Teorema (di Artin):

Dati K estensione di F, G sottogruppo finito di $\mathrm{Aut}_F(K)$, si ha:

$$[K : \mathrm{Fix}_K(G)] = |G|$$

Dim.:

$E = \mathrm{Fix}_K(G)$, $n = |G|$, $G = \{\varphi_1 = \mathrm{Id}, \varphi_2, \dots, \varphi_n\}$

$\Rightarrow E = \{b \in K \mid b = \varphi_1(b) = \dots = \varphi_n(b)\}$

$\Rightarrow$ per il Lemma di Dedekind si ha:

$$[K : E] \geq n$$

$\Rightarrow$ se fosse $[K : E] > n$, $\exists \{b_0, \dots, b_n\}$ in K lin. ind. su E (sono $n+1$ elementi)

$\Rightarrow$ calcoliamo la matrice associata:

$$A = \begin{pmatrix} \varphi_1^{-1}(b_0) & \dots & \varphi_1^{-1}(b_n) \\ \vdots & & \\ \varphi_n^{-1}(b_0) & \dots & \varphi_n^{-1}(b_n) \end{pmatrix}$$

$\Rightarrow v \longmapsto Av$ è E-lineare $E^{n+1} \longrightarrow E^n$

$\Rightarrow$ sia $\vec{a} = (a_0, \dots, a_n)^T \neq \vec{0}$ nello spazio nullo di A:

$$A\vec{a} = 0 \Rightarrow \sum_{i=0}^{n} \varphi_s^{-1}(b_i) a_i = 0 \quad \forall s = 1, \dots, n$$

$\Rightarrow$ se $c \in K$ si ha:

$$\sum_{i=0}^{n} \mathrm{Tr}_G(ca_i) b_i = \sum_{s=1}^{n} \sum_{i=0}^{n} \varphi_s(ca_i) b_i$$

$$= \sum_{s=1}^{n} \sum_{i=0}^{n} \varphi_s(ca_i)\varphi_s\varphi_s^{-1}(b_i) = \sum_{s=1}^{n} \sum_{i=0}^{n} \varphi_s(ca_i\varphi_s^{-1}(b_i))$$

$b_i = \varphi_s\varphi_s^{-1}(b_i)$

$$= \sum_{s=1}^{n} \varphi_s\Big(\overbrace{\sum_{i=0}^{n} ca_i\varphi_s^{-1}(b_i)}^{0}\Big) = 0$$

$\Rightarrow \sum_{i=0}^{n} Tr_G(ca_i) b_i = 0 \ \forall c \in K$, tuttavia $Tr_G(ca_i) \in E$

$\Rightarrow \{b_0, \dots, b_n\}$ è lin. ind., quindi:

$$Tr_G(ca_i) \ \forall c \in K, \ \forall i = 1, \dots, n$$

$\Rightarrow Tr_G(c) = Tr_G(ca_i a_i^{-1}) = Tr_G(ca_i) a_i^{-1} = 0 \ \forall c \in K$ ⚡

(Tr_G è non nulla)

q.e.d.

Cambiamo notazione:

$Aut_F(K) = Gal(K/F)$ (GRUPPO DI GALOIS DI K su F)

Proposizione:

Se K è estensione finita di F, si ha:

1) $Gal(K/F)$ è finito

2) $|Gal(K/F)| \mid [K:F]$

Dim.:

1) $\dim(Gal(K/F)) \leq n = [K:F]$. Se fosse $> n$, potrei considerare $\varphi_0, \dots, \varphi_n \in Gal(K/F)$ a due a due distinti e $L = \{b \in K \mid b = \varphi_i(b), i = 0, \dots, n\}$ sarebbe estensione di F, quindi per Dedekind si avrebbe:

$$[K:L] \geq n+1$$

Tuttavia $[K:F] = [K:L] \cdot [L:F]$ ⚡

$\Rightarrow$ sia $E = Fix_K(Gal(K/F))$, per Artin si ha:

$$[K:E] = |Gal(K/F)|$$

$\Rightarrow [K:F] = [K:E] \cdot [E:F]$

q.e.d.

esempi:

1) $d \in \mathbb{Z} \setminus \{0, \pm 1\}$ $\Rightarrow$ nessun quadrato di un primo divide d. Infatti:

$\mathbb{Q}(\sqrt{d})$ ha gruppo di Galois con 2 elementi

$\Rightarrow |Gal(\mathbb{Q}(\sqrt{d})/\mathbb{Q})| = 2$

$\Rightarrow \mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$

$\Rightarrow$ il polinomio minimo di $\sqrt{d}$ è $x^2 - d$ che è irriducibile per Eisenstein

$\Rightarrow$ se $\varphi \in Gal(\mathbb{Q}\sqrt{d}/\mathbb{Q})$, $\varphi(\sqrt{d})^2 = d$

$\Rightarrow \varphi(\sqrt{d}) = \pm\sqrt{d} \Rightarrow \varphi(a + b\sqrt{d}) = a \pm b\sqrt{d}$

$\Rightarrow$ si verifica che $a + b\sqrt{d} \longmapsto a - b\sqrt{d}$ è automorfismo

2) $\sqrt[3]{2} \in \mathbb{R} \Rightarrow$ se $\varphi \in Gal(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$, allora

$\varphi(\sqrt[3]{2})^3 = \varphi(2) = 2 \Rightarrow \varphi = Id$ quindi:

