孙笑涛《抽象代数》习题解答与补充

2025 年 1 月 3 日

仅供学习交流使用

目录

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...
7. 由于 $\mathbb{Z}_p$ 是 p-adic integers 的标准记号, 为防止混淆, 习题中出现的 $\mathbb{Z}_p$ 一律替换为 $\mathbb{Z}/p\mathbb{Z}$ 或 $\mathbb{F}_p$. 对一般的 n 我也会替换.
8. 和教材保持一致, 用 R^* 表示所有非零元 $R\setminus\{0\}$, 单位群用 $U(R)$ 或 $R^\times$ 表示. 域的时候两者是一样的, 主要是区分整环的情形.
9. 有时对域扩张 $K\subseteq L$ 会使用标准记号 L/K 表示.
10. 课程的参考书是 [Lan12] 和 [冯 09].
11. 教材答案有误的题目用 $*$ 标出.

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) $(a^{-1})^{-1}=a\quad(\forall\, a\in K,\ a\neq 0_K)$;

(4) $(a\cdot b)^{-1}=a^{-1}\cdot b^{-1}\quad(a\neq 0_K,\ b\neq 0_K)$;

(5) $(-a)^{-1}=-a^{-1}\quad(\forall a\neq 0_K)$;

(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

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

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,

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

负整数的部分定义为

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

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

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

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

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

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

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

当 $n < 0$ 时,

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

由于 $a^{-m} \cdot a^m \overset{(*)}{=} a^0 = 1_K$, 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 $F = \bigcap\limits_i K_i$ 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 $L = \bigcup\limits_i K_i$, 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, $\dfrac{1}{\sqrt{2} + \sqrt{3}} = \sqrt{3} - \sqrt{2} \in \mathbb{Q}[\sqrt{2} + \sqrt{3}]$, 故有 $\sqrt{2} = \dfrac{(\sqrt{2} + \sqrt{3}) - (\sqrt{3} - \sqrt{2})}{2} \in \mathbb{Q}[\sqrt{2} + \sqrt{3}]$, $\sqrt{3} = \dfrac{(\sqrt{2} + \sqrt{3}) + (\sqrt{3} - \sqrt{2})}{2} \in \mathbb{Q}[\sqrt{2} + \sqrt{3}]$. 因此 $\mathbb{Q}[\sqrt{2}, \sqrt{3}] \subseteq \mathbb{Q}[\sqrt{2} + \sqrt{3}]$. 故两者相等. □

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 $f:\mathbb{N}\to\mathbb{Q}$. 令 $f^{-1}:\mathbb{Q}\to\mathbb{N}$ 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: $\forall n,m,l\in\mathbb{N}$,

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

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 $f^{-1}(-f(n))$:

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

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 $f^{-1}(\dfrac{1}{f(n)})$:

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

分配律: $\forall n,m,l\in\mathbb{N}$,

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

□

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, $\mathbb{F}_p=\{\overline{0},\overline{1},\overline{2},\cdots,\overline{p-1}\}$ 是 $\mathbb{Z}$ 的模 p 剩余类域. 试计算:

(1) $\overline{2}$ 在 $\mathbb{F}_p$ 中的逆元 $\overline{2}^{-1}$;

(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 $\overline{1+kp}(k\in\mathbb{Z})$. 由于素数 $p>2$, $p+1$ 即可. i.e. $\overline{2}^{-1}=\overline{\frac{1}{2}(p+1)}$.

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

(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) $-(-a)=a,\quad a(b-c)=ab-ac\quad(\forall a,b,c\in R)$;

(4) $-(a+b)=(-a)+(-b)\quad(\forall a,b\in R)$;

(5) $a(-b)=(-a)b=-(ab)\quad(\forall a,b\in R)$;

(6) $(-a)(-b)=ab\quad(\forall a,b\in R)$;

(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

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

得 $a(-c) = -ac$, 这也是 (5) 的证明. 这里要注意仅使用 $-a \overset{(*)}{=} -1_R \cdot a$ 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

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

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

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

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

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

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

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

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

(9) (7) 和 (8) 的推论,

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

(10) 对 n 归纳,

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

□

注:

(7)-(9) 中实际上需要用归纳法证明的只有

$$n(a+b)=na+nb,$$
$$(m+n)a=ma+na,$$
$$(mn)a=m(na),$$

这三条加上 $1a=a$, 是在说任何一个 Abel 群都是 $\mathbb{Z}$-模 (5.1.4), 因为这几条的证明过程并未用到 R 的乘法, 把 R 换成任意的 Abel 群也是对的. 再反过来看1.1.1的 (6), 加上 $(ab)^n=a^nb^n$, 也是在说 K^* 是 $\mathbb{Z}$-模, 证明过程中用到了 K^* 关于域的乘法是 Abel 群.

另一方面, 可以先定义

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

这是一个自然的环同态 (使用归纳法证明)

$$N(m+n)=N(m)+N(n);$$
$$N(mn)=N(m)\cdot N(n).$$

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):

$$n(a+b)=n(1_R(a+b))=(n1_R)(a+b)\overset{dis}{=}(n1_R)a+(n1_R)b=na+nb.$$

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

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 Ring 中是始对象 (initial object), Ring 表示环范畴. 因此 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 指幺元.

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:

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

零元为 $\varnothing$,

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

负元为 A 本身,

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

即 $2A=0$.

(ii) $(P(X),\cdot)$ 是 (交换) 幺半群, 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 $\forall x\in S$

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

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, 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:

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

□

注:

使用形式级数是合理的, 从2.3.1可以看到形式级数环是有定义的, 且和多项式环一样是可以赋值的 (2.3.7).

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:

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

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).

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

□

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

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

将左边展开得

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

再证存在性, 将 $A(x)$ 写成多项式的形式,

$$A(x) = A_0 + A_1 x + A_2 x^2 + \cdots + A_k x^k, \quad A_i \in M_{n\times m}(K), 0 \leqslant i \leqslant k.$$

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:

$$\begin{aligned} A(x) &= A_0 + x(A_1 + A_2 x + \cdots + A_{k+1}x^k) \\ &= A_0 + x((xI_n - A)\tilde{B}(x) + \tilde{R}) \\ &= (xI_n - A)x\tilde{B}(x) + xI_n\tilde{R} - A\tilde{R} + A\tilde{R} + A_0 \\ &= (xI_n - A)(x\tilde{B}(x) + \tilde{R}) + A\tilde{R} + A_0. \end{aligned}$$

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, $\mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}, \cdots, \overline{m-1}\}$ 是 $\mathbb{Z}$ 的模 m 剩余类环. 试证明: $\overline{a} \in \mathbb{Z}/m\mathbb{Z}$ 可逆当且仅当 $(a, m) = 1$(即: a 与 m 互素).

proof

$\overline{a} \in \mathbb{Z}/m\mathbb{Z}$ 可逆,

$$\begin{aligned} &\iff \exists \overline{b} \in \mathbb{Z}, \quad \overline{a}\overline{b} = \overline{1} \\ &\iff ab = 1 + km, \quad k \in \mathbb{Z}, \\ &\iff (a, m) = 1. \quad \text{(Bézout's Identity)} \end{aligned}$$

□

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 $\overline{a}$ 是加法群 $(\mathbb{Z}/m\mathbb{Z}, +)$ 的生成元, 即 $\overline{a}$(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 $|a|\,|\,|G|$(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) $\mathbb{Z}/m\mathbb{Z}$ 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 $\mathbb{Z}/m\mathbb{Z}$ 有幂零元 $\bar{a}$, 则存在 $n>1(a\neq 0)$ 使得 $\bar{a}^n=\overline{a^n}=\bar{0}$. 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, $e_1,e_2,\cdots,e_r\geqslant 1$, 则 $p_i\mid a$, $1\leqslant i\leqslant r$, 故有 $p_1p_2\cdots p_r\mid a$. 因此有 $p_1p_2\cdots p_r\leqslant a<m$, 故必有某个 $e_i>1$, 即 $\exists 1\leqslant i\leqslant r$, $e_i\geqslant 2$, 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 $a=p_1p_2\cdots p_r$, $\bar{a}$ 为 $\mathbb{Z}/m\mathbb{Z}$ 的幂零元.

□

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

proof

先考虑

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

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 $1 \leqslant k < n$, $(ba)^k = b(ab)^k b^{-1} \neq e$. 因此 $|ba| = n$. 反之亦然.
若 $|ab| = \infty$, 则
$$\forall n \in \mathbb{Z}_{\geqslant 1}, \quad (ba)^n = b(ab)^n b^{-1} \neq e.$$
故 $|ba| = \infty$. 反之亦然. □

注:

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).
$$\sigma_a : G \to G, \quad g \mapsto aga^{-1}$$
是群 G 的一个自同构. 而对一般的群同态 $\varphi : G \to G'$, $|g| < \infty \implies |\varphi(g)| < \infty$

且 $|\varphi(g)|\,\big|\,|g|$. 因此若 φ 为同构, 则 $|g|=|\varphi(g)|$(包括左右为无穷的情况).

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 $(a^{-1})^{-1}=a$;

□

注:

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

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

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 $\mathrm{id}_{S_3}=e$, 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 $\mathscr{R}$, A 和 $\mathscr{R}$ 将唯一确定一个群 G, $(A\mid\mathscr{R})$ 称为 G 的一个展示 (presentation). 以 S_3 为例, S_3 的一个展示为 $(\{a,b\}\mid a^2,b^3,abab)$. 另外有二面体群 (Dihedral Groups)$D_{2n}=(a,b\mid a^2,b^n,abab)$
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 $f:X\to Y$ 和 $g:Y\to Z$ 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:

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

这样说的好处在于一眼能感觉出这个运算是不交换的. 当然这只是个人感觉, 也

有可能是我先入为主了, 因为我最开始接触到的范畴里的复合是这样写的. 如果引入范畴的记号, S_A 会记作 $\mathrm{Aut}_{\mathsf{Set}}(A)$, 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:

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

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 [Lan12] 和 [Hun03] 就做的很好. 它的范畴定义故意反了过来, 它写成 $\mathrm{Hom}_{\mathcal{C}}(Y, Z) \times \mathrm{Hom}_{\mathcal{C}}(X, Y) \to \mathrm{Hom}_{\mathcal{C}}(X, Z)$.
那么哪一个才对呢, 事实上都是对的, 你总能验证 S_A 确实时一个群. 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 $H_1, H_2 \lneqq G$ 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 $h_1 h_2 \in H_1 \implies h_2 \in H_1$) □

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) "$\Longleftarrow$": 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

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

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) "$\Longrightarrow$": 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 $G=\{a_1,a_2,\cdots a_n\}$. 对 $\forall 1\leqslant i,j\leqslant n$,

$$a_ia_1,a_ia_2,\cdots,a_ia_n$$

互异, 否则存在 $a_k\neq a_l$ 使得 $a_ia_k=a_ia_l$, 由消去律得 $a_k=a_l$ 矛盾. 因此 $\exists 1\leqslant t\leqslant n$, $a_ia_t=a_j$, 即方程 $a_ix=a_j$ 有解. 同理方程 $ya_i=a_j$ 也有解, 由1.3.8, G 是群. □

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 $G/\sim=\{\overline{g}\mid g\in G\}$, 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 $\#\overline{g}=1$, 否则 $\#\overline{g}=2$. 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 $m>0$. □

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,

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

可以用归纳法证明

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

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, $H_i < G, \forall \in I$. 验证 $H = \bigcap_{i \in I} H_i < G$: 首先 $e_G \in H$, $H \neq \varnothing$,

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

□

注:

教材中并未提及这个判断子群的命题, 但其实是最常用的.

命题 (子群的判定) 设 G 是一个群, $\varnothing \neq S \subseteq G$, 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 $\varphi : G \to G'$ 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)

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

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 $f(x) = \dfrac{1}{x}, g(x) = \dfrac{x-1}{x}$ 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 $f^2 = \mathrm{id}, g^3 = \mathrm{id}, fgfg = \mathrm{id}$.

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

□

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, $\phi : K[x] \to K[x]$ 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 $x = \phi(g(x)) \overset{!}{=} g(\phi(x)) = g(f(x))$, ! 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) $" \Longleftarrow "$: 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 $f : \mathbb{R} \to \mathbb{R}_{>0}$, $x \mapsto e^x$ 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 $f : \mathbb{Q} \to \mathbb{Q}_{>0}$, 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 $\sigma : \mathbb{Q} \to \mathbb{Q}$ 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 $\sigma|_{\mathbb{N}} = \mathrm{id}_{\mathbb{N}}$, 用负元延拓到 $\mathbb{Z}$, 再用逆元延拓到 $\mathbb{Q}$ 得 $\sigma = \mathrm{id}_{\mathbb{Q}}$. 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 $\phi : \mathbb{R} \to \mathbb{R}$ 是同构, 有上面可知 $\phi|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$. 另外, 可以证明 ϕ 保序结构, 即 $x \geqslant 0 \implies \phi(x) \geqslant 0$. 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 $\lim\limits_{n \to \infty} \phi(q_n) = \lim\limits_{n \to \infty} q_n$(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 R 中稠密, 从而 $\phi = \mathrm{id}_{\mathbb{R}}$.

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

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 $\varphi : \mathbb{Q}[\sqrt{2}] \to \mathbb{Q}[\sqrt{5}]$, 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, $K \supseteq L$ 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 $K \supseteq L$ 的次数);

(2) 如果 $K \supseteq \mathbb{R}$ 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

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

是数乘. 即要验证

$$\begin{aligned} (l_1 l_2)k &= l_1(l_2 k), \\ (l_1 + l_2)k &= l_1 k + l_2 k, \\ l(k_1 + k_2) &= lk_1 + lk_2, \\ 1k &= k = k1. \end{aligned}$$

这些都由域的定义得到.

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

(2) 可取 K 的一组基为 $1, \alpha$, 其中 $\alpha \in \mathbb{C} \setminus \mathbb{R}$. 因为我们需要的同构是要保持乘法的, 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 $\alpha = \dfrac{y \pm i\sqrt{|y^2 + 4x|}}{2}$. 故映射

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

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 (教材 5.1 节)

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

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

$$\begin{aligned}
f\left((x_1+iy_1)\cdot(x_2+iy_2)\right) &= f(x_1+iy_1)\cdot f(x_1+iy_1) \\
&= (x_1+y_1f(i))\cdot(x_2+y_2f(i)) \\
\implies f\left(x_1x_2-y_1y_2+(x_1y_2+x_2y_1)i\right) \\
&= x_1x_2+y_1y_2f(i)\cdot f(i)+(x_1y_2+x_2y_1)f(i) \\
\implies x_1x_2-y_1y_2+(x_1y_2+x_2y_1)f(i) \\
&= x_1x_2+y_1y_2f(i)\cdot f(i)+(x_1y_2+x_2y_1)f(i) \\
\implies f(i)\cdot f(i) = -1.
\end{aligned}$$

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 $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \mathbb{Z}/2\mathbb{Z}$.
由线性代数的结论, 可以直接得到 K 和 $\mathbb{C}$ 是作为 $\mathbb{R}$-线性空间同构, 但我们需要它们作为 $\mathbb{R}$ 的扩域是同构的, 所以这是不够的. 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 (1.4.8). 根据我们上述的讨论, 对于域扩张 $\mathbb{C}/\mathbb{R}$ 只有恒等和共轭两个线性映射是域同构, 因此我们需要找到一个从 K 到 $\mathbb{C}$ 的 $\mathbb{R}$-线性映射, 让它恰好是两者之一才是一个域同构. 这就是 (2) 的思路来源.

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

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

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). □

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

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

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

proof

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

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

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

proof

同1.4.9, 若 $\sigma \in \mathrm{Gal}\left(\mathbb{Q}[\sqrt{d}]/\mathbb{Q}\right)$, 则 $\sigma \in \mathrm{Aut}_{\mathbb{Q}-\mathsf{Vect}}\left(\mathbb{Q}[\sqrt{d}]\right)$, 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 $\mathrm{Gal}\left(\mathbb{Q}[\sqrt{d}]/\mathbb{Q}\right) = \mathbb{Z}/2\mathbb{Z}(= S_2)$, 两个同构分别为 id 和共轭. □

1.4.13 设 $V = (V, +)$ 是一个加法群, $\mathrm{Hom}(V)$ 表示它的自同态环. 对任意域 K, 如果存在一个数乘运算 $K \times V \to V$, $(\lambda, v) \mapsto \lambda \cdot v$, 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 $\varphi: K \to \mathrm{Hom}(V)$, 则数乘运算

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

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 $\phi: K \times V \to V$, 则映射

$$\varphi: K \to \mathrm{Hom}(V), \quad \lambda \mapsto \phi(\lambda, \cdot)$$

是一个环同态, 其中 $\phi(\lambda, \cdot): V \to V$ 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 $\varphi(1) = 1_{\mathrm{Hom(V)}} = \mathrm{id}_V$. 故 $\forall v \in V$ 有 $1v = \varphi(1)(v) = \mathrm{id}_V(v) = v$.

(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 $\phi(1, \cdot) = \mathrm{id}_V$.

(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 $\varphi: K \to \mathrm{Hom}(\mathbb{Z})$.

但是 $\mathrm{Hom}(\mathbb{Z})$ 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 $\mathrm{Char}(K) = \mathrm{Char}(\mathbb{Z}) = 0$, 从而 $\mathbb{Q} \subseteq K$. 这样也可以看出矛盾.

