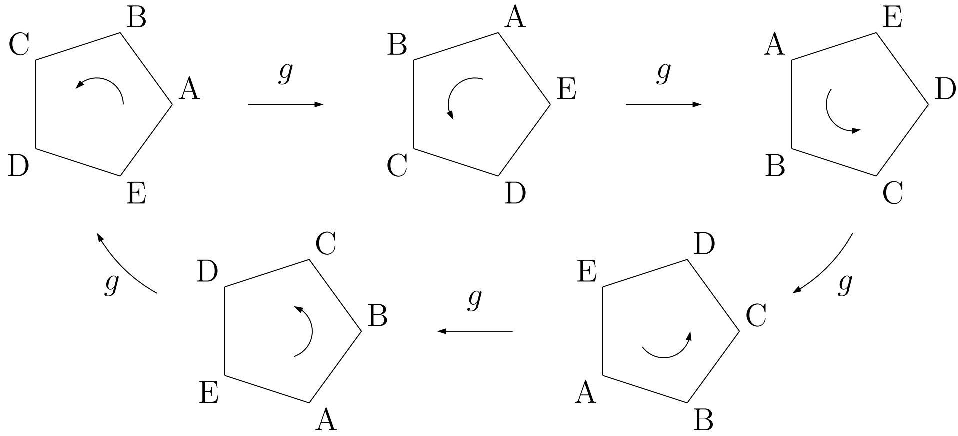
1　図形の対称性と群

1.1　巡回群



正 5 角形を中心の周りに 72° 回転して隣の頂点に重なる移動を g とおくと，2 つ隣に移る回転は g で 2 回移すので，積として考えて g^2，3 つ隣に移る回転は g^3，と表されます。5 回 g で回転すると，元の位置に戻ってくるので，

$$g^5 = e \quad (\text{恒等変換})$$

となります。よって，この回転移動全体

$$\{e,\ g,\ g^2,\ g^3,\ g^4\}$$

は群になります。回転移動は可換なので，この群は可換群です。
例えば，g^2 と g^4 の積は，1 周してさらに g の移動と同じなので，

$$g^2g^4 = g^6 = g^5g = g$$

と考えられます。要するに，積は指数の足し算をしていて，5 を超えると，5 を引けばよいのですね。
さて，何かと似ていることに気付きませんか？

整数を5で割った余りで分類すると

$$\{\cdots\cdots,\ -10,\ -5,\ 0,\ 5,\ 10,\ 15,\ \cdots\cdots\}$$
$$\{\cdots\cdots,\ -9,\ -4,\ 1,\ 6,\ 11,\ 16,\ \cdots\cdots\}$$
$$\{\cdots\cdots,\ -8,\ -3,\ 2,\ 7,\ 12,\ 17,\ \cdots\cdots\}$$
$$\{\cdots\cdots,\ -7,\ -2,\ 3,\ 8,\ 13,\ 18,\ \cdots\cdots\}$$
$$\{\cdots\cdots,\ -6,\ -1,\ 4,\ 9,\ 14,\ 19,\ \cdots\cdots\}$$

となります。これらはそれぞれ，

$$5m,\ 5m+1,\ 5m+2,\ 5m+3,\ 5m+4 \quad (m \in \mathbb{Z})$$

と表される整数です。これらをそれぞれ

$$\{0,\ 1,\ 2,\ 3,\ 4\}$$

で代表元として集合にすると，「足し算」が定義できます。例えば

$$2+4=6 \equiv 1 \pmod{5}$$

と書いたりします（合同式といいます)。この「足し算」について，この集合は群になっていて，回転移動の群と

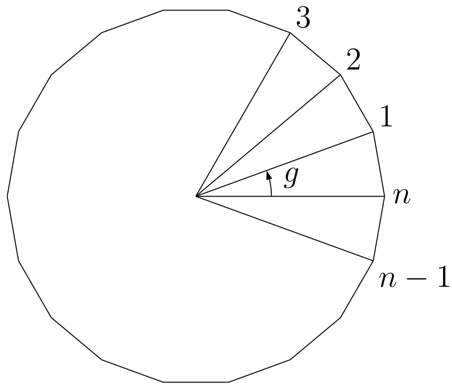
$$e \to 0, \quad g \to 1, \quad g^2 \to 2, \quad g^3 \to 3, \quad g^4 \to 4$$

と対応させると，2つの群が同型であることがいえます。
これらの群を位数5の**巡回群**といい，$\mathbb{Z}/5\mathbb{Z}$ とかきます。

$\boxed{\text{問題}}$ 巡回群 $\mathbb{Z}/5\mathbb{Z}$ の演算表を完成させましょう。

+	0	1	2	3	4
0					
1					
2					
3					
4					

一般に，正 n 角形を中心の周りに回転させて自分自身と重なるように動かすとき，その移動全体は位数 n の**巡回群**になり，$\mathbb{Z}/n\mathbb{Z}$ と表します。正 n 角形を中心の周りに $\dfrac{360^\circ}{n}$ 回転して隣の頂点に重なる移動を g とおくと，2 つ隣に移る回転は g で 2 回移すので g^2，3 つ隣に移る回転は g^3，と表されます。n 回 g で回転すると，元の位置に戻ってくるので，



