Then $\gcd\left(P_{\beta,E_1}, \frac{d P_{\beta,E_1}}{dX}\right)$ in $E_1[X]$

is the same in $\tilde{E} := F[a_1, \dots, a_d][X]$,

because the Euclidian algorithm does not see the field. So β is separable over $\tilde{E}$. So we have a tower of finite ~~separable~~ extensions

$$\tilde{E}[\beta] \,|\, \tilde{E} \,|\, F[\alpha_1, \dots, \alpha_d] \,|\, F[a_2, \dots, a_d] \,|\, \dots \,|\, F[a_d] \,|\, F$$

and every extension is generated by one element which is separable over the smaller field. Thus, by induction, we have $[\tilde{E}[\beta] : F]$ many extensions of id_F to $\tilde{E}[\beta]$ into F.

$\Rightarrow$ ~~We have~~ There are $[F[\beta] : F]$ many extensions of id_F to $F[\beta]$.

$\Rightarrow$ β is separable over F. $\square$

<u>Def 136:</u> Let $\bar{F}|F$ be an algebraic closure of F and $\alpha \in \bar{F}$ with $P_{\alpha,F} = (X - \alpha_1)(X - \alpha_2) \dots (X - \alpha_d)$. We call $\alpha_1, \dots, \alpha_d$ the conjugates of α in $\bar{F}$.

<u>Prop 137</u>: Suppose $E := F[\alpha, \beta] | F$ is algebraic and β is separable. Then there exists an element $\gamma \in E$ s.t. $E = F[\gamma]$.
(This is "Primitive Element Theorem Part II)

<u>Def 138</u>: 1) An element $\alpha \in E$ satisfying $E = F[\alpha]$ is called <u>primitive element</u> of E over F.

2) Let $E|F$ be an algebraic field extension. We call

$$F^{sep,E} := \{\alpha \in E \mid \alpha \text{ separable over } F\}$$

the separable closure of F in E.

3) An algebraic extension which is not separable is called inseparable. An algebraic extension $E|F$ that does not contain any separable element in $E \setminus F$ is called purely inseparable.

<u>Remark 139</u>: $F^{sep,E}$ is a field.

<u>Proof</u>: $\alpha, \beta \in E$ sep. over F
$\Rightarrow$ $F[\alpha, \beta] | F[\alpha] | F$ tower of sep. ext.

Prop 135 $\Rightarrow$ $F[\beta,2] \,|\, F$ is separable

$\Rightarrow$ $\alpha \pm \beta$, $\frac{\alpha}{\beta}$, $\alpha \cdot \beta$ $(\beta \neq 0)$ are separable over F $\square$

<u>Proof</u> (of Prop 137) $E := F[\alpha,\beta] \,|\, F$ is finite by Prop 114.

<u>Case 1:</u> If F is finite then a ~~the~~ cyclic generator of $F[\alpha,\beta]^\times$ generates $F[\alpha,\beta]$ over F.

<u>Case 2:</u> $|F| = \infty$

<u>Case 2.1:</u> α, β are separable over F

If $\beta \in F$, then $E = F[\alpha]$ ✓.

Suppose $\beta \notin F$. Let $\varphi_1, \dots, \varphi_l$ be the $[E:F]$ many extensions of id_F to E into $\bar{F}$.

$\beta \notin F \Rightarrow P := \prod_{i \neq j} (\varphi_i(\alpha) + X\varphi_i(\beta) - \varphi_j(\alpha) - X\varphi_j(\beta)) \in F[X]$

has degree ≥ 1.

$\Rightarrow \exists\, c \in F : P(c) \neq 0$, because $|F| = \infty$.

$\Rightarrow \gamma := \alpha + \beta$ has at least $[E:F]$ many conjugates in $\bar{F}$ $\Rightarrow E = F[\gamma]$.

<u>Case 2.2.</u> α is not separable over F

$\bar{F}^{sep,E}|F$ is separable and finite. By Case 2.1 and induction it is generated by one element, say w.l.o.g. $\bar{F}^{sep,E} = F[\beta]$.

Next lemma $\Rightarrow$ $\exists$ exactly $[F(\beta):F]$ many extension of id_F to E into $\bar{F}$, say $\varphi_1, \dots, \varphi_\ell$.

Again $p := \prod_{i \neq j} \left((\varphi_i(\beta) + X\varphi_i(\alpha)) - \varphi_j(\beta) - X\varphi_j(\alpha) \right)$

is a non-zero polynomial in $\bar{F}[X]$

$|F| = \infty \Rightarrow \exists c \in F : p(c) \neq 0$ and $c \neq 0$.

Then $\gamma := \beta + c\alpha$ has $\geq \ell$ conjugates in $\bar{F}$

$\Rightarrow [\bar{F}^{sep,F[\gamma]} : F] \geq \ell = [F[\beta]:F]$.

and $\bar{F}^{sep,F[\gamma]} \subseteq \bar{F}^{sep,E} = F[\beta]$.

$\Rightarrow F[\beta] = \bar{F}^{sep,F[\gamma]} \subseteq F[\gamma]$.

$\Rightarrow \beta \in F[\gamma] \underset{c \neq 0}{\Rightarrow} \beta, \alpha \in F[\gamma] \Rightarrow E = F[\gamma]$

$\square$

<u>End of lecture 26</u>

A simple example for Prop. 137.

$$E := \mathbb{Q}(\sqrt{2}, \sqrt{7}) \mid \mathbb{Q}$$

<u>Claim</u>: $\mathbb{Q}(\sqrt{2}+\sqrt{7}) = E$

<u>Proof</u>: $(\sqrt{2}+\sqrt{7})^2 = 9 + 2\sqrt{14}$.

$\Rightarrow \mathbb{Q}[\sqrt{14}] \subseteq \mathbb{Q}[\sqrt{2}+\sqrt{7}]$.

Assume "=" $\Rightarrow \sqrt{2}+\sqrt{7} = a + b\sqrt{14}$

for some $a, b \in \mathbb{Q}$.

