

14 Galois cohomology

14.1 群の cohomology

定義 14.1. G : 群、 M : 加法 (Abel) 群で G は M に加群としての作用をしているとする。ここで以下のよ
うに G^n から M への写像全体の集合を $C^n (n \in \mathbb{Z}_{\geq 0})$ として定める。

$$C^n = C^n(G, M) := \{f : G^n \longrightarrow M\} = \text{Map}(G^n, M)$$

ただし $G^0 = \{e\}$ と考えることで $C^0 := M$ と定める。この C^n の各元を n コチェイン (cochain) という。
 C^n 上へは $f, g \in C^n$ に対して $(f + g)(x) := f(x) + g(x)$ と演算を定めることで C^n は加法群となる。

定義 14.2. C^n から C^{n+1} への以下のように定まる写像 ∂ を考える。

$$\begin{aligned} \partial &= \partial^n : C^n \longrightarrow C^{n+1} \\ f &\longmapsto \partial f \end{aligned}$$

ここで $\partial f : G^{n+1} \longrightarrow M$ は G が M へ作用していることに注意して

$$\begin{aligned} \partial f(g_1, \dots, g_{n+1}) &= g_1 f(g_2, \dots, g_{n+1}) \\ &\quad + \sum_{i=1}^n (-1)^i f(g_1, \dots, g_i g_{i+1}, \dots, g_{n+1}) \\ &\quad + (-1)^{n+1} f(g_1, \dots, g_n) \end{aligned}$$

と定める。このときこの $\partial (= \partial^n) : C^n(G, M) \longrightarrow C^{n+1}(G, M)$ は加法群の準同型になり、これを
 n 次のコバウンダリー (双対境界) 作用素 (coboundary operator) とよぶ。

命題 14.3. コバウンダリー作用素 ∂ に対して $\partial^{n+1} \circ \partial^n = 0$ が成り立つ。

Proof. $4 \leq n$ でまず考える。

$(\partial^{n+1} \circ \partial^n)(f)(g_1, \dots, g_{n+2}) = \partial^{n+1}(\partial^n f)(g_1, \dots, g_{n+2})$ なので $f' := \partial^n f$ として $\partial^{n+1} f'(g_1, \dots, g_{n+2})$
は

$$\begin{aligned} \partial^{n+1} f'(g_1, \dots, g_{n+2}) &= g_1 f'(g_2, \dots, g_{n+2}) \\ &\quad + \sum_{i=1}^{n+1} (-1)^i f'(g_1, \dots, g_i g_{i+1}, \dots, g_{n+2}) \\ &\quad + (-1)^{n+1} f'(g_1, \dots, g_{n+1}) \end{aligned}$$

である。 $f'(g_1, \dots, g_i g_{i+1}, \dots, g_{n+2}) = \partial^n f(g_1, \dots, g_i g_{i+1}, \dots, g_{n+2})$ を i の値によって計算する。

・ $i = 1$ のとき

$$\begin{aligned} \partial^n f(g_1 g_2, \dots, g_{n+2}) &= g_1 g_2 f(g_3, \dots, g_{n+2}) \\ &\quad + (-1)^1 f((g_1 g_2) g_3, g_4, \dots, g_{n+2}) \\ &\quad + \sum_{k=3}^{n+1} (-1)^{k-1} f(g_1 g_2, g_3, \dots, g_k g_{k+1}, \dots, g_{n+2}) \\ &\quad + (-1)^{n+1} f(g_1 g_2, g_3, \dots, g_n) \end{aligned}$$

・ $i = 2$ のとき

$$\begin{aligned}
\partial^n f(g_1, g_2 g_3, g_4, \dots, g_{n+2}) &= g_1 f(g_2 g_3, g_4, \dots, g_{n+2}) \\
&+ (-1)^1 f(g_1(g_2 g_3), g_4, \dots, g_{n+2}) \\
&+ (-1)^2 f(g_1, (g_2 g_3)g_4, g_5, \dots, g_{n+2}) \\
&+ \sum_{k=4}^{n+1} (-1)^{k-1} f(g_1, g_2 g_3, g_4, \dots, g_i g_{i+1}, \dots, g_{n+2}) \\
&+ (-1)^{n+1} f(g_1, g_2 g_3, g_4, \dots, g_{n+1})
\end{aligned}$$