$$g^n = e \quad (\text{恒等変換})$$

となります。よって，

$$\mathbb{Z}/n\mathbb{Z} = \{e,\ g,\ g^2,\ \cdots\cdots,\ g^{n-1}\}$$

と表されます。回転移動は可換なので位数 n の巡回群は可換群です。
$k+l \leqq n-1$ のときは $g^k g^l = g^{k+l}$ で，
$k+l > n-1$ のときは $k+l = n+m\ (0 \leqq m \leqq n-1)$ とおいて，

$$g^k g^l = g^{k+l} = g^{n+m} = g^n g^m = g^m$$

となります。（ただし $g^0 = e$ とおく）
回転移動の積は指数の和に対応していて，n を超えると n を引きます。
よってこれは整数を n で割った余りで分類した集合

$$\{0,\ 1,\ 2,\ 3,\ \cdots\cdots,\ n-1\}$$

に「足し算」を入れて作った群と同型になります。

1.2　群の直積

2 つの群 $G,\ H$ が与えられたとき，集合

$$\{(g,\ h) \mid g \in G,\ h \in H\}$$

の中に群の演算

$$(g,\ h)(g',\ h') = (gg',\ hh')$$

として定義したものを，G と H の**直積**といい，$G \times H$ で表します。$G,\ H$ の単位元を $e,\ e'$ とすると，$G \times H$ の単位元は $(e,\ e')$ です。また，$(g,\ h)$ の逆元は $(g^{-1},\ h^{-1})$ です。
最も簡単な例は，2 つの位数 2 の巡回群の直積

$$(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) = \{(0,\ 0),\ (1,\ 0),\ (0,\ 1),\ (1,\ 1)\}$$

で，これは可換群です (よく登場するので，**クラインの 4 元群**という名前がついています)。いま，単位元を e，残りの元を $a,\ b,\ c$ と置き換えると，

$$a^2 = b^2 = c^2 = e, \quad ab = ba = c, \quad bc = cb = a, \quad ca = ac = b$$

という関係式が成り立ちます。

問題　$(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$ の元を書き出しましょう。

問題　上のそれぞれの元と $\mathbb{Z}/6\mathbb{Z}$ の元を対応させて，$(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$ と $\mathbb{Z}/6\mathbb{Z}$ は同型であることを確かめましょう。

一般に，m と n が互いに素（公約数が 1 のみ）のとき，

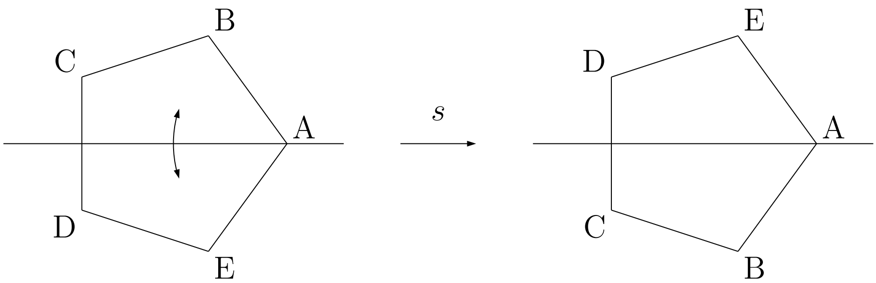
$$\mathbb{Z}/mn\mathbb{Z} \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$$

が成り立ちます。

1.3　正 2 面体群

正 n 角形を中心の周りに回転させて自分自身と重なるように動かすとき，その移動は巡回群になりました。いま，n 角形が空間の中にあるとします。回転に加えてさらに，中心を通るある軸に関して裏返すことによって自分自身に重なる移動も含めるとき，その移動全体はどのような群になるでしょう？

正 5 角形 ABCDE で考えてみましょう。中心の周りに 72° 回す回転移動を g とします。g によって，頂点 A，B，C，D，E は 1 つずつずれ，5 回回すと元の所に戻ってきます。よって，回転移動は g，g^2，g^3，g^4 の 4 種類です。また，A を通る軸による裏返しの対称移動を s とします。s によって，A はそのままで，B と E，C と D が互いに移りあいます。



回転移動 g によって，1 つずつずれた正 5 角形に対してそれぞれ，裏返しが存在します。よって，s，sg，sg^2，sg^3，sg^4 が裏返した正 5 角形に対応した移動となります。これに恒等変換 e を加えて全部で

$$D_5 = \{e,\ g,\ g^2,\ g^3,\ g^4,\ s,\ sg,\ sg^2,\ sg^3,\ sg^4\}$$

となります。

g は 72° 回転移動で，5 回まわると元に戻るので $g^5 = e$,
s は裏返しで，2 回裏返すと元に戻るので $s^2 = e$

となることは，すぐに分かります。g と s は非可換で $gs \neq sg$ なのですが,

$$sgsg = e$$

という大事な関係式がもう 1 つ成り立ちます。

$\boxed{\text{問題}}$ $gs \neq sg$ と $sgsg = e$ となることをそれぞれ図を使って確かめましょう。

$sgsg = e$ という関係式より $sgs = g^{-1}$ が成り立つので，$sg^m s = g^{-m}$ $(m \in \mathbb{Z})$ が成り立ちます。よって，積によって閉じていることが分かり，D_5 は群になっているといえます。

