

孙笑涛《抽象代数》习题解答（自制）

MathPlus

2024 年 11 月 12 日

仅供学习交流使用, 本人对此未做出任何学术贡献.

目录

第 1 章 群环域	3
习题 1.1 教材 p8-p9	3
习题 1.2 教材 p13-p14	9
习题 1.3 教材 p17-p18	19
习题 1.4 教材 p21-p22	24
第 2 章 唯一分解整环	33
习题 2.1 教材 p28-p29	33
习题 2.2 教材 p35-p36	42
习题 2.3 教材 p41-p42	48
习题 2.4 教材 p48-p49	55
第 3 章 域扩张	59
习题 3.1 教材 p52-54	59
习题 3.2 教材 p59	61
习题 3.3 教材 p64	61
习题 3.4 教材 p67-68	63
第 4 章 群论初步	65
习题 4.1 教材 p72	65
习题 4.2 教材 p77	66
习题 4.3 教材 p80	67
习题 4.4 教材 p84	68
习题 4.5 教材 p87-p88	69

目录	2
第 5 章 模论初步	71
习题 5.1 教材 p91	71
习题 5.2 教材 p95-p96	72
习题 5.3 教材 p101	73
参考文献	74

约定:

1. 由于教材中的 \subset 符号意义有些歧义, 我们统一用 \subseteq 表示子集, \subsetneq 表示真子集, 比如2.1.5中我对符号进行了修正.
2. 习题中也有其他错误, 对教材原文修改的地方我用红色标出
3. 环都是有 1 的. 如果看到把 n 看作 R 的元素, 请看1.2.1最后的注记.
4. 文中出现的教材指 [孙 22]
5. 对称群的乘法以教材为准, 见1.3.5注记.
6. PID 中的命题 $(a, b) = ua + vb$ 统一称为 Bézout's Identity. 主要是 Bézout's Theorem 现在都指代数几何里的一个定理了. 教材里的那个 Bézout's Theorem 感觉有些太普通了, 还是别叫它定理了吧...

第 1 章 群环域

习题 1.1 教材 p8-p9

1.1.1 设 K 是一个域, 试证明下述结论:

- (1) 如果 $a \cdot c = b \cdot c$, $c \neq 0_K$, 则 $a = b$ (乘法消去律);
- (2) $\forall a, b \in K$, 如果 $a \cdot b = 0_K$, 则 $a = 0_K$ 或 $b = 0_K$;
- (3) $(a^{-1})^{-1} = a$ ($\forall a \in K, a \neq 0_K$);
- (4) $(a \cdot b)^{-1} = a^{-1} \cdot b^{-1}$ ($a \neq 0_K, b \neq 0_K$);
- (5) $(-a)^{-1} = -a^{-1}$ ($\forall a \neq 0_K$);
- (6) $\forall a \neq 0_K, m, n \in \mathbb{Z}$, 则 $a^{m+n} = a^m \cdot a^n$, $a^{mn} = (a^m)^n$;

proof

(1) 由于 $c \neq 0$, 故可在原式左右同乘 c^{-1} , 得

$$a \cdot c \cdot c^{-1} = b \cdot c \cdot c^{-1} \implies a = b.$$

这告诉我们逆元的存在性强于乘法消去律, 乘法消去律已经可以保证乘法逆运算是良定的. 这对加法也是一样的道理, 见1.2.1的 (1).

也可以用分配律得到

$$a \cdot c = b \cdot c \implies (a - b) \cdot c = 0_K.$$

要得到 $a = b$ 需要使用 (2), 即域 K 是没有零因子 (zero-divisor) 的. 由于 $c \neq 0_K$, 则 $a - b = 0_K$, 即 $a = b$.

注: 无零因子的非零交换环称为整环 (integral domain), 见教材 2.1 节 p23.

- (2) 只需证明当 $a \neq 0_K$ 时有 $b = 0_K$, 同 (1), 在等式 $a \cdot b = 0_K$ 两端左乘 a^{-1} 即可.

这告诉我们域 \implies 整环. 结合 (1) 知一个环是整环的条件已经可以推出乘法消去律.

- (3) 即要证明 a^{-1} 的逆元是 a , 这是根据定义以及逆元的唯一性得到, 教材在域, 环, 群三处定义下的注记都有提及. 事实上只要 a 在某一个幺半群 (monoid) 中关于这个运算有逆元, 该结论都会成立, 如 1.2.1 的 (3).

- (4) 即要证明 $a \cdot b$ 的逆元是 $a^{-1} \cdot b^{-1}$. 此处需要交换律, 因此验证半边逆就够了.

$$(a^{-1} \cdot b^{-1}) \cdot (a \cdot b) = (a \cdot a^{-1}) \cdot (b \cdot b^{-1}) = 1_K.$$

非交换的情形为 $(ab)^{-1} = b^{-1}a^{-1}$, 见 1.3.2.

- (5) 即要证明 $-a$ 的逆元是 $-a^{-1}$. 我们用一下 1.2.1 的 (6)

$$(-a)(-a^{-1}) = aa^{-1} = 1_K, \quad (-a^{-1})(-a) = a^{-1}a = 1_K.$$

这样这一条对一个环中的单位都成立.

- (6) 首先需要明确定义, 教材关于 a^n 的定义并不清晰, 包括后面 1.2.1 中的 na 也是. 事实上, 这种和 \mathbb{Z} 有关的东西都应该由递归定义给出, 相对应的证明要用归纳法.

严格来说, 这是定义了一个映射

$$\mathbb{Z} \times K^* \rightarrow K^*, (n, a) \mapsto a^n,$$

这里 $K^* = K \setminus \{0_K\}$ (见 1.3.2), 自然数的部分应由递归定义给出,

$$a^0 := 1_K, \quad a^{n+1} := a^n \cdot a, \quad n \in \mathbb{N},$$

负整数的部分定义为

$$a^n := (a^{-1})^{-n}, \quad n < 0.$$

由该定义可以验证对任意整数 $n \in \mathbb{Z}$ 均有 $a^{n+1} = a^n \cdot a$ 以及 $a^{-n} = (a^{-1})^n$, 这样在使用这两个等式的时候不用再区分正负了.

回到原题, 对任意的 $m \in \mathbb{Z}$, 先用归纳法证明 $n \in \mathbb{N}$ 的情形, 负整数的情形可以结合定义得到.

$n = 0$ 时根据定义左右均为 a^m , 假设对 n 有 $a^{m+n} = a^m \cdot a^n$, 根据定义有

$$a^{m+n+1} = a^{m+n} \cdot a = a^m \cdot a^n \cdot a = a^m \cdot a^{n+1}.$$

由归纳法知

$$\forall m \in \mathbb{Z}, n \in \mathbb{N}, a^{m+n} = a^m \cdot a^n. \quad (*)$$

当 $n < 0$ 时, 则存在 $k \in \mathbb{Z}_{>0}$ 使得 $m + kn < 0$, 则有

$$\begin{aligned} a^{m+n} &= a^{m+kn+(-(k-1)n)} \\ &\stackrel{(*)}{=} a^{m+kn} \cdot a^{-(k-1)n} \\ &= (a^{-1})^{-m-kn} \cdot a^{n-kn} \\ &\stackrel{(*)}{=} (a^{-1})^{-m} \cdot (a^{-1})^{-kn} \cdot a^n \cdot a^{-kn} \\ &= a^m \cdot (a^{-1})^{-kn} \cdot (a^{-1})^{-n} \cdot a^{-kn} \\ &\stackrel{(*)}{=} a^m \cdot (a^{-1})^{-kn-n} \cdot a^{-kn} \\ &= a^m \cdot a^{(k+1)n} \cdot a^{-kn} \\ &\stackrel{(*)}{=} a^m \cdot a^{(k+1)n-kn} = a^m \cdot a^n. \end{aligned}$$

这里我避免使用了乘法交换律, 这样该结论对一般的环也成立.

同样地, 由于 $a^{m(n+1)} = a^{mn+m} = a^{mn} \cdot a^m = (a^m)^n \cdot a^m = (a^m)^{n+1}$, 对 n 归纳可得

$$\forall m \in \mathbb{Z}, n \in \mathbb{N}, a^{mn} = (a^m)^n. \quad (**)$$

当 $n < 0$ 时,

$$\begin{aligned} a^{mn} &= a^{-(m \cdot (-n))} \\ &= (a^{-1})^{m \cdot (-n)} \\ &\stackrel{(**)}{=} ((a^{-1})^m)^{-n} \\ &= (a^{-m})^{-n} = ((a^{-m})^{-1})^n \end{aligned}$$

由于 $a^{-m} \cdot a^m \stackrel{(*)}{=} a^0 = 1_K$, 即括号内确实为 a^m , 故上式等于 $(a^m)^n$.

□

1.1.2 设 K 是一个域, 证明: K 的任意一组子域 (可以无限多个) 的交集仍是子域. 如果 $K_i \subseteq K$ ($i \in \mathbb{N}$) 是满足条件 $K_i \subseteq K_{i+1}$ ($i \in \mathbb{N}$) 的子域, 则它们的并集也是 K 的子域.

proof

令 $F = \bigcap_i K_i$ 由子域定义, 需要验证

$$\forall a, b \in F, a - b \in F$$

$$\forall a, b \in F^*, ab^{-1} \in F^*, F^* = F \setminus \{0\}.$$

由于 K_i 均为子域, 且 $a, b \in F \subseteq K_i$, 故

$$\forall i \in \mathbb{N}, a - b \in K_i.$$

因此

$$a - b \in \bigcap_i K_i = F.$$

F^* 的部分同理, 故 F 为子域.

若还满足 $\forall i \in \mathbb{N}, K_i \subseteq K_{i+1}$, 令 $L = \bigcup_i K_i$, 如果 $a, b \in L$, 则存在 K_i 和 K_j 使得 $a \in K_i, b \in K_j$. 记 $r = \max(i, j)$, 则 $a, b \in K_r$. 由于 K_r 为子域, 可得

$$a - b \in K_r \subseteq L.$$

L^* 同理, 故 L 为子域. □

1.1.3 令 $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ 表示 \mathbb{C} 中包含 $\mathbb{Q}, \sqrt{2}, \sqrt{3}$ 的最小子域, 证明 $\mathbb{Q}[\sqrt{2}, \sqrt{3}] = \mathbb{Q}[\sqrt{2} + \sqrt{3}]$.

proof

该题本应该是域扩张的题, 此处我们只用定义来证明.

由于 $\sqrt{2} + \sqrt{3} \in \mathbb{Q}[\sqrt{2}, \sqrt{3}]$, 我们有 $\mathbb{Q}[\sqrt{2} + \sqrt{3}] \subseteq \mathbb{Q}[\sqrt{2}, \sqrt{3}]$. 反过来,

$$\frac{1}{\sqrt{2} + \sqrt{3}} = \sqrt{3} - \sqrt{2} \in \mathbb{Q}[\sqrt{2} + \sqrt{3}], \text{ 故有 } \sqrt{2} = \frac{(\sqrt{2} + \sqrt{3}) - (\sqrt{3} - \sqrt{2})}{2} \in$$

$$\mathbb{Q}[\sqrt{2} + \sqrt{3}], \sqrt{3} = \frac{(\sqrt{2} + \sqrt{3}) + (\sqrt{3} - \sqrt{2})}{2} \in \mathbb{Q}[\sqrt{2} + \sqrt{3}]. \text{ 因此 } \mathbb{Q}[\sqrt{2}, \sqrt{3}] \subseteq \mathbb{Q}[\sqrt{2} + \sqrt{3}]. \text{ 故两者相等. } \square$$

注:

实际上这个证明过程给出了一个 \mathbb{Q} -线性空间的基变换, 从而两者将同构 (见1.4.9).

1.1.4 设 \mathbb{N} 是所有正整数的集合, \mathbb{Q} 是有理数域. 因 \mathbb{Q} 是可数集, 故存在双射 $f: \mathbb{N} \rightarrow \mathbb{Q}$. 令 $f^{-1}: \mathbb{Q} \rightarrow \mathbb{N}$ 表示 f 的逆映射, 利用有理数的加法和乘法, 可通过双射 f 定义 \mathbb{N} 上的运算如下: $\forall n, m \in \mathbb{N}$,

$$n \oplus m = f^{-1}(f(n) + f(m)), \quad n \star m = f^{-1}(f(n)f(m)),$$

试证明: $\mathbb{N} = (\mathbb{N}, \oplus, \star)$ 是域, 并求它的零元和单位元.

proof

验证域公理, 加法交换律和乘法交换律易得.

结合律: $\forall n, m, l \in \mathbb{N}$,

$$\begin{aligned}(n \oplus m) \oplus l &= f^{-1}\left(f(f^{-1}(f(n) + f(m))) + f(l)\right) \\ &= f^{-1}(f(n) + f(m) + f(l)) \\ &\stackrel{!}{=} n \oplus (m \oplus l); \\ (n \star m) \star l &= f^{-1}\left(f(f^{-1}(f(n)f(m))) \cdot f(l)\right) \\ &= f^{-1}(f(n)f(m)f(l)) \\ &= n \star (m \star l).\end{aligned}$$

其中! 处是因为计算出来的结果关于 n, m, l 是轮换对称的, 后面同理.

零元为 $f^{-1}(0)$: $\forall n \in \mathbb{N}$,

$$\begin{aligned}n \oplus f^{-1}(0) &= f^{-1}(f(n) + f(f^{-1}(0))) \\ &= f^{-1}(f(n) + 0) \\ &= f^{-1}(f(n)) = n.\end{aligned}$$

n 的负元为 $f^{-1}(-f(n))$:

$$\begin{aligned}n \oplus f^{-1}(-f(n)) &= f^{-1}\left(f(n) + f(f^{-1}(-f(n)))\right) \\ &= f^{-1}(f(n) - f(n)) \\ &= f^{-1}(0).\end{aligned}$$

单位元为 $f^{-1}(1)$: $\forall n \in \mathbb{N}$,

$$\begin{aligned}n \star f^{-1}(1) &= f^{-1}(f(n) \cdot f(f^{-1}(1))) \\ &= f^{-1}(f(n)) = n.\end{aligned}$$

n 的逆元为 $f^{-1}(\frac{1}{f(n)})$:

$$\begin{aligned}n \star f^{-1}(\frac{1}{f(n)}) &= f^{-1}\left(f(n) \cdot f(f^{-1}(\frac{1}{f(n)}))\right) \\ &= f^{-1}(f(n) \cdot \frac{1}{f(n)}) \\ &= f^{-1}(1).\end{aligned}$$

分配律: $\forall n, m, l \in \mathbb{N}$,

$$\begin{aligned}
 n \star (m \oplus l) &= f^{-1} \left(f(n) \cdot f(f^{-1}(f(m) + f(l))) \right) \\
 &= f^{-1} (f(n) \cdot (f(m) + f(l))) \\
 &= f^{-1} (f(n)f(m) + f(n)f(l)) \\
 &= f^{-1} (f(n)f(m)) \oplus f^{-1} (f(n)f(l)) \\
 &= n \star m \oplus n \star l.
 \end{aligned}$$

□

1.1.5 证明: 在域的定义中, 加法的交换律可以由其他条件推出. 提示: 按两种方式展开 $(1+1) \cdot (a+b)$.

proof

一方面

$$(1+1) \cdot (a+b) = 1 \cdot (a+b) + 1 \cdot (a+b) = a+b+a+b;$$

另一方面

$$(1+1) \cdot (a+b) = (1+1) \cdot a + (1+1) \cdot b = a+a+b+b.$$

故有 $a+b+a+b = a+a+b+b$. 消去两端的一个 a 和一个 b 即得加法交换律. □

1.1.6 设 $p > 2$ 是素数, $\mathbb{F}_p = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{p-1}\}$ 是 \mathbb{Z} 的模 p 剩余类域. 试计算:

- (1) $\bar{2}$ 在 \mathbb{F}_p 中的逆元 $\bar{2}^{-1}$;
- (2) $\overline{p-1} \cdot \overline{p-2}$;
- (3) $\overline{p-2}$ 在 \mathbb{F}_p 中的逆元 $\overline{p-2}^{-1}$.

proof

- (1) 只需找到能被 2 整除的 $1+kp (k \in \mathbb{Z})$. 由于素数 $p > 2$, $p+1$ 即可. i.e.

$$\bar{2}^{-1} = \frac{1}{2}(p+1).$$

- (2) $\overline{p-1} \cdot \overline{p-2} = \overline{-1} \cdot \overline{-2} = \bar{2}.$

- (3) 由 (1), $\overline{p-2}^{-1} = \overline{-2}^{-1} = \overline{-\frac{1}{2}(p+1)} = \overline{\frac{1}{2}(p-1)}.$

□

习题 1.2 教材 p13-p14

1.2.1 设 R 是一个环, 试证明下述结论:

- (1) (加法消去律) 如果 $a + c = b + c$, 则 $a = b$;
- (2) $\forall a \in R$, 有 $a \cdot 0_R = 0_R$;
- (3) $-(-a) = a$, $a(b - c) = ab - ac$ ($\forall a, b, c \in R$);
- (4) $-(a + b) = (-a) + (-b)$ ($\forall a, b \in R$);
- (5) $a(-b) = (-a)b = -(ab)$ ($\forall a, b \in R$);
- (6) $(-a)(-b) = ab$ ($\forall a, b \in R$);
- (7) $\forall a \in R, m, n \in \mathbb{Z}$, 有 $(m + n)a = ma + na$, $(mn)a = m(na)$;
- (8) $\forall a, b \in R, n \in \mathbb{Z}$, 有 $n(a + b) = na + nb$, $n(ab) = a(nb)$;
- (9) $\forall a, b \in R, m, n \in \mathbb{Z}$, 有 $(ma) \cdot (nb) = mn(a \cdot b) = (mna) \cdot b$;
- (10) (二项式定理) $\forall a, b \in R$, 设 $ab = ba$, n 是正整数, 则

$$(a + b)^n = \sum_{i=0}^n \binom{n}{i} a^{n-i} b^i.$$

proof

(1) 两边同加 $-c$.

(2) 由于

$$a \cdot 0_R = a \cdot (0_R + 0_R) = a \cdot 0_R + a \cdot 0_R.$$

再用一下负元消去即可, $0_R \cdot a = 0_R$ 同理.

注:

这里需要用到: 分配律, 零元定义, 负元存在. 与之对比, $0_R \cdot 0_R = 0_R$ 只需要用到分配律, 零元和单位元. 因此在半环 (semiring) 中 (2) 是不成立的, 但仍有 $0_R \cdot 0_R = 0_R$, 这里半环要求 0 和 1 存在.

(3) 前一个为负元定义 (教材 p9 的注记); 后一个先由分配律,

$$a(b - c) = ab + a(-c),$$

又由于

$$a(-c) + ac = a(c + (-c)) = a \cdot 0_R \stackrel{(2)}{=} 0$$

得 $a(-c) = -ac$, 这也是 (5) 的证明. 这里要注意仅使用 $-a \stackrel{(*)}{=} -1_R \cdot a$ 也无法将负号提到前面, 需要 R 是交换环或者说明 $-1_R \cdot a = a \cdot (-1_R) = -a$.

(*) 的证明如下

$$-1_R \cdot a + a = -1_R \cdot a + 1_R \cdot a = (-1_R + 1_R) \cdot a = 0_R \cdot a \stackrel{(2)}{=} 0_R.$$

右乘 -1_R 同理.

(4) 利用 $-a = -1_R \cdot a$ 和分配律展开即可.

(5) 见 (3).

(6) (3) 和 (5) 的推论.

(7) 参考 1.1.1 的 (6), 明确定义:

$$0a := 0_R, (n+1)a := na + a, n \in \mathbb{N}$$

以及

$$na := -((-n)a), n < 0.$$

一样的, 可以验证对任意整数 $n \in \mathbb{Z}$ 都有 $(n+1)a = na + a$ 和 $na = -((-n)a)$. 先对 n 归纳得

$$(m+n)a = ma + na, \quad \forall m \in \mathbb{Z}, n \in \mathbb{N} \quad (\text{i})$$

然后 $n < 0$, 存在 $k \in \mathbb{Z}_{>0}$ 使得 $m + kn < 0$,

$$\begin{aligned} (m+n)a &= (m+kn - (k-1)n)a \\ &\stackrel{(\text{i})}{=} (m+kn)a + (- (k-1)n)a \\ &= -(-m-kn)a + (n-kn)a \\ &\stackrel{(\text{i})}{=} -((-m)a + (-kn)a) + na + (-kn)a \\ &\stackrel{(4)}{=} ma + (kn)a + na + (-kn)a = ma + na. \end{aligned}$$

第二个式子可直接利用第一个证明, $m = 0$ 根据定义左右均为 0_R , $m > 0$ 有,

$$\begin{aligned} (mn)a &= \left(\sum_{i=1}^m n \right) a \\ &= \sum_{i=1}^m (na) \\ &= m(na). \end{aligned}$$

$m < 0$ 利用 $mn = (-m)(-n)$, 做同样的操作.

(8) 对 n 归纳, 由于加法有交换律,

$$\begin{aligned}(n+1)(a+b) &= n(a+b) + a + b \\ &= na + nb + a + b \\ &= (n+1)a + (n+1)b.\end{aligned}$$

得

$$n(a+b) = na + nb, \quad \forall n \in \mathbb{N}$$

当 $n < 0$ 有

$$n(a+b) = -(-n(a+b)) = -((-n)a + (-n)b) \stackrel{(4)}{=} na + nb.$$

第二个等式使用分配律, $n = 0$ 根据定义左右均为 0_R , $n > 0$,

$$n(ab) = \sum_{i=1}^n ab = a \sum_{i=1}^n b = a(nb).$$

$n < 0$, 用 $n = -(-n)$, $n(ab) = -a((-n)b) \stackrel{(5)}{=} a(nb)$. 同样的也会有 $n(ab) = (na)b$.

