「ガロア理論と類体論」資料

2014.7.18 玉川安騎男

定義０　S を集合とする。
(1) $\mathrm{id}_S : S \to S$ で恒等写像を表す：$\mathrm{id}_S(a) = a$ $(\forall a \in S)$
(2) $\sharp(S)$ で S の濃度（元の数）を表す。
(3) S 上の関係 $\sim$ とは、各 $a, b \in S$ に対し $a \sim b$ かどうかが定められていること。
S 上の関係 $\sim$ が同値関係とは、次の (i)-(iii) がみたされていること：

(i) $a \sim a$ $(\forall a \in S)$
(ii) $a \sim b \implies b \sim a$ $(\forall a, b \in S)$
(iii) $a \sim b,\ b \sim c \implies a \sim c$ $(\forall a, b, c \in S)$

S 上の同値関係 $\sim$ が与えられたとき、部分集合 $C \subset S$ が S の $\sim$ 同値類であるとは、次の (i)-(iii) がみたされていること：

(i) $C \neq \emptyset$
(ii) $a, b \in C \implies a \sim b$
(iii) $a \in C,\ b' \in S - C \implies a \not\sim b'$.

S の $\sim$ 同値類全体のなす集合を、$S/\sim$ と表す。

定義１　$(K, 0, 1, +, -, \cdot, ^{-1})$ が［あるいは、K が］（可換）体 $\overset{\text{def}}{\iff}$

K: 集合
$0, 1 \in K$ 元
$+ : K \times K \to K,\ (a, b) \mapsto a + b$
$- : K \to K,\ a \quad \mapsto -a$
$\cdot : K \times K \to K,\ (a, b) \mapsto a \cdot b$
$^{-1} : K - \{0\} \to K,\ a \mapsto a^{-1}$

であって、次の (i)–(ix) が成立

(i) $(a + b) + c = a + (b + c)$ $(\forall a, b, c \in K)$
(ii) $a + 0 = 0 + a = a$ $(\forall a \in K)$
(iii) $a + (-a) = (-a) + a = 0$ $(\forall a \in K)$
(iv) $a + b = b + a$ $(\forall a, b \in K)$
(v) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ $(\forall a, b, c \in K)$
(vi) $a \cdot 1 = 1 \cdot a = a$ $(\forall a \in K)$
(vii) $a \cdot b = b \cdot a$ $(\forall a, b \in K)$
(viii) $a \cdot (b + c) = a \cdot b + a \cdot c,\ (a + b) \cdot c = a \cdot c + b \cdot c$ $(\forall a, b, c \in K)$
(ix) $a \cdot a^{-1} = a^{-1} \cdot a = 1$ $(\forall a \in K - \{0\})$
(x) $1 \neq 0$

が成立するとき、K を体という。

定義２　$(K, 0, 1, +, -, \cdot)$ が［あるいは、K が］（可換）環 $\overset{\text{def}}{\iff}$

K: 集合
$0, 1 \in K$ 元
$+ : K \times K \to K,\ (a, b) \mapsto a + b$
$- : K \to K,\ a \quad \mapsto -a$
$\cdot : K \times K \to K,\ (a, b) \mapsto a \cdot b$

であって、定義１の (i)–(viii) が成立

定義３　L, L' を体とする。体の準同型 $\phi : L \to L'$ とは、写像 $\phi : L \to L'$ で、次をみたすもののことをいう。

$\phi(a + b) = \phi(a) + \phi(b)\ (\forall a, b \in L)$
$\phi(0) = 0$
$\phi(-a) = -\phi(a)\ (\forall a \in L)$
$\phi(a \cdot b) = \phi(a) \cdot \phi(b)\ (\forall a, b \in L)$
$\phi(1) = 1$

さらに、体の射 $\psi : L' \to L$ があって $\psi \circ \phi = \mathrm{id}_L,\ \phi \circ \psi = \mathrm{id}_{L'}$ がみたされるとき、$\phi : L \to L'$ を体の同型という。
同型 $L \to L'$ が存在するとき、L, L' は同型といい、$L \simeq L'$ と表す。