$\boxed{\text{問題}}$ sg^3 の逆元を求めましょう。

$\boxed{\text{問題}}$ $sg^3sgsg^2sg^4s$ を簡単にしましょう。

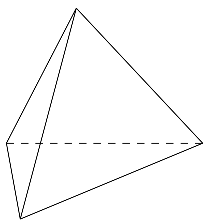
一般に，正 2 面体群 D_n $(n \geqq 3)$ は，正 n 角形の中心の周りの回転移動を g，中心を通るある軸に関する裏返しの移動を s とおくと，

$$D_n = \{e,\ g,\ g^2,\ \cdots\cdots,\ g^n,\ s,\ sg,\ sg^2,\ \cdots\cdots,\ sg^{n-1}\}$$
$$(g^n = e, \quad s^2 = e, \quad sgsg = e)$$

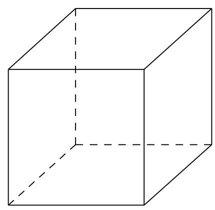
と表されます。正 2 面体群 D_n は位数 $2n$ の非可換群です。特に D_3 は位数 6 の非可換群で 3 次対称群 S_3 と同型です。

1.4　正多面体群

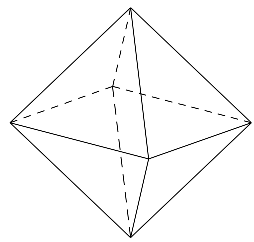
古代ギリシアの時代から正多面体は次の 5 種類しかないことは知られていました。証明はそんなに難しくはありません。できますか？



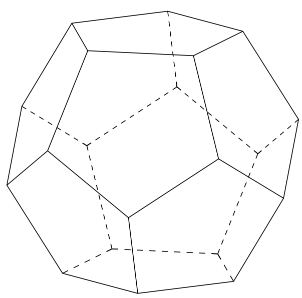
正 4 面体
tetrahedron



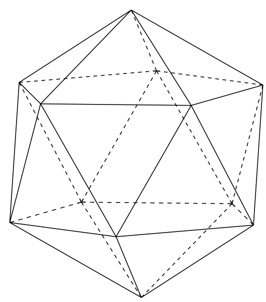
正 6 面体
hexahedron



正 8 面体
octahedron



正 12 面体
dodecahedron



正 20 面体
icosahedron

頂点の数と面の数，辺の数を表にすると，

	頂点の数	面の数	辺の数
正 4 面体			
正 6 面体			
正 8 面体			
正 12 面体			
正 20 面体			

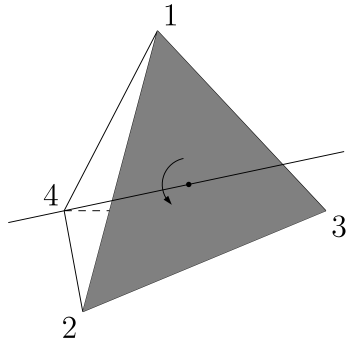
表 1

となります。

正多面体を中心を通る軸で回転させて自分自身に重なるように動かすとき，その移動全体は群になります。この群を**正多面体群**といいます。もう少し詳しく，各正多面体の種類によって，正 4 面体群，正 6 面体群，正 8 面体群，正 12 面体群，正 20 面体群といいます。これらを記号でそれぞれ $P(4)$, $P(6)$, $P(8)$, $P(12)$, $P(20)$ とかくことにします。

正 4 面体群 $P(4)$

4 つの頂点に 1，2，3，4 と番号をつけていくと，正 4 面体群の元の移動によって頂点 1，2，3，4 が移りあいます。よって，正 4 面体群の元は 4 次対称群 S_4 の元と対応させせることができます。右の図のように，頂点 4 と中心を通る軸で，120° 回転させると，1，2，3 が移りあうので，



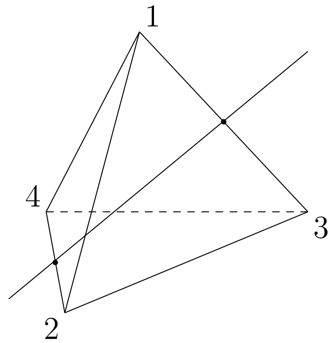
$$(1\ 2\ 3),\ (1\ 3\ 2)$$

という，長さ 3 の巡回置換と対応します。
同様に，他の頂点 3，2，1 を通る軸でそれぞれ回転させると，他の長さ 3 の巡回置換

$$(1\ 2\ 4),\ (1\ 4\ 2),\ (1\ 3\ 4),\ (1\ 4\ 3),\ (2\ 3\ 4),\ (2\ 4\ 3)$$

が現れます。

また，右の図のように，頂点 1 と 3 の中点と頂点 2 と 4 の中点を通る軸で 180° 回転すると，1 と 3，2 と 4 が移りあうので



$$(1\ 3)(2\ 4)$$

という置換が対応します。同様に，1 と 2，3 と 4 の中点を結ぶと (1 3)(2 4)，1 と 4，2 と 3 の中点を結ぶと (1 4)(2 3) という置換が対応します。

正 4 面体を自分自身に重ねる回転移動はこれらと，全く動かさない恒等変換 e だけで，全部合わせて

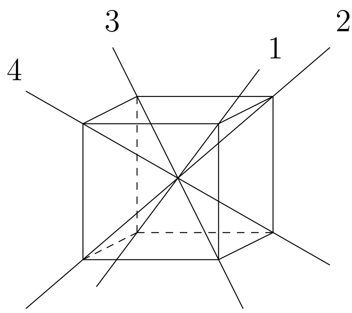
$$\{e,\ (1\ 2\ 3),\ (1\ 3\ 2),\ (1\ 2\ 4),\ (1\ 4\ 2),\ (1\ 3\ 4),\ (1\ 4\ 3),$$
$$(2\ 3\ 4),\ (2\ 4\ 3),\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\}$$

