(2) let α be a real cube root of 2

ie $\alpha^3 = 2$, and $\alpha \in \mathbb{R}$.

Then $\mathbb{Q}(\alpha) : \mathbb{Q}$ is a degree 3 extention

if $\sigma \in Gal(\mathbb{Q}(\alpha) : \mathbb{Q})$, $\sigma : \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha)$

then $(\sigma(\alpha))^3 = \sigma(\alpha^3) = \sigma(2) = 2$

Hence $\sigma(\alpha)$ is also a root of $x^3 - 2$

Since $\sigma(\alpha) \in \mathbb{Q}(\alpha) \subset \mathbb{R}$, $\sigma(\alpha) = \alpha$

Since σ fixes $\mathbb{Q}$ pointwise, σ fixes every elt $\mathbb{Q}(\alpha)$

Hence $Gal(\mathbb{Q}(\alpha) : \mathbb{Q}) = \{id\}$.

In these simple examples we really used the following general Lemma

Lemma 3-2: let $f \in K[x]$, L a splitting field of f over K. Let $R(f) \subset L$ be the roots of f. Then $Gal(L : K)$ permutes the roots of f

Pf: let $f(x) = a_n x^n + \dots + a_0 \in K[x]$, $\alpha \in R(f)$ and $\sigma \in Gal(L:K)$

Then $0 = \sigma(f(\alpha)) = \sigma(a_n \alpha^n + \dots + a_0)$

$= a_n \sigma(\alpha)^n + \dots + a_0$

Since σ fixes K pointwise, $\sigma(a_i) = a_i$)

Which implies $\sigma(\alpha) \in R(f)$
and $\sigma(R(f)) \subset R(f)$

Since σ is injective and $R(f)$ is finite we have that $\sigma(R(f)) = R(f)$

何.

Lemma 3.2' Let L be a splitting field of $f \in K[x]$. Then the restriction map defined by

$$Gal(L:K) \longrightarrow S_{R(f)}$$

$$\sigma \longmapsto \sigma|_{R(f)}$$ is an injective

group homomorphism. In particular $Gal(L:K)$ is isomorphic to a subgroup of $S_{R(f)}$

Proof If $\sigma, \eta \in Gal(L:K)$ then

$$(\sigma \circ \eta)|_{R(f)} = \sigma|_{R(f)} \circ \eta|_{R(f)}$$ hence the restriction map is a hom.

Let $R(f) = \{\alpha_1, \dots, \alpha_n\} \subset L = K(\alpha_1, \dots, \alpha_n)$

$$L = \left\{ \frac{p(\alpha_1, \dots, \alpha_n)}{q(\alpha_1, \dots, \alpha_n)} \;\middle|\; \begin{array}{l} p, q \in K[x_1, \dots, x_n] \\ q(\alpha_1, \dots, \alpha_n) \neq 0 \end{array} \right\}.$$

$$\sigma\left(\frac{p(\alpha_1, \dots, \alpha_n)}{q(\alpha_1, \dots, \alpha_n)}\right) = \frac{p(\sigma(\alpha_1), \dots, \sigma(\alpha_n))}{q(\sigma(\alpha_1), \dots, \sigma(\alpha_n))}$$

If $\sigma|_{R(f)} = \mathrm{Id}$ then $\sigma(\alpha_i) = \alpha_i$ $1 \leq i \leq n$

since $\sigma(k) = k$ as well we have that

$$\sigma(\ell) = \ell \quad \forall\, \ell \in L = K(\alpha_1, \ldots \alpha_n)$$

Hence σ is identity on L, which in return proves injectivity

☒

Example Recall the insep. poly

$$f(x) = x^p - t \in \mathbb{F}_p(t)[x]$$ which is irreducible and has 1 root α, which has multiplicity p, $(x-\alpha)^p = x^p - \alpha^p = x^p - t$

Thus $\mathcal{R}(f) = \{\alpha\}$

In particular the Galois gp of $x^p - t$ is the trivial group, since the restriction map $\mathrm{Gal}(L:K) \longrightarrow S_{\mathcal{R}(f)}$ is injective

and in this case $|\mathcal{R}(f)| = 1$.

