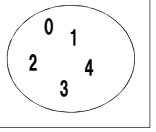
０６．群の定義

代数Ⅰ

代数系

集合　＋　代数的構造　＝　代数系

何かしらの数の集まり



四則演算などの
公理や定義

任意の演算

a＊b＝｜a－b｜

亜群
半群
モノイド
群

環
体

2

群

・空でない集合Gに対して，ある演算＊が定義

（１）閉鎖律

（２）結合律　$(x*y)*z = x*(y*z)$

（３）単位元 e の存在　$e*x = x*e = x$

（４）逆元 x' の存在　$x'*x = x*x' = e$

（５）可換律　$x*y = y*x$

可換群

位数n　$|G| = n$

亜群，半群，モノイド，群

閉鎖律（ある演算に関して閉じている）

集合Ｓは演算＊に関して亜群（groupid）

結合律（　（ｘ＊ｙ）＊ｚ＝ｘ＊（ｙ＊ｚ）　）

半群（semi-group）

単位元（　ｅ＊ｘ＝ｘ＊ｅ=ｘ　）

モノイド（monoid）

逆元（　ｘ’＊ｘ＝ｘ＊ｘ’=ｅ　）

群（group）

4

整数全体は加法に関して群か？

5

整数全体は乗法に関して群か？

6

部分群

群Gの空でない部分集合をHとする．
HがGの部分群であるための必要十分条件は
Hが次の条件(1)と(2)を満足していることである．
(1)$\forall a,b\in H \Rightarrow a\circ b\in H$
(2)$\forall a\in H \Rightarrow a^{-1}\in H$
さらに(1),(2)は，次の条件(3)と同値である．
(3)$\forall a,b\in H \Rightarrow a\circ b^{-1}\in H$

7

既約剰余類の部分群

$Z_6^{\times}=\{1,5\}$

×	1	5
1	1	5
5	5	1

自明な部分群
単位元のみの部分群$\{1\}$
全体集合$\{1,5\}$

$\{1\},\{1,5\}$　ともに正規部分群

8

既約剰余類の部分群

$Z_9^{\times}=\{1,2,4,5,7,8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

自明な部分群
$\{1\},\{1,2,4,5,7,8\}$
生成元は2と5
4からは{4,7,1}
7からは{7,4,1}
8からは{8,1}

すべて正規部分群

9

既約剰余類の部分群

$Z_{12}^{\times}=\{1,5,7,11\}$

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

自明な部分群
$\{1\},\{1,5,7,11\}$
5からは{5,1}
7からは{7,1}
11からは{11,1}
既約剰余類は乗法において可換
すべて正規部分群

10

巡回群

aの累乗の全体からなるGの部分集合
$<a>=\{a^n \mid n\in Z\}$はGの部分群になる．
また，この群はaを含むGの最小の部分群である．
部分群$<a>$をaで生成されたGの巡回部分群という．

Gをaによって生成される位数nの巡回群とする．
このとき，Gの元a^kの位数は$n/(n,k)$となる．
ただし,(n,k)はnとkの最大公約数を表す．
$|a^k|=n/(n,k)$

11

位数

群Gの元aに対して，$a^n=e$となるような
最小の正の整数をaの位数という．そのような
整数が無いとき，aの位数は無限という．
$|a|$でaの位数を表す．aの位数が無限のとき，
$|a|=\infty$

例題　加法群Z_{12}において，各元の位数を求めよ

$|0|=1,|1|=12,|2|=6,|3|=4,|4|=3,$
$|5|=12,\{5,10,3,8,1,6,11,4,9,2,7,0\}$
$|6|=2,|7|=12,|8|=3,|9|=4,|10|=5,|11|=12$

12

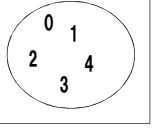
０６．群の定義

代数Ⅰ

代数系

集合　＋　代数的構造　＝　代数系

何かしらの数の集まり



四則演算などの
公理や定義

任意の演算

a＊b＝｜a－b｜

亜群
半群
モノイド
群

環
体

2

群

・空でない集合Gに対して，ある演算＊が定義

（１）閉鎖律

（２）結合律　$(x*y)*z = x*(y*z)$

（３）単位元 e の存在　$e*x = x*e = x$

（４）逆元 x' の存在　$x'*x = x*x' = e$

（５）可換律　$x*y = y*x$

可換群

位数n　$|G| = n$

亜群，半群，モノイド，群

閉鎖律（ある演算に関して閉じている）

集合Ｓは演算＊に関して亜群（groupid）

結合律（　（ｘ＊ｙ）＊ｚ＝ｘ＊（ｙ＊ｚ）　）

半群（semi-group）

単位元（　ｅ＊ｘ＝ｘ＊ｅ=ｘ　）

モノイド（monoid）

逆元（　ｘ’＊ｘ＝ｘ＊ｘ’=ｅ　）

群（group）

4

整数全体は加法に関して群か？

5

整数全体は乗法に関して群か？

6

部分群

群Gの空でない部分集合をHとする．
HがGの部分群であるための必要十分条件は
Hが次の条件(1)と(2)を満足していることである．
(1)$\forall a,b\in H \Rightarrow a\circ b\in H$
(2)$\forall a\in H \Rightarrow a^{-1}\in H$
さらに(1),(2)は，次の条件(3)と同値である．
(3)$\forall a,b\in H \Rightarrow a\circ b^{-1}\in H$

7

既約剰余類の部分群

$Z_6^{\times}=\{1,5\}$

×	1	5
1	1	5
5	5	1

自明な部分群
単位元のみの部分群$\{1\}$
全体集合$\{1,5\}$

$\{1\},\{1,5\}$　ともに正規部分群

8

既約剰余類の部分群

$Z_9^{\times}=\{1,2,4,5,7,8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

自明な部分群
$\{1\},\{1,2,4,5,7,8\}$
生成元は2と5
4からは{4,7,1}
7からは{7,4,1}
8からは{8,1}

すべて正規部分群

9

既約剰余類の部分群

$Z_{12}^{\times}=\{1,5,7,11\}$

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

自明な部分群
$\{1\},\{1,5,7,11\}$
5からは{5,1}
7からは{7,1}
11からは{11,1}
既約剰余類は乗法において可換
すべて正規部分群

10

巡回群

aの累乗の全体からなるGの部分集合
$<a>=\{a^n \mid n\in Z\}$はGの部分群になる．
また，この群はaを含むGの最小の部分群である．
部分群$<a>$をaで生成されたGの巡回部分群という．

Gをaによって生成される位数nの巡回群とする．
このとき，Gの元a^kの位数は$n/(n,k)$となる．
ただし,(n,k)はnとkの最大公約数を表す．
$|a^k|=n/(n,k)$

11

位数

群Gの元aに対して，$a^n=e$となるような
最小の正の整数をaの位数という．そのような
整数が無いとき，aの位数は無限という．
$|a|$でaの位数を表す．aの位数が無限のとき，
$|a|=\infty$

例題　加法群Z_{12}において，各元の位数を求めよ

$|0|=1,|1|=12,|2|=6,|3|=4,|4|=3,$
$|5|=12,\{5,10,3,8,1,6,11,4,9,2,7,0\}$
$|6|=2,|7|=12,|8|=3,|9|=4,|10|=5,|11|=12$

12

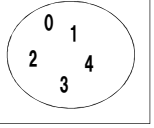
０６．群の定義

代数Ⅰ

代数系

集合　＋　代数的構造　＝　代数系

何かしらの数の集まり



四則演算などの
公理や定義

任意の演算

a＊b＝｜a－b｜

亜群
半群
モノイド
群

環
体

2

群

・空でない集合Gに対して，ある演算＊が定義

（１）閉鎖律

（２）結合律　$(x*y)*z = x*(y*z)$

（３）単位元 e の存在　$e*x = x*e = x$

（４）逆元 x' の存在　$x'*x = x*x' = e$

（５）可換律　$x*y = y*x$

可換群

位数n　$|G| = n$

亜群，半群，モノイド，群

閉鎖律（ある演算に関して閉じている）

集合Ｓは演算＊に関して亜群（groupid）

結合律（　（ｘ＊ｙ）＊ｚ＝ｘ＊（ｙ＊ｚ）　）

半群（semi-group）

単位元（　ｅ＊ｘ＝ｘ＊ｅ=ｘ　）

モノイド（monoid）

逆元（　ｘ’＊ｘ＝ｘ＊ｘ’=ｅ　）

群（group）

4

整数全体は加法に関して群か？

5

整数全体は乗法に関して群か？

6

部分群

群Gの空でない部分集合をHとする．
HがGの部分群であるための必要十分条件は
Hが次の条件(1)と(2)を満足していることである．
(1)$\forall a,b\in H \Rightarrow a\circ b\in H$
(2)$\forall a\in H \Rightarrow a^{-1}\in H$
さらに(1),(2)は，次の条件(3)と同値である．
(3)$\forall a,b\in H \Rightarrow a\circ b^{-1}\in H$

7

既約剰余類の部分群

$Z_6^{\times}=\{1,5\}$

×	1	5
1	1	5
5	5	1

自明な部分群
単位元のみの部分群$\{1\}$
全体集合$\{1,5\}$

$\{1\},\{1,5\}$　ともに正規部分群

8

既約剰余類の部分群

$Z_9^{\times}=\{1,2,4,5,7,8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

自明な部分群
$\{1\},\{1,2,4,5,7,8\}$
生成元は2と5
4からは{4,7,1}
7からは{7,4,1}
8からは{8,1}

すべて正規部分群

9

既約剰余類の部分群

$Z_{12}^{\times}=\{1,5,7,11\}$

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

自明な部分群
$\{1\},\{1,5,7,11\}$
5からは{5,1}
7からは{7,1}
11からは{11,1}
既約剰余類は乗法において可換
すべて正規部分群

10

巡回群

aの累乗の全体からなるGの部分集合
$<a>=\{a^n \mid n\in Z\}$はGの部分群になる．
また，この群はaを含むGの最小の部分群である．
部分群$<a>$をaで生成されたGの巡回部分群という．

Gをaによって生成される位数nの巡回群とする．
このとき，Gの元a^kの位数は$n/(n,k)$となる．
ただし,(n,k)はnとkの最大公約数を表す．
$|a^k|=n/(n,k)$

11

位数

群Gの元aに対して，$a^n=e$となるような
最小の正の整数をaの位数という．そのような
整数が無いとき，aの位数は無限という．
$|a|$でaの位数を表す．aの位数が無限のとき，
$|a|=\infty$

例題　加法群Z_{12}において，各元の位数を求めよ

$|0|=1,|1|=12,|2|=6,|3|=4,|4|=3,$
$|5|=12,\{5,10,3,8,1,6,11,4,9,2,7,0\}$
$|6|=2,|7|=12,|8|=3,|9|=4,|10|=5,|11|=12$

12

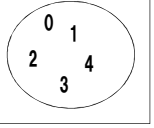
０６．群の定義

代数Ⅰ

代数系

集合　＋　代数的構造　＝　代数系

何かしらの数の集まり



四則演算などの
公理や定義

任意の演算

a＊b＝｜a－b｜

亜群
半群
モノイド
群

環
体

2

群

・空でない集合Gに対して，ある演算＊が定義

（１）閉鎖律

（２）結合律　$(x*y)*z = x*(y*z)$

（３）単位元 e の存在　$e*x = x*e = x$

（４）逆元 x' の存在　$x'*x = x*x' = e$

（５）可換律　$x*y = y*x$

可換群

位数n　$|G| = n$

亜群，半群，モノイド，群

閉鎖律（ある演算に関して閉じている）

集合Ｓは演算＊に関して亜群（groupid）

結合律（　（ｘ＊ｙ）＊ｚ＝ｘ＊（ｙ＊ｚ）　）

半群（semi-group）

単位元（　ｅ＊ｘ＝ｘ＊ｅ=ｘ　）

モノイド（monoid）

逆元（　ｘ’＊ｘ＝ｘ＊ｘ’=ｅ　）

群（group）

4

整数全体は加法に関して群か？

5

整数全体は乗法に関して群か？

6

部分群

群Gの空でない部分集合をHとする．
HがGの部分群であるための必要十分条件は
Hが次の条件(1)と(2)を満足していることである．
(1)$\forall a,b\in H \Rightarrow a\circ b\in H$
(2)$\forall a\in H \Rightarrow a^{-1}\in H$
さらに(1),(2)は，次の条件(3)と同値である．
(3)$\forall a,b\in H \Rightarrow a\circ b^{-1}\in H$

7

既約剰余類の部分群

$Z_6^{\times}=\{1,5\}$

×	1	5
1	1	5
5	5	1

自明な部分群
単位元のみの部分群$\{1\}$
全体集合$\{1,5\}$

$\{1\},\{1,5\}$　ともに正規部分群

8

既約剰余類の部分群

$Z_9^{\times}=\{1,2,4,5,7,8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

自明な部分群
$\{1\},\{1,2,4,5,7,8\}$
生成元は2と5
4からは{4,7,1}
7からは{7,4,1}
8からは{8,1}

すべて正規部分群

9

既約剰余類の部分群

$Z_{12}^{\times}=\{1,5,7,11\}$

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

自明な部分群
$\{1\},\{1,5,7,11\}$
5からは{5,1}
7からは{7,1}
11からは{11,1}
既約剰余類は乗法において可換
すべて正規部分群

10

巡回群

aの累乗の全体からなるGの部分集合
$<a>=\{a^n \mid n\in Z\}$はGの部分群になる．
また，この群はaを含むGの最小の部分群である．
部分群$<a>$をaで生成されたGの巡回部分群という．

Gをaによって生成される位数nの巡回群とする．
このとき，Gの元a^kの位数は$n/(n,k)$となる．
ただし,(n,k)はnとkの最大公約数を表す．
$|a^k|=n/(n,k)$

11

位数

群Gの元aに対して，$a^n=e$となるような
最小の正の整数をaの位数という．そのような
整数が無いとき，aの位数は無限という．
$|a|$でaの位数を表す．aの位数が無限のとき，
$|a|=\infty$

例題　加法群Z_{12}において，各元の位数を求めよ

$|0|=1,|1|=12,|2|=6,|3|=4,|4|=3,$
$|5|=12,\{5,10,3,8,1,6,11,4,9,2,7,0\}$
$|6|=2,|7|=12,|8|=3,|9|=4,|10|=5,|11|=12$

12

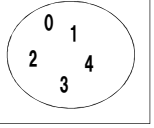
０６．群の定義

代数Ⅰ

代数系

集合　＋　代数的構造　＝　代数系

何かしらの数の集まり



四則演算などの
公理や定義

任意の演算

a＊b＝｜a－b｜

亜群
半群
モノイド
群

環
体

2

群

・空でない集合Gに対して，ある演算＊が定義

（１）閉鎖律

（２）結合律　$(x*y)*z = x*(y*z)$

（３）単位元 e の存在　$e*x = x*e = x$

（４）逆元 x' の存在　$x'*x = x*x' = e$

（５）可換律　$x*y = y*x$

可換群

位数n　$|G| = n$

亜群，半群，モノイド，群

閉鎖律（ある演算に関して閉じている）

集合Ｓは演算＊に関して亜群（groupid）

結合律（　（ｘ＊ｙ）＊ｚ＝ｘ＊（ｙ＊ｚ）　）

半群（semi-group）

単位元（　ｅ＊ｘ＝ｘ＊ｅ=ｘ　）

モノイド（monoid）

逆元（　ｘ’＊ｘ＝ｘ＊ｘ’=ｅ　）

群（group）

4

整数全体は加法に関して群か？

5

整数全体は乗法に関して群か？

6

部分群

群Gの空でない部分集合をHとする．
HがGの部分群であるための必要十分条件は
Hが次の条件(1)と(2)を満足していることである．
(1)$\forall a,b\in H \Rightarrow a\circ b\in H$
(2)$\forall a\in H \Rightarrow a^{-1}\in H$
さらに(1),(2)は，次の条件(3)と同値である．
(3)$\forall a,b\in H \Rightarrow a\circ b^{-1}\in H$

7

既約剰余類の部分群

$Z_6^{\times}=\{1,5\}$

×	1	5
1	1	5
5	5	1

自明な部分群
単位元のみの部分群$\{1\}$
全体集合$\{1,5\}$

$\{1\},\{1,5\}$　ともに正規部分群

8

既約剰余類の部分群

$Z_9^{\times}=\{1,2,4,5,7,8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

自明な部分群
$\{1\},\{1,2,4,5,7,8\}$
生成元は2と5
4からは{4,7,1}
7からは{7,4,1}
8からは{8,1}

すべて正規部分群

9

既約剰余類の部分群

$Z_{12}^{\times}=\{1,5,7,11\}$

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

自明な部分群
$\{1\},\{1,5,7,11\}$
5からは{5,1}
7からは{7,1}
11からは{11,1}
既約剰余類は乗法において可換
すべて正規部分群

10

巡回群

aの累乗の全体からなるGの部分集合
$<a>=\{a^n \mid n\in Z\}$はGの部分群になる．
また，この群はaを含むGの最小の部分群である．
部分群$<a>$をaで生成されたGの巡回部分群という．

Gをaによって生成される位数nの巡回群とする．
このとき，Gの元a^kの位数は$n/(n,k)$となる．
ただし,(n,k)はnとkの最大公約数を表す．
$|a^k|=n/(n,k)$

11

位数

群Gの元aに対して，$a^n=e$となるような
最小の正の整数をaの位数という．そのような
整数が無いとき，aの位数は無限という．
$|a|$でaの位数を表す．aの位数が無限のとき，
$|a|=\infty$

例題　加法群Z_{12}において，各元の位数を求めよ

$|0|=1,|1|=12,|2|=6,|3|=4,|4|=3,$
$|5|=12,\{5,10,3,8,1,6,11,4,9,2,7,0\}$
$|6|=2,|7|=12,|8|=3,|9|=4,|10|=5,|11|=12$

12

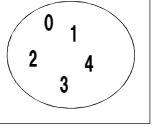
０６．群の定義

代数Ⅰ

代数系

集合　＋　代数的構造　＝　代数系

何かしらの数の集まり



四則演算などの
公理や定義

任意の演算

a＊b＝｜a－b｜

亜群
半群
モノイド
群

環
体

2

群

・空でない集合Gに対して，ある演算＊が定義

（１）閉鎖律

（２）結合律　$(x*y)*z = x*(y*z)$

（３）単位元 e の存在　$e*x = x*e = x$

（４）逆元 x' の存在　$x'*x = x*x' = e$

（５）可換律　$x*y = y*x$

可換群

位数n　$|G| = n$

亜群，半群，モノイド，群

閉鎖律（ある演算に関して閉じている）

集合Ｓは演算＊に関して亜群（groupid）

結合律（　（ｘ＊ｙ）＊ｚ＝ｘ＊（ｙ＊ｚ）　）

半群（semi-group）

単位元（　ｅ＊ｘ＝ｘ＊ｅ=ｘ　）

モノイド（monoid）

逆元（　ｘ’＊ｘ＝ｘ＊ｘ’=ｅ　）

群（group）

4

整数全体は加法に関して群か？

5

整数全体は乗法に関して群か？

6

部分群

群Gの空でない部分集合をHとする．
HがGの部分群であるための必要十分条件は
Hが次の条件(1)と(2)を満足していることである．
(1)$\forall a,b\in H \Rightarrow a\circ b\in H$
(2)$\forall a\in H \Rightarrow a^{-1}\in H$
さらに(1),(2)は，次の条件(3)と同値である．
(3)$\forall a,b\in H \Rightarrow a\circ b^{-1}\in H$

7

既約剰余類の部分群

$Z_6^{\times}=\{1,5\}$

×	1	5
1	1	5
5	5	1

自明な部分群
単位元のみの部分群$\{1\}$
全体集合$\{1,5\}$

$\{1\},\{1,5\}$　ともに正規部分群

8

既約剰余類の部分群

$Z_9^{\times}=\{1,2,4,5,7,8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

自明な部分群
$\{1\},\{1,2,4,5,7,8\}$
生成元は2と5
4からは{4,7,1}
7からは{7,4,1}
8からは{8,1}

すべて正規部分群

9

既約剰余類の部分群

$Z_{12}^{\times}=\{1,5,7,11\}$

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

自明な部分群
$\{1\},\{1,5,7,11\}$
5からは{5,1}
7からは{7,1}
11からは{11,1}
既約剰余類は乗法において可換
すべて正規部分群

10

巡回群

aの累乗の全体からなるGの部分集合
$<a>=\{a^n \mid n\in Z\}$はGの部分群になる．
また，この群はaを含むGの最小の部分群である．
部分群$<a>$をaで生成されたGの巡回部分群という．

Gをaによって生成される位数nの巡回群とする．
このとき，Gの元a^kの位数は$n/(n,k)$となる．
ただし,(n,k)はnとkの最大公約数を表す．
$|a^k|=n/(n,k)$

11

位数

群Gの元aに対して，$a^n=e$となるような
最小の正の整数をaの位数という．そのような
整数が無いとき，aの位数は無限という．
$|a|$でaの位数を表す．aの位数が無限のとき，
$|a|=\infty$

例題　加法群Z_{12}において，各元の位数を求めよ

$|0|=1,|1|=12,|2|=6,|3|=4,|4|=3,$
$|5|=12,\{5,10,3,8,1,6,11,4,9,2,7,0\}$
$|6|=2,|7|=12,|8|=3,|9|=4,|10|=5,|11|=12$

12

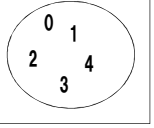
０６．群の定義

代数Ⅰ

代数系

集合　＋　代数的構造　＝　代数系

何かしらの数の集まり



四則演算などの
公理や定義

任意の演算

a＊b＝｜a－b｜

亜群
半群
モノイド
群

環
体

2

群

・空でない集合Gに対して，ある演算＊が定義

（１）閉鎖律

（２）結合律　$(x*y)*z = x*(y*z)$

（３）単位元 e の存在　$e*x = x*e = x$

（４）逆元 x' の存在　$x'*x = x*x' = e$

（５）可換律　$x*y = y*x$

可換群

位数n　$|G| = n$

亜群，半群，モノイド，群

閉鎖律（ある演算に関して閉じている）

集合Ｓは演算＊に関して亜群（groupid）

結合律（　（ｘ＊ｙ）＊ｚ＝ｘ＊（ｙ＊ｚ）　）

半群（semi-group）

単位元（　ｅ＊ｘ＝ｘ＊ｅ=ｘ　）

モノイド（monoid）

逆元（　ｘ’＊ｘ＝ｘ＊ｘ’=ｅ　）

群（group）

4

整数全体は加法に関して群か？

5

整数全体は乗法に関して群か？

6

部分群

群Gの空でない部分集合をHとする．
HがGの部分群であるための必要十分条件は
Hが次の条件(1)と(2)を満足していることである．
(1)$\forall a,b\in H \Rightarrow a\circ b\in H$
(2)$\forall a\in H \Rightarrow a^{-1}\in H$
さらに(1),(2)は，次の条件(3)と同値である．
(3)$\forall a,b\in H \Rightarrow a\circ b^{-1}\in H$

7

既約剰余類の部分群

$Z_6^{\times}=\{1,5\}$

×	1	5
1	1	5
5	5	1

自明な部分群
単位元のみの部分群$\{1\}$
全体集合$\{1,5\}$

$\{1\},\{1,5\}$　ともに正規部分群

8

既約剰余類の部分群

$Z_9^{\times}=\{1,2,4,5,7,8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

自明な部分群
$\{1\},\{1,2,4,5,7,8\}$
生成元は2と5
4からは{4,7,1}
7からは{7,4,1}
8からは{8,1}

すべて正規部分群

9

既約剰余類の部分群

$Z_{12}^{\times}=\{1,5,7,11\}$

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

自明な部分群
$\{1\},\{1,5,7,11\}$
5からは{5,1}
7からは{7,1}
11からは{11,1}
既約剰余類は乗法において可換
すべて正規部分群

10

巡回群

aの累乗の全体からなるGの部分集合
$<a>=\{a^n \mid n\in Z\}$はGの部分群になる．
また，この群はaを含むGの最小の部分群である．
部分群$<a>$をaで生成されたGの巡回部分群という．

Gをaによって生成される位数nの巡回群とする．
このとき，Gの元a^kの位数は$n/(n,k)$となる．
ただし,(n,k)はnとkの最大公約数を表す．
$|a^k|=n/(n,k)$

