第２回数学科リレー講座

「ガロア生誕２００年記念講習会」

第２日目

「集合から群まで」

小澤　嘉康

目 次

1 集合と演算 **1**

1.1 集合 1

1.2 特別な集合 2

1.3 写像 3

1.4 演算 4

2 数の拡張 **4**

2.1 自然数から有理数まで 5

2.2 有理数から実数・複素数へ 7

2.3 複素数のイメージ 9

2.4 代数学の基本定理の雰囲気 11

3 演算から群，環，体へ **17**

3.1 群 17

3.2 群の例 18

3.3 環 27

3.4 体 27

1　集合と演算

1.1　集合

数学ではまず考える対象の範囲を明確にする必要があるので**集合**というものを考える．
例えば山手線の駅でかっこいい駅を選ぼうとなったときに，考える範囲は山手線の駅の集合であって，これを Y とすると，

$$Y = \{ s \,\big|\, s \text{は山手線の駅} \}$$

となる．仮に大久保駅がとてもかっこよかったとしても，大久保駅は山手線の駅ではないので選ぶわけにはいかない．
集合の表し方には次の２通りある．１つめは集合を構成するものをすべて書き上げる方法で，山手線の駅の例では，

$$Y = \{ \text{新宿}, \text{新大久保}, \text{高田馬場}, \cdots, \text{原宿}, \text{代々木} \}$$

となる．もう１つは先の

$$Y = \{ s \,\big|\, s \text{は山手線の駅} \}$$

のように，$|$ の左側に集合を構成するものの「型」を書き，右側に「みたすべき条件」を書く方法である．
なお，集合を構成するものことを**元**または**要素**といい，

$$\text{新大久保} \in \boldsymbol{Y}$$

のように $\in$ を用いて表す．このとき，元「新大久保」は山手線の駅の集合「Y」に**属する**という．
逆に元でないときは，

$$\text{大久保} \notin Y$$

のように $\notin$ を用いて表す．

次にＪＲ東日本の駅の集合を E とする．つまり，

$$E = \{ s \,\big|\, s \text{はＥ電の駅} \}$$

とする．この場合，元をすべて書き上げることは不可能ではないにしても難しい．

山手線の駅 $s \in Y$ はすべてＪＲ東日本の駅なので $s \in E$ でもある．このように，

$$s \in Y \Rightarrow s \in E$$

のとき，集合 Y は集合 E に**含まれる**，または，集合 Y は集合 E の**部分集合**であるといい，

$$\boldsymbol{Y \subset E}$$

のように $\subset$ を用いて表す．
なお，当然

$$s \in Y \Rightarrow s \in Y$$

なので，$Y \subset Y$ であることに注意せよ．

また２つの集合 A, B があり，

$$A \subset B \text{ かつ } B \subset A$$

のとき，集合 A と集合 B は**等しい**といい，

$$\boldsymbol{A = B}$$

と表す．

集合の元の個数を**位数**といい，

$$\boldsymbol{|A|}$$

のように書く．先の山手線の駅の集合 Y では，

$$|Y| = 29$$

である．

1.2 特別な集合

数の集合は頻繁に用いるので特別な記号が用意されている．

自然数全体の集合　$\mathbb{N}$
整数全体の集合　$\mathbb{Z}$
有理数全体の集合　$\mathbb{Q}$
実数全体の集合　$\mathbb{R}$
複素数全体の集合　$\mathbb{C}$

数の集合の元のことを単に「数」ということもある．
それぞれの性質については後ほど順に説明する．
なお，自然数全体の集合に 0 を入れた方が便利なことが多いのだが，ここでは教科書通り，

$$\mathbb{N} = \{1, 2, 3, \cdots\}$$

とし，$0 \notin \mathbb{N}$ とする．(数学なので合理性や整合性が保たれ，無矛盾であればどのように定義してもよい．単なる好みの問題である．)

1.3 写像

２つの集合 A と B において，集合 A の各々の元に対して集合 B のある元が対応するような関係があることは少なくない．
例えば，集合 Y を相変わらず山手線の駅の集合とし，集合 H を $H = \mathbb{N}$ とする．そして，集合 Y の元 s に対して，集合 H の元への対応を「駅 s のホームの数」とする．すると集合 Y から集合 H への一つの関係ができる．
この関係を n と表すことにすると，

$$n(\text{新大久保}) = 1, \quad n(\text{代々木}) = 3, \quad n(\text{原宿}) = 1, \quad \cdots$$

のようになる．

問い：$n(\text{新宿}), \quad n(\text{池袋}), \quad n(\text{東京}), \quad n(\text{大久保})$ を求めよ．

注：大久保 $\notin Y$ なので，$n(\text{大久保})$ そもそも定義できない．よって値はなし．その他の駅の答えは各自で確認してみよ．

すべての $s \in Y$ に対し $n(s) \in H$ となるとき，

$$n : Y \to H, \quad s \mapsto n(s)$$

のように書き，このような対応の関係 n を**写像**という．また，$n(s)$ を写像の**値**という．(写像とは簡単にいえば**関数**と同じと思って良い．)

1.4　演算

特別な写像として**演算**というものがある．
写像 $\circ$ が演算であるとは，１つの集合 A において，A の２つの元 $a, b \in A$（a と b は同じでも構わない）に対し，値 $a \circ b$（写像本来の書き方からすれば $\circ(a, b)$ であるのだが演算のときは通常 $a \circ b$ と表す）が再び A の元になるとき，つまり $a \circ b \in A$ となるのときにいう．
このとき，集合 A には**演算 $\circ$ が入っている**という．

自然数全体の集合 $\mathbb{N}$ のどの２つの数 a, b においても，加法 $a + b$ は再び自然数になるので，自然数の集合 $\mathbb{N}$ には加法 $+$ という演算が入っている．
一方，減法 $-$ は演算にならない．実際 $5 - 3 \in \mathbb{N}$ であるが $3 - 5 \notin \mathbb{N}$ であるので，値が必ずしももとの集合に入らない場合があるときには演算が入っているとはいわない．

数字以外の元を持つ集合にも演算を入れることができる．例えば，集合 T を

$$T = \{\spadesuit, \heartsuit, \clubsuit, \diamondsuit\}$$

とする．このとき，演算 $\boxdot$ を次の表で定義する．

$\boxdot$	$\spadesuit$	$\heartsuit$	$\clubsuit$	$\diamondsuit$
$\spadesuit$	$\spadesuit$	$\heartsuit$	$\diamondsuit$	$\diamondsuit$
$\heartsuit$	$\diamondsuit$	$\spadesuit$	$\spadesuit$	$\diamondsuit$
$\clubsuit$	$\diamondsuit$	$\heartsuit$	$\clubsuit$	$\heartsuit$
$\diamondsuit$	$\heartsuit$	$\spadesuit$	$\heartsuit$	$\clubsuit$

この表の見方は，例えば，１行目左から２列目は $\spadesuit \boxdot \heartsuit = \heartsuit$，３行目左から４列目は $\clubsuit \boxdot \diamondsuit = \heartsuit$ のようになる．このように集合の２つの元に対し１つの元を対応させる表を作ることは，その集合に一つの演算を入れることと同じである．

2　数の拡張

前節の最後に見たように自然数全体の集合 $\mathbb{N}$ では減法 $-$ は演算にはならないが，整数全体の集合 $\mathbb{Z}$ では演算になる．一方，整数全体の集合 $\mathbb{Z}$ では乗法 $\times$ は演算になるが，除法 $\div$ は演算にならない．しかし，有理数全体の集合 $\mathbb{Q}$ では除法は演算になる[1]．