Rmk Suppose $K \subset L$, $c \in L$ is a zero of $f(x) \in K[x]$. Then $\sigma(c)$ is a zero of f for any $\sigma \in \mathrm{Gal}(L:K)$

In particular if $m = \min_{c,K}$ then m is also the min poly of $\sigma(c)$ over K as $\mathrm{Gal}(L:K)$ permutes the roots of the irred poly. The roots of $m_{c,K}$ are called K-conjugates of c

$\sigma(c)$ is a conjugate of c

Example ① $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, $K = \mathbb{Q}$.

If $\sigma \in Gal(L:K)$ then

$\sigma(1) = 1$

$\sigma(\sqrt{2}) = \pm\sqrt{2}$

$\sigma(\sqrt{3}) = \pm\sqrt{3}$.

$\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is a basis of L over $\mathbb{Q}$.
So there are 4 possibilites for $Gal(L:\mathbb{Q})$

$id : a+b\sqrt{2}+c\sqrt{3}+d\sqrt{3} \longrightarrow a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$

$\sigma_1 :$ " " $\longmapsto a+b\sqrt{2}-c\sqrt{3}-d\sqrt{6}$

$\sigma_2 :$ " " $\longmapsto a-b\sqrt{2}+c\sqrt{3}-d\sqrt{6}$

σ_3 " $\longmapsto a-b\sqrt{2}-c\sqrt{3}+d\sqrt{6}$

$id : \sqrt{2} \to \sqrt{2}$, $\sqrt{3} \to \sqrt{3}$ $\sigma_1 : \sqrt{2} \to \sqrt{2}$, $\sqrt{3} \to -\sqrt{3}$ $\sigma_2 : \sqrt{2} \to -\sqrt{2}$, $\sqrt{3} \to \sqrt{3}$

$\sigma_3 : \sqrt{2} \to -\sqrt{2}$, $\sqrt{3} \to -\sqrt{3}$. Note $\sigma_1^2 = \sigma_2^2 = \sigma_3^2 = id$.

$Gal(L:\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ In this case

$$|Gal(L:\mathbb{Q})| = [L:\mathbb{Q}] = 4$$

② For $L = \mathbb{Q}(\sqrt[3]{2})$ over $\mathbb{Q}$.
$|Gal(L:\mathbb{Q})| = 1$ where as $[L:\mathbb{Q}] = 3$.

Rmk Lemma 3.2 and remark on page 143 says that for $\alpha \in L$, $Gal(L:K)$ permutes the roots of $m_{\alpha,K}$, ie any $\sigma \in Gal(L:K)$ permutes the K-conjugates of α in L.

In the previous example $\sqrt{2}$ has minimal poly $x^2-2 \in \mathbb{Q}[x]$, with both roots $\pm\sqrt{2} \in L = \mathbb{Q}(\sqrt{2},\sqrt{3})$. A K-autom σ can send $\sqrt{2}$ to $\pm\sqrt{2}$, but it cannot send $\sqrt{2}$ to $\sqrt{3}$. And we had both options available for $\sqrt{2}$ ie there are autom $\sigma \in Gal(L:K)$ that send $\sqrt{2}$ to $\sqrt{2}$ and also autom that send $\sqrt{2}$ to $-\sqrt{3}$.

It is not always guaranteed that all options are available.

