习题课

May 27, 2022

1.关于验证集合是环, 需要验证其“加法”运算为Abel群, 去掉0元后, 其“乘法”运算为半群. 最后其“加法”和“乘法”要满足结合律. 一般情况下, 题目所给的集合一般是某个更大的环的子集, 所以这时只需证明该集合对相应的“加法”和“乘法”运算封闭即可. 例如: 书本3.1第3题, 验证环R上所有n阶上三角矩阵的集合和所有n阶对角矩阵的集合均是R上的n阶矩阵环的子环.

2.(3.1第12题) 设R 为环，如果R 中每个元素a均满足$a^2 = a$，则R 是交换环，且$a + a = 0$.

证明:

2.(3.1第12题) 设R 为环，如果R 中每个元素a均满足$a^2 = a$，则R 是交换环，且$a + a = 0$.

证明: $(a + a) = (a + a)^2 = 4a^2 = 4a = 2(a + a)$, 所以$a + a = 0$, 同时有$a = -a$. 其交换性：$a + b = (a + b)^2 = a^2 + ab + ba + b^2 = a + ab + ba + b$, 因此有$ab + ba = 0$, 从而$ab = -ba = ba$.

3.(3.1第14题) 设F是只有有限个元的域. 求证$a^{|F|} = a, \forall a \in F$.

证明:

3.(3.1第14题) 设F是只有有限个元的域. 求证$a^{|F|} = a, \forall a \in F$.

证明: $F^{\times} = F - \{0\}$ 是一个乘法群, 且有限, 所以F 中任意非零元素a均满足$a^{|F^{\times}|} = 1$, 从而$a^{|F|} = a$. 若$a = 0$, 则$a^{|F|} = a$显然成立.

4.(3.1第15题(v)) 设G 是阶不等于1的有限群，R为环，则群环$R[G]$有零因子。

证明:

4.(3.1第15题(v)) 设G 是阶不等于1的有限群，R为环，则群环$R[G]$有零因子。

证明: 因为G 是有限群, 所以$R[G]$存在非零元素

$$a = \sum_{g \in G} rg, \quad r \neq 0$$

任取R 中非零元素r', 任取G 中元素h, 则

$$r'ha = r' \sum_{g \in G} rhg = r' \sum_{g \in G} rg = r'a$$

所以

$$(r'e - r'h)a = 0$$

注意这里$\sum_{g \in G} rhg = \sum_{g \in G} rg$成立是因为等号两边均是$G$ 中所有元素乘以相同的系数再求和，所以相等.

5.(3.2第7题) 环$\mathbb{Z}/3\mathbb{Z}$与环$\mathbb{Z}/6\mathbb{Z}$的子环$2\mathbb{Z}/6\mathbb{Z}$是否同构?

证明:

5.(3.2第7题) 环$\mathbb{Z}/3\mathbb{Z}$与环$\mathbb{Z}/6\mathbb{Z}$的子环$2\mathbb{Z}/6\mathbb{Z}$是否同构?

证明: 是同构. 注意构造同构时需要把乘法单位元对应, $\mathbb{Z}/3\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}\}$ 的单位元为$\overline{1}$, $2\mathbb{Z}/6\mathbb{Z} = \{\overline{0}, \overline{2}, \overline{4}\}$ 的单位元为$\overline{4}$.

6.(3.2第12题) 设I是交换环R的一个理想,
则$\sqrt{I} = \{r \in R|$ 存在某个正整数n, 使得 $r^n \in I\}$ 是R的理想.

证明:

6.(3.2第12题) 设I是交换环R的一个理想，
则$\sqrt{I}=\{r\in R|$ 存在某个正整数n，使得 $r^n\in I\}$ 是R的理想.

证明：设$a^m, b^n\in I$, $c\in R$. 因为R 是交换环，所以$ac=ca$，从而有

$$(ac)^m=a^mc^m\in I$$

$$(a+b)^{m+n}=\sum_{i=0}^{m+n}C_{m+n}^{i}a^ib^{m+n-i}\in I$$

.

6.(3.2第12题) 设I是交换环R的一个理想,
则$\sqrt{I} = \{r \in R|$ 存在某个正整数n, 使得 $r^n \in I\}$ 是R的理想.

证明: 设$a^m, b^n \in I$, $c \in R$. 因为R 是交换环, 所以$ac = ca$, 从而有

$$(ac)^m = a^m c^m \in I$$

$$(a+b)^{m+n} = \sum_{i=0}^{m+n} C_{m+n}^{i} a^i b^{m+n-i} \in I$$

.

注意：上式中的$i \geq m$ 和$m+n-i \geq n$ 至少有一式成立。
即a^i, b^{m+n-i}中至少有一项属于I.

7. 设D 是整环, m, n是互素的正整数, $a, b \in D$, 且$a^m = b^m$和$a^n = b^n$, 则$a = b$.

