

2 次形式（整数論）



alg-d

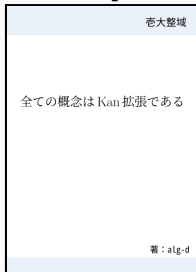
この講演は youtube でも配信されます
<https://www.youtube.com/live/4plTMAYUxZs>
(youtube 上に alg-d 以外の声は入りません)

このスライドは概要欄か ↓→ で DL 可
https://alg-d.com/math/number_theory/online10.pdf



自己紹介

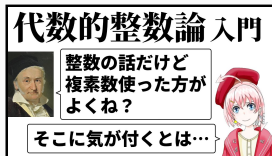
- alg-d twitter: https://x.com/alg_d
Youtube: <https://www.youtube.com/alg-dx>
WEB サイト: <https://alg-d.com/>
- 代表作 (?)
選択公理と同値な命題集 <https://alg-d.com/math/ac/>
常識的な圏論の PDF https://alg-d.com/math/kan_extension/



Amazon にて
好評発売中

- 専門: 代数的整数論
- 数学の中には「整数論」と呼ばれる分野があり
その中の一部として代数的整数論がある.

代数的整数論
の入門動画 ↓



代数的整数論入門

<https://www.youtube.com/watch?v=DCLXDwAZR5Q>

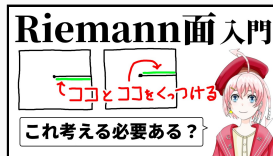
整数論で良く使う
Galois 理論の入門



代数体で Galois 理論
を触ってみる

<https://www.youtube.com/watch?v=21gAtZ5TpV8>

実質整数論である
Riemann 面の入門 ↓



Riemann 面の入門解説

<https://www.youtube.com/watch?v=0ZBfMUWy3po>

自己紹介

- 今日は整数論における **2 次形式** というものの話をします.
- 前提知識は, 整数や実数の四則演算が出来れば大丈夫です.
(途中から線型代数 (行列) を少し使います)
- まるで自分が詳しいものを紹介するような雰囲気を出しているが
今回話す内容の詳しい勉強を始めたのは 2026 年 8 月である.
何故勉強しているのかは最後まで聞くと分かる.

整数論とは

整数論とは

$0, 1, 2, \dots$ や $-1, -2, \dots$ を整数という.

整数の性質について調べる学問が「整数論」である.

??? 整数の性質 ???

整数については、古くから様々な問題が考えられてきた.

例えば以下のような問題がある.

整数論とは

- (1) 素数 p は整数 x, y を使って $p = \underline{x^2 + y^2}$ と書ける場合と書けない場合がある．例えば $5 = 1^2 + 2^2$, $13 = 2^2 + 3^2$, $37 = 1^2 + 6^2$ など書けるが, $7, 11, 23$ など書けない．書けるかどうか簡単に判定する方法はあるか？
- (2) $\underline{x^2 + y^2 = z^2}$ となる整数として例えば $x = 3, y = 4, z = 5$ があるが, このような整数 x, y, z は無限に存在するか？
- (3) $\underline{x^2 - xy - y^2} = 1$ となる整数 x, y は何があるか？
- (4) N を自然数とする． $\underline{x^2 + y^2 + z^2 + w^2} = N$ となるような整数 x, y, z, w は存在するか？

こういうが「整数の性質」で、これを調べるのが整数論．
ところで今回挙げた問題はどれも「2次」の式が使われている．

2 次形式

そこで次のように定義する.

【定義】

n 個の変数 $x_1, \dots, x_n$ についての, 次の式を **2 次形式** という.

$$\sum_{i,j=1}^n a_{ij}x_ix_j \quad (a_{ij} \text{ は整数の定数})$$

【例】

次のような式は 2 次形式である.

$$x^2, \quad x^2 + y^2, \quad 3xz - 2yz$$

2 次形式

2 次形式を使えば，さっきの問題は次のように解釈できる．

- (1) 素数 p は整数 x, y を使って $p = x^2 + y^2$ と書ける場合と書けない場合がある．例えば $5 = 1^2 + 2^2$ ， $13 = 2^2 + 3^2$ ， $37 = 1^2 + 6^2$ などは書けるが， $7, 11, 23$ などは書けない．書けるかどうか簡単に判定する方法はあるか？



$x^2 + y^2$ という 2 次形式に対して，
整数 x, y を動かしたときに現れる素数はどのようなものか？
(現れる素数を簡単に書き表せるか？)

2 次形式

(2) $x^2 + y^2 = z^2$ となる整数として例えば $x = 3$, $y = 4$, $z = 5$ があるが, このような整数 x, y, z は無限に存在するか?

↓

$x^2 + y^2 - z^2$ という 2 次形式の値が 0 になるような整数 x, y, z は無限に存在するか?

(3) $x^2 - xy - y^2 = 1$ となる整数 x, y は何があるか?

↓

$x^2 - xy - y^2$ という 2 次形式の値が 1 になるような整数 x, y はどのようなものか?

2 次形式

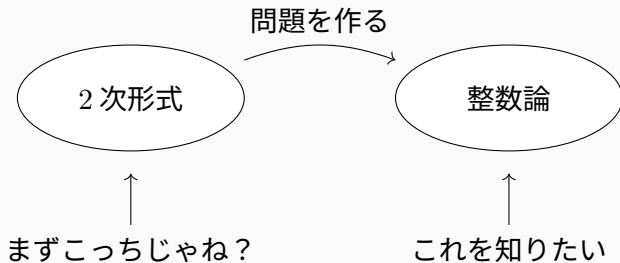
(4) N を自然数とする． $x^2 + y^2 + z^2 + w^2 = N$ となるような整数 x, y, z, w は存在するか？

↓

$x^2 + y^2 + z^2 + w^2$ という 2 次形式の値として現れる自然数はどのようなものか？

2次形式

このように多くの問題は2次形式から作られているから、整数について知るために、まずは2次形式のことを知るとよいのではないかと、という考え方が出てくる。



2 次形式

ここで最初の問題を考える

整数 x, y により $p = x^2 + y^2$ と書ける素数 p は？

この問題は $x^2 + y^2$ という 2 次形式が使われている。

2 次形式を変えれば（似たような）別の問題が得られる。

例えば $x^2 + 5y^2$ を使うと次のようになる。

整数 x, y により $p = x^2 + 5y^2$ と書ける素数 p は？

例えば $x^2 - 8y^2$ を使うと次のようになる。

整数 x, y により $p = x^2 - 8y^2$ と書ける素数 p は？

ちなみに問題の答え

本題からずれるが、ちなみに答えは以下ようになる。

【定理】

$p \neq 2$ を素数とするとき

$$\begin{aligned}\text{ある整数 } x, y \text{ により } p = x^2 + y^2 &\iff p \equiv 1 \pmod{4} \\ &\iff p \text{ を } 4 \text{ で割ると余り } 1\end{aligned}$$

【定義】

m, n, N を整数として $N > 0$ のとき

$m \div N$ の余りと $n \div N$ の余りが等しい

とき $m \equiv n \pmod{N}$ と書く。(余りは 0 から $N - 1$ で考える)

