

第 5 章 剰余類

作った部分群を活用してみる

第 2 章で乗積表 (図表 2-3) を作り、第 3 章で、図表 2-3 を元に部分群を作りました。群全体の中に、それ自身がまた群になっている部分がある。それが部分群でした。 D_3 には 6 つありました。

図表 2-3 から、もっとわかることはないだろうか。本章では、部分群を使いながら、さらに図表 2-3 を掘り進めていきます。

§5.1 再びの乗積表

部分群は、 $\{e, f\}$ を使いましょう。これから何度も出てくるので、 H と名付けます。 $H = \{e, f\}$ です。 H は操作の集まりです。群になるのは操作でした (§2.4)。

では、表を見てみます。

		列 (先)					
行 (後)	◦	e	r	r ²	f	rf	r ² f
	e	e	r	r ²	f	rf	r ² f
	r	r	r ²	e	rf	r ² f	f
	r ²	r ²	e	r	r ² f	f	rf
	f	f	r ² f	rf	e	r ²	r
	rf	rf	f	r ² f	r	e	r ²
	r ² f	r ² f	rf	f	r ²	r	e

図表 5-1 図表 2-3 の e の列と f の列に枠を付けたもの

$H = \{e, f\}$ の 2 列 (枠で囲んだところ) を上から見ていきます。 e の行には e と f 、 f の行には f と e があります。 $\{e, f\}$ が出てきました。 H そのものです。残りの r, r^2, rf, r^2f の行を見ると、 e も f も出てきません。

$\{e, f\}$ は、自分の行 $\{e, f\}$ の中に収まっていて、他の行にはみ出していません。 $\{e, f\}$ の列で、こういう収まり方をしているものは、他にないでしょうか。

§5.2 部分群で観察すると

		列 (先)					
行 (後)	◦	e	r	r^2	f	rf	r^2f
	e	e	r	r^2	f	rf	r^2f
	r	r	r^2	e	rf	r^2f	f
	r^2	r^2	e	r	r^2f	f	rf
	f	f	r^2f	rf	e	r^2	r
	rf	rf	f	r^2f	r	e	r^2
	r^2f	r^2f	rf	f	r^2	r	e

図表 5-2 $H = \{e, f\}$ に対応する列と、三つの組

ありました。 r の行と rf の行を見ると、どちらも $\{r, rf\}$ 。 r^2 の行と r^2f の行は $\{r^2, r^2f\}$ 。同じです。この 2 つのかたまりも、他の行には出てきません。

6 つの行が、3 つのかたまりに分かれました。 $\{e, f\}$ 、 $\{r, rf\}$ 、 $\{r^2, r^2f\}$ 。図表 5-2 で同じ色をしている所です。余っている操作も重なっている操作もなく、どのかたまりも 2 個です。

これは $H = \{e, f\}$ に左から同じ操作を合成した結果になっています。

式で書くと、例えば H に r を左から合成することは、 $r \circ e = r$ 、 $r \circ f = rf$

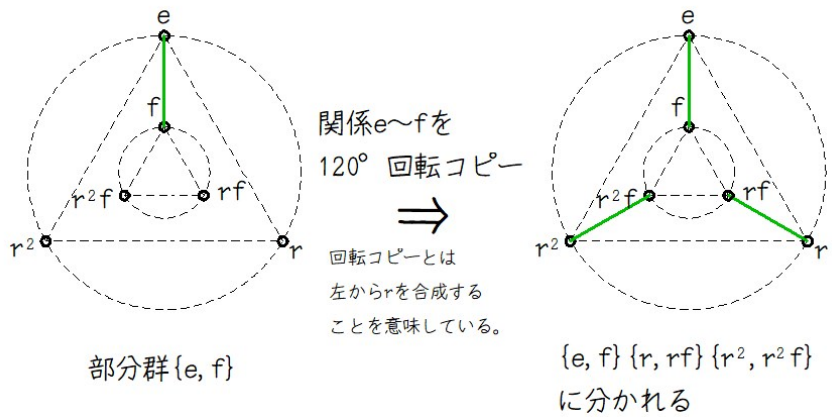
となり、 $\{r, rf\}$ ができます。

このように、 H 全体に同じ操作を左から合成すると、2 個ずつの組ができます。図表 5-2 では、その三つの組によって、 D_3 の 6 つの操作が重なりなく、余りなく分かれています。

