



# 抽象代数

Elegant $\text{\LaTeX}$  经典之作

作者: Hgo

时间: Jun 7, 2024



我们必须知道，我们终将知道。——希尔伯特

# 目录

<b>第 1 章 Elegant<math>\text{\LaTeX}</math> 系列模板介绍</b>	<b>1</b>
1.1 数学环境简介	1
1.1.1 定理类环境的使用	1
1.1.2 修改计数器	1
1.1.3 其他环境的使用	2
1.2 列表环境	2
1.3 参考文献	2
1.4 章后习题	3
第 1 章 练习	3
1.5 旁注	3
<b>第 2 章 ElegantBook 写作示例</b>	<b>5</b>
2.1 Lebesgue 积分	5
2.1.1 积分的定义	5
第 2 章 练习	7
<b>第 3 章 群论</b>	<b>8</b>
3.1 群的基本概念以及循环群	8
3.2 同态与同构陪集正规子群与商群	8
3.3 直积和半直积	8
3.4 群作用	9
3.4.1 轨道分解的应用	12
3.5 Sylow 定理 有限群分类	13
第 3 章 练习	15
<b>第 4 章 环</b>	<b>16</b>
4.1 环, 理想和商环	16
4.1.1 环	16
4.1.2 理想	17
4.2 中国剩余定理, 欧式整环和主理想整环	18
4.2.1 中国剩余定理	18
4.2.2 极大理想	19
4.2.3 素理想	20
4.3 唯一分解整环	21
4.3.1 欧式整环	21
4.3.2 素数在一般整环中的推广	22
4.3.3 唯一分解整环在 Gauss 整数环中的应用	23
4.3.4 一些不是 UFD 的例子	24
4.4 UFD 的多项式环的性质	24
4.4.1 UFD 上的多项式环	24
4.4.2 多项式不可约的判别法	24
4.4.3 多项式环商多项式的因式分解	24

---

<b>第 5 章 域论与 Galois 理论</b>	<b>26</b>
5.1 域扩张	26
5.1.1 域的特征	26
5.1.2 域扩张	26
5.1.3 域扩张的构造	27
5.2 正规扩张	30
5.2.1 分裂域	30
5.3 可分扩张和有限域	31
5.3.1 可分多项式	31
5.4 伽罗华理论	33
5.4.1 伽罗华群	33

# 第 1 章 Elegant $\text{\LaTeX}$ 系列模板介绍

## 1.1 数学环境简介

在我们这个模板中，我们定义了两种不同的定理模式 `mode`，包括简单模式（`simple`）和炫彩模式（`fancy`），默认为 `fancy` 模式，不同模式的选择为

```
\documentclass[simple]{elegantbook} %or
\documentclass[mode=simple]{elegantbook}
```

本模板定义了四大类环境

- 定理类环境，包含标题和内容两部分，全部定理类环境的编号均以章节编号。根据格式的不同分为 3 种
  - `definition` 环境，颜色为 `main`；
  - `theorem`、`lemma`、`corollary`、`axiom`、`postulate` 环境，颜色为 `second`；
  - `proposition` 环境，颜色为 `third`。
- 示例类环境，有 `example`、`problem`、`exercise` 环境（对应于例、例题、练习），自动编号，编号以章节为单位，其中 `exercise` 有提示符。
- 提示类环境，有 `note` 环境，特点是：无编号，有引导符。
- 结论类环境，有 `conclusion`、`assumption`、`property`、`remark`、`solution` 环境<sup>1</sup>，三者均以粗体的引导词为开头，和普通段落格式一致。

### 1.1.1 定理类环境的使用

由于本模板使用了 `tcolorbox` 宏包来定制定理类环境，所以和普通的定理环境的使用有些许区别，定理的使用方法如下：

```
\begin{theorem}{theorem name}{label}
  The content of theorem.
\end{theorem}
```

第一个必选项 `theorem name` 是定理的名字，第二个必选项 `label` 是交叉引用时所用到的标签，交叉引用的方法为 `\ref{thm:label}`。请注意，交叉引用时必须加上前缀 `thm:`。

在用户多次反馈下，4.x 之后，引入了原生定理的支持方式，也就是使用可选项方式：

```
\begin{theorem}[theorem name] \label{thm:theorem-label}
  The content of theorem.
\end{theorem}
% or
\begin{theorem} \label{thm:theorem-withou-name}
  The content of theorem without name.
\end{theorem}
```

其他相同用法的定理类环境有：

### 1.1.2 修改计数器

当前定理等环境计数器按章计数，如果想修改定理类环境按节计数，可以修改计数器选项 `thmcnt`：

<sup>1</sup> 本模板还添加了一个 `result` 选项，用于隐藏 `solution` 和 `proof` 环境，默认为显示（`result=answer`），隐藏使用 `result=noanswer`。

表 1.1: 定理类环境

环境名	标签名	前缀	交叉引用
definition	label	def	<code>\ref{def:label}</code>
theorem	label	thm	<code>\ref{thm:label}</code>
postulate	label	pos	<code>\ref{pos:label}</code>
axiom	label	axi	<code>\ref{axi:label}</code>
lemma	label	lem	<code>\ref{lem:label}</code>
corollary	label	cor	<code>\ref{cor:label}</code>
proposition	label	pro	<code>\ref{pro:label}</code>

```
\documentclass[section]{elegantbook} %or
\documentclass[thmcnt=section]{elegantbook}
```

### 1.1.3 其他环境的使用

其他三种环境没有选项，可以直接使用，比如 `example` 环境的使用方法与效果：

```
\begin{example}
  This is the content of example environment.
\end{example}
```

这几个都是同一类环境，区别在于

- 示例环境（`example`）、练习（`exercise`）与例题（`problem`）章节自动编号；
- 注意（`note`），练习（`exercise`）环境有提醒引导符；
- 结论（`conclusion`）等环境都是普通段落环境，引导词加粗。

## 1.2 列表环境

本模板借助于 `tikz` 定制了 `itemize` 和 `enumerate` 环境，其中 `itemize` 环境修改了 3 层嵌套，而 `enumerate` 环境修改了 4 层嵌套（仅改变颜色）。示例如下

- |   |  |
|---|--|
| <ul style="list-style-type: none"> <li>• first item of nesti;</li> <li>• second item of nesti;             <ul style="list-style-type: none"> <li>• first item of nestii;</li> <li>• second item of nestii;                 <ul style="list-style-type: none"> <li>• first item of nestiii;</li> <li>• second item of nestiii.</li> </ul> </li> </ul> </li> </ul> | <ol style="list-style-type: none"> <li>1. first item of nesti;</li> <li>2. second item of nesti;             <ol style="list-style-type: none"> <li>(a). first item of nestii;</li> <li>(b). second item of nestii;                 <ol style="list-style-type: none"> <li>I. first item of nestiii;</li> <li>II. second item of nestiii.</li> </ol> </li> </ol> </li> </ol> |
|---|--|

## 1.3 参考文献

文献部分，本模板调用了 `biblatex` 宏包，并提供了 `biber`（默认）和 `bibtex` 两个后端选项，可以使用 `bibend` 进行修改：

```
\documentclass[bibtex]{elegantbook}
\documentclass[bibend=bibtex]{elegantbook}
```

关于文献条目（`bib item`），你可以在谷歌学术，Mendeley，Endnote 中取，然后把它们添加到 `reference.bib` 中。在文中引用的时候，引用它们的键值（`bib key`）即可。



环境的标题文字可以通过这个环境的可选参数进行修改，修改方法为：

```
\begin{introduction}[Brief Introduction]
...
\end{introduction}
```

## 1.4 章后习题

前面我们介绍了例题和练习两个环境，这里我们再加一个，章后习题（`problemset`）环境，用于在每一章结尾，显示本章的练习。使用方法如下

```
\begin{problemset}
  \item exercise 1
  \item exercise 2
  \item exercise 3
\end{problemset}
```

效果如下：

### 第 1 章 练习

1. exercise 1
2. exercise 2
3. exercise 3
4. 测试数学公式

$$a^2 + b^2 = c_2(1, 2)[1, 23] \quad (1.1)$$

**注** 如果你想把 `problemset` 环境的标题改为其他文字，你可以类似于 `introduction` 环境修改 `problemset` 的可选参数。另外，目前这个环境会自动出现在目录中，但是不会出现在页眉页脚信息中（待解决）。

**解** 如果你想把 `problemset` 环境的标题改为其他文字，你可以类似于 `introduction` 环境修改 `problemset` 的可选参数。另外，目前这个环境会自动出现在目录中，但是不会出现在页眉页脚信息中（待解决）。

## 1.5 旁注

在 3.08 版本中，我们引入了旁注设置选项 `marginpar=margintrue` 以及测试命令 `\elegantpar`，但是由此带来一堆问题。我们决定在 3.09 版本中将其删除，并且，在旁注命令得到大幅度优化之前，不会将此命令再次引入书籍模板中。对此造成各位用户的不方便，非常抱歉！不过我们保留了 `marginpar` 这个选项，你可以使用 `marginpar=margintrue` 获得保留右侧旁注的版面设计。然后使用系统自带的 `\marginpar` 或者 `marginnote` 宏包的 `\marginnote` 命令。

**注** 在使用旁注的时候，需要注意的是，文本和公式可以直接在旁注中使用。

```
% text
\marginpar{margin paragraph text}

% equation
\marginpar{
  \begin{equation}
    a^2 + b^2 = c^2
  \end{equation}
}
```

```
\end{equation}  
}
```

但是浮动体（表格、图片）需要注意，不能用浮动体环境，需要使用直接插图命令或者表格命令环境。然后使用 `\captionof` 为其设置标题。为了得到居中的图表，可以使用 `\centerline` 命令或者 `center` 环境。更多详情请参考：[Caption of Figure in Marginpar](#)。

```
% graph with centerline command  
\marginpar{  
  \centerline{  
    \includegraphics[width=0.2\textwidth]{logo.png}  
  }  
  \captionof{figure}{your figure caption}  
}  
  
% graph with center environment  
\marginpar{  
  \begin{center}  
    \includegraphics[width=0.2\textwidth]{logo.png}  
    \captionof{figure}{your figure caption}  
  \end{center}  
}
```

## 第 2 章 ElegantBook 写作示例

### 内容提要

□ 积分定义 2.1

□ Fubini 定理 2.1

□ 最优性原理 2.1

□ 柯西列性质 2.1.1

□ 韦达定理

## 2.1 Lebesgue 积分

在前面各章做了必要的准备后,本章开始介绍新的积分。在 Lebesgue 测度理论的基础上建立了 Lebesgue 积分,其被积函数和积分域更一般,可以对有界函数和无界函数统一处理。正是由于 Lebesgue 积分的这些特点,使得 Lebesgue 积分比 Riemann 积分具有在更一般条件下的极限定理和累次积分交换积分顺序的定理,这使得 Lebesgue 积分不仅在理论上更完善,而且在计算上更灵活有效。

Lebesgue 积分有几种不同的定义方式。我们将采用逐步定义非负简单函数,非负可测函数和一般可测函数积分的方式。

由于现代数学的许多分支如概率论、泛函分析、调和分析等常常用到一般空间上的测度与积分理论,在本章最后一节将介绍一般的测度空间上的积分。

### 2.1.1 积分的定义

我们将通过三个步骤定义可测函数的积分。首先定义非负简单函数的积分。以下设  $E$  是  $\mathcal{R}^n$  中的可测集。

#### 定义 2.1 (可积性)

设  $f(x) = \sum_{i=1}^k a_i \chi_{A_i}(x)$  是  $E$  上的非负简单函数,其中  $\{A_1, A_2, \dots, A_k\}$  是  $E$  上的一个可测分割,  $a_1, a_2, \dots, a_k$  是非负实数。定义  $f$  在  $E$  上的积分为  $\int_a^b f(x)$

$$\int_E f dx = \sum_{i=1}^k a_i m(A_i) \quad (2.1)$$

一般情况下  $0 \leq \int_E f dx \leq \infty$ 。若  $\int_E f dx < \infty$ , 则称  $f$  在  $E$  上可积。



一个自然的问题是, Lebesgue 积分与我们所熟悉的 Riemann 积分有什么联系和区别? 在 4.4 节我们将详细讨论 Riemann 积分与 Lebesgue 积分的关系。这里只看一个简单的例子。设  $D(x)$  是区间  $[0, 1]$  上的 Dirichlet 函数。即  $D(x) = \chi_{Q_0}(x)$ , 其中  $Q_0$  表示  $[0, 1]$  中的有理数的全体。根据非负简单函数积分的定义,  $D(x)$  在  $[0, 1]$  上的 Lebesgue 积分为

$$\int_0^1 D(x) dx = \int_0^1 \chi_{Q_0}(x) dx = m(Q_0) = 0 \quad (2.2)$$

即  $D(x)$  在  $[0, 1]$  上是 Lebesgue 可积的并且积分值为零。但  $D(x)$  在  $[0, 1]$  上不是 Riemann 可积的。

有界变差函数是与单调函数有密切联系的一类函数。有界变差函数可以表示为两个单调递增函数之差。与单调函数一样,有界变差函数几乎处处可导。与单调函数不同,有界变差函数类对线性运算是封闭的,它们构成一线空间。练习题 2.1 是一个性质的证明。

 **练习 2.1** 设  $f \notin L(\mathcal{R}^1)$ ,  $g$  是  $\mathcal{R}^1$  上的有界可测函数。证明函数

$$I(t) = \int_{\mathcal{R}^1} f(x+t)g(x)dx \quad t \in \mathcal{R}^1 \quad (2.3)$$