【定理】

$p \neq 2, 5$ を素数とするとき

$$\text{ある整数 } x, y \text{ により } p = x^2 + 5y^2 \iff p \equiv 1, 9 \pmod{20}$$

【定理】

$p \neq 2$ を素数とするとき

$$\text{ある整数 } x, y \text{ により } p = x^2 - 8y^2 \iff p \equiv 1 \pmod{8}$$

すうがく徒のつどい@オンライン

代数的整数論 類体論入門

これらの定理の証明は前の「つどい」で
やったので気になる人は
配信アーカイブをご覧ください。

<https://www.youtube.com/watch?v=MtFluwn36bk>

異なる 2 次形式とは

2 次形式から問題が作れる．2 次形式は無限個ある．

つまり問題も無限個作れる

……と言いたいが話はそんなに単純ではない．

$x^2 + 5y^2$ を使うと

整数 x, y により $p = x^2 + 5y^2$ と書ける素数 p は？

$5x^2 + y^2$ を使うと

整数 x, y により $p = 5x^2 + y^2$ と書ける素数 p は？

この 2 つの 2 次形式は式としては違うが、 $a + b = b + a$ だから
この 2 つの問題は数学的には同じ問題である．

異なる2次形式とは

このように2次形式 f から問題 $P(f)$ を作るとき
 $f \neq g$ だとしても、問題 $P(f)$ と $P(g)$ も"異なる"とは限らない。

例えば今の例は、 $P(f)$ で問題

整数 x, y により $p = f(x, y)$ と書ける素数 p は？

を表したときに $f(x, y) = x^2 + 5y^2$ と $g(x, y) = 5x^2 + y^2$ を考える
と式としては $f \neq g$ だけど、問題としては $P(f) = P(g)$ では？
ということ。

※問題の $=$ とは何かという話もあるが

今回そこはあまり深く考えないことにする。

異なる 2 次形式とは

今の例は当たり前すぎるので、もう少し複雑な例を挙げる．

2 次形式 $f(x, y) = x^2 + y^2$ に対して変数変換

$$x = 2u + v$$

$$y = 3u + 2v$$

を考えることで $g(u, v) = f(2u + v, 3u + 2v)$ が得られる．

$$\begin{aligned} g(u, v) &= (2u + v)^2 + (3u + 2v)^2 \\ &= (4u^2 + 4uv + v^2) + (9u^2 + 12uv + 4v^2) \\ &= 13u^2 + 16uv + 5v^2 \end{aligned}$$

となるから $g(u, v) = 13u^2 + 16uv + 5v^2$ である．

異なる 2 次形式とは

この変数変換は逆変換 $\begin{cases} u = 2x - y \\ v = -3x + 2y \end{cases}$ を持つ.

これが"逆"なのは, 実際 $g(u, v)$ に代入してみると

$$\begin{aligned} g(2x - y, -3x + 2y) &= 13(2x - y)^2 + 16(2x - y)(-3x + 2y) \\ &\quad + 5(-3x + 2y)^2 \\ &= 13(4x^2 - 4xy + y^2) \\ &\quad + 16(-6x^2 + 7xy - 2y^2) \\ &\quad + 5(9x^2 - 12xy + 4y^2) \\ &= x^2 + y^2 = f(x, y) \end{aligned}$$

となり元に戻るから分かる.

異なる 2 次形式とは

この変数変換を使えば、素数 p に対して次が成り立つ.

ある整数 x, y により $p = x^2 + y^2$ と書ける

$\iff$ ある整数 u, v により $p = 13u^2 + 16uv + 5v^2$ と書ける

$f(x, y) = x^2 + y^2$ を使うと

整数 x, y により $p = x^2 + y^2$ と書ける素数 p は？

$g(u, v) = 13u^2 + 16uv + 5v^2$ を使うと

整数 u, v により $p = 13u^2 + 16uv + 5v^2$ と書ける素数 p は？

この 2 つも実質同じ問題である.

異なる 2 次形式とは

この問題に限らず

$$f(x, y) = x^2 + y^2, \quad g(u, v) = 13u^2 + 16uv + 5v^2$$

に対して、問題 $P(f)$ と $P(g)$ を考えれば $P(f) = P(g)$ だと思われる。

このように、互いに変数変換で移りあうような 2 次形式は
「2 次形式から問題を作る」という状況においては
実質同じものであると言って良さそうである。

異なる 2 次形式とは

【定義】

2 つの 2 次形式

$$f(x, y) = ax^2 + bxy + cy^2, \quad g(x, y) = a'x^2 + b'xy + c'y^2$$

を考える．これらが整数 a_i, b_i を使った変数変換により

$$f(a_0x + a_1y, a_2x + a_3y) = g(x, y)$$

$$g(b_0x + b_1y, b_2x + b_3y) = f(x, y)$$

と互いに変換できるとき， f と g は**同値**であるという．

より一般に n 変数の 2 次形式も考えることができるが
ここでは簡単のため一旦 2 変数にしておく．

異なる 2 次形式とは

この定義をしたとき、まず考えたいのは

同値でない 2 次形式は無限個あるのか？

ということである．

もし有限個しか無いのであれば
2 次形式から問題を作るというのは
意外と大したことがない、という話になる．

このことについて考えるため、次の定義をする．

判別式

【定義】

2 変数の 2 次形式 $f(x, y) = ax^2 + bxy + cy^2$ に対して $b^2 - 4ac$ を f の判別式といい D_f で表す.

【命題】

どんな 2 次形式 $f(x, y) = ax^2 + bxy + cy^2$ に対しても $D_f \equiv 0, 1 \pmod{4}$ となる.

証明.

以下 mod 4 で考える. 明らかに $D_f \equiv b^2$ である.

$$b = 2k \implies D_f \equiv (2k)^2 = 4k^2 \equiv 0.$$

$$b = 2k + 1 \implies D_f \equiv (2k + 1)^2 = 4k^2 + 4k + 1 \equiv 1. \quad \square$$

$$f(x, y) = ax^2 + bxy + cy^2$$

に対して $D_f = b^2 - 4ac$

【命題】

整数 D が $D \equiv 0, 1 \pmod{4}$ を満たすとき
 $D_f = D$ となる 2 次形式 $f(x, y)$ が存在する。

証明.

$D \equiv 0 \pmod{4}$ のとき, $f(x, y) = x^2 - \frac{D}{4}y^2$ とすれば

$$D_f = 0^2 - 4 \cdot 1 \cdot \left(-\frac{D}{4}\right) = D \text{ である.}$$

$D \equiv 1 \pmod{4}$ のとき, $f(x, y) = x^2 + xy - \frac{D-1}{4}y^2$ とすれば

$$D_f = 1^2 - 4 \cdot 1 \cdot \left(-\frac{D-1}{4}\right) = D \text{ である.} \quad \square$$

$$f(x, y) = ax^2 + bxy + cy^2$$

に対して $D_f = b^2 - 4ac$

【命題】

2 次形式 $f(x, y)$ と $g(x, y)$ が同値なとき $D_f = D_g$ である.

