代数学 III：代数学进阶

欧阳毅
中国科学技术大学
数学科学学院

Email: yiouyang@ustc.edu.cn

《代数学系列》序言

近世代数（或叫抽象代数）研究群、环、域和模等各种代数结构。它不仅是一个基本的数学分支，而且也是物理学、化学和力学等其他科学的重要数学工具。上世纪五十年代以来由于数字通信和数字计算技术的飞速发展，近世代数在信息科学和计算机科学也发挥愈来愈大的作用。更广一点来说，近世代数中所体现的数学思维方式（共性和个性，比较和分类，局部和整体，.....）对于人们从事任何社会活动都是有益的。

中国科学技术大学1958年建校以来，数学系一向重视近世代数学教学。上世纪六十年代，老一辈数学家华罗庚、万哲先、王元和曾肯成培养了不少从事代数教学、研究和应用领域的人才。我本人有幸聆听过王元的《数论导引》，万哲先和曾肯成的《抽象代数》（用van der Waerden的《代数学》一书），华罗庚和万哲先的“典型群”以及吴文俊先生的“代数几何”课。我们不仅学到了知识，更重要的是受到他们对学问的理解方式和研究经验的感染。他们风格各异的讲授方式对于年青学生今后成长的影响是至关重要的，是由所谓量化条件和单一标准约束出来的“名师”无可比拟的。半个世纪以来，科大教师一直努力继承这个传统。上个世纪八十年代至九十年代，我和李尚志、查建国、余红兵、章璞等志同道合者在近世代数教学、教材建设和培养人才方面做过一些努力。现在为了适应我国高等教育和数学发展的新形势，科大数学系欧阳毅、叶郁等人对于近世代数的教学做进一步的改革，编写这套新的教材，这是令人高兴的。

教学经验讲一下三点体会：

（1）把初等数论作为近世代数教学的有机组成部分。中国科学技术大学从上个世纪七十年代起，一直把初等数论作为本科生一年级的必修课，其目的不仅是传授整数性质和方程的整数解方面基本知识，更不是训练做数论难题，而是把初等数论视为近世代数的一个源头。十八世纪和十九世纪，伟大数学家欧拉和高斯对于费马关于整数和素数的一系列猜想产生浓厚的兴趣。他们花了不少精力研究整数的性质，得到一系列关于整除性和同余性的重要结果，所创造的一系列深刻的数学思想成为近世代数的源头，而初等数论本身也提供了近世代数中抽象代数结构的第一批具体例子。整数模m的同余类全体$\mathbb{Z}/m\mathbb{Z}$给出有限交换群和交换环的简单例子，中国剩余定理是交换环直和分解的原始模型。模素数p的原根g就是循环群$\mathbb{F}_p^\times$ 的生成元, 而$\mathbb{F}_p$ 给出第一批有限域。费马小定理和更一般的欧拉定理在近世代数中推广成有限群的Lagrenge定理。而高斯的二次互反律在后来的二百年中不断增添新的视野而得到最现代的形式。高斯在研究整数的二平方和问题时，考虑整数的推广（高斯整数），而为了证明任何数域中的代数整数形成环，Dedekind采用了一种新的代数概念，这就是“模”。库默尔（Kummer）在研究费马猜想时发明了“理想数”（ideal number）。后人发现这个概念本质上不是一个数，而是环中

的一类十分重要的集合，即环中的理想（ideal）。这些数学家在研究初等数论所产生的深刻数学思想和结果，是很值得后人学习和欣赏的。

（2）充分讲授域的扩张理论，特别是域扩张的伽罗华理论。目前高校的近世代数课程，由于学时所限无法讲授伽罗华理论，这是令人惋惜的。这不仅是由于这个理论非常漂亮，也因为它为数学发展上一个精彩的例子，表明数学家们为追求数学自身的完善而对人类文明所做的贡献。为了证明n次（$n \geq 5$）的一般代数方程是根式不可解的。伽罗华和阿贝尔考虑此方程所有根之间的置换，由此产生了群的概念，并且揭示出这类方程根式不可解的深层次原因：方程所有n个根允许一个最大可能的置换群S_n，而当$n \geq 5$ 时这个群的结果过于复杂（用现在的语言，S_n 是不可解群）。后来人们逐渐认识到，群是研究各种事物对称性的有力工具。从而群论（特别是群表示理论）在物理、化学、力学等各个领域中均起到重要作用。群的产生和非欧几何等许多思想一样源于数学内部问题的探究，我们不能低估人们追求真理和美对人类文明所起的作用。

（3）增加了传统近世代数课以外的许多内容。相对于分析课程，代数和几何教学在中国高校中非常薄弱，这是一个长期存在的问题，它直接影响我国数学研究的水平。当前的代数组合学研究需要交换代数和群表示理论工具，多复变和微分几何研究要求上同调理论，控制理论需要模论。本世纪初，我和清华大学数学科学系的同人文志英，欧阳毅，姚家燕和印林生等，与法国数学家合作，从一年级初等数论讲起至法国数学家为高年级讲现代代数几何。培养了几届具有现代代数素质的学生。记得我们与Illusie（Grothendieck的关门弟子）讨论法国数学家来华前我们需要对清华学生的前期准备时，他说只需要线性代数即可。进一步交换才知。他把群的线性表示，模论（环上的线性代数），以及交换代数中的许多内容均看作是线性代数。我们和法国对于代数学作用和地位在认识上有很大差距。所以，这套教材增加了群表示理论和模论的初步内容，把这些内容看作是大学生应当掌握的知识，是非常必要的。

教学事业其实并不如有些人搞的那么复杂，不需要花样翻新的标语和口号。只需要设计好教学内容，并且有好的老师，坚持至少五年，就会培养出好的学生，因为中国不缺乏勤奋能吃苦的学生。说到根本，只需要老师和学生都有一点精神。老师具有培养学生的热情，而学生要有对数学的热爱和提高数学素质非功利主义的动力。我预祝并且相信，在科大数学系师生共同努力之下，这套教材一定能培养出新一代年青代数学人材。

冯　克　勤

2015年12月11日

于

香港科技大学

编者前言

代数方法和分析方法是数学研究中两种最基本的方法，也是大学数学专业学生数学教育的重点。中国科学技术大学从创校伊始就受到华罗庚、王元、万哲先、曾肯成等前辈数论和代数大家的谆谆教导，代数和数论方面人才辈出。八十年代以来，在冯克勤教授和李尚志教授等领导下，中国科学技术大学的代数教学一直维持在较高水平，培养的代数和数论人才受到国内外同行高度称许。中国科大之所以能够在代数教学方面取得较好成果，一方面原因是学生们受到严格的《线性代数》基础训练；另一方面科大一直坚持为数学系学生开设《初等数论》和《近世代数》基础课程，并在高年级和研究生阶段开设《群表示论》,《交换代数》等课程，并配备有《整数与多项式》（冯克勤、余红兵编著),《近世代数引论》（冯克勤、李尚志、查建国、章璞编著),《群与代数表示论》（冯克勤、章璞、李尚志编著）等著名教材。

进入新世纪以来，新一代科大学生入学时的数学基础和上世纪八、九十年代学生有较大区别。这里面一部分原因是高中新课标和高考指挥棒的影响，大部分学生在高中时代受到题海战术的锤炼，但独立探索和抽象思维能力受到压制。他们更早接触到微积分的思想，对于高考中出现的各种题型十分熟练，但在平面几何、因式分解和三角函数等方面的基本训练远不如以前，在数学证明和逻辑严格性方面的训练也不如以前。另一方面，这一代学生或多或少参加过数学竞赛，而其中最体现抽象思维能力的初等数论问题常常是他们最头疼的问题类型。当同学们在大一开始接触《初等数论》课程时，上述两方面的原因就让同学们对于课程学习产生畏难情绪。到大二开始学习《近世代数》课程时，扑面而来的抽象代数思想，特别是群论思想和方法更让不少学生感到无所适从。因此科大的代数教学在前些年受到比较严重的挑战。另一方面，我们的教材没有及时体现新时期学生的最新情况，需要得到及时更新。从教学本身来看，通过多年教学和科研实践，我们发现各代数课程之间的衔接以及对应教材之间衔接不是特别流畅（各数学核心课程的衔接亦是如此），在统一的框架下对代数课程教学和教材建设进行规划成为必要。

2011年，在编者的组织下，数学科学学院全体教授对于代数系列课程的教学大纲和教学内容进行了热烈讨论,《代数系列课程纲要》数易其稿，最终得到通过。我们对代数方面涉及的6门课程进行全面改革和优化。原来的《初等数论》课程由《代数学基础》课程替代，与《近世代数》,《代数学》一起构成代数教学三门核心课程。它们由浅入深，目标是为数学学院学生奠定扎实的代数基础。基于课程改革的需要，我们当即着手对应的教材建设，计划在原来教材的基础上编写代数学三部系列教材:《代数学I: 代数学基础》,《代数学II：近世代数》和《代数学III：代数学进阶》。

本书是代数系列教材三部曲的最后一部，是研究生和高年级本科生数学核心课程《代数学》的教材。我们重点参考参考了Artin, Lang，Hungerford,

Dummit-Foote 等著名英文教材，特别是Rotman的Advanced Modern Algebra, 介绍模论、交换代数初步和有限群表示理论基本知识。本书共分三章。第一章是模论，介绍模论基本性质和基本定理，范畴和函子，自由模、投射模和内射模，张量积与平坦模，主理想整环上的有限生成模的结构定理等。第二章是交换代数初步，介绍诺特环与诺特模，Artin环与Artin模，Hilbert基定理，局部化，整性，根式理想与准素理想，仿射代数几何初步，Hilbert零点定理，Gröbner基和截式等内容。第三章是半单代数与有限群的线性表示，包括群表示与群代数的模，Schur引理，完全可约性和Maschke定理，半单代数与Wedderburn定理，表示的特征标，特征标表的计算及应用，Burnside定理，诱导表示，Frobenius互反律等知识。

本书适用于大学数学专业的本科生和研究生，以及其他对代数思想、方法感兴趣的学生和学者。修读本教材的一个主要目的，是让读者具备基本代数素养，能够顺利进入交换代数、同调代数、代数数论、代数几何和李代数等专门数学理论的学习。

本书初稿2016年秋到2018年秋相继在中国科学技术大学《代数学》课程中试用。编者向这些年来对代数课程体系调整和本书初稿提供宝贵意见的叶郁、陈小伍、陈洪佳、申伊塃、宋光天、郭文彬、盛茂等教授表示深深感谢。编者特别感谢冯克勤教授对代数学三部曲编写的关心和指导，特别感谢梁永祺教授对本书初稿的仔细阅读和勘误, 特别感谢申伊塃副教授提供的2016 年春季课程的讲义，特别感谢课程助教徐铮和李梦炜、胡益榕等同学对课程讲义提供的宝贵意见和修改建议，特别感谢许跃、李宋宋和刘洋等同学输入讲义初稿。编者欢迎大家继续提供宝贵意见。

编　　者

2019年3月17日

目 录

《代数学系列》序言 **i**

编者前言 **iii**

第一章 模论 **1**

1 模的定义, 例子和基本性质 1
1.1 定义和例子 1
1.2 同态与同构 3
1.3 模论基本定理 5
1.4 单模与合成列 7
1.5 直积与直和 9
1.6 正合列 13
2 范畴与函子 17
2.1 范畴 17
2.2 函子 22
2.3 阿贝尔范畴 22
3 自由模, 投射模和内射模 26
3.1 自由模 26
3.2 投射模 28
3.3 内射模 30
4 张量积与平坦模 32
4.1 张量积 32
4.2 平坦模 38
4.3 基变换 41
5 主理想整环上有限生成模的结构定理 43
5.1 模的扭元 43
5.2 有限生成无扭模 44
5.3 结构定理 46
5.4 从模论观点看史密斯标准形理论 50
习题 54

第二章 交换代数初步 **61**

1 诺特环, 诺特模, 阿廷环与阿廷模 61
1.1 诺特环与诺特模 61
1.2 阿廷环与阿廷模 64
2 局部化 67

3 整性 74
4 根式理想和准素理想 78
4.1 根式理想 78
4.2 准素理想 80
5 仿射代数几何初步 82
5.1 仿射代数集 82
5.2 希尔伯特零点定理 86
5.3 仿射代数集上的拓扑 87
5.4 交换环素谱上的拓扑 89
6 格罗布纳基 90
6.1 域上多元多项式环上的带余除法 90
6.2 格罗布纳基和布赫伯格算法 93
7 结式 98
习题 102

第三章 半单代数和有限群表示 **107**
1 一般环上的模 107
2 群的表示 110
3 半单代数 115
4 有限群的特征标理论 120
5 特征标表 124
5.1 基本性质 124
5.2 计算实例 126
5.3 特征标表的更多性质与应用 130
5.4 伯恩赛德定理 133
6 诱导表示 134
6.1 诱导表示和诱导特征 134
6.2 利用诱导特征计算特征标表 138
习题 140

参考文献 **145**

索 引 **147**

第一章　模论

在本书中, 所有的环均是含幺环. 若无特别约定, 本章考虑的环R 均是含幺交换环.

§1.1　模的定义, 例子和基本性质

§1.1.1　定义和例子

线性代数学习中最重要的一个概念是线性空间. 对于域k, k- 线性空间V是一个非空集合, 并配备加法和k 在V 上的数乘, 使得V 在加法意义下是阿贝尔群, 数乘满足结合律和与加法的分配律, 且$1v = v$ 对任意$v \in V$ 成立.

所谓模, 即是环上的线性空间. 也就是说, 在线性空间的定义中, 将域的数乘改为环的数乘.

定义1.1. 设R 是含幺交换环. 非空集合M 称为R-**模**(module) 是指M 是加法阿贝尔群, 且其上存在**数乘**(scalar multiplication, 或称标量乘法)

$$R \times M \to M,\ (r, m) \mapsto rm,$$

使得对所有$m, m' \in M$ 和$r, r' \in R$, 下列性质成立:

(i) **恒等元**: 若$1 = 1_R$ 是R 的幺元, 则$1m = m$.

(ii) **分配律**: $r(m + m') = rm + rm'$, $(r + r')m = rm + r'm$.

(iii) **结合律**: $(rr')m = r(r'm)$.

注记. 若R 是非交换环, 我们称满足如上定义的M 为左R-模, 称满足上述性质的数乘为左乘. 在本章我们主要考虑R 为交换环的情形, R 为非交换环的情形将在第三章中讨论.

由模的定义立知$0_R m = 0_M$. 事实上,

$$0_R m = (0_R + 0_R)m = 0_R m + 0_R m.$$

再由加法消去律即知$0_R m = 0_M$.

例1.2. 此处我们给出模的一些具体例子.

(1) 域k的模即k-线性空间.

(2) 阿贝尔群均有自然的$\mathbb{Z}$-模结构, 数乘na 即n个a之和(如$n \geq 0$), 或者$-n$个$-a$之和(如$n < 0$).

(3) 如果定义数乘$R \times R \to R$ 为R 上的乘法, 则每个交换环R 均可视为它自身的模. 更一般的, R 的理想I 均是R-模, 这是因为对于任意$r \in R$ 及$a \in I$, 均有$ra \in I$.

(4) 如环S 是交换环R 的子环, 则R 可视为S-模. 此时数乘$S \times R \to R$ 即环的乘法$(s, r) \mapsto sr$. 特别地, R 的多项式环$R[x]$ 是R-模.

(5) 设V 是域k 上的有限维线性空间, $T : V \to V$是线性变换. 我们定义数乘

$$k[x] \times V \to V, \quad \big(\sum_{i=0}^{n} c_i x^i, v\big) \mapsto \sum_{i=0}^{n} c_i T^i(v),$$

此处$T^0 = 1_V$, $T^i = T \circ T \circ \cdots \circ T$ (i 次复合, 如$i \geq 1$). 换言之, 数乘$f(x) \cdot v = f(T)(v)$. 根据这个数乘, 我们可以将V 看作是$k[x]$-模, 记之为V^T.

我们来讨论一个特殊情况. 设$V = k^n$ 是k 上的n 维列向量空间, A 是k 上的一个n 阶方阵. 记$T : k^n \to k^n$ 为线性变换$v \mapsto Av$. 则k^n 在数乘

$$k[x] \times k^n \to k^n, \quad (f(x), v) \mapsto f(A)v$$

下成为$k[x]$-模, 我们记之为$(k^n)^A$.

定义1.3. 如M 是R-模, 则M 的**子模**(submodule) 是指M 的一个加法子群N且其在数乘意义下封闭, 即对任意$n \in N$ 和$r \in R$, 均有$rn \in N$. 此时记为$N \subseteq M$.

M 的**真子模**(proper submodule)是指N是M的子模且$N \neq M$. 此时记为$N \subsetneqq M$.

例1.4. 我们给出子模的一些例子.

(1) $\{0\}$ 和M 均是M 的子模.它们称为M 的**平凡子模** (trivial submodule). 我们记$0 = \{0\}$.

(2) 将交换环R 视为自身的模, 则R 的子模即R 的理想, R 的真子模即R 的真理想.

(3) $\mathbb{Z}$-模的子模即阿贝尔群的子群. 线性空间的子模即线性子空间.

(4) 设$T : V \to V$ 是线性变换. 模V^T 的子模即是T 的不变子空间. 事实上, 如$W \subseteq V^T$ 为子模, 显然有$T(W) \subseteq W$. 反过来, 如$T(W) \subseteq W$, 则对任意$w \in W$ 有$xw = T(w) \in W$. 由归纳法知$f(x)w \in W$. 即W 对$k[x]$ 的数乘封闭.

(5) 设M 是R-模. 如$r \in R$, 则

$$rM = \{rm \mid m \in M\}$$

是M 的子模. 如J 为R 的理想, 则

$$JM = \Big\{ \sum_{\text{有限和}} \alpha_i m_i \mid \alpha_i \in J, m_i \in M \Big\}$$

是M 的子模.

(6) 如S 和T 是M 的子模, 则S 与T 的**和**

$$S+T=\{s+t \mid s\in S, t\in T\}$$

是M 的子模. 显见S 与T 均是$S+T$ 的子模.

(7) 如$\{S_i : i\in I\}$ 是M 的一簇子模, 则它们的**交** $\bigcap\limits_{i\in I} S_i$ 也是M 的子模.

(8) 设M 是R-模, $m\in M$. 则由m 生成的子模, 记为$\langle m\rangle$, 是指$\langle m\rangle = Rm=\{rm \mid r\in R\}$. 如$N$是$M$ 的子模并且$m\in N$, 则$\langle m\rangle\subseteq N$, 故$\langle m\rangle$ 是包含元素m 的最小子模.

更进一步地, 如X 是R-模M 的子集, 则X 中元素的所有线性组合

$$\langle X\rangle=\Big\{\sum_{\text{有限和}} r_i x_i \mid r_i\in R, x_i\in X\Big\}$$

是X 生成的子模. 同样, $\langle X\rangle$ 是包含集合X 的最小子模.

