CAMPI FINITI

mercoledì 1 dicembre 2021 11:56

- **L'omomorfismo di Frobenius**

  Char $K = p$ primo.

  $F: K \to K$, $a \to a^p$ F è omo iniettivo.

  anche F^j sono omo iniettivi.

- K campo $\varphi: K \to K$ omo. Allora $Fix\,\varphi = \{k \in K \mid \varphi(k) = k\} \equiv$ insieme degli ell. di K lasciati fissi da φ è sottocampo di K.

- **Teorema di classificazione dei campi finiti**

  Ogni campo finito ha $\# p^n$ con p primo e n intero positivo.
  $\forall p$ ed n $\exists$ un campo finito di $\# p^n$ unico a meno di iso.
  Per indicare tale campo uso $\mathbb{F}_{p^n}$

- **Corollario.**

  Dato $f(x) \in \mathbb{Z}_p[x]$ irrid. di grado n. il suo c.d.s è $\cong$ a $\mathbb{F}_{p^n}$

- Dato un campo finito $\mathbb{F}_{p^n}$ il gruppo moltiplicativo $\mathbb{F}_{p^n}^*$ è ciclico

- **Corollario**

  Dato un campo finito $\mathbb{F}_{p^n}$ sia α un generatore del gruppo ciclico $\mathbb{F}_{p^n}^*$. Se chiamo $f(x)$ il pol. minimo di α su $\mathbb{Z}_p[x]$ vale che $\deg f = n$.

  Dunque $\forall p$ ed n $\exists$ in $\mathbb{Z}_p[x]$ un pol. irrid di grado n.

- Dati p ed n. $x^{p^n} - x$ è il prodotto di tutti i polinomi monici irriducibili in $\mathbb{Z}_p[x]$ di grado d divisore di n.

- Dati p ed n. $\exists$ $\frac{\phi(p^n-1)}{n}$ pol. monici irriducibili in $\mathbb{Z}_p[x]$ di grado n tali che se chiamo $R = \{$tutte le radici di questi pol$\}$ vale che $R = \{$insieme dei generatori di $\mathbb{F}_{p^n}^*\}$
  Questi pol. vengono chiamati **primitivi**.

Sia L un campo finito. Char $L = p$. $\lvert L\rvert = p^n$ L è c.d.s di $x^{p^n} - x$ su $\mathbb{Z}_p$ indico L con $\mathbb{F}_{p^n}$

Quindi ....

Quindi ....

- $\mathbb{Z}_p \subseteq K$ • $|K| = p^n$
- Gli elt. di K sono tutte e sole le radici di $x^{p^n} - x$
- $\mathbb{Z}_p \subseteq \mathbb{F}_{p^n}$ è estensione di Galois. perché $\mathbb{F}_{p^n}$ è c.d.s di $x^{p^n} - x$ che ha tutte radici distinte $\Rightarrow$ è separabile.
- $Aut\left(\mathbb{F}_{p^n}/\mathbb{F}_p\right) \equiv$ gruppo di Galois.
- $\left|Aut\left(\mathbb{F}_{p^n}/\mathbb{F}_p\right)\right| = n$
- $(\mathbb{F}_{p^n})^*$ è ciclico generato da un $\gamma \Rightarrow ord(\gamma) = p^n - 1$.
- Frobenius $F \in Aut\left(\mathbb{F}_{p^n}/\mathbb{F}_p\right)$ e $F^n = id \Rightarrow ord(F) = n \Rightarrow$ **$Aut\left(\mathbb{F}_{p^n}/\mathbb{F}_p\right) \cong \mathbb{Z}_n$**
  $\hookrightarrow$ è il generatore
- Per la teoria di Galois so che, preso un sgr di $Aut\left(\mathbb{F}_{p^n}/\mathbb{F}_p\right) \cong \mathbb{Z}_n$, a lui associo un sottocampo.

Quindi $\forall\, d|n$ ho in $\mathbb{Z}_n$ un sgr $\cong \mathbb{Z}_d$ cioè il generato da $\langle \frac{n}{d} \rangle$
ma allora $J(\langle \frac{n}{d} \rangle)$ è sottocampo di $\mathbb{F}_{p^n}$ t.c. $[J(\langle \frac{n}{d} \rangle) : \mathbb{F}_p] = d$
$\Rightarrow$ tale sottocampo è $\mathbb{F}_{p^d}$

Quindi se ho $\underbrace{\mathbb{F}_p \subseteq K \subseteq \mathbb{F}_{p^n}}_{n} \Rightarrow [K : \mathbb{F}_p] \,|\, n = [\mathbb{F}_{p^n} : \mathbb{F}_p]$

Quindi i sottocampi di $\mathbb{F}_{p^n}$ sono tutti e soli gli $\mathbb{F}_{p^d}$ con $d|n$

• Conseguenze sui polinomi

- $\mathbb{F}_{p^d}$ è il c.d.s di $\forall$ pol. irrid. di grado d su $\mathbb{F}_p$
- Sia $f(x) \in \mathbb{F}_p[x]$ $f(x) = q_1(x) \dots q_k(x)$ con i $q_j(x)$ irrid. di grado rispettivamente $\beta_1, \dots, \beta_k$
  Allora il c.d.s di $f(x)$ su $\mathbb{F}_p$ è **$\mathbb{F}_{p^{m.c.m(\beta_1, \beta_2, \dots, \beta_k)}}$**

• altri fatti utili

- $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$, $[\mathbb{F}_{p^n} : \mathbb{F}_{p^m}] = \frac{n}{m}$
- $\underbrace{\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}}_{\text{è normale.}} \Leftrightarrow m|n$