§5.3 部分群はここにある

§5.2 では、左から同じ操作を合成すると組ができることを、表で見ました。同じことを図で見ると、別の姿になります。

図表 5-3 は、図表 1-7 の [123] のような状態表記を、三角形の頂点に振った操作名に置き換えたものです。6 つの状態と 6 つの操作は一対一対応なので (§1.4)、こういう置き換えができます。外側の 3 つが回転、内側の 3 つが鏡映で、図表 1-7 と同じく回転の順に並んでいます。

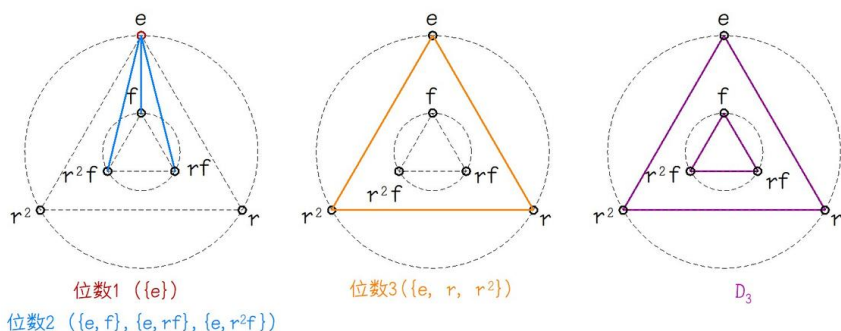


図表 5-3 6 つの状態を操作名で表した図

$H = \{e, f\}$ は、 e と f を結ぶ線分で表されます。これを 120° 回すと $\{r, rf\}$ 、

もう一度回すと $\{r^2, r^2f\}$ 。 $\{e, f\}$ に操作を加えると、6つの操作すべてが網羅されることが図から見えます。「線分を 120° 回す」は、代数では「左から r を合成する」ことです。 $\{e, f\}$ という一つの基準で、6つの操作を重なりなく余りなく3つの組に分けることができる、というわけです。

これは H に限りません。第3章で見た D_3 の部分群も、それぞれ図表 5-3 の中の図形として表現できます (図表 5-4)。



図表 5-4 D_3 の部分群を図表 5-3 の中の図形として表したもの

§5.4 剰余類

ここから、どれか一つの操作を指すのに g, h, k という文字を使います。 H の中のどれか一つを指すときは s 。数の話で x や y を使うのと同様です。

g を打ち消す操作は、 g^{-1} とします (§2.4 の条件 (3))。 $g^{-1} \circ g = e$ 、 $g \circ g^{-1} = e$ です。

H の各要素 s に対して、 $g \circ s$ を作り、集めたものを gH と書きます。

$H = \{e, f\}$ なら、 $gH = \{g \circ e, g \circ f\}$ です。

これを使うと、図表 5-2 と図表 5-3 で見た組は、 $rH = \{r, rf\}$ 、 $r^2H = \{r^2, r^2f\}$

と書き表せます。この gH を剰余類といいます。

6つの操作のうち、どの2つを選んでも、同じように重なりのない組み合わせができるわけではありません。例えば、 $A = \{e, r\}$ の各要素に左から r を合成すると、 $rA = \{r, r^2\}$ で、 A と rA には、どちらにも r が入ります。重なりのない組み合わせにはなりません。また、 A は $r \circ r = r^2$ が外に出てしまうので部分群ではありません (§3.3.2)。

§5.5 表を使わず剰余類を確認する

ここでは、群全体を G 、その部分群を H と書きます。

部分群を元に剰余類が作れると、

$$(G \text{ の位数}) = (H \text{ の位数}) \times (\text{剰余類の個数}) \quad \cdots \textcircled{1}$$

が言えそうです。さきほどの D_3 を例にとると、 $6 = 2 \times 3$ 。群の位数を、部分群の位数を使って、かけ算や割り算のように扱えそうです。ただし、これには、二つのことが前提になります。