定义1.5. 模M 称为**有限生成模**(finitely generated module), 是指M 由有限子集生成. 即存在$X=\{x_1,\cdots,x_n\}$ 使得$M=\langle X\rangle$. 特别地, 如M 由一个元素生成, 称M 为**循环模**(cyclic module).

例1.6. 线性空间是有限生成的当且仅当它的维数有限.

§1.1.2 同态与同构

定义1.7. 设R 是交换环, M 和N 是R-模. 映射$f: M\to N$ 称为**R-模同态**(module homomorphism, 亦称**R-模映射**或**R-同态**, 或者简称同态), 是指对任意$m,m'\in M$ 和$r\in R$, 均有

(i) $f(m+m')=f(m)+f(m')$;

(ii) $f(rm)=rf(m)$.

如R-模同态f 作为集合映射是单射, 则称f为**单同态**(monomorphism); 如f 是满射, 称f为**满同态**(epimorphism); 如f 既是单同态也是满同态, 称f 为R-模**同构**(module isomorphism, 亦称**R-同构**或简称同构), 此时记$f: M\xrightarrow{\sim} N$ 或$M\cong N$, 亦称M 与N 同构.

模到自身的同态称为**自同态**(endomorphism), 模到自身的同构称为**自同构**(automorphism).

根据定义, 我们首先注意到:

(1) R-模同态的复合是R-模同态;

(2) 如f 是R-模同构, 则它的逆映射f^{-1} 也是R- 模同构.

例1.8. 我们来看模同态和同构的一些例子.

(1) 如R 是域k, 则模同态、同构、自同态和自同构分别是线性代数课程中定义的k- 线性映射、可逆线性映射、线性变换和可逆线性变换.

(2) $\mathbb{Z}$-模同态即阿贝尔群之间的群同态.

(3) 如M 是R-模, 对于$r \in R$, 则r 乘映射$\mu_r : M \to M,\ m \mapsto rm$ 是R-模自同态. 这是因为R 是交换环, 故对任意$a \in R$ 和$m \in M$, 均有$\mu_r(am) = ram = arm = a\mu_r(m)$.

(4) 设V 是域k 上n 维线性空间, $\{v_1, \cdots, v_n\}$ 是V 的一组基. 设$T : V \to V$ 是线性变换, A 是T 在上述基下的矩阵. 令$e_i \in k^n$, 它的第i个分量是1而其余分量等于0. 则$\{e_1, \cdots, e_n\}$ 是k^n 的一组基. 线性映射

$$\varphi :\ V \to k^n, \quad v_i \mapsto e_i$$

是线性空间V 与k^n 之间的同构.

我们来考虑对应的$k[x]$-模映射. 由于

$$T(v_1, \cdots, v_n) = (v_1, \cdots, v_n)A,$$

故$T(v_i) = \sum_{j=1}^{n} a_{ji}v_j$. 我们有

$$\varphi(xv_i) = \varphi(T(v_i)) = \varphi\big(\sum_{j=1}^{n} a_{ji}v_j\big) = \sum_{j=1}^{n} a_{ji}e_j,$$

而

$$x\varphi(v_i) = A\varphi(v_i) = Ae_i = \sum_{j=1}^{n} a_{ji}e_j,$$

所以$\varphi(xv_i) = x\varphi(v_i)$. 由归纳法即知$\varphi(f(x)v) = f(x)\varphi(v)$ 对任意多项式$f(x) \in k[x]$ 成立. 因此$\varphi : V^T \to (k^n)^A$ 是$k[x]$-模同态. 由于φ 是线性空间同构, 故它也是$k[x]$-模同构.

命题1.9. *设V 是k-线性空间, T 与S 是V 上的线性变换. 则$V^T \cong V^S$ 当且仅当存在线性空间的同构映射$\varphi : V \to V$ 使得$S = \varphi T \varphi^{-1}$.*

证明. 如$\varphi : V^T \to V^S$ 是$k[x]$-模同构, 则$\varphi : V \to V$ 是线性空间的同构, 且$\varphi(f(x)v) = f(x)\varphi(v)$ 对于任意$f(x) \in k[x]$ 成立. 特别地, 取$f(x) = x$. 则$\varphi(xv) = x\varphi(v)$. 但$\varphi(xv) = \varphi(T(v))$ 而$x\varphi(v) = S\varphi(v)$, 故$S = \varphi T \varphi^{-1}$.

反过来, 如$S = \varphi T \varphi^{-1}$, 则$\varphi T = S\varphi$. 我们有$\varphi(xv) = x\varphi(v)$. 再由归纳法即知$\varphi(f(x)v) = f(x)\varphi(v)$ 对于任意$f(x) \in k[x]$ 成立. 故$\varphi : V^T \to V^S$ 是$k[x]$-模同构. □

推论1.10. *如k 是域, A 与B 是k 上的n 阶方阵, 则$(k^n)^A \cong (k^n)^B$ 当且仅当A 与B 相似.*

证明. 定义

$$T : k^n \to k^n, \quad T(y) = Ay,$$

$$S : k^n \to k^n, \quad S(y) = By.$$

则$(k^n)^A = (k^n)^T,\ (k^n)^B = (k^n)^S$. 由命题1.9 立得推论. □

定义1.11. 设M 和N 是R-模. 定义集合

$$\mathrm{Hom}_R(M,N)=\{f:M\to N\text{为}R\text{-模同态}\}.$$

如$f,g\in\mathrm{Hom}_R(M,N)$, 定义它们的和$f+g:M\to N$ 为映射

$$(f+g)(m)=f(m)+g(m).$$

记0 为模同态$M\to M,\ m\mapsto 0$.

特别地, 定义$\mathrm{End}_R(M)=\mathrm{Hom}_R(M,M)$.

命题1.12. *如R 是交换环, M 和N 是R-模, 则$\mathrm{Hom}_R(M,N)$ 也是R- 模, 其加法如上定义, 数乘则由*

$$rf:\ m\mapsto f(rm)$$

给出. 更进一步地, 如$p:M'\to M$ 和$q:N\to N'$ 是R- 模同态, 则对所有$f,g\in\mathrm{Hom}_R(M,N)$, 如下分配律成立:

$$(f+g)p=fp+gp,\quad q(f+g)=qf+qg.$$

特别地, 以映射复合作为乘法, $\mathrm{End}_R(M)$ 构成环, 零元是$0:M\to M$, 幺元是恒等映射.

证明. 我们验证$(rr')f=r(r'f)$, 其余结论的证明留给读者.

如$m\in M$, 则$((rr')f)(m)=f(rr'm)=f(r'rm)=(r'f)(rm)=(r(r'f))(m)$. 即$(rr')f=r(r'f)$. □

注记. 环$\mathrm{End}_R(M)$ 称为M **的R-自同态环**. 这个环一般而言不是交换环. 上述命题实际上说明了$\mathrm{Hom}_R(M,N)$ 是$\mathrm{End}_R(M)$-右模和$\mathrm{End}_R(N)$-左模.

例1.13. 在线性代数中, 域k 上的线性空间V 的**线性泛函**是指线性映射$\varphi:V\to k$. 例如, 设$V=\{$闭区间$[0,1]$到$\mathbb{R}$ 上的连续函数$\}$, 则V 是$\mathbb{R}$-线性空间, 积分 $f\mapsto\int_0^1 f(t)\mathrm{d}t$ 是V 上的一个线性泛函.

线性空间V 的**对偶空间**(dual space)

$$V^*=\mathrm{Hom}_k(V,k)$$

即是V 上所有线性泛函的全体. 由命题1.12即知V^* 也是k- 模, 即k-线性空间.

§1.1.3 模论基本定理

定义1.14. 设$f:M\to N$ 是R-模同态. 则f 的**核**(kernel)即

$$\ker f=f^{-1}(0)=\{m\in M\mid f(m)=0\},$$

f 的**像**(image)即

$$\mathrm{im}\,f=f(M)=\{f(m)\mid m\in M\}.$$

容易验证$\ker f$ 是M 的子模, $\operatorname{im} f$ 是N 的子模.

定义1.15. 设N 是R-模M 的子模, 则**商模**(quotient module) M/N 是指对应的商群M/N, 并配备数乘映射

$$r(m+N) = rm + N.$$

我们说明M/N 上的数乘是定义良好的. 事实上, 如$m+N = m'+N$, 则$m-m' \in N$, 故$rm - rm' \in N$. 所以$rm+N = rm'+N$.

易验证上述数乘的确给出了阿贝尔群M/N 的R-模结构, 并且自然映射

$$\pi : M \to M/N, \quad m \mapsto m+N$$

是R-模满同态, 其核$\ker \pi = N$.

定理1.16 (同态基本定理)**.** *如$f : M \to N$ 是R-模同态, 则f 诱导R-模同构*

$$\bar{f} : M/\ker f \to \operatorname{im} f, \quad m + \ker f \mapsto f(m).$$

证明. 由群的同态基本定理, 我们知道$\bar{f}$ 是定义良好的阿贝尔群间的同构. 又由于

$$r\bar{f}(m+\ker f) = rf(m) = f(rm),$$

而

$$\bar{f}(r(m+\ker f)) = \bar{f}(rm + \ker f) = f(rm),$$

故$\bar{f}$ 是R-模同态. □

注记. 同态基本定理又称**第一同构定理**. 它是说模同态$f : M \to N$ 可以分解为$f = i \circ \bar{f} \circ \pi$:

$$M \xrightarrow{\pi} M/\ker f \xrightarrow{\bar{f}} \operatorname{im} f \xrightarrow{i} N,$$

其中π 是自然的商映射(满同态), $\bar{f}$ 是诱导的同构, i 是自然的包含映射(单同态).

定理1.17 (第二同构定理)**.** *如S 和T 是模M 的子模, 则存在自然的R-模同构*

$$S/(S\cap T) \to (S+T)/T, \quad s + (S\cap T) \mapsto s + T.$$

证明. 令h 为复合映射$S \to S+T \to (S+T)/T$. 则h 为满同态且$\ker h = S \cap T$. 故由同态基本定理即得欲证. □

定理1.18 (第三同构定理)**.** *设模$T \subseteq S \subseteq M$. 则映射$M/T \to M/S$, $m+T \mapsto m+S$ 诱导R-模同构*

$$\frac{M/T}{S/T} \to M/S.$$

证明. 令$g : M/T \to M/S$, $m+T \mapsto m+S$. 首先g 是良好定义的: 如$m+T = m'+T$, 则$m-m' \in T \subseteq S$. 故$m+S = m'+S$. 其次$rg(m+T) = rm+S = g(r(m+T))$. 故$g$ 是模同态. 更进一步地, $\ker g = \{m+T \mid m \in S\} = S/T$ 且$\operatorname{im} g = M/S$. 故由同态基本定理即得欲证. □

如$f : M \to N$ 是模同态且S 是N 的子模, 容易验证

$$f^{-1}(S) = \{m \in M : f(m) \in S\}$$

是M 的子模, 它包含f的核$\ker f = f^{-1}(0)$.

定理1.19 (对应定理)**.** *设T 是模M 的子模, $\pi : M \to M/T$ 是自然商映射. 则存在一一对应*

$$\begin{aligned} \varphi : \{M\text{中包含}T\text{的中间模}\} &\longrightarrow \{M/T\text{的子模}\} \\ S &\longmapsto S/T, \end{aligned}$$

其逆映射为$\overline{S} \mapsto \pi^{-1}(\overline{S})$. 更进一步地, $S \subseteq S'$ 当且仅当$S/T \subseteq S'/T$.

证明. 如S 是T 与M 之间一个中间模, 由于S/T 对数乘封闭, 故S/T 是M/T 的子模, 因此φ 是良好定义的.

考虑群的对应定理, 则映射

$$\begin{aligned} \Phi : \{M \text{ 中包含}T \text{ 的中间群}\} &\longrightarrow \{M/T\text{的子群}\}, \\ A &\longmapsto A/T \end{aligned}$$

是一一对应, 其逆映射为

$$\Phi^{-1}(\overline{A}) = \pi^{-1}(\overline{A}) = \{m \in M : m+T \in \overline{A}\}.$$

故φ 是单射. 对于M/T 的子模$\overline{S}$,

$$\pi^{-1}(\overline{S}) \supseteq \pi^{-1}(0) = T$$

且对数乘封闭, 故它是M 与T 之间的中间模. 由于$\varphi(\pi^{-1}(\overline{S})) = \Phi(\pi^{-1}(\overline{S})) = \overline{S}$, 故$\varphi$ 也是满射. 至于$S \subseteq S'$ 当且仅当$S/T \subseteq S'/T$, 这由群的对应定理立得. □

§1.1.4 单模与合成列

命题1.20. *R-模M 是循环模当且仅当$M \cong R/I$, 其中I 是R 的理想.*

证明. 如$M = \langle m \rangle$ 为循环模, 定义映射

$$f : R \to M, \quad r \mapsto rm.$$

则f 是满同态且$\ker f \subseteq R$ 是R 的子模, 即是R 的理想. 故由同态基本定理即得$R/\ker f \cong M$.

反过来, $R/I = \langle 1+I \rangle$ 是循环模, 故若$M \cong R/I$, 则M 也是循环模. □

定义1.21. 非零模M 称为**单模**(simple module)或者**不可约模**(irreducible module) 是指它没有非平凡子模, 即它的子模只有0 和M.

例1.22. $\mathbb{Z}$-模M 为单模当且仅当阿贝尔群M 是单群, 这等价于$M \cong \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, 其中$p$ 为素数.

域k上的单模即1维线性空间, 它们均同构于k.

容易看出, 如M 为单模, m 是M 中任意非零元, 则$\langle m\rangle = M$. 故单模均是循环模.

推论1.23. *R-模M 是单模当且仅当$M \cong R/\mathfrak{m}$, 其中$\mathfrak{m}$ 是R 的极大理想.*

证明. 这由对应定理立得. □

注记. 由上述推论知, 单模的存在性等价于极大理想的存在性, 而后者的证明需要用到Zorn 引理, 参见[4, 命题3.67].

定义1.24. 对于R-模M, M的一个**合成列**(composition series) 是指如下的R-模链:

$$M = M_0 \supseteq M_1 \supseteq \cdots \supseteq M_n = 0,$$

其中M_i/M_{i+1} 是单模, n 称为该合成列的长度.

命题1.25. *设N 是M 的子模. 如M存在一个长度是n的合成列, 则N 的任意合成列长度均不大于n. 特别地, M 的任意合成列的长度均等于n.*

证明. 我们对n做归纳.

如$n = 1$, 则M是单模, 故$N = 0$或者$N = M$, 它的合成列长度不超过1.

现在设$n \geq 2$, $M = M_0 \supseteq M_1 \supseteq \cdots \supseteq M_n = 0$ 是M 的长度为n 的合成列. 则M_{n-1}是单模, $M/M_{n-1} = M_0/M_{n-1} \supseteq M_1/M_{n-1} \supseteq \cdots \supseteq M_{n-1}/M_{n-1} = 0$ 是M/M_{n-1} 的长度为$n-1$的合成列.

设$N = N_0 \supseteq N_1 \supseteq \cdots \supseteq N_r = 0$ 是N 的长度为r 的合成列. 由于M_{n-1}是单模, $N \cap M_{n-1} = 0$ 或者M_{n-1}. 如果$N \cap M_{n-1} = 0$, 则$N = N/(N \cap M_{n-1}) \cong (N + M_{n-1})/M_{n-1}$ 是M/M_{n-1} 的子模, 由归纳假设$r \leq n-1 < n$. 如果$N \cap M_{n-1} = M_{n-1}$, 设$0 \leq t < r$ 是最大的整数使得$N_t \cap M_{n-1} = M_{n-1}$. 由于$N_t/N_{t+1}$ 是单模, $N_{t+1} + M_{n-1} = N_t$. 从而对于$i \leq t$,

$$(N_i + M_{n-1})/M_{n-1} = N_i/M_{n-1},$$

对于$i \geq t+1$,

$$(N_i + M_{n-1})/M_{n-1} \cong N_i/N_i \cap M_{n-1} = N_i,$$

而

$$(N_t + M_{n-1})/M_{n-1} = N_{t+1} + M_{n-1}/M_{n-1}.$$

所以模N/M_{n-1} 有合成列

$$N/M_{n-1} \supseteq \cdots \supseteq N_t/M_{n-1} = (N_{t+1} + M_{n-1})/M_{n-1} \cong N_{t+1} \supseteq \cdots \supseteq N_r = 0,$$

其长度是$r-1$. 由归纳假设, $(N + M_{n-1})/M_{n-1}$ 作为M/M_{n-1} 的子模合成列长度$r - 1 \leq n - 1$, 所以$r \leq n$. □

定义1.26. 模M 的**长度**(length), 记为$\ell(M) = \ell_R(M)$, 是指它的合成列的长度. 如M 不存在有限长度合成列, 则记$\ell(M) = +\infty$.

容易看出, 长度有限的模都是有限生成模. 我们将在命题2.20中给出长度有限模的另外一种刻画.

§1.1.5 直积与直和

在群论和环论中, 我们学习过群和环的直积和直和. 对于模论, 同样有类似的概念. 下面我们来定义模的直积与直和.

定义1.27. 设R 是交换环, S 与T 是R-模. S 与T 的**直积**(direct product)就是它们的笛卡儿积$S \times T$, 并配备如下运算:

(1) 加法运算: $(s,t) + (s',t') = (s + s', t + t')$;

(2) 数乘运算: $r(s,t) = (rs, rt)$.

容易验证$S \times T$ 是R-模.

定义1.28. 设S 与T 是R-模M 的子模, 且满足条件

$$S + T = M, \quad S \cap T = \{0\},$$

则称M 是S 与T 的**直和**(direct sum), 记为$S \oplus T$.

由直和的定义可以看出, $M = S \oplus T$ 当且仅当M 中的元素m 均可唯一表示成$m = s + t$ 的形式, 其中$s \in S$, $t \in T$.

命题1.29. *对于R-模S, T 和M, 下列条件等价:*

(1)$M \cong S \times T$.

(2) *存在单同态*$i : S \to M$ *和*$j : T \to M$, *使得*

$$M = \operatorname{im} i \oplus \operatorname{im} j.$$

(3) *存在同态*$i : S \to M$ *和*$j : T \to M$, *使得对任意*$m \in M$, *都有唯一的*$s \in S$ *与*$t \in T$, *使得*

$$m = i(s) + j(t).$$

(4) *存在同态*$i : S \to M$, $j : T \to M$, $p : M \to S$ *和*$q : M \to T$, *使得*

$$pi = 1_S,\ qj = 1_T,\ pj = 0,\ qi = 0, \text{ 及 } ip + jq = 1_M.$$

证明. (1) $\Rightarrow$ (2) 不妨设$M = S \times T$. 令$i : S \to M,\ s \mapsto (s,0)$ 及$j : T \to M,\ t \mapsto (0,t)$. 则(2) 显然成立.