証明.

$f(x, y) = ax^2 + bxy + cy^2$ と $g(x, y) = a'x^2 + b'xy + c'y^2$ が同値であるとする. 即ち変数変換により

$$f(a_0x + a_1y, a_2x + a_3y) = g(x, y)$$

$$g(b_0x + b_1y, b_2x + b_3y) = f(x, y)$$

となっているとする.

$$f(x, y) = ax^2 + bxy + cy^2$$

に対して $D_f = b^2 - 4ac$

証明.

$$\begin{aligned} g(x, y) &= f(a_0x + a_1y, a_2x + a_3y) \\ &= a(a_0x + a_1y)^2 + b(a_0x + a_1y)(a_2x + a_3y) \\ &\quad + c(a_2x + a_3y)^2 \\ &= (aa_0^2x^2 + 2aa_0a_1xy + aa_1^2y^2) \\ &\quad + (ba_0a_2x^2 + (ba_0a_3 + ba_1a_2)xy + ba_1a_3y^2) \\ &\quad + (ca_2^2x^2 + 2ca_2a_3xy + ca_3^2y^2) \\ &= (aa_0^2 + ba_0a_2 + ca_2^2)x^2 \\ &\quad + (2aa_0a_1 + ba_0a_3 + ba_1a_2 + 2ca_2a_3)xy \\ &\quad + (aa_1^2 + ba_1a_3 + ca_3^2)y^2 \end{aligned}$$

$$f(x, y) = ax^2 + bxy + cy^2$$

に対して $D_f = b^2 - 4ac$

証明.

$$\begin{aligned} g(x, y) &= (aa_0^2 + ba_0a_2 + ca_2^2)x^2 \\ &\quad + (2aa_0a_1 + ba_0a_3 + ba_1a_2 + 2ca_2a_3)xy \\ &\quad + (aa_1^2 + ba_1a_3 + ca_3^2)y^2 \end{aligned}$$

となるから $g(x, y)$ の判別式 D_g は

$$\begin{aligned} &(2aa_0a_1 + ba_0a_3 + ba_1a_2 + 2ca_2a_3)^2 \\ &\quad - 4(aa_0^2 + ba_0a_2 + ca_2^2)(aa_1^2 + ba_1a_3 + ca_3^2) \end{aligned}$$

である.

$$f(x, y) = ax^2 + bxy + cy^2$$

に対して $D_f = b^2 - 4ac$

証明.

この D_g のそれぞれの項は

$$\begin{aligned} (\text{第1項}) &= (2aa_0a_1 + ba_0a_3 + ba_1a_2 + 2ca_2a_3)^2 \\ &= 4a^2a_0^2a_1^2 + \underline{b^2a_0^2a_3^2} + \underline{b^2a_1^2a_2^2} + 4c^2a_2^2a_3^2 \\ &\quad + 4aba_0^2a_1a_3 + 4aba_0a_1^2a_2 + \underline{8aca_0a_1a_2a_3} \\ &\quad + \underline{2b^2a_0a_1a_2a_3} + 4bca_0a_2a_3^2 + 4bca_1a_2^2a_3 \end{aligned}$$

$$\begin{aligned} -\frac{1}{4}(\text{第2項}) &= (aa_0^2 + ba_0a_2 + ca_2^2)(aa_1^2 + ba_1a_3 + ca_3^2) \\ &= a^2a_0^2a_1^2 + aba_0^2a_1a_3 + \underline{aca_0^2a_3^2} + aba_0a_1^2a_2 \\ &\quad + \underline{b^2a_0a_1a_2a_3} + bca_0a_2a_3^2 \\ &\quad + \underline{aca_1^2a_2^2} + bca_1a_2^2a_3 + c^2a_2^2a_3^2 \end{aligned}$$

$$f(x, y) = ax^2 + bxy + cy^2$$

に対して $D_f = b^2 - 4ac$

証明.

よってさっきの下線部分だけが残って

$$\begin{aligned} D_g &= b^2(a_0^2a_3^2 + a_1^2a_2^2 - 2a_0a_1a_2a_3) \\ &\quad - 4ac(-2a_0a_1a_2a_3 + a_0^2a_3^2 + a_1^2a_2^2) \\ &= (b^2 - 4ac)(a_0a_3 - a_1a_2)^2 \\ &= D_f X^2 \quad (X = a_0a_3 - a_1a_2) \end{aligned}$$

となる．即ち D_g は D_f の倍数である．

同様の計算を D_f に対して行えば， D_f は D_g の倍数となる．

D_f と D_g は整数だから $D_f = \pm D_g$ である．

ところが $D_g = D_f X^2$ で X も整数だから $D_f = D_g$ である． $\square$

【命題】

整数 D が $D \equiv 0, 1 \pmod{4}$ を満たすとき
 $D_f = D$ となる 2 次形式 $f(x, y)$ が存在する.

【命題】

2 次形式 $f(x, y)$ と $g(x, y)$ が同値なとき $D_f = D_g$ である.

【定理】

無限個の、互いに同値でない 2 次形式が存在する. □

このように判別式を使うことで
2 次形式が"本当に"無限個あることが分かる.

判別式

判別式	2 次形式の例
0	x^2
1	$x^2 + xy$
4	$x^2 - y^2$
5	$x^2 + xy - y^2$
8	$x^2 - 2y^2$
9	$x^2 + xy - 2y^2$
12	$x^2 - 3y^2$
13	$x^2 + xy - 3y^2$
16	$x^2 - 4y^2$
17	$x^2 + xy - 4y^2$
$\vdots$	$\vdots$

これらは互いに同値でない 2 次形式である。

【命題】

2 次形式 $f(x, y)$ と $g(x, y)$ が同値なとき $D_f = D_g$ である.

またこの命題の対偶を考えれば

$$D_f \neq D_g \implies f \text{ と } g \text{ は同値でない}$$

となる. つまり判別式は 2 次形式の "判別" に使える.

ところが $D_f = D_g$ だからと言って $f(x, y)$ と $g(x, y)$ が同値とは限らない.

【例】

$f(x, y) := 2xy$, $g(x, y) := x^2 - y^2$ とする.
 $D_f = 4 = D_g$ だが f と g は同値ではない.

証明.

まず $g(1, 0) = 1$ である.

もし f と g が同値なら, ある整数 a, b により $f(a, b) = 1$ となるはずである.

ところが明らかに $f(a, b) = 2ab$ は 2 の倍数であるから, このような a, b は存在しない. 即ち f と g は同値ではない. $\square$

そこで整数 D が与えられたときに「 $D_f = D$ となる 2 次形式 $f(x, y)$ はどのくらいあるのか？」という問題が気になるわけである。

実はこれは Lagrange が答えを見つけていた¹ らしく次の定理のようになる。

【定理】

与えられた判別式 $D \neq 0$ を持つ 2 変数 2 次形式のうち同値でないものは有限個しか存在しない。

ここでは $D < 0$ の場合の証明方法を紹介する。
($D > 0$ も似たような感じで出来る)

¹1775 年の論文らしい。

これを示すには，次の定理を示せばよい．

【定理】

$D < 0$ が与えられたとする． $D_f = D$ となる f は，次を満たす 2 次形式 $g(x, y) = Ax^2 + Bxy + Cy^2$ と同値である²．

$$|A|, |B|, |C| \leq |D|$$

この条件を満たす g はもちろん有限個しかない．

²実際はもっと厳しく条件を付けることができる．

判別式

$f(x, y) = ax^2 + bxy + cy^2$ が $D_f = D < 0$ を満たすとする.
簡単のためここでは $a > 0$ の場合のみ考える.

