1 Polinomi ciclotomici in caratteristica p

Proposizione 1.1. *Sia p primo e $n \in \mathbb{N}$ allora l'estensione $\mathbb{F}_p \subseteq \mathbb{F}_{p^n}$ è di Galois con gruppo $\mathbb{Z}_n$*

Dimostrazione. L'estensione è di Galois in quanto è il campo di spezzamento del polinomio separabile $x^{p^n} - 1$ (ha radici distinte).
Poichè l'estensione è di Galois, il gruppo ha cardinalità $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$.
Osserviamo che l'omomorfismo di Frobenius

$$\mathcal{F} : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n} \quad a \to a^p$$

è un generatore del gruppo di Galois.
Dal piccolo teorema di Fermat segue che $\mathcal{F}$ appartiene al gruppo.
Inoltre l'ordine di $\mathcal{F}$ divide n, mostriamo che è proprio n.
Supponiamo $\mathcal{F}^j = Id$ per un certo $j < n$ allora il polinomio $x^{p^j} - 1$ avrebbe p^n radici, il che è assurdo.

Da ora in avanti denotiamo con μ_n l'insieme delle radici del polinomio $x^n - 1 \in K[x]$.

Osservazione 1. μ_n è un sottogruppo moltiplicativo del campo di spezzamento di $x^n - 1$ dunque è un gruppo ciclico di ordine n,

Osservazione 2. Nel caso in cui $\mathbb{K} = \mathbb{F}_p$, $\mathbb{F}_p(\mu_n) = \mathbb{F}_{p^k}$ dunque $\mathbb{F}_p \subseteq \mathbb{F}_p(\mu_n)$ è di Galois per la proposizione precedente

Sia $\sigma \in \mathrm{Gal}(\mathbb{F}_p(\mu_n)/\mathbb{F}_p)$, possiamo considerare la restrizione di σ a μ_n dunque poichè $\mu_n = \langle\zeta\rangle$ $\sigma(\zeta) = \zeta^n$ dove ζ^a genera μ_n dunque i a e n sono coprimi.
Possiamo dunque definire la mappa

$$\vartheta : \mathrm{Gal}(\mathbb{F}_p(\mu_n)/\mathbb{F}_p) \to (\mathbb{Z}_n)^\star$$

tale che $\vartheta(\sigma) = a$.

Proposizione 1.2. *ϑ è iniettiva.*

Dimostrazione. Sia $\sigma \in \mathrm{Gal}(\mathbb{F}_p(\mu_n)/\mathbb{F}_p)$ tale che $\vartheta(\sigma) = id$ dunque $\sigma_{|\mu_n)} = Id$ e poichè $\sigma_{|\mathbb{F}_p} = Id$ ne segue che $\sigma = Id_{\mathrm{Gal}(\mathbb{F}_p(\mu_n)/\mathbb{F}_p)}$ □

Proposizione 1.3. *Sia n primo con p.*
La mappa ϑ ha immagine $\langle p\rangle$.

Dimostrazione. Come abbiamo dimostrato $\mathrm{Gal}(\mathbb{F}_p(\mu_n)/\mathbb{F}_p)$ è generato dall'omomorfismo di Frobenius.
Ora $\vartheta(\mathcal{F}) = p$ dunque $Im\theta$ è generato da p in $(\mathbb{Z}_n)^\star$

Corollario 1.4.

$$[\mathbb{F}_p(\mu_n) : \mathbb{F}_p] = \text{ ordine moltiplicativo di } p \text{ in } (\mathbb{Z}_n)^\star$$

Sia $\overline{\phi_n}$ l'n-esimo polinomio ciclotomico proiettato su $\mathbb{Z}_p$

Proposizione 1.5. *Sia n primo con p.*
I fattori irriducibili di $\overline{\phi_n}$ in $\mathbb{F}_p[x]$ sono distinti a hanno grado uguale all'ordine di p in $(\mathbb{Z}_n)^\star$

Dimostrazione. $\overline{\phi_n}$ è separabile essendolo $x^n - 1$.
Sia α una radice di $\overline{\phi_n}$, α è una radice primitiva da cui

$$\mathbb{F}_p(\alpha) = \mathbb{F}_p(\mu_n)$$

Sia $f(x)$ il polinomio minimo di α su $\mathbb{F}_p$ dunque

$$\deg f = [\mathbb{F}_p(\alpha) : \mathbb{F}_p] = [\mathbb{F}_p(\mu_n) : \mathbb{F}_p] = \text{ ordine di } p \text{ in } (\mathbb{Z}_n)^\star$$

Dunque tutti i fattori irriducibili (polinomi minimi di radici) di $\overline{\phi_n}$ hanno grado uguale all'ordine moltiplicativo di p. □

Corollario 1.6.

$$\overline{\phi_n} \text{ 'e irriducibile in } \mathbb{F}_p[x] \quad \Leftrightarrow \quad \begin{cases} M.C.D.(p,n) = 1 \\ \langle p \rangle = (\mathbb{Z}_n)^\star \end{cases}$$

Dimostrazione. $\Rightarrow$ Se $M.C.D(p,m) = 1$ allora abbiamo la seguente relazione in $\mathbb{Z}[x]$

$$\phi_{p^r m}(x) = \frac{\phi_m\left(x^{p^r}\right)}{\phi_m\left(x^{p^{r-1}}\right)}$$

(entrambi i polinomi sono monici, quello a sinistra è irriducibile, entrambi hanno una radice in comune)
Tale relazione "letta" in $\mathbb{Z}_p[x]$ diventa

$$\overline{\phi_{p^r m}}(x) = \left(\overline{\phi_m}(x)\right)^{p^r - p^{r-1}}$$

.
Dunque $\overline{\phi_n}$ irriducibile implica n e p primi tra loro.
Se $\overline{\phi_n}$ irriducibile allora l'ordine di p in $(\mathbb{Z}_n)^\star$ è uguale al grado del polinomio ciclotomico che è $\varphi(n)$.
Dunque p è un generatore del gruppo moltiplicativo.
$\Leftarrow$ se $M.C.D(p,n) = 1$ e p genera $(\mathbb{Z}_n)^\star$ allora per la proposizione precedente i fattori irriducibili di $\overline{\phi_n}$ devono avere grado $\varphi(n)$ che è il grado del polinomio dunque è irriducibile.

Corollario 1.7. *Se $(\mathbb{Z}_n)^\star$ non è ciclico.*
$\overline{\phi_n}$ si fattorizza in $\mathbb{Z}_p[x]$ per ogni primo p

Osservazione 3. Il caso più piccolo è per $n = 8$ infatti $\phi(8) = x^4 + 1$ si fattorizza in ogni $\mathbb{Z}_p$ con p primo