ヒルベルト『数論報告』に探る：体の判別式と素イデアル分解の深層

デデキントの基本定理への道筋

物語の主役：体の判別式 (Discriminante)

体 k の基底を $\omega_1, \ldots, \omega_m$ とするとき、その**判別式** d は以下の等式で定義される。

$$d = \begin{vmatrix} \omega_1 & \omega_2 & \cdots & \omega_m \\ \omega_1' & \omega_2' & \cdots & \omega_m' \\ \vdots & \vdots & \cdots & \vdots \\ \omega_1^{(m-1)} & \omega_2^{(m-1)} & \cdots & \omega_m^{(m-1)} \end{vmatrix}^2$$

基底の元 (Basis element)

共役元 (Conjugate element)

それは一つの整なる有理数である。

判別式 d は、数体 k の構造を特徴づける不変量であり、このプレゼンテーションの中心的な役割を担う。

なぜ判別式が重要なのか？

ヒルベルトは『数論報告』で次のように述べている：

「体論の発展にとって、体 k の判別式に現れるイデアル因子の研究は、本質的に重要な意味をもつ。」

この言葉は、判別式の素因数が体の数論的性質を解き明かす鍵であることを示唆している。我々はこの「本質的に重要な意味」を解き明かす旅に出る。

我々が目指す頂：デデキントの基本定理（定理31）

定理31: 数体 k の判別式 d は、その体に属するすべての有理素数因子 p を含むが、それらの素数は、ある素イデアルの平方によって可除なものである。

In simpler terms: 有理素数 p が判別式 d を割り切ることと、p が生成するイデアル (p) が体 k 内で素イデアルの平方で割り切れる（すなわち「分岐する」）ことは同値である。

$$p \mid d \iff (p) = p_1^{e_1} p_2^{e_2} \cdots p_i^{e_i} \cdots$$

$e_i > 1$

分岐 (Ramification)

証明の道具①：基本形式 (Fundamentalform)

Definition:
不定数 $u_1, \ldots, u_m$ と体 k の基底 $\omega_1, \ldots, \omega_m$ を用いて、
体 k の**基本形式 ξ** を次のように定義する：

$$\xi = u_1\omega_1 + u_2\omega_2 + \cdots + u_m\omega_m$$

Purpose:
特定の元に依存しない、体 k の「一般的な」元を表現するために不定数 u_i を導入する。これにより、証明が普遍性を持つことになる。

証明の道具②：基本方程式 (Fundamentalgleichung)

Definition: 基本形式 ξ は、係数が u_i の整関数であるような m 次の代数方程式を満たす。これを**基本方程式**と呼ぶ。

ξ とその共役元が根

$$F(x; u_1, \ldots, u_m) = (x - \xi)(x - \xi')\cdots(x - \xi^{(m-1)}) = 0$$

$$x^m + U_1 x^{m-1} + \cdots + U_m = 0$$

U_j は $u_1, \ldots, u_m$ の整係数有理関数

Central Idea: この方程式の法 p での因数分解が、素数 p の素イデアル分解を支配している。

核心概念：原始整関数 (Primitivfunction)

