Sottoestensione di $\mathbb{Q}(\zeta_p)$ di grado 2 su $\mathbb{Q}$

Giacomo Mezzedimi

February 1, 2015

Teorema: Sia $\mathbb{Q}(\zeta_p)$ la p-esima estensione ciclotomica di $\mathbb{Q}$, con $p > 2$ primo. Allora $\mathbb{Q}(\zeta_p)$ ha un'unica sottoestensione di grado 2 su $\mathbb{Q}$, che in particolare é $\mathbb{Q}(\sqrt{p})$ se $p \equiv 1\ (4)$, mentre é $\mathbb{Q}(\sqrt{-p})$ se $p \equiv 3\ (4)$.

Dimostrazione: Per la teoria di Galois, abbiamo che

$$Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q}) = \langle\sigma\rangle \cong \mathbb{Z}/(p-1)\mathbb{Z},$$

dove $\sigma : \zeta_p \to \zeta_p^a$, con $ord(a) = p-1$.

Allora, per il teorema di corrispondenza di Galois, le sottoestensioni di $\mathbb{Q}(\zeta_p)$ di grado 2 su $\mathbb{Q}$ corrispondono ai sottogruppi di indice 2 di $\langle\sigma\rangle$, che essendo ciclico ne ha solo uno.

In particolare, questa unica sottoestensione é $Fix(\langle\sigma^2\rangle) = \mathbb{Q}(\alpha)$, con $\alpha = \zeta_p + \zeta_p^{a^2} + \ldots + \zeta_p^{a^{p-3}}$.

$\mathbb{Q}(\alpha)$ ha grado 2 su $\mathbb{Q}$, dunque α é radice di un polinomio di secondo grado in $\mathbb{Q}[x]$.

Poniamo $\tilde{\alpha} = \zeta_p^a + \zeta_p^{a^3} + \ldots + \zeta_p^{a^{p-2}}$ e $\mu(x) = x^2 - (\alpha + \tilde{\alpha})x + \alpha\tilde{\alpha}$.

Si vede che $\alpha + \tilde{\alpha} + 1 = 1 + \zeta_p + \zeta_p^2 + \ldots + \zeta_p^{p-1} = 0$, dunque $\alpha + \tilde{\alpha} = -1$.

Ma allora $\mu(\alpha) = \alpha^2 + \alpha + \alpha\tilde{\alpha} = \alpha(-1-\tilde{\alpha}) + \alpha + \alpha\tilde{\alpha} = 0$; calcoliamo ora il prodotto $\alpha\tilde{\alpha}$ nei casi $p \equiv 1\ (4)$ e $p \equiv 3\ (4)$.

- Caso $p \equiv 1\ (4)$.

  Vediamo che in $\alpha\tilde{\alpha}$ non ci sono monomi 1: infatti essi possono nascere solo da un prodotto del tipo $\zeta_p^k \cdot \zeta_p^{-k}$, ma se $p \equiv 1\ (4)$, -1 é un quadrato modulo p e dunque k é un quadrato modulo $p \Leftrightarrow -k$ é un quadrato modulo p.

  Dunque $\alpha\tilde{\alpha} = s(\zeta_p + \zeta_p^2 + \ldots + \zeta_p^{p-1})$, in quanto le soluzioni delle equazioni $a^{2m} + a^{2n+1} = \gamma\ (p)$, con $\gamma \in \mathbb{F}_p^*$ sono in ugual numero $\forall\gamma$, poiché se $(m_1, n_1), \ldots, (m_s, n_s)$ sono le soluzioni dell'equazione $a^{2m} + a^{2n+1} = 1$

(p), allora $(n_1, m_1+1), \ldots, (n_s, m_s+1)$ sono le soluzioni dell'equazione $a^{2m} + a^{2n+1} = a$ (p), e non ce ne sono altre, poiché se ci fosse anche $(\tilde{m}, \tilde{n})$, allora $(\tilde{n}, \tilde{m}-1)$ sarebbe un'altra soluzione di $a^{2m} + a^{2n+1} = 1$ (p). Ma poiché $\tilde{\sigma} : 1 \to a$ é un automorfismo di $\mathbb{F}_p$, allora iterando questo ragionamento si ha ció che si voleva.

In particolare, $\alpha\tilde{\alpha}$ ha $(\frac{p-1}{2})^2$ monomi, dunque $s = \frac{(\frac{p-1}{2})^2}{p-1} = \frac{p-1}{4}$.

Allora $\alpha\tilde{\alpha} + s = s(1 + \zeta_p + \zeta_p^2 + \ldots + \zeta_p^{p-1}) = 0$, da cui $\alpha\tilde{\alpha} = -\frac{p-1}{4}$.

- Caso $p \equiv 3$ (4).

  Sappiamo che -1 non é un quadrato modulo p, dunque k é un quadrato modulo $p \Leftrightarrow -k$ non é un quadrato modulo p.

  Dunque $\tilde{\alpha} = \zeta_p^{-1} + \zeta_p^{-a^2} + \ldots + \zeta_p^{-a^{p-2}}$, da cui segue che in $\alpha\tilde{\alpha}$ ci sono $\frac{p-1}{2}$ monomi 1. I restanti monomi sono potenze di ζ_p; in particolare:

  $$\alpha\tilde{\alpha} = \frac{p-1}{2} + t(\zeta_p + \zeta_p^2 + \ldots + \zeta_p^{p-1})$$

  per un ragionamento analogo a quello nel caso precedente.

  Inoltre $t = \frac{(\frac{p-1}{2})^2 - \frac{p-1}{2}}{p-1} = \frac{p-3}{4}$, dunque $\alpha\tilde{\alpha} + (\frac{p-3}{4} - \frac{p-1}{2}) = t(1 + \zeta_p + \zeta_p^2 + \ldots + \zeta_p^{p-1}) = 0$, da cui $\alpha\tilde{\alpha} = \frac{p+1}{4}$.

Dunque, poiché $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$, allora $\mu(x)$ é il polinomio minimo di α su $\mathbb{Q}$, e se $p \equiv 1$ (4), α é radice del polinomio $x^2 + x - \frac{p-1}{4}$, cioé $\alpha = \frac{-1 \pm \sqrt{p}}{2}$, da cui $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{p})$, mentre se $p \equiv 3$ (4), α é radice del polinomio $x^2 + x + \frac{p+1}{4}$, cioé $\alpha = \frac{-1 \pm \sqrt{-p}}{2}$, da cui $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{-p})$. $\square$