($a < 0$ の場合は全体を -1 倍した 2 次形式 $-ax^2 - bxy - cy^2$ について考えればよい)

これが $g(x, y) = Ax^2 + Bxy + Cy^2$ ($|A|, |B|, |C| \leq |D|$) と同値にできることを示すのがこれからの目標.

まず $D_f = b^2 - 4ac < 0$ だから $b^2 < ac$ である.

即ち $0 < \frac{b^2}{a} < c$ となり, この場合 $c > 0$ も分かる.

次に整数 n に対する

さっきの変数変換 $\begin{cases} x = u + nv \\ y = v \end{cases}$ を考えると

(これは逆変換を持つことが分かる．即ち判別式を変えない)

$$\begin{aligned} f(u + nv, v) &= a(u + nv)^2 + b(u + nv)v + cv^2 \\ &= (au^2 + 2anuv + an^2v^2) + (buv + bnv^2) + cv^2 \\ &= au^2 + (2an + b)uv + (an^2 + bn + c)v^2 \end{aligned}$$

となる．このとき n を上手く選ぶことで次のようにできる．

$$|2an + b| \leq |a|$$

【例】

$f(x, y) = x^2 + 5xy + 7y^2$ を考える. $D_f = 5^2 - 4 \cdot 1 \cdot 7 = -3$

変数変換 $\begin{cases} x = u + nv \\ y = v \end{cases}$ を考えると

$$\begin{aligned} f(u + nv, v) &= (u + nv)^2 + 5(u + nv)v + 7v^2 \\ &= u^2 + (2n + 5)uv + (n^2 + 5n + 7)v^2 \end{aligned}$$

となる. そこで $n = -2$ とすれば $|2n + 5| \leq |a| = 1$ で

$$f(u - 2v, v) = u^2 + uv + v^2$$

である. (この場合, これで $|A|, |B|, |C| \leq |D| = 3$ になっている) □

実は $0 < a \leq |D|$ の場合は必ずこれで上手くいく.

【命題】

$f(x, y) = ax^2 + bxy + cy^2$ が

$$D_f = D < 0, \quad 0 < a \leq |D|$$

を満たすとする (このとき $c > 0$ も成り立つ).

このとき $|2an + b| \leq |a|$ となる n を取り $\begin{cases} x = u + nv \\ y = v \end{cases}$ と

変数変換した結果を $g(u, v) = au^2 + Buv + Cv^2$ と書くと
 $|C| \leq |D|$ である (もちろん $|a|, |B| \leq |D|$ も成立).

【命題】

$|a|, |B|, |C| \leq |D|$ である.

証明.

まず $D_g = D$ だから $B^2 - 4aC = D$ である.

よって $4aC = B^2 - D = B^2 + |D| > 0$ となり $C > 0$ である.

$$4aC = B^2 + |D| \leq a^2 + |D|$$

だから $a \leq |D|$ と $a \geq 1$ (即ち $\frac{1}{a} \leq 1$) を使うと

$$C \leq \frac{a}{4} + \frac{|D|}{4a} \leq \frac{|D|}{4} + \frac{|D|}{4} \leq |D|$$

□

$f(x, y) = ax^2 + bxy + cy^2$ が $a \leq |D|$ を満たす場合は OK.

一方で $a > |D|$ を満たす場合は

変数変換 $\begin{cases} x = u + nv \\ y = v \end{cases}$ では a は変わらないから

当然 $|a| \leq |D|$ にはできない.

【例】

$f(x, y) = 10x^2 + 26xy + 17y^2$ を考える.

$D_f = 26^2 - 4 \cdot 10 \cdot 17 = -4$ (よって $a > |D|$ である.)

変数変換 $\begin{cases} x = u + nv \\ y = v \end{cases}$ を考えると

$$\begin{aligned} f(u + nv, v) &= 10(u + nv)^2 + 26(u + nv)v + 17v^2 \\ &= 10u^2 + (20n + 26)uv + (10n^2 + 26n + 17)v^2 \end{aligned}$$

となる. そこで $n = -1$ とすれば $|20n + 26| \leq |a| = 10$ で

$$f(u - v, v) = 10u^2 + 6uv + v^2$$

である. (この場合, これで $|A|, |B| \leq |D| = 4$ にならない) $\square$

【命題】

$f(x, y) = ax^2 + bxy + cy^2$ が

$$D_f = D < 0, \quad a > |D|$$

を満たすとする.

このとき $|2an + b| \leq |a|$ となる n を取り $\begin{cases} x &= u + nv \\ y &= v \end{cases}$ と

変数変換した結果を

$$g(u, v) = au^2 + Buv + Cv^2$$

と書くと $0 < C < a$ である.

【命題】

$a > |D|$ のとき $0 < C < a$ である.

証明.

さっきと同様 $4aC = B^2 - D = B^2 + |D| > 0$ から $C > 0$.

これを踏まえて背理法を使う. $0 < C < a$ でないと仮定する.
 $C > 0$ は成り立つから $a \leq C$ である.

よって n の取り方から $|B| \leq a$ なので

$$|D| = 4aC - B^2 \geq 4aC - a^2 \geq 4aC - aC = 3aC$$

$|D|$ も a も C も正の整数だから $a \leq |D|$ となり, 矛盾. □

というわけで $a > |D|$ の場合は変数変換すると

$$au^2 + Buv + Cv^2, \quad |B| \leq a, \quad 0 < C < a$$

となる．よって変数 u と v を入れ替えれば， $f(x, y)$ は

$$Cu^2 + Buv + av^2, \quad |B| \leq a, \quad 0 < C < a$$

と同値になる．こうして最初の係数を小さくすることができる．

もし $C \leq |D|$ だったら，もう一度 n による変数変換をすれば全部 $|D|$ 以下にできる．

$C \leq |D|$ でない場合は，更に変数変換することで係数を C より小さくできる．

判別式

こうして変数変換を繰り返すことで、 $D_f = D < 0$ となる f は次を満たす 2 次形式 $g(x, y) = Ax^2 + Bxy + Cy^2$ に変形できる.

$$|A|, |B|, |C| \leq |D|, \quad B^2 - 4AC = D$$

【例】

さっきの $f(x, y) = 10x^2 + 26xy + 17y^2$ の場合

変数変換 $\begin{cases} x = u - v \\ y = v \end{cases}$ を考えると

$$f(u - v, v) = 10u^2 + 6uv + v^2$$

A と C を入れ替えて $g(x, y) = x^2 + 6xy + 10y^2$ を考えると変数

変換 $\begin{cases} x = u - 3v \\ y = v \end{cases}$ により

$$g(u - 3v, v) = u^2 + v^2$$

つまり $10x^2 + 26xy + 17y^2$ は $x^2 + y^2$ と同値になる.

