代数入門問題集 [20070702]

4 多項式環、体

1. 標数 $p>0$ の体 F の任意の二元 a,b に対して $(a+b)^p=a^p+b^p$ が成り立つことを示せ。
2. F を標数 $p>0$ の有限体とする。写像 $f:F\to F$ $(f(a)=a^p)$ は全単射であることを示せ。
3. 元数が 4 の有限体 $\mathbb{F}_4$ を構成し、その加法と乗法に関する演算表を書け。
4. K を体とし $f(x)$ $(\neq 0)$ を n 次の K 係数多項式とする。このとき $f(a)=0$ となる $a\in K$ は高々 n 個であることを示せ。($f(a)=0$ となる $a\in K$ を $f(x)$ の**根**という。)
5. K を体とし、$f(x)$ を K 係数多項式とする。$f(x)=\sum_{i=0}^{n}a_ix^i$ に対して $f'(x)=\sum_{i=1}^{n}ia_ix^{i-1}$ とおいて、これを $f(x)$ の**形式的な微分**という。
   (1) 多項式の形式的な微分についても、積の微分に関する公式 $(fg)'=f'g+fg'$ は成り立つことを示せ。
   (2) $f(x)$ が重根 a をもつことと $f(a)=f'(a)=0$ となることが同値であることを示せ。ただし a が $f(x)$ の重根であるとは、多項式 $g(x)$ が存在して $f(x)=(x-a)^2g(x)$ と書けることとする。
6. K を体とする。写像 $f:K\to K$ が**多項式写像**であるとは、ある K 係数多項式 F が存在して、任意の $a\in K$ に対して $f(a)=F(a)$ となることとする。K が有限体であるとき、任意の写像 $f:K\to K$ は多項式写像であることを示せ。
7. 体 K 上の二つの多項式で、多項式としては異なり、等しい多項式写像を定めるものを具体的に一つ答えよ。
8. $\sqrt{2}+\sqrt{3}$ を根にもつ次数最小で最高次係数が 1 の有理数係数多項式を求めよ。
9. $\mathbb{Q}[\sqrt{2}]=\{a+b\sqrt{2}\mid a,b\in\mathbb{Q}\}$ とおく。$\mathbb{Q}[\sqrt{2}]$ は通常の演算で体であることを示せ。
10. R を整域とし R の部分集合 S は
    - $1\in S$, $0\notin S$
    - $a,b\in S$ ならば $ab\in S$

    を満たすものとする。このとき S を R の**積閉集合**という。直積集合 $S\times R$ に $sr'=s'r$ のときに $(s,r)\sim(s',r')$ として関係 $\sim$ を定める。
    (1) $\sim$ は同値関係であることを示せ。
    (2) (s,r) を含む $\sim$ による同値類を r/s と書くことにする。また同値類全体の集合を $S^{-1}R$ と書く。$S^{-1}R$ に加法と乗法を
    $$r/s+r'/s'=(rs'+r's)/(ss'),\quad (r/s)(r'/s')=(rr')/(ss')$$
    によって定めることができることを示せ。
    (3) 上の演算が、加法に関する交換法則、結合法則、乗法に関する結合法則、分配法則を満たすことを示せ。
    (4) 以上より $S^{-1}R$ は環の構造をもつ。これを R の S による**商環**という。特に S として $R-\{0\}$ をとれば、これは積閉集合である。このときの商環 $S^{-1}R$ は体であることを示せ。(この体を整域 R の**商体**という。)
    (5) $R=\mathbb{Z}$ のとき、その商体は何かを考えよ。
11. (1) 整域 R 上の一変数多項式環 $R[x]$ はまた整域であることを示せ。
    (2) 整域 R 上の n 変数多項式環 $R[x_1,x_2,\cdots,x_n]$ は整域であることを示せ。
12. K を体とする。
    (1) K 上の一変数多項式環 $K[x]$ は単項イデアル整域 (§3 問 **??** 参照) であることを示せ。
    (2) $f(x),g(x)\in K[x]$ に対して $(f(x),g(x))=\{f(x)a(x)+g(x)b(x)\mid a(x),b(x)\in K[x]\}$ とおくと、$(f(x),g(x))$ は $K[x]$ のイデアルであることを示せ。
    (3) (1), (2) より、$f(x),g(x)\in K[x]-\{0\}$ に対して $(f(x),g(x))=(h(x))$ となる $h(x)\in K[x]$ が存在する。最高次係数で割って $h(x)$ の最高次係数は 1 であると仮定してよい。このとき $h(x)$ を $f(x)$ と $g(x)$ の**最大公約元**といい、$\gcd(f,g)$ と書くことにする。$f(x)=g(x)q(x)+r(x)$, $\deg r(x)<\deg f(x)$ とするとき $\gcd(f,g)=\gcd(g,r)$ であることを示せ。
13. K を体とする。$f(x)\in K[x]$ を既約な多項式とする。このとき $K[x]/(f(x))$ は体であることを示せ。

