模　论

林亚南

厦门大学数学科学学院，2008 年 6 月

这是在 2005-2006 学年的第三学期 (六周，每周 4 课时，其中最后一周为复习考试周) 为本科三年级开设《模论》选修课的讲稿. 2007-2008 学年的第三学期 (五周，每周 4 课时，其中最后两课时为考试) 授课时做了修改. 内容为介绍主理想整环上的有限生成模的分解定理，以及两个应用：线性变换的 Jordan 标准形理论，有限生成 Abel 群的结构定理. 假设选修的学生修过《抽象代数》课程.

课程要求：学习和掌握模与模同态的基本知识，特别是主理想整环上有限生成模的性质；掌握主理想整环上的有限生成模的分解定理内容和证明思路；理解和掌握线性变换的 Jordan 标准形新的证明方法. 通过课程学习，理解和掌握代数学研究代数系统的结构和表示的基本思路与方法. 要求及时完成作业. 完成作业后可在网站上查阅参考答案.

课程进度：§1, 2 课时；§2, 2 课时；§3, 2 课时；§4, 2 课时；§5, 4 课时；§6, 3 课时；§7, 1 课时；另外安排 2 课时的作业讨论.

参考文献：1. 龚升，线性代数五讲，科学出版社，2005 年
2. 聂灵沼，丁石孙，代数学引论，高等教育出版社，1987 年
3. T.S.Blyth, Module theory, 1976 年
4. T.W.Hungerford, Algebra, Gradute Texts in Nathematics 73, 1974 年
5. 张禾瑞，郝炳新，高等代数 (第四版), 高等教育出版社，1999 年
6. 莫宗坚，蓝以中，赵春来，代数学，北京大学出版社，1986 年

目　录

§1. 主理想整环

1.1 一些代数结构的定义

(1) 群：设 G 是一个非空集合，G 上有一个二元运算 $\circ$, 满足：

(i)(结合律) 对任意的 $a,b,c\in G$, 有 $(a\circ b)\circ c=a\circ(b\circ c)$;

(ii)(零元) 存在 $0\in G$, 使得对任意的 $a\in G$, 有 $a\circ 0=0\circ a=a$;

(iii)(逆元) 对任意的 $a\in G$ 存在 $a^{-1}\in G$, 使 $a\circ a^{-1}=a^{-1}\circ a=0$,

则称 $(G,\circ)$ 是一个 **群**.

若 $(G,\circ)$ 还满足

(iv) (交换律) 对任意的 $a,b\in G$, 有 $a\circ b=b\circ a$,

则称 $(G,\circ)$ 为 **Abel群** 或 **交换群**. 此时运算符号 $\circ$ 用 $+$ 代替，记 a^{-1} 为 $-a$.

(2) 环与理想：

设 R 是一个非空集合，在 R 上有两个二元运算 $+$ 和 $\cdot$, 满足：

(i)$(R,+)$ 是一个 Abel 群;

(ii)(结合律): 对任意的 $a,b,c\in R$ 有 $(a\cdot b)\cdot c=a\cdot(b\cdot c)$;

(iii)(分配律): 对任意的 $a,b,c\in R$ 有 $a\cdot(b+c)=a\cdot b+a\cdot c$; $(a+b)\cdot c=a\cdot c+b\cdot c$,

则称 $(R,+,\cdot)$ 是一个 (**结合**) **环**.

若环 R 还满足：

(iv)(交换律): 对任意的 $a,b\in R$ 有 $a\cdot b=b\cdot a$,

则 R 称为 **交换环**.

若 R 中有元素 1, 使得对任意的 $a\in R$ 有 $1\cdot a=a\cdot 1=a$, 则称 R 为有 **单位元**1 的环.

设 R 是一个环， R 的一个非空子集 I 称为 R 的 **理想**, 若满足：

(i) I 对 R 的加法成 Abel 子群;

(ii) 对任意的 $a\in I, b\in R$, 有 $ab\in I$ 且 $ba\in I$.

环 R 的理想 I 称为 **极大理想**, 如果不存在 R 的理想 J, 使得 $I\subsetneq J\subsetneq R$.

(3) 整环：交换环 R 中的非零元 r 称为 **零因子**, 如果存在 R 的非零元 s 使得 $sr=0$. 有单位元无零因子的交换环称为 **整环**.

(4) 除环：有单位元的环称为 **除环**, 如果所有非零元素全体对乘法成群.

(5) 域：交换的除环称为 **域**.

(6) 主理想整环

设 R 是有单位的交换环， $s_1,\cdots,s_n\in R$, 则

$$\langle s_1,s_2,\cdots,s_n\rangle:=\{a_1s_1+\cdots+a_ns_n\mid a_i\in R, 1\le i\le n\}$$

是 R 的一个理想，称为由 $s_1, s_2, \cdots, s_n$ 生成的理想. 由一个元素 a 生成的理想 $\langle a\rangle = \{ba \mid b \in R\}$ 称为 **主理想**.

