

A generalization of Hilbert's theorem 94

都立大・理 鈴木 浩志 (Hiroshi Suzuki)

次の定理を示す。

定理 有限次代数体 k の不分岐 Abel 拡大 K について、 K で単項になる k の ideal 類の個数は、拡大次数 $[K:k]$ で、割りきれれる。

capitulation homomorphism は、Galois 群の group-transfer に言い換えられるので、次を示せばじゅうぶんである。

定理 (The group-theoretical version) 有限群 H の、交換子群 H^c を含む部分群 N について、group-transfer $V_{H \rightarrow N}: H^{ab} \rightarrow N^{ab}$ の kernel の位数は、 $[H:N]$ で割りきれれる。

Hilbert の定理 94 や principal ideal theorem は、上から容易に従う。

1.

群 G について、その交換子群を G^c 、群環 $\mathbb{Z}[G]$ の augmentation ideal を、 I_G とかく。また、

$$\begin{aligned} G^{ab} &= G/G^c, \\ Tr_G &= \sum_{g \in G} g \in \mathbb{Z}[G], \\ A_G &= \mathbb{Z}[G]/\langle Tr_G \rangle \end{aligned}$$

とおく。 $\mathbb{Z}[G]$ -加群 M について、 M の G -不変な元全体からなる部分加群を M^G とかく。また、 $v_1, \dots, v_m \in M$ で生成された $\mathbb{Z}[G]$ -部分加群を、 $\langle v_1, \dots, v_m \rangle$ とかくことにする。有限集合 S の元の個数を $\#S$ とかく。

補題 1 有限 Abel 群 G 上、一つ元で生成された有限位数の加群 M について、 $H^{-1}(G, M)$ の位数は、 $H^0(G, M)$ の位数を割りきる。

先に次の事実を示す。

Fact 有限 Abel 群 G 上の有限位数の加群 N について、 $\sharp N/I_G N \cdot N^G = 0$ 。

$$N/I_G N = \bigoplus_{i=1}^r \mathbb{Z}/q_i \mathbb{Z}$$

とし、 $x_i \in N$ ($i = 1, \dots, r$) を、右辺の i -番目の生成元にうつるようにとり (i.e. $x_i \bmod N = (0, \dots, 0, 1, 0, \dots, 0)$)、 $y_i = q_i \cdot x_i$ ($i = 1, \dots, r$) とおく。また、

$$I_G N = \langle z_1, \dots, z_{r'} \rangle$$

とし、

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_r \\ z_1 \\ \vdots \\ z_{r'} \end{pmatrix}, \quad y = \begin{pmatrix} y_1 \\ \vdots \\ y_r \\ z_1 \\ \vdots \\ z_{r'} \end{pmatrix} \in \bigoplus^{r+r'} N$$

とおく。この時、もちろん対角行列

$$Q = \begin{pmatrix} q_1 & & & & 0 \\ & \ddots & & & \\ & & q_r & & \\ & & & 1 & \\ & & & & \ddots \\ 0 & & & & & 1 \end{pmatrix}$$

により、 $y = Q \cdot x$ であるが、

$$N = \langle x_1, \dots, x_r, z_1, \dots, z_{r'} \rangle$$

であることに注意すると、ある I_G -係数行列 $J \in M(r+r', I_G)$ が存在して、 $y = J \cdot x$ と書けることがわかる。よって、 $(Q - J) \cdot x = 0$ 。

$Q - J$ の余因子行列を、左からかければ、

$$\det(Q - J) \cdot x = 0 \quad \text{in} \quad \bigoplus^{r+r'} N.$$

さらに、 $\det(Q - J) \equiv q_1 \cdot \dots \cdot q_r \equiv \#N/I_G N \bmod I_G$ であるから、 $I_G \cdot N^G = 0$ より、Fact がわかる。

補題 1 の証明。

Fact で、 N を、 M の Pontrjagin dual $N = M^\wedge$ とすれば、

$$\#M^G \cdot M/I_G M = 0$$

が出る。ここで、仮定から、 $M/I_G M$ は巡回群である。よって、上は、

$$\#M/I_G M \mid \#M^G$$

を示している。この両辺を、 $M/\text{Ker}(Tr_G : M \rightarrow M) \cong Tr_G M$ の位数で割れば、補題 1 が、わかる。

