$\boxed{\text{問題 5-1}}$ Kは標数0の体であるとし，Lはその任意の拡大体であるとする．

K上の既約多項式がLの中に重根を持たないことを示せ． □

$\boxed{\text{解答例}}$ $f(x)=\sum_k a_k x^k \in L[x]$, $a_k \in L$ に対して，$f'(x)$ を $f'(x)=\sum_k a_k k x^{k-1}$ と定める．

Lの標数も0になるので，$\deg f(x) \geq 1$ ならば $\deg f'(x) = \deg f(x) - 1$ となる．

準備

今後自由に利用する．

($n=\deg f(x)$ とおくと，$f(x)=a_n x^n + \cdots + a_1 x + a_0$ なので，$f'(x) = n a_n x^{n-1} + \cdots + a_1$

なので $\deg f'(x) = n-1$. 注意 $\deg f(x)=0$ ならば $f(x)=\underset{\substack{\shortparallel \\ 0}}{a_0}$ の形になり，$f'(x)=0$ となり

$\deg f'(x) = \deg 0 = -\infty$)

$f(x)\in K[x]$ を任意にとる．

$f(x)$ と $f'(x)\in K[x]$ の最大公約多項式を $d(x)\in K[x]$ と書く． ← 最大公約多項式はEuclidの互助法によってK[x]内で計算される．

$f(x)$ が重根 $\alpha \in L$ を持つとき，$f(x)$ がK上既約でないこと（対偶）を示せばよい．

$f(x)$ の重根 $\alpha\in L$ が存在すると仮定する．

このとき，$f(x)=(x-\alpha)^2 g(x)$, $g(x)\in L[x]$ と書ける．

これ自体はL[x]の元でK[x]の元とは限らない．

$f'(x) = 2(x-\alpha)g(x) + (x-\alpha)^2 g'(x)$ より，$f(x)$ と $f'(x)$ は共通因子 $x-\alpha$ を持つ．

ゆえに $f(x)$ と $f'(x)$ の最大公約多項式 $d(x)\in K[x]$ の次数は1以上 $\deg f'(x) = \deg f(x)-1$ 以下になる．$f(x)$ は，そのような $d(x)\in K[x]$ で割り切れるので，K上既約ではない． □

$\boxed{\text{問題 5-2}}$ 正標数の体の標数が常に素数になることを示せ. □

(より一般に整域の定義の中に)

$\boxed{\text{解答例}}$ Kは正標数の体であると仮定する. (体の定義の中に $1 \neq 0$ が入っている.)

Nは正の整数であり, Kの中でのN個の1の和が0になると仮定する.

もしもNが素数でないならば $N = mn$ (m, n は2以上の整数) と書ける.

そのとき,

$$\underbrace{(\underbrace{1+\cdots+1}_{m}) + \cdots + (\underbrace{1+\cdots+1}_{m})}_{n} = 0.$$

両辺を $\underbrace{1+\cdots+1}_{m}$ でわると, $\underbrace{1+\cdots+1}_{n} = 0$ となって, Nより小さな正の整数 n で, Kの中での n 個の1の和が0になる. ($n < mn$ に注意せよ.)

ゆえに, 正の整数NでKの中でのN個の1の和が0になるものの最小値(=Kの標数)は素数でなければいけない. □

元の個数

例 素数 p に対して, $\mathbb{F}_p = \mathbb{Z}/(p) = \mathbb{Z}/p\mathbb{Z}$ とおく. $\mathbb{F}_p$ は標数 p で位数 p の体になる. □

問題5-3 p は素数であるとし，$L=\mathbb{F}_p(t)=$（1変数 t の $\mathbb{F}_p$ 上の有理函数体）とおく．
L の部分体 K と K 上の既約多項式 $F(x)\in K[x]$ の組 $(K, F(x))$ で
$F(x)$ が L の中に重根を持つものの1つを具体的に構成せよ． □

解答例 $K=\mathbb{F}_p(t^p)=\left\{\dfrac{f(t^p)}{g(t^p)}\,\middle|\, f(t), g(t)\in\mathbb{F}_p[t],\ g(t)\neq 0\right\}$ と L の部分体 K
を定め，$F(x)=x^p-t^p\in K[x]$ とおく．（$t\notin K$ が重要ポイント，$t^p\in K$）

$K=\mathbb{F}_p(t^p)$ は UFD $\mathbb{F}_p[t^p]$ の商体であり，t^p は $\mathbb{F}_p[t^p]$ の既約元である．
（$\mathbb{F}_p[t^p]$ は $t, t^2, \dots, t^{p-1}$ を含まないので，t^p は非自明な約数を持たない．）
ゆえに，$F(x)=x^p-t^p$ に，Eisensteinの判定法を適用すると，

$$t^p\nmid 1,\quad t^p\mid 0,\ \dots,\ t^p\mid 0,\quad t^p\mid(-t^p),\quad (t^p)^2\nmid t^p$$

なので，$F(x)=x^p-t^p$ は $K=\mathbb{F}_p(t^p)$ 上の既約多項式であることがわかる．

L の標数は p なので，$F(x)\underset{\uparrow}{=}(x-t)^p$ なので $F(x)$ は p 重根 $t\in L$ を持つ． □

次ページで証明

注意 上の $L/K=\mathbb{F}_p(t)/\mathbb{F}_p(t^p)$ は純非分離拡大の例になっている． □

注意　前ページの $(x-t)^p = x^p - t^p$ を示すためには次を示せば十分. □

補題　pは素数であるとし, 可換環Aの中でp個の1の和は0であると仮定する.
このとき, 任意の $a, b \in A$ について, $(a+b)^p = a^p + b^p$ かつ $(-a)^p = -a^p$.

証明　$p=2$のとき, $a+a = a(1+1) = a\cdot 0 = 0$ なので $-a=a$ となるので, $(-a)^p = -a^p$ が成立する. pが奇素数の場合は $(-a)^p = -a^p$ は自明である.

以下, Aの中でのn個の1の和を単にnと書く.

二項定理より,

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k, \quad \binom{p}{k} = \frac{p(p-1)\cdots(p-k+1)}{k!} \in \mathbb{Z}$$

$k=1,\dots,p-1$のとき, $\binom{p}{k}$ はpで割り切れるのでAの中で0になる. ゆえに,

$$(a+p)^p = \binom{p}{0} a^p + \binom{p}{p} b^p = a^p + b^p.$$

□

注意　$a \mapsto a^p$ はAからA自身への環の準同型になっている. ← $(ab)^p = a^p b^p$ は自明
それをAの <u>Frobenius準同型</u> と呼ぶ. □