Proof of theorem 2 (Stillwell)

Polinomio $p(x)$

$B \subseteq B(\alpha) \subseteq E$

(1) $Gal(E/B(\alpha))$ es normal subgrupo de $Gal(E/B)$

Veamos que es el ker de un homomorfismo

$$\varphi : Gal(E/B) \longrightarrow Gal(B(\alpha)/B)$$

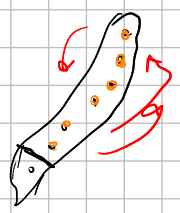
$$\varphi \longrightarrow \varphi|_{B(\alpha)}$$

Si $\varphi \in Gal(E/B(\alpha))$ entonces $\phi(\varphi) = id \Rightarrow Gal(E/B(\alpha)) \triangleleft Gal(E/B)$

Idea (más o menos)

$S^1 = \{$raíces del polinomio$\}$

Raíces de $\alpha^5 - 1 = 0$



$Gal(B(\alpha)/B)$ mueve las órbitas

$Gal(E/B(\alpha))$ órbitas en el espacio de raíces.

Las raíces de una de estas órbitas tienen que ser raíces de uno de los polinomios que aparecen de $p(x)$ cuando consideramos a α como nuevo coeficiente variable

Ejemplo $(x^2+x+1)^3 - 1 = 0$

$$\Downarrow$$

$$\begin{cases} x^2 + x = 0 \\ x^2 + x + 1 - \alpha = 0 \\ x^2 + x + 1 - \alpha^2 = 0 \end{cases}$$

siendo $\alpha = e^{2\pi i/3}$

(Q) $\dfrac{Gal(E/B)}{Gal(E/B(\alpha))}$ es abeliano

Idea $\dfrac{Gal(E/B)}{Gal(E/B(\alpha))} \leq$ (subgrupo) $Gal\left(\dfrac{B(\alpha)}{B}\right)$ y este grupo es abeliano porque $\alpha^p \in B$, p primo, y no hay más pth de la unidad. Veamos:

a) Si $\alpha^p = 1$, $\varphi, \psi \in Gal\left(\dfrac{B(\alpha)}{B}\right)$ $\quad \varphi(\alpha) = \alpha^i$, $\psi(\alpha) = \alpha^j$

$$\varphi \circ \psi(\alpha) = \alpha^{i\,j} = \psi\varphi(\alpha)$$

b) Si $\alpha^p \neq 1$, las otras p-ésimas están en B

$\varphi, \psi \in Gal\left(\dfrac{B(\alpha)}{B}\right)$ $\quad \varphi(\alpha)^p = \varphi(\alpha^p) = \alpha^p \Rightarrow \varphi(\alpha) = \xi^i \alpha$

$\psi(\alpha)^p = \psi(\alpha^p) = \alpha^p \Rightarrow \psi(\alpha) = \xi^j \alpha$

Luego $\varphi\psi(\alpha) = \xi^i \xi^j \alpha = \psi\varphi(\alpha)$. □