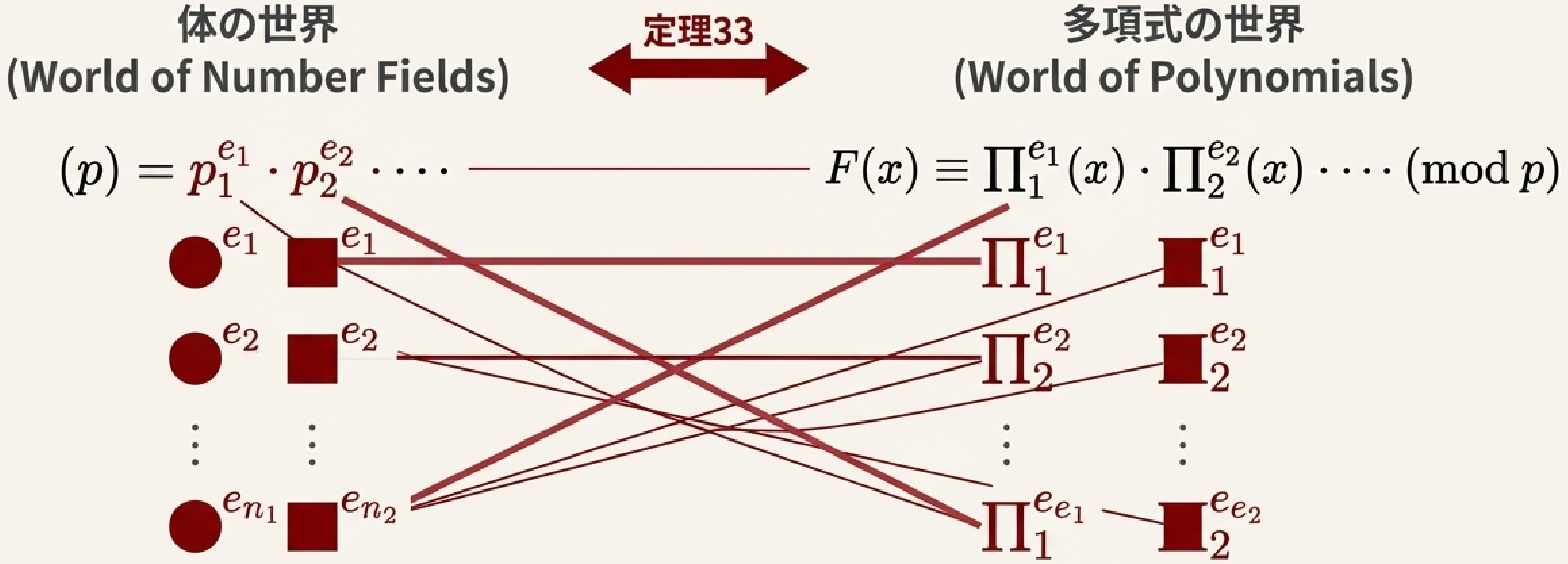
Definition: 整関数 $P(x; u_1, \ldots, u_m)$ が、法 p において、p で割り切れない有理整数係数の関数以外に因子を持たないとき、**法 p に関する原始整関数 (Primitivfunction nach p)** と呼ばれる。

よく知られた概念 (Familiar Concept)		ヒルベルトによる拡張 (Hilbert's Extension)
$\mathbb{Z}[x]$ における既約多項式 整数係数の多項式で、定数でない2つの整数係数多項式の積に分解できないもの。	→	**$\mathbb{Z}[x, u_1, \ldots, u_m]$ における法 p の原始整関数** 不定数 u_i を含む関数で、法 p において自明でない因子を持たないもの。

Significance: この概念により、**法 pでの基本方程式の一意的な分解**が可能になる。

重要な中間地点：分解法則の確立（定理33）

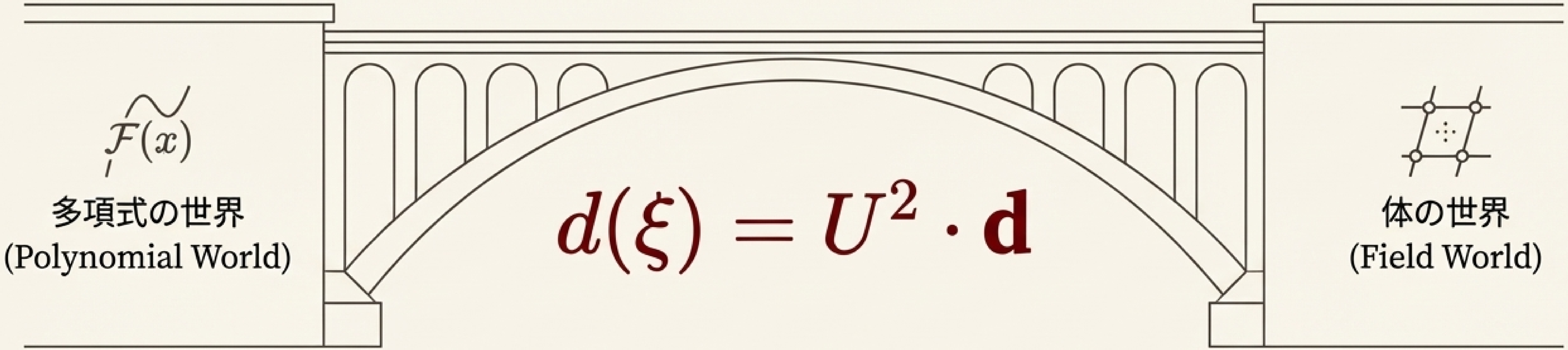
定理33: 有理素数 p の素イデアル分解が $p = p_1^{e_1} p_2^{e^2} \cdots$ であることと、基本方程式 $F(x)$ の法 p での原始整関数への分解が $F \equiv \prod_1^{e_1} \prod_2^{e^2} \cdots (\mathrm{mod}\, p)$ となることは同値である。



