問題 4-1 ($\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$ に関する問題)

(1) $\alpha = \sqrt{2}+\sqrt{3}$ の $\mathbb{Q}$ 上での最小多項式を求めよ。

(2) $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}1 \oplus \mathbb{Q}\sqrt{2} \oplus \mathbb{Q}\sqrt{3} \oplus \mathbb{Q}\sqrt{6}$ を示せ。

(3) $\mathbb{Q}(\sqrt{2},\sqrt{3})$ の体の自己同型 σ, τ で

$$\sigma(a) = a \ (a \in \mathbb{Q}), \quad \sigma(\sqrt{2}) = -\sqrt{2}, \quad \sigma(\sqrt{3}) = \sqrt{3}$$

$$\tau(a) = a \ (a \in \mathbb{Q}), \quad \tau(\sqrt{2}) = \sqrt{2}, \quad \tau(\sqrt{3}) = -\sqrt{3}$$

をみたすものが唯一つ存在することを示せ。

$\mathbb{Q}[x]/(x^2-2)$

|| おおざっぱ

($\mathbb{Q}[x]$ の中で x^2-2 を 0 とみなしてできる環)

||

($\mathbb{Q}[x]$ の中で $x^2=2$ とみなしてできる環)

解答例 問題 3-4 の結果より，$\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$.

$[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}] = 4$ を示そう。

x^2-2 は $\mathbb{Q}$ 上既約なので $\sqrt{2}$ の $\mathbb{Q}$ 上での最小多項式になる。

ゆえに，$\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}[x]/(x^2-2)$ なので $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = \dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}) = \dim_{\mathbb{Q}} \mathbb{Q}[x]/(x^2-2) = 2$ で

$\mathbb{Q}(\sqrt{2}) = \mathbb{Q}1 \oplus \mathbb{Q}\sqrt{2} = \{a+b\sqrt{2} \mid a,b \in \mathbb{Q}\}$

$\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ である。もしも $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$ ならば $\sqrt{3} = a+b\sqrt{2}$, $a,b \in \mathbb{Q}$ と書ける。

両辺を2乗すると，$3 = a^2+2b^2+2ab\sqrt{2}$ なので $3 = a^2+2b^2$ かつ $ab=0$ となる。

しかし，これは不可能なので，$\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$.

$\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ より, $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})] = [\mathbb{Q}(\sqrt{2})(\sqrt{3}) : \mathbb{Q}(\sqrt{2})] > 1$.

$\sqrt{3}$ は $x^2-3=0$ の解なので $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})] = [\mathbb{Q}(\sqrt{2})(\sqrt{3}) : \mathbb{Q}(\sqrt{2})] \leqq 2$.

したがって, $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$.

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

$$[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})]\,[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \times 2 = 4.$$

問題3-5の解答例を参照せよ.
別の方法もある.
(x^2-3 は $\mathbb{Q}(\sqrt{2})$ 上既約)

(1) $[\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] = 4$ より, $\sqrt{2}+\sqrt{3}$ の $\mathbb{Q}$ 上での最小多項式は4次式になる. ゆえに, $x=\sqrt{2}+\sqrt{3}$ で 0 になる $f(x) \in \mathbb{Q}[x]$ で4次のものが $\sqrt{2}+\sqrt{3}$ の $\mathbb{Q}$ 上での最小多項式になる.

$$f(x) = (x-(\sqrt{2}+\sqrt{3}))(x-(-\sqrt{2}+\sqrt{3}))(x-(\sqrt{2}-\sqrt{3}))(x-(-\sqrt{2}-\sqrt{3}))$$ ← ここがおかしい

$$= ((x+\sqrt{3})^2-2)((x-\sqrt{3})^2-2) = (x^2+1+2\sqrt{3}x)(x^2+1-2\sqrt{3}x)$$

$$= (x^2+1)^2 - 12x^2 = x^4 - 10x + 1 \in \mathbb{Q}[x].$$

この $f(x)$ が $\sqrt{2}+\sqrt{3}$ の $\mathbb{Q}$ 上での最小多項式になる.

