「応用代数 2021 第 5 講 − 群 (3): 群の構造の解析, 応用 − 」

講義日程: 6/24/2021 (月・木曜 7・8 講時), 教室: M1, M2
浅井信吉 (mail: nasai@u-aizu.ac.jp, ext: 2746, office: 303C)
URL: https://elms.u-aizu.ac.jp/

2021 年 6 月 27 日

5 群 (3): 群の構造の解析, 応用

5.1 有限群の基本性質

1. 任意の有限位数の群が存在する (同型を除き一通りの場合と、複数通りの場合もあり).

   例: $\mathbf{Z}_n \quad (n = 1, 2, \ldots) \Rightarrow |\mathbf{Z}_n| = n$

   群の性質を満す演算表が作成できる.

2. 有限群 G の部分群 H の位数 $|H|$ (要素の数) は G の位数 $|G|$ の約数である. (ラグランジュの定理を思い返せ)

3. 有限群 G の要素 a の位数 $\sharp(a)$ は群の位数 $|G| = n$ の約数である.

4. 群の位数 $|G| = n$ のとき, 任意の要素 $a \in G$ に対して $a^n = e$ を満たす. ⇐ 重要 (フェルマーの小定理は重要な応用)

5. 素数位数の群は巡回群に限られる. 単位元以外の要素は生成元である.

   $|G| = p$ が素数であれば $G = [a] \ (a \neq e)$

   演算表は一通りしかない.

例題 1 位数 5 の群 $G = \{a_0, a_1, a_2, a_3, a_4\}$ の単位元を求める方法を述べよ. 要素 a_i を並べ替えて $a_i = x^i$ とできる. これを用いて要素 $a_i \cdot a_j$ を計算する方法を述べ, 演算表を作成せよ.

解: 有限群の位数を n とすると任意の要素 $x \in G$ が $x^n = e$ (e: 単位元) を満す. 従って a_i^5 を計算すれば良い. $a_i = x^i$ とできるので $a_i \cdot a_j = x^i \cdot x^j = x^{i+j} = a_{i+j(\mathrm{mod.}\ 5)}$ で計算できる. 演算表は表 1 で与えられる.
有限群の性質を用いてフェルマーの小定理を示す.

表 1: $G = \{a_i\}$ の演算表

$\cdot$	a_0	a_1	a_2	a_3	a_4
a_0	a_0	a_1	a_2	a_3	a_4
a_1	a_1	a_2	a_3	a_4	a_0
a_2	a_2	a_3	a_4	a_0	a_1
a_3	a_3	a_4	a_0	a_1	a_2
a_4	a_4	a_0	a_1	a_2	a_3

定理 1 フェルマー (Fermat) の小定理
p を素数とする.

1. $x \not\equiv 0 \ (\mathrm{mod.}\ p)$ のとき, 等式 (1) が成り立つ.

$$x^{p-1} \equiv 1 \ (\mathrm{mod.}\ p) \tag{1}$$

2. 任意の x に対して等式 (2) が成り立つ.

$$x^p \equiv x \ (\mathrm{mod.}\ p) \tag{2}$$

証明: 定理の後半は前半から導かれるので前半を示す. $\mathbf{Z}_p^* = \{1, 2, \cdots, p-1\}$ は乗法に関して位数 $p-1$ の群になる. 群の位数が $p-1$ であるので有限群の基本性質 4 より任意の要素 $x \in \mathbf{Z}_p^*$ は $x^{p-1} = 1$ となる. これを剰余の関係式に置き換えれば良い. (証明完了)

フェルマーの小定理は大きな指数の剰余計算に有効である.

例題 2 $a = 123456789$ のとき $a^a (\mathrm{mod.}\ 101)$ を簡単にせよ.