是  $\mathcal{R}^1$  上的连续函数。

**解** 即  $D(x)$  在  $[0, 1]$  上是 Lebesgue 可积的并且积分值为零。但  $D(x)$  在  $[0, 1]$  上不是 Riemann 可积的。

**证明** 即  $D(x)$  在  $[0, 1]$  上是 Lebesgue 可积的并且积分值为零。但  $D(x)$  在  $[0, 1]$  上不是 Riemann 可积的。

### 定理 2.1 (Fubini 定理)

(1) 若  $f(x, y)$  是  $\mathcal{R}^p \times \mathcal{R}^q$  上的非负可测函数, 则对几乎处处的  $x \in \mathcal{R}^p$ ,  $f(x, y)$  作为  $y$  的函数是  $\mathcal{R}^q$  上的非负可测函数,  $g(x) = \int_{\mathcal{R}^q} f(x, y) dy$  是  $\mathcal{R}^p$  上的非负可测函数。并且

$$\int_{\mathcal{R}^p \times \mathcal{R}^q} f(x, y) dx dy = \int_{\mathcal{R}^p} \left( \int_{\mathcal{R}^q} f(x, y) dy \right) dx. \quad (2.4)$$

(2) 若  $f(x, y)$  是  $\mathcal{R}^p \times \mathcal{R}^q$  上的可积函数, 则对几乎处处的  $x \in \mathcal{R}^p$ ,  $f(x, y)$  作为  $y$  的函数是  $\mathcal{R}^q$  上的可积函数, 并且  $g(x) = \int_{\mathcal{R}^q} f(x, y) dy$  是  $\mathcal{R}^p$  上的可积函数。而且 2.4 成立。



### 2.1



**笔记** 在本模板中, 引理 (lemma), 推论 (corollary) 的样式和定理 2.1 的样式一致, 包括颜色, 仅仅只有计数器的设置不一样。

我们说一个实变或者复变量的实值或者复值函数是在区间上平方可积的, 如果其绝对值的平方在该区间上的积分是有限的。所有在勒贝格积分意义下平方可积的可测函数构成一个希尔伯特空间, 也就是所谓的  $L^2$  空间, 几乎处处相等的函数归为同一等价类。形式上,  $L^2$  是平方可积函数的空间和几乎处处为 0 的函数空间的商空间。

### 命题 2.1 (最优性原理)

如果  $u^*$  在  $[s, T]$  上为最优解, 则  $u^*$  在  $[s, T]$  任意子区间都是最优解, 假设区间为  $[t_0, t_1]$  的最优解为  $u^*$ , 则  $u(t_0) = u^*(t_0)$ , 即初始条件必须还是在  $u^*$  上。



我们知道最小二乘法可以用来处理一组数据, 可以从一组测定的数据中寻求变量之间的依赖关系, 这种函数关系称为经验公式。本课题将介绍最小二乘法的精确定义及如何寻求点与点之间近似成线性关系时的经验公式。假定实验测得变量之间的  $n$  个数据, 则在平面上, 可以得到  $n$  个点, 这种图形称为“散点图”, 从图中可以粗略看出这些点大致散落在某直线近旁, 我们认为其近似为一线性函数, 下面介绍求解步骤。

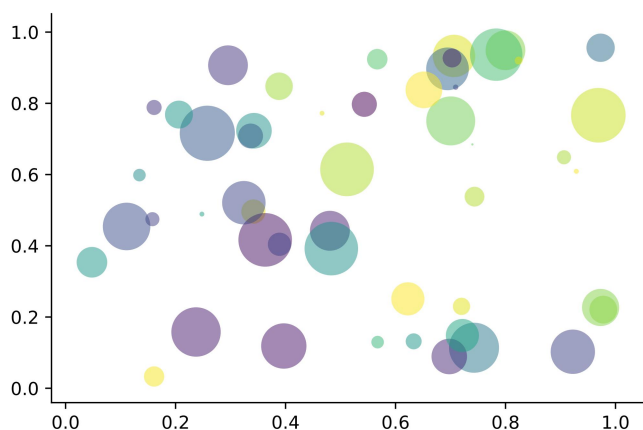


图 2.1: 散点图示例  $\hat{y} = a + bx$

以最简单的一元线性模型来解释最小二乘法。什么是一元线性模型呢? 监督学习中, 如果预测的变量是离散的, 我们称其为分类 (如决策树, 支持向量机等), 如果预测的变量是连续的, 我们称其为回归。回归分析中, 如果只包括一个自变量和一个因变量, 且二者的关系可用一条直线近似表示, 这种回归分析称为一元线性回归分析。如果回归分析中包括两个或两个以上的自变量, 且因变量和自变量之间是线性关系, 则称为多元线性回

归分析。对于二维空间线性是一条直线；对于三维空间线性是一个平面，对于多维空间线性是一个超平面。

**性质** 柯西列的性质

1.  $\{x_k\}$  是柯西列，则其子列  $\{x_k^i\}$  也是柯西列。
2.  $x_k \in \mathcal{R}^n$ ,  $\rho(x, y)$  是欧几里得空间，则柯西列收敛， $(\mathcal{R}^n, \rho)$  空间是完备的。

**结论** 回归分析 (regression analysis) 是确定两种或两种以上变量间相互依赖的定量关系的一种统计分析方法。运用十分广泛，回归分析按照涉及的变量的多少，分为一元回归和多元回归分析；按照因变量的多少，可分为简单回归分析和多重回归分析；按照自变量和因变量之间的关系类型，可分为线性回归分析和非线性回归分析。

## 第2章 练习

1. 设  $A$  为数域  $K$  上的  $n$  级矩阵。证明：如果  $K^n$  中任意非零列向量都是  $A$  的特征向量，则  $A$  一定是数量矩阵。
2. 证明：不为零矩阵的幂零矩阵不能对角化。
3. 设  $A = (a_{ij})$  是数域  $K$  上的一个  $n$  级上三角矩阵，证明：如果  $a_{11} = a_{22} = \cdots = a_{nn}$ ，并且至少有一个  $a_{kl} \neq 0 (k < l)$ ，则  $A$  一定不能对角化。

## 第3章 群论

### 3.1 群的基本概念以及循环群

#### 定义 3.1

群  $G$  的阶数是其作为集合的基数, 即  $|G|$



### 3.2 同态与同构陪集正规子群与商群

#### 命题 3.1

设  $G$  是一个有限群, 则以下命题等价

1.  $|G| = p$ , 其中  $p$  为素数;
2.  $G$  不是平凡群且没有非平凡子群;
3.  $G \cong \mathbb{Z}_p$ , 其中  $p$  为素数



证明

- $1 \Rightarrow 2$  这个结论是显然的;
- $2 \Rightarrow 3$  由于  $G$  不是平凡群, 取  $x \in G, x \neq e$ , 则  $\langle x \rangle \leq G$ , 从而  $\langle x \rangle = G$ , 即  $G$  是一个循环群, 设  $|G| = k$ . 事实上  $G$  中任何非单位元都是  $G$  的生成元, 从而  $k$  是素数, 即  $G \cong \mathbb{Z}_p$ ;
- $3 \Rightarrow 1$  显然

### 3.3 直积和半直积

#### 命题 3.2

设  $H, K \leq G$ , 则集合  $HK$  中的每个元素有  $|H \cap K|$  种表达方式, 特别地, 当  $|H \cap K| = 1$ ,  $HK$  中的每个元素表示唯一



证明 设  $hk = h'k', h, h' \in H, k, k' \in K$ , 则

$$(h')^{-1}h = k'k^{-1} \in H \cap K$$

这样  $h', k'$  就完全依赖于  $H \cap K$  中的元素, 得证

#### 定理 3.1 (Recognition Theorem)

设  $H, K \leq G$ , 且满足以下条件:

1.  $H, K \triangleleft G$ ;
2.  $H \cap K = \{e\}$

则  $HK \cong H \times K$



证明 容易知道此时  $HK$  的确构成了  $G$  的一个子群. 现在构成映射  $\varphi$

$$\varphi: H \times K \rightarrow HK$$

$$(h, k) \mapsto hk$$

$\varphi$  的满性是显然的, 由上述命题, 我们知道  $\varphi$  也是单的, 因此  $\varphi$  是一个双射, 下面再证明  $\varphi$  是一个同态, 只需要证明  $H, K$  是交换的. 对  $h \in H, k \in K$ , 我们考虑交换子  $h^{-1}k^{-1}hk$ , 由条件  $H, K \triangleleft G$ , 知  $h^{-1}k^{-1}h \in K, k^{-1}hk \in H$ , 从而  $h^{-1}k^{-1}hk \in H \cap K = \{e\}$ , 因此  $hk = kh$ .

**注** 在这种情况下  $H, K$  是交换的

以上的直积是构造群的一种方法, 下面再引入另一种方法, 我们放宽  $H, K$  的正规性要求, 得到半直积构造. 我们设  $H \triangleleft G, K \leq G, H \cap K = \{e\}$ , 这里不要求  $G$  是正规子群. 此时  $HK$  依然是  $G$  的子群, 但其上的群乘法却不显然

$$(h_1 k_1) \cdot (h_2 k_2) = h_1 \underbrace{k_1 h_2 k_1^{-1}}_{\text{in } H} \cdot k_1 k_2$$

由于这里  $K$  不是  $G$  的正规子群, 从而  $H, K$  不是交换.

### 定理 3.2 (Recognizing semidirect products)

设  $H, K \leq G$ , 且满足以下条件:

1.  $H \triangleleft G, K \leq G$ ;
2.  $H \cap K = \{e\}$

则  $HK \cong H \rtimes K$ , 这里的半直积依赖的群作用是共轭作用



## 3.4 群作用

### 内容提要

□ 群作用的定义

□ 类方程

### 定义 3.2

群  $G$  在集合  $X$  上的作用是一个映射  $G \times X \rightarrow X \quad (g, x) \mapsto gx$ , 使得对任意  $x \in X, g_1, g_2 \in G$ , 成立

- $ex = x$
- $(g_1 g_2)x = g_1(g_2 x)$



这里特别注意, 所谓  $gx$ , 不是说  $g, x$  通过  $G$  中二元运算相乘, 这只是一个记号, 更像函数的意思; 固定  $g$ , 我们实际上就得到了一个  $X$  上的自同构  $\phi_g: X \rightarrow X \quad x \mapsto gx$ . 这说明所谓  $G$  在  $X$  上的作用, 实际上是把每一个  $G$  中元素与  $X$  的自同构等价起来, 于是我们有以下的命题

### 命题 3.3

设群  $G$  作用在集合  $X$  上, 则有以下群同态

$$\begin{aligned} \varphi: G &\rightarrow S_X \\ g &\mapsto \sigma_g \end{aligned}$$

事实上, 群  $G$  在集合  $X$  上的作用与同态  $\varphi: G \rightarrow S_X$  是等价的



**证明**

这个同态  $\varphi$  也具有很多性质

### 命题 3.4

设群  $G$  作用在集合  $X$  上, 其诱导同态  $\varphi: G \rightarrow S_X$

1.  $\ker \varphi \triangleleft G$
2.  $\varphi(g) = \varphi(g') \Leftrightarrow g \ker \varphi = g' \ker \varphi$ , 于是  $G$  在  $X$  上的作用也可以视为  $G / \ker \varphi$  在  $X$  上的忠实作用



下面我们考虑一类十分重要的作用, 即  $G$  在本身上的作用

### 定理 3.3 (Cayley)

- 每个群都同构于一个对称群的子群
- 如果  $G$  是一个  $n$  阶群 ( $n < \infty$ ), 则  $G$  同构于  $S_n$  的子群

**证明** 实际上我们只需要找到一个  $G \rightarrow S_G$  的单同态即可, 我们无需考虑满性, 因为将  $G$  嵌入  $S_G$  后, 其自动会成为  $S_G$  的一个子群, 于是我们需要找到  $G$  到本身上的忠实作用. 这是容易的, 先前的左作用就是这样的作用

在进一步研究群作用之前, 我们先给出一些与群作用相关的定义

### 定义 3.3

设群  $G$  作用在集合  $X$  上, 对于任意  $x \in X$

1.  $Stab_G(x) := \{g \in G \mid gx = x\}$  称为  $x$  在  $G$  中的稳定子群
2.  $Orb_G(x) \triangleq Gx := \{gx \mid g \in G\}$  称为  $x$  在  $G$  中的轨道

### 命题 3.5

1.  $Stab_G(x) \leq G$
2. 如果  $Gx \cap Gy \neq \emptyset$ , 那么  $Gx = Gy$
3. 如果  $y = gx$ , 即  $x, y$  在同一轨道上, 则有  $Stab_G(x) = g \cdot Stab_G(y) \cdot g^{-1}$

从第二点看出, 两个轨道要么相等, 要么不相交, 这个性质与等价类十分相似, 这就引发我们思考: 在同一轨道上是否是一种等价关系? 用数学符号来表示, 即

$$x \sim y \Leftrightarrow \exists g \in G, y = gx$$

是否是一种等价关系, 的确如此. 于是我们便通过这个等价关系得到了集合  $X$  的通过轨道的分割

### 推论 3.1

$$X = \coprod_{\text{orbits } \mathcal{O}} \mathcal{O}.$$

接着我们将这些概念应用到共轭关系中, 因为它们经常出现, 我们给它们取新的名字

### 定义 3.4

考虑群  $G$  在自身上的共轭作用, 则

1. 对任意  $x \in G$ , 称轨道  $Gx = \{gxg^{-1} \mid g \in G\}$  是  $x$  的共轭类
2.  $Stab_G(x) = \{g \in G \mid gxg^{-1} = x\} = \{g \in G \mid gx = xg\} \triangleq C_G(x)$  是  $x$  的中心化子

自然地, 作为特例, 群  $G$  可以写成共轭类的不交并

以上是元素的中心化子, 自然地, 我们可以把上述概念推广到集合上

### 定义 3.5

设  $S \subset G$

1.  $C_G(S) = \{g \in G \mid gs = sg, \forall s \in S\} = \bigcap_{s \in S} C_G(s) \leq G$  称为集合  $S$  的中心化子
2.  $Z(G) := C_G(G) = \{g \in G \mid gx = xg, \forall x \in G\} = \ker(\text{Ad} : G \rightarrow S_G)$  称为  $G$  的中心, 特别地,  $Z(G)$  是一个 Abel 群

**定义 3.6**

设  $X$  是由  $G$  所有子群组成的集合, 考虑  $G$  在  $X$  上的共轭作用

$$\begin{aligned}\mathrm{Ad}_g : X &\rightarrow X \\ H &\mapsto gHg^{-1}\end{aligned}$$

定义如下集合, 称为  $H$  的正规化子:

$$N_G(H) = \mathrm{Stab}_G(H) = \{g \in G \mid gHg^{-1} = H\} \leq G$$



下面是正规化子的两个简单性质

**命题 3.6**

1.  $C_G(H) \leq N_G(H)$ ;
2.  $H \triangleleft N_G(H)$ .



