例題

$\alpha = \sqrt{3} + 2\sqrt{5}$, $\beta = \sqrt{3} - \sqrt{5}$ とおくとき、$c \in \mathbb{Q}$, $c \neq -1, 2$ ならば

$$\mathbb{Q}(\alpha + c\beta) = \mathbb{Q}(\sqrt{3}, \sqrt{5}).$$

[証明] 次のステップで証明する。

(1) $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$.
(2) $\sqrt{5} \notin \mathbb{Q}(\sqrt{3})$
(3) $[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}(\sqrt{3})] = 2$.
(4) $L = \mathbb{Q}(\sqrt{3}, \sqrt{5})$ は $\mathbb{Q}$ のガロア拡大であって、その拡大次数は 4.
(5) $\mathrm{Gal}(L/\mathbb{Q})$ の元 σ は $\sqrt{3}$ の行き先 $\sigma(\sqrt{3})$ ($\sqrt{3}, -\sqrt{3}$ の二通り。) と $\sqrt{5}$ の行き先 $\sigma(\sqrt{5})$ ($\sqrt{5}, -\sqrt{5}$ の二通り) により定まる。しかも、それら ($2 \times 2 =$) 4 通りの組み合わせはすべてガロア群の元として現れる。
(6) $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ の $\mathbb{Q}$ ベクトル空間としての基底として $\{1, \sqrt{3}, \sqrt{5}, \sqrt{15}\}$ を取ることができる。
(7) $c \neq -1, 2$ なら、 ガロア群 $\mathrm{Gal}(L/\mathbb{Q})$ の元で、$\alpha + c\beta$ を動かさないものは、ガロア群の単位元 (恒等写像) に限る。

上のように、ガロア理論を知った上でなら、次の補題の内容が分かりやすくなる。(この補題自体は、ガロア理論の構築そのものに必要であったので、ガロアの基本定理 (ガロア対応) を用いずに証明する必要があった。)

補題 11.1 (補題 6.8 再掲)**.** K は無限個の元を持つ体とする。K 上の代数的な元 α, β が、ともに K 上分離的ならば

$$K(\alpha, \beta) = K(\alpha + c\beta)$$

をみたす $c \in K$ が少なくともひとつ存在する。

二重根号について。

次のような等式がある。

$$\sqrt{3 + \sqrt{5}} = \frac{\sqrt{12 + 2\sqrt{5}}}{2} = \frac{\sqrt{12 + \sqrt{20}}}{2} = \frac{\sqrt{(\sqrt{10} + \sqrt{2})^2}}{2} = \frac{\sqrt{10} + \sqrt{2}}{2}$$

つまり、$\sqrt{3 + \sqrt{5}}$ は　右辺のように簡単化できる。これを**二重根号をはずす**という。同様に、次のような等式が成り立つことがわかる。

$$\sqrt{7 - 2\sqrt{6}} = \sqrt{6} - 1, \quad \sqrt{3 + \sqrt{2}} = \sqrt{6} - 1,$$

一方で、$\sqrt{3 + \sqrt{7}}$ は上のようには簡単にならない。これは、次のように説明できる。

(1) $\mathbb{Q}$ のガロア拡大 L で、$\alpha = \sqrt{3 + \sqrt{7}}$ を元として含むものは、 $\sqrt{3 - \sqrt{7}}$) も元として含む。
(2) $L = \mathbb{Q}(\sqrt{3 + \sqrt{7}}, \sqrt{3 - \sqrt{7}})$.
(3) $L \supset \mathbb{Q}(\sqrt{7}, \sqrt{2})$.
(4) $[L : \mathbb{Q}(\sqrt{7}, \sqrt{2})] = 2$.
(5) もし、α が有理数 x, y でもって $\sqrt{x}, \sqrt{y}$ の有理係数の有理式としてかけるなら、$L = \mathbb{Q}(\sqrt{x}, \sqrt{y})$ となって、上の事実と矛盾する。

[ガロア対応の証明]

体 K のガロア拡大 L が与えられているとする。$G = \mathrm{Gal}(L/K)$ の部分群 H に対して、

$$\mathcal{F}(H) = \{x \in L; g.x = x(\forall g \in H)\}$$

と定義する。L と K の中間体 M に対して、

$$\mathcal{G}(M) = \{g \in G; g.x = x(\forall x \in M)\}$$

と定義する。この時、次のことが成り立つ。(単調減少性)

(1) G の任意の部分群 H_1, H_2 に対して、

$$H_1 \subset H_2 \implies \mathcal{F}(H_1) \supset \mathcal{F}(H_2).$$

(2) L/K の任意の中間体 M_1, M_2 に対して、

$$M_1 \subset M_2 \implies \mathcal{G}(M_1) \supset \mathcal{G}(M_2).$$

(3) G の任意の部分群 H にたいして、

$$\mathcal{G}(\mathcal{F}(H)) \supset H.$$

(4) L/K の任意の中間体 M に対して、

$$\mathcal{F}(\mathcal{G}(M)) \supset M.$$

実は、上の (1)-(4) から、全く形式的な計算で次のことが成り立つことがわかる。
("3 回=1 回")

(1) G の任意の部分群 H にたいして、

$$\mathcal{F}(\mathcal{G}(\mathcal{F}(H))) = \mathcal{F}(H).$$

(2) L/K の任意の中間体 M に対して、

$$\mathcal{G}(\mathcal{F}(\mathcal{G}(M))) = \mathcal{G}(M).$$

ガロア理論では、さらに次のことが分かる。(狭義単調減少性)

(1) G の任意の部分群 H_1, H_2 に対して、

$$H_1 \subset H_2, \mathcal{F}(H_1) = \mathcal{F}(H_2) \implies H_1 = H_2$$

(補題 9.4 による。)

(2) L/K の任意の中間体 M_1, M_2 に対して、

$$M_1 \subset M_2, \mathcal{G}(M_1) = \mathcal{G}(M_2) \implies M_1 = M_2.$$

(命題 8.4 による。)

このことから、最後に次のことが分かる。
("2 回=0 回")

(1) G の任意の部分群 H にたいして、

$$\mathcal{G}(\mathcal{F}(H)) = H.$$

(2) L/K の任意の中間体 M に対して、

$$\mathcal{F}(\mathcal{G}(M)) = M.$$