抽象代数复习指南

1^{th} Edition, 2021 年 12 月 14 日

前言

开坑时间:2021.12.11.

本篇为复习资料, 顺便试用一下新模板.

有问题可随时联系我, 知乎:Infty

考试比我写过的随笔简单很多, 这篇复习资料不太清楚的地方, 只需稍作思考就能明白.

更多内容可以参考我的随笔.

给兄弟征婚:qq 号 1747330735, 本人长相为封面 logo

写在随笔前言的内容依旧贴在这里, 以菲尔兹奖得主的经历送给所有读者:

” 在我看来，数学书（包括论文）是最晦涩难懂的读物。将一本几百页的数学书从头到尾读一遍更是难上加难。翻开数学书，定义、公理扑面而来，定理、证明接踵而至。数学这种东西，一旦理解则非常简单明了，所以我读数学书的时候，一般都只看定理，努力去理解定理，然后自己独立思考数学证明。不过，大多数情况下都是百思不得其解，最终只好参考书中的证明。然而，有时候反复阅读证明过程也难解其意，这种情况下，我便会尝试在笔记本中抄写这些数学证明。在抄写过程中，我会发现证明中有些地方不尽如人意，于是转而寻求是否存在更好的证明方法。如果能顺利找到还好，若一时难以觅得，则多会陷入苦思，至无路可走、油尽灯枯才会作罢。按照这种方法，读至一章末尾，已是月余，开篇的内容则早被忘到九霄云外。没办法，只好折返回去从头来过。之后，我又注意到书中整个章节的排列顺序不甚合理。比如，我会考虑将定理七的证明置于定理三的证明之前的话，是否更加合适。于是我又开始撰写调整章节顺序的笔记。完成这项工作后，我才有真正掌握第一章的感觉，终于送了一口气，同时又因太耗费精力而心生烦忧。从时间上来说，想要真正理解一本几百页的数学书，几乎是一件不可能完成的任务。真希望有人告诉我，如何才能快速阅读数学书”

Infty

2021 年 12 月 14 日

目录

Chapter 1

第一题

1.1 题目概述

(1) Z_m 的定义,Z_m 的加法和乘法的定义, 对加法构成群, 对乘法不构成群. 从加群的角度看待生成元, 以及作为循环群的全部子群

(2) 对乘法有可逆元, 单位元是哪个, 找到逆元素

(3) 对于这类环来说, 不是可逆元就是零因子

(4) 可逆元构成单位群, 元素的阶怎么算

1.2 第一小问

Definition 1: 模 m 剩余类

Z 的一个分类:$Z_m : \bar{0}, \bar{1}, \cdots, m \bar{-} 1$, 称为模 m 的剩余类, 每个元素称为一个同余类或剩余类.

Definition 2: 模 m 剩余类加群

定义模 m 剩余类的加法,$\bar{a} + \bar{b} = a \bar{+} b$, 模 m 剩余类按照这个加法构成群

Definition 3: 模 m 剩余类单位群

定义模 m 剩余类的乘法,$\bar{a}\bar{b} = \bar{ab}$, 模 m 剩余类按照这个乘法构成不一定构成群, 原因是有些元素没有可逆元, 有可逆元的元素构成的集合对模 m 剩余类的乘法构成群, 称之为模 m 剩余类单位群.

Definition 4: 模 m 剩余类加群的生成元

模 m 剩余类加群的生成元为 $\bar{1}$, 但注意单位元是 $\bar{0}$, 因此单位元是不等于生成元的. 模 m 剩余类加群中每个元素都可以写成模 m 剩余类加群生成元 $\bar{1}$ 的倍数

Theorem 1: 无限循环群的子群

无限循环群 $G =< a >$ 的全部子群为 $H_k =< a^k >, k = 0, 1, 2, \cdots$

Theorem 2: 有限循环群的子群

对于 n 阶循环群 $G =< a >$ 的阶的每一个正因子都存在唯一的一个 s 阶子群, 他们构成 G 的全部子群.

Exercice 1

下列各组整数中, 哪两个模 4 同余.

- 3 与 7
- -11 与 2
- 21 与-7

Solution:

a 与 b 模 m 同余 $\Leftrightarrow m|(a-b)$, 也就是说 $a-b$ 是 m 的倍数

$7-3=4$ 是 4 的倍数, 故模 4 同余,$2-(-11)=13$ 不是 4 的倍数, 故不同余,$21-(-7)=28$ 是 4 的倍数, 故模 4 同余.

