第6章 环与域参考答案

计算证明

1. (10分)证明高斯整数环$\mathbb{Z}[i]=\{a+bi|a,b\in\mathbb{Z},i=\sqrt{-1}\}$关于复数的加法和乘法运算构成环.

证明 1）加法成Abel群：

i. 封闭：$\forall a_1,b_1,a_2,b_2\in\mathbb{Z}$，有$(a_1+b_1\sqrt{-1})+(a_2+b_2\sqrt{-1})=(a_1+a_2)+(b_1+b_2)\sqrt{-1}\in\mathbb{Z}[\sqrt{-1}]$.封闭性成立.

ii. 结合律：$\forall a_1,b_1,a_2,b_2,a_3,b_3\in\mathbb{Z}$，有

$[(a_1+b_1\sqrt{-1})+(a_2+b_2\sqrt{-1})]+(a_3+b_3\sqrt{-1})=(a_1+a_2+a_3)+(b_1+b_2+b_3)\sqrt{-1}=(a_1+b_1\sqrt{-1})+[(a_2+b_2\sqrt{-1})+(a_3+b_3\sqrt{-1})]$.结合律成立.

iii.幺元（即环的零元）：$\forall a,b\in\mathbb{Z}$，有$(a+b\sqrt{-1})+0=a+b\sqrt{-1}$. 幺元存在且为0.

iv. 逆元：$\forall a,b\in\mathbb{Z}$，$\exists a'=-a,b'=-b\in\mathbb{Z}$，有$(a+b\sqrt{-1})+(a'+b'\sqrt{-1})=0$. 逆元存在.

v.交换律：$\forall a_1,b_1,a_2,b_2\in\mathbb{Z}$，有$(a_1+b_1\sqrt{-1})+(a_2+b_2\sqrt{-1})=(a_1+a_2)+(b_1+b_2)\sqrt{-1}=(a_2+b_2\sqrt{-1})+(a_1+b_1\sqrt{-1})$.交换律成立.

2）乘法成半群：

i.封闭：$\forall a_1,b_1,a_2,b_2\in\mathbb{Z}$，有$(a_1+b_1\sqrt{-1})\times(a_2+b_2\sqrt{-1})=(a_1a_2-b_1b_2)+(a_1b_2+a_2b_1)\sqrt{-1}\in\mathbb{Z}[\sqrt{-1}]$.封闭性成立.

ii.结合律：$\forall a_1,b_1,a_2,b_2,a_3,b_3\in\mathbb{Z}$，有

$[(a_1+b_1\sqrt{-1})\times(a_2+b_2\sqrt{-1})]\times(a_3+b_3\sqrt{-1})=(a_1a_2a_3-b_1b_2a_3-b_1a_2b_3-a_1b_2b_3)+(a_1b_2a_3+a_1a_2b_3+b_1a_2a_3-b_1b_2b_3)\sqrt{-1}=(a_1+b_1\sqrt{-1})\times[(a_2+b_2\sqrt{-1})\times(a_3+b_3\sqrt{-}$
. 结合律成立.

3）分配律：$\forall a_1,b_1,a_2,b_2,a_3,b_3\in\mathbb{Z}$，有

$(a_1+b_1\sqrt{-1})\times[(a_2+b_2\sqrt{-1})+(a_3+b_3\sqrt{-1})]=[a_1(a_2+a_3)-b_1(b_2+b_3)]+[a_1(b_2+b_3)+b_1(a_2+a_3)]\sqrt{-1}=(a_1+b_1\sqrt{-1})\times(a_2+b_2\sqrt{-1})+(a_1+b_1\sqrt{-1})\times(a_3+b_3\sqrt{-1})$
.

$[(a_2+b_2\sqrt{-1})+(a_3+b_3\sqrt{-1})]\times(a_1+b_1\sqrt{-1})=[a_1(a_2+a_3)-b_1(b_2+b_3)]+[a_1(b_2+b_3)+b_1(a_2+a_3)]\sqrt{-1}=(a_2+b_2\sqrt{-1})\times(a_1+b_1\sqrt{-1})+(a_3+b_3\sqrt{-1})\times(a_1+b_1\sqrt{-1})$
. 分配律成立.

综上，高斯整数环$\mathbb{Z}[i]=\{a+bi|a,b\in\mathbb{Z},i=\sqrt{-1}\}$关于复数的加法和乘法运算构成环. 证毕.

