教職課程のための群論の授業の構想

宮崎大学教育文化学部紀要　創立 130 周年記念特別号

教職課程のための群論の授業の構想

谷本　洋

A Design of the Lecture on Group Theory for the Teaching Course

Hiroshi TANIMOTO

１．はじめに

教職課程のための群論の授業を約 30 年間行って来ている。その間，群論の理解が難しいようだという話を他の大学教員から何度か耳にした。私は「抽象代数学Ⅰ」という授業で群論を教えているが，私の授業も例外ではなく，群の定義を覚えること・群であることを示すこと等はできて点数は取れても，学んだことのイメージをどうも掴みにくいようで，記憶になかなか残らず，腑に落ちた理解が難しいようだ。この状況を克服したいと思い，群論の新しい授業を以下のように構想した。これは，その記録である。

２．現状分析による新たな構想

現状を見て，多くの学生に，新しいものになかなか慣れて行けないという面があるように思われる。しかし，例えば高校数学で微分・積分という新しいものを学生達は学んで来ている。この学んで来ることができている理由として，興味ある題材であることもあるかも知れないが，他の理由として，大学入試という強い動機付けがあったこともあるのではないだろうか？そうだとすれば，高校までの授業で群を扱うことはこれから先も多分ないのではないかと思われるので，群を学ぶ際に，「大学入試による強い動機付け」に頼ることはできないのではないか？また，群論は抽象的な色合いを感じさせることにもよるのかも知れない。そこで，「腑に落ちた理解が難しい」原因がこの動機付けと抽象性にあると仮説を立て，それに対して，群を学ぶことに対する動機付けと抽象性に対する配慮をどのようにすれば良いかを次のように考えた。

(a) 新しいものから出発してそれについて考えるというのではなく，なるべく学んだものの中から数学に関する身近で具体的な問題を見出せば，考えようという気持ちが湧くのではないだろうか？そして，一般の抽象的な群の立場からその問題を見るのではなく，今までに学んだものから少し背伸びして得られる具体的な群の立場から考察し，群を活用して問題を解決することで，学生達は学ぼうとし，印象にも残せるのではないだろうか？

(b) 新しい概念・記号等の導入はなるべく少なくし，既習事項を大切にすれば良いのではないだろうか？ただし，背景としての一般の群論については該当する場面で無理のない形で触れることとする。

次に，(a)の「学んだもの」の中から題材となる「問題」を選び出すために，これまでに学んで来た内容を振り返ってみた。

宮崎大学教育文化学部数学科において，「抽象代数学Ⅰ」は中学校教育コース数学専攻の必修科目であり，2 年後期に開講されている。(初等教育コースの学生の一部も受けているが，以下，中学校教育コース数学専攻を中心に述べる。) 2 年前期までに代数学において次の授業を学生達は受けて来ている。

1 年前期「初等代数学Ⅰ」(必修科目)

初等整数論の入門的内容を扱い，その内容は，整数の約数・倍数・素数・ユークリッドの互除法・素因数分解の定理等である。

1 年後期「初等代数学Ⅱ」(必修科目)

「初等代数学Ⅰ」に引き続いて，整数の合同式の入門的内容を扱い，その内容は，連立 1 次合同式・オイラーの定理等である。

2 年前期「線型代数学Ⅰ」(選択科目)

内容は行列・行列式である。

以上のことから，これまでに学んで来た流れを続けて行くことを方針とし，題材となる「問題」として次の 2 つを選んだ。

① 「初等代数学Ⅱ」の内容から連立 1 次合同式についての定理を取り上げる。「互いに素」という条件は本当に必要か，という点を問題とする。

② 「初等代数学Ⅱ」の内容からオイラーの定理を取り上げる。正則行列から成るアーベル群でない有限群の場合にもこの定理が成立するか，という点を問題とする。

考え易さという点から，流れは，アーベル群からアーベル群ではない群へとし，① → ② とする。

なお，この試みを始めて，小さな改良を加えながら 6 年になる。その経験による感想も「注意」としていくつか述べる。

3．問題①

(1) 剰余類群 $\mathbb{Z}_n$

剰余類群に関する記号として，$\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ が[3]では使われており，また，$\mathbb{Z}/n\mathbb{Z}$ が使われることもある。ここでは，

1) 書き易さから，剰余類群の記号は $\mathbb{Z}_n$ を，

2) $\mathbb{Z}$ の元との区別と扱い易さのために，$\mathbb{Z}_n$ の元を表す記号は $\overline{0}, \overline{1}, \dots, \overline{n-1}$ を

