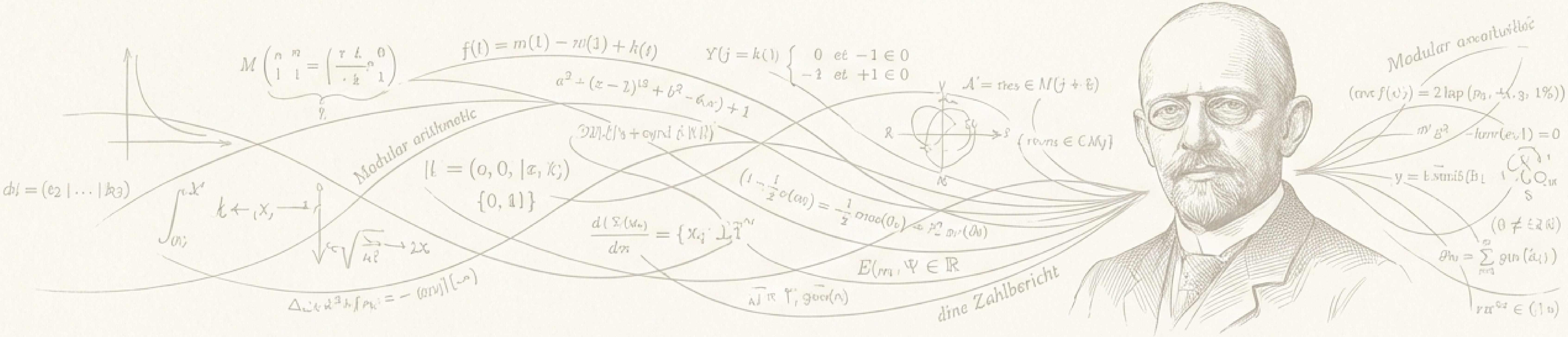
代数的整数論の黎明：ヒルベルト『数論報告』に見るイデアル算術の構築

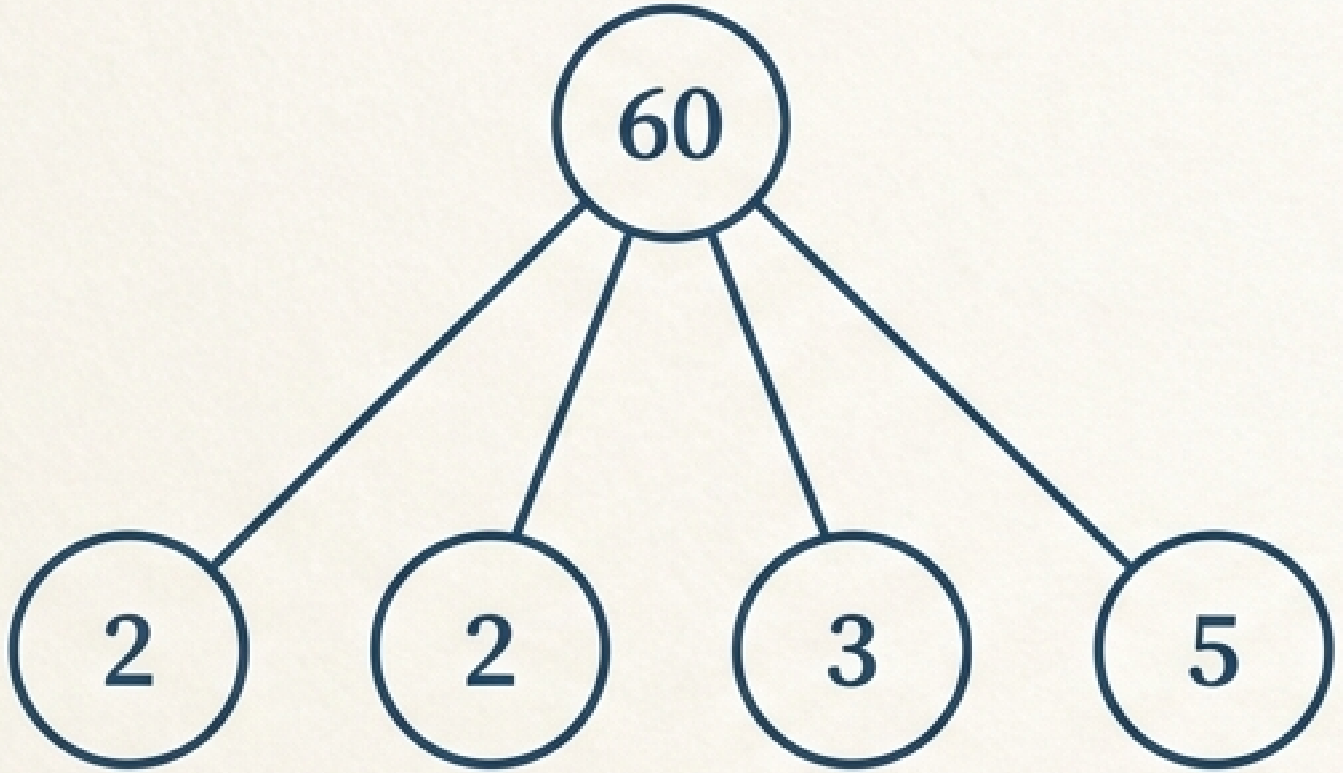
整数が織りなす秩序を、いかにして広大な代数体の世界へ拡張したか