と表されます。これは 4 次の交代群 A_4 に他なりません。このように 2 つの群 G_1 と G_2 の元が 1 対 1 に対応するとき，2 つの群は**同型**であるといい $G_1 \cong G_2$ とかきます。いま正 4 面体群 $P(4)$ は 4 次の交代群 A_4 と同型であることが分かりました。

$$P(4) \cong A_4$$

正 6 面体群 $P(6)$

正 4 面体のときと同様に，回転によって頂点が移りあうと考えると正 6 面体（立方体）は頂点が 8 つで，8 次対称群 S_8 の元と対応させることになり，これは大変です。正 6 面体の頂点は，中心をはさんで対称な位置に 2 つずつあります。これらを通る軸に，右の図のように 1，2，3，4 と番号をつけると，$P(6)$ の元によって，これらの 4 本の軸が互いに移りあうことになります。



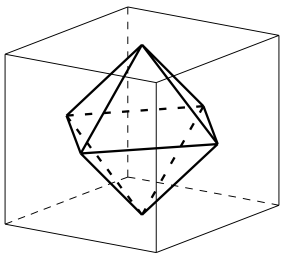
よって，4 次対称群 S_4 の元と対応がつけられます。

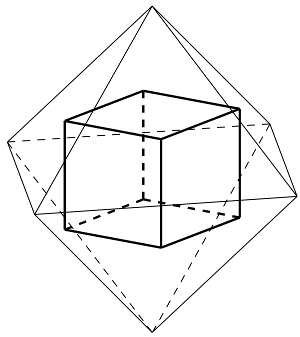
$\boxed{\text{発展}}$ 正 6 面体群 $P(6)$ と 4 次の対称群 S_4 は同型であることを確かめましょう。

$$P(6) \cong S_4$$

正 8 面体群 $P(8)$

正 6 面体の中心（重心であり，内心・外心でもある点）を頂点にとると正 8 面体ができます。逆に，正 8 面体の中心を頂点にとるとると正 6 面体ができます。このような 2 つの立体の関係を**双対**であるといいます。正 6 面体と正 8 面体は双対になっていることがわかります。





正 8 面体を自分自身に重ねる移動は，双対な正 6 面体も自分自身に重ねているので，正 8 面体群 $P(8)$ と正 6 面体群 $P(6)$ は同型であることがいえます。

$$P(8) \cong P(6) \cong S_4$$

正 12 面体群 $P(12)$**，正 20 面体群** $P(20)$

表 1 より，正 12 面体の各面の中心を頂点とする立体は正 20 面体で，逆に正 20 面体の各面の中心を頂点とする立体は正 12 面体なので，正 12 面体と正 20 面体も双対であることが分かります。よって，正 12 面体群 $P(12)$ と正 20 面体群 $P(20)$ は同型です。これらは 5 次交代群 A_5 と同型であることが知られています。群の位数は 60 なので，対応を書き出すのは大変ですが，余裕のある人はチャレンジしてみて下さい。

$$P(12) \cong P(20) \cong A_5$$

2　正規部分群と剰余群

2.1　部分群

3 次対称群

$$S_3 = \{e,\ (1\ 2),\ (2\ 3),\ (1\ 3),\ (1\ 2\ 3),\ (1\ 3\ 2)\}$$

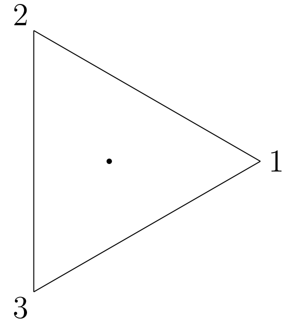
の要素 $(1\ 2)$ を 2 回かけると単位元 e になります。

$$(1\ 2)(1\ 2) = e$$

よって，集合

$$\{e,\ (1\ 2)\}$$

は演算に関して閉じています。また，単位元，逆元も存在しています。このように S_3 の部分集合で群となっているものを S_3 の**部分群**といいます。

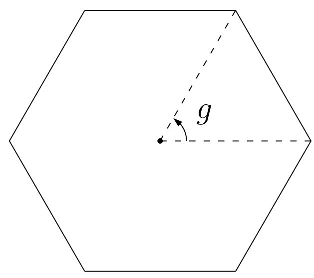


S_3 は正 2 面体群 D_3 と同型

S_3 の部分群をもっと見つけてみましょう。
$\{e,\ (2\ 3)\}$，　$\{e,\ (1\ 3)\}$ も部分群ですね。
他に $\{e,\ (1\ 2\ 3),\ (1\ 3\ 2)\}$ も部分群になっています。（これは 3 次交代群 A_3 という名前がついています。）
部分群は単位元 e を必ず含んでいることに気付きましたか？
あと，単位元 e のみという集合 $\{e\}$ も部分群ですし，S_3 自身も部分群と言えます。
S_3 の部分群はこれで全部です。一般に，群 G の部分集合 H が G の演算によって群となるとき H を G の**部分群**といいます。

問題

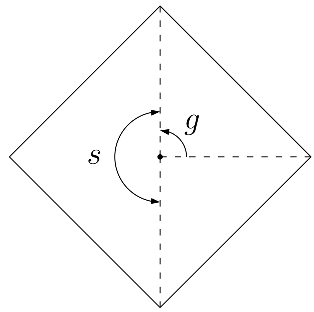
巡回群 $\mathbb{Z}/6\mathbb{Z} = \{e,\ g,\ g^2,\ g^3,\ g^4,\ g^5\}$　$(g^6 = e)$
の部分群をすべて見つけましょう。