(1) 剰余類の分かれ方

剰余類が重なりなく、余りなく分かれている。

(2) 剰余類の要素数

どの剰余類も、 H と同じ個数の要素を持つ。

(1) は、当たり前ではありません。§5.4 で、 $A = \{e, r\}$ と $rA = \{r, r^2\}$ が r だけを共有して、一部分だけ重なる例を見ました。組に分けたからといって、重ならない保証はないのです。

D_3 の場合は、表を作ることで、(1) も (2) も確認できました。しかし、表がな

い場合はどうでしょうか。

実は、表を使わずに確かめる方法があります。話は、剰余類から少し離れます。

5.5.1 関係が分かれば、組にできる

工場見学するため、6人の生徒 A, B, C, D, E, F を班に分けました。ところが、誰も名簿を持ってきていません。生徒達は、自分が誰と同じだったかは覚えていません。すると、先生は、A さんに「B さんと同じ？ C さんと同じ、...、F さんと同じ？」と聞いていきます。同じなら○、違うなら×です。この質問を、次は B さん、次は C さん...としていきます。こうして表ができました（図表 5-5）。余りも重なり也没有ありません。



	A	B	C	D	E	F	班の人数
A	○	×	×	○	×	×	2
B	×	○	×	×	○	×	2
C	×	×	○	×	×	○	2
D	○	×	×	○	×	×	2
E	×	○	×	×	○	×	2
F	×	×	○	×	×	○	2
班の人数	2	2	2	2	2	2	

図表 5-5 6 人の生徒を「同じ班か」という関係で分けた表

これと同様の質問を群に対して行います。「A さんは B さんと同じ班か」と問う代わりに「 g と h は同じ剰余類か」と問うのです（図表 5-6）。

剰余類が群 G を重なりなく、余りなく分けることを示すには、「同じ剰余類に入る」という関係を、同値関係として捉えればよさそうです（第 4 章参照）。

生徒の班分け	剰余類
Aさん、Bさん、Cさん…	e, r, r^2, f, rf, r^2f (G の要素)
1班、2班、3班	eH, rH, r^2H (剰余類)
「AさんはBさんと同じ班か」	「 g と h は同じ剰余類か」
$A \sim B$ (同じ班かの関係)	$g \sim h$ (同じ剰余類かの関係)

図表 5-6 g と h が同じ剰余類かを調べる表

そこで、§5.6 では、「 h が gH に入る」ことを、「 $g^{-1} \circ h$ が H の要素である」という式で判定できる形にします。

§5.7 では、『 $g^{-1} \circ h$ が H の要素である』という関係が同値関係の三律を満たすことを確かめます。§5.8 では、そこからできる同値類 (§5.6 で確かめるとおり、剰余類 gH そのもの) が、群 G を重なりなく、余りなく分けることを確かめます。これで §5.5(1) が示されます。

一方、§5.5(2) は、剰余類の中の操作の個数についての話です。これは「同じ組にいるかどうか」だけからはわかりません。そこで、§5.9 では別の方法で、どの剰余類も H と同じ個数の要素を持つことを確かめます。そこから、ラグランジュの定理を導きます。

§5.6 剰余類に入る条件

ここからは、 D_3 に限らない話になります。群を G 、その部分群を H と書きます (図表 5-7)。

§5.5 では、「 G の中から取ってきた 2 つの操作 g と h が、同じ剰余類にいるか」を判定できれば、剰余類の分かれ方が捉えられる、と述べました。そこで、 g を 1 つ選んで固定し、 h が gH に入るかを式で判定できる形にします。

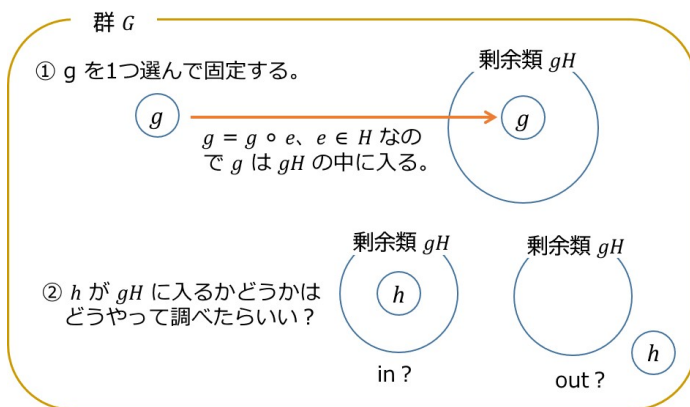
$g = g \circ e$ で、 e は H の要素なので、 g は gH の中にいます。 g 自身については