Exercice 2

在模 4 的剩余类中, 下列哪两个剩余类相等?

- $\bar{-3}$ 与 $\bar{9}$
- $\bar{-1}$ 与 $\bar{-11}$
- $\bar{-12}$ 与 $\bar{32}$

Solution:

看代表元相减是否是 4 的倍数

$9-(-3)=12$ 是 4 的倍数, 故两个剩余类相等,$-1-(-11)=10$ 不是 4 的倍数, 故不相等,$32-(-12)=44$ 是 4 的倍数, 故相等.

Exercice 3

找出 Z_{10} 的加群的全部子群

Solution: 有一个好用的定理:

Theorem 3

设 G 是群,$a \in G, |a| = n$ 则

(1) $a^m = e \Leftrightarrow n|m$

(2) $|a^k| = \frac{n}{(n,k)}, \forall k \in Z^+$

6 的因子有 1,2,3,6.
对应 1 阶的子群为 $\{\bar{0}\}$
对应 2 阶的子群为 $\{\bar{0}, \bar{3}\}$
对应 3 阶的子群为 $\{\bar{0}, \bar{2}, \bar{4}\}$
对应 6 阶的子群为 $\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$

1.3 第二小问

Theorem 4

$\bar{a} \in Z_m$ 可逆 $\Leftrightarrow (a, m) = 1, 0 \leq a \leq m-1$

Exercice 4

求出 Z_9 中所有的可逆元, 并指出相应的逆元素

Solution: 与 9 互素的元素有 $1,2,4,5,7,8$
$\bar{1}^{-1} = \bar{1}$
$\bar{2}^{-1} = \bar{5}$
$\bar{4}^{-1} = \bar{7}$
$\bar{5}^{-1} = \bar{2}$
$\bar{7}^{-1} = \bar{4}$
$\bar{8}^{-1} = \bar{8}$
事实上,Z_m 中可逆的元素集合构成单位群, 因此逆元也在这个单位群中.
请读者用以下题目练手

Exercice 5

求出 Z_{15} 中所有的可逆元, 并指出相应的逆元素

1.4 第三小问

对于模 m 剩余类环来说, 元素不是可逆元就是零因子

Definition 5: 零因子

设 R 是环,$a, b \in R$ 且 $a \neq 0, b \neq 0$. 若 ab=0, 则称 a 为 R 的一个左零因子,b 为 R 的右零因子, 都简称为零因子.

Theorem 5

零因子一定不可逆, 可逆元一定不是零因子

Solution: $ab = 0$b 是 a 的零因子, 假设 b 有可逆元记为 b^{-1}, 有 $bb^{-1} = e$, 两边同时左乘以 a,$abb^{-1} = ae$ $(ab)b^{-1} = a \Leftrightarrow 0b^{-1} = a$, 而 $a \neq 0$ 故矛盾, 故零因子不是可逆元, 同理可证可逆元不是零因子.

Theorem 6

对于模 m 剩余类环来说, 元素不是可逆元就是零因子

Exercice 6

写出 Z_6 中非平凡的零因子.

Solution: $Z_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$, 其中可逆元为与 6 互素的, 为 $\bar{1}, \bar{5}$, 故非平凡的零因子为 $\bar{2}, \bar{3}, \bar{4}$

1.5 第四小问

可逆元构成单位群, 元素的阶怎么算

Exercice 7

求出 Z_9 的单位群的各元素的阶.

Solution: $Z_9^* = \{\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{7}, \bar{8}\}$

(1) $\bar{1}^1 \Leftrightarrow |\bar{1}| = 1$

(2) $\bar{2}^6 \Leftrightarrow |\bar{2}| = 6$

(3) $\bar{4}^3 \Leftrightarrow |\bar{4}| = 3$

(4) $\bar{5}^6 \Leftrightarrow |\bar{5}| = 6$

(5) $\bar{7}^3 \Leftrightarrow |\bar{7}| = 3$

(6) $\bar{8}^1 \Leftrightarrow |\bar{8}| = 2$

Chapter 2

第二题

2.1 题目概述

(1) n 元对称群的运算, 轮换的定义, 变换可以写成不相交轮换的乘积.