[1]厳密には 0 を除く有理数全体の集合としなければ除法は演算として入らない．詳細は後述．

このことは，数の拡張という視点から見れば実は当たり前のことである．ここでは，この数の拡張について考える．

2.1 自然数から有理数まで

物を数えるのに必要な自然数全体の集合 $\mathbb{N} = \{1, 2, 3, 4, 5, \cdots\}$ から始める．
先ほどから何度も見ているように加法 $+$ は演算になるが減法 $-$ は演算にならない．このまま「もう引き算はやらない」とか「これからは大きい数から小さい数を引くことしかやらない」と決心しても構わないが，そうすると話がお終いになり，この講習も 4 日余り残して終了となってしまい，その結果，講習料の返却という事態まで発展しかねないので，何としても別の方針を立てなければいけない．
こんなとき数学では「自然数の集合に減法が入らなければ，減法ができように集合を拡張すればいい」という風な発想をする．そこで新しい集合 $\mathbb{Z}$ として，

$$\mathbb{Z} = \{a - b \,\big|\, a \in \mathbb{N},\, b \in \mathbb{N}\}$$

と定義する．
$a, b \in \mathbb{N}$ で $a < b$ のとき，$a - b$ はできなかったのでは？と心配になるかもしれないが，それは $\mathbb{N}$ で考えているからであり，今は $a - b$ は $\mathbb{N}$ に入るとは限らないので $a - b$ は自然数ではないかもしれない「数」とし，これらをすべて含む新しい数の全体を考えよう，ということである．この $\mathbb{Z}$ の元を整数ということにする．
また，

$$\mathbb{N} \subset \mathbb{Z}$$

であることは，次のように確認できる．$n \in \mathbb{N}$ に対し，$n+1 \in \mathbb{N}$ であるので，$a = n+1, b = 1$ とすると，$n = (n+1) - 1 = a - b$ より，$n \in \mathbb{Z}$ とわかる．
このように整数全体の集合を定義しているので，数の拡張という視点で見れば，加法と減法が入ることは当然なのである[2]．

次に，乗法 $\times$ について．整数全体の集合には乗法は演算として入っているのだが，除法 $\div$ は入っていない．そこで，自然数の減法のときのように問題が大きくなる前に対処をしなけれ

[2] とはいっても，実はこのことを厳密に示そうとすると，そもそも演算加法の定義は何？まで遡らなくてはいけない．結構面倒な作業である．自分では当たり前と思っていても実は当たり前ではないかもしれない，ということはよくあることだ．

ばいけない．そう，割り算がきちんとできるように集合を拡張するのである．そこで新しい集合として，

$$\{\frac{a}{b} \mid a \in \mathbb{Z},\ b \in \mathbb{Z}\}$$

を考えてみよう．

何か気がつくことがあるだろうか．

先の整数のときは $\mathbb{Z} =$ と名前が付いていたのに今回は $\mathbb{Q} =$ と付いていないのでミスプリである... ではない．このままでは数の集合として認められないのである．

$0 \in \mathbb{Z}$ であるので，分母が $b = 0$ となる可能性があり，$\frac{a}{0}$ はどのように定義しても整合性が保たれないので「数」として扱うわけにはいかない．よって，改めて新しい集合 $\mathbb{Q}$ を

$$\mathbb{Q} = \{\frac{a}{b} \mid a \in \mathbb{Z},\ b \in \mathbb{Z},\ b \neq 0\}$$

と定義する．そして $\mathbb{Q}$ の元，つまり「分数で表示することができる数」を有理数という．

一つだけコメントをしておくと，この $\mathbb{Q}$ の定義では $b \neq 0$ が必要であるが，せっかく自然数の集合には 0 が入っていないので

$$\mathbb{Q} = \{\frac{a}{b} \mid a \in \mathbb{Z},\ b \in \mathbb{N}\}$$

とすれば簡潔ではないかと思う人もいるかもしれない．確かに，どちらで定義しても集合としては等しいのであるが，ここでは整数全体の集合に除法が入るように拡張するという方針なので，分子分母ともに整数である必要がある．

問い：有理数の全体の集合 $\mathbb{Q}$ は除法で閉じているか確認せよ．

除法ができるように整数全体の集合を拡張したのだから閉じているに決まっているさ！ときちんと確認しなかった君 !! 周りの空気に飲まれてはいけない !!!

実は有理数全体の集合は除法では閉じていない．演算が閉じていることの定義を思い出してみよう．どんな２つの元においても必ず演算の結果がもとの集合に入らなければいけない．

有理数全体の集合を定義するときに分母が 0 になることのないようにしたわけであるが，0 そのものは有理数である．したがって，例えば $1 \in \mathbb{Q},\ 0 \in \mathbb{Q}$ であるが $1 \div 0 = \frac{1}{0} \notin \mathbb{Q}$ であるので，反例がある．

したがって，除法で閉じた集合にするには

$$\mathbb{Q}^{\times} = \{\frac{a}{b} \mid a \in \mathbb{Z},\ b \in \mathbb{Z},\ a \neq 0,\ b \neq 0\}$$

という別の集合 $\mathbb{Q}^\times$ を定義しなければならない.

問い：$\mathbb{Q}^\times$ は除法で閉じていることを確認せよ.

なお $\mathbb{Q}^\times$ は整数全体の集合の拡張にはなっていないことにも注意せよ.

なかなかうまくいかないものだなと感じているかもしれないが，実はそうではなく非常に重要な意味を持っている．この $\mathbb{Q}$ と $\mathbb{Q}^\times$ の関係は後ほど「体」の節で改めて詳しく述べる.

以上より，四則演算（ただし 0 で割ることを除く）ができる数全体の集合として有理数全体の集合まで定義できた.

2.2　有理数から実数・複素数へ

円の直径の長さに対する周の長さの比や，正方形の一辺の長さに対する対角線の長さの比が分数で表せないことは（証明できるかは別として）よく知られている．つまり，

$$\pi \notin \mathbb{Q}, \quad \sqrt{2} \notin \mathbb{Q}$$

である．よって，さらに数を拡張していこう[3].

累乗を考える．$a \in \mathbb{Q}$ に対し，a^2 は,

$$a^2 = a \times a$$

であるので $a^2 \in \mathbb{Q}$ であることはよい．しかし逆に，例えば，$2 \in \mathbb{Q}$ に対し

$$a^2 = 2$$

となる $a \in \mathbb{Q}$ はあるかという問いの答えは「否」である．つまり 2 乗して 2 になる「数」は有理数ではない，ということである.

問い：2 乗して 2 になる「数」は有理数ではないことをを証明せよ.（15 点）

[3] これから実数全体の集合 $\mathbb{R}$ と複素数全体の集合 $\mathbb{C}$ まで拡張していくのだが，しかしながら実は，今までのように何か演算ができるように「数」を付け加えていくという方法では有理数全体の集合を実数に拡張することができないことが知られている．さすがに証明は難しいので，興味のある人はこの講習の後半を担当する先生（K 先生，H先生，A先生）に質問してもらうことにして，ここでは，今少なくとも有理数全体の集合では足りないので「拡張する必要があるので拡張していこう」くらいのノリでいきたいと思う.

