a \cdot b \in S$ .

- def: se  $G_1, G_2$  sono due gruppi, un'applicazione  $\varphi : G_1 \rightarrow G_2$  si dice **OMOMORFISMO** di GRUPPI se

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$$

Inoltre si ha che:  $\varphi(1_{G_1}) = 1_{G_2}$ .

- def: sia  $\varphi : G_1 \rightarrow G_2$  omom. di gruppi, si chiama **NUCLEO** di  $\varphi$  il **SOTOGINSIEME** di  $G_1$ :

$$\text{Ker } \varphi = \{a \in G_1 / \varphi(a) = 1_{G_2}\}. \text{ Inoltre, Ker } \varphi \text{ è sotogruppo di } G_1.$$

- def: sia  $\varphi$  OMOMORFISMO, si dice:

- ) **EPIMORFISMO** se  $\varphi$  suriettivo
- ) **MONOMORFISMO** se  $\varphi$  iniettivo
- ) **ISOMORFISMO** se  $\varphi$  biiettivo

- def: sia  $G$  gruppo, un sotogruppo  $H$  di  $G$  si dice **NORMALE** se  $\forall g \in G : \{ghg^{-1} / h \in H\} \subseteq H$

- def: sia  $G$  gruppo,  $H$  sotogruppo,  $g \in G$ , con  $hg$  si intende l'insieme  $\{hg / h \in H\}$ , si chiama **LATERALE DESTRO** individuato da  $g$ . Analogamente:  $gh = \{gh / h \in H\}$  si dice **LATERALE SINISTRA**.

NOTA: se  $Hg = gh$   $\Rightarrow H$  sotogr. normale.

Inoltre:  $\{Hg / g \in G\}$  e  $\{gh / g \in G\}$  sono una PARTIZIONE di  $G$ .  
con BEZ. d'EQUIVALENZA:  $g_1 R g_2 \Leftrightarrow g_1^{-1} g_2 \in H$

- def: sia  $G$  gruppo,  $H$  e  $K$  sotogruppi. Se  $\exists g \in G$  t.c.  $H = \{gKg^{-1} / k \in K\}$  allora  $H$  e  $K$  si dicono **CONIUGATI** di  $G$ .

Nota: un sot. normale è coniugato solo con sé stesso.

- def: se  $G$  gruppo e  $H$  sotogr. normale di  $G$ , indichiamo con  $G/H$  l'insieme dei LATERALI:  $\{[g] / g \in G\}$   $[g] = \{gh / h \in H\}$ .

$G/H$  si chiama **GRUPPO QUOTIENTE**.

Su  $G/H$  si può dare un prodotto:

$$[g_1] \cdot [g_2] = [g_1 \cdot g_2]$$

Oss. se  $G$  ABELIANO, ogni suo sottogruppo è normale

NOTA: se  $G$  ABELIANO, si chiama l'op. con "+":  
 $H+g = \{h+g \mid h \in H\} = \{g+h \mid h \in H\} = g+H$

perché "+" è commutativa.

es: consideriamo il GR ABELIANO  $(\mathbb{Z}, +)$ , sia  $H \subseteq \mathbb{Z}$  l'insieme di tutti i multipli di 4:  $H = \{4k \mid k \in \mathbb{Z}\}$ .  $H$  è sottogr. normale.

$$[0] = \{4k+0 \mid k \in \mathbb{Z}\} = H$$

$$[1] = \{4k+1 \mid k \in \mathbb{Z}\} = H+1$$

$$[2] = H+2$$

$$[3] = H+3$$

$$\text{e } [4] = H+4 = [0]. \quad \text{Quindi: } \mathbb{Z}_H = \{[0], [1], [2], [3]\}$$

def: se  $G$  è un gruppo FINITO (ovvero ha un numero FINITO di elementi), si chiama ORDINE di  $G$  il suo numero di elementi. Si indica con  $|G|$ .

**TEOREMA (LAGRANGE):** se  $G$  GR. FINITO e  $H$  sottogr. di  $G$ , allora  $|H|$  divide  $|G|$ .

In particolare:  $|G/H| = |G|/|H|$ .

Sappiamo che i laterali di  $G$  formano una PARTIZIONE, quindi

$$|G| = |gH| / |G/gH|$$

Dall'osservazione sappiamo che  $|gH| = |H|$ .

$$\Rightarrow |G| = |H| / |G/H|, \text{ da cui la tesi.}$$

### TEOREMI DI OMOMORFISMO

I TEO. OMOMORFISMO: Siano  $G_1, G_2$  gruppi,  $\varphi: G_1 \rightarrow G_2$  omomorfismo di gruppi. Allora  $\exists! \pi: G_1 \xrightarrow{\text{Ker } \varphi} G_2$

INIEZIONE t.c. il seguente DIAGRAMMA COMMUTA:

$$G_1 \xrightarrow{\varphi} G_2 \quad \text{dove: } \pi: G_1 \xrightarrow{\text{Ker } \varphi} G_1 / \text{Ker } \varphi \quad \text{è la PROIEZIONE CANONICA in } G_1.$$

[un OMOMORFISMO tra gruppi si può scomporre in UN EPIMORFISMO e un MONOMORFISMO]

II TEO. OMOMORFISMO: sia  $G$  gruppo,  $H$  sottogr. normale di  $G$ .

Sia  $A = \{ \text{sottogr. di } G \text{ contenenti } H \}, B = \{ \text{sottogr. di } G/H \}$

Allora  $A \subset B$  sono in BIETIONE

In particolare:  $q: A \rightarrow B, q(K) = K/H \quad (K \trianglelefteq H)$

$$\psi: B \rightarrow A : \psi(U) = \pi^{-1}(U), U \text{ sottogr. di } G/H$$

dove:  $\pi: G \rightarrow G/H, \pi(g) = [g]_H$ .

III TEO. OMOMORFISMO: se  $\varphi: G_1 \rightarrow G_2$  è omom. suriettivo, allora

$$\frac{G_1}{\text{Ker } \varphi} \cong G_2$$

## GRUPPI DI PERMUTAZIONI

Sia  $X$  GRUPPO FINITO:  $X = \{1, 2, \dots, n\}$

L'insieme  $\mathbb{Z} = \{\varphi : X \rightarrow X / \varphi \text{ BIETIVA}\}$  è un INSIEME con

$n!$  elementi ed è un GRUPPO rispetto alla COMPOSIZIONE  
di applicazioni:  $\xrightarrow{\varphi} X, X \xrightarrow{\psi} X \xrightarrow{\varphi} X$

Ottieniamo il GRUPPO delle PERMUTAZIONI su.

Esempio:  $S_3 = \{(1 2 3), (1 2 3), \dots\}$

## GRUPPO CIClico

Def:  $G$  si dice GRUPPO CIClico se  $\exists g \in G$  t.c.  $G = \{g^n / n \in \mathbb{Z}\}$

Nota:  $(G, +)$  ar con NOTAZIONE ADDITIVA:  $G$  ciclico se  $\exists g \in G$ :

$$G = \{ng / n \in \mathbb{Z}\}, \text{ dove:}$$

$$\begin{cases} g + g + \dots + g & n\text{-volte se } n > 0 \\ 0 & \text{se } n = 0 \\ (-g) + \dots + (-g) & n\text{-volte se } n < 0 \end{cases}$$

Oss:  $G$  ciclico  $\Rightarrow G$  ABELIANO.

$\forall n \in \mathbb{N} \exists!$  GRUPPO ciclico con  $n$  elementi, a meno di ISOMorfismi.

Inoltre  $\exists$ , a meno di iso,  $\exists!$  GRUPPO ciclico INFINTO.

Se  $G_1 \cong G_2$  "G<sub>1</sub> e G<sub>2</sub> sono la stessa cosa", cioè tutte le PROPRIETÀ del PRIMO sono comuni al SECONDO.

"dim": sia isom.  $\varphi: G_1 \xrightarrow{\sim} G_2$ , sia  $h \in G_1$  di ordine 35.

$$\varphi(h) \in G_2 \text{ e } (\varphi(h))^{35} = \varphi(h)^{35} \dots \varphi(h) = \varphi(h^{35}) = \varphi(1) = 1_{G_2} \text{ - volta}$$

In generale: se  $m \in \mathbb{Z}$  t.c.  $\varphi(h)^m = 1 \Rightarrow \varphi(h^m) = 1 \Rightarrow \varphi(h^m) \in \ker \varphi$   
 $\Rightarrow h^m \in \{1\} \Rightarrow h^m = 1 \Rightarrow m \geq 35$ .

Q: consideriamo, in  $\mathbb{C}$ , le RADICI  $n$ -ESIME dell'unità, che sono della forma:  $\cos\left(\frac{2\pi k}{n}\right) + i \sin\left(\frac{2\pi k}{n}\right)$ ,  $k=0, \dots, n-1$ .  
consideriamo il numero complesso:

$$z = \cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right), (z)^n = 1 \xrightarrow{\text{in generale}}$$

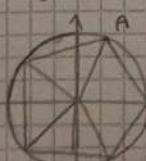
$$(\cos \alpha + i \sin \alpha)^n$$

$$= (\cos(n\alpha) + i \sin(n\alpha))$$

L'insieme  $C_n = \{\cos\left(\frac{2\pi k}{n}\right) + i \sin\left(\frac{2\pi k}{n}\right) / k=0, \dots, n-1\}$

è un insieme di  $n$  NUMERI COMPLESSI che si posizionano sui vertici di un POLIGONO REGOLARE di  $n$  LATI, inscritto nella CIRCONFERENZA di RAGGIO 1, con un VERTICE che cade in  $(1, 0)$ .

C<sub>n</sub> è chiuso rispetto al PRODOTTO in  $\mathbb{C}$  e risulta essere un GRUPPO ciclico generato da  $z$ .



$$\xrightarrow{n=5} (A)^5 = \text{id}$$

ANEGLIO  
FAM  
POLINOMI  
+ VARIABILI

def: sia  $G$  gruppo,  $g \in G$ , si dice ORDINE di  $g$  un numero  $n \in \mathbb{N}$  t.c.  $g^n = 1_G$ , con  $n$  il minimo possibile.

Se  $\exists n$  t.c.  $g^n = 1_G$ , si dice che  $g$  ha ORDINE INFINITO.

oss: se  $G$  è GR. FINITO, ogni elemento di  $G$  ha ORDINE FINITO.  
 dim: infatti, se  $g \in G$ ,  $G$  finito  $\Rightarrow \exists m_1, m_2$  t.c.  $g^{m_1} = g^{m_2}$ ,  $m_1 > m_2$ .  
 allora  $m_1 = m_2 + h \rightarrow g^{m_1} = g^{m_2} = g^h \Rightarrow g^h = 1$

quindi  $g$  ha ORDINE  $h$  o un numero minore di  $h$   
 → ha ORDINE FINITO.

Inizieremo con  $(\mathbb{Z})$  il GR. CICICO  $\{\mathbb{Z}^n / n \in \mathbb{Z}\}$ .

TEOREMA: se  $G$  è GR. CICICO FINITO di ordine  $n \Rightarrow G \cong (\mathbb{Z}_n, +)$ .  
 Se  $G$  è GR. CICICO INFINITO  $\Rightarrow G \cong (\mathbb{Z}, +)$ .

dim: se  $G$  GR. CICICO di ordine  $n$ :  $G = \{g\} = \{g^0, g^1, \dots, g^{n-1}, g^n, \dots\}$   
 e gli elementi di  $G$  sono:  $g^0 = 1, \dots, g^{n-1}$ , tutti diversi, in quanto, se  $g^i = g^j$ ,  $i < j < n \rightarrow g^{j-i} = 1 \Rightarrow$  non - ci quindi l'ORDINE NON SAREBBERE PIÙ  $n$ .

Consideriamo l'applicazione:  $\psi: \mathbb{Z} \rightarrow G = \{g\}$ , t.c.  $\psi(n) = g^n$ .  
 È suriettiva omom tra GRUPPI.

1. se l'ordine  $G$  è  $n$  (FINITO):

Ker  $\psi$ :  $\text{Ker } \psi = \{m \in \mathbb{Z} / m \in \mathbb{Z}^n = n \in \mathbb{Z}\}$ ,

per III TEO OMOM.:  $\mathbb{Z}/\text{Ker } \psi = \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n \cong G$ .

2. se  $G$  è INFINITO:  $\mathbb{Z}/\text{Ker } \psi = \mathbb{Z}/\{0\} = \mathbb{Z} \times$  II tbo omom.

$\psi: \mathbb{Z}/\{0\} \rightarrow G$  è monomorfismo, un QUOTIENTE  $\times$  def. GR. CICICO  
 $\Rightarrow$  ISOMORFISMO  $\Rightarrow \mathbb{Z}/\text{Ker } \psi = \mathbb{Z}/\{0\} = \mathbb{Z} \cong G$ .

### ANELLI

A insieme è un ANELLO se:

1)  $(A, +)$  è GR. ADDITIVO (con elem. neutro:  $0$ )

2) su A è def. PRODOTTO " $\cdot$ " t.c.:

→ PRODOTTO È ASSOCIAZIONE:  $(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \forall a, b, c \in A$

→ vale LEGGE DI DISTRIBUZIONE di  $\cdot$  rispetto a  $+$ :

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \forall a, b, c \in A$$

$$(a + b) \cdot c = a \cdot c + b \cdot c \quad \forall a, b, c \in A$$

$$a \cdot b = b \cdot a \quad \forall a, b \in A \quad (\text{COMMUTATIVITÀ?})$$

→ PR. È UNITARIO:  $\exists 1 \in A$  t.c.  $a \cdot 1 = 1 \cdot a = a \quad \forall a \in A$ .

ESEMPI DI ANELLI:  $(\mathbb{Z}, +, \cdot)$   $(\mathbb{Q}, +, \cdot)$   $(\mathbb{R}, +, \cdot)$   $(\mathbb{C}, +, \cdot)$

NOTA: noi considereremo SEMPRE ANELLI COMMUTATIVI E UNITARI.

• def: siamo  $A, B$  due ANELLI COMMI, UNITARI,

un'applicazione  $\varphi: A \rightarrow B$  si dice **OMOOMORFISMO** di ANELLI se valgono:

- $\varphi$  è omom. tra GRUPPI ABELIANI  $(A, +)$  e  $(B, +)$
- $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$   $\forall a, b \in A$ .
- $\varphi(1_A) = 1_B$

• def: sia  $A$  anello,  $I \subseteq A$  si dice **IDEALE** se:

1)  $I$  è SOTTOGRUPPO (NORMALE) rispetto a  $+$  di  $(A, +)$ .

2) vale la **REGOLA DI ASSORBIMENTO**:  $\forall a \in A, b \in I: a \cdot b \in I$ .  
↓ CONSIDERAZIONI:

→ un ANELLO contiene sempre almeno 2 IDEALI (BINNALI):  
 $\{0\}$  e  $A$

→ se un anello  $I$  contiene l'unità, allora  $I = A$ .

NOTA: l'IDEALE  $\{0\}$  si indica con  $(0)$

l'IDEALE  $A$  si indica con  $A$  ( $\neq$ )

Se  $A$  ANELLO,  $I$  IDEALE di  $A$ , si può considerare il QUOTIENTE  $A/I$  di GR. ABELIANO e si può definire un PRODOTTO:

$$[a] \cdot [b] := [a \cdot b], \text{ dove } [a] = \{b+a/b \in I\} = I+a.$$

$$[a] = [b] \Leftrightarrow a-b \in I \cdot a \equiv b \pmod{I}.$$

Sia quindi verificare che  $A/I$  è un ANELLO con quanto prodotto, tutto ANELLO QUOTIENTE di  $A$  rispetto ad  $I$ .

•  $(\mathbb{Z}, +, \cdot)$  è ANELLO. Chi sono gli IDEALI di  $\mathbb{Z}$ ?

Sono i SOTTOGRUPPI di  $\mathbb{Z}$ : se  $I \subseteq \mathbb{Z}$  è IDEALE,

o  $I = \mathbb{Z}$  oppure  $I$  è SOTTOGRUPPO proprio di  $\mathbb{Z}$ , ma i SOTTOGRUPPO proprio di  $\mathbb{Z}$  sono del tipo  $(n)$ , ovvero gr. ciclico, cioè  $(n) = \{kn/k \in \mathbb{Z}\}$  e  $(n)$  soddisfa legge assorbimento:

$\forall a \in \mathbb{Z}, b \in (n): ab \in (n)$ , ma  $b \in (n) \Rightarrow \exists k \in \mathbb{Z} \text{ t.c. } b = kn$   
allora:  $a \cdot b = a \cdot (kn) = (a \cdot k)n \in (n)$ .

Quindi  $\forall n \in \mathbb{N}, n \neq 1$ ,  $\mathbb{Z}/(n)$  è ANELLO perché QUOTIENTE:

$$\mathbb{Z}/(n) = \mathbb{Z}/(n) = \mathbb{Z}, \mathbb{Z}_1 = \mathbb{Z}/(1) = \{0, 1\} / 0 = \{1\}$$

• opp:  $\varphi: A \rightarrow B$  OMOM. tra ANELLI,  $\text{Ker}(\varphi) = \{a \in A / \varphi(a) = 0\} = \tilde{\varphi}^{-1}(0)$   
dove  $\text{Ker} \varphi$  è IDEALE infatti ("dim"):

$\forall a, b \in \text{Ker} \varphi, \varphi(ab) = \varphi(a)\varphi(b) = 0 \Rightarrow ab \in \text{Ker} \varphi$ .

• def: se  $A$  anello,  $S \subseteq A$  si dice SOTTOANELLO di  $A$  se  $S$  è SOTTOGRUPPO di  $A$  rispetto alla somma.

$S$  è CHIUSO per PRODOTTI ( $\forall a, b \in S \Rightarrow ab \in S$ )  
 $\neq \emptyset$

ANELLO AMPLIAMENTE

POLINOMI

### TEO. OMOMORFISMO (ANELLI):

$\varphi: A \rightarrow B$  omom di ANELLI, allora sia  $\pi: A \rightarrow A/\text{Ker}\varphi$  EPIMORE CANONICO. Allora  $\exists: \bar{\varphi}: A/\text{Ker}\varphi \rightarrow B$  MONOMORFISMO t.c il seguente DIAGRAMMA è commutativo:

$$\begin{array}{ccc} & \varphi & \\ A & \xrightarrow{\quad \pi \quad} & B \\ \text{con } \bar{\varphi}(a) = \bar{\varphi}(\pi(a)) = \bar{\varphi}([a]) \forall a \in A. & & \downarrow \bar{\varphi} \\ & & A/\text{Ker}\varphi \end{array}$$

Inoltre:  $\varphi(A)$  è sottanello di  $B$  e  $A/\text{Ker}\varphi \cong \varphi(A)$ .

aEA

• def: Sia  $A$  ANELLO, si dice UNITARIO (o INVERTIBILE) se  $\exists$  bEA t.c.  $ab = 1$ .  $b$  si dice INVERSO di  $a$  e si indica con  $a^{-1}$ .

Un elemento aEA si dice DIVISORE dello ZERO se  $\exists$  bEA,  $b \neq 0$  t.c.  $a \cdot b = 0$ . [ATTENZIONE: lo zero è DIVISORE dello zero]

$$\mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\} = \{1, 2, 3, 4, 5\}$$

divisori dello zero di  $\mathbb{Z}_6$ :  $0, 2, 3, 4$

INVERTIBILI e UNITARI:  $1, 5$

NON si può avere un  
elemento INVERTIBILE e  
DIVISORE dello ZERO

• def:  $A$  si dice DOMINIO di INTEGRITÀ se ha ALMENO DUE ELEMENTI ( $0$  e  $1$ ) e NON ha DIVISORI dello ZERO oltre al ZERO.

Va, bEA se  $ab = 0$  allora  $a = 0$  o  $b = 0$  \*

• def:  $A$  dom. INTEGRITÀ,  $\neq A$ ,  $\neq \emptyset$  e NON UNITARIO si chiama dico IRRIDUCIBILE se vale:  $a = \varphi \cdot g \Rightarrow \varphi$  UNITARIO oppure  $g$  UNITARIO.

• def: un elemento pEA, A dom. INTEGRITÀ  $p \neq 0$  e NON UNITARIO si dice PRIMO se vale: se  $p|ab$  allora  $p|a$  o  $p|b$ .

• PROP: se  $A$  è dom. pEA PRIMO  $\Rightarrow p$  è IRRIDUCIBILE.

dim: sia  $p$  PRIMO. Voglio vedere se  $p = \varphi g \Rightarrow \varphi$  oppure  $g$  UNITARIO

Sia  $p = \varphi g$ .  $p|p$  allora  $p|\varphi g \Rightarrow p|\varphi \circ p|g$ .

Supp.  $p|\varphi$   $\Rightarrow \exists$  kEA t.c.  $\varphi = kp$ .

$$p = \varphi g = (kp)g \Rightarrow p - Kg = p = 0 \Rightarrow p(1 - Kg) = 0$$

$$\Rightarrow p = 0 \text{ oppure } (1 - Kg) = 0, \text{ ma } p \text{ PRIMO} \Rightarrow (p \neq 0)$$

A dom. INT.  $\Rightarrow 1 - Kg = 0 \Rightarrow Kg = 1$  ma,  $K \neq 0 \Rightarrow g$  UNITARIO.

• def: sia  $A$  anello (non x forza dominio), un IDEALE PEA si dice PRIMO se  $\Rightarrow P \neq A$   $\Rightarrow ab \in P \Rightarrow a \in P \circ b \in P$  ~~abbastanza~~ ~~abbastanza~~

• PROP: A anello, PEA è PRIMO  $\Leftrightarrow A/P$  dom. INTEGR.

dim:

" $\Rightarrow$ ": PEA PRIMO  $\Rightarrow A/P$  dom. INTEGR.

Siamo  $[a] = P + a$ ,  $[b] = P + b$  due elementi di  $A/P$  t.c.

$$(P+a)(P+b) = P+0 \Rightarrow P+(ab) = P+0$$

$$[a][b] = [0] \quad [ab] = [0]$$

quindi:  $ab - 0 \in P \Rightarrow ab \in P \Rightarrow a \in P \circ b \in P$

$$\Rightarrow [a] = [0] \circ [b] = [0]$$

\* un DOMINIO di INTEGRITÀ con UNITA' si chiama ANELLO a IDEALI PRINCIPALI se  $A$  I è ideal di  $A$ ,  $\exists aEA$  t.c.  $I = (a)$ .

" $\subset$ ".

•)  $P \neq A$  infatti, se  $P = A \Rightarrow A/p \in \{[0] = [1]\}$

e non può accadere un def. di dom. INTEGRITÀ.

•) se  $a, b \in P \Rightarrow a \in P \circ b \in P$ .

Siano  $a, b \in A$  t.c.  $a, b \in P$  allora:  $[ab] = [0]$   
 $\Leftrightarrow [ab] = [a][b] = [0]$  e  $A/p$  DOM. INT.  $\Rightarrow [a] = [0] \circ [b] = [0]$   
 $\Rightarrow a \in P \circ b \in P$ .

### ASSOCIAZIONE

• def: un IDEALE  $M \neq A$  ( $A$  anullo) si dice MASSIMALE se vale:

$\rightarrow M \neq A$

•)  $A \neq I$  è A annulla, se  $M \neq I \Rightarrow I = M \circ I = A$ .

• PROP:  $M$  è massimale  $\Leftrightarrow A/M$  campo.

Dato che in campo è DOM. INT:  $M$  massimale  $\Rightarrow M$  primo.

NOTA: se  $p$  è A PRIMO,  $p \neq 0$   $\Leftrightarrow p$  non BOUNUNITARIO e vale:  
 $p|ab \Rightarrow p|a \circ p|b$ .

$p \in A$  PRIMO  $\Rightarrow$  l'IDEALE  $(p)$  è PRIMO.

Sia:  $a \in A$ ,  $a \cdot p \in (p)$   
 $\rightarrow ap + bp = p(a+b) \in (p)$   $\rightarrow a \in (p)$   
 $\therefore b(a \cdot p) = (ba) \cdot p$

• def: se  $A$  anullo, due elementi  $a, b \in A \setminus \{0\}$  si dicono ASSOCIATI se  $\exists m \in A$  UNITARIO t.c.  $a = mb$

NOTA: se  $A$  è campo, tutti gli elementi di  $A \neq 0$  sono tra loro ASSOCIATI. Infatti:  $a, b \in A \setminus \{0\} \Rightarrow a = (ab^{-1})b$

• def: sia  $A$  dominio,  $a, b \in A \setminus \{0\}$ , si dice che  $d \in A$ ,  $d \neq 0$  è un MASSIMO COMUN DIVISORE di  $a, b$  se valgono:

1.  $d | a$  e  $d | b$
2. se  $8 | a$  e  $8 | b \Rightarrow 8 | d$ .

NOTA: non è vero che  $\exists$  sempre il MCD di due elementi in un dominio.

NOTA: poniamo che, se  $a = 0 \Rightarrow \text{MCD}(a, b) = b$ .

### MASSIMO COMUN DIVISORE in $\mathbb{Z}$

esiste, e si può calcolare nel modo seguente (EUCLIDE):

1.  $\text{MCD}(a, b) = \text{MCD}(b, r)$
2.  $\text{MCD}(a, b) = \text{MCD}(a, b-a)$ , con  $b > a$ .

Perché (in  $\mathbb{Z}$ ): se  $d | a$  e  $d | b \Rightarrow d | b-a$  ( $b > a$ )

Inoltre:  $m \text{ MCD}(a, b) = \text{MCD}(a, r) \quad r = \text{resto della divisione di } b \text{ per } a$ .

• IDENTITÀ BEZOUT: se  $a, b \in \mathbb{Z}$  e  $d = \text{MCD}(a, b)$   
allora  $\exists x, y \in \mathbb{Z}$  t.c.  $d = ax + by$ .

NOTA: in  $\mathbb{Z}$  è sempre MCD, e si può calcolare con l'ALGORITMO DI EUCLIDE (IDENTITÀ BEZOUT).

• def: A dominio, siamo  $a, b \in A$  si dice che  $m \in A$  è il MINIMO COMUNE MULTIPLO di  $a$  e  $b$  se:

1.  $a | m$  e  $b | m$
2. se  $n \in A$ ,  $a | n$  e  $b | n$  allora  $m | n$ .

## CONGRUENZE IN $\mathbb{Z}$

Se  $a, b \in \mathbb{Z}$  e  $c \in \mathbb{N}, c > 1$ . Si dice che  $a$  è congruo a  $b$  modulo  $c$ ,  $a \equiv b \pmod{c}$ , se vale una delle seguenti CONDIZIONI EQUIVALENTE:

1.  $c | (a - b)$

2. il RESTO della divisione di  $a$  per  $c$  = RESTO divisione di  $b$  per  $c$   
3. nell'ANELLO QUOTIENTE  $\mathbb{Z}_c$ :  $[a] = [b]$ ,  $\mathbb{Z}_c = \mathbb{Z}/(c)$

es:  $3821 \equiv ? \pmod{42}$  : dividiamo 3821 per 42 e troviamo il RESTO

$$\begin{array}{r} 3821 \quad 42 \\ 378 \quad \quad 90 \\ \hline 41 \end{array}$$

$$3821 \equiv 41 \pmod{42}$$

es:  $42 \cdot 76 \equiv ? \pmod{9}$ , sappiamo che in  $\mathbb{Z}_9$  vale:  $[a \cdot b] = [a] \cdot [b]$

$$\begin{aligned} \rightarrow 42 &\equiv 6 \pmod{9} \\ 76 &\equiv 6 \pmod{9} \end{aligned} \quad \left\{ \begin{aligned} 42 \cdot 76 &\equiv 6 \cdot 4 = 24 \pmod{9} \\ &\Rightarrow 42 \cdot 76 \equiv 6 \pmod{9} \end{aligned} \right.$$

oss: quindi vale  $a \equiv a_1 \pmod{m}$   $b \equiv b_1 \pmod{m}$   $\Rightarrow a \cdot b \equiv a_1 \cdot b_1 \pmod{m}$

es:  $17^{236} \equiv ? \pmod{9}$

$$17^1 \equiv 8 \pmod{9}, (17^1)^2 = 8^2 \equiv 1 \pmod{9}, (17^2)^2 \equiv 1 \pmod{9}, \dots$$

Calcoliamo  $236$  in base 2:

$$\begin{array}{r} 236 \quad 2 \\ 236 \quad | 118 \quad 118 \quad 2 \\ \hline 0 \quad | 0 \quad 59 \quad 59 \quad 2 \\ \hline 1 \quad | 1 \quad 29 \quad 29 \quad 2 \\ \hline 1 \quad | 1 \quad 14 \quad 14 \quad 2 \\ \hline 0 \quad | 0 \quad 7 \quad 7 \quad 2 \\ \hline 1 \quad | 1 \quad 3 \quad 3 \quad 2 \\ \hline 1 \quad | 1 \quad 1 \quad 1 \quad 2 \\ \hline 0 \quad | 0 \quad 0 \quad 0 \quad 0 \\ \hline 1 \quad | 1 \quad 1 \quad 1 \quad 1 \quad 2 \\ \hline \end{array}$$

$$\Rightarrow (236)_{10} = (111001100)_2$$

$$\Rightarrow 236 = 2^7 + 2^6 + 2^5 + 2^3 + 2^2 \Rightarrow (17)_{10} = 17 \cdot 17 \cdot \dots \cdot 17^2$$

$$\cdot 17^2 \equiv 1 \pmod{9}, \dots, 17^2 \equiv 1 \pmod{9}$$

$$\Rightarrow (17)^{236} \equiv 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \equiv 1 \pmod{9}.$$

NOTA: quindi per risolvere il PROBLEMA  $a \equiv ? \pmod{m}$ ,  
svolgiamo questi PASSAGGI:

1. esprimiamo  $b$  in base 2:  $(b)_{10} = (\dots)_{10}$

$$\rightarrow b = \alpha_n 2^n + \alpha_{n-1} 2^{n-1} + \dots + \alpha_0 2^0, \text{ di } \alpha_i \in \{0, 1\}.$$

2. calcoliamo  $\begin{array}{l} a \\ a^2 \\ a^4 \\ \vdots \\ a^{2^n} \end{array} \pmod{m}$

$a^{2^n} \pmod{m}$  in base all'esponente massimo  
di  $b$  in base 2.