補題 2 位数 n の有限 Abel 群 G に対して、 $A_G = \mathbb{Z}[G]/(Tr_G)$ と書いた時、 $\bigoplus_{m=1}^{m-1} A_G \otimes_{\mathbb{Z}} \mathbb{Q}$ の、 m 個の元で生成された $\mathbb{Z}[G]$ -部分加群 Y について、 $Y/I_G Y$ の位数は、 n^{m-1} を割りきる。

証明。

Y の生成元を、 $\{y_1, \dots, y_m\}$ とする。 $A_G \otimes_{\mathbb{Z}} \mathbb{Q}$ の、各極大 ideal $\mathfrak{m}$ に対して、 $c_{\mathfrak{m}} \in A_G \setminus \mathfrak{m}$ を、 $\mathfrak{m}$ 以外の全ての $A_G \otimes_{\mathbb{Z}} \mathbb{Q}$ の極大 ideal に含まれる (すなわち、 $\mathfrak{m}$ 以外の極大 ideal での成分が 0 になる) ようにとる。この時、もし、ある $\mathfrak{m}$ について、

$$(\langle y_1, \dots, y_{m-1} \rangle \otimes_{\mathbb{Z}} \mathbb{Q})_{\mathfrak{m}} \neq (Y \otimes_{\mathbb{Z}} \mathbb{Q})_{\mathfrak{m}}$$

だったとすると、左辺の $(A_G \otimes_{\mathbb{Z}} \mathbb{Q})_{\mathfrak{m}}$ -線形空間の次元は、 $m-1$ より小さい。よって、この場合、 $(A_G \otimes_{\mathbb{Z}} \mathbb{Q})_{\mathfrak{m}}$ 上 無駄な生成元がある。その添数を $i = i(\mathfrak{m})$ とすると、

$$(\langle y_1, \dots, y_{i-1}, y_i + c_{\mathfrak{m}} y_m, y_{i+1}, \dots, y_{m-1} \rangle \otimes_{\mathbb{Z}} \mathbb{Q})_{\mathfrak{m}} = (Y \otimes_{\mathbb{Z}} \mathbb{Q})_{\mathfrak{m}}$$

である。そこで、 i -番目の生成元 y_i を、 $y_i + c_m y_m$ と取り換えれば、

$$(\langle y_1, \dots, y_{m-1} \rangle \otimes_{\mathbb{Z}} \mathbb{Q})_m = (Y \otimes_{\mathbb{Z}} \mathbb{Q})_m$$

とできる。この取り換えは、他の m には影響しないから、全ての m について、上が成立する、つまり

$$\langle y_1, \dots, y_{m-1} \rangle \otimes_{\mathbb{Z}} \mathbb{Q} = Y \otimes_{\mathbb{Z}} \mathbb{Q}$$

としてよいことがわかる。

次に、 $\bigoplus^{m-1} A_G \otimes_{\mathbb{Z}} \mathbb{Q}$ の標準的な番目の生成元 $\bar{e}_i$; $i = 1, \dots, m-1$ を、 y_i ; $i = 1, \dots, m-1$ にうつす $\mathbb{Z}[G]$ -準同型を、 $\pi: \bigoplus^{m-1} A_G \otimes_{\mathbb{Z}} \mathbb{Q} \rightarrow Y \otimes_{\mathbb{Z}} \mathbb{Q}$ と書く。さらに、 $y \in \bigoplus^{m-1} A_G \otimes_{\mathbb{Z}} \mathbb{Q}$ を、 $\pi(y) = y_m$ ととって、

$$Y' = \langle \bar{e}_1, \dots, \bar{e}_{m-1}, y \rangle \subseteq \bigoplus^{m-1} A_G \otimes_{\mathbb{Z}} \mathbb{Q}$$