(9) (7) 和 (8) 的推论,

$$\begin{aligned}(ma) \cdot (nb) &\stackrel{(8)}{=} m(a \cdot (nb)) \\ &\stackrel{(8)}{=} m(n(ab)) \\ &\stackrel{(7)}{=} mn(ab) \\ &\stackrel{(8)}{=} (mna) \cdot b.\end{aligned}$$

(10) 对 n 归纳,

$$\begin{aligned}(a+b)^n \cdot (a+b) &= \left(\sum_{i=0}^n \binom{n}{i} a^{n-i} b^i \right) \cdot (a+b) \\ &= \sum_{i=0}^n \binom{n}{i} a^{n-i} b^i a + \sum_{i=0}^n \binom{n}{i} a^{n-i} b^{i+1} \\ &\stackrel{ab=ba}{=} \sum_{i=0}^n \binom{n}{i} a^{n-i+1} b^i + \sum_{i=0}^n \binom{n}{i} a^{n-i} b^{i+1} \\ &= a^{n+1} + \sum_{i=1}^n \left(\binom{n}{i} + \binom{n}{i-1} \right) a^{n-i+1} b^i + b^{n+1} \\ &= \sum_{i=0}^{n+1} \binom{n+1}{i} a^{n+1-i} b^i.\end{aligned}$$

□

注:

(7)-(9) 中实际上需要用归纳法证明的只有

$$\begin{aligned} n(a+b) &= na+nb, \\ (m+n)a &= ma+na, \\ (mn)a &= m(na), \end{aligned}$$

这三条加上 $1a = a$, 是在说任何一个 Abel 群都是 \mathbb{Z} -模 (见教材 5.1 节). 再反过来看 1.1.1 的 (6), 加上 $(ab)^n = a^n b^n$, 也是在说 K^* 是 \mathbb{Z} -模, 因为 K^* 关于域的乘法是 Abel 群.

另一方面, 可以先定义

$$N: \mathbb{Z} \rightarrow R, \quad n \mapsto n1_R$$

这是一个自然的环同态 (使用归纳法证明)

$$\begin{aligned} N(m+n) &= N(m) + N(n); \\ N(mn) &= N(m) \cdot N(n). \end{aligned}$$

然后利用这个环同态得到 (注意用到的 $n(ab) = (na)b$ 的证明是直接使用分配律的, 因此不存在循环论证. N 表示使用了这个环同态, dis 表示使用了分配律, ass 表示使用了结合律):

$$\begin{aligned} n(a+b) &= n(1_R(a+b)) = (n1_R)(a+b) \stackrel{dis}{=} (n1_R)a + (n1_R)b = na + nb. \\ (m+n)a &= (m+n)(1_Ra) = ((m+n)1_R)a \stackrel{N}{=} (m1_R + n1_R)a \stackrel{dis}{=} (m1_R)a + (n1_R)a \\ &= ma + na. \\ (mn)a &= (mn)(1_Ra) = (mn1_R)a \stackrel{N}{=} (m1_Rn1_R)a \stackrel{ass}{=} (m1_R)((n1_R)a) \\ &= (m1_R)(na) = m(1_R(na)) = m(na). \end{aligned}$$

这个同态是唯一的, 因为我们要求环同态要把 1 映到 1, 因此 \mathbb{Z} 在 \mathbf{Ring} 中是始对象 (initial object), \mathbf{Ring} 表示环范畴. 因此 \mathbb{Z} 可以认为是任意环 R 的一个子环, n 可看作是 R 中的元素 $n1_R$. 所以此后在没有歧义的情况下, 默认 0 就指零元, 1 指么元.

1.2.2 假设集合 R 上有两个运算, 除加法的交换律外满足环的所有其他公理. 利用分配律证明: 加法是交换的 (从而 R 是环).

proof

这和 1.1.5 是一道题. □

1.2.3 设 X 是集合, $P(X)$ 表示 X 的所有子集形成的集合, 在 $P(X)$ 上定义“加法”和“乘法”: $A+B = A \cup B - A \cap B$, $A \cdot B = A \cap B$. 证明: 在这些运算下 $P(X)$ 是一个环, 且 $2A = 0 (\forall A \in P(X))$.

proof

这里 $A + B$ 为对称差, $A + B = A \cup B - A \cap B = (A - B) \cup (B - A)$. 用 A^c 表示 A 的补集. 那么,

$$A + B = (A \cap B^c) \cup (A^c \cap B).$$

(i) $(P(X), +)$ 是 Abel 群. 交换律由定义是显然的.

结合律:

$$\begin{aligned} (A + B) + C &= (((A \cap B^c) \cup (A^c \cap B)) \cap C^c) \\ &\quad \cup (((A \cap B^c) \cup (A^c \cap B))^c \cap C) \\ &= (A \cap B^c \cap C^c) \cup (A^c \cap B \cap C^c) \cup (A^c \cap B^c \cap C) \\ &\quad \cup (A \cap B \cap C) \\ &= A + (B + C). \quad (\text{轮换对称, 见1.1.4的结合律证明}) \end{aligned}$$

零元为 \emptyset ,

$$A + \emptyset = \emptyset + A = A \cup \emptyset - A \cap \emptyset = A.$$

负元为 A 本身,

$$A + A = A \cup A - A \cap A = A - A = \emptyset.$$

即 $2A = 0$.

(ii) $(P(X), \cdot)$ 是 (交换) 么半群, 单位元是 X . 由于 \cdot 就是交集 \cap , 因此这一点是显然的.

(iii) 分配律:

$$\begin{aligned} (A + B) \cdot C &= ((A \cap B^c) \cup (A^c \cap B)) \cap C \\ &= (A \cap B^c \cap C) \cup (A^c \cap B \cap C) \\ A \cdot C + B \cdot C &= (A \cap C \cap (B \cap C)^c) \cup ((A \cap C)^c \cap B \cap C) \\ &= (A \cap B^c \cap C) \cup (A^c \cap B \cap C). \end{aligned}$$

故有 $(A + B) \cdot C = A \cdot C + B \cdot C$. 另一部分证明类似.

因此 $(P(X), +, \cdot)$ 为一个 (交换) 环. □

1.2.4 设 R 是一个环, $S \subseteq R$ 是一个非空子集合. 试证明

$$C(S) := \{a \in R \mid ax = xa, \forall x \in S\}$$

是 R 的一个子环.

proof

该子环称为子集 S 的中心化子 (centralizer). 当 $S = R$ 时就是中心 (2.1.11).
 $\forall a, b \in C(S)$, 需要验证

$$a - b \in C(S), \quad ab \in C(S), \quad 1 \in C(S).$$

其中 $1 \in C(S)$ 是显然的. 对 $\forall x \in S$

$$\begin{aligned} (a - b)x &= ax + bx = xa + xb = x(a - b), \\ (ab)x &= a(bx) = a(xb) = (ax)b = (xa)b = x(ab). \end{aligned}$$

因此 $a - b, ab \in C(S)$, $C(S)$ 是子环. □

1.2.5 证明: 如果在环 R 中 $1 - ab$ 可逆, 则 $1 - ba$ 也可逆.

proof

设 $1 - ab$ 的逆为 c , 则 $ab = 1 - c^{-1}$.

考虑形式级数

$$(1 - x)^{-1} = \sum_{i=0}^{+\infty} x^i$$

则有

$$\begin{aligned} (1 - ba)^{-1} &= \sum_{i=0}^{+\infty} (ba)^i \\ &= 1 + b \left(\sum_{i=0}^{+\infty} (ab)^i \right) a \\ &= 1 + b(1 - ab)^{-1} \\ &= 1 + bca. \end{aligned}$$

验证 $1 + bca$ 确实是 $1 - ba$ 的逆:

$$\begin{aligned} (1 - ba)(1 + bca) &= 1 - ba + bca - b(abc)a \\ &= 1 - ba + bca - b(c - 1)a \\ &= 1 - ba + bca - bca + ba = 1 \\ (1 + bca)(1 - ba) &= 1 + bca - ba - b(cab)a \\ &= 1 + bca - ba - b(c - 1)a \\ &= 1. \end{aligned}$$

□

1.2.6 如果环 R 满足条件: $\forall x \in R, \quad x^2 = x$, 证明 R 是交换环.

proof

条件 $x^2 = x$ 称为乘法是幂等 (idempotent) 的. 考虑

$$(x+1)^2 = x^2 + 2x + 1 = x + 1,$$

或者直接带入 $-x$, 得

$$-x = x^2 = x.$$

再考虑

$$(x+y)^2 = x^2 + xy + yx + y^2 = x + xy + yx + y = x + y,$$

得

$$xy = -yx = yx.$$

□

1.2.7 (华罗庚恒等式) 设 a, b 是环 R 中的元素. 如果 $a, b, ab-1$ 可逆, 证明 $a-b^{-1}, (a-b^{-1})^{-1}-a^{-1}$ 也可逆, 且有下列恒等式:

$$((a-b^{-1})^{-1}-a^{-1})^{-1} = aba - a.$$

proof

由于 $a, b, ab-1$ 均可逆, 即 $a, b, ab-1 \in U(R)$. $U(R)$ 为环 R 的单位群 (1.3.2). 故

$$a-b^{-1} = (ab-1)b^{-1} \in U(R),$$

那么只需证明华罗庚恒等式. 直接验证即可. 由 1.2.5, $(ba-1)^{-1} = b(ab-1)^{-1}a-1$ 以及 1.3.2 证明的 (1).

$$\begin{aligned} ((a-b^{-1})^{-1}-a^{-1})^{-1} &= (((ab-1)b^{-1})^{-1}-a^{-1})^{-1} \\ &= (b(ab-1)^{-1}-a^{-1})^{-1} \\ &= ((b(ab-1)^{-1}a-1)a^{-1})^{-1} \\ &= a(b(ab-1)^{-1}a-1)^{-1} \\ &= a(ba-1) \\ &= aba - a. \end{aligned}$$

□

1.2.8 (多项式矩阵的带余除法) 设 $A \in M_n(K)$ 是一个给定的 n 阶矩阵. 对任意多项式矩阵 $A(x) \in M_{n \times m}(K[x])$, 证明存在唯一的 $B(x) \in M_{n \times m}(K[x])$, $R \in M_{n \times m}(K)$ 使得 $A(x) = (xI_n - A)B(x) + R$.

proof

先证唯一性, 若存在 $B'(x) \in M_{n \times m}(K[x])$ 和 $R' \in M_{n \times m}(K)$ 也满足条件, 则有

$$(xI_n - A)(B(x) - B'(x)) = R' - R \in M_{n \times m}(K).$$

设

$$B(x) - B'(x) = B_0 + B_1x + B_2x^2 + \cdots + B_kx^k, \quad B_i \in M_{n \times m}(K), 0 \leq i \leq k.$$

将左边展开得

$$\begin{aligned} B_k &= 0, \\ -AB_k + B_{k-1} &= 0 \implies B_{k-1} = 0, \\ -AB_{k-1} + B_{k-2} &= 0 \implies B_{k-2} = 0, \\ &\vdots \\ -AB_1 + B_0 &= 0 \implies B_0 = 0, \\ -AB_0 &= R' - R = 0. \end{aligned}$$

再证存在性, 将 $A(x)$ 写成多项式的形式,

$$A(x) = A_0 + A_1x + A_2x^2 + \cdots + A_kx^k, \quad A_i \in M_{n \times m}(K), 0 \leq i \leq k.$$

我们对 k 归纳, $k = 0$ 时, $A(x) = A_0$ 为常数矩阵, 取 $B(x) = O_{n \times m}$ (零矩阵), $R = A_0$ 即可.

假设对任意 k 次多项式 $A(x)$ 有 $B(x) \in M_{n \times m}(K[x])$, $R \in M_{n \times m}(K)$ 使得 $A(x) = (xI_n - A)B(x) + R$. 考查 $k+1$ 的情形:

$$\begin{aligned} A(x) &= A_0 + x(A_1 + A_2x + \cdots + A_{k+1}x^k) \\ &= A_0 + x((xI_n - A)\tilde{B}(x) + \tilde{R}) \\ &= (xI_n - A)x\tilde{B}(x) + xI_n\tilde{R} - A\tilde{R} + A\tilde{R} + A_0 \\ &= (xI_n - A)(x\tilde{B}(x) + \tilde{R}) + A\tilde{R} + A_0. \end{aligned}$$

取 $B(x) = x\tilde{B}(x) + \tilde{R} \in M_{n \times m}(K[x])$, $R = A\tilde{R} + A_0$ 即可. □

1.2.9 设 $m > 0$ 是任意整数, $\mathbb{Z}_m = \{\bar{0}, \bar{1}, \dots, \overline{m-1}\}$ 是 \mathbb{Z} 的模 m 剩余类环. 试证明: $\bar{a} \in \mathbb{Z}_m$ 可逆当且仅当 $(a, m) = 1$ (即: a 与 m 互素).

proof

 $\bar{a} \in \mathbb{Z}_m$ 可逆,

$$\iff \exists \bar{b} \in \mathbb{Z}, \quad \bar{a}\bar{b} = \bar{1}$$

$$\iff ab = 1 + km, \quad k \in \mathbb{Z},$$

$$\iff (a, m) = 1. \quad (\text{Bézout's Identity})$$

□

注:

一般用记号 $\mathbb{Z}/m\mathbb{Z}$ 表示模 m 剩余类环 (理想和商环, 教材 2.1 节 p25). 若 $(a, m) = 1$, 则 \bar{a} 是加法群 $(\mathbb{Z}/m\mathbb{Z}, +)$ 的生成元, 即 \bar{a} (在加法群) 的阶 (教材 1.3 节, p17) 是 m .

1.2.10 设 R 是仅有 n 个元素的环, 试证明对任意 $a \in R$ 有

$$na := \underbrace{a + a + \cdots + a}_n = 0.$$

proof

该题的证明归结为一句话, 加法群的阶 $(R, +)$ 为 n , 故 $na = 0$.

□

注:

有限群 G 内任一元素 a , 有 $|a| \mid |G|$ (教材 4.1 节 p70 推论 4.1.3), 因此必有 $a^{|G|} = e$, 在这道题就是 $na = 0$.

1.2.11 环 R 中非零元 x 称为幂零元 (nilpotent), 若存在 $n > 0$ 使 $x^n = 0$. 证明:

- (1) 如果 x 是幂零元, 则 $1 - x$ 是可逆元;
- (2) \mathbb{Z}_m 有幂零元当且仅当 m 可以被一个大于 1 的整数的平方整除.

proof

(1) 注意到

$$1 = 1 - x^n = (1 - x)(1 + x + x^2 + \cdots + x^{n-1})$$

(2) " \Rightarrow ": 若 \mathbb{Z}_m 有幂零元 \bar{a} , 则存在 $n > 1 (a \neq 0)$ 使得 $\bar{a}^n = \bar{a}^n = \bar{0}$. 即 $m \mid a^n$. 取素数 $p \mid m$, 则 $p \mid a^n$, 故 $p \mid a$. 因此, 若 m 的素因数分解为 $m = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, 其中 p_1, p_2, \cdots, p_r 为互异的素数, $e_1, e_2, \cdots, e_r \geq 1$, 则 $p_i \mid a$, $1 \leq i \leq r$, 故有 $p_1 p_2 \cdots p_r \mid a$. 因此有 $p_1 p_2 \cdots p_r \leq a < m$, 故必有某个 $e_i > 1$, 即 $\exists 1 \leq i \leq r, e_i \geq 2$, 这样 $p_i^2 \mid m$.

" \Leftarrow ": 反过来, 若 m 可以被某个大于 1 的平方整除, 则上述 e_i 中必有一

个大于 1, 此时取 $a = p_1 p_2 \cdots p_r$, \bar{a} 为 \mathbb{Z}_m 的幂零元.

□

1.2.12 设 R 是一个环, 如果 $(xy)^2 = x^2 y^2 (\forall x, y \in R)$, 则 R 是交换环.

proof

先考虑

$$((x+1)y)^2 = (x+1)^2 y^2 \implies xy^2 = yxy,$$

再将上式中 y 换成 $y+1$,

$$x(y+1)^2 = (y+1)x(y+1) \implies xy = yx.$$

□

1.2.13 如果环 R 满足条件: $x^6 = x (\forall x \in R)$. 证明:

- (1) $x^2 = x (\forall x \in R)$;
- (2) R 是一个交换环.

proof

(1) 先带入 $-x$,

$$-x = (-x)^6 = x^6 = x \implies 2x = 0.$$

考虑 $(x+1)^6$,

$$(x+1)^6 = x^6 + 6x^5 + 15x^4 + 20x^3 + 15x^2 + 6x + 1 = x + 1,$$

得到

$$6x^5 + 15x^4 + 20x^3 + 15x^2 + 6x = 0.$$

利用 $2x = 0$ 消去含 $2x$ 的项得

$$x^4 + x^2 = 0.$$

两边乘 x^2 得

$$x + x^4 = 0.$$

再相减得 $x^2 = x$.

(2) 由 (1) 和 1.2.6.

□

习题 1.3 教材 p17-p18

1.3.1 设 G 是一个群, 对于任意的 $a, b \in G$, 证明 ab 的阶和 ba 的阶相等.

proof

若 $|ab| = n < \infty$, 则

$$(ba)^n = b \cdot (ab)^n \cdot b^{-1} = bb^{-1} = e.$$

且对 $1 \leq k < n$, $(ba)^k = b(ab)^k b^{-1} \neq e$. 因此 $|ba| = n$. 反之亦然.

若 $|ab| = \infty$, 则

$$\forall n \in \mathbb{Z}_{\geq 1}, \quad (ba)^n = b(ab)^n b^{-1} \neq e.$$

故 $|ba| = \infty$. 反之亦然.

事实上, 群 G 内 g 和 $h = aga^{-1}$ 阶相等. h 称为 g 的一个共轭 (conjugate, 教材 p77).

$$\sigma_a : G \rightarrow G, \quad g \mapsto aga^{-1}$$

是群 G 的一个自同构. 而对一般的群同态 $\varphi : G \rightarrow G'$, $|g| < \infty \implies |\varphi(g)| < \infty$ 且 $|\varphi(g)| \mid |g|$. 因此若 φ 为同构, 则 $|g| = |\varphi(g)|$ (包括左右为无穷的情况). \square

1.3.2 设 R 是一个环, $U(R)$ 表示 R 中所有可逆元集合, 试证明: $U(R)$ 关于环 R 的乘法是一个群 (称为 R 的单位群).

proof

(1) 这里首先需要验证运算的封闭性, $\forall a, b \in U(R)$, 有 $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = 1$, 故 $ab \in U(R)$ 且 $(ab)^{-1} = b^{-1}a^{-1}$.

(2) $1 \in U(R)$, 因为 $1 \cdot 1 = 1$ 的确可逆;

(3) 由于乘法是 R 上的乘法, 故结合律成立;

(4) 若 $a \in U(R)$, 则由 1.1.1 的 (3), $a^{-1} \in U(R)$ 且 $(a^{-1})^{-1} = a$;

\square

注:

一般 $U(R)$ 也记作 R^* , 比如 K 是域时, $K^* = K \setminus \{0\}$.

1.3.3 证明除了单位元之外所有元素的阶都是 2 的群一定是交换群.

proof

由于任意 $a^2 = e$, 故 $a = a^{-1}$.

考虑

$$(ab)^2 = e \implies ab = b^{-1}a^{-1} = ba.$$

或直接验证

$$ab = ab \cdot (ba)^2 = abbaba = ba$$

□

1.3.4 令 $C(\mathbb{R}) = \left\{ \text{所有连续函数: } \mathbb{R} \xrightarrow{f} \mathbb{R} \right\}, \forall f, g \in C(\mathbb{R}),$

$$f + g \in C(\mathbb{R}), \quad f \cdot g \in C(\mathbb{R})$$

定义: $\forall x \in \mathbb{R}, (f + g)(x) = f(x) + g(x), (f \cdot g)(x) = f(g(x))$, 证明 $(C(\mathbb{R}), +)$ 是交换群. $(C(\mathbb{R}), +, \cdot)$ 是否为环?

proof

$(C(\mathbb{R}), +)$ 的零元为零函数 $\mathbf{0}: \mathbb{R} \rightarrow \mathbb{R}, x \mapsto 0, (f + \mathbf{0})(x) = f(x) + 0 = f(x) = 0 + f(x) = (\mathbf{0} + f)(x), \forall x \in \mathbb{R}.$

$f \in C(\mathbb{R})$ 的负元为 $-f: \mathbb{R} \rightarrow \mathbb{R}, x \mapsto -f(x), (f + (-f))(x) = ((-f) + f)(x) = f(x) - f(x) = 0 = \mathbf{0}(x).$

由于 $f + g$ 为逐点定义, 故交换律和结合律依赖于 \mathbb{R} 的加法, 是平凡的. 故 $(C(\mathbb{R}), +)$ 是 Abel 群.

若 f 不是 \mathbb{R} -线性函数, 如 $f(x) = x^2$, 则 $(f \cdot (g + h))(x) = f((g + h)(x)) = f(g(x) + h(x)) \neq f(g(x)) + f(h(x)).$ 故 $C(\mathbb{R}, +, \cdot)$ 不是环. □

1.3.5 写出对称群 S_3 的乘法表.

proof

记 $\text{id}_{S_3} = e$, 令 $a = (12), b = (123)$, 有 $a^2 = e, b^3 = e, abab = e \iff ba = ab^2$. 乘法表如下:

	e	a	b	b^2	ab	ab^2
e	e	a	b	b^2	ab	ab^2
a	a	e	ab	ab^2	b^2	b
b	b	ab^2	b^2	e	a	ab
b^2	b^2	ab	e	b	ab^2	a
ab	ab	b^2	a	ab^2	e	b
ab^2	ab^2	b	ab	a	b^2	e

□

注:

可以看到 S_3 , 若取 $a = (1\ 2)$, $b = (1\ 2\ 3)$, 则 S_3 可以由 a, b 生成, 即考虑所有可能的乘积, 一般可以表示为 $S_3 = \langle a, b \rangle$, $a = (1\ 2)$, $b = (1\ 2\ 3)$.

若不给 a, b 加任何限制, 便得到一个自由群 (free group) $F(\{a, b\})$. 一般地, 任意一个集合 A 都可以生成一个自由群 $F(A)$, A 就是生成元组成的集合. 可以证明任何一个群都同构于某个自由群的商群, 而对应的正规子群便是由生成元满足的某些关系确定 (将 A 看成字母表, Σ_A 表示单词的集合, 这些关系可以表示为一些满足 $w = e$ 单词 $w \in \Sigma_A$). 把这些 w 组成的集合记为 \mathcal{R} , A 和 \mathcal{R} 将唯一确定一个群 G , $(A \mid \mathcal{R})$ 称为 G 的一个展示 (presentation). 以 S_3 为例, S_3 的一个展示为 $(\{a, b\} \mid a^2, b^3, abab)$.