3. esprimiamo  $a = a^{2^n} a^{2^{n-1}} \dots a^{2^0} = ? \pmod{m}$  in base a quanto calcolato in 2.

PROP:  $(G, \cdot)$  GR. AB. FINITO, di ORDINE  $n$ , allora  $\forall g \in G$  vale  $g^n = 1$   
(1 è IDENTITÀ di  $G$ ). L'ORDINE DELL'ELEMENTO divide  $n$ .

dim: siano  $g_1, g_2, \dots, g_n$  gli elementi di  $G$ . Sia  $g \in G$ ,  
concediamo  $g, g_1, g_2, \dots, g_n$  sono  $n$  elementi DISTINTI

$\Rightarrow$  sono di nuovo tutti gli elementi di  $G$ .

$$\text{Allora } g \cdot g_1 \cdot g_2 \cdot \dots \cdot g_n = (g \cdot g_1) \cdot \dots \cdot (g \cdot g_n) = g^n (g_1 \cdot g_2 \cdot \dots \cdot g_n) \Rightarrow g^n = 1 \pmod{n}$$

CANCELLAZIONE.

### FUNZIONE DI EULERO

Consideriamo l'anello  $\mathbb{Z}_m$ . Sia  $U_m$  l'insieme degli elementi di  $\mathbb{Z}_m$  INVERTIBILI rispetto al PRODOTTO di  $\mathbb{Z}_m$ .

$U_m$  è un GRUPPO ABELIANO rispetto al PRODOTTO di  $\mathbb{Z}_m$ .  
(GR. ABELIANO MOLTIPLICATIVO)

Vale che  $a \in \mathbb{Z}_m$  è elemento di  $U_m$  se e solo se  $a, m$  sono COPRIMI  
 $\Rightarrow m \text{ MCD}(a, m) = 1$ .

$$\Leftrightarrow \mathbb{Z}_3 = \{[0], [1], \dots, [8]\} \rightarrow U_3 = \{[1], [2], [5], [4], [7], [8]\}$$

oss:

Quindi  $U_m$  è l'insieme delle classi di RESTO rappresentate da elementi COPRIMI con  $m$ .

Definiamo la FUNZIONE DI EULERO:  $\varphi: \mathbb{N} \rightarrow \mathbb{N} \setminus \{0\}$

t.c.:  $\varphi(m) = |U_m|$ , poniamo  $\varphi(1) = 1$  [ $\mathbb{Z}_1$  non ha senso].

Se  $[a] \in U_m$ , allora  $[a]^{q(m)} = [1]$ : un qualunque elemento elevato all'ORDINE del GRUPPO  $\varphi(a)$ .

### TEOREMA di EULERO

Sia  $a \in \mathbb{N}$  e sia  $m > 1$  un numero naturale.

Se  $a$  e  $m$  sono coprimi, allora  $a^{\varphi(m)} \equiv 1 \pmod{m}$ .

dim:  $a \in \mathbb{N}$  coprime con  $m \Rightarrow [a]$  è INVERTIBILE in  $\mathbb{Z}_m$ , cioè  $[a] \in U_m$   
allora  $[a]^{q(m)} = [1] \quad q(m)$   
 $\Rightarrow a^{\varphi(m)} \equiv 1 \pmod{m}$ .

Se  $m$  è PRIMO,  $U_m = \mathbb{Z}_m \setminus \{0\}$ . Quindi  $\varphi(p) = p-1 \quad \forall p \text{ PRIMO}$ .

Se  $p$  PRIMO vale il seguente TEOREMA:

### PICCOLO TEOREMA di FERMAT:

se  $a \in \mathbb{N}$  e  $p$  PRIMO t.c.  $p$  NON divide  $a$ , allora  $a^{p-1} \equiv 1 \pmod{p}$ .

dim: (conseguenza teorema euclero)

$p$  PRIMO,  $a \neq p$  coprimi  $\Rightarrow p \nmid a$ . Se  $p$  PRIMO,  $\varphi(p) = p-1$

quindi  $a^{p-1} \equiv 1 \pmod{p}$ .

Oss: negli enunciati abbiamo supposto che  $a \in \mathbb{N}$ , ma  
NON cambia se  $a \in \mathbb{Z}$ .

### APPLICATIONI TEO. FERMAT/EULERO:

es: trovare  $2^{-3} \pmod{11}$ . Da Fermat abbiamo che  $2^{10} \equiv 1 \pmod{11}$   
e  $2^{10} = 2 \cdot 2^9$  cioè  $[2^9]$  è l'INVERSO di  $[2]$  in  $\mathbb{Z}_{11}$ .

Troviamo inverso di  $[2]$  in  $\mathbb{Z}_{11}$ .  
 $2 \cdot 5 = 10 \equiv -1 \pmod{11} \Rightarrow 2(-5) \equiv 1 \pmod{11} \Rightarrow -5 \equiv 6 \pmod{11}$

$\Rightarrow 2^9 \equiv 6 \pmod{11}$ .

es: provare che l'ORDINE di  $[7]$  in  $\mathbb{Z}_{167}$  è almeno 80, sapendo che  $167$  è PRIMO.  
 $167 \text{ PRIMO} \Rightarrow 7^{\frac{166}{d}} \equiv 1 \pmod{167}; \quad 166 = 2 \cdot 83$

$[7]$  in  $U_{167} \rightarrow [7]^{\frac{166}{d}} = [1], \quad |[7]| \mid 166 = 2 \cdot 83 \Rightarrow |[7]| = 1, 2, 83 \text{ o } 166$ .

$\rightarrow [7]$  ha ORDINE di  $d$ ,  $d \mid 166 \rightarrow d \in \{1, 2, 83, 166\}$ .

$\rightarrow d=1 \text{ NO}; \quad \rightarrow d=2 \rightarrow 7^2 \equiv 1 \pmod{166}$

$\rightarrow d \in \{83, 166\} \Rightarrow d \geq 80$ .

NOTA: sia  $a \in \mathbb{Z}$ ,  $p$  primo. Dal Piccolo Teo Fermat, se  $p$  non divide  $a$ ,  
 $a^{p-1} \equiv 1 \pmod{p}$  da cui:  $a^p \equiv a \pmod{p}$  (anche se  $p|a$ )

In particolare ottieniamo:  $\forall a \in \mathbb{Z} \ \forall p$  primo vale:  $a^p \equiv a \pmod{p}$ .

• 10: provare che  $n^5 + 2n^3 + 3n^2 + 4n$  è SEMPRE divisibile per 5  
 $(\forall n \in \mathbb{N} \cup \mathbb{Z})$ .

Equivale a dimostrare che  $n^5 + 2n^3 + 3n^2 + 4n \equiv 0 \pmod{5}$ .

In generale vale:  $n^5 \equiv n \pmod{5}$ , quindi  $n^3 \equiv n^4 \cdot n \equiv n^4 \cdot n \equiv n^3 \equiv n \pmod{5}$

$$\Rightarrow n^5 + 2n^3 + 3n^2 + 4n \equiv n + 2n^3 + 3n^2 + 4n$$

$$\equiv 5n + 5n^3 \equiv 5(n + n^3) \equiv 0 \pmod{5}.$$

• 11: trovare se 247 è PRIMO

Teo Fermat dice che, se 247 è PRIMO, allora  $2^{246} \equiv 1 \pmod{247}$ .

ma NON è SUFFIC. perché è modo di verificare che un NUMERO NON sia PRIMO.

Risoluiamo:  $2^{246} \equiv ? \pmod{247}$ :

$$(247)_{10} = (11110110)_2 \Rightarrow 2^{246} = 2^{2^7 \cdot 2^6 \cdot 2^5 \cdot 2^4 \cdot 2^2} = 2^{2^7} \cdot 2^6 \cdot 2^5 \cdot 2^4 \cdot 2^2$$

e, trovando  $2^{2^7} \equiv ? \pmod{247}$ , ottieniamo:

$$\begin{aligned} 2^{2^7} &\equiv 61 \cdot 55 \cdot 139 \cdot 81 \cdot 16 \cdot 4 \pmod{247} \\ &\equiv 144 \cdot 144 \cdot 64 \pmod{247} \\ &\equiv 220 \pmod{247} \quad \rightarrow \text{NON È PRIMO.} \end{aligned}$$

• 12: provare che  $n^5 + 6n$  è sempre divisibile per 7 ( $\forall n \in \mathbb{Z}$ ).

Per il Piccolo Teo Fermat sappiamo che  $n^7 \equiv n \pmod{7}$

$$\Rightarrow n^5 + 6n \equiv n + 6n \pmod{7}$$

$$\equiv 7n \pmod{7}$$

$$\equiv 0 \pmod{7}.$$

### TEOREMA CINQUE dei RESTI

Siano  $m_1, \dots, m_r \in \mathbb{N} \setminus \{1\}$  a DUE a DUE coprimi.

Siano  $a_1, \dots, a_r \in \mathbb{Z}$ , consideriamo il seguente SISTEMA di CONGRUENZE:

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_r \pmod{m_r} \end{cases}$$

Il sistema ha SOLUZIONI (se  $x_0$  è una SOLUZIONE SPECIFICA, tutte le altre soluzioni sono del tipo:  $x_0 + k(m_1 \cdots m_r)$ ,  $k \in \mathbb{Z}$ ).

dim:

Consideriamo un caso particolare del sistema:  $\begin{cases} x \equiv 1 \pmod{m_1} \\ x \equiv 0 \pmod{m_2} \\ \vdots \\ x \equiv 0 \pmod{m_r} \end{cases}$

Allora i numeri  $m_1$  e  $m_2 \cdot m_3 \cdots m_r$  non hanno fattori in comune, cioè sono coprimi.

$\Rightarrow$  un BEZOUT:  $1 = \alpha m_1 + \beta m_2 \cdots m_r$ , con  $\text{MCD}(m_1, m_2 \cdots m_r) = 1$

Sia ora  $x_1 := 1 - \alpha m_1$ , vale che  $x_1 \equiv 1 \pmod{m_1}$  e  $x_1 \equiv \beta m_2 \cdots m_r \equiv 0 \pmod{m_2}, \dots, m_r$ .

Quindi  $x_1$  è soluzione del SISTEMA (\*)

Analogamente troviamo una soluzione  $x_2$  del sistema seguente:

$$\begin{cases} x \equiv 0 \pmod{m_1} \\ x \equiv 1 \pmod{m_2} \\ \vdots \\ x \equiv 0 \pmod{m_r} \end{cases}$$

Analogamente ottieni troviamo  $x_3, \dots, x_r$  come soluzioni di analoghi sistemi di congruenza.

Se poniamo  $x_0 = a_1 x_1 + a_2 x_2 + \dots + a_r x_r$ ,  $x_0$  è soluzione del SISTEMA INIZIALE:

$$\begin{cases} x_0 \equiv a_1 \cdot 1 + a_2 \cdot 0 + \dots + a_r \cdot 0 \pmod{m_1} \\ x_0 \equiv a_1 \cdot 0 + a_2 \cdot 1 + \dots + a_r \cdot 0 \pmod{m_2} \\ \vdots \\ x_0 \equiv a_1 \cdot 0 + a_2 \cdot 0 + \dots + a_r \cdot 1 \pmod{m_r} \end{cases}$$

$\Rightarrow x_0$  è soluzione del sistema di l.p. teorema:  $\begin{cases} x_0 \equiv a_1 \pmod{m_1} \\ x_0 \equiv a_2 \pmod{m_2} \\ \vdots \\ x_0 \equiv a_r \pmod{m_r} \end{cases}$

Sia  $y$  altra soluzione del SISTEMA:

$$\begin{cases} x_0 \equiv a_1 \pmod{m_1} & | \quad y \equiv a_1 \pmod{m_1} \\ \vdots & | \\ x_0 \equiv a_r \pmod{m_r} & | \quad y \equiv a_r \pmod{m_r} \end{cases}$$

$$\Rightarrow \begin{cases} x_0 - y \equiv 0 \pmod{m_1} \\ \vdots \\ x_0 - y \equiv 0 \pmod{m_r} \end{cases} \Rightarrow \begin{cases} m_1 \mid x_0 - y \\ \vdots \\ m_r \mid x_0 - y \end{cases}$$

e siccome  $m_1, \dots, m_r$  sono a due a due coprimi, anche il loro prodotto divide  $(x_0 - y)$ .

$$x_0 - y \equiv 0 \pmod{m_1 \cdots m_r}$$

$$\text{cioè } x_0 - y = K(m_1 \cdots m_r), \text{ cioè: } y = x_0 - K(m_1 \cdots m_r).$$

$$\text{es: } \begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 1 \pmod{2} \\ x \equiv 0 \pmod{5} \end{cases}$$

$$\text{troviamo } x_1: m_1 = 3, m_2 \cdot m_3 = 10 \rightarrow 1 = -3(m_1) + (m_2 \cdot m_3)$$

$$= -3(3) + 10$$

$$\rightarrow x_1 = 1 - (-3) \cdot 3 = 10$$

$$\text{troviamo } x_2: m_2 = 2, m_1 \cdot m_3 = 15 \rightarrow 1 = (-7)m_2 + m_1 \cdot m_3$$

$$\rightarrow x_2 = 15$$

$$\text{troviamo } x_3: m_1 \cdot m_2 = 6, m_3 = 5 \rightarrow 1 = m_1 \cdot m_2 + (-1)m_3$$

$$\rightarrow x_3 = 6$$

$$\text{una soluzione è } x_0 = 2 \cdot 10 + 1 \cdot 15 + 0 \cdot 6 = 35$$

$$\text{Le soluzioni sono del tipo: } y = 35 + K(3 \cdot 2 \cdot 5) = 35 + K(30)$$



RICHIAMI A, B ANELLI COMM. UNITARI.

L'insieme  $A \times B$  può essere dotato di STRUTTURA di ANELLO COMM. UNITARIO  
Ne definiamo la somma (con  $(A,+)$ ,  $(B,+)$ ) gr. abeliani:

$$(a,b) + (c,d) := (a+pc, b+d)$$

l'elemento neutro è  $(0,0) = (0_A, 0_B)$ , l'opposto di  $(a,b)$  è  $(a,-b)$ .  
Analogamente possiamo definire un PRODOTTO:

$$(a,b) \cdot (c,d) := (a \cdot c, b \cdot d) \text{ è COMMUTATIVO} \text{ perché } A, B \text{ sono anelli commutativi},$$

l'elemento neutro è  $(1_A, 1_B) = (1,1)$ .

L'anello  $A \times B$  si chiama ANELLO PRODOTTO e si indica con  $A \oplus B$ .

Consideriamo  $m_1, \dots, m_n \in \mathbb{N} \setminus \{0\}$  a 2 a 2 coprimi e  
consideriamo gli anelli  $\mathbb{Z}_{m_1}, \dots, \mathbb{Z}_{m_n}$ .

Sappiamo che  $\exists$  omomorfismo canonico  $\pi_i: \mathbb{Z} \rightarrow \mathbb{Z}_{m_i}$ ,  $\pi_i(x) = [x]_{m_i} = (m_i) + x$

e consideriamo l'applicazione:

$$\varphi: \mathbb{Z} \rightarrow \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \dots \times \mathbb{Z}_{m_n}$$

$$x \mapsto ([x]_{m_1}, [x]_{m_2}, \dots, [x]_{m_n})$$

$$\text{cioè: } x \mapsto (m_1 + x, m_2 + x, \dots, m_n + x)$$

$$\begin{aligned} \text{Inoltre } \varphi \text{ è omomorfismo di ANELLI: } \varphi(x+y) &= ([x+y]_{m_1}, \dots, [x+y]_{m_n}) = \\ &= ([x]_{m_1} + [y]_{m_1}, \dots, [x]_{m_n} + [y]_{m_n}) = ([x]_{m_1}, \dots, [x]_{m_n}) + ([y]_{m_1}, \dots, [y]_{m_n}) \\ &= \varphi(x) + \varphi(y). \end{aligned}$$

Analogamente per prodotto:  $\varphi(xy) = \varphi(x) \cdot \varphi(y)$ .

$\rightarrow \varphi$  È SURIETTIVA? prendiamo  $([a_1]_{m_1}, \dots, [a_n]_{m_n}) \in \mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_n}$   
con  $x \in \mathbb{Z}$ ,  $\varphi(x) = ([a_1]_{m_1}, \dots, [a_n]_{m_n})$

$$([x]_{m_1}, \dots, [x]_{m_n})$$

$$\text{quindi cerco } x \text{ t.c.: } \begin{cases} [x]_{m_1} = [a_1]_{m_1} \\ [x]_{m_2} = [a_2]_{m_2} \\ \vdots \\ [x]_{m_n} = [a_n]_{m_n} \end{cases} \text{ usando congruenze: } \begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

e x tro. cinese dei resti sappiamo  $\exists$  soluzione  $\Rightarrow \varphi$  suriettiva.

Applichiamo teo. omomorfismo:

$$\text{con } \text{Ker } \varphi = \{x \in \mathbb{Z} : x \equiv 0 \pmod{m_1}, \dots, x \equiv 0 \pmod{m_n}\}$$

$$= \{x \in \mathbb{Z} : m_1|x, \dots, m_n|x\} = \{x \in \mathbb{Z} : m_1 \cdots m_n|x\} =$$

$$= \{x \in \mathbb{Z} : x \in (m_1 \cdots m_n)\} = (m_1 \cdots m_n).$$

Allora x tro. omomorfismo  $\mathbb{Z}_{(m_1 \cdots m_n)} \cong \mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_n}$ .

Siamo arrivati ad un'altra formulazione del teo cinese dei resti.

\*  $\text{OSS:}$  è necessario che  $m_1, \dots, m_n$  siano a 2 a 2 coprimi,  
altrimenti l'applicazione  $\varphi: \mathbb{Z} \rightarrow \mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_n}$  NON È SURIETTIVA.

es.  $\mathbb{Z}_{10} \cong \mathbb{Z}_2 \times \mathbb{Z}_5$  ma  $\mathbb{Z}_2 \times \mathbb{Z}_5$  e  $\mathbb{Z}_2 \times \mathbb{Z}_2$  non sono isomorfi.

$$(\varphi: \mathbb{Z} \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_5, \text{Ker } \varphi = \{x \in \mathbb{Z} : 2|x \text{ e } 5|x\} = (6))$$

$$\rightarrow \mathbb{Z}/\text{Ker } \varphi = \mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \subset \mathbb{Z}_2 \times \mathbb{Z}_5 \text{ ma dominio ha } 6 \text{ elementi e codominio } 12 \rightarrow \text{NON È SURIETTIVA.}$$

## GRUPPI FINITI

$S_n =$  GRUPPO delle PERMUTAZIONI di  $n$ -elementi

abbiamo visto che l'insieme  $\{f : X \rightarrow X\}$  è bieettivo

ha  $n!$  elementi e si può dare un "prodotto" dato dalla composizione di applicazioni:  $f \cdot g = f \circ g$

Caso particolare:  $X = \{1, 2, \dots, n\}$ , mta  $\& \otimes : S_n \times S_n \rightarrow S_n$  bieettiva

si può rappresentare con una tabella come segue:

$$\begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$$

es:  $X = \{1, 2, 3\}$  le sue permutazioni sono:

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 1 & 3 \end{pmatrix}$$

$$e \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \begin{matrix} 1 \rightarrow 3 \rightarrow 3 \\ 2 \rightarrow 1 \rightarrow 2 \\ 3 \rightarrow 2 \rightarrow 1 \end{matrix}$$

RICHIAMI:

- TEO. CAYLEY: ogni gruppo finito è isomorfo a  $S_n$ .

- scomposizione in cicli disgiunti:

$$es: \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 4 & 6 & 5 \end{pmatrix} \in S_6 \quad \text{si può scomporre: } (1 \ 3 \ 2)(4 \ ) (5 \ 6)$$

- cicli disgiunti commutano:  $(1 \ 3 \ 2)(4 \ )(5 \ 6) = (5 \ 6)(4 \ )(1 \ 3 \ 2)$

TEOREMI:

- TEOREMA LAGRANGE: sia  $G$  GR. FINITO con  $m$  elementi.

Se  $H$  sottogr. di  $G$ , allora  $|H| \mid m$ .

dim:

consideriamo il caso (+ semplice) in cui  $G$  sia GR. FINITO  
ciclico:  $G = \langle g \rangle = \{g^k, k \in \mathbb{N}\}$ , se  $G$  ha ordine  $m$  e se

$n \mid m$ , allora  $\exists$  sottogruppo di  $G$  di ordine  $n$ .

dimostrazione:

sia  $g$  ciclico, con generatore  $g$ , di ordine  $m$ .

Considerate  $g^{\frac{m}{n}}$ ,  $h \in G$ .

Allora  $\langle h \rangle = \{h^0, h^1, \dots, h^n\}$ , ma per  $n$  opportuno.

Quante è l'ordine di  $h$ ?  $h^n = 1$ , infatti:  $(g^{\frac{m}{n}})^n = g^m = 1$  perché  $m \leq$  l'ordine di  $g$ .

Se  $h$  avesse ordine  $< n$ , allora:  $\exists$  l.c.  $l \mid n$  t.c.  $h^l = 1$ , cioè:

$$(g^{\frac{m}{n}})^l = 1, \text{ cioè } g^{\frac{ml}{n}} = 1; m \mid l \leq m \Rightarrow \frac{ml}{n} \leq m.$$

quando  $g$  elevato ad un esponente  $< m$  dovrebbe risultare 1, ma  $g$  ha ordine  $m$ .

Quindi  $h^n = 1$ ,  $n$  è il MINIMO POSSIBILE. Allora  $H$  ha ordine  $n$ .  
 $\Rightarrow G$  ha un sottogr. di ordine  $n$ .

### TEOREMA di CAYLEY:

Se  $G$  GR. ABELIANO FINITO con  $m$  elementi e se  $p$  è un numero PRIMO divisore di  $m$   $\Rightarrow$  ( $p \mid m$ ) allora esiste un  $\exists$  elemento di ORDINE  $p$  [quindi  $m$  è sommario di  $G$  se avesse  $p \mid (p)$ ]

dim: induzione completa su  $|G| = m$ :

•  $m = 2$ : unico  $p$  possibile è 2 (on)

→ vogliamo vedere che se il teo vale per  $|G|=m=1, 2, \dots, m-1$ , allora vale anche per  $m$ .

Se  $m$  PRIMO è CARO BANALE:  $m$  primo,  $p$  primo e  $p \mid m \Rightarrow p = m$ .

Supponiamo  $m$  NON PRIMO,  $p \mid m$ ,  $p$  PRIMO.  
Per ASSURDO supponiamo  $\nexists$  elementi di  $G$  di ordine  $p$ .  
allora NON ci sono essere elementi in  $G$  di ordine multiplo di  $p$ . Infatti, se ci fosse in  $K \in G$  di ordine multiplo di  $p$ ,  $(K)$  sarebbe un ciclico di ordine multiplo di  $p$ , quindi in  $(K)$  ci sono elementi di ordine qualunque multiplo di  $p$  divisore dell multiplo di  $p$ , in particolare di ordine  $p$ .

Sia  $h \in G$ ,  $h \neq 1$ ,  $(h) \neq G$  perché  $G$  non è ciclico, quindi il GRUPPO  $H = (h)$  è sotto-gruppo proprio di  $G$ . Inoltre  $H$  ha ordine non multiplo di  $p$ .

Considero  $G/H$ . È GR. ABELIANO perché  $H$  è sott-gruppo normale.  
 $G/H$  ha meno di  $m$  elementi, in quanto  $|G/H| = \frac{|G|}{|H|} = \frac{m}{|H|}$ , e siccome  $p \mid m$ ,  $p \mid |G/H|$ .

[infatti, se  $p \mid m$  per hp n  $p$  non divisibile  $\frac{m}{|H|}$ , allora  $p$  dovrebbe dividire  $\frac{m}{|H|}$ , ma quanto è contro PROPOSIZ. di PARTITA].

Quindi il GRUPPO  $G/H$  è di ORDINE  $\leq m$  ed è divisibile per  $p$ .

(per induzione completa)  $G/H$  ha 1 elemento di ordine  $p$ :  
sia  $[x]$  tale elemento, quindi  $[x]^p = 1$ , cioè  $x^p \in H$ , cioè:  $x^p = h^r$ , con  $r$  opportuno.

Sia  $h \in G$  e sia  $s = \text{ord}(h)$ , considero  $d = \text{gcd}(s, r)$ , qual è l'ordine dell'elemento  $x^{\frac{s}{d}}$ ?

$x^{\frac{s}{d}} \neq 1$ , infatti se  $x^{\frac{s}{d}} = 1$ , allora  $[x^{\frac{s}{d}}] = [1]$

$\Rightarrow [x] = [1]$ , ma  $[x] = p \Rightarrow p$  dovrebbe dividere  $\frac{s}{d}$ .

$\Rightarrow p \mid s/d \Rightarrow p \mid s \Rightarrow p \mid \text{ord}(h)$  ASSURDO.

Ora,  $(x^{\frac{s}{d}})^p = (x^p)^{\frac{s}{d}} = 1 \Rightarrow x^{\frac{s}{d}}$  ha ordine  $p$ .

In questo modo abbiamo ottenuto un elemento di  $G$  di ORDINE  $p$  contro hp teorema.  $\Rightarrow$  ASSURDO.

#### - RIASUNTO -

Se  $G$  è finito abelliano, di ordine  $m$ ,  $p \mid m \Rightarrow \exists$  elemento di ORDINE  $p$  in  $G$ .

1.  $m = 1, 2, 3$ , numero primo BANALI.

Quindi supp.  $m \geq 3$ ,  $m$  non primo. Per ASSURDO supp. ci sia GRUPPO di ORDINE  $m$  con  $p \mid m$  e non ci sia elemento di ORDINE  $p$ .

2. oss. che ogni elemento di  $G$  non è multiplo di  $p$ . Prendo  $h \neq 1$ ,  $h \in G$  e ne considero la ciclicità:  $(h)$ , sotto-gruppo proprio di  $G$ .

3. dato che  $H \neq 1$ , ne considero questo:  $|G/H| < m$  e con  $p \mid |G/H|$ ,  $x$  induzione completa.  $\exists [x] \in G/H$  di ordine  $p$  in  $G/H$ .  $[x]^p = [1] \Rightarrow x^p \in H$ , sia  $s = \text{ord}(h)$ , d'après  $\text{gcd}(s, r) = 1$   $x^p$  ha ordine  $p$  in  $G$ . In questo va contro hp. di assumere ASSURDO.

**TEOREMA:** sia  $G$  GR ABELIANO FINITO con  $m$  elementi.  
Sia  $n$  divisore di  $m \Rightarrow \exists$  sottogr. di  $G$  di ordine  $n$ .

dim (INDUZ. COMPIETA):

• se  $m = 1, 2, 3$ ;  $m$  PRIMO allora non c'è nulla da dimostrare.

• assumiamo  $m \geq 3$ ,  $m$  non PRIMO.

Sia  $n$  divisore di  $m$  e  $p$  PRIMO t.c.:  $p \mid n \Rightarrow p \mid m$

per teo Cayley  $\exists x \in G$  di ordine  $p$ .

Sia  $H = \langle x \rangle$ ,  $H$  è il gr. ciclico di ordine  $p$ .

Causi dunque il gr.  $G/H$ , ha ordine  $m/p \leq m$ ;

inoltre  $n \mid m$  allora  $\frac{n}{p} \mid m$ , quindi  $\frac{n}{p} \mid |G/H|$ .

Quindi x induz. completa:  $G/H$  ha sottogr. di ordine  $\frac{n}{p}$ .

