Lema A (Teorema de Artin parte A) ②

Sea E un cuerpo y sean $\gamma_1 - \gamma_n \in \text{Aut}\, E$ distintos
y sea $G = \{\gamma_1, - \gamma_n\}$.
$\Rightarrow [E : E^G] \geq n.$

Dem. Supongamos, para llegar a una contradicción, que $[E : E^G] = r < n$.

Sea $\{\alpha_1 - \alpha_r\}$ una base de E/E^G.

Aplicamos $\gamma_1 - \gamma_n$ a los elementos de la base:
y sean $x_1 - x_n$ variables. Escribimos el siguiente sistema de ecuaciones lineales:

$$\left.\begin{array}{l} \gamma_1(\alpha_1)x_1 + \cdots + \gamma_n(\alpha_1)x_n = 0 \\ \gamma_1(\alpha_2)x_1 + \cdots + \gamma_n(\alpha_2)x_n = 0 \\ \vdots \\ \gamma_1(\alpha_r)x_1 + \cdots + \gamma_n(\alpha_r)x_n = 0 \end{array}\right\} (*)$$

Como $r < n$ el sistema tiene una solución no trivial. $\Rightarrow \exists\ (a_1, -, a_n) \neq (0, 0 \ldots 0)$ en E^n tq. solución al sistema.

Sea ahora $\beta \in E$ un elemento cualquiera
$\Rightarrow \beta = \sum_{i=1}^{r} b_i \alpha_i$ con $b_i \in E^G$. Re-escribimos $(*)$

$$\left.\begin{array}{l} b_1 \gamma_1(\alpha_1)x_1 + - + b_1\gamma_n(\alpha_1)x_n = 0 \\ b_2\gamma_1(\alpha_2)x_1 + - + b_2\gamma_n(\alpha_2)x_n = 0 \\ \vdots \\ b_r\gamma_1(\alpha_r)x_1 + - + b_r\gamma_n(\alpha_r)x_n = 0 \end{array}\right\} (1)$$

Como $b_1 - b_r \in E^G \Rightarrow \gamma_i(b_j) = b_j$
para $i = 1 - n,\ j = 1 - r \Rightarrow$ reescribimos (1)

$$\left.\begin{array}{l} \gamma_1(b_1\alpha_1)x_1 + \dots + \gamma_n(b_1\alpha_1)x_n = 0 \\ \gamma_1(b_2\alpha_2)x_1 + \dots + \gamma_n(b_2\alpha_2)x_n = 0 \\ \vdots \\ \gamma_1(b_r\alpha_r)x_1 + \dots + \gamma_n(b_r\alpha_r)x_n = 0 \end{array}\right\} (2)$$

y ahora sumamos todas las ecuaciones:

$$\gamma_1\left(\sum_{i=1}^{r} b_i\alpha_i\right)x_1 + \dots + \gamma_n\left(\sum_{i=1}^{r} b_i\alpha_i\right)x_n = 0$$

$$\parallel$$

$$\gamma_1(\beta)x_1 + \dots + \gamma_n(\beta)x_n = 0 \Rightarrow$$

Como $\beta \in E$ era un elemento cualquiera

$\Rightarrow \quad \forall \beta \in E$

$$\gamma_1(\beta)x_1 + \dots + \gamma_n(\beta)x_n = 0$$

Pero recordamos ahora que el sistema $(*)$ y por tanto el sistema (2) tiene una solución no trivial $(a_1 \dots a_n) \in E^n \Rightarrow$

$$\gamma_1(\beta)a_1 + \dots + \gamma_n(\beta)a_n = 0 \quad \forall \beta \in E$$

$\Rightarrow \gamma_1 \dots \gamma_n$ no son linealmente independientes sobre E, lo que contradice el lema de Dedekind. ∎

Teorema de Artin parte B.

Sea $G = \{\sigma_1 - \sigma_n\}$ un subgrupo de $Aut(E) \supseteq G$
Entonces
$$[E : E^G] = |G|$$

Dem Por el Lema (A) basta probar que $[E : E^G] \leq |G|$
Para llegar a una contradicción supongamos que
$$[E : E^G] > |G| = n.$$

Sean $\{\omega_1 - \omega_n, \omega_{n+1}\} \subset E$ linealmente independientes sobre E^G.