11

位数

群Gの元aに対して，$a^n=e$となるような
最小の正の整数をaの位数という．そのような
整数が無いとき，aの位数は無限という．
$|a|$でaの位数を表す．aの位数が無限のとき，
$|a|=\infty$

例題　加法群Z_{12}において，各元の位数を求めよ

$|0|=1,|1|=12,|2|=6,|3|=4,|4|=3,$
$|5|=12,\{5,10,3,8,1,6,11,4,9,2,7,0\}$
$|6|=2,|7|=12,|8|=3,|9|=4,|10|=5,|11|=12$

12

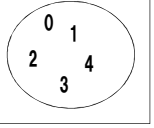
０６．群の定義

代数Ⅰ

代数系

集合　＋　代数的構造　＝　代数系

何かしらの数の集まり



四則演算などの
公理や定義

任意の演算

a＊b＝｜a－b｜

亜群
半群
モノイド
群

環
体

2

群

・空でない集合Gに対して，ある演算＊が定義

（１）閉鎖律

（２）結合律　$(x*y)*z = x*(y*z)$

（３）単位元 e の存在　$e*x = x*e = x$

（４）逆元 x' の存在　$x'*x = x*x' = e$

（５）可換律　$x*y = y*x$

可換群

位数n　$|G| = n$

亜群，半群，モノイド，群

閉鎖律（ある演算に関して閉じている）

集合Ｓは演算＊に関して亜群（groupid）

結合律（　（ｘ＊ｙ）＊ｚ＝ｘ＊（ｙ＊ｚ）　）

半群（semi-group）

単位元（　ｅ＊ｘ＝ｘ＊ｅ=ｘ　）

モノイド（monoid）

逆元（　ｘ’＊ｘ＝ｘ＊ｘ’=ｅ　）

群（group）

4

整数全体は加法に関して群か？

5

整数全体は乗法に関して群か？

6

部分群

群Gの空でない部分集合をHとする．
HがGの部分群であるための必要十分条件は
Hが次の条件(1)と(2)を満足していることである．
(1)$\forall a,b\in H \Rightarrow a\circ b\in H$
(2)$\forall a\in H \Rightarrow a^{-1}\in H$
さらに(1),(2)は，次の条件(3)と同値である．
(3)$\forall a,b\in H \Rightarrow a\circ b^{-1}\in H$

7

既約剰余類の部分群

$Z_6^{\times}=\{1,5\}$

×	1	5
1	1	5
5	5	1

自明な部分群
単位元のみの部分群$\{1\}$
全体集合$\{1,5\}$

$\{1\},\{1,5\}$　ともに正規部分群

8

既約剰余類の部分群

$Z_9^{\times}=\{1,2,4,5,7,8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

自明な部分群
$\{1\},\{1,2,4,5,7,8\}$
生成元は2と5
4からは{4,7,1}
7からは{7,4,1}
8からは{8,1}

すべて正規部分群

9

既約剰余類の部分群

$Z_{12}^{\times}=\{1,5,7,11\}$

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

自明な部分群
$\{1\},\{1,5,7,11\}$
5からは{5,1}
7からは{7,1}
11からは{11,1}
既約剰余類は乗法において可換
すべて正規部分群

10

巡回群

aの累乗の全体からなるGの部分集合
$<a>=\{a^n \mid n\in Z\}$はGの部分群になる．
また，この群はaを含むGの最小の部分群である．
部分群$<a>$をaで生成されたGの巡回部分群という．

Gをaによって生成される位数nの巡回群とする．
このとき，Gの元a^kの位数は$n/(n,k)$となる．
ただし,(n,k)はnとkの最大公約数を表す．
$|a^k|=n/(n,k)$

11

位数

群Gの元aに対して，$a^n=e$となるような
最小の正の整数をaの位数という．そのような
整数が無いとき，aの位数は無限という．
$|a|$でaの位数を表す．aの位数が無限のとき，
$|a|=\infty$

例題　加法群Z_{12}において，各元の位数を求めよ

$|0|=1,|1|=12,|2|=6,|3|=4,|4|=3,$
$|5|=12,\{5,10,3,8,1,6,11,4,9,2,7,0\}$
$|6|=2,|7|=12,|8|=3,|9|=4,|10|=5,|11|=12$

12

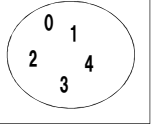
０６．群の定義

代数Ⅰ

代数系

集合　＋　代数的構造　＝　代数系

何かしらの数の集まり



四則演算などの
公理や定義

任意の演算

a＊b＝｜a－b｜

亜群
半群
モノイド
群

環
体

2

群

・空でない集合Gに対して，ある演算＊が定義

（１）閉鎖律

（２）結合律　$(x*y)*z = x*(y*z)$

（３）単位元 e の存在　$e*x = x*e = x$

（４）逆元 x' の存在　$x'*x = x*x' = e$

（５）可換律　$x*y = y*x$

可換群

位数n　$|G| = n$

亜群，半群，モノイド，群

閉鎖律（ある演算に関して閉じている）

集合Ｓは演算＊に関して亜群（groupid）

結合律（　（ｘ＊ｙ）＊ｚ＝ｘ＊（ｙ＊ｚ）　）

半群（semi-group）

単位元（　ｅ＊ｘ＝ｘ＊ｅ=ｘ　）

モノイド（monoid）

逆元（　ｘ’＊ｘ＝ｘ＊ｘ’=ｅ　）

群（group）

4

整数全体は加法に関して群か？

5

整数全体は乗法に関して群か？

6

部分群

群Gの空でない部分集合をHとする．
HがGの部分群であるための必要十分条件は
Hが次の条件(1)と(2)を満足していることである．
(1)$\forall a,b\in H \Rightarrow a\circ b\in H$
(2)$\forall a\in H \Rightarrow a^{-1}\in H$
さらに(1),(2)は，次の条件(3)と同値である．
(3)$\forall a,b\in H \Rightarrow a\circ b^{-1}\in H$

7

既約剰余類の部分群

$Z_6^{\times}=\{1,5\}$

×	1	5
1	1	5
5	5	1

自明な部分群
単位元のみの部分群$\{1\}$
全体集合$\{1,5\}$

$\{1\},\{1,5\}$　ともに正規部分群

8

既約剰余類の部分群

$Z_9^{\times}=\{1,2,4,5,7,8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

自明な部分群
$\{1\},\{1,2,4,5,7,8\}$
生成元は2と5
4からは{4,7,1}
7からは{7,4,1}
8からは{8,1}

すべて正規部分群

9

既約剰余類の部分群

$Z_{12}^{\times}=\{1,5,7,11\}$

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

自明な部分群
$\{1\},\{1,5,7,11\}$
5からは{5,1}
7からは{7,1}
11からは{11,1}
既約剰余類は乗法において可換
すべて正規部分群

10

巡回群

aの累乗の全体からなるGの部分集合
$<a>=\{a^n \mid n\in Z\}$はGの部分群になる．
また，この群はaを含むGの最小の部分群である．
部分群$<a>$をaで生成されたGの巡回部分群という．

Gをaによって生成される位数nの巡回群とする．
このとき，Gの元a^kの位数は$n/(n,k)$となる．
ただし,(n,k)はnとkの最大公約数を表す．
$|a^k|=n/(n,k)$

11

位数

群Gの元aに対して，$a^n=e$となるような
最小の正の整数をaの位数という．そのような
整数が無いとき，aの位数は無限という．
$|a|$でaの位数を表す．aの位数が無限のとき，
$|a|=\infty$

例題　加法群Z_{12}において，各元の位数を求めよ

$|0|=1,|1|=12,|2|=6,|3|=4,|4|=3,$
$|5|=12,\{5,10,3,8,1,6,11,4,9,2,7,0\}$
$|6|=2,|7|=12,|8|=3,|9|=4,|10|=5,|11|=12$

12

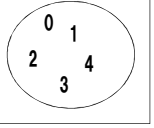
０６．群の定義

代数Ⅰ

代数系

集合　＋　代数的構造　＝　代数系

何かしらの数の集まり



四則演算などの
公理や定義

任意の演算

a＊b＝｜a－b｜

亜群
半群
モノイド
群

環
体

2

群

・空でない集合Gに対して，ある演算＊が定義

（１）閉鎖律

（２）結合律　$(x*y)*z = x*(y*z)$

（３）単位元 e の存在　$e*x = x*e = x$

（４）逆元 x' の存在　$x'*x = x*x' = e$

（５）可換律　$x*y = y*x$

可換群

位数n　$|G| = n$

亜群，半群，モノイド，群

閉鎖律（ある演算に関して閉じている）

集合Ｓは演算＊に関して亜群（groupid）

結合律（　（ｘ＊ｙ）＊ｚ＝ｘ＊（ｙ＊ｚ）　）

半群（semi-group）

単位元（　ｅ＊ｘ＝ｘ＊ｅ=ｘ　）

モノイド（monoid）

逆元（　ｘ’＊ｘ＝ｘ＊ｘ’=ｅ　）

群（group）

4

整数全体は加法に関して群か？

5

整数全体は乗法に関して群か？

6

部分群

群Gの空でない部分集合をHとする．
HがGの部分群であるための必要十分条件は
Hが次の条件(1)と(2)を満足していることである．
(1)$\forall a,b\in H \Rightarrow a\circ b\in H$
(2)$\forall a\in H \Rightarrow a^{-1}\in H$
さらに(1),(2)は，次の条件(3)と同値である．
(3)$\forall a,b\in H \Rightarrow a\circ b^{-1}\in H$

7

既約剰余類の部分群

$Z_6^{\times}=\{1,5\}$

×	1	5
1	1	5
5	5	1

自明な部分群
単位元のみの部分群$\{1\}$
全体集合$\{1,5\}$

$\{1\},\{1,5\}$　ともに正規部分群

8

既約剰余類の部分群

$Z_9^{\times}=\{1,2,4,5,7,8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

自明な部分群
$\{1\},\{1,2,4,5,7,8\}$
生成元は2と5
4からは{4,7,1}
7からは{7,4,1}
8からは{8,1}

すべて正規部分群

9

既約剰余類の部分群

$Z_{12}^{\times}=\{1,5,7,11\}$

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

自明な部分群
$\{1\},\{1,5,7,11\}$
5からは{5,1}
7からは{7,1}
11からは{11,1}
既約剰余類は乗法において可換
すべて正規部分群

10

巡回群

aの累乗の全体からなるGの部分集合
$<a>=\{a^n \mid n\in Z\}$はGの部分群になる．
また，この群はaを含むGの最小の部分群である．
部分群$<a>$をaで生成されたGの巡回部分群という．

Gをaによって生成される位数nの巡回群とする．
このとき，Gの元a^kの位数は$n/(n,k)$となる．
ただし,(n,k)はnとkの最大公約数を表す．
$|a^k|=n/(n,k)$

11

位数

群Gの元aに対して，$a^n=e$となるような
最小の正の整数をaの位数という．そのような
整数が無いとき，aの位数は無限という．
$|a|$でaの位数を表す．aの位数が無限のとき，
$|a|=\infty$

例題　加法群Z_{12}において，各元の位数を求めよ

$|0|=1,|1|=12,|2|=6,|3|=4,|4|=3,$
$|5|=12,\{5,10,3,8,1,6,11,4,9,2,7,0\}$
$|6|=2,|7|=12,|8|=3,|9|=4,|10|=5,|11|=12$

12

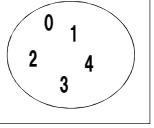
０６．群の定義

代数Ⅰ

代数系

集合　＋　代数的構造　＝　代数系

何かしらの数の集まり



四則演算などの
公理や定義

任意の演算

a＊b＝｜a－b｜

亜群
半群
モノイド
群

環
体

2

群

・空でない集合Gに対して，ある演算＊が定義

（１）閉鎖律

（２）結合律　$(x*y)*z = x*(y*z)$

（３）単位元 e の存在　$e*x = x*e = x$

（４）逆元 x' の存在　$x'*x = x*x' = e$

（５）可換律　$x*y = y*x$

可換群

位数n　$|G| = n$

亜群，半群，モノイド，群

閉鎖律（ある演算に関して閉じている）

集合Ｓは演算＊に関して亜群（groupid）

結合律（　（ｘ＊ｙ）＊ｚ＝ｘ＊（ｙ＊ｚ）　）

半群（semi-group）

単位元（　ｅ＊ｘ＝ｘ＊ｅ=ｘ　）

モノイド（monoid）

逆元（　ｘ’＊ｘ＝ｘ＊ｘ’=ｅ　）

群（group）

4

整数全体は加法に関して群か？

5

整数全体は乗法に関して群か？

6

部分群

群Gの空でない部分集合をHとする．
HがGの部分群であるための必要十分条件は
Hが次の条件(1)と(2)を満足していることである．
(1)$\forall a,b\in H \Rightarrow a\circ b\in H$
(2)$\forall a\in H \Rightarrow a^{-1}\in H$
さらに(1),(2)は，次の条件(3)と同値である．
(3)$\forall a,b\in H \Rightarrow a\circ b^{-1}\in H$

7

既約剰余類の部分群

$Z_6^{\times}=\{1,5\}$

×	1	5
1	1	5
5	5	1

自明な部分群
単位元のみの部分群$\{1\}$
全体集合$\{1,5\}$

$\{1\},\{1,5\}$　ともに正規部分群

8

既約剰余類の部分群

$Z_9^{\times}=\{1,2,4,5,7,8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

自明な部分群
$\{1\},\{1,2,4,5,7,8\}$
生成元は2と5
4からは{4,7,1}
7からは{7,4,1}
8からは{8,1}

すべて正規部分群

9

既約剰余類の部分群

$Z_{12}^{\times}=\{1,5,7,11\}$

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

自明な部分群
$\{1\},\{1,5,7,11\}$
5からは{5,1}
7からは{7,1}
11からは{11,1}
既約剰余類は乗法において可換
すべて正規部分群

10

巡回群

aの累乗の全体からなるGの部分集合
$<a>=\{a^n \mid n\in Z\}$はGの部分群になる．
また，この群はaを含むGの最小の部分群である．
部分群$<a>$をaで生成されたGの巡回部分群という．

Gをaによって生成される位数nの巡回群とする．
このとき，Gの元a^kの位数は$n/(n,k)$となる．
ただし,(n,k)はnとkの最大公約数を表す．
$|a^k|=n/(n,k)$

11

位数

群Gの元aに対して，$a^n=e$となるような
最小の正の整数をaの位数という．そのような
整数が無いとき，aの位数は無限という．
$|a|$でaの位数を表す．aの位数が無限のとき，
$|a|=\infty$

例題　加法群Z_{12}において，各元の位数を求めよ

$|0|=1,|1|=12,|2|=6,|3|=4,|4|=3,$
$|5|=12,\{5,10,3,8,1,6,11,4,9,2,7,0\}$
$|6|=2,|7|=12,|8|=3,|9|=4,|10|=5,|11|=12$

12

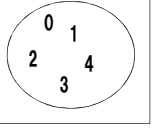
０６．群の定義

代数Ⅰ

代数系

集合　＋　代数的構造　＝　代数系

何かしらの数の集まり



四則演算などの
公理や定義

任意の演算

a＊b＝｜a－b｜

亜群
半群
モノイド
群

環
体

2

群

・空でない集合Gに対して，ある演算＊が定義

（１）閉鎖律

（２）結合律　$(x*y)*z = x*(y*z)$

（３）単位元 e の存在　$e*x = x*e = x$

（４）逆元 x' の存在　$x'*x = x*x' = e$

（５）可換律　$x*y = y*x$

可換群

位数n　$|G| = n$

亜群，半群，モノイド，群

閉鎖律（ある演算に関して閉じている）

集合Ｓは演算＊に関して亜群（groupid）

結合律（　（ｘ＊ｙ）＊ｚ＝ｘ＊（ｙ＊ｚ）　）

半群（semi-group）

単位元（　ｅ＊ｘ＝ｘ＊ｅ=ｘ　）

モノイド（monoid）

逆元（　ｘ’＊ｘ＝ｘ＊ｘ’=ｅ　）

群（group）

4

整数全体は加法に関して群か？

5

整数全体は乗法に関して群か？

6

部分群

群Gの空でない部分集合をHとする．
HがGの部分群であるための必要十分条件は
Hが次の条件(1)と(2)を満足していることである．
(1)$\forall a,b\in H \Rightarrow a\circ b\in H$
(2)$\forall a\in H \Rightarrow a^{-1}\in H$
さらに(1),(2)は，次の条件(3)と同値である．
(3)$\forall a,b\in H \Rightarrow a\circ b^{-1}\in H$

7

既約剰余類の部分群

$Z_6^{\times}=\{1,5\}$

×	1	5
1	1	5
5	5	1

自明な部分群
単位元のみの部分群$\{1\}$
全体集合$\{1,5\}$

$\{1\},\{1,5\}$　ともに正規部分群

8

既約剰余類の部分群

$Z_9^{\times}=\{1,2,4,5,7,8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

自明な部分群
$\{1\},\{1,2,4,5,7,8\}$
生成元は2と5
4からは{4,7,1}
7からは{7,4,1}
8からは{8,1}

すべて正規部分群

9

既約剰余類の部分群

$Z_{12}^{\times}=\{1,5,7,11\}$

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

自明な部分群
$\{1\},\{1,5,7,11\}$
5からは{5,1}
7からは{7,1}
11からは{11,1}
既約剰余類は乗法において可換
すべて正規部分群

10

巡回群

aの累乗の全体からなるGの部分集合
$<a>=\{a^n \mid n\in Z\}$はGの部分群になる．
また，この群はaを含むGの最小の部分群である．
部分群$<a>$をaで生成されたGの巡回部分群という．

Gをaによって生成される位数nの巡回群とする．
このとき，Gの元a^kの位数は$n/(n,k)$となる．
ただし,(n,k)はnとkの最大公約数を表す．
$|a^k|=n/(n,k)$

11

位数

群Gの元aに対して，$a^n=e$となるような
最小の正の整数をaの位数という．そのような
整数が無いとき，aの位数は無限という．
$|a|$でaの位数を表す．aの位数が無限のとき，
$|a|=\infty$

例題　加法群Z_{12}において，各元の位数を求めよ

$|0|=1,|1|=12,|2|=6,|3|=4,|4|=3,$
$|5|=12,\{5,10,3,8,1,6,11,4,9,2,7,0\}$
$|6|=2,|7|=12,|8|=3,|9|=4,|10|=5,|11|=12$

12

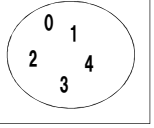
０６．群の定義

代数Ⅰ

代数系

集合　＋　代数的構造　＝　代数系

何かしらの数の集まり



四則演算などの
公理や定義

任意の演算

a＊b＝｜a－b｜

亜群
半群
モノイド
群

環
体

2

群

・空でない集合Gに対して，ある演算＊が定義

（１）閉鎖律

（２）結合律　$(x*y)*z = x*(y*z)$

（３）単位元 e の存在　$e*x = x*e = x$

（４）逆元 x' の存在　$x'*x = x*x' = e$

（５）可換律　$x*y = y*x$

可換群

位数n　$|G| = n$

亜群，半群，モノイド，群

閉鎖律（ある演算に関して閉じている）

集合Ｓは演算＊に関して亜群（groupid）

結合律（　（ｘ＊ｙ）＊ｚ＝ｘ＊（ｙ＊ｚ）　）

半群（semi-group）

単位元（　ｅ＊ｘ＝ｘ＊ｅ=ｘ　）

モノイド（monoid）

逆元（　ｘ’＊ｘ＝ｘ＊ｘ’=ｅ　）

群（group）

4

整数全体は加法に関して群か？

5

整数全体は乗法に関して群か？

6

部分群

群Gの空でない部分集合をHとする．
HがGの部分群であるための必要十分条件は
Hが次の条件(1)と(2)を満足していることである．
(1)$\forall a,b\in H \Rightarrow a\circ b\in H$
(2)$\forall a\in H \Rightarrow a^{-1}\in H$
さらに(1),(2)は，次の条件(3)と同値である．
(3)$\forall a,b\in H \Rightarrow a\circ b^{-1}\in H$

7

既約剰余類の部分群

$Z_6^{\times}=\{1,5\}$

×	1	5
1	1	5
5	5	1

自明な部分群
単位元のみの部分群$\{1\}$
全体集合$\{1,5\}$

$\{1\},\{1,5\}$　ともに正規部分群

8

既約剰余類の部分群

$Z_9^{\times}=\{1,2,4,5,7,8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

自明な部分群
$\{1\},\{1,2,4,5,7,8\}$
生成元は2と5
4からは{4,7,1}
7からは{7,4,1}
8からは{8,1}

すべて正規部分群

9

既約剰余類の部分群

$Z_{12}^{\times}=\{1,5,7,11\}$

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

自明な部分群
$\{1\},\{1,5,7,11\}$
5からは{5,1}
7からは{7,1}
11からは{11,1}
既約剰余類は乗法において可換
すべて正規部分群

10

巡回群

aの累乗の全体からなるGの部分集合
$<a>=\{a^n \mid n\in Z\}$はGの部分群になる．
また，この群はaを含むGの最小の部分群である．
部分群$<a>$をaで生成されたGの巡回部分群という．

Gをaによって生成される位数nの巡回群とする．
このとき，Gの元a^kの位数は$n/(n,k)$となる．
ただし,(n,k)はnとkの最大公約数を表す．
$|a^k|=n/(n,k)$

11

位数

群Gの元aに対して，$a^n=e$となるような
最小の正の整数をaの位数という．そのような
整数が無いとき，aの位数は無限という．
$|a|$でaの位数を表す．aの位数が無限のとき，
$|a|=\infty$

例題　加法群Z_{12}において，各元の位数を求めよ

$|0|=1,|1|=12,|2|=6,|3|=4,|4|=3,$
$|5|=12,\{5,10,3,8,1,6,11,4,9,2,7,0\}$
$|6|=2,|7|=12,|8|=3,|9|=4,|10|=5,|11|=12$

12

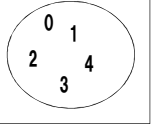
０６．群の定義

代数Ⅰ

代数系

集合　＋　代数的構造　＝　代数系

何かしらの数の集まり



四則演算などの
公理や定義

任意の演算

a＊b＝｜a－b｜

亜群
半群
モノイド
群

環
体

2

群

・空でない集合Gに対して，ある演算＊が定義

（１）閉鎖律

（２）結合律　$(x*y)*z = x*(y*z)$

（３）単位元 e の存在　$e*x = x*e = x$

（４）逆元 x' の存在　$x'*x = x*x' = e$

（５）可換律　$x*y = y*x$

可換群

位数n　$|G| = n$

亜群，半群，モノイド，群

閉鎖律（ある演算に関して閉じている）

集合Ｓは演算＊に関して亜群（groupid）

結合律（　（ｘ＊ｙ）＊ｚ＝ｘ＊（ｙ＊ｚ）　）

半群（semi-group）

単位元（　ｅ＊ｘ＝ｘ＊ｅ=ｘ　）

モノイド（monoid）

逆元（　ｘ’＊ｘ＝ｘ＊ｘ’=ｅ　）

群（group）

4

整数全体は加法に関して群か？

5

整数全体は乗法に関して群か？

6

部分群

群Gの空でない部分集合をHとする．
HがGの部分群であるための必要十分条件は
Hが次の条件(1)と(2)を満足していることである．
(1)$\forall a,b\in H \Rightarrow a\circ b\in H$
(2)$\forall a\in H \Rightarrow a^{-1}\in H$
さらに(1),(2)は，次の条件(3)と同値である．
(3)$\forall a,b\in H \Rightarrow a\circ b^{-1}\in H$

7

既約剰余類の部分群

$Z_6^{\times}=\{1,5\}$

×	1	5
1	1	5
5	5	1

自明な部分群
単位元のみの部分群$\{1\}$
全体集合$\{1,5\}$

$\{1\},\{1,5\}$　ともに正規部分群

8

既約剰余類の部分群

$Z_9^{\times}=\{1,2,4,5,7,8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

自明な部分群
$\{1\},\{1,2,4,5,7,8\}$
生成元は2と5
4からは{4,7,1}
7からは{7,4,1}
8からは{8,1}

すべて正規部分群

9

既約剰余類の部分群

$Z_{12}^{\times}=\{1,5,7,11\}$

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

自明な部分群
$\{1\},\{1,5,7,11\}$
5からは{5,1}
7からは{7,1}
11からは{11,1}
既約剰余類は乗法において可換
すべて正規部分群

10

巡回群

aの累乗の全体からなるGの部分集合
$<a>=\{a^n \mid n\in Z\}$はGの部分群になる．
また，この群はaを含むGの最小の部分群である．
部分群$<a>$をaで生成されたGの巡回部分群という．

