K/F extension of fields.

K field $\mathrm{Aut}(K) = \{$all field automorphisms $K \xrightarrow{\sigma} K\}$
" ring $\sigma(ab) = \sigma(a)\sigma(b)$ $\sigma(1) = 1$

$\mathrm{Aut}(K)$ is a group under composition $\sigma(a+b) = \sigma(a) + \sigma(b)$

$(\sigma \circ \tau)(a) = \sigma(\tau(a))$ $\mathrm{Aut}(\mathbb{R}) = \{Id\}$ $\mathrm{Aut}(\mathbb{C}) \ni$ conjugation

$\mathrm{Aut}(\mathbb{Q}) = \{Id\}$ (prove this) $\mathbb{C} \to \mathbb{C}$ $z \mapsto \bar{z}$

$z = x + iy$ $\bar{z} = x - iy$ $\overline{z\omega} = \bar{z}\bar{\omega}$ $\overline{z+\omega} = \bar{z} + \bar{\omega}$

$\mathrm{Aut}(\mathbb{C}) =$ infinite

K/F extn of fields $\mathrm{Gal}(K/F) = \{\sigma \in \mathrm{Aut}(K) \,/\, \sigma|_F = Id_F\}$

$\mathrm{Gal}(K/F)$ is a subgroup of $\mathrm{Aut}(K)$ (obvious)

operation = composition $\sigma(\alpha . a) = \sigma(\alpha)\sigma(a) = \alpha\sigma(a)$

$\sigma \in \mathrm{Gal}(K/F) \Rightarrow \sigma$ is a F linear map $K \to K$ $\alpha \in F$, $a \in K$

$\mathrm{Gal}(K/F) \subseteq \mathrm{Hom}_F(K, K) = \mathrm{End}_F(K)$

$\mathrm{Gal}(K/F) \subseteq \{$all F linear isom $K \to K\}$

$K = F(a_1, \ldots, a_n)$ fg extn of F, $a_i \in K$

$\sigma \in G(K/F) = \mathrm{Gal}(K/F)$ then σ is determined by $\sigma(a_1), \ldots, \sigma(a_n) \in K$

$\alpha \in K$ $\alpha = \dfrac{f(a_1, \ldots, a_n)}{g(a_1, \ldots, a_n)}$ $g(a_1, \ldots, a_n) \neq 0 \Rightarrow \sigma(\alpha) = \dfrac{f(\sigma(\alpha_1), \ldots, \sigma(\alpha_n))}{g(\sigma(\alpha_1), \ldots, \sigma(\alpha_n))}$

$\sigma, \tau \in G(K/F)$ $\sigma(a_i) = \tau(a_i)$ $\forall i = 1, \ldots, n$ then $\sigma = \tau$

$\alpha \in K/F$ algebraic over F $f(x) = \mathrm{Min}(F, \alpha)$ $f(\sigma(\alpha)) = \sigma(\underbrace{f(\alpha)}_{=0}) = \sigma(0)$

$\sigma(\alpha)$ is a root of $f(x) \Rightarrow \mathrm{Min}(F, \sigma(\alpha))$ divides $f(x)$

$\mathrm{Min}(F, \sigma(\alpha)) = f(x)$ as $f(x)$ is irred/F

$\sigma(\alpha)$ is a root of $f(x) \Rightarrow \mathrm{Min}(F, \sigma(\alpha))$ divides $f(x)$

$\mathrm{Min}(F, \sigma(\alpha)) = f(x)$ as $f(x)$ is irred$/F$.

σ permutes the roots of $f(x)$ (the roots which lie in K)

K/F finite extn $\Rightarrow G(K/F)$ is a finite group

$K = F(\alpha_1, \dots, \alpha_n)$ $\quad \alpha_i$ is alg$/F$ $\alpha_i \in K$

$\sigma \in G(K/F)$ is determined $\sigma(\alpha_i)$ and $\exists$ finitely many possibilities for the value of each $\sigma(\alpha_i)$ ($\sigma(\alpha_i)$ has to be one of the roots in K of $\mathrm{Min}(\alpha_i, F)$).

So $G(K/F)$ is finite.

Examples ① $G(\mathbb{C}/\mathbb{R}) = \{Id, conj\}$ $\quad \mathbb{C} = \mathbb{R}(i)$

② $G(\mathbb{Q}(i)/\mathbb{Q}) = \{Id, conj\}$ ③ $G(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{Id, \sqrt{2} \mapsto -\sqrt{2}\}$

$F(t) \supseteq$ $u(t) \notin F$, $u(t) = \frac{f(t)}{g(t)}$, $F(u(t))$, F

$\sigma(a + b\sqrt{2}) = a - b\sqrt{2}$

④ $G(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{Id\}$ $\quad x^3 - 2$ $\quad \sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$

⑤ $G(\mathbb{F}_2(t)/\mathbb{F}_2(t^2)) = \{Id\}$ $\quad x^2 - t^2$ is the min poly of t over $\mathbb{F}_2(t^2)$

$g(x)\, u(t) - f(x) = 1 \cdot t^2 - x^2$ $\quad x^2 - t^2 = (x-t)^2$ over $\mathbb{F}_2$

⑥ $\mathbb{F}_2[x] / \underset{\text{irred}}{(x^2+x+1)} = $ field with 4 elts $\quad \{0, 1, x, x+1\}$

$\longrightarrow$ is a v.s. of dim $2/\mathbb{F}_2$ $\quad x^2 = -x-1 = x+1$

$x(x+1) = x^2 + x = -x - 1 + x = -1 = 1$ $\quad (x+1)^2 = x^2 + 2x + 1 = -x - 1 + 1 = x$