Per teo omomorfismo il sottogr. in questione sarà del tipo:  $K/H$ , con  $K$  sottogr. di  $G$ .

$\frac{n}{p} = |K/H| = |K|/|H| = |K|/p \Rightarrow |K| = n$ . Quindi  $K$  è sottogr. di  $G$  di ordine  $n$ .

### TEOREMI DI SYLOW

Sia  $G$  GRUPPO con  $p^\alpha$  elementi dove  $p$  è PRIMO, allora  $G$  si dice  **$p$ -GRUPPO**.

Se  $G$  GR. e  $H \subseteq G$  sottogr. con  $p^\alpha$  elementi,  $H$  si dice  **$p$ -sottogr. di  $G$** .

Se  $G$  GR con  $m$  elementi e  $p$  PRIMO t.c.:  $p^\alpha \mid m$  è  $\alpha$  massimo possibile (cioè  $p^{\alpha+1} \nmid m$  non divide  $m$ ), allora un sottogr. di  $G$  con  $p^\alpha$  elementi si dice  **$p$ -sottogr. di Sylow.**

• def: se  $G$  GR FINITO,  $|G| = m$  e  $p$  PRIMO t.c.:  $p^\alpha \mid m$  ma  $p^{\alpha+1} \nmid m$ , allora un sottogr.  $H$  di  $G$  con  $p^\alpha$  elementi si dice  **$p$ -sottogr. di Sylow.**

#### I TEOREMA di SYLOW:

Sia  $G$  GR FINITO di ORDINE  $n$ . Sia  $p$  PRIMO t.c.:  $p^\alpha \mid n$ . Allora in  $G$   $\exists$  sottogr. di ordine  $p^\alpha$ .

#### II TEOREMA di SYLOW:

Sia  $G$  GR FINITO di ORDINE  $n$ . Sia  $p$  PRIMO t.c.:  $p^\alpha \mid n \in p^{\alpha+1}/n$  ( $p^\alpha$  max divisore di  $n$ ).

Allora ogni  $p$ -sottogr. di  $G$  è contenuto in un  $p$ -GRUPPO di ORDINE  $p^\alpha$ . [cioè: ogni  $p$ -sottogr. è contenuto in un  $p$ -sottogr. di Sylow].

Inoltre, se  $H, K$  sono due  $p$ -sottogr. di Sylow, allora sono CONIGUATI. Cioè:  $\exists g \in G$  t.c.:  $gHg^{-1} = K$ .

#### III TEOREMA SYLOW:

Sia  $G$  GR FINITO di ordine  $n$ . Sia  $p$  PRIMO e  $\alpha$  t.c.:  $p^\alpha \mid n \in p^{\alpha+1}/n$ . Quindi  $n = p^\alpha m$ , con  $m$  non divisibile per  $p$ .  
Allora: se  $N_p$  indica il numero di  $p$ -gruppi di Sylow, valgono:

- 1)  $N_p \mid m$
- 2)  $N_p \equiv 1 \pmod{p}$ .

es:  $G$  GR di ordine 72,  $H \subseteq G$ ,  $|H| = 2$  risulta anche  
 $2$  è PRIMO e  $2 \mid 72$ .

$H \subseteq H'$ , di ordine:  $|H'| = 8$  risulta:  $72 = 2^3 \cdot 9$

es: coss. Sia, sappiamo che  $|S_3| = 6$ , deve avere sottogr. di ORDINE 2 e 3, che saranno sottogr. di Sylow.

→ cerca sottogr. di ordine 2:  
deve contenere IDENTITÀ:  $(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{smallmatrix})$

$$H_1 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\} \quad |H_1| = 2$$

$$H_2 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}, \quad H_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\}$$

• III tipo Sylow:  $N_2 \mid 3 \quad N_2 \equiv 1 \pmod{2}$

Inoltre sappiamo (dato) che  $H_1$  e  $H_2$  sono coniugati  
perché  $g \in S_3 : gH_1g^{-1} = H_2 \Rightarrow gH_1 = H_2 g$ .

$$\begin{aligned} \text{1° tentativo: } g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \rightarrow gH_1 &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\} = \\ &= \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\} \\ H_2 g &= \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\} \cdot \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \right\} = \\ &= \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \right\} \end{aligned}$$

$\rightarrow$  se  $g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, gH_1 \neq H_2 g$ .

$$\begin{aligned} \text{2° tentativo: } g = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \rightarrow gH_1 &= \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\} \\ gH_2 &= \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\} \quad \text{OK.} \end{aligned}$$

$\Rightarrow H_1$  e  $H_2$  sono coniugati.

Ora cerchiamo sottogr. di ordine 3:

c'è un solo sottogr. di  $S_3$  di ordine 3, generato da:

$$\langle \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \rangle = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\}$$

questo sottogr. è per II tipo Sylow, deve essere normale  
e coniugato ad almeno altro sottogr. di Sylow  $\Rightarrow$  solo a sé stesso.

Dal II tipo Sylow:  $N_2 \mid 2 \quad N_2 \equiv 1 \pmod{3} \quad \{ N_3 = 1$ .

10: sia  $C_2$  un ciclico di ordine 2 generato da un elemento di  $G$   
 $\Rightarrow C_2 = \{1, a^2\}, a^2 = 1$ . Sia  $G$  ciclico,  $G = S_3 \times C_2, |G| = 2 \cdot 3 = 12$ .

Per il III tipo Sylow,  $G$  deve avere sottogr. di ordine 2, 3, 4 (esclusi binari).

I sottogr. di ordine 4 sono 2-Sylow sottogr.  
3 sono 3-Sylow sottogr.

Se  $N_2$  è il numero di 2-Sylow:  $\begin{cases} N_2 \mid 3 \\ N_2 \equiv 1 \pmod{2} \end{cases} \Rightarrow N_2 = 1 \circ 3$ .

Se  $N_3$  è il numero di 3-Sylow:  $\begin{cases} N_3 \mid 4 \\ N_3 \equiv 1 \pmod{3} \end{cases} \Rightarrow N_3 = 1 \circ 4$

$\rightarrow$  sottogr. di ordine 2 di  $G$ :

$$H_1 = \langle \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, 1 \rangle \quad H_3 = \langle \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, a \rangle$$

$$H_2 = \langle \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, a \rangle \quad H_4 = \langle \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, 1 \rangle \quad \text{ecc...}$$

sottoogr. di ordine 4 di  $G$ :

NON ci sono gr. ciclici di ordine 4:

$$H = \left\{ ((123), 1), ((123), 1), ((123), 1), ((123), 1) \right\}$$

$H$  è sottoogr. di  $G$  di 4 elementi,  $H$  è 2-oglio sottoogr.  
dovrebbero venire prima 3 sottoogr. di ordine 4.

10: Sia  $G$  gr. di ordine 77. Quanti sottoogr. normali ha  $G$ ?

$77 = 7 \cdot 11$  (primi)  $\Rightarrow$  ci sono 7-sylow sottoogr.  
 $11$ -sylow sottoogr.

$$\begin{cases} N_7 \mid 11 \\ N_7 \equiv 1 \pmod{7} \end{cases} \quad \begin{cases} N_7 = 1 \Rightarrow \text{c'è 1! 7-sylow sottoogr. di ordine 7} \\ \text{e inoltre è normale.} \end{cases}$$

$$\begin{cases} N_{11} \mid 7 \\ N_{11} \equiv 1 \pmod{11} \end{cases} \quad \begin{cases} N_{11} = 1 \Rightarrow \text{c'è 1! 11-sylow sottoogr. di ordine 11} \\ \Rightarrow \text{è normale.} \end{cases}$$

non: non ci possono essere altri sottoogr. NORMALI perché  
il loro ordine deve dividere ~~77~~ 77.  
Quindi  $G$  ha 4 sottoogr. normali ( $1 + \text{id} + G$ ).

11: Sia  $G$  gr. di ordine 6, cerchiamo tutti i possibili  
gr. di ordine  $G$ :

- pur Sylow  $G$  ha almeno 1 elemento di ordine 2

-  $\dots$  almeno 1 elem. di ordine 3

Sia  $X$  elemento di ordine 2 di  $G$ :  $X, X^2 = 1$ .  
e sia  $Y$  elem. di ordine 3 di  $G$ :  $Y, Y^2, Y^3 = 1$ .

Considera:  $\{1, X, Y, XY, XY^2, Y^2\}$  sono 6 elementi di  $G$ , TUTTI  
DISTINTI  
Infatti:  $y \neq X^2$  perché, se fosse così:  $1 = X^2$   
ma è imp. perché  $X$  sarebbe inverso di  $Y$ , ma sono elem. di  
ordine diverso.

Quanto fa  $Y \cdot X$ ?

$$\begin{aligned} &\rightarrow Y \cdot X = Y \text{ NO} \Rightarrow X = 1. \quad \rightarrow Y \cdot X = Y^2 \Rightarrow Y = X \text{ NO} \\ &\rightarrow Y \cdot X = X \text{ NO} \Rightarrow Y = 1. \end{aligned}$$

$$11 \quad Y \cdot X = \begin{cases} X \cdot Y & \text{se } G \text{ è COMMUTATIVO} \Rightarrow G \text{ comm} \Rightarrow G \cong \mathbb{Z}_6. \\ X \cdot Y & \text{se } G \text{ non è COMMUTATIVO} \end{cases}$$

nel secondo caso, dopo un po' di conti si arriva a:  $G \cong S_3$

QUINDI: se  $G$  ha con 6 elementi, può essere solo  
 $\mathbb{Z}_6$  o  $S_3$ , a meno di ISOMORFISMI.

## ANELLO dei POLINOMI

Sia  $A$  anello communitario, con 1 unità.

Costruiamo l'anello  $A[x]$  i cui elementi sono polinomi, cioè del tipo:  $f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$ ,  $a_i \in A$ .

- def: se dato  $f(x)$  polinomio come sopra, se  $a_n \neq 0$ ,  $a_n$  si dice COEFFICIENTE DIRETIVO del polinomio.  
Se  $a_n \neq 0$ , si dice che il GRADO di  $f(x)$  vale  $n$ .  
i polinomi del tipo:  $f(x) = a_0$ ,  $a_0 \neq 0$  hanno grado 0.  
Al polinomio nullo:  $f(x) = 0$  attribuiremo il grado  $-\infty$ .  
 $f(x) \in A[x]$ , in dichiariamo il grado di  $f$  con:  $\deg f$ .
- def: se  $f(x) = a_0 + \dots + a_n x^n$  e  $g(x) = b_0 + \dots + b_m x^m$ , allora se  $(a_0, b_0) \neq (0, 0)$ , definiscono il PRODOTTO  $f(x) \cdot g(x) = (a_0 b_0) + (a_0 b_1 + a_1 b_0) x + \dots + a_0 b_m (x^{m+n})$ .

Se  $a_n \cdot b_m \neq 0$ , allora  $f(x) \cdot g(x)$  è un polinomio di grado  $n+m$ .  
Se  $a_n \cdot b_m = 0$  (es: se  $A$  non è dom. int.) allora il grado del prodotto si abbassa (non è  $n+m$ ).

- PROP / OSS: se  $A$  è dom. integrità allora il grado del prodotto di due polinomi diversi da zero è la somma dei gradi dei polinomi.

- PROP: se  $A$  è dom. integrità, anche  $A[x]$  è dom. int.

dim: se  $f(x), g(x) \in A[x]$  e se  $f(x) \neq 0 \wedge g(x) \neq 0$  allora  
se  $f(x) = a_0 + a_1 x + \dots + a_n x^n$   
 $g(x) = b_0 + b_1 x + \dots + b_m x^m$   
 $\Rightarrow \deg(f(x) \cdot g(x)) = n+m$ , quindi  $f(x) \cdot g(x) \neq 0$ .

es.  $A = \mathbb{Z}_2 \quad (2+4x) \cdot (2) = 4+8x = 0$  in  $\mathbb{Z}_{16}$

$\rightarrow$  prodotto dei gradi di grado 1 e 0 da un polinomio nullo.

es:  $A = \mathbb{Z}_6[x] \quad (1+2x)(2+3x) = 2+3x+4x+6x^2 = 2+7x+6x^2 = 2+x$   
entrambi grado 1

Grado 1 (dom)  
(non 2)

Se  $A$  è anello communitario e  $f(x) \in A[x]$ ,  $f(x)$  può essere pensato se mai un'applicazione:  $A \rightarrow A$ .

$$\mathbb{Z}_2[x] = \begin{cases} f(x) = 1+x \\ g(x) = 1+x^2 \end{cases} \quad (\deg f = 1) \quad (\deg g = 2)$$

l'applicazione derivata da  $f(x)$  è:  $\mathbb{Z}_2 \xrightarrow{\quad} \mathbb{Z}_2$  t.c.:  
e anche da  $g(x)$  si ha:  $\mathbb{Z}_2 \xrightarrow{\quad} \mathbb{Z}_2$   
 $0 \rightarrow 1$   
 $1 \rightarrow 0$

Abbiamo ottenuto che da due polinomi diversi si ha la stessa mappo  $\mathbb{Z}_2 \rightarrow \mathbb{Z}_2$

### DIVISIONE TRA POLINOMI

per togliere termine II grado  
da I grado polinomio

es: siano  $x^2+3x+2 \in \mathbb{Q}[x]$  e  $2x+1$   $\Rightarrow (x^2+3x+2) - \frac{1}{2}x(2x+1) = \frac{5}{2}x+2$   
 $(\frac{5}{2}x+2) - \frac{5}{4}(2x+1) = \frac{3}{4}$

$$\Rightarrow (x^2+3x+2) - \frac{1}{2}x(2x+1) - \frac{5}{4}(2x+1) = \frac{3}{4}$$

$$(x^2+3x+2) = (2x+1)\left(\frac{1}{2}x + \frac{5}{4}\right) + \frac{3}{4}$$

- PROP: sia  $A$  anello,  $f(x) \in A[x]$ ,  $g(x) \in A[x]$ ,  $g(x) \neq 0$   
con coeff. direttivo invertibile in  $A$ .  
Allora  $\exists q(x), r(x) \in A[x]$  t.c.:  $f(x) = q(x) \cdot g(x) + r(x)$  con  
 $\deg r(x) < \deg g(x)$ .

Inoltre  $q(x)$  e  $r(x)$  sono unici;  $q(x)$  e  $r(x)$  si dicono QUOTIENTE e RESTO della DIVISIONE.

dim

dim. ESISTENZA (di  $q$  cd  $r$ ):

• Supp.  $\deg(g(x)) > \deg(\ell(x))$  o,  $g(x) = 0$  e  $r(x) = \ell(x)$ .

Allora:  $\ell(x) = g(x) \cdot q(x) + r(x)$  e il grado di  $r(x)$  è il grado di  $\ell(x)$ :  $\deg(r(x)) = \deg(\ell(x)) < \deg(g(x))$

• Se  $\deg(g(x)) \leq \deg(\ell(x))$ :  $\begin{array}{l} g = a_0 + a_1 x + \dots + a_m x^m \\ \ell = b_0 + b_1 x + \dots + b_n x^n, \text{ con } m \leq n. \end{array}$

NUOVE COMPROV.:

Supp. risultato sia vero per gradi di minori di  $n$ , proviamo che vale per grado  $n$ .

$$\begin{aligned} \text{Consideriamo } \ell_1 &= \ell - (b_n a_m x^{n-m})g = \\ &= (b_0 + b_1 x + \dots + b_{n-1} x^{n-1}) - x^{n-m}(b_n a_0 + b_n a_1 x + \dots \\ &\quad + b_n a_{m-1} x^{m-1}) = \\ &= (\dots) - (b_n a_{m-1} x^{m-1} + \dots + b_n x^n) = \\ &= (b_0 + b_1 x + \dots + b_{n-1} x^{n-1}) - (\dots + b_n x^n). \end{aligned}$$

\* polinomio di grado  $< n$ .

Quindi  $\ell_1$  ha grado  $< n$  = per ip. induuttiva  $\exists q_1, r_1$  t.c.

$$\ell_1 = q_1 g + r_1, \text{ con } \deg(r_1) < \deg(g)$$

Allora:  $(*) \ell - (b_n a_m x^{n-m})g = q_1 g + r_1$

$$\Rightarrow \ell = (b_n a_m x^{n-m} + q_1)g + r_1 = q_1 g + r_1, \text{ con } \deg r_1 < \deg g.$$

UNICITÀ (di  $q$  cd  $r$ ):

Supp.  $\ell = q_1 g + r_1$  e  $\ell = q_2 g + r_2$ ,  $\deg(r_1) < \deg(g)$ ,  $\deg(r_2) < \deg(g)$

Quindi:  $q_1 g + r_1 = q_2 g + r_2 \Rightarrow q_1(g - q_2) = r_2 - r_1$ , deve  $r_1 - r_2$  e polinomio di  $\deg(r_1 - r_2) < \deg(g)$ .

e  $\deg(g \cdot (q_1 - q_2)) = \deg(g) + \deg(q_1 - q_2)$ .

In generale:  $\deg(g \cdot (q_1 - q_2)) \leq \deg(g) + \deg(q_1 - q_2)$  e vale se  $\deg(g \cdot (q_1 - q_2)) = \deg(g) + \deg(q_1 - q_2)$  vale  $\alpha$ .

Il coeff. divisorio dovrebbe essere un divisore dello zero, ma è un elemento invertibile per ip.  $\Rightarrow$  grado del prodotto è somma dei gradi.

Quindi, se vale:  $\deg(g \cdot (q_1 - q_2)) = \deg(g) + \deg(q_1 - q_2)$

$$\text{se } \deg(q_1 - q_2) = 0$$

$$\frac{\deg(r_1) < \deg(g)}{\deg(r_2) < \deg(g)} \Rightarrow \deg(r_1) = \deg(r_2)$$

se vale:  $(*) q_1(g - q_2) = (r_2 - r_1)$  deve  $\begin{cases} \deg(g \cdot (q_1 - q_2)) \geq \deg(g) \\ \deg(r_2 - r_1) < \deg(g) \end{cases}$

$$\text{ugualanza vale } \Leftrightarrow \begin{cases} r_2 - r_1 = 0 \\ q_1 - q_2 = 0 \end{cases} \Rightarrow \begin{cases} r_2 = r_1 \\ q_1 = q_2 \end{cases}$$

**Teorema (di estensione):** Siano  $A, B$  due anelli (comm. unitari)

sia  $\varphi: A \rightarrow B$  omomorfismo di anelli e sia  $b \in B$  fissato.  
Allora  $\exists! \tilde{\varphi}: A[x] \rightarrow B$  omomorfismo di anelli t.c.

$$\tilde{\varphi}|_A = \varphi, \quad \tilde{\varphi}(x) = b.$$

dim: Supponiamo che  $\tilde{\varphi}$  esista, cerchiamo di capire come deve essere fatto

$$\tilde{\varphi}(ax) = b, \quad \tilde{\varphi}(x^2) = \tilde{\varphi}(x \cdot x) = b^2, \dots, \quad \tilde{\varphi}(x^n) = b^n \text{ affinché sia un omomorfismo.}$$

Prendiamo il monomio  $a_n x^n$ ,  $a \in A$ ,  $\tilde{\varphi}(a_n x^n) = \varphi(a_n) b^n$ ,

$$\tilde{\varphi}(x + y) = \tilde{\varphi}(x) + \tilde{\varphi}(y)$$

$$\begin{aligned} \tilde{\varphi}(a_0 + \dots + a_n x^n) &= \tilde{\varphi}(a_0) + \tilde{\varphi}(a_1 x) + \dots + \tilde{\varphi}(a_n x^n) \\ &= \varphi(a_0) + \varphi(a_1) b + \dots + \varphi(a_n) b^n. \end{aligned}$$

Se esiste  $\tilde{\varphi}$ , deve pur forza rispettare queste condizioni  
per essere omomorfismo, da cui segue unicità.

Per provare l'esistenza, chiediamo:  $\tilde{\varphi}(a_0 + a_1 x + \dots + a_n x^n) = \varphi(a_0) + \varphi(a_1) b + \dots + \varphi(a_n) b^n$ , e verifichiamo sia omomorfismo di ANELLI:

- conserva UNITÀ:  $\tilde{\varphi}(1_{A[x]}) = \varphi(1_A) = 1_B$ .

- sia  $f = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$   
 $g = b_0 + b_1 x + b_2 x^2 + \dots + b_m x^m$

$$\begin{aligned} \tilde{\varphi}(f + g) &= \tilde{\varphi}((a_0 + b_0) + (a_1 + b_1)x + \dots + a_n x^n) = \\ &= (\varphi(a_0 + b_0) + \varphi(a_1 + b_1)b + \dots + \varphi(a_m + b_m)b^m + \dots + \varphi(a_n)b^n) = \\ &= \varphi(a_0) + \varphi(a_1)b + \dots + \varphi(a_m)b^m + \varphi(b_0) + \dots + \varphi(b_m)b^m = \\ &= \tilde{\varphi}(f) + \tilde{\varphi}(g). \end{aligned}$$

- verifichiamo:  $\tilde{\varphi}(f \cdot g) = \tilde{\varphi}(f) \cdot \tilde{\varphi}(g)$

$$\begin{aligned} \tilde{\varphi}(f \cdot g) &= \tilde{\varphi}((a_0 + a_1 x + \dots)(b_0 + b_1 x + \dots)) = \\ &= \tilde{\varphi}((a_0 b_0) + (a_0 b_1 + a_1 b_0)x + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 + \dots) = \\ &= \varphi(a_0 b_0) + \varphi(a_0 b_1 + a_1 b_0)b + \dots = \\ &= (\varphi(a_0) + \varphi(a_1)b + \dots)(\varphi(b_0) + \varphi(b_1)b + \dots) = \\ &= \tilde{\varphi}(f) \cdot \tilde{\varphi}(g). \end{aligned}$$

#### • $\tilde{\varphi}$ : omomorfismo di valutazioni

A anello, se  $A$ , consideriamo l'applicazione:

$$\begin{aligned} \text{val}: A[x] &\longrightarrow A \text{ t.c. } \text{val}(x) = a \quad \forall a \in A \\ \text{val}(n) &= a. \end{aligned}$$

Per il TEOREMA DI ESTENSIONE, è omomorfismo di ANELLI.  
Dove, se  $\tilde{\varphi}(a_n) = a_0 + a_1 x + \dots + a_n x^n \in A[x]$ ,

$$\text{val}(\tilde{\varphi}) = a_0 + a_1 a + \dots + a_n a^n = \tilde{\varphi}(a).$$

**TEOREMA (RUFFINI)**: sia  $f(x) \in K[x]$ ,  $K$  campo compo.  
Sia  $a \in K$  allora la divisione di  $f$  per il polinomio  $(x-a)$  ha per resto  $f(a)$ .  
In particolare,  $f(x)$  è divisibile per  $(x-a)$  se e solo se  $f(a)=0$ .

**dimm:** sia  $f(x) \in K[x]$ . Divido  $f(x)$  per  $(x-a)$ .

Ottengo che  $f(x) = q(x)(x-a) + r(x)$ , con  $\deg q < \deg(x-a) = 1$   
 $\Rightarrow r(x)$  è una costante [perché  $\deg(r) < 1$ ].

In particolare ho che  $f(a) = q(a) \cdot (a-a) + r(a) = r(a)$   
 $r(a) = r \quad \forall a \in K$  costante.

e  $f(a) = r(a) = r \quad \forall a$ , quindi il RESTO della DIVISIONE È ZERO se e solo se  $f(a)=0$ .

**TEOREMA (D'ALAMBERT)**: sia  $f(x) \in K[x]$  di grado  $n \geq 0$ .  
Allora  $f(x)$  ha al massimo  $n$  radici (dette ZERI).

**dimm:** induzione su  $n$ :

- $\forall n=0$ :  $f$  è costante  $\Rightarrow$  ha 0 radici.
- Supp. valga fino a  $n-1$ :
- Verifichiamo  $n$ :  
sia  $f$  di grado  $n \geq 1$ , se non avesse radici il risultato sarebbe vero.  
Se  $f$  ha radici, sia  $a \in K$  una di queste  
 $\Rightarrow$  per RUFFINI:  $f = q(x-a)$ ,  $\deg(q) = n-1$  e  $q$  ha al massimo  $n-1$  radici per induzione  
 $\Rightarrow f$  ha per radici "a" e le radici di  $q$ , quindi ha al massimo  $(n-1)+1$  radici  $\Rightarrow$   $f$  ha al massimo  $n$  radici.

**COROLARIO**: siano  $f, g \in K[x]$ , con  $K$  campo FINITO INFINITO,  
allora il polinomio  $f$  è uguale al polinomio  $g$   
se  $f(a) = g(a) \quad \forall a \in K$ .

**dimm:** se  $f, g \in K[x]$  considerare il polinomio  $f-g$   
allora  $(f-g)(a) = 0 \quad \forall a \in K$

$\Rightarrow$  il polinomio  $f-g$  ha infinite radici in quanto  $K$  è INFINITO, quindi per teo D'Alambert è il polinomio nullo, cioè:  $f-g=0$

$\Rightarrow f=g$ .

Viceversa, se  $f=g$ , ovviamente  $f(a)=g(a) \quad \forall a \in K$

**dalle:** se  $f, g \in K[x]$ , allora  $\exists \text{ mcd}(f, g)$ .  
Il MASSIMO COMUN DIVISORE è sempre (si dice con ALGORITMO di EUCLIDE, analogamente a INTEG)

Cioè:  $\text{mcd}(f, g) = \text{mcd}(f, g)$ , con  $\exists$  resto divisione di  $f$  per  $g$ .

$$\begin{aligned} \text{es: } \text{mcd}(x^2+2x+1, x^2+3x+2) &= \text{mcd}(x^2+2x+1 - (x^2+3x+2), x^2+3x+2) \\ &= \text{mcd}(-x-1, x^2+3x+2 - x(x+1)) = \\ &= \text{mcd}(-x-1, 2x+2) = \text{mcd}(-x-1, 0) = -x-1. \end{aligned}$$

NOTA: dall'algo di EUCLIDE si vede che se  $d = \text{mcd}(f, g)$ , si riesce a calcolare due polinomi  $p, q \in K[x]$  t.c.  
 $d = pf + qg$

[IDENTITÀ di BEZOUT]

### IDENTITÀ DI BEZOUT (POLINOMI)

Siano  $f, g \in K[x]$ ,  $\exists d = \text{MCD}(f, g)$  s.t.  $\exists \alpha, \beta \in K[x]$  t.c.  $d = \alpha f + \beta g$ .

Perché in  $\mathbb{Z}$  ogni IDEALE è PRINCIPALE?

Sia  $I \subseteq \mathbb{Z}$  ideale, sia  $I = (a)$  è banalmente principale  
(tutti gli altri elem. sono multipli di  $a$ )

$\forall I \neq (0)$ ,  $I$  contiene numeri  $> 0$ .  
Allora l'insieme  $\{x = |a| \in I / a > 0\} \neq \emptyset$  quindi per proprietà  
di  $\mathbb{N}$ , ammette MINIMO.  
Sia  $m$  il minimo di  $X$ .  
Se  $I = (0)$ , sia  $f \in I$ , consideriamo la divisione di  $f$  per  $m$ .  
 $f = qm + r$ ,  $0 \leq r < m$   $\Rightarrow r = f - qm \in I \cap (m) \Rightarrow r = 0$

Quindi  $I = (m)$ .

• PROP: sia  $K$  campo ogni IDEALE di  $K[x]$  è PRINCIPALE.

dim: sia  $I \subseteq K[x]$  ideale.

Se  $I = (0)$  è PRINCIPALE (BANALE).

Se  $I \neq (0)$ , sia  $m \in I$  IL POLINOMIO NON NUOVO DI GMDO  
MINIMO POSSIBILE, sia ora  $f(x) \in I$ , considerare la DIVISIONE di  
 $f(x)$  per  $m(x)$ , quindi  $\exists q, r \in K[x]$  t.c.  $f = qm + r$   
con  $\deg(r) < \deg(m)$ .

$r = f - qm \in I$  unica possibilità per GMDO di  $r$  ( $\deg(r) = -\infty$ )

cioè:  $r = 0 \Rightarrow I = (m)$

PERCHÉ: se  $m = \deg(m) = 1$  non ci sarebbero polinomi di grado 0  
perché  $m(x)$  ha grado minimo  
 $\Rightarrow \deg(r) = -\infty$  per forza.

• Chi sono gli elementi INVERTIBILI di  $K[x]$ ?

Sia  $f(x) \in K[x]$  t.m.  $f(x) = a_0 + a_1 x + \dots + a_n x^n$ ,  $a_n \neq 0$   
e  $g(x) \in K[x]$ :  $g(x) = b_0 + \dots + b_m x^m$ ,  $b_m \neq 0$

$$f(x) \cdot g(x) = (a_0 + \dots + a_n x^n)(b_0 + \dots + b_m x^m) = 1$$

$$\Leftrightarrow m+n=0 \Rightarrow m=n=0.$$

OSS:  $K[x]$  NON È UN CAMPO, ma un DOMINIO DI INTEGRITÀ.