(2) $\Rightarrow$ (3) 显然.

(3) $\Rightarrow$ (4) 对于$m = i(s) + j(t)$, 令$p(m) = s,\ q(m) = t$. 则易验证p 与q 均为模同态且满足(4) 的条件.

(4) $\Rightarrow$ (1) 定义

$$\varphi :\ S \times T \to M, \quad (s,t) \mapsto i(s) + j(t).$$

则φ 是R-模同态. 由$1_M = ip + jq$, 可知$\varphi(p(m), q(m)) = m$, 故φ 是满同态. 如$\varphi(s,t) = 0$, 则$i(s) = -j(t)$, 于是

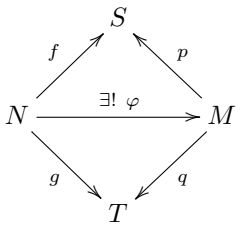
$$s = pi(s) = -pj(t) = 0,\ t = qj(t) = -qi(s) = 0,$$

故φ 是单同态. 所以φ 是同构. □

注记. 由上述命题可知$S \times T$ 与$S \oplus T$是典范同构的.

下面我们用另外一个观点来看直积与直和.

定义1.30. 设S 和T 是R-模. 三元组$(M;\ p,\ q)$, 其中M 是R-模, $M \xrightarrow{p} S$和$M \xrightarrow{q} T$是模同态, 称为S 与T 的**直积**是指对任意三元组$(N; f, g)$, 其中N 是R-模, $N \xrightarrow{f} S$ 和$N \xrightarrow{g} T$ 是模同态, 存在唯一的模同态$\varphi : N \to M$ 使得图表



交换, 即等式$f = p \circ \varphi,\ g = q \circ \varphi$ 成立.

命题1.31. (1) 如$(M; p, q)$ 和$(M'; p', q')$ 均是R-模S 与T 的直积, 则存在唯一的同构$\varphi_{M'M} : M' \to M$, 使得$p' = p \circ \varphi_{M'M},\ q' = q \circ \varphi_{M'M}$.

(2) $(S \times T;\ p : (s,t) \mapsto s,\ q : (s,t) \mapsto t)$ 是S 与T 的直积.

证明. (1) 由直积的定义. 存在同态$\varphi_{M'M} : M' \to M$ 和$\varphi_{MM'} : M \to M'$, 使得

$$\begin{aligned} p' &= p \circ \varphi_{M'M}, \quad q' = q \circ \varphi_{M'M}; \\ p &= p' \circ \varphi_{MM'}, \quad q = q' \circ \varphi_{MM'}. \end{aligned}$$

故

$$p = p \circ (\varphi_{M'M} \circ \varphi_{MM'}), \quad q = q \circ (\varphi_{M'M} \circ \varphi_{MM'}).$$

取$(N;f,g)=(M;p,q)$, 则存在唯一的$\varphi:M\to M$ 使得

$$p=p\circ\varphi,\quad q=q\circ\varphi.$$

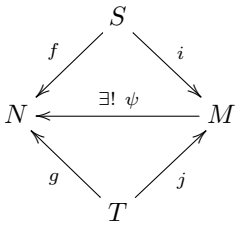
显然$\varphi=1_M$满足条件, 故$\varphi_{M'M}\circ\varphi_{MM'}=1_M$. 同理$\varphi_{MM'}\circ\varphi_{M'M}=1_{M'}$. 所以$\varphi_{M'M}:M'\to M$ 是模同构.

(2) 对任意三元组$(N;f,g)$, 令$\varphi:N\to S\times T$ 为映射

$$n\mapsto(f(n),g(n)).$$

容易验证φ 满足定义 1.30中的交换图表. 另一方面, 如$\varphi(n)=(s,t)$, 则$p\varphi(n)=s=f(n),\ q\varphi(n)=t=g(n)$. 故$\varphi$ 唯一. □

定义1.32. 设S 与T 是R-模. 三元组$(M;i,\ j)$, 其中M 是R-模, $S\xrightarrow{i}M$和$T\xrightarrow{j}M$是模同态, 称为S 与T 的**直和**是指对任意三元组$(N;f,g)$, 其中N 是模, $S\xrightarrow{f}N$ 和$T\xrightarrow{g}N$ 是模同态, 存在唯一的模同态$\psi:M\to N$ 使得图表



交换, 即等式$f=\psi\circ i,\ g=\psi\circ j$ 成立.

命题1.33. (1) 如$(M;i,j)$ 和$(M';i',j')$ 均是S 与T 的直和, 则存在唯一的同构$\psi_{MM'}:M\to M'$, 使得$i'=\psi_{MM'}\circ i, j'=\psi_{MM'}\circ j$.

(2) $(S\times T;i:s\mapsto(s,0),\ j:t\mapsto(0,t))$ 是S 与T 的直和.

(3) $(S\oplus T;i,j)$ 是S 与T 的直和.

证明. 与命题 1.31的证明类似, 留给读者. □

注记. 上述三命题说明$S\times T$ 既可以视为S 与T 的直积, 也可以视为它们的直和. 我们称满同态$p:S\times T\to S,(s,t)\mapsto s$ 与$q:S\times T\to T,(s,t)\mapsto t$ 为**典范投射** (canonical projection), 称单同态$i:S\to S\times T,s\mapsto(s,0)$ 与$j:T\to S\times T,t\mapsto(0,t)$ 为**典范嵌入映射**(canonical injection).

事实上, 直积与直和的定义可以推广到任意多个模的情形.

定义1.34. 设$\{S_\alpha\}_{\alpha\in I}$ 是R-模集合.

(1) 数组$(M;\ M\xrightarrow{\pi_\alpha}S_\alpha,\alpha\in I)$ 称为$\{S_\alpha\}_{\alpha\in I}$ 的**直积**是指对任意模同态族$\{f_\alpha:N\to S_\alpha\}_{\alpha\in I}$, 存在唯一的同态$\varphi:N\to M$ 使得$f_\alpha=\pi_\alpha\circ\varphi$ 对任意$\alpha\in I$ 成立.

(2) 数组$(M;\ S_\alpha \xrightarrow{\iota_\alpha} M, \alpha \in I)$ 称为$\{S_\alpha\}_{\alpha\in I}$ 的**直和**是指对任意模同态族$\{g_\alpha : S_\alpha \to N\}_{\alpha\in I}$, 存在唯一的同态$\psi : M \to N$ 使得$g_\alpha = \psi \circ \iota_\alpha$ 对任意$\alpha \in I$ 成立.

命题1.35. (1) $\{S_\alpha\}_{\alpha\in I}$ 的直积(或直和)若存在, 则必在同构的意义下唯一.

(2) $\prod\limits_{\alpha\in I} S_\alpha$, 即$\{S_\alpha\}_{\alpha\in I}$ 的笛卡儿积是它的直积, 典范投射$\pi_\alpha : \prod\limits_{\alpha\in I} S_\alpha \to S_\alpha$ 是满同态$(s_j)_{j\in I} \mapsto s_\alpha$.

(3) 令

$$\bigoplus_{\alpha\in I} S_\alpha = \{(s_\alpha)_{\alpha\in I} \in \prod_{\alpha\in I} S_\alpha : s_\alpha = 0 \text{对几乎所有} \alpha \text{ 成立}\}.$$

则$\bigoplus\limits_{\alpha\in I} S_\alpha$ 是$\prod\limits_{\alpha\in I} S_\alpha$ 的子模, 且是$\{S_\alpha\}_{\alpha\in I}$ 的直和, 典范嵌入映射ι_j 是单同态$S_j \to \bigoplus\limits_{\alpha\in I} S_\alpha, s_j \mapsto (0, \cdots, s_j, \cdots, 0)$.

证明. (1)的证明与命题 1.31(1)的证明类似, (2) 和(3) 容易验证. □

注记. (1) 由上述命题可以看出, 有限多个模的直积与直和是典范同构的, 而无限多个模的直积与直和是不一样的.

(2) 自此以后, 如不做特别说明, 我们记笛卡儿积$\prod\limits_{\alpha\in I} S_\alpha$ 为$\{S_\alpha\}_{\alpha\in I}$ 的直积, 命题中定义的$\bigoplus\limits_{i\in I} S_i$ 为它的直和.

命题1.36. 设M_α $(\alpha \in I)$ 和N 为R-模, 则

(1) $\mathrm{Hom}(\bigoplus\limits_{\alpha\in I} M_\alpha, N) \cong \prod\limits_{\alpha\in I} \mathrm{Hom}(M_\alpha, N)$.

(2) $\mathrm{Hom}(N, \prod\limits_{\alpha\in I} M_\alpha) \cong \prod\limits_{\alpha\in I} \mathrm{Hom}(N, M_\alpha)$.

证明. (1) 对于$\varphi \in \mathrm{Hom}(\bigoplus\limits_{\alpha\in I} M_\alpha, N)$, 定义$\varphi_\alpha = \varphi\circ\iota_\alpha$, 则$(\varphi_\alpha)_{\alpha\in I} \in \prod\limits_{\alpha\in I} \mathrm{Hom}(M_\alpha, N)$. 现在只要根据直和的定义验证$\varphi \mapsto (\varphi_\alpha)_{\alpha\in I}$ 是模同构即可.

(2) 对于$\psi \in \mathrm{Hom}(N, \prod\limits_{\alpha\in I} M_\alpha)$, 定义$\psi_\alpha = \pi_\alpha\circ\psi$, 则$(\psi_\alpha)_{\alpha\in I} \in \prod\limits_{\alpha\in I} \mathrm{Hom}(N, M_\alpha)$. 现在只要根据直积的定义验证$\psi \mapsto (\psi_\alpha)_{\alpha\in I}$ 是模同构即可. □

定义1.37. 模M 的子模S 称为M 的**直和项**(direct summand)是指存在M 的子模T 使得$M = S \oplus T$.

命题1.38. 子模S 是模M 的直和项当且仅当存在R-模同态$p : M \to S$ 使得$p\,|_S = 1_S$.

注记. 上述同态p 称为M 到S 的**收缩(retraction, 也称为保核收缩)**.

证明. $\Rightarrow$ 显然.

$\Leftarrow$ 令$T = \ker p$. 一方面因为$m = m - p(m) + p(m)$, 而$p(m - p(m)) = p(m) - p(p(m)) = 0$, 所以$M = S + T$. 另一方面如$m \in S \cap T$, 则$m = p(m) = 0$, 故$S \cap T = 0$. 所以$M = S \oplus T$. □

推论1.39. 如$M = S \oplus T$而A 是S 和M 之间的一个中间模, 则$A = S \oplus (A \cap T)$.

证明. 令$p : M \to S$ 是M 到S 的收缩$s + t \mapsto s$. 由$A \supseteq S$, 故$p\mid_A : A \to S$ 为A到S 的收缩, 此时$\ker p\mid_A = A \cap \ker p = A \cap T$. □

命题1.40. 设$\{S_i\}_{i=1}^n$ 是R-模M 的子模族. 则M 是此子族的直和当且仅当M中任意元素m 均可唯一分解为$m = s_1 + \cdots + s_n,\ s_i \in S_i$ 的形式.

证明. 如M 为直和, 令$\varphi : \prod_{i=1}^n S_i \xrightarrow{\sim} M$为对应的同构映射. 令$\iota_i : S_i \to \prod_{i=1}^n S_i$ 为典范嵌入映射, 则$\varphi\iota_i : S_i \to M$ 是典范嵌入映射. 对于$s \in \prod_{i=1}^n S_i$, $s = \sum_{i=1}^n \iota_i(s_i)$的分解式唯一, 故$m = \varphi(s) = \sum_{i=1}^n (\varphi\iota_i)(s_i) = \sum_{i=1}^n s_i$ 的分解式也唯一.

反过来, 如m 可唯一表示为$m = s_1 + \cdots + s_n$的形式, 令$\psi : M \to \prod_{i=1}^n S_i$ 为映射

$$\psi(m) = \sum_{i=1}^n \iota_i(s_i) = (s_1, \cdots, s_n).$$

则容易验证ψ 为同构. □

推论1.41. 令$M = S_1 + \cdots + S_n$. 则$M \cong S_1 \oplus \cdots \oplus S_n$ 当且仅当对每个i, $S_i \cap (S_1 + \cdots + \widehat{S_i} + \cdots + S_n) = 0$, 这里$\widehat{S_i}$ 表示去除S_i-项.

证明. 若$M \cong S_1 \oplus \cdots \oplus S_n$, 则对任意$m \in M$, m 可以唯一写为$s_1 + \cdots + s_n$的形式, 其中$s_i \in S_i$. 故对任意$s_i \in S_i$, $s_i = 0 + \cdots + s_i + \cdots + 0 \in M$. 若$s_i \in S_1 + \cdots + \widehat{S_i} + \cdots + S_n$, 则$s_i = \sum_{j \neq i} s_j,\ s_j \in S_j$. 由唯一性知$s_j = 0$和$s_i = 0$, 即$S_i \cap (S_1 + \cdots + \widehat{S_i} + \cdots + S_n) = 0$.

反过来, 若对每个i, $S_i \cap (S_1 + \cdots + \widehat{S_i} + \cdots + S_n) = 0$. 任取$m \in M = S_1 + \cdots + S_n$. 假设$m = s_1 + \cdots + s_n = s_1' + \cdots + s_n',\ s_i, s_i' \in S_i$. 则对每个$i$, $s_i - s_i' = \sum_{j \neq i} (s_j' - s_j) \in S_i \cap (S_1 + \cdots + \widehat{S_i} + \cdots + S_n) = 0$, 即$s_i = s_i'$. 故$m$ 的表示是唯一的, 所以M 是直和. □

§1.1.6 正合列

正合是同调代数最重要的概念. 我们首先介绍一下模论里的正合.

定义1.42. 设M_i 是R-模, $f_i : M_i \to M_{i-1}$ 是模同态. 序列

$$\cdots \longrightarrow M_{n+1} \xrightarrow{f_{n+1}} M_n \xrightarrow{f_n} M_{n-1} \longrightarrow \cdots$$

称为**在M_n 处正合**(exact)是指$\operatorname{im} f_{n+1} = \ker f_n$; 序列称为**正合列**(exact sequence)是指它在任意M_n 处均正合; 称为**复形**(complex)是指对任意n, 均有$f_n \circ f_{n+1} = 0$, 即$\operatorname{im} f_{n+1} \subseteq \ker f_n$.

由正合的定义, 下述命题显然成立:

命题1.43. (1) 序列$0 \longrightarrow A \xrightarrow{f} B$ 正合当且仅当f 是单射.
(2) 序列$A \xrightarrow{g} B \longrightarrow 0$ 正合当且仅当g 是满射.
(3) 序列$0 \longrightarrow A \xrightarrow{h} B \longrightarrow 0$ 正合当且仅当h 为同构.

定义1.44. 形如$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ 的正合列称为**短正合列**(short exact sequence). 我们也称此正合列为A **到**C **的扩展**(extension of A by C).

命题1.45. 如序列$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ 是短正合列, 则

$$A \cong \operatorname{im} f, \quad B/\operatorname{im} f \cong C.$$

证明. 由于f 是单射, g 是满射而且$\ker g = \operatorname{im} f$, 由同态基本定理即得需要求的两同构. □

注记. 我们看一个特例. 如A 是B 的子模, $f : A \hookrightarrow B$ 是包含映射. 则$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ 正合即是说g 诱导同构$B/A \cong C$. 例如, 对于模链$T \subseteq S \subseteq M$, 由第三同构定理即得到短正合列

$$0 \longrightarrow S/T \xrightarrow{f} M/T \xrightarrow{g} M/S \longrightarrow 0.$$

定义1.46. 短正合列$0 \longrightarrow A \xrightarrow{i} B \xrightarrow{p} C \longrightarrow 0$ 称为**分裂的**(splitting)是指存在同态$j : C \to B$ 使得$p \circ j = 1_C$.

命题1.47. 如正合列$0 \longrightarrow A \xrightarrow{i} B \xrightarrow{p} C \longrightarrow 0$分裂, 则$B \cong A \oplus C$.

证明. 视i 为包含映射, 从而$A = \operatorname{im} i$ 看作是B 的子模. 对于$b \in B$, 由于$p(b - jp(b)) = p(b) - pjp(b) = 0$, 故$b - jp(b) \in A$. 我们定义映射

$$\varphi : B \to A \oplus C,\ b \mapsto (b - jp(b), p(b)).$$

容易验证φ 为同态. 如$\varphi(b) = 0$, 则$p(b) = 0$, 且$b - jp(b) = b - j(0) = 0$, 所以$b = 0$, 即φ 为单射. 又$\varphi(a + j(c)) = (a, c)$, 故$\varphi$ 为满射. □

命题1.48. 序列$M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$ 是R-模正合列当且仅当对任意模N, 序列$0 \to \operatorname{Hom}_R(M'', N) \xrightarrow{p^*} \operatorname{Hom}_R(M, N) \xrightarrow{i^*} \operatorname{Hom}_R(M', N)$ 是正合列, 这里记号 *表示$f^*(h) = hf$.

证明. 我们先证$\Leftarrow$:

首先证明p 是满射: 取$N = M''/\operatorname{im} p$, $f : M'' \to N$ 为自然商映射. 则$p^*(f) = fp = 0$. 由于p^* 是单同态, 故$f = 0$ 是零映射, 所以$N = 0$, 即p 为满射.

取$N = M''$, $g = 1_N$. 则$g \in \operatorname{Hom}_R(M'', N)$ 且$0 = (pi)^*(g) = pi$. 所以$\operatorname{im} i \subseteq \ker p$.

取$N = M/\operatorname{im} i$, $h : M \to N$ 为自然商映射. 则$i^*(h) = hi = 0$. 故$h \in \ker i^* = \operatorname{im} p^*$, 即存在$h' \in \operatorname{Hom}_R(M'', N)$ 使得$h = p^*(h') = h'p$. 如$\operatorname{im} i \neq \ker p$, 则存在$b \in \ker p$ 但$b \notin \operatorname{im} i$, 故$p(b) = 0$ 且$h(b) \neq 0$. 但$h(b) = h'p(b) = 0$ 矛盾. 所以$\operatorname{im} i = \ker p$.

再证⇒:

对于$f \in \operatorname{Hom}_R(M'', N)$, $p^*(f) = fp$; $g \in \operatorname{Hom}_R(M, N)$, $i^*(g) = gi$. 故$i^*p^*(f) = fpi = 0$. 所以$\operatorname{im} p^* \subseteq \ker i^*$. 若$p^*(h) = hp = 0$, 由$p$ 是满射, 故$h = 0$, 所以p^* 是单射.