$\boxed{\text{問題}}$
正 2 面体群

$$D_4 = \{e,\ g,\ g^2,\ g^3,\ s,\ sg,\ sg^2,\ sg^3\}$$
$$(s^2 = g^4 = e,\ sgsg = e)$$

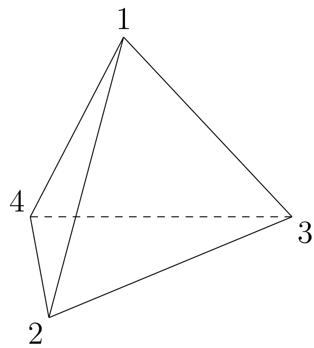
の部分群をすべて見つけましょう。



$\boxed{\text{発展}}$
4 次交代群

$$A_4 = \{e,\ (1\ 2\ 3),\ (1\ 3\ 2),\ (1\ 2\ 4),\ (1\ 4\ 2),\ (1\ 3\ 4),\ (1\ 4\ 3),$$
$$(2\ 3\ 4),\ (2\ 4\ 3),\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\}$$

の部分群をすべて見つけましょう。



A_4 と正 4 面体群は同型

2.2 正規部分群

ガロアの群論における最大の発見である正規部分群のお話をします。
3 次対称群

$$S_3 = \{e,\ (1\ 2),\ (1\ 3),\ (2\ 3),\ (1\ 2\ 3),\ (1\ 3\ 2)\}$$

の部分群

$$A_3 = \{e,\ (1\ 2\ 3),\ (1\ 3\ 2)\}$$

があります。S_3 を A_3 とそれ以外の集合に分けると

$$S_3 = \{e,\ (1\ 2\ 3),\ (1\ 3\ 2)\} \cup \{(1\ 2),\ (1\ 3),\ (2\ 3)\}$$

と表せます。後ろの集合 $\{(1\ 2),\ (1\ 3),\ (2\ 3)\}$ と A_3 をよく見て比べてみると，

$$\begin{aligned}(1\ 2) &= (1\ 2)\,e\\ (1\ 3) &= (1\ 2)(1\ 3\ 2)\\ (2\ 3) &= (1\ 2)(1\ 2\ 3)\end{aligned}$$

となっているではないですか！
この集合をまとめて $(1\ 2)A_3$ （A_3 の要素にそれぞれ左から $(1\ 2)$ をかけたもの）と書くと

$$S_3 = A_3 \cup (1\ 2)A_3$$

と表せます。さて，いまなぜ $(1\ 2)$ を左からかけたのでしょう？A_3 に右からかけたらダメ？
いえいえ。

$$\begin{aligned}(1\ 2) &= e\,(1\ 2)\\ (1\ 3) &= (1\ 2\ 3)(1\ 2)\\ (2\ 3) &= (1\ 3\ 2)(1\ 2)\end{aligned}$$

となるので，これも集合としては同じ。よって後ろの集合は $A_3(1\ 2)$ （A_3 の要素にそれぞれ右から $(1\ 2)$ をかけたもの）と表せて

$$S_3 = A_3 \cup A_3(1\ 2)$$

とも表せます。

さらにもう一つ疑問。これって $(1\ 2)$ だけの現象なのでしょうか？$(1\ 3)$ ではダメ？
いえいえ。

$$\begin{aligned}(1\ 3) &= (1\ 3)\,e\\ (1\ 2) &= (1\ 3)(1\ 2\ 3)\\ (2\ 3) &= (1\ 3)(1\ 3\ 2)\end{aligned}$$

となるので，少し順番は入れ替わりますが，集合としては一緒。後ろの集合は $(1\ 3)A_3$ とも表せます。
要するに，$(1\ 2)$，$(2\ 3)$，$(1\ 3)$ はどれでもよくて，A_3 にかけるのも，右からでも左からでもどちらでもよくて

$$S_3 = A_3 \cup gA_3 = A_3 \cup A_3 g \quad (g \text{ は } (1\ 2),\ (2\ 3),\ (1\ 3) \text{ のどれか})$$

と表されます。このように $g \in S_3$ に対して gA_3 と $A_3 g$ が同じ集合を表すとき，A_3 は S_3 の**正規部分群**であるといいます。

では，正規ではない部分群はどういうものでしょうか？
例えば S_3 の部分群 $H = \{e,\ (1\ 2)\}$ について，同様に H とそれ以外の集合で分けてみます。

$$S_3 = \{e,\ (1\ 2)\} \cup \{(1\ 3),\ (2\ 3),\ (1\ 2\ 3),\ (1\ 3\ 2)\}$$

後ろの集合をよく見比べてみると

$$\begin{aligned}(1\ 3) &= (1\ 3)\,e\\ (1\ 2\ 3) &= (1\ 3)(1\ 2)\\ (2\ 3) &= (2\ 3)\,e\\ (1\ 3\ 2) &= (2\ 3)(1\ 2)\end{aligned}$$

と表せるので，

$$S_3 = H \cup (1\ 3)H \cup (2\ 3)H$$

と表せます。しかし，右からかけたものを考えると

$$\begin{aligned}(1\ 3) &= e\,(1\ 3)\\ (1\ 3\ 2) &= (1\ 2)(1\ 3)\\ (2\ 3) &= e\,(2\ 3)\\ (1\ 2\ 3) &= (1\ 2)(2\ 3)\end{aligned}$$

