一、数域P.

P是一些数的集合，包含0和1，且对加、减、乘、除の四则运算是封闭的，则称P为一个数域.

二、一元多项式.

1. 形式表达式 $a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0=f(x)$

称为数域P上的一元多项式. $a_i\in P$.

若 $a_n\neq 0$. a_nx^n —— 首项.

a_n —— 首项系数

a_ix^i —— 第i项.

a_i —— 第i项的系数.

$\partial(f(x))=n$.

2. 多项式的相等. $f(x)=g(x)$.

系数全为0的多项式称为零多项式.

3. 多项式的计算. 设 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0=\sum_{i=0}^{n}a_ix^i$.

$g(x)=b_mx^m+b_{m-1}x^{m-1}+\cdots+b_0=\sum_{j=0}^{m}b_jx^j$.

$a_n\neq 0$. $b_m\neq 0$.

1°. 加法 $f(x)+g(x)=\sum_{i=0}^{n}(a_i+b_i)x^i$. $n\geq m$.

在 $g(x)$ 中令 $b_{m+1}=b_{m+2}=\cdots=b_n=0$.

2°. 乘法 $f(x)g(x)=a_nb_mx^{n+m}+(a_nb_{m-1}+a_{n-1}b_m)x^{n+m-1}$

$+\cdots+(a_1b_0+a_0b_1)x+a_0b_0=\sum_{s=0}^{m+n}\left(\sum_{i+j=s}a_ib_j\right)x^s$.

3°. 减法. $f(x)-g(x)=f(x)+(-g(x))$.

显然有 $\partial(f(x)\pm g(x))\le \max(\partial(f(x)),\partial(g(x)))$.

$\partial(f(x)g(x))=\partial(f(x))+\partial(g(x))$. $f(x)g(x)\neq 0$.

4. 多项式加、乘法的运算律.

1°. $f(x)+g(x)=g(x)+f(x)$.

$f(x)g(x)=g(x)f(x)$.

2°. $(f+g)+h=f+(g+h)$

$(f\cdot g)\cdot h=f\cdot(g\cdot h)$.

3°. $f(x)[g(x)+h(x)]=f(x)g(x)+f(x)h(x)$

4°. 若 $f(x)g(x)=f(x)h(x)$. 且 $f(x)\neq 0$. 则 $g(x)=h(x)$.

5. 定义. 一元多项式环 $P[x]$.

§3. 整除的概念.

以下讨论均在数域P上的一元多项式环 $P[x]$ 中进行.

一. 带余除法.

1. 引例. $f(x)=3x^3+4x^2-5x+6$

$g(x)=x^2-3x+1$

$$
\begin{array}{r l}
 & 3x+13 \quad \text{商} \\
x^2-3x+1 \;\big) & 3x^3+4x^2-5x+6 \\
\text{除式} & 3x^3-9x^2+3x \\
\hline
 & 13x^2-8x+6 \\
 & 13x^2-39x+13 \\
\hline
 & 31x-7 \quad \text{余式}
\end{array}
$$

$f(x)=\underset{\text{商}q(x)}{(3x+13)}\underset{g(x)\text{除式}}{(x^2-3x+1)}+\underset{\text{余式}\ r(x)}{31x-7}$

$$
\begin{array}{c|l|l}
 & \quad f(x) & \\
x^2-3x+1 & 3x^3+4x^2-5x+6 & 3x+13 \\
\overset{\shortparallel}{g(x)} & 3x^3-9x^2+3x & 商.\ \overset{\shortparallel}{q(x)} \\
\hline
 & \quad 13x^2-8x+6 & \\
 & \quad 13x^2-39x+13 & \\
\hline
 & \qquad \underset{\shortparallel}{31x-7} & \\
 & \qquad r(x) &
\end{array}
$$

$$f(x)=(3x+13)(x^2-3x+1)+31x-7.$$

2. 带余除法.

定理. 对 $P[x]$ 中任意两个多项式 $f(x)$ 与 $g(x)$，其中 $g(x)\neq 0$.

一定有 $P[x]$ 中唯一的多项式 $q(x)$ 及唯一的多项式 $r(x)$，使得

$$f(x)=q(x)g(x)+r(x).$$

其中 $\partial(r(x))<\partial(g(x))$ 或 $r(x)=0$.

称 $q(x)$ 为 $g(x)$ 除 $f(x)$ 的商式 (商).

$r(x)$ 为 $g(x)$ 除 $f(x)$ 的余式 (余).

证明: 先证存在性.

若 $f(x)=0$. 则 $f(x)=0\cdot g(x)+0$.

取 $q(x)=r(x)=0$ 即可.

若 $f(x)\neq 0$. 设 $\partial(f(x))=n$. $\partial(g(x))=m$.

若 $n<m$，取 $q(x)=0$. $r(x)=f(x)$ 即可.

例: $f(x)=x$. $g(x)=x^2+1$

$f(x)=\underset{q(x)}{\underset{\shortparallel}{0}}\cdot g(x)+\underset{r(x)}{\underset{\shortparallel}{\underset{f(x).}{\underset{\shortparallel}{x}}}}$

若 $n\geq m$. (用数学归纳法证明).

假设当次数小于n时，$q(x)$，$r(x)$的存在性已经成立。

下面考虑次数为n的情形。

设 $f(x)=ax^n+\cdots \quad a\neq 0 \qquad n\geq m$.