由于这本教材没有讲自由群, 所以想要了解的话需要查阅别的教材.(可参考 [Alu09]II.§5 和 II.§8.2)

BTW, 这本教材和很多教材一样, 会把集合 A 对称群 S_A 上的乘法写成 $f \cdot g := f \circ g$, 这个其实会有一点不舒服. 正常我们习惯于说: 映射 $f: X \rightarrow Y$ 和 $g: Y \rightarrow Z$ 的复合是 $g \circ f$. 这在范畴的定义也是习惯于这样, 复合会写成这样:

$$\text{Hom}_{\mathcal{C}}(X, Y) \times \text{Hom}_{\mathcal{C}}(Y, Z) \rightarrow \text{Hom}_{\mathcal{C}}(X, Z), (f, g) \mapsto g \circ f.$$

这样说的好处在于一眼能感觉出这个运算是不交换的 (个人感觉). 如果引入范畴的记号, S_A 会记作 $\text{Aut}_{\text{Set}(A)}$, 其中 Set 表示集合范畴. 那么 S_A 上的乘法按范畴的定义来写应该是:

$$S_A \times S_A \rightarrow S_A, (f, g) \mapsto f \cdot g := g \circ f$$

可以看到和 $f \cdot g := f \circ g$ 刚好是反过来的. 没有使用范畴语言的话就还好, 不会出现前后不自洽的问题, 但如果介绍了范畴语言, 那应该注意 S_A 上乘法的定义要和范畴定义不能冲突, 这一点 [Hum03] 就做的很好. 它的范畴定义故意反了过来, 它写成 $\text{Hom}_{\mathcal{C}}(Y, Z) \times \text{Hom}_{\mathcal{C}}(X, Y) \rightarrow \text{Hom}_{\mathcal{C}}(X, Z)$.

那么哪一个才对呢, 事实上都是对的, 你总能验证 S_A 确实是一个群. 原因在于, 当你只考虑所有的同构时, 就得到一个子范畴, 这是一个群胚 (groupoid), 它是一个自反范畴, 所以顺序就没区别了. 但我个人认为还是统一一下比较好, 主要是复合是非交换的, $f \circ g$ 和 $g \circ f$ 一般不等. 为了方便还是按照教材为准吧, 使用 $f \cdot g = f \circ g$. (尽管我是有点不习惯的)

1.3.6 证明: 一个群 G 不会是两个真子群 (不等于 G 的子群) 的并.

proof

反证, 假设 $H_1, H_2 \subsetneq G$ 且 $G = H_1 \cup H_2$, 则 $\exists h_1 \in G \setminus H_2 \subseteq H_1, h_2 \in G \setminus H_1 \subseteq H_2$, 有 $h_1 h_2 \in G = H_1 \cup H_2$, 矛盾. (不妨设 $h_1 h_2 \in H_1 \implies h_2 \in H_1$) \square

1.3.7-1.3.9为群的其他三种定义.

1.3.7 一个非空集合 G 带有满足结合律的“乘法”运算, 我们称之为半群. 如果 G 是一个半群, 且满足如下性质:

- (1) G 含有右单位元 1_r (即: $a \cdot 1_r = a, \forall a \in G$);
- (2) G 中的每个元素 a 有右逆 (即: 存在 $b \in G$, 使得 $a \cdot b = 1_r$).

试证明: G 是一个群.

proof

先证右逆为逆,

$$\begin{aligned} \forall a \in G \exists b \in G, ab &= 1_r, \\ \implies \exists c \in G, bc &= 1_r, \\ \implies ba &= (ba)1_r = (ba)(bc) = b(ab)c = b1_r c = bc = 1_r. \end{aligned}$$

再证右单位为单位,

$$1_r a = (ab)a = a(ba) = a1_r = a.$$

□

1.3.8 证明: 半群 G 是群的充要条件是: $\forall a, b \in G, ax = b$ 和 $ya = b$ 都有 (唯一) 解.

proof

- (1) " \Leftarrow ": 取定一个 $a \in G$, 方程 $ax = a$ 的解设为 e_a . 对 $\forall b \in G$, 方程 $ya = b$ 有解 y_b , 则有

$$be_a = (y_b a)e_a = y_b(ae_a) = y_b a = b.$$

即 e_a 是 G 的右单位, 记为 1_r , 又因为 $\forall a \in G$, 方程 $ax = 1_r$ 有解, 即 a 有右逆, 由 1.3.7 知 G 是群.

- (2) " \Rightarrow ": 若 G 是群, 则方程 $ax = b$ 的唯一解为 $a^{-1}b$, 方程 $ya = b$ 的唯一解为 ba^{-1} .

□

1.3.9 证明:

- (1) 在群中左右消去律都成立: 如果 $ax = ay$, 则 $x = y$; 如果 $xa = ya$, 则 $x = y$.
- (2) 左右消去律都成立的有限半群一定是群.

proof

设 $G = \{a_1, a_2, \dots, a_n\}$. 对 $\forall 1 \leq i, j \leq n$,

$$a_i a_1, a_i a_2, \dots, a_i a_n$$

互异, 否则存在 $a_k \neq a_l$ 使得 $a_i a_k = a_i a_l$, 由消去律得 $a_k = a_l$ 矛盾. 因此 $\exists 1 \leq t \leq n$, $a_i a_t = a_j$, 即方程 $a_i x = a_j$ 有解. 同理方程 $ya_i = a_j$ 也有解, 由 1.3.8, G 是群. \square

1.3.10 证明: 偶数阶有限群 G 中必有 2 阶元.

proof

设 $|G| = 2n$. 对 $e \neq g \in G$, $|g| = 2 \iff g = g^{-1}$. 定义 G 上的一个等价关系

$$g \sim g' \iff g = g' \vee g' = g^{-1}.$$

考虑商集 $G/\sim = \{\bar{g} \mid g \in G\}$, 用 $\#S$ 表示集合 S 的元素个数 (基数) 防止混淆. 若 $|g| = 2$ 或 $g = e$, 则 $\#\bar{g} = 1$, 否则 $\#\bar{g} = 2$. 因此若 m 为 G 中阶为 2 的元素的个数, 则 $2n = m + 1 + 2(\#(G/\sim) - m - 1)$, 故 $2n - m - 1$ 为偶数, 因此 $m > 0$. \square

注:

当然可以用 Sylow 定理一步到位.

1.3.11 证明: $GL_2(\mathbb{R})$ 中的元素 $x = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $y = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ 的阶分别是 4 和 3. 但 xy 是无限阶元.

proof

用 I_n 表示 n 阶单位阵, 计算可得

$$x^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, x^3 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, x^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2.$$

故 $|x| = 4$, 同理,

$$y^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, y^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2.$$

$|y| = 3$. 最后是 xy ,

$$xy = \begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix}, (xy)^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, (xy)^3 = \begin{pmatrix} -1 & -3 \\ 0 & -1 \end{pmatrix}, \dots$$

可以用归纳法证明

$$(xy)^n = (-1)^n \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \neq I_2, \forall n \in \mathbb{Z}_{\geq 1}.$$

故 $|xy| = \infty$. □

1.3.12 证明群的任意多个子群的交仍是子群.

proof

设 G 是群, 记 I 为指标集, $H_i < G, \forall i \in I$. 验证 $H = \bigcap_{i \in I} H_i < G$: 首先 $e_G \in H, H \neq \emptyset$,

$$\begin{aligned} \forall a, b \in H = \bigcap_{i \in I} H_i &\implies \forall i \in I, a, b \in H_i \\ &\implies ab^{-1} \in H_i, \quad \forall i \in I \\ &\implies ab^{-1} \in \bigcap_{i \in I} H_i = H. \end{aligned}$$

□

注:

教材中并未提及这个判断子群的命题, 但确实是最常用的.

命题 (子群的判定) 设 G 是一个群, $\emptyset \neq S \subseteq G$, 则 $S < G$ (S 是 G 的子群的记号) 当且仅当

$$\forall a, b \in S \iff ab^{-1} \in S.$$

证明可参考 [Alu09]p79.

习题 1.4 教材 p21-p22

1.4.1 设 $\varphi: G \rightarrow G'$ 是群同态, 试证明:

(1) $\ker(\varphi) := \{g \in G \mid \varphi(g) = e'\}$ ($e' \in G'$ 表示的单位元) 是 G 的子群 (称为群同态 φ 的核);

(2)

$$\varphi(G) = \{\varphi(g) \mid \forall g \in G\} \subset G'$$

是 G' 的子群 (称为群同态 φ 的像).

proof

教材命题 1.4.1 的 (1)(5) 直接使用.

(1) $e \in \ker(\varphi)$ 非空, 直接验证

$$\begin{aligned} \forall a, b \in \ker(\varphi), \varphi(ab^{-1}) &= \varphi(a)\varphi(b)^{-1} = e'e' = e' \\ \implies ab^{-1} &\in \ker(\varphi). \end{aligned}$$

(2) $e' \in \varphi(G)$ 非空, 直接验证

$$\begin{aligned} \forall x, y \in \varphi(G), \exists a, b \in G, x &= \varphi(a), y = \varphi(b) \\ \implies xy^{-1} &= \varphi(a)(\varphi(b))^{-1} = \varphi(a)\varphi(b^{-1}) = \varphi(ab^{-1}) \in \varphi(G). \end{aligned}$$

□

1.4.2 令 G 是函数 $f(x) = \frac{1}{x}, g(x) = \frac{x-1}{x}$ 关于函数的合成生成的一个群 (即群乘法为函数合成), 证明 G 同构于 S_3 .

proof

由 1.3.5 的注记, 只需验证 $f^2 = \text{id}, g^3 = \text{id}, fgfg = \text{id}$.

$$\begin{aligned} f^2(x) &= f(f(x)) = \frac{1}{\frac{1}{x}} = x. \\ g^2(x) &= g(g(x)) = 1 - \frac{1}{(1 - \frac{1}{x})} = -\frac{1}{x-1} \\ g^3(x) &= g(g^2(x)) = 1 - \left(\frac{1}{-\frac{1}{x-1}}\right) = 1 + x - 1 = x. \\ (fg)(x) &= f(g(x)) = \frac{x}{x-1}, \\ (fgfg)(x) &= (fg)^2(x) = 1 + \frac{1}{\frac{x}{x-1} - 1} = 1 + x - 1 = x. \end{aligned}$$

□

1.4.3 设 $R \xrightarrow{\varphi} R'$ 是环同态, 证明集合 $\ker(\varphi) = \{x \in R \mid \varphi(x) = 0_{R'}\}$ 满足:

- (1) $\ker(\varphi)$ 是 $(R, +)$ 的子群;
- (2) $\forall a \in \ker(\varphi), x \in R$ 有 $ax \in \ker(\varphi), xa \in \ker(\varphi)$. ($\ker(\varphi)$ 称为环同态 φ 的核)

proof

(1) 即 1.4.1(1);

(2) 直接验证

$$\forall a \in \ker(\varphi), x \in R, \varphi(xa) = \varphi(x)\varphi(a) = \varphi(x)0_{R'} = 0_{R'}$$

另一半同理.

□

注:

满足 (1)(2) 的 R 的子集称为 R 的一个理想 (ideal), 教材 p25 定义 2.1.4.

1.4.4 设 K 是一个域, $\phi: K[x] \rightarrow K[x]$ 是 K 的多项式环之间的环自同态. 如果对于任意的 $k \in K, \phi(k) = k$, 试证明: ϕ 是满同态的充分必要条件是存在 $a, b \in K (a \neq 0)$ 使得 $\phi(x) = ax + b$.

proof

(1) " \implies ": 记 $f(x) = \phi(x)$, 若 ϕ 是满的, 则存在 $g(x) \in K[x]$ 使得 $\phi(g(x)) = x$, 则 $x = \phi(g(x)) \stackrel{!}{=} g(\phi(x)) = g(f(x))$, ! 处是根据环同态的定义以及 $\phi(k) = k, \forall k \in K$ 得到. 考查次数 $1 = \deg(g(f(x))) = \deg(g) \cdot \deg(f)$ (域没有零因子). 因此 $\deg(f) = \deg(g) = 1$, i.e. $\phi(x) = f(x) = ax + b, \exists a \neq 0, b \in K$.

(2) " \impliedby ": 若存在 $a \neq 0, b \in K$ 使得 $\phi(x) = ax + b$, 则令 $y = ax + b$ 得到 $x = a^{-1}(y - b)$. 那么对任意的 $f(x) \in K[x]$, 存在 $g(x) = f(a^{-1}(x - b)) \in K[x]$ 使得 $\phi(g(x)) = g(\phi(x)) = g(y) = f(a^{-1}(y - b)) = f(x)$.

□

1.4.5 证明实数的加法群 $(\mathbb{R}, +)$ 和正实数的乘法群 $(\mathbb{R}_{>0}, \cdot)$ 同构.

proof

注意到 $f: \mathbb{R} \rightarrow \mathbb{R}_{>0}, x \mapsto e^x$ 是同构. $f^{-1}(x) = \ln x$.

□

注:

事实上, 由 $f(x+y) = f(x)f(y)$ 并利用归纳法和同态定义可以直接推出 $f(x) = a^x, a = f(1), x \in \mathbb{Q}$, 若有连续性则可以延拓到 \mathbb{R} 上.

1.4.6 证明有理数的加法群 $(\mathbb{Q}, +)$ 和正有理数的乘法群 $(\mathbb{Q}_{>0}, \cdot)$ 不同构.

proof

反证, 假设存在同构 $f: \mathbb{Q} \rightarrow \mathbb{Q}_{>0}$, 则设 $2 = f(a) = f(\frac{a}{2} + \frac{a}{2}) = f(\frac{a}{2}) \cdot f(\frac{a}{2}) = f(\frac{a}{2})^2$ 矛盾.

□

1.4.7 证明有理数域 \mathbb{Q} 和实数域 \mathbb{R} 的自同构都只有恒等映射.

proof

不妨设 $\sigma : \mathbb{Q} \rightarrow \mathbb{Q}$ 是同构, 根据定义, 有 $\sigma(0) = 0, \sigma(1) = 1, \sigma(-a) = -\sigma(a), \sigma(a^{-1}) = (\sigma(a))^{-1}$. 因此先用归纳法得到 $\sigma|_{\mathbb{N}} = \text{id}_{\mathbb{N}}$, 用负元延拓到 \mathbb{Z} , 再用逆元延拓到 \mathbb{Q} 得 $\sigma = \text{id}_{\mathbb{Q}}$. 事实上, 这个推导对于任何特征 0 的域都是对的, 即 \mathbb{Q} 是特征 0 最小域 (环的特征见教材 2.1 节 p27 定义 2.1.5). 对 \mathbb{R} , 首先若 $\phi : \mathbb{R} \rightarrow \mathbb{R}$ 是同构, 有上面可知 $\phi|_{\mathbb{Q}} = \text{id}_{\mathbb{Q}}$. 另外, 可以证明 ϕ 保序结构, 即 $x \geq 0 \implies \phi(x) \geq 0$. 这是因为对 $x > 0$ 总有 $\phi(x) = \phi(\sqrt{x} \cdot \sqrt{x}) = \phi(\sqrt{x})^2 > 0$. 保序则保极限, 即对单调有界有理数列 $\{q_n\}_{n \in \mathbb{N}}$ 有 $\lim_{n \rightarrow \infty} \phi(q_n) = \lim_{n \rightarrow \infty} q_n$ (实际上保序就可以保持 \mathbb{R} 上的拓扑结构, ϕ 是连续的). 由于 \mathbb{Q} 在 \mathbb{R} 中稠密, 从而 $\phi = \text{id}_{\mathbb{R}}$.

一般情况下子域的自同构是不一定能延拓到扩域上, 比如考虑 $\mathbb{Q}(\sqrt{2})$ 的共轭自同构 (类似复共轭, $\sqrt{2} \mapsto -\sqrt{2}$), 它不能延拓到 \mathbb{R} 上.

综上可得, $\text{Aut}_{\text{Ring}}(\mathbb{R}) = \text{Aut}_{\mathbb{Q}}(\mathbb{R})$ 是平凡群. (由于 \mathbb{R}/\mathbb{Q} 并不是 Galois 扩张, 因此没有用符号 $\text{Gal}(\mathbb{R}/\mathbb{Q})$, Ring 表示环范畴) \square

1.4.8 证明: $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$, $\mathbb{Q}[\sqrt{5}] = \{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\}$ 都是 \mathbb{R} 的子域. 它们是同构的域吗?

proof

由教材命题 1.4.1 的 (9), 两个域若存在同态则一定是单同态, 即只有两种可能, 一个域为另一个域的扩张或两者同构. 我们断言这两个域之间不存在同态.

假设存在同态 $\varphi : \mathbb{Q}[\sqrt{2}] \rightarrow \mathbb{Q}[\sqrt{5}]$, 则设 $\varphi(\sqrt{2}) = a + b\sqrt{5}$, $a, b \in \mathbb{Q}$. 注意到由同态定义有 $\varphi(2) = 2$, 立刻有

$$2 = \varphi(2) = \varphi(\sqrt{2})^2 = (a + b\sqrt{5})^2 = a^2 + 5b^2 + 2ab\sqrt{5}$$

这要求 $a^2 + 5b^2 = 2$ 且 $ab = 0$, 这是不可能的, 矛盾. \square

1.4.9 设 K, L 是两个域, 如果 L 是 K 的子域, 则 K 称为 L 的扩域, $K \supset L$ 称为域扩张, 试证明:

- (1) 域的加法和乘法使得 K 是一个 L -向量空间 ($[K : L] = \dim_L(K)$ 称为域扩张 $K \supset L$ 的次数);
- (2) 如果 $K \supset \mathbb{R}$ 是一个二次扩张 (即 $[K : \mathbb{R}] = 2$), 则 K 必同构于复数域 \mathbb{C} .

proof

- (1) $(K, +)$ 是一个 Abel 群, 这一点无需再说明. 乘法在这里可能有些歧义, 此处是要验证乘法限制在 $L \times K$ 上, 即

$$\cdot : L \times K \rightarrow K, \quad (l, k) \mapsto lk$$

是数乘. 即要验证

$$\begin{aligned}(l_1 l_2)k &= l_1(l_2 k), \\ (l_1 + l_2)k &= l_1 k + l_2 k, \\ l(k_1 + k_2) &= l k_1 + l k_2, \\ 1k &= k = k1.\end{aligned}$$

这些都由域的定义得到.

这也说明若同态 $K_1 \rightarrow K_2$ 保持 $L(K_1, K_2$ 为 L 的两个扩域), 则一定是 L -线性映射.

- (2) 由 (1), 扩域 \mathbb{C}/\mathbb{R} 的自同构一定是 \mathbb{R} -线性的. 设同构 $f: \mathbb{C} \rightarrow \mathbb{C}$, 则有 $f(x + yi) = x + yf(i)$, $x, y \in \mathbb{R}$, 且保持乘法, 即

$$\begin{aligned}f((x_1 + iy_1) \cdot (x_2 + iy_2)) &= f(x_1 + iy_1) \cdot f(x_2 + iy_2) \\ &= (x_1 + y_1 f(i)) \cdot (x_2 + y_2 f(i)) \\ &\implies f(x_1 x_2 - y_1 y_2 + (x_1 y_2 + x_2 y_1)i) \\ &= x_1 x_2 + y_1 y_2 f(i) \cdot f(i) + (x_1 y_2 + x_2 y_1) f(i) \\ &\implies x_1 x_2 - y_1 y_2 + (x_1 y_2 + x_2 y_1) f(i) \\ &= x_1 x_2 + y_1 y_2 f(i) \cdot f(i) + (x_1 y_2 + x_2 y_1) f(i) \\ &\implies f(i) \cdot f(i) = -1.\end{aligned}$$

因此 $f(i) = \pm i$. 也就是说 \mathbb{C}/\mathbb{R} 的自同构都只有恒等映射和共轭, 即 $\text{Gal}(\mathbb{C}/\mathbb{R}) = \mathbb{Z}/2\mathbb{Z}$.

由线性代数的结论, 可以直接得到 K 和 \mathbb{C} 是作为线性空间同构, 但这是不够的, 只有上述两个线性映射是域同构, 需要做基变换转为恒等或共轭才能保持乘法. 事实上只要存在一个基变换就能变回恒等映射, 恒等映射总是同构, 但前提是承载集合 (underlying set) 要一样. 比如 $\mathbb{Q}(\sqrt{2})$ 和 $\mathbb{Q}(\sqrt{3})$ 作为 \mathbb{Q} -线性空间也是同构的, 但他们之间没有域同态.

可取 K 的一组基为 $1, \alpha$, 其中 $\alpha \in \mathbb{C} \setminus \mathbb{R}$. 不可避免地要考虑 α^2 的结果, 由于 $1, \alpha$ 是基, 因此 α^2 可以被线性表出, 即 $\alpha^2 = x + y\alpha$. 由于 $\alpha \notin \mathbb{R}$, 有 $y^2 + 4x < 0$, 解二次方程得到 $\alpha = \frac{y \pm i\sqrt{|y^2 + 4x|}}{2}$. 故映射

$$f: K \rightarrow \mathbb{C}, u + v\alpha \mapsto u + v \frac{y \pm i\sqrt{|y^2 + 4x|}}{2}$$

是域同构.

□

注:

事实上, 若有环同态 $R \xrightarrow{\varphi} S$, 则 S 上自动有一个 R -模结构

$$R \times S \rightarrow S, \quad (r, s) \mapsto rs = \varphi(r)s$$

rs 是数乘, $\varphi(r)s$ 是 S 中的乘法. 域上的模就是线性空间.

(1) 对应的同态其实就是包含 (inclusion) $L \xrightarrow{i} K$.

1.4.10 设 d 是一个非零整数, 且 $\sqrt{d} \notin \mathbb{Q}$. 证明:

$$\mathbb{Q}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\} \supset \mathbb{Q}$$

是一个二次扩张 ($d < 0$ 时, $\mathbb{Q}[\sqrt{d}]$ 称为虚二次域, $d > 0$ 时称为实二次域).

proof

只需验证 $\mathbb{Q}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$ 确实是一个域. 这样它自动就是一个 2 维的 \mathbb{Q} -线性空间.