Ex Let $K=\mathbb{Q}$, $L=\mathbb{Q}(\sqrt[4]{2})$
Then $(\sqrt[4]{2})^2 = \sqrt{2} \in L$. And any $\sigma \in Gal(L:K)$ once again has to send $\sqrt{2}$ to $\sqrt{2}$ or $-\sqrt{2}$.
Similarly σ has to send $\sqrt[4]{2}$ to $\pm\sqrt[4]{2}$ since these are the 2 real roots of x^4-2 in L. (The other roots are complex and not in L). Since $\sqrt{2} = (\sqrt[4]{2})^2$
$\sigma(\sqrt{2}) = (\sigma(\sqrt[4]{2}))^2 = (\pm\sqrt[4]{2})^2 = \sqrt{2}$
Hence in fact any $\sigma \in Gal(L:K)$ sends $\sqrt{2}$ to $\sqrt{2}$ ie $\exists$ no $\mathbb{Q}$-Aut of $\mathbb{Q}(\sqrt[4]{2})$ which sends $\sqrt{2}$ to $-\sqrt{2}$.

Let L be a given field. To each subfield K of L we associated a group, $Gal(L:K)$ which is a subgp of Aut group of L.

$$Gal(L:K) \leq Aut(L)$$

We can also go in the other direction. Namely given a subgroup $H \leq Aut\, L$ we associate to H a subfield of L Namely

<u>Defn</u> Let $H \leq Aut\, L$, the <u>fixed field of H</u> denoted by $Fix(H)$ (or L^H)

$$\boxed{L^H = Fix(H) := \{x \in L \mid \sigma(x) = x \quad \forall \sigma \in H\}}$$

Fix H is a subfield of L since if $\sigma(a) = a$, $\sigma(b) = b$ then

$$\sigma(a \pm b) = \sigma(a) \pm \sigma(b) = a \pm b$$
$$\sigma(ab) = \sigma(a)\sigma(b) = ab$$
$$\sigma(a^{-1}) = \sigma(a)^{-1} = a^{-1}$$

This way we get an extension $L : L^H$

In this way given an extension $L:K$ we get 2 maps between

$$\mathcal{F} = \{\text{subfields } M \text{ of } L \text{ s.t } K \subseteq M\}$$

$$\mathcal{G} = \{\text{subgroups of the Galois gp } Gal(L:K)\}$$

$$\gamma : \mathcal{F} \longrightarrow \mathcal{G}$$
$$M \longmapsto \gamma(M) := Gal(L:M)$$

gamma for Galois groups

$$\phi : \mathcal{G} \longrightarrow \mathcal{F}$$
$$H \longmapsto L^H = Fix(H) = \{\ell \in L \mid \sigma(\ell) = \ell \ \forall \sigma \in H\}$$

phi for fixed field.

We record some of the simple properties of these maps in a Lemma, namely they reverse inclusions.

Lemma 3.3 1) $\gamma(K) = Gal(L:K)$

2) $\gamma(L) = Gal(L:L) = \{id\}$

3) If $M \subseteq N$ then $Gal(L:M) = \gamma(M) \supseteq \gamma(N)$
$= Gal(L:N)$

4) If $H \leq G$ then
$\phi(H) \supseteq \phi(G)$

Pf 1), 2) are definitions of the maps

3) This is true since any hom that fixes N pointwise fixes M pointwise

4) If $c \in \phi(G) = Fix(G)$ then
$\sigma(c) = c \quad \forall \sigma \in G$
Since $H \leq G$ then this is also true for any $\sigma \in H$. Hence $c \in Fix(H) = \phi(H)$

$\boxtimes$

The next thm is also easily proved

Thm 3.4 Suppose $L : K$ is an extension $G = Gal(L:K)$, $H \subseteq G$, $K \subseteq M \subseteq L$
then
① $\gamma\phi(H) \supseteq H$

② $\phi\gamma(M) \supseteq M$

③ $\phi\gamma\phi(H) = \phi(H)$

④ $\gamma\phi\gamma(M) = \gamma(M)$

Proof ① let $\sigma \in H \subset Gal(L:K)$, $l \in \phi(H)$
By defn of $\phi(H)$, $\sigma(l) = l$

That means $\sigma \in Gal(L : \phi(H)] = \gamma(\phi(H))$

(2) If ~~m~~ $m \in M$, $\sigma(m) = m$ for each $\sigma \in \gamma(M)$
$= Gal(L:M)$
so that $m \in \phi\gamma(M) = Fix(\gamma(M))$

