Lem 1.5(B) $K \subseteq F$, $H < J < \mathrm{Aut}_K F$.
If $[J:H] < \infty$, then $[H';J'] \le [J:H]$.

Rmk: Pf quite difficult.
Illustrate the result (not pf) by an ex.

char $=0$, $[F:K] < \infty$, $H = 1$, $J = \mathrm{Aut}_K F \Rightarrow H' = F$.

want: $[F : F^{\mathrm{Aut}_K F}] \le \#|\mathrm{Aut}_K F|$

Let $F = K(u)$, $f(T) = \mathrm{Irr}(u, K)$.

$\Rightarrow \#|\mathrm{Aut}_K F| = \#\{\text{roots of } f(T) \text{ in } F\}$

suppose $f(T) = \prod_{i=1}^{d} (T - u_i) \in \bar{K}[T]$, with $u_1, \dots, u_d \in F$.

$\Rightarrow \#|\mathrm{Aut}_K F| = d$.

Since $F^{\mathrm{Aut}_K F} \supseteq K$, $\Rightarrow F = F^{\mathrm{Aut}_K F}(u)$.

Claim: $\mathrm{Irr}(u, F^{\mathrm{Aut}_K F}) \mid \prod_{i=1}^{d} (T - u_i)$ (note $F^{\mathrm{Aut}_K F} = K''$)

Pf: It suffices if $\prod_{i=1}^{d} (T - u_i) \in F^{\mathrm{Aut}_K F}[T]$.

$\Leftarrow \mathrm{Aut}_K F$ permutes u_i. □

Thus, $[F : F^{\mathrm{Aut}_K F}] = \deg \mathrm{Irr}(u, F^{\mathrm{Aut}_K F}) \le d$. □

Pf of Lem 1.5(B): Let $[J:H] = n$, suppose $[H':J'] \ge n+1$.

Pick $u_1, \dots, u_{n+1} \in H'$, which are lin. indep over J'.

Let $J = \coprod_{1 \le i \le n} \tau_i H$, with $\tau_i \in J$.

Consider system of eqn:

$$(*) \begin{cases} \tau_1(u_1) T_1 + \tau_1(u_2) T_2 + \cdots + \tau_1(u_{n+1}) T_{n+1} = 0 \\ \vdots \\ \tau_n(u_1) T_1 + \cdots + \tau_n(u_{n+1}) T_{n+1} = 0 \end{cases}$$

This is $(n+1)$-eqns with n variables

$\Rightarrow \exists$ nonzero solutions (in F)

No.

Date

choose a nonzero solution with minimum nonzero elts.
WLOG, $T_1 = a_1, \cdots T_r = a_r$, $a_i \neq 0$, $T_{r+1} = \cdots = T_{n+1} = 0$
WLOG, can make $a_1 = 1$.

Since $J = \coprod \tau_i H \Rightarrow$ only one $\tau_i \in H$. WLOG, $\tau_1 \in H$
(1) of $\circledast \Rightarrow \sum_{i=1}^{r} u_i a_i = 0$, with $u_i \in H'$, $a_i \in H'$

u_i are indep over $J' \Rightarrow \exists a_i$, $a_i \notin J'$.
$a_1 = 1 \in J'$. WLOG, $a_2 \notin J'$. $\Rightarrow \exists \sigma \in J$, $\sigma(a_2) \neq a_2$.

Apply σ to $\circledast$. get $\sigma(\circledast) = \begin{cases} \sigma\tau_1(u_1) T_1 + \cdots + \sigma\tau_1(u_{n+1}) T_{n+1} = 0 \\ \vdots \\ \sigma\tau_n(u_1) T_1 + \cdots + \sigma\tau_n(u_{n+1}) T_{n+1} = 0 \end{cases}$
$\Rightarrow T_1 = \sigma(a_1) = 1, \cdots T_r = \sigma(a_r), T_{r+1} = \cdots = T_{n+1} = 0$ is a solution

However, $J = \coprod \tau_i H = \coprod \sigma\tau_i \cdot H$
indeed, if $\tau_i H = \sigma\tau_j \cdot H$, then
(i) of $\circledast$ = (j) of $\sigma(\circledast)$. (since H fixes u_i).
$\Rightarrow \circledast$ and $\sigma(\circledast)$ are the SAME sys of eqns
i.e. $T_1 = \sigma(a_1) = 1, \cdots, T_r = \sigma(a_r), T_{r+1} = \cdots = T_{n+1} = 0$ is solution of $\circledast$

$\Rightarrow \sigma(a_1) - a_1 = 0, \sigma(a_2) - a_2 \neq 0, \cdots \sigma(a_r) - a_r, 0 \cdots 0$
is also a nonzero solution of $\circledast$,
contradicting minimality of r. $\square$

Defn: (1) $K \subseteq E \subseteq F$, Say E is closed if $E'' = E$.
(2) $H < \mathrm{Aut}_K F$, Say H is closed if $H'' = H$.