14. $\mathbb{Q}[x]/(x^2-2)$ は本質的に $\mathbb{Q}[\sqrt{2}]$ (問 9 参照) と同じ体であることを示せ。(本質的に同じ体であるとは、集合としての全単射で、和と積を保つものが存在することをいうこととする。このとき二つの体は**同型**であるという。)

15. $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ (元数 2 の有限体) とする。

    (1) $\mathbb{F}_2$ 上の既約な 2 次多項式 $f(x)$ を見付けよ。

    (2) $\mathbb{F}_2[x]/(f(x))$ は本質的に問 3 の体 $\mathbb{F}_4$ と同じ体であることを示せ。

代数入門問題集・解答例と解説 [20070702]

4 多項式環、体

1. $(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i}$ であるが、$i \neq 0,\ p$ のとき $p \mid \binom{p}{i}$ なので主張が成り立つ。

2. $f(a) = f(b)$ とする。$a^p - b^p = 0$ である。

   - $p = 2$ ならば $a^2 - b^2 = a^2 + b^2 = (a+b)^2 = (a-b)^2$ である。
   - $p \neq 2$ ならば p は奇数なので $a^p - b^p = a^p + (-b)^p = (a-b)^p$ である。

   よっていずれの場合も $0 = (a-b)^p$ となる。F は体なので $a - b = 0$、すなわち $a = b$ となる。よって f は単射である。$|F| < \infty$ なので F から F への単射 f は全単射である。

3. $\mathbb{F}_4$ は $\mathbb{F}_2$ 上 2 次元ベクトル空間の構造をもつので、その基底を $1,\ \alpha$ とする。このとき $\mathbb{F}_4 = \{0,\ 1,\ \alpha,\ 1+\alpha\}$ である。また $\mathbb{F}_4$ の乗法群 $\mathbb{F}_4 - \{0\}$ は位数 3 の群になるので、それは巡回群である。以上より、以下の演算表を得る。

$+$	0	1	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

$\times$	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

   (一般に有限体 $\mathbb{F}_q$ の乗法群 $\mathbb{F}_q - \{0\}$ は素数位数でなくても巡回群になる。)

4. 次数に関する帰納法で示す。次数が 0 すなわち $f(x)$ が 0 でない定数ならば根はないので、主張は正しい。$f(x)$ を 1 次以上の次数の多項式とする。$f(x)$ が根をもたなければ主張は成り立つので、$f(x)$ は根 a をもつとする。因数定理により $f(x) = (x-a)g(x)$ と書けて $g(x)$ の次数は $n-1$ である。$b \neq a$ がやはり $f(x)$ の根であるとすると、$0 = f(b) = (b-a)g(b)$ である。$b - a \neq 0$ と K が体、よって整域であることにより $g(b) = 0$ である。したがって $f(x)$ の根は a であるか、または $g(x)$ の根である。帰納法の仮定により $g(x)$ の根は高々 $n-1$ 個なので、$f(x)$ の根は高々 n 個である。

   ($a \in K$ が多項式 $f(x)$ の根であることと $f(x) = (x-a)g(x)$ となる多項式 $g(x)$ が存在することは同値である。これを**因数定理**という。)