$\quad\ g(x)=bx^m+\cdots \quad b\neq 0$.

令 $f_1(x)=f(x)-ab^{-1}x^{n-m}g(x)$

则 $\partial(f_1(x))<n$，或 $f_1(x)=0$.

对于后者，取 $q(x)=ab^{-1}x^{n-m}$，$r(x)=0$ 即可。

对于前者，$\partial(f_1(x))<n$，对 $f_1(x)$，$g(x)$ 由归纳假设

$\exists\ q_1(x)$及$r_1(x)$，使得

$f_1(x)=q_1(x)g(x)+r_1(x)$，$\partial(r_1(x))<\partial(g(x))$ 或 $r_1(x)=0$.

$$\begin{aligned}
f(x)&=f_1(x)+a\cdot b^{-1}\cdot x^{n-m}g(x)\\
&=q_1(x)g(x)+r_1(x)+a\cdot b^{-1}x^{n-m}g(x)\\
&=(q_1(x)+a\cdot b^{-1}x^{n-m})g(x)+r_1(x)\\
&=q(x)g(x)+r_1(x).
\end{aligned}$$

由第二数学归纳法，即证明了$q(x)$及$r(x)$的存在性。

$f(x)=2x^3$，$g(x)=3x$ 时

$f_1(x)=\underbrace{2x^3}_{f(x)}-\underbrace{\frac{2}{3}x^2\cdot 3x}_{\frac{a}{b}x^{3-1}\cdot g(x)}=0$.

$2x^3=$

$f(x)=2x^3+x \quad g(x)=3x+1$

$f_1(x)=2x^3+x-\frac{2}{3}x^2(3x+1)$

$=x-\frac{2}{3}x^2$

下面证明唯一性.

若 $f(x)=q(x)g(x)+r(x)$ 其中 $\partial(r(x))<\partial(g(x))$ 或 $r(x)=0$

$f(x)=q_1(x)g(x)+r_1(x)$. $\partial(r_1(x))<\partial(g(x))$ 或 $r_1(x)=0$.

$\Longrightarrow [q(x)-q_1(x)]g(x)=r_1(x)-r(x)$.

用反证法证明: 若 $q(x)\neq q_1(x)$.

由题设 $g(x)\neq 0 \Longrightarrow r_1(x)-r(x)\neq 0$.

且有 $\partial[q(x)-q_1(x)]+\partial(g(x))=\partial(r_1(x)-r(x))$.

但是 $\partial(g(x))>\partial(r_1(x)-r(x))$ 矛盾!

$\Longrightarrow q(x)=q_1(x)$. 因此 $r_1(x)=r(x)$. 即唯一性成立 ∎

二. 整除.

1. 定义. 称数域P上的多项式 $g(x)$ 整除 $f(x)$. 若有 存在 数域P上的多项式 $h(x)$, 使得 $f(x)=g(x)h(x)$ 成立.

若 $g(x)$ 整除 $f(x)$. 记为 $g(x)\mid f(x)$.

否则, 称 $g(x)$ 不能整除 $f(x)$. 记为 $g(x)\nmid f(x)$.

2. 当 $g(x)\mid f(x)$ 时. 称 $g(x)$ 为 $f(x)$ 的因式, 而 $f(x)$ 为 $g(x)$ 的倍式.

例. $f(x)=(x+1)(x+2)$.

$x+1$. $x+2$ 为 $f(x)$ 的因式. 而 $f(x)$ 为 $x+1$. $x+2$ 的倍式.

$f(x)=g(x)h(x)$.

3. 注意：带余除法及整除的区别.

整除中，$g(x)$ 可以为于 0.

带余除法中，要求 $g(x)\neq 0$.

4. $g(x)|f(x)$ 的条件.

Th. 对于数域 P 上任意两个多项式 $f(x)$, $g(x)$. 其中 $g(x)\neq 0$.

则 $g(x)|f(x) \Longleftrightarrow g(x)$ 除 $f(x)$ 的余式为 0.

证明："$\Longleftarrow$". 若 $g(x)$ 除 $f(x)$ 的余式 $r(x)=0$.

据带余除法 $f(x)=q(x)g(x)$

据整除的定义. $\Longrightarrow g(x)|f(x)$.

"$\Longrightarrow$". 已知 $g(x)|f(x)$.

由整除的定义, $\exists h(x)$, 使 $f(x)=g(x)h(x)+0$. $\Rightarrow r(x)=0$ ∎

5. 若 $g(x)|f(x)$ 且 $g(x)\neq 0$ 时. $g(x)$ 除 $f(x)$ 所得的商为 $q(x)$.

有时也用 $\frac{f(x)}{g(x)}$ 来表示.

$$\frac{f(x)}{g(x)}=q(x) \qquad f(x)=q(x)g(x).$$

6. 性质.

1°. $f(x)|f(x)$. （任意一个多项式整除它自己）.

$\because$ $f(x)=1\cdot f(x)$.

2°. $f(x) \mid 0$ （任意一个多项式整除0多项式）.

$\because\ 0 = 0 \cdot f(x)$.

3°. 若 $a \neq 0$，则 $a \mid f(x)$ （零次多项式整除任意一个多项式）.

$\because\ f(x) = a \cdot \frac{1}{a} f(x)$.

4°. 零多项式只能整除零多项式.

$\because$ 若 $0 \mid f(x)$.

$\Rightarrow f(x) = 0 \cdot g(x) = 0$.

作业 P29. 1—3.