さらには，正の数も負の数も２乗すると正の数になるので，例えば，

$$a^2 = -1$$

となる「数」a は明らかに有理数ではない．

今までは，自然数全体の集合から，演算で閉じていくように数の集合を拡張していったのだが，ここでは趣をかえて，図形的な視点から「数」をとらえていこうと思う．まずはあのお馴染みの数直線である．
先の正方形の対角線の例でもわかるように，対角線は存在するので「長さ」があるはずだが，その「長さ」を表現する有理数がない，ということである．「長さ」がないわけではないので何らかの値は存在するのである．
直線上に「原点 O」と呼ばれる基準の点を一つ決め，この原点により直線は２つの半直線に分割されるのだが，一方に「１」と呼ばれるもう一つの基準の点をとり，原点から１までの「長さ」の値を「数」1 をみなす．「数」の加法を類推して数 $2, 3, \cdots$ に対応する点２，３，... をとっていく．他方の半直線上には $-1, -2, -3, \cdots$ を同様にとっていく．これにより直線は有理数全体を含むある「数」全体の集合をみなすことができる．この直線を数直線という．

$\mathbb{R} =$

数直線が表す「数」全体の集合を実数全体の集合といい $\mathbb{R}$ で表す．

しかしながら，どの実数であっても２乗して負の数にはならないので，

$$a^2 = -1$$

となる数 a は実数ではない．
そこで，２乗して -1 になる「数」を含む数の集合へと拡張していく．２乗して -1 になる「数」は１つとは限らないが，基準が決まればいいので，そのうちの１つを i や $\sqrt{-1}$ で表すことにする[4]．この $i = \sqrt{-1}$ を虚数単位という．

$$i^2 = \sqrt{-1}^{\,2} = -1\ .$$

[4]なぜ i を用いるのかについて．$i = \sqrt{-1} \notin \mathbb{R}$ であるので，古くは実数ではないので現実には存在しない想像上の数という意味で imaginary number（和訳は虚数：決して虚しい数という意味ではない）と名付けられた．この頭文字をとって i が使われるようになった．また i は 1 に似ているので違和感が少ない．

そして，２つの実数 $a, b \in \mathbb{R}$ とこの虚数単位 i を用いて

$$a + b\,i$$

と定義する数を複素数といい，複素数全体の集合を $\mathbb{C}$ で表す．

$$\mathbb{C} = \{a + b\,i \,\big|\, a, b \in \mathbb{R}\}$$

２つの複素数 $a + b\,i,\ c + d\,i$ の計算方法は，i^2 が出てきたら $i^2 = -1$ と直すことに注意すれば，通常の文字式のように計算すればいい．

例：$(3 + 4i) + (-2 - 5i) = 3 + 4i - 2 - 5i = (3 - 2) + (4 - 5)i = 1 - i$

$(3 + 4i)(-2 - 5i) = -6 - 15i - 8i - 20i^2 = -6 - 23i - 20 \times (-1) = 14 - 23i$

また，a が正の実数のときは，

$$\sqrt{-a} = \sqrt{a \times (-1)} = \sqrt{a} \times \sqrt{-1} = \sqrt{a}\,i$$

としてよいが，

$$\sqrt{-1} \times \sqrt{-1} = \sqrt{(-1) \times (-1)}$$

とはしてはいけない．

問い：なぜ，前者がよく，後者がダメなのかを考えてみよ．

複素数まで拡張することの最大の利点は，n 次方程式の解は必ず複素数の範囲で求まるということにある．(この事実を「代数学の基本定理」という)

例えば，２次方程式であっても，$x^2 + 3x + 4 = 0$ のように，判別式 $D = -7$ と負の数となると，実数解は持たないのであるが，複素数まで広げると，解は $x = \dfrac{-3 \pm \sqrt{-7}}{2} = \dfrac{-3 \pm \sqrt{7}\,i}{2}$ と求まる．実際，解の公式に代入してみればよい．

2.3　複素数のイメージ

実数全体の集合は数直線という明確なイメージがあるのだが，定義から複素数全体の集合を直ぐに実感するのは難しいと思われる．それゆえ古くは実在しない想像上の数といわれたのだ．ここではやはり実数における数直線のように，図形的なアプローチをしてみたい．

実数での $(-1) \times (-1) = 1$ と虚数の $i \times i = -1$ とを対比しながら考えていく．

実数での $(-1)\times(-1)=1$ を数直線上での動きとしてとらえると，例えば，正の数 3 に注目してみると，

$$3\times(-1)=-3$$

であり，さらに，

$$3\times(-1)\times(-1)=-3\times(-1)=3$$

のように，(-1) 倍すると，3 は数直線上で原点対称の -3 に移り，さらに (-1) 倍すると，-3 はさらに原点対称の 3 に移る．結果，２回原点対称移動するので 3 はもとの 3 に戻ってくることになる．

一方，i の方はどうだろうか．

$$i\times i=-1$$

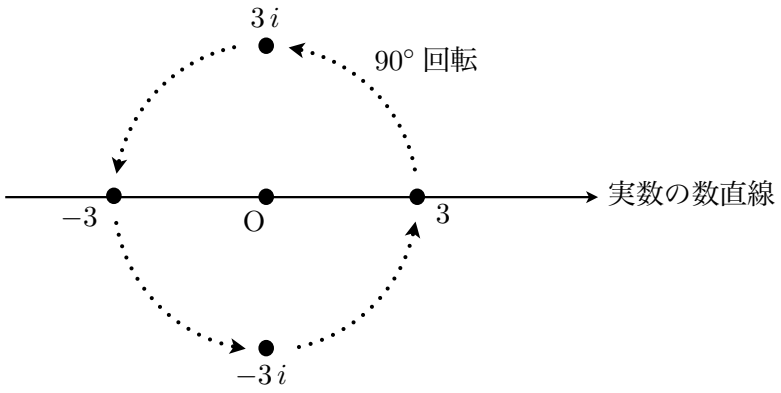
より，i 倍を２回することは原点対称移動に対応すると思われる．このことを図形の性質の知識を頼りに，２回すると原点対称移動になる移動を考えると，90° の回転移動が思いつく．例えば，3 に注目してみると，

$$3\times i=3i$$

であり，さらに，

$$3\times i\times i=3\times(-1)=-3$$

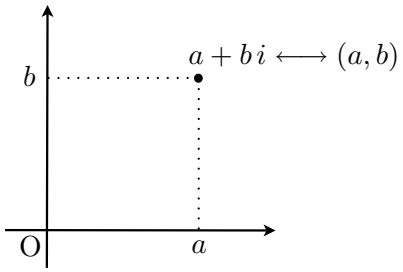
となり原点対称移動なので，



のようなイメージを持ってはどうであろうか．そもそも，虚数は（実数全体の集合）＝（直線上）にはないのだから，この新しい複素数全体の集合を図形的に表現しようとするならば，当然，数直線を含むような図形を考えなければいけないので，3 を原点を中心として 90° 回転移動した点は数直線からはみ出してしまうが，この点と $3i$ が対応するととらえることは，特に不自然なことはないことに気がつくであろう．

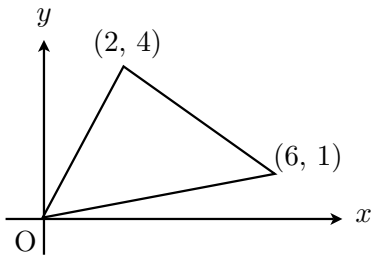
つまり，実数全体の集合が数直線に対応するように，複素数全体の集合は座標平面に対応させるとよさそうなことがわかった．

$$\mathbb{C} \ni a + b\,i \longleftrightarrow (a,\, b) \in (\text{座標平面})$$

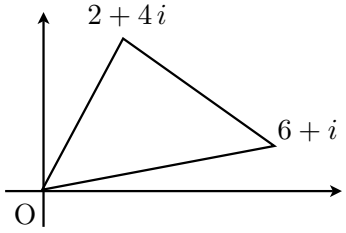


ということである．

このように複素数全体の集合は座標平面（数平面）として表現できるので，逆に，座標平面上の図形上の点を複素数としてとらえることができる．例えば，座標平面上の３点 $(0,\, 0),\ (2,\, 4),\ (6,\, 1)$ を頂点とする三角形は，