多項式の世界における分解の「指数」が、数体の世界における素イデアル分解の「指数」と完全に一致する。

判別式への接続（定理35）

定理35： 基本方程式の判別式 $d(\xi)$ と体の判別式 d の間には、次の関係が成り立つ。



$$d(\xi) = U^2 \cdot \mathbf{d}$$

ここで U は $u_1, \ldots, u_m$ に関する有理整関数であり、その係数は有理整数である（有理単数）。

Implication: この等式は、基本方程式 $d(\xi)$ の素因子を調べることで、体の判別式 d の素因子に関する情報が得られることを意味する。

最後の道具：微分イデアル (Differente)

Definition

体 k の**微分イデアル** (Differente) $\mathbf{b}$ とは、体の元 $(\omega_i - \omega_i^{(j)})$ たちから生成されるイデアルの積として定義される、体 k の重要なイデアルである。

$\mathbf{b} = \mathbf{e}'\mathbf{e}'' \cdots \mathbf{e}^{(m-1)}$, ここで

$\mathbf{e}^{(j)} = \big((\omega_1 - \omega_1^{(j)}), \ldots, (\omega_m - \omega_m^{(j)})\big)$

The Crucial Link (Theorem 37)

定理37: 体の微分イデアルのノルムは、体の判別式に等しい。

$$\mathrm{N}(\mathbf{b}) = |\mathbf{d}|$$

証明のクライマックス

1. 分岐の条件
素数 p が分岐する $\Leftrightarrow$ イデアル分解 $p = \cdots p_i^{e_i} \cdots$ で、ある $e_i > 1$ となる。

2. 分岐と微分イデアル
$F(x)$ の導関数 $\frac{\partial F}{\partial x}$ の法 p での振る舞いを分析すると、p が分岐することと、p が微分イデアル b を割り切ることは同値であることが示される。

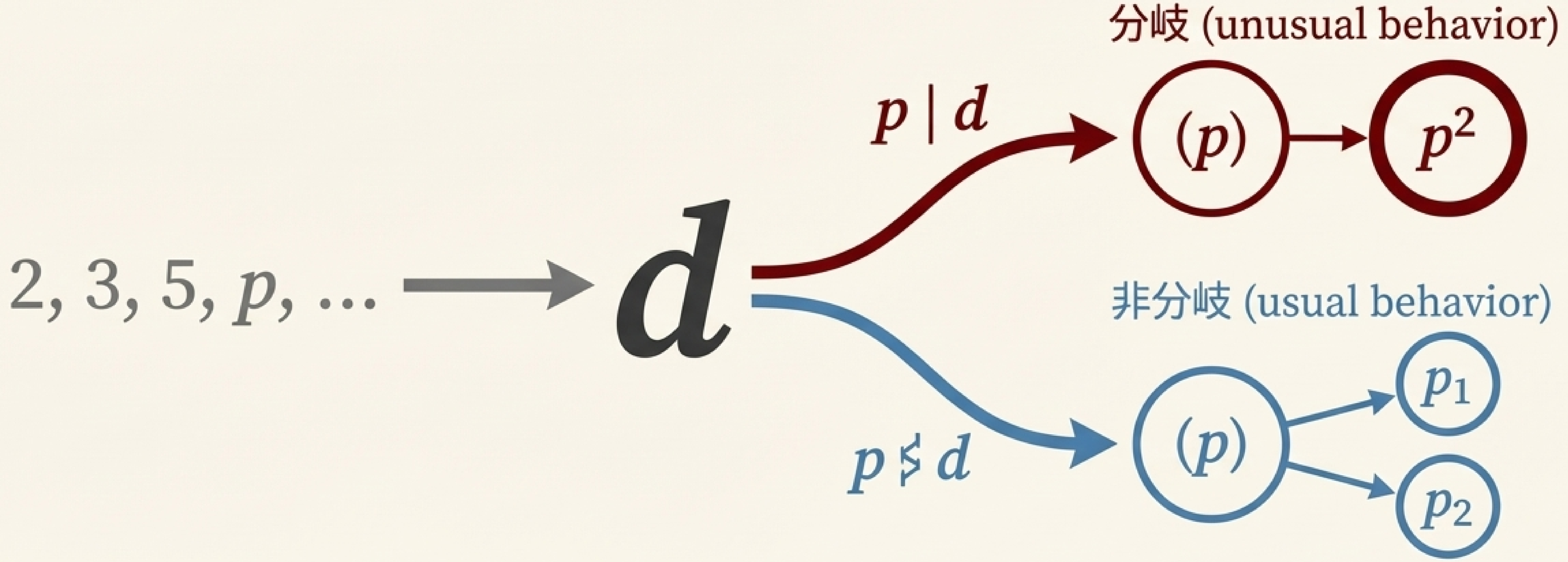
3. 微分イデアルと判別式
定理37より、$\mathrm{N}(b) = |d|$。ある素数 p がイデアル b を割り切ることは、そのノルム $\mathrm{N}(b)$ を割り切ることと同値である。