$|Gal(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})| = 1$ (gruppo banale $\{Id\}$

3) $v = \sqrt{7} + \sqrt{3} \Rightarrow v - \sqrt{3} = \sqrt{7} \Rightarrow (v - \sqrt{3})^2 = 7$

$\Rightarrow v^2 - 4 = 2v\sqrt{3} \Rightarrow v^4 - 8v^2 + 16 = 12v^2$

$\Rightarrow v^4 - 20v^2 + 16 = 0$

$\Rightarrow$ mostriamo che $x^4 - 20x^2 + 16$ è irriducibile:

le radici sono $\pm\sqrt{3}, \pm\sqrt{7} \notin \mathbb{Q}$

$\Rightarrow x^4 - 20x^2 + 16$ è irriducibile

4) $v = \sqrt{a} + \sqrt{b}$, $a, b \in \mathbb{Z}$ non quadrati con $a > b > 0$

$\Rightarrow v - \sqrt{b} = \sqrt{a} \Rightarrow \ldots \Rightarrow v^4 - 2v^2(a+b) + (a-b)^2 = 0$

$\Rightarrow$ mostriamo che $x^4 - 2x^2(a+b) + (a-b)^2$ è irriducibile:

$$\frac{1}{v} = \frac{1}{\sqrt{a}+\sqrt{b}} = \frac{\sqrt{a}-\sqrt{b}}{a-b} \in \mathbb{Q}(\sqrt{a}+\sqrt{b})$$

$\Rightarrow \sqrt{a}-\sqrt{b} \in \mathbb{Q}(\sqrt{a}+\sqrt{b}) \Rightarrow \mathbb{Q}(\sqrt{a},\sqrt{b}) = \mathbb{Q}(\sqrt{a}+\sqrt{b})$

$\Rightarrow [\mathbb{Q}(\sqrt{a},\sqrt{b}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{a},\sqrt{b}) : \mathbb{Q}\sqrt{a}] \cdot \underbrace{[\mathbb{Q}\sqrt{a} : \mathbb{Q}]}_{=2}$

$\Rightarrow \sqrt{b} \in \mathbb{Q}(\sqrt{a}) \Rightarrow \sqrt{b} = x + y\sqrt{a}$

$\Rightarrow b = x^2 + ay^2 + 2xy\sqrt{a}$ con $y \neq 0$ (b non è quadrato)

$\Rightarrow x \neq 0$ altrimenti $\frac{b}{a} = y^2 \dots$

$\Rightarrow ab = (ay)^2$ (ab è quadrato)

$\Rightarrow \sqrt{a} = \frac{b - x^2 - ay^2}{2xy} \in \mathbb{Q}$ ↯

$\Rightarrow [\mathbb{Q}(\sqrt{a},\sqrt{b}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{a}+\sqrt{b}) : \mathbb{Q}] = 4$

$\Rightarrow |Gal(\mathbb{Q}(\sqrt{a}+\sqrt{b}))| = 4$

In particolare $Gal(\mathbb{Q}(\sqrt{a}+\sqrt{b}))$ è abeliano.

Teorema:

Sia G sottogruppo finito di $Gal(K/F)$. Allora:

$$Gal(K/Fix_K(G)) = G$$

Dim.:

$E = Fix_K(G)$ è estensione di F, $G \subseteq Gal(K/E)$ è ovvio dalla definizione. Per Artin si ha:

$$[K : E] = |G|$$

Se $\varphi \in Gal(K/E) \setminus G$, si ha:

$$|Gal(K/E)| = n+1 \wedge |G| = n$$

$\Rightarrow L = \{b \in K \mid \varphi_1(b) = \dots = \varphi_n(b) = \varphi(b)\}$ con

$G = \{\varphi_1 = Id, \dots, \varphi_n\}$

$\Rightarrow E \subseteq L \Rightarrow$ per Dedekind $[K:L] \geq n+1 = |G|+1$

tuttavia:

$$[K:E] = [K:L]\cdot[L:E] \quad ⚡$$

q.e.d.

<u>Osservazione</u> (Spazi Vettoriali quoziente):

Sia V sp. vettoriale su un campo F. Se $U \subseteq V$, si ha che U è sottogruppo di $(V,+)$ e V/U è uno spazio vettoriale con $(v+U)+(w+U) = (v+w)+U$ e $\alpha(v+U) = \alpha v + U$. Inoltre:

$$\pi : V \longrightarrow V/U \text{ è lineare e suriettiva con } \operatorname{Ker}\pi = U$$

$\Rightarrow$ se V è finitamente generato, si ha:

$$\dim V = \dim U + \dim V/U$$

$$\Leftrightarrow \dim V/U = \dim V - \dim U$$

Se U è finitamente generato, allora lo è anche V/U

$\Rightarrow$ sia $\{v_1+U, \dots, v_k+U\}$ base di V/U, allora $\{v_1,\dots,v_k\}$ è lin. ind.

$\Rightarrow$ sia $\{u_1,\dots,u_n\}$ base di U

$\Rightarrow$ $\{v_1,\dots,v_k,u_1,\dots,u_n\}$ è base di V

$\Rightarrow$ Si ha:

$$\begin{tikzcd} V \arrow[r, "f"] \arrow[d, "\pi"'] & W \\ V/U \arrow[ur, "\tilde{f}"'] & \end{tikzcd}$$

con $\tilde{f}$ iniettiva t.c. $\operatorname{Im}\tilde{f} = \operatorname{Im} f$