Gをaによって生成される位数nの巡回群とする．
このとき，Gの元a^kの位数は$n/(n,k)$となる．
ただし,(n,k)はnとkの最大公約数を表す．
$|a^k|=n/(n,k)$

11

位数

群Gの元aに対して，$a^n=e$となるような
最小の正の整数をaの位数という．そのような
整数が無いとき，aの位数は無限という．
$|a|$でaの位数を表す．aの位数が無限のとき，
$|a|=\infty$

例題　加法群Z_{12}において，各元の位数を求めよ

$|0|=1,|1|=12,|2|=6,|3|=4,|4|=3,$
$|5|=12,\{5,10,3,8,1,6,11,4,9,2,7,0\}$
$|6|=2,|7|=12,|8|=3,|9|=4,|10|=5,|11|=12$

12

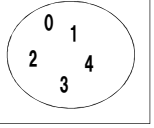
０６．群の定義

代数Ⅰ

代数系

集合　＋　代数的構造　＝　代数系

何かしらの数の集まり



四則演算などの
公理や定義

任意の演算

a＊b＝｜a－b｜

亜群
半群
モノイド
群

環
体

2

群

・空でない集合Gに対して，ある演算＊が定義

（１）閉鎖律

（２）結合律　$(x*y)*z = x*(y*z)$

（３）単位元 e の存在　$e*x = x*e = x$

（４）逆元 x' の存在　$x'*x = x*x' = e$

（５）可換律　$x*y = y*x$

可換群

位数n　$|G| = n$

亜群，半群，モノイド，群

閉鎖律（ある演算に関して閉じている）

集合Ｓは演算＊に関して亜群（groupid）

結合律（　（ｘ＊ｙ）＊ｚ＝ｘ＊（ｙ＊ｚ）　）

半群（semi-group）

単位元（　ｅ＊ｘ＝ｘ＊ｅ=ｘ　）

モノイド（monoid）

逆元（　ｘ’＊ｘ＝ｘ＊ｘ’=ｅ　）

群（group）

4

整数全体は加法に関して群か？

5

整数全体は乗法に関して群か？

6

部分群

群Gの空でない部分集合をHとする．
HがGの部分群であるための必要十分条件は
Hが次の条件(1)と(2)を満足していることである．
(1)$\forall a,b\in H \Rightarrow a\circ b\in H$
(2)$\forall a\in H \Rightarrow a^{-1}\in H$
さらに(1),(2)は，次の条件(3)と同値である．
(3)$\forall a,b\in H \Rightarrow a\circ b^{-1}\in H$

7

既約剰余類の部分群

$Z_6^{\times}=\{1,5\}$

×	1	5
1	1	5
5	5	1

自明な部分群
単位元のみの部分群$\{1\}$
全体集合$\{1,5\}$

$\{1\},\{1,5\}$　ともに正規部分群

8

既約剰余類の部分群

$Z_9^{\times}=\{1,2,4,5,7,8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

自明な部分群
$\{1\},\{1,2,4,5,7,8\}$
生成元は2と5
4からは{4,7,1}
7からは{7,4,1}
8からは{8,1}

すべて正規部分群

9

既約剰余類の部分群

$Z_{12}^{\times}=\{1,5,7,11\}$

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

自明な部分群
$\{1\},\{1,5,7,11\}$
5からは{5,1}
7からは{7,1}
11からは{11,1}
既約剰余類は乗法において可換
すべて正規部分群

10

巡回群

aの累乗の全体からなるGの部分集合
$<a>=\{a^n \mid n\in Z\}$はGの部分群になる．
また，この群はaを含むGの最小の部分群である．
部分群$<a>$をaで生成されたGの巡回部分群という．

Gをaによって生成される位数nの巡回群とする．
このとき，Gの元a^kの位数は$n/(n,k)$となる．
ただし,(n,k)はnとkの最大公約数を表す．
$|a^k|=n/(n,k)$

11

位数

群Gの元aに対して，$a^n=e$となるような
最小の正の整数をaの位数という．そのような
整数が無いとき，aの位数は無限という．
$|a|$でaの位数を表す．aの位数が無限のとき，
$|a|=\infty$

例題　加法群Z_{12}において，各元の位数を求めよ

$|0|=1,|1|=12,|2|=6,|3|=4,|4|=3,$
$|5|=12,\{5,10,3,8,1,6,11,4,9,2,7,0\}$
$|6|=2,|7|=12,|8|=3,|9|=4,|10|=5,|11|=12$

12

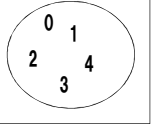
０６．群の定義

代数Ⅰ

代数系

集合　＋　代数的構造　＝　代数系

何かしらの数の集まり



四則演算などの
公理や定義

任意の演算

a＊b＝｜a－b｜

亜群
半群
モノイド
群

環
体

2

群

・空でない集合Gに対して，ある演算＊が定義

（１）閉鎖律

（２）結合律　$(x*y)*z = x*(y*z)$

（３）単位元 e の存在　$e*x = x*e = x$

（４）逆元 x' の存在　$x'*x = x*x' = e$

（５）可換律　$x*y = y*x$

可換群

位数n　$|G| = n$

亜群，半群，モノイド，群

閉鎖律（ある演算に関して閉じている）

集合Ｓは演算＊に関して亜群（groupid）

結合律（　（ｘ＊ｙ）＊ｚ＝ｘ＊（ｙ＊ｚ）　）

半群（semi-group）

単位元（　ｅ＊ｘ＝ｘ＊ｅ=ｘ　）

モノイド（monoid）

逆元（　ｘ’＊ｘ＝ｘ＊ｘ’=ｅ　）

群（group）

4

整数全体は加法に関して群か？

5

整数全体は乗法に関して群か？

6

部分群

群Gの空でない部分集合をHとする．
HがGの部分群であるための必要十分条件は
Hが次の条件(1)と(2)を満足していることである．
(1)$\forall a,b\in H \Rightarrow a\circ b\in H$
(2)$\forall a\in H \Rightarrow a^{-1}\in H$
さらに(1),(2)は，次の条件(3)と同値である．
(3)$\forall a,b\in H \Rightarrow a\circ b^{-1}\in H$

7

既約剰余類の部分群

$Z_6^{\times}=\{1,5\}$

×	1	5
1	1	5
5	5	1

自明な部分群
単位元のみの部分群$\{1\}$
全体集合$\{1,5\}$

$\{1\},\{1,5\}$　ともに正規部分群

8

既約剰余類の部分群

$Z_9^{\times}=\{1,2,4,5,7,8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

自明な部分群
$\{1\},\{1,2,4,5,7,8\}$
生成元は2と5
4からは{4,7,1}
7からは{7,4,1}
8からは{8,1}

すべて正規部分群

9

既約剰余類の部分群

$Z_{12}^{\times}=\{1,5,7,11\}$

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

自明な部分群
$\{1\},\{1,5,7,11\}$
5からは{5,1}
7からは{7,1}
11からは{11,1}
既約剰余類は乗法において可換
すべて正規部分群

10

巡回群

aの累乗の全体からなるGの部分集合
$<a>=\{a^n \mid n\in Z\}$はGの部分群になる．
また，この群はaを含むGの最小の部分群である．
部分群$<a>$をaで生成されたGの巡回部分群という．

Gをaによって生成される位数nの巡回群とする．
このとき，Gの元a^kの位数は$n/(n,k)$となる．
ただし,(n,k)はnとkの最大公約数を表す．
$|a^k|=n/(n,k)$

11

位数

群Gの元aに対して，$a^n=e$となるような
最小の正の整数をaの位数という．そのような
整数が無いとき，aの位数は無限という．
$|a|$でaの位数を表す．aの位数が無限のとき，
$|a|=\infty$

例題　加法群Z_{12}において，各元の位数を求めよ

$|0|=1,|1|=12,|2|=6,|3|=4,|4|=3,$
$|5|=12,\{5,10,3,8,1,6,11,4,9,2,7,0\}$
$|6|=2,|7|=12,|8|=3,|9|=4,|10|=5,|11|=12$

12

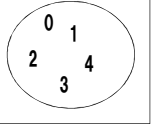
０６．群の定義

代数Ⅰ

代数系

集合　＋　代数的構造　＝　代数系

何かしらの数の集まり



四則演算などの
公理や定義

任意の演算

a＊b＝｜a－b｜

亜群
半群
モノイド
群

環
体

2

群

・空でない集合Gに対して，ある演算＊が定義

（１）閉鎖律

（２）結合律　$(x*y)*z = x*(y*z)$

（３）単位元 e の存在　$e*x = x*e = x$

（４）逆元 x' の存在　$x'*x = x*x' = e$

（５）可換律　$x*y = y*x$

可換群

位数n　$|G| = n$

亜群，半群，モノイド，群

閉鎖律（ある演算に関して閉じている）

集合Ｓは演算＊に関して亜群（groupid）

結合律（　（ｘ＊ｙ）＊ｚ＝ｘ＊（ｙ＊ｚ）　）

半群（semi-group）

単位元（　ｅ＊ｘ＝ｘ＊ｅ=ｘ　）

モノイド（monoid）

逆元（　ｘ’＊ｘ＝ｘ＊ｘ’=ｅ　）

群（group）

4

整数全体は加法に関して群か？

5

整数全体は乗法に関して群か？

6

部分群

群Gの空でない部分集合をHとする．
HがGの部分群であるための必要十分条件は
Hが次の条件(1)と(2)を満足していることである．
(1)$\forall a,b\in H \Rightarrow a\circ b\in H$
(2)$\forall a\in H \Rightarrow a^{-1}\in H$
さらに(1),(2)は，次の条件(3)と同値である．
(3)$\forall a,b\in H \Rightarrow a\circ b^{-1}\in H$

7

既約剰余類の部分群

$Z_6^{\times}=\{1,5\}$

×	1	5
1	1	5
5	5	1

自明な部分群
単位元のみの部分群$\{1\}$
全体集合$\{1,5\}$

$\{1\},\{1,5\}$　ともに正規部分群

8

既約剰余類の部分群

$Z_9^{\times}=\{1,2,4,5,7,8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

自明な部分群
$\{1\},\{1,2,4,5,7,8\}$
生成元は2と5
4からは{4,7,1}
7からは{7,4,1}
8からは{8,1}

すべて正規部分群

9

既約剰余類の部分群

$Z_{12}^{\times}=\{1,5,7,11\}$

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

自明な部分群
$\{1\},\{1,5,7,11\}$
5からは{5,1}
7からは{7,1}
11からは{11,1}
既約剰余類は乗法において可換
すべて正規部分群

10

巡回群

aの累乗の全体からなるGの部分集合
$<a>=\{a^n \mid n\in Z\}$はGの部分群になる．
また，この群はaを含むGの最小の部分群である．
部分群$<a>$をaで生成されたGの巡回部分群という．

Gをaによって生成される位数nの巡回群とする．
このとき，Gの元a^kの位数は$n/(n,k)$となる．
ただし,(n,k)はnとkの最大公約数を表す．
$|a^k|=n/(n,k)$

11

位数

群Gの元aに対して，$a^n=e$となるような
最小の正の整数をaの位数という．そのような
整数が無いとき，aの位数は無限という．
$|a|$でaの位数を表す．aの位数が無限のとき，
$|a|=\infty$

例題　加法群Z_{12}において，各元の位数を求めよ

$|0|=1,|1|=12,|2|=6,|3|=4,|4|=3,$
$|5|=12,\{5,10,3,8,1,6,11,4,9,2,7,0\}$
$|6|=2,|7|=12,|8|=3,|9|=4,|10|=5,|11|=12$

12

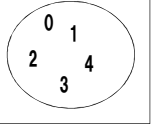
０６．群の定義

代数Ⅰ

代数系

集合　＋　代数的構造　＝　代数系

何かしらの数の集まり



四則演算などの
公理や定義

任意の演算

a＊b＝｜a－b｜

亜群
半群
モノイド
群

環
体

2

群

・空でない集合Gに対して，ある演算＊が定義

（１）閉鎖律

（２）結合律　$(x*y)*z = x*(y*z)$

（３）単位元 e の存在　$e*x = x*e = x$

（４）逆元 x' の存在　$x'*x = x*x' = e$

（５）可換律　$x*y = y*x$

可換群

位数n　$|G| = n$

亜群，半群，モノイド，群

閉鎖律（ある演算に関して閉じている）

集合Ｓは演算＊に関して亜群（groupid）

結合律（　（ｘ＊ｙ）＊ｚ＝ｘ＊（ｙ＊ｚ）　）

半群（semi-group）

単位元（　ｅ＊ｘ＝ｘ＊ｅ=ｘ　）

モノイド（monoid）

逆元（　ｘ’＊ｘ＝ｘ＊ｘ’=ｅ　）

群（group）

4

整数全体は加法に関して群か？

5

整数全体は乗法に関して群か？

6

部分群

群Gの空でない部分集合をHとする．
HがGの部分群であるための必要十分条件は
Hが次の条件(1)と(2)を満足していることである．
(1)$\forall a,b\in H \Rightarrow a\circ b\in H$
(2)$\forall a\in H \Rightarrow a^{-1}\in H$
さらに(1),(2)は，次の条件(3)と同値である．
(3)$\forall a,b\in H \Rightarrow a\circ b^{-1}\in H$

7

既約剰余類の部分群

$Z_6^{\times}=\{1,5\}$

×	1	5
1	1	5
5	5	1

自明な部分群
単位元のみの部分群$\{1\}$
全体集合$\{1,5\}$

$\{1\},\{1,5\}$　ともに正規部分群

8

既約剰余類の部分群

$Z_9^{\times}=\{1,2,4,5,7,8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

自明な部分群
$\{1\},\{1,2,4,5,7,8\}$
生成元は2と5
4からは{4,7,1}
7からは{7,4,1}
8からは{8,1}

すべて正規部分群

9

既約剰余類の部分群

$Z_{12}^{\times}=\{1,5,7,11\}$

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

自明な部分群
$\{1\},\{1,5,7,11\}$
5からは{5,1}
7からは{7,1}
11からは{11,1}
既約剰余類は乗法において可換
すべて正規部分群

10

巡回群

aの累乗の全体からなるGの部分集合
$<a>=\{a^n \mid n\in Z\}$はGの部分群になる．
また，この群はaを含むGの最小の部分群である．
部分群$<a>$をaで生成されたGの巡回部分群という．

Gをaによって生成される位数nの巡回群とする．
このとき，Gの元a^kの位数は$n/(n,k)$となる．
ただし,(n,k)はnとkの最大公約数を表す．
$|a^k|=n/(n,k)$

11

位数

群Gの元aに対して，$a^n=e$となるような
最小の正の整数をaの位数という．そのような
整数が無いとき，aの位数は無限という．
$|a|$でaの位数を表す．aの位数が無限のとき，
$|a|=\infty$

例題　加法群Z_{12}において，各元の位数を求めよ

$|0|=1,|1|=12,|2|=6,|3|=4,|4|=3,$
$|5|=12,\{5,10,3,8,1,6,11,4,9,2,7,0\}$
$|6|=2,|7|=12,|8|=3,|9|=4,|10|=5,|11|=12$

12

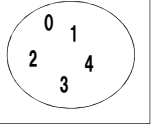
０６．群の定義

代数Ⅰ

代数系

集合　＋　代数的構造　＝　代数系

何かしらの数の集まり



四則演算などの
公理や定義

任意の演算

a＊b＝｜a－b｜

亜群
半群
モノイド
群

環
体

2

群

・空でない集合Gに対して，ある演算＊が定義

（１）閉鎖律

（２）結合律　$(x*y)*z = x*(y*z)$

（３）単位元 e の存在　$e*x = x*e = x$

（４）逆元 x' の存在　$x'*x = x*x' = e$

（５）可換律　$x*y = y*x$

可換群

位数n　$|G| = n$

亜群，半群，モノイド，群

閉鎖律（ある演算に関して閉じている）

集合Ｓは演算＊に関して亜群（groupid）

結合律（　（ｘ＊ｙ）＊ｚ＝ｘ＊（ｙ＊ｚ）　）

半群（semi-group）

単位元（　ｅ＊ｘ＝ｘ＊ｅ=ｘ　）

モノイド（monoid）

逆元（　ｘ’＊ｘ＝ｘ＊ｘ’=ｅ　）

群（group）

4

整数全体は加法に関して群か？

5

整数全体は乗法に関して群か？

6

部分群

群Gの空でない部分集合をHとする．
HがGの部分群であるための必要十分条件は
Hが次の条件(1)と(2)を満足していることである．
(1)$\forall a,b\in H \Rightarrow a\circ b\in H$
(2)$\forall a\in H \Rightarrow a^{-1}\in H$
さらに(1),(2)は，次の条件(3)と同値である．
(3)$\forall a,b\in H \Rightarrow a\circ b^{-1}\in H$

7

既約剰余類の部分群

$Z_6^{\times}=\{1,5\}$

×	1	5
1	1	5
5	5	1

自明な部分群
単位元のみの部分群$\{1\}$
全体集合$\{1,5\}$

$\{1\},\{1,5\}$　ともに正規部分群

8

既約剰余類の部分群

$Z_9^{\times}=\{1,2,4,5,7,8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

自明な部分群
$\{1\},\{1,2,4,5,7,8\}$
生成元は2と5
4からは{4,7,1}
7からは{7,4,1}
8からは{8,1}

すべて正規部分群

9

既約剰余類の部分群

$Z_{12}^{\times}=\{1,5,7,11\}$

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

自明な部分群
$\{1\},\{1,5,7,11\}$
5からは{5,1}
7からは{7,1}
11からは{11,1}
既約剰余類は乗法において可換
すべて正規部分群

10

巡回群

aの累乗の全体からなるGの部分集合
$<a>=\{a^n \mid n\in Z\}$はGの部分群になる．
また，この群はaを含むGの最小の部分群である．
部分群$<a>$をaで生成されたGの巡回部分群という．

Gをaによって生成される位数nの巡回群とする．
このとき，Gの元a^kの位数は$n/(n,k)$となる．
ただし,(n,k)はnとkの最大公約数を表す．
$|a^k|=n/(n,k)$

11

位数

群Gの元aに対して，$a^n=e$となるような
最小の正の整数をaの位数という．そのような
整数が無いとき，aの位数は無限という．
$|a|$でaの位数を表す．aの位数が無限のとき，
$|a|=\infty$

例題　加法群Z_{12}において，各元の位数を求めよ

$|0|=1,|1|=12,|2|=6,|3|=4,|4|=3,$
$|5|=12,\{5,10,3,8,1,6,11,4,9,2,7,0\}$
$|6|=2,|7|=12,|8|=3,|9|=4,|10|=5,|11|=12$

12

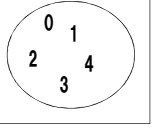
０６．群の定義

代数Ⅰ

代数系

集合　＋　代数的構造　＝　代数系

何かしらの数の集まり



四則演算などの
公理や定義

任意の演算

a＊b＝｜a－b｜

亜群
半群
モノイド
群

環
体

2

群

・空でない集合Gに対して，ある演算＊が定義

（１）閉鎖律

（２）結合律　$(x*y)*z = x*(y*z)$

（３）単位元 e の存在　$e*x = x*e = x$

（４）逆元 x' の存在　$x'*x = x*x' = e$

（５）可換律　$x*y = y*x$

可換群

位数n　$|G| = n$

亜群，半群，モノイド，群

閉鎖律（ある演算に関して閉じている）

集合Ｓは演算＊に関して亜群（groupid）

結合律（　（ｘ＊ｙ）＊ｚ＝ｘ＊（ｙ＊ｚ）　）

半群（semi-group）

単位元（　ｅ＊ｘ＝ｘ＊ｅ=ｘ　）

モノイド（monoid）

逆元（　ｘ’＊ｘ＝ｘ＊ｘ’=ｅ　）

群（group）

4

整数全体は加法に関して群か？

5

整数全体は乗法に関して群か？

6

部分群

群Gの空でない部分集合をHとする．
HがGの部分群であるための必要十分条件は
Hが次の条件(1)と(2)を満足していることである．
(1)$\forall a,b\in H \Rightarrow a\circ b\in H$
(2)$\forall a\in H \Rightarrow a^{-1}\in H$
さらに(1),(2)は，次の条件(3)と同値である．
(3)$\forall a,b\in H \Rightarrow a\circ b^{-1}\in H$

7

既約剰余類の部分群

$Z_6^{\times}=\{1,5\}$

×	1	5
1	1	5
5	5	1

自明な部分群
単位元のみの部分群$\{1\}$
全体集合$\{1,5\}$

$\{1\},\{1,5\}$　ともに正規部分群

8

既約剰余類の部分群

$Z_9^{\times}=\{1,2,4,5,7,8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

自明な部分群
$\{1\},\{1,2,4,5,7,8\}$
生成元は2と5
4からは{4,7,1}
7からは{7,4,1}
8からは{8,1}

すべて正規部分群

9

既約剰余類の部分群

$Z_{12}^{\times}=\{1,5,7,11\}$

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

自明な部分群
$\{1\},\{1,5,7,11\}$
5からは{5,1}
7からは{7,1}
11からは{11,1}
既約剰余類は乗法において可換
すべて正規部分群

10

巡回群

aの累乗の全体からなるGの部分集合
$<a>=\{a^n \mid n\in Z\}$はGの部分群になる．
また，この群はaを含むGの最小の部分群である．
部分群$<a>$をaで生成されたGの巡回部分群という．

Gをaによって生成される位数nの巡回群とする．
このとき，Gの元a^kの位数は$n/(n,k)$となる．
ただし,(n,k)はnとkの最大公約数を表す．
$|a^k|=n/(n,k)$

11

位数

群Gの元aに対して，$a^n=e$となるような
最小の正の整数をaの位数という．そのような
整数が無いとき，aの位数は無限という．
$|a|$でaの位数を表す．aの位数が無限のとき，
$|a|=\infty$

例題　加法群Z_{12}において，各元の位数を求めよ

$|0|=1,|1|=12,|2|=6,|3|=4,|4|=3,$
$|5|=12,\{5,10,3,8,1,6,11,4,9,2,7,0\}$
$|6|=2,|7|=12,|8|=3,|9|=4,|10|=5,|11|=12$

12

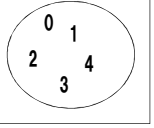
０６．群の定義

代数Ⅰ

代数系

集合　＋　代数的構造　＝　代数系

何かしらの数の集まり



四則演算などの
公理や定義

任意の演算

a＊b＝｜a－b｜

亜群
半群
モノイド
群

環
体

2

群

・空でない集合Gに対して，ある演算＊が定義

（１）閉鎖律

（２）結合律　$(x*y)*z = x*(y*z)$

（３）単位元 e の存在　$e*x = x*e = x$

（４）逆元 x' の存在　$x'*x = x*x' = e$

（５）可換律　$x*y = y*x$

可換群

位数n　$|G| = n$

亜群，半群，モノイド，群

閉鎖律（ある演算に関して閉じている）

集合Ｓは演算＊に関して亜群（groupid）

結合律（　（ｘ＊ｙ）＊ｚ＝ｘ＊（ｙ＊ｚ）　）

半群（semi-group）

単位元（　ｅ＊ｘ＝ｘ＊ｅ=ｘ　）

モノイド（monoid）

逆元（　ｘ’＊ｘ＝ｘ＊ｘ’=ｅ　）

群（group）

4

整数全体は加法に関して群か？

5

整数全体は乗法に関して群か？

6

部分群

群Gの空でない部分集合をHとする．
HがGの部分群であるための必要十分条件は
Hが次の条件(1)と(2)を満足していることである．
(1)$\forall a,b\in H \Rightarrow a\circ b\in H$
(2)$\forall a\in H \Rightarrow a^{-1}\in H$
さらに(1),(2)は，次の条件(3)と同値である．
(3)$\forall a,b\in H \Rightarrow a\circ b^{-1}\in H$

7

既約剰余類の部分群

$Z_6^{\times}=\{1,5\}$

×	1	5
1	1	5
5	5	1

自明な部分群
単位元のみの部分群$\{1\}$
全体集合$\{1,5\}$

$\{1\},\{1,5\}$　ともに正規部分群

8

既約剰余類の部分群

$Z_9^{\times}=\{1,2,4,5,7,8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

自明な部分群
$\{1\},\{1,2,4,5,7,8\}$
生成元は2と5
4からは{4,7,1}
7からは{7,4,1}
8からは{8,1}

すべて正規部分群

9

既約剰余類の部分群

$Z_{12}^{\times}=\{1,5,7,11\}$

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

自明な部分群
$\{1\},\{1,5,7,11\}$
5からは{5,1}
7からは{7,1}
11からは{11,1}
既約剰余類は乗法において可換
すべて正規部分群