$\Rightarrow \quad 9 + 2\sqrt{14} = a^2 + 14b^2 + 2ab\sqrt{14}$

$1, \sqrt{14}$ is a $\mathbb{Q}$-basis of $\mathbb{Q}[\sqrt{14}]$

$\Rightarrow \quad 2 = 2ab$ and $a^2 = 9 - 14b^2$

$\Rightarrow \quad ab = 1$ and $a^2 = 9 - 14\frac{1}{a^2}$

$\Rightarrow \quad a^4 - 9a^2 + 14 = 0$

$$\Rightarrow \quad a^2 = \frac{9}{2} \pm \sqrt{\underbrace{\left(\frac{9}{2}\right)^2 - 14}_{\frac{25}{4}}}$$

$$= \frac{9}{2} \pm \frac{5}{2} \in \left\{\frac{14}{2}, \underbrace{\frac{4}{2}}_{2}\right\} \lightning$$

$\frac{14}{2}$ and 2 are not squares in $\mathbb{Q}$.

So $[\mathbb{Q}(\sqrt{2}+\sqrt{7}) : \mathbb{Q}(\sqrt{14})] \geq 2$.

But $[\mathbb{Q}[\sqrt{2},\sqrt{7}]:\mathbb{Q}]$

$$= \underbrace{[\mathbb{Q}[\sqrt{2},\sqrt{7}]:\mathbb{Q}[\sqrt{2}]]}_{\leq 2}\underbrace{[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]}_{2}$$

$$\leq 4.$$

So $[\mathbb{Q}[\sqrt{2}+\sqrt{7}]:\mathbb{Q}] \geq [E:\mathbb{Q}]$

$\Rightarrow \quad E = \mathbb{Q}[\sqrt{2}+\sqrt{7}]$ $\square$

<u>Lemma 139:</u> Let $E|F$ be an algebraic extension, $\operatorname{char} F = p > 0$ and $[E:F] > 1$. T.a.e.:

1° $E|F$ is purely inseparable.

2° $\forall_{\alpha \in E} \exists_{n \in \mathbb{N}_0} : \alpha^{p^n} \in F$

3° $\exists!$ extension of id_F to E into $\overline{F}$.

<u>Proof:</u> $2° \Rightarrow 3°$ ✓ because $X^{p^n} - a$, $a \in F$ has exactly one root in $\overline{F}$.

$3° \Rightarrow 2°$ We have at least $[\overline{F}^{sep,E} : F]$ extensions of id_F, so by 3°,

$\overline{F}^{sep,E} = F$. $\Rightarrow 1°$.

$1° \Rightarrow 2°$ $\alpha \in E$. $P_{\alpha,F} = Q(X^{p^n})$ for some $n \in \mathbb{N}_0$, and Q has some summand aX^i with $p \nmid i$, in particular Q is separable (no double root and $\deg \geq 1$.)

because $\frac{dQ}{dX} \neq 0$. and Q is irreducible (factorization of Q give a factorization of $P_{\alpha,F}$)

$\Rightarrow \alpha^{p^n}$ is separable over $F \Rightarrow \alpha^{p^n} \in F$ $\square$

<u>Theorem 140:</u> (Primitive element Theorem Part II)

Let $E|F$ be an algebraic field extension.

T.a.e.:

1° $\exists \alpha \in E$: $E = F[\alpha]$

2° There are only finitely many intermediate fields between E and F.

<u>Proof:</u> 1° $\Rightarrow$ 2° $E = F[\alpha]$. in particular $[E:F] < \infty$.

We have $P_{\alpha,F} = (X - \alpha_1) \cdot \ldots \cdot (X - \alpha_\ell)$

($\alpha_1, \ldots, \alpha_\ell$ not necessarily pairwise different)

We attach to $\tilde{E}$ ($F \subseteq \tilde{E} \subseteq E$), a field, the polynomial $P_{\alpha,\tilde{E}}$.

$P_{\alpha,\tilde{E}}$ is monic and divides $P_{\alpha,F}$.

$\Rightarrow \exists S \subseteq \{1, \ldots, \ell\}$: $P_{\alpha,\tilde{E}} = \prod_{i \in S} (X - \alpha_i)$.

Suppose $P_{\alpha,\tilde{E}_1} = P_{\alpha,\tilde{E}_2}$ $\quad E \mid \tilde{E}_i \mid F$.

Define E_0 to be the field generated by the coefficients of $P_{\alpha,\tilde{E}_1}$ over F.

$\Rightarrow \quad P_{\alpha,E_0} = P_{\alpha,\tilde{E}_1} = P_{\alpha,\tilde{E}_2}$ and $E_0 \subseteq \tilde{E}_1 \cap \tilde{E}_2$.

$\Rightarrow \quad [E \mid E_0] = [E : \tilde{E}_i]$, $i = 1,2$.

because $\deg P_{\alpha,E_0} = \deg P_{\alpha,\tilde{E}_i}$.

$\underset{\substack{\uparrow \\ E_0 \subseteq \tilde{E}_1 \cap \tilde{E}_2}}{\Longrightarrow} \quad \tilde{E}_1 = E_0 = \tilde{E}_2$.

<u>$2^\circ \Rightarrow 1^\circ$:</u> (Induction $[E:F]$)

Note at first that $[E:F] < \infty$ by 2°

(Otherwise: $\underbrace{F \subsetneq F[\alpha_1]}_{\substack{\text{finite} \\ \text{(because algebraic)}}} \underbrace{\subsetneq F[\alpha_1,\alpha_2]}_{\text{finite}} \subsetneq \cdots$)

<u>$[E:F]=1$:</u> $\quad E = F[0]$.

<u>$[E:F]>1$:</u> $\quad$ Take $\alpha \in E \setminus F$. If $E = F[\alpha]$ ✓

If $[E:F[\alpha]] > 1$ then $\exists\, \beta \in E : E = F[\alpha,\beta]$ by (IH).

If F is finite then E is finite and $E = F[\gamma]$ for $\langle \gamma \rangle = E^\times$.

Suppose F is infinite.

$2^\circ \Rightarrow \exists\, \lambda_1, \lambda_2 \in F: \; F[\alpha + \lambda_1 \beta] = F[\alpha + \lambda_2 \beta]$.

$\Rightarrow \quad F[\alpha + \lambda_1 \beta] \ni \beta, \alpha$.

$\Rightarrow \quad F[\alpha + \lambda_1 \beta] = E$ $\square$

<u>Example:</u>

Between $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{2}, \sqrt[7]{3} + \sqrt{2} + \sqrt[1000]{5}, 7^{5/3}, i) =: E$

are only finitely many intermediate fields.