证明:

7. 设D 是整环，m, n是互素的正整数，$a, b \in D$，且$a^m = b^m$和$a^n = b^n$，则$a = b$.

证明:
因为m, n互素，所以存在整数x, y，使得$xm + yn = 1$. 不妨假设$x \geq 0$, $y \leq 0$，所以$bb^{-yn} = b^{1-yn} = b^{xm} = a^{xm} = a^{1-yn} = aa^{-yn} = ab^{-yn}$，因为$D$为整环，所以$b = a$.

8.(3.3第2题)设R 是非零含幺交换环，P 是R 的真理想。则P 是素理想当且仅当：若$ab \in P$, 则$a \in P$ 或者$b \in P$.

证明:

8.(3.3第2题)设R 是非零含幺交换环，P 是R 的真理想。则P 是素理想当且仅当: 若$ab \in P$, 则$a \in P$ 或者$b \in P$.

证明: 必要性：当P是R的素理想时，如果$ab \in P$,
则$\langle a \rangle \langle b \rangle = \langle ab \rangle \subset P$ （前面等号用到了R是交换的前提条件），
所以$\langle a \rangle$或$\langle b \rangle \subset P$，从而$a$或$b \in P$。

充分性：用反证法。假设P不是素理想，即存在理想I和J，使得$IJ \subset P$ 但$I, J \not\subset P$，则存在$a \in I$，$a \notin P$和$b \in J$，$b \notin P$。
但$ab \in IJ \subseteq P$，与假设条件矛盾。

8.(3.3第2题)设R 是非零含幺交换环，P 是R 的真理想。则P 是素理想当且仅当：若$ab \in P$，则$a \in P$ 或者$b \in P$.

证明：必要性：当P是R的素理想时，如果$ab \in P$，
则$\langle a \rangle \langle b \rangle = \langle ab \rangle \subset P$ （前面等号用到了R是交换的前提条件），
所以$\langle a \rangle$或$\langle b \rangle \subset P$，从而$a$或$b \in P$。

充分性：用反证法。假设P不是素理想，即存在理想I和J，使得$IJ \subset P$ 但$I, J \not\subset P$，则存在$a \in I$，$a \notin P$和$b \in J$，$b \notin P$。
但$ab \in IJ \subseteq P$，与假设条件矛盾。

注意到：充分性证明没有用到交换性，所以对一般非交换环，题目的条件是充分条件，也可以作为判断素理想的依据。

9.(3.3第5题极大理想版) 设R, S均是有单位元的非零环，$f : R \to S$ 是环的满同态, $K = \mathrm{Ker} f$. 求证：

(i) 若P是R的极大理想且$P \supseteq K$，则$f(P)$ 也是S的极大理想。

(ii) 若Q是S的极大理想，则Q的原象$f^{-1}(Q)$是R的极大理想。

(iii) S中极大理想与R中包含K的极大理想一一对应.

证明:

9.(3.3第5题极大理想版) 设R, S均是有单位元的非零环，$f : R \to S$ 是环的满同态，$K = \mathrm{Ker} f$. 求证：
(i) 若P是R的极大理想且$P \supseteq K$，则$f(P)$ 也是S的极大理想。
(ii) 若Q是S的极大理想，则Q的原象$f^{-1}(Q)$是R的极大理想。
(iii) S中极大理想与R中包含K的极大理想一一对应.

证明: （i）第一步先说明$f(P)$是真理想，若$f(P) = S$，则$R = f^{-1}(S)$和P的元素只相差一个K中的元素，但是$K \subseteq P$，因此$P = R$，矛盾. (注：因为$K \subseteq P$，所以实际上可证$f^{-1}(f(P)) = P$)
第二步说明它是极大理想：若存在S的理想Q，使得$f(P) \subsetneqq Q \subsetneqq S$. 则可验证$f^{-1}(Q)$是$R$的理想，且类似第一步可得$P \subsetneqq f^{-1}(Q) \subsetneqq R$，与$P$是极大理想的假设矛盾.

9.(3.3第5题极大理想版) 设R, S均是有单位元的非零环，$f : R \to S$ 是环的满同态, $K = \mathrm{Ker} f$. 求证：

(i) 若P是R的极大理想且$P \supseteq K$，则$f(P)$ 也是S的极大理想。

(ii) 若Q是S的极大理想，则Q的原象$f^{-1}(Q)$是R的极大理想。

(iii) S中极大理想与R中包含K的极大理想一一对应.

证明: （i）第一步先说明$f(P)$是真理想, 若$f(P) = S$, 则$R = f^{-1}(S)$和P的元素只相差一个K中的元素, 但是$K \subseteq P$, 因此$P = R$, 矛盾. (注：因为$K \subseteq P$，所以实际上可证$f^{-1}(f(P)) = P$)

第二步说明它是极大理想：若存在S的理想Q, 使得$f(P) \subsetneqq Q \subsetneqq S$. 则可验证$f^{-1}(Q)$是$R$的理想, 且类似第一步可得$P \subsetneqq f^{-1}(Q) \subsetneqq R$, 与$P$是极大理想的假设矛盾.

