10 February 2021 18:30

A, B comm. rings with 1

$f: A \to B$ ring hom, $I \subseteq A$ ideal, $I^e = f(I)B$, $J \subseteq B$ ideal, $J^c = f^{-1}(J)$

Then $I \subseteq I^{ec}$, $J^{ce} \subseteq J$ If $I = J^c \Rightarrow I = I^{ec}$

$$I \subseteq I^{ec} \qquad J^{ce} \subseteq J \Rightarrow J^{cec} \subseteq J^c = I$$

$$\Rightarrow I = I^{ec} \qquad \overset{\shortparallel}{I}{}^{ec}$$

Similarly, $J^{ce} = J$ if $J = I^e$ for some $I \subseteq A$.

This gives a bijection between contracted ideals of A & extended ideals of B (given by $J \to J^c$ & $I \to I^e$)

Recall : $\exists$ inclusion reversing bijection (given K/F)

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

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

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

$\sigma: K \to K$ $\quad \sigma \in Aut(K)$ $\quad \sigma: K^* \to K^*$ $\quad \sigma$ is mult hom

$\sigma(ab) = \sigma(a)\sigma(b)$ $\quad \sigma$ is called a character $\sigma: K^* \to K^*$

G group $\quad \sigma: G \to K^*$ hom $\quad \sigma(ab) = \sigma(a)\sigma(b)$ $\quad G = K^*$

σ called a character (of G) (defn of a repn of G)

G group K field A representation of G is a gp hom (n diml)

$$G \to GL_n(K)$$

$GL_1(K) = K^*$ (why?)

$GL_n(K)$ $\qquad GL_1(K) = K^*$ (why?)

character of G = 1 dim'l rep'n of G

<u>Dedekind</u>: Let $\sigma_1, \ldots, \sigma_n$ be n distinct characters $G \to K^*$ (G = group and K is a field) Then if $\sum_{i=1}^{n} c_i \sigma_i(g) = 0$ for all $g \in G$ and for some $c_i \in K$ then $c_i = 0 \; \forall i$

$\sum c_i \sigma_i \equiv 0$ (on G) $\Rightarrow c_i = 0 \; \forall i$ $\qquad$ linear independence of characters
(for some $c_i \in K$)

Defer proof

Lemma: K/F finite ext'n of fields Then $|G(K/F)| \leq [K:F]$

<u>Pf</u>: $[K:F] = n \qquad v_1, \ldots, v_n \in K$ basis of K over F

$|G(K/F)| = m$ (know it is finite) Suppose $m > n$ get contra

$G(K/F) = \{\sigma_1, \ldots, \sigma_m\}$ Each row $\in K^n$

$$\begin{array}{ccccc} & \multicolumn{4}{c}{\xleftrightarrow{\quad n \quad}} \\ c_1 & \sigma_1(v_1) & \sigma_1(v_2) & \cdots & \sigma_1(v_n) \\ & \vdots & & & \\ & \vdots & & & \\ c_m & \sigma_m(v_1) & \sigma_m(v_2) & \cdots & \sigma_m(v_n) \end{array} \Bigg\updownarrow m$$

There are m such rows $m > n$
There are lin. dep over K
$\exists \, c_1, \ldots, c_m$ not all zero, $c_i \in K$
s.t $\sum_{i=1}^{m} c_i \sigma_i(v_j) = 0 \;\; \forall j = 1, \ldots, n$

So $\sum_{i=1}^{m} c_i \sigma_i(v) = 0 \;\; \forall v \in K \qquad v_1, \ldots, v_n$ basis of K/F

$v \in K \Rightarrow v = \sum_{j=1}^{n} b_j v_j \quad b_j \in F \quad \sum_{i=1}^{m} c_i \sigma_i(v) = \sum_{i=1}^{m} c_i \sigma_i\left(\sum_{j=1}^{n} b_j v_j\right)$

Now $\sigma_i \in G(K/F) \subseteq \mathrm{Aut}(K) \qquad = \sum_{j=1}^{n} b_j \sum_{i=1}^{m} c_i \sigma_i(v_j) = 0$

hence $\sigma_i : K^* \to K^*$

$G(K/F) = \mathrm{Aut}(K)$ $\sum_{j=1} \sum_{i=1} c_i \sigma_i(v_j) = 0$

hence $\sigma_i : K^* \to K^*$ distinct characters $\Big\}$ $\sum c_i \sigma_i = 0$ on K^*

Dedekind $\Rightarrow$ $c_i = 0 \ \forall i$ contradiction so $\underset{m}{\underset{\wedge}{|G(K/F)|}} > \underset{n}{\underset{\|}{[K:F]}}$

so $[K:F] \geq |G(K/F)|$

K/F finite extn $\Rightarrow$ $|G(K/F)| \leq [K:F]$

Pf (Dedekind): $\sum_{i=1}^{n} c_i \sigma_i(g) = 0 \quad \forall g \in G$ $\quad \sigma_i : G \to K^*$ mult. hom distinct char

TST all $c_i = 0$. If not consider a relation which cannot be made smaller by discarding any σ_i's.

