体拡大のテンソル積による特徴付けとGrothendieckのGalois理論

> 本稿では、体の代数拡大（有限次拡大、分離拡大、正規拡大、Galois拡大）といった基本的な概念を、**「体のテンソル積 (tensor product)」** の視点から特徴付ける手法について解説します。
>
> 通常のGalois理論の基本定理の証明では、ArtinやDedekindによる線形代数的な「拡大次数の不等式評価」が鍵となります。しかし、テンソル積による特徴付けを用いると、この複雑な評価を回避し、「環のイデアルによる剰余」や「冪等元による直積分解」といった純粋に可換環論的・幾何学的な操作のみで、Galois対応を鮮やかに証明することができます。これは、代数幾何学におけるエタール基本群などへと繋がる **GrothendieckのGalois理論** の最も基礎的なアイデアです。
>
> 数学的な命題や証明は厳密さを期すため「だ・である調」で記述し、合間の解説は親しみやすいように「です・ます調」で記述しています。

1. 基礎概念の準備

まずは、本稿で用いる体論と環論の基本概念を整理しておきましょう。

定義 1.1 (体の拡大に関する諸概念)

K を体とし、L をその拡大体とする。

- **有限次拡大 (finite extension):** L が K-ベクトル空間として有限次元であること。その次元を $[L:K]$ で表す。
- **代数拡大 (algebraic extension):** L の任意の元 α が、K 係数の非零な多項式の根になること。α を根に持つモニックで次数最小の多項式を**最小多項式** (minimal polynomial)と呼ぶ。
- **分離拡大 (separable extension):** 代数拡大であって、任意の元の最小多項式が重根を持たない(分離多項式である) こと。
- **正規拡大 (normal extension):** 代数拡大であって、K 上の既約多項式が L に1つでも根を持てば、L 上で一次式に完全に分解すること。
- **Galois拡大 (Galois extension):** 分離的かつ正規な代数拡大であること。

定義 1.2 (テンソル積)

K を体、L, M を K を部分体として含む可換環とする。L と M の K 上の**テンソル積** (tensor product)

$L \otimes_K M$ とは、K-ベクトル空間としてのテンソル積に、自然な積 $(x \otimes y)(x' \otimes y') = (xx') \otimes (yy')$ を与えて可換環としたものである。

定義 1.3 (環論の諸概念)

- **被約環 (reduced ring):** $x^n = 0$ となるような非零元 (すなわち冪零元) を持たない可換環。
- **Artin環 (Artinian ring):** イデアルの降鎖条件を満たす環。**局所Artin環 (local Artinian ring)** とは、極大イデアルをただ1つ持つArtin環である。

体のテンソル積は一般には体にならず、直積環や被約でない環になることがあります。この「体から環への拡張」こそが、テンソル積が体拡大の構造を映し出す鏡となる理由です。

例 1.4

$K = \mathbb{R}, L = \mathbb{C}$ の場合を考える。$\mathbb{C} \cong \mathbb{R}[X]/(X^2+1)$ であるから、

$$\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}[X]/(X^2+1) \cong \mathbb{C}[X]/(X^2+1)$$

と計算できる。複素数体 $\mathbb{C}$ 上では $X^2+1 = (X-i)(X+i)$ と分解されるため、中国剰余定理より

$$\mathbb{C}[X]/((X-i)(X+i)) \cong \mathbb{C}[X]/(X-i) \times \mathbb{C}[X]/(X+i) \cong \mathbb{C} \times \mathbb{C}$$

体拡大の次数 $[\mathbb{C} : \mathbb{R}] = 2$ に対し、ちょうど2つの $\mathbb{C}$ の直積環に分解していることがわかる。

ここで、のちの証明で鍵となる、体の自己同型写像に関する重要な定理を2つ明記しておきます。

定理 1.5 (Dedekindの補題)