(3) If $H_1 \subset H_2$ then $\phi(H_1) \supset \phi(H_2)$ (lemma 3.3 (4))
From part (1) $\gamma\phi(H) \supset H$ it follows

(upon applying ϕ) $\phi\gamma\phi(H) \subset \phi(H)$

On the other hand applying (2) with $\phi(H)$ in place of M gives

$$\phi\gamma\phi(H) \supset \phi(H)$$

(4) If $K_1 \subseteq K_2$ then $\gamma(K_1) \supseteq \gamma(K_2)$

Applying this to (2) : $\phi\gamma(M) \supseteq M$ we get

$$\gamma\phi\gamma(M) \subseteq \gamma(M)$$

Applying (1) with $\gamma(M)$ instead of H

gives $\gamma\phi\gamma(M) \supseteq \gamma(M)$

$\boxtimes$.

Example We hae seen two examples in which the Galois group is trivial.

① If α is a real root of $x^3 - 2 \in \mathbb{Q}[x]$ then

$$\mathrm{Gal}(\mathbb{Q}(\alpha) : \mathbb{Q}) = \{e\} = \gamma(\mathbb{Q})$$

let $L = \mathbb{Q}(\alpha)$, $K = \mathbb{Q}$.

Hence $\phi\gamma(K) = \phi(e) = \mathrm{Fix}\{e\} = L$

Hence $K = \mathbb{Q} \subsetneq \phi\gamma(\mathbb{Q}) = \phi\gamma(K) = L$

$1 = |\mathrm{Gal}(L : K)| < [L : K] = 3$

② If $f(x) = x^p - t \in \mathbb{F}_p(t)[x]$

which is irreducible and has 1 root say α (with multiplicity p)

$$(x-\alpha)^p = x^p - \alpha^p = x^p - t$$

Hence $L = \mathbb{F}_p(t)(\alpha)$ is a splitting field and if $K = \mathbb{F}_p(t)$ then as before

$$\mathrm{Gal}(L : K) = \{e\}$$

In both ① and ②

$\mathrm{Gal}(L:K) = \gamma(K) = \{e\}$ and $\phi\gamma(K) = \phi(e) = \mathrm{Fix}\{e\} = L$

Hence $K \subsetneq \phi\gamma(K) = L$

$1 = |\mathrm{Gal}(L:K)| < [L:K] = p$.

On the other hand

3. $\mathbb{C} : \mathbb{R}$ we have, $\mathbb{C}$ = splitting field of x^2+1 over $\mathbb{R}$

$$Gal(\mathbb{C} : \mathbb{R}) = \{id, \tau\} = \mathbb{Z}_2$$

where τ is the complex conjugation map.

In this case $\phi(\gamma(\mathbb{R}))$

$$= \{ z \in \mathbb{C} \mid \begin{matrix} id(z) = z \text{ and} \\ \tau(z) = z \end{matrix} \}$$

$$= \{ z \in \mathbb{C} \mid \bar{z} = z \}$$

$$= \mathbb{R}$$

In this case $2 = |Gal(\mathbb{C} : \mathbb{R})| = [\mathbb{C} : \mathbb{R}]$

Natural question: Under which conditions the maps ϕ, γ are mutual inverses setting up an order reversing bijections between $\mathcal{F}$ = fixed fields and $\mathcal{G}$ = Galois groups?

The 2 examples ① and ② has problems of different sort.

In ① the poly $x^3 - 2$ has 3 roots in a splitting field over $\mathbb{Q}$ but the field $\mathbb{Q}(\sqrt[3]{2})$ is missing the complex roots.

This difficulty can be avoided if we restrict our attention to normal field extensions

In ② The poly $x^p - t$ has only one root in an splitting field over $\mathbb{F}_p(t)$.

No matter how much we enlarge $\mathbb{F}_p(t)$ the root α of $x^p - t$ will be sent to itself by each $\mathbb{F}_p(t)$ - autom since $x^p - t$ has only 1 root, α. with multiplicity.