使うこととした。また，(b)の意味から，一般的な剰余類群の定義と剰余類群の大切さにはあまり触れないこととし，触れても剰余類群という名前のみとすることにした。

自然数 n と整数 x, y について，

$\mathbb{Z}_n$ において $\overline{x} = \overline{y} \iff x \equiv y \pmod{n}$

が剰余類の相等と合同式を関係づける性質である。

なお，$\mathbb{Z}_n$ における積は問題②で扱うが，積を定義していない段階で $n\overline{x}$ を $\overline{n} \cdot \overline{x}$ と書いてしまう場合があることも考慮して，初めに和と積を定義する。

注意　剰余類群に関する記号に慣れるために，単なる計算問題だけではなく，少し工夫を要する，例えば次のような練習問題を出すと，学生達は結構考えようとする。

練習問題　$\mathbb{Z}_n$ における和 $S=\overline{1}\cdot\overline{2}+\overline{2}\cdot\overline{3}+\cdots+\overline{n-2}\cdot\overline{n-1}$ を，多くても 1 つ n を使って表せ。

(2)　問題①の設定

「初等代数学Ⅱ」で学んだよく知られた次の定理 A について，条件「互いに素」を外すとどのようになるか，という問題を設定する。

定理 A　互いに素な自然数 $m_1,m_2,\ldots,m_k$ と任意の整数 $a_1,a_2,\ldots,a_k$ について，$M=m_1m_2\ldots m_k$ とおけば，次の連立 1 次合同式

$$\begin{cases} x\equiv a_1 \pmod{m_1} \\ x\equiv a_2 \pmod{m_2} \\ \quad\vdots \\ x\equiv a_k \pmod{m_k} \end{cases}$$

は $mod\ M$ で唯 1 つの解を持つ。

(3)　問題①の解決

問題①を考えるために基本となるのは，剰余類群の言葉で定理 A を書き直した良く知られた次の定理である。

定理 B　定理 A の下で，次の写像は同型写像になる。

$$f:\mathbb{Z}_M\longrightarrow\mathbb{Z}_{m_1}\times\mathbb{Z}_{m_2}\times\cdots\times\mathbb{Z}_{m_k},\quad f(\overline{x})=(\overline{x},\overline{x},\ldots,\overline{x})$$

この定理を示したのち，これを一般化した次の定理を示す。

定理 C　自然数 $m_1,m_2,\ldots,m_k$ について，$L=LCM(m_1,m_2,\ldots,m_k)$ とおけば，次の写像は単射準同型写像になる。

$$f:\mathbb{Z}_L\longrightarrow\mathbb{Z}_{m_1}\times\mathbb{Z}_{m_2}\times\cdots\times\mathbb{Z}_{m_k},\quad f(\overline{x})=(\overline{x},\overline{x},\ldots,\overline{x})$$

これにより，例えば次の定理が示される。

定理 D　自然数 $m_1,m_2,\ldots,m_k$ に対し，任意の整数 $a_1,a_2,\ldots,a_k$ について，連立 1 次方程式

$$\begin{cases} \mathbb{Z}_{m_1}\text{ において}\quad \overline{x}=\overline{a_1} \\ \mathbb{Z}_{m_2}\text{ において}\quad \overline{x}=\overline{a_2} \\ \quad\vdots \\ \mathbb{Z}_{m_k}\text{ において}\quad \overline{x}=\overline{a_k} \end{cases}$$

が解を持つための必要十分条件は，$m_1,m_2,\ldots,m_k$ が互いに素であることである。

さらに，与えられた連立 1 次方程式が解を持つための条件が示される。

定理 E　自然数 $m_1,m_2,\ldots,m_k$ と整数 $a_1,a_2,\ldots,a_k$ について，任意の i,j に対し $M_{i,j}=GCD(m_i,m_j)$ とおけば，次の連立 1 次方程式

$$\begin{cases} \mathbb{Z}_{m_1} \text{ において} & \overline{x} = \overline{a_1} \\ \mathbb{Z}_{m_2} \text{ において} & \overline{x} = \overline{a_2} \\ \quad\vdots & \\ \mathbb{Z}_{m_k} \text{ において} & \overline{x} = \overline{a_k} \end{cases}$$

が解を持つための必要十分条件は，任意の i, j に対し $\mathbb{Z}_{M_{i,j}}$ において　$\overline{a_i} = \overline{a_j}$ が成り立つことである。しかもこのとき，$L = LCM(m_1, m_2, \ldots, m_k)$ とおけば，これは $mod\ L$ で唯 1 つの解を持つ。