L, M を体とする。相異なる環準同型写像 $\sigma_1, \dots, \sigma_m : L \to M$ は、M-ベクトル空間として一次独立である。すなわち、係数 $c_1, \dots, c_m \in M$ が存在して、すべての $x \in L$ に対して

$$\sum_{j=1}^{m} c_j \sigma_j(x) = 0$$

が成り立つならば、$c_1 = c_2 = \cdots = c_m = 0$ である。

定理 1.6 (自己同型群の位数と拡大次数)

L/K を有限次拡大とし、その拡大次数を $n = [L : K]$ とする。このとき、K-自己同型群 $\mathrm{Aut}_K(L)$ の位数 m は拡大次数 n を越えない。すなわち $m \leq n$ が成り立つ。

定理 1.6 の証明

背理法で示す。$G = \mathrm{Aut}_K(L)$ の位数が n より大きい、すなわち $m > n$ 個の相異なる自己同型

$\sigma_1, \sigma_2, \dots, \sigma_m \in G$ が存在すると仮定する。
L は K 上 n 次元ベクトル空間であるから、その K-基底を $\{x_1, \dots, x_n\}$ とする。
ここで、L に成分を持つ未知数 $c_1, \dots, c_m$ に関する以下の連立一次方程式を考える。

$$\sum_{j=1}^{m} c_j \sigma_j(x_i) = 0 \quad (i = 1, 2, \dots, n)$$

これは n 本の式に対して m 個の未知数を持つ同次連立一次方程式である。仮定より $m > n$ であるため、方程式の数よりも未知数の数が多い。線形代数学の基本定理より、この方程式は自明でない解を持つ。すなわち、すべてが 0 ではない $(c_1, \dots, c_m) \in L^m$ が存在する。
このとき、L の任意の元 x を取る。$\{x_i\}$ は基底であるから、$x = \sum_{i=1}^{n} a_i x_i$ $(a_i \in K)$ と表せる。各 σ_j は K-線形であるため、以下の計算が成り立つ。

$$\sum_{j=1}^{m} c_j \sigma_j(x) = \sum_{j=1}^{m} c_j \sigma_j \left(\sum_{i=1}^{n} a_i x_i \right) = \sum_{j=1}^{m} c_j \sum_{i=1}^{n} a_i \sigma_j(x_i)$$

和の順序を交換すると、

$$= \sum_{i=1}^{n} a_i \left(\sum_{j=1}^{m} c_j \sigma_j(x_i) \right) = \sum_{i=1}^{n} a_i \cdot 0 = 0$$

これは、すべてが 0 ではない係数 c_j を用いて、すべての $x \in L$ に対して $\sum_{j=1}^{m} c_j \sigma_j(x) = 0$ が恒等的に成り立つことを意味する。
しかし、これは先述の **Dedekindの補題** (定理 1.5) に明確に矛盾する。したがって、仮定 $m > n$ は誤りであり、$m \leq n$ が成り立つ。

2. 体拡大のテンソル積による特徴付け

以下、L を体 K の拡大体とし、$A = L \otimes_K L$ とおきます。A を L-ベクトル空間 (および L-代数) と見なすときは、第一成分の積 $x \cdot (a \otimes b) = (xa) \otimes b$ によって構造を定めます。

定理 2.1 (体拡大の特徴付け)

以下の条件について、それぞれ両方向の同値性が成り立つ。

1. L は K の有限次拡大である $\iff$ A は L-ベクトル空間として有限次元である。
2. L は K の分離拡大である $\iff$ A は被約環である。
3. L は K の正規拡大である $\iff$ L/K は代数拡大であり、任意の素イデアル $\mathfrak{p} \subset A$ に対し $\mathrm{Frac}(A/\mathfrak{p}) \cong L$ である。
4. L は K の有限次分離拡大である $\iff$ A は有限個の体の直積に同型である。
5. L は K の有限次正規拡大である $\iff$ A は有限個の局所Artin環の直積 $\prod_{i=1}^{r} A_i$ に同型で、各剰余体 $A_i/\mathfrak{m}_i \cong L$ である。
6. L は K の有限次Galois拡大である $\iff$ A は $[L : K]$ 個の体 L の直積に同型である。