The difficulty here is inseparability.

In the example ② we have $|\mathrm{Gal}(L:K)| < [L:K]$ where $L = \mathbb{F}_p(t)(\alpha)$

is the splitting field of $x^p - t$ over $\mathbb{F}_p(t)$

And in example ③ we have, $L = \mathbb{C}$, $K = \mathbb{R}$

$|\mathrm{Gal}(L:K)| = [L:K]$, L is splitting field of x^2+1 over $\mathbb{R}$.

In general we have as a consequence of Thm 2.19'

Thm 3.5. If L is a splitting field over K of a polynomial f in $K[x]$, then $|\mathrm{Gal}(L:K)| \le [L:K]$. If f is sep. then $|\mathrm{Gal}(L:K)| = [L:K]$

Pf: Recall Thm 2.19': If $\varphi : K \to \tilde{K}$ is an isom of fields, $f(x) \in K[x]$, L a splitting field of $f(x)$ over K and $\tilde{L}$ a splitting field of φf over $\tilde{K}$.
Then $[L:K] = [\tilde{L}:\tilde{K}]$ and φ extends to an isom $\sigma : L \to \tilde{L}$ and the number of such extentions is at most $[L:K]$

If f is separable than there are $[L:K]$ extentions of φ to an isom $\sigma : L \to \tilde{L}$

Apply Thm 2.19' with $\tilde{K} = K$, $\tilde{L} = L$ and $\varphi =$ identity function on K. The extensions of the identity function on K to isomorphism $L \to L$ are precisely the elements of $\mathrm{Gal}(L:K)$.

$\boxtimes$

Example Recall the example

$L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ $\quad K = \mathbb{Q}$

L is a splitting field of $(x^2-2)(x^2-3)$ which is seperable

$$\mathrm{Gal}(L:\mathbb{Q}) = \{\mathrm{id}, \sigma_1, \sigma_2, \sigma_3\}$$

where

$$\sigma_1 : \begin{array}{l} \sqrt{2} \to \sqrt{2} \\ \sqrt{3} \to -\sqrt{3} \end{array} \qquad \sigma_2 : \begin{array}{l} \sqrt{2} \to -\sqrt{2} \\ \sqrt{3} \to \sqrt{3} \end{array}$$

$\sigma_3 = \sigma_1 \circ \sigma_2$, $\mathrm{Gal}(L:\mathbb{Q}) = \mathbb{Z}_2 \times \mathbb{Z}_2$ has size 4 and $|\mathrm{Gal}(L:\mathbb{Q})| = [L:\mathbb{Q}] = 4$.

Remark In Thm 2.19' it is important that $\tilde{L}$ is a splitting field of the poly $(\varphi f)(X)$ and not the splitting field of $f(x)$ (unless φ is identity on K).

Thm 2.19' does not say that each autom of K extends to an autom of splitting field over K.
Such extensions might not exist if φ is not identity on K.

Example Let $K = \mathbb{Q}(i)$ and $\varphi = K \to K$
$a+bi \to a-bi$
the $\mathbb{Q}$-autom of K given by complex conjugation

$1+2i$ is not a square in K, since it's norm is 5, $N(1+2i) = 5$ which is not a square in $\mathbb{Q}$.

Thus the field $L = K(\sqrt{1+2i}) = \mathbb{Q}(i, \sqrt{1+2i})$ has degree 2 over K.
φ sends $f = X^2 - (1+2i)$ to $\varphi f = X^2 - (1-2i)$ in $K[X]$. So applying Thm 2.19' with $K' = K$, φ = complex conjugation we get that φ extends to an isom $\sigma : L \to \tilde{L} = \mathbb{Q}(i, \sqrt{1-2i})$ in 2 ways. These 2 extensions σ_1, σ_2 are determined where $\sqrt{1+2i} \in L$ is sent to $\tilde{L}$

$\sqrt{1+2i}$ must be sent to one of the roots of $\varphi f = x^2 - (1-2i)$ and both extensions exist

$\sigma_1 : L \longrightarrow \tilde{L}$ $\sigma_2 : L \longrightarrow \tilde{L}$

$\sqrt{1+2i} \longrightarrow \sqrt{1-2i}$ $\sqrt{1+2i} \longrightarrow -\sqrt{1-2i}$

$= \sigma_1 |_K = \varphi$ and $\sigma_2 |_K = \varphi$ where φ is the complex conjugation on K.