• TEOREMA: sia  $A$ anello  $\mathbb{Z} \circ K[x]$ , con  $K$  campo, allora in  $A$  vale

se  $\&$  IRREDUCIBILE allora  $\&$  è PRIMO.

[quindi in  $\mathbb{Z} \circ K[x]$  vale che, se PRIMO = IRREDUCIBILE]

dim ( $A = \mathbb{Z}$ ): sia  $\& \in \mathbb{Z}$ ,  $\& \neq 0$  NON UNITARIO ( $\& \neq \pm 1$ ) e supp.  
che  $\&$  sia IRREDUCIBILE.

Vogliamo provare che  $\&$  è PRIMO:  $\& | ab \Rightarrow \& | a \circ \& | b$ .

Sia  $d = \text{MCD}(\&, a)$  [abbiamo dim. che  $d \in \mathbb{Z}$ ],  $d | \&$  e d | a.  
 $d | \& \Rightarrow \& = d \cdot h$ ,  $\&$  IRREDUCIBILE  $\times$  UP.  $\Rightarrow d$  è UNITARIO  $\circ$   $d$  è UNITARIO.

$\Rightarrow$  CASO 1: d UNITARIO. (X)

$\Rightarrow$  CASO 2:  $\&$  e d SONO ASSOCIAZI (  $\& = d \cdot h$ , h UNITARIO) (XX)

(+) 1. usiamo id. Bezout:  $d = \alpha \& + \beta a$ , d UNITARIO, quindi  
 $\exists d^{-1} \Rightarrow$  multiplo per d:  $1 = \alpha d^{-1} \& + \beta d^{-1} a$ ,  
multiplo per b:  $b = \alpha d^{-1} b \& + \beta d^{-1} b a$  è divisibile per  $\&$ .  
 $\Rightarrow \& | b$ .

(+) 2.  $\& | ab$ ,  $d | \&$  d | a, in particolare  $d | a$  e  $d | b$  associaz.

$$d = h^{-1} \& \Rightarrow a = h^{-1} \& b \Rightarrow \& | a$$

$$a = d \cdot c$$

$$ab = h^{-1} \& b = h^{-1} \& d \cdot c = h^{-1} \& c$$

oss: Ie kring sono domini euclidi, avere delle regole di divisione.

\* def: sia  $A$  dom. integrità.  $A$  si dice dominio di fattorizzazione unica [UFD]

1. ogni elemento di  $A \neq 0$ , non unitario, è prodotto (finito) di irriducibili

2. se  $a \in A$ ,  $a \neq 0$  non unitario e se  $a = p_1 \cdots p_r$  e  $a = q_1 \cdots q_s$  con  $p_1, \dots, p_r, q_1, \dots, q_s$  EA IRRIDUCIBILI.

Allora  $r = s$  e inoltre, a meno di ricordino di fattori,  $p_1 \dots p_r$  sono associati,  $q_1 \dots q_s$  sono associati,  $p_1 \dots p_r$  sono associati.

\* TEOREMA: l'anello  $\mathbb{Z}$  è UFD.

dim: abbiamo verificare le PROPRIETÀ 1) e 2):

1) sia  $n \in \mathbb{Z}$ ,  $n \neq 0$  NON UNITARIO ( $\Rightarrow n \neq \pm 1$ ), consideriamo  $|n| > 1$ . Proviamo che  $|n|$  È PRODOTTO DI IRRIDUCIBILI INDUZIONE COMPLETA su  $|n|$ :

se  $|n| = 2$  allora  $2 = a \cdot b \Rightarrow a$  UNITARIO o  $b$  UNITARIO  $\Rightarrow 2$  IRRIDUCIBILI in  $\mathbb{Z}$ .

Consideriamo  $|n| > 2$ , se  $|n|$  È PRODOTTO DI IRRIDUCIBILI. abbiamo concluso, se  $|n|$  non fosse IRRIDUCIBILE  $\Rightarrow |n| = n_1 \cdot n_2$  con  $n_1, n_2$  NON UNITARI. Inoltre  $n_1, n_2 \in \mathbb{Z}$  quindi  $|n| = |n_1| \cdot |n_2|$ .

$|n_1| < |n|$  e  $|n_2| < |n|$ . Per induzione completa:

$|n_1| = p_1 \cdots p_k$  e  $|n_2| = p_{k+1} \cdots p_l$  con  $p_1, \dots, p_l \in \mathbb{Z}$  e IRRIDUCIBILI.

Se considero  $n$ , abbiamo che se  $n > 0$ ,  $n = p_1 \cdots p_l$  PRODOTTO DI IRRIDUCIBILI; se  $n < 0$ ,  $-n = p_1 \cdots p_l$ , quindi  $n = (-p_1) \cdots (-p_l)$  PROD di IRRIDUCIBILI perché  $(-p_1) \cdots (-p_l)$  è associato a  $p_1$ .

In entrambi i casi ( $n > 0$  o  $n < 0$ ) abbiamo che  $n$  È PRODOTTO DI IRRIDUCIBILI in  $\mathbb{Z}$ .

2) sia  $n \in \mathbb{Z}$  NON UNITARIO,  $n \neq 0$ . Supp.  $n = p_1 \cdots p_r$  e  $n = q_1 \cdots q_s$  IRRIDUCIBILI in  $\mathbb{Z}$ .

Proviamo che  $p_1, \dots, p_r$  e  $q_1, \dots, q_s$  sono UNICI a meno di ordine e di associatività.

Usiamo INDUZIONE SU  $\max\{|r, s|\}$ :

•) sia  $1 = \max\{|r, s|\} \Rightarrow r = s = 1$ ,  $n = p_1 \neq n = q_1 \Rightarrow p_1 = q_1$ . abbiamo verificato UNICITÀ al passo 0.

•) sia ora  $r = \max\{|r, s|\}$ , supp. che risultato sia vero fino a  $n-1$ , voglio dimo. valga per  $n$ .

se  $r = \max\{|r, s|\}$  (non perde di generalità),  $r \geq 2$ ,

considero  $q_1, \dots, q_{r-1} | n = p_1 \cdots p_r \Rightarrow q_1 | p_1 \cdots p_r$ ,  $q_1$  IRRIDUC.

$\Rightarrow q_1$  PRIMO. Allora  $q_1$  divide uno dei fattori di  $p_1 \cdots p_r$ .

Supp. che  $q_1 | p_1$ , quindi:  $p_1 = \alpha q_1$ ,  $\alpha \in \mathbb{Z}$ .  $p_1$  IRRIDUC. quindi  $\alpha$  è UNITARIO o  $\alpha$  è UNITARIO, ma  $q_1$  È IRRIDUCIBILE  $\Rightarrow \alpha$  UNITARIO  $\Rightarrow p_1$  è  $q_1$  ASSOCIATI.

Quindi:  $p_1 \cdots p_r = n = q_1 \cdots q_s \Rightarrow \alpha q_1 \cdot p_2 \cdots p_r = q_1 \cdots q_s$ , UNIT.

$\Rightarrow \alpha p_2 \cdots p_r = q_2 \cdots q_s$  sono due GRUPPI di  $r-s$  elementi IRRIDUCIBILI  $\Rightarrow r-s=1$ .

$\Rightarrow$  per ip. induzione:  $r-1 = s-1$ , cioè  $r = s$ . abbiamo  $p_1 \cdots p_r$  e  $q_1 \cdots q_s$  associati.

Quindi, se  $n \in \mathbb{N}, n \neq 0, 1, -1$ . se  $n$  POSITIVO,  $|n| = n$  È PROD. DI IRRIDUC. A SCOMP. UNICA  $\Rightarrow n \leq 0 \Rightarrow -n > 0 \Rightarrow -n = (-p_1) p_2 \cdots p_r$  FATTORI UNICI.

DEFINIZIONE

+ POLINOMI  
+ VARIABILI

es:  $15 = 5 \cdot 3 = 3 \cdot 5 = (-3)(-5) = (-5)(-3)$   
questa fattorizzazione sono tutte le UNICHE a meno di ASSOCIAZIONI E PERMUTAZIONI

NOTA: se  $n > 0$ , in più sono scritte come prodotto di irriducibili tutti positivi.

COROLARIO (TEO. FONDAM. ALGEBRA):

in  $\mathbb{N}$  tutti i NUMERI  $> 1$  sono PRODOTTO DI ELEMENTI PRIMI (= IRRIDUCIBILI)  
in  $\mathbb{N}$ , e questi sono in modo UNICO, a meno di PERMUTAZIONI.

TEOREMA: l'anello  $K[x]$  con  $K$  campo è UFD.

dim: si usa INDUZIONE COMPLETA sul grado dei polinomi  
di  $K[x]$ .

Sia  $f(x) \in K[x]$ ,  $\deg f > 0$ , NON UNITARIO  $\Rightarrow$   $\deg f \geq 1$ .

Proviamo che  $f$  è PRODOTTO DI POLINOMI IRRIDUCIBILI:

1.  $\deg f = 1 \Rightarrow f = ax + b$ ,  $a \neq 0$ ,  $f$  è IRRIDUCIBILE.  
Tutti sono PRODOTTI AVREBBERE GRADO  $\geq 1$ . ~~DEFINIZIONE~~

2. Sia  $N = \deg f$ ,  $N > 1$   $f$  IRRIDUCIBILE.  
Se  $f$  non è irriducibile allora  $f = g \cdot h$  con  $\deg g < N$ ,  $\deg h < N$

PER INDUZIONE:  $g = p_1 \cdots p_k$ ,  $h = q_1 \cdots q_l$ .

$f = p_1 \cdots p_k \cdot q_1 \cdots q_l$  con  $p_i, q_j$  PROPS. DI IRRIDUCIBILI.

UNITÀ: IN OVR. MUL MAX  $\deg f$ .

$\Rightarrow \max \{1, s\} = 1 \Rightarrow N = s = 1$  (OK)

Sia  $r = \max \{1, s\} \geq 1$  allora  $q_1 | p_1 \cdots p_k \Rightarrow$  SUPP.  $q_1 | p_1$

$\Rightarrow p_1 = q_1 \cdot \alpha$  IRRIDUCIBILE  $\Rightarrow \alpha$  UNITARIO  $\circ$   $q_1$  UNITARIO, ma  
 $q_1$  IRRIDUCIBILE  $\Rightarrow \alpha$  UNITARIO e  $p_1, q_1$  ASSOCIATI.

$\Rightarrow p_1 \cdots p_k = (\alpha p_1) \cdots p_k \Rightarrow p_1 \cdots p_k = \alpha q_1 \cdots q_s$   
sono  $r-1$  e  $s-1$  fattori  $\Rightarrow r-1+s-1=r=s$ .

$\Rightarrow p_1 \cdots p_k \in \alpha p_1 \cdots q_s$  sono due fattori. con  $r-1$  fattori

$\Rightarrow$  sono  $\Theta$  a meno di ASSOCIAZIONI E PERMUTAZIONI.

es:  $x^2 - 1 \in \mathbb{Q}[x]$ ,  $x^2 - 1 = (x-1)(x+1) = (15x-15)(\frac{1}{15}x + \frac{1}{15})$

→ Consideriamo gli anelli di polinomi:  $\mathbb{Q}[x]$ ,  $\mathbb{R}[x]$ ,  $\mathbb{C}[x]$ .  
vogliamo stabilire gli IRRIDUCIBILI in questi anelli.

$\Rightarrow$  tutti i polinomi di GRADO 1 sono IRRIDUCIBILI in  $\mathbb{C}[x]$ .

In particolare, se un polinomio in  $\mathbb{C}[x]$  è IRRIDUCIBILE, è di GRADO 1.

Inoltre, dal teo fondam dell'algebra, ogni polinomio  $\alpha$  ha almeno una RADICE in  $\mathbb{C}$ .

Quindi, sia  $f(x) = a_0 + \dots + a_n x^n$ ,  $a_n \neq 0$ , allora  $\exists x \in \mathbb{C} : f(x) = 0$ .  
per RUFFINI:  $f(x) = g(x)(x-\alpha)$ , cioè  $f(x)$  si può "separare"  
in un PRODOTTO.

Se  $\deg(f(x)) \geq 2$ , allora  $\deg(g(x)) \geq n$ , quindi  $f(x)$  non può essere IRRIDUCIBILE.

In  $\mathbb{C}[x]$  ogni polinomio di GRADO  $\geq 2$  è RIDUCIBILE.

$\Rightarrow$  in  $\mathbb{R}[x]$ : se il  $\deg$  del polinomio è DISPARI (ha SEMPRE RADICI).

Sia  $f(x) \in \mathbb{R}[x]$ ,  $\deg f \geq 2$ , se  $f$  ha RADICE in  $\mathbb{R}$  È RIDUCIBILE, se non ha RADICI in  $\mathbb{R}$ , ha una RADICE  $\bar{x} = x + ip \in \mathbb{C}$ .

allora ha anche  $\bar{x} = x - ip$  come RADICE.

$$f(\bar{x}) = 0 \quad a_0 + a_1 \bar{x} + \dots + a_n \bar{x}^n = 0 = \overline{a_0 + \dots + a_n x^n}$$

$$\Rightarrow \overline{a_0} + \overline{a_1} \bar{x} + \dots + \overline{a_n} \bar{x}^n = \overline{a_0} + \overline{a_1} \bar{x} + \dots + \overline{a_n} (\bar{x}^n) = 0 \Rightarrow f(\bar{x}) = 0.$$

Per RUFFINI  $f(x)$  in  $\mathbb{C}[x]$  è divisibile da  $x - \bar{x}$

$$\Rightarrow f(x) = f_1(x)(x - \bar{x})$$

$$0 = f(\bar{x}) = f_1(\bar{x})(\bar{x} - \bar{x}) \Rightarrow f_1(\bar{x}) = 0 \text{ quindi } \bar{x} - \bar{x} \neq 0.$$

Sempre per RUFFINI, in  $\mathbb{C}[x]$ :  $f_1(x) = f_2(x)(x - \bar{x})$ :

$$\Rightarrow f(x) = f_2(x)(x - \bar{x})(x - \bar{x}) = f_2(x)(x - \alpha - i\beta)(x - \alpha + i\beta) =$$

$$= f_2(x)(x^2 - 2\alpha x + \alpha^2 + \beta^2), \alpha, \beta \in \mathbb{R}.$$

$\Rightarrow f(x)$  è divisibile per  $(x^2 - 2\alpha x + \alpha^2 + \beta^2)$  in  $\mathbb{C}[x]$ .

• QUINDI: ogni polinomio di  $\mathbb{R}[x]$  di grado  $\geq 3$  è riducibile.

Se  $f(x) \in \mathbb{R}[x]$  è di grado 2, anche irriducibile in  $\mathbb{R}[x]$   
se non ha radice in  $\mathbb{R}[x] \Leftrightarrow$  il suo discriminante  
 $"\Delta" < 0$ .

•  $x^4 + 1 \in \mathbb{R}[x]$  è riducibile:

$$x^4 + 1 = (x^4 + 2x^2 + 1) - 2x^2 = (x^2 + 1)^2 - (\sqrt{2}x)^2 =$$

$$= (x^2 + 1 + \sqrt{2}x)(x^2 + 1 - \sqrt{2}x)$$

Conclusioni: se  $K$  campo, in  $K[x]$  tutti i polinomi di grado 1 sono irriducibili.

• se  $K = \mathbb{C}$ , non ci sono altri polinomi irriducibili in  $\mathbb{C}[x]$ .

• se  $K = \mathbb{R}$ , i polinomi irriducibili sono quelli di grado 1 e i polinomi di grado 2 della forma:  
 $\alpha x^2 + bx + c = 0, \alpha \neq 0 \text{ e } \Delta = b^2 - 4ac < 0$ .

OSS: per sapere se un polinomio di  $K[x]$  è riducibile, se il polinomio ha grado  $\leq 3$ , basta vedere se ha una radice in  $K$ .

Sia  $f \in K[x]$  di grado  $\leq 3$ , se  $f$  si "spezza" in un prodotto di fattori non unitari, nessuno di essi ha grado 1.

Quindi:  $f = f_1(ax + b)$ , d  $a \in K$ . Allora  $-ba^{-1}$  è radice di  $f$ .  
Se  $\deg f \geq 4$ , può succedere che  $f$  sia riducibile in  $K[x]$  ma che non abbia radici in  $K[x]$ .

### POLINOMI IN $\mathbb{Q}[x]$

$$\text{es: } f(x) = \frac{7}{3}x^4 + \frac{3}{5}x^2 + \frac{1}{5} \in \mathbb{Q}[x]$$

ma  $15f = 35x^4 + 9x^2 + 3$ ,  $15f \in \mathbb{Z}[x]$  sono associati.

OSS: se  $f \in \mathbb{Q}[x]$ ,  $f$  è associato ad un polinomio a coefficienti interi, cioè ad un polinomio in  $\mathbb{Z}[x]$ .

es:  $6x^2 + \frac{4}{3}x + \frac{8}{5} \in \mathbb{Q}[x]$  è associato (anche) al polinomio  $45x^2 + 10x + 12 \in \mathbb{Z}[x]$

che è un polinomio a coeff interi t.c. mcd dei suoi coeff vale 1.

• def: sia  $f(x)$  un polinomio in  $\mathbb{Q}[x]$  t.c. i suoi coeff siano numeri interi con mcd = 1. Allora  $f(x)$  si dice **POLINOMIO PRIMITIVO**.

• OSS: se  $f(x) \in \mathbb{Q}[x]$  è un polinomio, uno è associato ad un polinomio primitivo, infatti basta:

-) moltiplicare per il mcd dei denominatori dei coefficienti

-) dividere per tale mcd dei denominatori dei coefficienti

**PROP:** Siano  $f, g \in \mathbb{Q}[x]$  ( $\in \mathbb{Z}[x]$ ) PRIMITIVI.  
Allora  $f \cdot g$  è un polinomio PRIMITIVO.

**dim:** Supponiamo che  $f \cdot g$  NON sia PRIMITIVO.

Quindi il MCD dei suoi coeff. è diverso da  $\pm 1$ .

Allora sia  $p \in \mathbb{Z}$ ,  $p \neq 0, \pm 1$ , sia  $p$  PRIMO t.c.  $p | f \cdot g$  e  $p > 0$ .

Consideriamo l'applicazione  $\psi: \mathbb{Z}[x] \rightarrow \mathbb{Z}_p[x]$  t.c.  
 $\psi(x) = [x] \quad \forall x \in \mathbb{Z}, \quad \psi(x^n) = x^n, \quad \psi$  è omomorfismo, consideriamo  
 $\psi(f \cdot g) = \psi(f) \psi(g) = 0$  perché tutti i coeff. sono multipli  
di  $p \Rightarrow$  i coeff. in  $\mathbb{Z}_p$  sono 0.

$\mathbb{Z}_p[x]$  è dom. INTEGRITÀ perciò  $\mathbb{Z}_p$  campo.

Quindi:  $\psi(f) \cdot \psi(g) = 0 \Rightarrow$  uno dei due fattori è nullo in  $\mathbb{Z}_p[x]$

$\Rightarrow \psi(f) = 0 \Rightarrow$  con  $f = a_0 + a_1 x + \dots + a_n x^n$

$\psi(f) = [a_0] + \dots + [a_n] x^n = 0 \Rightarrow [a_0] = 0 \quad | p | a_0 \quad | f \text{ non è PRIMITIVO}$   
 $[a_n] = 0 \quad | p | a_n \quad (\text{ASSURDO} \times h.p.)$

**Lemma di GAUSS:** sia  $f \in \mathbb{Q}[x]$  a coeff. interi. Supp. che  $f \in \mathbb{Q}[x]$

$\exists a, b \in \mathbb{Q}[x]$  t.c.  $f = a \cdot b$ , allora  $\exists a_1, b_1 \in \mathbb{Q}[x]$  a coeff. interi t.c.  
 $a_1$  è associato ad  $a$ ,  $b_1$  è associato ad  $b$  ed  $f$  è PRODOTTO  $a_1 \cdot b_1 = f$   
[FACTORIZZAZIONE IN  $\mathbb{Z}[x]$ ]

es:  $x^2 - 4 \in \mathbb{Q}[x]$ ,  $x^2 - 4 = (3x - 2)(\frac{1}{3}x + \frac{2}{3})$

dove:  $\frac{3}{3}x - 2$  è associato a  $x^2 - 2$   
 $\frac{1}{3}x + \frac{2}{3} \quad \text{---} \quad$  o  $x + 2 \Rightarrow x^2 - 4 = (x - 2)(x + 2)$ .

**dim (Lemma di GAUSS)** ① Supp.  $f$  PRIMITIVO,  $f = a \cdot b$ ,  $a, b \in \mathbb{Q}[x]$ .

Sia  $a \in \mathbb{Q} : a_0 = a_1$  sia PRIMITIVO e  $b \in \mathbb{Q} : b_1 = b_2$  PRIMITIVO.  
Allora abbiamo che  $(a_0)(b_1) = a_1 b_1$  è PRIMITIVO perciò PRODOTTO

di PRIMITIVI.

Inoltre:  $a_0 \cdot b_2 = a_0 b_1$  e  $a_1 \cdot b_2 = a_1 b_1 \Rightarrow a_1 b_1 = a_0 b_2$  è associato ad  $f$

$\Rightarrow a_1 b_1$   
 $\Rightarrow a_1 b_1$  è PUR PRIMITIVO associato ad  $f$ , a sua volta PUR PRIMITIVO.  
 $\Rightarrow a_1 b_1 = 1 \circ a_1 b_1 = -1$

$$a_1 b_1 = a_0 b_1 \rightarrow \text{se } a_1 b_1 = 1 \Rightarrow f = a_1 b_1 \\ \rightarrow \text{se } a_1 b_1 = -1 \Rightarrow f = (-a_1) b_1$$

In entrambi i casi  $f$  è PRODOTTO di 2 polinomi a COEFF. INTERI  
associati ad  $a$  e  $b$ .

② Ora, supp.  $f$  non sia PRIMITIVO,  $f \in \mathbb{Q}[x]$ .

Sia  $d \in \mathbb{Z}$  il MCD dei coeff. di  $f$ . Quindi  $\frac{f}{d}$  è PRIMITIVO.

$\frac{1}{d} f = \frac{1}{d} a \cdot b \Rightarrow \frac{1}{d} f = a_1 b_1$ ,  $a_1$  associato a  $a$ ,  $b_1$  associato a  $b$  a coeff. interi

$f = d a_1 b_1$ , dai e  $b_1$  sono a coeff. interi associati ad  $a$  e  $b$

$\Rightarrow f$  è PRODOTTO di 2 polinomi a coeff. interi associati  
ad  $a$  e  $b$ .

**COROLARIO:** sia  $f \in \mathbb{Z}[x]$ , deg  $f \geq 1$ ,  $f$  PRIMITIVO.  
Allora  $f$  è IRREDUCIBILE in  $\mathbb{Z}[x] \Leftrightarrow f$  è IRRED. in  $\mathbb{Q}[x]$

dim:

• sia  $f$  IRREDUCIBILE in  $\mathbb{Z}[x]$ , supp. sia RIDUCIBILE in  $\mathbb{Q}[x]$  allora  
 $f = a \cdot b$  in  $\mathbb{Q}[x]$ , deg(a)  $\geq 1$  deg(b)  $\geq 1$ .  
Per il lemma di Gauss  $f = a \cdot b$  con  $a, b \in \mathbb{Z}[x]$  associati ad  $a, b$ .  
In particolare  $\deg(a) = \deg(a) \geq 1$  e  $\deg(b) = \deg(b) \geq 1$   
 $\Rightarrow f$  RIDUCIBILE in  $\mathbb{Z}[x]$  ASSURDO.

• se  $f$  IRREDUCIBILE in  $\mathbb{Q}[x]$  e non RIDUCIBILE in  $\mathbb{Z}[x]$  allora  
avrei che:  
 $f = g \cdot h$  con  $g, h \in \mathbb{Z}[x]$ ,  $\deg(g) \geq 1$   $\deg(h) \geq 1$ .  
Questo vale anche in  $\mathbb{Q}[x]$ , quindi  $f$  diventa  
RIDUCIBILE in  $\mathbb{Q}[x]$  contro ipotesi.

• es: situazione simile ma con risultati diversi.  
 $x^2 - 2 \in \mathbb{Q}[x]$  è IRREDUCIBILE in  $\mathbb{Q}[x]$ , ma in  $\mathbb{R}[x]$  è RIDUCIBILE.

• OSS: l'hp che  $f$  sia PRIMITIVO nel COROLARIO sono scrive:

$\rightarrow f = 6x^2 + 6 \in \mathbb{Z}[x]$  NON PRIMITIVO  
 $= 6(x^2 + 1) = 2 \cdot 3(x^2 + 1)$  È PRODOTTO DI 3 FATTOREI IRREDUCIBILI IN  $\mathbb{Z}[x]$ .  
 $\rightarrow 6x^2 + 6 \in \mathbb{Q}[x]$  È RIDUCIBILE,  $6x^2 + 6$  associato a  $x^2 + 1$  perché  
come in  $\mathbb{Q}$  è invertibile.

**LEMMA:** sia  $f \in \mathbb{Z}[x]$ , deg(f)  $\geq 1$ ,  $f$  PRIMITIVO, allora  $\exists q_1, \dots, q_r \in \mathbb{Z}[x]$  PRIMITIVI [chi  $q_1, \dots, q_r$  siano PRIMITIVI deriva da  $f$  PRIMITIVO]  
IRREDUCIBILI t.c.  $f = q_1 \cdots q_r$ .  
Questa FATTORIZZAZIONE È UNICA a meno di PERMUTAZIONI E SEGNO.

dim:  $f$  pensato in  $\mathbb{Q}[x]$  È PRODOTTO DI IRREDUCIBILI IN  $\mathbb{Q}[x]$ .  
 $\Rightarrow f = q_1 \cdots q_r$  con  $q_1, \dots, q_r$  IRREDUCIBILI IN  $\mathbb{Q}[x]$ .

applico LEMMA GAUSS (7 volte):  $\exists q_1, \dots, q_7$  associati a  $q_1, \dots, q_7$  t.c.  
 $f = q_1 \cdots q_7$  in  $\mathbb{Z}[x]$ . Inoltre, essendo  $q_1, \dots, q_7$  di GRADO  $\geq 1$   
anche  $q_1, \dots, q_7$  sono di GRADO  $\geq 1$ , sono anche PRIMITIVI, allora  
per COROLARIO precedente,  $q_1, \dots, q_7$  sono IRREDUCIBILI.

UNICITÀ (segue da UNICITÀ in  $\mathbb{Q}[x]$  UFD)

Sia  $f = q_1 \cdots q_r$  fattorizzazione in irriducibili in  $\mathbb{Z}[x]$ .  
Sia  $f = p_1 \cdots p_s$  un'altra fattorizzazione in irriducibili in  $\mathbb{Z}[x]$ .

Succome  $f$  è PRIMITIVO  $\deg(p_1) \geq 1, \dots, \deg(p_s) \geq 1$ . Per il corollario  
precedente sono  $p_i$  IRREDUCIBILI in  $\mathbb{Q}[x]$ .  
Quindi in  $\mathbb{Q}[x]$  abbiamo  $f = q_1 \cdots q_r = f = p_1 \cdots p_s$ .  
fattorizzazioni irriducibili in  $\mathbb{Q}[x]$ , che è UFD.

Quindi  $r = s$  inoltre, a meno di permutazioni  $q_i$  è associato  
a  $p_i$ ...

$q_1$  è associato a  $p_1 \Rightarrow q_1 = u_1 p_1$ ,  $\forall u \in \mathbb{Q}^\times$   $u^4 = 1$  in altre essere  $\pm 1$ .

• es:  $f = 12x^2 - 48 \in \mathbb{Z}[x]$   
 $= 12(x^2 - 4) = 2 \cdot 2 \cdot 3 \cdot (x-2)(x+2)$  fattorizz. in  $\mathbb{Z}[x]$  in  
fattori irriducibili.

$\rightarrow f$  in  $\mathbb{Q}[x]$  si fattorizza  $f = (2)(x-2)(x+2) = (12x-24)(x+2)$   
unitario in  $\mathbb{Q}[x]$  irriducibile in  $\mathbb{Q}[x]$

**LEMMA:** sia  $f \in \mathbb{Z}[x]$ , supp. che  $f = a \cdot f_1$ ,  $a \in \mathbb{Z}$  e  $f_1$  PRIMITIVO;  
con  $\deg(f_1) \geq 1$  e  $f = b \cdot f_2$  con  $f_2$  PRIMITIVO. Allora  $a = \pm b$  e  $f_1 = \pm f_2$ .  
esercizio)

DESENTRALIZZAZIONE

+ POLINOMI  
+ JACOBIANI

TEOREMA:  $\mathbb{Z}[x]$  è UFD.

dim: Sia  $f \in \mathbb{Z}[x]$ ,  $f \neq 0$  NON UNITARIO. Se  $\deg f = 0 \Rightarrow f$  è una costante  $\neq 0, 1, -1$ ,  $f \in \mathbb{Z}$ , lo fattorizziamo in  $\mathbb{Z}$  in IRREDUCIBILI di  $\mathbb{Z}$  ( $\mathbb{Z}$  è UFD, quindi si può fare). La fattorizzazione è anche fattorizzaz. in IRREDUCIBILI in  $\mathbb{Z}[x]$  e la fattorizzazione è UNICA perché  $\mathbb{Z}$  è UFD.