これらの証明を順に追っていきましょう。

証明 (1): 有限次拡大 $\iff$ L-有限次元

($\Longrightarrow$) $[L:K]=n<\infty$ とする。L の K-基底を $\{e_1,\dots,e_n\}$ とすると、$L=\bigoplus_{i=1}^n Ke_i$ である。テンソル積の分配律より、

$$A = L\otimes_K\left(\bigoplus_{i=1}^n Ke_i\right)\cong\bigoplus_{i=1}^n (L\otimes_K K)e_i\cong\bigoplus_{i=1}^n L(1\otimes e_i)$$

したがって、A は $\{1\otimes e_1,\dots,1\otimes e_n\}$ を基底とする n 次元の L-ベクトル空間である。

($\Longleftarrow$) $\dim_L(A)=n<\infty$ とする。A を K-ベクトル空間として見ると、
$\dim_K(A)=\dim_K(L)\dim_L(A)=n\dim_K(L)$ となる。一方、テンソル積の定義より $\dim_K(A)=(\dim_K(L))^2$ である。したがって $\dim_K(L)=n<\infty$ となり、L/K は有限次拡大である。

証明 (2): 分離拡大 $\iff$ 被約環

($\Longrightarrow$) L/K が分離拡大であるとする。任意の有限生成部分拡大 L_i/K は原始元定理より $L_i=K(\alpha_i)$ と書ける。α_i の最小多項式 $f_i(X)\in K[X]$ は分離多項式であるため、$L_i\otimes_K L_i\cong L_i[X]/(f_i(X))$ は重根を持たず、有限個の体の直積となり被約環である。L/K は有限次分離拡大の直極限 $L=\varinjlim L_i$ と書け、テンソル積は直極限と可換であるため $A=\varinjlim(L_i\otimes_K L_i)$ となる。被約環の直極限も被約環であるため、A は被約環である。

($\Longleftarrow$) 対偶を示す。L/K が分離拡大でないとする。このとき $\mathrm{char}(K)=p>0$ であり、非分離的な元 $\alpha\in L\setminus K$ とある整数 $e\geq 1$ が存在し、$\alpha^{p^e}=a\in K$ となる。 A において $u=\alpha\otimes 1-1\otimes\alpha$ とおく。1 と α は K 上一次独立なので $u\neq 0$ である。しかし、

$$u^{p^e}=(\alpha\otimes 1-1\otimes\alpha)^{p^e}=\alpha^{p^e}\otimes 1-1\otimes\alpha^{p^e}=a\otimes 1-1\otimes a=0$$

となり、u は非零の冪零元である。したがって A は被約環ではない。

証明 (3): 正規拡大 $\iff$ 剰余体が L に同型

($\Longrightarrow$) L/K が正規拡大であるとする。任意の素イデアル $\mathfrak{p}\subset A$ を取り、$E=\mathrm{Frac}(A/\mathfrak{p})$ とおく。L/K は代数拡大なので、A は L 上代数的な環である。したがって整域 $A/\mathfrak{p}$ も L 上代数的であり、体となる。すなわち $E=A/\mathfrak{p}$ である。
自然な準同型写像 $\phi_1(x)=x\otimes 1 \bmod \mathfrak{p}$ と $\phi_2(x)=1\otimes x \bmod \mathfrak{p}$ を考える。L は体なので、これらは零環ではない E への単射である。任意の $\alpha\in L$ の K 上の最小多項式を $f(X)\in K[X]$ とすると、
$f(\phi_2(\alpha))=f(1\otimes\alpha)\bmod\mathfrak{p}=1\otimes f(\alpha)\bmod\mathfrak{p}=0$ となる。L/K は正規拡大なので、$f(X)$ は L 上で一次式に完全に分解する。よって、その根である $\phi_2(\alpha)$ は $\phi_1(L)$ に含まれなければならない。対称性から
$\phi_1(L)=\phi_2(L)$ であり、E はこれらで生成されるため $E=\phi_1(L)\cong L$ となる。