「デデキントとクロネッカーによって切り拓かれた道を歩み、我々はガロア数体の理論を基礎とする、より簡潔な証明法をここに提示する。」

秩序から混沌へ：失われた「素因数分解の一意性」

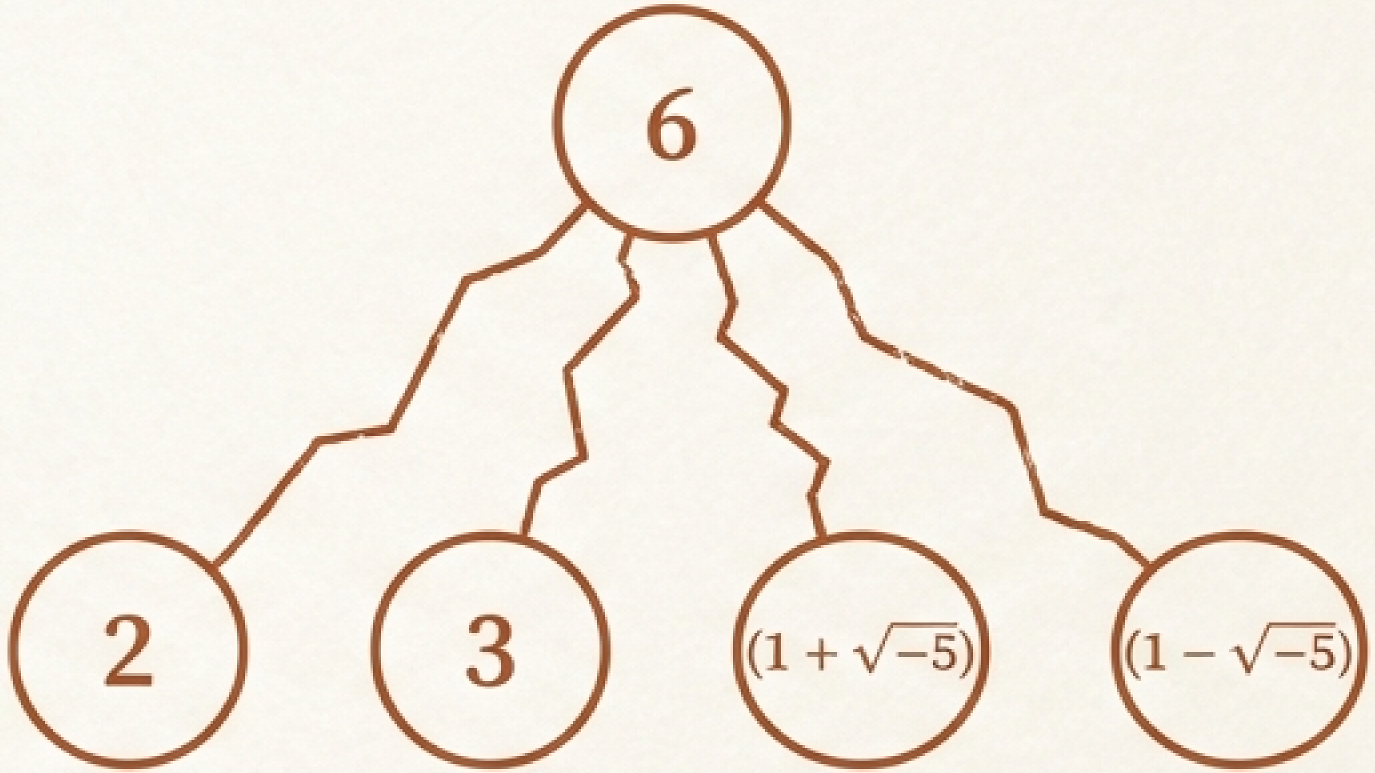
有理整数環 $\mathbb{Z}$ の美しき秩序



$$60 = 2^2 \cdot 3 \cdot 5$$