とおく。すると $\pi(Y') = Y$ であるから、 $Y/I_G Y$ の位数は、 $Y'/I_G Y'$ の位数を割りきる。そこで、 Y を Y' と取り換えれば、 $i = 1, \dots, m-1$ について

$$y_i = \bar{e}_i$$

は、 $\bigoplus^{m-1} A_G$ の標準的な i -番目の生成元で、最後の

$$y_m = y$$

は、 $\bigoplus^{m-1} A_G \otimes_{\mathbb{Z}} \mathbb{Q}$ の任意に与えられた元としてよいことがわかる。1 を、

$$e = 1 - 1/n \cdot \text{Tr}_G = \sum_{g \in G} -1/n \cdot (g - 1)$$

にうつすことにより、自然に $A_G \otimes_{\mathbb{Z}} \mathbb{Q}$ を、 $\mathbb{Q}[G]$ の直和因子 $I_G \otimes_{\mathbb{Z}} \mathbb{Q}$ と、同一視することにする。

$$\begin{aligned} pr: \bigoplus^{m-1} A_G \otimes_{\mathbb{Z}} \mathbb{Q} &\longrightarrow \bigoplus^{m-1} A_G \otimes_{\mathbb{Z}} \mathbb{Q} / \bigoplus^{m-1} I_G \\ &= \bigoplus^{m-1} I_G \otimes_{\mathbb{Z}} \mathbb{Q} / \mathbb{Z} \end{aligned}$$

を、自然な射影とする。容易に、

$$(\bigoplus^{m-1} I_G \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z})^G = \langle pr(\bar{e}_1), \dots, pr(\bar{e}_{m-1}) \rangle \cong \bigoplus^{m-1} \mathbb{Z}/n\mathbb{Z}$$

がわかる。特に、 $I_G \langle pr(\bar{e}_1), \dots, pr(\bar{e}_{m-1}) \rangle = 0$ である。そこで、 M を、一つ
の元 $pr(y)$ で生成された、 $\bigoplus^{m-1} I_G \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z}$ の有限位数の $\mathbb{Z}[G]$ -部分加群とす
ると、

$$\begin{aligned} & \#Y/I_G Y \\ &= \#pr(Y)/I_G pr(Y) \\ &= \#(M + \langle pr(\bar{e}_1), \dots, pr(\bar{e}_{m-1}) \rangle)/I_G M \\ &= \#(M + (\bigoplus^{m-1} I_G \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z})^G)/I_G M \\ &= \#M/I_G M \cdot \#(M + (\bigoplus^{m-1} I_G \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z})^G)/M \\ &= \#M/I_G M \cdot \#(\bigoplus^{m-1} I_G \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z})^G / \#M \cap (\bigoplus^{m-1} I_G \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z})^G \\ &= n^{m-1} \cdot \#H^{-1}(G, M) / \#H^0(G, M). \end{aligned}$$

となって、補題 1 により、補題 2 が示される。

2.

m を自然数とし、 $\tau: \bigoplus^m \mathbb{Z}[G] \longrightarrow I_G$ を、cokernel が有限の $\mathbb{Z}[G]$ -準同型と
する。 $I_G \text{Im} \tau$ の I_G の中での指数も有限である。

$$0 \longrightarrow \text{Ker} \tau \cap \bigoplus^m I_G \longrightarrow \bigoplus^m I_G \longrightarrow I_G \text{Im} \tau \longrightarrow 0$$

は exact で、 $I_G \otimes_{\mathbb{Z}} \mathbb{Q} = A_G \otimes_{\mathbb{Z}} \mathbb{Q}$ は、 $\mathbb{Q}$ の有限次拡大の有限直和であるか
ら、

(2.1)

$$\begin{aligned} & (\text{Ker} \tau \cap \bigoplus^m I_G) \otimes_{\mathbb{Z}} \mathbb{Q} \\ & \cong \bigoplus^{m-1} I_G \otimes_{\mathbb{Z}} \mathbb{Q} = \bigoplus^{m-1} A_G \otimes_{\mathbb{Z}} \mathbb{Q} \end{aligned}$$

特に、補題 2 は、 $\bigoplus^{m-1} A_G \otimes_{\mathbb{Z}} \mathbb{Q}$ の代わりに、 $\text{Ker } \tau \cap \bigoplus^m I_G$ としても、成立する。

ここで、次の補題を示す。

補題 3 自然数 t_i と、 $u_i \equiv t_i \cdot e_i \pmod{\bigoplus^m I_G}$ をみたす $\text{Ker } \tau$ の元 u_i が、 $i = 1, \dots, m$ について、与えられているとする。 $(e_i$ は、 $\bigoplus^m \mathbb{Z}[G]$ の、標準的な i -番目の生成元。) $U = \langle u_1, \dots, u_m \rangle$ 、 $W_0 = \bigoplus^m \mathbb{Z}[G]/U$ と、おいた時、 $H^{-1}(G, W_0)$ の位数は、 G の位数 n で、割りきれれる。