($\Longleftarrow$) 任意の素イデアルによる剰余体が L に同型であるとする。$\alpha\in L$ を任意に取り、その K 上の最小

多項式を $f(X)$ とする。$f(X)$ のある根 β を含む L の拡大体 Ω を取る。$\alpha \mapsto \beta$ とする K 上の同型は、環準同型 $\Phi : L \otimes_K L \to \Omega$ を $\Phi(x \otimes y) = x \cdot y'$ (y' は y を同型で写した像) によって誘導する。
$\ker(\Phi) = \mathfrak{p}$ は素イデアルであり、$A/\mathfrak{p}$ は Ω の部分体と同型になる。仮定より $\mathrm{Frac}(A/\mathfrak{p}) \cong L$ であるため、第二成分の像 (特に β) も第一成分の像 (すなわち L 自身のコピー) に含まれなければならない。よって $\beta \in L$ となり、$f(X)$ のすべての根は L に属するため正規拡大である。

証明 (4): 有限次分離拡大 $\iff$ 有限個の体の直積

($\Longrightarrow$) (2)の証明で示したように、有限次分離拡大ならば原始元定理より $L = K(\alpha)$ と書け、$A \cong L[X]/(f(X))$ となる。$f(X)$ は重根を持たないため、中国剰余定理により $A \cong \prod_{i=1}^{r} L[X]/(f_i(X))$ となり、各 f_i が既約であることから有限個の体の直積となる。

($\Longleftarrow$) $A \cong \prod_{i=1}^{r} F_i$ (各 F_i は体) であるとする。A は有限個の体の直積なので被約環であり、(2)より分離拡大である。また、各 F_i は L を含むため L-ベクトル空間として少なくとも1次元以上であり、A 全体としても有限次元である。したがって(1)より有限次拡大である。

証明 (5): 有限次正規拡大 $\iff$ 剰余体が L である局所Artin環の直積

($\Longrightarrow$) (1)より有限次なので、A は L 上有限次元、すなわちArtin環である。Artin環の構造定理より $A \cong \prod_{i=1}^{r} A_i$ (各 A_i は極大イデアル $\mathfrak{m}_i$ をもつ局所Artin環) と一意に分解される。A の素イデアルは $\mathfrak{m}_i$ に対応し、剰余環 $A/\mathfrak{m}_i$ は $A_i/\mathfrak{m}_i$ に同型である。さらに(3)より正規拡大であることから剰余体は L に同型である。よって $A_i/\mathfrak{m}_i \cong L$ である。

($\Longleftarrow$) $A \cong \prod_{i=1}^{r} A_i$ であるとする。A はArtin環なので L 上有限次元であり、(1)より有限次拡大である。また、各 A_i の剰余体が L に同型であることは、A の任意の素イデアルによる剰余体が L に同型であることを意味する。したがって(3)より正規拡大である。

特徴付け (6) の自己完結した直接証明

ここで、Galois群の位数 $|G|$ が拡大次数 $[L:K]$ に一致することを一切先行して仮定（当然視）せず、原始元定理と中国剰余定理から直積分解を直接構成する、厳密な証明を与えます。

証明 (6): 有限次Galois拡大 $\iff$ $[L:K]$ 個の体 L の直積

($\Longrightarrow$) L/K を有限次Galois拡大（すなわち有限次の分離かつ正規拡大）とし、その拡大次数を $[L:K] = n$ とする。また、L/K のGalois群を $G = \mathrm{Gal}(L/K)$ とする（この時点では群の位数 $|G|$ は未知である）。
L/K は有限次分離拡大であるため、**原始元定理 (primitive element theorem)** より、ある元 $\alpha \in L$ が存在して $L = K(\alpha)$ と表せる。α の K 上の最小多項式を $f(X) \in K[X]$ とすると、その次数は $\deg f = [L:K] = n$ である。
可換環の多項式環による剰余の性質から、次のような自然な同型が存在する。