□

こういう感じで次の定理が証明できる.

【定理】

与えられた判別式 $D \neq 0$ を持つ 2 変数 2 次形式のうち
同値でないものは有限個しか存在しない.



【例】

$D_f = -3$ となる $f(x, y) = ax^2 + bxy + cy^2$ ($a > 0$) は

$$0 < A \leq 3, \quad |B| \leq 3, \quad |C| \leq 3$$

となる $g(x, y) = Ax^2 + Bxy + Cy^2$ と同値になる.

$D_g = -3$ となる A, B, C は右の 6 通り.

A と C は入れ替えられるから

実質上の 4 通り. つまり

$$x^2 \pm xy + y^2, \quad x^2 \pm 3xy + 3y^2$$

と同値になる.

A	B	C
1	1	1
1	-1	1
1	3	3
1	-3	3
3	3	1
3	-3	1

【例】

$x^2 - xy + y^2$ は $n = 1$ の変換をすれば

$$(u + v)^2 - (u + v)v + v^2 = u^2 + uv + v^2$$

$x^2 + 3xy + 3y^2$ は $n = -1$ の変換をすれば

$$(u - v)^2 + 3(u - v)v + 3v^2 = u^2 + uv + v^2$$

$x^2 - 3xy + 3y^2$ は $n = 2$ の変換をすれば

$$(u + 2v)^2 - 3(u + 2v)v + 3v^2 = u^2 + uv + v^2$$

となり、全て $x^2 + xy + y^2$ と同値になる。

【例】

つまり $D_f = -3$ となる $f(x, y) = ax^2 + bxy + cy^2$ ($a > 0$) は
全て $x^2 + xy + y^2$ と同値になる. □

【例】

$D_f = -20$ となる $f(x, y) = ax^2 + bxy + cy^2$ ($a > 0$) は
 $x^2 + 5y^2$ か $2x^2 \pm 2xy + 3y^2$ と同値になる. □

というわけで、2次形式というものについて
少しずつ分かってきたのではないだろうか。

より一般の場合を考える

より一般の場合を考える

整数論について考えていたから、ここまでは整数のみを考えてきたが、2次形式の係数や変数の値としては「有理数」「実数」「複素数」なども考えることができる。(何故考えるのかというのはここでは置いておく。)例えば実数を考える場合は実係数の2次形式という。念のため定義すると次のようになる。

【定義】

n 個の変数 $x_1, \dots, x_n$ についての

$$\sum_{i,j=1}^n a_{ij}x_ix_j \quad (a_{ij} \text{ は実数の定数})$$

という形の式を**実係数の2次形式**という。

休憩

休憩中でありスライドに意味はありません！

【定理】

$f(x_1, \dots, x_n)$ を整数係数の 2 次形式とするととき、

$f(x_1, \dots, x_n) = 0$ が非自明な整数解を持つ

$\iff f(x_1, \dots, x_n) = 0$ が非自明な実数解を持ち、更に任意の素数 p に対して $f(x_1, \dots, x_n) = 0$ が非自明な p 進数解を持つ。

整数解を持つか判定するよりも、実数解を持つか判定する方が遥かに簡単である。

実は p 進数解を持つか判定するのも（整数に比べれば遥かに）簡単である。

無限個調べる必要が出るものの、整数解の判定を簡単にしてくれる定理である。

休憩中でありスライドに意味はありません！

p 進数については入門動画があるのでそちらをご覧ください。



【闇からの解放】 p 進数入門【整数論】

<https://www.youtube.com/watch?v=Lrj0STboq4o>

実係数の2次形式

実係数の 2 次形式

実数の場合は $b_{ij} = \frac{a_{ij} + a_{ji}}{2}$ と定義でき、 $b_{ij} = b_{ji}$ であり更に

$$\sum_{i,j=1}^n a_{ij}x_i x_j = \sum_{i,j=1}^n b_{ij}x_i x_j$$

である．例えば

$$x^2 + xy + y^2 = x^2 + \frac{1}{2}xy + \frac{1}{2}yx + y^2$$

である．つまり実係数の場合の 2 次形式は $a_{ij} = a_{ji}$ としても問題無い．そこで以下そのようにしておく．

(このようにする理由はこの後分かる．)

実係数の 2 次形式

2 次形式は行列の記法を使えば

$$\begin{aligned} f(x_1, \dots, x_n) &= \sum_{i,j=1}^n a_{ij} x_i x_j \\ &= \begin{pmatrix} x_1 & \cdots & x_n \end{pmatrix} \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \end{aligned}$$

と書くことができる．（この行列 (a_{ij}) を A_f と書くことにする）

実係数の 2 次形式

更に変数変換

$$\begin{cases} x_1 &= b_{11}y_1 + \cdots + b_{1n}y_n \\ &\vdots \\ x_n &= b_{n1}y_1 + \cdots + b_{nn}y_n \end{cases} \quad (b_{ij} \text{ は実数})$$

も行列を使って

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{n1} & \cdots & b_{nn} \end{pmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

と表示することができる．（この行列 (b_{ij}) を P とする）
この変換の「逆変換」があるというのは、 P が正則行列（逆行列を持つ）ということである．

実係数の 2 次形式

実係数の 2 次形式

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = P \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \quad \text{だから} \quad (x_1 \ \cdots \ x_n) = (y_1 \ \cdots \ y_n) {}^tP$$

$$f(x_1, \cdots, x_n) = (x_1 \ \cdots \ x_n) A_f \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

を変数変換して得られる 2 次形式を $g(y_1, \cdots, y_n)$ とすると

$$g(y_1, \cdots, y_n) = (y_1 \ \cdots \ y_n) {}^tP A_f P \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

となる．(${}^tP$ は転置行列)

実係数の 2 次形式

$$g(y_1, \dots, y_n) = \begin{pmatrix} y_1 & \cdots & y_n \end{pmatrix} {}^t P A_f P \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

そこで次のように定義できる.

【定義】

f と g を実係数の n 変数 2 次形式とする.

f と g が**同値**

$\iff$ ある $n \times n$ 実正則行列 P を使って $A_g = {}^t P A_f P$ とできる.

実係数の 2 次形式

2 次形式 $f(x_1, \dots, x_n) = \sum_{i,j=1}^n a_{ij}x_i x_j$ においては $a_{ij} = a_{ji}$ と仮定

しているから

$$A_f = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}$$

は対称行列である.

【定理】

対称行列は直交行列により対角化できる.



実係数の 2 次形式

行列の対角化というのは

$$A_f = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}$$

があったとき, P を上手く取ること

$$P^{-1}A_fP = \begin{pmatrix} c_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & c_n \end{pmatrix} \quad (c_i \text{ は実数, 対角以外は全て } 0)$$

とすることができる. ここで P が直交行列というのは

$$P^{-1} = {}^tP \quad (P^{-1} \text{ は逆行列})$$

という意味である.