<u>Proof:</u> $E|\mathbb{Q}$ is separable, because algebraic and $\operatorname{char} \mathbb{Q} = 0$.

$[E:\mathbb{Q}] < \infty$, because it is generated by finitely many algebraic (over $\mathbb{Q}$) elements.

Prop 137 $\Rightarrow \exists\, \alpha \in E: \; \mathbb{Q}[\alpha] = E \overset{\text{Thm 140}}{\Rightarrow}$ assertion. $\square$

III.5. Galois extensions

Def 141: $\overline{F}|F$ be an algebraic closure of F and $E|F$ a field extension in $\overline{F}$. $E|F$ is called

(a) <u>normal</u> if $\forall \varphi \in \mathrm{Hom}_{\text{field}}(\overline{F}, \overline{F})$:

$$\varphi(E) = E$$

(b) <u>Galois</u> if $E|F$ is separable and normal.

Def. 142: Let $P \in F[X]$ of degree ≥ 1. Let $E|F$ be a field extension.

E is called a <u>splitting field of P</u> (over F) if

- $\exists_{a \in F} \exists_{\alpha_1, \dots, \alpha_d \in E}: P = a(X - \alpha_1) \cdot \ldots \cdot (X - \alpha_d)$

and

- $E = F(\alpha_1, \dots, \alpha_d)$.

<u>Remark</u>: 1) A splitting field of a polynomial over F is algebraic over F, because it is generated by elements which are algebraic over F.

2) In Def 141 one only needs $E|F$ algebraic, because then one can find an algebraic closure $\bar{F}$ of F s.t. $\bar{F} \supseteq E$.

(Take $E|F \xhookrightarrow{\varphi} L|F$ L an algebraic closure of F.

$$\bar{F} := \{ x \in L \mid x \notin \varphi(E) \} \dot{\cup} E$$

Then

$$\begin{tikzcd}
\bar{F} \arrow[r, "\psi", "\sim"'] & L \\
E \arrow[u, hook] \arrow[r, "\varphi", "\sim"'] \arrow[ur, phantom, "\circlearrowleft"] & \varphi(E) \arrow[u, hook] \\
\bar{F} \setminus E \arrow[u, hook] \arrow[r, "id", "\sim"'] \arrow[uur, hook, bend right] \arrow[ur, phantom, "\circlearrowleft"] & L \setminus \varphi(E) \arrow[uu, hook, bend left]
\end{tikzcd}$$

as sets.

Now define $+$ and $\cdot$ on $\bar{F}$ using ψ and $+_L$, $\cdot_L$: $x +_{\bar{F}} y := \psi^{-1}(\psi(x) +_L \psi(y))$, etc.)

<u>Prop 143:</u> Let E_1 and E_2 be two splitting fields of a polynomial $P \in F[X] \setminus F$.

Then $E_1|F \simeq E_2|F$.

<u>Proof:</u> (exercise). $\square$

~~Proposition:~~

<u>Example:</u> 1) The splitting field of X^2-2 in $\mathbb{C}$ is $\mathbb{Q}[\sqrt{2}]$, because $-\sqrt{2} \in \mathbb{Q}(\sqrt{2})$!

2) What is the splitting field of

$P_{\sqrt{2}+\sqrt[3]{3},\mathbb{Q}}$?

Look at the conjugates of $\alpha := \sqrt{2}+\sqrt[3]{3}$ in $\mathbb{C}$. ~~Take~~

Conjugates of $\sqrt{2}$: $\underset{\beta_1}{\sqrt{2}}$, $\underset{\beta_2}{-\sqrt{2}}$

" of $\sqrt[3]{3}$: $\underset{\gamma_1}{\sqrt[3]{3}}$, $\underset{\gamma_2}{e^{\frac{2\pi}{3}i}\sqrt[3]{3}}$, $\underset{\gamma_3}{e^{\frac{4\pi}{3}i}\sqrt[3]{3}}$

So $\varphi \in \mathrm{Aut}_{\text{field}}(\overline{\mathbb{Q}})$ sends α to $\alpha_i + \beta_j$.

$$X^3 - 3 = P_{\sqrt[3]{3}, \mathbb{Q}(\sqrt{2})},$$

because none of the roots of ~~$P_{\sqrt[3]{3}, \mathbb{Q}}$~~ X^3-3 are in $\mathbb{Q}(\sqrt{2})$.

(If $P_{\sqrt[3]{3}, \mathbb{Q}(\sqrt{2})} \neq X^3-3$ then, as $P_{\sqrt[3]{3}, \mathbb{Q}(\sqrt{2})} \mid X^3-3$ in $\mathbb{Q}[\sqrt{2}][X]$, there is a linear factor of X^3-3 contained in $\mathbb{Q}[\sqrt{2}][X]$

$\Rightarrow \gamma_1 \in \mathbb{Q}[\sqrt{2}]$ for some i. $\lightning$)

Thus $\sqrt{2} \mapsto \pm\sqrt{2}$ each has three extension to $\mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$ into $\overline{\mathbb{Q}} \subset \mathbb{C}$ and they send γ_1 to one of the γ_i's.

$$\Rightarrow \forall_{i,j} \ \exists \ \varphi : \mathbb{Q}(\sqrt{2}, \sqrt[3]{3}) \longrightarrow \mathbb{C} :$$

$$\varphi(\sqrt{2}) = \beta_i \text{ and } \varphi(\sqrt[3]{3}) = \gamma_j.$$

$\Rightarrow$ The conjugates of α are

End of lecture 27. $\{\beta_i + \gamma_j \mid i = 1,2, \ j = 1,2,3\}$

<u>Claim:</u> The splitting field of

$P := P_{\sqrt{2}+\sqrt[3]{3},\mathbb{Q}}$ in $\mathbb{C}$ is

$$\mathbb{Q}(\sqrt{2}, \sqrt[3]{3}, i\sqrt{3}) =: L$$

<u>Proof:</u> Let K be the splitting field of P in $\mathbb{C}$.

$$\Rightarrow \quad \sqrt{2} = \frac{1}{2}((\beta_1 + \gamma_1) - (\beta_2 + \gamma_1)) \in K$$

$$\sqrt[3]{3} = \beta_1 + \gamma_1 - \sqrt{2} \in K$$

and $\frac{1}{\sqrt[3]{3}} \cdot (\gamma_2 + \beta_1) - \frac{1}{\sqrt[3]{3}} \beta_1$

$$= \frac{1}{\sqrt[3]{3}} \sqrt[3]{3}\left(-\frac{1}{2} + \frac{\sqrt{3}}{2} i\right) = -\frac{1}{2} + \frac{\sqrt{3}}{2} i \in K$$

$$\Rightarrow \quad L \subseteq K.$$

$K \subseteq L$ is an easy exercise. $\square$ (Claim)

What is the degree of L over $\mathbb{Q}$?