$$L \otimes_K L = L \otimes_K \big(K[X]/(f(X))\big) \cong L[X]/(f(X))$$

ここで、L/K は正規拡大かつ分離拡大であるため、最小多項式 $f(X)$ は L 係数の多項式として、相異なる n 個の一次式の積に完全に分解する。すなわち、

$$f(X) = (X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_n) \quad (\alpha_i \in L)$$

と書ける（ただし $\alpha_1 = \alpha$ であり、すべての $i \neq j$ について $\alpha_i \neq \alpha_j$）。
一変数の多項式環 $L[X]$ は主イデアル整域であり、各イデアル $(X-\alpha_i)$ たちは互いに素であるため、**中国剰余定理 (Chinese remainder theorem)** を適用することができる。これにより、次の環同型が得られる。

$$L[X]/(f(X)) \cong L[X]/(X-\alpha_1) \times L[X]/(X-\alpha_2) \times \cdots \times L[X]/(X-\alpha_n) \cong \prod_{i=1}^{n} L$$

以上の議論を組み合わせることで、拡大次数 $[L:K]=n$ とちょうど同じ個数である **n 個の体 L の直積への環同型** $\Phi : L \otimes_K L \xrightarrow{\sim} \prod_{i=1}^{n} L$ が得られた。

ここで、この同型の各成分への射影準同型 $\psi_i : L \otimes_K L \to L$ を考える。これは $\psi_i(x \otimes y) = x \cdot \sigma_i(y)$ の形をしており、$\sigma_i(y) = \psi_i(1 \otimes y)$ によって K 上の体の埋め込み $\sigma_i : L \to L$ が定まる。L/K は有限次拡大なので、これは K-自己同型写像（すなわち G の元）である。
多項式 X の各成分への像を追うと、$\psi_i(1 \otimes \alpha) = \sigma_i(\alpha) = \alpha_i$ となる。$\alpha_1, \dots, \alpha_n$ はすべて相異なるため、これらを誘導する自己同型写像 $\sigma_1, \dots, \sigma_n \in G$ もすべて相異なる。したがって、Galois群 G は少なくとも n 個の相異なる元を含むため、$|G| \geq n$ である。
一方、定理1.6により、有限次拡大において自己同型群の位数は拡大次数を越えられない（$|G| \leq n$）ことがすでに証明されている。ゆえに、等号 $|G| = n = [L:K]$ が成立しなければならない。これにより、直積の各成分のインデックス i は Galois群 G の元 σ と完全に1対1に対応し、同型 $\Phi : L \otimes_K L \xrightarrow{\sim} \prod_{\sigma \in G} L$ が完全に確立される。

($\Longleftarrow$ **)** L-代数としての同型写像 $\Phi : L \otimes_K L \xrightarrow{\sim} \prod_{i=1}^{n} L$ が存在すると仮定する。 L-ベクトル空間としての次元を比較すると、左辺の次元は $\dim_L(L \otimes_K L) = \dim_K(L) = [L:K]$ であり、右辺の次元は n である。したがって $[L:K]=n$ となり、L/K は有限次拡大である。
右辺の直積環には、各成分への射影写像 $p_i : \prod_{j=1}^{n} L \to L$ が n 個存在する。これらと Φ を合成することで、A から L への n 個の相異なる L-代数準同型 $\psi_i = p_i \circ \Phi$ を得る。ここで、各 ψ_i を用いて写像 $\sigma_i : L \to L$ を次のように定義する。

$$\sigma_i(y) = \psi_i(1 \otimes y)$$

ψ_i は環準同型であるため、σ_i も環準同型 (K 上の体の埋め込み) となる。L/K は有限次拡大であるため、L から L への K-線形な単射は必ず全射となり、σ_i は K-自己同型写像 (すなわち $\mathrm{Gal}(L/K)$ の元) である。
もし $\sigma_i = \sigma_j$ となる $i \neq j$ が存在したとすると、任意の $x, y \in L$ について

$$\psi_i(x \otimes y) = \psi_i(x \otimes 1)\psi_i(1 \otimes y) = x\sigma_i(y) = x\sigma_j(y) = \psi_j(x \otimes y)$$