4. 結論
したがって、「p **が分岐する** $\Leftrightarrow$ p **が** b **を割る** $\Leftrightarrow$ p **が** $N(b)$ **を割る** $\Leftrightarrow$ p **が** d **を割る**」が証明された。

Q.E.D.

頂からの眺め：判別式が語ること

The Big Picture: 判別式 d は単なる計算上の数値ではない。それは、その数体の「数論的指紋」である。
判別式の素因数分解は、どの有理素数がその体の中で「通常とは異なる」振る舞い（＝分岐）をするかを正確に教えてくれる。



理論から実践へ：素イデアル分解の計算 (ヒルベルト §13)

p

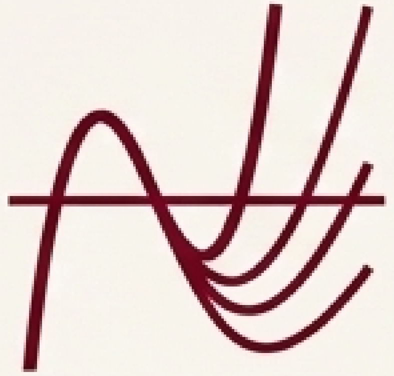
1. Choose a prime p

分解したい有理素数 p を選ぶ。

$u_i \longrightarrow a_i$

2. Specialize the variables

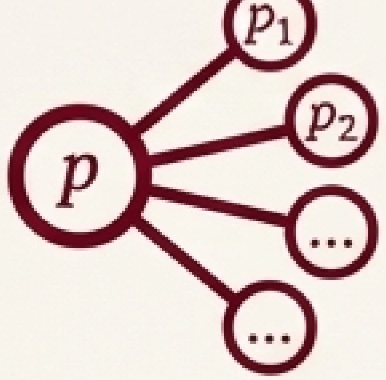
基本形式 ξ の不定数 u_i に、有理単数 U の「固定因子」を避けるように注意深く整数 a_i を代入し、元 $\alpha = a_1\omega_1 + \cdots$ を作る。



3. Factor the polynomial

α の最小多項式 $F_\alpha(x)$ を法 p で既約分解する。

$$F_\alpha(x) \equiv f_1(x)^{e_1} f_2(x)^{e_2} \cdots \pmod{p}$$



4. Read off the ideals

素イデアル分解は $p = \mathfrak{p}_1^{e^1}\mathfrak{p}_2^{e^2}\cdots$ となり、各 $\mathfrak{p}_i$ は $(p, f_i(\alpha))$ で与えられる。