加法:

$$(a_1 + b_1\sqrt{d}) + (a_2 + b_2\sqrt{d}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{d}$$

容易验证结合律, $0 = 0 + 0\sqrt{d}$, $-(a + b\sqrt{d}) = (-a) + (-b)\sqrt{d}$.

乘法:

$$(a_1 + b_1\sqrt{d}) \cdot (a_2 + b_2\sqrt{d}) = a_1a_2 + b_1b_2d + (a_1b_2 + a_2b_1)\sqrt{d}$$

其中 $1 = 1 + 0\sqrt{d}$, 逆元做一次分母有理化

$$(a + b\sqrt{d})^{-1} = \frac{1}{a + b\sqrt{d}} = \frac{a - b\sqrt{d}}{a^2 + b^2d} = \frac{a}{a^2 + b^2d} + \frac{-b}{a^2 + b^2d}\sqrt{d}$$

, 结合律是容易验证的 (计算出的结果是轮换对称的, 参考1.1.4和1.2.3). \square

1.4.11 设 $L \supset K$ 是一个域扩张, 证明: 下述集合

$$\text{Gal}(L/K) = \left\{ L \xrightarrow{\sigma} L \mid \sigma \text{ 是域同构, 且 } \sigma(a) = a \text{ 对任意 } a \in K \text{ 成立} \right\}$$

关于映射的合成是一个群 (称为域扩张 $L \supset K$ 的伽罗瓦群).

proof

$\text{Gal}(L/K) \subseteq \text{Aut}(L)$, 只需说明 $\text{Gal}(L/K)$ 是子群.

$\forall \varphi, \psi \in \text{Gal}(L/K)$, 由于 $\psi|_K = \text{id}_K$, 因此 $\psi^{-1}|_K = \text{id}_K$, 故 $(\varphi \circ \psi^{-1})|_K = \text{id}_K$, 即 $\varphi \circ \psi^{-1} \in \text{Gal}(L/K)$. \square

1.4.12 求 $\text{Gal}(\mathbb{Q}[\sqrt{d}]/\mathbb{Q})$, 此处 $d \in \mathbb{Z}$, $\sqrt{d} \notin \mathbb{Q}$.

proof

同1.4.9, 若 $\sigma \in \text{Gal}(\mathbb{Q}[\sqrt{d}]/\mathbb{Q})$, 则 $\sigma \in \text{Aut}_{\mathbb{Q}\text{-vect}}(\mathbb{Q}[\sqrt{d}])$, 因此 $\sigma(a + b\sqrt{d}) = a + b\sigma(\sqrt{d})$. 然后由于保持乘法得到 $\sigma(\sqrt{d}) \cdot \sigma(\sqrt{d}) = d$, 得到 $\sigma(\sqrt{d}) = \pm\sqrt{d}$.

因此 $\text{Gal}(\mathbb{Q}[\sqrt{d}]/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z}$, 两个同构分别为 id 和共轭. \square

1.4.13 设 $V = (V, +)$ 是一个加法群, $\text{Hom}(V)$ 表示它的自同态环. 对任意域 K , 如果存在一个数乘运算 $K \times V \rightarrow V, (\lambda, v) \mapsto \lambda \cdot v$, 使得加法群 $V = (V, +)$ 成为一个 K -线性空间, 则称该数乘运算是加法群 $V = (V, +)$ 上的一个 K -线性空间结构. 试证明:

(1) 如果存在一个环同态 $\varphi: K \rightarrow \text{Hom}(V)$, 则数乘运算

$$K \times V \rightarrow V, (\lambda, v) \mapsto \lambda \cdot v := \varphi(\lambda)(v)$$

是 V 上的一个 K -线性空间结构;

(2) 如果在 V 上存在 K -线性空间结构 $\phi: K \times V \rightarrow V$, 则映射

$$\varphi: K \rightarrow \text{Hom}(V), \lambda \mapsto \phi(\lambda, \cdot)$$

是一个环同态, 其中 $\phi(\lambda, \cdot): V \rightarrow V$ 定义为 $v \mapsto \phi(\lambda, v) := \lambda \cdot v$;

(3) 对任意域 K , 整数加法群 $\mathbb{Z} = (\mathbb{Z}, +)$ 上不存在 K -线性空间结构.

proof

(1) 验证数乘的四条:

(i) 由于 φ 是环同态, 因此 $\varphi(1) = 1_{\text{Hom}(V)} = \text{id}_V$. 故 $\forall v \in V$ 有 $1v = \varphi(1)(v) = \text{id}_V(v) = v$.

(ii) $\forall a, b \in K, v \in V (a + b)v = (\varphi(a + b))(v) = (\varphi(a) + \varphi(b))(v) = \varphi(a)(v) + \varphi(b)(v) = av + bv$.

(iii) $\forall a \in K, v, w \in V a(v + w) = \varphi(a)(v + w) = \varphi(a)(v) + \varphi(a)(w) = av + aw$.

(iv) $\forall a, b \in K, v \in V (ab)v = \varphi(ab)(v) = (\varphi(a) \circ \varphi(b))(v) = \varphi(a)(\varphi(b)(v)) = a(bv)$.

(2) (1) 的反向.

(i) $\forall a \in K, v, w \in V \varphi(a)(v + w) = \phi(a, v + w) = a(v + w) = av + aw = \phi(a, v) + \phi(a, w) = \varphi(a)(v) + \varphi(a)(w)$ 这说明 $\varphi(a)$ 保持加法.

(ii) $\forall a \in K, v \in V \varphi(a)(kv) = \phi(a, kv) = a(kv) = (ka)v = \phi(ka, a) = \varphi(ka)(v)$ 这说明 $\varphi(a)$ 保持数乘.

由 (i)(ii) 知 φ 是良定义的 (well-defined). 同时 (ii) 也说明 $\varphi(ab) = \varphi(a) \circ \varphi(b)$.

(iii) 由 ϕ 是数乘, 即 $1v = v, \forall v \in V$. 也就是说 $\phi(1, \cdot) = \text{id}_V$.

(iv) $\forall a, b \in K, v \in V, \varphi(a+b)(v) = \phi(a+b, v) = (a+b)v = av + bv = \phi(a, v) + \phi(b, v) = \varphi(a) + \varphi(b)$

(3) 用反证法, 假设 $(\mathbb{Z}, +)$ 上存在一个 K -线性空间结构, 即存在一个环同态 $\varphi: K \rightarrow \text{Hom}(\mathbb{Z})$.

但是 $\text{Hom}(\mathbb{Z})$ 和整数环 \mathbb{Z} 是同构的 (教材例 1.4.4). 我们又知道域出发的环同态一定是单的 (教材命题 1.4.1 的 (9)), 也就是说存在一个域 K 到 \mathbb{Z} 的单同态, 这是不可能的. 由 1.4.7, 一定有 $n \mapsto n, \forall n \in \mathbb{Z}$, 而同态一定会把单位映到单位, 但 \mathbb{Z} 中只有 ± 1 是单位.

1.4.7 也说明了环同态是保特征的, 因此 $\text{Char}(K) = \text{Char}(\mathbb{Z}) = 0$, 从而 $\mathbb{Q} \subseteq K$. 这样也可以看出矛盾.

□

注:

(1)(2) 即一个模结构的两种等价表述, 在群作用 (教材 4.5 节) 也会看到类似的定义.

1.4.14 证明: 在整数集合 \mathbb{Z} 上存在运算 $\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}, (a, b) \mapsto a \oplus b$, 使得 (\mathbb{Z}, \oplus) 是一个交换群, 但它与整数加法群 $(\mathbb{Z}, +)$ 不同构. 提示: 利用 \mathbb{Q} 是可数集和上题中的问题 (3).

proof

类似 1.1.4, 存在一个可数集之间的双射 $f: \mathbb{Z} \rightarrow \mathbb{Q}$, 由 \mathbb{Q} 的环结构导出 $(\mathbb{Z}, \oplus, \star)$.

则同态

$$f^{-1}: \mathbb{Q} \rightarrow (\mathbb{Z}, \oplus, \star)$$

会自然诱导出一个 \mathbb{Q} -线性空间结构 (1.4.9 的 (1)). 由 1.4.13 的 (3), (\mathbb{Z}, \oplus) 和 $(\mathbb{Z}, +)$ 不同构. □

注:

对于 \mathbb{Z} 还有一个重要的结论, \mathbb{Z} 的 (含么) 环结构是唯一的. 更严格来说, 在 $(\mathbb{Z}, +)$ 上添加乘法, 那么只能得到唯一的环结构.(可参考 [Alu09]III.2.15, 2.16)

第 2 章 唯一分解整环

习题 2.1 教材 p28-p29

2.1.1 设 R 是一个交换环, $I \subsetneq R$ 是一个理想. 证明

$$\sqrt{I} = \{r \in R \mid \exists m \in \mathbb{N} \text{ 使得 } r^m \in I\}$$

也是 R 的理想 (称为理想 I 的根).

注:

这题的理想根定义有误, 应是 \mathbb{N} 而不是 \mathbb{Z} . 一旦出现负整数意味着有可逆元, 从而 \sqrt{I} 是单位理想了.

proof

先验证加法子群,

$$\begin{aligned} \forall a, b \in \sqrt{I}, \exists m, n \in \mathbb{N}, a^m, b^n \in I, \\ \implies (a - b)^{m+n} \in I \end{aligned}$$

这是因为单项 $a^i b^j$ 的指数 $i + j = m + n$, 故 $i < m$ 和 $j < n$ 不能同时成立, 即 $i \geq m$ 或 $j \geq n$, i.e. $a^i \in I$ 或 $b^j \in I$. 从而 $(a - b)^{m+n} \in I$, $a - b \in \sqrt{I}$. 再验证吸收律 (交换验证单边即可),

$$\forall a \in \sqrt{I}, r \in R, \exists m \in \mathbb{N}, a^m \in I \implies (ar)^m = a^m r^m \in I$$

因此 $ar \in \sqrt{I}$. □

注:

零理想的根 $\sqrt{\{0\}} = \{x \in R \mid \exists n \in \mathbb{N}, x^n = 0\}$ 是所有幂零元 (nilpotent) 组成的理想, 叫做 R 的幂零根 (nilradical), 一般记作 $\mathfrak{N}(R)$. 可以证明 $\mathfrak{N}(R) =$

$\bigcap_{\mathfrak{p} \text{ 是素理想}} \mathfrak{p}$. (可以参考 [AM94]p5)

对任何的理想 I 可以清楚地看出 $I \subseteq \sqrt{I}$. 若 $\sqrt{I} = I$, 我们称 I 是一个根理想 (radical ideal). 任何的素理想 (2.1.5) 都是根理想.

2.1.2 设 R 是一个交换环, $p > 0$ 是一个素数. 如果 $p \cdot x = 0 (\forall x \in R)$. 试证明: $(x + y)^{p^m} = x^{p^m} + y^{p^m} (\forall x, y \in R, m > 0)$

proof

事实上, 这个 p 就是环 R 的特征. 若 $\text{Char}(R) \neq p$, 则由 $p = 0$, $\text{Char}(R) < p$. 那么 $(p, \text{Char}(R)) = 1$, 有 Bézout's Identity 得到 $1 = 0$, 这就没什么考虑的必要了.

对特征 p 的交换环, 有一个特别的同态 F 称为 Frobenius 自同态,

$$F : R \rightarrow R, \quad a \mapsto a^p$$

我们说明这确实是一个同态.

保持乘法是因为交换环, 不平凡的是保持加法.

$$(a + b)^p = a^p + \binom{p}{1} a^{p-1}b + \cdots + b^p.$$

其中 $1 \leq i \leq p-1$ 时,

$$\binom{p}{i} = \frac{p(p-1) \cdots (p-i+1)}{1 \cdot 2 \cdots i}$$

由于 p 是素数, $1, 2, \dots, i$ 都不整除 p , 而 $\binom{p}{i}$ 是整数, 因此只能是 $i! \mid (p-1) \cdots (p-i+1)$. 所以 $p \mid \binom{p}{i}$. 而 $p = 0$, 故 $(a+b)^p = a^p + b^p$.

因此 $\varphi : R \rightarrow R, x \mapsto x^{p^m}$ 也是自同态, $\varphi = F^m$, 这里 F^m 表示复合 m 次.

□

注:

Frobenius 一般在域中使用的多一些. 虽然对交换环 Frobenius 都是可以定义的, 但是整环才能保证 Frobenius 是单射. Frobenius 一般不是满的, 但对有限域就是自同构了.

2.1.3 证明: 只有有限个元素的整环一定是一个域.

proof

整环 R 有乘法消去律 1.1.1, 而 1.3.9 告诉我们, 满足消去律的有限半群是群. 因此 $(R \setminus \{0\}, \cdot)$ 是群, 即 R 是一个域. □

2.1.4 证明: 只有有限个理想的整环是一个域.

proof

事实上条件可以再减弱一点, 一个 Artin 整环一定是域.

设 $a \neq 0$, 考虑理想降链

$$(a) \supseteq (a^2) \supseteq \cdots$$

因此 $\exists n \in \mathbb{Z}_{>0}, (a^n) = (a^{n+1})$. 即有 $a^n \in (a^{n+1})$, 那么 $\exists b \in R, a^n = a^{n+1}b$, 从而 $ab = 1_R$. □

注:

Artin 环定义为任意理想降链稳定的环, i.e. 若有理想降链

$$I_1 \supseteq I_2 \supseteq \cdots$$

则存在 $n \in \mathbb{Z}_{>0}$ 使得 $\forall m > n, I_m = I_n$, 也就是说从某一个 n 开始就稳定了 $I_n = I_{n+1} = \cdots$. 这个条件称为 descending chain condition(d.c.c.), 与之对应的是 ascending chain condition(a.c.c.), 满足 a.c.c. 的正是 Noether 环.

2.1.5 理想 $P \subsetneq R$ 称为素理想, 如果: $ab \in P \Rightarrow a \in P$ 或 $b \in P$. 试证明: $P \subsetneq R$ 是素理想当且仅当 R/P 没有零因子.

proof

(1) " \Rightarrow ":

$$\begin{aligned} \forall \bar{a}, \bar{b} \in R/P, \bar{a}\bar{b} = \overline{ab} = \bar{0} &\Rightarrow ab \in P \Rightarrow a \in P \text{ 或 } b \in P \\ &\Rightarrow \bar{a} = \bar{0} \text{ 或 } \bar{b} = \bar{0}. \end{aligned}$$

(2) " \Leftarrow ":

$$ab \in P \Rightarrow \bar{a}\bar{b} = \overline{ab} = \bar{0} \Rightarrow \bar{a} = 0 \text{ 或 } \bar{b} = 0 \Rightarrow a \in P \text{ 或 } b \in P.$$

□

注:

1. 零理想 (0) 是素理想.
2. 一个交换环的 (Krull) dimension 定义为最长素理想链的长度, 其中, 若有素理想链

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$$

他的长度定义为 n . (可参考 [AM94]p89, [Alu09]p153)

交换 Artin 环 (2.1.4) 是 0 维的 Noether 环. 0 维即意味着所有的素理想都是极大理想.

3. 对交换环 R , $\text{Spec}(R) := \{\mathfrak{p} \mid \mathfrak{p} \text{ 是 } R \text{ 的素理想}\}$ 称为 R 的素谱 (spectrum). $\text{Spec}(R)$ 上有一个 Zariski 拓扑. (这个就不给参考书了, 自行搜索或查阅代数几何相关书籍吧)

2.1.6 理想 $m \subsetneq R$ 称为极大理想, 如果 R 中不存在真包含 m 的非平凡理想 (即: 如果 $I \supsetneq m$ 是 R 的理想, 则必有 $I = R$). 试证明: 当 R 是交换环时, $m \subsetneq R$ 是极大理想当且仅当 R/m 是一个域. 特别, 交换环中的极大理想必为素理想.

proof

(1) " \Rightarrow ":

$$\begin{aligned}\forall \bar{0} \neq \bar{a} \in R/m &\Rightarrow a \notin m \Rightarrow m \subsetneq m + (a) \Rightarrow m + (a) = R = (1) \\ &\Rightarrow \exists x \in m, b \in R, x + ab = 1 \Rightarrow \overline{ab} = \overline{1 - x} = \bar{1}.\end{aligned}$$

(2) " \Leftarrow ":

$$\begin{aligned}m \subsetneq I \underset{\text{ideal}}{\subseteq} R &\Rightarrow \exists a \in I \setminus m \text{ i.e. } \bar{a} \neq 0 \Rightarrow \exists b \in R, \bar{a}\bar{b} = \overline{ab} = \bar{1} \\ &\Rightarrow \exists x \in m \subsetneq I, ab = 1 + x \Rightarrow 1 = ab - x \in I \\ &\Rightarrow I = (1) = R.\end{aligned}$$

或者用同态基本定理, 包含 m 的理想和 R/m 的理想有一个一一对应, 而域的理想只有 $\{0\}$ 和本身.

□

注:

(1) 中用到了理想的和. 若 I, J 都是 R 的理想, $I + J := \{i + j \mid i \in I, j \in J\}$. 可以验证这确实是一个理想, 类似可以定义一族理想 $\{I_\alpha\}_{\alpha \in A}$ 的和,

$$\sum_{\alpha \in A} I_\alpha = \left\{ \sum_{\alpha \in A} i_\alpha \mid i_\alpha \in I_\alpha, \text{ 且只有有限个 } i_\alpha \neq 0 \right\}$$

即考虑所有可能的有限和. 所谓子集 $S \subseteq R$ 生成的理想, 是指理想

$$(S) = \sum_{a \in S} (a).$$

对一个理想 I , 若存在有限子集 S 生成 I , 则称 I 是有限生成的.

另外 $\bigcap_{\alpha \in A} I_\alpha$ 也是一个理想. 还有一个是理想的积, 相对要复杂一些,

$$\begin{aligned}IJ &:= (\{ij \mid i \in I, j \in J\}) \\ &= \left\{ \sum_{k=1}^n i_k j_k \mid \exists n \in \mathbb{N}, 1 \leq k \leq n, i_k \in I, j_k \in J \right\}\end{aligned}$$

他是所有乘积 ij 生成的理想. 那么一族理想的乘积就是考虑所有可能的有限乘积生成的理想.

2.1.7 设 $I \subsetneq \mathbb{Z}$ 是整数环的非零理想, 证明下述结论等价

(1) I 是极大理想;

(2) I 是素理想;

(3) 存在素数 p 使得 $I = (p)\mathbb{Z} = \{ap \mid \forall a \in \mathbb{Z}\}$.

proof

1. (1) \implies (2): 由于域一定是整环, 由2.1.5和2.1.6知极大理想是素理想.

2. (2) \implies (3): 由于 \mathbb{Z} 是 PID(带余除法可证), 故存在整数 p 使得 $I = (p)$. 由于是素理想, 因此 $ab \in (p) \implies a \in (p)$ 或 $b \in (p)$. 即

$$p \mid ab \implies p \mid a \text{ or } p \mid b$$

则 p 是素数 (若不然, $p = qr$, 取 $a = q, b = r$ 即导出矛盾).

3. (3) \implies (1): 设 $I = (p) \subsetneq J$, 则存在 $n \in J \setminus I$. 由于 p 是素数, 故有 $(n, p) = 1$. 由 Bézout's Identity, $\exists u, v \in \mathbb{Z}$ 使得 $nu + pv = 1$, 从而 $1 \in J, J = \mathbb{Z}$. (这和2.1.6的证明是类似的)

或直接用 $\mathbb{Z}/(p) = \mathbb{Z}/p\mathbb{Z}$ 是域.

□

2.1.8 设 $p \in \mathbb{Z}$ 是素数, 证明 $(p)\mathbb{Z}[x] = \{pf(x) \mid \forall f(x) \in \mathbb{Z}[x]\}$ 是整系数多项式环的素理想, 但不是 $\mathbb{Z}[x]$ 的极大理想.

proof

事实上若 I 是 R 的理想, 我们有

$$\frac{R[x]}{IR[x]} \cong \frac{R}{I}[x]$$

这是根据同态基本定理得到, 考虑同态

$$\varphi: R[x] \rightarrow \frac{R}{I}[x], \quad a_0 + a_1x + \cdots + a_nx^n \mapsto \overline{a_0} + \overline{a_1}x + \cdots + \overline{a_n}x^n$$

可以验证这确实是一个同态. 事实上, 它是 $R \twoheadrightarrow R/I \hookrightarrow \frac{R}{I}[x]$ 的一个延拓. 回到原题, 有

$$\frac{\mathbb{Z}[x]}{(p)\mathbb{Z}[x]} \cong \mathbb{Z}_p[x]$$

这里 $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ 是域. 因此 $\mathbb{Z}_p[x]$ 是 PID, 自然是整环, 但不是域 (x 没有逆). 因此由2.1.5和2.1.6, $(p)\mathbb{Z}[x]$ 是素理想但不是极大理想. □

注:

给定环同态 $R \xrightarrow{\varphi} S$, 其中 R 是交换环. 若 $\varphi(R) \subseteq C(S)$ (2.1.11), 根据我们之

前1.4.9说过的, 首先 S 上有一个 R -模结构. 其次有

$$(r_1 s_1)(r_2 s_2) = \varphi(r_1) s_1 \varphi(r_2) s_2 = \varphi(r_1) \varphi(r_2) s_1 s_2 = \varphi(r_1 r_2) s_1 s_2 = (r_1 r_2)(s_1 s_2).$$

即数乘和 S 本身的乘法是相容的. 这样的结构我们称为一个 R -代数 (R -algebra), 这也是2.1.12介绍的东西. 因此一个 R -代数就是带有加法, (R -) 数乘, 乘法的一个代数结构.

当 S 本身就是交换环时, 此时乘法是交换的, 且 $C(S) = S$, 这样会变得简单很多. 这时 S 称为一个交换 R -代数, 这也是交换代数会考虑的情形. 我们会把 S 看作一个有序对 (S, φ) , 一个交换 R -代数 S 也叫做一个 R -(交换) 环. 那么交换 R -代数构成的范畴是交换环范畴的余切片范畴 (coslice category).

