No.

Date. / /

习题1：

① 错误

零环{0}也是整环的子环，但{0}没有单位元，不是整环

② 错误

设a为$r_1+s_1\pi$，b为$r_2+s_2\pi$，$a,b\in\{r+s\pi : r,s\in\mathbb{Q}\}$。

但$a\times b=r_1r_2+(r_1s_2+r_2s_1)\pi+s_1s_2\pi^2$，因$\pi^2$为无理数且不可表示为$r+s\pi$ $(r,s\in\mathbb{Q})$

∴该子集对乘法不封闭

③ 正确

{0}显然对整数环的加法和乘法封闭，包含零元0，且0的加法逆元为0，满足定义

④ 正确

I_m是整环当且仅当m是素数。因为若m为合数，则$m=ab$ $(1<a<b<m)$，

则$[a][b]=[ab]=[m]=[0]$，有在零因子，不是整环；而素数是无限个。

习题2：

① 错误

例如$x\in\mathbb{Q}[x]$，假设$\exists g(x)\in\mathbb{Q}[x]$使$x\cdot g(x)=1$，设$g(x)=a_0+a_1x+\cdots+a_nx^n$，

则$x\cdot g(x)=a_0x+a_1x^2+\cdots+a_nx^{n+1}\neq 1$ ∴$\mathbb{Q}[x]$不是域

② 正确

环同态$f:R\to S$满足$f(a+b)=f(a)+f(b)$，$f(ab)=f(a)f(b)$对任意$a,b\in R$成立。其中

$f(a+b)=f(a)+f(b)$正是加法群同态的定义

③ 错误

以$K=\mathbb{Q}$为例，$p(x)=x^4+2x^2+1=(x^2+1)^2$，$p(x)$在$\mathbb{Q}$中没有根，但$p(x)$可约

No.
Date. / /

习题3：

对多项式系数进行模5运算，$x^3-7x+6 \equiv x^3+3x+1 \pmod 5$

使用欧几里得算法：$x^3+3x+1 = x(x^2-2x)+(5x+1) = x(x^2-2x)+1$

$\therefore \gcd(x^2-2x, x^3+3x+1)=1$

$\therefore$ 线性组合：$1 = 1\cdot(x^3+3x+1) - x\cdot(x^2-2x)$

习题4：

(a) $(x^4+x^2)(x^3+x+1) = x^7+x^5+x^4+x^5+x^3+x^2 = x^7+2x^5+x^4+x^3+x^2 \equiv x^7+x^4+x^3+x^2$

$\because x^5 \equiv -x^2-1 \pmod{x^5+x^2+1}$

$\therefore$ 原式 $\equiv x^2\cdot(-x^2-1)+x^4+x^3+x^2 \equiv x^3 \pmod{x^5+x^2+1}$

(b) 若要计算 $(x^3+x^2)^{-1} \pmod{x^5+x^2+1}$，即求 $a(x)$，使 $a(x)(x^3+x^2)+b(x)(x^5+x^2+1)\equiv 1$

取 $f(x)=x^5+x^2+1$，$g(x)=x^3+x^2$

$f(x)/g(x)$：$x^5+x^2+1 = x^2(x^3+x^2)+(-x^4+x^2+1)$，$q_1(x)=x^2$，$r_1(x)=-x^4+x^2+1$

$g(x)/r_1(x)$：$x(x^3+x^2) = (-1)\cdot(-x^4+x^2+1)+x^3+x^2+1$，$q_2(x)=0$，$r_2(x)=x^3+x^2+1$

$\therefore 1 = (x-1)(x^3+x^2)+(-x^4+x^2+1) = (x-1)(x^3+x^2)+(x^5+x^2+1)-x^2(x^3+x^2)$

$\equiv (x^2+x+1)(x^3+x^2)+(x^5+x^2+1) \pmod{(x^5+x^2+1)}$

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

(c) $(25)_{10} = (11001)_2$

① (1) result $= x$，base $= x^2$　　② (1) result $= x\cdot x^2 = x^3$，base $= x^2\cdot x^2 = x^4$

③ (0) base $= x^4\cdot x^4 = x^8$　　④ (0) base $= x^8\cdot x^8 = x^{16}$

⑤ (1) result $= x^3\cdot x^{16} = x^{19} = (x^5)^3\cdot x^4$

$(x^5)^3\cdot x^4 \equiv (-x^2-1)^3\cdot x^4 \equiv (-x^6-3x^4-3x^2-1)\cdot x^4 \equiv x^{10}+x^8+x^2+1 \equiv x^4+2x^2+1-x^5-x^3+x+1$

$\equiv x^4+x^3+1$

$\therefore x^{25} \equiv x^4+x^3+1 \pmod{(x^5+x^2+1)}$

No.

Date. / /

习题5：

若R[x]是域，则x有乘法逆元 $g(x)\in R[x]$

设 $g(x)=a_0+a_1x+\cdots+a_nx^n$，那么 $x\cdot g(x)=a_0x+a_1x^2+\cdots+a_nx^{n+1}=1$

而这个等式明显不成立. ∴x无乘法逆元

∴R[x]不是域

习题6：

①显然对矩阵加法封闭

②乘法封闭：

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix}=\begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix}$$

③非零矩阵有逆

对 $A=\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$，$A^{-1}=\frac{1}{a^2+b^2}\begin{pmatrix} a & -b \\ b & a \end{pmatrix}\in F$ 且 $A\cdot A^{-1}=A^{-1}\cdot A=I$

④显然对乘法也满足交换律

∴综上所述，该集合为域

习题7：

① $\forall a,b\in F_q$，有 $f(ab)=(ab)^p=a^pb^p=f(a)f(b)$ ∴乘法同态.

② $(a+b)^p=\sum_{k=0}^{p}\binom{p}{k}a^{p-k}b^k$ ∵ $k\in[1,p-1]$ 时 $\binom{p}{k}\equiv 0 \pmod p$

∴ $(a+b)^p\equiv a^pb^0\binom{p}{0}+a^0b^p\binom{p}{p}=a^p+b^p=f(a)+f(b)$ ∴加法同态.

④ $f(1)=1^p=1$ 满足单位元保持

∴f是 F_q 到自身的域同态