10

巡回群

aの累乗の全体からなるGの部分集合
$<a>=\{a^n \mid n\in Z\}$はGの部分群になる．
また，この群はaを含むGの最小の部分群である．
部分群$<a>$をaで生成されたGの巡回部分群という．

Gをaによって生成される位数nの巡回群とする．
このとき，Gの元a^kの位数は$n/(n,k)$となる．
ただし,(n,k)はnとkの最大公約数を表す．
$|a^k|=n/(n,k)$

11

位数

群Gの元aに対して，$a^n=e$となるような
最小の正の整数をaの位数という．そのような
整数が無いとき，aの位数は無限という．
$|a|$でaの位数を表す．aの位数が無限のとき，
$|a|=\infty$

例題　加法群Z_{12}において，各元の位数を求めよ

$|0|=1,|1|=12,|2|=6,|3|=4,|4|=3,$
$|5|=12,\{5,10,3,8,1,6,11,4,9,2,7,0\}$
$|6|=2,|7|=12,|8|=3,|9|=4,|10|=5,|11|=12$

12

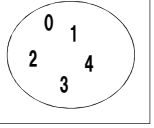
０６．群の定義

代数Ⅰ

代数系

集合　＋　代数的構造　＝　代数系

何かしらの数の集まり



四則演算などの
公理や定義

任意の演算

a＊b＝｜a－b｜

亜群
半群
モノイド
群

環
体

2

群

・空でない集合Gに対して，ある演算＊が定義

（１）閉鎖律

（２）結合律　$(x*y)*z = x*(y*z)$

（３）単位元 e の存在　$e*x = x*e = x$

（４）逆元 x' の存在　$x'*x = x*x' = e$

（５）可換律　$x*y = y*x$

可換群

位数n　$|G| = n$

亜群，半群，モノイド，群

閉鎖律（ある演算に関して閉じている）

集合Ｓは演算＊に関して亜群（groupid）

結合律（　（ｘ＊ｙ）＊ｚ＝ｘ＊（ｙ＊ｚ）　）

半群（semi-group）

単位元（　ｅ＊ｘ＝ｘ＊ｅ=ｘ　）

モノイド（monoid）

逆元（　ｘ’＊ｘ＝ｘ＊ｘ’=ｅ　）

群（group）

4

整数全体は加法に関して群か？

5

整数全体は乗法に関して群か？

6

部分群

群Gの空でない部分集合をHとする．
HがGの部分群であるための必要十分条件は
Hが次の条件(1)と(2)を満足していることである．
(1)$\forall a,b\in H \Rightarrow a\circ b\in H$
(2)$\forall a\in H \Rightarrow a^{-1}\in H$
さらに(1),(2)は，次の条件(3)と同値である．
(3)$\forall a,b\in H \Rightarrow a\circ b^{-1}\in H$

7

既約剰余類の部分群

$Z_6^{\times}=\{1,5\}$

×	1	5
1	1	5
5	5	1

自明な部分群
単位元のみの部分群$\{1\}$
全体集合$\{1,5\}$

$\{1\},\{1,5\}$　ともに正規部分群

8

既約剰余類の部分群

$Z_9^{\times}=\{1,2,4,5,7,8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

自明な部分群
$\{1\},\{1,2,4,5,7,8\}$
生成元は2と5
4からは{4,7,1}
7からは{7,4,1}
8からは{8,1}

すべて正規部分群

9

既約剰余類の部分群

$Z_{12}^{\times}=\{1,5,7,11\}$

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

自明な部分群
$\{1\},\{1,5,7,11\}$
5からは{5,1}
7からは{7,1}
11からは{11,1}
既約剰余類は乗法において可換
すべて正規部分群

10

巡回群

aの累乗の全体からなるGの部分集合
$<a>=\{a^n \mid n\in Z\}$はGの部分群になる．
また，この群はaを含むGの最小の部分群である．
部分群$<a>$をaで生成されたGの巡回部分群という．

Gをaによって生成される位数nの巡回群とする．
このとき，Gの元a^kの位数は$n/(n,k)$となる．
ただし,(n,k)はnとkの最大公約数を表す．
$|a^k|=n/(n,k)$

11

位数

群Gの元aに対して，$a^n=e$となるような
最小の正の整数をaの位数という．そのような
整数が無いとき，aの位数は無限という．
$|a|$でaの位数を表す．aの位数が無限のとき，
$|a|=\infty$

例題　加法群Z_{12}において，各元の位数を求めよ

$|0|=1,|1|=12,|2|=6,|3|=4,|4|=3,$
$|5|=12,\{5,10,3,8,1,6,11,4,9,2,7,0\}$
$|6|=2,|7|=12,|8|=3,|9|=4,|10|=5,|11|=12$

12

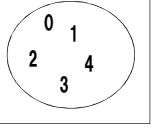
０６．群の定義

代数Ⅰ

代数系

集合　＋　代数的構造　＝　代数系

何かしらの数の集まり



四則演算などの
公理や定義

任意の演算

a＊b＝｜a－b｜

亜群
半群
モノイド
群

環
体

2

群

・空でない集合Gに対して，ある演算＊が定義

（１）閉鎖律

（２）結合律　$(x*y)*z = x*(y*z)$

（３）単位元 e の存在　$e*x = x*e = x$

（４）逆元 x' の存在　$x'*x = x*x' = e$

（５）可換律　$x*y = y*x$

可換群

位数n　$|G| = n$

亜群，半群，モノイド，群

閉鎖律（ある演算に関して閉じている）

集合Ｓは演算＊に関して亜群（groupid）

結合律（　（ｘ＊ｙ）＊ｚ＝ｘ＊（ｙ＊ｚ）　）

半群（semi-group）

単位元（　ｅ＊ｘ＝ｘ＊ｅ=ｘ　）

モノイド（monoid）

逆元（　ｘ’＊ｘ＝ｘ＊ｘ’=ｅ　）

群（group）

4

整数全体は加法に関して群か？

5

整数全体は乗法に関して群か？

6

部分群

群Gの空でない部分集合をHとする．
HがGの部分群であるための必要十分条件は
Hが次の条件(1)と(2)を満足していることである．
(1)$\forall a,b\in H \Rightarrow a\circ b\in H$
(2)$\forall a\in H \Rightarrow a^{-1}\in H$
さらに(1),(2)は，次の条件(3)と同値である．
(3)$\forall a,b\in H \Rightarrow a\circ b^{-1}\in H$

7

既約剰余類の部分群

$Z_6^{\times}=\{1,5\}$

×	1	5
1	1	5
5	5	1

自明な部分群
単位元のみの部分群$\{1\}$
全体集合$\{1,5\}$

$\{1\},\{1,5\}$　ともに正規部分群

8

既約剰余類の部分群

$Z_9^{\times}=\{1,2,4,5,7,8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

自明な部分群
$\{1\},\{1,2,4,5,7,8\}$
生成元は2と5
4からは{4,7,1}
7からは{7,4,1}
8からは{8,1}

すべて正規部分群

9

既約剰余類の部分群

$Z_{12}^{\times}=\{1,5,7,11\}$

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

自明な部分群
$\{1\},\{1,5,7,11\}$
5からは{5,1}
7からは{7,1}
11からは{11,1}
既約剰余類は乗法において可換
すべて正規部分群

10

巡回群

aの累乗の全体からなるGの部分集合
$<a>=\{a^n \mid n\in Z\}$はGの部分群になる．
また，この群はaを含むGの最小の部分群である．
部分群$<a>$をaで生成されたGの巡回部分群という．

Gをaによって生成される位数nの巡回群とする．
このとき，Gの元a^kの位数は$n/(n,k)$となる．
ただし,(n,k)はnとkの最大公約数を表す．
$|a^k|=n/(n,k)$

11

位数

群Gの元aに対して，$a^n=e$となるような
最小の正の整数をaの位数という．そのような
整数が無いとき，aの位数は無限という．
$|a|$でaの位数を表す．aの位数が無限のとき，
$|a|=\infty$

例題　加法群Z_{12}において，各元の位数を求めよ

$|0|=1,|1|=12,|2|=6,|3|=4,|4|=3,$
$|5|=12,\{5,10,3,8,1,6,11,4,9,2,7,0\}$
$|6|=2,|7|=12,|8|=3,|9|=4,|10|=5,|11|=12$

12

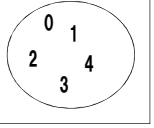
０６．群の定義

代数Ⅰ

代数系

集合　＋　代数的構造　＝　代数系

何かしらの数の集まり



四則演算などの
公理や定義

任意の演算

a＊b＝｜a－b｜

亜群
半群
モノイド
群

環
体

2

群

・空でない集合Gに対して，ある演算＊が定義

（１）閉鎖律

（２）結合律　$(x*y)*z = x*(y*z)$

（３）単位元 e の存在　$e*x = x*e = x$

（４）逆元 x' の存在　$x'*x = x*x' = e$

（５）可換律　$x*y = y*x$

可換群

位数n　$|G| = n$

亜群，半群，モノイド，群

閉鎖律（ある演算に関して閉じている）

集合Ｓは演算＊に関して亜群（groupid）

結合律（　（ｘ＊ｙ）＊ｚ＝ｘ＊（ｙ＊ｚ）　）

半群（semi-group）

単位元（　ｅ＊ｘ＝ｘ＊ｅ=ｘ　）

モノイド（monoid）

逆元（　ｘ’＊ｘ＝ｘ＊ｘ’=ｅ　）

群（group）

4

整数全体は加法に関して群か？

5

整数全体は乗法に関して群か？

6

部分群

群Gの空でない部分集合をHとする．
HがGの部分群であるための必要十分条件は
Hが次の条件(1)と(2)を満足していることである．
(1)$\forall a,b\in H \Rightarrow a\circ b\in H$
(2)$\forall a\in H \Rightarrow a^{-1}\in H$
さらに(1),(2)は，次の条件(3)と同値である．
(3)$\forall a,b\in H \Rightarrow a\circ b^{-1}\in H$

7

既約剰余類の部分群

$Z_6^{\times}=\{1,5\}$

×	1	5
1	1	5
5	5	1

自明な部分群
単位元のみの部分群$\{1\}$
全体集合$\{1,5\}$

$\{1\},\{1,5\}$　ともに正規部分群

8

既約剰余類の部分群

$Z_9^{\times}=\{1,2,4,5,7,8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

自明な部分群
$\{1\},\{1,2,4,5,7,8\}$
生成元は2と5
4からは{4,7,1}
7からは{7,4,1}
8からは{8,1}

すべて正規部分群

9

既約剰余類の部分群

$Z_{12}^{\times}=\{1,5,7,11\}$

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

自明な部分群
$\{1\},\{1,5,7,11\}$
5からは{5,1}
7からは{7,1}
11からは{11,1}
既約剰余類は乗法において可換
すべて正規部分群

10

巡回群

aの累乗の全体からなるGの部分集合
$<a>=\{a^n \mid n\in Z\}$はGの部分群になる．
また，この群はaを含むGの最小の部分群である．
部分群$<a>$をaで生成されたGの巡回部分群という．

Gをaによって生成される位数nの巡回群とする．
このとき，Gの元a^kの位数は$n/(n,k)$となる．
ただし,(n,k)はnとkの最大公約数を表す．
$|a^k|=n/(n,k)$

11

位数

群Gの元aに対して，$a^n=e$となるような
最小の正の整数をaの位数という．そのような
整数が無いとき，aの位数は無限という．
$|a|$でaの位数を表す．aの位数が無限のとき，
$|a|=\infty$

例題　加法群Z_{12}において，各元の位数を求めよ

$|0|=1,|1|=12,|2|=6,|3|=4,|4|=3,$
$|5|=12,\{5,10,3,8,1,6,11,4,9,2,7,0\}$
$|6|=2,|7|=12,|8|=3,|9|=4,|10|=5,|11|=12$

12

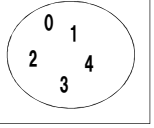
０６．群の定義

代数Ⅰ

代数系

集合　＋　代数的構造　＝　代数系

何かしらの数の集まり



四則演算などの
公理や定義

任意の演算

a＊b＝｜a－b｜

亜群
半群
モノイド
群

環
体

2

群

・空でない集合Gに対して，ある演算＊が定義

（１）閉鎖律

（２）結合律　$(x*y)*z = x*(y*z)$

（３）単位元 e の存在　$e*x = x*e = x$

（４）逆元 x' の存在　$x'*x = x*x' = e$

（５）可換律　$x*y = y*x$

可換群

位数n　$|G| = n$

亜群，半群，モノイド，群

閉鎖律（ある演算に関して閉じている）

集合Ｓは演算＊に関して亜群（groupid）

結合律（　（ｘ＊ｙ）＊ｚ＝ｘ＊（ｙ＊ｚ）　）

半群（semi-group）

単位元（　ｅ＊ｘ＝ｘ＊ｅ=ｘ　）

モノイド（monoid）

逆元（　ｘ’＊ｘ＝ｘ＊ｘ’=ｅ　）

群（group）

4

整数全体は加法に関して群か？

5

整数全体は乗法に関して群か？

6

部分群

群Gの空でない部分集合をHとする．
HがGの部分群であるための必要十分条件は
Hが次の条件(1)と(2)を満足していることである．
(1)$\forall a,b\in H \Rightarrow a\circ b\in H$
(2)$\forall a\in H \Rightarrow a^{-1}\in H$
さらに(1),(2)は，次の条件(3)と同値である．
(3)$\forall a,b\in H \Rightarrow a\circ b^{-1}\in H$

7

既約剰余類の部分群

$Z_6^{\times}=\{1,5\}$

×	1	5
1	1	5
5	5	1

自明な部分群
単位元のみの部分群$\{1\}$
全体集合$\{1,5\}$

$\{1\},\{1,5\}$　ともに正規部分群

8

既約剰余類の部分群

$Z_9^{\times}=\{1,2,4,5,7,8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

自明な部分群
$\{1\},\{1,2,4,5,7,8\}$
生成元は2と5
4からは{4,7,1}
7からは{7,4,1}
8からは{8,1}

すべて正規部分群

9

既約剰余類の部分群

$Z_{12}^{\times}=\{1,5,7,11\}$

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

自明な部分群
$\{1\},\{1,5,7,11\}$
5からは{5,1}
7からは{7,1}
11からは{11,1}
既約剰余類は乗法において可換
すべて正規部分群

10

巡回群

aの累乗の全体からなるGの部分集合
$<a>=\{a^n \mid n\in Z\}$はGの部分群になる．
また，この群はaを含むGの最小の部分群である．
部分群$<a>$をaで生成されたGの巡回部分群という．

Gをaによって生成される位数nの巡回群とする．
このとき，Gの元a^kの位数は$n/(n,k)$となる．
ただし,(n,k)はnとkの最大公約数を表す．
$|a^k|=n/(n,k)$

11

位数

群Gの元aに対して，$a^n=e$となるような
最小の正の整数をaの位数という．そのような
整数が無いとき，aの位数は無限という．
$|a|$でaの位数を表す．aの位数が無限のとき，
$|a|=\infty$

例題　加法群Z_{12}において，各元の位数を求めよ

$|0|=1,|1|=12,|2|=6,|3|=4,|4|=3,$
$|5|=12,\{5,10,3,8,1,6,11,4,9,2,7,0\}$
$|6|=2,|7|=12,|8|=3,|9|=4,|10|=5,|11|=12$

12

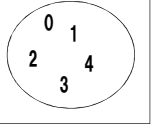
０６．群の定義

代数Ⅰ

代数系

集合　＋　代数的構造　＝　代数系

何かしらの数の集まり



四則演算などの
公理や定義

任意の演算

a＊b＝｜a－b｜

亜群
半群
モノイド
群

環
体

2

群

・空でない集合Gに対して，ある演算＊が定義

（１）閉鎖律

（２）結合律　$(x*y)*z = x*(y*z)$

（３）単位元 e の存在　$e*x = x*e = x$

（４）逆元 x' の存在　$x'*x = x*x' = e$

（５）可換律　$x*y = y*x$

可換群

位数n　$|G| = n$

亜群，半群，モノイド，群

閉鎖律（ある演算に関して閉じている）

集合Ｓは演算＊に関して亜群（groupid）

結合律（　（ｘ＊ｙ）＊ｚ＝ｘ＊（ｙ＊ｚ）　）

半群（semi-group）

単位元（　ｅ＊ｘ＝ｘ＊ｅ=ｘ　）

モノイド（monoid）

逆元（　ｘ’＊ｘ＝ｘ＊ｘ’=ｅ　）

群（group）

4

整数全体は加法に関して群か？

5

整数全体は乗法に関して群か？

6

部分群

群Gの空でない部分集合をHとする．
HがGの部分群であるための必要十分条件は
Hが次の条件(1)と(2)を満足していることである．
(1)$\forall a,b\in H \Rightarrow a\circ b\in H$
(2)$\forall a\in H \Rightarrow a^{-1}\in H$
さらに(1),(2)は，次の条件(3)と同値である．
(3)$\forall a,b\in H \Rightarrow a\circ b^{-1}\in H$

7

既約剰余類の部分群

$Z_6^{\times}=\{1,5\}$

×	1	5
1	1	5
5	5	1

自明な部分群
単位元のみの部分群$\{1\}$
全体集合$\{1,5\}$

$\{1\},\{1,5\}$　ともに正規部分群

8

既約剰余類の部分群

$Z_9^{\times}=\{1,2,4,5,7,8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

自明な部分群
$\{1\},\{1,2,4,5,7,8\}$
生成元は2と5
4からは{4,7,1}
7からは{7,4,1}
8からは{8,1}

すべて正規部分群

9

既約剰余類の部分群

$Z_{12}^{\times}=\{1,5,7,11\}$

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

自明な部分群
$\{1\},\{1,5,7,11\}$
5からは{5,1}
7からは{7,1}
11からは{11,1}
既約剰余類は乗法において可換
すべて正規部分群

10

巡回群

aの累乗の全体からなるGの部分集合
$<a>=\{a^n \mid n\in Z\}$はGの部分群になる．
また，この群はaを含むGの最小の部分群である．
部分群$<a>$をaで生成されたGの巡回部分群という．

Gをaによって生成される位数nの巡回群とする．
このとき，Gの元a^kの位数は$n/(n,k)$となる．
ただし,(n,k)はnとkの最大公約数を表す．
$|a^k|=n/(n,k)$

11

位数

群Gの元aに対して，$a^n=e$となるような
最小の正の整数をaの位数という．そのような
整数が無いとき，aの位数は無限という．
$|a|$でaの位数を表す．aの位数が無限のとき，
$|a|=\infty$

例題　加法群Z_{12}において，各元の位数を求めよ

$|0|=1,|1|=12,|2|=6,|3|=4,|4|=3,$
$|5|=12,\{5,10,3,8,1,6,11,4,9,2,7,0\}$
$|6|=2,|7|=12,|8|=3,|9|=4,|10|=5,|11|=12$

12

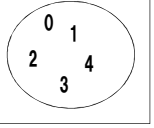
０６．群の定義

代数Ⅰ

代数系

集合　＋　代数的構造　＝　代数系

何かしらの数の集まり



四則演算などの
公理や定義

任意の演算

a＊b＝｜a－b｜

亜群
半群
モノイド
群

環
体

2

群

・空でない集合Gに対して，ある演算＊が定義

（１）閉鎖律

（２）結合律　$(x*y)*z = x*(y*z)$

（３）単位元 e の存在　$e*x = x*e = x$

（４）逆元 x' の存在　$x'*x = x*x' = e$

（５）可換律　$x*y = y*x$

可換群

位数n　$|G| = n$

亜群，半群，モノイド，群

閉鎖律（ある演算に関して閉じている）

集合Ｓは演算＊に関して亜群（groupid）

結合律（　（ｘ＊ｙ）＊ｚ＝ｘ＊（ｙ＊ｚ）　）

半群（semi-group）

単位元（　ｅ＊ｘ＝ｘ＊ｅ=ｘ　）

モノイド（monoid）

逆元（　ｘ’＊ｘ＝ｘ＊ｘ’=ｅ　）

群（group）

4

整数全体は加法に関して群か？

5

整数全体は乗法に関して群か？

6

部分群

群Gの空でない部分集合をHとする．
HがGの部分群であるための必要十分条件は
Hが次の条件(1)と(2)を満足していることである．
(1)$\forall a,b\in H \Rightarrow a\circ b\in H$
(2)$\forall a\in H \Rightarrow a^{-1}\in H$
さらに(1),(2)は，次の条件(3)と同値である．
(3)$\forall a,b\in H \Rightarrow a\circ b^{-1}\in H$

7

既約剰余類の部分群

$Z_6^{\times}=\{1,5\}$

×	1	5
1	1	5
5	5	1

自明な部分群
単位元のみの部分群$\{1\}$
全体集合$\{1,5\}$

$\{1\},\{1,5\}$　ともに正規部分群

8

既約剰余類の部分群

$Z_9^{\times}=\{1,2,4,5,7,8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

自明な部分群
$\{1\},\{1,2,4,5,7,8\}$
生成元は2と5
4からは{4,7,1}
7からは{7,4,1}
8からは{8,1}

すべて正規部分群

9

既約剰余類の部分群

$Z_{12}^{\times}=\{1,5,7,11\}$

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

自明な部分群
$\{1\},\{1,5,7,11\}$
5からは{5,1}
7からは{7,1}
11からは{11,1}
既約剰余類は乗法において可換
すべて正規部分群

10

巡回群

aの累乗の全体からなるGの部分集合
$<a>=\{a^n \mid n\in Z\}$はGの部分群になる．
また，この群はaを含むGの最小の部分群である．
部分群$<a>$をaで生成されたGの巡回部分群という．

Gをaによって生成される位数nの巡回群とする．
このとき，Gの元a^kの位数は$n/(n,k)$となる．
ただし,(n,k)はnとkの最大公約数を表す．
$|a^k|=n/(n,k)$

11

位数

群Gの元aに対して，$a^n=e$となるような
最小の正の整数をaの位数という．そのような
整数が無いとき，aの位数は無限という．
$|a|$でaの位数を表す．aの位数が無限のとき，
$|a|=\infty$

例題　加法群Z_{12}において，各元の位数を求めよ

$|0|=1,|1|=12,|2|=6,|3|=4,|4|=3,$
$|5|=12,\{5,10,3,8,1,6,11,4,9,2,7,0\}$
$|6|=2,|7|=12,|8|=3,|9|=4,|10|=5,|11|=12$

12

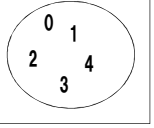
０６．群の定義

代数Ⅰ

代数系

集合　＋　代数的構造　＝　代数系

何かしらの数の集まり



四則演算などの
公理や定義

任意の演算

a＊b＝｜a－b｜

亜群
半群
モノイド
群

環
体

2

群

・空でない集合Gに対して，ある演算＊が定義

（１）閉鎖律

（２）結合律　$(x*y)*z = x*(y*z)$

（３）単位元 e の存在　$e*x = x*e = x$

（４）逆元 x' の存在　$x'*x = x*x' = e$

（５）可換律　$x*y = y*x$

可換群

位数n　$|G| = n$

亜群，半群，モノイド，群

閉鎖律（ある演算に関して閉じている）

集合Ｓは演算＊に関して亜群（groupid）

結合律（　（ｘ＊ｙ）＊ｚ＝ｘ＊（ｙ＊ｚ）　）

半群（semi-group）

単位元（　ｅ＊ｘ＝ｘ＊ｅ=ｘ　）

モノイド（monoid）

逆元（　ｘ’＊ｘ＝ｘ＊ｘ’=ｅ　）

群（group）

4

整数全体は加法に関して群か？

5

整数全体は乗法に関して群か？

6

部分群

群Gの空でない部分集合をHとする．
HがGの部分群であるための必要十分条件は
Hが次の条件(1)と(2)を満足していることである．
(1)$\forall a,b\in H \Rightarrow a\circ b\in H$
(2)$\forall a\in H \Rightarrow a^{-1}\in H$
さらに(1),(2)は，次の条件(3)と同値である．
(3)$\forall a,b\in H \Rightarrow a\circ b^{-1}\in H$