每个理想都是主理想的整环称为 **主理想整环**.

本讲义总假设 R 是有单位元 1 的 (结合) 环.

1.2 主理想整环 $F[x]$

定理 1: 设 F 是域，则一元多项式环 $F[x]$ 是主理想整环.

证明: 易知 $F[x]$ 是带单位元 1, 无零因子, 可交换, 因而 $F[x]$ 是整环. 设 I 是 $F[x]$ 的理想, 设 $g(x)$ 是 I 中次数最低的首一多项式. 首先证明 $g(x)$ 是唯一的. 假设首一多项式 $h(x) \in I$, $\deg h(x) = \deg g(x)$. 则 $b(x) = g(x) - h(x) \in I$ 且 $\deg b(x) < \deg g(x)$. 若 $b(x) \neq 0$, 设 $b(x)$ 的首项为 c. 令 $b_1(x) = \frac{1}{c}b(x)$, 则 $b_1(x)$ 为 I 中首一多项式，且 $\deg b_1(x) < \deg g(x)$, 矛盾. 所以 $b(x) = 0$, 即 $g(x) = h(x)$.

下面证明 $I = \langle g(x)\rangle$. 因 I 是 $F[x]$ 的理想，而 $g(x) \in I$. 故 $\langle g(x)\rangle \subseteq I$. 设 $f(x) \in I$. 则 $f(x) = g(x)q(x) + r(x)$. 这里或者 $r(x) = 0$ 或 $\deg r(x) < \deg g(x)$. 假设 $r(x) \neq 0$. 由于 I 是理想，所以 $r(x) = f(x) - g(x)q(x) \in I$. 设 $r(x)$ 的首项系数为 d, 令 $r_1(x) = \frac{1}{d}r(x)$, 则 $r_1(x)$ 是 I 中首一多项式且 $\deg r_1(x) = \deg r(x) < \deg g(x)$. 与 $g(x)$ 的取法矛盾. 故 $r(x) = 0$. 即 $f(x) = g(x)q(x) \in \langle g(x)\rangle$. 故 $I \subseteq \langle m(x)\rangle$. □

命题 1: 设 $f_1(x), f_2(x), \cdots, f_n(x) \in F[x]$. 则

$$\langle f_1(x), f_2(x), \cdots, f_n(x)\rangle = \langle (f_1(x), f_2(x), \cdots, f_n(x))\rangle$$

这里 $(f_1(x), f_2(x), \cdots, f_n(x))$ 是 $f_1(x), \cdots, f_n(x)$ 的最大公因式.

证明: 设 $I = \langle f_1(x), f_2(x), \cdots, f_n(x)\rangle$. 由定理 1 知 $I = \langle g(x)\rangle$. 下面证明 $g(x) = [f_1(x), f_2(x), \cdots, f_n(x)]$.

(1) 因 $f_i(x) \in \langle g(x)\rangle$. 故存在 $q_i(x) \in F[x]$ 使 $f_i(x) = q_i(x)g(x)$. 所以 $g(x)|f_i(x)$, $1 \leq i \leq n$.

(2) 设 $h(x)|f_i(x)$, $1 \leq i \leq n$. 由于 $g(x) \in \langle f_1(x), f_2(x), \cdots, f_n(x)\rangle$. 故存在 $a_i(x)$, $1 \leq i \leq n$, 使 $g(x) = a_1(x)f_1(x) + a_2(x)f_2(x) + \cdots + a_n(x)f_n(x)$. 故有 $h(x)|g(x)$. 这就证明了 $g(x) = [f_1(x), f_2(x), \cdots, f_n(x)]$. □

1.3 主理想整环的素元分解定理

定义 1: 设 R 是整环.

(1) $a, b \in R$, 称 a **整除**b, 记 $a|b$, 若存在 $c \in R$ 使得 $b = ac$;

(2) $u \in R$ 称为 **可逆元**, 若存在 $v \in R$ 使得 $uv = 1$;
(3) $a, b \in R$, 称 a, b**相伴**, 若存在可逆元 u 使 $a = ub$;
(4) 非零非可逆元 $p \in R$ 称为 **素元**, 若 $p|ab$ 可导出或 $p|a$ 或 $p|b$;
(5) 非零非可逆元 $p \in R$ 称为 **不可约**, 若 $p = ab$ 可导出或 a 或 b 是可逆元.

注 1: 设 R 是整环.
(1) $u \in R$ 为可逆元 $\Leftrightarrow \langle u \rangle = R$;
(2) $r|s \Leftrightarrow \langle s \rangle \subseteq \langle r \rangle \Leftrightarrow s \in \langle r \rangle$;
(3) r, s 相伴 $\Leftrightarrow \langle r \rangle = \langle s \rangle$;
(4) 当 R 是主理想整环时, r 不可约 $\Leftrightarrow \langle r \rangle$ 是极大理想.