$\square$

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 $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, (a, b) \mapsto a \oplus b$, 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 $f : \mathbb{Z} \to \mathbb{Q}$, 由 $\mathbb{Q}$ 的环结构导出 $(\mathbb{Z}, \oplus, \star)$.
则同态

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

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. $\square$

注:

对于 $\mathbb{Z}$ 还有一个重要的结论, $\mathbb{Z}$ 的 (含幺) 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:

这题的理想的根定义有误, 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,

$$\forall a, b \in \sqrt{I}, \exists m, n \in \mathbb{N}, a^m, b^n \in I,$$
$$\implies (a-b)^{m+n-1} \in I$$

这是因为单项 $a^i b^j$ 的指数 $i+j = m+n-1$, 故 $i < m$ 和 $j < n$ 不能同时成立, 即 $i \geqslant m$ 或 $j \geqslant n$, 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 $\mathfrak{N}(R) = \bigcap\limits_{\mathfrak{p} \text{ 是素理想}} \mathfrak{p}$.(需要 Zorn's Lemma, 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 $\mathrm{Char}(R) \neq p$, 则由 $p = 0$, $\mathrm{Char}(R) < p$. 那么 $(p, \mathrm{Char}(R)) = 1$, 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,

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

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 $1 \leqslant i \leqslant p-1$ 时,

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

由于 p 是素数, $1, 2, \cdots i$ 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 $\varphi : R \to R$, $x \mapsto x^{p^m}$ 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. Frobenius 是满射的特征 p 的域是完全域 (perfect field, 教材 3.3 节). 从证明过程可以看出, 这个同态和 x, y 并没有关系, 因此在特征 p 的多项式环上这个映射仍是一个同态.

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

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

由于理想个数有限, 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 $ab = 1$. □

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 condtion(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) " $\Longrightarrow$ ":

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

(2) " $\Longleftarrow$ ":

$$ab \in P \implies \bar{a}\bar{b} = \overline{ab} = \bar{0} \implies \bar{a} = 0 \text{ or } \bar{b} = 0 \implies a \in P \text{ or } b \in P.$$

□

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, $\mathrm{Spec}(R) := \{\mathfrak{p} \mid \mathfrak{p}$ 是R 的素理想$\}$ 称为 R 的素谱 (spectrum). $\mathrm{Spec}(R)$ 上有一个拓扑结构, Zariski 拓扑, 有兴趣可自行了解.

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) " $\Longrightarrow$ ":

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

(2) " $\Longleftarrow$ ":

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

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.

$\square$

注:

(1) 中用到了理想的和. 若 I,J 都是 R 的理想, $I+J \coloneqq \{i+j \mid i \in I, j \in J\}$. 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,

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

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

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

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.

命题 设 R 是交换环, 理想 $I \neq (1)$, 那么存在极大理想 $\mathfrak{m}$ 使得 $I \subseteq \mathfrak{m}$.

证明需要 Zorn's Lemma.

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) $\Longrightarrow$ (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) $\Longrightarrow$ (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) $\Longrightarrow$ (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 $\mathbb{Z}/p\mathbb{Z}$ 是域.

$\square$

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

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

可以验证这确实是一个同态 (教材引理 2.3.2). 记 $f = \sum_{i=0}^{n} a_i x^i$, $g = \sum_{j=0}^{m} b_i x^i$, 不妨设 $n > m$, 且令 $b_j = 0, m < j \leqslant n$. 由于 $R \to R/I$ 是同态, 这个映射是

良定义的, 且我们有

$$
\begin{aligned}
\varphi(f+g) &= \varphi\left(\sum_{i=0}^{n}(a_i+b_i)x^i\right) = \sum_{i=0}^{n}\overline{(a_i+b_i)}x^i = \sum_{i=0}^{n}(\overline{a_i}+\overline{b_i})x^i \\
&= \varphi(f)+\varphi(g), \\
\varphi(fg) &= \varphi\left(\sum_{k=0}^{n+m}\sum_{i+j=k}a_ib_jx^k\right) = \sum_{k=0}^{n+m}\sum_{i+j=k}\overline{a_ib_j}x^i = \sum_{k=0}^{n+m}\sum_{i+j=k}\overline{a_i}\overline{b_j}x^i \\
&= \varphi(f)\varphi(g), \\
\varphi(1) &= \overline{1}.
\end{aligned}
$$

事实上, 它是 $R \twoheadrightarrow R/I \hookrightarrow \dfrac{R}{I}[x]$ 的一个延拓.
回到原题, 有

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

这里 $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ 是域. 因此 $\mathbb{F}_p[x]$ 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

$$(r_1s_1)(r_2s_2) = \varphi(r_1)s_1\varphi(r_2)s_2 = \varphi(r_1)\varphi(r_2)s_1s_2 = \varphi(r_1r_2)s_1s_2 = (r_1r_2)(s_1s_2).$$

即数乘和 S 本身的乘法是相容的, 换句话说, S 上的乘法是 R-双线性的. 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)
既然提到泛性质, 那么需要对同态基本定理进行更详细的说明, 这里以环同态为例, 所谓的同态基本定理是 quotient 的泛性质, 教材的版本是相对弱一点的版本.

定理 设 R 是环, $I \subseteq R$ 是理想. 对任意的环同态 $R \xrightarrow{f} R'$, 若 $I \subseteq \ker(f)$,

则存在唯一的同态 $\overline{f}: R/I \to R'$ 使得图表交换

$$\begin{tikzcd} R \arrow[rr, "f"] \arrow[dr, "\pi"'] & & R' \\ & R/I \arrow[ur, "\exists!\overline{f}"'] & \end{tikzcd}$$

写成等式就是 $\overline{f}(\overline{r}) = f(r)$, 要说明这样的 $\overline{f}$ 是良定义的, 这和商同态的做法一样.

$$r + I = r' + I \implies r - r' \in I \subseteq \ker(f) \implies \overline{f}(\overline{r}) - \overline{f}(\overline{r'}) = f(r - r') = 0.$$

注意到 $\ker(\overline{f}) = \ker(f)/I$(作为 R-模, $\ker(f)/I$ 是商模), 这意味着 $I = \ker(f)$ 时 $\ker(\overline{f}) = \{0\}$, 此时 $\overline{f}$ 是单射, 刚好就是熟知的同态基本定理. 这里用到了一个等价的条件:

命题　设 $R \xrightarrow{\varphi} R'$ 是环同态, 则下列条件等价 (最后一条可以不用管):

(i) φ 是单射;

(ii) $\ker(\varphi) = \{0\}$;

(iii) $\varphi \circ \psi_1 = \varphi \circ \psi_2 \implies \psi_1 = \psi_2$, 即 φ 是 Ring 中的单态射.

上述讨论对群和模是类似的.

2.1.9　映射 $D: R[x] \longrightarrow R[x]$ 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 $n \geqslant m$, 且令 $b_k = 0, k > m$.

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

$$D(af) = D\left(\sum_{k=0}^{n} aa_kx^k\right) = \sum_{k=1}^{n} kaa_kx^{k-1} = a\sum_{k=1}^{n} ka_kx^{k-1} = aD(f).$$

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)

$$\begin{aligned} D(f\cdot g) = D\left(\sum_{k=0}^{n+m}\sum_{i+j=k} a_ib_jx^k\right) &= \sum_{k=1}^{n+m}\sum_{i+j=k} ka_ib_jx^{k-1} \\ &= \sum_{k=1}^{n+m}\sum_{i+j=k} (i+j)a_ib_jx^{i+j-1} \\ &= \sum_{k=1}^{n+m}\sum_{i+j=k} (ia_ix^{i-1})b_jx^j + a_ix^i(jb_jx^{j-1}) \\ &= \sum_{k=0}^{n+m-1}\sum_{(i-1)+j=k} (ia_i)b_jx^k + a_i(jb_j)x^k \\ &= D(f)\cdot g + f\cdot D(g). \end{aligned}$$

□

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

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

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

故 $f(x) = a_0$, $\deg(f) = 0$ 或 $f = 0$, 反过来是平凡的.
若 $\mathrm{Char}(F) = p$, 则 $p = 0$, 那么设 $\deg(f) = n = kp + r, 0 \leqslant r < p, k \in \mathbb{N}$,

$$\begin{aligned} & f = a_0 + a_1x + \cdots a_px^p + \cdots + a_{2p}x^{2p} + \cdots + a_{kp}x^{kp} + a_nx^n. \\ \implies & f' = a_1 + \cdots + pa_px^{p-1} + \cdots + kpa_{kp}x^{kp-1} + \cdots na_nx^{n-1} \\ & \quad = a_1 + \cdots + (p-1)a_{p-1}x^{p-2} + (p+1)a_{p+1}x^p + \cdots (kp-1)a_{kp-1}x^{kp-2} \\ & \quad + (kp+1)a_{kp+1}x^kp + \cdots + na_nx^{n-1}. \end{aligned}$$

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

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 $\alpha\in\mathbb{R}$.

$\square$

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 $K\to R$. $\square$

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

$$k_1M_1k_2M_2 = k_1k_2M_1M_2, k_1, k_2 \in K, M_1, M_2 \in M_n(K).$$

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 $\mathrm{End}_{\mathsf{Ab}}(R)$ 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,

$$R \to \mathrm{End}_{\mathsf{Ab}}(R), \quad r \mapsto \lambda_r$$

其中 $\lambda_r : R \to R$, $a \mapsto ra$, 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 $\mathrm{End}_{\mathsf{Ab}}(R)$ 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 $R \hookrightarrow \mathrm{Hom}_K(R) \cong M_n(K)$.

(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 $1, \alpha, \alpha^2, \cdots, \alpha^n$ 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 $\mathbb{F}_{3^2} = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \middle| a, b \in \mathbb{F}_3 = \mathbb{Z}/(3) \right\}$ 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. □

注:
$x\sim y :\Leftrightarrow \exists u\in U(R), x=uy \iff (x)=(y) \iff x\mid y$ 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 $(r)\subseteq I=(a)\iff a\mid r$. 又因为 PID 是 UFD, 因此又唯一分解 $r=p_1p_2\cdots p_n$, 从而 r 因子个数在相伴的意义下 (2.2.2的注记) 有限 $(\leqslant 2^n)$, 即包含 r 的理想有限. □

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

$$a=q_1b+r_1,\ b=q_2r_1+r_2,\ r_1=q_3r_2+r_3,\ \cdots,\ r_{k-2}=q_kr_{k-1}+r_k$$

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 $\delta(k) \leqslant \delta(b) - k$, 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 $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid \forall a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$, 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).

$\square$

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. 古典的代数数论的证明方法和 (2) 几乎一模一样. 具体细节参考代数数论的教材. 而交换代数的理论发展之后, 由 Hilbert's Basis Theorem 可以直接得到 $\mathcal{O}_K$ 是 Noether 环, 从而存在不可约分解.

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

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

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

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

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 $x=\dfrac{u+v}{2}, y=\dfrac{u-v}{2i}$. 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

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

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 $f=a_nu^n+a_{n+1}u^{n+1}+\cdots+a_mu^m, n,m\in\mathbb{Z}, n<m$ 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

$$\begin{aligned}a_1b_1-a_2b_2&=0,\\a_1b_2+a_2b_1&=0,\\a_1b_1+a_3b_3&=0,\\a_1b_3+a_3b_1&=1,\\a_2b_3+a_3b_2&=0.\end{aligned}$$

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.

$\square$

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), Laurent 级数展开是复分析中的一个重要概念.

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, $S \subseteq k[x_1, x_2, \cdots, x_n]$, 那么可以定义 S 中所有多项式的公共零点集

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

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

$$I = \left\{\sum f_i g_i \middle| f_i \in k[x_1, x_2, \cdots, x_n], g_i \in S\right\},$$

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 $Z(\varnothing) = k^n$), 而 Hilbert's Basis Theorem 告诉我们 $k[x_1, x_2, \cdots, x_n]$ 是 Noether 环, 所以理想都是有限生成的, 那么总有 $Z(I) = Z(f_1, f_2, \cdots, f_r)$.
反过来, 对 $X \subseteq \mathbb{A}_k^n$, 定义

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

可以验证 $\mathscr{I}(X)$ 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

$$\{\mathbb{A}_k^n \text{ 的代数集}\} \underset{Z}{\overset{\mathscr{I}}{\rightleftarrows}} \{k[x_1, x_2, \cdots x_n] \text{ 的根理想}\}$$

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 $\mathscr{I}(Z(I)) = I$. 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 $Z(J) = (0, 0)$, $\mathscr{I}(Z(J)) = (x, y) \neq J$. 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在相伴的意义下是一样的, 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) $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots$ 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

$$\begin{aligned} a_0b_0 &= 1, \\ a_1b_0+a_0b_1 &= 0, \\ a_2b_0+a_1b_1+a_0b_2 &= 0, \\ &\vdots \end{aligned}$$

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 $b_0 \in F$, $a_0b_0=1$. 我们可以通过上面的无穷个方程组递归的解出 $b_k(k \geqslant 1)$.

$$\begin{aligned} b_1 &= -a_1b_0^2, \\ b_2 &= -a_2b_0^2-a_1b_1b_0, \\ &\vdots \\ b_k &= -\sum_{i=1}^{k} a_i b_{k-i} b_0, \\ &\vdots \end{aligned}$$

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 $p(x)=xp_1(x)$. 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 $f_2 \mid f_1$.

$\square$

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). 相关证明请参考 [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

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

诱导了域嵌入 $\varphi|_F : F \hookrightarrow F[x]/I, a \mapsto \overline{a}$(如果将 F 与它的像等同, 则 $\overline{x} \in F[\overline{x}] := F[x]/I$ 是 $p(x)$ 在扩域 $F[\overline{x}]$ 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 (embbeding) 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, $K \subseteq F$ 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 f 不可约, f 不是单位, 即 $\deg(f) > 0$, 则有 $0 \leqslant \deg(f') < \deg(f)$. 若有非单位的公因式 $d(x)$, 则 $\deg(f) > \deg(f') \geqslant \deg(d) > 0$ 且 $d(x) \mid f(x)$ 与不可约矛盾. □

注:

这题说明特征零的域上的不可约多项式是可分的 (教材 3.3 节).

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

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n \in \mathbb{F}_2[x]$$

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

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

因此

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

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. □

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

(1) 映射

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

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 $\overline{f}(x)$ 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 $\overline{f} = \overline{g}\overline{h}$, 且 $\overline{g}$ 和 $\overline{h}$ 还是首一的次数大于 0 的多项式, 这和 $\overline{f}$ 不可约矛盾.

$\square$

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

proof

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

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

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 R-代数同态 (即要保持加法, 数乘和乘法)$\psi_u : R[x] \to A$ 使得图表交换:

$$\begin{tikzcd}
R[x] \arrow[rr, "\exists!\psi_u"] & & A \\
& \{1\} \arrow[ul, "i"] \arrow[ur, "f_u"'] &
\end{tikzcd}$$

其中 $i : \{1\} \to R[x]$, $1 \mapsto x$.
这个映射 ψ_u 的存在性实际上题干已经给出了,

$$\begin{aligned}
&\psi_u : R[x] \to A, \\
&f(x) = a_n x^n + \cdots + a_1 x + a_0 \mapsto \psi(a_n)u^n + \cdots + \psi(a_1)u + \psi(a_0)
\end{aligned}$$

我们只需验证这个映射确实是一个环同态即可, 其中保持加法只用到环的分配律, $\psi_u(1) = 1$ 也是平凡的, 而保持乘法需要条件 $\psi(R) \subseteq C(A)$, 这实际上在2.1.8的注记里已经证明. 这里重新按多项式写一遍, 设 $f(x) = a_n x^n + \cdots +$

a_1x+a_0, $g(x)=b_mx^m+\cdots+b_1x+b_0$. 那么

$$\psi_u(f(x)\cdot g(x))=\psi\left(\sum_{k=0}^{n+m}\sum_{i+j=k}a_ib_jx^k\right)=\sum_{k=0}^{n+m}\sum_{i+j=k}\psi(a_i)\psi(b_j)u^k.$$

$$\psi_u(f(x))\cdot\psi_u(g(x))=\left(\sum_{i=0}^{n}\psi(a_i)u^i\right)\cdot\left(\sum_{j=0}^{m}\psi(b_j)u^j\right)=\sum_{i=0}^{n}\sum_{j=0}^{m}\psi(a_i)u^i\psi_(b_j)u^j$$

因为 $\psi(R)\subseteq C(A)$, 所以才有 $u\psi(b_j)=\psi(b_j)u$, 那么第二个式子的结果才能和第一个是一样的.

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. 更详细的说, 设 $\widetilde{\psi}_u$ 是另一个环同态使得图表交换, 那么按定义必须有 $\widetilde{\psi}_u(x)=u,\widetilde{\psi}_u(a)=\psi(a),\forall a\in R$, 那么根据同态的定义, $\widetilde{\psi}_u(f(x))=\widetilde{\psi}_u(a_nx^n+\cdots+a_0)=\widetilde{\psi}_u=\psi(a_n)u^n+\cdots+\psi(a_0)=\psi_u(f(x))$. □

注:

这里 $\{1\}$ 可以换成任意集合 S

$$\begin{tikzcd}
R[S] \arrow[rr, "\exists!\psi_u"] & & A \\
& S \arrow[ul, "i"] \arrow[ur, "f_u"'] &
\end{tikzcd}$$

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

需要注意的是, 这里没有要求 R 是交换的, 实际上不太好, R 不交换的话则一般就有 $fg\neq gf$. R 不交换的话 $R[x]$ 就只是多项式环了, 一般不认为是一个 R-代数, 因此本题可以认为是一个条件稍弱的版本, 条件最弱的版本是2.4.5.

教材引理 2.3.2 是这个的推论.

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" $\Longrightarrow$ " 的方向.

记 $f(x)=\sum\limits_{k=0}^{n}a_kx^k$, 设存在 $g(x)=\sum\limits_{k=0}^{m}b_kx^k\neq 0$ 使得 $fg=0$, 并要求 $g(x)$ 是次数最低的. 考虑最高次项, $a_nb_m=0$. 那么 $a_ng(x)$ 是一个比 $g(x)$ 次数更小的多项式且 $f(x)(a_ng(x))=a_nf(x)g(x)=0$. 因此 $a_ng(x)=0$, 从而 $a_nb_k=0,0\leqslant k\leqslant m$. 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 $a_ib_m=0,\forall i$ 且 $b_m\neq 0$, 因此 $b_mf(x)=0$.