7

既約剰余類の部分群

$Z_6^{\times}=\{1,5\}$

×	1	5
1	1	5
5	5	1

自明な部分群
単位元のみの部分群$\{1\}$
全体集合$\{1,5\}$

$\{1\},\{1,5\}$　ともに正規部分群

8

既約剰余類の部分群

$Z_9^{\times}=\{1,2,4,5,7,8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

自明な部分群
$\{1\},\{1,2,4,5,7,8\}$
生成元は2と5
4からは{4,7,1}
7からは{7,4,1}
8からは{8,1}

すべて正規部分群

9

既約剰余類の部分群

$Z_{12}^{\times}=\{1,5,7,11\}$

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

自明な部分群
$\{1\},\{1,5,7,11\}$
5からは{5,1}
7からは{7,1}
11からは{11,1}
既約剰余類は乗法において可換
すべて正規部分群

10

巡回群

aの累乗の全体からなるGの部分集合
$<a>=\{a^n \mid n\in Z\}$はGの部分群になる．
また，この群はaを含むGの最小の部分群である．
部分群$<a>$をaで生成されたGの巡回部分群という．

Gをaによって生成される位数nの巡回群とする．
このとき，Gの元a^kの位数は$n/(n,k)$となる．
ただし,(n,k)はnとkの最大公約数を表す．
$|a^k|=n/(n,k)$

11

位数

群Gの元aに対して，$a^n=e$となるような
最小の正の整数をaの位数という．そのような
整数が無いとき，aの位数は無限という．
$|a|$でaの位数を表す．aの位数が無限のとき，
$|a|=\infty$

例題　加法群Z_{12}において，各元の位数を求めよ

$|0|=1,|1|=12,|2|=6,|3|=4,|4|=3,$
$|5|=12,\{5,10,3,8,1,6,11,4,9,2,7,0\}$
$|6|=2,|7|=12,|8|=3,|9|=4,|10|=5,|11|=12$

12

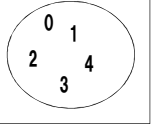
０６．群の定義

代数Ⅰ

代数系

集合　＋　代数的構造　＝　代数系

何かしらの数の集まり



四則演算などの
公理や定義

任意の演算

a＊b＝｜a－b｜

亜群
半群
モノイド
群

環
体

2

群

・空でない集合Gに対して，ある演算＊が定義

（１）閉鎖律

（２）結合律　$(x*y)*z = x*(y*z)$

（３）単位元 e の存在　$e*x = x*e = x$

（４）逆元 x' の存在　$x'*x = x*x' = e$

（５）可換律　$x*y = y*x$

可換群

位数n　$|G| = n$

亜群，半群，モノイド，群

閉鎖律（ある演算に関して閉じている）

集合Ｓは演算＊に関して亜群（groupid）

結合律（　（ｘ＊ｙ）＊ｚ＝ｘ＊（ｙ＊ｚ）　）

半群（semi-group）

単位元（　ｅ＊ｘ＝ｘ＊ｅ=ｘ　）

モノイド（monoid）

逆元（　ｘ’＊ｘ＝ｘ＊ｘ’=ｅ　）

群（group）

4

整数全体は加法に関して群か？

5

整数全体は乗法に関して群か？

6

部分群

群Gの空でない部分集合をHとする．
HがGの部分群であるための必要十分条件は
Hが次の条件(1)と(2)を満足していることである．
(1)$\forall a,b\in H \Rightarrow a\circ b\in H$
(2)$\forall a\in H \Rightarrow a^{-1}\in H$
さらに(1),(2)は，次の条件(3)と同値である．
(3)$\forall a,b\in H \Rightarrow a\circ b^{-1}\in H$

7

既約剰余類の部分群

$Z_6^{\times}=\{1,5\}$

×	1	5
1	1	5
5	5	1

自明な部分群
単位元のみの部分群$\{1\}$
全体集合$\{1,5\}$

$\{1\},\{1,5\}$　ともに正規部分群

8

既約剰余類の部分群

$Z_9^{\times}=\{1,2,4,5,7,8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

自明な部分群
$\{1\},\{1,2,4,5,7,8\}$
生成元は2と5
4からは{4,7,1}
7からは{7,4,1}
8からは{8,1}

すべて正規部分群

9

既約剰余類の部分群

$Z_{12}^{\times}=\{1,5,7,11\}$

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

自明な部分群
$\{1\},\{1,5,7,11\}$
5からは{5,1}
7からは{7,1}
11からは{11,1}
既約剰余類は乗法において可換
すべて正規部分群

10

巡回群

aの累乗の全体からなるGの部分集合
$<a>=\{a^n \mid n\in Z\}$はGの部分群になる．
また，この群はaを含むGの最小の部分群である．
部分群$<a>$をaで生成されたGの巡回部分群という．

Gをaによって生成される位数nの巡回群とする．
このとき，Gの元a^kの位数は$n/(n,k)$となる．
ただし,(n,k)はnとkの最大公約数を表す．
$|a^k|=n/(n,k)$

11

位数

群Gの元aに対して，$a^n=e$となるような
最小の正の整数をaの位数という．そのような
整数が無いとき，aの位数は無限という．
$|a|$でaの位数を表す．aの位数が無限のとき，
$|a|=\infty$

例題　加法群Z_{12}において，各元の位数を求めよ

$|0|=1,|1|=12,|2|=6,|3|=4,|4|=3,$
$|5|=12,\{5,10,3,8,1,6,11,4,9,2,7,0\}$
$|6|=2,|7|=12,|8|=3,|9|=4,|10|=5,|11|=12$

12

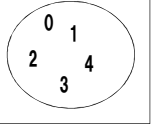
０６．群の定義

代数Ⅰ

代数系

集合　＋　代数的構造　＝　代数系

何かしらの数の集まり



四則演算などの
公理や定義

任意の演算

a＊b＝｜a－b｜

亜群
半群
モノイド
群

環
体

2

群

・空でない集合Gに対して，ある演算＊が定義

（１）閉鎖律

（２）結合律　$(x*y)*z = x*(y*z)$

（３）単位元 e の存在　$e*x = x*e = x$

（４）逆元 x' の存在　$x'*x = x*x' = e$

（５）可換律　$x*y = y*x$

可換群

位数n　$|G| = n$

亜群，半群，モノイド，群

閉鎖律（ある演算に関して閉じている）

集合Ｓは演算＊に関して亜群（groupid）

結合律（　（ｘ＊ｙ）＊ｚ＝ｘ＊（ｙ＊ｚ）　）

半群（semi-group）

単位元（　ｅ＊ｘ＝ｘ＊ｅ=ｘ　）

モノイド（monoid）

逆元（　ｘ’＊ｘ＝ｘ＊ｘ’=ｅ　）

群（group）

4

整数全体は加法に関して群か？

5

整数全体は乗法に関して群か？

6

部分群

群Gの空でない部分集合をHとする．
HがGの部分群であるための必要十分条件は
Hが次の条件(1)と(2)を満足していることである．
(1)$\forall a,b\in H \Rightarrow a\circ b\in H$
(2)$\forall a\in H \Rightarrow a^{-1}\in H$
さらに(1),(2)は，次の条件(3)と同値である．
(3)$\forall a,b\in H \Rightarrow a\circ b^{-1}\in H$

7

既約剰余類の部分群

$Z_6^{\times}=\{1,5\}$

×	1	5
1	1	5
5	5	1

自明な部分群
単位元のみの部分群$\{1\}$
全体集合$\{1,5\}$

$\{1\},\{1,5\}$　ともに正規部分群

8

既約剰余類の部分群

$Z_9^{\times}=\{1,2,4,5,7,8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

自明な部分群
$\{1\},\{1,2,4,5,7,8\}$
生成元は2と5
4からは{4,7,1}
7からは{7,4,1}
8からは{8,1}

すべて正規部分群

9

既約剰余類の部分群

$Z_{12}^{\times}=\{1,5,7,11\}$

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

自明な部分群
$\{1\},\{1,5,7,11\}$
5からは{5,1}
7からは{7,1}
11からは{11,1}
既約剰余類は乗法において可換
すべて正規部分群

10

巡回群

aの累乗の全体からなるGの部分集合
$<a>=\{a^n \mid n\in Z\}$はGの部分群になる．
また，この群はaを含むGの最小の部分群である．
部分群$<a>$をaで生成されたGの巡回部分群という．

Gをaによって生成される位数nの巡回群とする．
このとき，Gの元a^kの位数は$n/(n,k)$となる．
ただし,(n,k)はnとkの最大公約数を表す．
$|a^k|=n/(n,k)$

11

位数

群Gの元aに対して，$a^n=e$となるような
最小の正の整数をaの位数という．そのような
整数が無いとき，aの位数は無限という．
$|a|$でaの位数を表す．aの位数が無限のとき，
$|a|=\infty$

例題　加法群Z_{12}において，各元の位数を求めよ

$|0|=1,|1|=12,|2|=6,|3|=4,|4|=3,$
$|5|=12,\{5,10,3,8,1,6,11,4,9,2,7,0\}$
$|6|=2,|7|=12,|8|=3,|9|=4,|10|=5,|11|=12$

12

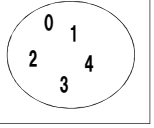
０６．群の定義

代数Ⅰ

代数系

集合　＋　代数的構造　＝　代数系

何かしらの数の集まり



四則演算などの
公理や定義

任意の演算

a＊b＝｜a－b｜

亜群
半群
モノイド
群

環
体

2

群

・空でない集合Gに対して，ある演算＊が定義

（１）閉鎖律

（２）結合律　$(x*y)*z = x*(y*z)$

（３）単位元 e の存在　$e*x = x*e = x$

（４）逆元 x' の存在　$x'*x = x*x' = e$

（５）可換律　$x*y = y*x$

可換群

位数n　$|G| = n$

亜群，半群，モノイド，群

閉鎖律（ある演算に関して閉じている）

集合Ｓは演算＊に関して亜群（groupid）

結合律（　（ｘ＊ｙ）＊ｚ＝ｘ＊（ｙ＊ｚ）　）

半群（semi-group）

単位元（　ｅ＊ｘ＝ｘ＊ｅ=ｘ　）

モノイド（monoid）

逆元（　ｘ’＊ｘ＝ｘ＊ｘ’=ｅ　）

群（group）

4

整数全体は加法に関して群か？

5

整数全体は乗法に関して群か？

6

部分群

群Gの空でない部分集合をHとする．
HがGの部分群であるための必要十分条件は
Hが次の条件(1)と(2)を満足していることである．
(1)$\forall a,b\in H \Rightarrow a\circ b\in H$
(2)$\forall a\in H \Rightarrow a^{-1}\in H$
さらに(1),(2)は，次の条件(3)と同値である．
(3)$\forall a,b\in H \Rightarrow a\circ b^{-1}\in H$

7

既約剰余類の部分群

$Z_6^{\times}=\{1,5\}$

×	1	5
1	1	5
5	5	1

自明な部分群
単位元のみの部分群$\{1\}$
全体集合$\{1,5\}$

$\{1\},\{1,5\}$　ともに正規部分群

8

既約剰余類の部分群

$Z_9^{\times}=\{1,2,4,5,7,8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

自明な部分群
$\{1\},\{1,2,4,5,7,8\}$
生成元は2と5
4からは{4,7,1}
7からは{7,4,1}
8からは{8,1}

すべて正規部分群

9

既約剰余類の部分群

$Z_{12}^{\times}=\{1,5,7,11\}$

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

自明な部分群
$\{1\},\{1,5,7,11\}$
5からは{5,1}
7からは{7,1}
11からは{11,1}
既約剰余類は乗法において可換
すべて正規部分群

10

巡回群

aの累乗の全体からなるGの部分集合
$<a>=\{a^n \mid n\in Z\}$はGの部分群になる．
また，この群はaを含むGの最小の部分群である．
部分群$<a>$をaで生成されたGの巡回部分群という．

Gをaによって生成される位数nの巡回群とする．
このとき，Gの元a^kの位数は$n/(n,k)$となる．
ただし,(n,k)はnとkの最大公約数を表す．
$|a^k|=n/(n,k)$

11

位数

群Gの元aに対して，$a^n=e$となるような
最小の正の整数をaの位数という．そのような
整数が無いとき，aの位数は無限という．
$|a|$でaの位数を表す．aの位数が無限のとき，
$|a|=\infty$

例題　加法群Z_{12}において，各元の位数を求めよ

$|0|=1,|1|=12,|2|=6,|3|=4,|4|=3,$
$|5|=12,\{5,10,3,8,1,6,11,4,9,2,7,0\}$
$|6|=2,|7|=12,|8|=3,|9|=4,|10|=5,|11|=12$

12

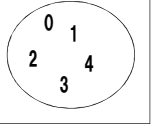
０６．群の定義

代数Ⅰ

代数系

集合　＋　代数的構造　＝　代数系

何かしらの数の集まり



四則演算などの
公理や定義

任意の演算

a＊b＝｜a－b｜

亜群
半群
モノイド
群

環
体

2

群

・空でない集合Gに対して，ある演算＊が定義

（１）閉鎖律

（２）結合律　$(x*y)*z = x*(y*z)$

（３）単位元 e の存在　$e*x = x*e = x$

（４）逆元 x' の存在　$x'*x = x*x' = e$

（５）可換律　$x*y = y*x$

可換群

位数n　$|G| = n$

亜群，半群，モノイド，群

閉鎖律（ある演算に関して閉じている）

集合Ｓは演算＊に関して亜群（groupid）

結合律（　（ｘ＊ｙ）＊ｚ＝ｘ＊（ｙ＊ｚ）　）

半群（semi-group）

単位元（　ｅ＊ｘ＝ｘ＊ｅ=ｘ　）

モノイド（monoid）

逆元（　ｘ’＊ｘ＝ｘ＊ｘ’=ｅ　）

群（group）

4

整数全体は加法に関して群か？

5

整数全体は乗法に関して群か？

6

部分群

群Gの空でない部分集合をHとする．
HがGの部分群であるための必要十分条件は
Hが次の条件(1)と(2)を満足していることである．
(1)$\forall a,b\in H \Rightarrow a\circ b\in H$
(2)$\forall a\in H \Rightarrow a^{-1}\in H$
さらに(1),(2)は，次の条件(3)と同値である．
(3)$\forall a,b\in H \Rightarrow a\circ b^{-1}\in H$

7

既約剰余類の部分群

$Z_6^{\times}=\{1,5\}$

×	1	5
1	1	5
5	5	1

自明な部分群
単位元のみの部分群$\{1\}$
全体集合$\{1,5\}$

$\{1\},\{1,5\}$　ともに正規部分群

8

既約剰余類の部分群

$Z_9^{\times}=\{1,2,4,5,7,8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

自明な部分群
$\{1\},\{1,2,4,5,7,8\}$
生成元は2と5
4からは{4,7,1}
7からは{7,4,1}
8からは{8,1}

すべて正規部分群

9

既約剰余類の部分群

$Z_{12}^{\times}=\{1,5,7,11\}$

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

自明な部分群
$\{1\},\{1,5,7,11\}$
5からは{5,1}
7からは{7,1}
11からは{11,1}
既約剰余類は乗法において可換
すべて正規部分群

10

巡回群

aの累乗の全体からなるGの部分集合
$<a>=\{a^n \mid n\in Z\}$はGの部分群になる．
また，この群はaを含むGの最小の部分群である．
部分群$<a>$をaで生成されたGの巡回部分群という．

Gをaによって生成される位数nの巡回群とする．
このとき，Gの元a^kの位数は$n/(n,k)$となる．
ただし,(n,k)はnとkの最大公約数を表す．
$|a^k|=n/(n,k)$

11

位数

群Gの元aに対して，$a^n=e$となるような
最小の正の整数をaの位数という．そのような
整数が無いとき，aの位数は無限という．
$|a|$でaの位数を表す．aの位数が無限のとき，
$|a|=\infty$

例題　加法群Z_{12}において，各元の位数を求めよ

$|0|=1,|1|=12,|2|=6,|3|=4,|4|=3,$
$|5|=12,\{5,10,3,8,1,6,11,4,9,2,7,0\}$
$|6|=2,|7|=12,|8|=3,|9|=4,|10|=5,|11|=12$

12

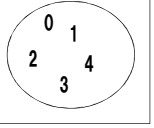
０６．群の定義

代数Ⅰ

代数系

集合　＋　代数的構造　＝　代数系

何かしらの数の集まり



四則演算などの
公理や定義

任意の演算

a＊b＝｜a－b｜

亜群
半群
モノイド
群

環
体

2

群

・空でない集合Gに対して，ある演算＊が定義

（１）閉鎖律

（２）結合律　$(x*y)*z = x*(y*z)$

（３）単位元 e の存在　$e*x = x*e = x$

（４）逆元 x' の存在　$x'*x = x*x' = e$

（５）可換律　$x*y = y*x$

可換群

位数n　$|G| = n$

亜群，半群，モノイド，群

閉鎖律（ある演算に関して閉じている）

集合Ｓは演算＊に関して亜群（groupid）

結合律（　（ｘ＊ｙ）＊ｚ＝ｘ＊（ｙ＊ｚ）　）

半群（semi-group）

単位元（　ｅ＊ｘ＝ｘ＊ｅ=ｘ　）

モノイド（monoid）

逆元（　ｘ’＊ｘ＝ｘ＊ｘ’=ｅ　）

群（group）

4

整数全体は加法に関して群か？

5

整数全体は乗法に関して群か？

6

部分群

群Gの空でない部分集合をHとする．
HがGの部分群であるための必要十分条件は
Hが次の条件(1)と(2)を満足していることである．
(1)$\forall a,b\in H \Rightarrow a\circ b\in H$
(2)$\forall a\in H \Rightarrow a^{-1}\in H$
さらに(1),(2)は，次の条件(3)と同値である．
(3)$\forall a,b\in H \Rightarrow a\circ b^{-1}\in H$

7

既約剰余類の部分群

$Z_6^{\times}=\{1,5\}$

×	1	5
1	1	5
5	5	1

自明な部分群
単位元のみの部分群$\{1\}$
全体集合$\{1,5\}$

$\{1\},\{1,5\}$　ともに正規部分群

8

既約剰余類の部分群

$Z_9^{\times}=\{1,2,4,5,7,8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

自明な部分群
$\{1\},\{1,2,4,5,7,8\}$
生成元は2と5
4からは{4,7,1}
7からは{7,4,1}
8からは{8,1}

すべて正規部分群

9

既約剰余類の部分群

$Z_{12}^{\times}=\{1,5,7,11\}$

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

自明な部分群
$\{1\},\{1,5,7,11\}$
5からは{5,1}
7からは{7,1}
11からは{11,1}
既約剰余類は乗法において可換
すべて正規部分群

10

巡回群

aの累乗の全体からなるGの部分集合
$<a>=\{a^n \mid n\in Z\}$はGの部分群になる．
また，この群はaを含むGの最小の部分群である．
部分群$<a>$をaで生成されたGの巡回部分群という．

Gをaによって生成される位数nの巡回群とする．
このとき，Gの元a^kの位数は$n/(n,k)$となる．
ただし,(n,k)はnとkの最大公約数を表す．
$|a^k|=n/(n,k)$

11

位数

群Gの元aに対して，$a^n=e$となるような
最小の正の整数をaの位数という．そのような
整数が無いとき，aの位数は無限という．
$|a|$でaの位数を表す．aの位数が無限のとき，
$|a|=\infty$

例題　加法群Z_{12}において，各元の位数を求めよ

$|0|=1,|1|=12,|2|=6,|3|=4,|4|=3,$
$|5|=12,\{5,10,3,8,1,6,11,4,9,2,7,0\}$
$|6|=2,|7|=12,|8|=3,|9|=4,|10|=5,|11|=12$

12

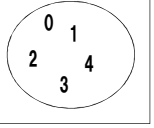
０６．群の定義

代数Ⅰ

代数系

集合　＋　代数的構造　＝　代数系

何かしらの数の集まり



四則演算などの
公理や定義

任意の演算

a＊b＝｜a－b｜

亜群
半群
モノイド
群

環
体

2

群

・空でない集合Gに対して，ある演算＊が定義

（１）閉鎖律

（２）結合律　$(x*y)*z = x*(y*z)$

（３）単位元 e の存在　$e*x = x*e = x$

（４）逆元 x' の存在　$x'*x = x*x' = e$

（５）可換律　$x*y = y*x$

可換群

位数n　$|G| = n$

亜群，半群，モノイド，群

閉鎖律（ある演算に関して閉じている）

集合Ｓは演算＊に関して亜群（groupid）

結合律（　（ｘ＊ｙ）＊ｚ＝ｘ＊（ｙ＊ｚ）　）

半群（semi-group）

単位元（　ｅ＊ｘ＝ｘ＊ｅ=ｘ　）

モノイド（monoid）

逆元（　ｘ’＊ｘ＝ｘ＊ｘ’=ｅ　）

群（group）

4

整数全体は加法に関して群か？

5

整数全体は乗法に関して群か？

6

部分群

群Gの空でない部分集合をHとする．
HがGの部分群であるための必要十分条件は
Hが次の条件(1)と(2)を満足していることである．
(1)$\forall a,b\in H \Rightarrow a\circ b\in H$
(2)$\forall a\in H \Rightarrow a^{-1}\in H$
さらに(1),(2)は，次の条件(3)と同値である．
(3)$\forall a,b\in H \Rightarrow a\circ b^{-1}\in H$

7

既約剰余類の部分群

$Z_6^{\times}=\{1,5\}$

×	1	5
1	1	5
5	5	1

自明な部分群
単位元のみの部分群$\{1\}$
全体集合$\{1,5\}$

$\{1\},\{1,5\}$　ともに正規部分群

8

既約剰余類の部分群

$Z_9^{\times}=\{1,2,4,5,7,8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

自明な部分群
$\{1\},\{1,2,4,5,7,8\}$
生成元は2と5
4からは{4,7,1}
7からは{7,4,1}
8からは{8,1}

すべて正規部分群

9

既約剰余類の部分群

$Z_{12}^{\times}=\{1,5,7,11\}$

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

自明な部分群
$\{1\},\{1,5,7,11\}$
5からは{5,1}
7からは{7,1}
11からは{11,1}
既約剰余類は乗法において可換
すべて正規部分群

10

巡回群

aの累乗の全体からなるGの部分集合
$<a>=\{a^n \mid n\in Z\}$はGの部分群になる．
また，この群はaを含むGの最小の部分群である．
部分群$<a>$をaで生成されたGの巡回部分群という．

Gをaによって生成される位数nの巡回群とする．
このとき，Gの元a^kの位数は$n/(n,k)$となる．
ただし,(n,k)はnとkの最大公約数を表す．
$|a^k|=n/(n,k)$

11

位数

群Gの元aに対して，$a^n=e$となるような
最小の正の整数をaの位数という．そのような
整数が無いとき，aの位数は無限という．
$|a|$でaの位数を表す．aの位数が無限のとき，
$|a|=\infty$

例題　加法群Z_{12}において，各元の位数を求めよ

$|0|=1,|1|=12,|2|=6,|3|=4,|4|=3,$
$|5|=12,\{5,10,3,8,1,6,11,4,9,2,7,0\}$
$|6|=2,|7|=12,|8|=3,|9|=4,|10|=5,|11|=12$

12

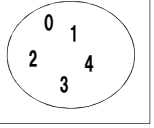
０６．群の定義

代数Ⅰ

代数系

集合　＋　代数的構造　＝　代数系

何かしらの数の集まり



四則演算などの
公理や定義

任意の演算

a＊b＝｜a－b｜

亜群
半群
モノイド
群

環
体

2

群

・空でない集合Gに対して，ある演算＊が定義

（１）閉鎖律

（２）結合律　$(x*y)*z = x*(y*z)$

（３）単位元 e の存在　$e*x = x*e = x$

（４）逆元 x' の存在　$x'*x = x*x' = e$

（５）可換律　$x*y = y*x$

可換群

位数n　$|G| = n$

亜群，半群，モノイド，群

閉鎖律（ある演算に関して閉じている）

集合Ｓは演算＊に関して亜群（groupid）

結合律（　（ｘ＊ｙ）＊ｚ＝ｘ＊（ｙ＊ｚ）　）

半群（semi-group）

単位元（　ｅ＊ｘ＝ｘ＊ｅ=ｘ　）

モノイド（monoid）

逆元（　ｘ’＊ｘ＝ｘ＊ｘ’=ｅ　）

群（group）

4

整数全体は加法に関して群か？

5

整数全体は乗法に関して群か？

6

部分群

群Gの空でない部分集合をHとする．
HがGの部分群であるための必要十分条件は
Hが次の条件(1)と(2)を満足していることである．
(1)$\forall a,b\in H \Rightarrow a\circ b\in H$
(2)$\forall a\in H \Rightarrow a^{-1}\in H$
さらに(1),(2)は，次の条件(3)と同値である．
(3)$\forall a,b\in H \Rightarrow a\circ b^{-1}\in H$