$[\mathbb{Q}[\sqrt{2}+\sqrt[3]{3}] : \mathbb{Q}] = 6$ because $\sqrt{2}+\sqrt[3]{3}$ has 6 conjugates and the ext. is separable (char $\mathbb{Q} = 0$).

$\sqrt{3}\,i \notin \mathbb{Q}(\sqrt{2}, \sqrt[3]{3}) = \mathbb{Q}(\sqrt{2} + \sqrt[3]{3})$

So $[L : \mathbb{Q}(\sqrt{2} + \sqrt[3]{3})] = 2$ and $[L : \mathbb{Q}] = 12$.

- $\mathbb{Q}(\sqrt{2}, \sqrt[3]{3}, i\sqrt{3}) \mid \mathbb{Q}$ is normal (because splitting fields are normal over the ground field) ~~because are automorphisms of the algebraic closure of the ground field~~

- $\mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$ is not normal, because it does not contain all conjugates of $\sqrt{2} + \sqrt[3]{3}$ in $\overline{\mathbb{Q}}$.

2) Let $E \mid \mathbb{F}_p$ be a field extension ~~of~~ in $\overline{\mathbb{F}_p} \mid \mathbb{F}_p$. Then $E \mid \mathbb{F}_p$ is normal.

<u>Proof:</u> $E = \bigcup_{\alpha \in E} \mathbb{F}_p[\alpha]$ and $\mathbb{F}_p[\alpha]$ is a finite field, $\alpha \in E$.

Example 2) after Prop. 130 $\Rightarrow$

$\forall_{\alpha \in E} \forall \varphi \in \mathrm{Aut}_{\text{fields}}(\overline{\mathbb{F}_p} / \mathbb{F}_p) : \varphi(\mathbb{F}_p[\alpha]) = \mathbb{F}_p[\alpha]$.

$\Rightarrow \forall \varphi \in \mathrm{Aut}_{\text{fields}}(\overline{\mathbb{F}_p} \mid \mathbb{F}_p) : \varphi(E) = E$. $\square$

3) Purely inseparable extensions are normal.

<u>Prop 144:</u> Let $E|F$ be algebraic and $\bar{F}$ be an algebraic closure of F containing E.

T.a.e.:

1° $E|F$ is normal

2° $\forall_{\alpha \in E}$: All conjugates of α in $\bar{F}$ lie in E.

3° E is generated by a union of splitting fields of polynomials over F.

<u>Proof:</u> 1° $\Rightarrow$ 2° ✓ easy.

2° $\Rightarrow$ 3° Let F_P be the splitting field of $P \in F[X] \setminus F$ over F. in $\bar{F}$.

Then $E = \bigcup_{\alpha \in E} F_{P_{\alpha,F}}$.

$\subseteq$ ✓

$\supseteq$ by 2°.

3° $\Rightarrow$ 1° Let $\{P_\lambda \mid \lambda \in \Lambda\}$ be a set of polynomials in $F[X] \setminus F$ s.t.

$E = F\left(\bigcup_{\lambda \in \Lambda} F_{P_\lambda}\right)$.

Take $\varphi \in \mathrm{Aut}_{\text{fields}}(\bar{F}|F)$.

$F_{p_\lambda}|F$ is normal $\Rightarrow$ $\varphi(E) = \varphi(F(\bigcup_{\lambda\in\Lambda} F_{p_\lambda}))$

$$= F(\bigcup_{\lambda\in\Lambda} \varphi(F_{p_\lambda})) = F(\bigcup_{\lambda\in\Lambda} F_{p_\lambda}) = E.$$

$\square$

<u>Def 14.5:</u> Recall: Let $E|F$ be a field extension.

1) $\mathrm{Aut}(E|F) := \{ f : E \xrightarrow{\sim} E \mid$

f is a field automorphism
(i.e. a bijective field homomorphism)
s.t. $f(x) = x$ for all $x \in F \}$

2) If $E|F$ is Galois then
we write $\mathrm{Gal}(E|F)$ for $\mathrm{Aut}(E|F)$ and
call it the Galois group of $E|F$.

<u>Remark:</u> 1) If $E|F$ is normal then the restriction map

$$\mathrm{Aut}(\bar{F}|F) \longrightarrow \mathrm{Aut}(E|F)$$
$$\varphi \longmapsto \varphi|_E$$

(for $\bar{F} \supseteq E$) is well-defined and surjective.

2) $(\mathrm{Aut}(E|F), \circ)$ is a group.

<u>Example:</u> 1) $\mathbb{C}|\mathbb{R}$ is Galois, because $\mathrm{char}(\mathbb{R}) = 0$ and $\mathbb{C}$ is an algebraic closure of $\mathbb{R}$.
$[\mathbb{C}:\mathbb{R}] = 2 \qquad (\mathbb{C} = \mathbb{R} \oplus \mathbb{R} i)$.

So $|\mathrm{Gal}(\mathbb{C}|\mathbb{R})| = 2$, in fact
$\mathrm{Gal}(\mathbb{C}|\mathbb{R}) = \{ id_{\mathbb{C}}, \overline{(\ )} \}$
complex conjugation.

2) $\mathrm{Gal}(\mathbb{F}_{p^n}|\mathbb{F}_p) = \{ id_{\mathbb{F}_{p^n}}, \varphi_p, \varphi_p^2, \dots, \varphi_p^{n-1} \}$
where φ_p is the Frobenius automorphism of $\mathbb{F}_{p^n}$. $\quad (\varphi_p(x) := x^p.)$

3) Suppose $E|F$ is normal. Then

$$\begin{aligned} \mathrm{Aut}(E|F) &\longrightarrow \mathrm{Aut}(F^{sep,E}|F) \\ \varphi &\longmapsto \varphi|_{F^{sep,E}} \end{aligned}$$

is a group isomorphism.
(exercise)

In particular, if $E|F$ is purely inseparable then $\mathrm{Aut}(E|F)$ is trivial.