2. 对$\mathbb{Z}[\sqrt{3}]=\{a+b\sqrt{3}|a,b\in\mathbb{Z}\}$：

（1）(10分)证明其关于数的加法和乘法运算构成交换整环.

（2）(5分)求其分式域.

证明 （1）对$(\mathbb{Z}[\sqrt{3}],+,\cdot)$是交换整环有：

1）加法成Abel群：

i. 封闭：$\forall a_1,b_1,a_2,b_2\in\mathbb{Z}$，有$(a_1+b_1\sqrt{3})+(a_2+b_2\sqrt{3})=(a_1+a_2)+(b_1+b_2)\sqrt{3}\in\mathbb{Z}[\sqrt{3}]$.封闭性成立.

ii. 结合律：$\forall a_1,b_1,a_2,b_2,a_3,b_3\in\mathbb{Z}$，有

$[(a_1+b_1\sqrt{3})+(a_2+b_2\sqrt{3})]+(a_3+b_3\sqrt{3})=(a_1+a_2+a_3)+(b_1+b_2+b_3)\sqrt{3}=(a_1+b_1\sqrt{3})+[(a_2+b_2\sqrt{3})+(a_3+b_3\sqrt{3})]$.结合律成立.

iii.幺元（即环的零元）：$\forall a,b\in\mathbb{Z}$，有$(a+b\sqrt{3})+0=a+b\sqrt{3}$. 幺元存在且为0.

iv. 逆元：$\forall a,b\in\mathbb{Z}$，$\exists a'=-a,b'=-b\in\mathbb{Z}$，有$(a+b\sqrt{3})+(a'+b'\sqrt{3})=0$. 逆元存在.

v.交换律：$\forall a_1,b_1,a_2,b_2\in\mathbb{Z}$，有$(a_1+b_1\sqrt{3})+(a_2+b_2\sqrt{3})=(a_1+a_2)+(b_1+b_2)\sqrt{3}=(a_2+b_2\sqrt{3})+(a_1+b_1\sqrt{3})$.交换律成立.

2）乘法成交换幺半群且不含零因子：

i.封闭：$\forall a_1,b_1,a_2,b_2\in\mathbb{Z}$，有$(a_1+b_1\sqrt{3})\times(a_2+b_2\sqrt{3})=(a_1a_2+3b_1b_2)+(a_1b_2+a_2b_1)\sqrt{3}\in\mathbb{Z}[\sqrt{3}]$.封闭性成立.

ii.结合律：$\forall a_1,b_1,a_2,b_2,a_3,b_3\in\mathbb{Z}$，有

$[(a_1+b_1\sqrt{3})\times(a_2+b_2\sqrt{3})]\times(a_3+b_3\sqrt{3})=(a_1a_2a_3+3b_1b_2a_3+3b_1a_2b_3+3a_1b_2b_3)+(a_1b_2a_3+a_1a_2b_3+b_1a_2a_3+3b_1b_2b_3)\sqrt{3}=(a_1+b_1\sqrt{3})\times[(a_2+b_2\sqrt{3})\times(a_3+b_3\sqrt{3})]$
. 结合律成立.

iii.幺元：$\forall a,b\in\mathbb{Z}$，有$(a+b\sqrt{3})\times 1=a+b\sqrt{3}$. 幺元存在且为1.

iv.交换律：$\forall a_1,b_1,a_2,b_2\in\mathbb{Z}$，有$(a_1+b_1\sqrt{3})\times(a_2+b_2\sqrt{3})=(a_1a_2+3b_1b_2)\times(a_1b_2+a_2b_1)\sqrt{3}=(a_2+b_2\sqrt{3})\times(a_1+b_1\sqrt{3})$.交换律成立.

v.无零因子：对$a_1,b_1,a_2,b_2\in\mathbb{Z}$，若有$(a_1+b_1\sqrt{3})\times(a_2+b_2\sqrt{3})=(a_1a_2+3b_1b_2)+(a_1b_2+a_2b_1)\sqrt{3}=0$，则

$\begin{cases}a_1a_2+3b_1b_2=0\\a_1b_2+a_2b_1=0\end{cases}\Leftrightarrow\begin{cases}a_1a_2b_2+3b_1b_2^2=0\\a_1a_2b_2+a_2^2b_1=0\end{cases}\Leftrightarrow b_1(3b_2^2-a_2^2)=0$.