7

既約剰余類の部分群

$Z_6^{\times}=\{1,5\}$

×	1	5
1	1	5
5	5	1

自明な部分群
単位元のみの部分群$\{1\}$
全体集合$\{1,5\}$

$\{1\},\{1,5\}$　ともに正規部分群

8

既約剰余類の部分群

$Z_9^{\times}=\{1,2,4,5,7,8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

自明な部分群
$\{1\},\{1,2,4,5,7,8\}$
生成元は2と5
4からは{4,7,1}
7からは{7,4,1}
8からは{8,1}

すべて正規部分群

9

既約剰余類の部分群

$Z_{12}^{\times}=\{1,5,7,11\}$

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

自明な部分群
$\{1\},\{1,5,7,11\}$
5からは{5,1}
7からは{7,1}
11からは{11,1}
既約剰余類は乗法において可換
すべて正規部分群

10

巡回群

aの累乗の全体からなるGの部分集合
$<a>=\{a^n \mid n\in Z\}$はGの部分群になる．
また，この群はaを含むGの最小の部分群である．
部分群$<a>$をaで生成されたGの巡回部分群という．

Gをaによって生成される位数nの巡回群とする．
このとき，Gの元a^kの位数は$n/(n,k)$となる．
ただし,(n,k)はnとkの最大公約数を表す．
$|a^k|=n/(n,k)$

11

位数

群Gの元aに対して，$a^n=e$となるような
最小の正の整数をaの位数という．そのような
整数が無いとき，aの位数は無限という．
$|a|$でaの位数を表す．aの位数が無限のとき，
$|a|=\infty$

例題　加法群Z_{12}において，各元の位数を求めよ

$|0|=1,|1|=12,|2|=6,|3|=4,|4|=3,$
$|5|=12,\{5,10,3,8,1,6,11,4,9,2,7,0\}$
$|6|=2,|7|=12,|8|=3,|9|=4,|10|=5,|11|=12$

12

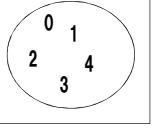
０６．群の定義

代数Ⅰ

代数系

集合　＋　代数的構造　＝　代数系

何かしらの数の集まり



四則演算などの
公理や定義

任意の演算

a＊b＝｜a－b｜

亜群
半群
モノイド
群

環
体

2

群

・空でない集合Gに対して，ある演算＊が定義

（１）閉鎖律

（２）結合律　$(x*y)*z = x*(y*z)$

（３）単位元 e の存在　$e*x = x*e = x$

（４）逆元 x' の存在　$x'*x = x*x' = e$

（５）可換律　$x*y = y*x$

可換群

位数n　$|G| = n$

亜群，半群，モノイド，群

閉鎖律（ある演算に関して閉じている）

集合Ｓは演算＊に関して亜群（groupid）

結合律（　（ｘ＊ｙ）＊ｚ＝ｘ＊（ｙ＊ｚ）　）

半群（semi-group）

単位元（　ｅ＊ｘ＝ｘ＊ｅ=ｘ　）

モノイド（monoid）

逆元（　ｘ’＊ｘ＝ｘ＊ｘ’=ｅ　）

群（group）

4

整数全体は加法に関して群か？

5

整数全体は乗法に関して群か？

6

部分群

群Gの空でない部分集合をHとする．
HがGの部分群であるための必要十分条件は
Hが次の条件(1)と(2)を満足していることである．
(1)$\forall a,b\in H \Rightarrow a\circ b\in H$
(2)$\forall a\in H \Rightarrow a^{-1}\in H$
さらに(1),(2)は，次の条件(3)と同値である．
(3)$\forall a,b\in H \Rightarrow a\circ b^{-1}\in H$

7

既約剰余類の部分群

$Z_6^{\times}=\{1,5\}$

×	1	5
1	1	5
5	5	1

自明な部分群
単位元のみの部分群$\{1\}$
全体集合$\{1,5\}$

$\{1\},\{1,5\}$　ともに正規部分群

8

既約剰余類の部分群

$Z_9^{\times}=\{1,2,4,5,7,8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

自明な部分群
$\{1\},\{1,2,4,5,7,8\}$
生成元は2と5
4からは{4,7,1}
7からは{7,4,1}
8からは{8,1}

すべて正規部分群

9

既約剰余類の部分群

$Z_{12}^{\times}=\{1,5,7,11\}$

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

自明な部分群
$\{1\},\{1,5,7,11\}$
5からは{5,1}
7からは{7,1}
11からは{11,1}
既約剰余類は乗法において可換
すべて正規部分群

10

巡回群

aの累乗の全体からなるGの部分集合
$<a>=\{a^n \mid n\in Z\}$はGの部分群になる．
また，この群はaを含むGの最小の部分群である．
部分群$<a>$をaで生成されたGの巡回部分群という．

Gをaによって生成される位数nの巡回群とする．
このとき，Gの元a^kの位数は$n/(n,k)$となる．
ただし,(n,k)はnとkの最大公約数を表す．
$|a^k|=n/(n,k)$

11

位数

群Gの元aに対して，$a^n=e$となるような
最小の正の整数をaの位数という．そのような
整数が無いとき，aの位数は無限という．
$|a|$でaの位数を表す．aの位数が無限のとき，
$|a|=\infty$

例題　加法群Z_{12}において，各元の位数を求めよ

$|0|=1,|1|=12,|2|=6,|3|=4,|4|=3,$
$|5|=12,\{5,10,3,8,1,6,11,4,9,2,7,0\}$
$|6|=2,|7|=12,|8|=3,|9|=4,|10|=5,|11|=12$

12

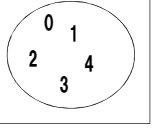
０６．群の定義

代数Ⅰ

代数系

集合　＋　代数的構造　＝　代数系

何かしらの数の集まり



四則演算などの
公理や定義

任意の演算

a＊b＝｜a－b｜

亜群
半群
モノイド
群

環
体

2

群

・空でない集合Gに対して，ある演算＊が定義

（１）閉鎖律

（２）結合律　$(x*y)*z = x*(y*z)$

（３）単位元 e の存在　$e*x = x*e = x$

（４）逆元 x' の存在　$x'*x = x*x' = e$

（５）可換律　$x*y = y*x$

可換群

位数n　$|G| = n$

亜群，半群，モノイド，群

閉鎖律（ある演算に関して閉じている）

集合Ｓは演算＊に関して亜群（groupid）

結合律（　（ｘ＊ｙ）＊ｚ＝ｘ＊（ｙ＊ｚ）　）

半群（semi-group）

単位元（　ｅ＊ｘ＝ｘ＊ｅ=ｘ　）

モノイド（monoid）

逆元（　ｘ’＊ｘ＝ｘ＊ｘ’=ｅ　）

群（group）

4

整数全体は加法に関して群か？

5

整数全体は乗法に関して群か？

6

部分群

群Gの空でない部分集合をHとする．
HがGの部分群であるための必要十分条件は
Hが次の条件(1)と(2)を満足していることである．
(1)$\forall a,b\in H \Rightarrow a\circ b\in H$
(2)$\forall a\in H \Rightarrow a^{-1}\in H$
さらに(1),(2)は，次の条件(3)と同値である．
(3)$\forall a,b\in H \Rightarrow a\circ b^{-1}\in H$

7

既約剰余類の部分群

$Z_6^{\times}=\{1,5\}$

×	1	5
1	1	5
5	5	1

自明な部分群
単位元のみの部分群$\{1\}$
全体集合$\{1,5\}$

$\{1\},\{1,5\}$　ともに正規部分群

8

既約剰余類の部分群

$Z_9^{\times}=\{1,2,4,5,7,8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

自明な部分群
$\{1\},\{1,2,4,5,7,8\}$
生成元は2と5
4からは{4,7,1}
7からは{7,4,1}
8からは{8,1}

すべて正規部分群

9

既約剰余類の部分群

$Z_{12}^{\times}=\{1,5,7,11\}$

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

自明な部分群
$\{1\},\{1,5,7,11\}$
5からは{5,1}
7からは{7,1}
11からは{11,1}
既約剰余類は乗法において可換
すべて正規部分群

10

巡回群

aの累乗の全体からなるGの部分集合
$<a>=\{a^n \mid n\in Z\}$はGの部分群になる．
また，この群はaを含むGの最小の部分群である．
部分群$<a>$をaで生成されたGの巡回部分群という．

Gをaによって生成される位数nの巡回群とする．
このとき，Gの元a^kの位数は$n/(n,k)$となる．
ただし,(n,k)はnとkの最大公約数を表す．
$|a^k|=n/(n,k)$

11

位数

群Gの元aに対して，$a^n=e$となるような
最小の正の整数をaの位数という．そのような
整数が無いとき，aの位数は無限という．
$|a|$でaの位数を表す．aの位数が無限のとき，
$|a|=\infty$

例題　加法群Z_{12}において，各元の位数を求めよ

$|0|=1,|1|=12,|2|=6,|3|=4,|4|=3,$
$|5|=12,\{5,10,3,8,1,6,11,4,9,2,7,0\}$
$|6|=2,|7|=12,|8|=3,|9|=4,|10|=5,|11|=12$

12

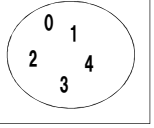
０６．群の定義

代数Ⅰ

代数系

集合　＋　代数的構造　＝　代数系

何かしらの数の集まり



四則演算などの
公理や定義

任意の演算

a＊b＝｜a－b｜

亜群
半群
モノイド
群

環
体

2

群

・空でない集合Gに対して，ある演算＊が定義

（１）閉鎖律

（２）結合律　$(x*y)*z = x*(y*z)$

（３）単位元 e の存在　$e*x = x*e = x$

（４）逆元 x' の存在　$x'*x = x*x' = e$

（５）可換律　$x*y = y*x$

可換群

位数n　$|G| = n$

亜群，半群，モノイド，群

閉鎖律（ある演算に関して閉じている）

集合Ｓは演算＊に関して亜群（groupid）

結合律（　（ｘ＊ｙ）＊ｚ＝ｘ＊（ｙ＊ｚ）　）

半群（semi-group）

単位元（　ｅ＊ｘ＝ｘ＊ｅ=ｘ　）

モノイド（monoid）

逆元（　ｘ’＊ｘ＝ｘ＊ｘ’=ｅ　）

群（group）

4

整数全体は加法に関して群か？

5

整数全体は乗法に関して群か？

6

部分群

群Gの空でない部分集合をHとする．
HがGの部分群であるための必要十分条件は
Hが次の条件(1)と(2)を満足していることである．
(1)$\forall a,b\in H \Rightarrow a\circ b\in H$
(2)$\forall a\in H \Rightarrow a^{-1}\in H$
さらに(1),(2)は，次の条件(3)と同値である．
(3)$\forall a,b\in H \Rightarrow a\circ b^{-1}\in H$

7

既約剰余類の部分群

$Z_6^{\times}=\{1,5\}$

×	1	5
1	1	5
5	5	1

自明な部分群
単位元のみの部分群$\{1\}$
全体集合$\{1,5\}$

$\{1\},\{1,5\}$　ともに正規部分群

8

既約剰余類の部分群

$Z_9^{\times}=\{1,2,4,5,7,8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

自明な部分群
$\{1\},\{1,2,4,5,7,8\}$
生成元は2と5
4からは{4,7,1}
7からは{7,4,1}
8からは{8,1}

すべて正規部分群

9

既約剰余類の部分群

$Z_{12}^{\times}=\{1,5,7,11\}$

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

自明な部分群
$\{1\},\{1,5,7,11\}$
5からは{5,1}
7からは{7,1}
11からは{11,1}
既約剰余類は乗法において可換
すべて正規部分群

10

巡回群

aの累乗の全体からなるGの部分集合
$<a>=\{a^n \mid n\in Z\}$はGの部分群になる．
また，この群はaを含むGの最小の部分群である．
部分群$<a>$をaで生成されたGの巡回部分群という．

Gをaによって生成される位数nの巡回群とする．
このとき，Gの元a^kの位数は$n/(n,k)$となる．
ただし,(n,k)はnとkの最大公約数を表す．
$|a^k|=n/(n,k)$

11

位数

群Gの元aに対して，$a^n=e$となるような
最小の正の整数をaの位数という．そのような
整数が無いとき，aの位数は無限という．
$|a|$でaの位数を表す．aの位数が無限のとき，
$|a|=\infty$

例題　加法群Z_{12}において，各元の位数を求めよ

$|0|=1,|1|=12,|2|=6,|3|=4,|4|=3,$
$|5|=12,\{5,10,3,8,1,6,11,4,9,2,7,0\}$
$|6|=2,|7|=12,|8|=3,|9|=4,|10|=5,|11|=12$

12

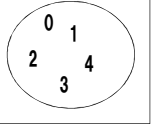
０６．群の定義

代数Ⅰ

代数系

集合　＋　代数的構造　＝　代数系

何かしらの数の集まり



四則演算などの
公理や定義

任意の演算

a＊b＝｜a－b｜

亜群
半群
モノイド
群

環
体

2

群

・空でない集合Gに対して，ある演算＊が定義

（１）閉鎖律

（２）結合律　$(x*y)*z = x*(y*z)$

（３）単位元 e の存在　$e*x = x*e = x$

（４）逆元 x' の存在　$x'*x = x*x' = e$

（５）可換律　$x*y = y*x$

可換群

位数n　$|G| = n$

亜群，半群，モノイド，群

閉鎖律（ある演算に関して閉じている）

集合Ｓは演算＊に関して亜群（groupid）

結合律（　（ｘ＊ｙ）＊ｚ＝ｘ＊（ｙ＊ｚ）　）

半群（semi-group）

単位元（　ｅ＊ｘ＝ｘ＊ｅ=ｘ　）

モノイド（monoid）

逆元（　ｘ’＊ｘ＝ｘ＊ｘ’=ｅ　）

群（group）

4

整数全体は加法に関して群か？

5

整数全体は乗法に関して群か？

6

部分群

群Gの空でない部分集合をHとする．
HがGの部分群であるための必要十分条件は
Hが次の条件(1)と(2)を満足していることである．
(1)$\forall a,b\in H \Rightarrow a\circ b\in H$
(2)$\forall a\in H \Rightarrow a^{-1}\in H$
さらに(1),(2)は，次の条件(3)と同値である．
(3)$\forall a,b\in H \Rightarrow a\circ b^{-1}\in H$

7

既約剰余類の部分群

$Z_6^{\times}=\{1,5\}$

×	1	5
1	1	5
5	5	1

自明な部分群
単位元のみの部分群$\{1\}$
全体集合$\{1,5\}$

$\{1\},\{1,5\}$　ともに正規部分群

8

既約剰余類の部分群

$Z_9^{\times}=\{1,2,4,5,7,8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

自明な部分群
$\{1\},\{1,2,4,5,7,8\}$
生成元は2と5
4からは{4,7,1}
7からは{7,4,1}
8からは{8,1}

すべて正規部分群

9

既約剰余類の部分群

$Z_{12}^{\times}=\{1,5,7,11\}$

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

自明な部分群
$\{1\},\{1,5,7,11\}$
5からは{5,1}
7からは{7,1}
11からは{11,1}
既約剰余類は乗法において可換
すべて正規部分群

10

巡回群

aの累乗の全体からなるGの部分集合
$<a>=\{a^n \mid n\in Z\}$はGの部分群になる．
また，この群はaを含むGの最小の部分群である．
部分群$<a>$をaで生成されたGの巡回部分群という．

Gをaによって生成される位数nの巡回群とする．
このとき，Gの元a^kの位数は$n/(n,k)$となる．
ただし,(n,k)はnとkの最大公約数を表す．
$|a^k|=n/(n,k)$

11

位数

群Gの元aに対して，$a^n=e$となるような
最小の正の整数をaの位数という．そのような
整数が無いとき，aの位数は無限という．
$|a|$でaの位数を表す．aの位数が無限のとき，
$|a|=\infty$

例題　加法群Z_{12}において，各元の位数を求めよ

$|0|=1,|1|=12,|2|=6,|3|=4,|4|=3,$
$|5|=12,\{5,10,3,8,1,6,11,4,9,2,7,0\}$
$|6|=2,|7|=12,|8|=3,|9|=4,|10|=5,|11|=12$

12

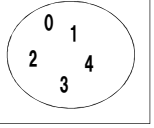
０６．群の定義

代数Ⅰ

代数系

集合　＋　代数的構造　＝　代数系

何かしらの数の集まり



四則演算などの
公理や定義

任意の演算

a＊b＝｜a－b｜

亜群
半群
モノイド
群

環
体

2

群

・空でない集合Gに対して，ある演算＊が定義

（１）閉鎖律

（２）結合律　$(x*y)*z = x*(y*z)$

（３）単位元 e の存在　$e*x = x*e = x$

（４）逆元 x' の存在　$x'*x = x*x' = e$

（５）可換律　$x*y = y*x$

可換群

位数n　$|G| = n$

亜群，半群，モノイド，群

閉鎖律（ある演算に関して閉じている）

集合Ｓは演算＊に関して亜群（groupid）

結合律（　（ｘ＊ｙ）＊ｚ＝ｘ＊（ｙ＊ｚ）　）

半群（semi-group）

単位元（　ｅ＊ｘ＝ｘ＊ｅ=ｘ　）

モノイド（monoid）

逆元（　ｘ’＊ｘ＝ｘ＊ｘ’=ｅ　）

群（group）

4

整数全体は加法に関して群か？

5

整数全体は乗法に関して群か？

6

部分群

群Gの空でない部分集合をHとする．
HがGの部分群であるための必要十分条件は
Hが次の条件(1)と(2)を満足していることである．
(1)$\forall a,b\in H \Rightarrow a\circ b\in H$
(2)$\forall a\in H \Rightarrow a^{-1}\in H$
さらに(1),(2)は，次の条件(3)と同値である．
(3)$\forall a,b\in H \Rightarrow a\circ b^{-1}\in H$

7

既約剰余類の部分群

$Z_6^{\times}=\{1,5\}$

×	1	5
1	1	5
5	5	1

自明な部分群
単位元のみの部分群$\{1\}$
全体集合$\{1,5\}$

$\{1\},\{1,5\}$　ともに正規部分群

8

既約剰余類の部分群

$Z_9^{\times}=\{1,2,4,5,7,8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

自明な部分群
$\{1\},\{1,2,4,5,7,8\}$
生成元は2と5
4からは{4,7,1}
7からは{7,4,1}
8からは{8,1}

すべて正規部分群

9

既約剰余類の部分群

$Z_{12}^{\times}=\{1,5,7,11\}$

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

自明な部分群
$\{1\},\{1,5,7,11\}$
5からは{5,1}
7からは{7,1}
11からは{11,1}
既約剰余類は乗法において可換
すべて正規部分群

10

巡回群

aの累乗の全体からなるGの部分集合
$<a>=\{a^n \mid n\in Z\}$はGの部分群になる．
また，この群はaを含むGの最小の部分群である．
部分群$<a>$をaで生成されたGの巡回部分群という．

Gをaによって生成される位数nの巡回群とする．
このとき，Gの元a^kの位数は$n/(n,k)$となる．
ただし,(n,k)はnとkの最大公約数を表す．
$|a^k|=n/(n,k)$

11

位数

群Gの元aに対して，$a^n=e$となるような
最小の正の整数をaの位数という．そのような
整数が無いとき，aの位数は無限という．
$|a|$でaの位数を表す．aの位数が無限のとき，
$|a|=\infty$

例題　加法群Z_{12}において，各元の位数を求めよ

$|0|=1,|1|=12,|2|=6,|3|=4,|4|=3,$
$|5|=12,\{5,10,3,8,1,6,11,4,9,2,7,0\}$
$|6|=2,|7|=12,|8|=3,|9|=4,|10|=5,|11|=12$

12

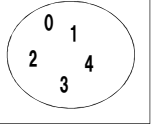
０６．群の定義

代数Ⅰ

代数系

集合　＋　代数的構造　＝　代数系

何かしらの数の集まり



四則演算などの
公理や定義

任意の演算

a＊b＝｜a－b｜

亜群
半群
モノイド
群

環
体

2

群

・空でない集合Gに対して，ある演算＊が定義

（１）閉鎖律

（２）結合律　$(x*y)*z = x*(y*z)$

（３）単位元 e の存在　$e*x = x*e = x$

（４）逆元 x' の存在　$x'*x = x*x' = e$

（５）可換律　$x*y = y*x$

可換群

位数n　$|G| = n$

亜群，半群，モノイド，群

閉鎖律（ある演算に関して閉じている）

集合Ｓは演算＊に関して亜群（groupid）

結合律（　（ｘ＊ｙ）＊ｚ＝ｘ＊（ｙ＊ｚ）　）

半群（semi-group）

単位元（　ｅ＊ｘ＝ｘ＊ｅ=ｘ　）

モノイド（monoid）

逆元（　ｘ’＊ｘ＝ｘ＊ｘ’=ｅ　）

群（group）

4

整数全体は加法に関して群か？

5

整数全体は乗法に関して群か？

6

部分群

群Gの空でない部分集合をHとする．
HがGの部分群であるための必要十分条件は
Hが次の条件(1)と(2)を満足していることである．
(1)$\forall a,b\in H \Rightarrow a\circ b\in H$
(2)$\forall a\in H \Rightarrow a^{-1}\in H$
さらに(1),(2)は，次の条件(3)と同値である．
(3)$\forall a,b\in H \Rightarrow a\circ b^{-1}\in H$

7

既約剰余類の部分群

$Z_6^{\times}=\{1,5\}$

×	1	5
1	1	5
5	5	1

自明な部分群
単位元のみの部分群$\{1\}$
全体集合$\{1,5\}$

$\{1\},\{1,5\}$　ともに正規部分群

8

既約剰余類の部分群

$Z_9^{\times}=\{1,2,4,5,7,8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

自明な部分群
$\{1\},\{1,2,4,5,7,8\}$
生成元は2と5
4からは{4,7,1}
7からは{7,4,1}
8からは{8,1}

すべて正規部分群

9

既約剰余類の部分群

$Z_{12}^{\times}=\{1,5,7,11\}$

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

自明な部分群
$\{1\},\{1,5,7,11\}$
5からは{5,1}
7からは{7,1}
11からは{11,1}
既約剰余類は乗法において可換
すべて正規部分群

10

巡回群

aの累乗の全体からなるGの部分集合
$<a>=\{a^n \mid n\in Z\}$はGの部分群になる．
また，この群はaを含むGの最小の部分群である．
部分群$<a>$をaで生成されたGの巡回部分群という．

Gをaによって生成される位数nの巡回群とする．
このとき，Gの元a^kの位数は$n/(n,k)$となる．
ただし,(n,k)はnとkの最大公約数を表す．
$|a^k|=n/(n,k)$

11

位数

群Gの元aに対して，$a^n=e$となるような
最小の正の整数をaの位数という．そのような
整数が無いとき，aの位数は無限という．
$|a|$でaの位数を表す．aの位数が無限のとき，
$|a|=\infty$

例題　加法群Z_{12}において，各元の位数を求めよ

$|0|=1,|1|=12,|2|=6,|3|=4,|4|=3,$
$|5|=12,\{5,10,3,8,1,6,11,4,9,2,7,0\}$
$|6|=2,|7|=12,|8|=3,|9|=4,|10|=5,|11|=12$

12

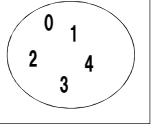
０６．群の定義

代数Ⅰ

代数系

集合　＋　代数的構造　＝　代数系

何かしらの数の集まり



四則演算などの
公理や定義

任意の演算

a＊b＝｜a－b｜

亜群
半群
モノイド
群

環
体

2

群

・空でない集合Gに対して，ある演算＊が定義

（１）閉鎖律

（２）結合律　$(x*y)*z = x*(y*z)$

（３）単位元 e の存在　$e*x = x*e = x$

（４）逆元 x' の存在　$x'*x = x*x' = e$

（５）可換律　$x*y = y*x$

可換群

位数n　$|G| = n$

亜群，半群，モノイド，群

閉鎖律（ある演算に関して閉じている）

集合Ｓは演算＊に関して亜群（groupid）

結合律（　（ｘ＊ｙ）＊ｚ＝ｘ＊（ｙ＊ｚ）　）

半群（semi-group）

単位元（　ｅ＊ｘ＝ｘ＊ｅ=ｘ　）

モノイド（monoid）

逆元（　ｘ’＊ｘ＝ｘ＊ｘ’=ｅ　）

群（group）

4

整数全体は加法に関して群か？

5

整数全体は乗法に関して群か？

6

部分群

群Gの空でない部分集合をHとする．
HがGの部分群であるための必要十分条件は
Hが次の条件(1)と(2)を満足していることである．
(1)$\forall a,b\in H \Rightarrow a\circ b\in H$
(2)$\forall a\in H \Rightarrow a^{-1}\in H$
さらに(1),(2)は，次の条件(3)と同値である．
(3)$\forall a,b\in H \Rightarrow a\circ b^{-1}\in H$