解: $10^2 = 100 \equiv -1 (\mathrm{mod.}\ 101)$ であるので $a = 123456789 \equiv 1 - 23 + 45 - 67 + 89 \equiv 45 (\mathrm{mod.}\ 101)$ である. 101 は素数で $123456789 = 1234567 \times 100 + 89$ と変形しフェルマーの小定理 $a^{100} \equiv 1 (\mathrm{mod.}\ 101)$ を用いて

$$a^a = a^{1234567 \times 100 + 89} = (a^{100})^{1234567} \cdot a^{89}$$

$$\equiv a^{89} \equiv 45^{89} (\text{mod. } 101)$$

5.2 巡回群とその構造

与えられた群の内部構造を解析する手法として部分群の構造を調べる手法がある．部分群を構成する最も基本的な方法として巡回群 (巡回部分群) がある．算法を用いて一つの要素 a から次々と要素を作り出すと言うことである．

例題 3 $\mathbf{Z}_n$ の加法群は巡回群 $[1]$ であることを示せ．

解: $\mathbf{Z}_n = \{0, 1, 2, \cdots, n-1\}$ は $1, 2 = 1+1, 3 = 2+1, \cdots, n-1 = (n-2)+1, n = n \times 1 = 0$ のように 1 を加えることで全ての要素を生成できるので 1 を生成元とする巡回群 $[1]$ である．

注意 1 : 1 を n 回加えることで初めて 0 に一致するので 1 の位数は $\sharp(1) = n$ である．

例題 4 加法の巡回群 $\mathbf{Z}_n$ の生成元を求めよ．

解: 例題 3 で見たように 1 は $\mathbf{Z}_n$ の生成元である．一般に a が n と互いに素な自然数であるとき，$x \cdot n + y \cdot a = 1$ を満す $x, y \in \mathbf{Z}$ が存在する[1]．従って $y \cdot a = 1(\text{mod. } n), (\langle y \rangle \langle a \rangle = \langle 1 \rangle)$ を満すことになる．即ち，任意の m に対して $\langle m \cdot y \rangle \langle a \rangle = \langle m \rangle$ を満すようにできるので a は生成元である．従って n が素数のときは $1, 2, \cdots, n-1$ が生成元となる． $1, 2, \cdots, n$ の中で n と互いに素な数の個数 $\varphi(n)$ は **Euler** の関数とよばれる[2]．

性質 1 巡回群の部分群は巡回群である．

証明: G を巡回群とする．$G = \{a^n | n \in \mathbf{Z}\}$ と書ける．G の任意の部分群 H の要素は全て a^n と書ける．H には逆元が含まれるので $a^n \in H$ に対して $a^{-n} \in H$ となるので $a^n \in H$ の指数 n は正の値を持つものがある．正の指数 n 全体には必ず最小値 n_0 が存在する．このとき，$H = \{a^{kn_0} | k \in \mathbf{Z}\}$ と書けることを示す．もし $a^m \in H$ が a^{kn_0} と書けないとする．ここで $m > 0$ として良い． m を n_0 で割った余りを r とする．$m = kn_0 + r \ (0 \leq r < n_0)$． ここで $r \neq 0$ とすると $a^r = a^{m-kn_0} = a^m \cdot (a^{kn_0})^{-1}, a^m \in H, (a^{kn_0})^{-1} \in H$ であるので $a^r \in H$ であり，正の指数で n_0 未満となり矛盾である．従って $r = 0$ 即ち任意の H の要素は $(a^{n_0})^k$ と書けることになり，巡回群であることが示された． (証明完了)

[1] これは第６講のイデアルで説明する．
[2] ” 高木, 初等整数論講義, p.42, 共立出版”

例題 5 $\mathbf{Z}_{12}$ の部分群 $(\neq \{e\}, \mathbf{Z}_{12})$ を全て決定せよ．

解: ラグランジュの定理から部分群の位数は $\mathbf{Z}_{12}$ の位数 12 の約数なので $1, 2, 3, 4, 6, 12$ となる．$\mathbf{Z}_{12}$ が巡回群であるので性質 1 から全ての部分群は巡回群となり，その位数が $2, 3, 4, 6$ の巡回部分群は，各々 $\{0, 6\} = [6], \{0, 4, 8\} = [4]$, および $\{0, 3, 6, 9\} = [3], \{0, 2, 4, 6, 8, 10\} = [2]$ で与えられる．

性質 2 $(\mathbf{Z}_p^*, \times)$ は p が素数のとき，乗法群であり，巡回群である．

解: $(\mathbf{Z}_p^*, \times)$ が乗法に関して群になることは第２講 (2.4) で示した．原始根 (生成元) の存在定理[3] により $\mathbf{Z}_p^* = [a]$ となる自然数 a が存在する．従って $(\mathbf{Z}_p^*, \times)$ は巡回群である．