となるので，

$$H(1\ 3) \neq (1\ 3)H, \quad H(2\ 3) \neq (2\ 3)H$$

となって，表される集合が変わってしまいます。よって，H は正規ではない部分群です。
　一般に，群 G の部分群 H が**正規部分群**であるとは，G の任意の元 g に対して，gH と Hg が一致することと定義します。

$\boxed{\text{問題}}$

巡回群 $\mathbb{Z}/6\mathbb{Z} = \{e,\ g,\ g^2,\ g^3,\ g^4,\ g^5\} \quad (g^6 = e)$ の正規部分群を見つけましょう。

$\boxed{\text{問題}}$

正 2 面体群 $D_4 = \{e,\ g,\ g^2,\ g^3,\ s,\ sg,\ sg^2,\ sg^3\}$ $(s^2 = g^4 = e,\ sgsg = e)$ の正規部分群を見つけましょう。

$\boxed{\text{発展}}$

4 次交代群

$$\begin{aligned} A_4 = \{&e,\ (1\ 2\ 3),\ (1\ 3\ 2),\ (1\ 2\ 4),\ (1\ 4\ 2),\ (1\ 3\ 4),\ (1\ 4\ 3), \\ &(2\ 3\ 4),\ (2\ 4\ 3),\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\} \end{aligned}$$

の正規部分群を見つけましょう。

2.3 剰余群

$$S_3 = A_3 \cup (1\ 2)A_3$$

において,

A_3 の元と A_3 の元をかけると A_3 の元,
A_3 の元と $(1\ 2)A_3$ の元をかけると，$(1\ 2)A_3$ の元
$(1\ 2)A_3$ の元と $(1\ 2)A_3$ の元をかけると，$(1\ 2)A_3$ の元

になります。これを集合同士のかけ算として表すと

$$\begin{aligned} A_3A_3 &= A_3 \\ A_3((1\ 2)A_3) &= (1\ 2)A_3 \\ ((1\ 2)A_3)((1\ 2)A_3) &= A_3 \end{aligned}$$

となり，集合同士がまた群の演算を満たしています！
このようにうまくいくのは，正規部分群で分けたときだけです。これらの集合がつくる群を**剰余群**といい，この場合

$$S_3/A_3 = \{A_3,\ (1\ 2)A_3\}$$

と表します。「剰余」というのは「割った余り」ということですが，この記号の通り,「S_3 を A_3 で割って S_3/A_3」という言い方をよくします。位数は確かに $|S_3/A_3| = |S_3|/|A_3|$ とように割り算になっています。S_3/A_3 は位数 2 の群で，巡回群 $\mathbb{Z}/2\mathbb{Z}$ と同じ型の群です。

　一般に，群 G の正規部分群 H があって，gH $(g \in G)$ （**剰余類**という）の集合に対して，演算

$$aH\,bH = abH$$

を入れると，群になります。この群を**剰余群**（または**商群**）といい，G/H とかきます。

$\boxed{\text{問題}}$

巡回群 $\mathbb{Z}/6\mathbb{Z} = \{e,\ g,\ g^2,\ g^3,\ g^4,\ g^5\} \quad (g^6 = e)$ の前問で求めた正規部分群による剰余群を作ってみましょう。

$\boxed{\text{問題}}$

正 2 面体群 $D_4 = \{e,\ g,\ g^2,\ g^3,\ s,\ sg,\ sg^2,\ sg^3\}$ $(s^2 = g^4 = e,\ sgsg = e)$ の前問で求めた正規部分群による剰余群を作ってみましょう。

$\boxed{\text{発展}}$

4 次交代群

$$\begin{aligned} A_4 = \{&e,\ (1\ 2\ 3),\ (1\ 3\ 2),\ (1\ 2\ 4),\ (1\ 4\ 2),\ (1\ 3\ 4),\ (1\ 4\ 3), \\ &(2\ 3\ 4),\ (2\ 4\ 3),\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\} \end{aligned}$$

の前問で求めた正規部分群による剰余群を作ってみましょう。

整数の群 $\mathbb{Z}$ の部分群 $n\mathbb{Z} = \{na \mid a \in \mathbb{Z}\}$ は正規部分群なので，剰余群 $\mathbb{Z}/n\mathbb{Z}$ が定義できます。これは n で割った余り 0, 1, 2, $\cdots$, $n-1$ で整数を分類した集合の群で，巡回群になっています。
一般に，可換群の部分群はすべて正規部分群で，剰余群も可換群です。

最後に

3 日間続いた群のお話は今日で終わりです。

明日，明後日は，方程式が解けるか解けないか（解の公式が存在するかどうか）というお話です。全く関係のないようなこの 2 つの事柄を，若きガロアはどんな素晴らしいアイディアでつなげて解決したのか？
明日が楽しみですね。

ガロアに始まった群の研究は，方程式のみならず，いろいろな分野で応用があり，研究がされています。物理で量子の回転を群で考えたり，ルービックキューブのようなパズルを群で説明したりもできます。
今回の講座で，君たちにとって少しでも「群」が身近になってくれれば幸いです。

問題の答え

P.2

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

P.4 $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) = \{(0,\ 0),\ (0,\ 1),\ (0,\ 2),\ (1,\ 0),\ (1,\ 1),\ (1,\ 2)\}$