「すべての整数は、順序を除いて一意的に素数の積で表せる」
—算術の基本定理。これは我々の数の世界の礎である。

代数体 $\mathbb{Q}(\sqrt{-5})$ での崩壊



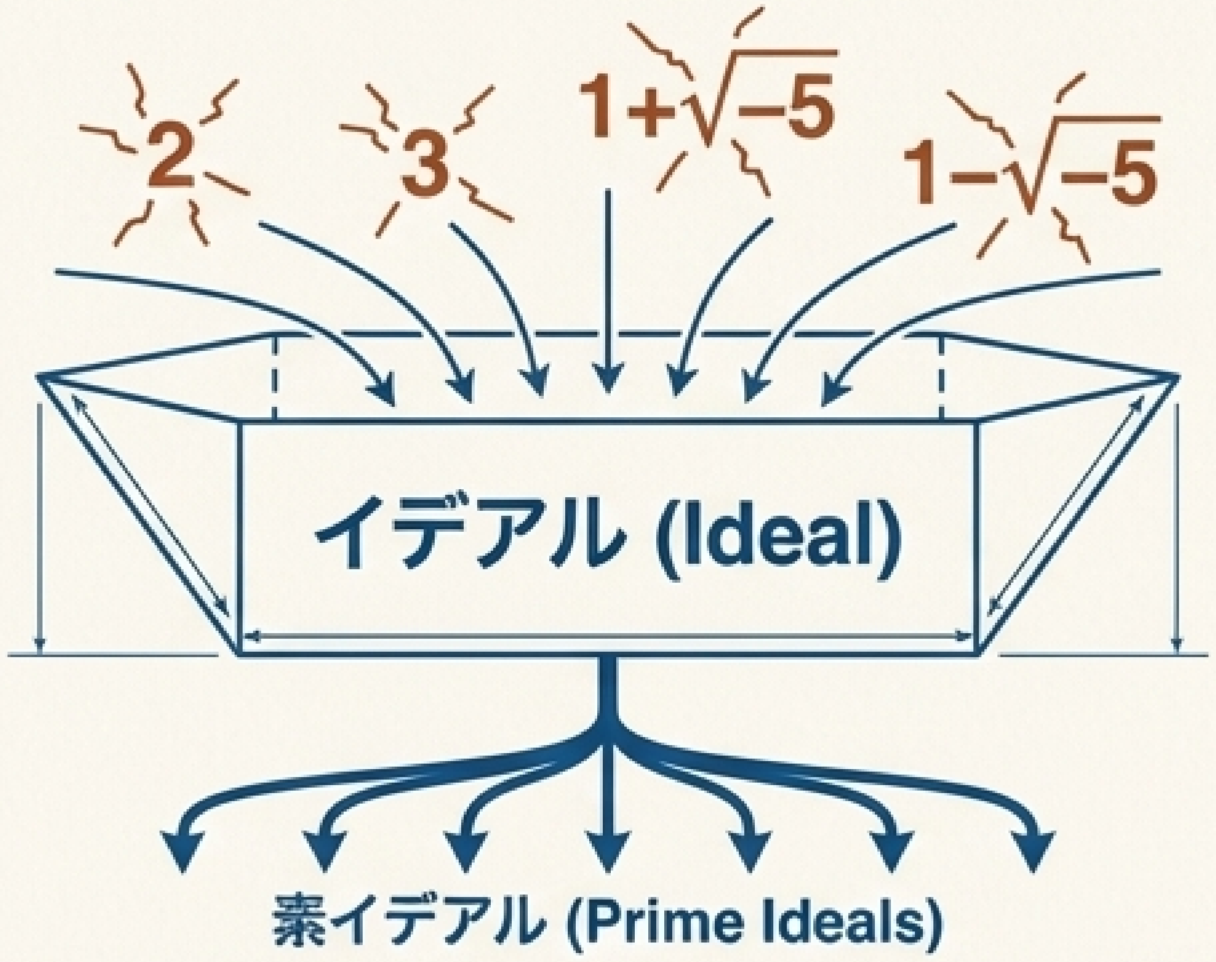
$$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$$

