# 群論演習 と J （その3）

Yahoo 知恵袋 の 問答から

中野 嘉弘（札幌市、86 歳）

## 1． 合同式を解け

1)これが群論かどうかは怪しいが、その積もりの質問があったので、
解いて見た。(H21.6.20)

問 次の合同式を解け。

1)3X ≡ 5 (mod 10)
(解 by J) (1+i.10) #〜 5 = 10 | 3*(1+i.10)
答 5

(by 知恵 1) try X=5, 15 ≡5 (mod 10)
OK! X ≡ 5 (答)

2) 5X + 2 ≡ 6 (mod 7)
(解 by J) (1+i.7) #〜 4 = 7 | 5*(1+i.7)
答 5

(by 知恵 2) 5X ≡ 4 (mod 7)
両辺を 3 倍し 15X ≡ 12 (mod 7) ･･･(1),
さて 5･3 = 1 (mod 7) より
(1) 式は 15X = 1X ≡ 12 (mod 7) ･･･(2)
故に、 X ≡ 5 (mod 7) (答)
● どうも、技巧的ですね！

3) 6X - 4 ≡ 10 (mod 17)
(解 by J) (1+i.17) #〜 14 = 17 | 6*(1+i.17)
答 8

(by 知恵 3) 6X ≡ 14 (mod 17) ･･･(1),
0X ≡ 0 (mod 17) -> ≡ 17 (mod 17) ･･･(2)
(2)-(1) -> 6X ≡ - 3 (mod 17)
上式に掛ける x 3 -> 18X ≡ -9
また 17X ≡ 0 (mod 17)
上下の式減算 X ≡ - 9 ≡ 17 - 9 = 8 (mod 17)(答)

● やっぱり、技巧的だ。
J 言語の解の方が、すっきり、していますね！

では、以下の問題はどうか？
4) 10X ≡ 8 (mod 22) を解け。
(解 by 知恵 4) この解の一つは 10X - 8 = 22 の解である。
最大公約数 2 で割り、5X - 4 = 11 の解でもあるので

X = 3 。
合同方程式としては、両辺が (mod 11) で割り切れる。
それで 11*n (n は整数) を加減しても良い。
一般解は X = 3 + 11*n 。

(解 by J) (1+i.11) #〜 4 = 11| 5*(1+i.11)
(答) 3

5) 5X ≡ 20 (mod 15) を解け。
(解 by 知恵 5) 解の一つは 5X - 20 = 15 から、5 で割って
X - 4 = 3 の解であるから、 X = 7。
直前の式は、合同方程式として、両辺とも (mod 3) で割り切れる。
従って、解の一つは、さらに簡単な X = 1 である。
即ち、一般解は X = 1 + 3*n (n は整数) である。

(解 by J) (1+i.15) #~ 20 = 15| 5*(1+i.15) にしろ、
(1+i.3) #~ 7 = 3| 1*(1+i.3) にしろ、
解は見つからない。(当然である)。
15 (または 3)で割った剰余が 20 (または 7) になる訳が無い！
J 言語の、この流儀では解けない。問題が不見識か？
本来は 5X ≡ 5 (mod 15)
または X ≡ 1 (mod 3) ならば良かったのかな？

## 2. 互換 の 積

Q1) 知恵袋 2009/4/27 fragrance さん「互換の積について」
質問例として: 4 次の巡回置換は
(1234)=(1 2)-> (2 3)-> (3 4) -> (4 1) だと思うが
互換の積 (13)(12) は、どう云う事か？

A1) 知恵袋 2009/4/27 、回答者 grothendieck さん
「置換の順序を、前から後へか？ または、後ろから前へか？、
どちらで定義しているかで違います。 大抵は、後ろから前へ
となっているようです。 しかし、反対向きもあります。」

今は「後ろから前へ」の場合を解説します。
後の (12) で、1 -> 2, 2 -> 1, 残りは不変で 3->3, 4->4。
次の (13) で、1 -> 2 -> 2, 2 -> 1 -> 3,
3 -> 3 -> 1, 4 -> 4 -> 4。

結局、 1 -> 2, 2 -> 3, 3 -> 1, 4 -> 4。
即ち、 1 2 3 4
2 3 1 4 となる。

A2) 同じ事を、最初から J 言語でやろう。nakano さんの回答。
0 原点を意識しながら、
(1 2 0 3) { (1 2 3 4) -> 2 3 1 4 である。
巧く行った！ しかし、これは
(2 3 1 4) - 1 -> (1 2 0 3) であるから、
結果を知って、演算したに過ぎない。

J の演算法:　(2 1) ((1 2) -1) } v = 1 2 3 4　から
　　2 1 3 4、
　　(3 1) ((2 3)-1) } v1=. 2 1 3 4　から
　　2 3 1 4　(結果)。
しかし、この類の計算を一々手でやるのは、しんどいな。