証明。

$$\begin{aligned} H^{-1}(G, W_0) &\cong H^0(G, U) \\ &\cong H^0(G, nU) \\ &\cong H^{-1}(G, \bigoplus^m \mathbb{Z}[G]/nU) \end{aligned}$$

であるから、 U の代わりに、 nU とすることにより、全ての i について、 t_i は n で割りきれれるとしてよい。 $d_i = t_i/n$ とおく。

$\text{Tr}_G \equiv n \pmod{I_G}$ であるから、

$$\begin{aligned} H^{-1}(G, W_0) &= \text{Ker}(\text{Tr}_G : W_0/I_G W_0 \longrightarrow W_0) \\ &= \text{Ker}(\text{Tr}_G|_{n(W_0/I_G W_0)} : n(W_0/I_G W_0) \longrightarrow W_0) \end{aligned}$$

がわかる。ここで、 ${}_n A = \{a \in A \mid na = 0\}$ 。また、 $n \mid t_i$ としたから、 ${}_n(W_0/I_G W_0) \cong \bigoplus^m \mathbb{Z}/n\mathbb{Z}$ で、これは、 $d_i \cdot e_i$; $i = 1, \dots, m$ により、生成されている。各 $i = 1, \dots, m$ について、 $y_i = d_i \cdot \text{Tr}_G \cdot e_i - u_i$ とおき、

$$Y = \langle y_1, \dots, y_m \rangle \quad (\subseteq \bigoplus^m I_G \cap \text{Ker } \tau)$$

とかくと、明らかに、 $I_G Y = I_G U$ である。さらに、 u_i についての条件から、

$$\begin{aligned} U/U \cap \bigoplus^m I_G &\cong U + \bigoplus^m I_G / \bigoplus^m I_G \\ &\cong \bigoplus^m \mathbb{Z} \cong U/I_G U \end{aligned}$$

となって、 $U \cap \bigoplus^m I_G = I_G U = I_G Y$ であることがわかる。よって、同型

$$\begin{aligned} (\text{Ker } \tau \cap (U + \bigoplus^m I_G))/U &\cong \text{Ker } \tau \cap \bigoplus^m I_G / U \cap \bigoplus^m I_G \cap \text{Ker } \tau \\ &= (\text{Ker } \tau \cap \bigoplus^m I_G)/I_G Y \end{aligned}$$

により、次の可換図式がえられる。

$$\begin{array}{ccc} {}_n(W_0/I_G W_0) & \xrightarrow{\text{Tr}_G} & (\text{Ker } \tau \cap (U + \bigoplus^m I_G))/U \hookrightarrow \text{Ker } \tau/U \\ \parallel & & \uparrow \cong \\ \bigoplus^m \mathbb{Z}/n\mathbb{Z} & \xrightarrow{\eta} & \text{Ker } \tau \cap \bigoplus^m I_G / I_G Y \\ & & \uparrow \\ & & Y/I_G Y \end{array}$$

ここで、 η は、 $\bigoplus^m \mathbb{Z}/n\mathbb{Z}$ の標準的な i -番目の生成元 $(0, \dots, 0, 1, 0, \dots, 0)$ を、 $y_i \bmod I_G Y$ にうつす、 $\mathbb{Z}[G]$ -準同型。従って、

$$H^{-1}(G, W_0) \cong \text{Ker } \eta$$

がわかる。この時、 Y が、上の、(2.1) の後半の条件を満たしていることに、注意すれば、 $\#Y/I_G Y$ は、 n^{m-1} を、割りきることがわかる。

$$\begin{aligned} \#H^{-1}(G, W_0) &= \# \text{Ker } \eta \\ &= n^m / \#(Y/I_G Y) \end{aligned}$$

であるから、 $H^{-1}(G, W_0)$ の位数は n で割りきれれる。

3. 定理の証明

$G = H/N$ とかく。 $V_{H \rightarrow N} = V_{H \rightarrow N'} \circ V_{N' \rightarrow N}$ であるから、 G は、ある素数 p について、Abel p -群としてよい。 $n = \#G$ とおく。

$(f_{g,h})$ を、群拡大

$$1 \longrightarrow N^{ab} \longrightarrow H/N^c \longrightarrow G \longrightarrow 1$$