Lem 1.6 $K \subseteq F$. Then $\exists$ bijection:

$$\{\text{closed interm. fields}\} \longrightarrow \{\text{closed subgps } < \mathrm{Aut}_K F\}$$
$$E \longmapsto E'$$

Pf: inj: $E_1' = E_2' \Rightarrow E_1'' = E_2'' \Rightarrow E_1 = E_2$.
surj: given $H < \mathrm{Aut}_K F$, $(H')' = H$. □.

Lem 1.7 $K \subseteq L \subseteq M \subseteq F$. $1 < H < J < \mathrm{Aut}_K F$.

(1) If L closed and $[M:L] < \infty$, then M is closed, and $[L':M'] = [M:L]$
(2) If H closed and $[J:H] < \infty$, then J is closed, and $[H':J'] = [J:H]$.
(3) If $[F:K) < \infty$, and F/K is Galois, then all interm. fields are closed, and all subgps of $\mathrm{Aut}_K F$ are closed.

Rmk ① Since $1 < \mathrm{Aut}_K F$ is closed, (2) $\Rightarrow$ any finite J is closed
② In situation of (3), $|\mathrm{Aut}_K F| = [F:K]$

Pf: (2): $[J:H] \leq [J'':H]$, since $J < J''$.
$= [J'':H'']$, H closed
$\leq [H':J']$ Lem 1.5 (A) for $M = H'$, $L = J'$
$\leq [J:H]$, Lem 1.5 (B)
$\Rightarrow$ equality holds everywhere.
(Careful. $[J'':H''] \leq [H':J']$. But also $[J'':H''] \geq [H''':J'''] = [H':J']$
so they are equal).
(1): Similar to (2)
(3): F/K Gal $\Rightarrow K$ is closed, (1) $\Rightarrow$ all interm. fields are closed.
Rmk ① $\Rightarrow$ all subgps are closed, □

No.

Date

Pf of Main Thm. (fund thm of Galois thy). Part 1:

Indeed, Lem 1.7 above $\Rightarrow$ Thm. 1.3 (1).

also $\Rightarrow$ $K \subseteq E \subseteq F$, then F/E Gal.

since E closed $\Rightarrow E'' = E \Rightarrow F/E$ Gal. $\square$

So it remains to show: E/K Gal $\Leftrightarrow E' < \mathrm{Aut}_K F$ is normal.

Defn. $K \subseteq E \subseteq F$. Say E is stable (relative to F/K), if
$\forall \sigma \in \mathrm{Aut}_K F$, $\sigma(E) \subseteq E$.

Note, $\sigma^{-1} \in \mathrm{Aut}_K F \Rightarrow \sigma^{-1}(E) \subseteq E \Rightarrow \sigma|_E \in \mathrm{Aut}_K E$.

Lem 1.8: $K \subseteq F$.
(1) $K \subseteq E \subseteq F$, E stable. Then $E' = \mathrm{Aut}_E F < \mathrm{Aut}_K F$ is normal.
(2) If $H < \mathrm{Aut}_K F$ normal, then H' is stable.

Pf: (1) Let $\tau \in \mathrm{Aut}_E F$, $\sigma \in \mathrm{Aut}_K F$ WANT: $\sigma^{-1}\tau\sigma \in \mathrm{Aut}_E F$,
i.e. fixes E.

Let $u \in E$. E stable $\Rightarrow \sigma(u) \in E$
τ fixes E $\Rightarrow \tau(\sigma(u)) = \sigma(u)$
$\Rightarrow \sigma^{-1}\tau\sigma(u) = u$.

