イントロダクション（2次方程式の場合）

我々は体のGalois理論についてやる。何をやりたいのか？

2次方程式

$a, b, c \in \mathbb{Q}$ であるとし，$a \neq 0$ と仮定する。

2次方程式 $ax^2 + bx + c = 0$ について考えよう。

よりシンプルな方程式に帰着していく。

両辺を a でわると，$x^2 + \frac{b}{a}x + \frac{c}{a} = 0$.

$p = \frac{b}{a}$，$q = \frac{c}{a}$ とおくと，$x^2 + px + q = 0$

$x = X - \frac{p}{2}$ とおくと，$X^2 \cancel{- pX} + \frac{p^2}{4} \cancel{+ pX} - \frac{p^2}{2} + q = 0$.

$$X^2 - \frac{p^2}{4} + q = 0. \qquad X^2 = \frac{p^2}{4} - q$$

$$X = \pm\sqrt{\frac{p^2}{4} - q}.$$

2次方程式は $X^2 = A$ 型の2次方程式に帰着される。平方根で2次方程式は解ける。

重要なポイント　0でない数の平方根のとり方は2通りある。

たとえば，2の平方根のとり方は $\pm\sqrt{2}$ の2つある。

-1 の平方根のとり方は $\pm i$ の2つある。$(i=\sqrt{-1})$

どちらをえらんでもよい。 ← あいまいな言い方 ← どういう意味か？

どういう意味か　（おおざっぱな説明）　加減乗除 ← 体の演算

$\sqrt{2}$ を $-\sqrt{2}$ でおきかえても四則演算がたもたれる。たとえば

$$\underbrace{(1+\sqrt{2})(2-3\sqrt{2}) = 2-3\sqrt{2}+2\sqrt{2}-3\cdot 2 = -4-\sqrt{2}}$$

この中の $\sqrt{2}$ をすべて $-\sqrt{2}$ でおきかえても等式が成立

$$\overbrace{(1-\sqrt{2})(2+3\sqrt{2}) = 2+3\sqrt{2}-2\sqrt{2}-3\cdot 2 = -4+\sqrt{2}}$$

OK

これを

どう定式化するか

これが体のGalois理論の基本的なアイデア！

体の言葉を使った定式化

体 K を $K=\mathbb{Q}$ と定める。 ← このLはKの拡大体の例になっている。

体 L を $L=\mathbb{Q}(\sqrt{2})=$ ($\mathbb{Q}$ と $\sqrt{2}$ を含む最小の($\mathbb{R}$の部分)体)

$$=\{a+b\sqrt{2} \mid a,b\in\mathbb{Q}\}$$

← こうなる。

(注) $\mathbb{Q}(-\sqrt{2})=\mathbb{Q}(\sqrt{2})=\mathbb{Q}(\sqrt{2},-\sqrt{2})$

← この σ が $\sqrt{2}$ を $-\sqrt{2}$ でおきかえる操作になっている。

写像 $\sigma: L\to L$ を $\sigma(a+b\sqrt{2})=a-b\sqrt{2}$ $(a,b\in\mathbb{Q})$ と定める。

このとき、σ は体 L の(自己)同型写像になっている。

σ は全単射なのでこれを示すためには、σ が四則演算を保つことを示せば十分である。

さらに、σ は $a\in\mathbb{Q}$ について $\sigma(a)=a$ をみたす。

すなわち、σ は $K=\mathbb{Q}$ の元を動かさない。

(σ は体 L の体 K 上での自己同型であるという。) ← これが後でGalois理論で使われる!

$\boxed{\text{問題 1-1}}$ 集合 $L=\{a+b\sqrt{2}\mid a,b\in\mathbb{Q}\}$ が $\mathbb{Q}$ と $\sqrt{2}$ を含む $\mathbb{R}$ の最小の部分体になっていることを証明せよ.

$\mathbb{R}$ の部分体とは $\mathbb{R}$ の部分環で体になっているもののことである.

証明するべきこと:

$L\supset\mathbb{Q}$, $L\ni\sqrt{2}$ は自明

(1) L は $\mathbb{R}$ の部分環でかつ体になっている.