4) $\underbrace{\mathbb{Q}(\sqrt{2}, \sqrt[3]{3}, i\sqrt{3})}_{=:L} \,|\, \mathbb{Q}(\sqrt{2})$ is Galois (Why?)

and of degree 6.

It is generated by $\sqrt[3]{3}$, ~~$\sqrt[3]{3}$~~

$\sqrt[3]{3} \cdot e^{\frac{2\pi}{3}}$ and $\sqrt[3]{3}\, e^{\frac{4\pi}{3}}$ because

L is the splitting field of $X^3 - 3$ over $\mathbb{Q}(\sqrt{2})$.

So $|\mathrm{Gal}(L \,|\, \mathbb{Q}(\sqrt{2}))| = 6$ and

We have $\mathrm{Gal}(L \,|\, \mathbb{Q}(\sqrt{2})) \hookrightarrow \mathrm{Bij}(\{\gamma_1, \gamma_2, \gamma_3\})$

Thus $\mathrm{Gal}(L \,|\, \mathbb{Q}(\sqrt{2})) \simeq \mathfrak{S}_3$.

5) <u>Further:</u> $\mathrm{Gal}(L \,|\, \mathbb{Q}(\sqrt{2}))$ has index 2 in $\mathrm{Gal}(L \,|\, \mathbb{Q})$, and infact

$$\mathrm{Gal}(L \,|\, \mathbb{Q}) = \mathrm{Gal}(L \,|\, \mathbb{Q}(\sqrt{2})) \cdot \mathrm{Gal}(L \,|\, \mathbb{Q}(\sqrt[3]{3}, e^{\frac{2\pi}{3}}))$$

Note that $\mathrm{Gal}(L \,|\, \mathbb{Q}(\sqrt{2}))$ is a normal subgroup as well as $\mathrm{Gal}(L \,|\, \mathbb{Q}(\sqrt[3]{3}, e^{\frac{2\pi i}{3}}))$.

(The second because $\mathbb{Q}(\sqrt[3]{3}, e^{\frac{2\pi i}{3}})$ is normal over $\mathbb{Q}$).

6) What does $Gal(L|\mathbb{Q}(\sqrt{2}))$ say about intermediate fields?

$\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3}\, i, \sqrt{2})$, $\mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$, $\mathbb{Q}(\sqrt{2}, \gamma_2)$

$\mathbb{Q}(\sqrt{2}, \gamma_3)$, L They are different.

(If $\gamma_3 \in \mathbb{Q}(\sqrt{2}, \gamma_2)$ then $\gamma_1 = \frac{3}{\gamma_2 \gamma_3} \in \mathbb{Q}(\sqrt{2}, \gamma_2)$

and therefore $L \subseteq \mathbb{Q}(\sqrt{2}, \gamma_2)$

$\Rightarrow [L:\mathbb{Q}] \leq 6$ ↯)

Are they all?

Subgroups of $\mathfrak{S}_3$: $\{id, \langle 1,2\rangle\}$.

$\{id, \langle 1,3\rangle\}$

$\{id, \langle 2,3\rangle\}$

$\{id\}$, $\{id, \langle 1,2,3\rangle, \langle 1,3,2\rangle\}$, $\mathfrak{S}_3$.

<u>Theorem 146:</u> (Fundamental Theorem of Galois Theory)

Let $E|F$ be a finite Galois extension.

Then 1) The map

$$\{L \mid F \subseteq L \subseteq E, L \text{ a field}\} \xrightarrow{\Phi} \{H \mid H \leq Gal(E|F)\}$$

$\Phi(L) := \mathrm{Gal}(E|L)$ is bijective.

2) The inverse of Φ is given by

$$\Phi^{-1}(H) = \{x \in E \mid \forall \varphi \in H : \varphi(x) = x\}$$
$$=: E^H.$$

(the "fixed point set of H")

3) For a field L, s.t. $F \subseteq L \subseteq E$ we have

$$L|F \text{ is Galois}$$
$$\Longleftrightarrow \quad \mathrm{Gal}(E|L) \trianglelefteq \mathrm{Gal}(E|F).$$

<u>Remark:</u> The most difficult part is to show that Φ is surjective. For that we need the following lemma of Artin.

<u>Lemma 147:</u> Suppose E is a field and
(Artin) $G \leq \mathrm{Aut}_{\text{fields}}(E)$ is a finite group. Put $F := E^G$. Then $E|F$ is Galois with $\mathrm{Gal}(E|F) = G$.

<u>Proof:</u> <u>Step 1:</u> $E|F$ is algebraic and separable.

$$\alpha \in E \Longrightarrow P = \prod_{\varphi \in G} (X - \varphi(\alpha)) \in F[X],$$

because the coefficients are fixed by every element of G.

$\ulcorner$ $\tilde{\varphi} \in G$ defines a ring-automorphism

$$\tilde{\varphi} : E[X] \xrightarrow{\sim} E[X]$$

$$\varphi\left(\sum a_i X^i\right) := \sum \tilde{\varphi}(a_i) X^i.$$

$\tilde{\varphi}$ fixes P because

$$\tilde{\varphi}(P) = \prod_{\varphi \in G} (X - \tilde{\varphi}(\varphi(a)))$$

$$\underset{\substack{\uparrow \\ \varphi \mapsto \tilde{\varphi} \circ \varphi \text{ is} \\ \text{a bijection of } G.}}{=} \prod_{\varphi \in G} (X - \varphi(a)) = P. \quad \lrcorner$$

$\Rightarrow$ α is algebraic over F and $P_{\alpha,F} \mid P$. In particular all conjugates of α in (any algebraic closure of E) are in E.

Let $\alpha = \alpha_1, \dots, \alpha_\ell$ be those conjugates.

Then $Q := (X - \alpha_1) \cdot \ldots \cdot (X - \alpha_\ell)$

is also fixed by G, because G permutes the conjugates of α.

$\Rightarrow Q \in F[X] \Rightarrow P_{\alpha,F} \mid Q$ is separable.

$\Rightarrow \alpha$ is separable over F.

<u>Step 2:</u> $E|F$ is normal, because

$\forall \alpha \in E$: All conjugates of α lie in E

by Step 1.