記号	指すもの	記号	指すもの
G	群全体	gH	剰余類
H	G の部分群	g^{-1}	g を打ち消す操作
g, h, h', k	G のうち、どれか一つ	$g \sim h$	$g^{-1} \circ h$ が H の要素である
s	H のうち、どれか一つ		

図表 5-7 記号のまとめ

分かったので、次に、任意の h が gH に入るかを考えます (図表 5-8)。

剰余類が全体を重なりなく分けることは、§5.7～§5.8 で確かめます。



図表 5-8 h が gH に入るか調べるには

以降、 g は剰余類 gH を作る代表元、 h は gH に入るかを判定される要素として使います。

① H の要素に、 g を合成して、剰余類 gH を作る

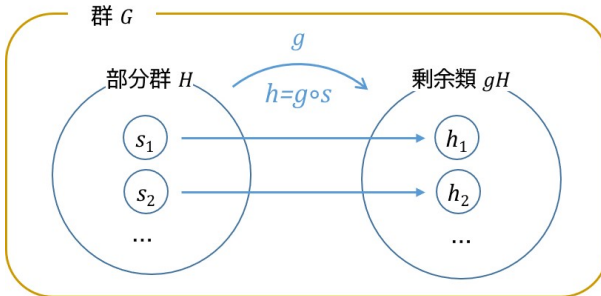
部分群 H の要素を、 $s_1, s_2, \dots$ とします。それぞれに左から同じ操作 g を合成して、 $h_1 = g \circ s_1, h_2 = g \circ s_2, \dots$ を作ります。

② $h_1, h_2, \dots$ を集めた組が gH

集めた組を、 gH と書きます (§5.4 で定義)。

③ $h_1, h_2, \dots$ は gH の中にある

作り方から、 $h_1, h_2, \dots$ は gH に入ります (図表 5-9)。



図表 5-9 部分群 H の各要素に左から g を合成し、剰余類 gH の要素を作る図

問題は、 G から任意に取った要素 h が、剰余類 gH に入るかどうかを、どう判定するかです。 gH の要素は一般には H の要素ではありません。例えば $g = r$ 、 $H = \{e, f\}$ なら、 $rH = \{r, rf\}$ で、 H とは要素がまったく違います。では、どう判定すればよいでしょうか。それが④以降です。

④ 判定の方針

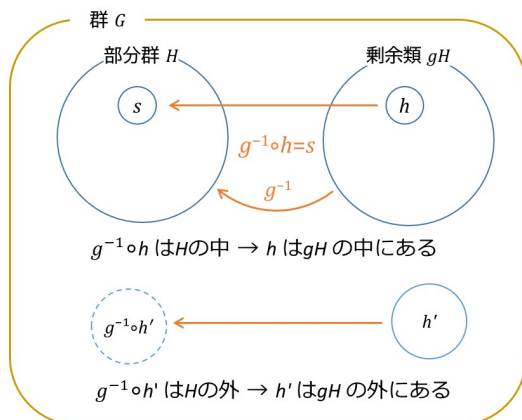
①～③で g を掛けて gH を作ったので、その逆をたどって H に戻れるかを確かめます (図表 5-10)。 h に左から g^{-1} を合成し、 $g^{-1} \circ h$ が部分群 H の要素になるかを見ます。

⑤ h が gH の中にあれば、 $g^{-1} \circ h$ は H の要素

h が gH の中にあるなら、 H のある要素 s を使って、 $h = g \circ s$ と書けます。両辺に左から g^{-1} を合成すると、 $g^{-1} \circ h = (g^{-1} \circ g) \circ s = e \circ s = s$ となります。 s はもともと H の要素なので、 $g^{-1} \circ h$ も H の要素です。