而这里提到的延拓其实是多项式环的泛性质 (universal property), 或者说是自由交换 R -代数的泛性质, 因为 $R[x]$ 就是一个的自由交换 R -代数.(可参考 [Alu09]III.§6.3)

2.1.9 映射 $D : R[x] \rightarrow R[x]$ 定义如下: $\forall f(x) = a_n x^n + \cdots + a_1 x + a_0$,

$$D(f) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \cdots + 2 a_2 x + a_1.$$

$\forall a \in R, f, g \in R[x]$, 试证明:

- (1) $D(f+g) = D(f) + D(g), D(af) = aD(f);$
- (2) $D(f \cdot g) = D(f) \cdot g + f \cdot D(g).$

($D(f)$ 称为 $f(x)$ 的导数. 记为 $f'(x) = D(f)$, $f^{(m)}(x) = \overbrace{D \cdots D}^m(f)$ 称为 $f(x)$ 的 m 次导数).

proof

按定义验证. 设 $f = a_n x^n + \cdots + a_1 x + a_0, g = b_m x^m + \cdots + b_1 x + b_0$.

(1) 不妨设 $n \geq m$, 且令 $b_k = 0, k > m$.

$$\begin{aligned} D(f+g) &= D\left(\sum_{k=0}^n (a_k + b_k) x^k\right) = \sum_{k=1}^n k(a_k + b_k) x^{k-1} \\ &= \sum_{k=1}^n k a_k x^{k-1} + \sum_{k=1}^m k b_k x^{k-1} = D(f) + D(g). \end{aligned}$$

$$D(af) = D\left(\sum_{k=0}^n a a_k x^k\right) = \sum_{k=1}^n k a a_k x^{k-1} = a \sum_{k=1}^n k a_k x^{k-1} = a D(f).$$

这里能把 a 提出来是因为 k 作为 $k1$ (1.2.1的注记), 有 $ka = ak$.

(2)

$$\begin{aligned}
D(f \cdot g) &= D\left(\sum_{k=0}^{n+m} \sum_{i+j=k} a_i b_j x^k\right) = \sum_{k=1}^{n+m} \sum_{i+j=k} k a_i b_j x^{k-1} \\
&= \sum_{k=1}^{n+m} \sum_{i+j=k} (i+j) a_i b_j x^{i+j-1} \\
&= \sum_{k=1}^{n+m} \sum_{i+j=k} (i a_i x^{i-1}) b_j x^j + a_i x^i (j b_j x^{j-1}) \\
&= \sum_{k=0}^{n+m-1} \sum_{(i-1)+j=k} (i a_i) b_j x^k + a_i (j b_j) x^k \\
&= D(f) \cdot g + f \cdot D(g).
\end{aligned}$$

□

2.1.10 如果 F 是特征零的域, 则 $f'(x) = 0 \Leftrightarrow \deg(f) = 0$ 或 $f(x) = 0$ (即常数); 如果 F 的特征是 $p > 0$, 则 $f'(x) = 0 \Leftrightarrow$ 存在 $g(x) \in F[x]$ 使得 $f(x) = g(x^p)$.

proof

$\text{Char}(F) = 0$, 即 $\forall n \in \mathbb{Z}_{>0}, n \neq 0$ (1.2.1 的注记), 那么

$$f'(x) = n a x^{n-1} + \cdots + a_1 = 0 \implies 1 \leq k \leq n, k a_k = 0 \implies 1 \leq k \leq n, a_k = 0$$

故 $f(x) = a_0$, $\deg(f) = 0$ 或 $f = 0$, 反过来是平凡的.

若 $\text{Char}(F) = p$, 则 $p = 0$, 那么设 $\deg(f) = n = kp + r, 0 \leq r < p, k \in \mathbb{N}$,

$$\begin{aligned}
f &= a_0 + a_1 x + \cdots + a_p x^p + \cdots + a_{2p} x^{2p} + \cdots + a_{kp} x^{kp} + a_n x^n. \\
\implies f' &= a_1 + \cdots + p a_p x^{p-1} + \cdots + k p a_{kp} x^{kp-1} + \cdots + n a_n x^{n-1} \\
&= a_1 + \cdots + (p-1) a_{p-1} x^{p-2} + (p+1) a_{p+1} x^p + \cdots + (kp-1) a_{kp-1} x^{kp-2} \\
&\quad + (kp+1) a_{kp+1} x^k p + \cdots + n a_n x^{n-1}.
\end{aligned}$$

此时 $f' = 0$ 有 $f = a_0 + a_p x^p + \cdots + a_{kp} x^{kp} = g(x^p)$. 这里 $g = a_0 + a_p x + \cdots + a_{kp} x^k$. 反过来也是类似的. □

2.1.11 设 R 是一个环, 子环 $C(R) = \{a \in R \mid ab = ba \forall b \in R\}$ 称为 R 的中心. 试证明:

- (1) 如果 R 是一个除环, 则 $C(R)$ 是一个域;
- (2) 令 \mathbb{H} 表示 Hamilton 四元数环, 则 $C(\mathbb{H}) = \mathbb{R}$.

proof

(1) 除环的子环自然是除环, $C(R)$ 和 R 中所有元素交换, 故 $C(R)$ 本身是交换环, 从而是域.

(2) 设 $\alpha = a + ib + jc + kd \in C(\mathbb{H})$, 则有

$$\alpha \cdot i = i \cdot \alpha$$

$$\alpha \cdot j = j \cdot \alpha$$

得到 $b = c = d = 0$, 即 $\alpha \in \mathbb{R}$.

□

2.1.12 设 K 是一个域. 如果 $C(R)$ 包含一个同构于 K 的子域, 则称环 R 为 K -代数. 试证明: 加法群 $(R, +)$ 通过 R 的乘法成为一个 K -向量空间.

proof

见1.4.9和2.1.8的注记. $C(R)$ 包含一个和 K 同构的子域, 等价地说就是有一个域同态 $K \rightarrow R$.

□

注:

$C(R)$ 包含一个同构于 K 的子域, 即存在同态 $K \xrightarrow{\varphi} R$ 使得 $\varphi(K) \subseteq C(R)$ (这是因为域出发的同态一定是单的). 这和之前说的是一样的.

2.1.13 设 R 是一个 K -代数, $\dim_K(R)$ 称为 R 的维数. 试证明:

- (1) 矩阵环 $M_n(K)$ 是一个 n^2 维 K -代数;
- (2) 任意 n 维 K -代数必同构于 $M_n(K)$ 的子环;
- (3) 如果 R 是一个有限除环, 则 R 是有限域上的有限维代数.

proof

(1) $M_n(K)$ 是 n^2 维 K -线性空间, 按2.1.8注记, 只需验证

$$k_1 M_1 k_2 M_2 = k_1 k_2 M_1 M_2, k_1, k_2 \in K, M_1, M_2 \in M_n(K).$$

这可以根据 $M_n(K)$ 的定义得到. 事实上 $C(M_n(K)) = \{kI_n \mid k \in K\} \cong K$.

(2) 由教材例 1.4.3, 对任意的环 R , 我们用 $\text{End}_{\text{Ab}}(R)$ 表示加法群的自同态环 (关于加法和复合). 有一个自然的环同态,

$$R \rightarrow \text{End}_{\text{Ab}}(R), \quad r \mapsto \lambda_r$$

其中 $\lambda_r : R \rightarrow R, a \mapsto ra$, 即左乘 r 这个自同态 (这里换成右乘也是一样的). 这是一个单同态, 所以 R 同构于 $\text{End}_{\text{Ab}}(R)$ 的一个子环.

那么当 R 是 n 维 K -代数时, λ_r 还是 K -线性映射. 因此有单射 $R \hookrightarrow \text{Hom}_K(R) \cong M_n(K)$.

- (3) R 是有限除环, 因此 $C(R)$ 是有限域 (2.1.11). 根据定义 R 是一个 $C(R)$ -代数, 且 R 有限, 故是有限维的 ($|R| = [R : C(R)][C(R)]$).

□

2.1.14 设 K 是一个域, R 是一个有限维 K -代数. 试证明:

- (1) $\forall \alpha \in R$, 存在非零多项式 $f(x) \in K[x]$ 使得 $f(\alpha) = 0$;
- (2) 如果 R 是除环, $\alpha \neq 0$, 则 α 的极小多项式 $\mu_\alpha(x) \in K[x]$ 不可约;
- (3) 如果 R 是除环, K 是代数闭域 (即 $K[x]$ 中次数大于零的多项式在 K 中必有根), 则 $R = K$.

历史上, 有限维可除 K -代数的分类是一个热门话题. 当 K 是实数域时, R 必同构于实数域, 复数域或 Hamilton 四元数环之一 (Frobenius 定理); 当 K 是有限域时, R 必为交换环 (Wedderburn 定理).

注:

零多项式是平凡的, 因此 (1) 我做了修改. 在域扩张中, 这样的元素称为 K 上的代数元 (algebraic element), 或者称 α 在 K 上代数 (algebraic over K). 给定域扩张 L/K , 若 $\forall \alpha \in L$ 都在 K 上代数, 则称该扩张是代数扩张.

proof

- (1) 设 $\dim_K R = n$. 则 $1, \alpha, \alpha^2, \dots, \alpha^n$ 线性相关. 或者考虑线性映射 $r \mapsto \alpha r$. 那么它对应的矩阵的特征多项式满足条件 (Cayley-Hamilton Theorem).
- (2) 按定义, μ_α 是满足 α 的次数最小的 (首一) 多项式. 假设 μ_α 可约, 即 $\mu_\alpha(x) = f(x)g(x)$, $\deg(f), \deg(g) > 0$, 则 $0 = \mu_\alpha(\alpha) = f(\alpha)g(\alpha)$. 由于除环无零因子, 故 $\deg(\mu_\alpha) = \deg(f) + \deg(g)$, 且 $f(\alpha) = 0$ 或 $g(\alpha) = 0$. 不妨设 $f(\alpha) = 0$, 但 $\deg(f) < \deg(\mu_\alpha)$ 与极小矛盾.
- (3) 代数闭域等价于任意多项式可分解成一次多项式的乘积. 这和代数基本定理是类似的. 此时 $K[x]$ 中的不可约多项式即为所有一次多项式. 由 (2), $\forall \alpha \in R$, 极小多项式 $\mu_\alpha(x) = x - k_\alpha, k_\alpha \in K$. 因此 $\alpha = k_\alpha \in K$. 即 $R = K$.

□

2.1.15 证明: 集合 $\mathbb{F}_{3^2} = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{F}_3 = \mathbb{Z}/(3) \right\}$ 关于矩阵的“加法”和“乘法”成为一个 9 元域. 若将定义中的 \mathbb{F}_3 换成 \mathbb{F}_5 , 上述集合是否是一个 25 元域, 为什么?

proof

这个集合是 \mathbb{F}_3 上的 2 维线性空间.

$$\mathbb{F}_{3^2} = \left\{ a\lambda + b\xi \mid \lambda = I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \xi = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, a, b \in \mathbb{F}_3 \right\}$$

其中 ξ 的特征多项式为 $x^2 + 1$, 可以验证它是不可约的. 又因为 $\mathbb{F}_3[x]$ 是 PID ($\mathbb{F}_3[x]$ 是域), 故 $(x^2 + 1)$ 是极大理想, $x^2 + 1$ 就是 ξ 的极小多项式. 则 $\mathbb{F}_{3^2} = \mathbb{F}_3[x]/(x^2 + 1)$ 是域.

但 $x^2 + 1$ 在 $\mathbb{F}_5[x]$ 中是可约的: 在 $\mathbb{F}_5[x]$ 中,

$$x^2 + 1 = x^2 - 4 = (x - 2)(x + 2).$$

□

习题 2.2 教材 p35-p36

2.2.1 设 m, n 是两个正整数, 证明它们在 \mathbb{Z} 中的最大公因数和它们在 $\mathbb{Z}[i]$ 中的最大公因数相同.

注意这里的相同指的在相伴的意义下相同.

proof

由于 $U(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$, 在相伴的意义下, 可以假设 (m, n) 在 \mathbb{Z} 和 $\mathbb{Z}[i]$ 中都是正整数, 分别记为 d 和 d' .

那么 PID 上 Bézout's Identity 成立, 有

$$d = mu + nv, \quad d' = m\alpha + n\beta.$$

其中 $u, v \in \mathbb{Z}$, $\alpha, \beta \in \mathbb{Z}[i]$. 设 $\alpha = a_1 + ia_2$, $\beta = b_1 + ib_2$, 由于我们假设的是 $d' \in \mathbb{Z}_{>0}$, 故 $d' = ma_1 + nb_1$, 从而 $d \mid m, d \mid n \implies d \mid d'$. 反过来也有 $d' \mid d$, 所以 $d = d'$. □

2.2.2 设 R 是整环, $p \in R$ 称为一个素元如果它生成的理想 $P = (p)R$ 是素理想. 证明: R 中素元必为不可约元.

proof

由定义 $(p) \neq (1)$, 因此 p 不可逆. 设 $p = ab$, 则 $ab \in (p)$, 由素理想知 $a \in (p)$ 或 $b \in (p)$, 不妨设 $a \in (p)$, 则 $(a) \subseteq (p)$. 另一方面 $(p) \subseteq (a)$, 因此 $(p) = (a)$, 从而 b 是单位. \square

注:

$x \sim y \Leftrightarrow \exists u \in U(R), x = uy \Leftrightarrow (x) = (y) \Leftrightarrow x \mid y$ 且 $y \mid x$.

2.2.3 设 R 是一个主理想整环 (PID), $0 \neq r \in R$. 证明: 在 R 中仅有有限个理想包含 r .

proof

R 是 PID, 即对任意理想 I , 存在 $a \in R$, 理想 $I = (a)$. 理想 I 包含 r 指 $r \in I$, 它等价于 $(r) \subseteq I = (a) \Leftrightarrow a \mid r$. 又因为 PID 是 UFD, 因此又唯一分解 $r = p_1 p_2 \cdots p_n$, 从而 r 因子个数在相伴的意义下 (2.2.2 的注记) 有限 ($\leq 2^n$), 即包含 r 的理想有限. \square

2.2.4 (辗转相除法) 设 R 是欧氏环, $a, b \in R$ 非零. 由带余除法得

$$a = q_1 b + r_1, b = q_2 r_1 + r_2, r_1 = q_3 r_2 + r_3, \cdots, r_{k-2} = q_k r_{k-1} + r_k$$

满足 $\delta(r_k) < \delta(r_{k-1}) < \cdots < \delta(r_2) < \delta(r_1) < \delta(b)$. 试证明:

- (1) 存在 k 使得 $r_{k+1} = 0$;
- (2) r_k 是 a, b 的一个最大公因子;
- (3) 求 $u, v \in R$ 使得 $r_k = ua + vb$.

proof

(1) 由于 $\delta(b) < \infty$, 且 $\delta(r_k)$ 是严格递减的自然数序列, 因此 $\delta(k) \leq \delta(b) - k$, 取 $k > \delta(b)$ 即可.

(2) 由 (1) 知最后一个等式为 $r_{k-1} = q_{k+1} r_k$. 且

$$(a, b) = (bq_1 + r_1, b) = (b, r_1) = (r_1, r_2) = \cdots = (r_{k-1}, r_k) = r_k.$$

(3) 根据辗转相除法的算式反过来表示 r_k .

$$\begin{aligned} r_k &= r_{k-2} - q_k r_{k-1} = u_1 r_{k-2} + v_1 r_{k-1}, \quad u_1 = 1, v_1 = -q_k \\ &= u_1 r_{k-2} + v_1 (r_{k-3} - q_{k-1} r_{k-2}), \quad (r_{k-3} = q_{k-1} r_{k-2} + r_{k-1}) \\ &= u_2 r_{k-3} + v_2 r_{k-2}, \quad u_2 = -q_k, v_2 = 1 + q_k q_{k-1} \\ &= \cdots \\ &= u_k a + v_k b \end{aligned}$$

递归关系是 $u_i = v_{i-1}, v_i = u_{i-1} - v_{i-1}q_{k-i+1}$.

□

注:

(1) 是著名的无穷递降的思路, 即递归的得到一系列对象且对应着一个严格递减的自然数序列, 根据自然数有下界 0 来得到矛盾或得出某个结论.

另外 (3) 的题干表述可能有些问题, 这里并不需要把 u, v 具体表达出来.

2.2.5 设 $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid \forall a, b \in \mathbb{Z}\} \subset \mathbb{C}$, 定义: $N(a + b\sqrt{-5}) = a^2 + 5b^2$. 试证明:

- (1) $U(R) = \{1, -1\}$;
- (2) R 中任意元素都有不可约分解;
- (3) $3, 2 + \sqrt{-5}, 2 - \sqrt{-5} \in R$ 是不可约元;
- (4) $9 = 3 \cdot 3 = (2 + \sqrt{-5}) \cdot (2 - \sqrt{-5})$ 是 9 的两个不相同的不可约分解.

proof

(1) 验证 N 满足 $N(\alpha\beta) = N(\alpha)N(\beta)$, 这和复数中 $|z_1 z_2| = |z_1| |z_2|$ 是类似的, 且 $N(\alpha) \in \mathbb{N}$. 那么若 α 是单位, 则存在 β 使得 $\alpha\beta = 1$, 故 $N(\alpha\beta) = N(\alpha)N(\beta) = N(1) = 1$, 故只能有 $N(\alpha) = N(\beta) = 1$, 解得 $\alpha = \pm 1$.

(2) 因为 R 是 Noether 环.(由 Hilbert's Basis Theorem)

或者可以用 $N(\alpha)$ 保持乘法的特性. 对任意 $\alpha \in R$, 若它不可约, 则已经是一个分解了; 否则 $\alpha = \beta\gamma$, 其中 β, γ 不是单位, 且有 $N(\alpha) = N(\beta)N(\gamma)$. 因此 $N(\beta), N(\gamma) < N(\alpha)$, 由于 $N(\alpha) < \infty$, 因此这样分解是有限的, 这和 Noether 环 \implies 存在分解的过程是类似的.

(3) 由于 $N(3) = N(2 + \sqrt{-5}) = N(2 - \sqrt{-5}) = 9 = 3^2$, 若它们可约, 则存在 α 使得 $N(\alpha) = 3$, 这是不可能的.

另外, 若 $N(\alpha)$ 是素数, 则一定不可约, 但是反过来不对, 比如这里 9 并不是素数.

(4) 由 (3).

□

注:

1. 这个 N 是范数 (norm). 它其实是 \mathbb{Q} -线性映射 $\beta \mapsto \alpha\beta$ 所对应矩阵的行列式. 这个概念在模论和代数数论都有提及.
2. (1) 和 (2) 的结论是可以推广的, 对于一个代数数域 K/\mathbb{Q} (即 \mathbb{Q} 的有限扩张), $\alpha \in \mathcal{O}_K$ 是单位当且仅当 $N_{K/\mathbb{Q}}(\alpha) = \pm 1$. 其中 \mathcal{O}_K 是对应的代数整数环. \mathcal{O}_K 是存在不可约分解的环. 其证明方法和 (2) 几乎一模一样. 具体细节参考代数数论的教材.

2.2.6 令 \mathbb{R}, \mathbb{C} 分别表示实数域和复数域, 试证明:

- (1) 若 R 是由关于 $\cos t$ 和 $\sin t$ 的实系数多项式组成的函数环, 则 $R \cong \mathbb{R}[x, y]/(x^2 + y^2 - 1)$;
- (2) $\mathbb{C}[x, y]/(x^2 + y^2 - 1)$ 是唯一分解整环 (提示: 证明其为 ED);
- (3) $\mathbb{R}[x, y]/(x^2 + y^2 - 1)$ 不是唯一分解整环.

proof

(1) 考虑同态

$$\varphi: \mathbb{R}[x, y] \rightarrow R = \mathbb{R}[\cos t, \sin t], \quad x \mapsto \cos t, y \mapsto \sin t,$$

这自然是一个满同态, 由同态基本定理, 关键在于证明

$$\ker(\varphi) = (x^2 + y^2 - 1)$$

若多项式 $f(x, y)$ 满足 $\varphi(f) = f(\cos t, \sin t) = 0$, 将 f 看成是关于 y 的多项式

$$f(x, y) = a_0(x) + a_1(x)y + \cdots + a_n(x)y^n, \quad a_i(x) \in \mathbb{R}[x], \quad 0 \leq i \leq n$$

由于 $x^2 + y^2 - 1$ 关于 y 是首一的, 因此可以做带余除法, 得 $f = gq + r$, 其中 $r(x, y) = r_0(x) + r_1(x)y$. 带入 $x = \cos t, y = \sin t$ 得 $r(\cos t, \sin t) = 0$, 即

$$r_0(\cos t) + r_1(\cos t) \sin t = 0$$

做代换 $t \mapsto -t$, 得

$$r_0(\cos t) - r_1(\cos t) \sin t = 0$$

两式相加得 $r_0 = 0$, 相减得 $r_1 = 0$, 从而 $r = 0$. 因此 $f \in (x^2 + y^2 - 1)$, 即 $\ker(\varphi) \subseteq (x^2 + y^2 - 1)$. 另一方面 $x^2 + y^2 - 1 \in \ker(\varphi)$, 故 $\ker(\varphi) = (x^2 + y^2 - 1)$.

- (2) 做基变换 $u = x + iy, v = x - iy$, 他有逆变换 $x = \frac{u+v}{2}, y = \frac{u-v}{2i}$. 因此有同构 $\mathbb{C}[u, v] \cong \mathbb{C}[x, y]$. 从而

$$\mathbb{C}[x, y]/(x^2 + y^2 - 1) \cong \mathbb{C}[u, v]/(uv - 1)$$

而同态

$$\mathbb{C}[u, v] \rightarrow \mathbb{C}[u, u^{-1}], u \mapsto u, v \mapsto u^{-1}$$

是满的, 且 kernel 是 $(uv - 1)$, 证明类似于 (1). 因此

$$\mathbb{C}[u, v]/(uv - 1) \cong \mathbb{C}[u, u^{-1}]$$

这个环称为 Laurent 多项式环, 这个环上可以做带余除法, 非零多项式的次数定义为最高次数 - 最低次数. 即 $f = a_n u^n + a_{n+1} u^{n+1} + \cdots + a_m u^m, n, m \in \mathbb{Z}, n < m$ 的次数为 $\deg(f) = m - n$. 因此这是一个 ED, 从而是 UFD.