However φ has no extension to an autom of L. To see this suppose there is $\Phi : L \to L$ extending $\varphi : K \to K$
$a+bi \mapsto a-bi$

Let $\alpha = \sqrt{1+2i}$ then $\alpha^2 = 1+2i$

Applying Φ on both sides we get

$\Phi(\alpha)^2 = 1-2i$. Hence $1-2i$ is a square (square of $\Phi(\alpha)$) in L

Hence $\sqrt{1-2i} \in L$ which in return implies $\mathbb{Q}(i, \sqrt{1+2i}) = L = \mathbb{Q}(i, \sqrt{1-2i}) = \tilde{L}$

But this is impossible. Since if $L = \tilde{L}$ then $K(\sqrt{1-2i}) = K(\sqrt{1+2i})$

$\Rightarrow \dfrac{1+2i}{1-2i} = -\dfrac{3}{5} + \dfrac{4}{5}i$ is a square in K

But then $-\frac{3}{5} + \frac{4}{5}i = (a+bi)^2$ w/ $a, b \in \mathbb{Q}$.

$\Rightarrow a^2 - b^2 = -3/5$, $b = 2/5a \Rightarrow a^2 - \dfrac{4}{25a^2} = -3/5$

But $0 = 25a^4 + 15a^2 - 4 = (5a^2-1)(5a^2+4)$ has no rational solns

There are 2 simple but useful corollaries of Thm 3.5

Cor 3.6 Let $L:K$ be a splitting field of a sep. poly $f \in K[x]$ of degree n. If f is irreducible then $n \mid |Gal(L:K)|$

Proof: Exercise

Cor 3.7 Let p be a prime. Then
$$G = Gal(\mathbb{F}_{p^n} : \mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$$

and a generator of G is given by the Frobenius hom $\varphi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$
$$x \mapsto x^p$$

Proof: Exercise

We've seen in Thm 3.5 that if L is a splitting field of a separable poly then

$Gal(L:K)$ is as large as possible

Namely $|Gal(L:K)| = [L:K]$

Defn let $L:K$ be a finite extension. L is said to be Galois over K and $L:K$ is a Galois extension if $|Gal(L:K)| = [L:K]$.

Rmk Thm 3.5 says $L:K$ is a Galois extension when L is a splitting field over K of a separable poly.

We'll see soon that converse is also true. ie if $L:K$ is a finite extension with $Gal(L:K)$ maximal ie $|Gal(L:K)| = [L:K]$ then L is a splitting field of a sep. poly.

For this we need a thm of Dedekind on the lin. independence of characters of gps which in return will give lin. independence of monomorphisms of fields.

Defn ① A <u>character</u> χ of a group G with values in a field L is a homomorphism from G to the multiplicative group of L.

$$\chi : G \longrightarrow L^{\times}$$

ie $\chi(g_1 g_2) = \chi(g_1)\chi(g_2) \quad \forall\, g_1, g_2 \in G$

and $\chi(g) \in L \setminus \{0\} \quad \forall\, g \in G$.

② The characters $\chi_1, \dots, \chi_n$ of G are said to be <u>linearly independent</u> over L if they are linearly independent as functions on G. ie there is no non-trivial relation

$$a_1\chi_1 + \dots + a_n\chi_n = 0$$ with ($a_1, \dots a_n \in L$ not all 0) as functions on G

ie $a_1\chi_1(g) + \dots + a_n\chi_n(g) = 0 \quad \forall g \in G$

$\Rightarrow a_1 = a_2 \dots = a_n = 0$