下面我们再考虑一类具有特殊性质的群作用, 它将导出重要的类方程

**定义 3.7**

称群  $G$  在集合  $X$  上的作用是可迁的 (transitive), 如果  $\forall x, y \in X, \exists g \in G, s.t. y = gx$



从等价关系的角度来看, 这就说明  $X$  的元素都是等价的, 即  $X$  只有一个轨道, 就是  $X$  本身. 此时为我们计数提供了方便, 如果我们可以找到  $X$  到某个集合的双射, 我们就可以对一个轨道的基数进行计算.

**命题 3.7**

如果群  $G$  在集合  $X$  上的作用是可迁的, 那么对任意  $x \in X$ , 存在双射:

$$\begin{aligned}\varphi : G/G_x &\rightarrow X \\ gG_x &\mapsto gx\end{aligned}$$



**证明** 需要证明良定性, 单性和满性, 都是容易的.

由于  $G$  在  $X$  上的作用是可迁的, 因此  $X$  就是一个轨道, 这样我们得到了  $x$  轨道的计数公式

$$|Gx| = [G : G_x]$$

回想我们证明 Lagrange 定理的过程, 类似地, 我们同样可以对

$$X = \coprod_{\text{orbits } \mathcal{O}} \mathcal{O}$$

两边进行计数, 从而得到下述一般性的定理

**定理 3.4**

设群  $G$  作用在集合  $X$  上, 则

$$|X| = \sum_{Gx} |Gx| = \sum_{Gx} [G : G_x]$$



我们将这一一般性结果运用在共轭关系中, 就可以得到类方程

**定理 3.5**

设  $G$  是一个有限群, 则

1.  $|\mathrm{Ad}(G)x| = [G : C_G(x)]$ ;



2. 设  $g_1, g_2, \dots, g_r$  是不在  $Z(G)$  中的共轭类的代表元, 则

$$|G| = |Z(G)| + \sum_{i=1}^r [G : C_G(g_i)]$$



### 命题 3.8

设  $H \leq G$ , 设  $G$  通过左平移作用在集合  $G/H$  诱导了同态  $G \rightarrow S_{G/H}$ , 则这个同态的核包含于  $H$



### 推论 3.2

如果  $H \leq G$ ,  $[G : H] = n$ , 且没有  $G$  的非平凡正规子群包含于  $H$ , 则  $G$  同构于  $S_n$  的子群



### 命题 3.9 (Burnside 引理)

设有限群  $G$  作用在有限集  $X$  上. 令  $X^g = \{x \in X \mid gx = x\}$ , 则有

$$|G \backslash X| |G| = \sum_{g \in G} |X^g|$$



**证明** 先考虑传递的作用, 由于  $\forall x_0 \in X, \text{Stab}_G(gx_0) = \text{Stab}_G(x_0)$ , 则

$$\sum_{g \in G} |X^g| = \sum_{x \in X} |\text{Stab}_G(x)| = [G : G_{x_0}] |\text{Stab}_G(x_0)| = |G|$$

在考虑一般的群作用, 则  $X = \coprod_{i=1}^n Gx_i := \coprod_{i=1}^n X_i$ , 此时在每个轨道上的作用都是传递的, 于是

$$\sum_{g \in G} |X^g| = \sum_{i=1}^n \sum_{g \in G} |X_i^g| = n|G|.$$

其中  $n = |G \backslash X|$ , 得证!

**注** 可以理解为  $G$  中每个元素平均固定了  $|G \backslash X|$  个元素.

## 3.4.1 轨道分解的应用

我们关系群作用下的不动点.

### 定义 3.8

设  $G$  作用在  $X$  上, 记  $X^G := \{x \in X \mid gx = x, \forall g \in G\}$ , 其中元素称为  $X$  在  $G$  作用下的不动点.



**注** 不动点在群  $G$  作用下的轨道只要本身一个元素.

### 定义 3.9

设  $p$  是素数, 若  $|G| = p^m, m \in \mathbb{N}$ , 则称  $G$  为  $p$ -群



### 命题 3.10

设  $p$ -群  $G$  作用在有限集  $X$  上, 则

$$|X| \equiv |X^G| \pmod{p}$$



**证明** 由于

$$|X| = |X^G| + \sum_{[G : G_{x_i}] > 1} [G : G_{x_i}]$$

且  $[G : G_{x_i}] \mid p^m$ , 故  $p \mid [G : G_{x_i}]$ , 得证.

**推论 3.3**

设  $G$  是非平凡  $p$ -群, 则  $Z(G) \neq \{1\}$ .



**证明** 令  $G$  通过共轭作用作用在  $G$  上, 则

$$|G| \equiv |Z(G)| \pmod{p}$$

于是  $p \mid |Z(G)|$ , 因此  $Z(G) \neq \{1\}$ .

**定理 3.6 (Cauchy 定理)**

设  $G$  是有限群,  $p$  是  $|G|$  的素因子, 则存在  $g \in G$ , 使得  $|g| = p$ .

**一些习题和可能有用的结论**

**练习 3.1** 如果  $G/Z(G)$  是循环群, 则  $G$  是一个 Abel 群

**练习 3.2** 设  $H < G$ , 且  $[G : H]$  有限, 则  $G$  包含一个有限指标的正规子群

**证明** 我们考虑  $G$  在  $X = G/H$  上的左平移作用, 即

$$\begin{aligned} \ell_g : X &\rightarrow X \\ xH &\mapsto gxH \end{aligned}$$

这个作用诱导了同态  $\varphi : G \rightarrow S_X$ , 由于  $H < G$ , 因此  $\varphi$  不是平凡的. 由第一同构定理, 得到  $G/\ker \varphi \cong \varphi(G)$ , 于是  $[G : \ker \varphi]$  有限且大于 1, 而  $\ker \varphi < G$  是恒成立的, 因此  $\ker \varphi$  就是所求的正规子群

**练习 3.3** 设  $|G| = pn$ ,  $p > n$  且  $p$  是素数, 若  $H$  是  $G$  的  $p$  阶子群, 则  $H < G$

**证明** 我们考虑  $G$  在  $X = G/H$  上的左平移作用, 即

$$\begin{aligned} \ell_g : X &\rightarrow X \\ xH &\mapsto gxH \end{aligned}$$

这个作用诱导了同态  $\varphi : G \rightarrow S_X$ . 要证明  $H < G$ , 即  $x^{-1}hx \in H, \forall x \in G, h \in H$ , 也即  $hxH = xH, \forall x \in G, h \in H$ . 换句话说,  $\forall h \in H, h$  都诱导了  $S_X$  中的平凡置换, 只要证明  $\varphi(H) = \{e\}$  即可. 由第一同构定理, 得到  $H/\ker \varphi \cong \varphi(H)$ , 从而  $|\varphi(H)| = |H/\ker \varphi| \mid |H| = p$ . 又  $\varphi(H) \leq S_X$ , 从而  $|\varphi(H)| \mid n!$ , 从而  $|\varphi(H)| = 1$ , 得证

**3.5 Sylow 定理 有限群分类**

我们想用抽象的方法去研究有限群及其分类

**引理 3.1**

如果  $G/C(G)$  是循环群, 则  $G$  一定是 Abel 群

**命题 3.11**

$p^2$  阶群  $G$  一定是 Abel 群, 其中  $p$  为素数, 也即  $G \cong \mathbb{Z}_{p^2}$  或  $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$

**定义 3.10**

设  $|G| = p^r m, r \geq 0, (p, m) = 1$ , 称  $G$  的  $p^r$  阶子群为西罗  $p$ -子群 (Sylow  $p$ -子群)



**注** 换句话说,  $G$  的 Sylow  $p$ -子群是最大的  $p$ -子群

**定理 3.7 (The First Sylow Theorem)**

设  $|G| = p^r m, r \geq 0, (p, m) = 1$ , 则  $G$  的 Sylow  $p$ -子群一定存在



**证明** 我们考虑对  $|G|$  进行归纳, 当  $|G| = 1$  时, 有平凡的 Sylow  $p$ -子群; 假设结论对较小的阶数成立.

1.  $p \mid |Z(G)|$  由于  $G$  是有限群, 从而  $Z(G)$  也是有限群, 特别的,  $Z(G)$  还是 Abel 群, 根据有限生成 Abel 群的分类定理, 我们知道有限 Abel 群一定有 Sylow  $p$ -子群. 设  $Z(G)_p$  是  $Z(G)$  的 Sylow  $p$ -子群, 由于  $Z(G)_p \triangleleft G$ , 所以考虑满同态:

$$\varphi: G \rightarrow \overline{G} = G/Z(G)_p$$

由于  $|Z(G)_p| = p^{r'} \geq p$ , 从而  $|\overline{G}| < |G|$ , 根据归纳假设, 设  $\overline{H}$  为  $\overline{G}$  的 Sylow  $p$ -子群. 考虑  $H = \varphi^{-1}(\overline{H})$ , 下面证明  $H$  就是  $G$  的 Sylow  $p$ -子群. 考虑  $|H|$  即可, 由于  $\varphi$  是满同态, 根据第一同构定理, 我们有  $|H| = |\ker \varphi| |\overline{H}|$ , 而  $\ker \varphi = Z(G)_p$ , 从而  $|\ker \varphi| = p^{r'}$ , 而  $|\overline{H}| = p^{r-r'}$ , 故  $|H| = p^r$ ,  $H$  的确是  $G$  的 Sylow  $p$ -子群;


2.  $p \nmid |Z(G)|$  这时我们用类方程来解决, 先排除一些平凡的情况, 即  $p \nmid |G|$ , 这时  $G$  的 Sylow  $p$ -子群就是平凡群, 一定存在. 下面考虑  $p \mid |G|$ , 根据类方程, 我们有

$$|G| = |Z(G)| + \sum_i [G : C_G(g_i)]$$

从而存在  $g = g_i$ , 使得  $p \nmid [G : C_G(g)]$ , 于是  $|C_G(g)| = p^r m'$ , 其中  $m' \mid m$  且  $m' \neq m$ , 因此可以对  $C_G(g)$  用归纳假设, 得到  $C_G(g)$  的 Sylow  $p$ -子群, 显然这就是  $G$  的 Sylow  $p$ -子群

**注** Sylow 第一定理表明, 任何有限群一定有 Sylow  $p$ -子群, 尽管可能是平凡的; 如果  $p \mid |G|$ , 那么一定有非平凡的 Sylow  $p$ -子群

### 定理 3.8 (The Second Sylow Theorem)

设  $|G| = p^r m$ ,  $r \geq 0$ ,  $(p, m) = 1$ ,  $P$  是  $G$  的 Sylow  $p$ -子群,  $Q$  是  $G$  的  $p$ -子群, 则存在  $g \in G$ , 使得  $Q \leq gPg^{-1}$  

**证明** 考虑  $Q$  在  $G/P = \{gP \mid g \in G\}$  上的左平移作用, 由类方程


$$|G/P| = \sum_i [Q : \text{Stab}_Q(g_i P)]$$

由于  $p \nmid |G/P|$ , 从而存在  $g = g_i$ , 使得  $p \nmid [Q : \text{Stab}_Q(gP)]$ , 但  $[Q : \text{Stab}_Q(gP)] \mid p^k$ , 这迫使  $[Q : \text{Stab}_Q(gP)] = 1$ , 从而  $Q = \text{Stab}_Q(gP)$ . 这表明  $\forall x \in Q$ , 有  $xgP = gP$ , 从而  $g^{-1}xg \in P$ , 即  $x \in gPg^{-1}$ , 故  $Q \leq gPg^{-1}$


### 推论 3.4

$G$  的所有 Sylow  $p$ -子群共轭 

### 推论 3.5


Sylow  $p$ -子群唯一当且仅当存在正规 Sylow  $p$ -子群 

### 推论 3.6

设  $P$  是  $G$  的 Sylow  $p$ -子群, 则  $P$  是  $N_G(P)$  的唯一 Sylow  $p$ -子群, 且  $N_G(N_G(P)) = N_G(P)$  

### 定理 3.9 (The Third Sylow Theorem)

设  $|G| = p^r m$ ,  $r \geq 0$ ,  $(p, m) = 1$ ,  $S = \{G \text{ 的所有 Sylow } p\text{-子群}\}$ , 记  $n_p = |S|$ , 则

1.  $n_p \mid m$ ;
  2.  $n_p \equiv 1 \pmod{p}$
- 

**证明**

1. 由第二 Sylow 定理知道, 所有的 Sylow  $p$ -子群都是共轭的, 自然的, 我们考虑  $G$  在  $S$  上的共轭作用, 那么这个作用就是可迁的. 那么由类方程我们得到

$$n_p = |S| = [G : N_G(P)]$$

其中  $P$  是某个 Sylow  $p$ -子群. 由于  $P \triangleleft N_G(P)$ , 于是  $p \nmid [G : N_G(P)]$ , 故  $n_p \mid m$

2. 我们同样考虑共轭作用, 只不过现在任取  $G$  的一个 Sylow  $p$ -子群  $P$ , 我们考虑  $P$  在  $S$  上的共轭作用, 由计数公式

$$n_p = \sum_i [P : \text{Stab}_P(P_i)]$$

注意到如果  $\text{Stab}_P(P_i) < P$ , 那么  $p \nmid [P : \text{Stab}_P(P_i)]$ , 因此实际上我们只要证明使得  $[P : \text{Stab}_P(P_i)]$  的  $P_i$  只有一个. 设  $\text{Stab}_P(P_i) = P$ , 那么  $P \leq N_G(P_i)$ , 由于  $N_G(P_i)$  有唯一的 Sylow  $p$ -子群  $P_i$ , 因此  $P_i = P$ , 从而唯一. 故  $n_p \equiv 1 \pmod{p}$

下面我们将运用 Sylow 定理对有限群进行分类, 在这之前, 我们先定义半直积 (semi-direct product) 的概念. 先来看一个典型的半直积的例子

### 命题 3.12

设  $K, H \leq G$ , 且  $K \leq N_G(H)$ ,  $H \cap K = \{e\}$ , 则  $HK \leq G$

### 定义 3.11

设  $H, K$  是群, 且  $\varphi: K \rightarrow \text{Aut}(H)$  是一个群同态, 则半直积  $H \rtimes K$  是一个群, 作为集合是  $H \times K$ , 带有如下的二元运算

$$(h_1, k_1)(h_2, k_2) = (h_1\varphi(k_1)(h_2), k_1k_2)$$

下面对  $pq$  阶群  $G$  进行分类, 其中  $p, q$  都是素数. 当  $p = q$  时  $G$  为 Abel 群. 不妨设  $p > q$ , 根据第三 Sylow 定理, 我们有  $n_p|q$ ,  $n_p \equiv 1 \pmod{p}$ , 从而  $n_p = 1$ , 即  $G$  只有一个 Sylow  $p$ -子群  $P$ , 故  $P \triangleleft G$ . 类似的, 我们再对  $q$  用第三 Sylow 定理, 得到  $n_q|p$ ,  $n_q \equiv 1 \pmod{q}$ , 由前者, 我们知道  $n_q = 1$  或  $n_q = p$ . 此时我们不能保证  $n_q$  的值, 需要分类.