Sia  $\deg(f) \geq 1$ ,  $f = a f_1$ ,  $a \in \mathbb{Z}$  è MCD dei coeff. di  $f$ , quindi  $f_1$  è PRIMITIVA e  $\deg f_1 \geq 1$ .

Dal lemma precedente:  $f_1$  è PRODOTTO in UNICO MODO di IRREDUCIBILI di  $\mathbb{Z}[x]$ .  
 $a \in \mathbb{Z}, a \neq 0$ , se  $a \neq \pm 1$ ,  $a$  è PRODOTTO di IRREDUCIBILI in UNICO MODO in  $\mathbb{Z} \Rightarrow f$  è PRODOTTO di IRREDUCIBILI in modo UNICO.  
⇒  $\mathbb{Z}[x]$  è UFD.

PROBLEMI:

• chi sono i POLINOMI IRREDUCIBILI in  $\mathbb{Q}[x]$ ? E come si può fattorizzare un polinomio di  $\mathbb{Q}[x]$  in polinomi IRREDUCIBILI?  
Come scoprire se un polinomio in  $\mathbb{Q}[x]$  ha UN FATTORE LINEARE (FATTORE di GRADO 1)? Cioè come trovare se un polinomio in  $\mathbb{Q}[x]$  ha UNA RADICE RAZIONALE?

Sia  $f \in \mathbb{Q}[x]$ ,  $f$  è associato ad un polinomio  $g \in \mathbb{Z}[x]$  PRIMITIVO cioè  $f = n \cdot g$ ,  $n \in \mathbb{Q}$  UNITARIO,  $g$  PRIMITIVO.  
Se  $p/q \in \mathbb{Q}$  è RADICE di  $f$ , allora  $p/q$  è RADICE di  $g$  e viceversa.

$$f(p/q) = n \cdot g(p/q).$$

• Sia  $f \in \mathbb{Z}[x]$  PRIMITIVO. Sia  $f(x) = a_0 + a_1 x + \dots + a_n x^n$ ,  $a_i \in \mathbb{Z} \forall i$ .  
Sia  $p/q \in \mathbb{Q}$  t.c.  $f(p/q) = 0$ . Allora  $a_0 + a_1(p/q) + \dots + a_n(p/q)^n = 0$ ,  
Supp.  $\text{MCD}(p, q) = 1$ ,  $\text{mcm}(p, q) = p \cdot q$ .

moltiplichiamo per  $q^n \Rightarrow a_0 q^n + a_1 p q^{n-1} + \dots + a_{n-1} p^{n-1} q + a_n p^n = 0$   
metto  $q$  in evidenza:  $q(a_0 q^{n-1} + a_1 p q^{n-2} + \dots + a_{n-1} p^{n-1}) = -a_n p^n$   
siccome  $q < p$  sono primi tra loro, anche  $q$  e  $p^n$  sono primi tra loro. Poiché  $q$  divide  $a_n p^n$  e  $q$  e  $p^n$  sono coprimi, abbiamo che  $q$  deve dividere  $a_n$ .

In modo analogo (mettendo in evidenza  $p$ ) abbiamo che  $p$  divide  $a_0$ .  
Quindi un numero RAZIONALE  $p/q$  che sia zero se  $f$  va cercato tra il numero finito di FRAZIONI del tipo  $\frac{a}{b}$  con  $a$  divisore di  $a_0$  e  $b$  divisore di  $a_n$ .

NOTA: è possibile che la radice non esista.

10: troviamo eventuali RADICI RAZIONALI di  $2x^3 + 3x^2 + x - 15$

Saranno del tipo:  $p/q$  con  $q$  divisore di 2 e  $p$  divisore di 15  
 $q \in \{1, 2, -2, -1, 4\}$ ,  $p \in \{1, 3, 5, -1, -3, -5, 15, -15\}$ .

Possibili SOLUZIONI:  $\left| \begin{array}{c} \frac{1}{1}, \frac{3}{1}, \frac{5}{1}, \frac{15}{1}, \frac{1}{2}, \frac{3}{2}, \frac{5}{2}, \frac{15}{2} \end{array} \right|$   
e soluzioni.

$$15: m \cdot x = 441x^2 + 220, \quad q | 441$$

le possibili  $p/q$  sono 216 e nessuna è soluzione  
(PROBLEMA)

### \* CRITERIO di EINSTEIN

Sia  $f(x) \in \mathbb{Z}[x]$  digr. 7.2. & PRIMITIVO,  $f = a_0 + a_1 x + \dots + a_n x^n$ ,  
Supp.  $\exists p \in \mathbb{N}$  Primo t.c.  $p \mid a_0, p \nmid a_1, \dots, p \nmid a_n$ ,  $p^2 \nmid a_0$ .

Allora  $f$  è IRREDUCIBILE n.m.  $\mathbb{Q}(x)$  e  $\mathbb{Z}(x)$ .

$\exists$ :  $x^2 + 7$  n.m. EINSTEIN è VERA, anche  $x^3 + 7, x^3 + 7x^2 + 7$

$x^2 + p, p$  PRIMO SONO INFINTI POLINOMI IRREDUCIBILI PER EINSTEIN  
 $n \in \mathbb{N}, n \geq 2$

Il CR EINSTEIN fornisce condiz. NECESSARIA, ma NON SUFFIC.

$\exists$ : c'è un polin. irriducibile di grado 2 che non soddisfi nei  
il Criterio di EINSTEIN.

$x^2 + 1, x^2 + 4$  unico primo che divide 4 | 2, ma  $2^2 \nmid 4$

OLM (IDEA): studiamo in senso PARTICOLARE

Supp. che  $f$  sia polinomio irriducibile t.c. per esempio,  
Sia il PRODOTTO di due polinomi di grado 2.

Quindi:  $f = (b_0 + b_1 x + b_2 x^2)(c_0 + c_1 x + c_2 x^2)$

$$a_0 = b_0 c_0$$

$$a_1 = b_0 c_1 + b_1 c_0$$

$$a_2 = b_0 c_2 + b_1 c_1 + b_2 c_0$$

$$a_3 = b_1 c_2 + b_2 c_1$$

$$a_4 = b_2 c_2$$

dalle ip. del teorema  $p \mid a_0 = b_0 c_0, p$  PRIMO  
 $\Rightarrow p \mid b_0 \circ p \mid c_0$  ma non entrambi  
 $\Rightarrow p$  divide uno solo tra  $b_0$  e  $c_0$   
altrimenti  $p^2$  dividerebbe  
il precedente  $b_0 c_0 \Rightarrow p^2 \mid a_0$  contro ip.

$p \mid a_1 = b_0 c_1 + b_1 c_0 \Rightarrow p \mid b_0 c_0 \Rightarrow p \mid b_1 \circ p \mid c_0$ , ma  $p \nmid c_0 \Rightarrow p \mid b_1$ .

$p \mid a_2 \Rightarrow p \mid b_0 c_2 + \dots \Rightarrow (\dots) \Rightarrow p \mid b_2 c_0 \Rightarrow p \mid b_2$

$p \mid a_3 = b_2 c_2$  una poch' p  $p \mid b_2$  ASSURDO perché  $p \nmid a_3$  per ip.

### CARATTERISTICA DI UN ANELLO

Sia  $A$  anello comm. unitario, se  $n \in \mathbb{N} \subset A \otimes A$ , allora  $\underbrace{a + \dots + a}_{n\text{-volte}} = \underbrace{(n \cdot a)}_{\text{elemento dell'anello}}$

se  $n$  è NEGATIVO, cioè  $-n \in \mathbb{N}$ , si pone  $n \cdot a = \underbrace{(-a) + \dots + (-a)}_{-n\text{-volte}}$  " $-n$  volte"

$a \text{ def. } = 0, a = 0$ .

In questo modo abbiamo definito il PRODOTTO  $n \cdot a \forall n \in \mathbb{Z}, \forall a \in A$ .

In particolare vale: se  $n = r-s$  in  $\mathbb{Z}$ , allora  $n \cdot a = r \cdot (s \cdot a)$

infatti,  $n \cdot a = \underbrace{(a + \dots + a)}_{r\text{-volte}} + \underbrace{(-a - \dots - a)}_{s\text{-volte}} + \dots + \underbrace{(-a - \dots - a)}_{s\text{-volte}} =$

$$= \underbrace{(s \cdot a)}_{r\text{-volte}} + \dots + \underbrace{(s \cdot a)}_{r\text{-volte}} = r \cdot (s \cdot a)$$

Se  $n < 0$  o  $n > 0$  si procede in modo analogo.

Si consideri l'applicazione  $\psi: \mathbb{Z} \rightarrow A$  t.c.  $\psi(n) = \underbrace{n \cdot z}_{n\text{-volte}} = \underbrace{z + \dots + z}_{n\text{-volte}}$

$\psi$  è omomorfismo.

$$\cdot \psi(m+n) = (m+n) \cdot z = \underbrace{z + \dots + z}_{m\text{-volte}} + \underbrace{z + \dots + z}_{n\text{-volte}} = \psi(m) + \psi(n)$$

$$\cdot \psi(m \cdot n) = m \cdot n \cdot z = \underbrace{(z + \dots + z)}_{m\text{-volte}} \cdot \underbrace{(z + \dots + z)}_{n\text{-volte}} = \psi(m) \cdot \psi(n)$$

$$\begin{aligned} \psi(m) \cdot \psi(n) &= (z + \dots + z) \cdot (z + \dots + z) = \underbrace{\underbrace{z \cdot z + z \cdot z + \dots + z \cdot z}_{m\text{-volte}} + \dots + \underbrace{z \cdot z + z \cdot z + \dots + z \cdot z}_{n\text{-volte}}}_{m \cdot n \text{-volte}} \\ &= (m \cdot n) \cdot z = \psi(m \cdot n) \end{aligned}$$

DEFINIZIONE

POLINOMI  
+ VARIABILI

Quindi  $\psi: \mathbb{Z} \rightarrow A$  t.c.  $\psi(n) = n \cdot 1$  è omom. di ANELLI.

Per tra. omom.:  $\mathbb{Z}/\text{Ker } \psi \cong \text{Im } \psi \subseteq A$ .

Chi è  $\mathbb{Z}/\text{Ker } \psi$ ?  $\text{Ker } \psi$  è IDEALE di  $\mathbb{Z}$ , ed è principale, cioè  $\text{Ker } \psi$  è generato da  $c \in \mathbb{N} \Rightarrow \text{Ker } \psi = (c)$ .

Quindi  $\mathbb{Z}/\text{Ker } \psi = \mathbb{Z}_c$  ANELLO CLASSE dei RESTI.

Se  $c \neq 0 \Rightarrow \mathbb{Z}_c$  è l'anello  $\mathbb{Z}/(c)$  che ha  $c$ -elementi.

M.  $c = 0 \Rightarrow \mathbb{Z}_c = \mathbb{Z}$ .

- Def: il numero  $c$  si chiama CARATTERISTICA dell'anello  $A$ .  
Quindi un anello ha una CARATTERISTICA che può essere ZERO o un numero FINITO.

$\mathbb{Z} \xrightarrow{\psi} A$   $\psi(n) = n \cdot 1$ ;  $\text{Ker } \psi = \{n \in \mathbb{Z} \text{ t.c. } \psi(n) = 0 \Rightarrow n \cdot 1 = 0\}$

$\Rightarrow \text{Ker } \psi = \{0\} \Rightarrow \text{Ker } \psi = (0)$  significa  $\{n \in \mathbb{Z} / n \cdot 1 = 0\} = \{0\}$   
cioè:  $n \cdot 1 \neq 0$  se  $n \neq 0$ .

Se  $\text{Ker } \psi \neq (0)$ , allora il generatore  $c$  di  $\text{Ker } \psi$  è il minimo tra gli  $n \in \mathbb{Z}_{>0}$  t.c.  $n \cdot 1 = 0$ . Cioè la CARATTERISTICA è il minimo numero t.c.  $n \cdot 1 = 0$ .

→ Come calcolare la caratteristica di un ANELLO?

Sia  $A \in A$ , cons. del caso:  $1, 1+1, 1+1+1, \dots$  se NON si ottiene mai 0, la CARATTERISTICA di  $A$  è 0 ( $c=0$ ); se ottengono ad un certo punto 0, il NUMERO di SOMME di 1 che per la PRIMA VOLTA da 0 è la CARATTERISTICA dell'anello  $A$ .

Ese:  $\mathbb{Q}, \mathbb{R}, \mathbb{Z}$  sono tutti anelli di CARATT. ZERO.  $\left\{ \begin{array}{l} 1+1=2 \neq 0 \\ 1+1+1=3 \neq 0 \\ \dots \neq 0 \end{array} \right.$

in  $\mathbb{Z}_7$ :  $[1] \neq [0]$   
 $[1] + [1] = [2] \neq [0]$   
 $\dots$   
 $[1] + \dots + [1] = [7] = [0]$   
 $\quad \quad \quad 7\text{-volte}$

$\left\{ \begin{array}{l} \mathbb{Z}_7 \text{ ha CARATTERISTICA } 7. \\ \Rightarrow \text{Ker } \psi = (7) \end{array} \right.$

In generale: ogni ANELLO UNITARIO ha CARATTERISTICA ( $\neq 0$ )  
Inoltre, se  $A$  è ANELLO di CARATTERISTICA  $c$ , anche  $A[\alpha]$  ha CARATT.  $c$ .

• PROP: se  $A$  DOM. INTEGRITÀ, allora  $A$  ha CARATT. 0 oppure un num. PRIMO.

dimm: se  $A$  non avesse caratter. 0, sia  $c$  la sua caratteristica, se  $c$  non fosse PRIMO  $\Rightarrow c = a \cdot b$ .

Considero  $c \cdot 1 = 0$ ,  $(a \cdot b) \cdot 1 = 0 \Rightarrow (a \cdot 1) \cdot (b \cdot 1) = 0$  PRODOTTO in  $A$ , ma  $A$  è DOM. INTEGRITÀ, allora  $a \cdot 1 = 0$  o  $b \cdot 1 = 0$  con  $a < c$ ,  $b < c$  e questo è ASSURDO  $\Rightarrow c$  È PRIMO.

TEOREMA

• CONSEG: se  $K$  CAMPO,  $K$  può avere solo caratteristica 0 o caratter. un NUMERO PRIMO.

• PROP: sia  $A$  anello di caratteristica  $p$ , con  $p$  PRIMO, siano  $a, b \in A$ , allora vale:  $(a+b)^p = a^p + b^p$

dimm:  $(a+b)^p = (a+b)(a+b) \dots (a+b)$   $p$ -volte moltiplicazione  
 $= a^p + \binom{p}{1} a^{p-1} b + \binom{p}{2} a^{p-2} b^2 + \dots + \binom{p}{p-1} a b^{p-1} + b^p$

Sviluppo BINOMIO NEWTON: sia  $\binom{p}{r}$  con  $r = 1, \dots, p-1$

$$\binom{p}{r} = \frac{p!}{(p-r)! r!} \in \mathbb{N}, i fattori di  $r!$  sono tutti  $\leq p-1$ , come$$

anche i fattori di  $(p-r)!$ .

Essendo  $p$  PRIMO, il fattore  $p$  del numeratore NON si cancella mai con alcun elemento del denominatore.

$\Rightarrow (P)$  è sempre minore di  $p$ ,  $\forall r=1, \dots, p-1$ .

Se  $A$  è di caratteristica  $p \Rightarrow P \cdot 1 = 0$  e  $n$  è un multiplo di  $p$   
 $\Rightarrow n \cdot 1 = (q \cdot p) \cdot 1 = q(p \cdot 1) = 0$ .

Quindi:  $\binom{n}{r} a^{P-r} b^r = 0 \quad \forall r=1, \dots, p-1 \Rightarrow (a+b)^P = a^P + b^P$ .  
(RIMANGONO SOLO questi termini).

NOTA: in campo di caratteristica 0 è infinito.

Sia  $K$  campo di CARATTERISTICA  $p$  (prima) e  $\psi$  si d. l'applicazione  
 $\psi: K \rightarrow K$  c.  $\psi(a) = a^p \quad \forall a \in K$ .

Vale che:  
•  $\psi(a+b) = (a+b)^p = a^p + b^p = \psi(a) + \psi(b)$   
•  $\psi(a \cdot b) = (a \cdot b)^p = a^p b^p = \psi(a) \psi(b)$ .  
•  $\ker(\psi) = \{0\}$

$\Rightarrow \psi$  è un OMOMORFISMO di ANELLI INIEZTIVO, detto  
MONOMORFISMO di FROBENIUS.

Se  $K$  è FINITO,  $\psi$  è anche SURIEZTIVO.

def: il campo  $K$  si dice CAMPO PERFETTO se  $\psi$  suriettivo. Cioè in  $K$  ogni elemento ha radice  $p$ -esima.  
suriettività:  $\forall b \in K \exists a \in K : \psi(a) = b \Rightarrow a^p = b \Rightarrow a = \sqrt[p]{b}$ .

Se  $K$  campo FINITO di CARATTER.  $p|K$  è CAMPO PERFETTO, in particolare  $\mathbb{Z}_p$  (p primo) è campo PERFETTO.

$a \in \mathbb{Z}_p$ ,  $\sqrt[p]{a} = b$  può essere TECERMINI:  $a^p = a \quad \forall a \in \mathbb{Z}_p$ .  
In questo caso l'omom. di FROBENIUS è l'IDENTITÀ.

Se  $\mathbb{Z}_{p^n}$  ha caratteristica  $p$ , è INFINTO ma non è campo.  
perché è dominio di INTEGRITÀ.

Campo dei QUOTIENTI:  $\Omega(\mathbb{Z}_{p^n})$  è esempio di campo INFINTO di CARATTERISTICA  $p$ .

def: sia  $K$  campo,  $f(x) \in K[x]$  con  $f(x) = a_0 + a_1 x + \dots + a_n x^n$ .  
Si dice DERIVATO di  $f(x)$  il seguente polinomio:

$$D(f(x)) = a_1 + 2a_2 x + 3a_3 x^2 + \dots + n a_n x^{n-1}, \text{ dove } n a_n = a_{n+1} + \dots + a_m \text{ u-volti}$$

$x$  non è elem. del campo.

$$\text{Vale: } D(f(x) + g(x)) = D(f(x)) + D(g(x))$$

$$D(f(x) \cdot g(x)) = D(f(x)) \cdot g(x) + f(x) \cdot D(g(x))$$

$$D(a) = 0 \quad \forall a \in K \quad D(D(f(x))) = D(D(f(x))) \cdot D(g(x))$$

verifica (REGOLA PRODOTTO):

$$1. f(x) = a_n x^n, \quad g(x) = b_n x^n$$

$$D(f(x) \cdot g(x)) = D(a_n b_n x^{m+n}) = (m+n) a_n b_n x^{m+n-1}$$

$$D(f(x) \cdot g(x)) + f(x) D(g(x)) = (m+n) a_n b_n x^{m+n-1} b_n x^n + a_n b_n (n b_n x^{m+n-1}) = \\ = a_n b_n m x^{m+n-1} + a_n b_n n x^{m+n-1} = a_n b_n (m+n) a_n b_n x^{m+n-1}$$

$$2. f(x) = a_n x^n, \quad g(x) = b_n + b_1 x + \dots + b_m x^m$$

$$D(f(x) \cdot g(x)) = D(a_n b_n x^{m+n} + a_n b_1 x^{m+n-1} + \dots + a_n b_m x^m) = \\ = a_n b_n m x^{m+n-1} + \dots + (m+n) a_n b_m x^{m+n-1}$$

$$- D(f) \cdot g + f \cdot D(g) = m a_n x^m (b_1 + \dots + b_m x^{m-1}) + a_n x^m (b_1 + \dots + b_m x^{m-1})$$

i le due espressioni sono uguali.

DEFINIZIONE

+ POLINOMI  
+ VERSAMENTE

3. se  $f = a_0 + a_1x + \dots + a_mx^m$  allora

$$\begin{aligned} D(f \cdot g) &= D(a_0 g) + D(a_1 x g) + \dots + D(a_m x^m g) = \\ &= D(a_0)g + a_0 D(g) + D(a_1 x)g + a_1 x D(g) + \dots + D(a_m x^m)g + \\ &\quad + a_m x^m D(g) \\ &= (D(a_0) + \dots + D(a_m x^m))g + (a_0 + a_1 x + \dots + a_m x^m)D(g) = \\ &= D(f)g + f \cdot D(g). \end{aligned}$$

Se  $f$  è del tipo:  $f = g_1^e \cdot g_2$ , es.  $[e \geq 1]$ .

$$\sim D(f) = D(g_1^e \cdot g_2) = D(g_1^e)g_2 + g_1^e D(g_2)$$

avendo  $f$ , calcolo  $D(f)$  e  $\text{mcd}(f, D(f))$  e trovo dei fattori multipli di  $f$ .

es:  $f = x^3 + 3x^2 \in \mathbb{Q}[x] \quad D(f) = 3x^2 + 6x$

$$\begin{aligned} \text{mcd}(x^3 + 3x^2, 3x^2 + 6x) &= \text{mcd}(x^3 + 3x^2 - x(x^2 + 2x), x^2 + 2x) = \\ &= \text{mcd}(x^2, x^2 + 2x) = \text{mcd}(0, x) = x. \end{aligned}$$

• PROPS: Sia  $K$  campo di caratteristica  $0$ . Sia  $f \in K[x]$  t.c.  $D(f) = 0$ . Allora  $f = a_0$ ,  $a_0$  costante di  $K$ .

Se  $K$  ha caratteristica  $p \neq K$  è perfetto, e se  $D(f) = 0$  allora  $\exists g \in K[x]$  t.c.  $f = g^p$ .

dim: sia  $f = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ .

$$D(f) = a_1 + 2a_2x + \dots + na_nx^{n-1} = 0 \quad \text{PRINCIPIO DI IDENTITÀ} \quad \left\{ \begin{array}{l} a_1 = 0 \\ 2a_2 = 0 \\ \vdots \\ na_n = 0 \end{array} \right\} \quad \left\{ \begin{array}{l} a_1 = 0 \\ (2-1)a_2 = 0 \\ \vdots \\ (n-1)a_n = 0 \end{array} \right\}$$

se caratteristica è zero,  $f \neq 0 \quad \forall k$ , in  $K$  campo  $\Rightarrow$  il fattore è 0.

$\Rightarrow \left\{ \begin{array}{l} a_1 = 0 \\ a_2 = 0 \\ \vdots \\ a_n = 0 \end{array} \right\} \Rightarrow f = a_0$  costante.

$$\text{se caratteristica è } p: \left\{ \begin{array}{l} a_1 = 0 \\ (p-1)a_2 = 0 \\ \vdots \\ (p-1)a_p = 0 \\ (2p-1)a_{2p} = 0 \\ \vdots \\ (n-1)a_n = 0 \end{array} \right\} \quad \begin{array}{l} \text{non abbiam alcuna} \\ \text{condiz. su } a_p, a_{2p}, \dots \end{array}$$

Quindi, non avendo alcuna condiz. sui coeff.  $a_p, a_{2p}, \dots$ , ottieniamo

$$D(f) = 0 \quad \text{in } f = a_0 + a_1x^p + \dots + a_kx^k$$

in  $K$  perfetto  $\Rightarrow \exists b_0, b_1, \dots, b_k$ :  $a_0 = b_0^p, \exists b_1: a_1 = b_1^p, \dots, \exists b_k: a_k = b_k^p$

$$\Rightarrow f = b_0^p + (b_1^p x^p)^p + \dots + (b_k^p x^k)^p = (b_0 + b_1 x + \dots + b_k x^k)^p$$

$$\Rightarrow f = g^p, g \in K[x].$$

TEOREMA: sia  $K$  campo,  $f \in K[x]$ , se  $f$  ha un fattore multiplo allora  $\text{mcd}(f, D(f)) \neq 1$  cioè non è unitario.

Se  $K$  è di carattere 0, o è perfetto di carattere  $p$ , vale che se  $\text{mcd}(f, D(f)) \neq 1$ , allora  $f$  ha fattore multiplo.

dimo: sia  $K$  qualunque,  $f = g^e \cdot h$ ,  $e \geq 2$ . Allora  $D(f) = D(g^e) \cdot h + g^{e-1} D(h)$

$$= e g^{e-1} D(g) \cdot h + g^e D(h) = g^{e-1} (e D(g) \cdot h + g D(h))$$

Quindi  $f$  e  $D(h)$  hanno in comune il fattore  $g^{e-1}$   
 $\Rightarrow \text{mcd}(f, D(f)) \neq 1$ .

Viceversa: sia  $f \in K[x]$ ,  $\text{mcd}(f, D(f))$  non unitario,  
 sia  $q$  fattore irriducibile di  $\text{mcd}(f, D(f))$ , cioè  $q | f$   
 $\Rightarrow f = q \cdot h$ , quindi  $D(f) = D(q) \cdot h + q D(h)$ .

$q | D(f) \Rightarrow q$  divide  $D(q) \cdot h$ ,  $q$  è primo  $\Rightarrow q | D(q) \circ q | h$ .

Caso 1:  $q | h$ , allora  $h = q \cdot l \Rightarrow f = q \cdot h = q \cdot q \cdot l = q^2 \cdot l$   
 $\Rightarrow f$  ha un fattore multiplo

Caso 2:  $q | D(q)$ ,  $D(q)$  polinomio con  $\deg(D(q)) < \deg(q)$ .

$q | D(q) \Rightarrow D(q) = 0$ .

Se la caratteristica di  $K$  è  $c = 0$ ,  $q$  è costante  $\Rightarrow$  ASSURDO  
 Tuttavia  $q$  è IRRIDUCIBILE  $\Rightarrow \deg(q) \geq 1$ .

Se  $K$  non è  $\mathbb{F}_p$ ,  $K$  perfetto,  $D(q) = 0 \Rightarrow q = g \cdot p$  (pero),  
 anche in questo caso si arriva ad un ASSURDO, dato che  
 $q$  è IRRIDUCIBILE  $\Rightarrow$  NON può essere un PRODOTTO.

$$\Leftrightarrow K = \mathbb{Q}, f = (x-1)(2x-2)(x-3) \left( \frac{1}{7}x - \frac{3}{7} \right) = \frac{2}{7}(x-1)^2(x-3)^2$$

in questo modo  $f \in K[x]$ ,  $K$  campo,  $\deg(f) \geq 1$  si può scrivere nella forma:  $f = n p_1^{a_1} \dots p_r^{a_r}$

con:  $a_1, \dots, a_r \geq 1$   
 $p_1, \dots, p_r$  a  $\geq 2$  non associati  
 in elem. UNITARIO.

CONGRUENZE TRA POLINOMI IN  $K[x]$ .

Sia  $K$  campo,  $f, g, h \in K[x]$  allora si dice che  $f$  è congruo a  $g$  se modulo  $h$   $f \equiv g$  mod  $h$  se vale:

$h$  divide  $f - g$  o, equivalentemente, il resto della divisione di  $f$  per  $h$  coincide con il resto della divisione di  $g$  per  $h$ .

o equivalentemente, se  $[f] = [g]$  nell'anello quoziente  $\frac{K[x]}{(h)}$   
 QUOTIENTE IN  $K[x]$ :

sia  $I$  ideale di  $K[x]$ ,  $I$  è PRINCIPALE quindi  $\exists h \in K[x]$  t.c.  
 $I = (h) = \{ \alpha h / \alpha \in K[x] \}$

$\Leftrightarrow$  tra  $\mathbb{Z}$  che è in "buon rappresentante di  $[47]$ ?  
 dividiamo 47 per 8 e si guarda il resto  
 (in questo caso il resto è 7,  $47 \leq 8$  quindi va bene)

Sia  $[f] \in K[x]$ , un buon rappres. per  $[f]$  potrebbe

essere il RESTO della divisione di  $f$  per  $h$ .  
 $\Rightarrow f = q \cdot h + r$   $\deg(r) < \deg(h)$ .