３つの複素数 $0,\ 2 + 4\,i,\ 6 + i$ を頂点とする三角形と見ることができる．



2.4　代数学の基本定理の雰囲気

n 次方程式の解は必ず複素数の範囲で求まることの雰囲気だけ感じてみよう[5]．

[5]やはりこれもさすがに証明は難しいので，興味のある人はやはりこれもこの講習の後半を担当する先生（K先生，H先生，A先生）に質問してみよう！

２次方程式 $x^2+3x+4=0$ を例にする．ここでの内容は一般の n 次方程式でも同じである．
複素数全体の集合から複素数全体の集合への写像（関数）f として，

$$f:\mathbb{C}\to\mathbb{C},\quad f(x)=x^2+3x+4,\ x\in\mathbb{C}$$

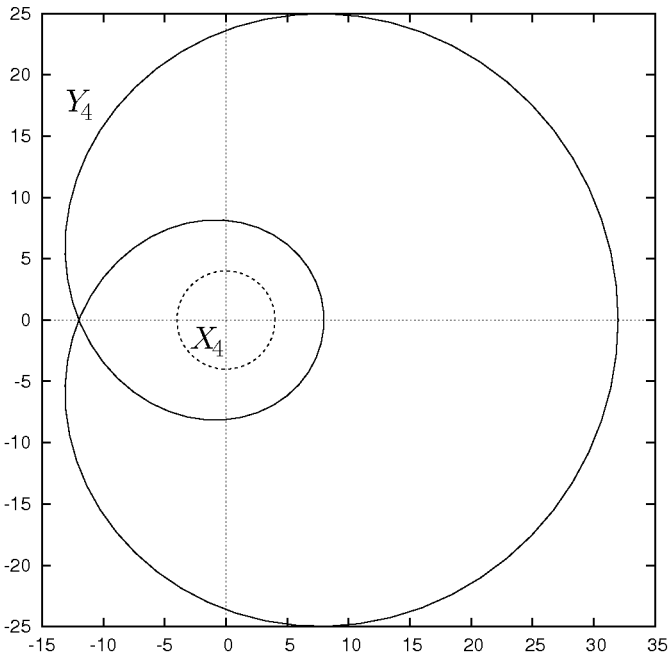
を考える．
また，$\mathbb{C}$ の部分集合 X_r を，

$$X_r=\{x\in\mathbb{C}\,\big|\,x \text{ は原点 O を中心とし半径 } r \text{ の円（周）上の点に対応する数 }\}$$

とする．なお，X の添字 r は半径なので正の実数をとるものとする．そして，$\mathbb{C}$ の部分集合 Y_r を，

$$Y_r=\{y\in\mathbb{C}\,\big|\,y=f(x),\ x\in X_r\}$$

とする．つまり，X_r に含まれる複素数 x（円上の点）を関数 $y=f(x)$ に代入したときの値 y に対応する平面上の点をすべてとったものである．X_r を定義域とする関数 $y=f(x)$ の値域が Y_r ということである．(簡単に考えれば Y_r は関数 $y=f(x)$ のグラフみたいなものと思っていれば十分.)
$r=4$ のときを平面上の図で見てみると，



内側の点線の円が半径 4 の円つまり X_4 を表し，外側のクルクル曲線が Y_4 を表している．

さて，このような図をかくことで何がみえてくるのだろうか？今の関心事は方程式

$$x^2 + 3x + 4 = 0$$

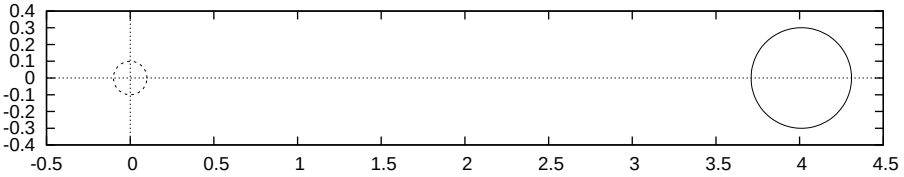
が複素数の解を持つかということである．これは $f(x) = x^2 + 3x + 4$ とおいているので，

$$f(x) = 0$$

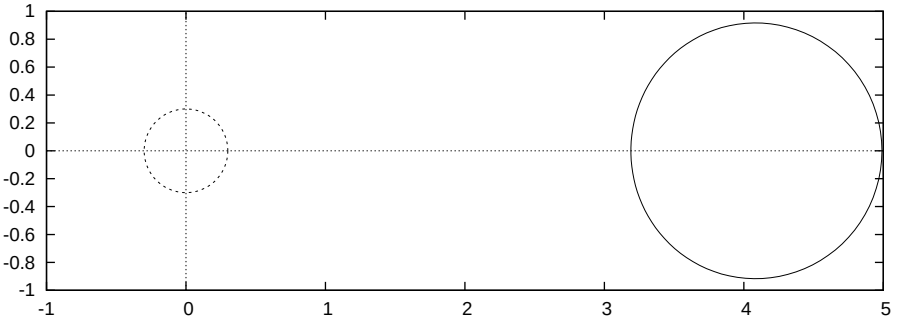
となる $x \in \mathbb{C}$ が存在するか，ということと同値である．
さて，この $f(x) = 0$ とは図ではどういう状態なのか．それは関数 $y = f(x)$ の値域である Y_r が原点 O を通過するということである．そしてこの r のとき，定義域である X_r 内の x で $f(x) = 0$ をみたすものが存在するということである．
よって，r の値を変化させたときに，どのような関数 f であっても必ず原点を通過する Y_r が存在することを示せばよい．