Consideramos el sistema de n-ecuaciones con n+1 incógnitas:

$$\left.\begin{aligned} \sigma_1(\omega_1)x_1 + \cdots + \sigma_1(\omega_{n+1})x_{n+1} = 0 \\ \vdots \\ \sigma_n(\omega_1)x_1 + \cdots + \sigma_n(\omega_{n+1})x_{n+1} = 0 \end{aligned}\right\} (*)$$

Como $n+1 > n \rightarrow$ el sistema $(*)$ tiene una solución no trivial sobre E. Tomemos una de esas soluciones no triviales con el menor nº de coordenadas no nulas. Reordenando $x_1 - x_{n+1}$ en el sistema, (si hace falta) podemos suponer que la solución es de la forma:
$$(a_1, \ldots, a_r, 0 \ldots 0).$$

Observaciones:

① $r \neq 1$. Si $r = 1$ entonces $\sigma_1(\omega_1)a_1 = 0$
Como $\omega_1 \neq 0 \Rightarrow \sigma_1(\omega_1) \neq 0$ (σ_1 es un automorfismo)
$\Rightarrow a_1 = 0$ y la solución sería trivial. Por tanto $r > 1$

② Podemos suponer que $a_r = 1$ (si no, multiplicamos $(a_1 \dots a_r, 0 \dots 0)$ por a_r^{-1} para que la última coordenada sea 1, y el vector obtenido sigue siendo solución del sistema (*)).

③ No todos los elementos $a_1 \dots a_r$ están en E^G, pues de lo contrario, en la fila de (*) con $\gamma_i = id$ se tendría que:

$$\gamma_i(w_1)x_1 + \dots + \gamma_i(w_{n+1})x_{n+1} = w_1x_1 + \dots + w_{n+1}x_{n+1} = 0$$

y reemplazando $x_1 \dots x_{n+1}$ por la solución $(a_1 \dots a_r, 0 \dots$ se tendría que:

$$w_1a_1 + \dots + a_rw_r = 0$$

obteniéndose una combinación lineal $\neq 0$ no trivial de $w_1 \dots w_r$ sobre E^G, lo que contradice el hecho de que $w_1 \dots w_{n+1}$ son linealmente independientes sobre E^G.

Así, podemos suponer, sin pérdida de generalidad, que, por ejemplo $a_1 \notin E^G$.

Resumiendo: tenemos una solución no trivial de (*) con el menor nº de coordenadas no nulas $(a_1 \dots a_r, 0 \dots 0)$ y sabemos que:

$$\boxed{\cdot\, r > 1, \quad a_r = 1, \quad a_1 \notin E^G.}$$

Como $a_1 \notin E^G$, $\exists k$ tal que $\gamma_k(a_1) \neq a_1$.

Reescribimos el sistema (*) evaluando en la solución $(a_1, \dots \underset{1}{\underset{\shortparallel}{a_r}}, \dots)$:

$$\left.\begin{array}{l} \gamma_1(w_1)a_1 + \cdots + \gamma_1(w_r) = 0 \\ \vdots \\ \gamma_n(w_1)a_1 + \cdots + \gamma_n(w_r) = 0 \end{array}\right\} (1)$$

Ahora aplicamos γ_k a todo el sistema (1)

$$\left.\begin{array}{l} \gamma_k(\gamma_1(w_1))\gamma_k(a_1) + \cdots + \gamma_k(\gamma_1(w_r)) = 0 \\ \vdots \\ \gamma_k(\gamma_n(w_1))\gamma_k(a_1) + \cdots + \gamma_k(\gamma_n(w_r)) = 0 \end{array}\right\} (2)$$

Como $\{\gamma_1 \ldots \gamma_n\}$ es un subgrupo de Aut(E)

$\underbrace{\{\gamma_k \circ \gamma_1, \ldots, \gamma_k \circ \gamma_n\}}$ $= \{\gamma_1 \ldots \gamma_n\}$

es sólo una reordenación de los elementos de Aut(E).

De modo que (2) se puede reescribir como:

$$\left.\begin{array}{l} \gamma_1(w_1)\gamma_k(a_1) + \cdots + \gamma_k(w_r) = 0 \\ \vdots \\ \gamma_n(w_1)\gamma_k(a_1) + \cdots + \gamma_k(w_r) = 0 \end{array}\right\} (3)$$

(quizás reordenando las filas de (2))

Ahora restamos a cada fila de (1) la correspondiente fila de (3) y nos queda:

$$\gamma_1(w_1)(a_1 - \gamma_k(a_1)) + \cdots + \gamma_1(w_{r-1})(a_{r-1} - \gamma_k(a_{r-1})) = 0$$

$$\vdots$$

$$\gamma_n(w_1)(a_1 - \gamma_k(a_1)) + \cdots + \gamma_n(w_{r-1})(a_{r-1} - \gamma_k(a_{r-1})) = 0$$

$\Rightarrow (\overset{\neq 0}{a_1 - \gamma_k(a_1)}, \ldots, a_{r-1} - \gamma_k(a_{r-1}), 0 \ldots 0)$

es una solución no trivial de (*) con menos coordenadas no nulas que $(a_1 \ldots a_r, 0 \ldots 0)$ Contradicción