$\Rightarrow [f] = [r]$ ; osserviamo: se  $[f] = [r]$  e  $[f] = [q]$  con  $\deg(r) < \deg(h)$   
 $\deg(r) < \deg(h) \Rightarrow r = 0$  perché il RESTO della  
 divisione di  $f$  per  $h$  è UNICO

BENEFICIO

+ POLINOMI  
+ VARIAZIONI

Quindi, se  $h = a_0 + a_1x + \dots + a_nx^n$ , i polinomi  $[\&]$  rappresentati dal resto della divisione per  $h$  sono del tipo seguenti:

$$r = b_0 + b_1x + \dots + b_{n-1}x^{n-1}; b_0, \dots, b_{n-1} \in K$$

Quindi gli elementi di  $K[x]/(h)$  sono della forma

$$[b_0 + b_1x + \dots + b_{n-1}x^{n-1}] = [b_0][1] + [b_1][x] + \dots + [b_{n-1}][x^{n-1}]$$

con  $b_0, b_1, \dots, b_{n-1} \in K$ .

sia  $\deg(h) \geq 1$ .

In questo caso  $[b] = [b']$  con  $b, b' \in K$  equivale a dire che  $h$  divide  $(b - b')$ . Quindi  $b - b' = 0$ , cioè  $b = b'$ .

Allora in  $K[x]$  vale:  $[b] = [b'] \Leftrightarrow b = b' \forall b, b' \in K$ .

in altre parole:  $K[x]/(h)$  contiene una copia di  $K$ .

$\Rightarrow K = \mathbb{Q}$ ,  $K[x]/(h) = A$  anello,  $[x^5 + 6x + 3] \in A$

dividiamo  $x^5 + 6x + 3$  per  $x^2 - 4$  per ottenere un rappresentante migliore della classe.

$$(x^5 + 6x + 3) - x^3(x^2 - 4) = 4x^3 + 6x + 3$$

$$(4x^3 + 6x + 3) - 4x(x^2 - 4) = 22x + 3$$

$$\text{Quindi: } x^5 + 6x + 3 = (x^3 + 4x)(x^2 - 4) + 22x + 3$$

$$\Rightarrow [x^5 + 6x + 3] = [22x + 3] = [22x] + [3] = 22[x] + 3[1].$$

$$\rightarrow [\&] = b_0[1] + b_1[x] \quad ; \quad b_0, b_1 \in \mathbb{Q}$$

è comb. lineare a coeff. in  $K = \mathbb{Q}$  di  $[1]$  e  $[x]$ .

**TEOREMA:** Sia  $K$  campo,  $h \in K[x]$  di  $\deg h \geq 1$ . Consideriamo l'ANELLO QUOTIENTE  $K[x]/(h)$ . Questo è uno SPAZIO VETTORIALE in  $K$  di dimensione  $\deg(h)$  e avrà una base data da  $[1], [x], \dots, [x^{n-1}]$ .

dim:

1.  $K[x]/(h)$  contiene una copia del campo  $K$ , infatti se  $b, b' \in K$  vale che  $[b] = [b'] \Leftrightarrow b = b'$ .

Quindi se  $[b] \in K[x]/(h)$ , con  $b \in K$  e  $[\&] \in K[x]/(h)$ ,  $\& \in K[x]$ ,

il PRODOTTO  $[b] \cdot [\&] = [b \cdot \&]$  può anche essere visto come  $b \cdot [\&] \Rightarrow$ , quindi come prodotto:  $K \times \frac{K[x]}{(h)} \rightarrow \frac{K[x]}{(h)}$

2.  $r[\&] \in K[x]/(h)$  supp. che  $r[\&] = [r]$  con  $r$  resto della divisione di  $f$  per  $h$ .

Quindi  $r = b_0 + b_1x + \dots + b_{n-1}x^{n-1}$ ;  $b_0, \dots, b_{n-1} \in K$  e  $\deg(r) < \deg(h)$ .

$$[\&] = b_0[1] + b_1[x] + \dots + b_{n-1}[x^{n-1}], b_0, \dots, b_{n-1} \in K.$$

Quindi  $[r]$  è comb. lin. a coeff. in  $K$  di  $[1], \dots, [x^{n-1}]$   
cioè  $[1], [x], \dots, [x^{n-1}]$  è sistema di generatori di  $K[x]/(h)$ .

Sono lin. indip.  $\lambda_0[1] + \lambda_1[x] + \dots + \lambda_{n-1}[x^{n-1}] = 0$ ,  $\lambda_i \in K$

$$\Rightarrow \lambda_0 + \lambda_1 x + \dots + \lambda_{n-1} x^{n-1} \text{ è multiplo di } h, \text{ di grado } n$$

$\Rightarrow$  deve essere polinomio nullo.

Per PRINCIPIO IDENTITÀ dei polinomi, i coeff.  $\lambda_i = 0 \ \forall i$

es: trovare divisioni dello zero in  $\mathbb{Q}[x]$   
 $(x^2+4)$

la classe  $[x^2+4]$  è divisore dello zero,  $[x^2+4] \neq 0$   
ma non ha grado < deg( $x^2+4$ ) e non è polinomio nullo.

$[x^2+2]$  è div. zero (ma non è t.c.)  
 $[x-2][x+2] = [x^2-4] = 0$ .

Ne cerchiamo altri: sia  $[b_0 + b_1 x]$  germino  
dell'elemento di  $K[x]$ , sia  $[a_0 + a_1 x]$  t.c.

$$[b_0 + b_1 x][a_0 + a_1 x] = 0 \quad ; \quad b_0, a_0, b_1, a_1 \in K.$$

$$\Rightarrow [b_0 a_0 + b_0 a_1 x + b_1 a_0 x + b_1 a_1 x^2] = [x(b_0 a_1 + b_1 a_0) + 4a_1 b_1 + 4a_0 b_1] = \\ (b_0 a_0 + b_0 a_1 x + b_1 a_0 x + b_1 a_1 x^2) - (b_0 a_1 x^2 + 4a_1 b_1 x^2) = 4a_1 b_1 + 2(a_0 a_1 + b_1 a_0) + b_0 a_0 \\ = [1] (b_0 a_0 + 4a_1 b_1) + (a_0 a_1 + b_1 a_0) x^2 = 0$$

sistema:  $\begin{cases} b_0 a_0 + 4a_1 b_1 = 0 & ; \quad a_0 a_1 + b_1 a_0 = 0 \\ b_0 a_1 + b_1 a_0 = 0 \end{cases}$

$$\rightarrow \begin{cases} b_0/b_1 & a_0 + 4a_1 = 0 \\ b_0 + b_1 a_0/a_1 = 0 & \end{cases} \quad ; \quad \begin{cases} b_0 = -b_1 a_0/a_1 & \\ -a_0/a_1 \cdot a_0 + 4a_1 = 0 & \end{cases}$$

$$\rightarrow -a_0^2 + 4a_1 = 0 \Rightarrow a_0^2 - 4a_1^2 = 0 \Rightarrow (2a_1 + a_0)(2a_1 - a_0) = 0 \\ a_0 = 2a_1 \\ a_0 = -2a_1$$

$$\Rightarrow [a_0 + a_1 x] = [2a_1 + a_1 x] = a_1 [x+2] \text{ se } a_0 = 2a_1$$

analoga mani:  $[b_0 + b_1 x] = a_1 [2-x] \text{ se } a_0 = -2a_1$ .

continuando sul sistema si ottiene che:

$$[b_0 + b_1 x] \text{ è div. zero} \Rightarrow$$

$[b_0 + b_1 x]$  è associato a  $2-x$  o  $2+x$

### TEO. CHINSE DEI RESTI (POLINOMI ad 1 VARIABILE)

siano  $m_1, \dots, m_k \in K[x]$  i k campi polinomi a 2 a 2 coprimi  
 $\text{deg}(\text{cdm}(m_i, m_j)) = 1 \quad \forall i \neq j \quad \& \quad f_1, \dots, f_k \in K[x]$

Allora il sistema di congruenze:  $\begin{cases} T \equiv f_1 \pmod{m_1} \\ \vdots \\ T \equiv f_k \pmod{m_k} \end{cases}$

ha una soluzione se

$$Se T_1 \text{ e } T_2 \text{ sono 2 soluzioni, allora } T_1 \equiv T_2 \pmod{m_1 \cdots m_k}.$$

Se imponiamo a T di aver grado minore di  $\text{deg}(m_1 \cdots m_k)$ , allora T è unico ( $\text{deg}(m_1 \cdots m_k) = \text{deg}(m_1) + \cdots + \text{deg}(m_k)$ ).

Supp. ora  $m_1, \dots, m_k$  di grado 1, quindi saranno del tipo:  
 $(x-a_1), \dots, (x-a_n)$  con  $a_1, \dots, a_n \in K$ . coprimi

• Congruenza di due polinomi  $f \equiv g \pmod{x-a}$ :  $f \equiv g \pmod{(x-a)}$ ?

$(x-a) | (f-g)$  quando  $(f-g)(a) = 0 \Leftrightarrow f(a) = g(a)$ .

• TEOREMA: siano  $a_1, \dots, a_n \in K$  a 2 a 2 distinti, siano  $b_1, \dots, b_n \in K$  qualsiasi, allora  $\exists!$  polinomio  $T(x) \in K[x]$  di grado  $\leq n-1$  t.c.  $T(a_i) = b_i, \dots, T(a_n) = b_n$ .

DIM: nel teo chino dei resti prendiamo  $m_i = x - a_i$ ,  $f_i = b_i x$ .  
 $\exists! T$  di grado  $\leq n-1$  t.c.  $\text{deg}(m_1) + \cdots + \text{deg}(m_n) = n$  (ma non hanno tutti  $\text{deg} = 1$ ) t.c.

$$\begin{cases} T \equiv b_1 \pmod{x-a_1} \\ \vdots \\ T \equiv b_n \pmod{x-a_n} \end{cases} \Leftrightarrow \begin{cases} T(a_1) = b_1 \\ \vdots \\ T(a_n) = b_n \end{cases}$$

• METODO di FATTORIZZAZIONE di polinomi in  $\mathbb{Z}_p[x]$ , p PRIMO.

$$\text{es: } x^{10} + 6x^5 + 2x^3 - 4x^2 + 2x + 1 \in \mathbb{Z}_3[x]$$

si può fattor in  $\mathbb{Z}$  finito di passi ma è lungo  
con tecniche usate fino ad ora.

1 metodo:

1. Siano  $f, g$  due polinomi di  $\mathbb{Z}_p[x]$  t.c. sono primi fra loro.  
Sia  $h \in \mathbb{Z}_p[x]$ . Allora  $\text{mcd}(h, f \cdot g) = \text{mcd}(h, f) \cdot \text{mcd}(h, g)$ .

2. il polinomio  $x^p - x \in \mathbb{Z}_p[x]$ , per il piccolo teorema di Fermat ha tutti gli elementi di  $\mathbb{Z}_p$  come radici.

$$\text{Allora } x^p - x = (x - 0)(x - 1) \dots (x - (p-1))$$

3.  $x \in \mathbb{Z}_p[x]$  allora  $g^p - g = (g - 0)(g - 1) \dots (g - (p-1))$   
questa uguagli si vede se si considera l'applicazione:

$$4: \mathbb{Z}_p[x] \rightarrow \mathbb{Z}_p[x] \text{ t.c.: } 4(a) = a \quad \forall a \in \mathbb{Z}_p$$

un'extensione,  $4$  è omomorfismo di anelli.

$$4(x^p - x) = 4(x^p) - 4(x) = g^p - g$$

$$4((x-0)(x-1) \dots (x-(p-1))) = [4(x_1 - 4(0))] \cdot [4(x_1 - 4(1))] \dots [4(x_1 - 4(p-1))] \\ = (g - 0)(g - 1) \dots (g - (p-1)).$$

• TEOREMA (PRIMO TEOREMA di BERLEKAMP):

sia  $f \in \mathbb{Z}_p[x]$ ,  $\deg f \geq 2$  e  $g \in \mathbb{Z}_p[x]$  t.c.:

$$1. 1 \leq \deg(g) \leq \deg(f)$$

$$2. f \mid (g^p - g),$$

allora vale che:  $f = \text{mcd}(f, g - 0) \cdot \text{mcd}(f, g - 1) \dots \text{mcd}(f, g - (p-1))$

procedere di fatto procedere di  $f$ .

dim: poiché  $\deg(g) < \deg(f)$ ,  $\text{mcd}(f, g - i)$  ha grado  $< \deg(f)$ .  
Quindi, se  $f$  è come nell'hp., ci dovranno essere dei

proponi propri

Per hp:  $f \mid g^p - g$  quindi  $\text{mcd}(f, g^p - g) = f$  e anche

$\text{mcd}(f, (g - 0)(g - 1) \dots (g - (p-1)))$

I polinomi  $(g - i) \dots (g - j)$ ,  $i \neq j$ , sono coprimi perché, se

$h \mid g - i, h \mid g - j \Rightarrow h \mid (g - i) - (g - j) \Rightarrow h \mid j - i$ , quindi  $h$  è

divisore di  $(j - i)$  resto zero  $\Rightarrow h$  è costante  $\Rightarrow$  polinomi sono primi fra loro.

Per hp 1.  $\text{mcd}(f, (g - 0) \dots (g - (p-1))) = \text{mcd}(f, g - 0)$ .

Il problema è trovare il polinomio  $g$  come nel teorema:  
sia  $f \in \mathbb{Z}_p[x]$ ,  $d = \deg f$ , cerco  $g$  con le proprietà:

$$1. \deg(g) \leq \deg(f) = d \quad 2. f \mid g^p - g.$$

$$\Rightarrow g = b_0 + b_1 x + \dots + b_{d-1} x^{d-1}, \quad g^p = b_0^p + b_1^p x^p + \dots + b_{d-1}^p x^{(d-1)p} = b_0 + b_1 x^p + \dots + b_{d-1} x^{(d-1)p} \quad \begin{matrix} \text{x Piccolo} \\ \text{Teo Fermat} \end{matrix}$$

ora dobbiamo dividere  $g^p - g$  per  $f$  e studiarne il resto:

$$f \mid g^p - g \Leftrightarrow \text{resto} = 0.$$

$$\text{Poniamo } x^p = q, f = r_i, \deg(r_i) < \deg(f) = d.$$

$$\text{Intanto } g^p - g = b_0 x^0 + b_1 x^1 + \dots + b_{d-1} x^{d-1} - b_0 - b_1 x - \dots - b_{d-1} x^{d-1} = b_0(q_0 f + r_1) + b_1(q_1 f + r_2) + \dots + b_{d-1}(q_{d-1} f + r_d) - b_0 - b_1 x - \dots - b_{d-1} x^{d-1} = f(b_0 q_0 + b_1 q_1 + \dots + b_{d-1} q_{d-1}) + b_0 r_0 + \dots + b_{d-1} r_d - b_0 - b_1 x - \dots - b_{d-1} x^{d-1}$$

il polinomio  $b_0 r_0 + \dots + b_{d-1} r_d - b_0 - b_1 x - \dots - b_{d-1} x^{d-1}$  è il resto della divisione di  $g^p - g$  per  $f$  (in quanto ha ordine  $< d$ )

Basta capire quando il polinomio è nullo, in questo caso  $f \mid g^p - g$

esplorando i polinomi  $\tau_{00}, \tau_{01}, \dots, \tau_{0,d-1}$ :

$$\tau_{00} = \tau_{00} + \tau_{10}x + \dots + \tau_{d-1,0}x^{d-1}$$

$$\tau_{0d} = \tau_{0,d0} + \tau_{1,d0}x + \dots + \tau_{d-1,d0}x^{d-1} \quad \text{con } \tau_{ij} \in \mathbb{Z}_p.$$

Quindi il polinomio diventa:

$$ba(\tau_{00} + \tau_{10}x + \dots + \tau_{d-1,0}x^{d-1}) + \dots + bd_1(\tau_{0,d1} + \dots + \tau_{d-1,d1}x^{d-1}) - ba - \dots - bd_1x^{d-1} = \\ = (ba\tau_{00} + b_1\tau_{01} + \dots + bd_1\tau_{0,d1} - ba)x^0 + \dots + (ba\tau_{d-1,0} + \dots + bd_1\tau_{d-1,d1} - bd_1)x^{d-1}$$

il resto è 0  $\Leftrightarrow$  tutti i coeff. sono zero, cioè:

$$\left\{ \begin{array}{l} ba(\tau_{00} + \tau_{10} + \dots + \tau_{d-1,0}) = 0 \\ \vdots \\ ba(\tau_{0,d1} + \dots + \tau_{d-1,d1} - 1) = 0 \end{array} \right.$$

Poniamo:  $Q = \begin{pmatrix} \tau_{00} & \tau_{01} & \dots & \tau_{0,d-1} \\ \vdots & \vdots & & \vdots \\ \tau_{0,d0} & \dots & \dots & \tau_{0,d-1} \end{pmatrix}, \quad B = \begin{pmatrix} ba \\ \vdots \\ bd_1 \end{pmatrix}$

il sistema diventa:  $(Q-I)B=0$

Dove la matrice  $Q$  è ottenuta mettendo nelle colonne i coeff. dei polinomi ottenuti come resto della divisione di  $x^p$  per  $f$ .

**RASSUMO:** riesce a fattorizzare un polinomio  $g$  se trova  $g$  t.c.  $\deg(g) < \deg(f)$  e  $\deg(g) = d$ .  
 $\& | g^p - g$ , quindi il resto scrivendo i polinomi  $\tau_j$  esplicitamente.

$Q$  è matrice quadrata di ordine  $d$  e i coeff.  $(ba, \dots, bd_1)$  sono t.c.  
 $\& | g^p - g \Leftrightarrow (ba, \dots, bd_1)$  sono t.c.  $(Q-I)\begin{pmatrix} ba \\ \vdots \\ bd_1 \end{pmatrix} = 0$ .

Cioè:  $ba, \dots, bd_1 \in \mathbb{Z}_p$  sono t.c. il polinomio  $g = ba + b_1x + \dots + b_{d-1}x^{d-1}$   
 soddisfa la condizione  $\& | g^p - g \Leftrightarrow \begin{pmatrix} ba \\ \vdots \\ bd_1 \end{pmatrix} \in \ker(Q-I)$ .

Consideriamo l'insieme  $G = \{g \in \mathbb{Z}_p[x] \text{ t.c. } \deg(g) \leq d, \& | g^p - g\}$   
 si vede che è uno  $\mathbb{Z}_p$ -spazio vettoriale.

Inoltre:  $g_1, g_2 \in G, \quad g_1 + g_2 \in G$ :

$$(g_1 + g_2)^p - (g_1 + g_2) = g_1^p + g_2^p - g_1 - g_2 = (g_1^p - g_1) + (g_2^p - g_2)$$

$$\Rightarrow \& | (g_1^p - g_1) + (g_2^p - g_2) \Rightarrow g_1 + g_2 \in G.$$

$$\text{Se } \lambda \in \mathbb{Z}_p, \quad g \in G, \quad \lambda g \in G: \quad (\lambda g)^p - (\lambda g) = \lambda^p g^p - \lambda g = \lambda(g^p - g)$$

Da questi ultimi risultati ottieniamo quindi:

#### TEOREMA (II TEO BERLEKAMP).

Sia  $f \in \mathbb{Z}_p[x]$ ,  $\deg f \geq 2$ . Sia  $Q$  matrice quadrata di ordine  $d = \deg f$   
 le cui colonne siano i resti di  $x^p$  quando divisi per  $f$ , con  
 $j = 0, 1, \dots, d-1$ .

Allora  $\ker(Q-I)$  è un isomorfismo fra gli spazi vettoriali  $G$  e  $\ker(Q-I)$ .

esempio: sia  $f = x^4 + 2 \in \mathbb{Z}_3[x]$  allora  $\ker(Q-I)$  è un isomorfismo fra  $G$  e Berlekamp

$$\text{Resto di } x^p \text{ diviso per } f: \quad \begin{array}{c} x^0 = 1 = 0 \cdot x^3 + 1 \\ x^1 = 2 = 2 + 0 \cdot x^3 \\ x^2 = 1 = 0 \cdot x^3 + 1 \\ x^3 = 2 = 2 + 0 \cdot x^3 \end{array}$$

$$x^4 = 1 = 0 \cdot x^3 + 1 = 2 + 0 \cdot x^3 + 0 \cdot x^2 + 0 \cdot x^1$$

$$x^5 =$$

$$\text{dove } G = \{g \in \mathbb{Z}_3[x] \text{ t.c. } \deg(g) \leq d, \& | g^p - g\}$$



12: vediamo in altro modo di fattorizzare  $\mathfrak{d} = x^4 + 2 \in \mathbb{Z}_3[x]$   
 (solo per trovare RESTI di  $x^j$ ):

$$x^{3j}, j = 0, 1, 2, 3.$$

→ Cerco il resto della divisione di  $x^6$  per  $\mathfrak{d}$ : considero l'anello  
 quoziente  $\mathbb{Z}_3[x]/(\mathfrak{d})$ .  
 Qui  $[x^4 + 2] = 0 \Rightarrow [x^4] + [2] = 0 \Rightarrow [x^4] = [-2] = [1]$

Vogliamo rappresentare canonico di  $[x^6]$  in  $\mathbb{Z}_3[x]/(x^4 + 2)$ :

$$[x^6] = [x^4 \cdot x^2] = [x^4][x^2] = [1][x^2]$$

→ resto di  $x^6$  per  $\mathfrak{d}$  è  $x^2$ .

→ Stesso ragionamento per  $x^9$  diviso per  $\mathfrak{d}$ :

$$[x^9] = [x^4 \cdot x^4 \cdot x] = [x^4][x^4][x] = [1][x]$$

→ resto di  $x^9$  per  $\mathfrak{d}$  è  $x$ .

12: La fattorizzazione di  $\mathfrak{d} = x^{20} + 1 \in \mathbb{Z}_5[x]$ .

Vedendo fare come prima, dovremmo lavorare con  
 una matrice  $10 \times 10$ , che non è molto conveniente.

→ cerchiamo di manipolare il polinomio:

$$x^{20} + 1 = x^{20} + 1^{20} = (x^4)^5 + (1^4)^5 = (x^4 + 1)^5 \Rightarrow \text{fattorizziamo } \mathfrak{d} = x^4 + 1 \in \mathbb{Z}_5[x]$$

$$\alpha = 4, p = 5 \Rightarrow j = 0, -1, 2, 3 \quad \text{resti} = x^0, x^5, x^{10}, x^{15}$$

1.  $x^0 = 1$  ha grado  $< 5 \Rightarrow$  è esso stesso il resto.

$$\text{in } \mathbb{Z}_5[x]/(\mathfrak{d}) = (x^4 + 1) : [x^0] = [0] \Rightarrow [x^4] = [-1] = [4]$$

$$2. x^5 = x^4 \cdot x \equiv (4) \cdot x = 4x \pmod{\mathfrak{d}}$$

$$3. x^{10} = x^4 \cdot x^4 \cdot x^2 \equiv 16x^2 \equiv x^2 \pmod{\mathfrak{d}}$$

$$4. x^{15} = x^4 \cdot x^4 \cdot x^4 \cdot x^3 \equiv (-1)^3 \cdot x^3 \equiv 4x^3 \pmod{\mathfrak{d}}$$

$$\Rightarrow Q = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 4 \end{pmatrix} \Rightarrow (Q-I) \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{pmatrix} = 0 \Leftrightarrow \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \Rightarrow \begin{cases} 0 = 0 \\ 3b_1 = 0 \\ 3b_2 = 0 \\ 3b_3 = 0 \end{cases} \Rightarrow \begin{cases} b_0 = 0 \\ b_1 = 0 \\ b_2 = 0 \\ b_3 = 0 \end{cases} \begin{cases} \text{b_0 libero} \\ \text{b_1 libero} \\ \text{b_2 libero} \\ \text{b_3 libero} \end{cases}$$

$$\Rightarrow \text{Ker}(Q-I) = \text{Span} \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \right\} \Rightarrow (\text{es}) \alpha_j = 1, \alpha_j = x^j$$

$$\Rightarrow \mathfrak{d} = \text{mcd}(x^4 + 1, x^0 - 1) \text{mcd}(x^4 + 1, x^5 - 1) \text{mcd}(x^4 + 1, x^{10} - 1) \text{mcd}(x^4 + 1, x^{15} - 1)$$

$$\cdot \text{mcd}(x^4 + 1, x^5 - 4) =$$

$$= (1 \cdots) = 1 \cdot 1 \cdot (x^5 - 2)(x^5 - 3) \cdot 1$$

$$\Rightarrow x^{20} + 1 = (x^4 + 1)^5 = (x^5 - 2)^5 (x^5 - 3)^5 = (x^5 - 2)^5 (x^5 + 2)^5$$

• osserviamo appunto  $x^5$

**TEOREMA (II TEO. BERLEKAMP):**

Sia  $f \in \mathbb{Z}_p[x]$ ,  $\deg f \geq 2$ . Sia  $Q$  la matrice dei resti di  $x^p$  diviso per  $f$ , con  $f = 0, \dots, d-1$ ,  $d = \deg(f)$ .  
Allora:

1.  $\dim_{\mathbb{Z}_p} \text{Ker}(Q-I) = \# \text{fattori irriducibili di } f$  [associati ad  $f$ ]

2.  $f$  è IRRIDUCIBILE  $\Leftrightarrow \dim \text{Ker}(Q-I) = 1$  e  $\text{mcd}(f, D(f)) = 1$

dim:

1. sia  $g$  t.c.  $g \mid g^p - g$  (dalla matrice  $Q-I$ ),  $g = u \cdot q_1^{\alpha_1} \cdots q_n^{\alpha_n}$ ,  
 $u$  invertibile,  $\alpha_1, \dots, \alpha_n \geq 1$ ,  $q_i$  NON assoc a  $g$  in  $\mathbb{Z}_p$  [IRRIDUCIBILI E DISJUNTI IN  $\mathbb{Z}_p^p$ ]

Consideriamo  $q_i$ ,  $q_i \mid g \Rightarrow q_i \mid g^p - g = (g-0)(g-1) \cdots (g-(p-1))$ ,  
 $q_i$  irrid.  $\Rightarrow \exists$   $s_i \in \mathbb{Z}_p$  t.c.  $q_i \mid (g - s_i)$ , cioè  $q_i$  divide uno dei fattori  $(g-0), (g-1), \dots, (g-p+1)$ .

Se  $q_i$  divide anche un altro fattore del tipo  $g - s_j$  con  $s_i \neq s_j$ , avremo  $q_i \mid g - s_i$  e  $q_i \mid g - s_j$ .

Ma sappiamo che  $g - s_i$  e  $g - s_j$  sono coprimi se  $s_i \neq s_j$ , quindi, siccome  $q_i \mid g \Rightarrow q_i \mid g - s_i \forall i = 1, \dots, n$ .

In particolare, dato che  $g \in G = \{g \in \mathbb{Z}_p[x] / f \mid (g^p - g)\}$  e  $\deg(g) < d$  e ad esso associamo gli elementi di  $\mathbb{Z}_p$  che sono  $(s_1, s_2, \dots, s_n)$ .

In questo modo abbiamo associato una  $\mathbb{Z}_p^n$ -upla  $(s_1, \dots, s_n) \in \mathbb{Z}_p^n$ .  
Quindi abbiamo un'applicazione:  $\psi: G \rightarrow \mathbb{Z}_p^n$  t.c.

$$g = \prod_{i=0}^{p-1} (g - s_i) \in G, \quad \psi(g) = (s_1, \dots, s_n).$$

Tale  $\psi$  è SURGETTIVA, infatti: sia  $(t_1, \dots, t_n) \in \mathbb{Z}_p^n$ , cerco  $g$  t.c.  
 $\psi(g) = (t_1, \dots, t_n)$ .

Consideriamo i polinomi  $q_1^{\alpha_1}, \dots, q_n^{\alpha_n}$ , che siano a  $2a^2$  coprimi.  
Allora dal teo chiusura dei resti  $\exists! \gamma \in \mathbb{Z}_p[x]$ :

$$\begin{cases} \gamma \equiv t_1 \pmod{q_1^{\alpha_1}} \\ \vdots \\ \gamma \equiv t_n \pmod{q_n^{\alpha_n}} \end{cases}$$

con  $\deg \gamma \leq \deg(q_1^{\alpha_1}) + \cdots + \deg(q_n^{\alpha_n}) = \deg f = d$ .

nel sistema segue:  $q_1^{\alpha_1} \mid (\gamma - t_1), \dots, q_n^{\alpha_n} \mid (\gamma - t_n)$ .

Quindi  $q_1^{\alpha_1} \cdots q_n^{\alpha_n} \mid (\gamma - t_1)(\gamma - t_2) \cdots (\gamma - t_n)$ , da questo si deduce  
che  $q_1^{\alpha_1} \cdots q_n^{\alpha_n}$  divide  $(\gamma - 0) \cdots (\gamma - (p-1))$   $\Rightarrow$   $\gamma$  è unico nel piano.

~~Perché  $\gamma$  è unico~~

$$\Rightarrow q_1^{\alpha_1} \cdots q_n^{\alpha_n} \mid \gamma^p - \gamma \Rightarrow \gamma \mid \gamma^p - \gamma.$$

$\deg(\gamma) < \deg(f) = d \Rightarrow \gamma \in G$  e  
 $\psi(\gamma) = (t_1, \dots, t_n) \Rightarrow \psi$  surgettiva.