(2) 轮换和奇偶性 (写成对换)

(3) 置换的阶 (轮换的阶)

2.2 第一小问

Definition 6: n 元对称群

当 Ω 为有限集合时,Ω 到自身的一个双射叫做 Ω 的一个置换. 设 Ω 有 n 个元素, 这时 Ω 的置换称为 n 元置换, 并称此时的全变换群为 n 元对称群

Definition 7: 轮换

设 $\sigma(i_1) = i_2, \sigma(i_2) = i_3, \cdots, \sigma(i_{r-1}) = i_r, \sigma(i_r) = i_1$ 并且保持其余的元素不变, 则称 σ 为 S_n 中的一个 $r-$ 轮换, 记作 $\sigma = (i_1 i_2 \cdots i_r)$

Exercice 8

在 S_5 中, 设:

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 2 & 4 \end{pmatrix}, \sigma_2 = \sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix}$$

(1) 求 $\sigma_1\sigma_2, \sigma_2\sigma_1$

Exercice 8

(2) 分别写出 σ_1, σ_2 的轮换分解式

(3) 求 $\sigma_1^{-1}, \sigma_1\sigma_2\sigma_1^{-1}$

(4) 分别写出 σ_1, σ_2 的一种对换分解式

(5) 说出 σ_1, σ_2 是偶置换还是奇置换

(6) 求出 σ_1, σ_2 的阶数

Solution: (1).$\sigma_1 = (13542), \sigma_2 = (143)(25)$

$\sigma_1\sigma_2 = (13542)(143)(25) = (1245)(3)$

$\sigma_2\sigma_1 = (143)(25)(13542) = (1)(2453)$

(2).$\sigma_1 = (13542), \sigma_2 = (143)(25)$

(3).$\sigma_1^{-1} = (12453)$

$\sigma_1\sigma_2\sigma_1^{-1} = (1245)(3)(12453) = (14)(253)$

2.3 第二小问

Definition 8: 对换

2-轮换也被称为对换

Theorem 7

每一个轮换都可以表示成一些对换的乘积 $(i_1i_2\cdots i_r) = (i_1i_r)(i_1i_{r-1})\cdots(i_1i_3)(i_1i_2)$

Definition 9: 奇偶性

一个 n 元置换 σ 称为偶 (奇) 置换当且仅当 σ 可以表示成偶 (奇) 数个对换的乘积

Solution: (4). $\sigma_1 = (13542) = (12)(14)(15)(13)$

$\sigma_2 = (143)(25) = (13)(14)(25)$

(5).σ_1 是偶置换,σ_2 是奇置换

2.4 第三小问

Theorem 8

任一个 n 元置换都能表示成一些两两不相交的轮换的乘积, 出去排列次序以外, 表示法唯一

Theorem 9

r-轮换的阶为 r

Theorem 10

n 元置换的阶等于分解出的轮换的阶的最小公倍数

Solution: (6).$|\sigma_1| = 5, |\sigma_2| = 6$

Chapter 3

第三题

3.1 题目概述

验证群同态, 求群同态的核和像, 群同态基本定理得出结论.

3.2 第一小问

Definition 10: 群同态

设 $(G,\circ),(G',*)$ 是两个群, 如果存在映射 $\sigma : G \to G'$ 使得 $\sigma(a\circ b) = \sigma(a) * \sigma(b), \forall a, b \in G$ 其中 σ 称为 G 到 G' 的一个同态映射, 进一步, 若 σ 是单射, 称为单同态; 若满射, 则称为满同态.

Definition 11: 核

设 $\sigma : G \to G'$ 为群同态, 定义

$ker\sigma = \{a \in G|\sigma(a) = e'\} = \sigma^{-1}(e')$

Theorem 11: 群同态基本定理

设 σ 是群 G 到 G' 的一个同态, 则 $G/ker\sigma \cong Im\sigma$

Exercice 9

设 f 是实数加法群 R 到非零复数乘法群 C^* 的一个映射:$f(x) = e^{2\pi ix}, \forall x \in R$

证明:

- f 是一个同态
- 求 $Kerf$ 和 Imf

Exercice 9

- $R/Z \cong C$

Solution: (1).

$\forall x, y \in R$, 证明:$f(x+y) = f(x) * f(y)$

$f(x+y) = e^{2\pi i(x+y)} = e^{2\pi ix} * e^{2\pi iy} = f(x) * f(y)$

故同态

(2).