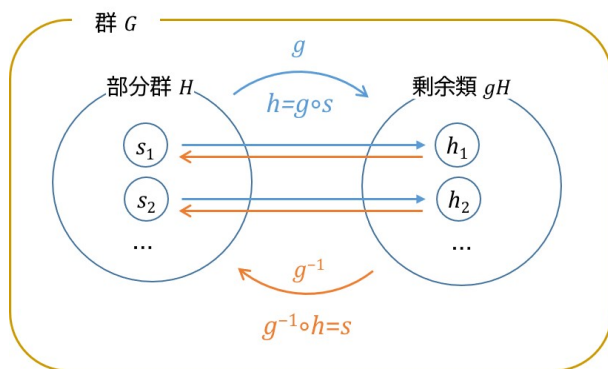
⑥ $g^{-1} \circ h$ が H の要素なら、 h は gH に入る

逆に、 $g^{-1} \circ h$ が H の要素であるとしします。その要素を s とすると、 $s = g^{-1} \circ h$



図表 5-10 剰余類 gH から部分群 H へ戻して判定する方針

です。両辺に左から g を合成すると、 $g \circ s = g \circ (g^{-1} \circ h) = (g \circ g^{-1}) \circ h = e \circ h = h$ となり、 $h = g \circ s$ と書けます。 s は H の要素なので、 h は剰余類 gH の中にあります。



図表 5-11 g と g^{-1} による二方向の対応

以上から、「 h が gH に入る」ことと、「 $g^{-1} \circ h$ が H の要素である」ことは同じ意味です。

そこで、「 $g^{-1} \circ h$ が H の要素である」という関係を、 $g \sim h$ と書くことにし

ます。

例えば、 $H = \{e, f\}$ 、 $g = r$ の場合、 $gH = rH = \{r, rf\}$ です。 $h = rf$ とすれば、 $g^{-1} \circ h = r^{-1} \circ rf = f$ で、これは H の要素です。ですから $r \sim rf$ です。

次に、この関係 $g \sim h$ が同値関係か確かめていきます。

§5.7 同値関係か確かめる

§5.6 で作ったルール「 $g^{-1} \circ h$ が H の要素である」（すなわち $g \sim h$ ）が、同値関係の三律を満たすかを確かめます。 H が部分群であること（ H 自身が群の3条件を満たすこと。§3.3）が、ここで効いてきます。

(1) 反射律

g と自分自身 g にルールを適用すると、 $g^{-1} \circ g = e$ です。 H は部分群なので、 e を持ちます (§3.3(2))。したがって、 $g^{-1} \circ g$ は H の要素です。つまり反射律は成立します。

(2) 対称律

$g \sim h$ が成り立つとします。このとき、 $g^{-1} \circ h$ は H の要素です。 $h \sim g$ が成り立つには、 $h^{-1} \circ g$ が H の要素であることが言えればよい。

H は部分群なので、その要素 $g^{-1} \circ h$ を打ち消す操作も H の要素です (§3.3(3))。打ち消す操作とは、 $(g^{-1} \circ h)^{-1} = h^{-1} \circ g$ 。合成した操作を打ち消すときは、逆の順序でそれぞれを打ち消します。 g^{-1} を打ち消す操作は g です (§5.4、 $g \circ g^{-1} = e$)。この $h^{-1} \circ g$ は H の要素なので、対称律は成立します。

(3) 推移律

$g \sim h$ と $h \sim k$ が成り立つとします。このとき、 $g^{-1} \circ h$ と $h^{-1} \circ k$ は、どちらも H の要素です。 H は部分群なので、この二つを合成したものも H の要素

です (§3.3(1))。これを式で書くと、

$$(g^{-1} \circ h) \circ (h^{-1} \circ k) = g^{-1} \circ (h \circ h^{-1}) \circ k = g^{-1} \circ e \circ k = g^{-1} \circ k$$

したがって、 $g^{-1} \circ k$ は H の要素です。よって $g \sim k$ が成立し、推移律は成立します。

以上、三律が成立したので、「 $g^{-1} \circ h$ が H の要素である」というルールは、同値関係です。

§5.8 同値類は全体を分ける

§5.6 で確かめたとおり、 g の同値類 (g と関係を持つ要素の集まり) は剰余類 gH そのものです。

同値関係からできる同値類が、なぜ重なりなく、余りなく分かれるのか。第4章で先送りにした理由が、これです。剰余類に限らない話なので、第4章と同じ x, y, z で書きます。