□

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. □

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

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

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 $f(x)=\dfrac{p(x)}{q(x)}$, $p,q\in\mathbb{R}[x]$, $q\neq 0$, $(p,q)=1$. 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:

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

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 $\dfrac{a_n}{b_n}\notin\mathbb{Z}$, 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 $\dfrac{a_n}{b_n}\in\mathbb{Z}$, 则可以得到 m 足够大时都有 $f(m)=\dfrac{a_n}{b_n}=k\in\mathbb{Z}$, 即

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

则可得 $a_nb_i=a_ib_n$, $i=0,1,\cdots,n-1$, 即 $\dfrac{a_i}{b_i}=\dfrac{a_n}{b_n}=k$. 因此 $f(x)=\dfrac{a_n}{b_n}$ 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 $f(x)=s(x)+\dfrac{r(x)}{q(x)}$, 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 $\deg(\Delta_1 f)<\deg(f)$(其中 $s(x)$ 会消去最高次项, 而 $\dfrac{r(x)}{q(x)}$ 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 $f(x)=c_nx^n+\cdots+c_0$, 任意选择 $n+1$ 个不同整数 $m_0,m_1,\cdots,m_n$ 带入得到一个关于 $a_0,a_1,\cdots,a_n$ 的整系数线性方程组 $\sum\limits_{k=0}^{n} m_i^k a_k=b_i$, $i=0,1,\cdots,n$, 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. □

习题 2.4　教材 p48-p49

2.4.1　设 F 是一个域, $R=F[x_1,x_2,\cdots,x_n]$, 令 $R_m\subseteq R$ 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

$$f=\sum_{i_1+i_2+\cdots+i_n=m} a_{i_1i_2\cdots i_n}x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}$$

$a_{i_1i_2\cdots i_n}\in F$ 允许为 0, $i_k\geqslant 0, 1\leqslant k\leqslant n$. 那么 f 的表达式中共有 $\binom{m+n-1}{m}$ 项. 记 $N=\binom{m+n-1}{m}$, $I=\{(i_1,i_2,\cdots,i_n)\in\mathbb{N}^n\mid i_1+i_2+\cdots+i_n=m\}$. 因此映射

$$R_m\to F^N,\quad f\mapsto(a_{i_1i_2\cdots i_n})_{(i_1,i_2,\cdots,i_n)\in I}$$

是 (线性) 同构. □

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

proof

" $\Longrightarrow$ " 这个方向提出公因式 t^m 即可, 下证" $\Longleftarrow$ ":
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

$$f(tx_1,tx_2,\cdots,tx_n)=f_0(x_1,\cdots,x_n)+tf_1(x_1,\cdots,x_n)+\cdots+t^kf_k(x_1,\cdots,x_n)$$

这是一个 $F[x_1,x_2,\cdots,x_n]$ 上的关于 t 的多项式. 若有 $f(tx_1,tx_2,\cdots,tx_n)=$

$t^m f(x_1, x_2, \cdots, x_n)$, 对比系数知 $f = f_m$. □

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

" $\Longrightarrow$ " 的部分按定义直接验证, 下证" $\Longleftarrow$ ":
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. □

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

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

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

从而

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

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

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

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

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

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

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 $u_1, u_2, \cdots, u_n$, 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

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

就是环同态. 交换的条件是用在保持乘法上, 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 $u_1, \cdots, u_n$, ψ_u 都是同态, 才能说 A 是一个 R-代数. □

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 $R = M_n(K)$, $\psi : R \to R$ 是恒等映射, 则取值映射 $\psi_u : R[x] \to A$ 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 自然是是同构. ψ_u 的存在唯一性是用了2.4.5. 这里 ψ 实际上是包含 $\psi : R \to A = R[\lambda]$. 若要严格一些, 那么说明这个映射是双射即可.　实际上可以反过来用一次2.4.5. 考虑 ψ 以及 $x \in R[x]$. 得到的映射恰好为 ψ_u 的逆映射. □

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

2.4.8　设 K 是一个域, $M_m(K)$ 是 m-阶矩阵环, $\psi : K \to M_m(K)$ 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 $\psi_u : K[x_1, x_2] \to M_m(K)$, $f(x_1, x_2) \mapsto f(A, B)$, 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 $f(x_1, x_2) = x_1 x_2 = x_2 x_1$ 即可. □

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, 2.4.7, 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 $\psi : R \to A$ 诱导的唯一的同态 $\psi_u : R[x] \to A$, 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

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

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.

$R[x_1, x_2, \cdots, x_n]$ 要求所有未定元 $x_1, x_2, \cdots, x_n$ 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 $R[x_1, x_2, \cdots, x_n]$ 是交换环. R 是交换环的时候, $R[x_1, x_2, \cdots, x_n]$ 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.

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

我们总可以在 $f(x)$ 的分裂域上考虑因式分解. 由2.4.3可知, a 是 $f(x)$ 和 $f'(x)$ 的公共根当且仅当 a 是 $f(x)$ 的重根. 而 $f(x)$ 和 $f'(x)$ 的公共根当且仅当是 $d(x)$ 的根, 从而 $f(x)$ 的单根为 $g(x)$ 的根. 且若 a 是 $k(>1)$ 重根, 则按定义有 $f(x) = (x-a)^k f_1(x)$, $f_1(a) \neq 0$. 那么 $f'(x) = (x-a)^{k-1}(kf_1(x) + (x-a)f_1'(x))$, 记 $h(x) = kf_1(x) + (x-a)f_1'(x)$, 有 $h(a) = kf_1(a) \neq 0$. 即有 $(x-a)^{k-1} \mid d(x)$ 但 $(x-a)^k \nmid d(x)$, 因此 $g(x)$ 有单因子 $(x-a)$, 即重根 a 是 $g(x)$ 的单根. □

3.1.2　设 $K \subseteq L$ 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

(1) 回忆2.2.6和2.3.2,

$$\ker(\psi_\alpha) = \{f \in K[x] \mid f(\alpha) = 0\}$$

是一个理想. 类似2.2.6, 有 $(\mu_\alpha(x)) \subseteq \ker(\psi_\alpha)$ 且 $(\mu_\alpha(x))$ 是极大理想 (由 $K[x]$ 是 PID, 2.3.2), 且 $\ker(\psi_\alpha) \neq K[x]$, 因此只能是 $\ker(\psi_\alpha) = (\mu_\alpha(x))$.

(2) 由2.3.2, $\overline{x}$ 为 μ_α 在扩域 $K[x]/(\mu_\alpha(x))$ 中的一个根. 那么映射

$$\varphi : K[x]/(\mu_\alpha(x)) \to K[\alpha], \quad \overline{x} \mapsto \alpha$$

是同构, 这是因为 $\psi_\alpha(K[x]) = K[\alpha] = K(\alpha)$(见注记), 那么由同态基本定理就得到同构.

□

注:

教材出现了有限生成扩张 (p7-8) 但并未单独列出这个的定义, 这里需要用一下所以先把这个定义提一下.

定义 设 $K \subseteq L$ 是一个域扩张, $S \subseteq L$ 是一个子集, $K(S)$ 称为由 F 和 S 生成的子域, 即包含 F 和 S 的最小域:

$$K(S) := \cap\{E \subseteq L \mid F \cup S \subseteq E\}$$

若 $T \subseteq L$ 是另一个子集, 则定义 $K(S)(T) := K(S \cup T)$.
若存在有限子集 S 使得 $L = K(S)$, 即存在有限个 $u_1, u_2, \cdots, u_n \in L$ 使得 $L = K(u_1, u_2, \cdots, u_n)$, 则称该扩张是有限生成的 (finitely generated).

$$K(u_1, u_2, \cdots, u_n) := \cap\{E \subseteq L \mid K \subseteq E,\ u_1, u_2, \cdots, u_n \in E\}$$

$n = 1$ 时称为单扩张 (simple extension).

下面要验证的事实是, 当 $u_1, u_2, \cdots, u_n$ 都是 K 上代数元的时候,
$K(u_1, u_2, \cdots, u_n) = K[u_1, u_2, \cdots, u_n]$, 且此时该扩张是有限扩张, 否则是无限扩张. 即对域扩张而言:

$$\text{algebraic} + \text{finitely generated} = \text{finite}$$

反过来是非常简单的, 有限扩张 $\Longrightarrow$ 代数扩张, 利用 $1, \alpha, \cdots, \alpha^n$ 线性相关即可, $n = \dim_K L$. 有限扩张 $\Longrightarrow$ 有限生成, 取一组基就行.
对任意的单扩张 $K \subseteq K(\alpha)$, 很自然的想法就是用2.3.7的赋值映射来讨论. 对包含 $K \xhookrightarrow{i} K(\alpha)$ 用泛性质, 存在唯一的同态

$$\psi_\alpha : K[x] \to K(\alpha), \quad f(x) \mapsto f(\alpha).$$

由同态基本定理, $K[x]/\ker(\psi_\alpha) \cong \psi_\alpha(K[x]) = K[\alpha] \subseteq K(\alpha)$. 由于 $K(\alpha)$ 按定义是域, 因此是整环. 而 $K[\alpha]$ 是子环, 从而也是整环, 因此 $\ker(\psi_\alpha)$ 是素理想. 而 $K[x]$ 是一个 PID, 因此只有两种情况.

Case 1 $\ker(\psi_\alpha) = \{0\}$, 此时 ψ_α 是单射. 这意味着 $\{f(x) \in K[x] \mid f(\alpha) = 0\} = \{0\}$, 即零多项式是唯一使得 $f(\alpha) = 0$ 的多项式, 换言之 α 是 K 上的超越元. 注意 $K(x)$ 是 $K[x]$ 的分式域, 由分式域 (或者说 localization) 的泛性质 (单独放在后面), 存在唯一的同态使得图表交换:

$$\begin{tikzcd} K(x) \arrow[rr, "\varphi_\alpha"] & & K(\alpha) \\ & K[x] \arrow[ul] \arrow[ur, "\psi_\alpha"'] & \end{tikzcd}$$

即

$$\varphi_\alpha : K(x) \to K(\alpha), \quad \frac{p(x)}{q(x)} \mapsto \frac{p(\alpha)}{q(\alpha)}$$

这是一个单射 (因为 $K(x)$ 是域). 考虑 φ_α 的像, 它一定是一个域, 且包含 K 和 α, 因此按定义就有 $K(\alpha) \cong \varphi_\alpha(K(x)) \cong K(x)$, 那么 $K \subseteq K(\alpha)$ 扩张次数为无穷 ($1, \alpha, \alpha^2, \cdots$ 线性无关). 如 $\mathbb{Q}(\pi) \cong \mathbb{Q}(x)$.

Case 2 $\ker(\psi_\alpha) = (p(x))$, $p(x)$ 是一个不可约多项式. 注意到 $\alpha = \psi_\alpha(x)$, 此时 $K[\alpha] = \psi_\alpha(K[x]) \cong K[x]/(p(x))$ 是包含 α 的域, 而根据 ψ_α 的构造, $K[\alpha] \subseteq K(\alpha)$, 由 $K(\alpha)$ 的定义, 只能是 $K[\alpha] = K(\alpha) \cong K[x]/(p(x))$. 此时是有限扩张, 扩张次数为 $\deg(p(x))$, 且 $p(x)$ 和 α 的极小多项式 $\mu_\alpha(x)$ 是相伴的 ($(p(x)) = (\mu_\alpha(x))$, 即就差一个常数, $p(x)$ 除掉首项系数就是 $\mu_\alpha(x)$). 在这个域同构下 $\overline{x} \in K[x]/(p(x))$ 的像就是 α, 这就是为什么2.3.2在最后提到, $\overline{x}$ 是多项式 $p(x)$ 在扩域 $K[x]/(p(x))$ 上的根.

多元的情形由归纳法即可,

$$\begin{aligned} K(u_1, u_2, \cdots, u_n) &= K(u_1, u_2, \cdots, u_{n-1})(u_n) = K[u_1, u_2, \cdots, u_{n-1}](u_n) \\ &= K[u_1, u_2, \cdots, u_{n-1}][u_n] = K[u_1, u_2, \cdots, u_n] \end{aligned}$$

, 且

$$\begin{aligned} &[K[u_1, u_2, \cdots, u_n] : K] \\ &\quad = [K[u_1, u_2, \cdots, u_n] : K[u_1, u_2, \cdots, u_{n-1}]] \cdot [K[u_1, u_2, \cdots, u_{n-1}] : K] < \infty. \end{aligned}$$

值得注意的是多元的时候, 这里只是说明可以由 $u_1, u_2, \cdots, u_n$ 通过多项式生成, 但仍有可能由更少的代数元生成, 如1.1.3, $\mathbb{Q}$ 加上 $\sqrt{2}$ 和 $\sqrt{3}$ 后仍是一个单扩张. 又比如 $\mathbb{Q}[\sqrt{2}, \sqrt[4]{2}] = \mathbb{Q}[\sqrt[4]{2}]$.
上面提到的 localization 可以理解成分式域的推广. 设 A 是交换环, $S \subseteq A$ 是一个乘法封闭子集 (multiplicatively closed subset), 即 $\forall s, t \in S \implies st \in S$ 并要求 $1 \in S$. 换句话说, S 是 $(A, \cdot)$ 的一个子幺半群. 则 $A \times S$ 上有一个等价关系:

$$(a, s) \sim (a', s') \iff \exists t \in S, (as' - a's)t = 0$$

记商集 $A \times S/\sim$ 为 $S^{-1}A$, 可以验证这是一个环, A 是它的子环, 称为 A 对 S 的分式环. 它是包含 A 的并使得 S 中元素都可逆的“最小”的环. 这个构造通常称为环的局部化 (localization). 当 A 是整环且取 $S = A \setminus \{0\}$ 时就是分式域, 如 $\mathbb{Q}$, $K(x)$. 若 $0 \in S$ 则得到零环, 因此一般尽量排除这种平凡的情况. 当 $\mathfrak{p} \subseteq A$ 是素理想时, 按素理想的定义可以验证 $S = A \setminus \mathfrak{p}$ 是乘法封闭的 (事实上反过来也是对的). 此时 $S^{-1}A$ 一般记作 $A_\mathfrak{p}$, 这是一个局部环 (2.3.1), 如 $\mathbb{Z}_p$(p-adic integers).
上述的“最小”对应它的泛性质:
$S^{-1}A$ 的元素记为 $\dfrac{a}{s}$, 我们有一个自然的同态

$$f_S : A \to S^{-1}A, \quad a \mapsto \frac{a}{1}$$

$f(s)=\dfrac{s}{1}$ 在 $S^{-1}A$ 中都是可逆的, 逆是 $\dfrac{1}{s}$. 若环同态 $\varphi: A\to B$ 满足对任意的 $s\in S$, $\varphi(s)$ 在 B 中可逆, 那么存在唯一的环同态 $\varphi_S: S^{-1}A\to B$ 使得图表交换:

$$\begin{tikzcd} S^{-1}A \arrow[rr, "\varphi_S"] & & B \\ & A \arrow[ul, "f_S"] \arrow[ur, "\varphi"'] & \end{tikzcd}$$

事实上 $\varphi_S(\dfrac{a}{s})=\varphi(a)\varphi(s)^{-1}$, 我们需要验证这个映射是良定义的, 即若 $(a,s)\sim(a',s')$, 那么要有 $\varphi(a)\varphi(s)^{-1}=\varphi(a')\varphi(s')^{-1}$. 由定义 $\exists t\in S$ 使得 $(as'-a's)t=0$, 用 φ 作用在等式两边就有 $(\varphi(a)\varphi(s')-\varphi(a')\varphi(s))\varphi(t)=0$, 根据条件 $\varphi(t)$ 可逆, 所以 $\varphi(a)\varphi(s')-\varphi(a')\varphi(s)=0$, 又 $\varphi(s),\varphi(s')$ 可逆, 则有 $\varphi(a)\varphi(s)^{-1}=\varphi(a')\varphi(s')^{-1}$ 得证. 另外还要说明这确实是一个环同态,

$$\begin{aligned}\varphi_S(\frac{a}{s}+\frac{b}{t})&=\varphi_S(\frac{at+bs}{st})=(\varphi(a)\varphi(t)+\varphi(b)\varphi(s))\varphi(s)^{-1}\varphi(t)^{-1}\\&=\varphi(a)\varphi(s)^{-1}+\varphi(b)\varphi(t)^{-1}=\varphi_S(\frac{a}{s})+\varphi_S(\frac{b}{t}).\\ \varphi_S(\frac{a}{s}\cdot\frac{b}{t})&=\varphi_S(\frac{ab}{st})=\varphi(a)\varphi(b)\varphi(s)^{-1}\varphi(t)^{-1}=(\varphi(a)\varphi(s)^{-1})(\varphi(b)\varphi(t)^{-1})\\&=\varphi_S(\frac{a}{s})\varphi_S(\frac{b}{t}).\\ \varphi_S(1)&=\varphi_S(\frac{1}{1})=\varphi(1)\varphi(1)^{-1}=1.\end{aligned}$$

注意一般情况下 f_S 不一定是单的, 事实上是非整环的情形有零因子导致的, 因此 A 是整环的时候且不考虑 $0\in S$, 等价关系 $\sim$ 简化为和分式域的情况一样, 即

$$(a,s)\sim(a',s')\iff as'=a's$$

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

利用 $u^3=u^2-u-2$ 消去次数大于 2 的项.

$$(u^2+u+1)(u^2-u)=(u^3-1)u=(u^2-u-3)u=u^2-u-2-u^2-3u=-4u-2.$$

第二个可以用形式级数处理

$$\begin{aligned}(u-1)^{-1}=\frac{1}{u-1}&=-(1+u+u^2+u^3(1+u+u^2+\cdots))\\&=-(1+u+u^2+\frac{u^2-u-2}{1-u})\\&=-(1+u^2-\frac{2}{1-u})\end{aligned}$$

因此 $\dfrac{1}{u-1} = -\dfrac{1}{3}(1+u^2)$. $\square$

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

proof

参考1.4.8, $\sqrt{3}\notin\mathbb{Q}[\sqrt{2}]$, 即不存在 $\mathbb{Q}[\sqrt{2}]$ 上的一次多项式使得 $\sqrt{3}$ 是根, 因此 x^2-3 是 $\mathbb{Q}[\sqrt{2}]$ 上的不可约多项式. 更详细的说, 若 x^2-3 在 $\mathbb{Q}[\sqrt{2}]$ 上可约, 则按定义 $x^2-3=(x-\alpha_1)(x-\alpha_2)$, 其中 $\alpha_i=a_i+b_i\sqrt{2}$, $a_i,b_i\in\mathbb{Q}$. 右边展开对比系数一样得到矛盾.
$\sqrt{3}$ 是 x^2-3 的根, 因此它是 $\sqrt{3}$ 对于 $\mathbb{Q}[\sqrt{2}]$ 的极小多项式. 从而有

$$\left[\mathbb{Q}[\sqrt{2},\sqrt{3}]:\mathbb{Q}[\sqrt{2}]\right]=\left[\mathbb{Q}[\sqrt{2}][\sqrt{3}]:\mathbb{Q}[\sqrt{2}]\right]=\deg(x^2-3)=2.$$

故

$$\left[\mathbb{Q}[\sqrt{2},\sqrt{3}]:\mathbb{Q}\right]=\left[\mathbb{Q}[\sqrt{2},\sqrt{3}]:\mathbb{Q}[\sqrt{2}]\right]\cdot\left[\mathbb{Q}[\sqrt{2}]:\mathbb{Q}\right]=4$$

$\square$

注:
对于二次多项式而言, 若能只能分解成一次多项式的乘积, 因此一个二次多项式 $f(x)\in K[x]$ 可约当且仅当它的根 $u_1,u_2\in K$.

