UEC 代数勉強会 02 回目

ONZI

January 9, 2021

冪乗

g^n の定義

g を群または環の元とするとき, $n \in \mathbb{Z}$ に対し, g^n を以下のように定める.

1. $n = 0$ のとき、$g^0 = e$(単位元)
2. $g^1 = g$, また $2 \leq n$ のときは $g^n = g^{n-1} \circ g$ により帰納的に求める
3. $n < 0$ のとき, $g^n = (g^{-}1)^{-n}$ と定める (ただし環の場合は情報の逆元 $g^{-}1$ が存在するときに限る)

指数法則

1. e を乗法の単位元とすれば $\forall n \in \mathbb{Z}$ に対し $e^n = e$ 特に $e^{-}1 = 0$
2. $(g^n)^{-1} = (g^n)^{-1}$ 特に, g に逆元が存在すれば, $\forall n > 0$ について g^n にも逆元が存在する.
3. $\forall m, n \in \mathbb{Z}$ に対し $g^m \circ g^n = g^{m+n}$ 特に $g^n \circ g^m$
4. $\forall m, n \in \mathbb{Z}$ に対し $(g^m)^n = g^{mn}$

計算例

冪乗の計算をする際には for 文とかで愚直に n 回かけるよりも効率が良い方法がある.

g^{16} の計算例

$$
\begin{aligned}
g_2 &= g \circ g \\
g_4 &= g_2 \circ g_2 \\
g_8 &= g_4 \circ g_4 \\
g_{16} &= g_8 \circ g_8
\end{aligned}
$$

計算例

冪乗の計算をする際には for 文とかで愚直に n 回かけるよりも効率が良い方法がある.

g^{15} の計算例

$$
\begin{aligned}
g_2 &= g \circ g \\
g_4 &= g_2 \circ g_2 \\
g_8 &= g_4 \circ g_4 \\
g_{16} &= ((g \circ g_2) \circ g_4) \circ g_8
\end{aligned}
$$

バイナリ法

$n = \varepsilon_0 + 2\varepsilon_1 + \cdots + 2^k\varepsilon_k,\ k = \lfloor \log_2 n \rfloor$ **したとき以下の方法で冪乗が計算できる**.

バイナリ法

1. $z = g$(g **の冪を入れる変数の初期化**)
2. $\varepsilon_0 = 0$ **なら** $x = e$, $\varepsilon = 1$ **なら** $x = g$(**答えw入れる変数の初期化**)
   $i = 1 \ldots k$ **について以下** 3,4 **を繰り返す**.
3. $z \circ z$ $(z \leftarrow g^{2^i})$
4. $\varepsilon_i = 1$ **のとき** $x \leftarrow x \circ z$

詳しくはこちら

https://compro.tsutaj.com//archive/170926_binary.pdf

バイナリ法

問題

自分の好きな言語でいいからバイナリ法を実装してなんか計算してみましょう (丸投げ).

いろいろ定義

減法の定義

$a + (-b)$ を $a - b$ と表記し，減法とよぶ．これは一次方程式 $x + b = a$ の唯一つの会である．この演算に対しても分配律 $c(a - b) = ca - cb$, $(a - b)c = ac - bc$ が成り立つ．

除法の定義

乗法が可能なとき，ab^{-1} を a/b あるいは $a \div b$ と記し除法と呼ぶ．これは一次方程式 $bx = a$ のただ一つの解である，

部分代数系

部分代数系

代数系 X の部分集合が, もとの代数系と同じ演算に関して同じ小売を満たしているとき, 部分 X と呼ぶ. $X =$ 群, 環, 体のとき, 順に部分群, 部分環, 部分体である. また, $X =$ 線形空間のときは線型部分空間となる.

部分群の例

置換群と交代群

対称群 S_n の部分群を一般に置換群とよぶ. 特に偶置換全体の集合 A_n は部分軍を成す. これ交代群と呼ぶ.

置換群と交代群

群 G の元 g を任意に取るときこれの冪乗の全体は G の部分軍を成す. これを g により生成される G の巡回部分群と呼ぶ. $g^n = e$ おなる正整数 n が存在すれば, 有限巡回群だが, そうでなければ加法群 Z と同系な可換群.

一般線形群

一般線形群 $GL(n, \mathbb{K})$ とは, 任意の体 K に対して, K の元を要素とする可逆な行列全体が成す群として定義される. これは, 線形空間 K^n の可逆な線形写像の全体がなす群とみなされ, 集合 K^n の可逆な線形写像の全体が成すぐんとみなされ, 集合 K^n の変換軍の中で, 線形性を持つ写像だけを集めて作られた部分群.

特殊線形群

特殊線形群 $SL(n,\mathbb{R})$ とは, 一般線形群 $GL(n,\mathbb{R})$ の中で, 行列式が 1 のものが成す部分群. 部分群をなすことは行列式が乗法的なことからわかる.