Y_r の動きを調べるために，r を小さいところから順にいくつか値を入れた図を見てみよう．
点線の円が X_r で実線の曲線が Y_r である．

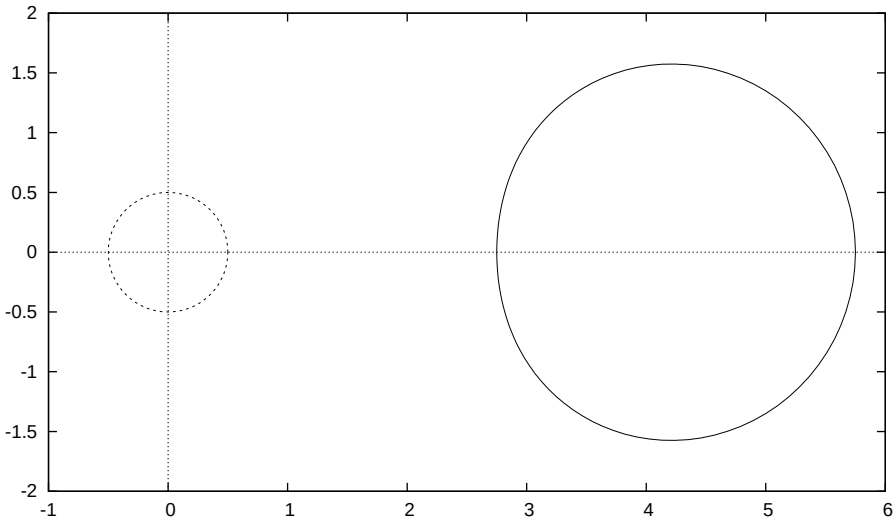
$r = 0.1$



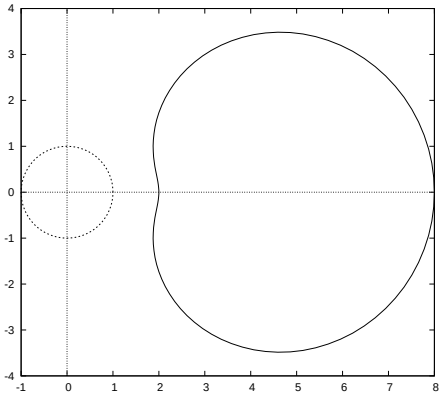
$r = 0.3$



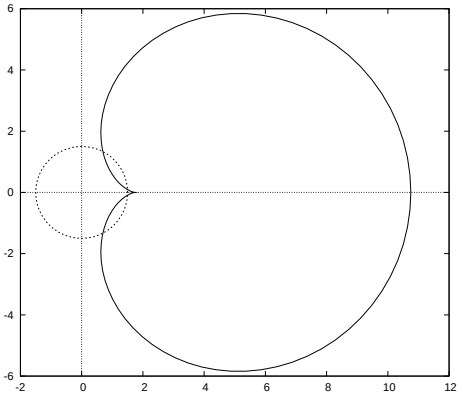
$r = 0.5$


2
1.5
1
0.5
0
-0.5
-1
-1.5
-2
-1
0
1
2
3
4
5
6

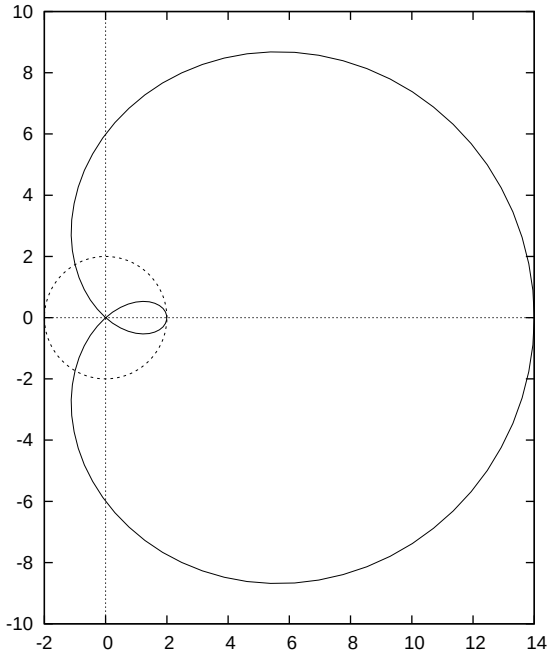
$r = 1$


4
3
2
1
0
-1
-2
-3
-4
-1
0
1
2
3
4
5
6
7
8

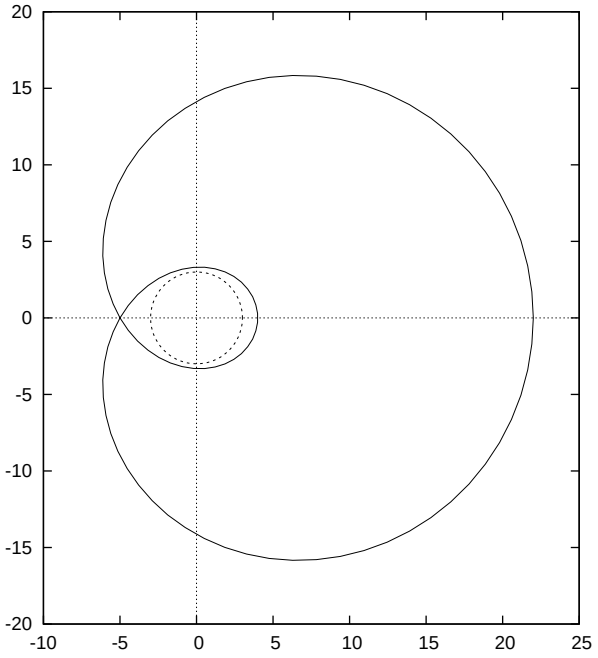
$r = 1.5$


6
4
2
0
-2
-4
-6
-2
0
2
4
6
8
10
12

$r = 2$



$r = 3$



目盛りの縮尺が同じでないのでわかりにくいかもしれないが，r が 0 に近いときは Y_r も小さいのだが，r が大きくなるにつれ Y_r もどんどん大きくなっていくことがわかるだろうか．r を 0 から連続的に大きくしていったときの Y_r のどんどん大きくなる様子をアニメーション

のような感覚で想像すると，ある瞬間 Y_r が原点 O を通過するときが少なくとも 1 回はあることがわかるだろう．

この例では $r = 2$ のときである．しかもクルクル曲線なので $r = 2$ のときに曲線は 2 回原点を通過しているのである．よって，2 次方程式 $x^2 + 3x + 4 = 0$ の解 x は $x \in X_2$，つまり，原点より 2 離れたところにある数ということである．

このことを確認してみよう．2 次方程式であれば解の公式に代入して解を求めることができる．解は，

$$x = \frac{-3 - \sqrt{7}\,i}{2},\ \frac{-3 + \sqrt{7}\,i}{2}$$

である．複素数と座標平面上の点の対応は

$$a + b\,i \longleftrightarrow (a,\, b)$$

であったので，

$$\frac{-3 - \sqrt{7}\,i}{2} \longleftrightarrow \left(-\frac{3}{2},\, -\frac{\sqrt{7}}{2}\right)$$

$$\frac{-3 + \sqrt{7}\,i}{2} \longleftrightarrow \left(-\frac{3}{2},\, \frac{\sqrt{7}}{2}\right)$$

となる．

これら 2 つの点が原点を中心とする半径 2 の円上にあることは三平方の定理より明らかである．

3　演算から群，環，体へ

今まで色々な演算を見てきた．加法，乗法，あるいは累乗．また，先の集合$T = \{\spadesuit, \heartsuit, \clubsuit, \diamondsuit\}$での演算 $\boxdot$ のように対応表をつくることはその集合に一つの演算を決めることになるので，無数の演算があることがわかる．
その中で，何となく雰囲気でも構わないが，似ている演算があることに気がつくだろうか？例えば整数全体の集合 $\mathbb{Z}$ における加法 $+$ と，有理数全体の集合から 0 を除いた集合 $\mathbb{Q}^\times$ における乗法 $\times$．直ぐに納得できる人もいれば，できない人もいるのは，どのように見ると似ているあるいは同じとなるのか，その視点の定め方によるからである．

3.1　群

ここでは，様々な重要な演算の多くが持っている「群」という性質について見ていく．

集合 G 上に演算 $\circ$ が入っており，次の 3 つの条件をみたすとき，集合 G と演算 $\circ$ の組 $(\boldsymbol{G}, \circ)$，あるいは単に集合 $\boldsymbol{G}$ を**群**という．

(i) どんな G の元 a, b, c において，$(a \circ b) \circ c = a \circ (b \circ c)$ が成り立つ．これを**結合法則**という．これは計算は式のどこから始めてもよいということなので $a \circ b \circ c$ と表せる．

(ii) G の中に**単位元**と呼ばれる特別な元 $\varepsilon \in G$ が存在し，どんな $a \in G$ に対しても，$a \circ \varepsilon = \varepsilon \circ a = a$ をみたす．

(iii) G のどんな元 a の各々に対し**逆元**と呼ばれる元 $a' \in G$ が存在し，$a \circ a' = a' \circ a = \varepsilon$ をみたす．