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

注意到 $x^p-1=(x-1)(x^{p-1}+\cdots+x+1)$. 由于 $z\neq1$, 因此 z 是多项式 $\Phi_p(x)=x^{p-1}+\cdots+x+1$ 的根, 这是一个不可约多项式 (教材例 2.3.4), 从而是 z 的极小多项式. 因此 $[\mathbb{Q}[z]:\mathbb{Q}]=\deg(\Phi_p)=p-1$. $\square$

注:
这是分圆多项式中 n 为素数的情况.

3.1.6　证明:

(1) $U_n=\{z\in\mathbb{C}\mid z^n=1\}$ 是一个循环群;

(2) $z=\cos\dfrac{\pi}{6}+i\sin\dfrac{\pi}{6}$ 是 U_{12} 的一个生成元, 但 $[\mathbb{Q}[z]:\mathbb{Q}]=4$;

(3) 求 $z=\cos\dfrac{\pi}{6}+i\sin\dfrac{\pi}{6}$ 在 $\mathbb{Q}$ 上的极小多项式.

proof

(1) $\zeta_n = e^{\frac{2\pi i}{n}}$ 是 U_n 的生成元.

(2) $z = \cos\dfrac{\pi}{6} + i\sin\dfrac{\pi}{6} = e^{\frac{2\pi i}{12}} = \zeta_{12}$, 即 (1) 中提到的生成元. 而

$$\begin{aligned} x^{12}-1 &= (x^4-1)(x^8+x^4+1) \\ &= (x^2-1)(x^2+1)(x^4+x^2+1)(x^4-x^2+1) \\ &= (x-1)(x+1)(x^2+1)(x^2-x+1)(x^2+x+1)(x^4-x^2+1) \end{aligned}$$

是不可约分解, 其中 x^4-x^2+1 是 $\Phi_{12}(x)$, 它的根是 12 次本原单位根 $\zeta_{12}, \zeta_{12}^5, \zeta_{12}^7, \zeta_{12}^{11}$, $x-1$ 为 $\Phi_1(x)$, 根是 $1=\zeta_{12}^0$; $x+1$ 为 $\Phi_2(x)$, 根是 $-1=\zeta_{12}^6$; x^2+1 为 $\Phi_4(x)$, 根是 $i=\zeta_{12}^3, -i=\zeta_{12}^9$; x^2+x+1 为 $\Phi_3(x)$, 根是 $\zeta_{12}^4, \zeta_{12}^8$; x^2-x+1 为 $\Phi_6(x)$, 根是 $\zeta_{12}^2, \zeta_{12}^{10}$. 故 x^4-x^2+1 是 ζ_{12} 的极小多项式, $[\mathbb{Q}[z]:\mathbb{Q}] = \deg(\Phi_{12}(x)) = 4$.

(3) 见 (2).

□

注:

1. (1.2.9, 4.3.1) 教材循环群的定义为由一个元素生成的 (自由) 群 $\langle a\rangle = \{a^n \mid n \in \mathbb{Z}\}$, 等价的说就是和 $\mathbb{Z}/n\mathbb{Z}$ 同构的群 ($n=0$ 时为 $\mathbb{Z}$ 本身). 对于 $\mathbb{Z}/n\mathbb{Z}$ 有一个和初等数论有关的结论就是 Euler 函数 $\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$, 其中 $(\mathbb{Z}/n\mathbb{Z})^\times$ 是单位群 $U(\mathbb{Z}/n\mathbb{Z}) = \{\overline{m} \in \mathbb{Z}/n\mathbb{Z} \mid (m,n)=1\}$. 即 $\phi(n)$ 是 0 到 $n-1$ 中和 n 互素的元素个数. Fermat 小定理的推广便是
$$(a,n)=1 \implies a^{\phi(n)} \equiv 1 \pmod n$$
且有恒等式
$$n = \sum_{\substack{d\mid n\\ d>0}} \phi(d)$$
2. 易见 $U_n \cong \mathbb{Z}/n\mathbb{Z}$, U_n 中的 1 对应 $\mathbb{Z}/n\mathbb{Z}$ 中的 0, ζ_n 对应 1, 若 $(k,n)=1$, k 就是生成元, 对应 U_n 中的 $\zeta_n^k = e^{\frac{2k\pi i}{n}}$. U_n 的生成元称为 n 次本原单位根. 分圆多项式 $\Phi_n(x)$ 是 ζ_n 的极小多项式, 事实上
$$\Phi_n(x) = \prod_{0\leqslant k<n, (n,k)=1} (x-\zeta_n^k)$$
且有恒等式
$$x^n - 1 = \prod_{\substack{d\mid n\\ d>0}} \Phi_d(x)$$

因此可以递归的计算出 $\Phi_n(x)$,

$$\Phi_n(x)=\frac{x^n-1}{\prod\limits_{\substack{d\mid n\\0<d<n}}\Phi_d(x)}$$

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

由于 $K[u^2]\subseteq K[u]$, 即 $K[u^2]$ 是中间域, 设 $\mu_u(x)\in K[x]$ 是 u 的极小多项式, 则

$$\deg(\mu_u(x))=[K[u]:K]=\left[K[u]:K[u^2]\right]\cdot\left[K[u^2]:K\right]$$

是奇数. 而 u 是多项式 $x^2-u^2\in K[u^2][x]$ 的根, 因此 $\left[K[u]:K[u^2]\right]\leqslant 2$. 但由于奇数不可能有因子 2, 故 $\left[K[u]:K[u^2]\right]=1$, 即 $K[u^2]=K[u]$. $\square$

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

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

注:

按正确的记号应该是用圆括号表示生成, 见3.1.2的注记.

proof

设 $\{\alpha_1,\alpha_2,\cdots,\alpha_n\}$ 是 E_1 的一组 K-基, $\{\beta_1,\beta_2,\cdots,\beta_m\}$ 是 E_2 的一组 K-基, 并要求 $\alpha_1=\beta_1=1$(总是可以乘上一个 α_1^{-1} 或 β_1^{-1}, 而这一组元素仍是基). 只需说明 $S=\{\alpha_i\beta_j\}$ 可以生成 $E=K(E_1,E_2)=K(E_1\cup E_2)$. 按定义, 若 $e_1\in E_1,e_2\in E_2$, $e_1=\sum\limits_{i=1}^{n}k_i\alpha_i$, $e_2=\sum\limits_{j=1}^{m}l_j\beta_j$. 由于取 $\alpha_1=\beta_1=1$, 因此 $\alpha_i,\beta_j\in S$, 那么 $e_1\pm e_2,e_1e_2,e_i^{-1}$(若 e_i 不为零) 都可以由 S 生成. $\square$

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

proof

按定义说明 E 中非零元可逆即可. 设 $0\neq u\in E\subseteq L$, 则 u 在 L 上代数, 那么 $K(u)=K[u]\subseteq E$ 是域扩张, 则 $u\in K[u]$ 可逆. $\square$

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

proof

任取 $v \in E \setminus K$, 那么按定义 $v = \dfrac{p(u)}{q(u)}$, 则 $p(u) - vq(u) = 0$, 即 u 是多项式 $p(x) - vq(x) \in E[x]$ 的根. $\square$

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

注:

单扩张见3.1.2的注记, 由于3.3.14又写成单扩张了, 干脆把这里的“单纯”也改成“单”.

proof

任取 $u \in L \setminus K$, 和3.1.7的讨论类似,

$$p = [L : K] = [L : K[u]] \cdot [K[u] : K]$$

由 p 是素数, 且 $[K[u] : K] \neq 1$(因为 $u \notin K$), 可知 $[L : K[u]] = 1, [k[u] : K] = p$, 即 $L = K[u]$. $\square$

3.1.12 设域扩张 $K \subseteq L$ 满足条件:

(1) $[L : K] < +\infty$;

(2) 对任意两个中间域 $K \subseteq E_1 \subseteq L$, $K \subseteq E_2 \subseteq L$, 必有 $E_1 \subseteq E_2$ 或者 $E_2 \subseteq E_1$.

证明: $K \subseteq L$ 必为单扩张(即: 存在 $u \in L$, 使 $L = K[u]$).

proof

由3.1.2的注记, 有限扩张是有限生成代数扩张, 故存在代数元 $u_1, u_2, \cdots, u_n$, $L = K[u_1, \cdots, u_n]$, 那么 $K[u_i]$ 都是中间域, 若 $K[u_i] \subseteq K[u_j]$, 则 $K[u_i, u_j] = K[u_j][u_i] = K[u_j]$. 那么存在某个 $u \in \{u_1, \cdots, u_n\}$ 使得 $K[u] = \bigcup_{i=1}^{n} K[u_i] = K[u_1, \cdots, u_n] = L$. $\square$

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

记 $\beta = \sqrt[3]{2}$.

$$\begin{aligned}
&\alpha - 2 = \beta + \beta^2 = \beta(1 + \beta) \\
\Longrightarrow\ &(\alpha - 2)^3 = \beta^3(1 + \beta)^3 = 2(1 + 3\beta + 3\beta^2 + 2) = 6 + 6(\alpha - 2) \\
\Longrightarrow\ &\alpha^3 - 6\alpha^2 + 6\alpha - 2 = 0
\end{aligned}$$

由 Eisenstein 判别法知该多项式不可约, 故极小多项式是 x^3-6x^2+6x-2.

□

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

proof

只需说明 x^5-5 是 $\sqrt[5]{5}$ 在 K 上的极小多项式. 我们证明 $\left[\mathbb{Q}[\sqrt[3]{3},\sqrt[5]{5}]:\mathbb{Q}[\sqrt[3]{3}]\right]=5$ 即可.
由 Eisenstein 判别法容易说明 x^3-3 和 x^5-5 在 $\mathbb{Q}$ 上不可约, 从而有 $\left[\mathbb{Q}[\sqrt[3]{3}]:\mathbb{Q}\right]=3$, $\left[\mathbb{Q}[\sqrt[5]{5}]:\mathbb{Q}\right]=5$. 由于

$$\left[\mathbb{Q}[\sqrt[3]{3},\sqrt[5]{5}]:\mathbb{Q}\right]=\left[\mathbb{Q}[\sqrt[3]{3},\sqrt[5]{5}]:\mathbb{Q}[\sqrt[3]{3}]\right]\cdot\left[\mathbb{Q}[\sqrt[3]{3}]:\mathbb{Q}\right] \tag{1}$$

那么只需说明 $\left[\mathbb{Q}[\sqrt[3]{3},\sqrt[5]{5}]:\mathbb{Q}\right]=15$. 记 $\alpha=\sqrt[3]{3}$, $\beta=\sqrt[5]{5}$. 则 $\mathbb{Q}[\alpha]$ 的基为 $\{1,\alpha,\alpha^2\}$, $\mathbb{Q}[\beta]$ 的基为 $\{1,\beta,\beta^2,\beta^3,\beta^4\}$. 由3.1.8, 说明 $\{\alpha^i\beta^j\mid 0\leqslant i\leqslant 2, 0\leqslant j\leqslant 4\}$ 是 $\mathbb{Q}$-线性无关的即可, 这是比较直观的但是证明起来有点麻烦.
更好的一个技巧是还是像3.1.7一样分析 degree(该方法已在上课时提出).
注意在等式(1)中, $\left[\mathbb{Q}[\sqrt[3]{3}]:\mathbb{Q}\right]=3$. 而 $x^5-5\in\mathbb{Q}[x]\subseteq K[x]$ 且 $\sqrt[5]{5}$ 是它的根, 自然有 $\left[\mathbb{Q}[\sqrt[3]{3},\sqrt[5]{5}]:\mathbb{Q}[\sqrt[3]{3}]\right]\leqslant 5$, 那么 $\left[\mathbb{Q}[\sqrt[3]{3}]:\mathbb{Q}\right]\leqslant 15$. 另一方面也可以将 $\mathbb{Q}[\sqrt[5]{5}]$ 作为中间域, 有

$$\left[\mathbb{Q}[\sqrt[3]{3},\sqrt[5]{5}]:\mathbb{Q}\right]=\left[\mathbb{Q}[\sqrt[3]{3},\sqrt[5]{5}]:\mathbb{Q}[\sqrt[5]{5}]\right]\cdot\left[\mathbb{Q}[\sqrt[5]{5}]:\mathbb{Q}\right] \tag{2}$$

这里 $\left[\mathbb{Q}[\sqrt[5]{5}]:\mathbb{Q}\right]=5$(且 $\left[\mathbb{Q}[\sqrt[3]{3},\sqrt[5]{5}]:\mathbb{Q}[\sqrt[5]{5}]\right]\leqslant 3$). 但 3 和 5 都是 $\left[\mathbb{Q}[\sqrt[3]{3},\sqrt[5]{5}]:\mathbb{Q}\right]$ 的因子且 3 和 5 是两个素数, 因此有 $15\Big|\left[\mathbb{Q}[\sqrt[3]{3},\sqrt[5]{5}]:\mathbb{Q}\right]$, 结合上面的 $\left[\mathbb{Q}[\sqrt[3]{3}]:\mathbb{Q}\right]\leqslant 15$, 只能是 $\left[\mathbb{Q}[\sqrt[3]{3}]:\mathbb{Q}\right]=15$. 那么确实有 $\left[\mathbb{Q}[\sqrt[3]{3},\sqrt[5]{5}]:\mathbb{Q}[\sqrt[3]{3}]\right]=5$.

□

注:

3.1.4是直接证不可约得到扩张次数, 这里是用扩张次数来得到不可约. 当然这里也可以直接按定义证, x^5-5 的根是比较简单的.

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 $[L:K]=p^2$.

注:

代数无关是多元的超越, $a_1,a_2,\cdots,a_n$ 代数无关指不存在满足它们的代数方程, 即不存在多项式 $f(x_1,x_2,\cdots,x_n)\in k[x_1,x_2,\cdots,x_n]$ 使得 $f(a_1,a_2,\cdots,a_n)=0$.

proof

x, y 代数无关, 按定义 x, y 就是超越元, 根据3.1.2的注记, K 和 L 视为有理函数域处理即可. 考虑中间域 $k(x, y^p)$, 由 Eisenstein 判别法, x^p 是 $k[x^p, y^p]$ 的不可约元, 则 $t^p - x^p \in k[x^p, y^p][t]$ 是不可约多项式, 而 K 是 $k[x^p, y^p]$ 的分式域, 从而在 $K[t]$ 内也不可约 (教材推论 2.3.1). 那么 $t^p - x^p$ 是 $x \in k(x, y^p)$ 在 K 上的极小多项式. $[k(x, y^p) : K] = \deg(t^p - x^p) = p$. 同理 $[L : k(x, y^p)] = p$. 因此 $[L : K] = [L : k(x, y^p)] \cdot [k(x, y^p) : K] = p^2$. □

注:

证明过程没有用到特征 p, 因此该结论对任意域都是是对的.
另外对3.1.2多元的情况进行补充, 若 $u_1, u_2, \cdots, u_n$ 代数无关, 则由归纳法可知

$$K(u_1, \cdots, u_n) = K(u_1, \cdots, u_{n-1})(u_n) \cong K(x_1, \cdots, x_{n-1})(x_n) = K(x_1, \cdots, x_n)$$

和多元的有理函数域同构.