・ $3 \leq i \leq n-1$ のとき

$$\begin{aligned}
\partial^n f(g_1, \dots, g_i g_{i+1}, \dots, g_{n+2}) &= g_1 f(g_2, \dots, g_i g_{i+1}, \dots, g_{n+2}) \\
&+ \sum_{k=1}^{i-2} (-1)^k f(g_1, \dots, g_k g_{k+1}, \dots, g_i g_{i+1}, \dots, g_{n+2}) \\
&+ (-1)^{i-1} f(g_1, \dots, g_{i-2}, g_{i-1}(g_i g_{i+1}), g_{i+2}, \dots, g_{n+2}) \\
&+ (-1)^i f(g_1, \dots, g_{i-1}, (g_i g_{i+1})g_{i+2}, g_{i+3}, \dots, g_{n+2}) \\
&+ \sum_{k=i+2}^{n+1} (-1)^{k-1} f(g_1, \dots, g_i g_{i+1}, \dots, g_k g_{k+1}, \dots, g_{n+2}) \\
&+ (-1)^{n+1} f(g_1, \dots, g_i g_{i+1}, \dots, g_{n+1})
\end{aligned}$$

・ $i = n$ のとき

$$\begin{aligned}
\partial^n f(g_1, \dots, g_n g_{n+1}, g_{n+2}) &= g_1 f(g_2, \dots, g_n g_{n+1}, g_{n+2}) \\
&+ \sum_{k=1}^{n-2} (-1)^k f(g_1, \dots, g_k g_{k+1}, \dots, g_n g_{n+1}, g_{n+2}) \\
&+ (-1)^{n-1} f(g_1, \dots, g_{n-1}(g_n g_{n+1}), g_{n+2}) \\
&+ (-1)^n f(g_1, \dots, g_{n-1}, (g_n g_{n+1})g_{n+2}) \\
&+ (-1)^{n+1} f(g_1, \dots, g_{n-1}, g_n g_{n+1})
\end{aligned}$$

・ $i = n+1$ のとき

$$\begin{aligned}
\partial^n f(g_1, \dots, g_{n+1} g_{n+2}) &= g_1 f(g_2, \dots, g_{n+1} g_{n+2}) \\
&+ \sum_{k=1}^{n-1} (-1)^k f(g_1, \dots, g_k g_{k+1}, \dots, g_n, g_{n+1} g_{n+2}) \\
&+ (-1)^n f(g_1, \dots, g_{n-1}, g_n(g_{n+1} g_{n+2})) \\
&+ (-1)^{n+1} f(g_1, \dots, g_n)
\end{aligned}$$

となる。

また、 $g_1 f'(g_2, \dots, g_{n+2})$ と $(-1)^{n+2} f'(g_1, \dots, g_{n+1})$ は以下のようになる。

$$\begin{aligned}
g_1 \partial^n f(g_2, \dots, g_{n+2}) &= g_1 (g_2 f(g_3, \dots, g_{n+2}) \\
&\quad + \sum_{i=2}^{n+1} (-1)^{i-1} f(g_2, \dots, g_i g_{i+1}, \dots, g_{n+2}) \\
&\quad + (-1)^{n+1} f(g_2, \dots, g_{n+1})) \\
(-1)^{n+2} \partial^n f(g_1, \dots, g_{n+1}) &= (-1)^{n+2} (g_1 f(g_2, \dots, g_{n+1}) \\
&\quad + \sum_{i=1}^n (-1)^i f(g_1, \dots, g_i g_{i+1}, \dots, g_{n+1}) \\
&\quad + (-1)^{n+1} f(g_1, \dots, g_n))
\end{aligned}$$