7

既約剰余類の部分群

$Z_6^{\times}=\{1,5\}$

×	1	5
1	1	5
5	5	1

自明な部分群
単位元のみの部分群$\{1\}$
全体集合$\{1,5\}$

$\{1\},\{1,5\}$　ともに正規部分群

8

既約剰余類の部分群

$Z_9^{\times}=\{1,2,4,5,7,8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

自明な部分群
$\{1\},\{1,2,4,5,7,8\}$
生成元は2と5
4からは{4,7,1}
7からは{7,4,1}
8からは{8,1}

すべて正規部分群

9

既約剰余類の部分群

$Z_{12}^{\times}=\{1,5,7,11\}$

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

自明な部分群
$\{1\},\{1,5,7,11\}$
5からは{5,1}
7からは{7,1}
11からは{11,1}
既約剰余類は乗法において可換
すべて正規部分群

10

巡回群

aの累乗の全体からなるGの部分集合
$<a>=\{a^n \mid n\in Z\}$はGの部分群になる．
また，この群はaを含むGの最小の部分群である．
部分群$<a>$をaで生成されたGの巡回部分群という．

Gをaによって生成される位数nの巡回群とする．
このとき，Gの元a^kの位数は$n/(n,k)$となる．
ただし,(n,k)はnとkの最大公約数を表す．
$|a^k|=n/(n,k)$

11

位数

群Gの元aに対して，$a^n=e$となるような
最小の正の整数をaの位数という．そのような
整数が無いとき，aの位数は無限という．
$|a|$でaの位数を表す．aの位数が無限のとき，
$|a|=\infty$

例題　加法群Z_{12}において，各元の位数を求めよ

$|0|=1,|1|=12,|2|=6,|3|=4,|4|=3,$
$|5|=12,\{5,10,3,8,1,6,11,4,9,2,7,0\}$
$|6|=2,|7|=12,|8|=3,|9|=4,|10|=5,|11|=12$

12

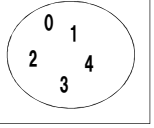
０６．群の定義

代数Ⅰ

代数系

集合　＋　代数的構造　＝　代数系

何かしらの数の集まり



四則演算などの
公理や定義

任意の演算

a＊b＝｜a－b｜

亜群
半群
モノイド
群

環
体

2

群

・空でない集合Gに対して，ある演算＊が定義

（１）閉鎖律

（２）結合律　$(x*y)*z = x*(y*z)$

（３）単位元 e の存在　$e*x = x*e = x$

（４）逆元 x' の存在　$x'*x = x*x' = e$

（５）可換律　$x*y = y*x$

可換群

位数n　$|G| = n$

亜群，半群，モノイド，群

閉鎖律（ある演算に関して閉じている）

集合Ｓは演算＊に関して亜群（groupid）

結合律（　（ｘ＊ｙ）＊ｚ＝ｘ＊（ｙ＊ｚ）　）

半群（semi-group）

単位元（　ｅ＊ｘ＝ｘ＊ｅ=ｘ　）

モノイド（monoid）

逆元（　ｘ’＊ｘ＝ｘ＊ｘ’=ｅ　）

群（group）

4

整数全体は加法に関して群か？

5

整数全体は乗法に関して群か？

6

部分群

群Gの空でない部分集合をHとする．
HがGの部分群であるための必要十分条件は
Hが次の条件(1)と(2)を満足していることである．
(1)$\forall a,b\in H \Rightarrow a\circ b\in H$
(2)$\forall a\in H \Rightarrow a^{-1}\in H$
さらに(1),(2)は，次の条件(3)と同値である．
(3)$\forall a,b\in H \Rightarrow a\circ b^{-1}\in H$

7

既約剰余類の部分群

$Z_6^{\times}=\{1,5\}$

×	1	5
1	1	5
5	5	1

自明な部分群
単位元のみの部分群$\{1\}$
全体集合$\{1,5\}$

$\{1\},\{1,5\}$　ともに正規部分群

8

既約剰余類の部分群

$Z_9^{\times}=\{1,2,4,5,7,8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

自明な部分群
$\{1\},\{1,2,4,5,7,8\}$
生成元は2と5
4からは{4,7,1}
7からは{7,4,1}
8からは{8,1}

すべて正規部分群

9

既約剰余類の部分群

$Z_{12}^{\times}=\{1,5,7,11\}$

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

自明な部分群
$\{1\},\{1,5,7,11\}$
5からは{5,1}
7からは{7,1}
11からは{11,1}
既約剰余類は乗法において可換
すべて正規部分群

10

巡回群

aの累乗の全体からなるGの部分集合
$<a>=\{a^n \mid n\in Z\}$はGの部分群になる．
また，この群はaを含むGの最小の部分群である．
部分群$<a>$をaで生成されたGの巡回部分群という．

Gをaによって生成される位数nの巡回群とする．
このとき，Gの元a^kの位数は$n/(n,k)$となる．
ただし,(n,k)はnとkの最大公約数を表す．
$|a^k|=n/(n,k)$

11

位数

群Gの元aに対して，$a^n=e$となるような
最小の正の整数をaの位数という．そのような
整数が無いとき，aの位数は無限という．
$|a|$でaの位数を表す．aの位数が無限のとき，
$|a|=\infty$

例題　加法群Z_{12}において，各元の位数を求めよ

$|0|=1,|1|=12,|2|=6,|3|=4,|4|=3,$
$|5|=12,\{5,10,3,8,1,6,11,4,9,2,7,0\}$
$|6|=2,|7|=12,|8|=3,|9|=4,|10|=5,|11|=12$

12

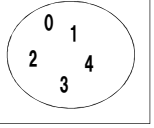
０６．群の定義

代数Ⅰ

代数系

集合　＋　代数的構造　＝　代数系

何かしらの数の集まり



四則演算などの
公理や定義

任意の演算

a＊b＝｜a－b｜

亜群
半群
モノイド
群

環
体

2

群

・空でない集合Gに対して，ある演算＊が定義

（１）閉鎖律

（２）結合律　$(x*y)*z = x*(y*z)$

（３）単位元 e の存在　$e*x = x*e = x$

（４）逆元 x' の存在　$x'*x = x*x' = e$

（５）可換律　$x*y = y*x$

可換群

位数n　$|G| = n$

亜群，半群，モノイド，群

閉鎖律（ある演算に関して閉じている）

集合Ｓは演算＊に関して亜群（groupid）

結合律（　（ｘ＊ｙ）＊ｚ＝ｘ＊（ｙ＊ｚ）　）

半群（semi-group）

単位元（　ｅ＊ｘ＝ｘ＊ｅ=ｘ　）

モノイド（monoid）

逆元（　ｘ’＊ｘ＝ｘ＊ｘ’=ｅ　）

群（group）

4

整数全体は加法に関して群か？

5

整数全体は乗法に関して群か？

6

部分群

群Gの空でない部分集合をHとする．
HがGの部分群であるための必要十分条件は
Hが次の条件(1)と(2)を満足していることである．
(1)$\forall a,b\in H \Rightarrow a\circ b\in H$
(2)$\forall a\in H \Rightarrow a^{-1}\in H$
さらに(1),(2)は，次の条件(3)と同値である．
(3)$\forall a,b\in H \Rightarrow a\circ b^{-1}\in H$

7

既約剰余類の部分群

$Z_6^{\times}=\{1,5\}$

×	1	5
1	1	5
5	5	1

自明な部分群
単位元のみの部分群$\{1\}$
全体集合$\{1,5\}$

$\{1\},\{1,5\}$　ともに正規部分群

8

既約剰余類の部分群

$Z_9^{\times}=\{1,2,4,5,7,8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

自明な部分群
$\{1\},\{1,2,4,5,7,8\}$
生成元は2と5
4からは{4,7,1}
7からは{7,4,1}
8からは{8,1}

すべて正規部分群

9

既約剰余類の部分群

$Z_{12}^{\times}=\{1,5,7,11\}$

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

自明な部分群
$\{1\},\{1,5,7,11\}$
5からは{5,1}
7からは{7,1}
11からは{11,1}
既約剰余類は乗法において可換
すべて正規部分群

10

巡回群

aの累乗の全体からなるGの部分集合
$<a>=\{a^n \mid n\in Z\}$はGの部分群になる．
また，この群はaを含むGの最小の部分群である．
部分群$<a>$をaで生成されたGの巡回部分群という．

Gをaによって生成される位数nの巡回群とする．
このとき，Gの元a^kの位数は$n/(n,k)$となる．
ただし,(n,k)はnとkの最大公約数を表す．
$|a^k|=n/(n,k)$

11

位数

群Gの元aに対して，$a^n=e$となるような
最小の正の整数をaの位数という．そのような
整数が無いとき，aの位数は無限という．
$|a|$でaの位数を表す．aの位数が無限のとき，
$|a|=\infty$

例題　加法群Z_{12}において，各元の位数を求めよ

$|0|=1,|1|=12,|2|=6,|3|=4,|4|=3,$
$|5|=12,\{5,10,3,8,1,6,11,4,9,2,7,0\}$
$|6|=2,|7|=12,|8|=3,|9|=4,|10|=5,|11|=12$

12

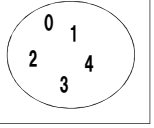
０６．群の定義

代数Ⅰ

代数系

集合　＋　代数的構造　＝　代数系

何かしらの数の集まり



四則演算などの
公理や定義

任意の演算

a＊b＝｜a－b｜

亜群
半群
モノイド
群

環
体

2

群

・空でない集合Gに対して，ある演算＊が定義

（１）閉鎖律

（２）結合律　$(x*y)*z = x*(y*z)$

（３）単位元 e の存在　$e*x = x*e = x$

（４）逆元 x' の存在　$x'*x = x*x' = e$

（５）可換律　$x*y = y*x$

可換群

位数n　$|G| = n$

亜群，半群，モノイド，群

閉鎖律（ある演算に関して閉じている）

集合Ｓは演算＊に関して亜群（groupid）

結合律（　（ｘ＊ｙ）＊ｚ＝ｘ＊（ｙ＊ｚ）　）

半群（semi-group）

単位元（　ｅ＊ｘ＝ｘ＊ｅ=ｘ　）

モノイド（monoid）

逆元（　ｘ’＊ｘ＝ｘ＊ｘ’=ｅ　）

群（group）

4

整数全体は加法に関して群か？

5

整数全体は乗法に関して群か？

6

部分群

群Gの空でない部分集合をHとする．
HがGの部分群であるための必要十分条件は
Hが次の条件(1)と(2)を満足していることである．
(1)$\forall a,b\in H \Rightarrow a\circ b\in H$
(2)$\forall a\in H \Rightarrow a^{-1}\in H$
さらに(1),(2)は，次の条件(3)と同値である．
(3)$\forall a,b\in H \Rightarrow a\circ b^{-1}\in H$

7

既約剰余類の部分群

$Z_6^{\times}=\{1,5\}$

×	1	5
1	1	5
5	5	1

自明な部分群
単位元のみの部分群$\{1\}$
全体集合$\{1,5\}$

$\{1\},\{1,5\}$　ともに正規部分群

8

既約剰余類の部分群

$Z_9^{\times}=\{1,2,4,5,7,8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

自明な部分群
$\{1\},\{1,2,4,5,7,8\}$
生成元は2と5
4からは{4,7,1}
7からは{7,4,1}
8からは{8,1}

すべて正規部分群

9

既約剰余類の部分群

$Z_{12}^{\times}=\{1,5,7,11\}$

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

自明な部分群
$\{1\},\{1,5,7,11\}$
5からは{5,1}
7からは{7,1}
11からは{11,1}
既約剰余類は乗法において可換
すべて正規部分群

10

巡回群

aの累乗の全体からなるGの部分集合
$<a>=\{a^n \mid n\in Z\}$はGの部分群になる．
また，この群はaを含むGの最小の部分群である．
部分群$<a>$をaで生成されたGの巡回部分群という．

Gをaによって生成される位数nの巡回群とする．
このとき，Gの元a^kの位数は$n/(n,k)$となる．
ただし,(n,k)はnとkの最大公約数を表す．
$|a^k|=n/(n,k)$

11

位数

群Gの元aに対して，$a^n=e$となるような
最小の正の整数をaの位数という．そのような
整数が無いとき，aの位数は無限という．
$|a|$でaの位数を表す．aの位数が無限のとき，
$|a|=\infty$

例題　加法群Z_{12}において，各元の位数を求めよ

$|0|=1,|1|=12,|2|=6,|3|=4,|4|=3,$
$|5|=12,\{5,10,3,8,1,6,11,4,9,2,7,0\}$
$|6|=2,|7|=12,|8|=3,|9|=4,|10|=5,|11|=12$

12

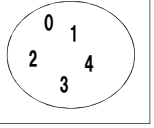
０６．群の定義

代数Ⅰ

代数系

集合　＋　代数的構造　＝　代数系

何かしらの数の集まり



四則演算などの
公理や定義

任意の演算

a＊b＝｜a－b｜

亜群
半群
モノイド
群

環
体

2

群

・空でない集合Gに対して，ある演算＊が定義

（１）閉鎖律

（２）結合律　$(x*y)*z = x*(y*z)$

（３）単位元 e の存在　$e*x = x*e = x$

（４）逆元 x' の存在　$x'*x = x*x' = e$

（５）可換律　$x*y = y*x$

可換群

位数n　$|G| = n$

亜群，半群，モノイド，群

閉鎖律（ある演算に関して閉じている）

集合Ｓは演算＊に関して亜群（groupid）

結合律（　（ｘ＊ｙ）＊ｚ＝ｘ＊（ｙ＊ｚ）　）

半群（semi-group）

単位元（　ｅ＊ｘ＝ｘ＊ｅ=ｘ　）

モノイド（monoid）

逆元（　ｘ’＊ｘ＝ｘ＊ｘ’=ｅ　）

群（group）

4

整数全体は加法に関して群か？

5

整数全体は乗法に関して群か？

6

部分群

群Gの空でない部分集合をHとする．
HがGの部分群であるための必要十分条件は
Hが次の条件(1)と(2)を満足していることである．
(1)$\forall a,b\in H \Rightarrow a\circ b\in H$
(2)$\forall a\in H \Rightarrow a^{-1}\in H$
さらに(1),(2)は，次の条件(3)と同値である．
(3)$\forall a,b\in H \Rightarrow a\circ b^{-1}\in H$

7

既約剰余類の部分群

$Z_6^{\times}=\{1,5\}$

×	1	5
1	1	5
5	5	1

自明な部分群
単位元のみの部分群$\{1\}$
全体集合$\{1,5\}$

$\{1\},\{1,5\}$　ともに正規部分群

8

既約剰余類の部分群

$Z_9^{\times}=\{1,2,4,5,7,8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

自明な部分群
$\{1\},\{1,2,4,5,7,8\}$
生成元は2と5
4からは{4,7,1}
7からは{7,4,1}
8からは{8,1}

すべて正規部分群

9

既約剰余類の部分群

$Z_{12}^{\times}=\{1,5,7,11\}$

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

自明な部分群
$\{1\},\{1,5,7,11\}$
5からは{5,1}
7からは{7,1}
11からは{11,1}
既約剰余類は乗法において可換
すべて正規部分群

10

巡回群

aの累乗の全体からなるGの部分集合
$<a>=\{a^n \mid n\in Z\}$はGの部分群になる．
また，この群はaを含むGの最小の部分群である．
部分群$<a>$をaで生成されたGの巡回部分群という．

Gをaによって生成される位数nの巡回群とする．
このとき，Gの元a^kの位数は$n/(n,k)$となる．
ただし,(n,k)はnとkの最大公約数を表す．
$|a^k|=n/(n,k)$

11

位数

群Gの元aに対して，$a^n=e$となるような
最小の正の整数をaの位数という．そのような
整数が無いとき，aの位数は無限という．
$|a|$でaの位数を表す．aの位数が無限のとき，
$|a|=\infty$

例題　加法群Z_{12}において，各元の位数を求めよ

$|0|=1,|1|=12,|2|=6,|3|=4,|4|=3,$
$|5|=12,\{5,10,3,8,1,6,11,4,9,2,7,0\}$
$|6|=2,|7|=12,|8|=3,|9|=4,|10|=5,|11|=12$

12

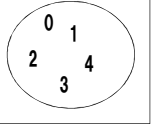
０６．群の定義

代数Ⅰ

代数系

集合　＋　代数的構造　＝　代数系

何かしらの数の集まり



四則演算などの
公理や定義

任意の演算

a＊b＝｜a－b｜

亜群
半群
モノイド
群

環
体

2

群

・空でない集合Gに対して，ある演算＊が定義

（１）閉鎖律

（２）結合律　$(x*y)*z = x*(y*z)$

（３）単位元 e の存在　$e*x = x*e = x$

（４）逆元 x' の存在　$x'*x = x*x' = e$

（５）可換律　$x*y = y*x$

可換群

位数n　$|G| = n$

亜群，半群，モノイド，群

閉鎖律（ある演算に関して閉じている）

集合Ｓは演算＊に関して亜群（groupid）

結合律（　（ｘ＊ｙ）＊ｚ＝ｘ＊（ｙ＊ｚ）　）

半群（semi-group）

単位元（　ｅ＊ｘ＝ｘ＊ｅ=ｘ　）

モノイド（monoid）

逆元（　ｘ’＊ｘ＝ｘ＊ｘ’=ｅ　）

群（group）

4

整数全体は加法に関して群か？

5

整数全体は乗法に関して群か？

6

部分群

群Gの空でない部分集合をHとする．
HがGの部分群であるための必要十分条件は
Hが次の条件(1)と(2)を満足していることである．
(1)$\forall a,b\in H \Rightarrow a\circ b\in H$
(2)$\forall a\in H \Rightarrow a^{-1}\in H$
さらに(1),(2)は，次の条件(3)と同値である．
(3)$\forall a,b\in H \Rightarrow a\circ b^{-1}\in H$

7

既約剰余類の部分群

$Z_6^{\times}=\{1,5\}$

×	1	5
1	1	5
5	5	1

自明な部分群
単位元のみの部分群$\{1\}$
全体集合$\{1,5\}$

$\{1\},\{1,5\}$　ともに正規部分群

8

既約剰余類の部分群

$Z_9^{\times}=\{1,2,4,5,7,8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

自明な部分群
$\{1\},\{1,2,4,5,7,8\}$
生成元は2と5
4からは{4,7,1}
7からは{7,4,1}
8からは{8,1}

すべて正規部分群

9

既約剰余類の部分群

$Z_{12}^{\times}=\{1,5,7,11\}$

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

自明な部分群
$\{1\},\{1,5,7,11\}$
5からは{5,1}
7からは{7,1}
11からは{11,1}
既約剰余類は乗法において可換
すべて正規部分群

10

巡回群

aの累乗の全体からなるGの部分集合
$<a>=\{a^n \mid n\in Z\}$はGの部分群になる．
また，この群はaを含むGの最小の部分群である．
部分群$<a>$をaで生成されたGの巡回部分群という．

Gをaによって生成される位数nの巡回群とする．
このとき，Gの元a^kの位数は$n/(n,k)$となる．
ただし,(n,k)はnとkの最大公約数を表す．
$|a^k|=n/(n,k)$

11

位数

群Gの元aに対して，$a^n=e$となるような
最小の正の整数をaの位数という．そのような
整数が無いとき，aの位数は無限という．
$|a|$でaの位数を表す．aの位数が無限のとき，
$|a|=\infty$

例題　加法群Z_{12}において，各元の位数を求めよ

$|0|=1,|1|=12,|2|=6,|3|=4,|4|=3,$
$|5|=12,\{5,10,3,8,1,6,11,4,9,2,7,0\}$
$|6|=2,|7|=12,|8|=3,|9|=4,|10|=5,|11|=12$

12

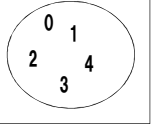
０６．群の定義

代数Ⅰ

代数系

集合　＋　代数的構造　＝　代数系

何かしらの数の集まり



四則演算などの
公理や定義

任意の演算

a＊b＝｜a－b｜

亜群
半群
モノイド
群

環
体

2

群

・空でない集合Gに対して，ある演算＊が定義

（１）閉鎖律

（２）結合律　$(x*y)*z = x*(y*z)$

（３）単位元 e の存在　$e*x = x*e = x$

（４）逆元 x' の存在　$x'*x = x*x' = e$

（５）可換律　$x*y = y*x$

可換群

位数n　$|G| = n$

亜群，半群，モノイド，群

閉鎖律（ある演算に関して閉じている）

集合Ｓは演算＊に関して亜群（groupid）

結合律（　（ｘ＊ｙ）＊ｚ＝ｘ＊（ｙ＊ｚ）　）

半群（semi-group）

単位元（　ｅ＊ｘ＝ｘ＊ｅ=ｘ　）

モノイド（monoid）

逆元（　ｘ’＊ｘ＝ｘ＊ｘ’=ｅ　）

群（group）

4

整数全体は加法に関して群か？

5

整数全体は乗法に関して群か？

6

部分群

群Gの空でない部分集合をHとする．
HがGの部分群であるための必要十分条件は
Hが次の条件(1)と(2)を満足していることである．
(1)$\forall a,b\in H \Rightarrow a\circ b\in H$
(2)$\forall a\in H \Rightarrow a^{-1}\in H$
さらに(1),(2)は，次の条件(3)と同値である．
(3)$\forall a,b\in H \Rightarrow a\circ b^{-1}\in H$

7

既約剰余類の部分群

$Z_6^{\times}=\{1,5\}$

×	1	5
1	1	5
5	5	1

自明な部分群
単位元のみの部分群$\{1\}$
全体集合$\{1,5\}$

$\{1\},\{1,5\}$　ともに正規部分群

8

既約剰余類の部分群

$Z_9^{\times}=\{1,2,4,5,7,8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

自明な部分群
$\{1\},\{1,2,4,5,7,8\}$
生成元は2と5
4からは{4,7,1}
7からは{7,4,1}
8からは{8,1}

すべて正規部分群

9

既約剰余類の部分群

$Z_{12}^{\times}=\{1,5,7,11\}$

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

自明な部分群
$\{1\},\{1,5,7,11\}$
5からは{5,1}
7からは{7,1}
11からは{11,1}
既約剰余類は乗法において可換
すべて正規部分群

10

巡回群

aの累乗の全体からなるGの部分集合
$<a>=\{a^n \mid n\in Z\}$はGの部分群になる．
また，この群はaを含むGの最小の部分群である．
部分群$<a>$をaで生成されたGの巡回部分群という．

Gをaによって生成される位数nの巡回群とする．
このとき，Gの元a^kの位数は$n/(n,k)$となる．
ただし,(n,k)はnとkの最大公約数を表す．
$|a^k|=n/(n,k)$

11

位数

群Gの元aに対して，$a^n=e$となるような
最小の正の整数をaの位数という．そのような
整数が無いとき，aの位数は無限という．
$|a|$でaの位数を表す．aの位数が無限のとき，
$|a|=\infty$

例題　加法群Z_{12}において，各元の位数を求めよ

$|0|=1,|1|=12,|2|=6,|3|=4,|4|=3,$
$|5|=12,\{5,10,3,8,1,6,11,4,9,2,7,0\}$
$|6|=2,|7|=12,|8|=3,|9|=4,|10|=5,|11|=12$