$f(x) = 1 \Rightarrow f(x) = e^{2\pi ix} = e^{2\pi in}, n \in Z$

$x = n, Kerf = Z, Imf = C$,C 为复平面上的单位圆盘

(3).

由群同态基本定理,φ 为同态映射,$C^*/Ker\varphi = Im\varphi$, 故 $R/Z \cong C$

Exercice 10

设 φ 是非零复数乘法群 C^* 到自身的一个映射:$\varphi(z) = \frac{z}{|z|}, \forall z \in C^*$

证明:

- 证明 f 是一个同态
- 求 $Kerf$ 和 Imf
- $C^*/R^+ = C$,C 是复平面上的单位元

Solution: (1). $\varphi(ab) = \frac{ab}{|ab|} = \frac{a}{|a|}\frac{b}{|b|} = \varphi(a)\varphi(b)$

(2).$z \in Ker\varphi \Leftrightarrow \varphi(z) = 1 \Leftrightarrow z/|z| = 1 \Leftrightarrow z \in R^+$

$ker\varphi = R^+, Im\varphi = C$

(3). 由群同态基本定理,φ 为同态映射,$C^*/Ker\varphi = Im\varphi$, 故 $C^*/R^+ \cong C$

Chapter 4

第四题

4.1 题目概述

了解群的定义, 验证是否能构成群

4.2 第一小问

Definition 12: 群

设 G 是一个非空集合, 如果满足下列 4 个条件:

- 在 G 中定义了一个代数运算 ”$\circ$”, 即满足封闭性,$\forall a, b \in G$, 有 $a \circ b \in G$
- 运算满足结合律:$\forall a, b, c \in G$, 有 $(a \circ b) \circ c = a \circ (b \circ c)$
- 存在 $e \in G$, 使得 $a \circ e = e \circ a = a, \forall a \in G$
- 对每一个 $a \in G$, 都存在 $b \in G$, 使得 $a \circ b = b \circ a = e$

则称 $(G, \circ)$ 是一个群, 简记 G.

如果一个群满足交换律, 我们称其为 abel 群.

Definition 13: 半群和幺半群

如果 G 只满足运算的封闭性和结合律, 则称 G 为半群, 如果半群 G 还含有单位元, 则称之为幺半群. 有时候单位元也称为幺元.

Exercice 11

试说明 Z 对运算 $a \circ b = a + b + 4$ 是否构成群?

Solution: (1). 封闭性, 任取 $a, b \in Z, a \circ b = a + b + 4 \in Z$

(2). 半群 (结合律): 任取 $a, b, c \in Z, (a \circ b) \circ c = (a + b + 4) \circ c = a + b + 4 + c + 4 = a + (b + c + 4) + 4 = a \circ (b \circ c)$

(3). 幺元 (单位元): 任取 a, e 使得 $a \circ e = a + e + 4 = a \Leftrightarrow e = -4$

(4). 逆元:$\forall a \in Z$, 都有 $b \in Z$, 使得 $a \circ b = a + b + 4 = e \Leftrightarrow b = -8 - a \in Z$

Chapter 5

第五题

5.1 题目概述

有限域的构造

5.2 第一小问

Theorem 12: 有限域的构造

设 F_q 是含有 q 个元素的有限域, 其中 $q = p^r$,p 是素数, 如果 $m(x) = a_0 + a_1 x + \cdots + a_n x^n \in F_q[x]$ 是 n 次不可约多项式, 则 $F_q[x]/(m(x))$ 是含有 q^n 个元素的有限域, 且它的每一个元素可唯一地表示成 $c_0 + c_1 u + \cdots + c_{n-1} u^{n-1}$ 其中 $c_i \in F_q, 0 \leq i \leq n, u = x + (m(x)), u$ 满足 $m(u) = 0$

事实上, 有限域 F 的元素个数一定是一个素数 p 的方幂.