定理 2: 设 R 是主理想整环, $p \in R$, 则 p 是素元 $\Leftrightarrow p$ 是不可约元.

证明: 必要性. 设 p 是素元, 故 p 非零非可逆. 为证 p 是不可约元, 设 $p = ab$ 则 $p|ab$. 故或 $p|a$ 或 $p|b$. 若 $p|a$, 则 $a = pc, c \in R$. 故 $a = abc, a(1 - bc) = 0$. 因 R 是整环, $a \neq 0$. 所以 $1 - bc = 0$, 即 b 为可逆元. 同理, 若 $p|b$ 可得到 a 为可逆元. 故 p 不可约.

充分性. 设 p 是不可约元, 故 p 非零非可逆. 为证 p 是素元, 设 $p|ab$, 即 $ab \in \langle p \rangle$. 设 $p \nmid a$, 即 $a \notin \langle p \rangle$. 由于 $\langle p \rangle$ 是极大理想. 故 $\langle a, p \rangle = R$, 所以存在 $c_1, c_2 \in R$ 使 $1 = c_1 a + c_2 p$ 即 $b = c_1 ab + c_2 pb$. 由 $p|ab$, 可得 $p|b$. 故 p 是素元. $\square$

命题 2: 设 R 是主理想整环, 则对任一理想升链

$$\langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \langle a_3 \rangle \subseteq \cdots \subseteq \langle a_n \rangle \subseteq \cdots$$

存在正整数 m, 使得 $\langle a_m \rangle = \langle a_{m+i} \rangle$, $\forall i \in \mathbb{N}$.

证明: 令 $I = \bigcup_{i=1}^{\infty} \langle a_i \rangle$, 则 I 是理想. 事实上. 对 $a, b \in I$ 则 $a \in \langle a_i \rangle, b \in \langle a_j \rangle$. 不妨设 $i \leq j$, 则 $a, b \in \langle a_j \rangle$ 故 $a - b \in \langle a_j \rangle \subseteq I$. 且对 $\forall r \in R, rb \in \langle a_j \rangle \subseteq I$. 因 R 是主理想整环, 设 $I = \langle d \rangle$. 由 I 的定义, 存在 m, 使 $d \in \langle a_m \rangle$. 故 $I \subseteq \langle a_m \rangle$. 反之显然 $\langle a_m \rangle \subseteq I$. 所以 $\langle a_m \rangle = I$. 对 $\forall i \in \mathbb{N}, I = \langle a_m \rangle \subseteq \langle a_{m+i} \rangle \subseteq I$, 所以 $\langle a_m \rangle = \langle a_{m+i} \rangle, \forall i \in \mathbb{N}$. $\square$

定理 3: 设 R 是主理想整环, $0 \neq a \in R$, 则

$$a = u p_1 p_2 \cdots p_n,$$

其中 u 是可逆元, p_i 是素元, $1 \leq i \leq n$. 适当排列下标次序, 这样的分解在相伴的意义下是唯一的, 即若 $a = v q_1 q_2 \cdots q_m$, 其中 v 是可逆元, q_j 是素元, $1 \leq j \leq m$. 则 $m = n$, 且适当排列下标次序后 p_i 与 q_i 相伴, $1 \leq i \leq n$.

证明：由定理 2, 主理想整环上素元与不可约元是一致的.

分解的存在性. 设 a 为不可约元, 则存在性证毕. 若不是, 则 $a = a_1a_2$ 且 a_1, a_2 均非可逆元. 若 a_1, a_2 不可约, 存在性得证. 若不是, 不妨设 a_2 可约. 即 $a_2 = a_3a_4$, 且 a_3, a_4 均非可逆元. 这一步骤可一直进行, 得

$$a = a_1a_2 = a_1(a_3a_4) = a_1a_3(a_5a_6) = a_1a_3a_5(a_6a_7) = \cdots$$

这种分解一定在有限步后停止. 否则, 得到升链

$$\langle a\rangle \subseteq \langle a_2\rangle \subseteq \langle a_4\rangle \subseteq \langle a_6\rangle \subseteq \cdots,$$

因 a_i 均可逆, 上面理想链是真包含, 与命题 2 矛盾.