1.  $n_q = 1$  此时我们同样有唯一的 Sylow  $q$ -子群  $Q$ ,  $Q \triangleleft G$ . 我们考虑  $P \cap Q$ , 则  $P \cap Q \leq P$  且  $P \cap Q \leq Q$  于是  $|P \cap Q| = 1$ , 即  $P \cap Q = \{e\}$ , 从而  $PQ \cong P \times Q$ , 于是  $G = PQ \cong P \times Q \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$
2.  $n_q = p$  设  $Q$  是  $G$  的一个 Sylow  $q$ -子群, 则  $Q$  一定将  $P$  正规化, 且  $P \cap Q = \{e\}$ , 因此  $PQ \cong P \rtimes Q$ , 故  $G \cong \mathbb{Z}_p \rtimes \mathbb{Z}_q$

## 第3章 练习

1. 如果  $a^2 = e$  对任意  $a \in G$  都成立, 则  $G$  是 Abel 群.
2. 设  $G$  是 Abel 群,  $a, b \in G$  且  $|a| = m$ ,  $|b| = n$ , 则存在  $c \in G$  使得  $|c| = [m, n]$ .
3. 只要有限个子群的群一定是有限群.
- 4.

## 第4章 环

### 4.1 环,理想 and 商环

#### 4.1.1 环

##### 定义 4.1

环  $R$  是带有两个二元运算  $+$ ,  $\cdot$  的集合,  $\forall a, b, c \in R$ , 满足:

1.  $(R, +)$  是一个 Abel 群, 其单位元记作  $0_R$ ;
2.  $\cdot$  满足结合律:  $(ab)c = a(bc)$ ;
3. 满足分配律:  $(a+b)c = ac + bc, c(a+b) = ca + cb$

如果  $R$  还带有乘法单位元  $1_R$ , 则称这个环是 unital (含单位元)



##### 命题 4.1

设  $R$  是环, 则以下命题成立:

1.  $0_R a = a 0_R = 0$ ;
2.  $-ab = (-a)b = a(-b)$ .



##### 定义 4.2

称环  $R$  是交换环, 如果  $ab = ba, \forall a, b \in R$



##### 定义 4.3

称环  $R$  是一个可除环 (division ring), 如果  $\forall a \in R, a \neq 0, \exists b \in R, s.t. ab = ba = 1$



##### 定义 4.4

设环  $R, S$ , 称映射  $\varphi: R \rightarrow S$  是一个环同态, 如果  $\forall a, b \in R$  成立:

1.  $\varphi(a+b) = \varphi(a) + \varphi(b)$ ;
2.  $\varphi(ab) = \varphi(a)\varphi(b)$ ;
3.  $\varphi(1_R) = 1_S$



##### 命题 4.2

设  $\varphi: R \rightarrow S$  是环同态, 则以下命题成立:

1.  $\varphi(0_R) = 0_S$ ;
2.  $\varphi(-a) = -\varphi(a), \forall a \in R$



##### 定义 4.5

设  $\varphi: R \rightarrow S$  是环同态, 则  $\varphi$  的核定义为:  $\ker \varphi = \varphi^{-1}(0_S)$



##### 命题 4.3

$\varphi$  是单射  $\Leftrightarrow \ker \varphi = \{0_R\}$



**定义 4.6**

1. 称  $0 \neq a \in R$  是零因子 (zero-divisor), 如果  $\exists 0 \neq b \in R$ , 使得  $ab = 0$  或  $ba = 0$ ;
2. 称  $u \in R$  是可逆元 (unit) 或单位, 如果  $\exists v \in R$ , 使得  $uv = vu = 1$ . 记  $R$  中可逆元组成的集合为  $R^\times$
3. 称环  $R$  是整环 (integral domain), 如果  $R$  交换且没有零因子



整环满足消去律

**例题 4.1**

1.  $\mathbb{Z}_n^\times = \{a \bmod n \mid (a, n) = 1\}$ .  $\mathbb{Z}_n$  的零因子是  $\{a \bmod n \mid (a, n) \neq 1, a \bmod n \neq 0 \bmod n\}$ ;
2. 设  $R$  是整环, 则  $R[X]$  也是整环 (首项系数非 0)

下面的命题给出了整环和域之间的关系

**命题 4.4**

有限整环是域



**证明** 对  $a \in R, a \neq 0$ , 我们定义映射

$$\varphi_a : R \rightarrow R$$

$$x \mapsto ax$$

这显然是一个加法群同态. 域是非零元都有逆的交换环, 因此只需要证明  $1 \in \varphi_a(R)$ , 这也表明  $\varphi_a$  是满的. 由于  $R$  有限, 因此满等价于单, 我们只需要考虑  $\varphi_a$  的单性即可.  $\ker \varphi_a = \{b \in R \mid ab = 0\} = \{0\}$ , 得证

**4.1.2 理想**

我们知道, 在群论中构造商群需要正规子群, 那么自然的, 想要构造商环, 我们就需要思考正规子群在环论中的类比概念是什么? 这就引入了理想的概念

**定义 4.7**

设  $R$  是环,  $I \subset R$  是  $R$  的左理想, 如果满足:

1.  $\forall a, b \in I, a + b \in I$ ;
2.  $\forall a \in I, r \in R, ra \in I$ .

类似的,  $I \subset R$  是  $R$  的右理想, 如果满足:

1.  $\forall a, b \in I, a + b \in I$ ;
2.  $\forall a \in I, r \in R, ar \in I$ .

$I$  是  $R$  的 (双边) 理想, 如果  $I$  既是左理想又是右理想.



一般情况下, 理想  $I$  不是一个环, 因为如果  $1_R \in I$ , 则  $I = R$ .

**定义 4.8**

设  $I \subsetneq R$  是理想, 定义商环  $R/I = \{x + I \mid x \in R\}$ , 带有如下两个二元运算:

- $(x + I) + (y + I) = x + y + I$ ;
- $(x + I)(y + I) = xy + I$ .



此时我们有自然的满环同态:

$$\pi : R \rightarrow R/I$$

$$x \mapsto x + I$$

其中  $\ker \pi = I$  我们在前面提到, 同态核的定义只涉及加法运算, 而没有涉及乘法运算, 因此核应该具有更多的结构, 事实上, 核就是一个理想.



**定理 4.1**

设  $\varphi: R \rightarrow S$  是环同态, 则  $\ker \varphi$  是  $R$  的理想,  $\varphi(R)$  是  $S$  的子环, 且存在环同构

$$\bar{\varphi}: R/\ker \varphi \rightarrow \varphi(R)$$

$$x + \ker \varphi \mapsto \varphi(x)$$

**定理 4.2**

设  $I \subset J \subset R$  是理想, 则  $J/I \subset R/I$  是理想且存在同构

$$(R/I)/(J/I) \cong R/J$$

**定义 4.9**

设  $R$  是交换环,  $\{a_i \mid i \in S\}$ , 其中  $S$  为某个指标集, 记  $\{a_i \mid i \in S\}$  生成的理想为

$$(a_i \mid i \in S) = \left\{ \text{有限和} \sum_{i \in S} r_i a_i \mid r_i \in R \right\}$$

如果  $|S| = n < \infty$ , 则

$$(a_1, a_2, \dots, a_n) = \left\{ \sum_{i=1}^n r_i a_i \mid r_i \in R \right\}$$

**例题 4.2**

1.  $R = \mathbb{Z}, (4, 6) = \{4x + 6y \mid x, y \in \mathbb{Z}\} = 2\mathbb{Z} = (2)$ ;
2. 设  $R$  是交换环,  $a \in R$ , 考虑赋值映射:

$$\varphi_a: R[x] \rightarrow R$$

$$f(x) \mapsto f(a)$$

我们考虑  $\ker \varphi_a = \{f(x) \in R[x] \mid f(a) = 0\} = (x - a)$ , 因此由第一同构定理得  $R[x]/(x - a) \cong R$

3. 考虑

$$\varphi: \mathbb{R}[x] \rightarrow \mathbb{C}$$

$$f(x) \mapsto f(i)$$

而  $\ker \varphi = (x^2 + 1)$ , 因此  $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$

上述例子可以让我们看到商环的实际意义, 即在生成元中添加关系. 在上述例 3 中, 实际上我们在  $\mathbb{R}[x]$  中额外添加了生成关系  $x^2 + 1 = 0$ , 这使得  $\mathbb{R}[x]$  与  $\mathbb{C}$  有相同的结构

下面介绍理想的一些操作

**定义 4.10**

设  $I, J$  是  $R$  的理想, 则

1.  $I + J = \{a + b \mid a \in I, b \in J\}$  称为理想  $I, J$  的和;
2.  $IJ = \left\{ \text{有限和} \sum_{i=1}^n a_i b_i \mid a_i \in I, b_i \in J, n \geq 0 \right\}$  称为理想  $I, J$  的积



## 4.2 中国剩余定理, 欧式整环和主理想整环

### 4.2.1 中国剩余定理

本节我们将证明一般的中国剩余定理, 先回顾中国剩余定理.

**定理 4.3 (中国剩余定理)**

设  $n_1, n_2, \dots, n_r$  是两两互素的整数, 则

$$\begin{aligned}\varphi: \mathbb{Z} &\rightarrow \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z} \\ a &\mapsto (a \bmod n_1, \dots, a \bmod n_r)\end{aligned}$$

是满射且  $\ker \varphi = n_1\mathbb{Z} \cap \cdots \cap n_r\mathbb{Z} = n_1 \cdots n_r\mathbb{Z}$ , 于是

$$\mathbb{Z}/n_1 \cdots n_r\mathbb{Z} \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$$

**定义 4.11**

设  $I, J$  都是交换环  $R$  的理想, 我们称  $I, J$  是 comaximal, 如果  $I + J = R$



下面给出环论中一般的中国剩余定理

**定理 4.4**

设  $R$  是交换环,  $I_1, I_2, \dots, I_r$  两两 comaximal, 那么

1.  $I_1 \cap I_2 \cap \cdots \cap I_r = I_1 I_2 \cdots I_r$ ;
2.  $\varphi: R \rightarrow R/I_1 \times \cdots \times R/I_r$  是满射.

于是  $R/I_1 I_2 \cdots I_r \cong R/I_1 \times \cdots \times R/I_r$



**证明** The first claim on  $\phi$  being a homomorphism with kernel  $I_1 \cap \cdots \cap I_k$  is clear. We now prove (1) and (2).

We first assume that  $k = 2$ . As  $I_1 I_2 \subseteq I_1$  and  $I_1 I_2 \subseteq I_2$ , we have  $I_1 I_2 \subseteq I_1 \cap I_2$ . Now, if  $R = I_1 + I_2$ , we may write  $1 = a_1 + a_2$  with  $a_1 \in I_1$  and  $a_2 \in I_2$ . Then for  $b \in I_1 \cap I_2$

$$b = \underbrace{ba_1}_{\text{in } I_2 I_1} + \underbrace{ba_2}_{\text{in } I_1 I_2} \in I_1 I_2.$$

This implies that  $I_1 I_2 = I_1 \cap I_2$ .

To see that  $\phi$  is surjective in this case, we note that

$$\begin{aligned}\phi(a_1) &= (a_1 \bmod I_1, a_1 = 1 - a_2 \bmod I_2) = (0, 1); \\ \phi(a_2) &= (a_2 = 1 - a_1 \bmod I_1, a_2 \bmod I_2) = (1, 0);\end{aligned}$$

Thus, for any  $(x_1 \bmod I_1, x_2 \bmod I_2) \in A/I_1 \times A/I_2$ , it is  $\phi(a_1 x_2 + a_2 x_1)$ .

In general, we use induction to show

$$\phi: R \longrightarrow R/I_1 \times R/I_2 \cdots I_k \twoheadrightarrow R/I_1 \times \cdots \times R/I_k.$$

For this, we need to check  $I_1$  and  $I_2 \cdots I_k$  are comaximal, i.e.  $I_1 + I_2 \cdots I_k = R$ . This is because for each  $i = 2, \dots, k$ ,  $1 = a_i + b_i$  for  $a_i \in I_1$  and  $b_i \in I_i$ . Thus

$$1 = (a_2 + b_2) \cdots (a_k + b_k) = \underbrace{a_2 \cdots a_k + \text{product with some } a_i}_{\text{in } I_1} + \underbrace{b_1 \cdots b_k}_{\text{in } I_2 \cdots I_k}.$$

**4.2.2 极大理想**

下面介绍两类特殊的理想.