- (3) 由 (2), $\mathbb{C}[\cos t, \sin t]$ 是 UFD, 用待定系数, 假设

$$\cos t = (a_1 \cos t + a_2 \sin t + a_3)(b_1 \cos t + b_2 \sin t + b_3)$$

其中 $a_i, b_i \in \mathbb{C}, i = 1, 2, 3$. 我们要忽略掉 $a_1 = b_3 = 1$ 其余都是 0 这种平凡的情况, 左右展开得到

$$a_1 b_1 - a_2 b_2 = 0,$$

$$a_1 b_2 + a_2 b_1 = 0,$$

$$a_1 b_1 + a_3 b_3 = 0,$$

$$a_1 b_3 + a_3 b_1 = 1,$$

$$a_2 b_3 + a_3 b_2 = 0.$$

由第一个式子得 $b_1 = \frac{a_2}{a_1} b_2$, 带入第二个式子得 $a_2 = \pm i a_1$, 从而 $b_1 = \pm i b_2$.

由一, 三又能得到 $a_2 b_2 = -a_3 b_3$, 类似地, 带入第五个式子, 有 $a_3 = \pm a_2, b_2 = \pm b_3$.

再用四, 五得 $a_1 b_3 = a_3 b_1 = \frac{1}{2}$.

把上述关系带入

$$\begin{aligned} \cos t &= a_1 b_3 (\cos t \pm i \sin t \pm i)(\pm i \cos t \pm \sin t + 1) \\ &= \frac{1}{2} (\cos t \pm i \sin t \pm i)(\pm i \cos t \pm \sin t + 1) \end{aligned}$$

检查正负号, 得到结果

$$\cos t = \frac{1}{2}(\cos t + i \sin t - i)(i \cos t + \sin t + 1)$$

类似有

$$1 - \sin t = \frac{1}{2}(\cos t + i \sin t - i)(\cos t - i \sin t + i).$$

带入 $-t$ 就是 $1 + \sin t$ 的分解.

但这种方法比较难检查等式右边的因式确实为不可约元, 我们可以利用同构 $\mathbb{C}[x, y]/(x^2 + y^2 - 1) \cong \mathbb{C}[u, u^{-1}]$, 那么等式变为

$$x = \frac{1}{2}(u + u^{-1}) = \frac{u^{-1}}{2}(u - i)(u + i)$$

注意到 $U(\mathbb{C}[u, u^{-1}]) = \mathbb{C} \cup \{u^n \mid n \in \mathbb{Z}\}$. 右边为两个都是一次的且常数项不为 0, 容易验证不可逆 (注意这里 $x = \frac{1}{2}(u + u^{-1})$ 次数为 2). 对 $1 - \sin t$ 同理.

因此 $\cos t$ 和 $1 \pm \sin t$ 无法在 $\mathbb{R}[\cos t, \sin t]$ 中分解 (分解出的系数中一定带 i). 这样就有 $\cos^2 t = \cos t \cos t = (1 - \sin t)(1 + \sin t)$. 因此不是 UFD.

□

注:

(2) 中若允许正次数到无穷的话, 则该环称为 Laurent 形式级数域 (可以验证确实是一个域).

另外, 可以说 $x^2 + y^2 - 1$ 是单位圆的“极小多项式”. 但这种说法是有些不合理的, 因为这样 $a_{ij}x^i y^j$ 次数将定义成 $i + j$, $f(x, y)$ 的次数定义成单项次数的最大值, 一旦这么定义就无法做带余除法, 就无法得到满足某个点集 (一般是代数集, 即某些多项式的共同零点) 的多项式是其极小多项式的倍数.

一般地设 k 是一个域, $S \subseteq k[x_1, x_2, \dots, x_n]$, 那么可以定义 S 中所有多项式的公共零点集

$$Z(S) = \{(a_1, a_2, \dots, a_n) \in k^n \mid \forall f \in S, f(a_1, a_2, \dots, a_n) = 0\}$$

按定义有 $S \subseteq S' \implies Z(S') \subseteq Z(S)$. 考虑 S 生成的理想 $I = (S)$ (见 2.1.6 的注记), 则有 $Z(I) \subseteq Z(S)$. 另一方面, 根据 $I = \left\{ \sum f_i g_i \mid f_i \in k[x_1, x_2, \dots, x_n], g_i \in S \right\}$, 立刻得到 $Z(S) \subseteq Z(I)$. 从而 $Z(S) = Z(I)$. 我们称 $Z(S)$ 这种点集为代数集 (algebraic set), 用 \mathbb{A}_k^n 代替的 k^n 表示将它看作一个代数集 (因为按定义 $Z(\emptyset) = k^n$), 而 Hilbert's Basis Theorem 告诉我们 $k[x_1, x_2, \dots, x_n]$ 是 Noether 环, 所以理想都是有限生成的, 那么总有 $Z(I) = Z(f_1, f_2, \dots, f_r)$.

反过来, 对 $X \subseteq \mathbb{A}_k^n$, 定义

$$\mathcal{I}(X) = \{f \in k[x_1, x_2, \dots, x_n] \mid \forall (a_1, a_2, \dots, a_n) \in X, f(a_1, a_2, \dots, a_n) = 0\}$$

可以验证 $\mathcal{I}(X)$ 是根理想 (2.1.1 的注记). 当 k 是代数闭域 (algebraic closed field) 时, 有一一对应

$$\{\mathbb{A}_k^n \text{ 的代数集}\} \xrightleftharpoons[Z]{\mathcal{I}} \{k[x_1, x_2, \dots, x_n] \text{ 的根理想}\}$$

这就是 Strong Nullstellensatz.

那么 (1) 中 $I = (x^2 + y^2 - 1)$, $Z(I) = \{(x, y) \in \mathbb{R}^2 \mid \forall f \in I, f(x, y) = 0\} = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$, 恰好是单位圆. 那么 (1) 的关键在于说明 $\mathcal{I}(Z(I)) = I$. 可惜的是一般情况下这个并不成立, 比如还是在 $\mathbb{R}[x, y]$ 上考虑, 记 $J = (x^2 + y^2)$, 那么 $Z(J) = (0, 0)$, $\mathcal{I}(Z(J)) = (x, y) \neq J$. 这里 $x^2 + y^2$ 是不可约的, 所以即使是单独一个不可约多项式也不一定可以有这个等式, $x^2 + y^2 - 1$ 这个不可约多项式还是比较特殊的.

域扩张中的极小多项式和不可约是一样的, 这是由于 $K[x]$ 是一个 PID, 不可约元对应极大理想, 从而对应极小多项式.

习题 2.3 教材 p41-p42

2.3.1 设 F 是一个域, $F[[x]]$ 是系数在 F 中的形式幂级数环, 试证明:

- (1) $f(x) = a_0 + a_1x + a_2x^2 + \dots$ 在 $F[[x]]$ 中可逆 $\Leftrightarrow a_0 \neq 0$;
- (2) $F[[x]]$ 中任意不可约元 $p(x)$ 均与 x 相伴, 即 $p(x) \sim x$;
- (3) $F[[x]]$ 是主理想整环, 它是欧氏整环吗? 如果是, 请写出一个欧氏映射.

proof

(1) 按定义, 存在 $g = \sum_{k=0}^{\infty} b_k x^k$ 使得 $fg = 1$. 则

$$a_0 b_0 = 1,$$

$$a_1 b_0 + a_0 b_1 = 0,$$

$$a_2 b_0 + a_1 b_1 + a_0 b_2 = 0,$$

$$\vdots$$

因此 $a_0 \neq 0$.

反过来, 若 $a_0 \neq 0$, 由 F 是域, a_0 可逆. 即存在 $b_0 \in F$, $a_0 b_0 = 1$. 我们可

以通过上面的无穷个方程组递归的解出 $b_k (k \geq 1)$.

$$\begin{aligned} b_1 &= -a_1 b_0^2, \\ b_2 &= -a_2 b_0^2 - a_1 b_1 b_0, \\ &\vdots \\ b_k &= -\sum_{i=1}^k a_i b_{k-i} b_0, \\ &\vdots \end{aligned}$$

从而存在 $g = \sum_{k=0}^{\infty} b_k x^k$ 为 f 的逆.

- (2) 设 $p(x) = \sum_{k=0}^{\infty} a_k x^k$. p 不可约则不是可逆元, 由 (1), $a_0 = 0$, 因此 $p(x) = x p_1(x)$. 又因为不可约, 且 x 不是可逆元, 因此 p_1 是可逆元, 故 $p(x) \sim x$.
- (3) 由 (2), $\forall f(x) \in F[[x]]$, 则有唯一分解 $f(x) = x^n g(x)$, 其中 $g(x)$ 是可逆的, 即 g 的常数项非零, 也就是 $a_n \neq 0$. 那么 $n = \min\{i \in \mathbb{N} \mid a_i \neq 0\}$. 令 $\delta(f) = n$, 这就是一个欧氏映射. 带余除法是比较显然的, 设 $f_1 = x^n g_1, f_2 = x^m g_2$, 不妨设 $n > m$, 由于 g_2 可逆, $f_1 = x^n g_2 (g_2^{-1} g_1) = f_2 (x^{n-m} g_2^{-1} g_1)$. 因此得到的结论更强, 只要 $n > m$, 就有 $f_2 \mid f_1$.

□

注:

由 (1)(2) 知, $f(x) \in F[[x]]$, 要么是单位, 否则一定在理想 (x) 中. 这说明 (x) 是 $F[[x]]$ 唯一的极大理想, 这种环称为局部环 (local ring).

请参考 [AM94]p4.

2.3.2 设 F 是一个域, $p(x) \in F[x]$ 不可约, 令 $I = p(x)F[x]$ 表示由 $p(x)$ 生成的理想, 试证明: 商环 $F[x]/I$ 是一个域, 且环同态

$$\varphi: F[x] \rightarrow F[x]/I, \quad f(x) \mapsto \overline{f(x)}$$

诱导了域嵌入 $\varphi|_F: F \hookrightarrow F[x]/I, a \mapsto \bar{a}$ (如果将 F 与它的像等同, 则 $\bar{x} \in F[x] := F[x]/I$ 是 $p(x)$ 在扩域 $F[x]$ 中的一个根).

proof

2.2.6 注记的最后已经提到过, 这里再详细解释一下. 由于 F 是域, 因此 $F[x]$ 是 PID, 因此若 $p(x)$ 是不可约的, 则 $I = p(x)F[x]$ 是极大理想. 因为不可约

元按定义在所有主理想中是极大的, 这一点可以参考2.2.2的注记, 设 p 是不可约元就能得到

$$(p) \subseteq (p') \implies p' \mid p \implies p' \sim p \text{ 或 } p' \sim 1 \implies (p') = (p) \text{ 或 } (p') = (1)$$

. 因此由2.1.6知 $F[x]/I$ 是域.

所谓的域嵌入 (embedding) 在这里实际上就是单同态, 这其实就是同态复合了一下

$$F \hookrightarrow F[x] \twoheadrightarrow F[x]/I$$

这是域之间的同态, 因此一定是单的. □

2.3.3 设 F 是一个域, $K \subset F$ 是一个子域, $f(x), g(x) \in K[x]$. 试证明: $f(x), g(x)$ 在 $K[x]$ 中互素 $\Leftrightarrow f(x), g(x)$ 在 $F[x]$ 中互素.

proof

利用 PID 上满足 Bézout Identity 立得. □

2.3.4 设 F 是特征零的域, $f(x) \in F[x]$ 不可约. 证明 $f(x)$ 与 $f'(x)$ 互素.

proof

由于 $0 \leq \deg(f') < \deg(f)$ 且 f 不可约, 若有非单位的公因式 $d(x)$, 则 $\deg(f) > \deg(f') \geq \deg(d) > 0$ 且 $d(x) \mid f(x)$ 与不可约矛盾.

特征零是为了排除 $f' = 0$ 的情况. □

2.3.5 设 $\mathbb{F}_2 = \mathbb{Z}/(2) = \{\bar{0}, \bar{1}\}$ 是一个二元域. 证明:

$$f(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \in \mathbb{F}_2[x]$$

没有一次因子 (即不被一次多项式整除) $\Leftrightarrow a_n \left(1 + \sum_{i=1}^n a_i\right) \neq 0$. 写出 $\mathbb{F}_2[x]$ 中所有次数不超过 3 的所有不可约多项式.

proof

\mathbb{F}_2 只有两个一次多项式 x 和 $x+1$. 其中比较简单的是

$$x \mid f(x) \iff a_0 = 0,$$

另一个

$$x+1 \mid f(x) \iff f(x) = (x+1)g(x)$$

设 $g(x) = x^{n-1} + \cdots + b_{n-1}$, 对比系数

$$a_n = b_{n-1}, a_{n-1} = b_{n-1} + b_{n-2}, \cdots, a_1 = b_1 + 1$$

由于 \mathbb{F}_2 里 $-1 = 1$, 因此可以得到

$$b_1 = a_1 - 1 = a_1 + 1, b_2 = a_2 - b_1 = a_2 + a_1 + 1, \dots, a_n = b^{n-1} = 1 + \sum_{k=0}^{n-1} a_k$$

因此

$$x + 1 \mid f(x) \iff 1 + \sum_{k=1}^n a_k = 2a_n = 0.$$

不过也可以不这么麻烦, 一次多项式对应 $f(x)$ 的根, 所以 $f(x)$ 无一次因子等价于 $f(0) \neq 0$ 且 $f(1) \neq 0$, 即 $a_0 \neq 0$ 和 $1 + \sum_{k=1}^n a_k \neq 0$.

次数不超过 3 的多项式只有有限个, 可以列举出来, 去掉比较明显的可约多项式

$$\begin{aligned} & x, x + 1, \\ & x^2 + 1, x^2 + x + 1 \\ & x^3 + 1, x^3 + x + 1, x^3 + x^2 + 1 \end{aligned}$$

注意 $x^2 + 1 = x^2 - 1 = (x - 1)(x + 1) = (x + 1)^2$ 可约, $x^3 + 1$ 同理, 其余五个为不可约多项式. \square

2.3.6 设 p 是素数, $\mathbb{Z} \rightarrow \mathbb{F}_p = \mathbb{Z}/(p)\mathbb{Z}$, $a \mapsto \bar{a}$, 是商同态. 证明:

(1) 映射

$$\phi_p : \mathbb{Z}[x] \rightarrow \mathbb{F}_p[x], \quad f(x) = \sum_{i=1}^n a_i x^i \mapsto \bar{f}(x) = \sum_{i=1}^n \bar{a}_i x^i$$

是环同态;

(2) 对于首项系数为 1 的多项式 $f(x) \in \mathbb{Z}[x]$, 如果存在素数 p 使 $\bar{f}(x)$ 在 $\mathbb{F}_p[x]$ 中不可约, 则 $f(x)$ 在 $\mathbb{Z}[x]$ 中也不可约.

proof

(1) 2.1.8 的注记或教材引理 2.3.2 (我才发现教材有写延拓)

(2) 用反证法, 假设 $f(x)$ 可约, $f(x) = g(x)h(x)$, 则 $\deg(g), \deg(h) > 0$ 且 g, h 都是首一的. 那么根据同态有 $\bar{f} = \bar{g}\bar{h}$, 且 \bar{g} 和 \bar{h} 还是首一的次数大于 0 的多项式, 这和 \bar{f} 不可约矛盾. \square

2.3.7 设 R, A 是两个环, $C(A) \subset A$ 是 A 的中心, $\psi : R \rightarrow C(A)$ 是一个环同态. 证明: $\forall u \in A$, 存在唯一环同态 $\psi_u : R[x] \rightarrow A$ 满足:

$$\psi_u(x) = u, \quad \psi_u(a) = \psi(a) \quad (\forall a \in R).$$

所以, $\forall f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in R[x]$, 它在 ψ_u 下的像

$$\psi_u(f(x)) = \psi(a_n)u^n + \psi(a_{n-1})u^{n-1} + \cdots + \psi(a_1)u + \psi(a_0) \in A$$

称为 $f(x)$ 在 $u \in A$ 的取值, 记为 $f(u) := \psi_u(f(x))$.

proof

2.1.8的注记. 在这里重新阐述的详细一点. 给定环同态 $\psi: R \rightarrow C(A)$, 我们可以指定一个集合的映射

$$f_u: \{1\} \rightarrow A, 1 \mapsto u$$

所谓的自由交换 R -代数的泛性质是指, 对任意给定的集合映射 f_u , 存在唯一的同态 $\psi_u: R[x] \rightarrow A$ 使得图表交换:

$$\begin{array}{ccc} R[x] & \xrightarrow{\exists! \psi_u} & A \\ & \swarrow i \quad \searrow f_u & \\ & \{1\} & \end{array}$$

其中 $i: R \rightarrow R[x], 1 \mapsto x$.

因为 $\psi(R) \subseteq C(A)$, 因此 ψ_u 才能保持乘法, 这在2.1.8的注记里已经证明. 验证了 ψ_u 是环同态就相当于证明了存在性, 而唯一性是根据定义就能得到, ψ_u 是被给定的 ψ 和 f_u 唯一确定的. \square

注:

这里 $\{1\}$ 可以换成任意集合 S

$$\begin{array}{ccc} R[S] & \xrightarrow{\exists! \psi_u} & A \\ & \swarrow i \quad \searrow f_u & \\ & S & \end{array}$$

$u = (u_s)_{s \in S} \in A^S, f_u(s) = u_s$. (2.4.5为 S 是有限集的情形)

2.3.8 设 R 是一个交换环, $f(x) \in R[x]$. 证明: $f(x)$ 是环 $R[x]$ 中的零因子当且仅当存在 $0 \neq r \in R$ 使得 $r \cdot f(x) = 0$.

proof

由于 $R \subseteq R[x]$, 只需证“ \implies ”的方向.

记 $f(x) = \sum_{k=0}^n a_k x^k$, 设存在 $g(x) = \sum_{k=0}^m b_k x^k \neq 0$ 使得 $fg = 0$, 并要求 $g(x)$ 是次数最低的. 考虑最高次项, $a_n b_m = 0$. 那么 $a_n g(x)$ 是一个比 $g(x)$ 次数更小的多项式且 $f(x)(a_n g(x)) = a_n f(x)g(x) = 0$. 因此 $a_n g(x) = 0$, 从而 $a_n b_k = 0, 0 \leq k \leq m$. 那么此时 $n+m-1$ 项的系数变为 $a_{n-1} b_m = 0$, 于是可

以重复讨论. 根据归纳法最后得到 $a_i b_m = 0, \forall i$ 且 $b_m \neq 0$, 因此 $b_m f(x) = 0$. \square

2.3.9 证明多项式 $f(x) = x^4 - 10x^2 + 1$ 在 $\mathbb{Z}[x]$ 中不可约, 但是对任意的素数 p , 它在 $\mathbb{F}_p[x]$ 中总是可约的.

proof

注意到 $f(x)$ 是关于 x^2 的二次方程且有正实根 $x_{1,2} = 5 \pm 2\sqrt{6}$, 而且恰好有 $5 \pm 2\sqrt{6} = (\sqrt{2} \pm \sqrt{3})^2$, 记 $\alpha_1 = \sqrt{2} + \sqrt{3}, \alpha_2 = \sqrt{2} - \sqrt{3}$,

$$x^4 - 10x^2 + 1 = (x + \alpha_1)(x - \alpha_1)(x + \alpha_2)(x - \alpha_2)$$

这是一个 $\mathbb{R}[x]$ 上的唯一分解. 因此可以得到 $f(x)$ 在 \mathbb{Z} 上不可分, 因为无论怎组合都得不到整系数的因式.

在 $\mathbb{F}_p[x]$ 上, 根据二次剩余的结论 (见注记), 可以知道 $Q_p = \{a^2 \mid a \in \mathbb{F}_p^*\}$ (即所有的非零二次剩余) 是一个子群. 且当 $p > 2$ 时, $[\mathbb{F}_p^* : Q_p] = 2$. 那么对 \mathbb{F}_p^* 中任意两个元素 a, b , a, b, ab 中必有一个为二次剩余.

现在将之前的因式分解做组合, 得到三种分解

$$\begin{aligned} f(x) &= (x^2 - 5 - 2\sqrt{6})(x^2 - 5 + 2\sqrt{6}) \\ &= ((x - \sqrt{2})^2 - 3)((x + \sqrt{2})^2 - 3) \\ &= ((x - \sqrt{3})^2 - 2)((x + \sqrt{2})^2 - 2) \end{aligned}$$

因此 $p > 3$, 取 $a = 2, b = 3$, 则上面必有一种是 $\mathbb{F}_p[x]$ 中的分解, 而 $p = 2, 3$ 时 $6 = 0$, 取第一种就行. \square

注:

若 $a \in \mathbb{F}_p$ 使得同余方程

$$x^2 \equiv a \pmod{p}$$

有解, 则称 a 为一个二次剩余, 其中 0 是平凡的情形. 该方程自然有两个根 x 和 $-x$. 当 $p > 2$ 时 p 为奇数, 因此 $x \neq -x$. 此时考虑平方映射

$$f: \mathbb{F}_p^* \rightarrow \mathbb{F}_p^*, \quad x \mapsto x^2$$

由于乘法交换, 这是一个群同态, $f(\mathbb{F}_p^*) = Q_p < \mathbb{F}_p^*$. 我们考虑映射自带的一个等价关系

$$x \sim y \iff f(x) = f(y)$$

等价类即为 $[x] = f^{-1}(f(x)) = \{x, -x\}$. 那么就有 $[\mathbb{F}_p^* : Q_p] = 2$.

2.3.10 设 $f(x) \in \mathbb{R}(x)$ 是一个有理函数. 如果对任意整数 $m \in \mathbb{Z}$ 必有

$f(m) \in \mathbb{Z}$, 试证明 $f(x)$ 必为多项式. 这样的 $f(x)$ 是否必为有理系数多项式? 请证明你的结论.

proof

根据有理函数的定义, 设 $f(x) = \frac{p(x)}{q(x)}$, $p, q \in \mathbb{R}[x]$, $q \neq 0$, $(p, q) = 1$. 若 $p = 0$ 结论平凡, 因此只考虑 $p \neq 0$ 的情况.

这题可以用一些分析的想法.

注:

$q(x)$ 有整数根的时候, 会存在某个整数使得 $f(m)$ 无定义, 因此本题题目条件默认 $q(m) \neq 0, \forall m \in \mathbb{Z}$.

