ARITMETICA 18 DIC 2017

$(\mathbb{Z}/p\mathbb{Z})^*$ è un gruppo ciclico.

$\Uparrow$

$\mathbb{F}_{p^n}^*$ è un gruppo ciclico

Teo. Sia K un campo, e sia $G < K^*$ un gruppo finito. Allora G è ciclico.

Dim. $|G| = n$. Se $a \in G$ allora $\mathrm{ord}(a) = d \mid n$.

$$G = \bigcup_{d \mid n} G^{(d)} \quad \rightarrow \text{unione disgiunta.}$$

dove $G^{(d)}$ è il sottoinsieme degli elementi di G che hanno ordine d.

Se $k_d = |G^{(d)}|$ ho che $n = \sum_{d \mid n} k_d$.

Cosa può valere k_d?

(obiettivo: $k_n \neq 0$).

In teoria, può succedere che $k_1 = 0$

Oss Ogni elemento a di ordine d ha proprietà

$$a^d = 1 \quad \Rightarrow$$

è radice del polinomio $X^d - 1$

Eventuali elementi di ordine d sono radici di $X^d - 1$.

$\leq d$ radici.

Se a è radice, anche a^i è radice: $(a^i)^d = (a^d)^i = 1^i = 1$.

Se inoltre a ha ordine d, $|\langle a \rangle| = d$ e quindi

le radici sono esattamente quelle di $\langle a \rangle$.

n° di elementi di ordine $= d$ è $\phi(d)$.

Quindi $k_d = \begin{cases} 0 \\ \phi(d) \end{cases}$

$$n = \sum_{d \mid n} k_d.$$

$$\Rightarrow k_d = \phi(d) \quad \forall d$$

$$n = \sum_{d \mid n} \phi(d)$$

In particolare $k_n = \phi(n)$ e G è ciclico.

<u>Corollario</u> $\mathbb{F}_p^*$ è ciclico.

$$\mathbb{F}_{p^n}^* = \langle \gamma \rangle .$$

$$\mathbb{F}_p(\gamma) = \mathbb{F}_{p^n} = \{0\} \cup \langle \gamma \rangle$$

Cor. 2 In $\mathbb{F}_p[X]$ esistono polinomi irriducibili di qualsiasi grado.

Dim. $[\mathbb{F}_p(\gamma) : \mathbb{F}_p]$ = grado del polinomio minimo di γ su $\mathbb{F}_p$ $= [\mathbb{F}_{p^n} : \mathbb{F}_p] = n$.

↓

IRRIDUCIBILE.

Per quali valori interi di a e b si ha

$$\mathbb{F}_{p^a} \subseteq \mathbb{F}_{p^b} ?$$

$$\left(p \neq q \Rightarrow \mathbb{F}_{p^a} \subsetneq \mathbb{F}_{q^b} \right).$$

$$p^a \neq q^b$$

Se $\mathbb{F}_{p^a} \subseteq \mathbb{F}_{p^b}$, allora $\mathbb{F}_{p^b}$ è uno s.v su $\mathbb{F}_{p^a}$.

Base $\{x_1, \dots, x_k\}$

$$\mathbb{F}_{p^b} = \{ c_1 x_1 + \dots + c_k x_k \mid c_i \in \mathbb{F}_{p^a} \}$$

$$|\mathbb{F}_{p^b}| = p^{ak}. \qquad b = ak.$$

Quindi $a \mid b$

La condizione è sufficiente. Supponiamo che $a \mid b$.

$$\mathbb{F}_{p^a} = \{ x \mid x^{p^a} - x = 0 \} = \{0\} \cup \{ x \mid x^{p^a - 1} = 1 \}$$

$$\mathbb{F}_{p^b} = \{ x \mid x^{p^b} - x = 0 \} = \{0\} \cup \{ x \mid x^{p^b - 1} = 1 \}$$

$a \mid b \Rightarrow p^a - 1 \mid p^b - 1$

$b = ak$ $\quad p^b - 1 = p^{ak} - 1 = (p^a)^k - 1$

$$= (p^a - 1)(p^{a(k-1)} + p^{a(k-2)} + \dots + p^a + 1)$$

$x^{p^a - 1} = 1 \Rightarrow x^{p^b - 1} = 1$, $\quad \mathbb{F}_{p^a} \subseteq \mathbb{F}_{p^b}$

$f(x) \in \mathbb{F}_p[x]$ f irriducibile di grado n.