$\mathbb{Z}/6\mathbb{Z} = \{0,\ 1,\ 2,\ 3,\ 4,\ 5\}$

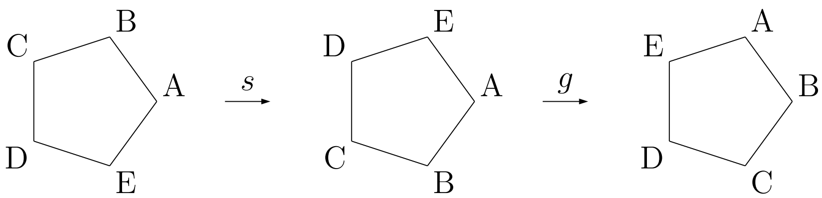
とすると，

$$\begin{aligned} &0 \to (0,\ 0), \quad 1 \to (1,\ 2), \quad 2 \to (0,\ 1), \\ &3 \to (1,\ 0), \quad 4 \to (0,\ 2), \quad 5 \to (1,\ 1) \end{aligned}$$

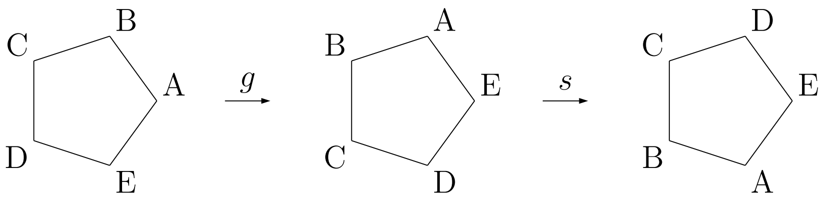
と対応させると $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \cong \mathbb{Z}/6\mathbb{Z}$ がいえる。

P. 6

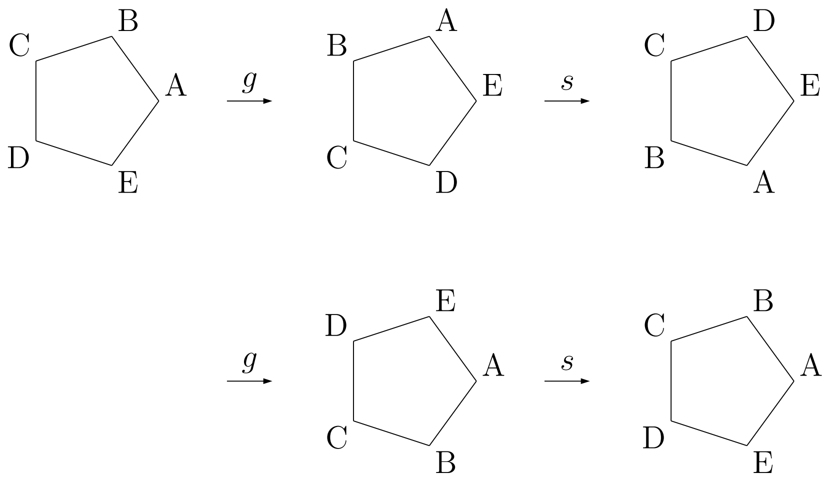
$gs:$



$sg:$



よって $gs \neq sg$



よって $sgsg = e$

$$sg^3sg^3 = e \qquad \therefore\ (sg^3)^{-1} = sg^3$$
$$sg^3sgsg^2sg^4s = sg^3(sgs)g^2(sg^4s) = sg^3g^{-1}g^2g^{-4} = s$$

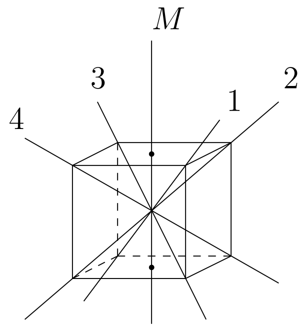
P.7 の表

	頂点の数	面の数	辺の数
正 4 面体	4	4	6
正 6 面体	8	6	12
正 8 面体	6	8	12
正 12 面体	20	12	30
正 20 面体	12	20	30

P.9　$P(6) \cong S_4$ となること

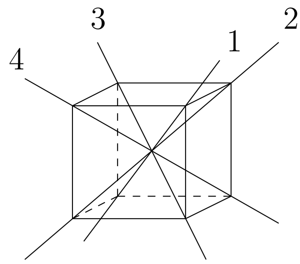
- (1 2 3 4) に対応する移動

  右の図の M を軸として 90° 回転すると，
  1 が 2，2 が 3，3 が 4，4 が 1 に移る。
  さらに回転を繰り返し，(1 3)(2 4)，(1 4 3 2) もできる。
  向かい合う 2 面の中心を通る軸が他に 2 つあり，
  (1 2 4 3)，(1 3 2 4) とその 2 乗，3 乗ができる。



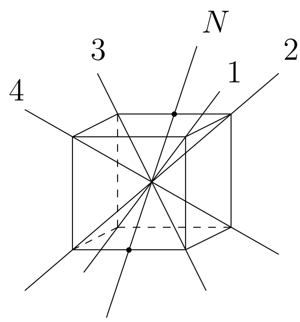
- (1 2 3) に対応する移動

  右の図の 4 を軸として 120° 回転すると，
  1 が 2，2 が 3，3 が 1 に移る。
  さらに 120° 回転をすると (1 3 2) もできる。
  同様に，1，2，3 をそれぞれ軸として回転すると
  (2 3 4)，(1 3 4)，(1 2 4) とその 2 乗ができる。