若$b_1=0$，则有$\begin{cases}a_1a_2=0\\a_1b_2=0\end{cases}$，得到$a_1=0$或$\begin{cases}a_2=0\\b_2=0\end{cases}$. 若$3b_2^2-a_2^2=0$，得到$\begin{cases}a_2=0\\b_2=0\end{cases}$.

说明无零因子.

3）分配律：$\forall a_1,b_1,a_2,b_2,a_3,b_3\in\mathbb{Z}$，有

$(a_1+b_1\sqrt{3})\times[(a_2+b_2\sqrt{3})+(a_3+b_3\sqrt{3})]=[a_1(a_2+a_3)+3b_1(b_2+b_3)]+[a_1(b_2+b_3)+b_1(a_2+a_3)]\sqrt{3}=(a_1+b_1\sqrt{3})\times(a_2+b_2\sqrt{3})+(a_1+b_1\sqrt{3})\times(a_3+b_3\sqrt{3})$. 又有交换律成立，可知分配律成立.

综上，$\mathbb{Z}[\sqrt{3}]$关于数的加法和乘法运算构成交换整环.

（2）由于整数环$\mathbb{Z}$的分式域为 $\mathbb{Q}$，易知其分式域 F 为 $\mathbb{Q}[\sqrt{3}]$.（可使用定理6.1.5的方法构造 $F=\mathbb{Z}[\sqrt{3}]\times\mathbb{Z}^*[\sqrt{3}]/\sim$，$F\cong\mathbb{Q}[\sqrt{3}]$ ）

3. (5分)若环 R 的非零元素 e 满足$e^2=e$，则称 e为幂等元. 证明若无零因子环 R 有幂等元 e，则 R 为整环且幺元为 e .

证明 只需要证明 R 有乘法幺元即可. $\forall r\in R$，$e^2r=er$ 得到 $e(er-r)=0$. 因为 R 无零因子且e为非零元，则$er-r=0$，即$er=r$. 证毕.

4. (10分)证明交换环 R 中任意一族理想的交是 也是R 的理想.

证明 设 $R_i(i\in I)$ 是 R 在相同运算下的一簇理想，其中 I 为某个指标的集合. 易知$\bigcap\limits_{i\in I}R_i\subseteq R$.

1) $\forall i\in I$，R_i为R的理想，易知 $0\in R_i$，则 $0\in\bigcap\limits_{i\in I}R_i$.

2) $\forall a,b\in\bigcap\limits_{i\in I}R_i$ ，有 $a,b\in R_i$，R_i为R的理想，易知 $a-b\in R_i$，则 $a-b\in\bigcap\limits_{i\in I}R_i$.

3) $\forall r\in R,r_0\in\bigcap\limits_{i\in I}R_i$ ，有 $r_0\in R_i$，R_i为R的理想，易知 $rr_0\in R_i$，则 $rr_0\in\bigcap\limits_{i\in I}R_i$.

综上易知，$\bigcap\limits_{i\in I}R_i$是 R 的理想. 证毕.

5. 对高斯整环$\mathbb{Z}[\sqrt{-5}]$：

（1）(5分)证明不是唯一析因环.

（2）(10分)证明 $\sqrt{-5}$ 是其素元素.

证明 （1）(反例）$6=2\times3=(1+\sqrt{-5})(1-\sqrt{-5})$. 由于2、3与$1\pm\sqrt{-5}$均不相伴. 是不同的分解. 证毕.

（2）首先，易知 $\sqrt{-5}\in\mathbb{Z}[\sqrt{-5}]\backslash U$. 若 $\sqrt{-5}\mid ab$ 其中$a,b\in\mathbb{Z}[\sqrt{-5}]$，则 $\exists t\in\mathbb{Z}[\sqrt{-5}]$，$\sqrt{-5}t=ab$，则对于任意$\alpha=a+b\sqrt{-5}$给定范数$N(\alpha)=a^2+5b^2$. 有$N(\sqrt{-5})N(t)=N(a)N(b)$，即 $5\mid N(a)N(b)$ ，由于5是素数，则 $5\mid N(a)$ 或 $5|N(b)$. 由范数的定义易知，只有 $\pm\sqrt{-5}$的范数为5. 验证知 $\sqrt{-5}\mid a$ 或 $\sqrt{-5}\mid b$ 。所以$\sqrt{-5}$是 $\mathbb{Z}[\sqrt{-5}]$的素元素.