(1) 余りがない

反射律により、どの要素も自分自身と同値です。したがって、どの要素も必ず自分の同値類に入り、余りはありません。

(2) 一部分だけ重なることはない

二つの同値類に共通する要素がある場合を考えます。 x の同値類と y の同値類の両方に、 z が入っているとします。すると、 $x \sim z$ 、 $y \sim z$ です。対称律により、 $z \sim y$ なので、推移律から、 $x \sim y$ が成り立ちます。

ここで、 x の同値類に入る要素を一つ取り、 w とします。すると、 $x \sim w$ です。また、 $x \sim y$ なので、対称律から $y \sim x$ です。したがって、推移律によ

り、 $y \sim w$ となります。 w はどれを選んでもよかったので、 x の同値類に入る要素は、すべて y の同値類にも入ります。

x と y を入れ替えても同じことが言えるので、二つの同値類の中身は同じです。

したがって、同値関係からできる二つの同値類は、まったく重ならないか、同じものになるかのどちらかです。異なる同値類が一部分だけ重なることはありません。

以上から、同値関係からできる同値類は、全体を重なりなく、余りなく分けま
す。したがって、剰余類は、群 G を重なりなく、余りなく分けま
す。これで (1) が示されました。

5.8.1 部分群でない場合

§5.4 で見た $A = \{e, r\}$ を思い出してください。 $A = \{e, r\}$ と $rA = \{r, r^2\}$ は、 r だけを共有して、一部分だけ重なっていました。

A は部分群ではないので、§5.7 で使った性質が成り立ちません。対称律には、 A の要素の逆元も A の中にあることが必要です。実際、 $r \in A$ ですが、 $r^{-1} = r^2 \notin A$ です。

また、推移律には、 A の 2 つの要素を合成したものも A の中にあることが必要です。しかし、 $r \circ r = r^2$ は A の要素ではありません。

§5.9 ラグランジュの定理

§5.8 で、「剰余類は、群 G を重なりなく、余りなく分ける」ことが示されました。では、§5.5(2)「どの剰余類も、 H と同じ個数の要素を持つ」の証明に進

みます。

5.9.1 部分群と剰余類の一对一対応

H の各要素 s に、左から g を合成すると、剰余類 gH の要素 $g \circ s$ ができます。また、できた要素に左から g^{-1} を合成すれば、 $g^{-1} \circ (g \circ s) = s$ となり、元の s に戻ります。別々の s からは、別々の要素ができ、それぞれ元に戻るので、 H の要素と gH の要素は一つずつ対応します。したがって、 H と gH の要素数は同じです (図表 5-11)。

これで、どの剰余類も H と同じ個数の要素を持つことが確かめられました。
§5.5 で挙げた (2) が示せました。

5.9.2 式①の証明

§5.8 で §5.5(1) が、いま §5.9.1 で §5.5(2) が示せたので、二つを合わせると、 G の要素は、いくつかの剰余類に、重なりなく余りなく分かれます。また、どの剰余類も、 H と同じ個数の要素を持ちます。

剰余類の個数を n とすると、

$$(G \text{ の位数}) = (H \text{ の位数}) \times n$$

と言えます。これで、§5.5 の式①が証明できました。

これは、群 G の位数は、部分群 H の位数で割り切れるということです。これをラグランジュの定理といい、 n を指数といいます。

この定理から、 D_3 に位数が 4 や 5 の部分群がないことは明らかです。6 は 4 や 5 で割り切れません。

5.9.3 有限群

この定理は、群 G の要素数が有限であることを前提にしています。これまで扱ってきた D_3 は 6 個の要素でできていて、要素数が有限でした。このように、要素数が有限な群を有限群といいます。要素数が無限の群を無限群といいます。例えば、整数全体を要素とし、足し算を演算とする群がそうです。無限群では、要素の個数を数えて割り算をするというラグランジュの定理の考え方が、そのままでは使えません。

