121020 初版 121128 更新

http://goo.gl/MFRFj

整式再考 1

1.1 整式

このペーパーの目的は整式の考えを再確認することにある。

整式とは x^3-2x^2+x-3 のようなものであった。ここでは不定元が 1 文字 x だけの整式を考える。

まず x は集合 $\mathcal{M}$ の元であるとする。$\mathcal{M}$ は実数のような気がしているが，x^2+x+1 の零点すなわち方程式 $x^2+x+1=0$ の解を考えると，それは実数には存在しない。だから，x はその係数体よりちょっと大きいようである。

x には (すなわち $\mathcal{M}$ の元には) 実数が左から作用している。

どういうことかというと，

まず，集合 $\mathcal{M}$ には加法と乗法が定義されていて，どちらも，結合法則と交換法則が成り立つ。また，分配法則も成り立つ。そして，加法の単位元 (通常は 0 とかく) と乗法の単位元 (通常は 1 とかく) がある。$\mathcal{M}$ は加法について閉じていることを仮定するので，$x+x$ を $2x$ と書くことにして自然数倍が考えられる。

$x+y\in\mathcal{M},\quad x\in\mathcal{M}$ ならば，$y\in\mathcal{M}$ が成り立つことを仮定するので，$-x\in\mathcal{M}$ である。これで整数倍を考えている。

$n\in\mathbb{Z}$ (n は整数), $nx\in\mathcal{M}$ ならば，$x\in\mathcal{M}$ が成り立つことを仮定するので，$\frac{1}{n}x\in\mathcal{M}$ である。これで有理数倍を考えている。

極限を考えないときは実数まで広くなくてもよい。

$\mathcal{M}$ には係数体として有理数が作用している。

x はそんな背景をしばらく忘れてただの文字であると見る。それを不定元という。

自然数 n について x^n は x の n 個の積である。x^0 は $\mathcal{M}$ によって異なるが，$\mathcal{M}$ の乗法の単位元である。通常は 1 である。x が行列であれば単位行列である。x の累乗については自然と指数法則が成り立つ。x^m と x^n は m と n が異なるとき，まとめることができない。ax^n ($a\in\mathbb{Q}$ 実数でなくても十分) をひとつの項として，項を並べて多項式を作ることができる。(代数和)

ちゃんというと係数を有理数とする 1 変数多項式環 $\mathbb{Q}[x]$ という。

1.2 整式の加法・減法

x^m と x^n は m と n が異なるとき，まとめることができない。

同じとき (同類項) は，分配法則を逆に使ってまとめることができる。$ax+bx=(a+b)x$

係数には負の数があるので，それで減法を定義することができる。

1.3 整式の乗法

分配法則 $kx(ax+b)=kax^2+kbx$ で，整式の乗法を定義することができる。この辺りは，教科書は実はしっかり書いてある。ただの計算 (TDN) なのだが，定義と性質の記述はぬかりがない。

1.4 倍数 約数

再度確認したいのだが，x は不定元である。ただの文字である。

$(x-1)(x-2)=x^2-3x+2$ なので，x^2-3x+2 は $x-1$ の倍数であるという。$x-1$ (あるいは $x-2$) は x^2-3x+2 の約数であるという。

すなわち，整式 A, B について，AB は A の (あるいは B の) 倍数である，A は (あるいは B は)AB の約数である，という。

$x^2-3x+2=(x-1)(x-2)$ なので，x^2-3x+2 は $x-1$ の倍数である
$x^2-2x+1=(x-1)^2$ なので，x^2-2x+1 は $x-1$ の倍数である
$x^2-x=(x-1)x$ なので，x^2-x は $x-1$ の倍数である
$x^2-1=(x-1)(x+1)$ なので，x^2-1 は $x-1$ の倍数である
$x^2+x-2=(x-1)(x+2)$ なので，x^2+x-2 は $x-1$ の倍数である
$x^2+2x-3=(x-1)(x+3)$ なので，x^2+2x-3 は $x-1$ の倍数である
$x^2+3x-4=(x-1)(x+4)$ なので，x^2+3x-4 は $x-1$ の倍数である

いくつかやってみると楽しいものである。

倍数には面白い性質がある。

倍数の性質

整式 A が整式 B の倍数ならば,
整式 Q に対して，$A-BQ$ も B の倍数である。
逆に，$A-BQ$ が B の倍数ならば，A は B の倍数である。

