24.4.24

The first cor. of Thm 3.8 is that $[L:K]$ is an upper bound for $\mathrm{Gal}(L:K)$ for <u>any</u> finite extension.

Cor 3.9 Let $L:K$ be a finite extension $G = \mathrm{Gal}(L:K) = \gamma(K)$ then

$$|\mathrm{Gal}(L:K)| \leq [L:K] \quad \text{with}$$

equality if and only if $K = \phi(G) = \mathrm{Fix}\, G = L^{\mathrm{Gal}(L:K)}$.

i.e. $[L:K]$ is Galois $\iff$ $K = \phi\gamma(K)$

$$\Updownarrow$$

$$|\mathrm{Gal}(L:K)| = [L:K]$$

Proof Let $L_0 = \mathrm{Fix}(G)$, so that

$$K \subseteq L_0 \subseteq L$$

By Thm 3.8 $[L:L_0] = |\mathrm{Gal}(L:K)|$

Hence
$$\begin{aligned}[L:K] &= [L:L_0][L_0:K] \\ &= |\mathrm{Gal}(L:K)|\,[L_0:K]\end{aligned}$$

which proves $|\mathrm{Gal}(L:K)| \leq [L:K]$

and $[L:K] = |\mathrm{Gal}(L:K)| \iff L_0 = K \iff \mathrm{Fix}\, G = K$
$$\iff \phi(\gamma(K)) = K. \quad \square$$

Cor 3.10 Let G be a finite s/gp of $Aut(L)$ and $K = Fix\, G$. Then every automorphism of L fixing K is contained in G.

Ie $Gal(L:K) = G$ so that $L:K$ is Galois with Galois group G.

Proof. By definition, K is fixed by all elements of G. So
$$G \subseteq Gal(L:K) \quad \text{and} \quad |G| \leq |Gal(L:K)|$$

The question is whether there are any autom of L fixing K not in G.
By Thm 3.8 we have
$$|G| = [L:L^G] = [L:K]$$

By Cor 3.9 $\quad |Gal(L:K)| \leq [L:K]$

This gives $\quad [L:K] \underset{\text{thm } 3.8}{=} |G| \leq |Gal(L:K)| \underset{\text{Cor } 3.9}{\leq} [L:K]$

Hence we have equalities throughout

$\blacksquare$

Cor 3.11 If $G_1 \neq G_2$ are 2 distinct finite subgroups of $Aut(L)$ then their fixed fields are also distinct.

Proof Suppose $F_1 = \text{Fix}\, G_1$, $F_2 = \text{Fix}\, G_2$
Suppose $F_1 = F_2$ then by definition F_1 is fixed by G_2. By Cor 3.10 any autom fixing F_1 is contained in G_1
Hence $G_2 \leq G_1$. Similarly $G_1 \leq G_2$ and $G_1 = G_2$ $\blacksquare$

Cor 3.12 Let $G = \text{Gal}(L:K)$, $[L:K] < \infty$ and H a subgroup of G. Then

$$[L^H : K] = [\phi(H) : K] = [L:K]/|H|$$

Proof By Thm 3.8, applied to H we have

$$[L : L^H] = [L : \phi(H)] = |H|$$

On the other hand $[L : \phi(H)][\phi(H) : K] = [L:K]$

Hence $[\phi(H) : K] = \dfrac{[L:K]}{[L:\phi(H)]} = \dfrac{[L:K]}{|H|}$ as wanted $\blacksquare$

Rmk

$$\begin{tikzcd} L \arrow[d, dash] & 1 \arrow[d, dash] \\ \phi(H) \arrow[d, equal] & H \arrow[l, "\phi"'] \arrow[d, dash] \\ K' \arrow[r, "\gamma"'] & \text{Gal}(L'/K) \end{tikzcd}$$

Cor 3.12 can also be written as $|H| = \dfrac{(L:K]}{[\phi(H):K]}$

Note: $|H| \neq [\phi(H):K]$!!!

We've defined $L:K$ to be Galois if

$$[L:K] = |\mathrm{Gal}(L:K)|$$

and have seen that this is equivalent to (Cor 3.9)

$$\phi(\gamma(K)) = K.$$

Our next goal is to develop another criteria for a finite extension to be Galois which does not require explicitly counting autom of L over K

§4 Galois $\Leftrightarrow$ normal and separable.

Recall : ① $K \subset L$ normal if every irred poly $f \in K[x]$ which has a zero in L splits in L.

② $K \subset L$ an alg extension is separable if every $\alpha \in L$ is sep over K
ie $m_{K,\alpha}$ has no multiple root

③ $L:K$ normal, finite $\Leftrightarrow$ L is a splitting field for some poly f over K.