ここで，(ii) の $a \circ \varepsilon = \varepsilon \circ a$ や，(iii) の $a \circ a' = a' \circ a$ は当たり前でどちらか一方のみでよく，他の一方は敢えてあげる必要はないのでは，と感じるかもしれないが，実は一般の演算においては必ずしも，

$$a \circ b = b \circ a$$

が成り立つとは限らず，

$$a \circ b \neq b \circ a$$

となるものが少なくない．よって，(ii)，(iii) では両方あげる必要がある．このことが成り立つかどうかの区別は重要なので，さらに次のように定義を続ける．

群 $(G, \circ)$ が，さらに次の条件をみたすとき，**可換群**あるいは**アーベル群**という．

(iv) G のどんな元 a, b において，$a \circ b = b \circ a$ が成り立つ．これを**交換法則**という．

なお，一般の群で (iv) が成り立たないことを強調するときは**非可換群**という．

3.2 群の例

まず，数の集合は群になるのか調べていく．

$(\mathbb{Z}, +)$ は可換群になる．
実際 $a, b, c \in \mathbb{Z}$ において．
(i) 結合法則：$(a+b)+c = a+(b+c)$ は加法の意味を考えれば成り立つことは直ぐにわかる．
(ii) 単位元：$a + 0 = 0 + a = a$ が成り立つので，加法においては $0 \in \mathbb{Z}$ が単位元である．
(iii) 逆元：$a + (-a) = (-a) + a = 0$ が成り立つので，$a \in \mathbb{Z}$ に対しては $-a \in \mathbb{Z}$ が逆元である．
また，(iv) 交換法則：$a + b = b + a$ が成り立つことも加法の意味より明かである．
よって，$(\mathbb{Z}, +)$ は可換群であることがわかった．
整数全体の集合は，自然数全体の集合を加法に関して群になるように拡張したものだといえる．

問い：$(\mathbb{Z}, \times)$ は群になるか．なるとすれば単位元，逆元は何か．また交換法則は成り立つか．確認せよ．

$(\mathbb{Z}, \times)$ は群にはならないが，整数全体の集合における乗法はかなりいい性質を持っていることは確かである．整数全体の集合は加法において群だけでなく「環」とよばれる性質を持っている．詳細は後述．

問い：では $(\mathbb{Q}, \times)$ は群になるか．なるとすれば単位元，逆元は何か．また交換法則は成り立つか．確認せよ．

$(\mathbb{Q}, \times)$ は群にはならない．しかしながら，$(\mathbb{Q}^\times, \times)$ は可換群になる．
実際 $a, b, c \in \mathbb{Q}^\times$ において．
(i) 結合法則：$(a \times b) \times c = a \times (b \times c)$ は分子分母各々での整数の乗法の意味を考えれば成り立つことは直ぐにわかる．

(ii) 単位元：$a \times 1 = 1 \times a = a$ が成り立つので，乗法においては $1 \in \mathbb{Q}^{\times}$ が単位元である．
(iii) 逆元：$a \times \dfrac{1}{a} = \dfrac{1}{a} \times a = 1$ が成り立つので，$a \in \mathbb{Q}^{\times}$ に対しては $\dfrac{1}{a} \in \mathbb{Q}^{\times}$ が逆元である．
また，(iv) 交換法則：$a \times b = b \times a$ が成り立つことも整数の乗法の意味より明かである．

整数全体の集合と同様に $(\mathbb{Q}, +)$ は群になるが $(\mathbb{Q}, \times)$ は群にはならない．しかしながら，有理数全体の集合における乗法は，整数全体の集合における乗法よりさらによい性質を持っている．有理数全体の集合は「体」とよばれる性質を持っている．詳細はやはり後述．

次に演算の節でててきたトランプのマークの集合 $(T, \boxdot)$ について調べてみる[6]．

$$T = \{\spadesuit, \heartsuit, \clubsuit, \diamondsuit\}$$

$\boxdot$	$\spadesuit$	$\heartsuit$	$\clubsuit$	$\diamondsuit$
$\spadesuit$	$\spadesuit$	$\heartsuit$	$\diamondsuit$	$\diamondsuit$
$\heartsuit$	$\diamondsuit$	$\spadesuit$	$\spadesuit$	$\diamondsuit$
$\clubsuit$	$\diamondsuit$	$\heartsuit$	$\clubsuit$	$\heartsuit$
$\diamondsuit$	$\heartsuit$	$\spadesuit$	$\heartsuit$	$\clubsuit$

(i) の結合法則について．例えば，$\spadesuit$, $\clubsuit$, $\heartsuit$ では，

$$(\spadesuit \boxdot \clubsuit) \boxdot \heartsuit = \diamondsuit \boxdot \heartsuit = \spadesuit$$

となるが，一方，

$$\spadesuit \boxdot (\clubsuit \boxdot \heartsuit) = \spadesuit \boxdot \heartsuit = \heartsuit$$

となるので，

$$(\spadesuit \boxdot \clubsuit) \boxdot \heartsuit \neq \spadesuit \boxdot (\clubsuit \boxdot \heartsuit)$$

となり，さっそく成り立たない．よって，$(T, \boxdot)$ は群にはならないことがわかる．

しかしながら，せっかくトランプのマークの集合を考えたのに，このまま終わりにしてはMOTTAINAI ので，集合 T に別の演算を入れて群にしてみよう．例えば，

[6] この例は海城中学校・高等学校　研究集録　第３２集「こういうのも数学（前編）」の一部を抜粋し表現等を修正したものである

$$T = \{\spadesuit, \heartsuit, \clubsuit, \diamondsuit\}$$

⊞	♠	♡	♣	♢
♠	♠	♡	♣	♢
♡	♡	♣	♢	♠
♣	♣	♢	♠	♡
♢	♢	♠	♡	♣

はどうだろうか.

問い：$(T, \boxplus)$ は群であるか確認せよ.

集合 T に別の演算を入れて群にしてみよう，といって出てきた演算の表なのだから群になっているに決まってるさ！ときちんと確認しなかった君 !! もしかして同じ注意は２回目ではないか？
本当に群になっているかを確かめるには，今までのように，(i) 結合法則は成り立ってるか (ii) 単位元はあるか (iii) どの元にも逆元はあるか，と順に調べていくのも一つの方法ではあるが，はっきりいって面倒である.

そこで**「同一視」**という数学の考え方を用いた方法を紹介する.「同一視」とは「一対一対応」ともいわれ，一見異なる２つの集合に対し，２つの集合の各元がそれぞれ過不足なく，かつ，重複することなく，互いに一対一の関係にあるとき，２つの集合を**同じもの**として扱おうという考え方である.
例えば，あるクラスの生徒の集合と出席番号の集合には一対一の関係があるので，２つの集合は同一視できる．出席番号 1 番の生徒といえば 1 人（仮に大久保君としよう）が決まるし，逆に大久保君といえば出席番号 1 番の生徒だと決まる.

話を戻す．集合 T の４つの元を次のように 0, 1, 2, 3 に一対一対応させる.

♠	♡	♣	♢
↕	↕	↕	↕
0	1	2	3

そして，演算 ⊞ に足し算 $+$ を対応させる．ただ新しい集合は $\{0, 1, 2, 3\}$ なので，普通の整数での足し算では演算にならない．そこで２つの元の和が T からはみ出す，つまり 4 以上に

なったときは 4 を引くという条件をつける．例えば，$2+3$ は $2+3=5$ で 4 以上なので $5-4$ として，

$$2+3=1$$

とする．集合 $\{0, 1, 2, 3\}$ に上の意味での演算 $+$ を入れた演算表を書いてみると，

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

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

となる．集合 $T=\{\spadesuit, \heartsuit, \clubsuit, \diamondsuit\}$ の演算 $\boxplus$ の演算表と比べてどうだろうか？

$\boxplus$	$\spadesuit$	$\heartsuit$	$\clubsuit$	$\diamondsuit$
$\spadesuit$	$\spadesuit$	$\heartsuit$	$\clubsuit$	$\diamondsuit$
$\heartsuit$	$\heartsuit$	$\clubsuit$	$\diamondsuit$	$\spadesuit$
$\clubsuit$	$\clubsuit$	$\diamondsuit$	$\spadesuit$	$\heartsuit$
$\diamondsuit$	$\diamondsuit$	$\spadesuit$	$\heartsuit$	$\clubsuit$

$\spadesuit \leftrightarrow 0$
$\heartsuit \leftrightarrow 1$
$\clubsuit \leftrightarrow 2$
$\diamondsuit \leftrightarrow 3$

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

ちゃんと対応していることがわかる．

なお，この集合 $\{0, 1, 2, 3\}$ は演算 $+$ について群になっていることは，集合の元が数字なので，簡単に確認することができる．マークを数字に置き換えただけなのにこんなに見やすくなる「同一視」の効果を実感できただろうか．

なお，この $\{0, 1, 2, 3\}$ にこのような和 $+$ をいれた集合は，整数全体の集合 $\mathbb{Z}$ を 4 で割った余りで分類した集合で，mod4 の集合という．

以上が可換群の例である．次に非可換群の例をあげる．

ガロア理論で重要な役割をなす群として**対称群**がある．これは非可換群であるが，詳細は明日の講義をお楽しみに !!

