Chapter 5 作业

1. 设p是特征为p的交换环，a、b∈R，有 $(a-b)^p=a^p-b^p$.

证明：$(a-b)^p = a^p + C_p^1 a^{p-1}\cdot(-b) + \cdots + C_p^{p-1} a\cdot(-b)^{p-1} + b^p$.

对：$1 \le k \le p-1$： $C_p^k = \frac{p!}{k!(p-k)!} = \frac{p\cdot(p-1)!}{k!(p-k)!}$ → 整数

$\Rightarrow k!(p-k)! \mid p\cdot(p-1)!$ 又∵ $k!(p-k)!$ 与素数 p 互素.

$\Rightarrow k!(p-k)! \mid (p-1)! \Rightarrow C_p^k$ 是p的倍数 $\Rightarrow \underbrace{C_p^k\cdot a^{p-k}\cdot b^k}_{p\text{的倍数}} = 0$

$\Rightarrow (a-b)^p = a^p + (-b)^p$ 又∵ p为素数

∴ ① $p>2$时，p为奇 $\Rightarrow (a-b)^p = a^p - b^p$

② $p=2$时，$(a-b)^p = (a-b)^2 = a^2+b^2$?

2. Z为整数环，在集合 $S=Z\times Z$ 上定义：

$$(a,b)+(c,d) = (a+c,\ b+d)$$
$$(a,b)\cdot(c,d) = (ac+bd,\ ad+bc)$$

证明：S在这两个运算下成一具有单位元素的环.

① (S,+)交换群：
1° 封闭性：$Z\times Z$ 上显然封闭
2° 结合律：$[(a,b)+(c,d)]+(e,f) = (a+c,b+d)+(e,f)$
$= (a+c+e,\ b+d+f)$
$= (a,b)+[(c,d)+(e,f)]$
3° 零元：$(a,b)+\underline{(0,0)} = (a,b)$
4° 负元：$(a,b)+(-a,-b) = (0,0)$
5° 交换：$(a,b)+(c,d) = (c,d)+(a,b)$.

② S满足乘法结合：$[(a,b)\cdot(c,d)](e,f) = (ac+bd,\ ad+bc)\cdot(e,f)$
$= [e(ac+bd)+f(ad+bc),\ f(ac+bd)+e(ad+bc)]$
$= (a,b)\cdot[(c,d)\cdot(e,f)]$

③ 乘对加满足分配律：$(a,b)\cdot[(c,d)+(e,f)]$

$=(a,b)\cdot[c+e,\ d+f] = a(c+e)+b(d+f),\ a(d+f)+b(c+e)$

$=[(a,b)\cdot(c,d)]+[(a,b)\cdot(e,f)]$

3. 在整数集 Z 上定义加法"$\oplus$"与乘法"$\odot$"为：

$a\oplus b=ab,\quad a\odot b=a+b$

试问 Z 在这2个运算下是否成环？

解：①：$(Z,\oplus)$ 交换群：显然满足封闭性、结合性.

单位元：$a\oplus 1=a$.

逆元：$a\oplus\frac{1}{a}=1$ $\because a\in Z,\ \frac{1}{a}\notin Z$ ∴无逆元.

∴不构成环.

4. 设 $Z[i]=\{a+bi\mid a,b\in Z,\ i^2=-1\}$，证明：$Z[i]$ 关于复数的加法和乘法构成一个环：

证明：① $\langle Z[i],+\rangle$ 交换群：1° $(a_1+b_1i)+(a_2+b_2i)\in Z[i]$ 封闭

2° $[(a_1+b_1i)+(a_2+b_2i)]+(a_3+b_3i)=(a_1+b_1i)+[(a_2+b_2i)+(a_3+b_3i)]$

∴结合

3° 单位元：$0+0i$

4° 逆元：$[-a_1+(-b_1)i]$

② $Z[i]$ 乘法结合：$[(a_1+b_1i)\cdot(a_2+b_2i)]\cdot(a_3+b_3i)$

$=(a_1a_2+(a_1b_2+a_2b_1)i-b_1b_2)\cdot(a_3+b_3i)$

$=(a_1a_2-b_1b_2)\cdot a_3+[(a_1a_2-b_1b_2)b_3+(a_1b_2+a_2b_1)a_3]i-b_3(a_1b_2+a_2b_1)$

$=(a_1+b_1i)\cdot[(a_2+b_2i)\cdot(a_3+b_3i)]$

③ 乘对加分配：

$(a_1+b_1i)\cdot[(a_2+b_2i)+(a_3+b_3i)]$

$=(a_1+b_1i)\cdot[a_2+a_3+(b_2+b_3)i] = a_1(a_2+a_3)+[a_1(b_2+b_3)+b_1(a_2+a_3)]i$
$-b_1(b_2+b_3)$

$=(a_1+b_1i)\cdot(a_2+b_2i)+(a_1+b_1i)\cdot(a_3+b_3i)$

∴得证.

5. 证明：一个至少有2个元但无0因子的有限环是除环

证：即证明：R^*是群（乘法）

① R中无0因子：R^*对乘法封闭

② 选$a\neq 0\in R$，若$aa_i=aa_j$，则$a_i=a_j$

因此$\{aa_1, aa_2, \ldots aa_n\}=\{a_1, a_2 \ldots a_n\}$

同理，$\{a_1a, a_2a, \ldots a_na\}=\{a_1, a_2 \ldots a_n\}$

故对$\forall a,b\in R^*$，$ax=b$和$xa=b$在R中有解

$\Rightarrow R^*$是群.

$\Rightarrow$ R是除环

∴得证

6. 举例：$\{\mathbb{Z}_{18}, +(\mathrm{mod}\ 18), \times(\mathrm{mod}\ 18)\}$

$\{3\}=\{0,3,6,9,12,15\}=0+I=3+I=6+I=9+I=12+I=15+I$

单位元 $\leftarrow \{1,4,7,10,13,16\}$

$\{2,5,8,11,14,17\} \rightarrow$ 逆元.