「この新たな数世界に、我々はどのようにして秩序を取り戻すことができるのか？」

この根本的な問題意識が、デデキントによる「イデアル」という画期的な概念の導入へと繋がった。

秩序の再建者：「イデアル」という新たな数

数そのものではなく、
数の「集合」。



例: (2) は $\mathbb{Z}$ の中の全ての偶数を表すイデアル。

核心的アイデア：個々の数の分解ではなく、イデアルの分解を考えれば、
素因数分解の一意性（素イデアル分解の一意性）が回復する。

構築のロードマップ

1. 第一部：大きさの定義 — イデアルの「ノルム」
2. 第二部：関係性の再構築 — イデアルによる「合同」
3. 第三部：世界の構造の探求 — 素イデアルが作る「剰余体」

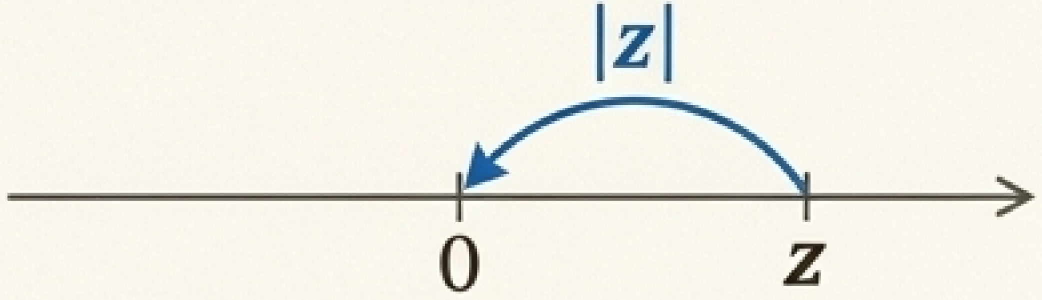
第一部：イデアルの「大きさ」を測る道具（ノルム）

イデアルのノルム $n(\mathfrak{a})$

イデアル $\mathfrak{a}$ を法として互いに合同でない全ての整数の個数。

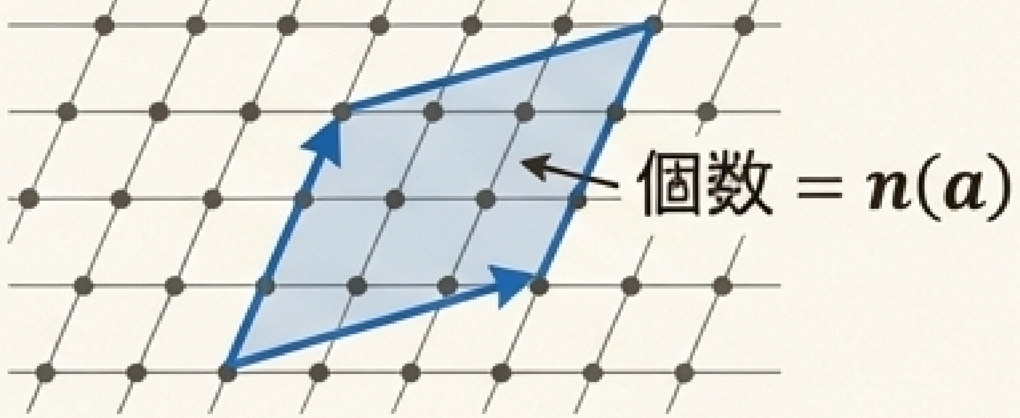
整数の世界

$|z|$（絶対値）



イデアルの世界

$n(\mathfrak{a})$（ノルム）



最初の重要な性質（定理17）

素イデアル $\mathfrak{p}$ のノルム $n(\mathfrak{p})$ は、それが含む有理素数 p の冪 p^f となる。

$$n(\mathfrak{p}) = p^f$$

次数（Grad): この指数 f を素イデアル $\mathfrak{p}$ の次数と呼ぶ。

解説：素イデアルの「大きさ」は、我々が知る素数と直接結びついている。

ノルムが持つべき「美しい性質」

性質1：乗法性 (定理18)

$$n(ab) = n(a)n(b)$$

意味：「積の大きさ」は「大きさの積」に等しい。これは絶対値 $|xy| = |x||y|$ が持つ性質と完璧に呼応する。

性質2：計算可能性 (定理19)

$$n(a) = |\det(A)|$$

ただし $t_i = \sum a_{ij}\omega_j$

意味：抽象的な定義だけでなく、具体的な計算手段が存在する。

性質3：理論的整合性 (定理20)