6. (10分)设 R 为Euclid环且$\delta(ab)=\delta(a)\delta(b)$，证明：$a\in U$ 当且仅当 $\delta(a)=1$.

证明 $\forall a\in R$，取b 为幺元 e，则有 $\delta(a)=\delta(ae)=\delta(a)\delta(e)$，得到 $\delta(e)=1$.

必要性. 由 $a\in U$，知 $\exists a^{-1}$ 且 $a^{-1}\in U$. 则 $\delta(e)=\delta\left(aa^{-1}\right)=\delta(a)\delta\left(a^{-1}\right)=1$，故 $\delta(a)=\delta\left(a^{-1}\right)=1$.

充分性. 由 R 是Euclid环可知，有 $e=qa+r$，其中 $q,r\in R$ 且 $\delta(r)<\delta(a)=1$. 则 $\delta(r)=0$. 取 $a=b=0$，有$\delta(0)=\delta(0)\delta(0)$得到 $\delta(0)=0$或$\delta(0)=1$. 而 δ为单射且$\delta(1)=1$，则 $\delta(0)=0$且$r=0$，有$e=qa$，即$q=a^{-1}$. 则 $a\in U$. 证毕.

7. (10分)分别在在 $\mathbb{Q},\mathbb{R},\mathbb{C},\mathbb{Z}_5$中对多项式：$x^2+1$和$x^2+x+1$进行因式分解.

解

	x^2+1	x^2+x+1
$\mathbb{Q}$	不可约	不可约
$\mathbb{R}$	不可约	不可约
$\mathbb{C}$	$(x+i)(x-i)$	$(x+\frac{1-\sqrt{-3}}{2})(x+\frac{1+\sqrt{-3}}{2})$
$\mathbb{Z}_5$	$(x-2)(x-3)$	不可约

8. (5分)求奇素数 p 满足在 $\mathbb{Z}_p[x]$上有 $x+2\mid x^4+x^3+x^2-x+1$.

解 奇素数 p 满足在 $\mathbb{Z}_p[x]$上有 $x+2|x^4+x^3+x^2-x+1$ 等价于 取 $x\equiv-2\equiv p-2$使得 $x^4+x^3+x^2-x+1\equiv0$，即 $p\mid(p-2)^4+(p-2)^3+(p-2)^2-(p-2)+1$，得到 $p\mid pM+15$，其中M是p的一个三次多项式. 那么奇素数 p 为3或5满足.

9. (10分)构造由8个元素构成的域（以加法群表和乘法群表的形式给出）.

解 取域$\mathbb{Z}_2$，再取其多项式环上3次不可约多项式 x^3+x+1得到由8个元素构成的域 $\mathbb{Z}_2[x]/<x^3+x+1>$.其加法群表和乘法群表分别为：

加法	**0**	**1**	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	1	x	x+1	x^2	x^2+1	x^2+x	x^2+x+1
1	1	0	$x+1$	x	x^2+1	x^2	x^2+x+1	x^2+x
x	x	$x+1$	0	1	x^2+x	x^2+x+1	x^2	x^2+1
$x+1$	$x+1$	x	1	0	x^2+x+1	x^2+x	x^2+1	x^2
x^2	x^2	x^2+1	x^2+x	x^2+x+1	0	1	x	$x+1$

加法	**0**	**1**	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x^2+1	x^2+1	x^2	x^2+x+1	x^2+x	1	0	$x+1$	x
x^2+x	x^2+x	x^2+x+1	x^2	x^2+1	x	$x+1$	0	1
x^2+x+1	x^2+x+1	x^2+x	x^2+1	x^2	$x+1$	x	1	0

乘法	**0**	**1**	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	0	0	0	0	0	0	0
1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	0	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
x^2	0	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
x^2+1	0	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+x	x^2	$x+1$

10.(10分)求$\mathbb{Z}_2[x]$中次数不超过5的所有不可约多项式.

解

次数	不可约多项式
0	1
1	x，$x+1$
2	x^2+x+1
3	x^3+x^2+1，x^3+x+1
4	$x^4+x^3+x^2+x+1$，x^4+x^3+1，x^4+x+1
5	$x^5+x^3+x^2+x+1$，$x^5+x^4+x^2+x+1$，$x^5+x^4+x^3+x+1$，$x^5+x^4+x^3+x^2+1$，x^5+x^3+1，x^5+x^2+1