実係数の 2 次形式

よって A_f を対角化する直交行列 P を取れば $f(x_1, \dots, x_n)$ を

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = P \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

と変数変換して得られるのは

$$\begin{aligned} g(y_1, \dots, y_n) &= \begin{pmatrix} y_1 & \cdots & y_n \end{pmatrix} {}^t P A_f P \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \\ &= c_1 y_1^2 + \cdots + c_n y_n^2 \end{aligned}$$

実係数の 2 次形式

変数の順番を入れ替えることで

$$c_1 \neq 0, \dots, c_m \neq 0, c_{m+1} = \dots = c_n = 0$$

とすることができる。つまり

$$g(y_1, \dots, y_n) = c_1 y_1^2 + \dots + c_m y_m^2$$

である。更に $y_i = z_i / \sqrt{|c_i|}$ と変数変換して、変数の順番を変えれば

$$z_1^2 + \dots + z_k^2 - z_{k+1}^2 - \dots - z_m^2$$

となる。つまり（整数ではなく）実数の範囲で考える場合 2 次形式は必ずこのような簡単な形で表せる。

実係数の 2 次形式

ここで変数の数について注意しておく． $f(x_1, \dots, x_n)$ を

$$c_1 y_1^2 + \dots + c_n y_n^2$$

$$c_1 \neq 0, \dots, c_m \neq 0, c_{m+1} = \dots = c_n = 0$$

と書いたとき， f は表記上は n 変数だが，実質的には m 変数である．こういう場合，初めから m 変数として扱っておいた方が良さそうである．そこで次の定義をする．

【定義】

$f(x_1, \dots, x_n)$ が**非退化**

$\iff f$ を変数変換して $c_1 y_1^2 + \dots + c_n y_n^2$ の形にしたとき
 $c_1, \dots, c_n$ は全て $\neq 0$ である．

線型代数を使えば，これは A_f が正則行列と言い換えられる．

【定理】

n 変数の非退化な実係数 2 次形式 $f(x_1, \dots, x_n)$ は実質

$$\begin{aligned} & x_1^2 + x_2^2 + \cdots + x_{n-1}^2 + x_n^2 \\ & x_1^2 + x_2^2 + \cdots + x_{n-1}^2 - x_n^2 \\ & \vdots \\ & x_1^2 - x_2^2 - \cdots - x_{n-1}^2 - x_n^2 \\ & -x_1^2 - x_2^2 - \cdots - x_{n-1}^2 - x_n^2 \end{aligned}$$

の $n+1$ 通りしかない。



この $n+1$ 個は、それぞれ同値ではない。

つまり n 変数の非退化なものは丁度 $n+1$ 個あると言ってよい。

実係数の 2 次形式

これは言い換えると，整数 $p, q \geq 0$ に対して
($p + q$) 変数の非退化な実係数 2 次形式

$$x_1^2 + \cdots + x_p^2 - y_1^2 - \cdots - y_q^2$$

が得られて，これが非退化な実係数 2 次形式の全てである．

※但し，これだと $p = q = 0$ の場合に"無"の式が出てしまうが，
ここではこれを「0 変数の非退化な実係数 2 次形式」として認めることにする．

実係数の 2 次形式

つまり，同値な 2 次形式は"等しい"と思ってしまえば，2 つの集合

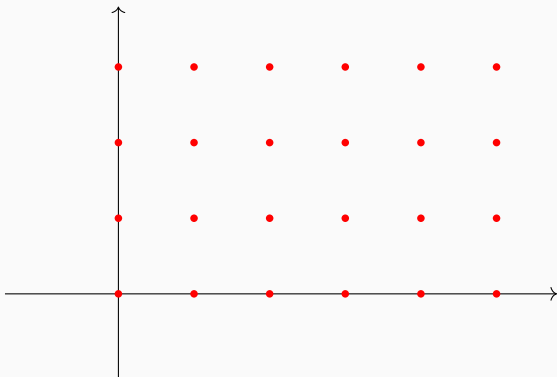
$$\{f \mid f \text{ は非退化な実係数 2 次形式} \}$$

$$\{(p, q) \mid p, q \geq 0 \text{ は整数} \}$$

は実質同じ集合だと思えるということである．

実係数の 2 次形式

絵で描くと，次の赤点が非退化な実係数 2 次形式である．



実係数の 2 次形式

(集合論が分かる人向け)

これは $X := (\text{非退化な実係数 2 次形式})$ として
 $\cong$ で 2 次形式の同値を表せば全単射

$$F: X/\cong \rightarrow \mathbb{N} \times \mathbb{N}$$

が存在するということである.

2 次形式同士の足し算

2 次形式同士の足し算

ここから先，なぜこのようなことを考えるのかについては説明しません．（難しい説明しか見つからなかったため）

こういう面白いことが出来るんだと思って楽しんでください．

まあ要するにこうすることで 2 次形式への理解が深まるということです．

2 次形式同士の足し算

2 つの実係数 2 次形式

$$f = \sum_{i,j=1}^n a_{ij}x_ix_j, \quad g = \sum_{i,j=1}^m b_{ij}y_iy_j$$

があったとき, そこから $(n+m)$ 変数の 2 次形式

$$f \oplus g := \sum_{i,j=1}^n a_{ij}x_ix_j + \sum_{i,j=1}^m b_{ij}y_iy_j$$

を作ることができる.

※ f と g の両方に同じ変数が含まれる場合, 片方の変数を取り換えて, 変数の重複を無くしてから $\oplus$ を考える.

2 次形式同士の足し算

言い換えれば $f \oplus g$ は行列

$$\begin{pmatrix} A_f & O \\ O & A_g \end{pmatrix}$$

で表される 2 次形式である.

このように 2 次形式の〈足し算〉を定義すると
さっきの"無"の 2 次形式を o と書けば

$$f \oplus o = f, \quad o \oplus f = f$$

となる.

2 次形式同士の足し算

【命題】

自然数，整数，実数などの足し算については

任意の x に対して $x + 0 = x$ と $0 + x = x$

が成り立つ.



つまり 2 次形式に $\oplus$ という〈足し算〉を定義すると

$$f \oplus o = f, \quad o \oplus f = f$$

となり， o はまるで 0 のような役割をしてくれる．

2 次形式同士の引き算

2 次形式の〈足し算〉が出来るのなら〈引き算〉はできるか？

〈引き算〉とは「マイナス元を足すこと」である．

【命題】

x が数（自然数，整数，実数など）のとき， $-x$ とは

$$x + y = 0$$

となるような数 y のことである．



つまり 2 次形式 f に対して $-f$ とは

$$f \oplus g = o$$

となる 2 次形式 g のことである．

2 次形式同士の引き算

$\oplus$ をすると変数の数が増えていくから、 g を足すことで 0 変数になることはありえない。

しかし次の定理が成り立つ。

($\cong$ は 2 次形式の同値を表す)

【定理】 (Witt cancellation)

f, g, h が実係数の非退化 2 次形式で $f \oplus h \cong g \oplus h$ のとき $f \cong g$ である。

□

つまり

$$f \oplus h \cong g \oplus h \implies f \cong g$$

という意味で、両辺から h を〈引き算〉してよいのである。

2 次形式同士の引き算

ところが実は Witt cancellation は整数の範囲では成り立たない.