5. (1) 形式的な微分が和とスカラー倍を保つこと、すなわち $(f+g)' = f' + g',\ (af)' = af'\ (a \in K)$ となること、は計算によってすぐに確かめることができる。
   単項式の積 $x^n = x^m x^{n-m}$ について示す。$(x^n)' = nx^{n-1}$ であり、また $(x^m)'x^{n-m} + x^m(x^{n-m})' = mx^{n-1} + (n-m)x^{n-1} = nx^{n-1}$ なので、この場合には $(x^n)' = (x^m)'x^{n-m} + x^m(x^{n-m})'$ は成り立つ。
   一般の場合を考える。$f(x) = \sum_{i=0}^{m} a_i x^i,\ g(x) = \sum_{j=0}^{n} b_j x^j$ とする。

$$\begin{aligned}(f(x)g(x))' &= \sum_{i=0}^{m}\sum_{j=0}^{n} a_i b_j (x^{i+j})' = \sum_{i=0}^{m}\sum_{j=0}^{n} a_i b_j ((x^i)'(x^j) + (x^i)(x^j)' \\ &= \sum_{i=0}^{m}\sum_{j=0}^{n} a_i b_j (x^i)'(x^j) + \sum_{i=0}^{m}\sum_{j=0}^{n} a_i b_j (x^i)(x^j)' = f'(x)g(x) + f(x)g'(x)\end{aligned}$$

   が成り立つ。

   (2) a が $f(x)$ の重根であるとすると $f(x) = (x-a)^2 g(x)$ と書ける。このとき $f'(x) = 2(x-a)g(x) + (x-a)^2 g'(x)$ なので $f(a) = f'(a) = 0$ である。
   $f(a) = f'(a) = 0$ と仮定する。因数定理より $f(x) = (x-a)g(x)$ と書ける。$f'(x) = g(x) + (x-a)g'(x)$ より $0 = f'(a) = g(a)$ である。よって因数定理より $g(x) = (x-a)h(x)$ と書くことができ、a は $f(x)$ の重根である。

6. K の元数を q とする。K から K への写像は q^q 個ある。一方で、$q-1$ 次以下の多項式も q^q 個あるので、これらがすべて写像として異なることをいえばよい。

   $f(x), g(x)$ を $q-1$ 次以下の多項式とし、K から K への写像として等しいと仮定する。このとき $h(x) = f(x) - g(x)$ も $q-1$ 次以下の多項式であって、K の任意の元が $h(x)$ の根になる。$h(x) \neq 0$ ならば、問 4 によってその根の数は高々 $q-1$ 個であり、これは矛盾である。よって $h(x) = 0$、すなわち $f(x) = g(x)$ となる。

   (多項式 $x^q - x$ は K のすべての元を根にもち、写像としては 0 と等しくなる。)

7. (問 6 参照。) $K = \mathbb{Z}/2\mathbb{Z}$ とする。このとき $f(x) = x^2 + x$ は多項式としては 0 ではないが $f(0) = 0^2 + 0 = 0$, $f(1) = 1^2 + 1 = 0$ であり、0 と同じ多項式写像を与える。

8. $a = \sqrt{2} + \sqrt{3}$ とおく。
$$a^2 = 5 + 2\sqrt{6}, \quad a^3 = 11\sqrt{2} + 9\sqrt{3}, \quad a^4 = 49 + 20\sqrt{6}$$
である。ここで $\{1, a\}$, $\{1, a, a^2\}$,$\{1, a, a^2, a^3\}$ はいずれも $\mathbb{Q}$ 上一次独立であることが簡単に分かり、したがって a は 3 次以下の多項式の根にはならない。4 次式については $a^4 - 10a^2 + 1 = 0$ が成り立つことが分かるので、求める多項式は $x^4 - 10x^2 + 1$ である。

($x^4 - 10x^2 + 1 = 0$ の根は $\pm\sqrt{2} \pm \sqrt{3}$ である。)

9. $\mathbb{Q}[\sqrt{2}]$ が通常の和、差、積で閉じていること、すなわち $\mathbb{C}$ の部分環であることは明らかである。したがって $0 \neq x = a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ が逆元をもつことを示せばよい。もちろん x は $\mathbb{C}$ では逆元をもち、それは
$$x^{-1} = \frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2}$$
である。よって x^{-1} も $\mathbb{Q}[\sqrt{2}]$ の元であり、したがって $\mathbb{Q}[\sqrt{2}]$ は体である。

(同様にして、一般に $\mathbb{Q}[\sqrt{m}] = \{a + b\sqrt{m} \mid a, b \in \mathbb{Q}\}$ $(m \in \mathbb{Z})$ も体であることが分かる。)

10. (1) 対称律、反射律は明らかである。推移律を示す。$(s, r) \sim (s', r')$ かつ $(s', r') \sim (s'', r'')$ と仮定する。このとき $sr' = s'r$, $s'r'' = s''r'$ である。したがって $ss'r'' = ss''r' = s's''r$ である。ここで $s' \in S$ より $s' \neq 0$ で、かつ R が整域なので $sr'' = s''r$ となる。よって $(s, r) \sim (s'', r'')$ が成り立つ。