体 (でもよい)

(2) M を $\mathbb{R}$ の部分環でかつ $\mathbb{Q}$ と $\sqrt{2}$ を含むものとするとき, $L\subset M$.

この2つを示せば十分である. □

$\mathbb{Q}[\alpha]=(\mathbb{Q}$ と α を含む $\mathbb{R}$ の最小の部分環$)$

$\boxed{\text{問題 1-2}}$ $\alpha,\beta\in\mathbb{R}$ のとき, $\mathbb{Q}(\alpha)=(\mathbb{Q}$ と α を含む $\mathbb{R}$ の最小の部分体$)$,

$\mathbb{Q}(\alpha,\beta)=(\mathbb{Q}$ と α,β を含む $\mathbb{R}$ の最小の部分体$)$ とおく. このとき,

$$\mathbb{Q}(\sqrt{2})=\mathbb{Q}(-\sqrt{2})=\mathbb{Q}(\sqrt{2},-\sqrt{2})$$

となることを示せ.

□

$\boxed{\text{記号の約束}}$ Lは体でKはその部分体とし，$\alpha_1,\dots,\alpha_r \in L$ であるとする；

- $K[\alpha_1,\dots,\alpha_r]$ = (Kと$\alpha_1,\dots,\alpha_r$を含むLの最小の部分環)
- $K(\alpha_1,\dots,\alpha_r)$ = (Kと$\alpha_1,\dots,\alpha_r$を含むLの最小の部分体)

商体

かっこの形 ( ) と [ ] のちがいに注意

注意 $K[\alpha_1,\dots,\alpha_r] = K(\alpha_1,\dots,\alpha_r)$ となることもある。

$\boxed{\text{問題 1-3}}$ $L = \mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} \mid a,b \in \mathbb{Q}\}$ とおき，

写像 $\sigma : L \to L$ を $\sigma(a+b\sqrt{2}) = a-b\sqrt{2}$ $(a,b\in\mathbb{Q})$ と定める。

このとき，以下が成立することを示せ：$a \in \mathbb{Q}$，$\alpha,\beta \in L$ のとき

(0) $\sigma(a) = a$.

(1) $\sigma(\alpha+\beta) = \sigma(\alpha)+\sigma(\beta)$.

(2) $\sigma(\alpha-\beta) = \sigma(\alpha)-\sigma(\beta)$.

(3) $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$.

(4) $\alpha \neq 0$ のとき，$\sigma\left(\frac{1}{\alpha}\right) = \frac{1}{\sigma(\alpha)}$.

□

ここで動画をストップし，資料のつづきを見ることもやめて，問題を解いてみよ。

$\boxed{\text{解答例}}$

$\boxed{\text{問題 1-1}}$ 集合 $L=\{a+b\sqrt{2} \mid a,b\in\mathbb{Q}\}$ が $\mathbb{Q}$ と $\sqrt{2}$ を含む $\mathbb{R}$ の最小の部分体になっていることを証明せよ。

$\mathbb{R}$ の部分体とは $\mathbb{R}$ の部分環で体になっているもののことである。

証明するべきこと:　　　$L\supset\mathbb{Q}$, $L\ni\sqrt{2}$ は自明

(1) L は $\mathbb{R}$ の部分環でかつ体になっている。

(2) M を $\mathbb{R}$ の部分環でかつ $\mathbb{Q}$ と $\sqrt{2}$ を含むものとするとき，$L\subset M$.

この2つを示せば十分である。□

$\boxed{\text{解答例}}$ $\mathbb{Q}\subset L\subset\mathbb{R}$, $\sqrt{2}\in L$ は自明なので (1),(2) を示せば十分である。

(1) $\underbrace{0,1\in L \text{ でかつ, } \alpha,\beta\in L \text{ のとき, } \alpha+\beta,\ -\alpha,\ \alpha\beta\in L}_{\text{部分環}}$ でかつ $\underbrace{\alpha\neq 0 \Rightarrow \frac{1}{\alpha}\in L}_{\text{さらに体}}$

