群、環、体について

暗号など、情報セキュリティで利用するアプリケーションでは、限られた範囲の整数を用いて様々な計算を行うことが多い。そのような「計算」を矛盾なく定義するために、演算体系を数学的に整理した概念である、群、環、体を理解しておく必要がある。

群（Group）とは

- 何らかの集合Gと、Gの要素間に演算○が定義されているとする。以下の条件を満たすとき、集合Gと演算○は群（Group）であるという

1. 【閉性】任意の2元a,b∈Gについて、a○b∈Gである
2. 【結合則】任意の元a,b,c∈Gに対して、a○(b○c)=(a○b)○cが成り立つ
3. 【単位元】任意の元a∈Gに対して、a○e=e○a=aとなる元e（単位元という）が存在する
4. 【逆元】任意の元a∈Gに対して、a○b=b○a=eとなる元b（aの逆元という）が存在する

（注）群の定義では、演算○が具体的にどのような演算であるかは決めていない。これらの性質を満たせば、どのような演算であっても群と呼ぶ

群（Group）の例（１）

- 整数の集合Zについて、加算+を考えると群である。

1. 整数と整数を加えると整数なので閉性を満たす
2. 任意の整数a,b,cについて、a+(b+c)=(a+b)+cであり結合則を満たす
3. 任意の整数aに対して、a+0=0+a=aであるので、0が単位元（演算が＋の場合、零元ともいう）
4. 任意の整数aに対して、a+(-a)=(-a)+a=0であるので、aの逆元は-aである

- 群において、a○b=b○a（交換法則）を満たすとき、可換群またはアーベル群と呼ぶ。
- 整数の集合は、乗算×の場合は群にならない。なぜか？

群（Group）の例（２）

- 法nの法演算（加算）において、数の範囲を0,1,…,n-1とする（例えば、n=5の場合、以下のような加算表ができる）

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

- これは、群になっている

1. 明らかに閉性を満たしている
2. 明らかに結合法則を満たしている
3. ０が単位元（零元）である
4. 任意の元について逆元がある（表の各行、各列について必ず0があるから）
   （例）2の逆元は3（2+3=0だから）
5. 明らかに交換法則が成り立つので可換群でもある

- このように、要素の数が有限個の群を有限群という
- 群Gの要素の数を位数と呼び、|G|と表す

群（Group）の例（３）

- 法p（pは素数）の法演算（乗算）において、数の範囲を1,2,…,p-1とする。例えば、p=5の場合、以下の演算表ができる。

×	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

- これは群になっている

1. 明らかに閉性を満たしている
2. 明らかに結合法則を満たしている
3. 単位元は1（a×1=1×a=aだから）
4. 任意の元について逆元がある（各行、各列に必ず1があるから）
   （例）2の逆元は3（2×3=1だから）
5. 明らかに交換法則が成り立つので、可換群でもある

- この例のような群は、Z_p^*と表記されることがある。

巡回群

- 前頁の例（Z_5^*）において、$g = 2$とし、$y = g^x (mod\ 5)$を考える。

x	1	2	3	4
y	2	4	3	1

- この群の全ての元は、g^xと表記できる。
- このような群は巡回群と呼ばれ、$G =< g >$ と表記される。
- 元gは生成元（または原始元）と呼ばれる。
- $a \in G$のとき$a^e = 1$となる最小の正整数eを元aの位数と呼ぶ
- この例では、元3も生成元である（確認してみよ）
- 元4は生成元ではない($4^2 = 1(mod\ 5)$だから)

環（Ring）とは

- 集合Rと、Rの元の間に2種類の演算（+と×とする）が定義されているとする。以下の条件を満たすとき、Rと演算(+,×)は環（Ring）であるという。

1. Rは演算+に関して可換群である
2. 【閉性】任意の2元a,b∈Rに対して、a×b∈Rである
3. 【結合則】任意の元a,b,c∈Rに対して、a×(b×c)=(a×b)×cが成立する
4. 【分配則】任意の元a,b,c∈Rに対して a×(b+c)=a×b+a×c および(b+c)×a=b×a+c×aが成立する。

- なお、上記に加えてa×b=b×a（交換法則）が成り立つときは、特に可換環と呼ばれる
- 有限群と同様、要素の数が有限個の環は有限環と呼ばれる
- （注）2種類の演算は必ずしも+と×でなくてもよいが、ここでは分かりやすいように+と×を使っている

環（Ring）の例（１）

- 整数の集合Zにおいて、加算＋と乗算×を考えると、環になっている

1. 整数は加算に関して可換群である（群の例（１）参照）
2. 整数同士を掛けた結果は整数であるので閉性を満たす
3. 整数の乗算に関して結合則を満たす
4. 整数の計算で分配法則が成り立つ

- 整数の乗算では交換法則が成り立つので可換環である
- （可換環でない例）整数を要素に持つ2×2の行列の集合について行列の和と積を考えると、これは環であるが可換環ではない（行列の乗算では一般に交換法則が成り立たないから）

環（Ring）の例（２）

- 法nの法演算（加算+と乗算×）において数の範囲を0,1,⋯,n-1とする。例えば、n=6の場合、以下のような演算表ができる

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

- これは環になっている

1. 加算について可換群である（群の例（２）で確認）
2. 乗算について閉じている
3. 乗算について結合法則が成立
4. 分配法則が成り立つ
5. 乗算について交換法則が成り立つので可換環である

- この例のような環は、整数の剰余類環と呼ばれ、多くの暗号方式で用いられている

体（Field）とは

- 集合FとFの元の間に2種類の演算（+と×とする）が定義されているとする。以下の条件を満たすとき、集合Fと演算(+,×)は体（Field）であるという

1. Fは可換環である
2. 任意の元a∈Fに対して、a×u=u×a=aとなる単位元u∈Fが存在する
3. 零元でない任意の元a∈Fに対して、a×b=b×a=uとなる元b∈F（aの（乗法に関する）逆元という）が存在する

- 有限個の要素からなる体は有限体と呼ばれる
- （注）3.の条件は、いわゆる割り算を定義していることになる

体（Field）の例（１）

- 実数の集合Rは通常の加算と乗算のもとで体である
1. 実数は可換環である
2. 単位元は1である
3. 0以外の任意の実数aについて、逆元は1/aである
- 複素数の集合や有理数（分数）の集合も体である
- 整数の集合は体ではない（例えば、数3の逆元（逆数）は整数の範囲では存在しない）
- {0,1}の集合で以下のような演算を考えると体である（有限体）

＋	0	1
0	0	1
1	1	0

×	0	1
0	0	0
1	0	1

1. 可換環になっている（確認してみよ）
2. 単位元は1
3. 0以外の任意の要素（１しかないが）に逆元がある
   （1×1=1だから1の逆元は1である）

体（Field）の例（２）

- 法p（pは素数）の法演算（加算+と乗算×）において、数の範囲を0,1,…,p-1とする。例えば、p=5の場合、以下のような演算表ができる

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

- これは体（有限体）になっている

1. 可換環である（環の例(2)参照）
2. 単位元は1
3. 零元でない任意の元に逆元がある（例えば4の逆元は4、4×4=1だから）

- （注）法が素数でない場合は体にならない。例えば、環の例（２）（法が6の場合）で、体ではない（条件3を満たさない）ことを確認してみよ
- この例のような体は、整数の剰余類体と呼ばれている