これを $\partial^{n+1}(\partial^n f)(g_1, \dots, g_{n+2})$ の式に代入すると

$$\begin{aligned}
\partial^{n+1}(\partial^n f)(g_1, \dots, g_{n+2}) = & \{g_1 g_2 f(g_3, \dots, g_{n+2}) \\
& + \sum_{i=2}^{n+1} (-1)^{i-1} g_1 f(g_2, \dots, g_i g_{i+1}, \dots, g_{n+2}) \\
& + (-1)^{n+1} g_1 f(g_2, \dots, g_{n+1})\} \\
& + (-1)^1 \{g_1 g_2 f(g_3, \dots, g_{n+2}) \\
& + (-1)^1 f((g_1 g_2) g_3, g_4, \dots, g_{n+2}) \\
& + \sum_{k=3}^{n+1} (-1)^{k-1} f(g_1 g_2, g_3, \dots, g_i g_{i+1}, \dots, g_{n+2}) \\
& + (-1)^{n+1} f(g_1 g_2, g_3, \dots, g_n)\} \\
& + (-1)^2 \{g_1 f(g_2 g_3, g_4, \dots, g_{n+2}) \\
& + (-1)^1 f(g_1 (g_2 g_3), g_4, \dots, g_{n+2}) \\
& + (-1)^2 f(g_1, (g_2 g_3) g_4, g_5, \dots, g_{n+2}) \\
& + \sum_{k=4}^{n+1} (-1)^{k-1} f(g_1, g_2 g_3, g_4, \dots, g_i g_{i+1}, \dots, g_{n+2}) \\
& + (-1)^{n+1} f(g_1, g_2 g_3, g_4, \dots, g_{n+1})\} \\
& + \sum_{i=3}^{n-1} (-1)^i \{g_1 f(g_2, \dots, g_i g_{i+1}, \dots, g_{n+2}) \\
& + \sum_{k=1}^{i-2} (-1)^k f(g_1, \dots, g_k g_{k+1}, \dots, g_i g_{i+1}, \dots, g_{n+2}) \\
& + (-1)^{i-1} f(g_1, \dots, g_{i-2}, g_{i-1} (g_i g_{i+1}), g_{i+2}, \dots, g_{n+2}) \\
& + (-1)^i f(g_1, \dots, g_{i-1}, (g_i g_{i+1}) g_{i+2}, g_{i+3}, \dots, g_{n+2}) \\
& + \sum_{k=i+2}^{n+1} (-1)^{k-1} f(g_1, \dots, g_i g_{i+1}, \dots, g_k g_{k+1}, \dots, g_{n+2}) \\
& + (-1)^{n+1} f(g_1, \dots, g_i g_{i+1}, \dots, g_{n+1})\} \\
& + \{g_1 f(g_2, \dots, g_n g_{n+1}, g_{n+2}) \\
& + \sum_{k=1}^{n-2} (-1)^k f(g_1, \dots, g_k g_{k+1}, \dots, g_n g_{n+1}, g_{n+2}) \\
& + (-1)^{n-1} f(g_1, \dots, g_{n-1} (g_n g_{n+1}), g_{n+2}) \\
& + (-1)^n f(g_1, \dots, g_{n-1}, (g_n g_{n+1}) g_{n+2}) \\
& + (-1)^{n+1} f(g_1, \dots, g_{n-1}, g_n g_{n+1})\} \\
& + \{g_1 f(g_2, \dots, g_{n+1} g_{n+2}) \\
& + \sum_{k=1}^{n-1} (-1)^k f(g_1, \dots, g_k g_{k+1}, \dots, g_n, g_{n+1} g_{n+2}) \\
& + (-1)^n f(g_1, \dots, g_{n-1}, g_n (g_{n+1} g_{n+2})) \\
& + (-1)^{n+1} f(g_1, \dots, g_n)\} \\
& + \{(-1)^{n+2} (g_1 f(g_2, \dots, g_{n+1}) \\
& + \sum_{i=1}^n (-1)^i f(g_1, \dots, g_i g_{i+1}, \dots, g_{n+1}) \\
& + (-1)^{n+1} f(g_1, \dots, g_n))\}
\end{aligned}$$

□

定義 14.4. 以下のように $n \in \mathbb{Z}_{\geq 0}$ に対して定める Z^n を n -th (次) コサイクル (双対輪体) といい、 B^n を n -th (次) コバウンダリー (境界輪体) という。

$$\begin{aligned} Z^n &= Z^n(G, M) := \ker(\partial^n) \\ B^n &= B^n(G, M) := \text{Im}(\partial^{n-1}) \end{aligned}$$

ただし $B^0 := 0$ とする。このとき命題 (14.3) から $\partial^n \circ \partial^{n-1} = 0$ なので $\partial^n(\text{Im}(\partial^{n-1})) = 0$ より $B^n \subset Z^n$ が成り立っている。よって剰余群 Z^n/B^n が定義できて

$$H^n = H^n(G, M) := Z^n(G, M)/B^n(G, M)$$

を G の M 係数の n -th (次) コホモロジー群 (cohomology) という。

例 14.5. $n = 0$ のときのコホモロジー群を考える。 $Z^0 = \ker(\partial^0)$ であり、定義から $\partial^0 : C^0(= M) \rightarrow C^1, x \mapsto \partial^0 x$ と、 $\partial^0 x(g) = gx - x$ なので $Z^0 = \{gx - x = 0 \Leftrightarrow gx = x | x \in M, \forall g \in G\}$ となる。 gx は M の元への G の作用でありそれがどんな $g \in G$ でも x になるから M の中で G によって固定されるので $Z^0 = M^G$ である。 $B^0 := 0$ だったのでコホモロジー群 H^0 は $H^0 = Z^0/B^0 = M^G$ である。