非可換群の別の例として，図形の合同をあげることができる[7]．

[7]この例も「こういうのも数学（前編）」の一部を抜粋し表現等を修正したものである

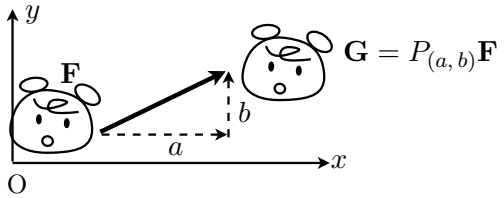
２つの平面図形 $\mathbf{F}$ と $\mathbf{G}$ が合同であるとは，一方の図形をその形を変えずに，位置や向きを変えることで，他方の図形にぴったり重ねることができることをいった．

さて，図形の合同と群とはどのように結びつくのだろうか？ポイントは，合同の定義で「位置や向きを変える」のところである．図形の「位置や向きを変える」という「操作」（これを合同変換という）の一つ一つを元に持つ集合を考えると，その集合が群になる．以下これを詳しく見ていく．

合同変換は，次の３つの移動の組合せで表現できる．

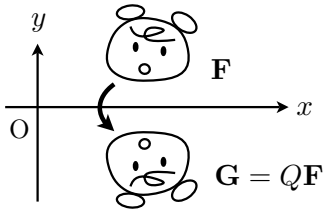
平行移動： 下の図のように図形の向きを変えない移動．

x 軸方向に a，y 軸方向に b の平行移動を $\boldsymbol{P_{(a,\,b)}}$ で表すことにする．



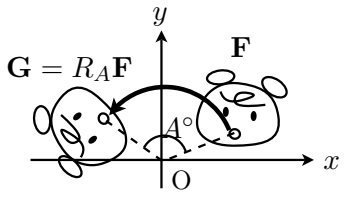
対称移動： あたかも x 軸上にある鏡に映したような移動．

対称移動を $\boldsymbol{Q}$ で表すことにする．



回転移動： 原点を中心にして左回り（反時計回り）に図形を回す移動．

角 $A°$ の回転移動を $\boldsymbol{R_A}$ で表すことにする．



ただし，右回りに角 A° の回転は左回りを基準にするので左回りに $-A^\circ$ と考える．したがって R_{-A} のようになる．

式の書き方は，例えば，図形 **F** を平行移動 $P_{(a,\,b)}$ で移動した図形を **G** とするとき，$\mathbf{G} = P_{(a,\,b)}\mathbf{F}$ のように，元の図形 **F** の左側に移動を表す記号 $P_{(a,\,b)}$ を書くことにする．続けていくつもの移動をする合同変換を考えるとき，例えば，平行移動 $P_{(a,\,b)}$ して，回転移動 R_A して，また平行移動 $P_{(c,\,d)}$ して最後に対称移動 Q する，ようなときは，丁寧に書けば，

$$\mathbf{G} = Q(P_{(c,\,d)}(R_A(P_{(a,\,b)}\mathbf{F})))$$

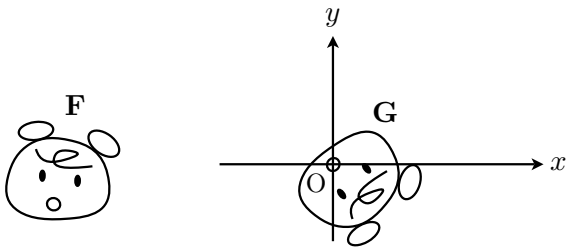
のようになるが，( ) が何重にもなって見づらいので単に，

$$\mathbf{G} = QP_{(c,\,d)}R_AP_{(a,\,b)}\mathbf{F}$$

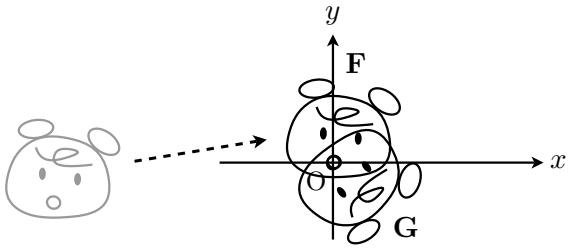
と書く．このとき，**F** から見て**左側に順に付け加えるよう**に書いていることに注意せよ．

実際に一つやってみよう．

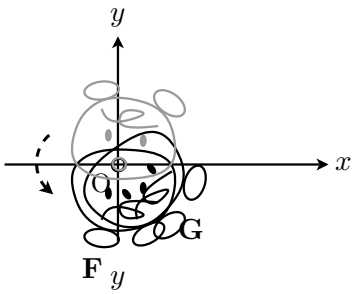
図の２匹のクマ **F** と **G** は合同であるがどのような合同変換によって移りあうのか．



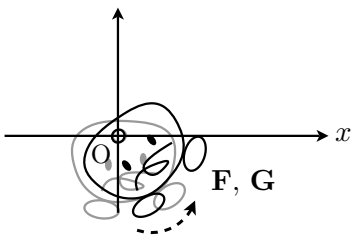
一方のクマ（ここでは **G** の方とする）のわかりやすいところ（今回は口にする）を基準にして座標をとる．



まず，他方のクマ（ここでは **F**）を大雑把に移動する．クマ **F** の口が座標の原点に来るように平行移動 $P_{(a,\,b)}$ をする．



よく見ると2匹のクマの眉毛の巻き方の向きが逆である．そのときは x 軸での対称移動 Q をする．



最後に顔の向きを合わせるために，原点 O を中心とする回転移動 R_A をする．

これより，クマ **F** をクマ **G** に移動するには，

$$G = R_A Q P_{(a,\,b)} F$$

とすれば良いことがわかった．なお，この移動の仕方は一例で，別の移動の仕方もあるので色々考えてみよ．

さて，いよいよ群になる集合を定義する．合同変換はこれら 3 種類の移動を組み合わせれば表現できるので，次のような集合

$$\mathcal{C} = \{L \mid L \text{ は}, P_{(a,\,b)},\, Q,\, R_A \text{ のいくつかの組合せ }\}$$

を考える．これより，2つの図形 **F** と **G** が合同であるとは，$L \in \mathcal{C}$ を用いて $\mathbf{G} = L\mathbf{F}$ を表せることだと定義し直すこともできる．

次に演算であるが，合同変換 $L,\, M \in \mathcal{C}$ において．図形 **F** に対し，$ML\mathbf{F}$ と続けて合同変換を行うと，この図形 $ML\mathbf{F}$ も **F** と合同なので，ML も一つの合同変換を表す．このように「続けて行う」ことを演算と考える．