注意 2 : 例えば素数 $p = 101$ に対して $a, a^2, a^3, \cdots, a^{99}, a^{100} = 1(\text{mod. } 101)$ を満す a が存在することを意味している．

例題 6 以下の性質を示せ．(演習課題)
「巡回群 G の位数が n であれば $G \simeq \mathbf{Z}_n$ であり，位数が 0 (要素数が無限) であれば $G \simeq \mathbf{Z}$ である．」

例題 7 以下の性質を示せ．(演習課題)
「無限巡回群の任意の部分群 $(\neq \{0\})$ は無限巡回群である．」

5.3 位数 $1, 2, 3$ の有限群

5.3.1 $G_1 = \{e\}$

単位元からなる群．e の逆元は e．

5.3.2 $G_2 = \{e, a\}$

素数位数であるので G_2 は巡回群である． すなわち $a^2 = e$ を満す．演算表を表 2 に示す．

表 2: G_2 の演算表

$\cdot$	e	a
e	e	a
a	a	e

[3] ” 高木, 初等整数論講義, 共立出版, p.62”

表 2 は $\mathbf{Z}_2 = \{0, 1\}$ の加法，乗法の演算表 (第２講注意２) の加法の演算表 (表 3 左) と同型 ($f(e) = 0, f(a) = 1$) になる．$a^2 = e$ は加法群の $1 + 1 = 0$ に対応する．

表 3: $\mathbf{Z}_2 = \{0, 1\}$ の加法，乗法の演算表

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

5.3.3 $G_3 = \{e, a, b\}$

素数位数であるので G_3 は巡回群である．すなわち，$a^3 = b^3 = e$ を満す．演算表 (表 4) を完成せよ．

表 4: G_3 の演算表

$\cdot$	e	a	b
e	e	a	b
a	a		
b	b		

例題 8 第２講例題 12 で扱った剰余体

$$\mathbf{Z}_2[x]/(x^2 + x + 1) = \{0, 1, x, x + 1\}$$

の 0 を除く３つの要素 $1, x, x + 1$ は乗法に関して群になる．その演算表を作成せよ．この乗法群は巡回群で G_3 と同型となることを示せ．

解: 演算表は表 5 の通りである．要素数が 3 であるので巡回群となり，G_3 と同型となる．具体的に言えば，x を生成元とする位数 3 の巡回群であり，$x, x^2, x^3 = 1$ を満し，x は生成元である．従って同型写像の要素間の対応関係は例えば表 6 のようにすれば良い．

表 5: 剰余体 $\mathbf{Z}_2[x]/(x^2 + x + 1)$ の乗法群の演算表

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

表 6: 同型写像 f の対応関係の例

G_3 の要素		$\mathbf{Z}_2[x]/(x^2 + x + 1)$ の要素	
e	a^0	1	x^0
a	a^1	x	x^1
b	a^2	$x + 1$	x^2

5.4 位数 4 の群

４つの要素を持つ群は巡回群 $(\mathbf{Z}_4, +)$ と非巡回群 G_4 がある．これは第１講のタイヤ交換 G_{tire} とマットレス返し G_{bed} を例にして学んだ．第１講の黄金律を満す要素とは巡回群の生成元に対応する．マットレス返し G_{bed} は黄金律を満さなかったので巡回群ではなかった．巡回群ではない構造の群 $G_4 = \{e, a, b, c\}$ の構成法を考える．

例題 9 G_4 の要素 a, b, c の位数を求めよ．

解: 要素 a, b, c の位数はラグランジュの定理 (第３講 定理２) から導かれる性質６から群の位数の約数となる．すなわち $|G_4| = 4$ であるので $1, 2, 4$ となる．位数が 1 の要素は単位元に限られるので要素 a, b, c の位数は $2, 4$ となる．しかしながら 4 とすると G_4 は巡回群となってしまうので 4 もあり得ない．従って a, b, c の位数は 2 に限られる．位数が 2 であるとは $a^2 = a \cdot a = e$ であり， a 自身が a の逆元であることを意味する．b, c についても同様である．