要证明$\operatorname{im} p^* = \ker i^*$, 只要证对任意$g \in \ker i^*$, 存在$f \in \operatorname{Hom}_R(M'', N)$ 使得$g = p^*(f)$. 如$g \in \ker i^*$, 则$gi = 0$, 即对任意$x' \in M'$, 均有$gi(x') = 0$. 对于$x'' \in M''$, 令$x \in M$ 使得$x'' = p(x)$. 定义$f(x'') = g(x)$. 我们首先验证f 是良定义的: 如$p(x_1) = x''$, 则$p(x_1 - x) = 0$, 所以存在$x' \in M'$, $x_1 - x = i(x')$, 因此$g(x_1 - x) = 0$, 即$g(x_1) = g(x)$. 我们其次验证f 是R-模映射: 如$p(x) = x''$, 则$p(rx) = rx''$, 所以$f(rx'') = g(rx) = rg(x) = rf(x'')$. 由$f$ 的定义即知$g = p^*(f)$. □

同理我们有

命题1.49. *序列$0 \to M' \xrightarrow{i} M \xrightarrow{p} M''$ 是R-模正合列当且仅当对任意模N, 序列$0 \to \operatorname{Hom}_R(N, M') \xrightarrow{i_*} \operatorname{Hom}_R(N, M) \xrightarrow{p_*} \operatorname{Hom}_R(N, M'')$ 是正合列, 这里记号 $_*$表示$f_*(h) = fh$.*

定义1.50. 设$f : M \to N$ 是模同态. f 的余核(cokernel), 记为$\operatorname{coker} f$, 即商模$N/\operatorname{im} f$.

由定义, 任意模同态$f : M \to N$ 诱导正合列

$$0 \to \ker f \to M \xrightarrow{f} N \to \operatorname{coker} f \to 0.$$

给定R-模交换图表

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow{\scriptstyle d_A} & & \downarrow{\scriptstyle d_B} \\ A' & \xrightarrow{f'} & B', \end{array}$$

我们有如下的交换图表:

$$\begin{array}{ccccccc} \ker(d_A) & \xrightarrow{i} & A & \xrightarrow{d_A} & A' & \xrightarrow{p} & \operatorname{coker}(d_A) \\ \downarrow{\scriptstyle f_*} & \searrow^{f\circ i} & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f'} & \searrow^{p\circ f'} & \downarrow{\scriptstyle f'_*} \\ \ker(d_B) & \xrightarrow{i} & B & \xrightarrow{d_B} & B' & \xrightarrow{p} & \operatorname{coker}(d_B). \end{array}$$

对于$m' \in \ker d_A$, $d_B(f(m')) = f'(d_A(m')) = 0$, 所以$f(m') \in \ker d_B$, 我们得到映射$f_* : \ker(d_A) \to \ker(d_B)$, $m' \mapsto f(m')$. 如$n'_1 - n' \in d_A(A)$, 记$n'_1 -$

$n' = d_A(m')$, 则$f'(n'_1 - n') = f'(d'(m')) = d(f(m')) \in d_B(B)$. 由此可知映射$f'_* : \operatorname{coker}(d_A) \to \operatorname{coker}(d_B)$, $n' + d_A(A) \mapsto f'(n') + d_B(B)$, 是定义良好的. 容易验证$f_*$ 和f'_*是唯一的模同态使得上述图表交换.

定理1.51 (蛇形引理, Snake Lemma). 行正合交换图表

$$\begin{array}{ccccccc} & & X' & \xrightarrow{f} & X & \xrightarrow{g} & X'' \longrightarrow 0 \\ & & \downarrow{\scriptstyle d'} & & \downarrow{\scriptstyle d} & & \downarrow{\scriptstyle d''} \\ 0 & \longrightarrow & Y' & \xrightarrow{p} & Y & \xrightarrow{q} & Y'' \end{array}$$

诱导正合列

$$\ker(d') \xrightarrow{f_*} \ker(d) \xrightarrow{g_*} \ker(d'') \xrightarrow{\delta} \operatorname{coker}(d') \xrightarrow{p_*} \operatorname{coker}(d) \xrightarrow{q_*} \operatorname{coker}(d'').$$

证明. 首先连接映射$\delta : \ker(d'') \to \operatorname{coker}(d')$ 如下给出: 对于$m'' \in \ker(d'')$, 取$m \in X$ 使得$g(m) = m''$. 则$qd(m) = d''g(m) = 0$. 故$d(m) = p(n')$ 对某个唯一的$n' \in Y'$ 成立. 我们定义$\delta(m'') = n' + d'(X')$.

我们证明δ 是良定义的: 如$m_0 \in X$ 也满足$g(m_0) = m''$, 则$m - m_0 = f(m')$. 故$d(m - m_0) = df(m') = pd'(m')$. 所以$p^{-1}(d(m - m_0)) \in d'(X')$. 故$\delta$ 是良定义的.

我们证明序列在$\ker(d)$ 处正合. 一方面由于$g_*f_*(m') = gf(m') = 0$, 所以$\operatorname{im}(f_*) \subseteq \ker(g_*)$. 反之, 若$g_*(m) = 0$, 则$g(m) = 0$. 故存在$m' \in X'$ 使得$m = f(m')$. 令$n' = d'(m')$, 则$p(n') = df(m') = d(m) = 0$. 由于第二行是正合列, 故$n' = 0$, $m' \in \ker(d')$. 故有$m = f_*(m')$, 即$\operatorname{im} f_* \supseteq \ker g_*$.

我们证明序列在$\ker(d'')$ 处正合. 由δ 的定义$\delta g_*(m) = \delta g(m) = p^{-1}(d(m)) = 0$. 所以$\ker(\delta) \supseteq \operatorname{im}(g_*)$. 反之, 若$\delta(m'') = 0$, 令$m$ 为m'' 的原像. 则$d(m) = p(n')$ 对于某个$n' \in d'(X')$ 成立. 即$d(m) = pd'(m')$. 令$m_0 = m - f(m')$, 则m_0 也是m'' 的原像, 且$d(m_0) = d(m) - df(m') = d(m) - pd'(m') = 0$, 即$m_0 \in \ker d$, $m'' = g_*(m_0)$. 所以$\ker\delta \subseteq \operatorname{im} g_*$.

我们证明序列在$\operatorname{coker}(d')$ 处正合. 一方面$p_*\delta(m'') = p_*(n' + d'(X')) = p(n') + d(X)$. 但$p(n') = d(m) \in d(X)$, 这里$m$ 是m'' 的原像. 故$p_*\delta = 0$, $\operatorname{im}\delta \subseteq \ker p_*$. 反过来, 如$p(n') = d(m)$ 对某个$m \in X$ 成立, 则$d''g(m) = qd(m) = qp(n') = 0$, 故$g(m) = m'' \in \ker(d'')$. 此时$\delta(m'') = n' + d'(X') \in \ker(p_*)$, 因此$\operatorname{im}\delta \supseteq \ker(p_*)$.

我们最后证明序列在$\operatorname{coker}(d)$ 处正合. 一方面对于$n' + d'(X') \in \operatorname{coker}(d')$, $q_*p_*(n' + d'(X')) = qp(n') + d''(X'') = 0$. 故$\operatorname{im}(p_*) \subseteq \ker(q_*)$. 反之, 若$n + d(X) \in \operatorname{coker} d$ 且$q_*(n + d(X)) = q(n) + d''(X'') = 0$, 则$q(n) = d''(m'')$. 取$m \in X$, $g(m) = m''$, 则$q(n - d(m)) = d''(m'') - d''g(m) = 0$. 由第二行的正合性, 存在$n' \in Y'$, $n - d(m) = p(n')$. 所以$p_*(n' + d'(X')) = n + d(X)$, 故$\operatorname{im}(p_*) \supseteq \ker(q_*)$. □

§1.2 范畴与函子

§1.2.1 范畴

所谓范畴是由**对象**和**对象间的态射**构成的数学系统. 这是现代数学研究中应用范围最广泛的数学概念之一. 详言之, 我们有如下定义:

定义1.52. 所谓**范畴**(category) 是指这样的数学系统$\mathcal{C}$, 它包含如下两组数据:

(1) **对象**(object): 通常用$A, B, C, \cdots$ 表示. 所有对象构成的类记为$\mathrm{ob}(\mathcal{C})$.

(2) **态射**(morphism): 对于对象A 和B, 有态射集$\mathrm{Hom}(A, B)$, 其中元素, 记为$f : A \to B$, 称为A 到B 的态射. 所有态射集构成的集合类记为$\mathrm{Ar}(\mathcal{C})$.

对于$A, B, C \in \mathrm{ob}(\mathcal{C})$, 存在复合态射

$$\mathrm{Hom}(B, C) \times \mathrm{Hom}(A, B) \to \mathrm{Hom}(A, C),\ (g, f) \mapsto gf$$

且满足如下公理:

(A1) **两两不交性**: 态射集$\mathrm{Hom}(A, B)$与$\mathrm{Hom}(A', B')$ 互不相交, 除非$A = A'$且$B = B'$.

(A2) **恒等态射存在性**: 对于每个对象$A \in \mathrm{ob}(\mathcal{C})$, 存在态射$1_A \in \mathrm{Hom}(A, A)$, 使得对任意态射$f : A \to B$ 和$g : C \to A$, 有

$$f1_A = f, \quad 1_A g = g.$$

1_A 称为A 的**恒等态射**.

(A3) **结合律**: 对于态射$f : A \to B$, $g : B \to C$ 和$h : C \to D$, 有

$$h(gf) = (hg)f.$$

注记. (1) 范畴里的对象可以是点集, 也可以不是.

(2) 容易看出, 恒等态射1_A 是唯一确定的: 如$\varepsilon \in \mathrm{Hom}(A, A)$ 也满足公理(A2), 则$\varepsilon = \varepsilon 1_A = 1_A$.

(3) 我们常记$\mathrm{Hom}(A, A)$ 为$\mathrm{End}(A)$. 公理(A2) 和(A3) 说明在态射的复合作为乘法的意义下, $\mathrm{End}(A)$ 是含幺半群, 其幺元是1_A.

定义1.53. 对于态射$f : A \to B$, 如存在态射$g : B \to A$ 使得

$$gf = 1_A \quad 且 \quad fg = 1_B,$$

则称f 为**同构**, 称g 是f 的**逆**. 也称A 与B 同构.

例1.54. 此处我们列举一些熟悉的范畴的例子.

(1) $\mathcal{S}$ets 是(某给定宇宙下)所有集合构成的范畴. 它的对象是 集合, 态射即集合间的映射, 恒等态射即恒等映射, 同构即集合间的一一对应.

(2) $\mathcal{G}$roups 是所有群构成的范畴. 它的对象是群, 态射即群同态, 同构即群同构.

(3) $\mathcal{R}$ings 是所有环构成的范畴. 它的对象是环, 态射是环同态. 同样, $\mathcal{C}$omRings 是所有交换环构成的范畴, 它的对象是交换环, 态射还是环同态.

(4) 设R 是含幺交换环. $\mathcal{R}$-mod 是所有R-模构成的范畴, 它的对象是R-模, 态射即R- 模同态. 这是我们主要研究的范畴.

特别地, 如$R = \mathbb{Z}$, 所有阿贝尔群构成的范畴通常记为$\mathcal{A}$b.

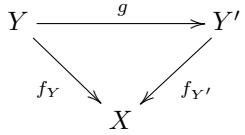
(5) 设X 是$\mathbb{R}^n$ 中的开集. X 上的连续函数范畴$C^0(X)$ 和C^∞函数范畴$C^\infty(X)$的对象是X 的开子集, 态射分别是开集间的连续和C^∞ 映射.

(6) 设U 是复平面$\mathbb{C}$ 中的开集. U 上的全纯映射范畴$H(U)$的对象是U 中的开子集, 态射是开集间的全纯映射.

定义1.55. 设$\mathcal{C}$ 为范畴, X 是$\mathcal{C}$ 中的一固定对象. 令范畴$\mathcal{C}_X$ 如下给出: $\mathcal{C}_X$ 的对象是态射$Y \xrightarrow{f_Y} X$, 两对象间的态射集

$$\mathrm{Hom}(Y \xrightarrow{f_Y} X, Y' \xrightarrow{f_Y} X) = \{g \in \mathrm{Hom}(Y, Y') : f_{Y'} g = f_Y\},$$

即$\mathcal{C}_X$ 的态射是$\mathcal{C}$中的态射$g : Y \to Y'$ 使得图表



交换. 容易验证$\mathcal{C}_X$ 的确满足范畴定义的公理.

定义1.56. 设$\mathcal{C}$ 为范畴. $\mathcal{C}$ 的**反范畴** (opposite category) 是指范畴$\mathcal{C}^{\mathrm{op}}$, 它的对象是$\mathcal{C}$ 的对象, 但态射集

$$\mathrm{Hom}_{\mathcal{C}^{\mathrm{op}}}(A, B) = \mathrm{Hom}_{\mathcal{C}}(B, A),$$

即$\mathcal{C}^{\mathrm{op}}$ 的态射$f : A \to B$ 是$\mathcal{C}$ 中的态射$f : B \to A$.

定义1.57. 设$\mathcal{C}$ 为范畴. $\mathcal{C}$ 中的对象P 称为**始对象**(initial object)是指对任意$A \in \mathrm{ob}(\mathcal{C})$, 存在唯一的态射$P \xrightarrow{i_A} A$.

$\mathcal{C}$ 中的对象P 称为**终对象**(final object)是指对任意$A \in \mathrm{ob}(\mathcal{C})$, 存在唯一的态射$A \xrightarrow{p_A} P$.

如P 既是始对象也是终对象, 称P 为**零对象**(zero object), 记为0.

命题1.58. (1) *始对象(终对象)如存在, 则必唯一, 即两始对象(终对象)间存在唯一的同构.*

(2) 如P 是范畴$\mathcal{C}$ 的始对象(终对象), 则P 是范畴$\mathcal{C}^{\mathrm{op}}$ 的终对象(始对象).

(3) $X \xrightarrow{1_X} X$ 是范畴$\mathcal{C}_X$ 的终对象.

证明. (1) 若P和P' 均是始对象, 则$\mathrm{Hom}(P,P') = \{i_{PP'}\}$, $\mathrm{Hom}(P',P) = \{i_{P'P}\}$, $\mathrm{Hom}(P,P) = \{1_P\}$ 和$\mathrm{Hom}(P',P') = \{1_{P'}\}$ 都是一元集. 由复合映射的性质即知$i_{PP'}i_{P'P} = 1_{P'}$, $i_{P'P}i_{PP'} = 1_P$. 故P 与P' 同构. 对于P 与P' 均是终对象的情形, 证明类似.

(2)与(3) 由定义立知. □

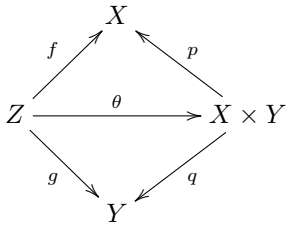
例1.59. (1) 对于群范畴$\mathcal{G}$roups, $\{1\}$ 既是始对象也是终对象, 即是零对象.

(2) 对于集合范畴$\mathcal{S}$ets, 空集是始对象而独点集是终对象, 它没有零对象.

(3) 对于环范畴$\mathcal{R}$ings, 整数环$\mathbb{Z}$ 是始对象, 零环是终对象, 它没有零对象.

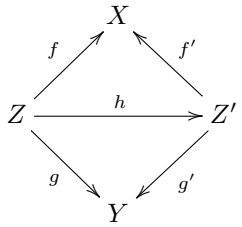
定义1.60. 设$\mathcal{C}$ 为范畴, X 与Y 是$\mathcal{C}$ 中的对象. X 与Y 的**乘积**(product) 是指三元组$(X\times Y; p, q)$, 其中$X\times Y$ 是$\mathcal{C}$ 中的对象, $p: X\times Y \to X$ 和$q: X\times Y \to Y$ 是态射, 常称为投射, 满足如下条件:

对于任何三元组$(Z; f, g)$, 其中$Z \in \mathrm{ob}(\mathcal{C})$, $f: Z \to X$ 和$g: Z \to Y$ 是态射, 存在唯一的态射$\theta: Z \to X\times Y$ 使得图表



交换, 即$f = p\theta$ 和$g = q\theta$.

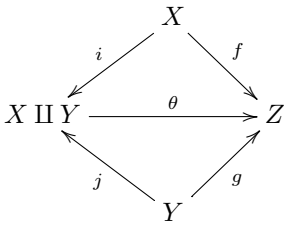
我们令$\mathcal{C}'$ 的对象为三元组$(Z; f, g)$, 其中$Z \in \mathrm{ob}(\mathcal{C})$, $f: Z \to X$ 和$g: Z \to Y$ 为态射, 而$\mathcal{C}'$ 的态射$h: (Z; f, g) \to (Z'; f', g')$ 是$\mathcal{C}$ 中的态射$h: Z \to Z'$ 使得图表



交换, 即$f'h = f$ 和$g'h = g$. 则容易验证$\mathcal{C}'$ 的确是范畴. 那么X 与Y 的乘积就是范畴$\mathcal{C}'$ 中的终对象. 由命题 1.58知X与Y 的乘积在同构意义下唯一.

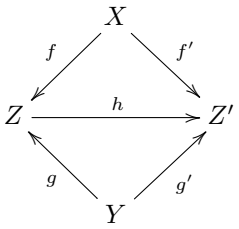
定义1.61. 设$\mathcal{C}$ 为范畴, X 与Y 是$\mathcal{C}$ 中的对象. X 与Y 的**上乘积**(coproduct) 是指三元组$(X \amalg Y; i, j)$, 其中$X \amalg Y \in \mathrm{ob}(\mathcal{C})$, $i: X \to X \amalg Y$ 与$j: Y \to X \amalg Y$ 为态射, 称为内射, 满足如下条件:

对于任意三元组$\{Z; f, g\}$, 其中$Z \in \mathrm{ob}(\mathcal{C})$, $f : X \to Z$ 和$g : Y \to Z$为态射. 存在唯一的态射$\theta : X \amalg Y \to Z$ 使得$\theta i = f$ 和$\theta j = g$. 即图表



交换.

与乘积的情形一样, 如果我们令范畴$\mathcal{D}'$ 的对象是三元组$(Z; f, g)$, 其中$Z \in ob(\mathcal{C}), f : X \to Z$ 和$g : Y \to Z$ 为态射, $\mathcal{D}'$ 的态射$h : (Z; f, g) \to (Z'; f', g')$ 是$\mathcal{C}$中的态射$h : Z \to Z'$ 使得图表



交换, 即$f' = hf$ 和$g' = hg$. 则X 与Y 的上乘积即是范畴$\mathcal{D}'$ 中的始对象, 故在同构意义下它是唯一的. 事实上容易看出$\mathcal{D}' = (\mathcal{C}')^{\mathrm{op}} = (\mathcal{C}^{\mathrm{op}})'$.