**定义 4.12**

设  $R$  是环, 理想  $\mathfrak{m}$  是  $R$  的极大理想, 如果  $\mathfrak{m} \neq R$  且包含  $\mathfrak{m}$  的理想只有  $\mathfrak{m}$  和  $R$



**命题 4.5**

任何真理想包含于某个极大理想中



下述命题给出了判断极大理想的重要方法

**命题 4.6**

设  $R$  是交换环, 则真理想  $\mathfrak{m} \subset R$  是极大理想当且仅当商环  $R/\mathfrak{m}$  是域



**证明** 由对应定理, 我们知道包含  $\mathfrak{m}$  的理想和  $R/\mathfrak{m}$  的理想是一一对应的, 因此  $\mathfrak{m}$  是极大理想等价于  $R/\mathfrak{m}$  的理想只有零理想和  $R$  本身, 于是只要证明交换环  $R$  的理想只有零理想和  $R$  本身等价于  $R$  是域, 这是容易的

**例题 4.3**

1. 对  $\mathbb{Z}$ , 由于  $\mathbb{Z}/p\mathbb{Z}$  是域, 因此  $(p) = p\mathbb{Z}$  是极大理想;
2. 由于  $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$ , 因此  $(x^2 + 1)$  是  $\mathbb{R}[x]$  的极大理想;
3. 对  $a \in \mathbb{R}$ , 由于  $\mathbb{R}[x]/(x - a) \cong \mathbb{R}$ , 因此  $(x - a)$  是  $\mathbb{R}[x]$  的极大理想;

**4.2.3 素理想****定义 4.13**

设  $R$  是交换环, 称真理想  $\mathfrak{p} \subset R$  是素理想, 如果对任意  $a, b \in R, ab \in \mathfrak{p} \Rightarrow a \in \mathfrak{p}$  或  $b \in \mathfrak{p}$



素理想实际上是对整数环  $\mathbb{Z}$  的由素数  $p$  生成的理想的模仿, 因为如果  $ab \in (p)$ , 就有  $p \mid ab$ , 那么  $p \mid a$  或  $p \mid b$ . 另外  $p\mathbb{Z}[x]$  是  $\mathbb{Z}[x]$  的素理想, 不过这不显然, 我们可以通过下面的命题得出.

**命题 4.7**

设  $R$  是交换环, 则真理想  $\mathfrak{p} \subset R$  是素理想当且仅当商环  $R/\mathfrak{p}$  是整环



**证明**

**推论 4.1**

在交换环中, 极大理想一定是素理想



下面介绍三类特殊的整环, 它们发源于整数环相比于一般的整环所额外具有的性质.

**定义 4.14**

由一个元素生成的理想  $(a) = aR$  称为主理想. 如果整环  $R$  的每个理想都是主理想, 称  $R$  是主理想整环 (principal ideal ring; PID)



我们说在交换环中, 极大理想一定是素理想, 但反之不对. 但在 PID 中, 极大理想和素理想几乎是一样的, 只差了一个零理想.

**命题 4.8**

PID 中的每个非零素理想都是极大理想

**例题 4.4**

1.  $\mathbb{Z}$  是一个 PID;
2. 设  $F$  是域, 则  $F[x]$  是一个 PID;
3. Gauss 整数环 (Ring of Gauss integers)  $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$

我们现在不证明上述结论, 因为它们属于一类更特殊的 PID, 即欧式整环 (Euclidean domain)

**推论 4.2**

在整数环  $\mathbb{Z}$  中, 非零真理想  $I$  是素理想当且仅当  $I = (p)$ , 其中  $p$  是素数



**证明** 对于  $\mathbb{Z}$  中非零真理想  $I$ , 由于  $\mathbb{Z}$  是 PID, 因此存在  $a \in \mathbb{Z}_{>0}$ , 使得  $I = (a)$ .  $\mathbb{Z}/I = \mathbb{Z}/(a)$  是域当且仅当  $a$  为素数. 因此  $I = (p) \Leftrightarrow I$  是极大理想  $\Leftrightarrow I$  是素理想

**命题 4.9**

设  $R, S$  是交换环,  $\varphi: R \rightarrow S$  是环同态,  $\mathfrak{p}$  是  $S$  的素理想, 则  $\varphi^{-1}(\mathfrak{p})$  是  $R$  的素理想.



**证明** 我们考虑同态

$$\begin{aligned} f: R &\rightarrow S/\mathfrak{p} \\ r &\mapsto \varphi(r) + \mathfrak{p} \end{aligned}$$

因此  $\ker f = \varphi^{-1}(\mathfrak{p})$ , 由第一同构定理, 得  $R/\varphi^{-1}(\mathfrak{p}) \cong S/\mathfrak{p}$ , 故  $\varphi^{-1}(\mathfrak{p})$  是  $R$  的素理想.

**推论 4.3**

设  $R, S$  都是交换环, 且  $S$  是  $R$  的子环, 设  $\mathfrak{p}$  是  $R$  的素理想, 则  $\mathfrak{p} \cap S$  是  $S$  的素理想



**证明** 取上述的  $\varphi$  为嵌入映射即可

## 4.3 唯一分解整环

### 4.3.1 欧式整环

**定义 4.15**

设  $R$  是整环, 如果存在函数  $N: R \rightarrow \mathbb{Z}_{\geq 0}$ , 满足

1.  $N(0) = 0$ ;
2. 对任意  $a, b \in R, b \neq 0$ , 存在  $q, r \in R$ , 使得  $a = qb + r$ , 且  $r = 0$  或  $N(r) < N(b)$ .

此时称  $R$  为欧式整环 (Euclidean domain)



通过赋予以下整环合适的范数, 我们可以证明以下整环都是 ED.

**例题 4.5**

1.  $F$  是域, 令  $N(a) = 0, \forall a \in F$ ;
2.  $\mathbb{Z}$ , 令  $N(a) = |a|$ ;
3.  $F[X]$ , 令  $N(f(x)) = \deg f(x)$ ;
4.  $\mathbb{Z}[i]$ , 令  $N(a + bi) = |a + bi|^2 = a^2 + b^2$

我们说过 ED 是更特殊的 PID, 现在证明 ED 都是 PID, 这里的思想和辗转相除法一致.

**命题 4.10**

欧式整环  $R$  是主理想整环.



**证明**  $R$  的零理想显然是主理想, 因此取非零理想  $I \subset R$ , 我们取  $b \in I - \{0\}$ , 使得  $N(b)$  最小, 这是可以做到的, 因为这是在自然数集中取值.  $\forall a \in I$ , 有  $a = qb + r$ , 也即  $r = a - qb \in I$ , 其中  $r = 0$  或  $N(r) < N(b)$ . 显然由  $b$  的选取方式知  $r = 0$ , 即  $a = qb, a \in (b)$ . 再由  $a$  的任意性, 知  $I = (b)$

### 4.3.2 素数在一般整环中的推广

正如我们前面所说的, 我们对环的研究是在模仿  $\mathbb{Z}$  中所具有的性质, 而素数在  $\mathbb{Z}$  中至关重要, 因此我们考虑将素数推广到一般的整环中.

#### 定义 4.16

设  $R$  是整环, 有如下定义:

1. 对  $a, b \in R, a \neq 0$ , 称  $a \mid b$ , 如果存在  $c \in R$ , 使得  $b = ac$  (也即  $b \in (a)$ );
2. 对  $p \in R, p \neq 0$ , 如果  $p \mid ab \Rightarrow p \mid a$  或  $p \mid b$ , 则称  $p$  为素元;
3. 设  $r$  不是零元也不是单位, 如果  $r = ab \Rightarrow a \in R^\times$  或  $b \in R^\times$ , 则称  $r$  是不可约元;
4. 设  $a, b \in R$ , 称  $a, b$  是相伴的, 如果存在  $u \in R^\times$ , 使得  $a = bu$ .



#### 注

1. 相伴关系是一种等价关系;
2.  $a, b \neq 0$  是相伴的  $\Leftrightarrow a \mid b, b \mid a$ ;
3. 相伴元素生成的理想是相同的.

#### 证明

在整数环, 所有素数都是不可约的, 同样我们也可以把这一结论推广到一般的整环. 下面的命题还给出了在 PID 中, 不可约元和素元是一样的

#### 命题 4.11

1. 在整环中, 素元一定是不可约元;
2. 在 PID 中, 不可约元一定是素元.



#### 证明

#### 定义 4.17

称整环  $R$  是唯一分解整环 (unique factorization domain; UFD), 如果对  $R$  中非零非单位元  $r$ , 满足:

1.  $r = p_1 p_2 \cdots p_n$ , 其中  $p_i$  都是不可约元;
2. 以上分解在重排和相伴的意义下是唯一的, 即如果  $r = q_1 q_2 \cdots q_m$  是  $r$  的另一个不可约分解, 则  $n = m$ , 且存在  $\sigma \in S_n$ , 使得  $p_i$  和  $q_{\sigma(i)}$  相伴



我们有两个主要的结论需要证明

1.  $\text{PID} \Rightarrow \text{UFD}$ ;
2.  $R$  是  $\text{UFD} \Leftrightarrow R[x]$  是  $\text{UFD}$ .

前面我们说 PID 中的不可约元都是素元, 事实上我们可以对这个命题加强, 证明在 UFD 中不可约元都是素元

#### 命题 4.12

在 UFD 中, 非零元素  $p$  是素元等价于  $p$  是不可约元



UFD 的重要意义是我们可以定义最大公因式

#### 定理 4.5

如果  $R$  是 PID, 则  $R$  一定是 UFD



### 4.3.3 唯一分解整环在 Gauss 整数环中的应用

考虑 Gauss 整数环  $\mathbb{Z}[i]$ , 这是一个 ED, 因此也是一个 PID, UFD. 考虑其上的范数

$$N: \mathbb{Z}[i] \rightarrow \mathbb{Z}_{\geq 0}$$

$$x + yi \mapsto x^2 + y^2 = |x + yi|^2$$

同时由复数的运算性质, 容易得到  $\mathbb{Z}[i]^\times = \{a \in \mathbb{Z}[i] \mid N(a) = 1\} = \{1, -1, i, -i\}$

#### 定理 4.6 (Fermat 平方和定理)

素数  $p$  是两个整数的平方和当且仅当  $p = 2$  或  $p \equiv 1 \pmod{4}$

上述定理实际在对  $\mathbb{Z}[i]$  中的不可约元进行分类后可以简单推得

#### 定理 4.7

Gauss 整数环  $\mathbb{Z}[i]$  中的不可约元一定是如下形式 (在相伴的意义下):

1.  $1 + i$  ( $Norm = 2$ );
2. 素数  $p$ , 使得  $p \equiv 3 \pmod{4}$  ( $Norm = p^2$ );
3.  $x + yi$  和  $x - yi$ , 其中  $p = x^2 + y^2$ , 对  $x, y \in \mathbb{Z}$ , 且素数  $p \equiv 1 \pmod{4}$  ( $Norm = p$ )

**证明** 证明分为三步

1. 证明范数为素数的元素都是不可约元.

设  $\pi \in \mathbb{Z}[i]$ ,  $N(\pi) = p$  是素数. 令  $\pi = ab$ , 则  $p = N(\pi) = N(a)N(b)$ , 从而  $N(a) = 1$  或  $N(b) = 1$ , 因此  $a, b$  中一定有一个是单位, 故  $\pi$  不可约;

2. 任一不可约元的范数一定是  $p$  或  $p^2$ , 其中  $p$  为素数.

设  $\pi \in \mathbb{Z}[i]$ ,  $\pi$  是不可约元, 我们考虑  $(\pi) \cap \mathbb{Z}$ , 证明  $(\pi) \cap \mathbb{Z}$  是  $\mathbb{Z}$  的素理想. 考虑  $a, b \in \mathbb{Z}$ ,  $ab \in (\pi) \cap \mathbb{Z}$ , 也即  $ab \in (\pi)$ . 由于  $\mathbb{Z}[i]$  是一个 ED, 从而  $\pi$  作为不可约元也是素元, 从而  $(\pi)$  是  $\mathbb{Z}[i]$  的素理想, 将  $a, b$  看成  $\mathbb{Z}[i]$  中的元素, 有  $ab \in (\pi)$  蕴含  $a \in (\pi)$  或  $b \in (\pi)$ , 从而  $a \in (\pi) \cap \mathbb{Z}$  或  $b \in (\pi) \cap \mathbb{Z}$ , 即  $(\pi) \cap \mathbb{Z}$  是  $\mathbb{Z}$  的素理想. 整数环的非零素理想一定是由素数生成的主理想, 从而存在素数  $p$  使得  $(\pi) \cap \mathbb{Z} = (p)$ , 从而存在  $b \in \mathbb{Z}[i]$ , 使得  $p = \pi b$ , 两边取范数, 得  $p^2 = N(p) = N(\pi)N(b)$ , 从而  $N(\pi) = p^2$  或  $N(\pi) = p$ .

- $N(\pi) = p^2$ , 则  $N(b) = 1$ , 从而  $\pi$  与  $p$  相伴;
- $N(\pi) = p$ , 则这个素数  $p$  可以实现为某个不可约元的范数, 即可以写成平方和

3. 对不可约元进行分类

- $p = 2 = (1 + i)(1 - i) = N(1 + i)$ , 因此  $1 + i$  是不可约元;
- $p \equiv 3 \pmod{4}$ . 我们断言  $p$  在  $\mathbb{Z}[i]$  中是不可约的. 否则设  $p = \pi b$ , 其中  $\pi$  为不可约元,  $b$  非单位, 两边取范数, 得  $p^2 = N(p) = N(\pi)N(b)$ . 由于  $N(b) > 1$ , 因此  $N(\pi) = p$ , 于是  $p = x^2 + y^2 \equiv 3 \pmod{4}$ , 但这是不可能的, 因为  $x^2 \equiv 0, 1 \pmod{4}$ , 从而  $x^2 + y^2 \equiv 0, 1, 2 \pmod{4}$ . 因此  $p$  不可约.
- $p \equiv 1 \pmod{4}$ . 我们希望证明  $p$  是可约, 因为我们在上面看到, 素数  $p$  如果可约, 就可以写出平方和的形式. 考虑  $\mathbb{Z}_p^\times \cong \mathbb{Z}_{p-1}$ , 由于  $p \equiv 1 \pmod{4}$ , 因此  $\mathbb{Z}_{p-1}$  中一定有 4 阶元, 也即  $\mathbb{Z}_p^\times$  中存在 4 阶元, 故存在  $a \in \mathbb{Z}$ , 使得

$$a^4 \equiv 1 \pmod{p}$$

$$a^2 \not\equiv 1 \pmod{p}$$

从而  $p \mid (a^2 + 1) = (a + i)(a - i)$ . 假设  $p$  是不可约元, 则在  $\text{UFD}\mathbb{Z}[i]$  中,  $p$  也是素元, 故  $p \mid a + i$  或  $p \mid a - i$ , 显然矛盾, 从而  $p$  可约.