結合法則を確かめてみよう．$L,\, M,\, N \in \mathcal{C}$ とする．まず，図形 **F** に対し $(ML)\mathbf{F}$ とはどのようなことなのかを確認しておこう．確かに $ML \in \mathcal{C}$ なので，別の元 $T \in \mathcal{C}$ を用いて $T = ML$ と表せるので，$(ML)\mathbf{F}$ を図形 **F** を一つの合同変換 T で移動した図形 $T\mathbf{F}$ と捉えることができる．しかし一方では，やはり $T = ML$ なので図形 **F** に合同変換 L をして続けて合同変換 M をしたことと同じである．そもそも「続けて行う」ことを演算としているので当然のことである．このことを踏まえると，

$$N(ML)\mathbf{F} = N((ML)\mathbf{F}) = N(M(L\mathbf{F})) = (NM)(L\mathbf{F}) = (NM)L\mathbf{F}$$

となる．この式変形において図形 $\mathbf{F}$ には特別な条件を付けてはいないのでどんな図形でも成り立つ．つまり集合 $\mathcal{C}$ の元として，結合法則：

$$N(ML) = (NM)L$$

が成り立つことがわかった．

単位元は，まったく移動しないという移動であるので，$P_{(0,\,0)}$ あるいは R_{0° で表現できる．単位元の存在が確かめられたので，単位元を $\boldsymbol{I}$ で表すことにする．

逆元について．まず個々の移動については，$P_{(a,\,b)}$ の逆元は $P_{(-a,\,-b)}$，Q の逆元は Q そのもの，R_A の逆元は R_{-A} となる．これより，例えば，合同変換 $L \in \mathcal{C}$ が，

$$L = QP_{(c,\,d)}R_AP_{(a,\,b)}$$

であったとすると，最後から逆にたどっていけば良いので，L の逆元を M とすると，

$$M = P_{(-a,\,-b)}R_{-A}P_{(-c,\,-d)}Q$$

となる．実際に確かめると，

$$\begin{aligned}
ML &= (P_{(-a,\,-b)}R_{-A}P_{(-c,\,-d)}Q)(QP_{(c,\,d)}R_AP_{(a,\,b)}) \\
&= P_{(-a,\,-b)}R_{-A}P_{(-c,\,-d)}(QQ)P_{(c,\,d)}R_AP_{(a,\,b)} \\
&= P_{(-a,\,-b)}R_{-A}P_{(-c,\,-d)}IP_{(c,\,d)}R_AP_{(a,\,b)} \\
&= P_{(-a,\,-b)}R_{-A}(P_{(-c,\,-d)}P_{(c,\,d)})R_AP_{(a,\,b)} \\
&= P_{(-a,\,-b)}R_{-A}IR_AP_{(a,\,b)} \\
&= P_{(-a,\,-b)}(R_{-A}R_A)P_{(a,\,b)} \\
&= P_{(-a,\,-b)}IP_{(a,\,b)} \\
&= P_{(-a,\,-b)}P_{(a,\,b)} \\
&= I
\end{aligned}$$

となるので，確かめられた．なお，上の計算で結合法則を用いている事に気が付いただろうか．群の定義に結合法則が必要な理由も理解できると思う．

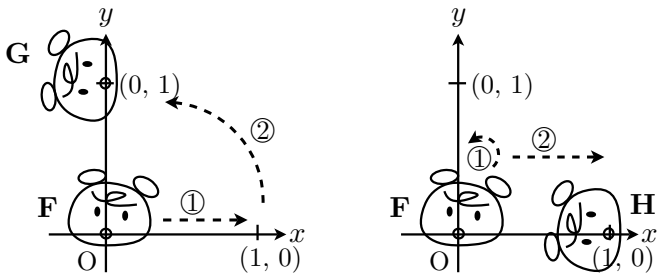
また，この合同変換群には交換法則が成り立たない．反例として，例えば，$R_{90^\circ}P_{(1,\,0)}$ と $P_{(1,\,0)}R_{90^\circ}$ を考えてみる．下の図でクマ $\mathbf{F}$ の口を基準する．クマ $\mathbf{G}$ を

$$\mathbf{G} = R_{90^\circ}P_{(1,\,0)}\mathbf{F}\,,$$

つまり① x 軸方向に 1，y 軸方向に 0 の平行移動をして ② 原点を中心に 90° 回転したクマとする．一方，クマ $\mathbf{H}$ を

$$\mathbf{H} = P_{(1,\,0)} R_{90^\circ} \mathbf{F}$$

つまり① 原点を中心に 90° 回転して ② x 軸方向に 1，y 軸方向に 0 の平行移動をしたクマとする．

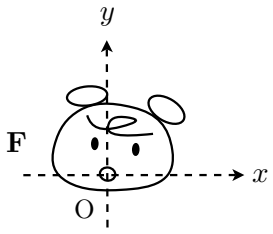


クマ $\mathbf{G}$ とクマ $\mathbf{H}$ は位置が異なるから $\mathbf{G} \neq \mathbf{H}$ である．これより少なくともクマ $\mathbf{F}$ については，

$$R_{90^\circ} P_{(1,\,0)} \neq P_{(1,\,0)} R_{90^\circ}$$

がいえたので，一般に交換法則は成り立たないことが証明された．

問い：口のところに原点があり左を向いているクマ $\mathbf{F}$ を次の合同変換で移動するとどうなるか答えよ．また，この合同変換をできるだけ簡潔に書き直せ．



$$P_{(0,\,-1)} R_{-90^\circ} Q P_{(-1,\,-1)} Q R_{90^\circ} P_{(1,\,0)} \mathbf{F}$$

3.3 環

集合 R 上に和とよばれる演算 $+$ と積とよばれる演算 $\times$ の 2 つの演算が入っており，次の 3 つの条件をみたすとき，$(\boldsymbol{R}, +, \times)$，あるいは単に集合 $\boldsymbol{R}$ を**環**という．

(i) 和 $+$ に関して可換群である．

(ii) 積 $\times$ に関しては，結合法則が成り立ち，単位元が存在する

(iii) R の元 a, b, c において，$a \times (b+c) = a \times b + a \times c$，$(a+b) \times c = a \times c + b \times c$ が成り立つ．これを**分配法則**という．

普通，和 $+$ に関する単位元を 0 で表し，積 $\times$ に関する単位元を 1 で表す．

環 $(R, +, \times)$ がさらに積に関して交換法則が成り立つとき**可換環**といい，交換法則が成り立たないことを強調するとき**非可換環**というのは群のときと同じである．

問い：$(\mathbb{Z}, +, \times)$ は可換環になることを確認せよ．

整式（単項式と多項式）全体の集合を P とおくと，$(P, +, \times)$ は可換環になる．「環」という整数とよく似た性質があるので「整式」という名称が付いている．2 つの整式の共通因数を求めるには整数と同様にユークリッドの互除法が使えるのもよく似ている性質である．

3.4 体

集合 K 上に和とよばれる演算 $+$ と積とよばれる演算 $\times$ の 2 つの演算が入っており，次の 2 つの条件をみたすとき，$(\boldsymbol{K}, +, \times)$，あるいは単に集合 $\boldsymbol{K}$ を**体**という．

(i) $(K, +, \times)$ は可換環である．

(ii) 積 $\times$ に関しては，和の単位元 0 を除く元に対し逆元が存在する．

つまり，四則演算が自由にできる数全体の集合（ただし 0 を除く）のことを体という．

問い：$(\mathbb{Q}, +, \times)$ は体になることを確認せよ．

$(\mathbb{Q}^{\times}, \times)$ が可換群になるので，$(\mathbb{Q}, +, \times)$ が体になることがわかる．
有理数全体の集合は，整数全体の集合を体になるように拡張したものだといえる．

問い：$(\mathbb{R}, +, \times)$，$(\mathbb{C}, +, \times)$ も体になることを確認せよ．