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

事实上正五边形是可以由尺规作图得到的, 因此 $54°$ 是可构造的, 又由于 $60°$ 是可构造的, 故 $6°$ 可构造, 进而 $3°$ 可构造. □

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 $\mathbb{Q} \subseteq L$ 的中间域使 $L = \mathbb{Q}[\zeta_{17}]$ 成为 $\mathbb{Q}$ 上的一个二次根塔.

proof

记 $\alpha = \sqrt{17}$. 根据教材 p59 页的公式, 先做二次扩张 $\mathbb{Q} \subseteq \mathbb{Q}[\alpha]$, 得到

$$\cos(\frac{2\pi}{17}) = -\frac{1}{16}+\frac{1}{16}\alpha+\frac{1}{16}\sqrt{2\alpha^2 - 2\alpha}+\frac{1}{8}\sqrt{\alpha^2 + 3\alpha - \sqrt{2\alpha^2 - 2\alpha} - 2\sqrt{2\alpha^2 + 2\alpha}}$$

那么令 $\beta = \sqrt{2\alpha^2 - 2\alpha}$, 得到 $\mathbb{Q} \subseteq \mathbb{Q}[\alpha] \subseteq \mathbb{Q}[\alpha, \beta]$. 注意到

$$\frac{\alpha}{\beta} = \frac{\alpha}{\sqrt{2\alpha^2 - 2\alpha}} = \frac{\alpha\sqrt{2\alpha^2 + 2\alpha}}{\sqrt{4\alpha^4 - 4\alpha^2}} = \frac{\sqrt{2\alpha^2 + 2\alpha}}{2 \cdot \sqrt{\alpha^2 - 1}} = \frac{1}{8}\sqrt{2\alpha^2 + 2\alpha}$$

因此有

$$\cos(\frac{2\pi}{17}) = -\frac{1}{16} + \frac{1}{16}\alpha + \frac{1}{16}\beta + \frac{1}{8}\sqrt{\alpha^2 + 3\alpha - \beta - 2 \cdot \frac{8\alpha}{\beta}}$$

那么令 $\gamma=\sqrt{\alpha^2+3\alpha-\beta-2\cdot\frac{8\alpha}{\beta}}$, 就有 $\cos(\frac{2\pi}{17})\in\mathbb{Q}[\alpha,\beta,\gamma]$. 最后只需构造 $\sin(\frac{2\pi}{17})=\sqrt{1-\cos^2(\frac{2\pi}{17})}$, 因此令 $\delta=\sqrt{1-\cos^2(\frac{2\pi}{17})}$ 即可. 那么

$$\mathbb{Q}\subseteq\mathbb{Q}[\alpha]\subseteq\mathbb{Q}[\alpha,\beta]\subseteq\mathbb{Q}[\alpha,\beta,\gamma]\subseteq\mathbb{Q}[\alpha,\beta,\gamma,\delta]=L$$

是一个二次根塔, 因为由3.1.5, $L=\mathbb{Q}[\zeta_{17}]\implies[L:K]=16=2^4$, 而 $\zeta_{17}\in\mathbb{Q}[\alpha,\beta,\gamma,\delta]$, $[\mathbb{Q}[\alpha,\beta,\gamma,\delta]:\mathbb{Q}]\leqslant 2^4$, 从而只能取等号. □

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

由于 $u_1\in E$ 是 $f(x)$ 的根, 因此在 $E[x]$ 中有分解 $f(x)=(x-u_1)f_1(x)$. 而 $\deg(f)=2$, 故只能是 $\deg(f_1)=1$, 即 $f_1=x-u_2$, $u_2\in E$ 自然是 $f(x)$ 的另一个根.

或设 $f(x)$ 的分裂域是 E', 令 f 的另一个根为 $u_2\in E'$, 则有 $u_1+u_2=a\in K\subseteq E$. 而 $u_1\in E$, 因此 $u_2\in E$, 即 $E'=E$. □

注:

若要严谨一点, 则不能在 E 中直接使用韦达定理, 因为 $u_2\in E$ 是要证的结论. 韦达定理实际上是 f 在其分裂域可以分解成一次因式的乘积 (即分裂), 再对比系数得到的结论. 而按分裂域的定义可知它是使得 f 分裂的最小扩域. 那么直接使用韦达定理是在用结论证结论. 不过由于代数闭包总存在且唯一 (见3.3.2和3.3.6), 我们总能把任意多项式分解成一次多项式的乘积, 所以直接使用事实上是没问题的.

这题也告诉我们, 二次扩张都是正规扩张.

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

教材例 3.3.4.

由于 $\mathbb{Q}\subseteq\mathbb{C}$, 而 $\mathbb{C}$ 是代数闭域, 我们可以把所有根都明确的写出来. x^3-2 的根为 $\alpha_k=\sqrt[3]{2}e^{\frac{2k\pi i}{3}}=\sqrt[3]{2}\zeta_3^k$, $k=0,1,2$, $u_1=\alpha_0$. 而 $\mathbb{Q}[u_1]\subseteq\mathbb{R}$, $\alpha_{1,2}\in\mathbb{C}\setminus\mathbb{R}$. □

注:

借此补充代数扩张的一个结论, 任何域在同构的意义下都有唯一的代数闭包. 这个结果的证明分为两部分, 一是存在性, 二是3.3.6提到的延拓.

定义　若域 K 满足任意次数大于 1 的多项式 $f(x)\in K[x]$ 在 K 中都有根, 我们称 K 是一个代数闭域. 根据教材的定义 2.4.2, K 是代数闭域等价于 $K[x]$ 中的不可约多项式都是一次多项式. 即 $f(x)$ 总能分解成一次多项式的乘积.

由定义, K 是代数闭域意味着 K 无法再做非平凡的代数扩张了. 若有代数扩张 $K\subseteq L$ 且 $[L:K]>1$, 则存在 $\alpha\in L\setminus K$ 在 K 上代数, 即存在非零多项式 $f(x)\in K[x]$ 使得 $f(\alpha)=0$, 而 K 是代数闭域, $f(x)$ 的所有根都在 K 里, 这就矛盾了. 换句话说, 代数闭域做代数扩张只能得到它自己. 反过来也是对的, 若 K 没有非平凡代数扩张, 且有次数大于 1 的不可约多项式, 那根据3.1.2就能做真代数扩张, 矛盾.

定义　设域扩张 $K\subseteq L$, 考虑所有的代数元

$$E=\{\alpha\in L\mid \alpha \text{ 在} K \text{ 上代数}\}$$

由教材的推论 3.1.1 可知 E 是一个中间域, 且 $K\subseteq E$ 是代数扩张. E 称为 K 在 L 中的 (相对) 代数闭包.

比如对于扩张 $\mathbb{Q}\subseteq\mathbb{R}$, 这里的 E 就是所有的实代数数. 把 $\mathbb{R}$ 换成 $\mathbb{C}$, E 就是所有的复代数数, 也就是 $\mathbb{Q}$ 的代数闭包, 一般用 $\overline{\mathbb{Q}}$ 表示.

相对代数闭包 E 在 L 内没有非平凡代数扩张, 即若 $E\subseteq E'\subseteq L$ 且 $E\subseteq E'$ 是代数扩张, 则 $E=E'$. 证明这个结论需要一个很基本的定理.

定理　代数扩张的代数扩张仍是代数扩张, 即代数扩张是可以传递的. [冯 09]p105, [Lan12]p228. 即对域扩张 $K\subseteq E\subseteq L$, L/K 是代数扩张 $\iff$ E/K 和 L/E 都是代数扩张.

那么 E'/E 代数, E/K 代数, 就有 E'/K 代数. 但根据 E 的定义是所有 K 上代数元构成的中间域, 因此 $E'\subseteq E$, 所以 $E'=E$.

定义　设 $K\subseteq L$ 是代数扩张, 若 L 是代数闭域, 称 L 是 K 的 (绝对) 代数闭包. 一般用记号 $\overline{K}$ 表示. (所以教材定理 3.3.2 的记号容易引起误解)

一般说代数闭包默认指绝对代数闭包.

命题　设 $K\subseteq L$ 是域扩张, L 是代数闭域, E 是 K 在 L 中的相对代数闭包, 则 $E=\overline{K}$.

只需证明这样得到的相对代数闭包是一个代数闭域, 注意到次数大于 1 的多项式 $f(x)\in E[x]\subseteq L[x]$, 而 L 是代数闭的, 因此 $f(x)=(x-\alpha_1)\cdots(x-\alpha_n)$, $\alpha_1,\cdots,\alpha_n\in L$ 在 E 上代数, 自然就在 K 上代数, 按 E 的定义就有 $\alpha_1,\cdots,\alpha_n\in E$. 从而 $f(x)\in E[x]$ 总能在 E 上分解称一次多项式的乘积.

命题　对任意域 K, 存在代数闭域 L 使得 $K\subseteq L$. [Lan12]§V.2 Theorem 2.5

若该命题成立, 那么根据上面的讨论, 任何域都存在代数闭包, 唯一性见3.3.6. 这个命题的证明是构造性的, 构造方法属于 Artin, 需要用到2.1.6注记里补充的命题. 基本的思路就是构造一个域扩张 $K\subseteq K_1$ 使得 $K[x]$ 中所有非常数多项式在 K_1 中都有至少一个根, 这个操作做可数次之后就能得到一个代数闭域. 类似2.3.2和3.1.2中说的那样, 令 $S=\{X_f\mid f\in K[x]\backslash K\}$, 即用 $K[x]$ 里的非常数多项式来编号, 得到一个无穷的未定元构成的集合, 然后考虑多项式环 $K[S]$. 此时记 $K[S]$ 的一个理想 $I=(f(X_f))_{f\in K[x]\backslash K}=\sum\limits_{f\in K[x]\backslash K}(f(X_f))$, 即所有这种形式的 $K[S]$ 里的多项式生成的理想 (2.1.6的注记), 如果商掉这个理想, 那么和2.3.2一样, $\overline{X_f}$ 就是 f 的一个根, 但 I 不一定是极大理想, 因此需要用到2.1.6注记里补充的命题 (新增加的), 即考虑 $I\subseteq\mathfrak{m}$, 其中 $\mathfrak{m}$ 是极大理想. 不过需要先验证 $I\neq(1)$, 这是容易的, 若 $I=(1)$, 意味着 $1=\sum\limits_{i=1}^{n}a_if_i(X_{f_i})$, 而这是不可能的, 因为我们可以用 n 次3.1.2得到扩张 $K\subseteq E$ 让这里的 f_i 都有根, 赋值 (这里用的是多元的2.4.5) 之后就得到 $1=0$, 矛盾. 因此这样我们得到了 $K_1=K[S]/\mathfrak{m}$. 然后做可数次 $K\subseteq K_1\subseteq\cdots\subseteq K_i\subseteq\cdots$. 最终得到的代数闭域就是 $L=\bigcup\limits_{i=1}^{\infty}K_i$.

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

proof

对 n 归纳.

$n=1$ 或 f 已经在 K 上分裂, 都有 $[L:K]=1$. 假设结论对 n 成立, 现考虑 $\deg(f)=n+1$, 且 f 在 K 上不分裂, 那么存在 f 的不可与因子 g 满足 $\deg(g)>1$(否则 f 在 K 上分裂). 设 $u\in L$ 是 $g(x)$ 的一个根, 由3.1.2, $K[u]\cong K[x]/(g(x))$ 是中间域, $[K[u]:K]=\deg(g)\leqslant\deg(f)=n+1$, 且在 $K[u][x]$ 上有分解 $f(x)=(x-u)h(x)$, $\deg(h)=n$. 由归纳假设, 此时 L 是 n 次多项式 $h(x)\in K[u][x]$ 的分裂域, 有 $[L:K[u]]\leqslant n!$, 从而 $[L:K]=[L:K[u]]\cdot[K[u]:K]\leqslant(n+1)!$. □

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

仍使用3.1.14分析 degree 的方法, x^5-2 的根为 $\sqrt[5]{2}\zeta_5^k$, $k=0,1,2,3,4$. $L=\mathbb{Q}\left[\sqrt[5]{2}\zeta_5^i\right]=\mathbb{Q}\left[\sqrt[5]{2},\zeta_5\right]$. 借助中间域 $\mathbb{Q}[\sqrt[5]{2}]$. 一方面, $\left[\mathbb{Q}[\sqrt[5]{2}]:\mathbb{Q}\right]=5$(3.1.14); 另一方面, $[\mathbb{Q}[\zeta_5]:\mathbb{Q}]=4$(3.1.5). 因此 $5,4\mid[L:\mathbb{Q}]$, 由于 $(4,5)=1$, 因此 $4\cdot5=20\mid[L:\mathbb{Q}]$, 另一方面 $x^5-2\in\mathbb{Q}[\zeta_5][x]$ 仍是 $\sqrt[5]{2}$ 的化零多项式, 又有 $[L:\mathbb{Q}]\leqslant 20$, 故 $[L:\mathbb{Q}]=20$. □

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

特征 p 的域的多项式环上 Frobenius(2.1.2) 也是成立的, 故有 $x^{p^n}-1=x^{p^n}-1^{p^n}=(x-1)^{p^n}$. 从而 x^{p^n} 在 $\mathbb{F}_p$ 上分裂, 分裂域即 $\mathbb{F}_p$. $\square$

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

proof

按分裂域定义, 存在 $\alpha_1,\alpha_2,\cdots,\alpha_m\in L$ 使得 $f(x)=c(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_m)$, 且 $L=K[\alpha_1,\cdots,\alpha_m]$. 由于 $K\subseteq E\subseteq L$, $f(x)\in K[x]\subseteq E[x]$, 将 $f(x)$ 视为 $E[x]$ 中的多项式. $f(x)$ 仍有这样的分解. 且 $L=K[\alpha_1,\cdots,\alpha_m]\subseteq E[\alpha_1,\cdots,\alpha_m]\subseteq L$, 故 L 也是 $f(x)$ 在 E 上的分裂域. 由于 $\varphi|_K=\mathrm{id}_K$, 因此 $\varphi(f(x))=f(x)$, 那么 L 也是 $f(x)$ 在 $\varphi(E)$ 上的分裂域. 由教材的定理 3.3.2, 由于 $f(x)$ 是可分多项式, 因此 $f(x)$ 在 $\varphi(E)$ 中无重根, 有 $|\{$域同构$L\xrightarrow{\psi}L\mid\psi|_E=\varphi\}|=[L:E]>0$, 即该集合非空, 那么存在同构 $\psi:L\to L$ 使得 $\psi|_E=\varphi$. $\square$

注:

接3.3.2注记, 这种延拓对代数扩张是都成立的.

命题 已知对任意域 K 存在代数闭域 L 使得 $K\subseteq L$. 记 $i_K:K\to L$ 是域嵌入, 那么对任意代数扩张 $K\subseteq E$, 存在嵌入 $i:E\to L$ 使得 $i|_K=i_K$. 若 E 是代数闭域且 $L/i_K(K)$ 是代数的, 那么 i 是同构. 因此代数闭包在同构的意义下一定唯一. 证明需要 Zorn's Lemma. [Lan12] §V.2 Theorem 2.8.

另外也可以参考 [冯 09]p136 引理 1, 这个是单代数扩张的版本, 相对简单一些, 如果只考虑有限扩张, 那么用这个版本就够了. 事实上这只是3.1.2的进一步解释, 在此基础上加了一个同构让他变成如下的交换图 (实际是教材定理 3.3.2 最后一段证明).

命题 若 $\eta:K\to K'$ 是域同构, 则根据教材引理 2.3.2, η 可以延拓成环同构 $\tilde{\eta}:K[x]\xrightarrow{\sim}K'[x]$. 设 E/K 和 E'/K' 是域扩张, $\alpha\in E$ 在 K 上代数, $\mu_\alpha(x)\in K[x]$ 是 α 的极小多项式, 那么 η 可以扩充成 $\varphi:K[\alpha]\to E'$ 当且仅当 $\tilde{\eta}(\mu_\alpha(x))$ 在 E' 中有根 α', 并且 $\alpha'=\varphi(\alpha)$, α' 的极小多项式 $\mu_{\alpha'}(x)=\tilde{\eta}(\mu_\alpha(x))$.

画成交换图就是这样:

$$
\begin{tikzcd}
 & E & E' & \\
K[x]/(\mu_\alpha(x)) \arrow[r, "\sim"] & K(\alpha) \arrow[u, phantom, sloped, "\subseteq"] \arrow[r, "\varphi"] & K'(\alpha') \arrow[u, phantom, sloped, "\subseteq"] & K'[x]/(\mu_{\alpha'}(x)) \arrow[l, "\sim"'] \\
 & K \arrow[u, hook] \arrow[r, "\eta"] & K' \arrow[u, hook] &
\end{tikzcd}
$$

按定义 $\tilde{\eta}$ 这个同构会把不可约多项式映到不可约多项式. 当延拓后的 φ 存在时, $\alpha' = \varphi(\alpha)$ 自然是不可约多项式 $\tilde{\eta}(\mu_\alpha(x))$ 的根, 因此自然时 α' 的极小多项式. 主要是反过来需要证一下, 若 $\alpha' \in E'$ 是 $\tilde{\eta}(\mu_\alpha(x))$ 的根, 这个多项式不可约, 从而是 α' 的极小多项式. 考虑如下的交换图表:

$$
\begin{tikzcd}
 & K[x] \arrow[r, "\tilde{\eta}"] \arrow[d, two heads, "\pi"] & K'[x] \arrow[d, two heads, "\pi'"] & \\
K(\alpha) \arrow[r, "\sim"] \arrow[rrr, bend right, "\varphi"'] & K[x]/(\mu_\alpha(x)) \arrow[r, "\bar{\tilde{\eta}}"] & K'[x]/(\mu_{\alpha'}(x)) \arrow[r, "\sim"] & K'(\alpha')
\end{tikzcd}
$$

注意到 $(\mu_\alpha(x)) \subseteq \ker(\pi' \circ \tilde{\eta})$, 由 quotient 的泛性质 (也就是同态基本定理的推广, 2.1.8增加的命题) 得到 $\bar{\tilde{\eta}}$, 而这是域之间的满同态, 故只能是同构, 进而得到同构 φ, 且 $\varphi|_K = \eta$. 注意根据我们 φ 的构造一定是 $\varphi(\alpha) = \alpha'$, φ 可能的个数就是 $\mu_{\alpha'}(x)$ 在 E' 中根的个数. 若这里 $\eta = \mathrm{id}_K$, 那么 φ 就是把 α 换成 $\mu_\alpha(x)$ 的其中一个根.