例題 10 表 7 の演算表を作成せよ．

解: $a \cdot b$ などは何になるべきか？ (cf: $a \cdot a = e$) $a \cdot b = e, a, b, c$ の可能な取り得る値は何か？

表 7: G_4 の演算表

$\cdot$	e	a	b	c
e				
a				
b				
c				

例題 11 G_4 の全ての部分群を決定せよ．

解: 部分群の位数はラグランジュの定理から $1, 2, 4$ となる．従って $\{e\}, \{e, a\}, \{e, b\}, \{e, c\}, G_4$ に限られる．位数 2 の群は巡回群であり， G_2 と同型である．

例題 **12** $\mathbf{Z}_4$ の全ての部分群を決定せよ

解: 部分群の位数はラグランジュの定理から $1, 2, 4$ となる．位数が 2 の $\mathbf{Z}_4$ の要素は 2 に限られるので部分群は以下の通りである．

$$\{0\} = [0], \{0, 2\} = [2], \mathbf{Z}_4 = [1]$$

例題 **13** G_4 と $\mathbf{Z}_4 = \{0, 1, 2, 3\}$ とは同型か？

解: G_4 は巡回群でないのに対して $\mathbf{Z}_4$ は巡回群である．従って同型ではあり得ない．上の例題でも確認したように部分群の構造が異なっている．

例題 **14** G_4 の部分群 $H = \{e, a\}$ による G_4 の同値類による分割 (分類) を求めよ．剰余群 G_4/H の位数を求めよ．

解: 同値類は２個であり，一方は $H = e \cdot H = \langle e \rangle = a \cdot H = \langle a \rangle$ である．もう一方の同値類は以下のように計算される．

$$\langle b \rangle = b \cdot H = \{b \cdot e, b \cdot a\} = \{b, c\} = c \cdot H = \langle c \rangle$$

従って $G_4 = H \cup b \cdot H = \langle a \rangle \cup \langle b \rangle$ のように分割される．ラグランジュの定理から $|G_4/H| = |G_4|/|H| = 4/2 = 2$ である．

例題 **15** $\mathbf{Z}_4$ の部分群 $H' = \{0, 2\}$ による $\mathbf{Z}_4$ の同値類による分割 (分類) を求めよ．

解: 同値類は２個であり，一方は $H' = 0 + H' = \langle 0 \rangle = 2 + H' = \langle 2 \rangle$ である．もう一方の同値類は以下のように計算される．

$$\langle 1 \rangle = 1 + H' = \{1 + 0, 1 + 2\} = \{1, 3\} = 3 + H' = \langle 3 \rangle$$

従って $\mathbf{Z}_4 = H' \cup (1 + H') = \langle 0 \rangle \cup \langle 1 \rangle$ のように分割される．

例題 **16** G_4/H の演算表 (表 8) を完成せよ．

$$\langle a \rangle \cdot \langle a \rangle = \langle a \cdot a \rangle = ?$$

$G_4/H \simeq \mathbf{Z}_4/H' \simeq \mathbf{Z}_2$ を満す．

注意 3 : G_4 はのちに出てくる群である．クラインの４元群 (Klein four-group) ともよばれる．

注意 4 : G_4 は剰余体 $\mathbf{Z}_2[x]/(x^2+x+1) = \{0, 1, x, x+1\}$ の加法群と同型である (演習課題 5.8.2)．

表 8: G_4/H の演算表

$\cdot$	$\langle a \rangle$	$\langle b \rangle$
$\langle a \rangle$		
$\langle b \rangle$		

5.5 有限群の応用: $\mathbf{Z}_2[x]$ の剰余体

第２講 宿題で $\mathbf{Z}_2[x]$ の３次既約多項式 $x^3 + x + 1$ を用いて剰余体 $\mathbf{Z}_2[x]/(x^3 + x + 1)$ を構成した．剰余の乗法の演算表の性質を有限群と関連させて再考しよう．

1. $\mathbf{Z}_2[x]$ の３次多項式を列挙せよ．

   解: ３次多項式であるので $x^3 + ax^2 + bx + c$ の形であり，$a, b, c \in \mathbf{Z}_2$ であるので各々 $0, 1$ の 2 種類ずつ値を取り得る．従って $x^3, x^3+1, x^3+x+1, x^3+x^2+x+1, x^3+x^2, x^3+x, x^3+x^2+1, x^3+x^2+x$ の８個である．