$$n(F) = n(a)$$

(ここで a は形式 F の内容)

意味：異なる理論体系とも整合性が取れており、概念の正しさを裏付けている。

ノルムへの異なる視点：共役イデアル

共役イデアルの導入 (from §7)

イデアル a の全ての数 α を、その共役 α' に置き換えることで得られるイデアルを a' と書く。

重要な帰結（定理18, 20より）

$$a \cdot a' \cdot a'' \cdot \cdots = (n(a))$$

解説：これは整数のノルム（α とその共役の積）の定義と完全に一致する。イデアルのノルムが、より根源的な体の構造から自然に導かれることを示唆している。

ノルムの具体性（定理21）

定理21: 任意のイデアル i において、そのノルム $n(i)$ を最大公約数として持つような2つの整数が必ず存在する。

意味：イデアルのノルムという抽象的な数も、最終的には我々が知る整数の関係性の中にその姿を現す。

第二部：関係性の再構築（イデアルによる合同）

整数の世界 (mod m)

$$a \equiv b \pmod{m}$$

意味: a − b が整数 m で割り切れる。

イデアルの世界 (mod a)

$$\alpha \equiv \beta \pmod{a}$$

意味: $\alpha - \beta$ がイデアル a に属する。

かつて整数と素数を舞台とした偉大な定理が、今や代数的整数とイデアルという新たな役者を得て、再びその美しい脚本を演じる。

偉大な定理の一般化：フェルマーとオイラーの遺産

フェルマーの小定理の拡張 (定理22)	オイラーの定理の拡張 (定理24)	オイラーのϕ関数 (定理23)
p を次数 f の素イデアルとすると、体の任意の整数 ω に対して、 $$\omega^{p^f} \equiv \omega \pmod{p}$$ p^f は $n(p)$ であることに注意。	イデアル a と素な任意の整数 ω に対して、 $$\omega^{\phi(a)} \equiv 1 \pmod{a}$$	$\phi(a)$ は a と互いに素な剰余類の個数。 $$\phi(a) = n(a) * \prod\left(1 - \frac{1}{n(p_i)}\right)$$

