Lema: Sea $F \subseteq E$ una extensión separable de grado finito. Entonces existe $L \supseteq E$ tal que L es Galois sobre F.

Dem:

Por un lema anterior existe $L \supseteq E$ y $g \in F[x]$ tales que L es el campo de descomposición de g sobre F y cada factor monico irreducible de g en $F[x]$ tiene una raiz en E. Cada uno de estos factores irreducibles de g son de la forma $\min_F(\alpha)$ para un $\alpha \in E$. Por hipotesis, estos polinomios son separables Por lo tanto g es separable y así $L \supseteq F$ es de Galois..

Teorema: Sea $F \subseteq E$ una extensión separable de grado finito. Entonces $E = F[\alpha]$ para algún $\alpha \in E$.

Dem:

Usando el lema anterior tomamos una extension $L \supseteq E$ tal que $L \supseteq F$ es de Galois. Entonces el conjunto de campos intermedios entre L y F esta en biyeccion con cierto subconjunto de subgrupos de $Gal(L/F)$. Como $L \supseteq F$ es finita, $Gal(L/F)$ tiene orden finito y por lo tanto

tiene un numero finito de subgrupos.
Esto implica que solo hay un numero
finito de campos intermedios entre $L \supseteq F$
En particular solo hay un numero finito de
campos intermedios entre $E \supseteq F$. Por un
resultado anterior la extchsion $E \supseteq F$
es simple, ie, $E = F[\alpha]$ p.q. $\alpha \in E$.

Cor. Sea $F \subseteq E$ una extensión de grado finito. Entonces $|Gal(E/F)| \mid [E:F]$.
Más aún, $|Gal(E/F)| = [E:F]$ si y solo si $F \subseteq E$ es de Galois.

Dem:

Sup que $F \subseteq E$ es de Galois. En particular $F \subseteq E$ es separable. Por el lema anterior existe $\alpha \in E$ tal que $E = F[\alpha]$.
Sea $f = \min_F(\alpha)$. Así $[E:F] = [F[\alpha]:F] = gr(f)$
Sea Λ la orbita de α bajo $G = Gal(E/F)$
Entonces $|\Lambda| = gr(f)$. Además por ser $E \supseteq F$ de Galois, G actua transitivamente

en el conjunto de raices de f, en este caso en el conjunto Λ. Por el teorema Orbita-estabilizador $|\Lambda| = [G : G_\alpha]$ donde G_α es el estabilizador de α. Como $E = F[\alpha]$ entonces $E \subseteq Fix(G_\alpha)$. Entonces $G_\alpha = \{e\}$. Por lo tanto $|\Lambda| = |G|$

$\therefore$ $gr(f) = [E : F] = |\Lambda| = |G|$

Consideremos una extension de grado finito $F \subseteq E$ con $G = Gal(E/F)$ y $K = Fix(G)$.

Entonces la extension $K \subseteq E$ es de Galois. ya que $F \subseteq K \subseteq E$

$$G = Gal(E/F) \supseteq Gal(E/K) = Gal(E/Fix(G)) = G$$

Por lo anterior $|E:K| = |Gal(E/K)| = |G|$

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

$$\therefore |G| \mid [E:F]$$

Notemos que $|G| = [E:F] \iff K = F$

$\iff F = \mathrm{Fix}(G) \iff E \supseteq F$ es de Galois.

Teorema. Sea $G \subseteq Aut(E)$, donde E es un campo y $F = Fix(G)$. Si G es finito, entonces:

i) $|G| = [E:F]$.

ii) $G = Gal(E/F)$, y

iii) $E \supseteq F$ es de Galois.

Dem:

Sea $\alpha \in E$ y sea Λ la orbita de α bajo G. Como G es un grupo finito, $|\Lambda| < \infty$. Por un lema anterior α es separable y algebraico sobre F.

Ademas $[F[\alpha]:F] = gr(min_F(\alpha)) = |\Lambda| \leq |G|$

Como el grado $[F[\alpha]:F]$ está acotado para toda $\alpha \in E$, podemos escoger $\alpha \in E$ tal que $[F[\alpha]:F]$ es maximo. Afirmamos que $F[\alpha] = E$

Sup. que $F[\alpha] < E$. Entonces existe $\beta \in E$ pero $\beta \notin F[\alpha]$, así $F[\alpha] < F[\alpha, \beta] \subseteq E$

Como cada elemento de $F[\alpha, \beta]$ es separable, entonces existe $\gamma \in F[\alpha, \beta]$ tal que $F[\alpha, \beta] = F[\gamma]$. Esto implica que $[F[\alpha]:F] < [F[\gamma]:F]$ ↯

Esto contradice la eleccion de α

Por lo tanto $F[\alpha] = E$ y así $[E:F] \leq |G|$

Tenemos que $G \subseteq Gal(E/F)$ y por el corolario anterior $|Gal(E/F)| \leq [E:F]$ y la igualdad se da si y solo si $F \subseteq E$ es de Galois.

Tenemos

$|G| \leq |Gal(E/F)| \leq [E:F] \leq |G|$. Por lo tanto

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

Por lo tanto se cumplen i), ii) y iii).

Sea $F \subseteq E$ una extensión finita con $G = Gal(E/F)$. Entonces G es un grupo finito. Sea H un subgrupo de G. Si aplicamos el teorema anterior al grupo H, tenemos que $H = Gal\left(E/Fix(H)\right)$. Por lo tanto todo subgrupo de G está en G_0, i.e., $G = G_0$.