例 14.6. $n = 1$ のときのコホモロジー群を考える。 $Z^1 = \ker(\partial^1)$ で $\partial^1 : C^1 \rightarrow C^2, f \mapsto \partial^1 f$ となって $\partial^1 f(g_1, g_2) = g_1 f(g_2) - f(g_1 g_2) + f(g_1)$ となるから $Z^1 = \{f \in C^1 | g_1 f(g_2) - f(g_1 g_2) + f(g_1) = 0 \Leftrightarrow f(g_1 g_2) = g_1 f(g_2) + f(g_1), \forall g_1, g_2 \in G\}$ となる。 $B^1 = \text{Im}(\partial^0) = \{\partial^0 x | x \in M, \partial^0 x(g) = gx - x\}$ となっている。いま作用が $G \times M \rightarrow M, (g, x) \mapsto gx = x$ として自明なものであるときを考えると $Z^1 = \{f \in C^1 | f(g_1 g_2) = f(g_1) + f(g_2), \forall g_1, g_2 \in G\}$ でこれは G から M への群準同型なので $Z^1 = \text{Hom}_{\#}(G, M)$ となる。 $B^1 = \{\partial^0 x | x \in M, \partial^0 x(g) = gx - x = x - x = 0\} = 0$ となるから $n = 1$ のときのコホモロジー群 H^1 は $H^1 = \text{Hom}_{\#}(G, M)$ となる。

Fact 14.7. G 加群 $M_i (1 \leq i \leq 3)$ に対して以下の加群の完全列が存在するとする。

$$0 \rightarrow M_1 \rightarrow M_2 \rightarrow M_3 \rightarrow 0$$

このとき以下のような無限の長さの完全列が存在する。

$$\begin{aligned} 0 &\rightarrow H^0(G, M_1) \rightarrow H^0(G, M_2) \rightarrow H^0(G, M_3) \\ &\rightarrow H^1(G, M_1) \rightarrow H^1(G, M_2) \rightarrow H^1(G, M_3) \\ &\rightarrow H^2(G, M_1) \rightarrow \dots \end{aligned}$$

14.2 Galois cohomology

定義 14.8. A を群 G が作用する Abel とは限らない群とする。このとき例 (14.5) より 0 次のコホモロジー群を $H^0(G, A) := A^G$ としても矛盾しないのでそのように定義する。

また、 $\alpha \in C^1(G, A)$ を

$$\begin{aligned} \alpha &: G \rightarrow A \\ g &\mapsto \alpha_g \end{aligned}$$

と定めると、 A の演算を非可換性を表すため積で書くことにすると

$$\begin{aligned}\partial^1(\alpha)(g, h) &= g\alpha_h \cdot \alpha_{gh}^{-1} \cdot \alpha_g \\ \alpha \in Z^1 = \ker(\partial^1) &\Leftrightarrow \forall g, h \in G, g\alpha_h \cdot \alpha_{gh}^{-1} \cdot \alpha_g = 1 \\ &\Leftrightarrow \alpha_{gh}^{-1} \cdot \alpha_g = (g\alpha_h)^{-1} \\ &\Leftrightarrow \alpha_g(g\alpha_h) = \alpha_{gh}\end{aligned}$$

となるから例 (14.6) より 1 次のコサイクルは $Z^1 = \{\alpha \in C^1 \mid \forall g, h \in G, \alpha_{gh} = \alpha_g \cdot g\alpha_h\}$ となるのでそのように定義する。

定義 14.9. 群 G とそれが作用する非可換群 A の 1 次コサイクル Z^1 について $\alpha, \beta \in Z^1$ が cohomologous ($\alpha \sim \beta$) とは

$$\exists a \in A \text{ s.t. } \forall g \in G, \beta_g = a^{-1} \cdot \alpha_g \cdot ga$$

となることであり、これは同値関係になる。 G が恒等的な作用をするのであれば $ga = a$ よりこれは α_g と β_g が共役な関係になってることと同じになる。つまり共役から ga の分だけねじれているともみれる。

Proof. 同値関係になることをしめす。

まず、 $\forall g \in G$ と $\forall a \in A$ について $(ga)^{-1} = ga^{-1}$, $g(1) = 1$ が成り立つことを示す。定義から G が A に加群のように作用するので $g(1) = g(1 \cdot 1) = g(1) \cdot g(1)$ から $g(1) = g(1) \cdot g(1)^{-1} = 1$ より成立。これを用いれば $1 = g(1) = g(a \cdot a^{-1}) = ga \cdot ga^{-1} \Leftrightarrow (ga)^{-1} = ga^{-1}$ より成立。