解説：これらの定理が全く同じ形で成立することは、イデアルによる合同という概念が、整数論の構造を正しく捉えていることの強力な証拠である。

構造の解明：複数の条件を同時に満たす解

中国剰余定理（定理25）

主張：イデアル $a_1, \ldots, a_q$ が互いに素であるならば、任意の整数 $\alpha_1, \ldots, \alpha_q$ に対して、連立合同式

$$
\begin{aligned}
\omega &\equiv \alpha_1 \pmod{a_1} \\
\omega &\equiv \alpha_2 \pmod{a_2} \\
&\vdots \\
\omega &\equiv \alpha_q \pmod{a_q}
\end{aligned}
$$

は、必ず解 ω を持つ。

合同方程式の解の個数（定理26）

r 次の合同式 $a_r x^r + \cdots + a_0 \equiv 0 \pmod{p}$ は、素イデアル p を法として、高々 r 個の解しか持たない。

意味：イデアルの世界でも、連立方程式を解き、解の個数を評価するという、洗練された操作が可能になる。

第三部：素イデアルが作る「世界」の構造を探る

素数 p を法とする世界 $\mathbb{Z}/p\mathbb{Z}$ は、乗法構造が巡回群となる美しい体（有限体）をなす。
同様に、素イデアル p を法とする世界 k/p もまた、$n(p) = p^f$ 個の元を持つ有限体をなす。

新たな主役の登場 (from §9)

原始数（Primitivzahl）θ

p を法として、その冪 $\theta, \theta^2, \ldots, \theta^{(n(p)-1)}$ が、p と素な全ての剰余類を生成する数。
これは、古典的な整数論における「原始根」の完璧なアナロジーである。