(2) $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2$ より, $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}1 \oplus \mathbb{Q}\sqrt{2}$,

$[\mathbb{Q}(\sqrt{2})(\sqrt{3}):\mathbb{Q}(\sqrt{2})] = [\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})] = 2$ より, $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2})1 \oplus \mathbb{Q}(\sqrt{2})\sqrt{3}$

これらより, 任意の $\beta \in \mathbb{Q}(\sqrt{2},\sqrt{3})$ は, ある $a,b,c,d \in \mathbb{Q}$ によって,

$$\beta = (a1+b\sqrt{2})1 + (c1+d\sqrt{2})\sqrt{3} = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$$

と表される.

もしも, $a,b,c,d \in \mathbb{Q}$ かつ $a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} = (a1+b\sqrt{2})\cdot 1+(c1+d\sqrt{2})\sqrt{3} = 0$ ならば,

1 と $\sqrt{3}$ の $\mathbb{Q}(\sqrt{2})$ 上での一次独立性より, $a1+b\sqrt{2} = c1+d\sqrt{2} = 0$ となり,

1 と $\sqrt{2}$ の $\mathbb{Q}$ 上での一次独立性より, $a=b=c=d=0$ となる.

ゆえに, $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ は $\mathbb{Q}$ 上一次独立である.

以上によって, $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}1 \oplus \mathbb{Q}\sqrt{2} \oplus \mathbb{Q}\sqrt{3} \oplus \mathbb{Q}\sqrt{6}$ が示された.

以上の証明は, 体の拡大の列 $M/L, L/K$ $(M \supset L \supset K)$ が与えられたとき,

$$[M:K] = [M:L][L:K] \quad ([M/K]=[M/L][L/K])$$

が成立することの証明の特殊化になっている.

(3) 体の同型写像たち $\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2})(\sqrt{3}) \xrightarrow{\sim} \mathbb{Q}(\sqrt{2})[x]/(x^2-3) \xrightarrow{\sim} \mathbb{Q}(\sqrt{2})(-\sqrt{3})=\mathbb{Q}(\sqrt{2},\sqrt{3})$

$$f(\sqrt{3}) \longmapsto \overline{f(x)} \longmapsto f(-\sqrt{3})$$

の合成をτと書く。τも体の同型写像で

$\tau(\beta)=\beta\ (\beta\in\mathbb{Q}(\sqrt{2}))$ ゆえに $\tau(a)=a\ (a\in\mathbb{Q})$ かつ $\tau(\sqrt{2})=\sqrt{2}$, $\tau(\sqrt{3})=-\sqrt{3}$

をみたす。これでほしいτの存在が示された。

τが$\mathbb{Q}(\sqrt{2},\sqrt{3})$の体の自己同型でかつ $\tau(a)=a\ (a\in\mathbb{Q})$, $\tau(\sqrt{2})=\sqrt{2}$, $\tau(\sqrt{3})=-\sqrt{3}$ をみたしているならば，任意の $a,b,c,d\in\mathbb{Q}$ について

$$\begin{aligned}\tau(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}) &= \tau(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{2}\sqrt{3})\\ &= \tau(a)+\tau(b)\tau(\sqrt{2})+\tau(c)\tau(\sqrt{3})+\tau(d)\tau(\sqrt{2})\tau(\sqrt{3})\\ &= a+b\sqrt{2}-c\sqrt{3}-d\sqrt{6}.\end{aligned}$$

τの形が一意に決まってしまった。これでほしいτの一意性も示された。

√3を−√3にうつすτの作り方と一意性

σの存在と一意性は√2と√3の立場を取り換えた同様の議論で証明される。 □

㊟ $\mathbb{Q}(\sqrt{2},\sqrt{3})\cong\mathbb{Q}[x,y]/(x^2-2,y^2-3)$ を用いて，ほしいσとτの存在を示すこともできる。この方針の証明も自分で考えてみよ。 □