【例】

$f(x, y) := 2xy$, $g(x, y) := x^2 - y^2$ とする.

さっき示した通り $f \not\cong g$ である.

次に $h(z) := z^2$ として

$f' := f \oplus h$ と $g' := g \oplus h$ を考える.

このとき $f' \cong g'$ となる.

2 次形式同士の引き算

証明.

まず

$$f'(x, y, z) = 2xy + z^2, \quad g'(x, y, z) = x^2 - y^2 + z^2$$

であり, これらを表す対称行列はそれぞれ

$$A_{f'} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad A_{g'} := \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

である.

2 次形式同士の引き算

証明.

そこで行列

$$P = \begin{pmatrix} -1 & -1 & 0 \\ 0 & 1 & -1 \\ -1 & -1 & 1 \end{pmatrix}$$

を考えると $\det(P) = -1$ だから P による変数変換は逆変換も整数係数であり、更に

2 次形式同士の引き算

証明.

$$\begin{aligned} {}^t P A_{f'} P &= \begin{pmatrix} -1 & 0 & -1 \\ -1 & 1 & -1 \\ 0 & -1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} -1 & -1 & 0 \\ 0 & 1 & -1 \\ -1 & -1 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 0 & -1 & -1 \\ 1 & -1 & -1 \\ -1 & 0 & 1 \end{pmatrix} \begin{pmatrix} -1 & -1 & 0 \\ 0 & 1 & -1 \\ -1 & -1 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = A_{g'} \end{aligned}$$

2 次形式同士の引き算

証明.

よって $f(x, y) = 2xy$, $g(x, y) = x^2 - y^2$, $h(z) = z^2$ のとき
 $f \not\equiv g$ だが $f \oplus h \cong g \oplus h$ である. □

こうして整数係数では, Witt cancellation は成立しない.
つまり 〈引き算〉 はできない.

※一般に, K が標数 2 でない体であれば, K 上の 2 次形式
について Witt cancellation が成り立つ.

ところが整数係数でも 〈引き算〉 を定義する方法があり,
それが Witt 群である.

Witt 群とは、ざっくり言うと「 $\text{mod } (x^2 - y^2)$ で考える」というものである。

【例】

自然数だけ考える場合、 $n > 0$ にはマイナス元は存在しない。
つまり

$$n + m = 0$$

となる m は無い。ところが $\text{mod } N$ で考えると

$$n + m \equiv 0 \pmod{N}$$

となる m は存在するから、これを $-n$ と思うことができる。 $\square$

まず実係数で考えると、非退化 2 次形式 f は必ず

$$x_1^2 + \cdots x_p^2 - y_1^2 - \cdots - y_q^2$$

という形に書けた．このとき $x^2 - y^2$ という形の部分があれば，そこは o として考えるのである．

【例】

$$x^2 + y^2 + z^2 - w^2 = x^2 + y^2$$

$$x^2 - y^2 - z^2 - w^2 = -z^2 - w^2$$

$f(x) = x^2$ と $g(x) = -x^2$ のとき

$$f \oplus g = x^2 - y^2 = o$$

つまり f のマイナス元は g となる．



このようにすれば、非退化 2 次形式

$$x_1^2 + \cdots + x_p^2 - y_1^2 - \cdots - y_q^2$$

のマイナス元として

$$z_1^2 + \cdots + z_q^2 - w_1^2 - \cdots - w_p^2$$

を必ず取ることができるから、〈引き算〉 $f \ominus g$ を必ずすることができる。

(群を知っている人向け)

これは $X := (\text{非退化な実係数 2 次形式全体の集合}) / \cong$ とすると
 $\text{mod } (x^2 - y^2)$ という同値関係 $\sim$ を考えれば $X/\sim$ が

$$[f] + [g] := [f \oplus g] \quad (f, g \in X)$$

により群になるということである. ($[o]$ が単位元)

$X = \mathbb{N} \times \mathbb{N}$ で $x^2 - y^2$ は $(1, 1) \in \mathbb{N} \times \mathbb{N}$ に対応するから
この群は $\mathbb{Z}$ と同型である.

ここまでは実係数の 2 次形式で Witt 群を考えたが
Witt 群は整数係数の 2 次形式でも考えることができる.

つまり $f(x, y) = ax^2 + bxy + cy^2$ が $x^2 - y^2$ と同値になるとき
 $f = o$ とみなすのである.

【定理】

Witt 群 $W(\mathbb{Z})$ は $\mathbb{Z}$ と同型である.



Witt 群以外にも, 2 次形式に関連する群として K 群, L 群などがあり, 幾何学における「手術理論」で使われているらしい.

おまけ

$\mathcal{C}$ を stable ∞ -category とする.

$\mathcal{S}p$ を spectrum 全体とする. (これも stable ∞ -category らしい)

∞ -関手 $F: \mathcal{C}^{\text{op}} \rightarrow \mathcal{S}p$ に対して $\langle \text{Taylor 展開} \rangle$ を考えられる.

(関数のときと同様, 必ず出来る訳ではない.)

(これを Goodwillie calculus という.)

F が n -excisive $\iff F$ を $\langle \text{Taylor 展開} \rangle$ したら $\langle n$ 次以下 $\rangle$ のみ

F が reduced $\iff F$ を $\langle \text{Taylor 展開} \rangle$ したら $\langle 1$ 次以下 $\rangle$ が消滅

つまり 2-excisive かつ reduced な F は $\langle 2$ 次形式 $\rangle$ に相当する.

これにより 2 次形式の ∞ -関手を考えることができる.

【定義】

$F: \mathcal{C} \rightarrow \mathcal{D}$ が reduced $\iff F$ が零対象と交換する.

【定義】

$F: \mathcal{C} \rightarrow \mathcal{D}$ が 1-excisive $\iff F$ が pushout square を pullback square に送る.

【定義】

$F: \mathcal{C} \rightarrow \mathcal{D}$ が 2-excisive $\iff F$ が strongly cocartesian 3-cube を cartesian 3-cube に送る.

square とは単体的集合の射 $f: \Delta^1 \times \Delta^1 \rightarrow \mathcal{C}$ のこと.

3-cube とは単体的集合の射 $f: \Delta^1 \times \Delta^1 \times \Delta^1 \rightarrow \mathcal{C}$ のこと.

2 次形式は、より一般に環 R 上で定義することができる。
 R 上でも同様に Witt 群が定義できるのでそれを $W(R)$ と書く。

Witt 群はモノイド

$$X = (R \text{ 上の非退化 2 次形式全体})/\cong$$

を更に割ることで群にしていたが、わざわざ割らなくても
 $\mathbb{N}$ から $\mathbb{Z}$ を作るのと同じ方法で群を作ることもできる。
これを Grothendieck-Witt 群という。 $GW(R)$ と書く。

【例】

$GW(\mathbb{R}) \cong \mathbb{Z}^2$ である。

($X \cong \mathbb{N}^2$ だったのでマイナス元を増やすと $\mathbb{Z}^2$ になる.)