原始数の存在（定理28）

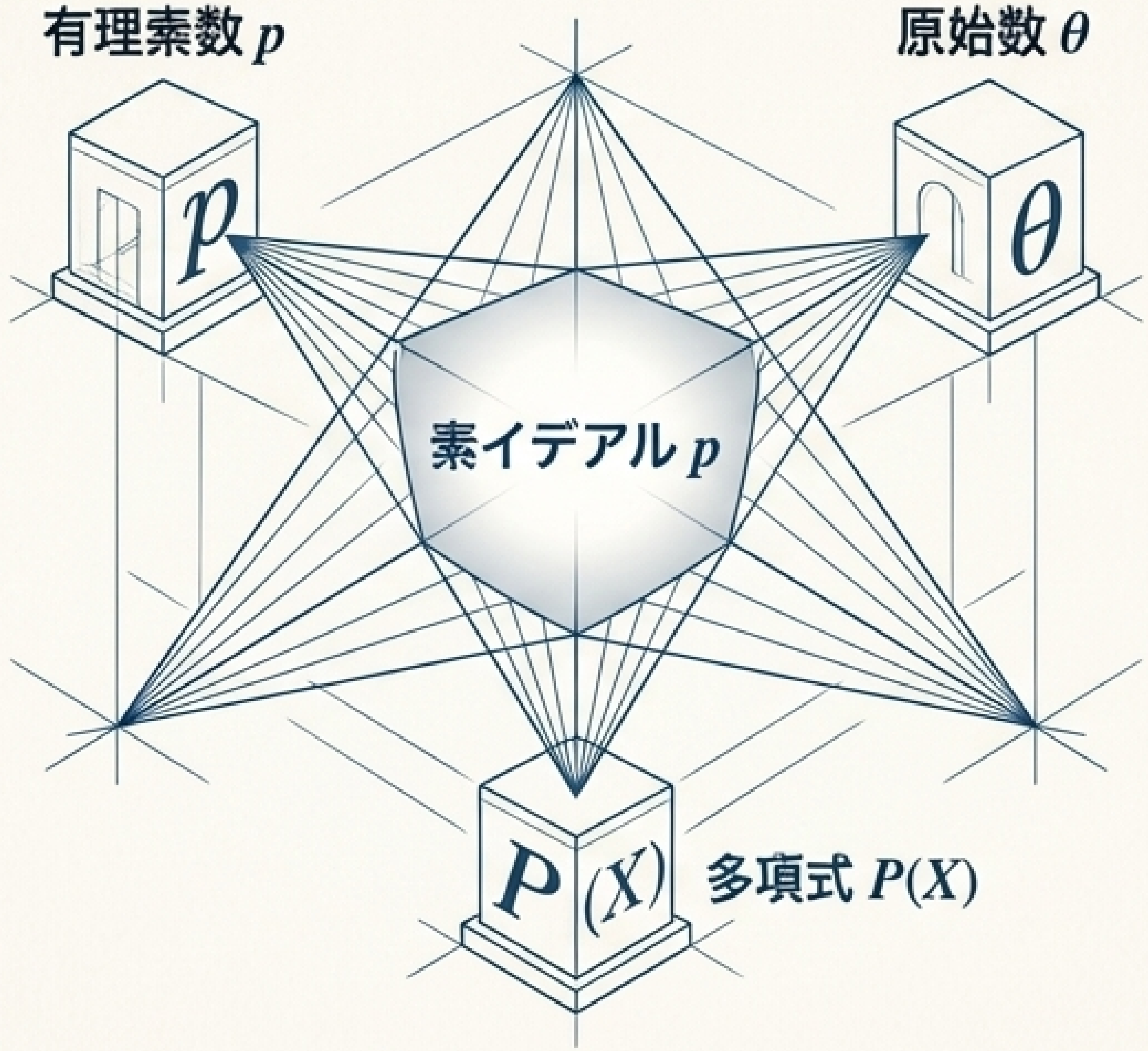
任意の素イデアル p に対して、原始数は常に $\Phi(n(p)-1)$ 個存在する。

解説：原始数の存在は、p を法とする複雑な世界が、たった一つの元の冪乗というシンプルなルールで記述できることを保証する。

集大成：素イデアルの具体的表現

定理30（from §10）

次数 f の素イデアル $\mathfrak{p}$ が与えられたとき、体の整数 θ（定理29で述べられた性質を持つ原始数）と、次数 f の有理係数多項式 $P(X)$ が存在して、右のように表せる。



$$\mathfrak{p} = (p, P(\theta))$$

この定理の威力

抽象から具体へ： 捉えどころのなかった素イデアル $\mathfrak{p}$ が、有理素数 p と、原始数 θ の値 $P(\theta)$ という、たった2つの具体的な数で生成されるイデアルとして記述できた。

理論の統合： この表現は、素イデアルの「次数 f」、体の整数「θ」、有理素数「p」という、これまでの議論の要素を一つに結びつけている。

構築の完了、そして次なる地平へ

我々が達成したこと

- 有理整数環 $\mathbb{Z}$ の算術（大きさ、合同、剰余類）を、一般の代数体におけるイデアルの算術として見事に再構築した。
- 素イデアル p を $(p, P(\theta))$ の形で具体的に表現する手法を獲得した。

新たなる問いの始まり (from §10)

ヒルベルトは次に「体の判別式 d」の議論へと進む。

$$\boxed{d = \det(\sigma_i(\omega_j))^2}$$

判別式の役割: イデアルの算術を用いて、今度は体そのものが持つ「個性」（どの素数が分岐するのか、など）を解明するための鍵となる。

イデアル算術の構築は、代数的整数論という壮大な理論の第一章に過ぎない。
この強固な土台の上に、さらなる深い構造が築かれていく。