・反射律

$a = 1 \in A$ としてとれば $\alpha_g = 1 \cdot \alpha_g \cdot 1 = 1^{-1} \cdot \alpha_g \cdot g(1)$ が任意の $g \in G$ で成り立つので $\alpha \sim \alpha$ より反射律が成り立つ。

・対称律

$\alpha \sim \beta$ のときある $a \in A$ で $\beta_g = a^{-1} \cdot \alpha_g \cdot ga$ となっているので逆元をそれぞれかけて $\alpha_g = a \cdot \beta_g \cdot (ga)^{-1}$ となっていて上で述べたことより $b := a^{-1} \in A$ を取る時 $(ga)^{-1} = ga^{-1} = gb$ から $\alpha_g = b^{-1} \cdot \beta_g \cdot gb$ となるので $\beta \sim \alpha$ より対称律がなりたつ。

・推移律

$\alpha \sim \beta, \beta \sim \gamma$ となっているとするとある $a, b \in A$ で $\beta_g = a^{-1} \cdot \alpha_g \cdot ga$ と $\gamma_g = b^{-1} \cdot \beta_g \cdot gb$ となっている。 β_g に代入すると $\gamma_g = b^{-1} \cdot (a^{-1} \cdot \alpha_g \cdot ga) \cdot gb = (b^{-1}a^{-1}) \cdot \alpha_g \cdot (ga \cdot gb) = (ab)^{-1} \cdot \alpha_g \cdot g(ab)$ となり $ab \in A$ なので $\alpha \sim \gamma$ から推移律が成り立つ。□

定義 14.10. Galois cohomology とは有限次 Galois 拡大 L/K があるとき $G := \text{Gal}(L/K)$ としてこれが作用する群 M についてのコホモロジー群 $H^n(G, M)$ のことである。とくに M として $L, L^n, GL_n(L)$ 等を考える。ただし $GL_n(L)$ は L 成分の n 次正則行列全体の積による群であり、一般に L に作用する群を G としたとき $\sigma \in G$ は $X = (x_{ij}) \in M_n(L) := (n \text{ 次正方行列全体の集合})$ に対して $\sigma(X) := (\sigma(x_{ij}))$ と定める。

命題 14.11. 体 L と有限群 $G \subset \text{Aut}(L)$ について以下が成り立つ。

- (1) $\forall n \in \mathbb{Z}_{\geq 1}$ について $H^n(G, L) = 0$ となる。
- (2) $\forall n \in \mathbb{Z}_{\geq 1}$ について $H^1(G, GL_n(L)) = 1$ となる。とくに $H^1(G, L^\times) = 1$ となる。これは一つの成分だけの正則行列が $GL_1(L) = L^\times$ となることからすぐ導かれる。

Proof. (2)

一般に定義 (14.4) から $B^1 \subset Z^1$ だから $Z^1 \subset B^1$ を示せば $B^1 = Z^1$ から $H^1 = Z^1/B^1 = 1$ が示される。
 まず、0 次コバウンダリー作用素 ∂^0 に対して $B^1 = \text{Im}(\partial^0) = \{\partial^0 X | X \in GL_n(L)\}$ となっていて例 (14.6) の B^1 から $\partial^0 X$ は $GL_n(L)$ での演算は積であることに注意すれば

$$\begin{aligned}\partial^0 X : G &\longrightarrow GL_n(L) \\ g &\longmapsto \partial^0 X(g) = gX \cdot X^{-1}\end{aligned}$$

となっている。したがって $\forall \alpha \in Z^1$ に対して $\forall g \in G, \alpha_g = \partial^0 X(g) = gX \cdot X^{-1}$ となる $X \in GL_n(L)$ が存在すればよい。いま、ある $X \in GL_n(L)$ について

$$b := \sum_{h \in G} \alpha_h \cdot h(X)$$

と定義すると $b \in GL_n(L)$ である。 $h \in G \subset \text{Aut}(L)$ より Dedekind の補題 (??) から M を L とみればその対偶を取ることで $\alpha_h \in GL_n(L)$ はより任意の $h \in G$ で $\alpha_h \neq 0$ となるからある $x_{ij} \in L$ が存在して $\sum_{h \in G} \alpha_h \cdot hx_{ij} \neq 0$ となる。 \square