となることを示せばよい。

$\mathbb{Q}\subset L$ より, $0,1\in L$ は自明. $\alpha,\beta\in L$ を任意にとる。

α,β は $\alpha=a+b\sqrt{2}$, $\beta=c+d\sqrt{2}$ $(a,b,c,d\in\mathbb{Q})$ と表わされる。

つづく

$$\alpha+\beta=(a+b\sqrt{2})+(c+d\sqrt{2})=(a+c)+(b+d)\sqrt{2}\in L.$$

$$-\alpha=-(a+b\sqrt{2})=(-a)+(-b)\sqrt{2}\in L.$$

$$\alpha\beta=(a+b\sqrt{2})(c+d\sqrt{2})=(ac+2bd)+(ad+bc)\sqrt{2}\in L.$$

$\alpha=a+b\sqrt{2}\neq 0$ のとき，　分子分母に $a-b\sqrt{2}$ をかける

$$\frac{1}{\alpha}=\frac{1}{a+b\sqrt{2}}=\frac{a-b\sqrt{2}}{a^2-2b^2}=\frac{a}{a^2-2b^2}+\frac{-b}{a^2-2b^2}\sqrt{2}\in L.$$

余談
（$\mathbb{R}$ の部分体は常に $\mathbb{Q}$ を含む
$\mathbb{C}$ の部分体も常に $\mathbb{Q}$ を含む）

(2)　M は $\mathbb{R}$ の部分環でかつ $\mathbb{Q}$ と $\sqrt{2}$ を含むものであるとする．

任意に $\alpha\in L$ をとる．$\alpha=a+b\sqrt{2}$，$a, b\in\mathbb{Q}$ と書ける．

$a, b, \sqrt{2}\in M$ でかつ M が加法と乗法でとじていることより，

$\alpha=a+b\sqrt{2}\in M$．　これで $L\subset M$ が示された．　$\square$

$\mathbb{Q}[\alpha]=(\mathbb{Q}$ と α を含む $\mathbb{R}$ の最小の部分環$)$ ← おまけの話

$\boxed{\text{問題 1-2}}$ $\alpha,\beta\in\mathbb{R}$ のとき, $\mathbb{Q}(\alpha)=(\mathbb{Q}$ と α を含む $\mathbb{R}$ の最小の部分体$)$,

ここがちがう

$\mathbb{Q}(\alpha,\beta)=(\mathbb{Q}$ と α,β を含む $\mathbb{R}$ の最小の部分体$)$ とおく. このとき,

$$\mathbb{Q}(\sqrt{2})=\mathbb{Q}(-\sqrt{2})=\mathbb{Q}(\sqrt{2},-\sqrt{2})$$

となることを示せ.

$\boxed{\text{解答例}}$ $\mathbb{Q}(\sqrt{2})\overset{(1)}{\subset}\mathbb{Q}(-\sqrt{2})\overset{(2)}{\subset}\mathbb{Q}(\sqrt{2},-\sqrt{2})\overset{(3)}{\subset}\mathbb{Q}(\sqrt{2})$ を示せばよい.

(1) $-1\in\mathbb{Q}\subset\mathbb{Q}(-\sqrt{2})$, $-\sqrt{2}\in\mathbb{Q}(-\sqrt{2})$ と $\mathbb{Q}(-\sqrt{2})$ が乗法でとじていることより,

$\sqrt{2}=(-1)(-\sqrt{2})\in\mathbb{Q}(-\sqrt{2})$.

$\mathbb{Q}(\sqrt{2})$ は $\mathbb{Q}$ と $\sqrt{2}$ を含む $\mathbb{R}$ の部分体の中で最小であるので $\mathbb{Q}(\sqrt{2})\subset\mathbb{Q}(-\sqrt{2})$.

(2) $\mathbb{Q}(\sqrt{2},-\sqrt{2})$ は $\mathbb{Q},\pm\sqrt{2}$ を含む $\mathbb{R}$ の部分体で,

$\mathbb{Q}(-\sqrt{2})$ が $\mathbb{Q},-\sqrt{2}$ を含む $\mathbb{R}$ の部分体の中で最小であることより $\mathbb{Q}(-\sqrt{2})\subset\mathbb{Q}(\sqrt{2},-\sqrt{2})$.

