代数学 I 特論要約 NO.4

今日のテーマ

有限体上の方程式、根の添加

元の個数が有限個の体を有限体と呼ぶ。この講義で既にでて来たのは $\mathbb{F}_p$ (p は素数) であるが、それ以外にも存在する。

有限体上の方程式は総当たりで解くことができる。

例えば $\mathbb{F}_{11}$ 上の方程式 $X^2-2=0$ は解をもたないが、$X^2-3=0$ は解 ± 5 をもつことがわかる。

$\mathbb{F}_{11}$ には 2 の平方根がない訳だが、($\mathbb{R}$ に $\sqrt{-1}$ を付け加えて $\mathbb{C}$ を得たように) $\mathbb{F}_{11}$ を拡大した体 K をつくって、K では 2 が平方根をもつようにできる。

命題 4.1. 体 K 上の一変数既約多項式 $f(X) \in K[X]$ にたいして、$I=f(X)K[X]$ とおくと、I は $K[X]$ のイデアルで、$L=K[X]/I$ は体である。f の次数を d とすると、L は K 上の d 次元ベクトル空間の構造をあわせもち、K が有限体ならば L の元の個数は $\#(K)^d$ 個である。

上の命題の後半はもっと一般化できて、次のことがわかる。

補題 4.1. K は有限体で、L はその拡大体であるとする。このとき、

(1) L は K 上のベクトル空間の構造をもつ。(*L の K-ベクトル空間としての次元を $[L:K]$ とよび、L の K 上の拡大次数と呼ぶ。*)

(2) K が有限体で、拡大次数 $[L:K]$ も有限ならば、L も有限体で、

$$\#(L)=\#(K)^{[L:K]}$$

がなりたつ。

(3) 任意の有限体 K に対して、その標数 p は正で、K の元の個数 $\#(K)$ は p の巾である。

問題 4.1. 7 以上の素数 p を二つ選んで、おのおのの p について $X^2-3X+5=0$ が $\mathbb{F}_p$ で解をもつかどうか判定しなさい。