## 4.3.4 一些不是 UFD 的例子

## 4.4 UFD 的多项式环的性质

## 4.4.1 UFD 上的多项式环

## 引理 4.1 (Gauss 引理)

设  $R$  是 UFD,  $F = \text{Frac}(R)$ , 对于  $f(x) \in R[x]$ , 如果  $f(x)$  在  $F[x]$  上可约, 则  $f(x)$  在  $R[x]$  上也可约.



## 4.4.2 多项式不可约的判别法

## 命题 4.13 (Eisenstein 判别法)

设  $R$  是整环,  $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in R[x]$ , 如果存在  $R$  的素理想  $\mathfrak{p}$ , 使得

1.  $a_i \in \mathfrak{p}, i = 0, 1, \cdots, n-1$ ;
2.  $a_0 \notin \mathfrak{p}^2$ .

则  $f(x)$  在  $R[x]$  上不可约.



## 4.4.3 多项式环商多项式的因式分解

## 引理 4.2

设  $F$  是域 (此时  $F[x]$  是 ED), 则多项式  $f(x)$  不可约当且仅当  $F[x]/(f(x))$  是域.



**证明** 当  $F$  是域时,  $F[x]$  是 ED, 因此也是 PID, UFD. 则

$$\begin{aligned} f(x) \text{ 不可约} &\Leftrightarrow f(x) \text{ 是素元} \Leftrightarrow (f(x)) \text{ 是素理想} \\ &\Leftrightarrow (f(x)) \text{ 是极大理想} \\ &\Leftrightarrow F[x]/(f(x)) \text{ 是域} \end{aligned}$$

## 定理 4.8

设  $F$  是域,  $f(x) \in F[x]$ ,  $f(x) = p_1(x)^{n_1} \cdots p_r(x)^{n_r}$  是  $f(x)$  的不可约分解, 则

$$\frac{F[x]}{(f(x))} \cong \frac{F[x]}{(p_1(x)^{n_1})} \times \frac{F[x]}{(p_2(x)^{n_2})} \times \cdots \times \frac{F[x]}{(p_r(x)^{n_r})}$$



**证明** 由于  $p_i(x)^{n_i}$  两两互素, 因此  $(p_i(x)^{n_i}) + (p_j(x)^{n_j}) = (\gcd(p_i(x)^{n_i}, p_j(x)^{n_j})) = (1), \forall i \neq j$ , 即  $p_i(x)^{n_i}$  与  $p_j(x)^{n_j}$  comaximal, 于是由中国剩余定理, 马上得到结论

## 引理 4.3

设  $F$  是域,  $f(x) \in F[x]$  有不同的零点  $\alpha_1, \cdots, \alpha_n$ , 则  $(x - \alpha_1) \cdots (x - \alpha_n) \mid f(x)$ . 特别地, 次数为  $n$  的多项式至多有  $n$  个根.



## 推论 4.4

设  $F$  是域,  $G$  是  $F$  的有限子群, 则  $G$  是循环群. 特别地, 如果  $F$  是有限群, 则  $F^\times$  是循环群.



**证明** 设  $|G| = n$ , 由于  $F$  是域, 因此  $G$  是有限生成的 Abel 群, 由有限生成的 Abel 群的分类定理, 得到

$$G \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}$$

其中  $n_1 \mid n_2 \mid \cdots \mid n_r, n = n_1 + \cdots + n_r$

假设  $G$  不是循环群, 则  $r > 1, n_r < n$ , 但  $\forall g \in G, g^{n_r} = 1$ , 于是  $x^{n_r} - 1$  有  $n$  个根, 矛盾!

## 第5章 域论与 Galois 理论

### 5.1 域扩张

我们遵循以下主线:

1. 从所谓素域出发, 即  $\mathbb{Q}$  和  $\mathbb{F}_p$ , 最小的域;
2. 从已知域去构造更大的域.

但是这两个域似乎相去甚远, 但它们实际上是由不同特征的域导出的素域.

#### 5.1.1 域的特征

设  $F$  是域, 我们考虑以下环同态:

$$\begin{aligned}\varphi: \mathbb{Z} &\rightarrow F \\ n &\mapsto n \cdot 1_F\end{aligned}$$

由于我们要求环同态把 1 映到 1, 因此上述环同态实际上是唯一的. 由第一同构定理, 得到

$$\mathbb{Z}/\ker \varphi \cong \varphi(\mathbb{Z}) \subset F$$

由于  $F$  是域, 因此  $F$  一定是整环, 从而  $\varphi(\mathbb{Z})$  也是整环, 故  $\ker \varphi$  是  $\mathbb{Z}$  的素理想, 从而  $\ker \varphi = 0$  或  $\ker \varphi = p\mathbb{Z}$ , 这就引出  $F$  的特征的概念

##### 定义 5.1 (域的特征)

设  $F$  是域, 对环同态  $\varphi: \mathbb{Z} \rightarrow F$

- 如果  $\ker \varphi = p\mathbb{Z}$ , 则定义  $\text{char} F = p$ ;
- 如果  $\ker \varphi = 0$ , 则定义  $\text{char} F = 0$ .

换句话说,  $\text{char} F$  是使得  $n \cdot 1_F = 0$  最小的正整数  $n$ , 如果这个  $n$  存在; 否则  $\text{char} F = 0$ .



##### 定义 5.2 (素域)

域  $F$  的素域是包含  $1_F$  的最小的域, 根据  $F$  的特征, 有如下两种情况:

- $\mathbb{F}_p$ , 如果  $\text{char} F = p$ ;
- $\mathbb{Q}$ , 如果  $\text{char} F = 0$ .



#### 5.1.2 域扩张

##### 定义 5.3

设  $F \subset K$  都是域, 则称  $K$  是  $F$  的域扩张, 记作  $K/F$ . 如果  $E$  是满足  $F \subset E \subset K$  的域, 则称  $E$  是  $K/F$  的中间域.



由于  $K$  可以看作  $F$  上的线性空间, 因此有了以下定义

##### 定义 5.4

域扩张  $K/F$  的次数定义为  $\dim_F K$ , 记作  $[K:F]$ , 即  $[K:F] = \dim_F K$ .

我们称域扩张  $K/F$  是有限(无限)的, 如果  $[K:F] < \infty (= \infty)$



**定理 5.1**

设  $F \subset E \subset K$  都是域, 则  $[K : F] = [K : E][E : F]$



注

1.  $[K : E] = \infty \Rightarrow [K : F] = \infty$ ;
2.  $[E : F] = \infty \Rightarrow [K : F] = \infty$ ;
3.  $[K : F] = \infty, [K : E], [E : F]$  至少一个无限;
4. 如果  $[K : F] < \infty$ , 则  $[E : F], [K : E] \mid [K : F]$ .

**5.1.3 域扩张的构造****引理 5.1**

设  $F, E$  都是域, 则同态

$$\varphi : F \rightarrow E$$

是单射, 即  $E$  可以视为  $\varphi(F) \cong F$  的域扩张.



**证明** 考虑  $\ker \varphi$ , 其为域  $F$  的理想, 而域的理想只有零理想和本身, 但  $\varphi(1_F) = 1_E$ , 从而  $\ker \varphi \neq F$ , 故  $\ker \varphi = 0$ ,  $\varphi$  为单射

设  $F$  是域,  $p(x) \in F[x]$  是  $n$  次不可约多项式. 由于  $F[x]$  是 ED, 从而也是 PID, 因此  $p(x)$  是  $F[x]$  上的素元, 故  $(p(x))$  是素理想也是极大理想, 这表明:

$$K := F[x]/(p(x))$$

是域. 设  $\theta := x + (p(x)) \in K$ . 那么

$$K = \{a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1} \mid a_0, \dots, a_{n-1} \in F\}.$$

显然  $K$  是  $F$  上的  $n$  维线性空间, 且  $F$  嵌入到  $K$  中作为常数多项式. 我们称  $K$  是  $F$  由  $p(x)$  决定的  $n$  次扩张.

**引理 5.2**

方程  $p(x) = 0$  在  $K$  中一定有零点.



**证明** 显然  $p(\theta) = 0$ .

**例题 5.1**

1. 我们知道

$$\mathbb{R}[x]/(x^2 + 1) \xrightarrow{\cong} \mathbb{C}$$

$$a + bx \mapsto a + bi$$

$\mathbb{R}[x]/(x^2 + 1)$  是  $\mathbb{R}$  的一个抽象的域扩张, 它同构于  $\mathbb{C}$ , 我们有两种同构方式

$$\phi_1, \phi_2 : \mathbb{R}[x]/(x^2 + 1) \xrightarrow{\cong} \mathbb{C}$$

$$\phi_1(a + bx) = a + bi \quad \phi_2(a + bx) = a - bi$$

**定义 5.5**

设  $K/F$  是域扩张,  $\alpha_1, \alpha_2, \dots, \alpha_n \in K$

1. 域  $F$  由  $\alpha_1, \alpha_2, \dots, \alpha_n$  生成的域扩张是包含  $F$  和  $\alpha_1, \alpha_2, \dots, \alpha_n$  的  $K$  的最小子域, 记作  $F(\alpha_1, \alpha_2, \dots, \alpha_n)$ ;
2. 如果  $K = F(\alpha)$ , 对某个  $\alpha \in K$ , 称  $K/F$  是单扩张;
3. 如果  $K = F(\alpha_1, \alpha_2, \dots, \alpha_n)$ , 则称  $K/F$  是有限生成扩张.



下面这个命题帮助我们看清这个扩域到底包含怎么样的元素

### 命题 5.1

设  $K/F$  是域扩张, 对  $\alpha, \alpha_i \in K$ , 则有

1. 子域  $F(\alpha)$  由以下形式的元素组成:  $f(\alpha)/g(\alpha)$ , 其中  $f, g \in F[x]$ , 且  $g(\alpha) \neq 0$ ;
2. 子域  $F(\alpha_1, \alpha_2, \dots, \alpha_n)$  由以下元素组成:  $h(\alpha_1, \alpha_2, \dots, \alpha_n)/k(\alpha_1, \alpha_2, \dots, \alpha_n)$ , 其中  $h, k \in F[x_1, x_2, \dots, x_n]$ , 且  $k(\alpha_1, \alpha_2, \dots, \alpha_n) \neq 0$ .



下面定理给出了单扩张的完整刻画, 它告诉我们, 如果添加元素  $\alpha$  可以实现为  $F[x]$  中某个  $n$  次不可约多项式  $p(x)$  的根, 则  $F(\alpha) \cong F[x]/(p(x)) = \{a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1} \mid a_0, \dots, a_{n-1} \in F\}$ ; 如若不能, 则  $F(\alpha) \cong \text{Frac}(F[x])$ , 即同构于  $F$  上的有理函数域.

### 定理 5.2

设  $K/F$  是域扩张,  $\alpha \in K$ , 则有如下情况二选一:

1. 要么  $1, \alpha, \alpha^2, \dots$  在  $F$  上线性无关, 则  $F(\alpha) \cong \text{Frac}(F[x]) := F(x)$ ;
2. 或  $1, \alpha, \alpha^2, \dots$  在  $F$  上线性相关, 则存在唯一的首一不可约多项式  $m_\alpha(x) \in F[x]$ , 使得  $m_\alpha(\alpha) = 0$ , 称为  $\alpha$  在  $F$  上的极小多项式. 在这种情况下,  $F(\alpha) \cong F[x]/(m_\alpha(x))$  是  $F$  的  $\deg m_\alpha(x)$  次域扩张.



**证明** 我们考虑同态

$$\begin{aligned}\varphi: F[x] &\rightarrow K \\ f(x) &\mapsto f(\alpha)\end{aligned}$$

1. 由于  $1, \alpha, \alpha^2, \dots$  线性无关, 因此  $\ker \varphi = 0$ , 即  $\varphi$  是单射. 因此  $\varphi$  可以扩充成

$$\begin{aligned}\varphi: F(x) &\hookrightarrow K \\ f(x)/g(x) &\mapsto f(\alpha)/g(\alpha)\end{aligned}$$

因为  $g(\alpha) \neq 0$ , 则  $F(x) \cong \varphi(F(x)) = F(\alpha)$

2. 此时  $\ker \varphi \neq 0$ , 则  $F[x]/\ker \varphi \cong \varphi(F[x]) \subset K$ , 故  $\ker \varphi$  是非零素理想, 由于  $F[x]$  是 PID, 因此  $\ker \varphi = (m_\alpha(x))$ , 可以取  $m_\alpha(x)$  首一, 因此  $m_\alpha(x)$  是首一不可约多项式, 其次数的最小性是其作为  $\ker \varphi$  的生成元所保证的. 于是  $F[x]/(m_\alpha(x)) \cong \text{Im} \varphi = F[\alpha]$ . 事实上  $F[\alpha]$  是域且  $F[\alpha] \subset F(\alpha)$ , 从而  $F[\alpha] = F(\alpha)$ , 故  $F[x]/(m_\alpha(x)) \cong F(\alpha)$ .

### 定义 5.6

在上述定理的假设下

1. 在第一种情况下, 称  $\alpha$  在  $F$  上是超越的;
2. 在第二种情况下, 称  $\alpha$  在  $F$  上是代数的.

称扩张  $K/F$  是代数扩张, 如果对任意  $\alpha \in K$  在  $F$  上都是代数的, 即  $[F(\alpha) : F] < \infty, \forall \alpha \in K$ .