这也说明我们在同构的意义下考虑域扩张是可行的. 但对代数闭包而言, 不一定是有限扩张, 比如 $\overline{\mathbb{Q}}/\mathbb{Q}$.

有了代数闭包, 可分多项式的等价定义为: $f(x) \in K[x]$ 是可分的, 即 $f(x)$ 的不可约因子在 $\overline{K}$ 中 (或者说在 $f(x)$ 的分裂域中) 无重根. 这也解释了2.4.3和3.1.1的关系, 特征零的不可约多项式可分, 从而特征零的代数扩张一定是可分扩张. 按这个等价定义还可以得到: L/K 是可分扩张, E 是中间域, 则 L/E 是可分的 (3.3.10, 4.4.4).

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 $u_1 = \overline{x} \in \mathbb{Q}[x]/(x^2-2)$. 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 $u_2 = \overline{x} \in K[x]/(x^2-3)$) 是 $f(x) = (x^2-2)(x^2-3)$ 的分裂域, 且 $[L:\mathbb{Q}] = 4$.

proof

(1) K 是域是因为 (x^2-2) 是极大理想, 见3.1.2和3.1.14. x^2-3 在 K 中不可约在3.1.4已证.

(2) 根据3.1.2和 (1), $L=\mathbb{Q}[u_1,u_2]$ 是域. 且有分解 $f(x)=(x-u_1)(x+u_1)(x-u_2)(x+u_2)$, 因此 L 是 $f(x)$ 的分裂域 (3.3.1). 且有 $[L:\mathbb{Q}]=[L:K]\cdot[K:\mathbb{Q}]=2\cdot 2=4$.

□

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

考虑 x^p-c 的分裂域 E, 或者直接考虑 F 的代数闭包, 那么有分解 $x^p-c=(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_p)$. 我们证两次逆否.

" $\Longrightarrow$ " 若 x^p-c 在 F 中有根, 根据教材定义 2.4.2, x^p-c 有一次因式, 可约.

" $\Longleftarrow$ " 若 x^p-c 可约, 按定义有 $x^p-c=f(x)g(x)$, 那么不妨设 $f(x)=(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$, 其中 $0<n<p$, 那么根据 Bézout's Identity, 存在 $u,v\in\mathbb{Z}$ 使得 $nu+pv=1$. 记 $\alpha=\alpha_1\alpha_2\cdots\alpha_n\in F$(韦达定理), 注意到 α_i 都是 x^p-c 的根, $\alpha_i^p=c$. 那么 $\alpha^p=\alpha_1^p\alpha_2^p\cdots\alpha_n^p=c^n$, 从而 $\alpha^{pu}=c^{nu}$, 那么 $(\alpha^u c^v)^p=c^{nu}c^{pv}=c$. 这样 $\alpha^u c^v$ 是 x^p-c 的一个根, 且 $\alpha\in F$, 因此 $\alpha^u c^v\in F$.

□

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 $\mathrm{Gal}(K/\mathbb{Q})$, 并证明: K 是 $\mathbb{Q}$ 的正规扩张.

proof

直接带入 $\alpha=u^2-2$, 得

$$\begin{aligned}\alpha^3+\alpha^2-2\alpha-1&=u^6-6u^4+12u^2-8+u^4-4u^2+4-2u^2+4-1\\&=u^6-5u^4+6u^2-1\\&=(u^2-2u-1)^2+5u(u^2-2u-1)+6u^2-1\\&=u^4+u^3-2u^2-u\\&=u(-u^2+2u+1+u^2-2u-1)\\&=0\end{aligned}$$

因此 u^2-2 是根, 由韦达定理可知 $-u^2-u+1$ 也是根. 因此 K 是 x^3+x^2-2x-1 的分裂域, 从而是 Galois 扩张, 自然是正规扩张. 注意 x^3+x^2-2x-1 是不可约多项式 (由于是三次的, 若可约则一定有一次因式, 即意味着有根在 $\mathbb{Q}$ 里, 矛盾, 或用 Eisenstein, 因为根据教材的 2.3 节 $\mathbb{Q}$ 上的不可约等价于在 $\mathbb{Z}$ 上不可约), 故 $|\mathrm{Gal}(K/\mathbb{Q})|=[K:\mathbb{Q}]=3$, 从而 $\mathrm{Gal}(K/\mathbb{Q})=A_3$(3.4.2注记). □

注:

[Lan12]§V.3 Theorem3.3 给出了正规扩张的三个等价定义, 其中 (ii) 是用到代数闭包的:
设 L/K 是代数扩张,

(i) 若不可约多项式 $f(x)\in K[x]$ 在 L 有根, 则 $f(x)$ 所有根都在 L 中, 即 $f(x)$ 一定在 L 中分裂成一次因式的乘积.

(ii) 任意延拓后的域嵌入 $\varphi:L\to\overline{K}$ 是 L 的自同构, 即 $\varphi(L)=L$.

(iii) L 是一族 $K[x]$ 中多项式的分裂域.

(iii) 中一族多项式的分裂域的定义是教材没有的, 但其实差别不大, 仍是两条: 对一族多项式 $\{f_i(x)\}_{i\in I}$, $f_i(x)$ 在 L 上能分解成一次因式的乘积且 L 由所有 $f_i(x)$ 的所有根生成. 即最小的代数扩张使得 $f_i(x)$ 分裂. (iii) 加上3.3.6证明中提到的, 若 L/F 是正规扩张, E 是中间域, 那么 L 可以看成是 E 上一族多项式的分裂域, 则 L/E 也是正规扩张 (??, 4.4.4).

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

由3.3.1, $\mathbb{Q}[\sqrt[4]{2}]/\mathbb{Q}[\sqrt{2}]$ 是二次扩张, 从而是正规扩张. 另一方面, 和3.3.2类似, $\sqrt[4]{2}$ 在 $\mathbb{Q}$ 上的的极小多项式 x^4-2 有非实数根 $\sqrt[4]{2}i$ 的存在, 自然不是正规

扩张. □

3.3.12　设 $f(x)\in K[x]$ 不可约, $\mathrm{Char}(K)=p>0$. 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 $\mathrm{Char}(K)=0$, 且 K 包含全部 d 次单位根, 则 $K\subseteq L$ 是正规扩张.

proof

这是3.3.4的一般情况. 设 $1=\omega_0,\omega_1,\cdots\omega_{d-1}$ 是 x^d-1 的根, 根据题设, $\omega_i\in L=K[\alpha], 0\leqslant i<d$. 而 $(\omega_i\alpha)^d=\omega^d\alpha^d=1\cdot a=a$, 从而 $\omega_i\alpha\in L$ 是 x^d-a 的 d 个根. 因此按定义 L 是 x^d-a 的分裂域. 由3.3.14的注记是 Galois 扩张, 自然是正规扩张. □

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) $\mathrm{Gal}(L/K)=\{1\}$ (但 $[L:K]=p^2$);

(2) $K\subseteq L$ 有无穷多个中间域;

(3) $K\subseteq L$ 不是单扩张, 即不存在 $\alpha\in L$ 使得 $L=K[\alpha]$.

proof

这题是3.1.15的延续.

(1) 设 $\eta\in\mathrm{Gal}(L/K)$, 只需证 $\eta=\mathrm{id}_L$. 由3.3.6, x 是 K 上的代数元, 且 x 的极小多项式是 t^p-x^p, 因此 $\eta(x)$ 是多项式 t^p-x^p 的根, 而根据3.1.15, t^p-x^p 只有一个 p 重根 x, 因此 $\eta(x)=x$. 同理 $\eta(y)=y$, 从而 $\eta=\mathrm{id}_L$.

(2) 设 E 是一个非平凡中间域, 由于 $[L:K]=[L:E][E:K]=p^2$, 因此只能是 $[L:E]=[E:K]=p$. 而形如 $E_c=k(x+cy,y^p)$ 就是非平凡的中间域, 其中 $c\in K$ 而 K 是无穷域. 且 $c_1\neq c_2\implies E_{c_1}\neq E_{c_2}$. 因此有无穷多个中间域.

(3) 由 Frobenius 同态可知, $\forall\alpha\in L$, $\alpha^p\in K$, 则 $t^p-\alpha^p\in K[t]$ 是 α 的化零多项式. 从而 $[K[\alpha]:K]\leqslant p<p^2$. 因此 $K[\alpha]\neq L$.

□

注:

这题教材答案的错误比较严重, K 并不是完全域, x^p 不是 K 中任何一个元素的 p 次方, 但 L/K 确实不是一个可分扩张, x 在 K 上的极小多项式 $t^p - x^p$ 在 K 上不是可分的. 事实上教材的定理 3.3.4 已经告诉我们完全域的代数扩张一定是可分扩张, 而 L/K 是有限扩张, 自然是代数扩张, 因此教材的答案是前后矛盾的.

事实上, 完全域应该定义为任意代数扩张都是可分扩张的域, 因此包括所有特征零的域. 在完全域上取分裂域得到的扩张一定是 Galois 扩张 (教材定理 3.4.1), 这也是为什么要有完全域这个概念.

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

由3.1.5和3.1.6, $f(x)$ 的所有根构成循环群, α 是生成元, 因此按定义 $\mathbb{Q}[\alpha]$ 是 $f(x)$ 的分裂域, 由3.3.14的注记, 这是一个 Galois 扩张. $|\mathrm{Gal}(L/\mathbb{Q})| = p-1$, 而 $\alpha \mapsto \alpha^i, 1 \leqslant i \leqslant p-1$ 恰好为 $p-1$ 个 $L/\mathbb{Q}$ 的自同构. 从而 $\mathrm{Gal}(L/\mathbb{Q}) = \mathbb{F}_p^* \cong \mathbb{Z}/(p-1)\mathbb{Z}$. □

注:

用到了结论: 当 p 是素数时, $(\mathbb{Z}/p\mathbb{Z})^* \cong \mathbb{Z}/(p-1)\mathbb{Z}$. 证明这个结论需要一个命题.

命题 设 G 是 Abel 群, 若 $g \in G$ 有最大的有限阶, 则 $\forall h \in G, |h| < \infty \implies |h|\,\big|\,|g|$.

这个需要对阶进行一些分析. 按阶的定义可以得到一个常用的等式是 $|g^n| = \dfrac{|g|}{(n,|g|)} = \dfrac{[n,|g|]}{n}$, 这里 $[a,b]$ 表示两个正整数的最小公倍数. 根据这个等式可以得到, 若 $gh = hg$ 且 $(|g|,|h|) = 1$, 则 $|gh| = |g| \cdot |h|$. 下面用反证法证明这个命题.

假设 $|h| \nmid |g|$, 考虑他们的素因子分解, 那么将存在某个素数 p 使得 $|g| = p^m r, |h| = p^n s, (p,r) = (p,s) = 1, m < n$. 此时我们计算 $g^{p^m}h^s$ 的阶

$$
\begin{aligned}
|g^{p^m}| &= \frac{|g|}{(p^m,|g|)} = r, \\
|h^s| &= \frac{|h|}{(s,|h|)} = p^n, \\
(p^n, r) = 1 &\implies |g^{p^m}h^s| = |g^{p^m}||h^s| = p^n r > |g|
\end{aligned}
$$

从而和 g 有最大有限阶矛盾. (这个证明的技巧性还是挺强的, 以上都在教材 4.3

节)
有了这个命题, 由于 $(\mathbb{Z}/p\mathbb{Z})^*$ 是有限群, 从而存在这样的 g 有最大的有限阶, 我们证明 $|g|=p-1$ 即可. 一方面根据 Fermat 小定理 $g^{p-1}=1$, 因此 $|g|\leqslant p-1$; 另一方面, 任意的 $h\in(\mathbb{Z}/p\mathbb{Z})^*$ 都有 $|h|\,||g|$, 因此 $h^{|g|}=1$, 也就是说多项式 $x^{|g|}-1$ 在 $\mathbb{F}_p$ 上有 $p-1$ 个根, 那么 $|g|\geqslant p-1$. 从而只能是 $|g|=p-1$.

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

proof

该题的后半部分已在上课时讲过.
由3.3.2, $\sqrt[3]{2}$ 的极小多项式是 x^3-2, 且三个根中只有 $\sqrt[3]{2}\in L$, 根据3.3.6, 若 $\sigma\in\mathrm{Gal}(L/K)$, 则 $\sigma(\sqrt[3]{2})\in L$ 也是 x^3-2 的根, 那么只能是 $\sigma(\sqrt[3]{2})=\sqrt[3]{2}$, 从而 $\sigma=\mathrm{id}_L$.
类似3.1.14, 3.3.4, 同样的分析 degree 的操作可以得到 $[\overline{L}:K]=3\cdot 2=6$. 注意到 $\zeta_3=e^{\frac{2\pi i}{3}}=-\frac{1}{2}+\frac{\sqrt{-3}}{2}$, 因此 $\overline{L}=K[\sqrt[3]{2},\sqrt{-3}]=K[\sqrt[3]{2},\zeta_3]$, 正好是 x^3-2 的分裂域. 由3.3.14的注记, $\overline{L}/K$ 是 Galois 扩张. 此时 $\eta\in\mathrm{Gal}(\overline{L}/K)$, 对两个中间域 $K[\sqrt[3]{2}]$ 和 $K[\zeta_3]$ 分别考虑3.3.6, $\eta(\sqrt[3]{2})=\sqrt[3]{2}\zeta_3^i, i=0,1,2$, $\eta(\zeta_3)=\zeta_3^j, j=1,2$. 那么记

$$\alpha: L\to L,\ \sqrt[3]{2}\mapsto\sqrt[3]{2}\zeta_3, \zeta_3\mapsto\zeta_3,\ \beta: L\to L,\ \sqrt[3]{2}\mapsto\sqrt[3]{2},\ \zeta_3\mapsto\zeta_3^2$$

根据1.3.5可以验证 α,β 正是生成元, $\mathrm{Gal}\big(\overline{L}/K\big)\cong S_3$. 而中间域 $K[\sqrt{-3}]=K[\zeta_3]$, 根据 Galois 对应 (教材定理 3.4.2, 定理 4.4.1), $H=\mathrm{Gal}\big(\overline{L}/K[\zeta_3]\big), \overline{L}^H=K[\zeta_3]$. 那么 $\big|[G:H]\big|=\big[K[\zeta_3]:K\big]=2$, $G/H=\mathbb{Z}/2\mathbb{Z}$; $|H|=\big[\overline{L}:K[\zeta]\big]=3$, $H=A_3$. □

注:
阶数 3 以下的群是唯一的, 直接分析乘法表就行, 4 阶群有两种 (4.2.7). A_3 实际上是 3 阶的循环群, S_3 中所有偶置换显然只能是 3-循环, 用1.3.5的记号的话, A_3 就是子群 $\langle b\rangle$.

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

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

是一个子域链, 令

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

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

(1) $K_i \subseteq K_{i+1}$ 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 $\eta \cdot G_{i+1} \cdot \eta^{-1} \subseteq G_i$ 是一个子群, 且

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

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

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

$$\overline{\eta} = \eta|_{K_{i+1}} : K_{i+1} \to K_{i+1},$$

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

proof

$\square$

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

(1) " $\Longrightarrow$ ", 若 φ 是同态, 对 $\forall g, h \in G$, 有 $g^{-1}h^{-1}gh = (gh)^{-1}gh = 1$, 而 $g^{-1}h^{-1} = (hg)^{-1}$(1.3.2), 从而有 $gh = hg$.

(2) " $\Longleftarrow$ ", G 是 Abel 群则有 $(gh)^{-1} = h^{-1}g^{-1} = g^{-1}h^{-1}$. 因此 φ 是同态.

□

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

proof

即教材的推论 4.1.6.

由定义, $H \lhd G \iff \forall g \in G, gHg^{-1} = gg^{-1}H = H$. 那么我们实际上要证明的是 $\forall g \in G, gHg^{-1} \subseteq H \implies gHg^{-1} = H$. 即只需说明此时也有反向的包含. 对 $\forall h \in H, g \in G$, 考虑 $g^{-1} \in G$, 则有 $g^{-1}Hg \subseteq H$. 则 $g^{-1}hg \in H$, 即 $g^{-1}hg = h' \implies h = gh'g^{-1} \in gHg^{-1}$. 因此 $H \subseteq gHg^{-1}$. □

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 $H' \subseteq G', H = \varphi^{-1}(H') \subseteq G$ 是子群, 且包含 K.

(2) 当 φ 是满射时, $H' \mapsto \varphi^{-1}(H')$ 建立了集合

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

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

proof

类似定理 2.1.2.

(1) 注意到 $1 \in H'$ 而按定义 $K = \ker(\varphi) = \varphi^{-1}(1)$. 故有 $K \subseteq \varphi^{-1}(H')$. 验证是一个子群用1.3.12后提到的命题即可, $\forall a, b \in \varphi^{-1}(H')$,

$$\varphi(a), \varphi(b) \in H' \implies \varphi(ab^{-1}) = \varphi(a)\varphi(b)^{-1} \in H' \implies ab^{-1} \in \varphi^{-1}(H')$$

而反过来, 若 $H \subseteq G$ 是子群, $\varphi(H) \subseteq G'$ 也是子群.

注:

需要注意对于环同态 $R \xrightarrow{\varphi} R'$ 来说, $\varphi^{-1}(J)$ 是理想, 但 $\varphi(I)$ 只有当 φ 是满射时才是理想, 其中 $I \subseteq R, J \subseteq R'$ 是理想.