α radice $\Rightarrow [\mathbb{F}_p(\alpha) : \mathbb{F}_p] = n$ $\quad \mathbb{F}_p(\alpha) = \mathbb{F}_{p^n}$

β altra radice $\Rightarrow [\mathbb{F}_p(\beta) : \mathbb{F}_p] = n$ $\quad \mathbb{F}_p(\beta) = \mathbb{F}_{p^n}$

$$\mathbb{F}_p(\alpha) = \mathbb{F}_p(\beta) = \mathbb{F}_{p^n}$$

α, β di $f(x) = \mathbb{F}_{p^n}$.

f non necessariamente irriducibile.

$f = f_1 f_2 \cdots f_r$, f_i irriducibili,

$\deg f = n \qquad \deg f_i = k_i \qquad n = k_1 + k_2 + \dots + k_r .$

c.d.s. di $f_1 = \mathbb{F}_{p^{k_1}}$

$\vdots$

c.d.s. di $f_r = \mathbb{F}_{p^{k_r}}$

c.d.s. di $f = \mathbb{F}_{p^k}$ dove

$k = \operatorname{mcm}(k_1, \dots, k_r)$.

Esempio speciale: c.d.s. su $\mathbb{F}_p$ di $X^n - 1$.

$n = p^k m$ con $\boxed{(m,p)=1}$ $(p^k \| n)$

$$X^n - 1 = X^{mp^k} - 1 = (X^m - 1)^{p^k}.$$

c.d.c di $X^n - 1$ = c.d.s. di $X^m - 1$

↳ Insieme delle radici $\overset{G}{\smile}$ forma un gruppo

$1 \in G$ $\quad a, b \in G$ $\quad a^m = 1,\ b^m = 1 \Rightarrow (ab)^m = 1$

$a \in G$ $\quad a^m = 1$ $\quad (a^{-1})^m = (a^m)^{-1} = 1$.

G è un gruppo ciclico.

DERIVATA di $X^m - 1 = mX^{m-1} \neq 0$.

$\Rightarrow$ l'unica radice della derivata è 0.

$\Rightarrow$ NON CI SONO RADICI MULTIPLE

$\Rightarrow$ G è un gruppo ciclico di ordine $= m$. $G = \langle \gamma \rangle$.

c.d.s. $= \mathbb{F}_p(\gamma)$.

Quando $\mathbb{F}_{p^k}$ ∋ elemento di ordine m?

Cond. necessaria: $\mathbb{F}_{p^k}^* \supseteq \langle \gamma \rangle$

$m \mid p^k - 1 = \text{ord}(\mathbb{F}_{p^k}^*)$

La condizione è sufficiente. Infatti se $m \mid p^k - 1$, poiché $\mathbb{F}_{p^k}^*$ è ciclico, contiene un sgr di ordine m

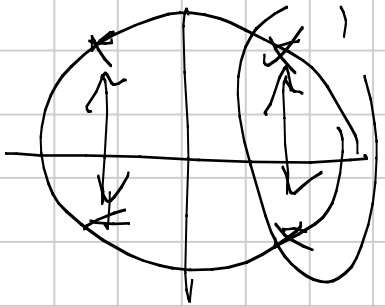
c.d.s. $= \mathbb{F}_{p^k}$ dove k è il più piccolo intero per cui

$$m \mid p^k - 1 \qquad p^k \equiv 1 \pmod{m}$$

Questo è $\operatorname{ord}(\bar{p})$ in $(\mathbb{Z}/m\mathbb{Z})^*$

Esempio $X^4 + 1 \in \mathbb{Z}[X]$ è IRRIDUCIBILE

ma È RIDUCIBILE modulo p $\forall$ primo p.



RADICI RAZIONALI NO.

$$\left(X - \frac{\sqrt{2}}{2} - \frac{i\sqrt{2}}{2}\right)\left(X - \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right)$$

$$= \left(X - \frac{\sqrt{2}}{2}\right)^2 - \left(\frac{i\sqrt{2}}{2}\right)^2$$

$$= X^2 - \sqrt{2}X + \frac{1}{2} + \frac{1}{2} \notin \mathbb{Z}[X]$$

Primi:

$p = 2 \qquad X^4 + 1 = (X+1)^4$ RIDUCIBILE

$p \neq 2$ $\qquad X^4+1 = \dfrac{X^8-1}{X^4-1}$

radici di X^4+1 $\longrightarrow$ radici di X^8-1

$\|$

esattamente quelle di ordine $=8$,

$\text{o.d.r.} = p^k$ dove k è il min intero positivo

per cui $\qquad p^k \equiv 1 \pmod 8$

$$\begin{cases} p \equiv 1 \pmod 8 & \Rightarrow k=1 \\ p \equiv 3,5,7 \pmod 8 & \Rightarrow k=2 \end{cases}$$

Quindi il grado del comp. di riferimento è = 1,2

= m.c.m. dei gradi dei fattori irriducibili.