定理 E について，[2]では，これと同じ問題が連立 1 次合同式の問題として扱われている。そこでは帰納的な方法が使われている。ここでは，この方法は採らず，[2]で紹介されているガウスの方法を使って直接に示される。([4]を参照)

注意　ガウスの方法を使って直接に示されるため，次のような練習問題も解き易くなる。ただし，答えを出すための本質的ではない最終的な数値計算はする必要はないとする。

練習問題　自然数 $3^2 4, 4^2 5, 5^2 3$ について，整数 a_1, a_2, a_3 が次の各値を取るとき，連立 1 次方程式

$$\begin{cases} \mathbb{Z}_{3^2 4} \text{ において} & \overline{x} = \overline{a_1} \\ \mathbb{Z}_{4^2 5} \text{ において} & \overline{x} = \overline{a_2} \\ \mathbb{Z}_{5^2 3} \text{ において} & \overline{x} = \overline{a_3} \end{cases}$$

が解を持つかどうかを判定し，解を持つ場合は，$mod\ 3^2 4^2 5^2$ においてその解を求めよ。

1)　$a_1 = 3, a_2 = 11, a_3 = 26$

2)　$a_1 = 31, a_2 = 19, a_3 = 34$

(4)　<u>問題 ① の付録</u>

位数が等しい 2 つの有限群 G, H の乗積表が「そっくり」となる条件を，同型写像を用いて述べることができる。これは[1]で，「まったく同じ」という言葉を用いて 2 行で扱われている。この内容を 2 行で終わらせるのはもったいなく思われる。そこで，ここではまず，「まったく同じ」という言葉は使わず「そっくり」という言葉を定義し，群の元を並べ替えて 2 つの乗積表を「そっくり」にできるか，という問題を掲げる。その後，同型写像による特徴付けを行い，具体例を用いて丁寧に扱う。

注意　例えば，次のような一連の練習問題を出すと学生達の興味を結構引き，解こうとするようである。

練習問題　$\mathbb{Z}_6$ の元を $\overline{0}, \overline{1}, \overline{2}, \cdots$ と順に並べてそれについて作った乗積表と，$\mathbb{Z}_2 \times \mathbb{Z}_3$ の元を辞書式順序に並べてそれについて作った乗積表を作り，その 2 つは「そっくり」ではないことを確認せよ。そののち，$\mathbb{Z}_2 \times \mathbb{Z}_3$ の元を適当に並べ替えて 2 つの乗積表を「そっくり」にせよ。

この練習問題を解かせた上で，次の練習問題を出す。

練習問題　$\mathbb{Z}_8$ の元を $\overline{0}, \overline{1}, \overline{2}, \cdots$ と順に並べてそれについて作った乗積表と，$\mathbb{Z}_2 \times \mathbb{Z}_4$ の元を適当に並べて作った乗積表について，$\mathbb{Z}_2 \times \mathbb{Z}_4$ の元の並べ方は $8! = 40320$ 通りあるが，$\mathbb{Z}_2 \times \mathbb{Z}_4$ の元をどのように並べて作っ

た乗積表も $\mathbb{Z}_8$ のそれとは「そっくり」にならないことを示せ。

この練習問題の解き方の 1 つは，多くの学生達が苦手とする背理法を使うものであり，この意味からも適切かもしれない。

(5)　①で使われる概念・用語

剰余類，剰余類群，二項演算，群，アーベル群，加法群，乗法群，群の位数，有限群，無限群，群の直積，準同型写像，同型写像，同型，乗積表

4．問題②

(1)　既約剰余類から成る乗法群 $\mathbb{Z}_n^*$

自然数 n に対し，

$$\mathbb{Z}_n^* = \{\, \overline{a} \in \mathbb{Z}_n \mid (a,n) = 1 \,\}$$

とおき，既約剰余類から成る乗法群 $\mathbb{Z}_n^*$ を定義する。そして，$\mathbb{Z}_n^*$ は，位数が $\varphi(n)$ のアーベル群になることを示す。このとき，次の事柄にも注意しておく。

命題　$\mathbb{Z}_n^*$ の元 $\overline{a}$ について，$\overline{a}$ の任意の元 b に対し $(b,n) = 1$ となる。

このようなアーベル群の例を挙げる一方で，m 次正則行列全体の部分集合で行列の積に関して群となるアーベル群ではない有限群の例も挙げる。

(2)　問題②の設定

まず，「初等代数学Ⅱ」におけるオイラーの定理を有限群 $\mathbb{Z}_n^*$ の定理と見て，次のように言い表す。

定理 F　2 以上の自然数 n について，任意の $\overline{a} \in \mathbb{Z}_n^*$ に対し $\overline{a}^{|\mathbb{Z}_n^*|} = \overline{1}$ が成立する。