(2) $(r, s) \sim (a, b)$, $(r', s') \sim (a', b')$ と仮定する。仮定より $rb = sa$, $r'b' = s'a'$ が成り立っている。したがって
$$(rs' + r's)bb' = rs'bb' + r'sbb' = ss'ab' + ss'a'b = ss'(ab' + a'b)$$
となり $(rs' + r's, ss') \sim (ab' + a'b, bb')$ が成り立つ。よって和は矛盾なく定義される。また $rr'bb' = ss'aa'$ より $(rr', ss') \sim (aa', bb')$ であり、積も矛盾なく定義される。

(3)
- [加法に関する交換法則、結合法則] 加法についての交換法則が成り立つことはすぐに分かる。$(r/s + r'/s') + r''/s'' = (rs' + r's)/ss' + r''/s'' = (rs's'' + r'ss'' + r''ss')/ss's''$ であり $r/s + (r'/s' + r''/s'') = r/s + (r's'' + r''s')/s's'' = (rs's'' + r'ss'' + r''ss')/ss's''$ であるから結合法則は成り立つ。
- [乗法に関する結合法則] $(r/s \cdot r'/s') \cdot r''/s'' = (rr')/(ss') \cdot r''/s'' = (rr'r'')/(ss's'') = (r/s) \cdot (r'r''/s's'') = r/s \cdot (r'/s' \cdot r''/s'')$ であるから結合法則は成り立つ。
- [分配法則] $(r/s + r'/s') \cdot r''/s'' = (rs' + r's)/ss' \cdot r''/s'' = (rr''s' + r'r''s)/ss's'' = rr''s'/ss's'' + r'r''s/ss's''$ ここで R が整域で $s \neq 0$, $s' \neq 0$ であるから $(r/s + r'/s') \cdot r''/s'' = rr''/ss'' + r'r''/s's'' = r/s \cdot r''/s'' + r'/s' \cdot r''/s''$ となる。

(4) $S^{-1}R$ の零元は $0/1$ であり、単位元は $1/1$ であることに注意しておく。$r/s \in S^{-1}R - \{0\}$ とすると $0 \neq r \in R$, $0 \neq s \in R$ である。よって $s/r \in S^{-1}R$ となり $(r/s)(s/r) = 1_{S^{-1}R}$ となる。したがって 0 でない任意の元が正則元となり $S^{-1}R$ は体である。

(5) $\mathbb{Z}$ の商体は有理数体 $\mathbb{Q}$ である。

11. (1) $f(x) = \sum_{i=0}^{m} a_i x^i$, $g(x) = \sum_{j=0}^{n} b_j x^j$ とし、$f(x) \neq 0$, $g(x) \neq 0$ と仮定する。係数が 0 である項を略して $a_m \neq 0$, $b_n \neq 0$ と仮定してよい。このとき $f(x)g(x) = \sum_{k=0}^{m+n} \sum_{i+j=k} a_i b_j x^k$ であり、特に x^{m+n} の係数は $a_m b_n$ である。$a_m \neq 0$, $b_n \neq 0$ で R が整域であることにより $a_m b_n \neq 0$ である。よって $f(x)g(x) \neq 0$ である。

(2) n に関する帰納法で示す。$n = 1$ のときは (1) である。$n > 1$ とする。$R[x_1, x_2, \cdots, x_n]$ は $R[x_1, x_2, \cdots, x_{n-1}]$ 上一変数多項式環 $R[x_1, x_2, \cdots, x_{n-1}][x_n]$ と見ることができる。帰納法の仮定から $R[x_1, x_2, \cdots, x_{n-1}]$ は整域であるから (1) より $R[x_1, x_2, \cdots, x_n]$ も整域である。

12. (1) I を $K[x]$ の 0 でないイデアルとする。I の 0 でない元で、次数最小のものを $f(x)$ とする。($f(x)$ は一意的ではないが、その一つをとり固定する。)
$g(x) \in I$ とする。多項式の割り算を考えれば
$$g(x) = q(x)f(x) + r(x), \quad \deg(r(x)) < \deg(f(x))$$
となる $q(x)$, $r(x) \in K[x]$ が存在する。ここで $r(x) = g(x) - q(x)f(x) \in I$ となるので、$f(x)$ の次数の最小性から $r(x) = 0$ である。したがって $g(x) \in f(x)K[x]$ である。よって $I \subset f(x)K[x]$ となる。一方で $f(x) \in I$ なので $f(x)K[x] \subset I$ は明らかに成り立ち $I = f(x)K[x]$ となる。したがって I は単項イデアルである。
問 11 より $K[x]$ は整域なので $K[x]$ は単項イデアル整域である。