**注**

1. 如果  $\alpha$  在  $F$  上代数, 则  $\alpha$  在  $F$  的任何扩域上也代数.;
2. 对  $m(x) \in F[x], m(\alpha) = 0$ , 则  $m(x)$  是  $\alpha$  在  $F$  上的极小多项式当且仅当  $m(x)$  在  $F[x]$  上不可约.

### 推论 5.1

设  $F$  是域,  $p(x) \in F[x]$  是不可约多项式,  $\alpha, \beta$  是  $p(x)$  的根, 则

$$F(\alpha) \cong F[x]/(p(x)) \cong F(\beta)$$

即  $F[x]/(p(x))$  就是由  $F$  添加  $p(x)$  的一个根扩张而来.



**命题 5.2**

设  $\varphi: F \rightarrow F'$  是域同构,  $f(x) \in F[x]$  是不可约多项式, 则  $\varphi(f(x)) \in F'[x]$  也是不可约多项式, 且  $F[x]/(f(x)) \cong F'[x]/(\varphi(f(x)))$ .



**证明** 由于  $F[x]$  是 ED, 因此也是 PID, UFD,  $(f(x)) \in F[x]$  是素理想, 因此是极大理想. 从而  $(\varphi(f(x))) \in F'[x]$  也是素理想, 从而  $\varphi(f(x))$  不可约且  $(\varphi(f(x)))$  是极大理想. 由第一同构定理, 得  $F[x]/(f(x)) \cong F'[x]/(\varphi(f(x)))$

**引理 5.3**

设  $K/E/F$  是连续的域扩张, 设  $\alpha \in K$  在  $F$  上代数, 则  $[E(\alpha):E] \leq [F(\alpha):F]$ .



**证明** 由于  $m_{\alpha,F}(x) \in F[x] \subset E[x]$ ,  $m_{\alpha,F}(\alpha) = 0$ , 因此  $m_{\alpha,E}(x) \mid m_{\alpha,F}(x)$ , 从而  $\deg m_{\alpha,E}(x) \leq \deg m_{\alpha,F}(x)$ , 即  $[E(\alpha):E] \leq [F(\alpha):F]$ .

**定义 5.7**

设  $K_1, K_2$  是域扩张  $K/F$  的中间域, 则它们的复合  $K_1K_2$  定义为包含  $K_1, K_2$  的最小的中间域.

**推论 5.2**

如果  $[K_i:F] < \infty, i = 1, 2$ , 则  $[K_1K_2:F] \leq [K_1:F][K_2:F]$ .



事实上我们并没有更精细的结果, 因为上述的不等式是可以严格取到的, 如取  $K_1 = K_2$ , 对一个非平凡扩张, 有严格不等号. 而以下情况, 则可以取等.

**命题 5.3**

如果  $[K_1:F] = m, [K_2:F] = n, (n, m) = 1$ , 则  $[K_1K_2:F] = [K_1:F][K_2:F]$ .



**证明**  $[K_1:F] \mid [K_1K_2:F], [K_2:F] \mid [K_1K_2:F]$ , 结合  $(n, m) = 1$  有  $[K_1:F][K_2:F] \mid [K_1K_2:F]$ , 即  $[K_1:F][K_2:F] \leq [K_1K_2:F]$ , 从而  $[K_1:F][K_2:F] = [K_1K_2:F]$

**定理 5.3**

设  $K/F$  是一个域扩张, 则以下命题等价

1.  $K/F$  是有限扩张;
2.  $K/F$  是有限生成扩张且是代数扩张.

**证明**

1.  $1 \Rightarrow 2$  由于  $K$  在  $F$  上是有限维线性空间, 因此直接考虑  $K$  的一组基  $\alpha_1, \alpha_2, \dots, \alpha_n$ , 从而  $K = F(\alpha_1, \alpha_2, \dots, \alpha_n)$ , 即  $K$  是  $F$  的有限扩张; 对任意  $\alpha \in K$ , 都有  $[F(\alpha):F] \mid [K:F] < \infty$ , 因此  $\alpha$  是代数的.
2.  $2 \Rightarrow 1$

**推论 5.3**

设  $K/F$  是域扩张,  $\alpha, \beta \in K, \beta \neq 0$  在  $F$  上是代数的, 则  $\alpha \pm \beta, \alpha\beta, \alpha/\beta$  在  $F$  上也是代数的, 则  $\{\alpha \in K \mid \alpha \text{ 在 } F \text{ 上代数}\}$  是  $K$  的子域, 叫做  $F$  在  $K$  中的代数闭包.

**推论 5.4**

如果  $K/E, E/F$  都是代数扩张, 则  $K/F$  也是代数扩张.





## 5.2 正规扩张

### 5.2.1 分裂域

#### 定义 5.8

设  $K/F$  是域扩张, 称  $K$  是  $f(x) \in F[x]$  在  $F$  上的分裂域, 如果

1.  $f(x)$  在  $K$  上完全分裂, 即  $f(x) = c(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$ , 其中  $\alpha_1, \alpha_2, \dots, \alpha_n \in K$ ;
2.  $K = F(\alpha_1, \alpha_2, \dots, \alpha_n)$ .



#### 定理 5.4

对  $F[x]$  中的任何  $n$  次多项式  $f(x)$ , 其在  $F$  上的分裂域  $K$  一定存在, 进一步, 有  $[K : F] \leq n!$ .



#### 例题 5.2

1. 取等号的例子:  $x^3 - 2$  在  $\mathbb{Q}$  上的分裂域  $\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$ ,  $[\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3}) : \mathbb{Q}] = 6$ ;
2. 严格小于的例子:  $x^4 + 4$  在  $\mathbb{Q}$  上的分裂域  $\mathbb{Q}(i)$ ,  $[\mathbb{Q}(i) : \mathbb{Q}] = 2$ .

#### 定义 5.9

设代数扩张  $K/F$  是正规扩张, 如果对任意不可约多项式  $t(x) \in F[x]$ ,  $t(x)$  在  $K$  中有零点, 则  $t(x)$  在  $K$  中完全分裂.



#### 定理 5.5

设  $L/E/F$  是域扩张, 且  $E$  是  $F[x]$  中某个多项式  $g(x)$  的分裂域,  $\sigma : L \rightarrow L$  是自同构, 且  $\sigma|_F = \text{id}_F$ , 则  $\sigma(E) = E$ .



#### 定理 5.6

有限扩张  $K/F$  是正规扩张当且仅当  $K$  是  $F[x]$  中某个多项式  $f(x)$  的分裂域.



#### 推论 5.5

如果  $K/F$  是有限正规扩张,  $E$  是  $K/F$  的中间域, 则  $K/E$  是正规扩张.



**注**  $E/F$  不一定是正规的, 如  $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ .

#### 定义 5.10

设  $E/F$  是有限扩张, 如果  $K$  是  $E$  的扩张, 使得

1.  $K/F$  是正规扩张;
2. 如果  $K' \subset K$  是  $F$  的正规扩张, 则  $K = K'$ .

则称  $K$  是  $E/F$  的正规闭包.



#### 引理 5.4

设  $E/F$  是有限扩张, 则  $E/F$  的正规扩张存在且在同构的意义下唯一.



#### 定义 5.11

对于域  $F$ , 如果对任意  $f(x) \in F[x]$ ,  $\deg f(x) \geq 1$ ,  $f(x)$  在  $F$  中至少有一个零点 (等价于  $f(x)$  在  $F$  中完全分裂), 则称  $F$  是一个代数闭域.



**定义 5.12**

称域  $\bar{F}$  是  $F$  的代数闭包, 如果  $\bar{F}/F$  是代数扩张, 且任意  $f(x) \in F[x]$  在  $\bar{F}$  中完全分裂.



**注** 换句话说,  $\bar{F}$  为所有在  $F$  上代数的元素所组成的域.  $F = \bar{F} \Leftrightarrow F$  是代数闭域.

**命题 5.4**

设  $\bar{F}$  是  $F$  的代数闭包, 则  $\bar{F}$  是代数闭域



**证明** 设  $f(x) \in \bar{F}[x]$ ,  $\alpha$  是  $f(x)$  的根. 要证明  $\alpha \in \bar{F}$ , 只要证明  $\alpha$  在  $F$  上代数, 即  $F(\alpha)/F$  是代数扩张. 这点可以利用连续的代数扩张依然是代数扩张证明. 我们知道  $\bar{F}/F$  是代数扩张, 而  $\bar{F}(\alpha)/\bar{F}$  是有限扩张, 从而也是代数扩张, 因此  $\bar{F}(\alpha)/F$  是代数扩张, 特别地  $\alpha$  在  $F$  上代数.

## 5.3 可分扩张和有限域

### 5.3.1 可分多项式

**定义 5.13**

对  $F$  上的不可约多项式  $f(x)$ , 如果  $f(x)$  没有重根 (在它的分裂域内), 则称  $f(x)$  可分, 反之则不可分.



下面推导一个是否有可分的判断定理.

**命题 5.5**

设  $f(x) \in F[x]$ , 则  $f(x)$  在它的分裂域内没有重根当且仅当  $(f(x), f'(x)) = 1$ .



**证明** 设  $(x - \alpha)^2 \mid f(x)$ , 则  $(x - \alpha) \mid f'(x)$ . 由 Bezout 定理, 知  $f(x)g(x) + f'(x)h(x) = 1$ , 对  $g(x), h(x) \in F[x]$ , 从而得到  $(x - \alpha) \mid 1$ , 矛盾! 另一方面,

**推论 5.6**

特征 0 的域  $F$  上的不可约多项式  $f(x)$  一定是可分的.



**证明** 设  $\deg f = n$ , 由于  $\text{char} F = 0$ , 从而  $\deg f' = n - 1$ . 由于  $f$  不可约, 因此如果  $f, f'$  不互素, 必有  $f(x) \mid f'(x)$ , 但  $\deg f' < \deg f$ , 因此不成立.

但上述结论在特征  $p$  的域中不成立, 关键点在于  $\deg f' = n - 1$  对特征  $p$  的域不成立, 下面就来研究特征  $p$  的域. 我们考虑所谓 Frobenius 自同态:

$$\begin{aligned}\sigma : F &\rightarrow F \\ x &\mapsto x^p\end{aligned}$$

我们需要证明映射  $\sigma$  的确是域同态, 由于  $\sigma$  把 0 映到 0, 1 映到 1, 特别地我们只需要证明  $\sigma$  保持减法和乘法即可保持乘法是显然, 而保持减法需要用到二项式展开,  $p \mid \binom{p}{i}, i \neq 0, p$  以及  $(-1)^p = -1$  对任何素数  $p$ . 从而有  $\sigma(x - y) = \sigma(x) - \sigma(y)$ . 我们知道域同态都是单射, 自然的, 我们想知道在什么域内  $\sigma$  会是满射, 从而会成为同构, 有限域就是典型的例子.

**定义 5.14**

如果  $\sigma$  是满射, 则称  $F$  是完全域, 等价的, 每个  $a \in F, a$  都是某个元素的  $p$  次方.

**例题 5.3**

1. 有限域显然是一个完全域;
2. 对  $F = \mathbb{F}_p, \sigma = \text{id}_F$ , 这点可以通过 Fermat 小定理得出.

下面的定理给出了特征  $p$  的域上的不可分多项式的完整刻画.

### 定理 5.7

如果  $\text{char} F = p, f(x) \in F[x]$  不可约且不可分, 则  $f(x) = g(x^p)$ , 其中  $g(x) \in F[x]$  也是不可约多项式. 进一步, 只有非完全域存在不可分多项式.



**证明** 设  $f(x) = a_0 + a_1x + a_2x^2 + \cdots$  是不可约多项式且有重根,  $f'(x) = a_1 + 2a_2x + \cdots + ia_ix^{i-1} + \cdots = 0$ . 因此  $a_i = 0$ , 对任意  $p \nmid i$ , 从而  $f(x) = a_0 + a_px^p + a_{2p}x^{2p} + \cdots = g(x^p)$ , 其中  $g(x) = a_0 + a_px + a_{2p}x^2 + \cdots$ . 显然, 如果  $g(x)$  可约, 则  $f(x)$  也可约, 因此  $g(x)$  不可约. 如果在完全域内, 设  $a_{ip} = b_i^p$ , 从而  $f(x) = b_0^p + b_1^p x^p + \cdots = (b_0 + b_1x + \cdots)^p$ , 即  $f(x)$  可约, 矛盾! 因此完全域上的不可约多项式一定是可分的.

### 推论 5.7

1. 特征  $p$  的有限域上的不可约多项式可分;
2. 设域  $F$  特征  $p, f(x) \in F[x]$  不可约, 则  $f(x) = g(x^{p^e})$ , 其中  $e \geq 0, g(x)$  是可分不可约多项式. 同时  $f(x)$  有  $\deg g(x)$  个不同零点.



### 定义 5.15

设  $K/F$  是代数扩张.

1. 称  $\alpha \in K$  在  $F$  上可分或不可分, 如果  $m_{\alpha, F}(x)$  可分或不可分;
2. 称  $K/F$  是可分扩张, 如果对任意  $\alpha \in K$  均可分.



下面我们给出可分扩张的等价刻画. 设  $K/F$  是有限扩张, 我们设想一个  $K$  的扩张, 使得  $M/F$  是正规扩张. 这是可以做到的, 如取  $K/F$  的正规闭包. 我们要考虑的是,  $K$  要多少种方法嵌入到  $M$  中, 且要保持  $F$ .

### 定义 5.16

$\text{Hom}_F(K, M) = \{\text{域嵌入 } \varphi : K \hookrightarrow M, \text{ s.t. } \varphi|_F = \text{id}_F\}$



### 引理 5.5

设  $m_{\alpha, F}(x) = g(x^{p^e})$ , 其中  $g(x)$  是不可约可分多项式, 那么

$$\sharp \text{Hom}_F(F(\alpha), M) = \deg g(x) \leq \deg m_{\alpha, F}(x) = [F(\alpha) : F]$$

当且仅当  $\alpha$  在  $F$  上可分时取等.