Inoltre, essendo  $\gamma$  unico, abbiamo anche INIEZIVITÀ  
 $\Rightarrow \psi$  BIETTIVA.

$G$  e  $\mathbb{Z}_p^n$  sono in biezione tramite  $\psi$ , ma anche  $G$  e  $\text{Ker}(Q-I)$  lo sono.

Quindi  $\text{Ker}(Q-I) \cap \mathbb{Z}_p^n$  sono in biezione.

Essendo in biezione hanno lo stesso numero di elementi:  $p^n = |\mathbb{Z}_p^n|$ .

Inoltre  $\text{Ker}(Q-I)$  è sp. vettoriali, possa sia  $v_1, \dots, v_k$  una base di  $\text{Ker}(Q-I)$  come  $\mathbb{Z}_p^n$  vett.

Gli elementi di  $\text{Ker}(Q-I)$  sono del tipo  $\lambda_1 v_1 + \cdots + \lambda_k v_k$ ,  $\lambda_1, \dots, \lambda_k \in \mathbb{Z}_p$   
 $\in \text{Ker}(Q-I)$  ha  $p^k$  elementi.

Allora:  $p^k = p^n \Rightarrow k = n \Rightarrow \dim \text{Ker}(Q-I) = n = \# \text{fattori irriducibili di } f$

2.  $\& \in \text{IRRIDUCIBILE} \Rightarrow r=1 \Rightarrow \dim \text{Ker}(Q-I) = 1$ .  
 Inoltre  $\& \in D(\&)$  non possiede altre fattori comuni  $\Rightarrow \text{MCD}(\&, D(\&)) = 1$

Se viceversa:  $\dim \text{Ker}(Q-I) = 1 \Rightarrow \& = q_1^{\alpha_1}$ , se  $\text{MCD}(\&, D(\&)) = 1$ ,  
 $\Rightarrow \&$  NON ha fattori multipli  $\Rightarrow \alpha_1 = 1 \Rightarrow \& = q_1 \in \text{IRRIDUCIBILE}$ .

$\therefore$  :  $\&$  fattorizziamo  $x^5+1 \in \mathbb{Z}_2[x]$ , costruiamo  $Q$   
 per  $P=2$ ,  $d=5 \Rightarrow x^5 = x^0, x^1, x^2, x^3, x^4, x^5$ .

$$\begin{aligned} &\cdot x^0 \equiv 1 \pmod{x^5+1} \\ &\cdot x^2 \equiv x^3 \quad " \\ &\cdot x^4 \equiv x^5 \quad " \\ &\cdot x^0 \equiv x^5, x \equiv (-1)x \equiv x \pmod{x^5+1} \\ &\cdot x^8 \equiv (-1)x^3 \equiv x^5 \pmod{x^5+1} \end{aligned}$$

$$Q = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \Rightarrow (Q-I)B = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix} \begin{matrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \end{matrix} = 0$$

regime:  $\begin{cases} b_0 = 0 \\ b_1 + b_3 = 0 \\ b_1 + b_2 = 0 \\ b_0 + b_4 = 0 \\ b_2 + b_4 = 0 \end{cases} \begin{cases} b_3 = -b_1 = b_1 \\ b_2 = -b_1 = b_1 \\ b_4 = -b_3 = b_1 \\ b_2 = b_4 = b_1 \\ b_0 \text{ libero} \end{cases} \Rightarrow b_1 = b_2 = b_3 = b_4$

$\Rightarrow \text{Ker}(Q-I) = \text{Span}((1, 0, 0, 0, 0), (0, 1, 1, 1, 1)) \Rightarrow \dim \text{Ker}(Q-I) = 2$ .  
 Quindi  $x^5+1$  si scomponga nel prodotto di 2 fattori irriconducibili.

$$g = x + x^2 + x^3 + x^4$$

$$\begin{aligned} &\text{mcd}(x^5+1, g=0) = \text{mcd}(x^5+1, x^4+x^3+x^2+x) = \text{mcd}(x^5+1-x^4-x^3-x^2-x^2, x^4+x^3+x^2+x) = \text{mcd}(x^4+x^3+x^2-1, x^5+x^3+x^2+x) = \\ &= \text{mcd}(x+1, x^4+x^3+x^2+x) = \text{mcd}(x+1, x^2+x) = \text{mcd}(x+1, 0) = x+1 \\ &\text{mcd}(x^5+1, x^4+x^3+x^2+x-1) = \text{mcd}(x^5+1, x^4+x^3+x^2+x-1) = \\ &= \text{mcd}(x^4+x^3+x^2+x-1, x^5+x^3+x^2+x-1) = \text{mcd}(x^4+x^3+x^2+x-1) \end{aligned}$$

$$\Rightarrow x^5+1 = (x+1)(x^4+x^3+x^2+x-1)$$

Nota: abbiamo trovato metoda per fattori polinomi in  $\mathbb{Z}_p[x]$ , se prima con p suff. grande  $\mathbb{Z}_p[x] \sim \mathbb{Z}[x]$   
 $\Rightarrow$  si può arrivare a fattorizz. in  $\mathbb{C}[x]$ .

METODA DI KRONECKER per fattorizzare polinomi in  $\mathbb{C}[x]$ .

Sia  $\&(x) \in \mathbb{C}[x]$  polinomio dato, con  $\deg \& = d$ .  
 Sia  $\&(x) = g(x)h(x)$  fattore in  $\mathbb{C}[x]$ ...

$$\&(x) = x^2 - 5x + 6$$

$$\&(7) = 49 - 35 + 6 = 20 = g(7)h(7) \rightarrow g(7) = \begin{pmatrix} \pm 20 \\ \pm 10 \\ \pm 5 \\ \pm 4 \end{pmatrix}$$

$$\&(6) = 12 = g(6)h(6) \rightarrow g(6) = \begin{pmatrix} \pm 6 \\ \pm 3 \\ \pm 2 \\ \pm 1 \end{pmatrix}$$

$$\&(x) = a_0 + a_1 x$$

$$\text{Ora faccio una scelta: } g(6) = -3, g(7) = 10: \begin{cases} a_0 + 6a_1 = -3 \\ a_0 + 7a_1 = 10 \end{cases} \Rightarrow \begin{cases} a_1 = 1 \\ a_0 = -2 \end{cases}$$

$$\text{oppure: } g(6) = 4 : \begin{cases} a_0 + 6a_1 = 4 \\ a_0 + 7a_1 = 5 \end{cases} \Rightarrow \begin{cases} a_1 = 1 \\ a_0 = -2 \end{cases}$$

$$\Rightarrow g = x-2 \text{ è un fattore.}$$

### METODO DI KRONECKER:

Sia  $f(x) \in \mathbb{Z}[x]$  di grado  $d$ , pari. Cerco, se  $\exists$ , un fattore di  $f$  in  $\mathbb{Z}[x]$ :  $x = g/h$ .  
Un eventuale fattore di  $f$  avrà grado  $\leq \lfloor d/2 \rfloor = n$ .

- scegliamo  $n+1$  numeri a 2 a 2 distinti  $b_1, \dots, b_{n+1}$
- calcoliamo  $f(b_1), \dots, f(b_{n+1})$  e ne trovo  $x$  ciascuno tutti i divisori
- scopro  $(s_1, \dots, s_{n+1}) \in \mathbb{Z}^{n+1}$  t.c.:  $s_i \mid f(b_1), \dots, s_{n+1} \mid f(b_{n+1})$
- considero il polinomio  $g(x) = a_0 + a_1 x + \dots + a_n x^n$ , con  $a_0, \dots, a_n$  incognite e considero il s.s.  

$$\left\{ \begin{array}{l} a_0 + a_1 b_1 + \dots + a_n b_1^n = s_1 \\ \vdots \\ a_0 + a_1 b_{n+1} + \dots + a_n b_{n+1}^n = s_{n+1} \end{array} \right.$$
 e ottengo un polinomio  $g$ .

• divido  $g$  per  $f$ .

Oss: cerco  $g$  t.c.:  $g(b_1) = s_1$  cioè:  $g(x) \equiv s_1 \pmod{x - b_1}$   
 $g(b_{n+1}) = s_{n+1}$  cioè:  $g(x) \equiv s_{n+1} \pmod{x - b_{n+1}}$

Cioè:  $g$  si trova come soluzione delle congruenze:  $\left\{ \begin{array}{l} g \equiv s_1 \pmod{x - b_1} \\ \vdots \\ g \equiv s_{n+1} \pmod{x - b_{n+1}} \end{array} \right.$

### POLINOMI IN PIÙ VARIABILI

Sia  $A$  anello comm. unitario. Costruiamo l'anello dei polinomi  $A[x]$ .  
Gli elementi (polinomi) sono della forma:  $a_0 + a_1 x + \dots + a_n x^n$ .

A partire da  $A[x]$  costruiamo l'anello dei polinomi con coeff. in  $A[x]$  nella variabile  $y$ .

Gli elementi saranno del tipo:  $b_0 + b_1 y + \dots + b_m y^m$ , con  $b_0, \dots, b_m \in A[x]$ . Indicheremo tale anello con:  $(A[x])[y]$ .

$$b_0 = a_{0,0} + a_{0,1} x + \dots + a_{0,n} x^n$$

$$b_m = a_{m,0} + a_{m,1} x + \dots + a_{m,n} x^n$$

$\Rightarrow b_0 + b_1 y + \dots + b_m y^m$  diventa:  $(a_{0,0} + a_{0,1} x + \dots + a_{0,n} x^n) y + \dots + (a_{m,0} + a_{m,1} x + \dots + a_{m,n} x^n)$   
quindi ottengo:

$$a_{0,0} + a_{0,1} x + a_{0,2} x^2 + a_{0,3} x^3 + a_{0,4} x^4 + a_{1,0} y + a_{1,1} x y + a_{1,2} x^2 y + a_{1,3} x^3 y + a_{1,4} x^4 y + \dots$$

Gli elementi di  $(A[x])[y]$  sono quindi espressioni del tipo:

$$\sum_{(i,j) \in I} a_{i,j} x^i y^j \quad \text{dove } I \text{ è un insieme finito di coppie e } a_{i,j} \in A.$$

es:  $(A[x])[y] \ni x + 3xy^2 + 4x^2y^3 + 2x^4 = \sum_{(i,j) \in \{(1,0), (1,1), (2,3), (0,4), 0\}} a_{i,j} x^i y^j$   
dove:  $a_{0,0} = 1$ ,  $a_{1,1} = 3$ ,  $a_{2,3} = 4$ ,  $a_{0,4} = 2$ .

L'anello  $(A[x])[y]$  così costruito si indica con  $A[x,y]$ .

def: espressioni del tipo  $a_{i,j} x^i y^j$  si chiamano **TERMINI**,  
espressioni del tipo  $a_{i,j} x^i y^j$  si chiamano **MONOMI**, altr.

Un polinomio è somma finita di monomi.

Oss: l'anello dei polinomi  $A[x,y]$  può essere pensato sia come costruito da polinomi in  $y$  con coeff. in  $A[x]$ , sia come polinomi in  $x$  con coeff. in  $A[y]$ .

$$(A[x])[y] = (A[y])[x].$$

def: dato un monomio  $a_{i,j} x^i y^j$ ,  $a \neq 0$ , si dice **GRADO** di questo monomio il numero  $i+j$  ( $a_{i,j} \neq 0$ ).

notare:

• def: dato un polinomio  $\sum_{(i,j) \in I} a_{ij}x^i y^j$  si dice grado globale del polinomio il massimo dei gradi dei suoi monomi.

• nota: dato un polinomio  $A[x, y]$  si può considerare parlare di grado nella  $x$  o nella  $y$  ( $\deg_x f, \deg_y f$ ).

es:  $f(x, y) = 2x + 3x^2y^2 + 4x^2y - 5y^4$

: grado di  $f$  nella  $x$  è 2 :  $\deg_x f = 2$

: " " "  $y$  è 4 :  $\deg_y f = 4$

: " globale" di  $f$  è 4 :  $\deg f = 4$

• prop: se  $A$  è dominio int.  $\Rightarrow A[x, y]$  è dom. int.  
[applich. 2 vvv & fatto che  $A$  dom  $\Rightarrow A[x]$  dom.]

Inoltre se  $f, g \in A[x]$  e  $A$  dom, allora il grado globale di  $f+g$  è la somma degli gradi di  $f$  e di  $g$ .

Abbiamo visto che  $K[x]$  è UFD (K campo).  
vale anche che, se  $K$  è campo,  $K[x, y]$  è UFD.

Se  $K$  è campo,  $K[x]$  dom a IDEALE PR. (PID)  
ma NON vale per  $K[x, y]$  perché in  $K[x, y]$  non si fanno divisioni con Euclideo.

es: troviamo un IDEALE di  $\mathbb{Q}[x, y]$ , che non può essere PRINCIP., cioè non è generato da un UNICO ELEMENTO:

$$I = (x, y) := \{ f(x, y) \cdot x + g(x, y) \cdot y \mid f, g \in \mathbb{Q}[x, y] \}$$

procedo x assunendo considerando questo ideale, pensando quindi che  $\mathbb{Q}[x, y]$  sia PID.

I ha due generatori e non può succedere che abbia un solo generatore:  $\exists h \in \mathbb{Q}[x, y]$  t.c.  $I = (h)$ ;

se fosse così:  $\exists h \in \mathbb{Q}[x, y]$  t.c.  $h = f(x, y) \cdot x + g(x, y) \cdot y$ ,  
 $\forall x \in I \Rightarrow \forall h \in (h) \Rightarrow x = h \cdot 1$   
 $\forall y \in I \Rightarrow y = h \cdot 1$

$$\Rightarrow h = f \cdot x + g \cdot y \quad \forall h = f \cdot x + g \cdot y \Rightarrow \deg_x h = \deg_x f + \deg_y g = \deg_x f = 0$$

inoltre:  $x = h \cdot 1$ ,  $\deg_x x = 0 = \deg_x h \cdot 1 = \deg_x h + \deg_y 1 = \deg_y h = 0$ ,

cioè nel polinomio  $h$  non compare variabile  $y$ .

Per ragionare analogo arriviamo al fatto che nel polin.  $h$  non compare la variabile  $x$ .

$\Rightarrow h$  deve essere una COSTANTE.

$$\therefore h = 0 \Rightarrow (x, y) = 0 \quad \underline{\text{ASSURDO}}$$

$$\therefore h \neq 0 \Rightarrow (h) = \mathbb{Q}[x, y] = (\mathbb{1}) \Rightarrow 1 = f \cdot x + g \cdot y$$

se  $(x, y) = (h) \Rightarrow (x, y) = \mathbb{Q}[x, y]$ , in particolare,  
 $\exists f, g \in \mathbb{Q}[x, y]$  t.c.  $1 = f \cdot x + g \cdot y$

se multichiamo  $y = 0$ , ottieniamo:  $1 = f(x, 0) \cdot x + 0$   
 $\Rightarrow f(x, 0) \cdot x = 1$  in  $\mathbb{Q}[x]$ , da quanto segue che  $x$  in  $\mathbb{Q}[x]$  è INVERT., ma non è possibile  $\Rightarrow \underline{\text{ASSURDO}}$ .

$\Rightarrow \mathbb{Q}[x, y]$  non è PID.

### POLINOMI IN $n$ VARIABILI

**POLINOMI IN 3 VARIABILI:** in  $(A[x_1, x_2])[z] = A[z, x_1, x_2]$ , un polinomio generico è del tipo  $\sum_{i,j,k} a_{ijk} x^i y^j z^k$ .

**POLINOMI IN  $n$ -VARIABILI  $x_1, \dots, x_n$ :**  
se conosciamo i polinomi a coefficienti in  $A$  nelle variabili  $x_1, \dots, x_{n-1}$ , cioè  $A[x_1, \dots, x_{n-1}]$ , possiamo definire l'anello dei polinomi in  $n$ -variabili come:  $(A[x_1, \dots, x_{n-1}])[x_n] = A[x_1, \dots, x_n]$ .  
Gli elementi di  $A[x_1, \dots, x_n]$  sono delle espressioni del tipo

$$\sum_{(i_1, \dots, i_n) \in \mathbb{Z}^n} a_{i_1, \dots, i_n} x_1^{i_1} \cdots x_n^{i_n}$$

Se  $A$  è campo  $K$ ,  $K[x_1, \dots, x_n]$  è UFD NON È PID.

### TEOREMA DI ESTENSIONE:

Siano  $A, B$  anelli e  $\varphi: A \rightarrow B$  omomorfismo. Sia  $A$  anello,  $X \subseteq A$  sussistente. Si dice di anelli e siano  $b_1, \dots, b_n \in B$  elem. fissati.

Allora  $\exists! \Phi$  omom. di anelli,

$\Phi: A[x_1, \dots, x_n] \rightarrow B$  t.c.:

$$\Phi|_A = \varphi \text{ e } \Phi(x_i) = b_i \quad \forall i=1, \dots, n.$$

dim: induzione su  $n$ :

$\Rightarrow$  se  $n=2$  il teo è già stato dim.

Supponiamo vero fino a  $n-1$ , vogliamo vedere valga per  $n$ :

Siano  $b_1, \dots, b_n$ , consideriamo  $b_1, \dots, b_{n-1}, b_n \in B$  e applico ip. induktiva (permo  $n-1$ -esimo), allora  $\exists \Phi_1$

$$\Phi_1: A[x_1, \dots, x_{n-1}] \rightarrow B \text{ con } \Phi_1(a) = \varphi(a) \quad \forall a \in A \text{ e} \\ \Phi_1(x_i) = b_i, \quad i=1, \dots, n-1$$

Per teo estensione, ciata  $\Phi_2: A[x_1, \dots, x_{n-1}, x_n] \rightarrow B$ , dato  $b_n \in B$ ,

$$\exists! \Phi: A[x_1, \dots, x_{n-1}, x_n] \rightarrow B \text{ t.c. } \Phi|_{A[x_1, \dots, x_{n-1}]} = \Phi_1$$

$$\Phi(x_i) = \begin{cases} b_i & \text{in } i=n \\ \Phi_1(x_i) = b_i & \text{in } i=1, \dots, n-1 \end{cases}$$

$$\text{Quindi: } \Phi|_A = \Phi_1|_A = \varphi(a), \quad \Phi(a) = \Phi_1(a) = \varphi(a) \quad \forall a \in A.$$

$\Rightarrow$  così d. l'applicazione  $\tilde{\varphi}: Q[x] \rightarrow Q$  ottiene passando gli elementi di  $Q$  e mandando  $x$  in 2.

Troviamo NUCLEO di  $\tilde{\varphi}$ .

$$a \xrightarrow{\tilde{\varphi}} a \quad \forall a \in Q, \quad a_0 + a_1 x + \dots + a_n x^n \xrightarrow{\tilde{\varphi}} a_0 + 2a_1 + \dots + 2^n a_n$$

$$x \xrightarrow{\tilde{\varphi}} 2$$

$$\tilde{\varphi}(g(x)) = g(2), \quad \ker \tilde{\varphi} = \{g(x) / g(2) = 0\} = \{g(x) / g(2) = 0\} = (x-2).$$

Teo omom:  $Q[x] \cong Q \Rightarrow Q[x]/(x-2) \cong Q$ .  
Quindi  $(x-2)$  è massimale perché QUOTIENTE È UN CAMPO.

es. Sia  $F: \mathbb{Q}[x] \rightarrow \mathbb{Q}$  l.c.  $F(a) = a$   $\forall a \in \mathbb{Q}$ ,  $F(x) = 2$ ,  $F(y) = -1$  e  $F$  estesa con il th. estensione. Chi è  $\text{Ker } F$ ?  
Cerchiamo  $x-2, y+1 \in \text{Ker } F$ .

$(x-2, y+1) \subseteq \text{Ker } F$ ;  $x+2y = 1(x-2) + 2(y+1) \in (x-2, y+1)$   
voglio dim. che  $(x-2, y+1) = \text{Ker } F$

$g(x, y) \in \text{Ker } F \Rightarrow F(g(x, y)) = 0 = g(2, -1)$ .

$g(x, y) \in \mathbb{Q}[x, y] = \mathbb{Q}[x] \cap \mathbb{Q}[y]$

Possiamo usare divisione per il polinomio  $g$  del polin.  $g(x, y)$  e pensando con coeff. in  $\mathbb{Q}[x]$  e nella variabile  $y$ .

$g(x, y) = q(x, y)(y+1) + R(x, y)$   
 $\deg_y R(x, y) < \deg(y+1) = 1$ . Da  $\deg_y R(x, y) < 1$  allora

$R(x, y)$  risulta polinomio nullo sece  $x = \bar{R}(x)$ .

$\bar{R}(x) \in \mathbb{Q}[x]$  dividibile per  $x-2$ :  $\bar{R}(x) = q_1(x)(x-2) + T$ ,  
 $\deg_x T < 1$ , cioè  $T$  è costante.

Quindi:  $g(x, y) = q(x, y)(y+1) + q_1(x)(x-2) + T$ ,  $T$  costante ( $T \in \mathbb{Q}$ )  
siccome  $g(x, y) \in \text{Ker } F$  otteniamo che:  
 $g(2, -1) = 0 = q(2, -1) \cdot 0 + q_1(2) \cdot 0 + T \Rightarrow T = 0$ .

Quindi  $g(x, y) = q(x, y)(y+1) + q_1(x)(x-2) \in (x-2, y+1)$   
conclusione:  $\text{Ker } F = (x-2, y+1)$ .

$F: \mathbb{Q}[x, y] \rightarrow \mathbb{Q}$

$$\begin{matrix} x & \mapsto & 2 \\ y & \mapsto & 1 \end{matrix} \quad F \text{ multativa, tec. omom}: \frac{\mathbb{Q}[x, y]}{\text{Ker } F} \cong \mathbb{Q}$$

Per  $\text{Ker } F = (x-2, y+1)$ , quindi  $\frac{\mathbb{Q}[x, y]}{(x-2, y+1)} \cong \mathbb{Q}$ .

Allora  $(x-2, y+1)$  è massimale (degli massimali non trovati).

In  $\frac{\mathbb{Q}[x, y]}{(x-2, y+1)}$ ,  $[x] = ?$ ,  $[y] = ?$ ,  $[y] = ?$

sappiamo che:  $[x+2] = 0 \Rightarrow [x] = \text{deg } 2 \Rightarrow [x] = -2$ ,  
 $[y+1] = 0 \Rightarrow [y] = -1$ .

$$[x^2 + 4xy + 7y] = [2^2 + 4 \cdot 2 \cdot (-1) + 7(-1)] = [-11] = -11.$$

Se  $a, b \in \mathbb{Q}$ ,  $[a] = [b] \Rightarrow a = b$ .

$$a - b \in (x-2, y+1) \Rightarrow a - b = \alpha(x-2) + \beta(y+1) = \alpha(2, -1)(-2) + \beta(2, -1)(-1+1) = 0.$$

Siano  $A, B$  due anelli (comm. unitari) t.c.  $A \subseteq B$ ,  $A$  non sovraccarico  $B$ .

Siano  $b_1, \dots, b_n \in B$

1)  $\exists$  il più piccolo anello contenuto in  $B$  che contiene  $A$  e  $b_1, \dots, b_n$ ?  
2) In 1), come è fatto?

L'oss:

- chiamare un anello contenente  $A \cup b_1, \dots, b_n$   $C \subseteq B$ .
- se due anelli contengono  $A \cup b_1, \dots, b_n \Rightarrow$  questi sono contenuti anche nell'estensione dei 2 anelli.
- se  $(A \cup b_1, \dots, b_n)$  sono anelli che contengono  $A \cup b_1, \dots, b_n$ , allora sono contenuti in  $\cap A$ .

Allora  $\exists \cap A$  anello contenente  $A \cup b_1, \dots, b_n$  ed è il più piccolo, o ma come è fatto?

Siano  $a_1, \dots, a_n \in A$ , questo anello deve contenere anche  $b_1, \dots, b_n$  e  $b_1, \dots, b_n$ .

$a_1, \dots, a_n \in A$ ,  $a_1, \dots, a_n$  deve stare nell'anello.

se  $a_1, \dots, a_n \in A$  e  $a_1, \dots, a_n \in \mathbb{N}$ ,  $a_1, \dots, a_n \in \mathbb{N}$  anche.

$a_1, \dots, a_n + b_1, \dots, b_n$  deve stare nell'anello, quindi deve contenere espressioni del tipo:

$\sum a_i b_i$ ,  $a_i, b_i \in \mathbb{N}$ , con  $a_i, b_i \in A$   $(*)$   
 $(a_1, \dots, a_n) \in \mathbb{N}^n$

e questo è il polinomio:  $\sum a_{i_1 \dots i_n} x_1^{i_1} \dots x_n^{i_n}$  è  $A[x_1, \dots, x_n]$

valutato in  $x_1 = b_1, \dots, x_n = b_n$ .

Per il trao di estensione:  $f: A \rightarrow B$  t.c.  $f(a) = a \forall a \in A$ ,

$\Phi: A[x_1, \dots, x_n] \rightarrow B$  t.c.  $\Phi(a) = f(a) = a \forall a \in A$ ,  $\Phi(x_i) = b_i$   
e dal trao estensione:

$$\Phi\left(\sum a_{i_1 \dots i_n} x_1^{i_1} \dots x_n^{i_n}\right) = \sum a_{i_1 \dots i_n} b_1^{i_1} \dots b_n^{i_n}$$

Osserviamo allora che tutti gli elementi della forma (\*) trovata prima devono stare nel più piccolo anello contenente  $A$  e  $b_1, \dots, b_n$  sono nell'immagine di  $\Phi$ .

Ma l'immagine di  $\Phi$  è un anello  $\subset B$  (contiene gli elementi di  $A$  e  $b_1, \dots, b_n$ ).

Inoltre l'imm. di  $\Phi$  coincide con l'insieme: {elementi della forma (\*) |

Quindi il più piccolo anello contenente  $A$  e  $b_1, \dots, b_n$  è dato da  $\text{Im } \Phi$  ed è costituito da polinomi di  $A[b_1, \dots, b_n]$  valutati in  $b_1, \dots, b_n$ .

NOTA:  $\text{Im } \Phi$  si indica anche con  $A[b_1, \dots, b_n]$ .

dici:

Siano  $K, L$  due campi con  $K$  sottocampo di  $L$ , cioè  $K \subseteq L$  sottocampo

$L$  si dice anche ESTENSIONE del CAMPO  $K$ .

Se  $b_1, \dots, b_n \in L$  è il più piccolo campo contenente  $K$  e  $b_1, \dots, b_n$ ; esso si indica con  $K[b_1, \dots, b_n]$  ed è il campo dei QUOTIENTI di  $K$ ?

- NOTA: se L estensione di K, si usa la notazione:  $L : K$
- se L estensione di K, L è un K-sp. vett., infatti:  
 $K \times L \rightarrow L$  t.c.  $(a, x) \mapsto a \cdot x$  (produttivo in L)
- in questo modo L diventa K-sp.vett.

la dimensione di L come sp. vett. si indica così:  $[L : K]$  e si chiama GRADO dell'estensione.

- dici: sia K campo, L estensione di K. Un elemento  $a \in L$  si dice ALGEBRICO se su K si  $\exists \&(x) \in K[x]$  polinomio a coeff. in K non nullo t.c.  $\&(a) = 0$ .

Se  $a \in L$  non è ALGEBRICO allora si dice TRASCENDENTE.  
Cioè  $\&$  polinomio  $\& \in K[x]$ ,  $\& \neq 0$ , vale che  $\&(a) \neq 0$ .

es:  $K = \mathbb{Q}, L = \mathbb{R}$

- 1) sia  $a = \sqrt{2}$ , è un elemento algebrico in  $\mathbb{Q}$  perché  $\sqrt{2} \notin \mathbb{Q}$ .  
Infatti il polinomio  $x^2 - 2 \in \mathbb{Q}[x]$  è  $\neq 0$  e  $(x^2 - 2)$  valutato in  $\sqrt{2}$  da zero.

Anche  $x^4 - 2 \in \mathbb{Q}[x]$  è  $\neq 0$  e si annulla in  $\sqrt[4]{2}$ .  
(...)

- 2)  $\mathbb{Q} \subset \mathbb{R}$ , per  $R: \mathbb{R}$   
 $a = \sqrt{3}$  è alg.  $x^2 - 3$  è un pol. che si annulla in  $\sqrt{3}$ .

$$a = \sqrt{2} + 1, a - 1 = \sqrt{2} \\ a^2 - 2a + 1 = 2 \Rightarrow a^2 - 2a - 1 = 0$$

Consideriamo:  $\&(x) = x^2 - 2x - 1$ , vale  $\&(x) \in \mathbb{Q}[x]$ ,  $\&(x) \neq 0$ ,  $\&(a) = 0$ .

- 3)  $\mathbb{Q} : \mathbb{Q}$ ,  $i \in \mathbb{Q}$ ,  $i = \sqrt{-1}$  è algebrico o trasc. in  $\mathbb{Q}$ ? alg.  $x^2 + 1$ .