(2) $\alpha(x), \beta(x) \in (f(x), g(x))$, $h(x) \in K[x]$ とする。$\alpha(x) = f(x)a(x) + g(x)b(x)$, $\beta(x) = f(x)a'(x) + g(x)b'(x)$ となる $a(x),\ a'(x),\ b(x),\ b'(x) \in K[x]$ が存在する。このとき

$$\begin{aligned} \alpha(x) - \beta(x) &= f(x)(a(x) - a'(x)) + g(x)(b(x) - b'(x)) \in (f(x), g(x)) \\ h(x)\alpha(x) &= f(x)(h(x)a(x)) + g(x)(h(x)b(x)) \in (f(x), g(x)) \end{aligned}$$

であるから $(f(x), g(x))$ は $K[x]$ のイデアルである。

(3) (1) よりイデアルの次数最小の元はスカラー倍を除いて一意的に定まるので $(f(x), g(x)) = (g(x), r(x))$ を示せば十分である。$f(x) = g(x)q(x) + r(x) \in (g(x), r(x))$, $g(x) \in (g(x), r(x))$ であるから $(f(x), g(x)) \subset (g(x), r(x))$ が成り立つ。また $g(x) \in (f(x), g(x))$, $r(x) = f(x) - q(x)g(x) \in (f(x), g(x))$ より $(f(x), g(x)) \supset (g(x), r(x))$ が成り立つ。よって $(f(x), g(x)) = (g(x), r(x))$ である。

13. $g(x) \in K[x]$ に対して $g(x) + (f(x)) \in K[x]/(f(x))$ を $\overline{g(x)}$ と書くことにする。$\overline{g(x)} \neq 0$、すなわち $g(x) \notin (f(x))$ とする。このとき $\overline{g(x)}$ が逆元をもつことを示せばよい。$f(x)$ を割り切る多項式は 1 と $f(x)$ 自身しかないので、問 12 によって $\gcd(f(x), g(x)) = 1$ である。よって、やはり問 12 によって $f(x)a(x) + g(x)b(x) = 1$ となる $a(x), b(x) \in K[x]$ が存在する。このとき $\overline{g(x)b(x)} = \overline{1}$ となり、$\overline{b(x)}$ が $\overline{g(x)}$ の逆元である。

14. 自然な全射 $\mathbb{Q}[x] \to \mathbb{Q}[x]/(x^2 - 2)$ による $f(x) \in \mathbb{Q}[x]$ の像を $\overline{f(x)}$ と書くことにする。$\overline{x^2} = \overline{2}$ に注意すれば、任意の $f(x) \in \mathbb{Q}[x]$ は $\overline{a + bx}$ $(a, b \in \mathbb{Q})$ と一意的に表されることが分かる。このとき $\Gamma : \mathbb{Q}[x]/(x^2 - 2) \to \mathbb{Q}[\sqrt{2}]$ を $\Gamma(\overline{a + bx}) = a + b\sqrt{2}$ と定めれば、これは全単射である。Γ が和を保存することはすぐに分かる。また

$$\begin{aligned} \Gamma((\overline{a + bx})(\overline{c + dx})) &= \Gamma((ac + 2bd) + (ad + bc)x) = (ac + 2bd) + (ad + bc)\sqrt{2} \\ &= (a + b\sqrt{2})(c + d\sqrt{2}) = \Gamma(\overline{a + bx})\Gamma(\overline{c + dx}) \end{aligned}$$

となり、積を保存することも分かる。

15. (1) $x^2 + x + 1$ は既約である。(既約でないならば 0 または 1 を根にもたなくてはならない。)

(2) $\mathbb{F}_2[x]/(f(x)) = \{\overline{0},\ \overline{1},\ \overline{x},\ \overline{1 + x}\}$ である。加法、乗法の演算表を書けば問 3 の体と同じになることが分かる。(実際、問 3 の解答例にある α は $\alpha^2 + \alpha + 1$ を満たしている。)