(2) Let $\sigma \in \mathrm{Aut}_K F$, $u \in H' \Leftrightarrow \forall \tau \in H$, $\tau(u) = u$.
WANT $\sigma(u) \in H' \Leftrightarrow \forall \tau \in H$, $\tau(\sigma(u)) = \sigma(u)$
$\Leftrightarrow \sigma^{-1}\tau\sigma(u) = u$
But $H \lhd \mathrm{Aut}_K F \Rightarrow \sigma^{-1}\tau\sigma \in H$. $\square$

Lem 1.9 $K \subseteq E \subseteq F$, F/K Gal and E stable. Then E/K is Gal.

Pf: Recall E/K Gal $\Leftrightarrow \forall\, u \in E-K$, $\exists\ \sigma \in \mathrm{Aut}_K E$, s.t. $\sigma(u) \neq u$.

Since F/K Gal $\Rightarrow \exists\ \tilde{\sigma} \in \mathrm{Aut}_K F$, s.t. $\tilde{\sigma}(u) \neq u$.

So can take $\sigma = \tilde{\sigma}|_E \in \mathrm{Aut}_K E$ since E stable.

□

Lem 1.10 $K \subseteq E \subseteq F$, E/K alg and Gal. Then E is stable.

Pf: Let $u \in E$, WANT: $\sigma \in \mathrm{Aut}_K F$, $\sigma(u) \in E$

Let $\mathrm{Irr}(u, K) = f(T) = \prod_{i=1}^{n} (T - u_i)$, $u_1 = u$.

WLOG, suppose $u_1, \cdots, u_r$ are all the distinct roots in E

(note, a priori, u_i could be same, and not in E)

Let $g(T) = \prod_{i=1}^{r} (T - u_i)$

However, $\mathrm{Aut}_K E$ permutes these u_i, $\Rightarrow \mathrm{Aut}_K E$ fixes $g(T)$

$\Rightarrow$ coeff of $g(T)$, which $\in E$, are in $E^{\mathrm{Aut}_K E} = K$ (since K/E Gal)

$\Rightarrow g(T) \in K[T]$.

Since $g(T) \mid f(T)$, and $g(u) = 0 \Rightarrow g(T) = f(T)$

$\Rightarrow u_1 \cdots, u_n$ are distinct, all in E.

Now, for $\sigma \in \mathrm{Aut}_K F$, $\sigma(u)$ is a root of $f(T)$

$\Rightarrow \sigma(u) \in \{u_1 \cdots, u_n\} \subseteq E$.

□

No.

Date

Defn $K \subseteq E \subseteq F$. $\tau \in \mathrm{Aut}_K E$ is called *extendible* to F if $\exists\, \sigma \in \mathrm{Aut}_K F$, s.t. $\sigma|_E = \tau$.

Lem 1.11 $K \subseteq E \subseteq F$, E stable. ($\Rightarrow \mathrm{Aut}_E F \lhd \mathrm{Aut}_K F$).
Then $\mathrm{Aut}_K F / \mathrm{Aut}_E F$ is isom. to the gp of K-automorphisms of E that are extendible to F.

Pf. The map $\mathrm{Aut}_K F \longrightarrow \mathrm{Aut}_K E$, $\sigma \mapsto \sigma|_E$ is gp hom,
$\ker = \mathrm{Aut}_E F$, and Im = extendible elts. □

Finally. Pf of Main Thm. **Part 2**
Recall: WANT to show, $K \subseteq E \subseteq F$, F/K Gal, $[F:K] < \infty$.
Then E/K Gal $\Leftrightarrow \mathrm{Aut}_E F \lhd \mathrm{Aut}_K F$.
And if so, then $\mathrm{Aut}_K E \simeq \mathrm{Aut}_K F / \mathrm{Aut}_E F$.

Pf "$\Rightarrow$": E/K Gal $\Rightarrow$ E stable, by Lem 1.10
$\Rightarrow E/K$ Gal, by Lem 1.9

"$\Leftarrow$": $E = \mathrm{Aut}_E F$ normal $\Rightarrow$ E'' stable, by Lem 1.8 (2)
but all interm. ext are closed $\Rightarrow E = E''$ stable
$\Rightarrow E/K$ Gal, by Lem 1.9.

If E/K Gal, Lem 1.11 $\Rightarrow \mathrm{Aut}_K F / \mathrm{Aut}_E F \hookrightarrow \mathrm{Aut}_K E$.
But $\#(\mathrm{LHS}) = [F:K]/[F:E] = [E:K] = \#(\mathrm{RHS})$
$\Rightarrow$ it is an isomorphism. □