(2) φ 是满射时, 由同态基本定理, $G' \cong G/K$, 我们把 φ 看成商映射 $g \mapsto gK$. 由 (1), $H' \in \Gamma'$, $\varphi^{-1}(H') \in \Gamma$, 且 $\varphi^{-1}(H') = \{g \in G \mid gK \in H'\}$; $H \in \Gamma$, $\varphi(H) \in \Gamma'$, 且 $\varphi(H) = \{hK \mid h \in H\} = H/K$(把 φ 限制在 H 上, 而且 $\ker(\varphi) = K \subseteq H$, 因此按定义 $\ker(\varphi|_H)$ 仍是 K, 因此 $K \lhd H$, 商群 H/K 在这里是合理的). 我们只需说明 $H \mapsto \varphi(H)$ 和 $H' \mapsto \varphi^{-1}(H')$ 互逆, 按定义这是很简单的:

$$\begin{aligned}
&\varphi^{-1}(\varphi(H)) = \varphi^{-1}(H/K) = \{g \in G \mid gK \in H/K\} = H,\\
&\varphi(\varphi^{-1}(H')) = \varphi(\{g \in G \mid gK \in H'\}) = \{hK \mid h \in \{g \in G \mid gK \in H'\}\} = H'
\end{aligned}$$

剩下的部分使用注记中的定理来说明. 根据上面的双射, 我们设 $H' = \varphi(H) = H/K$, $H \in \Gamma$.

" $\Longrightarrow$ " 当 $H/K \lhd G' = G/K$ 时, 我们考虑商映射 $\pi' : G/K \to \dfrac{G/K}{H/K}$ 和 φ 的复合 f, 即

$$\begin{tikzcd}
G \arrow[r, two heads, "\varphi"'] \arrow[rr, bend left, "f"] & G/K \arrow[r, two heads, "\pi'"'] & \dfrac{G/K}{H/K}
\end{tikzcd}$$

注意到 $\ker(f) = \{g \in G \mid gK \in H/K\} = H$, 从而 $H \lhd G$.

" $\Longleftarrow$ " 反过来若 $H \lhd G$, 则考虑商映射 $\pi : G \to G/H$. 注意到 $K \subseteq \ker(\pi) = H$, 由注记中的商群的泛性质, 存在唯一的同态

$$\overline{\pi} : G/K \to G/H$$

且 $\ker(\overline{\pi}) = H/K = H'$, 则有 $H' \lhd G/K = G'$.

□

注:

和2.1.8一样, 群同态基本定理也要推广为商群的泛性质:

定理　设 G 是群, $H \lhd G$, 对任意的同态 $G \xrightarrow{f} G'$, 若 $H \subseteq \ker(f)$, 则存在唯

一的同态 $\overline{f}: G/H \to G'$ 使得图表交换:

$$\begin{tikzcd} G \arrow[rr, "f"] \arrow[dr, "\pi"'] & & G' \\ & G/H \arrow[ur, "\exists!\overline{f}"'] & \end{tikzcd}$$

同样的有 $\ker(\overline{f}) = \ker(f)/H$, $H = \ker(f)$ 时就是同态基本定理.

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

(1) 证明 $\overline{H}$ 是 $\overline{G}$ 的正规子群.

(2) 证明 $G/H \cong \overline{G}/\overline{H}$.

proof

这题实际上是上题的推论, 此处我们考虑的同态是商同态 $\pi: G \to G/N$.

(1) 根据4.1.3, $\overline{H} = \pi(H)$, $\overline{G} = \pi(G)$. 由于 $H \lhd G$, 所以有 $\overline{H} = \pi(H) \lhd G/N = \overline{G}$.

(2) 这里的同构实际上是在4.1.3" $\Longleftarrow$ " 的部分最后再用一下同态基本定理. 记商同态 $f: G \to G/H$, 则有 $N \subseteq H = \ker(f)$, 由商群的泛性质, 存在唯一的同态 $\overline{f}: G/N \to G/H$, 且 $\ker(\overline{f}) = H/N$, 因此有同构 $\overline{G}/\overline{H} = \dfrac{G/N}{H/N} \cong G/H$.

□

4.1.5 设 $H \subseteq G$ 是 G 的子群, $K \lhd G$, 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 $G \to G/K$, $(g \mapsto \overline{g})$ 下的像是 $(H \cdot K)/K$;

(3) $\varphi: H \to (HK)/K$, $(\varphi(h) = \overline{h})$ 的核是 $H \cap K$;

(4) φ 诱导群同构 $H/(H \cap K) \cong (HK)/K$.

proof

(1) 考虑商同态 $\pi: G \to G/K$. 注意这里前两题不一样, H 和 K 不一定有包含关系,

$$\pi(H) = \{hK \mid h \in H\} \implies \pi^{-1}(\pi(H)) = \bigcup_{h \in H} hK = HK.$$

因此 HK 是 G 的子群 (4.1.3的 (1)).

(2) 见 (1).

(3) 由 (1), 把 π 限制在 H 上, 就得到

$$\varphi: H \to (HK)/K$$

因此

$$\ker(\varphi) = \{\overline{h} = hK = \overline{1} = K \mid h \in H\} = \{h \in K \mid h \in H\} = H \cap K$$

(4) 对 (3) 中的 φ 用同态基本定理.

□

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

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

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

proof

(1) 这是教材推论 4.2.2 的直接结果, 任意置换总能写成有限个对换的乘积, 而 $(i\,j) = (1\,i)(1\,j)(1\,i)$.

(2) 由 (1), 只需证明 $(1\,3), \cdots, (1\,n)$ 都可以被 $(1\,2)$ 和 $(1\,2 \cdots n)$ 生成. 事实上 $(1\,n) = (1\,2 \cdots n)^{-1}(1\,2)(1\,2 \cdots n)$, $(1\,i) = (1\,(i+1))(i\,(i+1))(1\,(i+1))$, 且 $(i\,(i+1)) = (1\,2 \cdots n)^{-(n-i+1)}(1\,2)(1\,2 \cdots n)^{n-i+1}, 2 < i < n$(其实就是把 i 和 $i+1$ 先移到 1 和 2 的位置上, 用 $(1\,2)$ 对换, 再移回去).

□

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

$\square$

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

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

(2) A_n 由 3-循环生成，事实上，$A_n = \langle(1\,2\,3),\ (1\,2\,4),\ \cdots(1\,2\,n)\rangle$.(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

(1) $\pi \mapsto \varepsilon_\pi$ 实际上是一个群同态 $S_n \to \{1,-1\} \cong \mathbb{Z}/2\mathbb{Z}$. 而 A_n 恰好是这个同态的 kernel.

(2) 根据提示有 $(a\,b)(c\,d) = (abc)(bcd)$，因此所有的 3-循环能生成 A_n，只需说明任意 3-循环在 $\langle(1\,2\,3),\ (1\,2\,4),\ \cdots(1\,2\,n)\rangle$ 中. 我们可以做拆解，对 $i,j,k \neq 1,2$，反复用上面的等式凑出来 $(1\,2\,m)$.

$$
\begin{aligned}
(1\,j\,k) &= (k\,1)(1\,j) = (k\,1)(1\,2)(1\,2)(2\,k)(2\,k)(1\,j) = (1\,2\,k)(1\,2\,k)(1\,j)(2\,k)\\
&= (1\,2\,k)(1\,2\,k)(1\,j)(1\,2)(1\,2)(2\,k) = (1\,2\,k)(1\,2\,k)(1\,2\,j)(1\,2\,k)
\end{aligned}
$$

同样的可以凑出

$$
(i\,j\,k) = (i\,j)(1\,j)(1\,j)(j\,k) = (1\,i\,j)(1\,j\,k)
$$

$\square$

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 $n \geqslant 5$，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

(1) 按定义验证, 若 $\pi \cdot \alpha \cdot \pi^{-1}(i) = \pi(\alpha(\pi^{-1}(i)))$. 若 $i \notin \{\pi(i_1), \pi(i_2), \cdots, \pi(i_r)\} \iff \pi^{-1}(i) \notin \{i_1, i_2, \cdots, i_r\}$, 则 $\pi(\alpha(\pi^{-1}(i))) = \pi(\pi^{-1}(i)) = i$. 反之 $i \in \{\pi(i_1), \pi(i_2), \cdots, \pi(i_r)\}$, 有 $\pi(\alpha(\pi^{-1}(i))) = \pi(\alpha(i_k)) = (\pi(i_1)\,\pi(i_2)\cdots\pi(i_r))(i)$.

(2) (1) 的推论. 若 α 是 3-循环, 任意的 $\pi \in S_n$, $\pi\alpha\pi^{-1}$ 仍是 3-循环. 具体来说, 对两个 3-循环 $\alpha_1 = (a_1\, b_1\, c_1)$ 和 $\alpha_2 = (a_2\, b_2\, c_2)$, 则令 $\pi = \begin{pmatrix} a_1 & b_1 & c_1 & \cdots \\ a_2 & b_2 & c_2 & \cdots \end{pmatrix}$ 即可.

(3) 设 $x = (i_1\, i_2\, i_3), y = (j_1\, j_2\, j_3)$. 当 $n \geqslant 5$ 时, 由 (2), 考虑

$$a_1 = \begin{pmatrix} i_1 & i_2 & i_3 & i_4 & i_5 & \cdots \\ j_1 & j_2 & j_3 & j_4 & j_5 & \cdots \end{pmatrix}, a_2 = \begin{pmatrix} i_1 & i_2 & i_3 & i_4 & i_5 & \cdots \\ j_1 & j_2 & j_3 & j_5 & j_4 & \cdots \end{pmatrix}$$

则由 (2) 可知 $k = 1, 2$ 都满足 $a_k x a_k^{-1} = y$, 但是 $a_2 = a_1(j_4, j_5)$, 即刚好差一个对换, 那么 a_1, a_2 必然一奇一偶, 因此存在 $a \in A_n$ 使得 $axa^{-1} = y$.

□

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

对于这种阶很小的群, 我们可以直接分析 4 阶群的乘法表, 这其实和数独有点像. 乘法表的每一行或每一列是不能有相同元素的, 因为左乘映射是单的 $ga = gb \implies a = b$, 右乘也一样.

设 $G = \{e, a, b, c\}$, e 是单位元. 那么首先有

$$\begin{array}{c|cccc} & e & a & b & c \\ \hline e & e & a & b & c \\ a & a & & & \\ b & b & & & \\ c & c & & & \end{array}$$

由1.3.10, G 有 2 阶元, 不妨设 $a^2 = e$, 则 $ab \neq e, a, b$, 只能是 c, ac, ba, ca 同理, 得到

$$\begin{array}{c|cccc} & e & a & b & c \\ \hline e & e & a & b & c \\ a & a & e & c & b \\ b & b & c & & \\ c & c & b & & \end{array}$$

此时若 $b^2 = e$, 则得到

$$\begin{array}{c|cccc} & e & a & b & c \\ \hline e & e & a & b & c \\ a & a & e & c & b \\ b & b & c & e & a \\ c & c & b & a & e \end{array}$$

否则 $b^2 = a$, 得到

$$\begin{array}{c|cccc} & e & a & b & c \\ \hline e & e & a & b & c \\ a & a & e & c & b \\ b & b & c & a & e \\ c & c & b & e & a \end{array}$$

第二种实际上是 $\mathbb{Z}/4\mathbb{Z}$ 是循环群, 生成元是 b 或者 c, 自然是交换群. 第一种就是题干中的克莱因 4 元群. $\square$

注:

对于阶很大的群这种方法便不适用了. 事实上若 $|G| = p^2$, 则 G 一定是 Abel 群, 其中 p 是素数. 这是共轭作用得到的分类公式的直接推论. 即教材引理 4.2.2 证明的中间结果

$$|G| = C(G) + \sum_{O(x)>1} |O(x)|, \quad |O(x)| = [G : H_x]$$

这里的 H_x 是在共轭作用 $g \cdot x = gxg^{-1}$ 下的稳定子, 又称做 x 的中心化子 (所

有和 x 交换的元素构成的子群), 和1.2.4是类似, 一般记作 $C(x)$. 这个等式的每一项都是 $|G|$ 的因子, 因此若 G 不是 Abel 群, 即 $C(G) \neq G$, 那么只能是 $|C(G)| = p$. 但这是不可能的. 因为对 $x \notin C(G)$, $|C(x)|$ 也是 p^2 的因子, 而按定义 $C(G)$ 是严格包含于 $C(x)$ 的, $C(G) \subsetneq C(x)$, 这意味着 $|C(x)| > |C(G)| = p$, 那么 $|C(x)| = p^2$, 这就矛盾了, 因为 $x \notin C(G)$, 所以 $C(x)$ 不可能等于 G.
对一般的群作用 $G \times X \to X$, X 是有限集, 教材的引理 4.5.2 事实上可以表示为分类公式 (class formula)

$$|S| = |Z| + \sum_{|O(x)|>1} [G : \mathrm{stab}(x)] = |Z| + \sum_{|O(x)|>1} |O(x)|.$$

其中 Z 称为该群作用下的不动点集, $x \in Z \iff \mathrm{stab}(x) = G \iff O(x) = \{x\}$. 若 G 是 p-群, 则有

$$|Z| \equiv |S| \mod p$$

4.2.8 找出交错群 A_4 的所有子群.

注:
这题是 Sylow 定理, 应该放到习题 4.5.

proof

$\square$

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

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

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

proof

该题在3.1.6的注记有提及. 已经指出 G 是 n 阶循环群即 $G \cong \mathbb{Z}/n\mathbb{Z}$, 因此只需证 (2), 而 (2) 是1.2.9. 因此只证 (3).
对 $\sigma \in \mathrm{Aut}(G)$, 注意到 $\sigma(\overline{m}) = m\sigma(\overline{1})$, 故可以验证映射

$$\mathrm{Aut}(G) \to U(\mathbb{Z}/n\mathbb{Z}), \quad \sigma \mapsto \sigma(\overline{1})$$

是一个群同构. 事实上只需要验证 $(\sigma_1 \circ \sigma_2)(\overline{1}) = \sigma_1(\overline{1}) \cdot \sigma_2(\overline{1})$, 这由群同态的定义得到. 而 $\sigma \in \mathrm{Aut}(G)$ 可逆, 因此 $\sigma(\overline{1}) \in \mathbb{Z}/n\mathbb{Z}$ 关于乘法可逆, 必须有

$\sigma(\bar{1}) \in U(\mathbb{Z}/n\mathbb{Z})$. □

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

任意 F^* 的有限子群 G, 设 $|G| = n$, 那么 $\forall \alpha \in G$, 有 $\alpha^n = 1$. 因此 G 是 $U_n(F)$ 的一个子群, 而循环群的子群一定是循环群. □

注:

$\mathbb{Z}$ 的子群一定是 $n\mathbb{Z}$, n 为该子群中最小的自然数. 循环群是 $\mathbb{Z}$ 的一个商群, 因此对同态 $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ 用4.1.3, 那么 $\mathbb{Z}/n\mathbb{Z}$ 的子群是某个 $d\mathbb{Z}$ 的像, 这里要求 $n\mathbb{Z} \subseteq d\mathbb{Z}$, 即 $d \mid n$. 从而该子群就是 $\langle \bar{d} \rangle$.

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: $\mathrm{Gal}(L/K)$ 同构于 $U(\mathbb{Z}/n\mathbb{Z})$ 的一个子群. 特别地, $\mathrm{Gal}(L/K)$ 总是交换群.

proof

这是分圆域的一般情形 (3.1.6), 设 $\theta \in L$ 是 n 次本原单位根, 即 $x^n - 1$ 的根, $\sigma \in \mathrm{Gal}(L/K)$. 那么 $x^n - 1 = (x-1)(x-\theta)\cdots(x-\theta^{n-1})$. 对等式两边以 σ 作用, 就有 $x^n - 1 = (x-1)(x-\sigma(\theta))\cdots(x-\sigma(\theta)^{n-1})$. 因此 $\sigma(\theta)$ 也是本原单位根, 则有同态

$$\mathrm{Gal}(L/K) \to U(\mathbb{Z}/n\mathbb{Z}) = \langle \theta \rangle, \sigma \mapsto \sigma(\theta)$$

因此 $\mathrm{Gal}(L/K)$ 同构于 $U(\mathbb{Z}/n\mathbb{Z})$ 的一个子群, 即它的像. 而交换群的子群自然是交换的. □

注:

若 K 特征零或特征 p 满足 $(p,n) = 1$, 则 $x^n - 1$ 是可分多项式, 因此无重根, 此时单位根群 $U_n(K) \cong \mathbb{Z}/n\mathbb{Z}$. 这时有

$$\mathrm{Gal}(L/K) = \begin{cases} U(\mathbb{Z}/n\mathbb{Z}) & \theta \notin K, \\ \{\mathrm{id}\} & \theta \in K. \end{cases}$$

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

(1) 和3.3.2, 3.3.4类似, $E=\mathbb{Q}[\sqrt[4]{2},i](\zeta_4=i)$, $[E:\mathbb{Q}]=4\cdot 2=8$. 这是一个 Galois 扩张, 求中间域等价求 $\mathrm{Gal}(E/\mathbb{Q})$ 的子群, 记

$$\alpha: E\to E,\ \sqrt[4]{2}\mapsto\sqrt[4]{2}i,\ i\mapsto i,\ \beta: E\to E,\ \sqrt[4]{2}\mapsto\sqrt[4]{2},\ i\mapsto -i$$

那么 $\mathrm{Gal}(E/\mathbb{Q})=(\alpha,\beta\mid\alpha^4,\beta^2,\alpha\beta\alpha\beta)=D_8$(1.3.5). 根据 Sylow 定理它有 2 阶和 4 阶子群, 2 阶的有

$$\langle\beta\rangle,\langle\alpha\beta\rangle,\langle\alpha^2\rangle,\langle\alpha^2\beta\rangle,\langle\alpha^3\beta\rangle$$

4 阶的有

$$\langle\alpha\rangle,\langle\alpha^2,\beta\rangle,\langle\alpha^2,\alpha\beta\rangle$$

因此共有 8 个中间域, 按上面的顺序计算不动域 E^H 依次为

$$\mathbb{Q}[\sqrt[4]{2}],\ \mathbb{Q}[\sqrt[4]{2}(1+i)],\ \mathbb{Q}[\sqrt{2},i],\ \mathbb{Q}[\sqrt[4]{2}i],\ \mathbb{Q}[\sqrt[4]{2}(1-i)]$$

$$\mathbb{Q}[i],\ \mathbb{Q}[\sqrt{2}],\ \mathbb{Q}[\sqrt{2}i]$$

(2) $E^H/\mathbb{Q}$ 是有限可分扩张 (3.3.6的注记以及 Galois 对应), 因此和 Galois 扩张之间只差正规性, 根据 Galois 理论的基本定理, $H\lhd\mathrm{Gal}(E/\mathbb{Q})\iff E^H/\mathbb{Q}$ 正规, 因此只需找出 (1) 中正规子群对应的不动域 E^H:

$$E^{\langle\alpha^2\rangle}=\mathbb{Q}[\sqrt{2},i],E^{\langle\alpha\rangle}=\mathbb{Q}[i],E^{\langle\alpha^2,\beta\rangle}=\mathbb{Q}[\sqrt{2}],E^{\langle\alpha^2,\alpha\beta\rangle}=\mathbb{Q}[\sqrt{2}i]$$

共轭子群对应共轭域: $\mathbb{Q}[\sqrt[4]{2}(1+i)]$ 和 $\mathbb{Q}[\sqrt[4]{2}(1-i)]$, $\mathbb{Q}[\sqrt[4]{2}]$ 和 $\mathbb{Q}[\sqrt[4]{2}i]$. 因为 $\beta\langle\alpha\beta\rangle\beta^{-1}=\langle\alpha^3\beta\rangle$, $\alpha\langle\beta\rangle\alpha^{-1}=\langle\alpha^2\beta\rangle$.