Exercice 12

构造含有 125 个元素的有限域

Solution: $125 = 5^3$. 在 $Z_5[x]$ 中找一个 3 次不可约多项式. 令 $m(x) = x^3 + x + 1$. 直接计算可知, Z_5 中,0,1,2,3,4 都不是 $m(x)$ 的根, 又由于 $degm(x) = 3$, 因此 $m(x)$ 是不可约多项式, 从而 $Z_5[x]/(x^3 + x + 1)$ 是含有 5^3 个元素的有限域. 令

$$u = x + (x^3 + x + 1)$$

则 $Z_5[x]/(x^3 + x + 1) = \{c_0 + c_1 u + c_2 u^2 | c_i \in Z_5, i = 0, 1, 2\}$, 其中 u 满足 $u^3 + u + 1 = 0$, 即 $u^3 = 4u + 4$

+	0	u	1	1+u
0	0	u	1	1+u
u	u	0	u+1	1
1	1	1+u	0	u
1+u	1+u	1	u	0

*	0	u	1	1+u
0	0	0	0	0
u	0	u+1	u	1
1	0	u	1	1+u
1+u	0	u	1+u	u

Exercice 13

构造 4 个元素的有限域, 写出它的加法表和乘法表

Solution: $4=2^2$, 在 $Z_2[x]$ 中找一个 2 次不可约多项式. 令 $m(x)=x^2+x+1$. 直接计算可知, Z_2 中,0,1 都不是 $m(x)$ 的根, 又由于 $degm(x)=2$, 因此 $m(x)$ 是不可约多项式, 从而 $Z_2[x]/(x^2+x+1)$ 是含有 2^2 个元素的有限域. 令

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

则 $Z_2[x]/(x^3+x+1)=\{c_0+c_1u|c_i\in Z_2, i=0,1\}$, 其中 u 满足 $u^2+u+1=0$, 即 $u^2=u+1$

Exercice 14

构造 9 个元素的有限域.

Solution: $4=3^2$, 在 $Z_3[x]$ 中找一个 2 次不可约多项式. 令 $m(x)=x^2+1$. 直接计算可知, Z_3 中,0,1,2 都不是 $m(x)$ 的根, 又由于 $degm(x)=2$, 因此 $m(x)$ 是不可约多项式, 从而 $Z_3[x]/(x^2+1)$ 是含有 3^2 个元素的有限域. 令

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

则 $Z_3[x]/(x^2+1)=\{c_0+c_1u|c_i\in Z_3, i=0,1,2\}$, 其中 u 满足 $u^2+1=0$, 即 $u^2=2$

Exercice 15

构造含 8 个元素的有限域

Solution: $4=2^3$, 在 $Z_2[x]$ 中找一个 3 次不可约多项式. 令 $m(x)=x^3+x+1$. 直接计算可知, Z_3 中,0,1,2 都不是 $m(x)$ 的根, 又由于 $degm(x)=3$, 因此 $m(x)$ 是不可约多项式, 从而 $Z_3[x]/(x^3+x+1)$ 是含有 3^2 个元素的有限域. 令

$$u=x+(x^3+x+1)$$

则 $Z_3[x]/(x^3+x+1)=\{c_0+c_1u+c_2u^2|c_i\in Z_3, i=0,1,2\}$, 其中 u 满足 $u^3+u+1=0$

Chapter 6

第六题

6.1 题目概述

对于整数环生成理想的乘法, 并运算, 以及生成理想的表达式.

6.2 第一小问

Definition 14: 生成理想

设 S 是环 R 的一个非空子集, 环 R 的包含 S 的所有理想的交称为由 S 生成的理想, 记作 (S), 如果 $S = \{a_1, a_2. \cdots, a_n\}$, 则称 (S) 是有限生成的, 并且把 (S) 记成 $(a_1, a_2, \cdots, a_n)$

Theorem 13: 生成理想的结构

设 R 是一个环 (不一定有单位元, 也不一定是交换环), 则一个元素 a 生成的理想 (a) 为

$$(a) = \{r_1 a + a r_2 + ma + \sum_{i=1}^{n} x_i a y_i | r_1, r_2, x_i, y_i \in R, m \in Z, n \in Z^*\}$$

设 R 是有单位元的交换环,$a_1, a_2, \cdots, a_n \in R$ 容易证明

$$(a_1, a_2, \cdots, a_n) = \{r_1 a_1 + r_2 a_2 + \cdots + r_n a_n | r_i \in R, i = 1, 2, \cdots, n\}$$

Theorem 14: 整数环的运算

在整数环 Z 中, 容易看出

$(n)(m) = (nm)$

Theorem 14: 整数环的运算

$(n) \cap (m) = ([n, m])$
$(n) + (m) = ((n, m))$

Chapter 7

第七题

7.1 题目概述

代数数域的运算,$Q(t)$

7.2 第一小问

Definition 15: 极小多项式

满足:

- 首项系数为 1
- 不可约有理多项式
- 以 t 为复根

称其为 t 在 Q 上的极小多项式

Theorem 15: 整系数多项式有理根

设 $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ 是一个整系数多项式, 而 $\frac{r}{s}$ 是它的一个有理根, 其中 r,s 互素, 那么必有 $s \mid a_n, r \mid a_0$, 特别地, 如果 f(x) 的首项系数为 1, 那么 f(x) 的有理根都是整根, 而且是 a_0 的因子.