となり、$\psi_i = \psi_j$ となってしまうが、これは ψ_i が n 個の相異なる写像であることに矛盾する。 したがって、$\{\sigma_1, \dots, \sigma_n\}$ はすべて相異なる n 個の L の K-自己同型である。拡大次数 $[L:K]=n$ に対して自己同型群の位数 $|G|$ が少なくとも n 以上（かつ最大でも n）であるため、$|G| = [L:K] = n$ となり、定義に

より L/K は有限次Galois拡大である。

3. GrothendieckのGalois理論への応用

ここまでで証明した $L \otimes_K L \cong \prod_{\sigma \in G} L$ という関係式が、Galois対応の証明にどのように威力を発揮するのかを見ていきましょう。このアプローチでは、「環の直積分解」を制御する **冪等元 (idempotent, $e^2 = e$ を満たす元)** と、群作用の組み合わせが主役になります。

例 3.1 ($\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ における冪等元の構造)

$L = \mathbb{C}, K = \mathbb{R}$ とする。Galois群は $G = \{\mathrm{id}, \sigma\}$ (ここで σ は複素共役) である。 同型 $\Phi : \mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \xrightarrow{\sim} \mathbb{C} \times \mathbb{C}$ は $\Phi(x \otimes y) = (xy, x\overline{y})$ で与えられる。
直積環 $\mathbb{C} \times \mathbb{C}$ には、明らかな冪等元 $f_1 = (1, 0)$ と $f_2 = (0, 1)$ が存在する。これらに対応するテンソル積側の元 $e_1 = \Phi^{-1}(f_1), e_2 = \Phi^{-1}(f_2)$ を探す。
$f_1 + f_2 = (1, 1) = \Phi(1 \otimes 1)$
$f_1 - f_2 = (1, -1) = \Phi(-i \otimes i)$ (なぜなら $\Phi(-i \otimes i) = (-i^2, -i(\overline{i})) = (1, -i(-i)) = (1, -1)$)
これを解くと、

$$e_1 = \frac{1 \otimes 1 - i \otimes i}{2}, \quad e_2 = \frac{1 \otimes 1 + i \otimes i}{2}$$

が得られる。実際に $e_1^2 = \frac{1\otimes1 - 2i\otimes i + i^2 \otimes i^2}{4} = \frac{1\otimes1 - 2i\otimes i + 1\otimes1}{4} = e_1$ となり、確かに冪等元をなしている。このように、テンソル積の内部には「成分を切り出す」ための幾何学的な射影演算子が潜んでいる。

それでは、この同型を用いたGalois対応の証明を行います。Artinの不等式評価は一切登場しません。

定理 3.2 (Galois対応の基本定理)

L/K を有限次Galois拡大、そのGalois群を G とする。 中間体 M と、部分群 $H \subset G$ は、対応 $H \mapsto L^H$ (不変体) および $M \mapsto \mathrm{Gal}(L/M)$ によって1対1に対応する。

証明

同型 $\Phi : L \otimes_K L \xrightarrow{\sim} \prod_{\sigma \in G} L$ において、Galois群 G の元 τ は、テンソル積の右側の成分に対して $\tau \cdot (x \otimes y) = x \otimes \tau(y)$ として作用する。この作用は右辺の直積成分のインデックスを $(\tau \cdot \mathbf{c})_\sigma = c_{\sigma\tau}$ のようにシフトさせる。