$L:K$ Galois means the group $Gal(L:K)$ is as large as possible
ie $|Gal(L:K)| = [L:K]$.
$\Leftrightarrow$ $\phi\gamma(K) = K$.

We will use normality and separability to construct enough K-autom. of L and show that $L:K$ is Galois iff $L:K$ is normal and separable.

We first show that $L:K$ Galois $\Rightarrow$ $L:K$ normal and separable

Thm 4.1 Let $L:K$ be a finite Galois extension, i.e. $|Gal(L:K)| = [L:K]$ (or equivalently $Fix\, G = L^{Gal(L:K)} = K$)
Then $L:K$ is normal and separable and $L:K$ is splitting field of a separable polynomial

Proof Let $G = Gal(L:K) = \{\sigma_1, \ldots \sigma_n\}$
where $\sigma_1 = id$.
To show $L:K$ is normal
consider an irreducible $f(x) \in K[x]$
with a root $\alpha \in L$. w.t.s f splits in L
Apply each autom in G to α, $\sigma_1(\alpha), \ldots \sigma_n(\alpha)$
Suppose there are r distinct
images $\alpha = \alpha_1 = \sigma_1(\alpha)$
$\alpha_2 = \sigma_2(\alpha), \ldots \alpha_r = \sigma_r(\alpha)$
(after renumbering if necessary of σ_i's).
Now if $\sigma \in G$, then σ maps each
α_i to some α_j. Since σ is an injective
map of the $\{\alpha_1 \ldots \alpha_r\}$ to itself
it is also surjective, ie σ permutes
α_i.
Since σ permutes α_i, σ fixes
symmetric functions on the α_i
ie if $s_1 = \sum_{i=1}^{r} \alpha_i$ $\quad s_2 = \sum_{i<j} \alpha_i \alpha_j$

$$\ldots \quad s_r = \prod_{i=1}^{r} \alpha_i$$

then $\sigma(s_i) = s_i$

Thus $s_i \in \mathrm{Fix}(G) = K$ by the hypothesis that $L:K$ is Galois.

Now we form a monic polynomial whose roots are the α_i:

$$g(x) := (x-\alpha_1) \cdots (x-\alpha_r)$$
$$= x^r - s_1 x^{r-1} + s_2 x^{r-2} + \cdots + (-1)^r s_r$$

Since $s_i \in K$, $g(x) \in K[x]$. Since $\alpha_i = \sigma_i(\alpha) \in L$, g splits over L.

We claim $g = m_{\alpha, K}$. To see this let $h(x) = b_0 + b_1 x + \cdots + b_m x^m$ be any poly in $K[x]$ which has α as a root, $h(\alpha) = 0$

Applying σ_i to $b_0 + b_1\alpha + \cdots + b_m \alpha^m$ gives that $\sigma_i(\alpha) = \alpha_i$ is also a root of h

Hence $g \mid h$ and therefore $g = \min_{\alpha, K}$

But our original polynomial $f \in K[x]$ is irreducible and has α as a root. So f must be a constant multiple of g. Consequently f splits over L proving $L:K$ is normal.

Since the α_i's, $i = 1, \ldots, r$ are distinct f is separable. Thus α is separable over K which shows that the extension $L:K$ is separable

Since $L:K$ is normal and separable and finite write $L = K(\alpha_1 \ldots \alpha_n)$ and let $p_i(x)$ be the min poly of α_i over K.
Since $L:K$ is normal and $\alpha_i \in L$ is a root of p_i, L has all roots of p_i.
Since $L:K$ is separable p_i is a sep. poly
Therefore L is splitting field over K of the product of the $p_i(x)$'s and that product is separable

$\blacksquare$

<u>Remark</u> Note in Thm 4-1 we showed that

$$L:K \text{ Galois} \overset{\text{Cor 3.9}}{\Longleftrightarrow} L^{Gal(L:K)} = K \overset{\text{Cor 3.9}}{\Longleftrightarrow} [L:K] = |Gal(L:K)|$$

$\overset{\text{Thm 4-1}}{\Longrightarrow}$ $L:K$ separable and normal

$\overset{\text{Thm 4-1}}{\Longrightarrow}$ $L:K$ is splitting field of a separable polynomial

This last statement in return implies

$$|Gal(L:K)| = [L:K] \quad \text{ie } L:K \text{ is Galois}$$

using Thm 3.5. In fact we have as a cor of Thm 4-1 and Thm 3.5

$\boxed{\text{Thm 4.2 Let } L:K \text{ be a finite extension. Then } L:K \text{ Galois} \Longleftrightarrow L:K \text{ normal separable.}}$

Recall we've seen that

① $K \subseteq M \subseteq L$ and $L:K$ is separable then $[M:K]$ is separable and $[L:M]$ is separable. (Lemma 2.25)

② If $K \subseteq M \subseteq L$, $[L:K] < \infty$ if $L:K$ is normal then $L:M$ is normal. (Follows easily from $[L:K] < \infty$, normal $\Leftrightarrow$ L is a splitting field

Using these and thm 4.2 we have

Thm 4.3 If $L:K$ is a Galois extension and $K \subseteq M \subseteq L$ then $L:M$ is a Galois extension.