例1.62. (1) 对于模范畴$\mathcal{R}$-mod, 则§§1.1.5中定义的模M 与N 的直积即本节定义的乘积, §§1.1.5中定义的直和即上面定义的上乘积. 我们知道M 与N的直积与直和本质上是同构的.

(2) 对于集合范畴$\mathcal{S}$ets, X 与Y 的上乘积$X \amalg Y$ 是集合的不交并$X' \sqcup Y'$, 其中$X' = X \times \{1\}$ 与$Y' = Y \times \{2\}$ 是笛卡儿积$X \times Y$ 的子集合. 事实上只要定义映射$i : X \to X' \subset X \amalg Y,\ x \mapsto (x, 1)$, 映射$j : Y \to Y' \subset X \amalg Y,\ y \mapsto (y, 2)$, 而映射$\theta : X \amalg Y \to Z,\ \theta(x, 1) = f(x),\ \theta(y, 2) = g(y)$ 即可.

集合X 与Y 的乘积, 就是它们的笛卡儿积, 此时映射$p : X \times Y \to X,\ (x, y) \mapsto x$, 映射$q : X \times Y \to Y,\ (x, y) \mapsto y$.

同样可以定义任意多个对象的乘积与上乘积.

定义1.63. 设$\mathcal{C}$ 为范畴, $\{X_\alpha\}_{\alpha \in I}$ 是$\mathcal{C}$ 的一组对象.

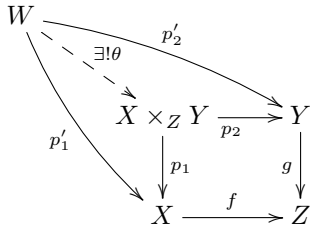
$\{X_\alpha\}_{\alpha \in I}$ 的**上乘积** 是指组$(\coprod\limits_{\alpha \in I} X_\alpha; (\iota_\alpha)_{\alpha \in I})$, 其中$\coprod\limits_{\alpha \in I} X_\alpha \in \mathrm{ob}(\mathcal{C})$, 态射$\iota_\alpha : X_\alpha \to \coprod\limits_{\alpha \in I} X_\alpha$, 满足如下泛性质: 对任意组$(Z; f_\alpha : X_\alpha \to Z)$, 存在唯一的态射$\theta : \coprod\limits_{\alpha \in I} X_\alpha \to Z$ 使得$\theta \iota_\alpha = f_\alpha$ 对所有$\alpha \in I$ 成立.

$\{X_\alpha\}_{\alpha\in I}$ 的**乘积**是指组$(\prod\limits_{\alpha\in I} X_\alpha; (\pi_\alpha)_{\alpha\in I})$, 其中$\prod\limits_{\alpha\in I} X_\alpha \in \mathrm{ob}(\mathcal{C})$, 态射$\pi_\alpha : \prod\limits_{\alpha\in I} X_\alpha \to X_\alpha$, 满足泛性质: 对任意组$(W; g_\alpha : W \to X_\alpha)$, 存在唯一的态射$\tilde{\theta} : W \to \prod\limits_{\alpha\in I} X_\alpha$ 使得$g_\alpha = \pi_\alpha\tilde{\theta}$ 对所有$\alpha \in I$ 成立.

例1.64. 对于模范畴$\mathcal{R}$-mod, $\{X_\alpha\}_{\alpha\in I}$ 的上乘积 $\coprod\limits_{\alpha\in I} X_\alpha = \bigoplus\limits_{\alpha\in I} X_\alpha$, 乘积 $\prod\limits_{\alpha\in I} X_\alpha$ 即$\{X_\alpha\}_{\alpha\in I}$ 的笛卡儿积.

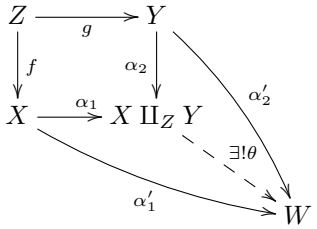
现在假设$\mathcal{C}$ 是范畴, Z 是$\mathcal{C}$ 中一个对象.

定义1.65. 态射$f : X \to Z$ 和$g : Y \to Z$ 的**拉回**(pullback), 又称**纤维积**(fibered product), 是 指三元组$(X \times_Z Y; p_1, p_2)$, 其中$p_1 : X \times_Z Y \to X$, $p_2 : X \times_Z Y \to Y$ 且$fp_1 = gp_2$, 满足如下泛性质: 对任意$(W; p_1' : W \to X, p_2' : W \to Y)$ 且$fp_1' = gp_2'$, 存在唯一的态射$\theta : W \to X \times_Z Y$ 使得$p_1' = p_1\theta, p_2' = p_2\theta$, 即图表



交换. 换言之, $(X \times_Z Y; p_1, p_2)$ 是范畴$\mathcal{C}_Z$ 的乘积. 我们常简称$X \times_Z Y$ 为X 与Y 在Z 上的纤维积.

定义1.66. 态射$f : Z \to X$ 和$g : Z \to Y$ 的**推出**(pushout), 又称**纤维上积**(fibered coproduct) 或**纤维和**(fibered sum), 是指$(X \amalg_Z Y; \alpha_1, \alpha_2)$, 其中$\alpha_1 : X \to X \amalg_Z Y$, $\alpha_2 : Y \to X \amalg_Z Y$ 且$\alpha_1 f = \alpha_2 g$, 满足泛性质: 对任意$(W; \alpha_1' : X \to W, \alpha_2' : Y \to W)$ 且$\alpha_1' f = \alpha_2' g$, 存在唯一的态射$\theta : X \amalg_Z Y \to W$ 使得$\alpha_1' = \theta\alpha_1$, $\alpha_2' = \theta\alpha_2$, 即图表



交换. 换言之, $(X \amalg_Z Y; \alpha_1, \alpha_2)$ 是范畴$\mathcal{C}_Z^{\mathrm{op}}$ 的乘积. 我们常简称$X \amalg_Z Y$ 为X 与Y 在Z 上的纤维上积.

例1.67. (1) 设$f : X \to Z$ 与$g : Y \to Z$ 是群同态, 则在群范畴$\mathcal{G}$roups 里, $X \times_Z Y = \{(x, y) \in X \times Y \mid f(x) = g(y)\}$.

(2) 设$f : B \to A$ 与$g : C \to A$ 是模同态, 则在模范畴$\mathcal{R}$-mod 里, $B \times_A C = \{(b, c) \in B \oplus C \mid f(b) = g(c)\}$.

(3) 反过来, 设$f : A \to B$ 与$g : A \to C$ 是模同态. 则在$\mathcal{R}$-mod 里, $B \amalg_A C = (B \oplus C)/S$, 这里$S = \{(f(a), -g(a)) \in B \oplus C \mid a \in A\}$.

解. 留作练习. □

§1.2.2 函子

函子就是范畴间的映射.

定义1.68. 设$\mathcal{A}$ 与$\mathcal{B}$ 是范畴.

对应$F : \mathcal{A} \to \mathcal{B}$ 称为**协变函子**或**共变函子**(covariant functor) 是指对于$\mathcal{A}$ 中的任意对象A, $F(A)$ 是$\mathcal{B}$ 中的对象, 对于$\mathcal{A}$ 中的任意态射$A \xrightarrow{f} B$, $F(A) \xrightarrow{F(f)} F(B)$ 是$\mathcal{B}$ 中的态射, 且满足条件$F(1_A) = 1_{F(A)}$ 和$F(gf) = F(g)F(f)$.

对应$F : \mathcal{A} \to \mathcal{B}$ 称为**反变函子**或**逆变函子**(contravariant functor) 是指对于$\mathcal{A}$ 中的任意对象A, $F(A)$ 是$\mathcal{B}$ 中的对象, 对于$\mathcal{A}$ 中的任意态射$A \xrightarrow{f} B$, $F(B) \xrightarrow{F(f)} F(A)$ 是$\mathcal{B}$中的态射, 且满足条件$F(1_A) = 1_{F(A)}$ 和$F(gf) = F(f)F(g)$. 换言之, F 是$\mathcal{A}^{\mathrm{op}}$ 到$\mathcal{B}$ 的协变函子.

例1.69. (1) 恒等函子(identity functor)和常函子(constant functor):

$$\mathrm{Id} : \ \mathcal{C} \to \mathcal{C}, \ A \mapsto A \text{ 且 } f \mapsto f;$$
$$C_A : \ \mathcal{C} \to \mathcal{C}, \ C_A(B) = A, \ C_A(f) = 1_A.$$

它们都是协变函子.

(2) 设$A \in \mathrm{ob}(\mathcal{C})$. 函子$T_A : \mathcal{C} \to \mathcal{S}\mathrm{ets}$,

$$T_A(B) = \mathrm{Hom}(A, B), \quad T_A(f) = (f_* : h \mapsto fh)$$

是协变函子. 函子$T'_A : \mathcal{C} \to \mathcal{S}\mathrm{ets}$,

$$T'_A(B) = \mathrm{Hom}(B, A), \quad T'_A(f) = (f^* : h \mapsto hf)$$

是反变函子.

(3) 特别地, 设M 为R-模, 则函子$(N \mapsto \mathrm{Hom}_R(M, N), \ f \mapsto f_*)$ 是$\mathcal{R}$-mod 上的协变函子, 而函子$(N \mapsto \mathrm{Hom}_R(N, M), \ f \mapsto f^*)$ 是$\mathcal{R}$-mod 上的反变函子.

§1.2.3 阿贝尔范畴

模论中的很多结果都可以推广到一般阿贝尔范畴中. 这里给出阿贝尔范畴的概念和简单性质.

定义1.70. 范畴$\mathcal{C}$ 称为**加性范畴**(additive category)是指$\mathcal{C}$ 满足如下三条件:

(1) 对于$\mathcal{C}$ 中任意对象A 和B, 集合$\mathrm{Hom}(A,B)$ 具备(加法)阿贝尔群结构且复合态射

$$\mathrm{Hom}(B,C)\times\mathrm{Hom}(A,B)\to\mathrm{Hom}(A,C)$$

是$\mathbb{Z}$-双线性映射.

(2) $\mathcal{C}$ 中有零对象.

(3) 对任意对象A 和B, 上乘积$A\amalg B$ 与乘积$A\times B$ 均存在.

对于加性范畴, 复合映射$A\to 0\to B$, 记为0, 称为A 到B 的**零映射**.

命题1.71. *加性范畴中$A\amalg B\cong A\times B$.*

证明. 考虑态射$A\xrightarrow{1_A}A$ 与$B\xrightarrow{0}A$, 则由上乘积的泛性质, 存在态射$p':A\amalg B\to A$ 使得$p'i=1_A$, $p'j=0$. 考虑态射$B\xrightarrow{1_B}B$ 与$A\xrightarrow{0}B$, 则由上乘积的泛性质, 存在态射$q':A\amalg B\to B$ 使得$q'i=0$, $q'j=1_B$. 故$(ip'+jq')i=i$, $(ip'+jq')j=j$. 再由上乘积的泛性质知$ip'+jq'=1_{A\oplus B}$.

类似地, 利用乘积的泛性质, 我们有态射$i':A\to A\times B$ 和$j':B\to A\times B$ 使得$pi'=1_A$, $pj'=0$, $qi'=0$, $qj'=1_B$. 故$i'p+j'q=1_{A\times B}$.

现在令$\Phi=ip+jq:A\times B\to A\amalg B$, $\Psi=i'p'+j'q':A\amalg B\to A\times B$. 容易验证$\Phi$ 和Ψ 互为逆态射. □

注记. 常记上乘积$A\amalg B$ 为$A\oplus B$, 称之为A 与B 的直和, 称乘积为直积.

定义1.72. *设$\mathcal{C}$ 是范畴, $f:A\to B$ 是$\mathcal{C}$中的态射.*

如对任意态射$g_1,g_2:C\to A$ 满足条件$fg_1=fg_2$, 均有$g_1=g_2$ 成立, 则称f 为**单射**(monomorphism).

如对任意态射$h_1,h_2:B\to D$ 满足条件$h_1f=h_2f$, 均有$h_1=h_2$ 成立, 则称f 为**满射**(epimorphism).

如态射既是单射, 又是满射, 则称其为**双射** (bijection).

注记. 双射不一定是同构. 例如在环范畴$\mathcal{R}$ings中, $\mathbb{Z}\hookrightarrow\mathbb{Q}$ 既单又满, 但它不是同构.

反过来, 可以证明, 同构一定是双射.

命题1.73. *设$\mathcal{C}$ 是加性范畴, $f:A\to B$ 是$\mathcal{C}$中的态射.*

(1) *f 是单射当且仅当对于任意$g:C\to A$, $fg=0$ 推出$g=0$.*

(2) *f 是满射当且仅当对于任意$h:B\to D$, $hf=0$ 推出$h=0$.*

证明. 由定义立得. □

命题1.74. *对于加性范畴中的对象集合$\{X_\alpha\}_{\alpha\in I}$, 如它的乘积$\prod\limits_{\alpha\in I}X_\alpha$ 存在, 则*

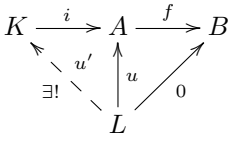
$$\pi_\alpha:\ \prod_{\alpha\in I}X_\alpha\ \to\ X_\alpha$$

是满射. 如它的上乘积 $\coprod\limits_{\alpha\in I} X_\alpha$ 存在, 则$\iota_\alpha:\ X_\alpha \to \coprod\limits_{\alpha\in I} X_\alpha$ 是单射.

证明. 令$\varphi_\alpha = 1_{X_\alpha} : X_\alpha \to X_\alpha$, $\varphi_\beta = 0 : X_\alpha \to X_\beta$ (如$\beta \neq \alpha$), 则它们诱导态射$i_\alpha : X_\alpha \to \prod\limits_{\alpha\in I} X_\alpha$, 使得$\pi_\alpha \circ i_\alpha = \varphi_\alpha = 1_{X_\alpha}$. 由此显见$\pi_\alpha$ 是满射. 同理可证ι_α 是单射. □

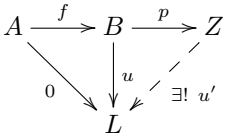
定义1.75. 设$f : A \to B$ 为加性范畴$\mathcal{C}$ 中的态射.

(1) f 的**核**, 记为$\ker f$, 是指对象$K \in \mathrm{ob}(\mathcal{C})$, $i : K \to A$ 为单射, $fi = 0$ 且满足泛性质: 对任意$L \xrightarrow{u} A$, $fu = 0$, 存在唯一的态射$L \xrightarrow{u'} K$, 使得$u = iu'$, 即图表



交换.

(2) f 的**余核**, 记为$\mathrm{coker}\, f$, 是指对象$Z \in \mathrm{ob}(\mathcal{C})$, $p : B \to Z$ 为满射, $pf = 0$ 且满足泛性质: 对任意$u : B \to L$, $uf = 0$, 存在唯一的态射$u' : Z \to L$ 使得$u'p = u$, 即下面图表交换



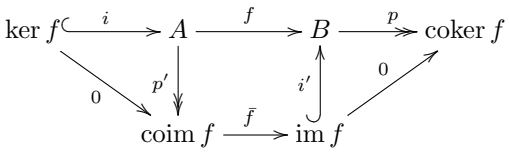
注记. 由定义知, 态射的核和余核如存在, 则(在同构意义下)必唯一. 另外, 核的定义中的条件"i 是单射" 不是必要的, 它由泛性质直接给出. 同样, 余核的定义中的条件"p 是满射" 不是必要的.

现在假设$\mathcal{C}$ 为加性范畴且对任意$f : A \to B$, f 的核与余核均存在. 我们定义

$$\mathrm{coim}\, f = \mathrm{coker}\,(\ker f \xrightarrow{i} A),$$
$$\mathrm{im}\, f = \ker\,(B \xrightarrow{p} \mathrm{coker}\, f).$$

命题1.76. 如$\mathcal{C}$ 是加性范畴且其上态射的核和余核均存在, 则$\mathcal{C}$ 中态射f 诱导态射$\bar{f} : \mathrm{coim}\, f \to \mathrm{im}\, f$.

证明. 我们有交换图表:



由于$fi=0$, 而$\operatorname{coim} f$ 是i 的余核, 故存在唯一态射$\alpha:\operatorname{coim} f\to B$, 使得$\alpha p'=f$. 由$p\cdot\alpha p'=pf=0=0\cdot p'$, 而$p'$ 是满射, 故$p\alpha=0$. 由$\operatorname{im} f=\ker p$ 知存在态射$\bar{f}:\operatorname{coim} f\to\operatorname{im} f$. □

定义1.77. 加性范畴$\mathcal{C}$ 称为**阿贝尔范畴**(abelian category), 如它满足如下两条公理:

$(AB1)$ $\mathcal{C}$上任意态射u的核$\ker u$ 和余核$\operatorname{coker} u$ 均存在.

$(AB2)$ 态射u 的诱导态射$\bar{u}:\operatorname{coim} u\to\operatorname{im} u$ 是同构.

例1.78. R 模范畴$\mathcal{R}$-mod 是阿贝尔范畴.

对于阿贝尔范畴, 如同模范畴的情形, 可以引入正合的概念.

定义1.79. 设$\mathcal{C}$ 为阿贝尔范畴. 序列

$$\cdots\to A\xrightarrow{f}B\xrightarrow{g}C\to\cdots$$

称为在B 处**正合**是指$gf=0$ 且诱导的态射$\operatorname{im} f\to\ker g$ 是同构.

如序列在每一点均正合, 称序列为**正合列**. 特别地, 如序列$0\to A\xrightarrow{f}B\xrightarrow{g}C\to 0$ 在A,B,C 处均正合, 称该序列为**短正合列**.

命题1.80. (1) *序列*$0\to A\xrightarrow{f}B$ *正合当且仅当*f *是单射.*

(2) *序列*$B\xrightarrow{f}C\to 0$ *正合当且仅当*g *是满射.*

(3) *序列*$0\to A\xrightarrow{f}B\xrightarrow{g}C\to 0$ *为短正合列当且仅当*f *是单射,* g *是满射且*$\bar{g}:\operatorname{coker} f\to C$ *是同构.*

证明. 留作练习. □

定义1.81. 设$F:\mathcal{A}\to\mathcal{B}$ 是阿贝尔范畴间的协变函子. 对于$\mathcal{A}$ 中任意短正合列$0\to A\to B\to C\to 0$, 如$0\to F(A)\to F(B)\to F(C)$ 是正合的, 则称F 是**左正合函子**(left exact functor), 如$F(A)\to F(B)\to F(C)\to 0$ 是正合的, 则称F 是**右正合函子**(right exact functor), 如$0\to F(A)\to F(B)\to F(C)\to 0$ 是正合的, 则称F 是**正合函子**(exact functor).