- (2 3) に対応する移動

  右の図の N は 2 と 3 の通る頂点の中点を通っている。N を軸として 180° 回転すると，
  2 が 3，3 が 2 に移る。
  平行な 2 辺の中点を通る軸は他に 5 つあり，
  (1 2)，(1 3)，(1 4)，(2 4)，(3 4) ができる。



P.11　$\mathbb{Z}/6\mathbb{Z}$ の部分群は

$$\{e\},\quad \mathbb{Z}/6\mathbb{Z},\quad (\text{自明な部分群})$$
$$\{e,\ g^3\},\quad (\cong \mathbb{Z}/2\mathbb{Z}),\qquad \{e,\ g^2,\ g^4\}\quad (\cong \mathbb{Z}/3\mathbb{Z})$$

P.12　D_4 の部分群は

$$\{e\},\quad D_4,\quad (\text{自明な部分群})$$
$$\{e,\ g^2\},\quad \{e,\ s\},\quad \{e,\ sg\},\quad \{e,\ sg^2\},\quad \{e,\ sg^3\},\quad (\cong \mathbb{Z}/2\mathbb{Z})$$
$$\{e,\ g,\ g^2,\ g^3\},\quad (\cong \mathbb{Z}/4\mathbb{Z})$$
$$\{e,\ g^2,\ s,\ sg^2\}\quad (\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$$

P.12　A_4 の部分群は

$$\{e\},\quad A_4\quad (\text{自明な部分群})$$
$$\{e,\ (1\ 2)(3\ 4)\},\quad \{e,\ (1\ 3)(2\ 4)\},\quad \{e,\ (1\ 4)(2\ 3)\}\quad (\cong \mathbb{Z}/2\mathbb{Z})$$
$$\{e,\ (1\ 2\ 3),\ (1\ 3\ 2)\},\quad \{e,\ (1\ 2\ 4),\ (1\ 4\ 2)\}$$
$$\{e,\ (1\ 3\ 4),\ (1\ 4\ 3)\},\quad \{e,\ (2\ 3\ 4),\ (2\ 4\ 3)\}\quad (\cong \mathbb{Z}/3\mathbb{Z})$$
$$\{e,\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\}\quad (\cong \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z})$$

P.15　$\mathbb{Z}/6\mathbb{Z}$ の正規部分群は

$$\{e\},\quad \mathbb{Z}/6\mathbb{Z},\quad \{e,\ g^3\},\quad \{e,\ g^2,\ g^4\}$$

（要するに，部分群は全て正規部分群）

D_4 の正規部分群は

$$\{e\},\quad D_4,\quad \{e,\ g^2\},\quad \{e,\ g,\ g^2,\ g^3\},\quad \{e,\ g^2,\ s,\ sg^2\}$$

A_4 の正規部分群は

$$\{e\},\quad A_4,\quad \{e,\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\}$$

P.17　$\mathbb{Z}/6\mathbb{Z}$ の剰余群は

$$(\mathbb{Z}/6\mathbb{Z})/\{e\} = \{\{e\},\ \{g\},\ \{g^2\},\ \{g^3\},\ \{g^4\},\ \{g^5\}\} \cong \mathbb{Z}/6\mathbb{Z}$$
$$(\mathbb{Z}/6\mathbb{Z})/(\mathbb{Z}/6\mathbb{Z}) = \{\mathbb{Z}/6\mathbb{Z}\} \cong \{e\}$$
$$(\mathbb{Z}/6\mathbb{Z})/\{e,\ g^3\} = \{\{e,\ g^3\},\ \{g,\ g^4\},\ \{g^2,\ g^5\}\} \cong \mathbb{Z}/3\mathbb{Z}$$
$$(\mathbb{Z}/6\mathbb{Z})/\{e,\ g^2,\ g^4\} = \{\{e,\ g^2,\ g^4\},\ \{g,\ g^3,\ g^5\}\} \cong \mathbb{Z}/2\mathbb{Z}$$

自明な正規部分群による剰余群は自分自身か $\{e\}$ と同型になるので，以下では省略。

D_4 の剰余群は

$$D_4/\{e,\ g^2\} = \{\{e,\ g^2\},\ \{g,\ g^3\},\ \{s,\ sg^2\},\ \{sg,\ sg^3\}\} \cong \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$$
$$D_4/\{e,\ g,\ g^2,\ g^3\} = \{\{e,\ g,\ g^2,\ g^3\},\ \{s,\ sg,\ sg^2,\ sg^3\}\} \cong \mathbb{Z}/2\mathbb{Z}$$
$$D_4/\{e,\ g^2,\ s,\ sg^2\} = \{\{e,\ g^2,\ s,\ sg^2\},\ \{g,\ g^3,\ sg,\ sg^3\}\} \cong \mathbb{Z}/2\mathbb{Z}$$

A_4 の剰余群は $V = \{e,\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\}$ として

$$\begin{aligned} A_4/V = \{&\{e,\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\},\\ &\{(1\ 2\ 3),\ (2\ 4\ 3),\ (1\ 4\ 2),\ (1\ 3\ 4)\},\\ &\{(1\ 3\ 2),\ (2\ 3\ 4),\ (1\ 2\ 4),\ (1\ 4\ 3)\}\} \cong \mathbb{Z}/3\mathbb{Z} \end{aligned}$$