定義４　L を体とする。体の同型 $L \to L$ を、L の自己同型という。L の自己同型全体のなす集合を $\mathrm{Aut}(L)$ と書く。

定義５　体 K, L の間に包含関係 $L \supset K$ があり、L の $(0, 1, +, -, \cdot, ^{-1})$ を K に制限したものが K の $(0, 1, +, -, \cdot, ^{-1})$ になっているとき、「L/K は体の拡大である」「L は K の拡大体である」「K は L の部分体である」という。

定義６　K を体、L, L' を K の拡大体とする。K 準同型 $\phi : L \to L'$ とは、体の準同型 $\phi : L \to L'$ で、K に制限すると id_K となるものをいう。
さらに、ϕ が体の同型のとき、$\phi : L \to L'$ を K 同型という。
K 同型 $L \to L'$ が存在するとき、L, L' は K 同型といい、$L \underset{K}{\simeq} L'$ と表す。

定義７　L/K を体の拡大とする。体の K 同型 $L \to L$ を、L の K 自己同型という。L の K 自己同型全体のなす集合を $\mathrm{Aut}_K(L)$ と書く。

定義８　L/K を体の拡大とする。L が K ベクトル空間として有限次元のとき、L/K を有限次拡大という。このとき、$[L : K] = \dim_K(L)$ と書き、拡大 L/K の次数という。

定義９　L/K を体の有限次拡大とする。$\sharp(\mathrm{Aut}_K(L)) = [L : K]$ がみたされるとき、L/K をガロア拡大という。このとき、$\mathrm{Gal}(L/K) = \mathrm{Aut}_K(L)$ と書き、L/K のガロア群という。

定義１０　$(G, e, *, \iota)$ が［あるいは、G が］群 $\overset{\text{def}}{\iff}$

G: 集合
$e \in G$ 元
$* : G \times G \to G,\ (a, b) \mapsto a * b$
$\iota : G \to G,\ a \mapsto \iota(a)$

であって、次の (i)–(iii) が成立

(i) $(a * b) * c = a * (b * c)\ (\forall a, b, c \in G)$
(ii) $a * e = e * a = a\ (\forall a \in G)$
(iii) $a * \iota(a) = \iota(a) * a = e\ (\forall a \in G)$

さらに、

(iv) $a * b = b * a\ (\forall a, b \in G)$

もみたされるとき、$(G, e, *, \iota)$ は［あるいは、G は］アーベル群という。

定義１１　G, G' を群とする。群の準同型 $\phi : G \to G'$ とは、写像 $\phi : G \to G'$ で、次をみたすもののことをいう。

$\phi(a * b) = \phi(a) * \phi(b)\ (\forall a, b \in G)$
$\phi(e) = e$
$\phi(\iota(a)) = \iota(\phi(a))\ (\forall a \in G)$

さらに、群の準同型 $\psi : G' \to G$ があって $\psi \circ \phi = \mathrm{id}_G,\ \phi \circ \psi = \mathrm{id}_{G'}$ がみたされるとき、$\phi : G \to G'$ を群の同型という。
同型 $G \to G'$ が存在するとき、G, G' は同型といい、$G \simeq G'$ と表す。

定義１２　群 G, H の間に包含関係 $G \supset H$ があり、G の $(e, *, \iota)$ を H に制限したものが H の $(e, *, \iota)$ になっているとき、H は G の部分群であるという。

定義１３　群 G の部分群 H が与えられたとき、G の上の同値関係 $\sim$ を次のように定める：

$$a \sim b \overset{\text{def}}{\iff} a^{-1}b \in H$$

この同値関係による商集合 $G/\sim$ を G/H と表す。
さらに、G がアーベル群のときは、自然な全射 $G \to G/H$ が準同型になるような G/H の群構造が唯一つ存在する。これにより G/H を群と考えるとき、G/H を G の商群という。

定義１４　有理数体 $\mathbb{Q}$ の有限次拡大体を代数体という。

定義１５　K を代数体とするとき、

$$O_K \overset{\text{def}}{=} \{a \in K \mid \exists f(x) \in \mathbb{Z}[x] \text{: monic 多項式, s.t. } f(a) = 0\}$$

を、K の整数環という。

定義１６　R を環とし、$a, b, b' \in R$ とする。
(1) $a \mid b \overset{\text{def}}{\iff} \exists c \in R, \text{ s.t. } b = ca$
(2) $b \equiv b' \mod a \overset{\text{def}}{\iff} a \mid (b - b')$