- 4)  $a = \sqrt{2} + \sqrt{3} \in \mathbb{R}$ ,  $\mathbb{R} : \mathbb{Q}$

$$a^2 = 2 + 2\sqrt{2}\sqrt{3} + 3 = 5 + 2\sqrt{6} \rightarrow a^2 - 5 = 2\sqrt{6} \rightarrow a^4 - 10a^2 + 25 = 24$$

$$\Rightarrow a^4 - 10a^2 + 1 = 0, \&(x) = x^4 - 10x^2 + 1 \text{ mostra che } a \text{ è algebrico in } \mathbb{Q}$$

- NOTA: in un'estensione  $L : K$  ogni elem.  $a \in L$  è ma. in  $K$ , basta prendere il polinomio  $x - a \in K[x]$ .

### POLINOMIO MINIMO

Sia  $L \subset K$ ,  $a \in L$  algebrico. L'insieme  $I = \{ f(x) \in K[x] / f(a) = 0 \}$  contiene polinomi non nulli.  $I$  è ideale di  $K[x]$ .

- $f(x), g(x) \in I$ ,  $f(x) + g(x)$  valutato in  $a$  è  $0 \Rightarrow f(x) + g(x) \in I$
- $x^r a(x) \in K[x]$  è  $f(x) \in I$ ,  $x^r a(x) \cdot f(x)$  valutato in  $a$  è  $0$   
 $\Rightarrow x^r a(x) \in I$

$I$  è principale, è quindi generato da un polinomio  $m(x)$  che è di grado + piccolo possibile tra i polinomi di  $I$ .

- sia  $a \in L$  algebrico in  $K$ . Il polinomio monico che si annulla in  $a$  di grado minimo possibile è il generatore di  $I$ , ed è detto POLINOMIO MINIMO di  $a$  in  $K$ .

Il polinomio minimo è unico se  $m_1(x)$  e  $m_2(x)$  sono entrambi monici, che si annullano in  $a$  e di grado minimo possibile, allora:

$$\deg m_1 = \deg m_2, m_1(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0 \\ m_2(x) = x^n + b_{n-1}x^{n-1} + \dots + b_0$$

Consideriamo:  $m_1(x) - m_2(x)$  è polin. di grado  $< n$  e si annulla in  $a$ .

Inoltre  $n$  è minimo  $\Rightarrow m_1(x) - m_2(x)$  deve essere polinomio nullo.

$$\text{Cioè: } m_1(x) - m_2(x) = 0 \Rightarrow m_1(x) = m_2(x).$$

Sia  $L \subset K$ ,  $a \in L$  algebrico in  $K$ . Chi è  $K[a]$ ? è  $K(a)$ ?

$$K[a] = K[x] \xrightarrow{\Phi} L \text{ t.c. } \begin{array}{c} x \mapsto a \\ a \mapsto a \end{array} \forall a \in K$$

sia  $\Phi$  l'unico omom. con tali proprietà  $\Rightarrow \text{Im } \Phi \in K[a]$ .

$$K[x] \xrightarrow{\Phi} L, \text{ chi è } \ker \Phi?$$

$\ker \Phi = \{ f(x) \in K[x] / f(a) = 0 \} \Rightarrow \ker \Phi$  è l'ideale di primo e quindi  $\ker \Phi = (m)$ , dove  $m$  è il pol. minimo di  $a$  in  $K$ .

$$\text{TEO. OMOM: } \frac{K[x]}{\ker \Phi} \cong \text{Im } \Phi = K[a] \Rightarrow \frac{K[x]}{(m)} \cong K[a].$$

- PROP: il polinomio minimo di  $a \in L$  in  $K$  è IRREDUC.

dim:  $m(x) = f(x) \cdot g(x)$ ,  $m(a) = 0 = f(a) \cdot g(a) \Rightarrow f(a) = 0$  o  $g(a) = 0$   
 se  $f(a) = 0 \Rightarrow \deg f(x) = \deg m(x)$ , perché in pol. min  $\Rightarrow \deg g = 0$   
 $\Rightarrow g$  costante  $\neq 0 \Rightarrow$  è elem. invertibile.

Quindi  $m(x)$  IRREDUC.

- OSS: Intanto  $((m(x)))$  è massimale. Quindi  $K[x]/(m)$  è campo.  
 Allora  $K[a]$  è campo  $= K(a)$ .

Quindi, se  $a$  è algebrico in  $K$ , il più piccolo anello contenente  $K$  e  $a$  è uguale al più piccolo campo contenente  $K$  e  $a$  è isomorfo a  $K[a] \cong (m(x))$ .

- Q: chi è  $\mathbb{Q}[\sqrt{2}]$ ?  $\mathbb{Q}[\sqrt{2}] \cong \mathbb{Q}[x]/(x^2 - 2)$ . Gli elem. di  $\mathbb{Q}[\sqrt{2}]$  sono classi del tipo  $[ax + b\sqrt{2}]$  ( $x^2 - 2$ )

$$[x^2 + 4x^2 - 3x + 1] \in \mathbb{Q}[x]/(x^2 - 2) \quad (*) \quad [x^2] = 2 \\ \stackrel{(*)}{=} [x^4 + 4x^2] = [2x + 8]$$

$$[2x + 8 - 3x + 1] = [-x + 9]$$

$$\mathbb{Q}[x]/(x^2 - 2) \xrightarrow{\sim} \mathbb{Q}[\sqrt{2}]$$

$$[-x + 9] \rightarrow 9 - \sqrt{2} \in \mathbb{Q}[\sqrt{2}]$$

$$[a + b\sqrt{2}] \rightarrow a + b\sqrt{2}$$

quindi:  $\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} / a, b \in \mathbb{Q}\}$ , abbiamo dim. che è un campo.  
Che è l'inverso di  $2 + 3\sqrt[3]{2}$ ?

$$\frac{1}{2+3\sqrt[3]{2}} \cdot \frac{2-3\sqrt[3]{2}}{2-3\sqrt[3]{2}} = \frac{2-3\sqrt[3]{2}}{4-18} = -\frac{1}{7} + \frac{3}{14}\sqrt[3]{2} \text{ è l'inverso.}$$

NOTE/OSS:

se  $L:K$  è estensione e se si ael è algebrico su  $K$ .  
 $K[a]$  è campo che contiene  $K \subseteq K[a]$ .  
 $K[a]$  è estensione di  $K$ .

Quanto vale  $[K(a):K]$ ? cioè il grado dell'estensione  $[K(a):K]$  di  $K$ .

$$K(a) \cong \frac{K[x]}{(m(x))} = \left\{ [a_0 + \dots + a_n x^n] / a_0, \dots, a_n \in K, n = \deg m(x) \right\} = \\ = \{ a_0[1] + a_1[x] + \dots + a_{n-1}[x^{n-1}] / a_0, \dots, a_{n-1} \in K \}$$

quindi gli elementi di  $K(x)$  sono comb. lineari di  
 $[1], [x], \dots, [x^{n-1}]$  che sono base su  $K$ .

Quindi  $K[x]/(m(x))$  è  $K$ -sv. con dim.  $n = \deg m(x)$ . Allora  
 $K[a]$  è su di dim.  $n = \deg m(x)$  su  $K$ . cioè  $[K(a):K] = \deg m(x)$ .

es:  $\mathbb{Q}(\sqrt[3]{2})$ ,  $\sqrt[3]{2} \in \mathbb{R}$  è algebrico su  $\mathbb{Q}$  e il polin. minimo è  $x^3 - 2$ .

Quindi:  $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}] = 3$ .

Che è una base di  $\mathbb{Q}(\sqrt[3]{2})$  su  $\mathbb{Q}$ ? E di  $\mathbb{Q}(\sqrt[3]{2})/(x^3 - 2)$  su  $\mathbb{Q}$ ?

Base di  $\mathbb{Q}(\sqrt[3]{2})$  è data da:  $1, \sqrt[3]{2}, (\sqrt[3]{2})^2 = \sqrt[3]{4}$ .

$$\Rightarrow \mathbb{Q}(\sqrt[3]{2}) = \{ a + b\sqrt[3]{2} + c\sqrt[3]{4} / a, b, c \in \mathbb{Q} \}.$$

def: se ael è alg. su  $K$  con polin. minimo  $m(x)$  di grado  $n$ ,  
a si dice ELEMENTO ALGEBRICO di grado  $n$ .

Sia ora ael trascendente su  $K$ ,  $K[a] \cong K[x]$ :

$$K[x] = \frac{\Phi}{\begin{array}{c} \Phi \neq 0 \\ a \in K \\ a \neq 0 \end{array}} \quad \left\{ \begin{array}{l} K \cap \Phi = \{0\} \\ \dim \Phi = n \end{array} \right\} \Rightarrow \frac{K[x]}{K \cap \Phi} \cong K[a].$$

Cioè:  $K[x] \cong K[a]$ .

OSS: in  $\mathbb{R}$  ci sono elem. trascendenti su  $\mathbb{Q}$ :

$$0,100\overline{100\dots 010\dots 0} \in \mathbb{R} \text{ è TRASCENDENTE, come } e \text{ e } \pi.$$

def: siamo  $K, L$  campi con  $L$  estensione di  $K$ , allora è estensione  
L si dice algebrica di  $K$  se ogni elem. di  $L$  è algebrico su  $K$ .

es:  $\mathbb{Q} \subset \mathbb{R}$  non è estensione algebrica

prop: se  $L:K$  estensione e se  $[L:K]$  è finito, allora  $L$  è  
estensione algebrica di  $K$ .

dim: sia ael. Sia polinomio:  $f(x) = a_0 + a_1 x + \dots + a_n x^n \in K[x]$ , valutato  
in a diventa:  $a_0 + a_1 a + \dots + a_n a^n$ ,  $a_0, \dots, a_n \in K$  è comb. lineare  
di  $1, a, a^2, \dots, a^n$  ai coeff. in  $K$ . Sia  $[L:K] = n$  finito.  
considero  $a^0, a^1, \dots, a^n$  ai sono tutti elem. di  $L$ , quindi sono  
lin. dep. su  $K$ . Allora  $\exists$  coeff.  $a_0, \dots, a_n \in K$  non tutti nulli.  
t.c.  $a_0 \cdot 1 + a_1 \cdot a + \dots + a_n a^n = 0$ .

D'q. il polinomio:  $f(x) = a_0 + a_1 x + \dots + a_n x^n$ ,  $f(x) = f(a) = 0$   
 $\Rightarrow a$  alg. su  $K$

Se  $a \in L$  è alg. su  $K$ , allora  $K[a]$  è est. alg. di  $K$

• TEOREMA della TORRE:

Siano  $M, L, K$  tre campi t.c.  $L$  è estensione di  $K$  e  $M$  è estensione di  $L$ . Supponiamo che  $[L:K] = m$ ,  $[M:L] = n$ .

Allora  $M$  è est. di  $K$  finita, di grado  $m \cdot n$ .

dim:

Se  $L$  è estensione di  $K$  di grado  $m$ , siano  $v_1, \dots, v_m$  el. base di  $L$  in  $K$ . Analogamente siano  $w_1, \dots, w_n$  el. base di  $M$  in  $L$ .



Sia  $a \in M$ . Pertanto  $a = \mu_1 v_1 + \dots + \mu_m v_m$ ,  $\mu_1, \dots, \mu_m \in L$ , comb. lineare di  $v_1, \dots, v_m$ .

Quindi:  $\lambda_1 = \mu_1 v_1 + \dots + \mu_m v_m$

$$\lambda_1 = \mu_1 v_1 + \dots + \mu_m v_m, \mu_i \in K$$

$$\Rightarrow a = (\mu_1 v_1 + \dots + \mu_m v_m) w_1 + \dots + (\mu_1 v_1 + \dots + \mu_m v_m) w_n \quad (1)$$

$$= \mu_1 v_1 w_1 + \dots + \mu_m v_m w_n + \dots + \mu_m v_m w_n. \quad (2)$$

Quindi  $a$  è comb. lineare di  $v_1 w_1, \dots, v_m w_m$ ,  $i=1, \dots, n$ ,  $j=1, \dots, m$  con coeff. in  $K$ . Quindi  $v_1 w_1, \dots, v_m w_m$  sono lin. indip. in  $M$  come sv in  $K$ .

Proviamo che  $v_i w_j$  sono lin. indip. in  $K$ :

$a = \lambda_1 v_1 + \dots + \lambda_n v_n$ ,  $\lambda_1, \dots, \lambda_n \in L$ , che sono comb. lineare di  $v_1, \dots, v_m$ .

Proviamo che  $\{v_i w_j\}$  sono lin. indip. in  $K$ . Prendiamo una comb. lineare e la poniamo = 0, come in (1). Da (2) mettendo in evidenza  $w_1, \dots, w_n$  (2).

Ma se (2) = 0, poiché  $w_1, \dots, w_n$  sono lin. indip. in  $L$ , deve essere:  $\mu_1 v_1 + \dots + \mu_m v_m = 0$  }  $v_1, \dots, v_m$  sono lin. indip.

$\mu_1 v_1 + \dots + \mu_m v_m = 0$  } allora:  $\mu_{ij} = 0 \forall i, j$ .

• PROP: sia  $K$  campo,  $\beta \in K[x]$  pol. irriduc. Allora  $\exists L$  unico estensione di  $K$  t.c. amm.  $\beta$  una RADICE o in  $L$ .

dim: sia  $L = \frac{K[x]}{(f)}$ .  $L$  è un campo finito  $\& \beta \in L$ . E quindi  $(f)$  è massimale,  $L$  estensione di  $K$ .

Sia  $\xi = [x] \in L$ ,  $\xi$  può essere pensato come polinomio e vale che:  $\beta(\xi) = 0$ .

Sia  $\varphi = a_0 + a_1 x + \dots + a_n x^n$ ,  $a_i \in K$ .

$$\begin{aligned} \varphi(\xi) &= a_0 + a_1 \xi + \dots + a_n \xi^n = a_0 + a_1 [\alpha^0] + \dots + a_n [\alpha^n] = \\ &= a_0 + [\alpha^0] + \dots + [\alpha^n] = [a_0 + \dots + a_n \alpha^n] = [\varphi] = 0. \end{aligned}$$

•  $\Rightarrow \varphi(x) = x^2 + 1 \in Q[x]$ ,  $\&$  IRRED. Costruiamo  $L = \frac{Q[x]}{(x^2 + 1)}$

che è uno zero di  $\varphi$  in  $L$ ?  $\xi = [x]$ .

$$[x^2 + 1] = 0 \Rightarrow [x^2] = -1, \text{ ciò è uno zero di } \varphi \text{ in } L.$$

Ora non c'è nulla di:

Quindi, se  $\beta = i$  il nostro polin. ha per radice  $i$ .

COSTRUZIONE DEL CAMPO DI RIDUCIBILITÀ DERIVATA DA UN POLINOMIO

Sia  $f(x) \in K[x]$  un polinomio (con  $K$  campo). Allora  $\exists$  un campo  $M$  estensione di  $K$  t.c. pensato come polinomio in  $M[x]$  si speri nel progetto:

$$a(x - \xi_1)(x - \xi_2) \cdots (x - \xi_n) \text{ con } \xi_1, \dots, \xi_n \in M, a = \deg f.$$

$M[x]$  si dice campo di riducibilità completa.

dim: per induzione su  $\deg f$ .

$K[x]$  UFD  $\Rightarrow \forall f = g \cdot h, g, h \in K[x]$ .

Per induz. completa sapp. che il risultato sia vero per  $\deg f$  e proviamo sia vero anche per  $\deg f$ .

Per  $\deg f$  precedente  $\exists L$  campo, estensione tratta di  $K$  t.c.  $g$  abbia radice  $\xi$  in  $L$ . Quindi, per Ruffini in  $L[x]$  possiamo scrivere  $g = (x - \xi_1)g_1$  con gli opportuni  $g_i \in L[x]$ ,  $\xi_i \in L$ .

Allora  $f(x) = (x - \xi_1)g(x)$  in  $L[x]$ ; il polinomio  $g(x)$  è di grado  $\deg f(x) - 1$ .

Quindi  $x$  induce  $\exists M$  campo estensione di  $L$  t.c.  $g(x)$  diventi  $a(x - \xi_1) \cdots (x - \xi_n)$ .

Pertanto  $f(x) = a(x - \xi_1) \cdots (x - \xi_n)$ .

Resta da dim parmo  $\deg f = 1$ :  $f(x) = ax + b, \forall a, b \in K$   
 $= a(x - (-\frac{b}{a})) = a(x - \xi_1)$

es:  $\mathbb{Q}[\sqrt[3]{5}]$  è campo, si v. in  $\mathbb{Q}$  un num. 3. Hanno più  $1, \sqrt[3]{5}, \sqrt[3]{25}$

$a = \sqrt[3]{2}$  poi pol minimo di  $a$  in  $\mathbb{Q}[x]$ .

In generale il numero  $\sqrt[p]{p}$ ,  $p$  primo, è algebrico su  $\mathbb{Q}$  di grado  $n$ . Perché il polinomio  $x^n - p$  è il pol. minimo di  $\sqrt[p]{p}$ .

$\mathbb{Q}[\sqrt[p]{p}]$  è campo quando  $n \in \mathbb{Q}$

#### CAMPI FINITI

def: un campo  $K$  si dice finito se ha un numero finito di elementi.

Sia  $K$  campo finito, allora ha caratteristica positiva e deve essere un numero primo  $p$ .

Quindi  $K$  contiene  $\mathbb{Z}_p$ ,  $\mathbb{Z}_p$  è campo quindi  $K$  è estensione di  $\mathbb{Z}_p$ .  $K$  è  $\mathbb{Z}_p$ -sv.  $[K : \mathbb{Z}_p] = n$  per forza  $n$  uguale a  $n \in \mathbb{N}$ .

Sia  $K$  campo finito di caratteristico.

Sia  $[K : \mathbb{Z}_p] = n$ . Allora  $K$  ha  $p^n$  elementi.

dim: sia  $a \in K$  e  $v_1, \dots, v_n$  una base di  $K$  in  $\mathbb{Z}_p$ , allora

$$a = \lambda_1 v_1 + \dots + \lambda_n v_n, \lambda_i \in \mathbb{Z}_p$$

$\lambda_i$  può essere scelto  $p$  volte, così anche  $\lambda_2, \lambda_3, \dots, \lambda_n$ .

Quindi abbiamo  $p \cdots p$  possibilità elem. di  $K \Rightarrow K$  ha  $p^n$  elem.

consegu:  $\exists$  campi finiti con ( $n$ ) 6, 15, 63, ... elementi  
perché non sono del tipo  $p^n$ .

#### TEOREMA DELL'ELEMENTO PRIMITIVO

Sia  $K$  campo finito. Allora  $(K^*)_{\text{ord} \neq 1}$  è GR ABELIANO, cioè  $\exists d \in K^*$  t.c. tutti gli elementi di  $K^*$  sono una potenza di  $d$ .  $d$  si dice ELEMENTO PRIMITIVO del campo.  
[cioè:  $(K^*)_{\text{ord} \neq 1}$  è ciclico]

es: i campi  $\mathbb{Z}_p$ , primo, sono finiti.

in  $\mathbb{Z}_7$   $2, 2^2 = 4, 2^3 = 8, \dots, 2^6 = 2$  NON È PRIMITIVO.

**Teorema:** sia  $K$  campo finito di caratter.  $p$ . Allora  $\exists$  un polinomio irriducibile  $q(x) \in \mathbb{Z}_p[x]$  t.c.  $K \cong \mathbb{Z}_p[x]/(q)$

dim: se  $K$  campo finito  $\exists$  elem. primitivo  $\beta \in K$ .

Considero l'omomorfismo  $\psi: \mathbb{Z}_p[x] \rightarrow K$  dato da  $\psi(a) = a$  per  $a \in \mathbb{Z}_p$  (ricordo che  $K \subset \mathbb{Z}_p$ ) e  $\psi(x) = \beta$ .

$\psi$  è suriettiva perché  $\psi(x^p) = \beta^p$ , quindi nell'immagine di  $\psi$  ci sono tutti gli elementi di  $K \cong \mathbb{Z}_p$ . Inoltre:  $\psi(0) = 0$ .

Pur  $\psi$  omo m:  $\mathbb{Z}_p[x]_{\text{ker } \psi} \cong K$ ,  $\text{ker } \psi$  ideale di  $\mathbb{Z}_p[x]$ , quindi  $\text{ker } \psi = (q)$  con  $q$  opportuno poiché  $\mathbb{Z}_p[x]$  ha ideali principali.

Quindi:  $K \cong \mathbb{Z}_p[x]/(q)$  poiché  $\mathbb{Z}_p[x]/(q)$  campo e  $q$  irriduc.

**Oss:** se  $K$  campo finito,  $K$  ha  $p^n$  elem. con  $n$  opportuna.

Per  $\exists q \in \mathbb{Z}_p[x]$  t.c.  $K \cong \mathbb{Z}_p/(q) \cong \mathbb{Z}_p[x]/(q)$  è sp. rett. di dimensione  $\deg q$  in  $\mathbb{Z}_p$ . (calcolate mto)

$\mathbb{Z}_p/(q)$  è su di dim  $\deg q$  in  $\mathbb{Z}_p$ . Quindi ha  $p^{\deg q}$  elem.

se  $K$  ha  $p^n$  elem.  $\Rightarrow n = \deg q$ .

Se  $K$  campo finito con  $p^n$  elem.  $\Rightarrow \exists q \in \mathbb{Z}_p[x]$ ,  $\deg q = n$ . irriduc. t.c.  $K \cong \mathbb{Z}_p[x]/(q)$ .

**es:** trovare campo con 4 elem.:  $4 = 2^2 \Rightarrow p=2$ ,  $\deg q = 2$ .

prendiamo  $q = x^2 + x + 1 \in \mathbb{Z}_2[x]$ ,  $M = \mathbb{Z}_2[x]/(x^2 + x + 1)$

è campo con 4 elementi.

**Teorema:** siano  $p$  primo,  $n \in \mathbb{N}$  fissati  $\Rightarrow \exists$  almeno un campo finito con  $p^n$  elementi.

**dim:** sia  $x^{p^n} - x \in \mathbb{Z}_p[x]$ ; tutti gli elem. di  $\mathbb{Z}_p$  sono zeri del polinomio, in part. ha  $p^n$  radici.

Il polin.  $x^{p^n} - x$  non ha fattori multipli, infatti  $\text{mcd}(x^{p^n} - x, D(x^{p^n} - x)) = \text{mcd}(x^{p^n} - x, p^n x^{p^n-1} - 1) = \text{mcd}(x^{p^n} - x, p^n x^{p^n-1}) = 1$  unitano.

Sia  $L$  campo (estensione di  $\mathbb{Z}_p$ ) di esp. composta di  $x^{p^n} - x$ ,  $L$  contiene tutti gli zeri di  $x^{p^n} - x$ , che sono  $p^n$  (sono tutti i punti il polin. non ha fattori comuni multipli).

Sia  $F = \{$  tutte le radici di  $x^{p^n} - x$  in  $L$   $\} = \{ a \in L / a^{p^n} - a = 0 \}$  s.t.  $F$  ha  $p^n$  elem.,  $L$  campo: sono  $a, b \in F$   $a+b \in F$ ?

$$\Rightarrow a^{p^n} - a = 0 \quad b^{p^n} - b = 0, \quad (a+b)^{p^n} = (a+b)^p = a^p + b^p$$

$$(a+b)^p = (a^p + b^p)^2 = a^{p^2} + b^{p^2}$$

$$(a+b)^{p^n} = a^{p^n} + b^{p^n} = a+b$$

$$\Rightarrow a+b \in F. \text{ Inoltre } (a+b)^{p^n} - (a+b) = 0.$$

$$\Rightarrow a \cdot b \in F? \quad (a \cdot b)^{p^n} = a^{p^n} b^{p^n} = ab \Rightarrow ab \in F.$$

$$\Rightarrow 1 \in F, -1 \in F \Rightarrow a \in F \Rightarrow a \in F$$

$$\Rightarrow a \in F, a^{-1} \in F, a \cdot a^{-1} \sim (a^{-1})^{p^n} = (a^{p^n})^{-1} = a^{-1} \Rightarrow a^{-1} \in F.$$

$\Rightarrow F$  è campo con  $p^n$  elementi.

**COROLARIO** V p primo,  $n \in \mathbb{N}$  almeno un polinomio di grado n in  $\mathbb{Z}_p[x]$ .

dim: Siano  $p, n \in \mathbb{N}$  campo,  $p^n$  elem. ( $\exists$  per teo princi)

$K = \mathbb{Z}_p[x]/(q)$  (dimostrare) un q min di deg q = n.

**Lemma:** sia q in  $\mathbb{Z}_p[x]$  polinomio di grado n. Allora q divide  $x^{p^n} - x$ .

dim: consider  $\pi: \mathbb{Z}_p[x] \rightarrow \mathbb{Z}_p[x]/(q)$ ,  $\pi$  proiez. canonica  
 $\pi(x^{p^n} - x) = \pi(x^{p^n}) - \pi(x) = [x^{p^n}]^p - [x] = 0$ .

$K = \mathbb{Z}_p[x]/(q)$  è campo con  $p^n$  elem. K ha q in Gc AB. un  $p^{n-1}$  elem.

sia  $[x] \neq 0$ ,  $[x] \in K \setminus \{0\}$

$$\Rightarrow [x]^{p^n} = 1 \Rightarrow [x]^{p^n} - [x] = [x]^{p^n} - [x] = 0 \Rightarrow [x^{p^n} - x] = 0$$

$$\Rightarrow \pi(x^{p^n} - x) = 0 \Rightarrow x^{p^n} - x \in \text{Ker } \pi = (q).$$

$$\Rightarrow x^{p^n} - x = q \cdot a \Rightarrow q | x^{p^n} - x. \text{ Se } [x] = 0 \Rightarrow [x^{p^n} - x] = 0$$

$$\Rightarrow x^{p^n} - x \in \text{Ker } \pi = (q) \Rightarrow q | x^{p^n} - x.$$

**teo:** ogni elem. di  $\mathbb{Z}_p$  è radice di  $x^{p^n} - x$ . Inoltre  $a \in \mathbb{Z}_p$ ,

$$a^p \equiv a \quad (\text{piccolo teo F.})$$

$$(a^p)^p = a^p = a \dots (a^p)^n = a$$

**TEOREMA:** siano  $F_1, F_2$  due campi con  $p^n$  elem. Allora  $F_1 \cong F_2$ .

(a meno di isom.  $\exists!$  campo FINITO con  $p^n$  elem.)

dim:

sia F campo FINITO  $\Rightarrow F \cong \mathbb{Z}_p[x]/(q)$  con q irriduc.

Quindi abbiamo che  $F_1 \cong \mathbb{Z}_p[x]/(q_1) \subset F_2 \cong \mathbb{Z}_p[x]/(q_2)$  con  $q_1, q_2$  irriduc. di grado n.

Sia  $\varphi$  il campo di rid. completa  $x^{p^n} - x$  a  $\varphi: F_1 \rightarrow F_2$  con  $p^n$  elem.

Se riuscissimo a vedere che  $\varphi$  campo della forma  $\mathbb{Z}_p[x]/(q)$  con q polin. irriduc. deg q = n e isomorfo a F, avremmo finito.

Sia q irriduc. in  $\mathbb{Z}_p[x]$ , deg q = n. Poiché  $q | x^{p^n} - x$  allora in F c'è uno zero di q:  $x^{p^n} - x = qh$ .

Sia  $\beta \in F$  uno zero di q, consideriamo  $\mathbb{Z}_p[x] \xrightarrow{\psi} F$ , con  $\psi$  ottenuta da teo istanziate

$$\begin{array}{ccc} a & \mapsto & a \\ x & \mapsto & \beta \end{array} \text{ da } \mathbb{Z}_p$$

cos' è  $\text{Ker } \psi$ ?

Certamente  $q \in \text{Ker } \psi$  [ $\psi(q) = \psi(q(\beta)) = 0$ ]

$(q) \subseteq \text{Ker } \psi = (h)$ ,  $q, h$  irriduc.  $\Rightarrow \text{Ker } \psi$  è ideale primo

$[\mathbb{Z}_p[x]/\text{Ker } \psi \cong F \in \text{dom. } \psi \Rightarrow \text{Ker } \psi \text{ deve essere isomorfo primo}]$

$\Rightarrow (q) = (h) = \text{Ker } \psi$ .

TEO OMOM:  $\mathbb{Z}_p[x]/(q) \cong F$  hanno entrambi  $p^n$  elementi

$$\Rightarrow \mathbb{Z}_p[x]/(q) = F \Rightarrow F_1 \cong F_2 \cong \mathbb{Z}_p[x]/(q).$$

**def:** dato  $p$  primo,  $n \in \mathbb{N}$ , l'UNICO campo FINITO con  $p^n$  elem. si chiama **Campo di GAUSS** e si indica.

$GF(p, n)$ .