Pf Using characterization of Galois extension as separable normal extension we have that separability and normality are both preserved in the passage from $L:K$ to $L:M$ since the minimal poly over M of each elt of L divides the min. poly over K. But $M:K$ need not be Galois

Rmk. ①

$$\begin{array}{ll} L & \\ | & \text{Galois} \\ M & \\ | & \text{need not be Galois} \\ K & \end{array} \quad \text{Galois } (L:K)$$

$$\begin{array}{ll} \mathbb{Q}(\sqrt[4]{2}, i) & \text{— splitting field of } x^4-2 \text{ hence Galois over } \mathbb{Q} \\ |\, 2 & \\ \mathbb{Q}(\sqrt[4]{2}) & \\ |\, 4 & \\ \mathbb{Q} & \end{array}$$

not normal has 1 root but not others

if $L:M$, $M:K$ are Galois
This does not imply that $L:K$ is Galois

$L \quad \mathbb{Q}(\sqrt[4]{2})$

$\quad\; 2 \,|$ — splitting field of $x^2 - \sqrt{2} \in \mathbb{Q}(\sqrt{2})[x]$ hence Galois

$M \quad \mathbb{Q}(\sqrt{2})$

$\quad\; 2 \,|$ — splitting field of $x^2 - 2 \in \mathbb{Q}[x]$. hence Galois

$K \quad \mathbb{Q}$.

$L:K$ not Galois!

—o—

For the Galois correspondence and its proof it is helpful to look at separability and normality in terms of K-monomorphism of a field M into L. which is a generalization of K-atoms of a field L.

Defn Suppose K is a subfield of the fields M and L. Then a K-monomorphism of M into L is a map $\phi: M \to L$ which is a field monom s.t. $\phi(k) = k \quad \forall k \in K$.

<u>Example</u> $K = \mathbb{Q}$, $M = \mathbb{Q}(\sqrt[3]{2})$, $L = \mathbb{C}$
$\alpha = \sqrt[3]{2}$, $\alpha^3 = 2$

We can define
$$\phi : M \to L$$
$$\alpha \mapsto \alpha\rho \qquad \rho = e^{2\pi i/3}$$
$$k \to k.$$
$$a + b\alpha + c\alpha^2 \mapsto a + b\alpha\rho + c\alpha^2\rho^2$$
Then ϕ is a K-monom of M into L.

if $K \subseteq M \subseteq L$ then any K-autom of L restricts to a K-monom of $M \mapsto L$

We are interested in reversing this process if possible. Ie given a K monom $M \to L$ when can be extend it a K autom of L.

Next thm says this is possible if $L:K$ finite and normal

<u>Thm 4.4</u> Suppose $L:K$ is finite normal extension $K \subseteq M \subseteq L$. Let ϕ be any K-monom $M \to L$. Then $\exists$ a K autom $\sigma : L \to L$ s.t $\sigma|_M = \phi$

<u>Proof</u>. Since $L:K$ finite normal, L is a splitting field of some polynomial f over K. Hence it is a splitting field of f over M and over $\phi(M) \subset L$ for $\phi(f) = f$

Recall Thm 2.19: If $\phi : K \to \tilde{K}$ is an isom of fields $f(x) \in K[x]$ and if L is a splitting field of $f(x)$ over K and $\tilde{L}$ is a splitting field of $\phi(f)$ over $\tilde{K}$. Then ϕ extends to an isom $\sigma : L \to \tilde{L}$

Applying Thm 2.19 to the isom $\phi : M \to \phi(M)$

we get $\exists$ $\sigma : L \to L$ s.t $\sigma|_M = \phi$

Since $\sigma|_K = \phi|_K$ is identity on K
σ is a K-autom of L ☒

As a corollary we get

Prop 4.5 Suppose $L:K$ normal finite extension α, β are zeroes in L of an irred poly $f \in K[x]$
Then $\exists$ a K-autom $\sigma : L \to L$ s.t
$\sigma(\alpha) = \beta$.

Proof. We've seen that there is an isom
$\phi : K(\alpha) \to K(\beta)$ s.t $\phi(k) = k$, $\phi(\alpha) = \beta$
By thm 4.4 this extends to an
K-aut σ of L. ☒

Rmk Normality guarantees that you can always find an autom σ of L that will send any root $\alpha \in L$ of an irred poly to another root $\beta \in L$.