习题课

2012-4-25

14.28 在$Z[x]$环中，令I为由x和2生成的一个理想，证明

(1) I是所有带偶常数的所有多项式的集合

证明：由题意$I=\{x\cdot f(x)+2\cdot g(x)\mid f(x),g(x)\in Z[x]\}$

而所有常数为偶数的多项式的集合可以表示为

$F=\{x\cdot f(x)+2k\mid f(x)\in Z[x], k\in Z\}$

思路 $\Rightarrow$ 证明$I\subseteq F$，$F\subseteq I$

显然$F\subseteq I$(令$k=g(x)$)

又对任意$p=x\cdot f(x)+2\cdot g(x)\in I$,

令$g(x)=xg'(x)+k$

则$p=x(f(x)+2g'(x))+2k\in F$

$\therefore I\subseteq F$ #

(2) I不是主理想

证明：反证法

假设I为主理想， 且$I=(a)=\{af(x)\mid f(x)\in Z[x]\}$, $a\in Z[x]$

$\because 2\in I$, $\therefore \exists f(x)\in Z[x]$, s.t. $af(x)=2$

$\therefore a$为常数，$a=\pm 1, \pm 2$

显然$a\neq \pm 1$(否则$1\in I$，矛盾)

$\therefore a=\pm 2$,

而$(\pm 2)=\{$偶系数多项式$\}$

矛盾，例如

$x+2\in I$，$\notin(\pm 2)$

#

(3) 商环Z[x]/I同构于Z_2

证明：环同态定理

构造φ:Z[x]→Z_2为

$$\varphi(f(x))=\begin{cases}[0], f(x)\text{的常数项为偶数}\\ [1], \ f(x)\text{的常数项为奇数}\end{cases}$$

易证φ为同态映射，+&·

又显然有kerφ=I

所以Z[x]/I≅Z_2

14.31 证明$Z_2[x]/(x^2+x+1)$是域，并写出加法乘法运算表

证明：利用定理14.17，只要证明x^2+x+1在$Z_2[x]$上不可约

参考例14.15, 说明[0],[1]均不是根，所以不可约

运算表略

14.32 证明$Q[x]/(x^2-2)$是域，写出其元素表达式，并求$(x^2-2)+3x+4$与$(x^2-2)+5x-6$之和与之积；求元素$(x^2-2)+x+1$的逆元

证明：证明x^2-2在$Q[x]$不可约

即证明$\sqrt{2}\notin Q$,略

$(x^2-2)+3x+4 \oplus (x^2-2)+5x-6=(x^2-2)+8x-2$

$(x^2-2)+3x+4 \otimes (x^2-2)+5x-6=(x^2-2)+2x+6$

设$(x^2-2)+x+1$的逆元为$(x^2-2)+ax+b$, 则

$(x+1)(ax+b) \equiv 1 \bmod x^2-2$

$\Rightarrow a=1, b=-1$

14.35 设R是环，R1是R的子环，I是R的理想，证明(R1+I)/I≅R1/(R1∩I),其中R1+I={a+b | a∈R1, b∈I}

证明：环同态定理

构造 $\varphi: R_1 \longrightarrow (R_1+I)/I$，$\varphi(r)=I+r, r\in R_1.$

则 $Ker\phi=\{r \mid r\in R_1, I+r=I+0=I\}$

$=\{r \mid r\in R_1, r\in I\}$

$=\{r \mid r\in R_1\cap I\}$

再证明φ为同态映射即可。#

14.36 (1)证明:Z[x]上的理想$I=(3, x^3-x^2+2x-1)$不是主理想。

证明：反证法

假设$I=(a)=\{af(x) \mid f(x)\in Z[x]\}$, $a\in Z[x]$

$\because 3\in I$, $\therefore a=\pm 1, \pm 3$

若$a=\pm 3$,显然$x^3-x^2+2x-1 \notin (\pm 3)$

$\therefore a=\pm 1$, $(a)=Z[x]$

假设存在$f(x)=\sum_{i=0}^{n}a_ix^i, g(x)=\sum_{i=0}^{m}b_ix^i$满足

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

易知$n=m+3$,且

$$3a_{m+3}+b_m=0 \Rightarrow b_m \equiv 0 \bmod 3$$

$$3a_{m+2}+b_{m-1}-b_m=0 \Rightarrow b_{m-1} \equiv 0 \bmod 3$$

$$3a_{m+1}+b_{m-2}-b_{m-1}+2b_m=0 \Rightarrow b_{m-2} \equiv 0 \bmod 3$$

$$3a_m+b_{m-3}-b_{m-2}+2b_{m-1}-b_m=0 \Rightarrow b_{m-3} \equiv 0 \bmod 3$$

...

$$3a_3+b_0-b_1+2b_2-b_3=0 \Rightarrow b_0 \equiv 0 \bmod 3$$

$$3a_2-b_0+2b_1-b_2=0$$

$$3a_1+2b_0-b_1=0$$

$$3a_0-b_0=1,$$矛盾!