部分環の定義

例 1

有利整数環 $\mathbb{Z}$ の中で偶数全体は部分環を成す．ただし乗法の単位元を含まない

例 2

有理数体 $\mathbb{Q}$ を環とみなしたとき，整数の全体 $\mathbb{Z}$ は部分環となる．また分母が特定の素数の冪だけの有理数も部分感を成す．

例 3

実係数行列環 $M(n, \mathbb{R})$ の中で整数を要素とする行列の全体 $M(n, \mathbb{Z})$ は部分群となる．

部分体の例

例 1

実数体は複素数体の部分体である．有理数帯は実数体の部分体である．もちろん，有理数帯は複素数帯の部分体である．

例 2

実係数一変数有理関数体 $\mathbb{R}(\curvearrowleft)$ の中で実数の全体は部分帯を成す．これを $\mathbb{R}(\curvearrowleft)$ の整数帯と呼ぶ．

係数拡大

複素係数の一変数有理関数体 $\mathbb{C}(\curvearrowleft)$ の中で実係数のいち変数有理関数対 $\mathbb{R}(\curvearrowleft)$ は部分体を成す．前者を校舎の定数体拡大，係数拡大と呼ぶ．

部分代数系の判定条件

代数系 X の部分集合は部分代数系になるためには, 代数系の定義に必要な演算の結果がその部分集合飛びなさないこと (演算で閉じている) が必要かつ十分.

命題 1.7

群 G の部分集合 H が部分群となるためには, 次の条件が成り立っていることが必要十分である.

1. H は G の単位元 e を含む.
2. $x, y \in H$ なら $x \circ y \in H$
3. $x \in H$ なら $x^{-1} \in H$

実は次を仮定するだけでいい

命題 1.8

群 G **の部分集合** H **が部分群となるためには, 次の条件が成り立っていることが必要十分である**.

1. $\forall x, y \in H$ **に対し** $x \circ y^{-1}$ **を含む**.

命題 1.7$\rightarrow$ **命題** 1.8 **は命題** 1.7(3) **から** $y^{-1} \in H$ **がわかり, 次に命題** 1.7(2) **から** $x \circ y^{-1} \in H$ **がわかる**. **逆に, 命題** 1.8$\rightarrow$ **命題** 1.7 **は** $\forall x \in H$ **に対し,** $x = y$ **とすれば** $x \circ x^{-1} = e \in H$. $\forall y \in H$ **に対して以下の式が成り立つ**.

$$e \circ y^{-1} = y^{-1} \in H$$

したがって $x \circ y = x \circ (y^{-1})^{-1} \in H$

環と体の条件

命題 1.9

環 A の空でない部分集合 B が部分環となるためには, 次の条件が成り立っていることが必要十分である.

1. $\forall x, y \in B$ **に対し** $x - y \in B$.
2. $\forall x, y \in B$ **に対し** $xy \in B$.

命題 1.10

環 K の二つ以上の元を含む部分集合 L が部分体となるためには, 次の条件が成り立っていることが必要十分である.

1. $\forall x, y \in L$ **に対し** $x - y \in L$.
2. $\forall x, y \in L \backslash 0$ **に対し** $x/y \in L$.

演習問題

教科書問 1.16

教科書問 1.16 **をやりましょう (問題略)**

命題 1.11

体 K について, 次のいずれか一方が成立する.

1. **$x \in K^{\mp}$ なら, 任意の正整数 n について, $nx \neq 0$.**
2. **素数 p で, $\forall x \in K$ に対し, $px = 0$ となるようなものがただ一つ存在する.**

前者のとき, 体 K の標数は 0 であるといい, 後者のときは, 標数 p であるという, また後者のような体を総称して正標数の体と呼ぶ.

$n \cdot 1 := 1 + \cdots + 1$ を考えると, これが任意の正整数 n について 0 以外か 0 になるかのどちらかであることは明らか. $n \cdot 1 = 0$ のとき $\forall x \in K$ について $n \cdot x = n(1 \cdot x) = (n \cdot 1)x = 0 \cdot x = 0$. よって、このような n の最小値が素数となることを言えば良い. もし, $n = pq$, $1 < p$, $q < n$ と因数分解されたら次のように変形できる.

$$0 = n \cdot 1 = (1 + \cdots + 1) \times (1 + \cdots + 1) = p \cdot 1 \times q \cdot 1$$

故に, $p \cdot = 0$ または $q \cdot = 0$. これは n の最小性に反する.

系 1.12

体 K の標数が $p \iff K$ は $\mathbb{F}_p$ を部分帯として含む. 体 K の標数 $0 \iff K$ は有理数体 $\mathbb{Q}$ を部分体として含む. 特に, 有限体は必ず正標数であり, 標数 0 の体は無限体である.