我々の足跡：基本定理への論理の道筋

登頂: p が d を割り切ることが、p が分岐することの必要十分条件であることを証明。

最終連結: **微分イデアル`$\boldsymbol{b}$** を通じて、分岐と判別式を直結させる (定理37)。

架け橋: 方程式の判別式 $d(\xi)$ と体の判別式 d を結びつける (定理35)。

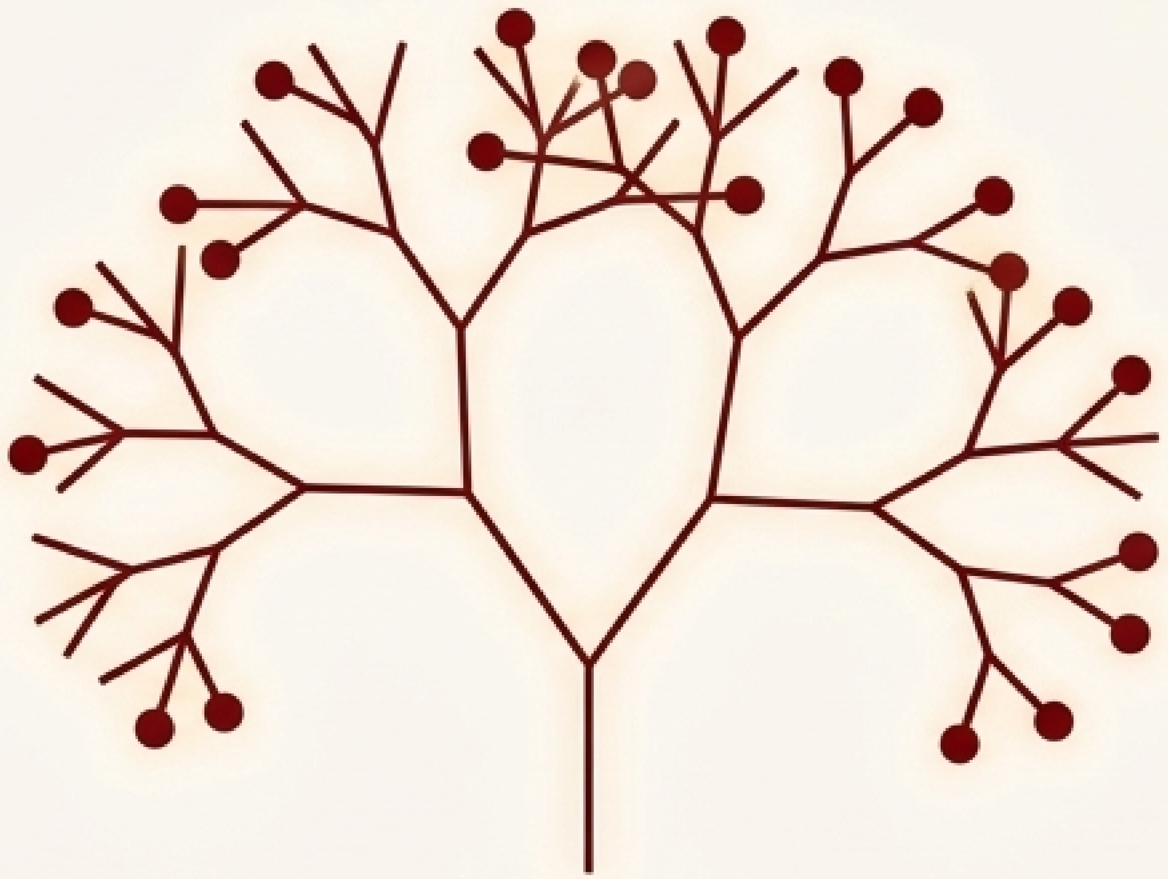
第一の発見: $F(x)$ の法 p 分解が、イデアル (p) の分解を反映することを発見 (定理33)。

道具の準備: **基本形式 $\boldsymbol{\xi}$** と **基本方程式** $F(x)$ を構築。

目標設定: d と素数の分岐を結びつける (定理31)。

出発点: **判別式 $\boldsymbol{d^*}$** を定義。

数論の礎



判別式と素イデアル分解を結びつけるこの基本定理は、単なる一つの美しい結果ではない。それは、類体論をはじめとする20世紀の代数的整数論の壮大な理論体系を築く上での、不可欠な礎石となった。ヒルベルトが『数論報告』で示したこの道筋は、今なお我々を数の世界の深淵へと導き続けている。