(3) $\mathbb{Q}(\sqrt{2})$ が $\mathbb{Q}$ と $\pm\sqrt{2}$ を含む $\mathbb{R}$ の部分体で, $-\sqrt{2}=(-1)\sqrt{2}\in\mathbb{Q}(\sqrt{2})$

$\mathbb{Q}(\sqrt{2},-\sqrt{2})$ が $\mathbb{Q},\pm\sqrt{2}$ を含む $\mathbb{R}$ の部分体の中で最小であることより $\mathbb{Q}(\sqrt{2},-\sqrt{2})\subset\mathbb{Q}(\sqrt{2})$. □

$\boxed{\text{問題 1-3}}$ $L = \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ とおき,
写像 $\sigma : L \to L$ を $\sigma(a+b\sqrt{2}) = a - b\sqrt{2}$ $(a, b \in \mathbb{Q})$ と定める.
このとき, 以下が成立することを示せ: $a \in \mathbb{Q}$, $\alpha, \beta \in L$ のとき

(0) $\sigma(a) = a$.

(1) $\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta)$.

(2) $\sigma(\alpha - \beta) = \sigma(\alpha) - \sigma(\beta)$.

(3) $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$.

(4) $\alpha \neq 0$ のとき, $\sigma\left(\frac{1}{\alpha}\right) = \frac{1}{\sigma(\alpha)}$.

□

(σ は L の $\mathbb{Q}$ 上での自己同型になっている.)

$\boxed{\text{解答例}}$

(0) $\sigma(a) = \sigma(a + 0\sqrt{2}) = a - 0\sqrt{2} = a$

$\alpha = a + b\sqrt{2}$, $\beta = c + d\sqrt{2}$, $a, b, c, d \in \mathbb{Q}$ と書ける. (この a は上の a とは別)

(1, 2) $\sigma(\alpha \pm \beta) = \sigma((a \pm c) + (b \pm d)\sqrt{2}) = (a \pm c) - (b \pm d)\sqrt{2}$

$\sigma(\alpha) \pm \sigma(\beta) = (a - b\sqrt{2}) \pm (c - d\sqrt{2})$ //

(3) $\sigma(\alpha\beta) = \sigma((ac + 2bd) + (ad + bc)\sqrt{2}) = (ac + 2bd) - (ad + bc)\sqrt{2}$

$\sigma(\alpha)\sigma(\beta) = (a - b\sqrt{2})(c - d\sqrt{2}) = (ac + 2bd) - (ad + bc)\sqrt{2}$ //

(4) $\alpha = a + b\sqrt{2} \neq 0$ のとき,

$$\sigma\left(\frac{1}{\alpha}\right) = \sigma\left(\frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2}\right) = \frac{a}{a^2 - 2b^2} - \frac{-b}{a^2 - 2b^2}\sqrt{2}$$

$$\frac{1}{\sigma(\alpha)} = \frac{1}{a - b\sqrt{2}} = \frac{a + b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} + \frac{b}{a^2 - 2b^2}\sqrt{2}$$

OK

$\boxed{\text{(4)の別証}}$ (0), (3) $\Rightarrow$ (4) を示す.

(0) $\sigma(a)=a$ $(a\in\mathbb{Q})$, (3) $\sigma(\alpha\beta)=\sigma(\alpha)\sigma(\beta)$ $(\alpha,\beta\in L)$ から

(4) $\sigma\left(\frac{1}{\alpha}\right)=\frac{1}{\sigma(\alpha)}$ $(\alpha\in L, \alpha\neq 0)$ を示そう.

$$\left.\begin{array}{l}\alpha\cdot\frac{1}{\alpha}=1\in\mathbb{Q} \text{ より, } \sigma\left(\alpha\cdot\frac{1}{\alpha}\right)=\sigma(1)\overset{(0)}{=}1. \\ (3) \text{ より, } \sigma\left(\alpha\cdot\frac{1}{\alpha}\right)=\sigma(\alpha)\sigma\left(\frac{1}{\alpha}\right).\end{array}\right\} \text{ ゆえに, } \sigma(\alpha)\sigma\left(\frac{1}{\alpha}\right)=1.$$

したがって, $\sigma\left(\frac{1}{\alpha}\right)=\frac{1}{\sigma(\alpha)}$. $\square$