2. $\mathbf{Z}_2[x]$ の３次多項式の既約，可約を判定せよ．可約の場合には因数分解せよ．可約であるとすると必ず一方は１次式 $x - a$ となることを利用せよ．

   解: 既約多項式は x^3+x+1, x^3+x^2+1 の２個，他は例えば $x^3+x^2+x+1 = (x^2+1)(x+1) = (x+1)^3$ と因数分解できる．ここで係数は $\mathbf{Z}_2$ の要素であるので因数定理で確認するのは $0, 1$ のみであり，$f(0), f(1)$ の値が 0 になるかを確認することになる．

3. x^i $(i = 1, 2, \cdots, 7)$ の多項式 $x^3 + x + 1$ での剰余 (割った余り) を計算せよ．

   解: $x^3 \equiv x + 1$ であることを用いて高い次数の剰余を低次にする．$x, x^2, x^3 \equiv x+1, x^4 = xx^3 \equiv x(x+1) = x^2+x, x^5 = xx^4 \equiv x(x^2+x) = x^3+x^2 \equiv x^2+x+1, x^6 = xx^5 \equiv x(x^2+x+1) = x^3+x^2+x = x+1+x^2+x \equiv x^2+1, x^7 = xx^6 \equiv x(x^2+1) = x^3+x \equiv 1 (\text{mod. } x^3+x+1)$ である．

4. 多項式 $x^3 + x + 1$ での剰余 $0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1$ に対する乗法の演算表を作成せよ．ここで $x^i \cdot x^j = x^{i+j}$ であることを利用せよ．

解: 小問３から要素に対応する x^i を満す i を求め，$x^i \cdot x^j = x^{i+j}$ で定まる $i+j$ を並べると以下のようになる．例えば $(x^2+1)(x^2+x+1)$ は $x^2+1 = x^6$, $x^2+x+1 = x^5$ であるのでその積は $(x^2+1)(x^2+x+1) = x^6 \cdot x^5 = x^{11} = x^7 x^4 = x^4 = x^2 + x$．小問２から $\mathbf{Z}_2[x]$ の多項式 x^3+x+1 は既

表 9: $\mathbf{Z}_2[x]/(x^3+x+1)$ の演算表 (指数版)

·	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
	0	1	3	2	6	4	5
0	0	1	3	2	6	4	5
1	1	2	4	3	0	5	6
3	3	4	6	5	2	0	1
2	2	3	5	4	1	6	0
6	6	0	2	1	5	3	4
4	4	5	0	6	3	1	2
5	5	6	1	0	4	2	3

約であるので剰余類の集合 $\mathbf{Z}_2[x]/(x^3+x+1)$ は体になる．$\mathbf{Z}_2[x]/(x^3+x+1)$ の要素の数は８個であり，0 以外の７個の要素は乗法に関して群になっている．表 9 は多項式の剰余の乗算は $0,1,2,\cdots,6$ の数に対する $i+j(\mathrm{mod.}\ 7)$ で計算できることを示している．さらに表 9 の x^k を逆に対応する剰余を求めることで表 10 を得る．

この考え方は剰余多項式の積に関して効率の良い計算法と言うだけでなくメモリーの節約となる．積の演算表を保持するためには要素の数 N の２乗 (N^2) の配列が必要となる．一方，多項式の指数表示 `index[]` およびその逆表示 `reverse[]` の配列は $N+N=2N$ である．これらを用いて剰余 $f_i(x), f_j(x)$ の積を求める関数 `multi(i,j)` は以下で実現できる．

```
multi(i,j) = reverse[(index[i]+index[j])%N]
```

小問 3 で $x^7 \equiv 1(\mathrm{mod.}\ x^3+x+1)$ は剰余体 $\mathbf{Z}_2[x]/(x^3+x+1)$ の 0 以外の要素は群であり，さらに位数が 7 の群であるので，巡回群となる．従って素数位数の巡回群であるので単位元 1 以外の任意の要素が生成元である．$x^7=1$ すなわち x の位数 $\sharp(x)=7$ であることに対応している．単位元以外の任意の元が生成元であるので例えば $a=x^2+x+1$ に対して $a,a^2,a^3,\cdots,a^7=1$ を満すことになる．