<u>Step 3:</u> $\mathrm{Gal}(E|F) = G$. ("$\supseteq$" is trivial)

"$\subseteq$". $\varphi \in \mathrm{Gal}(E|F)$. Suppose that

$\varphi \notin G$. Then $\forall \psi \in G\ \exists\, \alpha_\psi \in E$:

$\varphi(\alpha_\psi) \neq \psi(\alpha_\psi)$.

$L := F[\alpha_\psi \mid \psi \in G]$. the compositum of all $F[\alpha_\psi]$, $\psi \in G$.

Then $\varphi|_L \neq \psi|_L\ \forall \psi \in G$.

$L|F$ is finite and separable.

Primitive Element Theorem (Part 1)

$\Rightarrow \exists \gamma \in L : L = F[\gamma]$.

$\varphi(\gamma)$ is a conjugate of γ.

Step 1 $\Rightarrow \exists \psi \in G : \psi(\gamma) = \varphi(\gamma)$

$\Rightarrow \varphi|_L = \psi|_L$ ↯.

$\square$

Now we can prove Thm 146.

<u>Proof:</u> 1) Surjectivity of Φ: $(\Phi(L) := Gal(E|L))$

Take $H \leq Gal(E|F)$.

Lemma of Artin (147)

$\Rightarrow H = Gal(E|E^H) = \Phi(E^H)$

Injectivity of Φ: Suppose $\Phi(L_1) = \Phi(L_2)$

Let L be $L_1 L_2$.

$$\begin{aligned} Gal(E|L) &= Gal(E|L_1) \cap Gal(E|L_2) \\ &= \Phi(L_1) \cap \Phi(L_2) \\ &\underset{\Phi(L_1) = \Phi(L_2)}{=} Gal(E|L_1) = Gal(E|L_2). \end{aligned}$$

 So we need to show $L = L_1 = L_2$.

So w.l.o.g. $L_2 \supseteq L_1$.

If $L_2 \supsetneq L_1$, then $\exists\ \varphi : \in \mathrm{Hom}_{\text{fields}}(L_2|L_1; E|L_2)$

$\varphi \neq \mathrm{incl}_{L_2 \hookrightarrow E}$.

φ extends to E: $\psi : E \longrightarrow E$ and

$\psi(E) = E$ because $E|F$ is normal.

$\Rightarrow \exists\ \psi \in \mathrm{Gal}(E|F) : \psi|_{L_2} = \varphi$.

$\Rightarrow \psi \notin \mathrm{Gal}(E|L_2)$ and $\psi \in \mathrm{Gal}(E|L_1)$ ↯

So $L_2 = L_1$.

3) exercise $\square$

<u>Remark:</u> The intermediate fields given in 6) in the Example after Def 145 are all.

$E := \mathbb{Q}(\sqrt{2} + \sqrt[3]{3}, \sqrt{3}\,i)$, $F := \mathbb{Q}(\sqrt{2})$.

$H \leq Gal(E\|F)$	E^H
$\{id, \langle \gamma_1, \gamma_2 \rangle\}$	$\mathbb{Q}(\sqrt{2}, \gamma_3)$
$\{id, \langle \gamma_1, \gamma_3 \rangle\}$	$\mathbb{Q}(\sqrt{2}, \gamma_2)$
$\{id, \langle \gamma_2, \gamma_3 \rangle\}$	$\mathbb{Q}(\sqrt{2}, \gamma_1)$
$\{id\}$	$\cancel{Gal(E\|F)}$ E
$\{id, \langle \gamma_1, \gamma_2, \gamma_3 \rangle, \langle \gamma_1, \gamma_3, \gamma_2 \rangle\}$	$\mathbb{Q}(\sqrt{2}, \sqrt{3}\,i)$
$Gal(E\|F)$	$\mathbb{Q}(\sqrt{2}) = F$

III.6. Roots of polynomial as radical expressions of the coefficients (?)

<u>Question:</u> Given a polynomial

$P \in \mathbb{C}[X] \setminus \mathbb{C}$,

$$P = \sum_{i=0}^{d} a_i X^i \qquad d = \deg(P).$$

Is there a term

$\Phi(a_0, \dots, a_d)$, just made of

$\mathbb{Q}, +, \cdot, \sqrt[m]{\ }$ (in $\mathbb{C}$), such that $\Phi(a_0, \dots, a_d)$

is a zero of P?

We call such a Φ a <u>radical expression</u>.

<u>Examples:</u> 1) $P = X - a$

$$\Phi(x) := a$$

2) $P = X^2 + pX + q$

$$\Phi(p,q) = -\frac{p}{2} \pm \sqrt{\left(\frac{p}{2}\right)^2 - q}$$

3) $P = X^3 + pX + q \quad (\zeta := e^{\frac{2\pi i}{3}})$

$$x_j = \zeta^j u + \frac{\left(-\frac{p}{3}\right)}{\zeta^j u}, \qquad j = 0, 1, 2.$$

where u is a solution of $u^3 = -\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}$,

for $p \neq 0$.

4) $\deg P = 4$: Ferrari's formula.

What about $\deg(P) \geq 5$?

<u>Example</u>: $P = X^5 - 9X + 3$

We will see, that for this polynomial the roots are not radical expressions in the coefficients of P.

From now on in this lecture we only deal with fields of characteristic 0.

<u>Def 148:</u> Let F be a field of char. 0 and $\bar{F}$ an alg. closure of F.

1) $P \in F[X] \setminus F$ is called solvable (or solvable by radicals) over F

$\forall \alpha \in \mathrm{Zero}_{\bar{F}}(P)$ $\exists$ radical expression Φ_α s.t. $\alpha = \Phi_\alpha(a_0, \dots, a_\ell)$

where $a_0, \dots, a_\ell$ are elements of F.

<u>end of lecture 29</u>

2) Let $E|F$ be a finite extension in $\bar{F}|F$. We call $E|F$ solvable by radicals if

$\exists$ $E'|E$ a finite extension in $\bar{F}$:

$\exists$ tower of extensions

$$E' = E_m | E_{m-1} | E_{m-2} | \dots | E_2 | E_1 = F$$

s.t. $E_{i+1}|E_i$ is radical. (see 3))

3) A finite extension $E|F$ is called radical if $\exists \alpha \in E$ $\exists n \in \mathbb{N}$: $E = F[\alpha]$ and $\alpha^n \in F$.