设$F:\mathcal{A}\to\mathcal{B}$ 是阿贝尔范畴间的反变函子. 对于$\mathcal{A}$ 中任意短正合列$0\to A\to B\to C\to 0$, 如$0\to F(C)\to F(B)\to F(A)$ 是正合的, 则称F 是**左正合函子**, 如$F(C)\to F(B)\to F(A)\to 0$ 是正合的, 则称F 是**右正合函子**, 如$0\to F(C)\to F(B)\to F(A)\to 0$ 是正合的, 则称F 是**正合函子**.

例1.82. 设M是R-模. 则由命题1.48和1.49可知, 函子$N\mapsto\operatorname{Hom}_R(N,M)$ 是左正合反变函子, 而$N\mapsto\operatorname{Hom}_R(M,N)$ 是左正合协变函子.

在阿贝尔范畴中, 根据核与余核的定义, 态射$f:A\to B$ 诱导正合列

$$0\to\ker f\to A\xrightarrow{f}B\to\operatorname{coker} f\to 0.$$

给定交换图表

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow{\scriptstyle d_A} & & \downarrow{\scriptstyle d_B} \\ A' & \xrightarrow{f'} & B', \end{array}$$

我们有如下的交换图表:

$$\begin{array}{ccccccc} \ker(d_A) & \xrightarrow{i_A} & A & \xrightarrow{d_A} & A' & \xrightarrow{p_A} & \operatorname{coker}(d_A) \\ \downarrow{\scriptstyle f_*} & \searrow^{f\circ i_A} & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f'} & \searrow^{p_B\circ f'} & \downarrow{\scriptstyle f'_*} \\ \ker(d_B) & \xrightarrow{i_B} & B & \xrightarrow{d_B} & B' & \xrightarrow{p_B} & \operatorname{coker}(d_B), \end{array}$$

这里由于$d_B \circ (f \circ i_A) = f' \circ d_A \circ i_A$, 故由核的泛性质(相对于态射$d_B$), 存在唯一的态射

$$f_* : \ker(d_A) \to \ker(d_B)$$

使得图表交换; 由于$(p_B \circ f') \circ d_A = p_B \circ d_B \circ f = 0$, 故由余核的泛性质(相对于态射$d_A$), 存在唯一的态射

$$f'_* : \operatorname{coker}(d_A) \to \operatorname{coker}(d_B)$$

使得图表交换.

我们同样有蛇形引理:

定理1.83 (蛇形引理)**.** 设$\mathcal{C}$ 为阿贝尔范畴. 则行正合交换图表

$$\begin{array}{ccccccccc} & & X' & \xrightarrow{f} & X & \xrightarrow{g} & X'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle d'} & & \downarrow{\scriptstyle d} & & \downarrow{\scriptstyle d''} & & \\ 0 & \longrightarrow & Y' & \xrightarrow{p} & Y & \xrightarrow{q} & Y'' & & \end{array}$$

诱导正合列

$$\ker(d') \xrightarrow{f_*} \ker(d) \xrightarrow{g_*} \ker(d'') \xrightarrow{\delta} \operatorname{coker}(d') \xrightarrow{p_*} \operatorname{coker}(d) \xrightarrow{q_*} \operatorname{coker}(d'').$$

§1.3 自由模, 投射模和内射模

§1.3.1 自由模

定义1.84. 设M 是非零R-模. 如存在子集$S \subseteq M$ 使得$M = \langle S \rangle$ 且S 中的元素之间是线性无关的, 则称M 为S 生成的**自由模**(free module), S 称为M 的一组**基**(basis).

设$S = \{x_i\}_{i\in I}$ 是自由模M 的一组基. 根据定义, M 中的元素m 均可唯一写为有限和

$$m = r_1 x_1 + \cdots + r_n x_n,\ r_i \in R,\ x_i \in S \text{ 两两不同.}$$

由此, 立刻有如下定理:

定理1.85. *设M 是以$\{x_i\}_{i\in I}$ 为基的自由模, N 是任意R-模且$\{y_i\}_{i\in I}$ 是N 中的任意一组元素, 则存在唯一的同态$f: M\to N$ 使得$f(x_i)=y_i$.*

特别地, 如N 是自由模, $\{y_i\}_{i\in I}$ 是N 的一组基, 则f 是同构.

证明. 如$m=r_1x_1+\cdots+r_nx_n$, 若$f(x_i)=y_i$, 必有$f(m)=\sum\limits_{i=1}^{n}r_iy_i$, 即$f$ 是唯一确定的. 另一方面这样定义的f 的确是模同态.

如N 是以$\{y_i\}_{i\in I}$为基的自由模, 则f的逆即$g:\ N\to M,\ g(y_i)=x_i$. □

推论1.86. *如M 是由$S=\{x_i\}_{i\in I}$ 为基的自由模, 则$M\cong\bigoplus\limits_{i\in I}R$.*

证明. 对于$j\in I$, 令$e_j\in\bigoplus\limits_{i\in I}R$, 它的第$j$ 个分量是1而其它分量等于0. 则$\{e_i\}_{i\in I}$是自由模$\bigoplus\limits_{i\in I}R$ 的一组基. 由上述定理, 存在唯一的同态$f: M\to\bigoplus\limits_{i\in I}R,\ f(x_i)=e_i$, 也存在唯一的同态$g:\bigoplus\limits_{i\in I}R\to M,\ g(e_i)=x_i$. f 与g 显然互为逆映射. □

定义1.87. 自由模M 的**秩**, 记为$\mathrm{rank}\,(M)$, 是指它的一组基的元素个数.

定理1.88. *自由模M 的秩 独立于基的选取.*

证明. 设$\{x_i\}_{i\in I}$ 与$\{y_j\}_{j\in J}$ 是M 的两组基. 只要证明如$|I|\neq|J|$, 则$M=\bigoplus\limits_{i\in I}R$ 与$N=\bigoplus\limits_{j\in J}R$ 不同构即可. 如不然设$f: M\to N$ 为同构. 令$f(e_i)=e_i'$, 则$\{e_i'\}_{i\in I}$ 是N 的一组基. 令$\mathfrak{m}$ 是R 的一个极大理想, 则$f(\mathfrak{m}M)\subseteq\mathfrak{m}N$. 反过来, 对于$n\in N$, 记$n=\sum\limits_{i=1}^{s}r_ie_i'$. 则对任意$r\in\mathfrak{m}$, $f(r\sum\limits_{i=1}^{k}r_ie_i)=rn$. 故$f(\mathfrak{m}M)=\mathfrak{m}N$. 由此即知$f$ 诱导同构$M/\mathfrak{m}M\xrightarrow{\sim}N/\mathfrak{m}N$. 但我们有$M/\mathfrak{m}M\cong\bigoplus\limits_{i\in I}k$, 其中$k=R/\mathfrak{m}$. 所以$\bigoplus\limits_{i\in I}k\cong\bigoplus\limits_{j\in J}k$. 将两边均视为$k$- 线性空间, 当$|I|\neq|J|$时, 这是不可能的. □

推论1.89. *如M 与N 均是自由模且秩相等, 则M 与N 同构.*

现在设M 是有限秩自由模. 设$|I|=n$ 有限, $\{x_i\}_{i\in I}$ 与$\{y_i\}_{i\in I}$ 是M的两组基. 则

$$x_i=\sum_{j\in I}\alpha_{ij}y_j,\quad y_i=\sum_{j\in I}\beta_{ij}x_j\quad(\alpha_{ij},\ \beta_{ij}\in R)$$

而且表达式唯一. 令$A=(\alpha_{ij})_{i,j\in I}$, $B=(\beta_{ij})_{i,j\in I}$, 则$AB=BA=I_n$. 我们有:

命题1.90. *设M 是秩为n 的自由模, $\{x_i\}_{i=1}^n,\{y_i\}_{i=1}^n$ 是它的两组基. 令两组基间的变换矩阵为A, 即*

$$(y_1,\cdots,y_n)=(x_1,\cdots,x_n)A.$$

则$A\in\mathrm{GL}_n(R)$. 反过来, 如$\{x_i\}_{i=1}^n$ 为M 的一组基, $(y_1,\cdots,y_n)=(x_1,\cdots,x_n)A$, $A\in\mathrm{GL}_n(R)$, 则$\{y_i\}_{i=1}^n$ 也是M 的一组基.

命题1.91. 设Q 是环R 的理想, $M=\bigoplus\limits_{i\in I}Rx_i$ 是自由R-模. 则Qx_i 是Rx_i 的子模且

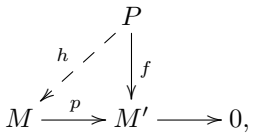
$$M/QM\cong\bigoplus_{i\in I}Rx_i/Qx_i\cong\bigoplus_{i\in I}R/Q$$

是环R/Q 上的自由模, 它的一组基是$\{\bar{x}_i=x_i+QM\}_{i\in I}$.

证明. 显然. 留作练习. □

§1.3.2 投射模

定义1.92. 模P 称为**投射模**(projective module)是指对任意行正合图表



存在同态$h:P\to M$ 使得f 沿h 分解, 即$f=ph$.

定理1.93. 下列条件等价:

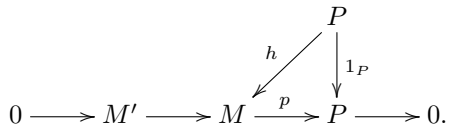
(1) P 是投射模.

(2) 任意正合列$0\to M'\to M\to P\to 0$ 均分裂.

(3) 存在模M 使得$P\oplus M$ 为自由模. 即P 是自由模的直和项.

(4) 函子: $M\mapsto \mathrm{Hom}_R(P,M)$ 是正合函子.

证明. (1) ⇒ (2) 我们考虑



则由于P 是投射模, 存在$h:P\to M$, $1_P=ph$. 故正合列$0\to M'\to M\to P\to 0$ 分裂.

(2) ⇒ (3) 令F 是P 生成的自由模, 则存在满射$f:F\to P$. 令$M=\ker(f)$, 我们有正合列$0\to M\to F\to P\to 0$. 由(2)知$F=P\oplus M$.

(3) ⇒ (4) 令N 为R-模使得$P\oplus N=F=\bigoplus\limits_{i\in I}R$ 为自由模. 由于对任意模M, 由命题1.36知$\mathrm{Hom}_R(F,M)\cong\prod\limits_{i\in I}M$, 故函子: $M\mapsto\mathrm{Hom}_R(F,M)$ 正合. 对于正合列$0\to M'\to M\to M''\to 0$, 我们有行正合交换图表

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{Hom}_R(F,M') & \longrightarrow & \mathrm{Hom}_R(F,M) & \longrightarrow & \mathrm{Hom}_R(F,M'') \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & \mathrm{Hom}_R(P,M') & \longrightarrow & \mathrm{Hom}_R(P,M) & \xrightarrow{g} & \mathrm{Hom}_R(P,M'') \dashrightarrow 0.
\end{array}$$

通过图表追踪知g 是满射, 即函子$M \mapsto \mathrm{Hom}_R(P, M)$ 正合.

(4) $\Rightarrow$ (1) 对于正合列

$$0 \longrightarrow M' = \ker(p) \longrightarrow M \xrightarrow{p} M'' \longrightarrow 0,$$

由函子: $M \mapsto \mathrm{Hom}_R(P, M)$ 的正合性知$p^* : \mathrm{Hom}_R(P, M) \to \mathrm{Hom}_R(P, M'')$ 是满射, 这等价于对任意同态$f : P \to M''$, 存在同态$h : P \to M$ 使得$f = ph$. □

命题1.94. 设A 是R-模. 则A 是投射模当且仅当存在集合$\{a_i\}_{i\in I} \subseteq A$ 以及R-模同态$\{\varphi_i : A \to R\}_{i\in I}$ 使得

(1) 对于任意$x \in A$, $\varphi_i(x)$ 几乎处处为0.

(2) 对任意$x \in A$, $x = \sum\limits_{i\in I} \varphi_i(x)a_i$.

更进一步地, 此时A 由$\{a_i\}_{i\in I}$ 生成.

证明. 如A 是投射模, 令$\psi : F \twoheadrightarrow A$, 其中$F = \bigoplus\limits_{i\in I} Re_i$ 为自由模. 故存在$\varphi : A \to F$ 使得$\psi\varphi = 1_A$. 我们令$a_i = \psi(e_i)$. 设$\varphi(x) = \sum\limits_{i\in I} r_i e_i$. 令$\varphi_i : A \to R$, $x \mapsto r_i$. 则

$$x = \psi\varphi(x) = \sum_{i\in I} r_i\psi(e_i) = \sum_{i\in I} \varphi_i(x)a_i.$$

反过来, 令$F = \bigoplus\limits_{i\in I} Re_i$, 令$\psi : F \to A$, $e_i \mapsto a_i$. 定义$\varphi : A \to F$, $x \mapsto \sum\limits_{i\in I} \varphi_i(x)e_i$, 则$\psi\varphi(x) = x$, 即$\psi\varphi = 1_A$. 故$A$ 是投射模. □

命题1.95. 给定正合列

$$0 \longrightarrow K \xrightarrow{i} P \xrightarrow{\pi} M \longrightarrow 0,$$

$$0 \longrightarrow K' \xrightarrow{i'} P' \xrightarrow{\pi'} M \longrightarrow 0,$$

其中P 与P' 为投射模, 则$K \oplus P' \cong K' \oplus P$.

证明. 考虑交换图表

$$\begin{array}{ccccccccc}
0 & \longrightarrow & K & \xrightarrow{i} & P & \xrightarrow{\pi} & M & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \| & & \\
0 & \longrightarrow & K' & \xrightarrow{i'} & P' & \xrightarrow{\pi'} & M & \longrightarrow & 0
\end{array}$$

由P 是投射模, 故存在$\beta : P \to P'$ 使得$\pi = \pi'\beta$. 再由$\pi'\beta i = \pi i = 0$. 故存在$\alpha : K \to K'$ 使得$i'\alpha = \beta i$. 我们考虑序列

$$0 \longrightarrow K \xrightarrow{\theta} P \oplus K' \xrightarrow{\psi} P' \longrightarrow 0, \qquad (*)$$

其中同态$\theta : x \mapsto (i(x), \alpha(x))$, $\psi : (u, y) \mapsto \beta(u) - i'(y)$. 则显然$\theta$ 是单同态. 对于$u' \in P'$, 取$u \in P$ 使得$\pi(u) = \pi'(u')$, 则$\pi'(u' - \beta(u)) = 0$. 故存在$y \in K'$

使得$u'-\beta(u)=-i'(y)$. 所以$u'=\psi((u,y))$, 即ψ 是满同态. 设$(u,y)\in\ker\psi$, 则$\beta(u)=i'(y)$, 所以$\pi(u)=\pi'\beta(u)=0$. 故存在$x\in K$, $u=i(x)$. 因此$\beta(u)=i'\alpha(x)=i'(y)$. 由$i'$ 为单射, 故$\alpha(x)=y$, $(u,x)\in\operatorname{im}\theta$. 另一方面, 显然有$\psi\theta=0$, 故$(*)$ 是正合列. 再由P' 是投射模即得$K\oplus P'\cong K'\oplus P$. □

§1.3.3 内射模

定义1.96. 模E 称为**内射模**(injective module)是指对任意行正合图表

$$\begin{array}{ccccc} & & E & & \\ & & \uparrow{\scriptstyle f} & \nwarrow{\scriptstyle g} & \\ 0 & \longrightarrow & A & \xrightarrow{i} & B, \end{array}$$

存在同态$g:B\to E$ 使得$gi=f$.

定理1.97. *下列条件等价:*

(1) *E 是内射模.*

(2) *任意正合列$0\to E\to B\to C\to 0$ 均分裂.*

(3) *函子: $M\mapsto \operatorname{Hom}_R(M,E)$ 是正合函子.*

证明. (1) ⇒ (2) 只需考虑

$$\begin{array}{ccccccccc} & & E & & & & & & \\ & & \uparrow{\scriptstyle 1_E} & & & & & & \\ 0 & \longrightarrow & E & \xrightarrow{i} & B & \longrightarrow & C & \longrightarrow & 0 \end{array}$$

即可.

(2) ⇒ (1) 考虑图表

$$\begin{array}{ccccc} & & E & \xrightarrow{\alpha} & D \\ & & \uparrow{\scriptstyle f} & & \uparrow{\scriptstyle \beta} \\ 0 & \longrightarrow & A & \xrightarrow{i} & B \end{array}$$

令D 是i 与f 的推出, 即$D=(E\oplus B)/S$, 其中

$$S=\{(f(a),-i(a))\mid a\in A\}.$$

由i 是单同态, 则α 也是单同态. 故由(2), E 是D 的直和项. 令$q:D\to E$, $q\alpha=1_E$, 则$g=q\beta$, 满足$gi=f$.

(1) ⇔ (3) 是例行公事, 证明略. □

推论1.98. *如E 是内射模且是模M 的子模, 则E 是M 的直和项.*

命题1.99. *设$\{E_i\}_{i\in I}$ 是内射模, 则$\prod\limits_{i\in I}E_i$ 也是内射模.*

证明. 这是因为$\mathrm{Hom}_R(M, \prod_{i\in I} E_i) \cong \prod_{i\in I} \mathrm{Hom}_R(M, E_i)$. □

推论1.100. 内射模的有限直和均是内射模.

定理1.101 (白尔(Baer) 判别法)**.** 模E 是内射模当且仅当对R 的任意理想I, 同态$f : I \to E$ 均可延拓到同态$g : R \to E$, 即$g|_I = f$.

证明. $\Rightarrow$ 由定义立得.

$\Leftarrow$ 对于正合列$0 \to A \to B$, 我们视A 为B 的子模. 对于同态$f : A \to E$, 令

$$X = \{(A', g') : A \subseteq A' \subseteq B, g' : A' \to E是f \text{ 的延拓, 即} g'|_A = f\}.$$

在集合X 中我们定义偏序:

$$(A', g') \leq (A'', g'')当且仅当A' \subseteq A'' \text{ 且} g''|_{A'} = g'.$$

由于$(A, f) \in X$, 故X 非空. 由佐恩引理(Zorn Lemma) 知X 中有极大元, 记之为(A_0, g_0). 如$A_0 \neq B$, 取$b \in B$, $b \notin A_0$, 定义

$$I = \{r \in R \mid rb \in A_0\}.$$

则I 是R 中的真理想. 定义$h : I \to E$, $r \mapsto g_0(rb)$. 则由已知条件, 存在模同态$h^* : R \to E$ 使得h^* 是h 的延拓. 令$A_1 = A_0 + \langle b\rangle \supsetneqq A$,

$$g_1 : A_1 \to E,\ a_0 + rb \mapsto g_0(a_0) + rh^*(1),$$

其中$a_0 \in A_0$, $r \in R$. 如$a_0 + rb = a_0' + r'b$, 则$(r - r')b = a_0' - a_0 \in A_0$. 故$g_0(a_0' - a_0) = g_0((r - r')b) = h(r - r') = (r - r')h^*(1)$, 所以$g_1$ 是定义良好的模同态. 容易看出$g_1|_{A_0} = g_0$, 这与(A_0, g_0) 的极大性矛盾. □

例1.102. 如R 为整环, 则它的商域$K = \mathrm{Frac}R$ 是内射R-模. 这是因为对于

$$\begin{array}{ccccc} & & K & & \\ & & \uparrow{\scriptstyle f} & & \\ 0 & \longrightarrow & I & \longrightarrow & R \end{array}$$

总有$f(ab) = af(b) = bf(a)$, 故$\frac{f(a)}{a} = \frac{f(b)}{b} = c \in K$ 对于所有$0 \neq a, b \in I$ 均成立. 我们定义

$$g : R \to K, \quad r \mapsto rc.$$

则$g|_I = f$.