12

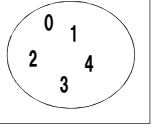
０６．群の定義

代数Ⅰ

代数系

集合　＋　代数的構造　＝　代数系

何かしらの数の集まり



四則演算などの
公理や定義

任意の演算

a＊b＝｜a－b｜

亜群
半群
モノイド
群

環
体

2

群

・空でない集合Gに対して，ある演算＊が定義

（１）閉鎖律

（２）結合律　$(x*y)*z = x*(y*z)$

（３）単位元 e の存在　$e*x = x*e = x$

（４）逆元 x' の存在　$x'*x = x*x' = e$

（５）可換律　$x*y = y*x$

可換群

位数n　$|G| = n$

亜群，半群，モノイド，群

閉鎖律（ある演算に関して閉じている）

集合Ｓは演算＊に関して亜群（groupid）

結合律（　（ｘ＊ｙ）＊ｚ＝ｘ＊（ｙ＊ｚ）　）

半群（semi-group）

単位元（　ｅ＊ｘ＝ｘ＊ｅ=ｘ　）

モノイド（monoid）

逆元（　ｘ’＊ｘ＝ｘ＊ｘ’=ｅ　）

群（group）

4

整数全体は加法に関して群か？

5

整数全体は乗法に関して群か？

6

部分群

群Gの空でない部分集合をHとする．
HがGの部分群であるための必要十分条件は
Hが次の条件(1)と(2)を満足していることである．
(1)$\forall a,b\in H \Rightarrow a\circ b\in H$
(2)$\forall a\in H \Rightarrow a^{-1}\in H$
さらに(1),(2)は，次の条件(3)と同値である．
(3)$\forall a,b\in H \Rightarrow a\circ b^{-1}\in H$

7

既約剰余類の部分群

$Z_6^{\times}=\{1,5\}$

×	1	5
1	1	5
5	5	1

自明な部分群
単位元のみの部分群$\{1\}$
全体集合$\{1,5\}$

$\{1\},\{1,5\}$　ともに正規部分群

8

既約剰余類の部分群

$Z_9^{\times}=\{1,2,4,5,7,8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

自明な部分群
$\{1\},\{1,2,4,5,7,8\}$
生成元は2と5
4からは{4,7,1}
7からは{7,4,1}
8からは{8,1}

すべて正規部分群

9

既約剰余類の部分群

$Z_{12}^{\times}=\{1,5,7,11\}$

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

自明な部分群
$\{1\},\{1,5,7,11\}$
5からは{5,1}
7からは{7,1}
11からは{11,1}
既約剰余類は乗法において可換
すべて正規部分群

10

巡回群

aの累乗の全体からなるGの部分集合
$<a>=\{a^n \mid n\in Z\}$はGの部分群になる．
また，この群はaを含むGの最小の部分群である．
部分群$<a>$をaで生成されたGの巡回部分群という．

Gをaによって生成される位数nの巡回群とする．
このとき，Gの元a^kの位数は$n/(n,k)$となる．
ただし,(n,k)はnとkの最大公約数を表す．
$|a^k|=n/(n,k)$

11

位数

群Gの元aに対して，$a^n=e$となるような
最小の正の整数をaの位数という．そのような
整数が無いとき，aの位数は無限という．
$|a|$でaの位数を表す．aの位数が無限のとき，
$|a|=\infty$

例題　加法群Z_{12}において，各元の位数を求めよ

$|0|=1,|1|=12,|2|=6,|3|=4,|4|=3,$
$|5|=12,\{5,10,3,8,1,6,11,4,9,2,7,0\}$
$|6|=2,|7|=12,|8|=3,|9|=4,|10|=5,|11|=12$

12

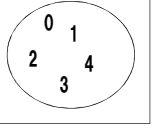
０６．群の定義

代数Ⅰ

代数系

集合　＋　代数的構造　＝　代数系

何かしらの数の集まり



四則演算などの
公理や定義

任意の演算

a＊b＝｜a－b｜

亜群
半群
モノイド
群

環
体

2

群

・空でない集合Gに対して，ある演算＊が定義

（１）閉鎖律

（２）結合律　$(x*y)*z = x*(y*z)$

（３）単位元 e の存在　$e*x = x*e = x$

（４）逆元 x' の存在　$x'*x = x*x' = e$

（５）可換律　$x*y = y*x$

可換群

位数n　$|G| = n$

亜群，半群，モノイド，群

閉鎖律（ある演算に関して閉じている）

集合Ｓは演算＊に関して亜群（groupid）

結合律（　（ｘ＊ｙ）＊ｚ＝ｘ＊（ｙ＊ｚ）　）

半群（semi-group）

単位元（　ｅ＊ｘ＝ｘ＊ｅ=ｘ　）

モノイド（monoid）

逆元（　ｘ’＊ｘ＝ｘ＊ｘ’=ｅ　）

群（group）

4

整数全体は加法に関して群か？

5

整数全体は乗法に関して群か？

6

部分群

群Gの空でない部分集合をHとする．
HがGの部分群であるための必要十分条件は
Hが次の条件(1)と(2)を満足していることである．
(1)$\forall a,b\in H \Rightarrow a\circ b\in H$
(2)$\forall a\in H \Rightarrow a^{-1}\in H$
さらに(1),(2)は，次の条件(3)と同値である．
(3)$\forall a,b\in H \Rightarrow a\circ b^{-1}\in H$

7

既約剰余類の部分群

$Z_6^{\times}=\{1,5\}$

×	1	5
1	1	5
5	5	1

自明な部分群
単位元のみの部分群$\{1\}$
全体集合$\{1,5\}$

$\{1\},\{1,5\}$　ともに正規部分群

8

既約剰余類の部分群

$Z_9^{\times}=\{1,2,4,5,7,8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

自明な部分群
$\{1\},\{1,2,4,5,7,8\}$
生成元は2と5
4からは{4,7,1}
7からは{7,4,1}
8からは{8,1}

すべて正規部分群

9

既約剰余類の部分群

$Z_{12}^{\times}=\{1,5,7,11\}$

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

自明な部分群
$\{1\},\{1,5,7,11\}$
5からは{5,1}
7からは{7,1}
11からは{11,1}
既約剰余類は乗法において可換
すべて正規部分群

10

巡回群

aの累乗の全体からなるGの部分集合
$<a>=\{a^n \mid n\in Z\}$はGの部分群になる．
また，この群はaを含むGの最小の部分群である．
部分群$<a>$をaで生成されたGの巡回部分群という．

Gをaによって生成される位数nの巡回群とする．
このとき，Gの元a^kの位数は$n/(n,k)$となる．
ただし,(n,k)はnとkの最大公約数を表す．
$|a^k|=n/(n,k)$

11

位数

群Gの元aに対して，$a^n=e$となるような
最小の正の整数をaの位数という．そのような
整数が無いとき，aの位数は無限という．
$|a|$でaの位数を表す．aの位数が無限のとき，
$|a|=\infty$

例題　加法群Z_{12}において，各元の位数を求めよ

$|0|=1,|1|=12,|2|=6,|3|=4,|4|=3,$
$|5|=12,\{5,10,3,8,1,6,11,4,9,2,7,0\}$
$|6|=2,|7|=12,|8|=3,|9|=4,|10|=5,|11|=12$

12

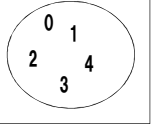
０６．群の定義

代数Ⅰ

代数系

集合　＋　代数的構造　＝　代数系

何かしらの数の集まり



四則演算などの
公理や定義

任意の演算

a＊b＝｜a－b｜

亜群
半群
モノイド
群

環
体

2

群

・空でない集合Gに対して，ある演算＊が定義

（１）閉鎖律

（２）結合律　$(x*y)*z = x*(y*z)$

（３）単位元 e の存在　$e*x = x*e = x$

（４）逆元 x' の存在　$x'*x = x*x' = e$

（５）可換律　$x*y = y*x$

可換群

位数n　$|G| = n$

亜群，半群，モノイド，群

閉鎖律（ある演算に関して閉じている）

集合Ｓは演算＊に関して亜群（groupid）

結合律（　（ｘ＊ｙ）＊ｚ＝ｘ＊（ｙ＊ｚ）　）

半群（semi-group）

単位元（　ｅ＊ｘ＝ｘ＊ｅ=ｘ　）

モノイド（monoid）

逆元（　ｘ’＊ｘ＝ｘ＊ｘ’=ｅ　）

群（group）

4

整数全体は加法に関して群か？

5

整数全体は乗法に関して群か？

6

部分群

群Gの空でない部分集合をHとする．
HがGの部分群であるための必要十分条件は
Hが次の条件(1)と(2)を満足していることである．
(1)$\forall a,b\in H \Rightarrow a\circ b\in H$
(2)$\forall a\in H \Rightarrow a^{-1}\in H$
さらに(1),(2)は，次の条件(3)と同値である．
(3)$\forall a,b\in H \Rightarrow a\circ b^{-1}\in H$

7

既約剰余類の部分群

$Z_6^{\times}=\{1,5\}$

×	1	5
1	1	5
5	5	1

自明な部分群
単位元のみの部分群$\{1\}$
全体集合$\{1,5\}$

$\{1\},\{1,5\}$　ともに正規部分群

8

既約剰余類の部分群

$Z_9^{\times}=\{1,2,4,5,7,8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

自明な部分群
$\{1\},\{1,2,4,5,7,8\}$
生成元は2と5
4からは{4,7,1}
7からは{7,4,1}
8からは{8,1}

すべて正規部分群

9

既約剰余類の部分群

$Z_{12}^{\times}=\{1,5,7,11\}$

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

自明な部分群
$\{1\},\{1,5,7,11\}$
5からは{5,1}
7からは{7,1}
11からは{11,1}
既約剰余類は乗法において可換
すべて正規部分群

10

巡回群

aの累乗の全体からなるGの部分集合
$<a>=\{a^n \mid n\in Z\}$はGの部分群になる．
また，この群はaを含むGの最小の部分群である．
部分群$<a>$をaで生成されたGの巡回部分群という．

Gをaによって生成される位数nの巡回群とする．
このとき，Gの元a^kの位数は$n/(n,k)$となる．
ただし,(n,k)はnとkの最大公約数を表す．
$|a^k|=n/(n,k)$

11

位数

群Gの元aに対して，$a^n=e$となるような
最小の正の整数をaの位数という．そのような
整数が無いとき，aの位数は無限という．
$|a|$でaの位数を表す．aの位数が無限のとき，
$|a|=\infty$

例題　加法群Z_{12}において，各元の位数を求めよ

$|0|=1,|1|=12,|2|=6,|3|=4,|4|=3,$
$|5|=12,\{5,10,3,8,1,6,11,4,9,2,7,0\}$
$|6|=2,|7|=12,|8|=3,|9|=4,|10|=5,|11|=12$

12

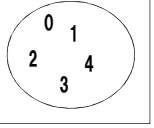
０６．群の定義

代数Ⅰ

代数系

集合　＋　代数的構造　＝　代数系

何かしらの数の集まり



四則演算などの
公理や定義

任意の演算

a＊b＝｜a－b｜

亜群
半群
モノイド
群

環
体

2

群

・空でない集合Gに対して，ある演算＊が定義

（１）閉鎖律

（２）結合律　$(x*y)*z = x*(y*z)$

（３）単位元 e の存在　$e*x = x*e = x$

（４）逆元 x' の存在　$x'*x = x*x' = e$

（５）可換律　$x*y = y*x$

可換群

位数n　$|G| = n$

亜群，半群，モノイド，群

閉鎖律（ある演算に関して閉じている）

集合Ｓは演算＊に関して亜群（groupid）

結合律（　（ｘ＊ｙ）＊ｚ＝ｘ＊（ｙ＊ｚ）　）

半群（semi-group）

単位元（　ｅ＊ｘ＝ｘ＊ｅ=ｘ　）

モノイド（monoid）

逆元（　ｘ’＊ｘ＝ｘ＊ｘ’=ｅ　）

群（group）

4

整数全体は加法に関して群か？

5

整数全体は乗法に関して群か？

6

部分群

群Gの空でない部分集合をHとする．
HがGの部分群であるための必要十分条件は
Hが次の条件(1)と(2)を満足していることである．
(1)$\forall a,b\in H \Rightarrow a\circ b\in H$
(2)$\forall a\in H \Rightarrow a^{-1}\in H$
さらに(1),(2)は，次の条件(3)と同値である．
(3)$\forall a,b\in H \Rightarrow a\circ b^{-1}\in H$

7

既約剰余類の部分群

$Z_6^{\times}=\{1,5\}$

×	1	5
1	1	5
5	5	1

自明な部分群
単位元のみの部分群$\{1\}$
全体集合$\{1,5\}$

$\{1\},\{1,5\}$　ともに正規部分群

8

既約剰余類の部分群

$Z_9^{\times}=\{1,2,4,5,7,8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

自明な部分群
$\{1\},\{1,2,4,5,7,8\}$
生成元は2と5
4からは{4,7,1}
7からは{7,4,1}
8からは{8,1}

すべて正規部分群

9

既約剰余類の部分群

$Z_{12}^{\times}=\{1,5,7,11\}$

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

自明な部分群
$\{1\},\{1,5,7,11\}$
5からは{5,1}
7からは{7,1}
11からは{11,1}
既約剰余類は乗法において可換
すべて正規部分群

10

巡回群

aの累乗の全体からなるGの部分集合
$<a>=\{a^n \mid n\in Z\}$はGの部分群になる．
また，この群はaを含むGの最小の部分群である．
部分群$<a>$をaで生成されたGの巡回部分群という．

Gをaによって生成される位数nの巡回群とする．
このとき，Gの元a^kの位数は$n/(n,k)$となる．
ただし,(n,k)はnとkの最大公約数を表す．
$|a^k|=n/(n,k)$

11

位数

群Gの元aに対して，$a^n=e$となるような
最小の正の整数をaの位数という．そのような
整数が無いとき，aの位数は無限という．
$|a|$でaの位数を表す．aの位数が無限のとき，
$|a|=\infty$

例題　加法群Z_{12}において，各元の位数を求めよ

$|0|=1,|1|=12,|2|=6,|3|=4,|4|=3,$
$|5|=12,\{5,10,3,8,1,6,11,4,9,2,7,0\}$
$|6|=2,|7|=12,|8|=3,|9|=4,|10|=5,|11|=12$

12

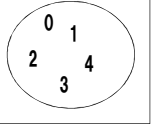
０６．群の定義

代数Ⅰ

代数系

集合　＋　代数的構造　＝　代数系

何かしらの数の集まり



四則演算などの
公理や定義

任意の演算

a＊b＝｜a－b｜

亜群
半群
モノイド
群

環
体

2

群

・空でない集合Gに対して，ある演算＊が定義

（１）閉鎖律

（２）結合律　$(x*y)*z = x*(y*z)$

（３）単位元 e の存在　$e*x = x*e = x$

（４）逆元 x' の存在　$x'*x = x*x' = e$

（５）可換律　$x*y = y*x$

可換群

位数n　$|G| = n$

亜群，半群，モノイド，群

閉鎖律（ある演算に関して閉じている）

集合Ｓは演算＊に関して亜群（groupid）

結合律（　（ｘ＊ｙ）＊ｚ＝ｘ＊（ｙ＊ｚ）　）

半群（semi-group）

単位元（　ｅ＊ｘ＝ｘ＊ｅ=ｘ　）

モノイド（monoid）

逆元（　ｘ’＊ｘ＝ｘ＊ｘ’=ｅ　）

群（group）

4

整数全体は加法に関して群か？

5

整数全体は乗法に関して群か？

6

部分群

群Gの空でない部分集合をHとする．
HがGの部分群であるための必要十分条件は
Hが次の条件(1)と(2)を満足していることである．
(1)$\forall a,b\in H \Rightarrow a\circ b\in H$
(2)$\forall a\in H \Rightarrow a^{-1}\in H$
さらに(1),(2)は，次の条件(3)と同値である．
(3)$\forall a,b\in H \Rightarrow a\circ b^{-1}\in H$

7

既約剰余類の部分群

$Z_6^{\times}=\{1,5\}$

×	1	5
1	1	5
5	5	1

自明な部分群
単位元のみの部分群$\{1\}$
全体集合$\{1,5\}$

$\{1\},\{1,5\}$　ともに正規部分群

8

既約剰余類の部分群

$Z_9^{\times}=\{1,2,4,5,7,8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

自明な部分群
$\{1\},\{1,2,4,5,7,8\}$
生成元は2と5
4からは{4,7,1}
7からは{7,4,1}
8からは{8,1}

すべて正規部分群

9

既約剰余類の部分群

$Z_{12}^{\times}=\{1,5,7,11\}$

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

自明な部分群
$\{1\},\{1,5,7,11\}$
5からは{5,1}
7からは{7,1}
11からは{11,1}
既約剰余類は乗法において可換
すべて正規部分群

10

巡回群

aの累乗の全体からなるGの部分集合
$<a>=\{a^n \mid n\in Z\}$はGの部分群になる．
また，この群はaを含むGの最小の部分群である．
部分群$<a>$をaで生成されたGの巡回部分群という．

Gをaによって生成される位数nの巡回群とする．
このとき，Gの元a^kの位数は$n/(n,k)$となる．
ただし,(n,k)はnとkの最大公約数を表す．
$|a^k|=n/(n,k)$

11

位数

群Gの元aに対して，$a^n=e$となるような
最小の正の整数をaの位数という．そのような
整数が無いとき，aの位数は無限という．
$|a|$でaの位数を表す．aの位数が無限のとき，
$|a|=\infty$

例題　加法群Z_{12}において，各元の位数を求めよ

$|0|=1,|1|=12,|2|=6,|3|=4,|4|=3,$
$|5|=12,\{5,10,3,8,1,6,11,4,9,2,7,0\}$
$|6|=2,|7|=12,|8|=3,|9|=4,|10|=5,|11|=12$

12

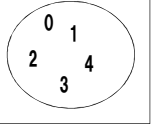
０６．群の定義

代数Ⅰ

代数系

集合　＋　代数的構造　＝　代数系

何かしらの数の集まり



四則演算などの
公理や定義

任意の演算

a＊b＝｜a－b｜

亜群
半群
モノイド
群

環
体

2

群

・空でない集合Gに対して，ある演算＊が定義

（１）閉鎖律

（２）結合律　$(x*y)*z = x*(y*z)$

（３）単位元 e の存在　$e*x = x*e = x$

（４）逆元 x' の存在　$x'*x = x*x' = e$

（５）可換律　$x*y = y*x$

可換群

位数n　$|G| = n$

亜群，半群，モノイド，群

閉鎖律（ある演算に関して閉じている）

集合Ｓは演算＊に関して亜群（groupid）

結合律（　（ｘ＊ｙ）＊ｚ＝ｘ＊（ｙ＊ｚ）　）

半群（semi-group）

単位元（　ｅ＊ｘ＝ｘ＊ｅ=ｘ　）

モノイド（monoid）

逆元（　ｘ’＊ｘ＝ｘ＊ｘ’=ｅ　）

群（group）

4

整数全体は加法に関して群か？

5

整数全体は乗法に関して群か？

6

部分群

群Gの空でない部分集合をHとする．
HがGの部分群であるための必要十分条件は
Hが次の条件(1)と(2)を満足していることである．
(1)$\forall a,b\in H \Rightarrow a\circ b\in H$
(2)$\forall a\in H \Rightarrow a^{-1}\in H$
さらに(1),(2)は，次の条件(3)と同値である．
(3)$\forall a,b\in H \Rightarrow a\circ b^{-1}\in H$

7

既約剰余類の部分群

$Z_6^{\times}=\{1,5\}$

×	1	5
1	1	5
5	5	1

自明な部分群
単位元のみの部分群$\{1\}$
全体集合$\{1,5\}$

$\{1\},\{1,5\}$　ともに正規部分群

8

既約剰余類の部分群

$Z_9^{\times}=\{1,2,4,5,7,8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

自明な部分群
$\{1\},\{1,2,4,5,7,8\}$
生成元は2と5
4からは{4,7,1}
7からは{7,4,1}
8からは{8,1}

すべて正規部分群

9

既約剰余類の部分群

$Z_{12}^{\times}=\{1,5,7,11\}$

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

自明な部分群
$\{1\},\{1,5,7,11\}$
5からは{5,1}
7からは{7,1}
11からは{11,1}
既約剰余類は乗法において可換
すべて正規部分群

10

巡回群

aの累乗の全体からなるGの部分集合
$<a>=\{a^n \mid n\in Z\}$はGの部分群になる．
また，この群はaを含むGの最小の部分群である．
部分群$<a>$をaで生成されたGの巡回部分群という．

Gをaによって生成される位数nの巡回群とする．
このとき，Gの元a^kの位数は$n/(n,k)$となる．
ただし,(n,k)はnとkの最大公約数を表す．
$|a^k|=n/(n,k)$

11

位数

群Gの元aに対して，$a^n=e$となるような
最小の正の整数をaの位数という．そのような
整数が無いとき，aの位数は無限という．
$|a|$でaの位数を表す．aの位数が無限のとき，
$|a|=\infty$

例題　加法群Z_{12}において，各元の位数を求めよ

$|0|=1,|1|=12,|2|=6,|3|=4,|4|=3,$
$|5|=12,\{5,10,3,8,1,6,11,4,9,2,7,0\}$
$|6|=2,|7|=12,|8|=3,|9|=4,|10|=5,|11|=12$

12

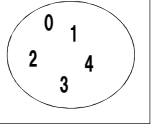
０６．群の定義

代数Ⅰ

代数系

集合　＋　代数的構造　＝　代数系

何かしらの数の集まり



四則演算などの
公理や定義

任意の演算

a＊b＝｜a－b｜

亜群
半群
モノイド
群

環
体

2

群

・空でない集合Gに対して，ある演算＊が定義

（１）閉鎖律

（２）結合律　$(x*y)*z = x*(y*z)$

（３）単位元 e の存在　$e*x = x*e = x$

（４）逆元 x' の存在　$x'*x = x*x' = e$

（５）可換律　$x*y = y*x$

可換群

位数n　$|G| = n$

亜群，半群，モノイド，群

閉鎖律（ある演算に関して閉じている）

集合Ｓは演算＊に関して亜群（groupid）

結合律（　（ｘ＊ｙ）＊ｚ＝ｘ＊（ｙ＊ｚ）　）

半群（semi-group）

単位元（　ｅ＊ｘ＝ｘ＊ｅ=ｘ　）

モノイド（monoid）

逆元（　ｘ’＊ｘ＝ｘ＊ｘ’=ｅ　）

群（group）

4

整数全体は加法に関して群か？

5

整数全体は乗法に関して群か？

6

部分群

群Gの空でない部分集合をHとする．
HがGの部分群であるための必要十分条件は
Hが次の条件(1)と(2)を満足していることである．
(1)$\forall a,b\in H \Rightarrow a\circ b\in H$
(2)$\forall a\in H \Rightarrow a^{-1}\in H$
さらに(1),(2)は，次の条件(3)と同値である．
(3)$\forall a,b\in H \Rightarrow a\circ b^{-1}\in H$

7

既約剰余類の部分群

$Z_6^{\times}=\{1,5\}$

×	1	5
1	1	5
5	5	1

自明な部分群
単位元のみの部分群$\{1\}$
全体集合$\{1,5\}$

$\{1\},\{1,5\}$　ともに正規部分群

8

既約剰余類の部分群

$Z_9^{\times}=\{1,2,4,5,7,8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

自明な部分群
$\{1\},\{1,2,4,5,7,8\}$
生成元は2と5
4からは{4,7,1}
7からは{7,4,1}
8からは{8,1}

すべて正規部分群

9

既約剰余類の部分群

$Z_{12}^{\times}=\{1,5,7,11\}$

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

自明な部分群
$\{1\},\{1,5,7,11\}$
5からは{5,1}
7からは{7,1}
11からは{11,1}
既約剰余類は乗法において可換
すべて正規部分群

10

巡回群

aの累乗の全体からなるGの部分集合
$<a>=\{a^n \mid n\in Z\}$はGの部分群になる．
また，この群はaを含むGの最小の部分群である．
部分群$<a>$をaで生成されたGの巡回部分群という．

Gをaによって生成される位数nの巡回群とする．
このとき，Gの元a^kの位数は$n/(n,k)$となる．
ただし,(n,k)はnとkの最大公約数を表す．
$|a^k|=n/(n,k)$

11

位数

群Gの元aに対して，$a^n=e$となるような
最小の正の整数をaの位数という．そのような
整数が無いとき，aの位数は無限という．
$|a|$でaの位数を表す．aの位数が無限のとき，
$|a|=\infty$

例題　加法群Z_{12}において，各元の位数を求めよ

$|0|=1,|1|=12,|2|=6,|3|=4,|4|=3,$
$|5|=12,\{5,10,3,8,1,6,11,4,9,2,7,0\}$
$|6|=2,|7|=12,|8|=3,|9|=4,|10|=5,|11|=12$

12