Definition 16: 代数数和超越数

如果一个复数 t 是 $Q[x]$ 中某个非零多项式的根, 称 t 为一个代数数, 否则称 t 为一个超越数.

Definition 17: 代数数域

如果 t 是一个代数数, 则存在一个以 t 为根的次数最低的首项系数为 1 的多项式 $p(x)$, 它一定是 $Q[x]$ 中的不可约多项式, 并且 $Q[x]/(p(x)) \cong Q[t]$ 于是 $Q[t]$ 是一个域. 这表明有理数域 Q 添加一个代数数 t 得到的子环 Q[t] 是一个域, 称之为代数数域.

Exercice 16

设 t 为 $f(x)=x^3-x+1$ 的一个复根. 在代数数域 $Q[t]$ 中, 求 $(5t^2+3t-1)(2t^2-2t+6)$ 和 $(3t^2-t+2)^{-1}$

Solution: 由本节定理, 显然 $f(x)=x^3-x+1$ 为一个不可约多项式, 从而 $f(x)$ 是 t 在 Q 上的极小多项式.
$Q[t]=\{c_0+c_1t+c_2t^2 \mid c_0,c_1,c_2 \in Q\}$ 且每一个元素的表示方式唯一, 其中 $f(t)=0 \Rightarrow t^3=t-1$.
$(5t^2+3t-1)(2t^2-2t+6)=10t^4-4t^3+22t^2+20t-6=32t^2+6t-2$

$$
\begin{aligned}
&(3t^2-t+2)^{-1}=at^2+bt+c\\
&(3t^2-t+2)(at^2+bt+c)=1\\
&(3c-b+5a)t^2+(5b-4a-c)t+(2c-3b+a)=1
\end{aligned}
$$

由元素表示唯一可知:

$$
\begin{cases}
3c-b+5a=0\\
5b-4a-c=0\\
2c-3b+a=1
\end{cases}
$$

$$
\begin{cases}
a=-\frac{2}{7}\\
b=-\frac{1}{7}\\
c=\frac{3}{7}
\end{cases}
$$

$(3t^2-t+2)^{-1}=-\frac{2}{7}t^2-\frac{1}{7}t+\frac{3}{7}$

Exercice 17

证明:$t=\sqrt{2}+\sqrt{3}$ 是一个代数数, 求 t 在 Q 上的极小多项式.

这就太简单了.

Chapter 8

第八题

8.1 题目概述

内直积的概念以及性质, 子群是否为正规子群, 是否同构.

8.2 第一小问

Definition 18: 直积

设 $(G,\circ),(G',*)$ 是两个群, 在笛卡尔积 $G\times G'=\{(g,g')|g\in G,g'\in G'\}$ 上, 定义运算: $(g_1,g_1')(g_2,g_2')=(g_1\circ g_2,g_1'*g_2')$, 容易得到 $G\times G'$ 按上述运算构成一个群称为直积

其中单位元:(e,e'), 逆元 $(g,g')^{-1}=(g^{-1},g'^{-1})$

Theorem 16: 内直积的概念和性质

设 G 是群,$H<G,K<G$, 如果

(1) $G=HK$

(2) $H\cap K=\{e\}$

(3) $hk=kh,\forall h\in H,k\in K$

则称 $G\cong H\times K$ 此时称 G 是子群 H 与 K 的内直积, 记作 $G=H\times K$

Definition 19: 正规子群

设 G 是群,$N<G$, 如果 $gH=Hg,\forall g\in G$, 则称 N 是 G 的正规子群, 记作 $N\lhd G$ 的正规子群, 记作 $N\lhd G$, 特别的,abel 群的任一子群都是正规子群

Theorem 17: 正规子群的判定

设 H 是群 G 的子群, 则下列条件等价:

(1) $aH = Ha, \forall a \in G$

(2) $aHa^{-1} \subset H, \forall a \in G$

(3) $aha^{-1} \in H, \forall a \in G, h \in H$

(4) $aHa^{-1} = H, \forall a \in G$

Exercice 18

设群 G 是它的子群 H 和 K 的内直积, 证明:

(1) $H \lhd G, K \lhd G$

(2) $G/H \cong K, G/K \cong H$

Solution: 首先, 群 G 是 H 和 K 的内直积, 也就是说 $G = HK$, 且 HK 的元素满足内直积的性质.