（ii）先说明$f^{-1}(Q)$是真理想（略）. 若$f^{-1}(Q)$ 不是极大理想, 则存在R 的理想P，使得$f^{-1}(Q) \subsetneqq P \subsetneqq R$, 则$Q \subsetneqq f(P) \subsetneqq S$

(iii)结合（i）和（ii）可得结论。

10.(3.3第7题) 设$m \geq 2$，确定$\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$的所有素理想和极大理想.

解：

10.(3.3第7题) 设$m \geq 2$，确定$\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$的所有素理想和极大理想.

解：考虑满态射$f : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$, 用上一题结论. 因为$\mathbb{Z}$ 中素理想是极大理想, 均是形如$< p >$, 其中p 为素数. 故$\mathbb{Z}_m$的素理想为$p\mathbb{Z}/m\mathbb{Z}$, 其中p为m的素因子.

11.(3.4第2题) 设I, J是环R的两个理想. 定义环同态$f: R \to R/I \oplus R/J$, $f(f) = (r+I, r+J)$, $\forall r \in R$. 证明
(i)$\mathrm{Ker} f = I \cap J$.
(ii)f是满同态当且仅当$I + J = R$.

证明:

11.(3.4第2题) 设I, J是环R的两个理想. 定义环同态$f: R \to R/I \oplus R/J$, $f(f) = (r+I, r+J)$, $\forall r \in R$. 证明
(i)$\mathrm{Ker} f = I \cap J$.
(ii)f是满同态当且仅当$I + J = R$.

证明: (i)设$r \in \mathrm{Ker} f$, 即$(r+I, r+J) = 0$, 这等价于$r \in I \cap J$.

(ii) f 是满同态当且仅当对任意$r_1, r_2 \in R$, 存在$r \in R$ 使得$f(r) = (r+I, r+J) = (r_1 + I, r_2 + J)$.

假设f为满同态, 对任意的$r \in R$, 考虑$(r+I, J)$ 在f的原象, 不妨设$r' \in R$ 使得$f(r') = (r+I, J)$, 则$r' \in J$ 且$r - r' \in I$, 所以$r = r - r' + r' \in I + J$.

假设$I + J = R$, 设任意的$x, y \in R$, 则可固定分解$x = x_1 + x_2$, $y = y_1 + y_2$, 其中$x_1, y_1 \in I$, $x_2, y_2 \in J$. 则取$r = x_2 + y_1$, 可得$f(r) = (x_2 + I, y_1 + J) = (x + I, y + J)$.

12.(3.5第4题) 判断下列多项式在$\mathbb{Q}[x]$中是否可约. (i) $x^p + px + 1$, p为素数. (ii) $x^p - px - p + 1$, p为素数.

解:

12.(3.5第4题) 判断下列多项式在$\mathbb{Q}[x]$中是否可约. (i) $x^p + px + 1$, p为素数. (ii) $x^p - px - p + 1$, p为素数.

解: 统一记多项式为f. (1)当$p = 2$ 时，$f = (x+1)^2$ 可约.
当$p \neq 2$ 时，即p 为奇素数，令$x = y - 1$，
则$f(y-1) = (y-1)^p + p(y-1) + 1 = y^p + pyg(y) - p$, 其中$g(y)$是关于$y$的一个多项式. 则由艾森斯坦判别法知$f(y-1)$不可约.

(2)当$p = 2$ 时，$f = x^2 - 2x - 1$没有有理根，所以在$\mathbb{Q}$上不可分解，即不可约。当p 为奇素数时，设$x = y - 1$，
$f(y-1) = (y-1)^p - p(y-1) - p + 1$，恰好常数项和一次项系数均为0, 故有因式$y^2$.

13.(3.5第8题) 设D是整环但不是域，求证$D[x]$不是主理想整环.

证明:

13.(3.5第8题) 设D是整环但不是域，求证$D[x]$不是主理想整环.

证明: 设d是D中非零的不可逆元，则$\langle d,x\rangle$不是主理想。否则，设$\langle d,x\rangle=\langle f(x)\rangle$。则由$d\in\langle d,x\rangle$知$f(x)$只能是零次多项式，记为$c$。于是

$$\langle d,x\rangle=\langle c\rangle,\ c\in D$$

再由$x\in\langle c\rangle$可知c是D中的可逆元，从而$d\in\langle d,x\rangle=D[x]$。于是存在$g(x),h(x)\in D[x]$使得

$$1=dg(x)+xh(x)$$

因此$1=dg_0$，g_0是$g(x)$的常数项。这与d的选取矛盾。