そして，定理 F について，有限群が

1)　いくつかの $\mathbb{Z}_n^*$ の直積である場合，

さらには，

2)　(1) で挙げた「アーベル群ではない有限群」である場合

にも成立するか，という問題を掲げる。

(3)　問題②の解決

肯定的な問題②の答えについて，1)の場合は，「初等代数学Ⅱ」におけるオイラーの定理と同様な方法で乗法群の言葉で証明し，2)の場合は，巡回群・ラグランジュの定理を利用して証明するという良く知られた方法を取る。

(4)　問題②の付録

まず，定理 B を利用してよく知られた次の定理を示す。

定理 G　自然数 $m_1, m_2, \ldots, m_k$ が互いに素であるとき，定理 B の写像 f を $\mathbb{Z}_M^*$ に制限することにより，次の群の同型写像 g を得る。

$$g : \mathbb{Z}_M^* \longrightarrow \mathbb{Z}_{m_1}^* \times \mathbb{Z}_{m_2}^* \times \cdots \times \mathbb{Z}_{m_k}^*, \quad g(\overline{x}) = (\overline{x}, \overline{x}, \ldots, \overline{x})$$

次に，これを一般化した次の定理を示す。

定理 H　自然数 $m_1, m_2, \ldots, m_k$ について $L = LCM(m_1, m_2, \ldots, m_k)$ とおけば，定理 C の写像 f を $\mathbb{Z}_L^*$ に制限することにより，次の群の単射準同型写像 g を得る。

$$g : \mathbb{Z}_L^* \longrightarrow \mathbb{Z}_{m_1}^* \times \mathbb{Z}_{m_2}^* \times \cdots \times \mathbb{Z}_{m_k}^*, \quad g(\overline{x}) = (\overline{x}, \overline{x}, \ldots, \overline{x})$$

これにより，例えば定理 D に比べ若干弱い形の次の定理が示される。

定理 I　定理 H の単射準同型写像 g が同型写像になる，すなわち $\varphi(L) = \varphi(m_1)\varphi(m_2)\cdots\varphi(m_k)$ となるための必要十分条件は，任意の異なる i, j に対し $GCD(m_i, m_j) \leqq 2$ が成立することである。

次に，例えば $\mathbb{Z}_8^*$ において，任意の元が巾乗して 1 となる最小の共通の巾乗数は 2 となり，$\varphi(8) = 4$ ではない。これにより，各 $\mathbb{Z}_n^*$，あるいは群の直積 $\mathbb{Z}_{m_1}^* \times \mathbb{Z}_{m_2}^* \times \cdots \times \mathbb{Z}_{m_k}^*$ において，このような最小の共通の巾乗数は何か，ということが問題になる。これについては，[1]において，素数 p と自然数 n に対して群 $\mathbb{Z}_{p^n}^*$ の構造が分かっている。よって，[1]における記述を $\mathbb{Z}_{p^n}^*$ の言葉で書き直したあとで，この構造と定理 G を用いてこの共通の巾乗数を特徴付けることができる。この数値は，手計算で実際に調べることができるので，適切な問題と思われる。

(5)　②で使われる，3(5)で挙げられたもの以外の概念・用語

巡回群，群の指数

5．構想を実施後の感想

以上の構想を実施してみた感想は，まず，進む速度が遅くなりがちなことである。問題①は終わるが，問題②に入るかどうかというあたりで授業は終わりとなる。それは，学生達の理解の度合いを測りながら進めていることによるのかも知れない。あるいは，「写像」と言うと緊張が走るような雰囲気もやや感じられ，その都度なるべく感覚的に分かるような説明をするよう配慮していることによるのかも知れない。しかし，一方で，何かが良い方向に動いているような印象もある。例えば，「なるほど，そういうことか。」とか「面白かった。」とか「今までに学んだことが全て関係している。」などという感想が聞かれることも少しある。これは今までになかった良いことである。そこで，今しばらく話す順序を変えたり，説明の仕方を変えたり，思い付いた題材を付け加えたり，練習問題を変えてみたりなどして，工夫を重ねて行ってみようと思う。

参考文献

[1]「群論」浅野啓三，永尾汎，岩波書店，1973

[2]「初等整数論講義」高木貞治，共立出版，1991

[3]「初等代数学」硲文夫，森北出版，1993

[4]「一般の連立 1 次合同式に関する 1 つの注意」谷本洋，宮崎大学教育文化学部紀要（130 周年特別号），2015