同様にして $\mathbf{Z}_2[x]$ の５次既約多項式 $f_5(x)=x^5+x^3+1$ を用いて剰余体 $\mathbf{Z}_2[x]/(f_5(x))$ を作る．このとき $\mathbf{Z}_2[x]/(f_5(x))$ の要素の数は 32 であり，0 以外の要素は乗法群であり，31 は素数であるので素数位数の群は巡回群に限ること，1 以外の要素は巡回群の生成元であることを用いて $x,x^2,\cdots,x^{30},x^{31}=1,\sharp(x)=31$ となることがわかる．

例題 17 ７次既約多項式 $f_7(x)$ を用いて剰余体 $\mathbf{Z}_2[x]/(f_7(x))$ を構成したとき，剰余体の要素数は $2^7=128$ であり，要素 x に対して $x,x^2,\cdots,x^{126},x^{127}=1,\ (\sharp(x)=127)$ を満すことを説明せよ

解: 剰余記号に置き換えれば以下の式になる．

$$x^{127} \equiv 1 \pmod{f_7(x)}$$

注意 5 : n 次既約多項式 $f_n(x)$ を用いた剰余体 $\mathbf{Z}_2[x]/(f_n(x))$ の要素数は 2^n であり，0 を除く乗法群の要素数 (位数) 2^n-1 が素数の場合も同様である．

5.6 自然数 N の可逆化

体のお話で、改めて述べるので、ここでは手続きのみを簡単に述べる。
自然数 $\mathbf{N}=\{1,2,3,\cdots\}$ と加法 $+$ に対し、次の手順で可逆化する（整数を構築する)。

1. 正則な元の集合: $E^*=\mathbf{N}$
2. 同値関係 $(x_1,y_1)\sim(x_2,y_2)$

   $x_1+y_2=x_2+y_1$

   差を知っている我々は上の式を変形して $x_1-y_1=x_2-y_2$，すなわち，差が同じものを同値としている．
3. $\overline{E}=\mathbf{N}\times E^*/\sim\ =\{\langle(x,y)\rangle\}$

   全ての自然数の組で差が同じものをまとめて同値類 (部分集合) とする．
4. $x\ \to\ \langle(x+y,y)\rangle$ で自然数 x と $\langle(x+y,y)\rangle$ を同一視する (同じものと見なす)．即ち，x と差が $x=(x+y)-y$ となる同値類を同一視する．

表 10: $\mathbf{Z}_2[x]/(x^3+x+1)$ の乗算の演算表

$\cdot$	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	0	0	0	0	0	0	0
1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	0	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
x^2	0	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
x^2+1	0	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+x	x^2	$x+1$

5. $\langle(z,z)\rangle$ **は単位元 (即ち差が** 0 **のもの)**

6. $\langle(x+y,y)\rangle$ **の逆元は** $\langle(y,x+y)\rangle$ **(即ち** $-x$**)**

可逆化の手続きでゼロ (加算の単位元) と負の整数を作り出し，整数の集合 Z が構成できた．

5.7 巡回群の直和分解

定理 2 巡回群 G **の位数が** mn **で** m,n **が互いに素なら** G **は位数** m,n **の 巡回群の直積 (直和) に分解される．**

証明: 巡回群は可換であり $|G|=mn$ **であるので** $G=\{a,2a,3a,\ldots,mn\cdot a=0\}$ **と書ける．**

$$H_1=\{na,2na,3na,\ldots,mn\cdot a=0\},$$

$$H_2=\{ma,2ma,3ma,\ldots,mn\cdot a=0\}$$

とすると H_1,H_2 **は** G **の部分群であり，さらに可換であるので正規部分群である．**H_i **の定義と** m,n **が互いに素であることから** $km=ln(1\le k\le n,1\le l\le m)$ **となるのは** $k=n,l=m$ **に限られるので** $H_1\cap H_2=\{0\}$ **である．また** m,n **が互いに素であるので任意の** $t(1\le t\le mn)$ **に対して** $\alpha m+\beta n=t$ **を満たす** $\alpha,\beta\in\mathbf{Z}$ **が存在する．従って** $ta=\alpha ma+\beta na\in H_1+H_2$ **と表わされるので，第 4 講定理 3 から** $G=H_1\oplus H_2$ **と直和分解される．(証明完了)**