首先证明 $H \lhd G$, 即证明:$\forall h \in H, g \in G, ghg^{-1} \in H$

而 g 可以表示成 $g = h_1k_1$ 的形式

$(h_1k_1)h(h_1k_1)^{-1} = (h_1k_1)h(k_1^{-1}h_1^{-1})$

K 是子群,$k \in K, k^{-1} \in K$, 由内直积的定义 (性质)$hk = kh$, 因此

$(h_1k_1)h(h_1k_1)^{-1} = (h_1h)k_1k_1^{-1}h_1^{-1} = h_1hh_1^{-1} \in H$

故 H 为正规子群, 同理 K 为正规子群.

其次, 设映射 $\sigma : G \to K, g = hk \to k$.

下证明这是一个同态:

$\sigma(g_1g_2) = \sigma((h_1k_1)(h_2k_2)) = \sigma((h_1h_2)(k_1k_2)) = k_1k_2 = \sigma(g_1)\sigma(g_2)$

故这确实是一个同态, 其中核为 $\sigma(g) = e_k, \sigma(hk) = e_k, k = e_k, g = he_k = h$, 故 $ker\sigma = H$

显然像集为 H, 即 $Im\sigma = K$

由群同态基本定理,σ 为同态映射,$G/Ker\sigma = Im\sigma$, 故 $G/H \cong K$

同理可以证明得:$G/K \cong H$

Chapter 9

第九题

9.1 题目概述

一元多项式环和整数环的理想结构, 主理想, 极大理想, 素理想的概念, 一元多项式环的理想是主理想.

9.2 第一小问

Definition 20: 主理想

环 R 中由一个元素 a 生成的理想称为主理想, 记作 (a)

Definition 21: 极大理想

设 R 是环,M 是 R 的理想, 且 $M \neq R$, 如果 R 中包含 M 的理想只有 M 和 R, 则 M 称为 R 的一个极大理想

Definition 22: 素理想

设 R 是有单位元 1 的交换环,P 是 R 的一个理想, 且 $P \neq R$, 如果从 $ab \in P$ 可以退出 $a \in P$ 或 $b \in P$, 则称 P 为 R 的一个素理想

Exercice 19

整数环 Z 的每一个理想都是由一个非负整数生成的主理想

Proof: 设 I 是 Z 的一个理想, 如果 $I = (0)$, 则 I 是主理想, 下面设 $I \neq (0)$. 于是存在 $a \in I, a \neq 0$. 如果 a 是负整数, 则 $-a = (-1)a \in I$ 因此 I 必含有正整数. 在 I 里的正整数中取一个最小的数, 设为 m, 证明 $I = (m)$, 任取 $b \in I$, 作带余除法:

$$b = qm + r, 0 \leq r < m$$

于是 $r = b - qm \in I$, 假如 $r \neq 0$, 则与 m 的取法矛盾, 因此 $r = 0, b = qm \in (m)$, 因此 $I \subseteq (m)$, 从而 $I = (m)$ □

Exercice 20

域 F 上的一元多项式环 F[x] 的每一个理想都是主理想, 其中非零理想可以由首项系数为 1 的多项式生成

Proof: I 是 F(x) 的理想, 显然 I 为零多项式生成的理想时一定是主理想, 设 $f(x)$ 是 $F[x]$ 中最小的多项式, 证:$I = (f(x))$

对 $\forall g(x) \in I, g(x) = q(x)f(x) + r(x)$, 若 $r(x) \neq 0$, 则 $deg(r(x)) < deg((f(x)))$, 则 $r(x) = g(x) - q(x)f(x)$, 由理想的吸收性,r(x) 也是 I 中的元素, 这与 f(x) 的选取矛盾, 因此 $r(x) = 0$.

因此 $g(x) = q(x)f(x), I \subseteq (f(x))$, 从而 $I = (f(x))$