定义1.103. 设R 是整环. 模D 称为**可除模**(divisible module)是指对任意$d \in D$ 和非零$r \in R$, 存在$d' \in D$, 使得$d = rd'$.

例1.104. (1) 整环R 的商域Frac$R$ 是可除R-模.

(2) 如D_1 和D_2 是可除模, 则$D_1 \oplus D_2$ 也是可除模, 如$\{D_i\}_{i\in I}$ 是可除模, 则$\bigoplus_{i\in I} D_i$ 也是可除模. 特别地, Frac$R$ 上的线性空间都是可除R-模.

(3) 可除模的商模是可除模.

引理1.105. *如R 是整环, E 是内射模, 则E 也是可除模.*

证明. 设$e \in E$, $0 \neq r_0 \in R$. 定义同态$f : I = (r_0) \to E$, $rr_0 \mapsto re$. 由于E 是内射模, 存在同态$h : R \to E$ 是f 的延拓, 故$e = f(r_0) = h(r_0) = r_0 h(1)$. □

推论1.106. *如R 是*PID*, 则内射模和可除模两个概念重合.*

证明. 只要证此时可除模也是内射模即可.

设$f : I \to E$ 为同态. 由R 为PID, $I = (r_0)$. 由E 是可除模, 故存在$e \in E$, $r_0 e = f(r_0)$. 我们定义

$$h : R \to E,\ r \mapsto re.$$

则h 是f 的延拓. □

§1.4 张量积与平坦模

§1.4.1 张量积

定义1.107. 设R 是交换环, $M_1, \cdots, M_n, N$ 是R-模. 模映射$f : M_1 \times \cdots \times M_n \to N$ 称为**多重线性映射**, 是指f 满足条件

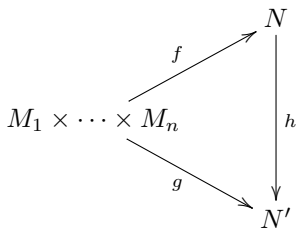
(1) $f(\cdots, x_i + x_i', \cdots) = f(\cdots, x_i, \cdots) + f(\cdots, x_i', \cdots)$ 对任意$x_i, x_i' \in M_i$ 成立.

(2) $f(\cdots, rx_i, \cdots) = rf(\cdots, x_i, \cdots)$ 对任意$r \in R$ 成立.

给定环R和模$M_1, \cdots, M_n$, 我们如下定义范畴$\mathcal{C}$:

(i) $\mathcal{C}$ 的对象是多重线性映射$f : M_1 \times \cdots \times M_n \to N$.

(ii) 两对象间的态射是指R-模同态$h : N \to N'$ 使得图表



交换, 即$g = hf$.

定义1.108. 模$M_1,\cdots,M_n$ 在R 上的**张量积**(tensor product) 是范畴$\mathcal{C}$ 的始对象, 即多重线性映射

$$\varphi : M_1 \times \cdots \times M_n \to U$$

使得对任意多重线性映射$f : M_1\times\cdots\times M_n \to N$, 存在唯一$R$-模同态$h : U \to N$ 使得$f = h\varphi$.

通常记$U = M_1 \otimes_R \cdots \otimes_R M_n$, 并称之为$M_1,\cdots,M_n$ 在R 上的张量积, 记$\varphi(x_1,\cdots,x_n) = x_1\otimes\cdots\otimes x_n$, 称之为$x_1,\cdots,x_n$ 的张量积.

由多重线性映射的定义即知

$$x_1\otimes\cdots\otimes(x_i+x_i')\otimes\cdots\otimes x_n = x_1\otimes\cdots\otimes x_i\otimes\cdots\otimes x_n + x_1\otimes\cdots\otimes x_i'\otimes\cdots\otimes x_n,$$

$$r(x_1\otimes x_2\otimes\cdots\otimes x_n) = (rx_1)\otimes x_2\otimes\cdots\otimes x_n = x_1\otimes(rx_2)\otimes\cdots\otimes x_n = \cdots$$

我们的第一个问题是: 范畴$\mathcal{C}$ 中始对象U 是否一定存在?

令E 是集合$M_1\times\cdots\times M_n = \{(x_1,\cdots,x_n) : x_i \in M_i\}$ 生成的自由R-模, F 是由形如$(x_1,\cdots,x_i+x_i',\cdots,x_n) - (x_1,\cdots,x_i,\cdots,x_n) - (x_1,\cdots,x_i',\cdots,x_n)$ 及$(x_1,\cdots,rx_i',\cdots,x_n) - r(x_1,\cdots,x_n)$ 的元素生成的E的子模. 令

$$\varphi :\ M_1\times\cdots\times M_n \to E \to E/F, \quad (x_1,\cdots,x_n)\mapsto \overline{(x_1,\cdots,x_n)}.$$

则容易验证φ 是多重线性映射. 对于任意多重线性映射

$$f : M_1\times\cdots\times M_n \to N$$

自然定义模映射$f' : E \to N$, $(x_1,\cdots,x_n)\mapsto f(x_1,\cdots,x_n)$. 则容易验证$F \subseteq \ker(f')$. 故$f'$ 诱导模映射

$$h : E/F \to N,$$

使得$f = h\varphi$. 我们有:

命题1.109. *如上定义的商模E/F 及模同态$\varphi : M_1\times\cdots\times M_n \to E/F$ 是$M_1,\cdots,M_n$ 的张量积.*

我们下面讨论张量积的性质. 首先对于$M_1\otimes M_2$, 可以看出它的元素都是有限和

$$\sum_{i=1}^{n} x_i\otimes y_i,\ \text{其中}\ x_i\in M_1,\ y_i\in M_2.$$

它们满足关系

$$(x+x')\otimes y = x\otimes y + x'\otimes y,\ x\otimes(y+y') = x\otimes y + x\otimes y',$$

$$(rx)\otimes y = x\otimes(ry) = r(x\otimes y).$$

例1.110. 令$R=\mathbb{Z}, M=\mathbb{Z}/m\mathbb{Z}, N=\mathbb{Z}/n\mathbb{Z}$. 如$m$ 与n 互素, 则存在整数k_1和k_2 使得$k_1m+k_2n=1$. 由于$(mx)\otimes y=0$ 且$(nx)\otimes y=x\otimes(ny)=0$, 故$(k_1m+k_2n)x\otimes y=0$, 即$x\otimes y=0$. 所以当$m$ 和n 互素时, $\mathbb{Z}/m\mathbb{Z}\otimes_{\mathbb{Z}}\mathbb{Z}/n\mathbb{Z}=0$.

例1.111. 数乘映射$R\times M\to M$ 是双线性映射, 诱导模同构$R\otimes_R M\xrightarrow{\sim} M$, $r\otimes m\mapsto rm$, 逆映射是$m\mapsto 1\otimes m$.

命题1.112. *存在唯一同构*

$$(M_1\otimes M_2)\otimes M_3\xrightarrow{\sim} M_1\otimes(M_2\otimes M_3)\xrightarrow{\sim} M_1\otimes M_2\otimes M_3,$$

使得

$$(x\otimes y)\otimes z\mapsto x\otimes(y\otimes z)\mapsto x\otimes y\otimes z.$$

证明. 由于$M_1\otimes M_2\otimes M_3$ 由$x\otimes y\otimes z$ 生成, 唯一性显然成立. 下证存在性.

对于$x\in M_1$, 考虑

$$\lambda_x:\ M_2\times M_3\longrightarrow(M_1\otimes M_2)\otimes M_3,\quad (y,z)\longmapsto(x\otimes y)\otimes z.$$

则容易验证λ_x 是双线性映射, 故它诱导同态

$$\bar{\lambda}_x:\ M_2\otimes M_3\longrightarrow(M_1\otimes M_2)\otimes M_3,\quad y\otimes z\longmapsto(x\otimes y)\otimes z.$$

再考虑映射

$$M_1\times(M_2\otimes M_3)\longrightarrow(M_1\otimes M_2)\otimes M_3,\quad (x,\alpha)\longmapsto\bar{\lambda}_x(\alpha).$$

故$(x,y\otimes z)\mapsto(x\otimes y)\otimes z$. 容易验证此映射还是双线性映射, 故它诱导同态

$$M_1\otimes(M_2\otimes M_3)\longrightarrow(M_1\otimes M_2)\otimes M_3,\quad x\otimes(y\otimes z)\longmapsto(x\otimes y)\otimes z.$$

由对称性, 有同态映射

$$(M_1\otimes M_2)\otimes M_3\longrightarrow M_1\otimes(M_2\otimes M_3),\quad (x\otimes y)\otimes z\longmapsto x\otimes(y\otimes z).$$

上述两映射显然互为逆映射, 即为同构.

同样, 双线性映射

$$M_1\times(M_2\otimes M_3)\longrightarrow M_1\otimes M_2\otimes M_3,\quad (x,y\otimes z)\longmapsto x\otimes y\otimes z$$

诱导同态$M_1\otimes(M_2\otimes M_3)\to M_1\otimes M_2\otimes M_3$, 而三线性映射

$$M_1\times M_2\times M_3\longrightarrow M_1\otimes(M_2\otimes M_3),\quad (x,y,z)\longmapsto x\otimes(y\otimes z)$$

诱导同态映射

$$M_1\otimes M_2\otimes M_3\longrightarrow M_1\otimes(M_2\otimes M_3),\quad x\otimes y\otimes z\longmapsto x\otimes(y\otimes z),$$

它们互为逆映射. □

命题1.113. *存在唯一的同构映射$M \otimes N \xrightarrow{\sim} N \otimes M$, $x \otimes y \mapsto y \otimes x$.*

证明. 映射$M \times N \to N \otimes M$, $(x, y) \mapsto y \otimes x$ 是双线性映射, 故诱导映射$M \otimes N \to N \otimes M$, $x \otimes y \mapsto y \otimes x$. 由对称性知它显然是同构映射. 而唯一性也是显然的. □

设$f_i : M_i' \to M_i$ $(1 \leq i \leq n)$ 是模同态. 则

$$\begin{aligned} f = \prod_{i=1}^{n} f_i : \ & M_1' \times \cdots \times M_n' \longrightarrow M_1 \times \cdots \times M_n, \\ & (x_1, \cdots, x_n) \longmapsto (f_1(x_1), \cdots, f_n(x_n)) \end{aligned}$$

也是模同态. 故有模同态映射

$$\begin{aligned} & M_1' \times \cdots \times M_n' \longrightarrow M_1 \otimes \cdots \otimes M_n, \\ & (x_1, \cdots, x_n) \longmapsto f_1(x_1) \otimes \cdots \otimes f_n(x_n). \end{aligned}$$

容易验证它是n 重线性映射, 因此诱导同态

$$\begin{aligned} \bigotimes_{i=1}^{n} f_i : \ & M_1' \otimes \cdots \otimes M_n' \longrightarrow M_1 \otimes \cdots \otimes M_n, \\ & (x_1 \otimes \cdots \otimes x_n) \longmapsto f_1(x_1) \otimes \cdots \otimes f_n(x_n). \end{aligned}$$

即有交换图表

$$\begin{array}{ccc} M_1' \times \cdots \times M_n' & \xrightarrow{\varphi'} & M_1' \otimes \cdots \otimes M_n' \\ {\scriptstyle \prod f_i}\downarrow & & \downarrow{\scriptstyle \otimes f_i} \\ M_1 \times \cdots \times M_n & \xrightarrow{\varphi} & M_1 \otimes \cdots \otimes M_n. \end{array}$$

下面命题是显然的:

命题1.114. *设$f, f_1, f_2 : M' \to M$ 与$g, g_1, g_2 : N' \to N$ 为同态映射, $r \in R$. 则*

$$\begin{aligned} & f \otimes (g_1 + g_2) = f \otimes g_1 + f \otimes g_2, \\ & (f_1 + f_2) \otimes g = f_1 \otimes g + f_2 \otimes g, \\ & f \otimes (rg) = rf \otimes g = r(f \otimes g). \end{aligned}$$

命题1.115. *直和与张量积可以交换次序, 即对于R-模$(M_i)_{i \in I}$ 和N, 有*

$$(\bigoplus_{i \in I} M_i) \otimes N \cong \bigoplus_{i \in I} (M_i \otimes N).$$

证明. 首先考虑指标集I 有限情形. 不妨设$I = \{1, \cdots, n\}$. 此时

$$(\bigoplus_{i=1}^{n} M_i) \times N \longrightarrow \bigoplus_{i=1}^{n} (M_i \otimes N), \quad ((x_i), y) \longmapsto (x_i \otimes y)$$

是双线性映射, 它诱导同态映射

$$(\bigoplus_{i=1}^{n} M_i) \otimes N \longrightarrow \bigoplus_{i=1}^{n} (M_i \otimes N), \quad (x_i) \otimes y \longmapsto (x_i \otimes y).$$

反过来, 对于$i = 1, \cdots, n$, 双线性映射

$$M_i \times N \longrightarrow (\bigoplus_{i=1}^{n} M_i) \otimes N, \quad (x_i, y) \longmapsto (0, \cdots, x_i, \cdots, 0) \otimes y$$

诱导映射

$$M_i \otimes N \longrightarrow (\bigoplus_{i=1}^{n} M_i) \otimes N, \quad x_i \otimes y \longmapsto (0, \cdots, x_i, \cdots, 0) \otimes y.$$

再由直和的泛性质, 得到映射

$$\bigoplus_{i=1}^{n} (M_i \otimes N) \to (\bigoplus_{i=1}^{n} M_i) \otimes N, \quad (x_i \otimes y_i) \mapsto \sum_{i} (0, \cdots, x_i, \cdots, 0) \otimes y_i.$$

它与前面的映射互为逆映射.

对于一般情形. 一方面同样有映射

$$\varphi : \bigoplus_{i \in I} (M_i \otimes N) \to (\bigoplus_{i \in I} M_i) \otimes N, \quad (x_i \otimes y_i) \mapsto \sum_{i \in I} (0, \cdots, x_i, \cdots, 0) \otimes y_i.$$

对于任意有限子集$I_0 \subseteq I$, 我们有交换图表

$$\begin{array}{ccc} \bigoplus\limits_{i \in I} (M_i \otimes N) & \xrightarrow{\varphi} & (\bigoplus\limits_{i \in I} M_i) \otimes N \\ \uparrow \text{单} & & \uparrow \\ \bigoplus\limits_{i \in I_0} (M_i \otimes N) & \xrightarrow[\varphi|_{I_0}]{\sim} & (\bigoplus\limits_{i \in I_0} M_i) \otimes N. \end{array}$$

对于$x = \sum\limits_{i \in I} (m_i \otimes n_i) \in \ker \varphi$, 令$I_0 = \{i \in I \mid m_i \otimes n_i \neq 0\}$. 若$I_0 = \emptyset$, 则$x = 0$. 否则$I_0$ 有限, 故$x \in \ker \varphi|_{I_0} = \{0\}$, 所以$\varphi$ 是单同态. 另一方面, 对于$y = \sum\limits_{j=1}^{n} (m_{j,i}) \otimes n_j$, 令$I_0 = \{i \in I \mid m_{j,i} \neq 0\}$. 若$I_0 = \emptyset$, 则$y = 0$, $\varphi(0) = y$. 否则I_0 为有限集, $y \in (\bigoplus\limits_{i \in I_0} M_i) \otimes N$. 故存在$x \in \bigoplus\limits_{i \in I_0} (M_i \otimes N) \subseteq \bigoplus\limits_{i \in I} (M_i \otimes N)$ 使得$\varphi(x) = y$. 故φ 为满同态. 综合起来即知φ 是同构. □

推论1.116. *若N 是自由模, $\{v_i\}_{i \in I}$ 是N 的一组基, 则$M \otimes N \cong \bigoplus\limits_{i \in I} M$.*

证明. 若$N = Rv_i$, 则$M \otimes N \to M$, $x \otimes (rv_i) \mapsto rx$ 是同构映射. 一般地,

$$M \otimes N \cong M \otimes (\bigoplus_{i \in I} Rv_i) \cong \bigoplus_{i \in I} (M \otimes Rv_i) \cong \bigoplus_{i \in I} M. \qquad \square$$

推论1.117. 如M,N 均为自由模, 则$M\otimes N$ 也是自由模, 其秩为$\operatorname{rank}(M)\times\operatorname{rank}(N)$. 特别地, 对于$k$-线性空间$V_1$ 和V_2, 它们的张量积$V_1\otimes V_2$ 是$\dim V_1\times\dim V_2$ 维线性空间.

命题1.118. 设$0\to M'\xrightarrow{i}M\xrightarrow{p}M''\to 0$ 是正合列, N 是任意模. 则$N\otimes M'\xrightarrow{i_*}N\otimes M\xrightarrow{p_*}N\otimes M''\to 0$ 也是正合列, 其中$i_*=1_N\otimes i$, $p_*=1_N\otimes p$. 换言之, 函子$M\mapsto N\otimes M$ 是$\mathcal{R}$-mod 上的右正合协变函子.

证明. 先证p_* 是满同态. 对任意$m''\in M'',n\in N$, 令$m\in M$, $p(m)=m''$. 则$p_*(n\otimes m)=n\otimes m''$, 故$p_*$ 是满的.

对于任意$m'\in M'$,

$$p_*\circ i_*(n\otimes m')=p_*(n\otimes i(m'))=n\otimes p(i(m'))=0.$$

故$p_*\circ i_*=0$, 所以$\ker(p_*)\supseteq\operatorname{im}(i_*)$.

要证$\ker(p_*)=\operatorname{im}(i_*)$, 令$I=\operatorname{im}(i_*)$, 只要证$\bar{p}_*:(N\otimes M)/I\to N\otimes M''$ 为同构, 这等价于寻找$\bar{p}_*$ 的逆映射$g:N\otimes M''\to(N\otimes M)/I$. 考虑映射

$$N\times M''\to(N\otimes M)/I,\quad(n,m'')\mapsto(n\otimes m)+I,$$

其中$p(m)=m''$. 如$p(\tilde{m})=p(m)=m''$, 则$p(\tilde{m}-m)=0$. 故存在$m'\in M'$ 使得$i(m')=\tilde{m}-m$. 所以$n\otimes\tilde{m}-n\otimes m=n\otimes i(m')\in I$, 故上述映射是良定义的. 容易看出它是双线性映射, 故诱导映射

$$g:N\otimes M''\to(N\otimes M)/I,\ n\otimes m''\mapsto(n\otimes m)+I.$$

它是$\bar{p}_*$ 的逆映射. □

命题1.119. $M/IM\cong R/I\otimes_R M$.