第 5 章のまとめ

- 部分群 H のすべての要素 s に、左から群 G の操作 g を合成し、でき上がる組を gH と書く。この組を剰余類という。
- ラグランジュの定理：剰余類の個数（指数）を n とすると、

$$(G \text{ の位数}) = (H \text{ の位数}) \times n$$

- 剰余類による分類は、はじめから同じ個数ずつに分けようとしたものではない。 H に群の要素を掛けて作った集合で分けた結果、同じ個数ずつになったのである。 D_3 を $H = \{e, f\}$ で分けると、各剰余類は H と同じ 2 個の要素を持ち、全部で 3 組（指数 3）になる。

問題

問 5-1

$H = \{e, rf\}$ で D_3 を分けると、どうなるでしょうか。図表 2-3 の e の列と rf の列に枠を移して読んでください。

問 5-2

「回転か、鏡映か」で D_3 の 6 つの操作を分けると、何組できるでしょうか。

問 5-3

問 5-1 の分け方で、組どうしを合成できるでしょうか。 $\{r, r^2f\}$ と $\{r^2, f\}$ から一つずつ選んで合成し、結果がどの組に入るかを、選び方を変えて比べてください。

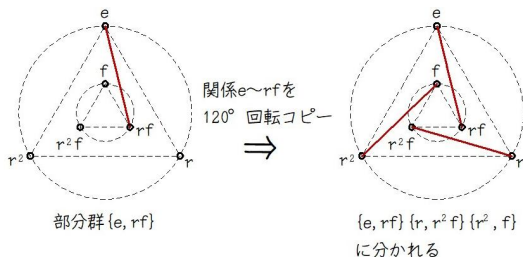
問 5-4

位数 12 の群に、位数 5 の部分群はあるでしょうか。

解答

5-1 $\{e, rf\}$ 、 $\{r, r^2f\}$ 、 $\{r^2, f\}$ の3組、2個ずつ。 $6 = 2 \times 3$ です。

e	e	r	r ²	f	rf	r ² f
e	e	r	r ²	f	rf	r ² f
r	r	r ²	e	rf	r ² f	f
r ²	r ²	e	r	r ² f	f	rf
f	f	r ² f	rf	e	r ²	r
rf	rf	f	r ² f	r	e	r ²
r ² f	r ² f	rf	f	r ²	r	e



図表 5-12

5-2 2組です。 $\{e, r, r^2\}$ と $\{f, rf, r^2f\}$ 。 $6 = 3 \times 2$ です。この2組は、図表 1-7 の外側（回転）と内側（鏡映）にあたります。分ける基準に使った $\{e, r, r^2\}$ は、第3章で見つけた位数3の部分群です。

この分け方には、組同士を合成できるという性質があります。回転に回転を合成すると回転。回転に鏡映を合成すると鏡映。鏡映に鏡映を合成すると回転。鏡映に回転を合成すると鏡映。図表 2-3 で確かめられます。組が2つあって、その2つの間にも合成があります。組そのものを、新しい群の要素と見なせそうです。ところが、位数2の部分群 ($\{e, f\}$ 、 $\{e, rf\}$ 、 $\{e, r^2f\}$) で分けると、これできません。このことを問うのが問 5-3 です。

5-3

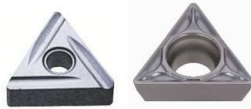
できません。 $r \circ r^2 = e$ で、これは $\{e, rf\}$ の組です。ところが $r^2f \circ r^2 = f$ で、これは $\{r^2, f\}$ の組です。同じ2組を合成したのに、どの代表を選ぶかで行き先が変わります（図表 5-13）。同じ群を、同じやり方で分けたのに、片方は合成でき、片方はできません。これは、 $\{e, r, r^2\}$ と $\{e, rf\}$ の違いです。詳しくは7章で扱います。

o	r^2	f
r	e	rf
r^2f	f	r^2

図表 5-13

5-4 ありません。5 で 12 は割り切れないからです。ラグランジュの定理より、この群が位数 5 の部分群を持たないことは、乗積表を書き出さなくても言えます。

Column



これは、旋盤のバイトの超硬チップです。このチップに入っている溝はチップブレーカーといいます。図表 5-3 や図表 5-12 を作っているとき、剰余類が三角を等分しているように見え、「何かに似てるぞ。あっ!」と思ったのが、これでした。