(2) $Z[x]/I \cong Z_3[x]/(x^3-x^2+2x-1)$

证明：环同态定理

构造$\varphi: Z[x] \to Z_3[x]/(x^3-x^2+2x-1)$

对任意$p(x) \in Z[x]$,可以表示为

$p(x)=h(x) \cdot f(x)+3q(x)+ax^2+bx+c$, $ax^2+bx+c \in Z_3[x]$

则$\varphi(p(x))=(x^3-x^2+2x-1)+ax2+bx+c$

易证， φ为同态映射

而由I的定义易得，$\ker\varphi=I$

得证。

(3) $Z[x]/I$是否为整环。

解：是整环。

利用(2),证明$Z_3[x]/(x^3-x^2+2x-1)$为域

由于x^3-x^2+2x-1在$Z_3[x]$上不可约

([0],[1],[2]均不是根)

所以，$Z[x]/I$为域，为整环

15.2 证明有理数Q是素域。

采用反证法，假设Q存在真子域P，

因为P中单位元1既是Q中单位元，

所以$\forall m, n \in Z$,都有$m, n \in P$

于是$\forall mn^{-1} \in Q$,我们可以证明 $mn^{-1} \in P$

这样，就证明了 $Q \subseteq P$ 这与P为Q的真子域矛盾

因此，Q不存在真子域，又因为任何域都有素子域，故Q本身就是素域

15.3 F及F’为域，证明：如F≌F’，则charF=charF’。反之如何？

证明：注意分charF为0和素数p两种情况讨论。

因为 $F \cong F'$ ， 可设其同构映射为φ,有 $\varphi(e)=e', \varphi(0)=0'$

(1)若 charF=p, 则$pe' = p\varphi(e) = \varphi(pe) = \varphi(0) = 0'$

不妨设 $charF' = q$,于是 q | p,

又 $\varphi(qe) = q\varphi(e) = qe' = 0' = \varphi(0) \Rightarrow qe = 0$

所以 p | q, 因此p=q.

(2)若 charF=0, 且 $charF' = q \neq 0$

由 $\varphi(qe) = q\varphi(e) = qe' = 0' = \varphi(0) \Rightarrow qe = 0$

可得 $charF \neq 0$,矛盾

综合(1)(2)可知命题成立。

反之不一定成立。反例，charQ=charR=0,但Q与R不同构。

15.5 Q为有理数域，求[Q(i, $\sqrt{2}$):Q]，写出Q(i, $\sqrt{2}$)之元素表达式。

解：$Q(i,\sqrt{2})=Q(i)(\sqrt{2})$

$$Q(i)=\{a_1+b_1 i \mid \forall a_1,b_1\in Q\}$$

$$Q(i)(\sqrt{2})=\{c_1(a_1+b_1 i)+d_1(a_1+b_1 i)\sqrt{2} \mid \forall a_1,b_1,c_1,d_1\in Q\}$$

$$=\{a+bi+c\sqrt{2}+di\sqrt{2} \mid \forall a,b,c,d\in Q\}$$

$$[Q(i,\sqrt{2}):Q]=4$$

16.7在$Q(\sqrt[3]{2})$中求$1+\sqrt[3]{2}+\sqrt[3]{4}$之逆元。

解：$Q(\sqrt[3]{2})=\{a+b\sqrt[3]{2}+c\sqrt[3]{4} \mid a,b,c\in Q\}$

设 $(1+\sqrt[3]{2}+\sqrt[3]{4})^{-1}=a+b\sqrt[3]{2}+c\sqrt[3]{4}$

$$(1+\sqrt[3]{2}+\sqrt[3]{4})(a+b\sqrt[3]{2}+c\sqrt[3]{4})=1$$

展开，解出a=-1,b=1,c=0,

设 $(1+\sqrt[3]{2}+\sqrt[3]{4})^{-1}=-1+\sqrt[3]{2}$

补充1：在$Z_2[x]$上求x^7+x+1关于多项式$(x^8+x^4+x^3+x+1)$的逆。

解：求解$1 \equiv a(x^7+x+1) \bmod (x^8+x^4+x^3+x+1)$

即求$1= s(x^8+x^4+x^3+x+1) + t(x^7+x+1)$

利用Extended-GCD算法

$s=x^6+x^2+x+1$

$t=x^7$

即所求逆为x^7

补充2：设A,B是环R的两个理想，并且$B \subseteq A$,证明

(1)A/B是R/B的理想；

证明：利用定义证明

$A/B=\{B+a \mid a\in A\};R/B=\{B+r \mid r\in R\}$

$\because A\subseteq R, \therefore A/B\subseteq R/B$

对任意$B+a, B+b\in A/B, B+r\in R/B$

$(B+a)\ominus(B+b)=B+(a-b)$

$(B+a)\otimes(B+r)=B+ar$

$\because$A为R的理想，所以$a-b\in A,ar\in A$

$\therefore(B+a)\ominus(B+b)\in A/B, (B+a)\otimes(B+r) \in A/B$

同理有，$(B+r)\otimes(B+a) \in A/B$ #

(2) $(R/B)/(A/B) \cong R/A$

证明：环同态定理

构造$\varphi: R/B \to R/A$满足$\varphi(B+r)=A+r, r\in R$;则显然有

$\varphi((B+r_1)\oplus(B+r_2))=(A+r_1)\oplus(A+r_2)$

$\varphi((B+r_1)\otimes(B+r_2))=(A+r_1)\otimes(A+r_2)$

$\therefore \varphi$为同态映射。

R/A的单位元为$A+0=A$，即$\ker\varphi=\{B+r|\varphi(B+r)=A, r\in R\}$

$\because$对$r\in A$,有$\varphi(B+r)=A+r=A$

$\therefore A/B \subseteq \ker\varphi$

又$\because$对任意$A+r=A$,由于$0\in A$，$\therefore r\in A$

$\therefore \ker\varphi \subseteq A/B \Rightarrow \ker\varphi = A/B$

综上，$(R/B)/(A/B) \cong R/A$ #