分解的唯一性. 设 $a = up_1p_2\cdots p_n$ 且 $a = vq_1q_2\cdots q_m$, 这里 u, v 是可逆元, $p_i, 1 \le i \le n, q_j, 1 \le j \le m$ 是不可约元. 对 n 做归纳法. 当 $n = 1$ 时, $a = up_1vq_1q_2\cdots q_m$, 由 p_1 是不可约元, 则 $m = 1$,p_1 与 q_1 相伴. 假设 $n-1$ 时命题成立, 考虑情况 n 时, 由 $p_1|vq_1q_2\cdots q_m$ 可得 p_1 整除某一个 q_j, 不妨设 $p_1|q_1$, 因 p_1, q_1 均为素元, 故 p_1 与 q_1 相伴, 设 $q_1 = cp_1$, 其中 c 为可逆元, 可得

$$up_2\cdots p_n = vcq_2\cdots q_m$$

由归纳假设 $n = m$, 且适当调整下标顺序后 p_i 与 q_i 相伴, $2 \le i \le n$. □

注 2: 设 R 是主理想整环, $0 \ne a \in R$, 则

$$a = up_1^{e_1}p_2^{e_2}\cdots p_m^{e_m},$$

其中 u 是可逆元, p_i 是素元, $e_i \in \mathbb{N}, 1 \le i \le m$. 这样的分解在相伴的意义下是唯一的.

推论 1: 设 $0 \ne f(x) \in F[x]$ 则 $f(x) = ap_1(x)p_2(x)\cdots p_n(x)$, 其中 $a \in F, p_i(x)$ 是首一不可约多项式, 在不考虑顺序情况下, 这一分解是唯一的. □

因为整数环是主理想整环 (习题 1), 故有

推论 2: 设 $0 \ne a \in \mathbb{Z}$, 则 $a = p_1p_2\cdots p_n$, 这里 $c = \pm 1, p_i$ 是正素数, 在不考虑顺序情况下, 这一分解是唯一的. □

附录: Zorn 引理

设 S 是一个非空集合, S 上的一个关系 "$\le$" 称为偏序关系如果满足:

(1) 反身性: $a \le a$;

(2) 反对称性: $a \le b$ 且 $b \le a$, 则有 $a = b$;

(3) 传递性： $a \leq b, b \leq c$ 则 $a \leq c$.

此时称 $(S, \leq)$ 是一个偏序集.

偏序集 S 中的元素 a 称为 S 的一个子集 $\{b_i\}_{i \in I}$ 的上界，如果 $b_i \leq a, i \in I$.

偏序集 S 中的元素 a 称为极大元，如果对 $b \in S$, $a \leq b$, 则总有 $b = a$.

Zorn 引理 设 $(S, \leq)$ 是一个偏序集. 若 S 中的任意升链 $b_1 \leq b_2 \leq \cdots \leq b_n \leq \cdots$ 都有上界，则 S 中存在极大元.

习题：

1. 证明： (1) $\mathbb{Z}$ 是主理想整环;

(2) 设 $a_1, a_2, \cdots a_n \in \mathbb{Z}$. 则 $\langle a_1, a_2, \cdots, a_n \rangle = \langle (a_1, a_2, \cdots, a_n) \rangle$, 这里 $(a_1, a_2, \cdots, a_n)$ 是 $a_1, a_2, \cdots, a_n$ 的最大公因数.

2. 证明 1.3 中注记 (1)-(4).

3. 设 R 是主理想整环. 对 $a, b \in R$, 如果 $\langle a \rangle + \langle b \rangle = \langle d \rangle$, 则 d 是 a, b 的最大公因子且存在 $c_1, c_2 \in R$, 使得 $d = c_1 a + c_2 b$.

4. 设 p, q 是整环 R 的不相伴的素元. 证明：

(1) $\langle pq \rangle = \langle p \rangle \cap \langle q \rangle$;

(2) $R/\langle pq \rangle \cong R/\langle p \rangle \oplus R/\langle q \rangle$.

5. 设 I 是环 R 的一元多项式环 $R[x]$ 的理想. 记 J_i 是 I 中所有 i 次多项式的首项系数与 0 构成的集合. 求证：

(1) J_i 是 R 的理想， $i \in \mathbb{Z}$;

(2) 存在 R 的理想链 $J_0 \subseteq J_1 \subseteq J_2 \subseteq \cdots \subseteq J_n \subseteq \cdots$.

6. 证明：设 R 是有单位元的交换环， $p \in R$, 则 p 是素元的充分必要条件是 $\langle p \rangle$ 是极大理想.

7. 证明：设 R 是有单位元的交换环， I 是 R 的理想，则商环 R/I 是域的充分必要条件为 I 是 R 的极大理想.

8. 设 V 是域 F 上线性空间， V 的一个非空向量组 A(可能是有限集或无限集)成称为线性无关的，如果 A 中的任意有限个向量都是线性无关的． V 的一个非空向量组 A 称为 V 的一个基，如果 A 线性无关并且 V 中的任意向量均可由 A 中有限个向量线性表示．用 Zorn 引理证明：域 F 上线性空间必存在基.

9. 用 Zorn 引理证明：任意有单位元的环一定有极大理想.