**证明** 由于  $\varphi \in \text{Hom}_F(F(\alpha), M)$  保持  $F$ , 因此对  $m_{\alpha, F}(\alpha) = 0$ , 有  $m_{\alpha, F}(\varphi(\alpha)) = 0$ . 事实上, 由于  $F(\alpha)$  是由  $F$  添加  $\alpha$  生成的, 因此  $\varphi$  完全由  $\varphi(\alpha)$  决定, 又  $\varphi(\alpha)$  也是  $m_{\alpha, F}$  的根, 因此  $\sharp \text{Hom}_F(F(\alpha), M) = \deg g(x)$ . 显然  $\deg g(x) \leq \deg m_{\alpha, F}(x) = [F(\alpha) : F]$ , 当且仅当  $e = 0$ , 即  $\alpha$  可分时取等, 得证.

### 推论 5.8

设  $K/F$  是有限扩张,  $K \subset M$  且  $M/F$  是正规扩张.

1.  $\sharp \text{Hom}_F(K, M) \leq [K : F]$ ;
2. 以下命题等价:
  - (a).  $K = F(\alpha_1, \alpha_2, \cdots, \alpha_n)$ , 其中  $\alpha_i$  在  $F$  上可分;
  - (b).  $\sharp \text{Hom}_F(K, M) = [K : F]$ ;
  - (c).  $K/F$  是可分扩张.



**证明** 由于  $K/F$  是有限扩张, 因此也是有限生成扩张, 设  $K = F(\alpha_1, \alpha_2, \cdots, \alpha_n), \alpha_i \in K$ . 通过逐步添加  $\alpha_i$ , 容易证明  $\sharp \text{Hom}_F(K, M) \leq [K : F]$ , 当且仅当  $\alpha_{i+1}$  在  $F(\alpha_1, \cdots, \alpha_i)$  上可分时取等.

(c)  $\Rightarrow$  (a) 是显然的, (a)  $\Rightarrow$  (b) 也是容易的, 因为  $\alpha_i$  在  $F$  上可分可以推出在  $F(\alpha_1, \cdots, \alpha_{i-1})$  上也可分. 现在证明

(b)  $\Rightarrow$  (c). 假设  $\alpha \in K$  在  $F$  上不可分, 则  $\sharp \text{Hom}_F(F(\alpha), M) < [F(\alpha) : F]$ . 同时  $\sharp \text{Hom}_{F(\alpha)}(K, M) \leq [K : F(\alpha)]$ , 因此  $\sharp \text{Hom}_F(K, M) < [K : F]$ , 矛盾!

**定理 5.8**

1. 如果  $\alpha$  在  $F$  上可分, 则  $F(\alpha)/F$  是可分扩张;
2. 如果  $L/K$  和  $K/F$  是有限可分扩张, 则  $L/F$  也是可分扩张.



**证明** 第一个结论显然. 考虑  $M$  是  $L$  的域扩张, 且  $M/F$  是正规扩张, 则  $M/K$  也是正规扩张. 于是有  $\sharp \text{Hom}_K(L, M) = [L : K]$ ,  $\sharp \text{Hom}_F(K, M) = [K : F]$ , 故  $\sharp \text{Hom}_F(L, M) = [L : F]$ , 即  $L/F$  可分.

**定理 5.9 (本原元素定理)**

任何有限可分扩张  $K/F$  都是单扩张, 即存在  $\theta \in K$ , 使得  $K = F(\theta)$ .

**证明**

下面定理给出了有限域的完整刻画, 它告诉我们, 任何有限域的阶数一定是素数  $p$  的  $n$  次幂, 且在同构的意义下唯一, 可以实现为多项式  $x^{p^n} - x$  的分裂域.

**定理 5.10**

1. 如果  $F$  是有限域, 则  $|F| = p^n$ , 其中  $p = \text{char} F$ ,  $n = [F : \mathbb{F}_p]$ ;
2. 对任何  $n \geq 1$ , 在同构的意义下, 存在唯一的  $F$ , 使得  $|F| = p^n$ . 事实上,  $F$  是  $x^{p^n} - x \in \mathbb{F}_p[x]$  的分裂域, 记作  $\mathbb{F}_{p^n}$ .



**证明** 第一点是显然的. 设  $|F| = p^n$ , 则  $F^\times \cong \mathbb{Z}_{p^n-1}$ , 于是对任意  $a \in F^\times$ , 有  $a^{p^n-1} = 1$ , 即  $a^{p^n} - a = 0$ , 因此任意  $a \in F^\times$  均是多项式  $x^{p^n} - x \in \mathbb{F}_p[x]$  的根, 由于  $x^{p^n} - x$  至多  $p^n$  个不同零点, 因此  $F$  就是  $x^{p^n} - x$  的分裂域. 反过来, 还需要证明对任意  $n \geq 1$ , 都存在  $F$  使得  $|F| = p^n$ . 由于  $(x^{p^n} - x)' = p^n x^{p^n-1} - 1 = -1$ , 因此  $(x^{p^n} - x, (x^{p^n} - x)') = 1$ , 从而  $x^{p^n} - x \in \mathbb{F}_p[x]$  无重根, 取其所有根组成集合  $F$ , 则  $|F| = p^n$ , 容易验证  $F$  对加减乘除都封闭, 因此  $F$  是域.

**命题 5.6**

1.  $\mathbb{F}_{p^m}$  是  $\mathbb{F}_{p^n}$  的子域当且仅当  $m \mid n$ ;
2.  $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$ , 其中  $\deg m_{\alpha, \mathbb{F}_p}(x) = n$ .

**推论 5.9**

对任意的  $n \geq 1$ , 存在  $\mathbb{F}_p[x]$  上的  $n$  次不可约多项式.



## 5.4 伽罗华理论

### 5.4.1 伽罗华群

**定义 5.17**

称域扩张  $K/F$  是 Galois 扩张, 如果  $K/F$  是可分正规扩张.

**定义 5.18**

对 Galois 扩张  $K/F$ , 定义 Galois 群

$$\text{Gal}(K/F) := \text{Aut}_F(K)$$

如果  $K/F$  有限, 则  $\#\text{Gal}(K/F) = [K:F]$ .



### 命题 5.7


设  $K/F$  是域扩张, 则以下命题等价

1.  $K/F$  是有限 Galois 扩张;
2.  $K$  是  $F$  上可分多项式在  $F$  上的分裂域;



### 证明

1.  $\Rightarrow$  设  $\alpha_1, \alpha_2, \dots, \alpha_n$  是  $K$  作为  $F$  上线性空间的一组基, 则  $K = F(\alpha_1, \alpha_2, \dots, \alpha_n)$ . 设  $p_i(x)$  是  $\alpha_i$  在  $F$  上的极小多项式. 设  $g(x)$  是  $\prod_{i=1}^n p_i(x)$  去除多余的重因式得到. 此时  $g(x)$  是可分多项式
2.  $\Leftarrow$  设  $K$  是可分多项式  $f(x) \in F[x]$  在  $F$  上的分裂域, 于是  $K/F$  是有限正规扩张, 且  $K = F(\alpha_1, \dots, \alpha_n)$ . 要证明  $K/F$  可分, 只要证明  $\alpha_i$  都是可分元素即可. 由于  $f(\alpha_i) = 0$ , 因此  $(f(x), m_{\alpha_i, F}(x))_K \neq 1$ , 从而  $(f(x), m_{\alpha_i, F}(x))_F \neq 1$ , 于是  $m_{\alpha_i, F}(x) \mid_F f(x)$ , 因此  $m_{\alpha_i, F}(x)$  无重根, 故  $\alpha_i$  均可分.

 **练习 5.1** 设  $F$  不是特征 2 的域,  $K/F$  是二次扩张, 则  $K/F$  是 Galois 扩张.

### 例题 5.4

1. Galois 扩张的 Galois 扩张不一定是 Galois 扩张, 如  $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[3]{2})$

### 定理 5.11

对于有限 Galois 扩张  $K/F$  及其 Galois 群  $G = \text{Gal}(K/F)$ , 成立

1. 存在双射

$$\{K/F \text{ 的中间域} \} \longleftrightarrow \{G \text{ 的子群} \}$$

$$E \longrightarrow \text{Gal}(K/E)$$

$$K^H \longleftarrow H$$

2. 以上对应存在反包含关系:

$$H_1 \subseteq H_2 \Leftrightarrow K^{H_1} \supseteq K^{H_2}$$

3. 这个对应将域扩张的次数归结为群的指标, 即

$$|H| = [K:K^H], [G:H] = [K^H:F]$$

4. 如果  $H \longleftrightarrow E = K^H$ , 则

$$gHg^{-1} \longleftrightarrow g(E)$$

5.  $H \triangleleft G \iff K^H/F$  是正规扩张, 此时

$$\text{Gal}(K^H/F) \cong G/H$$

6. 如果  $H_1, H_2 \longleftrightarrow E_1, E_2$ , 则

$$H_1 \cap H_2 \longleftrightarrow E_1 E_2$$

$$\langle H_1, H_2 \rangle \longleftrightarrow E_1 \cap E_2$$



### 证明

1. (a). 证明  $K/E$  是 Galois 扩张. 由于  $K/F$  是有限 Galois 扩张, 因此  $K$  一定是  $f(x) \in F[x]$  在  $F$  上的分裂域, 同时也是  $f(x) \in F[x] \subseteq E[x]$  在  $E$  上的分裂域, 从而  $K/E$  是正规扩张. 其次由于  $K/F$  是 Galois 扩张, 因此  $K$  中任何元素在  $F$  上是可分的, 从而在  $E$  上也可分. 于是  $K$  由  $E$  中有限个可分元素生成, 故  $K/E$  可分. 综上  $K/E$  是 Galois 扩张.  
(b). 证明  $H = \text{Gal}(K/K^H)$ . 显然  $H \subseteq \text{Gal}(K/K^H)$ , 于是只要证明  $|H| \geq |\text{Gal}(K/K^H)|$ , 我们知道

$|\text{Gal}(K/K^H)| = [K : K^H]$ , 因此只要证明  $|H| \geq [K : K^H]$ . 由本原元素定理, 存在  $\alpha \in K$ , 使得  $K = K^H(\alpha)$ , 此时  $[K : K^H] = \deg m_{\alpha, K^H}(x)$ . 考虑到极小多项式次数的最小性, 如果我们可以构造一个  $K^H$  系数的以  $\alpha$  为零点的  $|H|$  次数多项式, 就解决了问题. 设

$$f(x) = \prod_{h \in H} (x - h(\alpha))$$

则  $f(x)$  就满足上述条件, 从而  $|H| \geq [K : K^H]$ , 因此  $H = \text{Gal}(K/K^H)$ .

(c). 证明  $E = K^{\text{Gal}(K/E)}$ . 显然  $E \subseteq K^{\text{Gal}(K/E)}$ , 于是  $[K : E] = \#\text{Gal}(K/E) = [K : K^{\text{Gal}(K/E)}]$ , 从而  $E = K^{\text{Gal}(K/E)}$ .

2.  $H_1 \subseteq H_2 \Rightarrow K^{H_1} \supseteq K^{H_2}, E_1 \subseteq E_2 \Rightarrow \text{Gal}(K/E_1) \supseteq \text{Gal}(K/E_2)$ , 由 Galois 对应即得.

3.  $|H| = [K : K^H]$  由 Galois 对应证明中得到.

$$[K : K^H][K^H : F] = [K : F] \Rightarrow |H|[K^H : F] = |G| \Rightarrow [K^H : F] = [G : H]$$

4.  $a \in K^{gHg^{-1}} \Leftrightarrow ghg^{-1}(a) = a \Leftrightarrow hg^{-1}(a) = g^{-1}(a) \Leftrightarrow g^{-1}(a) \in K^H \Leftrightarrow a \in g(K^H) = g(E)$ .

5. (a).  $\Leftarrow$  此时  $K^H$  是某个  $F$  系数多项式  $f(x)$  的分裂域, 对任意  $g \in G, g$  置换  $f(x)$  的根, 因此  $g(K^H) = K^H = K^{gHg^{-1}}$ , 于是  $H = gHg^{-1}$ , 故  $H \triangleleft G$ .

(b).  $\Rightarrow$  考虑正规扩张的定义, 设不可约多项式  $f(x) \in F[x]$  有根  $\alpha$  落在  $K^H$  中. 构造多项式

$$g(x) = \prod_{\sigma \in G} (x - \sigma(\alpha))$$

显然  $g(x)$  被  $G$  中元素固定, 即  $g(x) \in F[x]$ , 且  $g(\alpha) = 0$ , 由于  $(f(x), g(x))_K \neq 1$ , 从而  $(f(x), g(x))_F \neq 1$ , 因此  $f(x) \mid_F g(x)$ , 于是只要证明  $\sigma(\alpha) \in K^H, \forall \sigma \in G$ . 由于  $\sigma(\alpha) \in \sigma(K^H) = K^H$ , 得证.

(c). 考虑群同态

$$\varphi : \text{Gal}(K/F) \rightarrow \text{Gal}(K^H/F)$$

$$\sigma \mapsto \sigma|_{K^H}$$

由于 Galois 对应, 得  $\ker \varphi = H$ , 由第一同构定理, 得  $G/H \cong \text{Gal}(K^H/F)$ .

6. 容易证明  $\text{Gal}(K/E_1E_2) = H_1 \cap H_2, K^{(H_1, H_2)} = E_1 \cap E_2$ .

#### 命题 5.8

设  $H \subseteq G = \text{Aut}(K), F$  是  $H$  的不动域, 则  $[K : F] = |H|$ .

#### 命题 5.9

设  $K/F$  是有限扩张, 则  $|\text{Aut}(K/F)| \leq [K : F]$ , 当且仅当  $F$  是  $\text{Aut}(K/F)$  的不动域时取等.

#### 推论 5.10

设  $H \subseteq G = \text{Aut}(K), F$  是  $H$  的不动域, 则  $\text{Aut}(K/F) = H$ , 因此  $K/F$  是 Galois 扩张, 其 Galois 群是  $H$ .

**注** 这个结论告诉我们任何一个固定  $F$  的自同构都在  $H$  中.

#### 推论 5.11

设  $H_1, H_2 \subseteq G = \text{Aut}(K), H_1 \neq H_2, F_1, F_2$  分别是  $H_1, H_2$  的不动域, 则  $F_1 \neq F_2$ .