$G\left(\mathbb{F}_2[x]/(x^2+x+1) / \mathbb{F}_2\right) = \{Id, \sigma\}$ $\quad \sigma(x) = x+1$ $\quad \sigma(0) = 0$, $\sigma(1) = 1$

$\sigma(x+1) = \sigma(x) + \sigma(1) = x + 1 + 1 = x$

(7) K/F extn $F \subseteq L \subseteq K$ L intermediate field

$L \longrightarrow G(K/L) = \{\sigma \in Aut(K) / \sigma|_L = Id\}$ subgp of $G(K/F)$

H subgp of $G(K/F)$ $\mathcal{F}(H) = K^H := \{a \in K / \sigma(a) = a \ \forall \sigma \in H\}$

$\mathcal{F}(H) = K^H$ is an intermediate field $F \subseteq K^H \subseteq K$

$F \subseteq K^H \subseteq K$ obvious K^H field obvious $\boxed{K/F \text{ fixed \& given}}$

$\left\{\begin{array}{c}\text{intermediate fields } L \\ F \subseteq L \subseteq K\end{array}\right\}$ $\{\text{subgroups of } G(K/F)\}$

$F \rightsquigarrow G(K/F)$

$K \rightsquigarrow G(K/K) = \{Id\}$

$K \leftsquigarrow \{Id\}$

$\{a \in K / \sigma(a) = a \ \forall \sigma \in G(K/F)\} \leftsquigarrow G(K/F)$

$\cup\!\!\!\mid\ F$

$L \rightsquigarrow G(K/L) = \{\sigma \in G(K/F) / \sigma \text{ fixes } L\}$
$\sigma|_L = Id$

$\mathcal{F}(H) = K^H = \mathcal{F}(G(K/L)) \leftsquigarrow \overset{\shortparallel}{H}$

$= K^{G(K/L)} = \{a \in K \mid \sigma(a) = a \ \forall \sigma \in G(K/L) = H\}$

$L \subseteq \mathcal{F}(G(K/L)) = K^{G(K/L)}$

$H < G(K/F) \rightsquigarrow \mathcal{F}(H) = K^H \rightsquigarrow G(K/K^H) = G(K/\mathcal{F}(H)) = \{\sigma|_{K^H} = Id\} \supseteq H$

$H < G(K/\mathcal{F}(H)) = G(K/K^H)$, $L \subseteq \mathcal{F}(G(K/L)) = K^{G(K/L)}$

$L_1 \subseteq L_2 \Rightarrow G(K/L_2) \subseteq G(K/L_1)$ inclusion reversing

$H_1 \leq H_2 \Rightarrow \mathcal{F}(H_2) = K^{H_2} \subseteq K^{H_1} = \mathcal{F}(H_1)$ $\shortparallel$

K/F extn of fields Then $\exists$ a 1-1 inclusion reversing

K/F extn of fields. Then $\exists$ a 1-1 inclusion reversing correspondence between the following 2 sets

$$\{F \subseteq L \subseteq K \mid L = \mathcal{F}(H) = K^H \text{ for some } H < G(K/F)\} \rightleftarrows \{H < G(K/F) \mid H = G(K/L) \text{ for some } K \supseteq L \supseteq F\}$$

$$L \mapsto G(K/L)$$

$$K^H = \mathcal{F}(H) \leftarrow H$$

$$H \rightsquigarrow L = K^H \rightsquigarrow G(K/L) \rightsquigarrow K^{G(K/L)} \supseteq L$$

$$H \subseteq G(K/K^H) \rightsquigarrow L = K^H \supseteq K^{G(K/K^H)} = K^{G(K/L)}$$

$$\boxed{L = K^{G(K/L)}}$$

$$L \rightsquigarrow \underset{G(K/L)}{\overset{\shortparallel}{H}} \rightsquigarrow K^H \rightsquigarrow G(K/K^H) \supseteq H$$

$$L \subseteq K^{G(K/L)} \rightsquigarrow H = G(K/L) \supseteq G(K/K^H)$$

$$H = G(K/K^H)$$

$A \xrightarrow{f} B$ f ring hom A, B 2 comm rings with 1

$I \subseteq A \longrightarrow f(I)B =: I^e \subseteq B$ extended ideal

$J^c = f^{-1}(J)$ $J \subseteq B$

contracted ideal

$$\{\text{ideals of } A\} \rightleftarrows \{\text{ideals of } B\}$$

$$I \longmapsto I^e$$

$$J^c \longleftarrow J$$

$I^{ec} \supseteq I$

$J^{ce} \supseteq J$

$I_1 \subseteq I_2$

$I_1^e \subseteq I_2^e$

$J_1 \subseteq J_2$

$J_1^c \subseteq J_2^c$

$$\{\text{all contracted ideals of } A\} \longleftrightarrow \{\text{all extended ideals of } B\}$$

$I = J^c$ $I^e = J$

$\underline{I^{ec} \supseteq I} \supseteq I^{ec}$

$\underline{I = J^c}$ then $\underline{I^{ec} = I}$

$J = I^e$ then $J^{ce} = J$

$I = J^c$

$J^c \supseteq J^{cec}$

$I^e = J^{ce} \supseteq J$

$I^{ec} = J^{cec} = \ldots$

Atiyah Macdonald

Atiyah Macdonald
Ch 1 exercise

$I^{ec} = J^{cec} \supseteq J^{c} =$