<u>Prop 145:</u> (char $F=0$) Let E be the splitting field of some polynomial P over F. T.a.e.:

1° P is solvable

2° $E|F$ is solvable by radicals.

<u>Proof:</u> $1^\circ \Rightarrow 2^\circ$ ✓ easy. Just resolve the radical expressions of the zeros of P.

$2^\circ \Rightarrow 1^\circ$ Take $E'|E$ finite with a tower

$$E' = E_m | E_{m-1} | \dots | E_2 | E_1 = F$$

of radical extensions.

Say $E_m = E_{m-1}[\beta]$ and $\beta^n \in E_{m-1}$.

Take $\alpha \in \mathrm{zero}_{\bar{F}}(P)$. Then

$$\exists\, b_0, \dots, b_{n-1} \in E_{m-1} : \quad \alpha = \sum_{i=0}^{n-1} b_i \beta^i$$

Now continue by induction until $b_i \in E_{m-1}$. □

How can we see that $E|F$ is solvable by radicals?

<u>Def. 150:</u> 1) Let G be a group. We call the sequence of subgroups

$$G \geq \underset{\substack{\| \\ [G;G]}}{D(G)} \geq D^2(G) \geq D^3(G) \geq \ldots$$

where $D^{i+1}(G) = D(D^i(G)) = [D^i(G); D^i(G)]$, $i \geq 0$ and $D^0(G) = G$ the derived series of G.

2) A group G is called solvable if $\exists i \geq 0$ $D^i(G) = \{1_G\}$.

<u>Example:</u> 1) If G is abelian then G is solvable. $[G;G] = \langle \{a;b\} = aba^{-1}b^{-1} \rangle_G$

$$= \langle 1_G \rangle_G = \{1_G\}.$$

2) $G := \left\{ \begin{pmatrix} x & a & c \\ & y & b \\ & & z \end{pmatrix} \;\middle|\; \begin{matrix} a, b, c \in \mathbb{R} \\ x, y, z \in \mathbb{R}^\times \end{matrix} \right\} =: B_3(\mathbb{R})$

is solvable. ("standard Borel subgroup of $GL_3(\mathbb{R})$")

$$D(G) = [G, G] = \left\{ \begin{pmatrix} 1 & a & c \\ & 1 & b \\ & & 1 \end{pmatrix} \;\middle|\; a, b, c \in \mathbb{R} \right\}$$

$$D^2(G) = [D^1(G), D^1(G)] = \left\{ \begin{pmatrix} 1 & 0 & a \\ & 1 & 0 \\ & & 1 \end{pmatrix} \;\middle|\; a \in \mathbb{R} \right\}$$

$$D^3(G) = \left\{ \begin{pmatrix} 1 & & \\ & 1 & \\ & & 1 \end{pmatrix} \right\},$$

3) $SL_2(\mathbb{R})$ is not solvable.

(HW) because $[SL_2(\mathbb{R}), SL_2(\mathbb{R})] = SL_2(\mathbb{R})$ ($SL_2(\mathbb{R})$ is perfect.)

4) A_n is not solvable for $n \geq 5$ because A_n is simple and not abelian. (S. Lang Ch 1. Thm 5.5)

<u>Prop 151</u>: Let G be a non-trivial group. T.a.e.

1° G is solvable.

2° $\exists_m \exists\, G_0 = G \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \ldots \trianglerighteq G_m = \{1\}$.

s.t. $\forall i = 0, \dots, m-1$: G_i / G_{i+1} is abelian.

(for $|G| < \infty$) 3° $\exists m \in \mathbb{N}_0$ $\exists$ $G_0 = G \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \dots \trianglerighteq G_m = \{1\}$

$\forall i = 0, \dots, m-1$: G_i / G_{i+1} is cyclic

of prime order

<u>Proof:</u> 1° ⇒ 2° ✓ because $D^i G / D^{i+1} G$

is abelian.

2° ⇒ 3° We only need to

refine the series in 2°,

so only need to consider

the factors G_i / G_{i+1}, so

w.l.o.g. G is abelian.

(and for 3°: $|G| < \infty$)

$\Rightarrow G \simeq \mathbb{Z}/p_1^{\gamma_1}\mathbb{Z} \times \mathbb{Z}/p_2^{\gamma_2}\mathbb{Z} \times \dots \times \mathbb{Z}/p_\ell^{\gamma_\ell}\mathbb{Z}$

$$\frac{\mathbb{Z}/p_i^{\nu_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_i^{\nu_1}\mathbb{Z}}{\mathbb{Z}/p_{i+1}^{\nu_i}\mathbb{Z} \times \mathbb{Z}/p_i^{\nu_1}\mathbb{Z}}$$

$$\simeq \mathbb{Z}/p_i^{\nu_i}\mathbb{Z}$$

and $\mathbb{Z}/p_i^{\nu_i}\mathbb{Z} \trianglerighteq p_i\mathbb{Z}/p_i^{\nu_i}\mathbb{Z} \trianglerighteq p_i^2\mathbb{Z}/p_i^{\nu_i}\mathbb{Z} \trianglerighteq \cdots \trianglerighteq \{1\}$

has cyclic factors of order p_i.

$3^\circ \Rightarrow 2^\circ$ ✓

$2^\circ \Rightarrow 1^\circ$ Take a series

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_m = \{1_G\}$$

s.t. G_i/G_{i+1} is abelian $\forall_{m>i\geq 0}$.

Consider $q: G_0 \twoheadrightarrow G_0/G_1$.

$g \mapsto [g]_{G_1}$

$$\varphi([a,b]) = \varphi(a)\varphi(b)\varphi(a)^{-1}\varphi(b)^{-1}$$
$$= [e]_{G_1} \text{ because}$$

G_0/G_1 is abelian.

$\Rightarrow D(G) \subseteq G_1$.

Induction: $D^i(G) \leq G_i \Rightarrow$

$$D^{i+1}G = D(D^i(G)) \leq DG_i$$

$$\leq G_{i+1} \quad \text{(base case)}$$

$\Rightarrow D^m G \leq G_m = \{1_G\}$. $\square$

<u>Def 152:</u> Let $E|F$ be an algebraic extension then $E|F$ is called solvable, cyclic, abelian if $E|F$ is Galois and $G(E|F)$ is solvable, cyclic, abelian respectively.