5.8 第 5 講 演習課題

5.8.1 フェルマーの小定理 (クイズ)

例題 2 にならって、$a=987654321$ **のとき** $a^a(\mathrm{mod.}\ 11)$ **を簡単にせよ．**
hint:$10\equiv -1(\mathrm{mod.}\ 11)$ **とフェルマーの小定理を併用する。**

5.8.2 クラインの 4 元群 G_4 について

G_4 **および剰余体** $\mathbf{Z}_2[x]/(x^2+x+1)=\{0,1,x,x+1\}$ **(第 2 講例題 12) における加法群に関して要素の対応関係を具体的に述べ同型写像を作成せよ．**

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

5.8.3 位数 4 の群について

位数 4 の群は $G_4,\mathbf{Z}_4$ **が知られている．同型を除いてこれ以外の構造の群は存在しないことを示せ．**

5.8.4 無限巡回群の性質

以下が成り立つことを示せ．
「無限巡回群の任意の部分群 $(\neq\{0\})$ **は無限巡回群である.」**

5.8.5 $\mathbf{Z}_2[x]/(x^3+x+1)^*$ と同型な群 (宿題)

$\mathbf{Z}_2[x]/(x^3+x+1)^*$ **の乗法についての演算表を作成せよ。これと同型になる** $\mathbf{Z}_n$ **の** n **と** $\mathbf{Z}_2[x]/(x^3+x+1)^*\to\mathbf{Z}_n$ **の同型写像を作成せよ。**

5.8.6 $\mathbf{Z}_2[x]/(x^5+x^3+1)$ の乗法の演算表

$\mathbf{Z}_2[x]$ **の 5 次既約多項式** $f_5(x)=x^5+x^3+1$ **に対する剰余体** $\mathbf{Z}_2[x]/(f_5(x))$ **の乗法の演算表を作成せよ．**

5.8.7 巡回群の特徴付け

以下が成り立つことを示せ．
「巡回群 G **の位数が** n **であれば** $G\simeq\mathbf{Z}_n$ **であり，位数が** 0 **(要素数が無限) であれば** $G\simeq\mathbf{Z}$ **である.」**

5.8.8　$\mathbf{Z}_3[x]$ の剰余体について

1. $\mathbf{Z}_3 = \{0, 1, 2\}$ の代表元を $0, 1, -1$ とする．$1, -1$ の乗算に関する演算表を作成せよ．

2. $\mathbf{Z}_3[x]$ における１次式 $ax + b$ を列挙せよ．

3. $\mathbf{Z}_3[x]$ の多項式 $x^2 + x + 1$ を因数分解せよ．

4. $\mathbf{Z}_3[x]$ の２次多項式 $f(x) = x^2 + 1$ は $f(0) = \square$, $f(\pm 1) = \square$ であるので因数定理より既約である．

5. $\mathbf{Z}_3[x]$ の２次多項式 $f(x) = x^2 + 1$ の剰余 $ax + b$ の数は$\square$個である．

6. 剰余類 $\mathbf{Z}_3[x]/(x^2 + 1)$ は体になるので 0 以外の要素を G とすると G は乗算に関して群であり，単位元は $\square$ である．G は $\square$ 個の要素を持つので，ラグランジュの定理から部分群の位数は$\square$ である．

7. G の要素 x に対して $x^2 = -1, x^4 = 1$ であるので要素 x の位数は $\square$ である．一方，$(x + 1)^2 = x^2 + 2x + 1 = -x, (x + 1)^4 = x^2 = -1, (x + 1)^8 = 1$ であるので要素 $x + 1$ の位数は$\square$ である．

8. 位数が 2 の G の要素は $\square$ である．

9. G は $\square$ を生成元とする巡回群である．従って $f : G \to \mathbf{Z}_8$ の準同型写像を作成すると $f(x + 1) = \square$ であり， １対１かつ上への写像であるので同型となる．

AA2021/Quiz-5	**(6/24/2021)**
氏名:	**学籍番号:**