A3) J 言語の関数　tran　( script は末尾)

　　v =. 1 2 3 4
(1 2) tran　v　->　2 1 3 4
さらに (1 3) tran　2 1 3 4 ->　2 3 1 4

　これを逆順にやれば、
　(1 3) tran　v ->　3 2 1 4
さらに　(1 2) tran　3 2 1 4 ->　3 1 2 4

　これが、互換の積の順序の効果である。 いずれにしても、
数字 4 は、不変である。

## 3.　置換 から 互換 へ

A4) J言語:置換から互換へ　関数 simperm (末尾)

```
(1 2 3 4) simperm (2 1 3 4) -> (1 2)
(1 2 3 4) simperm (3 2 1 4)  -> (1 3)
(3 2 1 4) simperm (3 1 2 4)  -> (2 1)
(1 2 3 4) simperm (3 1 2 4)  -> (1 2 3) -> (1 2)(1 3)
(1 2 3 4 5) simperm (3 1 2 4 5) -> (1 2 3)
```

この最後の 2 式では、前例によれば、互換の積の順序の検討が別途、
必要らしいな。

● 例題的質問:H21.6.21(Sun)
Q) 知恵袋 2009/6/4 umikua さん
「線形代数です。 置換の積の計算を！
　(1342)(13524)(132)

A1) kurekure さん

　置換が3つ出てきますが前から ABC とすると計算は CBA の順番にします。
まず、1がどこに移るか考えます。
C より1は3に移ります。
B より3は5に移ります。
A より5は不変ですから5に移ります。
よって最終的に1から5に移りました。

　同じようにすると、
2は1に移り、1は3に移り、3は4に移る。
よって最終的に 2 から 4 に移りました。

3は2に移り、2は4に移り、4は2に移る。
よって最終的に 3 から 2 に移りました。

4は4に移り、4は1に移り、1は3に移る。
よって最終的に 4 から 3 に移りました。

5は5に移り、5は2に移り、2は1に移る。
よって最終的に 5 から 1 に移りました。

よって答えは、
１２３４５
５４２３１
となります。
一々、言葉で云わなきゃならぬのか！？

A2) nakano さん
◆ 演算順序によっては、答は異なり、
5 2 3 4 1 ではないか？

A3) nakano さん
演算順序の問題は、
● 行列 Matrix 計算を経由した方が判り易い。
置換 ( 1 3 2 ) の行列表現 A は、数ベクトル
(1 2 3 4 5) -> (3 1 2 4 5) の変換と同じ故、
```
0 0 1 0 0
1 0 0 0 0
0 1 0 0 0
0 0 0 1 0
0 0 0 0 1
```
である。
次に、( 1 3 5 2 4 ) の行列表現 B は、数ベクトル
(1 2 3 4 5) -> (3 4 5 1 2) の変換と同じ故、
```
0 0 1 0 0
0 0 0 1 0
0 0 0 0 1
1 0 0 0 0
0 1 0 0 0
```
である。
最後に、( 1 3 4 2 ) の行列表現 C は、数ベクトル
(1 2 3 4 5) -> (3 1 4 2 5 ) の変換と同じ故、
```
0 0 1 0 0
1 0 0 0 0
0 0 0 1 0
0 1 0 0 0
0 0 0 0 1
```
である。
数ベクトル v = 1 2 3 4 5 に対して、
行列演算 A･v -> 3 1 2 4 5。
次に B･(A･v) -> 2 4 5 3 1。
最後に C･(B･(A･v)) -> 5 2 3 4 1。
即ち、v = 1 2 3 4 5 に対して、
D･v --> 5 2 3 4 1 と変換する行列 D が解である。
それは、行列の積 C･(B･(A)) であるので、パソコン
乃至、筆算をすれば良い。もっとも、直接的にも殆ど
自明であって、答は
```
0 0 0 0 1
0 1 0 0 0
```

```
0 0 1 0 0
0 0 0 1 0
1 0 0 0 0
```
である。
今の最終結果は (1 5 )(2)(3)(4)
即ち (1 5) となる。
この様に、演算すれば、置換の積の順序如何などの
心配は軽くなろうか？
・・・・・・・・・・・・・・・・・・・・・・・・・

◆ 次に、逆順に演算して見よう。
即ち、数ベクトル v = 1 2 3 4 5
に対し、最初に左端の変換をして、
C･v -> 3 1 4 2 5。
次に、B･(C･v) ->4 2 5 3 1。
最後に右端の変換で、
A･(B･(C･v)) -> 5 4 2 3 1。
これは、前述の結果と違い、別な回答者
k さんの結果と合うようだ。さらに
(1 5)(2 3 4) なる2 ケの置換の積に
まとめられる。
何だか？妙だな？
どちらを正解としようか？

（しかし、行列演算可能なパソコンや高級電卓が手元に
あれば、大変便利であろう。原理は、この回答が判り
易い筈ですね。説明が丁寧過ぎたかな？
ま、答が判ってから、理由付けするのは簡単ですが？）

## 4. 中野 関数 の Scripts

```
tran=: 3 : 0
 :
 v=.y
 x0=. 0 { x
 x1=. 1 { x
 v1=. v i. x1
 va=. (_1*x0) v1 } v
 v0=. va i. x0
  |vb=.(x1) v0 }va
)

simperm =: 3 : 0
 :
NB.  (1 2 3 4) simperm (1 4 3 2) -> (2 4)
n=. # x
 (-.(((x - y) =0))) # x
)
```