□

注:

证明中的计算细节. 不动域的定义为:

$$E^H=\{x\in E\mid\sigma(x)=x,\forall\sigma\in G\}$$

而 $\mathrm{Gal}(E/\mathbb{Q})$ 中的同构一定是 $\mathbb{Q}$-线性的, 最直接的方法就是找到 E 的一组 $\mathbb{Q}$-基, 然后观察不变量, 同时注意扩张次数. 记 $a=\sqrt[4]{2}$, 可以取基为 $\{1,a,a^2=\sqrt{2},a^3,i,ai,a^2i,a^3i\}=\{e_k\},k=1,\cdots,8$.

- $H=\langle\beta\rangle$, 有 $\beta(a)=a$, $\beta(i)=-i$, 因此 $\mathbb{Q}[a,a^2,a^3]=\mathbb{Q}[a]=\mathbb{Q}[\sqrt[4]{2}]\subseteq E^H$. 又因为 $[E:E^H]=|H|=2$, 因此 $E^H=\mathbb{Q}[\sqrt[4]{2}]$.

- $H=\langle\alpha\beta\rangle$, 有 $\alpha\beta(a)=ai$, $\alpha\beta(ai)=\alpha(-ai)=a$. 因此 $\alpha\beta(a+ai)=a+ai$, $\mathbb{Q}[a(1+i)]\subseteq E^H$. 又因为 $[E:E^H]=|H|=2$, 故相等.

- $H = \langle \alpha^2 \rangle$, $\alpha(a^2) = \alpha(a)^2 = -a^2 \implies \alpha^2(a^2) = a^2$; $\alpha(i) = i$.
- ...

4.4.2 设 $K \supseteq F$ 是伽罗瓦扩张, $f(x)$ 是 $\alpha \in K$ 在 F 上的极小多项式, $g(x) = \prod_{\sigma \in \mathrm{Gal}(K/F)} (x - \sigma(\alpha))$. 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) $\mathrm{Gal}\,(\mathbb{Q}[\xi]/\mathbb{Q})$ 同构于乘法群 $\mathbb{F}_{13}^* = \mathbb{F}_{13} \setminus \{0\}$.

(2) $\big[\mathbb{Q}[\xi] : \mathbb{Q}[\alpha]\big] = 6$.

(3) 求 α 在 $\mathbb{Q}$ 上的极小多项式.

proof

(1) 3.4.1.

(2) 由3.4.1, 这是一个 Galois 扩张, $\mathbb{Q}[\alpha]$ 是中间域. 记 $\sigma_i \in \mathrm{Gal}\,(\mathbb{Q}[\xi]/\mathbb{Q})$ 是同构 $\xi \mapsto \xi^i$. 而 α 的每一项恰好是子群 $\langle \sigma_4 \rangle$ 里的元素, 也就是说 $\sigma_4(\alpha) = \alpha$. 那么根据 Galois 理论基本定理, $\mathbb{Q}[\xi]^{\langle \sigma_4 \rangle} = \mathbb{Q}[\alpha]$, $\big[\mathbb{Q}[\xi] : \mathbb{Q}[\alpha]\big] = |\langle \sigma_4 \rangle| = 6$.

(3) 由 (2) 知 $\big[\mathbb{Q}[\alpha] : \mathbb{Q}\big] = 2$, 极小多项式次数为 2, 因此计算 α^2.

$$\begin{aligned}
\alpha^2 &= 3\xi^2 + 3\xi^8 + 3\xi^6 + 3\xi^{11} + 3\xi^5 + 3\xi^7 + 2\xi^4 + 2\xi^{10} + 2\xi^3 + 2\xi + 2\xi^{12} \\
&\quad + 2\xi^9 + 6 \\
&= 3(-1 - \alpha) + 2\alpha + 6 \\
&= -\alpha + 3
\end{aligned}$$

记 $\beta = \xi^2 + \xi^5 + \xi^6 + \xi^7 + \xi^8 + \xi^{11}$. 这里使用了

$$0 = \frac{\xi^{13} - 1}{\xi - 1} = 1 + \xi + \cdots + \xi^{12} = \alpha + 1 + \beta.$$

因此 α 的极小多项式是 $x^2 + x - 3$.

□

4.4.4 设 $p > 2$ 是素数, $\xi_p = e^{\frac{2\pi i}{p}}$, ξ_{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 $\mathrm{Gal}(\mathbb{Q}(\xi_p)/\mathbb{Q}) \cong F_p^*$;

(2) 求 $\mathbb{Q}(\xi_{p^2})/\mathbb{Q}$ 的扩张次数, 并确定 $\mathrm{Gal}(\mathbb{Q}(\xi_{p^2})/\mathbb{Q})$(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

(1) 3.4.1.

(2) 由4.3.3, $\mathrm{Gal}(\mathbb{Q}(\xi_{p^2})/\mathbb{Q}) \cong U(\mathbb{Z}/p^2\mathbb{Z})$, 因此 $|\mathrm{Gal}(\mathbb{Q}(\xi_{p^2})/\mathbb{Q})| = p(p-1)$.

(3) 由 (2), $\left[\mathbb{Q}(\xi_{p^2}) : \mathbb{Q}(\xi_p)\right]\left[\mathbb{Q}(\xi_p) : \mathbb{Q}\right] = \left[\mathbb{Q}(\xi_{p^2}) : \mathbb{Q}\right] = p(p-1)$. 从而 $\left[\mathbb{Q}(\xi_{p^2}) : \mathbb{Q}(\xi_p)\right] = p$. 它是 Galois 扩张是因为 $\mathbb{Q}(\xi_{p^2})/\mathbb{Q}$ 是 Galois 扩张.

□

注:

对于 Galois 扩张 L/K, 对中间域 E 来说, L/E 总是 Galois 扩张, 这是因为 L 是 K 上可分多项式 $f(x)$ 的分裂域, 从而也能看成 $f(x) \in E[x]$ 的分裂域 (3.3.6). 对无穷 Galois 扩张而言也是对的 (3.3.6, 3.3.10), 一般的 Galois 扩张是可分正规扩张, 有限的 Galois 对应 (即教材介绍的) 是比较简单的, 对于无穷 Galois 对应则需要引入 Galois 群的 Krull 拓扑.

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 $\mathrm{Gal}(\mathbb{Q}[\xi_n]/\mathbb{Q})$;

(3) 设 $n > 2$ 为奇数, 证明 $\mathbb{Q}[\xi_n] \cap \mathbb{R} = \mathbb{Q}[\xi_n + \xi_n^{-1}]$.

proof

(1) 4.3.3, 3.1.6. $\mathbb{Q}(\xi_n)$ 是分圆多项式 $\Phi_n(x)$ 的分裂域.

(2) 4.3.3, $\mathrm{Gal}(\mathbb{Q}[\xi_n]/\mathbb{Q}) \cong U(\mathbb{Z}/12\mathbb{Z})$, 是 4 阶的克莱因群 (4.2.7), 因为 $\xi_{12} \mapsto \xi_{12}^5$ 的阶是 2.

(3) 这题要用分析...

□

习题 4.5　教材 p87-p88

习题 4.5 中除了 4.5.1 和 4.5.8, 其余都是 Sylow 定理的应用.

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

(1) 若 $G \times X \to X$, $(g, x) \mapsto g \cdot x$, 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 $\rho(g) \in \mathrm{Aut}(X)$ 且映射

$$\rho : G \to \mathrm{Aut}(X),\ g \mapsto \rho(g)$$

是群同态.

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

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

是一个群作用.

proof

(1) 由于 G 是群, g^{-1} 是存在的, 从而这里定义的左乘映射 $\rho(g)$ 自然是一个双射. 只需验证 ρ 是保持乘法的. 对 $\forall x \in X$

$$\rho(g_1 g_2)(x) = (g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x) = \rho(g_1)(\rho(g_2)(x)) = (\rho(g_1) \circ \rho(g_2))(x).$$

因此有 $\rho(g_1 g_2) = \rho(g_1) \circ \rho(g_2)$ 保持乘法, ρ 是群同态.

(2) 反过来, 若 ρ 是群同态, 则 $\rho(1) = 1$, 即 $\rho(1) = \mathrm{id}_X$. 那么对 $\forall x \in X$ 自然有 $1 \cdot x = \rho(1)(x) = \mathrm{id}_X(x) = x$. 另一方面,

$$(g_1 g_2) \cdot x = \rho(g_1 g_2)(x) = (\rho(g_1) \circ \rho(g_2))(x) = \rho(g_1)(\rho(g_2)(x)) = g_1 \cdot (g_2 \cdot x)$$

因此 $G \times X \to X$, $(g, x) \mapsto \rho(g)(x)$ 是一个群作用.

□

注:

这题是群作用的两种表述, 若看成一个群同态 $\rho : G \to \mathrm{Aut}(X)$ 则更贴近表示论的观点. 比如同态

$$\rho : G \to \mathrm{GL}(V), \quad g \mapsto \rho(g)$$

称为群 G 的一个 k-表示 (a k-representation, or a representation over field k). 其中 V 是一个 k-线性空间, $\mathrm{GL}(V)$ 为 V 上所有可逆线性变换构成的群.
一般地, 对于范畴 $\mathcal{C}$ 中的对象 X, 群 G 在 X 上的作用是群同态

$$\rho : G \to \mathrm{Aut}_{\mathcal{C}}(X)$$

此观点在模的定义中也是类似的, 见5.1.3, 即一个 R-模实际上是环 R 在 Abel 群 M 上的一个作用.

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^aq^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: $(h_1, h_2)(x) = h_2xh_1^{-1}$ 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:

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

定义了 M 的一个 R-模结构使得 M 成为一个 R-模.

proof

由5.1.3, M 是一个 R'-模, 即存在同态 $R' \to \mathrm{End}(M)$, 那么复合上 φ 就得到同态 $R \xrightarrow{\varphi} R' \to \mathrm{End}(M)$, 即 M 有一个 R-模结构, 正好是题干中的这个定义. □

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

(1) $\mathrm{Ann}(M) \subseteq R$ 是理想;

(2) 对任意理想 $I \subseteq R$, 若 $I \subseteq \mathrm{Ann}(M)$, 则 $R/I \times M \to M$, $(\overline{a}, x) \mapsto ax$, 定义了 M 的一个 R/I-模结构.

proof

(1) 直接验证, $\forall a, b \in \mathrm{Ann}(M), r \in R, x \in M$

$$(a - b)x = ax - bx = 0, (ra)x = r(ax) = r0 = 0, (ar)x = a(rx) = 0$$

(2) 我希望在这里用一下5.1.3.

M 是 R-模等价的说是有环同态

$$\eta : R \to \mathrm{End}_{\mathsf{Ab}}(M)$$

$\mathrm{End}_{\mathsf{Ab}}(M)$ 是 M 作为 Abel 群的所有群自同态构成的环. 考虑这个同态的 kernel, $r \in \ker(\eta)$, 按定义 $\eta(r) = 0$, 即 $\forall x \in M, rx = \eta(r)(x) = 0$, 也就是说 $\mathrm{Ann}(M) = \ker(\eta)$. 因此若 $I \subseteq \mathrm{Ann}(M) = \ker(\eta)$, 根据 quotient 的泛性质 (2.1.8的注记), 存在唯一的环同态 $\overline{\eta} : R/I \to \mathrm{End}_{\mathsf{Ab}}(M)$, 即 M 有一个 R/I-模结构.

□

注:

理想 $\mathrm{Ann}(M)$ 称为 M 的 annihilator, 直译过来是消去子, 即 R 中把 M 中所有元素化为零的那些元素.

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

(1) $\mathrm{End}(M)\times M\to M$, $(\varphi,x)\mapsto\varphi\cdot x:=\varphi(x)$, 是 M 的一个 $\mathrm{End}(M)$-模结构. (因此, M 是一个 $\mathrm{End}(M)$-模.)

(2) 设 R 是一个环, 则 M 有一个 R-模结构 $R\times M\to M$, $(a,x)\mapsto ax$ 的充要条件是存在环同态 $R\xrightarrow{\eta}\mathrm{End}(M)$ 使得 $ax=\eta(a)(x)$ 对任意 $a\in R,x\in M$ 成立.

proof

其中 (2) 的证明过程类似4.5.1.

(1) 由 (2), $\mathrm{End}(M)$ 的恒等映射决定了 M 有一个 $\mathrm{End}(M)$-模结构.

(2) 若 M 是 R-模, 定义

$$\eta(a):M\to M,\quad x\mapsto ax$$

首先验证 $\eta(a)\in\mathrm{End}(M)$, 即验证这是一个群同态,

$$\eta(a)(x+y)=a(x+y)=ax+ay=\eta(a)(x)+\eta(a)(y).$$

再验证 η 是环同态, $\forall a,b\in R,x\in M$,

$$\eta(a+b)(x)=(a+b)x=ax+bx=\eta(a)(x)+\eta(b)(x)$$

即 $\eta(a+b)=\eta(a)+\eta(b)$.

$$\eta(ab)(x)=(ab)x=a(bx)=\eta(a)(\eta(b)(x))=(\eta(a)\circ\eta(b))(x)$$

即 $\eta(ab)=\eta(a)\circ\eta(b)$.

$$\eta(1)(x)=1x=x$$

即 $\eta(1)=\mathrm{id}_M=1$.

反过来, 若 η 是同态, 我们定义 M 上的 R-模结构为

$$R\times M\to M,\quad (a,x)\mapsto\eta(a)(x)$$

只需验证这确实是一个 R-模结构. $\forall a,b\in R,x,y\in M$,

$$\begin{aligned}1x&=\eta(1)(x)=\mathrm{id}_M(x)=x,\\(a+b)x&=\eta(a+b)(x)=(\eta(a)+\eta(b))(x)=\eta(a)(x)+\eta(b)(x)=ax+bx,\\a(x+y)&=\eta(a)(x+y)=\eta(a)(x)+\eta(a)(y)=ax+ay,\\(ab)x&=\eta(ab)(x)=(\eta(a)\circ\eta(b))(x)=\eta(a)(\eta(b)(x))=a(bx).\end{aligned}$$

□

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

见1.2.1的注记. □

5.1.5　设 R-模 M 的模结构由环同态 $R \xrightarrow{\eta} \mathrm{End}(M)$ 确定, $\varphi \in \mathrm{End}(M)$. 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

φ 是模同态即要求它保持 R-数乘, 即 $\forall a \in R, x \in M$, $\varphi(ax) = a\varphi(x)$. 而根据5.1.3, 这里的 $ax = \eta(a)(x)$. 因此保持数乘即 $\varphi \circ \eta(a) = \eta(a) \circ \varphi$ 成立. □

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 $I \subseteq R$ 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 $M_1 \to M_2$ 必为同构.

proof

□

注:
Schur's Lemma 是研究表示论的一个常用的引理.

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

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

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

$$\overline{\varphi} : M/\ker(\varphi) \to \mathrm{Im}(\varphi),\ \overline{\varphi}(\overline{x}) = \varphi(x),$$

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, $\eta : R^n \to R^n$ 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, $e_1, e_2, \cdots, e_n \in R^n$ 是一组基. 令

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

证明:

(1) $f_1, f_2, \cdots, f_n$ 生成一个秩为 n 的子模 $K \subseteq R^n$ 的充要条件是 $\det(A) \neq 0$;

(2) $\forall \overline{x} \in R^n/K$, 则 $\det(A) \cdot \overline{x} = 0$.

proof

□

5.2.4　设 $K \subseteq \mathbb{Q}[\lambda]^3$ 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 $(\delta : R^* \to \mathbb{N})$, $A \in M_n(R)$ 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 $d_i \neq 0\,(1 \leqslant i \leqslant n)$, $\delta(b_{ji}) < \delta(d_i)$.

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 $M = R \cdot z$, $\operatorname{ann}(z) = (p)$, $p \in R$ 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 $M = R \cdot z$, $\operatorname{ann}(z) = (p^e)$, $p \in R$ 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.

[Lan12] Serge Lang. *Algebra*, volume 211. Springer Science & Business Media, 2012.

[冯 09] 冯克勤、李尚志、章璞. *近世代数引论*. 中国科学技术大学精品教材. 中国科学技术大学出版社, 2009.

[孙 22] 孙笑涛. *抽象代数*. 科学出版社, 2022.