ステップ1：部分群 H から出発し、$\mathrm{Gal}(L/L^H) = H$ を示す
任意の部分群 $H \subset G$ を取り、対応する中間体を $M = L^H$ とする。$L \otimes_K L$ と $\prod_{\sigma \in G} L$ の双方において、H の作用で不変な部分環 (H-不変部分) を考える。

- 左辺の H-不変部分は $(L \otimes_K L)^H = L \otimes_K (L^H) = L \otimes_K M$ であり、その L-ベクトル空間としての次元は $\dim_K(M) = [M : K]$ である。

- 右辺の直積環の元 $\mathbf{c}$ が H-不変であるとは、任意の $h \in H$ と $\sigma \in G$ について $c_\sigma = c_{\sigma h}$ となること。すなわち左剰余類 σH の上で定数になることである。左剰余類は $[G : H] = |G|/|H|$ 個存在するため、不変部分の L-次元は $[G : H]$ である。

したがって $[M : K] = [G : H]$ を得る。$[L : K] = |G| = [L : M][M : K]$ より、直ちに $[L : M] = |H|$ となる。明らかに $H \subset \mathrm{Gal}(L/M)$ であり、(後述のステップ2により) $\mathrm{Gal}(L/M)$ の位数は $[L : M]$ に等しいため、包含関係と位数が一致し $H = \mathrm{Gal}(L/M)$ が従う。

ステップ2：中間体 M から出発し、$L^{\mathrm{Gal}(L/M)} = M$ を示す
任意の中間体 $K \subset M \subset L$ を取り、$H_M = \mathrm{Gal}(L/M)$ とする。 自然な全射環準同型 $\pi : L \otimes_K L \twoheadrightarrow L \otimes_M L$ を考える。この全射の核 I_M は、集合 $\{1 \otimes m - m \otimes 1 \mid m \in M\}$ で生成されるイデアルである。すなわち $(L \otimes_K L)/I_M \cong L \otimes_M L$ となる。
同型 Φ を通じて、この生成元の像を計算すると、

$$\Phi(1 \otimes m - m \otimes 1) = (\sigma(m) - m)_{\sigma \in G}$$

となる。イデアル $\Phi(I_M)$ は、「すべての $m \in M$ に対して $\sigma(m) = m$ となる成分」、すなわち $\sigma \in H_M$ に対応する成分においてのみ値が 0 となる元の集合によって生成される。したがって、このイデアルで右辺の直積環を割ると、H_M に対応する成分だけが生き残り、

$$\prod_{\sigma \in G} L \Big/ \Phi(I_M) \cong \prod_{\sigma \in H_M} L$$

という同型が得られる。この同型は左辺の剰余環 $L \otimes_M L$ と結ばれるため、$L \otimes_M L \cong \prod_{\sigma \in H_M} L$ となる。
両辺の L-ベクトル空間としての次元を比較する。左辺の次元は $[L : M]$ であり、右辺の次元は直積の成分数 $|H_M|$ である。したがって $[L : M] = |H_M|$ を得る。
ステップ1の次元計算を $H = H_M$ に対して適用すると $[L : L^{H_M}] = |H_M|$ となる。$M \subset L^{H_M}$ でありながら、L までの拡大次数が互いに $|H_M|$ で完全に一致するため、$M = L^{H_M}$ でなければならない。これでGalois対応の全単射性が完全に証明された。

このように、可換環のテンソル積は体の枠組みを越えてGalois理論を展開するための強力な言語を提供してくれます。これはトポロジーにおける被覆空間 (covering space) の理論と完全にパラレルな関係にあり、現代数学の豊かさを感じさせる美しい理論です。

4. 参考文献

1. N. Bourbaki, *Algebra II, Chapters 4 - 7*, Springer-Verlag, 1990. [Link]
2. A. Grothendieck, *Séminaire de Géométrie Algébrique du Bois Marie - 1960-61 - Revêtements étales et groupe fondamental - (SGA 1)*, Lecture Notes in Mathematics 224, Springer, 1971. (Available at arXiv:math/0206203) [Link]