実際，$A=A'B$ とすると，$A-BQ=A'B-BQ=(A'-Q)B$
逆は，$A-BQ=BQ'$ とすると，$A=BQ+BQ'=B(Q+Q')$

整式の最高次の項の次数を整式の次数という。

除法の原理

整式 A, B に対して,
$A-BQ=R$ かつ R の次数は B の次数より小さい
となる整式 Q, R が存在する。R は 0 かも知れない。

121020 初版 121128 更新
http://goo.gl/MFRFj

整式再考 2

2.1 除法

このペーパーの目的は整式の考えを再確認することにある。

整式とは x^3-2x^2+x-3 のようなものであった。ここでは不定元が 1 文字 x だけの整式を考える。

除法の原理

整式 A, B に対して,
$A-BQ=R$ かつ R の次数は B の次数より小さい
となる整式 Q, R が存在する。R は 0 かも知れない。
Q を商，R を余りという。

剰余の定理

整式 A を $x-k$ で割った余りは A の x に k を代入したものに等しい。

実際，$A(x)=(x-k)Q+r$ ならば，$A(k)=r$

これは，A の約数を見つけて因数分解するとき，さらには方程式 $A(x)=0$ の解を求めることに使われる。

2.2 スーパー剰余の定理

剰余の定理は 1 次式で割った余りの場合だけだが，因数分解できない 2 次式 ($\mathbb{Q}$ 上既約な 2 次式という) で除法の原理を適用してみる。

スーパー剰余の定理

整式 A と $\mathbb{Q}$ 上既約な 2 次式 B について,
$A-BQ=ax+b$ となる Q, $ax+b$ を求めることと,
A に B の零点を代入することは同じことをしている。

2.3 具体的な利用

例 1

ω は x^2+x+1 の零点とする。

$x^2=(x^2+x+1)-x-1$ より，$\omega^2=-\omega-1$

$x^3=(x^2+x+1)(x)-x^2-x=(x^2+x+1)(x-1)+1$ より，$\omega^3=1$

$x^4=(x^2+x+1)(x^2-x)+x$ より，$\omega^4=\omega$

例 2

α は x^2-x+1 の零点とする。

$x^2=(x^2-x+1)+x-1$ より，$\alpha^2=\alpha-1$

$x^3=(x^2-x+1)(x)+x^2-x=(x^2-x+1)(x+1)-1$ より，$\alpha^3=-1$

$x^4=(x^2-x+1)(x^2+x)-x$ より，$\alpha^4=-\alpha$

$x^3+x^2=(x^2-x+1)(x+2)+x-2$ より，$\alpha^3+\alpha^2=\alpha-2$

例 3

β は x^2+x-1 の零点とする。

$x^2=(x^2+x-1)-x+1$ より，$\beta^2=-\beta+1$

$x^3=(x^2+x-1)(x)-x^2+x=(x^2+x-1)(x-1)+2x-1$ より，$\beta^3=2\beta-1$

$x^4=(x^2+x-1)(x^2-x)+2x^2-x=(x^2+x-1)(x^2-x+2)-3x+2$ より，$\beta^4=-3\beta+2$

$x^3+x^2=(x^2+x-1)(x)+x$ より，$\beta^3+\beta^2=\beta$

1			1	−1	2
−1		−1	1	−2	
	1	−1	2	−3	2

(x^4 を x^2+x-1 で割った余りが $-3x+2$ であることを計算した図。ひとつ前まででやめると, x^3 の余りが $2x-1$ であることもわかる。)

行列の累乗への応用

例 4

$A=\begin{pmatrix} 1 & -1 \\ 7 & -3 \end{pmatrix}$ は $X^2+2X+4E$ の零点である。(ハミルトン・ケーリーの定理)

$X^2=(X^2+2X+4E)-2X-4E$ より，$A^2=-2A-4E$

$X^3=(X^2+2X+4E)(X)-2X^2-4X=(X^2+2X+4E)(X-2E)+8E$ より，$A^3=8E$

$X^4=(X^2+2X+4E)(X^2-2X)+8X$ より，$A^4=8A$

-4			−4	8	0
−2		−2	4	0	
	1	−2	0	8	0

(x^4 を x^2+2x+4 で割った余りが $8x$ であることを計算した図。ひとつ前まででやめると, x^3 の余りが 8 であることもわかる。)