我们利用一个简单的结论:

$$\lim_{m \rightarrow \infty} f(m) = \lim_{m \rightarrow \infty} \frac{p(m)}{q(m)} = \begin{cases} 0 & \deg(p) < \deg(q), \\ \infty & \deg(p) > \deg(q), \\ \frac{a_n}{b_n} & \deg(p) = \deg(q) = n. \end{cases}$$

这里 a_n 和 b_n 分别是 $p(x)$ 和 $q(x)$ 的首项系数.

注意 $p(x)$ 最多只有 $\deg(p)$ 个根, 因此最多只有 $\deg(p)$ 个整数使得 $f(m) = 0$. 那么利用 $\deg(p) < \deg(q)$ 时的结果, 存在 $N \in \mathbb{Z}_{>0}$ 使得任意 $m > N$ 有 $0 < |f(m)| < 1$, 和条件矛盾.

$\deg(p) = \deg(q)$ 时, 若 $\frac{a_n}{b_n} \notin \mathbb{Z}$, 利用极限的定义可以得到类似的矛盾 (即 m 足够大时把 $|f(m)|$ 限制在一个无整数的区间内). 而若 $\frac{a_n}{b_n} \in \mathbb{Z}$, 则可以得到 m 足够大时都有 $f(m) = \frac{a_n}{b_n} = k \in \mathbb{Z}$, 即

$$f(m) = \frac{a_n m^n + \cdots + a_0}{b_n m^n + \cdots + b_0} = \frac{a_n}{b_n}$$

则可得 $a_n b_i = a_i b_n, i = 0, 1, \cdots, n-1$, 即 $\frac{a_i}{b_i} = \frac{a_n}{b_n} = k$. 因此 $f(x) = \frac{a_n}{b_n}$ 是常整数多项式.

当 $\deg(p) > \deg(q)$ 时只需证明 $q(x) \mid p(x)$, 此时需要一些技巧. 先用带余除法令 $p(x) = q(x)s(x) + r(x)$, $\deg(r) < \deg(q)$, 那么 $f(x) = s(x) + \frac{r(x)}{q(x)}$, 需要证明 $r = 0$.

注:

注意此时并不能用之前的结论, $s(m)$ 是否为整数并不知道.

基本的想法是保持整数的情况下去降次, 利用差分就可以做到这一点. 考虑

$$\Delta_1 f(x) = f(x+1) - f(x)$$

若记 $\deg(f) = \deg(p) - \deg(q)$, 则有 $\deg(\Delta_1 f) < \deg(f)$ ($s(x)$ 会消去最高次项, $\frac{r(x)}{q(x)}$ 的部分指数不会增加), 且对任意整数 m 也有 $\Delta_1 f(m) \in \mathbb{Z}$. 记 $k = \deg(f)$, 则 $\Delta_1^k f$ (k 阶差分) 化归为第二种情况. 而由 $\Delta_1^{k-1} f(x+1) - \Delta_1^{k-1} f(x) = \Delta_1^k f(x)$ 可知, 若 $\Delta_1^k f(x)$ 是多项式, 则 $\Delta_1^{k-1} f(x)$ 也是多项式 (分式项做差分无法消去), 从而反推得 $f(x)$ 是多项式.

因此 $f(x) \in \mathbb{R}[x]$, 记 $f(x) = c_n x^n + \cdots + c_0$, 任意选择 $n+1$ 个不同整数 m_0, m_1, \dots, m_n 带入得到一个关于 a_0, a_1, \dots, a_n 的整系数线性方程组 $\sum_{k=0}^n m_i^k a_k = b_i, i = 0, 1, \dots, n$, 系数矩阵的行列式恰为 Vandenmonde 行列式, 因此不为零, 方程组有唯一有理数解. \square

习题 2.4 教材 p48-p49

2.4.1 设 F 是一个域, $R = F[x_1, x_2, \dots, x_n]$, 令 $R_m \subset R$ 表示所有 m 次齐次多项式的集合 (并上零多项式). 证明: R_m 是域 F 上的 $\binom{m+n-1}{m}$ 维向量空间.

proof

设 $f \in R_m$, 根据 R_m 的定义, f 可以写成

$$f = \sum_{i_1+i_2+\dots+i_n=m} a_{i_1 i_2 \dots i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$$

$a_{i_1 i_2 \dots i_n} \in F$ 允许为 0, $i_k \geq 0, 1 \leq k \leq n$. 那么 f 的表达式中共有 $\binom{m+n-1}{m}$ 项. 记 $N = \binom{m+n-1}{m}$, $I = \{(i_1, i_2, \dots, i_n) \in \mathbb{N}^n \mid i_1 + i_2 + \dots + i_n = m\}$. 因此映射

$$R_m \rightarrow F^N, \quad f \mapsto (a_{i_1 i_2 \dots i_n})_{(i_1, i_2, \dots, i_n) \in I}$$

是 (线性) 同构. \square

2.4.2 证明: $f(x_1, x_2, \dots, x_n) \in F[x_1, x_2, \dots, x_n]$ 是 m 次齐次多项式当且仅当 $f(tx_1, tx_2, \dots, tx_n) = t^m f(x_1, x_2, \dots, x_n)$, (t 是一个新的不定元).

proof

” \implies ” 这个方向提出公因式 t^m 即可, 下证 ” \Leftarrow ”:

由于 f 可以唯一表示成齐次多项式的和, 即

$$f = f_0 + f_1 + \cdots + f_k$$

其中 k 是 f 的最高次数. 那么有

$$f(tx_1, tx_2, \dots, tx_n) = f_0(x_1, \dots, x_n) + tf_1(x_1, \dots, x_n) + \dots + t^k f_k(x_1, \dots, x_n)$$

这是一个 $F[x_1, x_2, \dots, x_n]$ 上的关于 t 的多项式. 若有 $f(tx_1, tx_2, \dots, tx_n) = t^m f(x_1, x_2, \dots, x_n)$, 对比系数知 $f = f_m$. \square

2.4.3 设 F 是一个域, $K \supseteq F$ 是 F 的一个扩域, 试证明: $a \in K$ 是多项式 $f(x) \in F[x]$ 的重根 $\Leftrightarrow f(a) = 0, f'(a) = 0$.

proof

” \Rightarrow ”的部分按定义直接验证, 下证” \Leftarrow ”:

由 $f(a) = 0$, 可以得到 $f(x) = (x-a)f_1(x)$. 那么 $f'(x) = f_1(x) + (x-a)f_1'(x)$.

由 $f'(a) = f_1(a) = 0$, 得到 $f_1(x) = (x-a)f_2(x)$. 因此 $f(x) = (x-a)^2 f_2(x)$, 即 a 是重根. \square

2.4.4 设 F 是一个无限域, $f(x_1, x_2, \dots, x_n) \in F[x_1, x_2, \dots, x_n]$ 是一非零多项式. 试证明: 存在 $a_1, a_2, \dots, a_n \in F$, 使 $f(a_1, a_2, \dots, a_n) \neq 0$.

proof

对 n 归纳.

$n=1$ 时, $f(x_1)$ 至多有 $\deg(f)$ 个根, 由 F 无限, 存在 $a_1 \in F$ 使得 $f(a_1) \neq 0$.

现假设结论对 n 成立, 考虑多项式

$$f(x_1, \dots, x_n, x_{n+1}) \in F[x_1, \dots, x_n, x_{n+1}] = F[x_1, \dots, x_n][x_{n+1}].$$

从而

$$f(x_1, \dots, x_n, x_{n+1}) = c_m(x_1, \dots, x_n)x_{n+1}^m + \dots + c_0(x_1, \dots, x_n)$$

其中 $c_m(x_1, \dots, x_n) \neq 0$. 由归纳假设存在 $(a_1, \dots, a_n) \in F^n$ 使得 $c_m(a_1, \dots, a_n) \neq 0$, 那么对多项式 $g(x_{n+1}) = f(a_1, \dots, a_n, x_{n+1}) \in F[x_{n+1}]$ 使用 $n=1$ 的结论即可. \square

2.4.5 设 $\psi: R \rightarrow A$ 是环同态, $u = (u_1, u_2, \dots, u_n) \in A^n$ 满足:

$$u_i u_j = u_j u_i, \quad u_i \psi(a) = \psi(a) u_i \quad (\forall a \in R, 1 \leq i, j \leq n).$$

请直接验证取值映射 $\psi_u: R[x_1, x_2, \dots, x_n] \rightarrow A$,

$$f = \sum_{i_1 i_2 \dots i_n} a_{i_1 i_2 \dots i_n} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n} \mapsto \psi_u(f) := \sum_{i_1 i_2 \dots i_n} \psi(a_{i_1 i_2 \dots i_n}) u_1^{i_1} u_2^{i_2} \dots u_n^{i_n},$$

是一个环同态.

proof

参考2.3.7, 实际上这题是把条件减到了最弱的情况, 取定的 n 个 A 中的 u_1, u_2, \dots, u_n , 只需要它们互相之间是交换的且和所有 $\psi(a)$ 也是交换的 (也就是说 $\forall i, u_i \in C(\psi(R))$, 中心化子, 见1.2.4), 那么映射

$$\psi_u : R[x_1, \dots, x_n] \rightarrow A, \quad x_i \mapsto u_i, \quad \psi_u|_R = \psi$$

就是环同态. 交换的条件是用于保持乘法上, 保 1 是平凡的, 保加法只需要分配律. 但要注意, 此时不能说 A 是 R -代数, 因为按定义是要求任意给定 u_1, \dots, u_n , ψ_u 都是同态, 才能说 A 是一个 R -代数. \square

2.4.6 设 K 是一个域, $A = \{(a_{ij})_{n \times n} | a_{ij} \in K[\lambda]\}$ 是 n 阶 λ -矩阵环, $u = \lambda \cdot I_n \in A$ 表示对角线上全为 λ 的矩阵. 试证明: 如果 $R = M_n(K)$, $\psi : R \rightarrow R$ 是恒等映射, 则取值映射 $\psi_u : R[x] \rightarrow A$ 是一个环同构.

proof

按定义 $A = M_n(K[\lambda])$, 由于 $K \subseteq K[\lambda]$, 所以自然有 $R = M_n(K) \subseteq M_n(K[\lambda]) = A$. 但事实上 $A = R[\lambda]$, 在1.2.8可以看到这一点. 但是对一个矩阵 $B \in M_n(K)$, $B\lambda$ 和 $B(\lambda \cdot I_n)$ 是一样的. 因此 $A = R[\lambda \cdot I_n] = R[u]$. u 和 λ, x 一样是和 R 无关的变量, 所以只是换了个字母而已, 那么 ψ_u 自然是同构. \square

2.4.7 设 R 是一个无零因子的非交换环, $\psi : R \rightarrow R$ 是恒等映射. 证明存在 $u \in R$ 使得 $\psi_u : R[x] \rightarrow R$, $f(x) \mapsto f(u)$, 不是一个映射.

proof

由非交换性知存在 $u, v \in R$ 使得 $uv \neq vu$. 而 $R[x]$ 关于 x 是交换的, 所以可以取 $f(x) = vx = xv$. 那么带入 u , 有 uv 和 vu 两个值, 因此 ψ_u 在 $f(x)$ 处不是良定义的, ψ_u 不是一个映射. \square

2.4.8 设 K 是一个域, $M_m(K)$ 是 m -阶矩阵环, $\psi : K \rightarrow M_m(K)$ 定义为 $\psi(a) = a \cdot I_m$ (对角线元素为 a 的数量矩阵). 令

$$u = (A, B) \in M_m(K) \times M_m(K), \quad AB \neq BA,$$

试证明 $\psi_u : K[x_1, x_2] \rightarrow M_m(K)$, $f(x_1, x_2) \mapsto f(A, B)$, 不是一个映射.

proof

和上题是类似的, 用于赋值的 A 和 B 是非交换的, 但 x_1 和 x_2 是交换的. 所以取 $f(x_1, x_2) = x_1x_2 = x_2x_1$ 即可. \square

注:

现在把涉及到多项式环的题目放在一起看, 2.3.7, 2.4.5, 2.4.6, 2.4.7, 2.4.8.

我们希望“多项式”可以满足我们一直以来的直觉, 其中最重要的一条应该是可以赋值, 也就是说我们希望一个多项式同时也是一个多项式函数. “赋值”这个操作在2.3.7解释为由环同态 $\psi: R \rightarrow A$ 诱导的唯一的同态 $\psi_u: R[x] \rightarrow A$, ψ_u 的含义就是代入 u , 也就是说此时多项式 $f(x)$ 确实是一个函数

$$f: R \rightarrow A, \quad u \mapsto f(u) = \psi_u(f(x)).$$

可以看到交换环的条件在多项式里是很重要的, 没有交换环, 多项式就不一定是函数了, 2.4.7和2.4.8分别为一元和多元的反例.

$R[x_1, x_2, \dots, x_n]$ 要求所有未定元 x_1, x_2, \dots, x_n 是两两交换, 以及所有 x_i 要和 R 中所有元素交换. 可以看到 R 是交换环等价于 $R[x]$ 是交换环, 自然也等价于 $R[x_1, x_2, \dots, x_n]$ 是交换环. R 是交换环的时候, $R[x_1, x_2, \dots, x_n]$ 的结构已经很清楚了, 就是自由交换 R -代数, 它满足和其他自由对象类似的泛性质, 正是这个泛性质保证了赋值的唯一性, 从而多项式函数才是一个良定义的东西.

2.4.5虽然减弱了条件, 但也失去了一般性, 所以 R 非交换的时候, 就没有那么好的泛性质了. 这也是为什么在定义 R -代数的时候需要要求 R 是一个交换环.

而2.4.6其实有更深刻的含义. 泛性质有很多, 某个特定对象的泛性质都是“对任意的一些态射, 存在唯一的态射使得图表交换”这种形式. 这其实是和 Yoneda Lemma, representable functor, limit 等有关系. 这种对象其实是某个新的范畴里的 final object(或者 initial object, 这俩是对偶的, 就差一个反范畴). 而 final object 的定义里就是该范畴里一个特殊的对象: 任意对象到 final object 存在唯一的态射. 正是这个存在唯一, 保证了 final object 在同构的意义下是唯一的. 所以当有两个东西满足同一个泛性质, 它们俩一定是同构的.

第3章 域扩张

习题 3.1 教材 p52-54

3.1.1 设 K 是特征零的域, $f(x) \in K[x]$ 是次数大于零的首项系数为 1 的多项式, $d(x) = (f(x), f'(x))$ 是 $f(x)$ 与 $f'(x)$ 的最大公因子. 令

$$f(x) = d(x) \cdot g(x).$$

证明: $g(x)$ 与 $f(x)$ 有相同的根且 $g(x)$ 没有重根.

proof

□

3.1.2 设 $K \subset L$ 是域扩张, $\alpha \in L$ 是域 K 上的代数元. 令 $K[x] \xrightarrow{\psi_\alpha} L$, $f(x) \mapsto f(\alpha)$, 表示多项式在 $x = \alpha$ 的取值映射. 试证明:

- (1) $\ker(\psi_\alpha)$ 由极小多项式 $\mu_\alpha(x)$ 生成;
- (2) ψ_α 诱导了域同构 $\mathbb{K}[x]/(\mu_\alpha(x)) \cong K[\alpha]$.

proof

□

3.1.3 设 $E = \mathbb{Q}[u]$, $u^3 - u^2 + u + 2 = 0$. 试将 $(u^2 + u + 1)(u^2 - u)$ 和 $(u - 1)^{-1}$ 表示成 $au^2 + bu + c$ ($a, b, c \in \mathbb{Q}$) 的形式.

proof

□

3.1.4 求 $[\mathbb{Q}[\sqrt{2}, \sqrt{3}] : \mathbb{Q}]$ (提示: 证明 $[\mathbb{Q}[\sqrt{2}, \sqrt{3}] : \mathbb{Q}[\sqrt{3}]] = 2$).

proof

□

3.1.5 设 p 是一个素数, $z \in \mathbb{C}$ 满足 $z^p = 1$ 且 $z \neq 1$, 试证明 $[\mathbb{Q}[z] : \mathbb{Q}] = p - 1$.

proof

□

3.1.6 证明:

- (1) $U_n = \{z \in \mathbb{C} \mid z^n = 1\}$ 是一个循环群;
- (2) $z = \cos \frac{\pi}{6} + i \sin \frac{\pi}{6}$ 是 U_{12} 的一个生成元, 但 $[\mathbb{Q}[z] : \mathbb{Q}] = 4$;
- (3) 求 $z = \cos \frac{\pi}{6} + i \sin \frac{\pi}{6}$ 在 \mathbb{Q} 上的极小多项式.

proof

□

3.1.7 设 $E = K[u]$ 是一个代数扩张, 且 u 的极小多项式的次数是奇数. 证明: $E = K[u^2]$.

proof

□

3.1.8 设 E_1, E_2 是域扩张 $K \subset L$ 的中间域 (即: $K \subset E_i \subset L$), 且 $[E_i : K] < +\infty$. 令 $E = K[E_1, E_2] \subset L$ 是由 E_1, E_2 生成的子域. 证明:

$$[E : K] \leq [E_1 : K] \cdot [E_2 : K].$$

proof

□

3.1.9 设 $K \subset L$ 是代数扩张, $E \subset L$ 是中间子环 (即: $K \subset E \subset L$). 证明: $E \subset L$ 必为子域 (所以任何有限扩张 $K \subset L$ 的中间子环必为域).

proof

□

3.1.10 设 $L = K(u)$, u 是 K 上的超越元, $E \neq K$ 是 $K \subset L$ 的中间域. 证明: u 是 E 上的代数元.

proof

□

3.1.11 设 p 是素数, $K \subset L$ 是 p 次扩张. 证明: $K \subset L$ 必为单纯扩张 (即: 存在 $u \in L$, 使 $L = K[u]$).

proof

□

3.1.12 设域扩张 $K \subset L$ 满足条件:

- (1) $[L : K] < +\infty$;
 - (2) 对任意两个中间域 $K \subset E_1 \subset L$, $K \subset E_2 \subset L$, 必有 $E_1 \subset E_2$ 或者 $E_2 \subset E_1$.
- 证明: $K \subset L$ 必为单纯扩张 (即: 存在 $u \in L$, 使 $L = K[u]$).

proof

□

3.1.13 设 $\alpha = 2 + \sqrt[3]{2} + \sqrt[3]{4}$, 给出一个首项系数为 1 的最低次数的多项式 $f(x) \in \mathbb{Q}[x]$ 使 $f(\alpha) = 0$.

proof

□

3.1.14 设 $K = \mathbb{Q}[\sqrt[3]{3}]$, 证明: $x^5 - 5$ 在 $K[x]$ 中不可约.

proof

□

3.1.15 设 k 是特征 $p > 0$ 的域, x, y 是 k 上的代数无关元. 令 $K = k(x^p, y^p)$, $L = k(x, y)$. 试证明 $[L : K] = p^2$.

proof

□

习题 3.2 教材 p59

3.2.1 解释说明 3° 角可以由尺规作出, 但是 1° 角不可作.

proof

□

3.2.2 设 $\zeta_{17} = \cos(2\pi/17) + i \sin(2\pi/17)$, $L = \mathbb{Q}[\zeta_{17}]$. 请利用高斯关于 $\cos(2\pi/17)$ 的公式写出 $\mathbb{Q} \subset L$ 的中间域使 $L = \mathbb{Q}[\zeta_{17}]$ 成为 \mathbb{Q} 上的一个二次根塔.

proof

□

习题 3.3 教材 p64

3.3.1 设 $f(x) = x^2 + ax + b \in K[x]$ 不可约, $E = K[u_1]$ (其中 $f(u_1) = 0$) 证明: E 必包含 $f(x) = 0$ 的另一个根 (所以 E 是 $f(x)$ 的分裂域).

proof

□

3.3.2 设 $f(x) = x^3 - 2 \in \mathbb{Q}[x]$, $u_1 = \sqrt[3]{2}$. 证明: $E = \mathbb{Q}[u_1]$ 不包含 $f(x) = 0$ 的其他两个根.

proof

□

3.3.3 设 L 是 n 次多项式 $f(x) \in K[x]$ 的分裂域, 证明: $[L : K] \leq n!$.

proof

□

3.3.4 构造 $x^5 - 2 \in \mathbb{Q}[x]$ 的一个分裂域 L , 并求 $[L : \mathbb{Q}]$.

proof

□

3.3.5 确定多项式 $x^{p^n} - 1 \in \mathbb{F}_p[x]$ 在 \mathbb{F}_p 上的分裂域 ($n \in \mathbb{N}$).

proof

□

3.3.6 设 L 是可分多项式 $f(x) \in K[x]$ 的一个分裂域, $K \subset E \subset L$ 是任意中间域. 证明: 对任意单同态 $\varphi : E \rightarrow L$, 若 $\varphi|_K = \text{id}_K$, 则 φ 一定可以延拓成域同构 $\bar{\varphi} : L \rightarrow L$.

proof

□

3.3.7 令 $f(x) = (x^2 - 2)(x^2 - 3)$, $K = \mathbb{Q}[x]/(x^2 - 2) = \mathbb{Q}[u_1]$, 此处 $u_1 = \bar{x} \in \mathbb{Q}[x]/(x^2 - 2)$. 试证明:

- (1) K 是一个域, 且 $x^2 - 3$ 在 $K[x]$ 中不可约;
- (2) $L = K[x]/(x^2 - 3) = K[u_2]$ (此处 $u_2 = \bar{x} \in K[x]/(x^2 - 3)$) 是 $f(x) = (x^2 - 2)(x^2 - 3)$ 的分裂域, 且 $[L : \mathbb{Q}] = 4$.

proof

□

3.3.8 设 $p \in \mathbb{Z}$ 是一个素数, F 是一个域, $c \in F$. 求证: $x^p - c$ 在 $F[x]$ 中不可约当且仅当 $x^p - c$ 在 F 中无根.

proof

□

3.3.9 设 $f(x)$ 是 $\mathbb{Q}[x]$ 中奇数次的不可约多项式, α 和 β 是 $f(x)$ 在 \mathbb{C} 中的两个不同的根. 试证明 $\alpha + \beta \notin \mathbb{Q}$ 且 $\alpha\beta \notin \mathbb{Q}$.

proof

□

3.3.10 设 $K = \mathbb{Q}[u]$, $u^3 + u^2 - 2u - 1 = 0$. 验证 $\alpha = u^2 - 2$ 也是多项式 $x^3 + x^2 - 2x - 1$ 的根. 试确定 $\text{Gal}(K/\mathbb{Q})$, 并证明: K 是 \mathbb{Q} 的正规扩张.

proof

□

3.3.11 证明: $\mathbb{Q}[\sqrt[4]{2}]$ 是 $\mathbb{Q}[\sqrt{2}]$ 的正规扩张, 但不是 \mathbb{Q} 的正规扩张.

proof

□

3.3.12 设 $f(x) \in K[x]$ 不可约, $\text{Char}(K) = p > 0$. 证明: 存在不可约的可分多项式 $g(x) \in K[x]$ 使得 $f(x) = g(x^{p^n})$ (n 是某个整数). 由此证明 $f(x)$ 在分裂域中的每个根都是 p^n 重根.

proof

□

3.3.13 设 $L = K[\alpha]$, α 是多项式 $x^d - a \in K[x]$ 的根. 如果 $\text{Char}(K) = 0$, 且 K 包含全部 d 次单位根, 则 $K \subset L$ 是正规扩张.

proof

□

3.3.14 设 k 是特征 $p > 0$ 的域, x, y 是 k 上的代数无关元. 令 $K = k(x^p, y^p)$, $L = k(x, y)$. 试证明:

- (1) $\text{Gal}(L/K) = \{1\}$ (但 $[L : K] = p^2$);
- (2) $K \subset L$ 有无穷多个中间域;
- (3) $K \subset L$ 不是单扩张, 即不存在 $\alpha \in L$ 使得 $L = K[\alpha]$.

proof

□

习题 3.4 教材 p67-68

3.4.1 设 $p > 2$ 是素数, $\alpha \in \mathbb{C}$ 是 $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 \in \mathbb{Q}[x]$ 的根. 证明: 域 $L = \mathbb{Q}[\alpha]$ 的自同构群 G 是一个 $p-1$ 阶的循环群.

proof

□

3.4.2 设 $K = \mathbb{Q}$, $L = K[\sqrt[3]{2}]$. 证明: $G = \text{Gal}(L/K) = \{1\}$ (所以 $L^G = L \neq K$). 如果令 $\bar{L} = K[\sqrt[3]{2}, \sqrt{-3}]$, 试证明: $\text{Gal}(\bar{L}/K) \cong S_3$. 并求出中间域 $K \subset K[\sqrt{-3}] \subset \bar{L}$ 对应的子群 $H \subset \text{Gal}(\bar{L}/K)$, 即: 求 $H \subset \text{Gal}(\bar{L}/K)$ 使得 $\bar{L}^H = K[\sqrt{-3}]$. (提示: $H = \text{Gal}(\bar{L}/K[\sqrt{-3}]) \cong A_3$.)

proof

□

3.4.3 设 $K \subset L$ 是有限, 可分, 正规扩张, $G = \text{Gal}(L/K)$. 设

$$K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_i \subset K_{i+1} \subset \cdots \subset K_m = L$$

是一个子域链, 令

$$\{1\} = G_m \subset G_{m-1} \subset G_{m-2} \subset \cdots \subset G_{i+1} \subset G_i \subset \cdots \subset G_0 = G$$

是其对应的子群链, 其中 $G_i = \text{Gal}(L/K_i)$. 证明:

(1) $K_i \subset K_{i+1}$ 是正规扩张 $\Leftrightarrow \forall \eta \in G_i, \eta(K_{i+1}) = K_{i+1}$ (提示: 应用推论 3.3.4).