Theorem 153: (char $F = 0$)

Let $E|F$ be a finite Galois extension. T.a.e.

1° $E|F$ is solvable by radicals

2° $E|F$ is solvable.

Lemma 154: A quotient of a solvable group is solvable.

(exercise)

Lemma 155: A splitting field of a polynomial $X^n - a \in F[X] \setminus F$ is solvable over F.

Proof: Let ζ be a primitive nth root of unity in F, i.e. $\zeta^n = 1$ and $\zeta^i \neq 1$ $\forall_{1 \leq i \leq n-1}$. (easy, because char $F = 0$)

$E_1 := F[\rho] = F[\rho, \rho^2, \dots, \rho^n]$

is the splitting field of $X^n - 1$

over F.

$\varphi_1, \varphi_2 \in Gal(E_1|F)$, $\varphi_1(\rho) = \rho^i$, $\varphi_2(\rho) = \rho^j$

$\varphi_1 \circ \varphi_2(\rho) = \varphi_1(\rho^j) = \varphi_1(\rho)^j = \rho^{ij}$

$= \varphi_2 \circ \varphi_1(\rho)$.

$\Rightarrow Gal(E_1|F)$ is abelian

$E|E_1$ is Galois, because $E|F$ is.

$\psi_1, \psi_2 \in Gal(E|E_1)$, say $\alpha^n = a$.

$\psi_1(\alpha) = \alpha \cdot \rho^i$

$\psi_2(\alpha) = \alpha \cdot \rho^j$

$\psi_1 \circ \psi_2(\alpha) = \psi_1(\alpha \rho^j) = \psi_1(\alpha)\, \psi_1(\rho^j)$

$\underset{\rho^j \in E_1}{=} \alpha \rho^i \rho^j = \alpha \rho^{i+j} = \psi_2 \circ \psi_1(\alpha)$

$\Rightarrow Gal(E|E_1)$ is abelian $\square$

Lemma 156: If $E|F$ is cyclic then it is solvable by radicals

Proof: $E = F[\alpha]$ for some α, because $E|F$ separable and finite. $Gal(E|F) = \langle \varphi \rangle$

Put $n := |Gal(E|F)|$

We want to find α such $\alpha \in (\alpha)$

W.l.o.g. E contains a primitive ζ (ζ) nth root of unity ζ.

Hilbert 90 (next Lemma)

$\Rightarrow \exists \alpha \in E^\times : \frac{\varphi(\alpha)}{\alpha} = \zeta$.

$\Rightarrow P_{\alpha,F} = (X-\alpha)(X-\alpha\zeta)(X-\alpha\zeta^2) \cdot (X-\alpha\zeta^{n-1}) = X^n - \alpha^n$.

$\square$

To prove Hilbert 90' we need another Theorem:

<u>Theorem 157</u> (Artin's Theorem)

Let E be a field and $\chi_1, \dots, \chi_m \in \mathrm{Aut}_{\text{field}}(E)$ be pairwise different field automorphisms of E.

Then $\chi_1, \dots, \chi_m$ are E-linear independend, i.e.

$$\forall \beta_1, \dots, \beta_m \in E : \left(\sum_{i=1}^{m} \beta_i \chi_i = 0 \in \mathrm{Hom}_{\text{rings}}(E, E) \right.$$

$$\left. \Longrightarrow \beta_1 = \dots = \beta_m = 0 \in E \right)$$

<u>Proof:</u> Assume that $\exists \beta_1, \dots, \beta_m \in E$ not all zero s.t. $\sum_{i=1}^{m} \beta_i \chi_i = 0_{\text{map}}$

We take m to be smallest with this property, in particular $\beta_1 \cdots \beta_m \neq 0$.

<u>Claim:</u> $m \geq 2$:

<u>Proof:</u> If $m=1$ then $\beta_1 \chi_1 = 0_{map}$ and $\beta_1 \neq 0$

$\Rightarrow \forall x \in E: \ \chi_1(x) = \beta_1^{-1} 0_{map}(x) = \beta_1^{-1} 0_E = 0_E$

$\Rightarrow \chi_1$ is not a field automorphism $\lightning$ $\square$

Take $\alpha \in E$ s.t. $\chi_1(\alpha) \neq \chi_2(\alpha)$

Then (I) $\sum_{i=1}^{m} \beta_i \chi_1(\alpha) \chi_i = 0_{map}$

and (II) $\sum_{i=1}^{m} \chi_1(\alpha) \beta_i \chi_i = 0_{map}$

(I) − (II) $\Rightarrow \sum_{i=2}^{m} \beta_i (\chi_i(\alpha) - \chi_1(\alpha)) \chi_i = 0_{map}$

$\lightning$ to the minimality of m, because

$\chi_2(\alpha) - \chi_1(\alpha) \neq 0_E$. $\square$

Now we can prove Hilbert 90:

<u>Lemma 158</u> (Hilbert 90)

Let $E|F$ be a finite cyclic field extension, $Gal(E|F) = \{id, \sigma, \dots, \sigma^{n-1}\}$, $[E:F] =: n$. Let $\alpha \in E$, s.t. $\alpha \sigma(\alpha) \cdots \sigma^{n-1}(\alpha) = 1$.

Then $\exists\ \gamma \in E^{\times}$: $\alpha = \dfrac{\gamma}{\sigma(\gamma)}$.

<u>Proof:</u> ~~Instead of~~

The map

$$f := id_E + \alpha\cdot\sigma + \alpha\sigma(\alpha)\sigma^2 + \alpha\sigma(\alpha)\sigma^2(\alpha)\sigma^3 + \dots + \alpha\sigma(\alpha)\sigma^2(\alpha)\cdots\sigma^{n-2}(\alpha)\sigma^{n-1}$$

is non-zero by Artin's Theorem.

$\Rightarrow \exists\ \theta \in E^{\times}$: $f(\theta) \neq 0$.

Put $\gamma := f(\theta)$. $\Rightarrow$ $\alpha\cdot\sigma(\gamma) \overset{\alpha\sigma(\alpha)\sigma^2(\alpha)\cdots\sigma^{n-1}(\alpha)=1}{=} \gamma$

$\Rightarrow$ $\alpha = \dfrac{\gamma}{\sigma(\gamma)}$. $\square$