□

Witt 群は Grothendieck-Witt 群を部分群で割って定義すると考えることもできて、これにより完全列

$$K_0(R)_{C_2} \rightarrow GW(R) \rightarrow W(R) \rightarrow 0$$

が得られる．($K_0(R)$ は R の K 群と呼ばれるもの)

この完全列の左側はどうなっているのだろうか？

→ 高次の K 群 $K_n(R)$

高次の Grothendieck-Witt 群 $GW_n(R)$

高次の L 群 $L_n(R)$ ，を使うらしい．

($L_0(R) = W(R)$ らしい.)

ところが $GW_n(\mathbb{Z})$ が何になるかは $n \geq 3$ ではあまり厳密には分かっていなかったらしい.

$$GW_0(\mathbb{Z}) \cong \mathbb{Z}^2$$

$$GW_1(\mathbb{Z}) \cong (\mathbb{Z}/2\mathbb{Z})^3$$

$$GW_2(\mathbb{Z}) \cong (\mathbb{Z}/2\mathbb{Z})^2$$

$$GW_3(\mathbb{Z}) \cong (\mathbb{Z}/3\mathbb{Z}) \oplus (\text{何か})$$

$$GW_4(\mathbb{Z}) \cong \mathbb{Z} \oplus (\text{何か})$$

$$\vdots$$

これを解決したのが 2026 年の次の論文である。
(arXiv は 2020 年)

B. Calmès, E. Dotto, Y. Harpaz, F. Hebestreit, M. Land, K. Moi, D. Nardin, T. Nikolaus, W. Steimle, Hermitian K-theory for stable ∞ -categories III: Grothendieck-Witt groups of rings, Ann. of Math. (2) 204(1) (2026), 119–220, arXiv: 2009.07225

$$\mathrm{GW}_n(\mathbb{Z}) = \begin{cases} \mathbb{Z} \oplus \mathbb{Z} & (n = 0) \\ \mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z}) & (n = 8k \neq 0) \\ (\mathbb{Z}/2\mathbb{Z})^3 & (n = 8k + 1) \\ (\mathbb{Z}/2\mathbb{Z})^2 \oplus (\mathbb{Z}/c_{2k+1}\mathbb{Z}) & (n = 8k + 2) \\ \mathbb{Z}/w_{4k+2}\mathbb{Z} & (n = 8k + 3) \\ \mathbb{Z} & (n = 8k + 4) \\ 0 & (n = 8k + 5) \\ \mathbb{Z}/c_{2k+2}\mathbb{Z} & (n = 8k + 6) \\ \mathbb{Z}/w_{4k+4}\mathbb{Z} & (n = 8k + 7) \end{cases}$$

c_n は $\left| \frac{B_{2n}}{4n} \right|$ の分子, w_{2n} は $\left| \frac{B_{2n}}{4n} \right|$ の分母, B_m は Bernoulli 数

n	$\mathrm{GW}_n(\mathbb{Z})$	n	$\mathrm{GW}_n(\mathbb{Z})$	n	$\mathrm{GW}_n(\mathbb{Z})$
0	$\mathbb{Z} \oplus \mathbb{Z}$	8	$\mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})$	16	$\mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})$
1	$(\mathbb{Z}/2\mathbb{Z})^3$	9	$(\mathbb{Z}/2\mathbb{Z})^3$	17	$(\mathbb{Z}/2\mathbb{Z})^3$
2	$(\mathbb{Z}/2\mathbb{Z})^2$	10	$(\mathbb{Z}/2\mathbb{Z})^2$	18	$(\mathbb{Z}/2\mathbb{Z})^2$
3	$\mathbb{Z}/24\mathbb{Z}$	11	$\mathbb{Z}/504\mathbb{Z}$	19	$\mathbb{Z}/264\mathbb{Z}$
4	$\mathbb{Z}$	12	$\mathbb{Z}$	20	$\mathbb{Z}$
5	0	13	0	21	0
6	0	14	0	22	$\mathbb{Z}/691\mathbb{Z}$
7	$\mathbb{Z}/240\mathbb{Z}$	15	$\mathbb{Z}/480\mathbb{Z}$	23	$\mathbb{Z}/65520\mathbb{Z}$

n	1	2	3	4	5	6
$\frac{B_{2n}}{4n}$	$\frac{1}{24}$	$-\frac{1}{240}$	$\frac{1}{504}$	$-\frac{1}{480}$	$\frac{1}{264}$	$-\frac{691}{65520}$

良い $\langle 2$ 次形式 $\Omega: \mathcal{C}^{\text{op}} \rightarrow \mathcal{S}\mathcal{P}$ に対して
 Grothendieck-Witt 空間と呼ばれる空間 $\mathcal{GW}(\mathcal{C}, \Omega)$ を定義する.
 $\mathcal{GW}_n(\mathcal{C}, \Omega) := \pi_n \mathcal{GW}(\mathcal{C}, \Omega)$ を n 次の Grothendieck-Witt 群と
 いう.

可換環 R に対して, 有限生成射影的 R -加群の有界な複体全体が
なす安定 ∞ -圏 $\mathcal{D}^p(R)$ を考える.

$$\Omega_R(X) := (X \text{ 上定義された 2 次形式全体})$$

みたいな感じで $\Omega_R: \mathcal{D}^p(R)^{\text{op}} \rightarrow \mathcal{S}_p$ を定義すると
 $\text{GW}_n(R) := \text{GW}_n(\mathcal{D}^p(R), \Omega_R)$ が R の Grothendieck-Witt 群で
ある.

これにより $\text{GW}_n(\mathbb{Z})$ が分かるらしい?

∞ 圏に関する話



すべ Kan4: 序章 <https://www.youtube.com/watch?v=2VU0jI89IhE>

∞ 圏の定義の雰囲気解説



位相空間は ∞ 圏である <https://www.youtube.com/watch?v=vXasynblPsY>

良ければチャンネル登録高評価よろしくお願いします

500 年後くらいには
PDF が完成している
かもしれない。
490 円メンバー discord
に投げておきます。

Hermitian K-Theory

alg-d

https://alg-d.com/math/kan_extension/

2026 年 9 月 13 日

この PDF では 2 次形式を良い ∞ -圏 $\mathcal{C}$ に対して拡張する。即ち $\mathcal{C}$ 上の $\langle 2$ 次形式 $\rangle$ を与える ∞ -関手 $\mathcal{Q}: \mathcal{C}^{\mathrm{op}} \rightarrow \mathcal{S}p$ を定義し、これに対して Grothendieck-Witt 群 $GW_n(\mathcal{C}, \mathcal{Q})$ などを定義する。このような一般化をすることで $\mathbb{Z}$ の Grothendieck-Witt 群 $GW_n(\mathbb{Z})$ を完全に決定することができる [\[2\]](#)。

目次

1	∞ -category of spaces	2
2	spectrum	2
3	安定 ∞ -圏	4
4	Poincaré	5
5	2 次形式	10
6	metabolic	11
7	L 群	16
8	group completion	17
9	Grothendieck-Witt 空間	18