$\Rightarrow$ $c_i \neq 0 \ \forall i = 1, \ldots, n$ $\quad n \geq 2$

$\sigma_1 \neq \sigma_2$ $\quad \sigma_1(h) \neq \sigma_2(h)$ for some $h \in G$

$$\cancel{c_1 \sigma_1(h) \sigma_1(g)} + c_2 \sigma_1(h) \sigma_2(g) + \cdots + c_n \sigma_1(h) \sigma_n(g) = 0$$

$$-\cancel{c_1 \sigma_1(h) \sigma_1(g)} + c_2 \sigma_2(h) \sigma_2(g) + \cdots + c_n \sigma_n(h) \sigma_n(g) = 0$$

$c_2(\sigma_1(h) - \sigma_2(h)) \neq 0$

$$\sum_{i=2}^{n} \underline{c_i(\sigma_1(h) - \sigma_i(h))} \sigma_i(g) = 0 \quad \forall g \in G$$

$\sum_{i=2}^{n} d_i \sigma_i = 0$ on G smaller set of σ_i's

$d_2 = c_2(\sigma_1(h) - \sigma_2(h)) \neq 0$ contradiction

hence $c_i = 0 \ \forall i$ Dedekind: linear ind of distinct char

Thm: K field $G \subseteq \mathrm{Aut}(K)$ G is a finite subgroup of $\mathrm{Aut}(K)$

$F = \mathcal{F}(G) = K^G$ Then $|G| = [K : K^G]$ and

$F = \mathcal{F}(G) = K^G$ Then $\underline{|G| = [K : K^G]}$ and $\underline{G = Gal(K/K^G)}$ $\Longrightarrow$

Proof: $[K : K^G] \geq |Gal(K/K^G)|$ (by applying result $|G(K/F)| \leq [K:F] < \infty$

$Gal(K/K^G) \supseteq G$

$|Gal(K/K^G| \geq |G| = [K : K^G]$

$\Rightarrow |Gal(K/K^G)| = |G| \Longrightarrow G = Gal(K/K^G)$ since $G \subseteq Gal(K/K^G)$

$G \subseteq Aut(K)$ $|G| = [K : K^G]$ Suppose $|G| < [K : K^G]$

$|G| \leq |Gal(K/K^G)| \leq [K : K^G]$ then will get the follwg contradiction

$|G| = n$ $G = \{\sigma_1, \ldots, \sigma_n\}$ $[K : K^G] > n$

$\exists$ $(n+1)$ lin indep elts of K/K^G $v_1, \ldots, v_{n+1}$

$$\left.\begin{matrix} \sigma_1(v_1) & \sigma_1(v_2) & \cdots & \sigma_1(v_{n+1}) \\ & & & \\ \sigma_n(v_1) & \sigma_n(v_2) & \cdots & \sigma_n(v_{n+1}) \end{matrix}\right| n$$
$$\underbrace{\qquad\qquad\qquad\qquad\qquad}_{n+1}$$

The $(n+1)$ columns are l.d$/K$

$$\sum_{i=1}^{n+1} c_i \sigma_j(v_i) = 0 \quad \forall j = 1, \ldots n$$

Relabel the columns & chose k minimal s.t $\sum_{i=1}^{k} c_i \sigma_j(v_i) = 0$

WMA wlog $c_1 \neq 0$ hence $c_1 = 1$

All c_i's cannot $\underline{\text{belong to}}$ $\underset{=K^G}{F}$ $0 = \sum c_i \sigma_j(v_i) = \sum \sigma_j(\sum c_i v_i)$ $\forall j$

$\Rightarrow \sum c_i v_i = 0$ (σ_j is an aut) contradicts v_i's are l.ind

$\sigma \in G$ $0 = \sigma(\sum_{i=1}^{k} c_i \sigma_j(v_i)) = \sum_{i=1}^{k} \sigma(c_i) \sigma\sigma_j(v_i) = \sum_{i=1}^{k} \sigma(c_i) \sigma_l(v_i)$

k k

$\sigma \in G \quad 0 = \sigma\left(\sum_{i=1} c_i \, \sigma_j(v_i)\right) = \sum_{i=1} \sigma(c_i)\, \sigma\sigma_j(v_i) = \sum_{i=1} \sigma(c_i)\, \sigma_\ell(v_i)$

$0 = \sum_{i=1}^{k} c_i \, \sigma_\ell(v_i) \qquad \sum_{i=2}^{k} (c_i - \sigma(c_i))\, \sigma_\ell(v_i) = 0$

Minimality $\Rightarrow \; c_i = \sigma(c_i) \;\; \forall i = 2, .. k \;\; \forall \sigma \in G \;\Big|\; \underset{\text{not possible}}{c_i \in F = K^G}$

$\Rightarrow \; c_i \in K^G \quad i = 2, .. k \quad c_1 = 1$

This gives a contradiction

$K|F$ Galois finite $\qquad [K:F] = |\mathrm{Gal}(K/F)|$

$K/K^G \qquad [K:K^G] = |\overset{\overset{G}{\shortparallel}}{\mathrm{Gal}(K/K^G)}| = |G|$

$\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$ is a finite extn of degree 6 (Why?)

This is a finite Galois extn Why?

$\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ is a finite extn of degree 4 (Why?)

This is a finite Galois extn Why?

$\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is a Galois extn