(2) $\forall \eta \in G_i$, 则 $\eta \cdot G_{i+1} \cdot \eta^{-1} \subset G_i$ 是一个子群, 且

$$\eta(K_{i+1}) = L^{\eta G_{i+1} \eta^{-1}},$$

此处 $\eta \cdot G_{i+1} \cdot \eta^{-1} := \{\eta \cdot x \cdot \eta^{-1} \mid \forall x \in G_{i+1}\}$.

(3) 如果 $K_i \subset K_{i+1}$ 是正规扩张, $\forall \eta \in G_i$, 令

$$\bar{\eta} = \eta|_{K_{i+1}} : K_{i+1} \rightarrow K_{i+1},$$

则 $\bar{\eta} \in \text{Gal}(K_{i+1}/K_i)$, 映射 $G_i \xrightarrow{\phi} \text{Gal}(K_{i+1}/K_i), \eta \mapsto \bar{\eta}$, 是满同态, 而且 $\ker(\phi) = G_{i+1}$.

proof

□

第 4 章 群论初步

习题 4.1 教材 p72

4.1.1 设 G 是一个群, 定义映射 $G \xrightarrow{\varphi} G, x \mapsto x^{-1}$. 试证明: φ 是 G 的自同构当且仅当 G 是阿贝尔群.

proof

□

4.1.2 证明: 子群 $H \subset G$ 是正规子群当且仅当, $\forall g \in G, gHg^{-1} \subset H$.

proof

□

4.1.3 设 $G \xrightarrow{\varphi} G'$ 是群同态, $K = \ker(\varphi)$ 是同态 φ 的核. 试证明:

- (1) 对于任意子群 $H' \subset G', H = \varphi^{-1}(H') \subset G$ 是子群, 且包含 K .
- (2) 当 φ 是满射时, $H' \mapsto \varphi^{-1}(H')$ 建立了集合

$$\Gamma' = \{H' \subset G' \mid H' \text{ 是子群}\},$$

与集合 $\Gamma = \{H \subset G \mid H \text{ 是 } G \text{ 的子群, 且 } H \supset K\}$ 之间的双射, 此时 $H' \subset G'$ 是正规子群当且仅当 $\varphi^{-1}(H') \subset G$ 是正规子群.

proof

□

4.1.4 设 H, N 都是 G 的正规子群, 并且 $N \subseteq H$. 令 $\bar{H} = H/N, \bar{G} = G/N$.

- (1) 证明 \bar{H} 是 \bar{G} 的正规子群.
- (2) 证明 $G/H \cong \bar{G}/\bar{H}$.

proof

□

4.1.5 设 $H \subset G$ 是 G 的子群, $K \triangleleft G$, 试证明:

- (1) $H \cdot K = \{hk \mid \forall h \in H, k \in K\}$ 是 G 中包含 H 和 K 的子群;
- (2) H 在商同态 $G \rightarrow G/K, (g \mapsto \bar{g})$ 下的像是 $(H \cdot K)/K$;
- (3) $\varphi: H \rightarrow (HK)/K, (\varphi(h) = \bar{h})$ 的核是 $H \cap K$;
- (4) φ 诱导群同构 $H/(H \cap K) \cong (HK)/K$.

proof

□

习题 4.2 教材 p77

4.2.1 设群 $G = AB$, 其中 A, B 都是 G 的 Abel 子群 (即交换子群), 且 $AB = BA$. 令 $G^{(1)}$ 表示 G 的换位子群, 证明:

(1) $\forall a, x \in A, b, y \in B$, 总有 $[x^{-1}, y^{-1}][a, b][x^{-1}, y^{-1}]^{-1} = [a, b]$;

(2) $G^{(1)}$ 是 Abel 群.

proof

□

4.2.2 证明:

(1) $S_n = \langle (1\ 2), (1\ 3), \dots, (1\ n) \rangle$, 即 S_n 由对换 $(1\ 2), (1\ 3), \dots, (1\ n)$ 生成;

(2) S_n 可由 $(1\ 2)$ 和 $(1\ 2\ 3 \cdots n)$ 生成, 即

$$S_n = \langle (1\ 2), (1\ 2\ 3 \cdots n) \rangle.$$

proof

□

4.2.3 证明: 循环 $\pi = (1\ 2 \cdots n) \in S_n$ 的 k 次幂 π^k 是 d 个互不相交的循环之积, 每个循环的长度为 $q = \frac{n}{d}$, 其中 $d = (n, k)$ 是 n 和 k 的最大公因子.

proof

□

4.2.4 设 $A_n = \{\pi \in S_n \mid \varepsilon_\pi = 1\} \subset S_n$, 证明:

(1) $A_n \triangleleft S_n$ (即 A_n 是 S_n 的正规子群);

(2) A_n 由 3-循环生成, 事实上, $A_n = \langle (1\ 2\ 3), (1\ 2\ 4), \dots, (1\ 2\ n) \rangle$. (提示: 利用 $(a\ b) \cdot (b\ c) = (a\ b\ c)$, $(a\ b) \cdot (c\ d) = (a\ b) \cdot (b\ c) \cdot (b\ c) \cdot (c\ d)$.)

proof

□

4.2.5 群 G 中的两个元素 x, y 称为在 G 中共轭, 如果存在 $a \in G$, 使 $axa^{-1} = y$. 试证明:

(1) $\forall \pi \in S_n \alpha = (i_1 i_2 \cdots i_r) \in S_n$ 有公式

$$\pi \cdot \alpha \cdot \pi^{-1} = (\pi(i_1) \pi(i_2) \cdots \pi(i_r)).$$

(2) 所有 3-循环在 S_n 中相互共轭. (所以 S_n 中包含 3-循环的正规子群必包含 A_n .)

(3) 如果 $n \geq 5$, 则所有 3-循环在 A_n 中相互共轭, 即对于任意 3-循环 $x, y \in A_n$, 存在 $a \in A_n$, 使 $axa^{-1} = y$.

proof

□

4.2.6 证明: 对任意给定整数 $n > 0$, 在同构意义下仅有有限个 n 阶群. (提示: 任意 n 阶群均同构于 S_n 的一个子群.)

proof

□

4.2.7 证明: 所有 4 阶群 G 都是交换群. 在同构意义下, G 要么是循环群, 要么同构于下述克莱因 4 元群:

$$V_4 = \{(1), (12)(34), (13)(24), (14)(23)\} \subseteq S_4.$$

(提示: 如果 $x^2 = 1$ 对 G 中所有元成立, 则 $\forall a, b \in G$, 有 $abab = 1 \implies ab = b^{-1}a^{-1} = b(b^{-1})^2 \cdot (a^{-1})^2 a = ba$.)

proof

□

4.2.8 找出交错群 A_4 的所有子群.

proof

□

习题 4.3 教材 p80

4.3.1 设 $G = \langle \alpha \rangle$ 是 n 阶循环群, 试证明:

(1) α^m 是 G 的生成元 (即 $G = \langle \alpha^m \rangle$) $\Leftrightarrow (m, n) = 1$;

(2) 若 \mathbb{Z}_n 表示模 n 的剩余类环, $U(\mathbb{Z}_n)$ 是它的单位群, 则

$$\bar{m} \in U(\mathbb{Z}_n) \Leftrightarrow (m, n) = 1;$$

(3) 设 $\text{Aut}(G)$ 表示群 G 的自同构群, 则 $\text{Aut}(G) \cong U(\mathbb{Z}_n)$.

proof

□

4.3.2 设 F 是一个域, $F^* = F \setminus \{0\}$, 证明乘法群 F^* 的任何有限子群都是循环群.

proof

□

4.3.3 设 K 是特征零的域, L 是多项式 $x^n - 1 \in K[x]$ 的分裂域. 试证明: $\text{Gal}(L/K)$ 同构于 $U(\mathbb{Z}_n)$ 的一个子群. 特别地, $\text{Gal}(L/K)$ 总是交换群.

proof

□

习题 4.4 教材 p84

4.4.1 设 E 是 $x^4 - 2$ 在 \mathbb{Q} 上的分裂域.

- (1) 试求出 E/\mathbb{Q} 的全部中间域;
- (2) 试问哪些中间域是 \mathbb{Q} 的伽罗瓦扩张, 哪些域彼此共轭?

proof

□

4.4.2 设 $K \supset F$ 是伽罗瓦扩张, $f(x)$ 是 $\alpha \in K$ 在 F 上的极小多项式, $g(x) = \prod_{\sigma \in \text{Gal}(K/F)} (x - \sigma(\alpha))$. 证明: $g(x) \in F[x]$ 并且存在正整数 n 使得 $g = f^n$.

proof

□

4.4.3 设 $\xi = e^{\frac{2\pi i}{13}}, \alpha = \xi + \xi^4 + \xi^3 + \xi^{12} + \xi^9 + \xi^{10}$, 证明:

- (1) $\text{Gal}(\mathbb{Q}[\xi]/\mathbb{Q})$ 同构于乘法群 $\mathbb{F}_{13}^* = \mathbb{F}_{13} \setminus \{0\}$.
- (2) $[\mathbb{Q}[\xi] : \mathbb{Q}[\alpha]] = 6$.
- (3) 求 α 在 \mathbb{Q} 上的极小多项式.

proof

□

4.4.4 设 $p > 2$ 是素数, $\xi_p = e^{\frac{2\pi i}{p}}, \xi_{p^2}$ 为 p^2 次本原单位根.

- (1) 求 $\mathbb{Q}(\xi_p)/\mathbb{Q}$ 的扩张次数, 并证明 $\text{Gal}(\mathbb{Q}(\xi_p)/\mathbb{Q}) \cong F_p^*$;

- (2) 求 $\mathbb{Q}(\xi_{p^2})/\mathbb{Q}$ 的扩张次数, 并确定 $\text{Gal}(\mathbb{Q}(\xi_{p^2})/\mathbb{Q})$ (提示: 该群是 $(\mathbb{Z}/p^2\mathbb{Z})^*$);
- (3) 试确定 $\mathbb{Q}(\xi_{p^2})/\mathbb{Q}(\xi_p)$ 的扩张次数, 并证明这是一个伽罗瓦扩张.

proof

□

4.4.5 设 ξ_n 是 n 次本原单位根 (即 $\xi_n = e^{\frac{2\pi i}{n}}$).

- (1) 证明 $\mathbb{Q}(\xi_n)/\mathbb{Q}$ 是伽罗瓦扩张;
- (2) 当 $n = 12$ 时, 求伽罗瓦群 $\text{Gal}(\mathbb{Q}[\xi_n]/\mathbb{Q})$;
- (3) 设 $n > 2$ 为奇数, 证明 $\mathbb{Q}[\xi_n] \cap \mathbb{R} = \mathbb{Q}[\xi_n + \xi_n^{-1}]$.

proof

□

习题 4.5 教材 p87-p88

4.5.1 设 $\text{Aut}(X)$ 表示集合 X 的自同构群. 试证明:

- (1) 若 $G \times X \rightarrow X, (g, x) \mapsto g \cdot x$, 是群 G 在 X 上的一个作用, $\forall g \in G$, 定义映射 $X \xrightarrow{\rho(g)} X, x \mapsto g \cdot x$. 则 $\rho(g) \in \text{Aut}(X)$ 且映射

$$\rho: G \rightarrow \text{Aut}(X), g \mapsto \rho(g)$$

是群同态.

- (2) 若 $\rho: G \rightarrow \text{Aut}(X)$ 是一个群同态, 则映射

$$G \times X \rightarrow X, (g, x) \mapsto \rho(g)(x)$$

是一个群作用.

proof

□

4.5.2 20 阶群中共有多少个 5 阶元?

proof

□

4.5.3 证明 15 阶的群一定是循环群.

proof

□

4.5.4 证明 6 阶非 Abel 群一定同构于 S_3 .

proof

□

4.5.5 证明 12 阶群共有 5 个同构类, 即 12 阶群本质上只有 5 个.

proof

□

4.5.6 设 p, q 是两个不同的素数, 则 pq 或 p^2q 阶群一定不是单群. (事实上: $p^a q^b$ 阶群一定是可解群.)

proof

□

4.5.7 证明 200 阶群一定不是单群.

proof

□

4.5.8 设 H 为群 G 的有限子群.

- (1) 证明: $(h_1, h_2)(x) = h_2 x h_1^{-1}$ 定义了 $H \times H$ 在群 G 上的作用;
- (2) 证明: H 为 G 的正规子群当且仅当上述作用的每条轨道都恰有 $|H|$ 个.

proof

□

4.5.9 试证明若 $|G| < 60$ 且 G 是一个单群, 那么 G 一定是素数阶的循环群.

proof

□

4.5.10 若 G 是 60 阶单群, 那么 G 一定同构于 A_5 , 从而得到阶数最小的非交换单群是 A_5 .

proof

□

第 5 章 模论初步

习题 5.1 教材 p91

5.1.1 设 $R \xrightarrow{\varphi} R'$ 是环同态, M 是一个 R' -模. 证明:

$$R \times M \rightarrow M, \quad (a, x) \mapsto \varphi(a)x,$$

定义了 M 的一个 R -模结构使得 M 成为一个 R -模.

proof

□

5.1.2 设 M 是一个 R -模, $\text{Ann}(M) = \{a \in R \mid ax = 0, \forall x \in M\}$, 证明:

- (1) $\text{Ann}(M) \subset R$ 是理想;
- (2) 对任意理想 $I \subset R$, 若 $I \subset \text{Ann}(M)$, 则 $R/I \times M \rightarrow M, (\bar{a}, x) \mapsto ax$, 定义了 M 的一个 R/I -模结构.

proof

□

5.1.3 设 $M = (M, +, 0)$ 是加法群, $\text{End}(M) = \{M \xrightarrow{\varphi} M \mid \varphi \text{ 是群同态}\}$ 是 M 所有群自同态组成的环. 试证明:

- (1) $\text{End}(M) \times M \rightarrow M, (\varphi, x) \mapsto \varphi \cdot x := \varphi(x)$, 是 M 的一个 $\text{End}(M)$ -模结构. (因此, M 是一个 $\text{End}(M)$ -模.)
- (2) 设 R 是一个环, 则 M 有一个 R -模结构 $R \times M \rightarrow M, (a, x) \mapsto ax$ 的充要条件是存在环同态 $R \xrightarrow{\eta} \text{End}(M)$ 使得 $ax = \eta(a)(x)$ 对任意 $a \in R, x \in M$ 成立.

proof

□

5.1.4 设 $M = (M, +, 0)$ 是任意加法群, 证明: M 有唯一的 \mathbb{Z} -模结构.

proof

□

5.1.5 设 R -模 M 的模结构由环同态 $R \xrightarrow{\eta} \text{End}(M)$ 确定, $\varphi \in \text{End}(M)$. 试证明: $M \xrightarrow{\varphi} M$ 是 R -模同态当且仅当 $\varphi \circ \eta(a) = \eta(a) \circ \varphi, \forall a \in R$.

proof

□

5.1.6 R -模 M 称为不可约模, 如果 $M \neq 0$ 且 M 没有非平凡子模. 证明: R -模 M 不可约当且仅当存在极大左理想 $I \subset R$ 使得 $M \cong R/I$.

proof

□

5.1.7 (舒尔 (Schur) 引理) 证明: 如果 M_1, M_2 是不可约 R -模, 则任何非零模同态 $M_1 \rightarrow M_2$ 必为同构.

proof

□

5.1.8 (同态基本定理) 设 $\varphi: M \rightarrow M'$ 是 R -模同态. 证明: φ 的核

$$\ker(\varphi) = \{x \in M \mid \varphi(x) = 0\}$$

和像 $\text{Im}(\varphi) = \{\varphi(x) \mid \forall x \in M\}$ 必为子模, 且 φ 的诱导映射

$$\bar{\varphi}: M/\ker(\varphi) \rightarrow \text{Im}(\varphi), \bar{\varphi}(\bar{x}) = \varphi(x),$$

必为同构.

proof

□

习题 5.2 教材 p95-p96

5.2.1 设 R 是任意环, 证明: $R^m \cong R^n$ 当且仅当存在 $A \in M_{m \times n}(R), B \in M_{n \times m}(R)$ 使得 $AB = I_m, BA = I_n$.

proof

□

5.2.2 设 R 是交换环, $\eta: R^n \rightarrow R^n$ 是满同态. 证明 η 必为双射. 如果 η 是单射, 它一定是满射吗?

proof

□

5.2.3 设 R 是交换整环, $e_1, e_2, \dots, e_n \in R^n$ 是一组基. 令

$$(f_1, f_2, \dots, f_n) = (e_1, e_2, \dots, e_n)A, \quad A \in M_n(R).$$

证明:

- (1) f_1, f_2, \dots, f_n 生成一个秩为 n 的子模 $K \subset R^n$ 的充要条件是 $\det(A) \neq 0$;
- (2) $\forall \bar{x} \in R^n/K$, 则 $\det(A) \cdot \bar{x} = 0$.

proof

□

5.2.4 设 $K \subset \mathbb{Q}[\lambda]^3$ 是由 $f_1 = (2\lambda - 1, \lambda, \lambda^2 + 3)$, $f_2 = (\lambda, \lambda, \lambda^2)$, $f_3 = (\lambda + 1, 2\lambda, 2\lambda^2 - 3)$ 生成的 $\mathbb{Q}[\lambda]$ -子模. 试求 K 的一组基.

proof

□

5.2.5 设 R 是欧氏环 ($\delta: R^* \rightarrow \mathbb{N}$), $A \in M_n(R)$ 且 $\det(A) \neq 0$. 证明: 存在可逆矩阵 $P \in M_n(R)$ 使得

$$PA = \begin{pmatrix} d_1 & b_{12} & b_{13} & \cdots & b_{1n} \\ & d_2 & b_{23} & \cdots & b_{2n} \\ & & d_3 & \cdots & b_{3n} \\ & & & \ddots & \vdots \\ & & & & d_n \end{pmatrix}$$

是上三角矩阵且 $d_i \neq 0 (1 \leq i \leq n)$, $\delta(b_{ji}) < \delta(d_i)$.

proof

□

习题 5.3 教材 p101

5.3.1 设 M 是主理想整环 R 上的挠模. 证明: M 是不可约 R -模当且仅当 $M = R \cdot z$, $\text{ann}(z) = (p)$, $p \in R$ 不可约.

proof

□

5.3.2 设 M 是主理想整环 R 上的有限生成挠模, M 称为不可分解模, 如果 M 不能写成两个非零子模的直和. 证明: M 不可分解当且仅当 $M = R \cdot z$, $\text{ann}(z) = (p^e)$, $p \in R$ 不可约.

proof

□

参考文献

- [Alu09] P. Aluffi. *Algebra: Chapter 0*. Graduate studies in mathematics. American Mathematical Society, 2009.
- [AM94] M.F. Atiyah and I.G. MacDonald. *Introduction To Commutative Algebra*. Addison-Wesley series in mathematics. Avalon Publishing, 1994.
- [Hun03] T.W. Hungerford. *Algebra*. Graduate Texts in Mathematics. Springer New York, 2003.
- [孙 22] 孙笑涛. 抽象代数. 科学出版社, 2022.