の cohomology 類を与える 2-cocycle とする。Artin の splitting module W は、 $\{x_g \mid g \in G \setminus \{1\}\}$ を、 $G \setminus \{1\}$ で parametrize された symbol として、

$$W = N^{ab} \oplus \left(\bigoplus_{g \in G \setminus \{1\}} \mathbb{Z} \cdot x_g \right)$$

に、 G の作用を

$$g \cdot x_h = x_{g \cdot h} - x_g + f_{g,h} \quad x_1 = 1 \quad (g, h \in G)$$

で与えて定義される。この時、各 $g \in G \setminus \{1\}$ について、 $g - 1 \in I_G$ を、 x_g に、うつす写像により、exact

$$0 \longrightarrow N^{ab} \longrightarrow W \longrightarrow I_G \longrightarrow 0$$

がえられ、さらに $W/I_G W \cong H^{ab}$ で、trace homomorphism $Tr_G: W/I_G W \longrightarrow N^{ab}$ は、目的の group-transfer $V_{H \rightarrow N}: H^{ab} \longrightarrow N^{ab}$ に、一致することがわかる (Artin-Tate, Class Field Theory 参照)。従って、 $\#H^{-1}(G, W) \geq n$ を示せばよいことがわかる。よって、次を示せば十分である。

Fact 補題 3 のタイプの W_0 から、 W への $\mathbb{Z}[G]$ -準同型 $\psi: W_0 \longrightarrow W$ で、 G -不変な剰余の p -part に、同型

$$\bar{\psi}_p: (W_0/I_G W_0)_p \longrightarrow (W/I_G W)_p$$

を、引き起こすものが存在する。

証明。

$$H^{ab} = W/I_G W \cong \bigoplus_{i=1}^m \mathbb{Z}/q_i \mathbb{Z}$$

とかく。 $\bigoplus \mathbb{Z}[G]$ の i -番目の生成元 $e_i = (0, \dots, 0, 1, 0, \dots, 0)$ を、 $\bigoplus_{i=1}^m \mathbb{Z}/q_i \mathbb{Z}$ の i -番目の生成元 $h_i = (0, \dots, 0, 1, 0, \dots, 0)$ の代表にうつすような、 $\mathbb{Z}[G]$ -準同型 $\varphi: \bigoplus \mathbb{Z}[G] \longrightarrow W$ を、一つとると、次の可換図式がえられる。

$$\begin{array}{ccccccc} 0 & \longrightarrow & \text{Ker } \text{nat} \circ \varphi & \longrightarrow & \bigoplus^m \mathbb{Z}[G] & \xrightarrow{\text{nat} \circ \varphi} & I_G \\ & & \downarrow & & \downarrow \varphi & & \parallel \\ 0 & \longrightarrow & N^{ab} & \longrightarrow & W & \xrightarrow{\text{nat}} & I_G \longrightarrow 0 \end{array}$$

さらに、中山の補題により、 φ の (p) での局所化は、全射である。すなわち、 φ の cokernel は、 p と素な有限位数 s の $\mathbb{Z}[G]$ -加群である。よって、各 $i = 1, \dots, m$ について、 $u_i \in \text{Ker } \varphi$ が、 $u_i \equiv s \cdot q_i \cdot e_i \pmod{\bigoplus I_G}$ ととれる。 $U =$

$\langle u_1, \dots, u_m \rangle$ 、 $W_0 = \bigoplus^m \mathbb{Z}[G]/U$ とおき、 ψ を、 φ で引き起こされた $\mathbb{Z}[G]$ -準同型 とすると、明らかに、 ψ は、

$$\bar{\psi}_p : (W_0/I_G W_0)_p \longrightarrow (W/I_G W)_p$$

を引き起こす。さらに、 $\tau = \text{nat} \circ \varphi$ 、各 i について $t_i = s \cdot q_i$ とおけば、これらが、求めるものである。

以上で定理が示された。

注意 上の証明を逆にたどれば、少なくとも、各 q_i が全て n で割りきれた時は、丁度 $\# \text{Ker } V_{H \rightarrow N} = [H : N]$ となる有限群 H が、存在することがわかる。

補題 1 の証明が、わかりやすくなっているのは、岩澤先生のおかげである。この場をかりて感謝したい。