证明. 考虑

$$R/I\times M\to M/IM,\ (\bar{a},x)\mapsto ax+IM,$$

它是双线性映射, 诱导同态

$$R/I\otimes_R M\to M/IM,\ \bar{a}\otimes x\mapsto ax+IM.$$

另一方面,

$$M\to R/I\otimes_R M,\ x\mapsto\bar{1}\otimes x$$

为模同态, 其核显然包含IM. 故我们有同态

$$M/IM\to R/I\otimes_R M,\ x+IM\mapsto\bar{1}\otimes x.$$

这两个同态互为逆映射, 故得同构. □

§1.4.2 平坦模

定义1.120. 设F 是R-模. 称F 为**平坦模**(flat module)是指任何正合列$M' \xrightarrow{i} M \xrightarrow{j} M''$ 均诱导正合列$F \otimes M' \xrightarrow{i_*} F \otimes M \xrightarrow{j_*} F \otimes M''$.

命题1.121. 下列命题等价

(1) F 是平坦模.

(2) 函子$(M \mapsto F \otimes M)$ 是正合函子.

(3) 对任意单同态$i : M' \to M$, 则$i_* : F \otimes M' \to F \otimes M$ 也是单同态.

证明. (2) 即是说正合列$0 \to M' \xrightarrow{i} M \xrightarrow{j} M'' \to 0$ 诱导正合列$0 \to F \otimes M' \xrightarrow{i_*} F \otimes M \xrightarrow{j_*} F \otimes M'' \to 0$. (1) $\Rightarrow$ (2) $\Leftrightarrow$ (3)是显然的, 我们证(3) $\Rightarrow$ (1).

由正合列$M' \xrightarrow{i} M \xrightarrow{j} M''$, 我们有短正合列$0 \to \operatorname{im} i \to M \to \operatorname{im} j \to 0$. 故有正合列$0 \to F \otimes \operatorname{im} i \to F \otimes M \to F \otimes \operatorname{im} j \to 0$. 注意到$\mathrm{id} \otimes j : F \otimes M \to F \otimes \operatorname{im} j \to F \otimes M''$. 由$\operatorname{im} j \hookrightarrow M$ 为单, 知$F \otimes \operatorname{im} j \to F \otimes M''$ 是单同态. 故

$$\ker(\mathrm{id} \otimes j) = \ker(F \otimes M \to F \otimes \operatorname{im} j) = F \otimes \operatorname{im} i = \operatorname{im}(\mathrm{id} \otimes i). \qquad \square$$

命题1.122. (1) R 是平坦R-模.

(2) 设$F = \bigoplus_{i \in I} F_i$ 是直和, 则F 是平坦模当且仅当对每个$i \in I$, F_i 也是平坦模. 故自由模是平坦模, 平坦模的直和项也是平坦模.

(3) 投射模是平坦模.

证明. (1) 这由$M \otimes_R R \cong M$ 立得.

(2) 由于$(\bigoplus_{i \in I} F_i) \otimes M \cong \bigoplus_{i \in I} (F_i \otimes M)$, 映射$(\bigoplus_{i \in I} F_i) \otimes M' \to (\bigoplus_{i \in I} F_i) \otimes M$ 是单同态等价于$\bigoplus_{i \in I} (F_i \otimes M' \to F_i \otimes M)$ 是单同态, 也等价于对每个i, $F_i \otimes M' \to F_i \otimes M$ 是单同态.

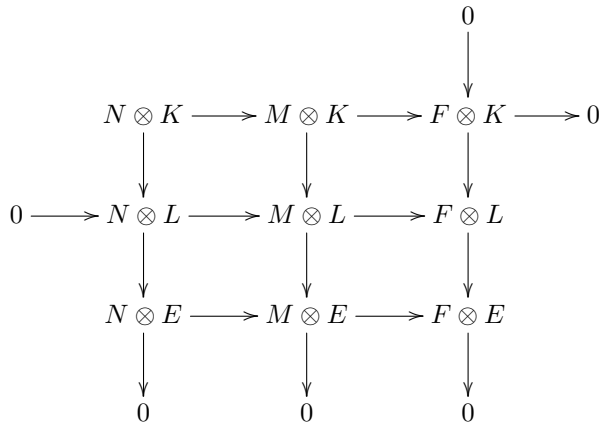
(3) 这是由于投射模是自由模的直和项. $\square$

例1.123. 设R 是整环, $M \cong R/I$, I 是R 的非平凡理想, 则M 不是平坦模. 这是因为单同态$R \to K = \mathrm{Frac} R$ 诱导零同态$R/I = R/I \otimes R \to R/I \otimes K = 0$.

引理1.124. 设F 是平坦模, 则对于正合列$0 \to N \to M \to F \to 0$ 及任意R-模E, 序列$0 \to N \otimes E \to M \otimes E \to F \otimes E \to 0$ 也是正合列.

证明. 设L 为自由模, 且有正合列$0 \to K \to L \to E \to 0$. 则我们有正合交换

图表



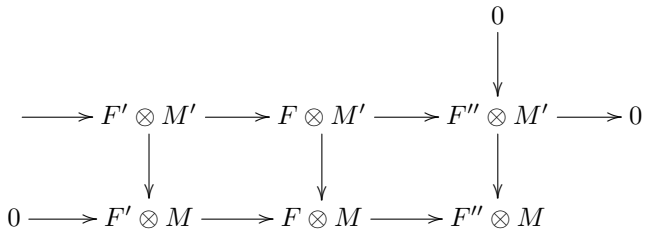
由蛇形引理即得$N \otimes E \to M \otimes E$ 是单同态. □

命题1.125. *设$0 \to F' \to F \to F'' \to 0$ 是正合列且F'' 平坦, 则F 是平坦模当且仅当F' 平坦. 特别地, 对于正合列*

$$0 \to F^0 \to F^1 \to \cdots \to F^n \to 0.$$

如$F^1, \cdots, F^n$ 均平坦, 则F^0 也平坦.

证明. 如$M' \to M$ 是单射, 则有正合交换图表



由蛇形引理,

$$\ker(F' \otimes M' \to F' \otimes M) = \ker(F \otimes M' \to F \otimes M)$$

故F' 平坦等价于F 平坦.

对于一般情况, 首先有$\ker(F^{n-1} \to F^n) = \operatorname{im}(F^{n-2} \to F^{n-1})$ 平坦. 由归纳法知$\operatorname{im}(F^i \to F^{i+1})$ 平坦. 特别地, F^0 平坦. □

命题1.126. *F 是平坦模等价于对任意理想$I \subset R$, 有$I \otimes F \cong IF$.*

我们需要两个引理.

引理1.127. *如对E 的任意子模E', $F \otimes E' \to F \otimes E$ 是单同态, 则对于任意$E_1' \hookrightarrow E_2'$ 及$M' \hookrightarrow M$, 其中E_1', E_2' 为E 的子模, M 为E 的商模, 映射$F \otimes E_1' \to F \otimes E_2'$ 及$F \otimes M' \to F \otimes M$ 还是单同态.*

证明. 对于子模, 这是由于$F \otimes E_1' \to F \otimes E_2' \hookrightarrow F \otimes E$ 是单同态.

对于商模M, 令p 是商映射, $N = \ker p$. 令$E' = \{x \in E \mid p(x) \in M'\}$, 我们有行正合交换图表

$$\begin{array}{ccccccccc}
 & & & & 0 & & & & \\
 & & & & \downarrow & & & & \\
0 & \longrightarrow & N & \longrightarrow & E' & \longrightarrow & M' & \longrightarrow & 0 \\
 & & \| & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & N & \longrightarrow & E & \xrightarrow{p} & M & \longrightarrow & 0.
\end{array}$$

对图表每项$\otimes F$, 我们有

$$\begin{array}{ccccccccc}
 & & & & 0 & & & & \\
 & & & & \downarrow & & & & \\
 & & F \otimes N & \longrightarrow & F \otimes E' & \longrightarrow & F \otimes M' & \longrightarrow & 0 \\
 & & \| & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & F \otimes N & \longrightarrow & F \otimes E & \longrightarrow & F \otimes M & & \\
 & & \downarrow & & & & & & \\
 & & 0 & & & & & &
\end{array}$$

由蛇形引理即知$F \otimes M' \to F \otimes M$ 是单同态. □

引理1.128. *若对所有E_i 及所有$E_i' \hookrightarrow E_i$ 均有$F \otimes E_i' \hookrightarrow F \otimes E_i$. 则对所有$E' \hookrightarrow E = \bigoplus\limits_{i \in I} E_i$ 有$F \otimes E' \hookrightarrow F \otimes E$.*

证明. 先考虑$|I| = 2$ 的情形. 设$E = E_1 \oplus E_2$, 令$E_1' = E_1 \cap E', E_2' = \operatorname{im}(E' \to E_2)$. 则有正合交换图表

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & E_1' & \longrightarrow & E' & \longrightarrow & E_2' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & E_1 & \longrightarrow & E & \longrightarrow & E_2 & \longrightarrow & 0
\end{array}$$

它给出正合交换图表

$$\begin{array}{ccccccccc}
 & & 0 & & & & 0 & & \\
 & & \downarrow & & & & \downarrow & & \\
 & & F \otimes E_1' & \longrightarrow & F \otimes E' & \longrightarrow & F \otimes E_2' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & F \otimes E_1 & \longrightarrow & F \otimes E & \longrightarrow & F \otimes E_2 & &
\end{array}$$

由蛇形引理, $F \otimes E' \to F \otimes E$ 为单同态. 归纳假设即知对I 有限成立.

对于一般情形, 要证$\alpha : F \otimes E' \to \bigoplus_{i\in I}(F \otimes E_i)$ 是单同态. 如$x \in \ker\alpha$, 我们可以假设$x = \sum_j m_j \otimes x_j, m_j \in F, x_j \in E'$. 故$x_j$ 落在E 的有限多个分量上, 将$\alpha(x) = \sum_{i\in I} m_i \otimes y_i$ 写成生成元之和, 则可以假设指标集I 有限从而得到$x = 0$. □

命题*1.126*的证明. 一方面, 由正合列$0 \to I \to R \to R/I \to 0$, 如$F$ 平坦, 则$R/I \otimes F \cong F/(I \otimes F)$. 但$R/I \otimes F \cong F/IF$.

另一方面, 由上述两引理, 我们知

(1) 对任意$M' \hookrightarrow \bigoplus_{i\in I} R, F \otimes M' \hookrightarrow F \otimes (\bigoplus_{i\in I} R)$.

(2) 对于$\bigoplus_{i\in I} R$ 的任意商模M 及$M' \hookrightarrow M$, 有$F \otimes M' \hookrightarrow F \otimes M$.

但任意模均是自由模的商模, 故命题得证. □

§1.4.3 基变换

设$f : R \to S$ 是交换环的同态, 则S 自然视为R-模: $r \cdot s = f(r)s$, 且任意S-模均可视为R-模.

设M 是R-模, 则$S \otimes_R M$ 是R-模. 设$s \in S$, 映射

$$S \times M \to S \otimes_R M,\ (s', m) \mapsto ss' \otimes m$$

是R-双线性映射, 故诱导映射

$$\mu_s : S \otimes_R M \to S \otimes_R M,\ s' \otimes m \mapsto (ss') \otimes m.$$

由此我们得到映射

$$S \times (S \otimes_R M) \to S \otimes_R M,\ (s, s' \otimes m) \mapsto (ss') \otimes m.$$

容易验证这满足数乘映射的两个性质, 因此$S \otimes_R M$ 成为S-模, 记之为M_S.

例1.129. 设$I \subseteq R$ 为理想, $\pi : R \to \overline{R} = R/I$ 为自然商映射. 则$\overline{M} = R/I \otimes_R M \cong M/IM$ 是$\overline{R}$- 模, 称为M 模I 的**约化** (reduction modulo I).

例1.130. 设R 为整环, $K = \mathrm{Frac}R$ 为其分式域, $i : R \to K$ 为自然包含映射. 则$M_K = K \otimes_R M$ 是K-线性空间.

命题1.131. *设M' 是R-模, M 是S-模, $f : R \to S$ 为环同态. 则存在S-模同构映射*

$$M \otimes_S M'_S \xrightarrow{\sim} M \otimes_R M'.$$

证明. 首先设$s \in S$, 则映射

$$M \times M' \to M \otimes_R M',\ (m, m') \mapsto (sm) \otimes m'$$

是R-双线性映射, 故有映射

$$\mu_s : M \otimes_R M' \to M \otimes_R M',\ m \otimes m' \mapsto (sm) \otimes m'.$$

由此定义的映射

$$S \times (M \otimes_R M') \to M \otimes_R M',\ (s, m \otimes m') \mapsto (sm) \otimes m'$$

是数乘映射. 即$M \otimes_R M'$ 也是S-模.

考虑映射

$$M \times M'_S \to M \otimes_R M',\ (m, s \otimes m') \mapsto (sm) \otimes m'.$$

它是S-双线性映射, 故诱导S-模同态

$$\varphi : M \otimes_S M'_S \to M \otimes_R M',\ m \otimes (s \otimes m') \mapsto (sm) \otimes m'.$$

另一方面, $M \otimes_S M'_S$ 作为S-模, 自然视为R-模,

$$M \times M' \to M \otimes_S M'_S,\ (m, m') \mapsto m \otimes (1 \otimes m')$$

是R-模双线性映射, 故得R-模同态

$$\psi : M \otimes_R M' \to M \otimes_S M'_S,\ m \otimes m' \mapsto m \otimes (1 \otimes m').$$

由于φ 与ψ 互为逆映射, 故φ 与ψ 是S- 模同构. □

推论1.132. *设$R \to S \to T$ 为环同态, 则*

$$M_T = T \otimes_R M \cong T \otimes_S M_S = T \otimes_S (S \otimes_R M).$$

命题1.133. *设$R \to A$ 为环同态.*

(1) (*基变换, Base Change*). *如F 是平坦R-模, 则$F_A = A \otimes_R F$ 是平坦A-模.*

(2) *如A 是平坦R-模, M 是平坦A-模, 则M 视为R-模也是平坦R-模.*

证明. (1) 如$M' \hookrightarrow M$ 为A-模单同态, 将M' 与M 视为R- 模, 有单同态$M' \otimes_R F \to M \otimes_R F$. 但由上述命题, 我们有交换图表

$$\begin{array}{ccc} M' \otimes_R F & \xrightarrow{\text{单}} & M \otimes_R F \\ \downarrow \wr & & \downarrow \wr \\ M' \otimes_A F_A & \longrightarrow & M \otimes_A F_A. \end{array}$$

故$M' \otimes_A F_A \hookrightarrow M \otimes_A F_A$. 所以$F_A$ 是平坦A- 模.

(2) 设$N' \hookrightarrow N$ 为R-模单同态. 由A 是平坦R- 模, 则$N'_A \hookrightarrow N_A = N \otimes_R A$ 是A-模单同态. 再由M 是平坦R-模及交换图表

$$\begin{array}{ccc} M \otimes_A N'_A & \xrightarrow{\text{单}} & M \otimes_A N_A \\ \downarrow \wr & & \downarrow \wr \\ M \otimes_R N' & \longrightarrow & M \otimes_R N, \end{array}$$

知$M \otimes_R N' \to M \otimes_R N$ 是单同态, 故M 是平坦R-模. □

§1.5 主理想整环上有限生成模的结构定理

§1.5.1 模的扭元

我们首先仍然假设R 是含幺交换环.

定义1.134. 设M 是R 模, $m \in M$. 理想

$$\mathrm{ann}(m) := \{r \in R \mid rm = 0\} \subseteq R$$

称为m 的**零化子**(annihilator)或**阶**(order). 如m的零化子$\mathrm{ann}(m) \neq 0$, 则m 称为**有限阶元**(element of finite order) 或**扭元**(**挠元**, torsion element).

可以看出

$$\varphi:\ R \to M,\ r \mapsto rm$$

诱导同构$R/\mathrm{ann}(m) \cong \langle m \rangle$.

定义1.135. 对于R-模M, 子集

$$M_{\mathrm{tor}} := \{m \in M \mid m\text{的阶有限}\}.$$

命题1.136. *如R 是整环, 则M_{tor} 是M 的子模.*

证明. 如a, b 扭, $r \in R$, 设$s, t \neq 0$, $sa = tb = 0$. 则$st \neq 0$, $st(a+b) = 0$, $sra = 0$, 故$a + b$ 与ra 均是扭元. □

注记. 如R 不是整环, 则M_{tor} 不一定有子模结构. 如$R = \mathbb{Z}/6\mathbb{Z}$, $M = R$, 则$[3], [4] \in M_{\mathrm{tor}}$ 但$[3] + [4] = [1] \notin M_{\mathrm{tor}}$.

定义1.137. 如$M = M_{\mathrm{tor}}$, M 称为**扭模** 或**挠模**(torsion module). 如$M_{\mathrm{tor}} = 0$, M 称为**无扭模** 或**无挠模**(torsion free module).

命题1.138. *设R 为整环. 则*

(1) *M/M_{tor} 是无扭模.*

(2) *如$M \cong M'$, 则$M_{\mathrm{tor}} \cong M'_{\mathrm{tor}}$ 且$M/M_{\mathrm{tor}} \cong M'/M'_{\mathrm{tor}}$.*

证明. (1) 如$\bar{m} \in M/M_{\text{tor}}$ 扭, 则存在$r \neq 0$, $r\bar{m} = \bar{0}$. 所以$rm = m' \in M_{\text{tor}}$, 存在$r' \neq 0$, $r'm' = 0$. 故$r'rm = 0$. 即$m \in M_{\text{tor}}$, $\bar{m} = 0$.

(2) 如$\varphi : M \to M'$ 为模同态, 则$\varphi(M_{\text{tor}}) \subseteq M'_{\text{tor}}$, 即$\varphi$ 诱导同态$M_{\text{tor}} \to M'_{\text{tor}}$. 如$\varphi$ 是同构, 则φ^{-1} 诱导同态$M'_{\text{tor}} \to M_{\text{tor}}$. 这两个诱导同态互为逆映射.

另一方面, 设$\varphi : M \to M'$ 为同构. 记$\bar{\varphi}$ 为复合映射$M \to M' \to M'/M'_{\text{tor}}$. 则

$$m \in \ker \bar{\varphi} \Leftrightarrow \varphi(m) \in M'_{\text{tor}} \Leftrightarrow m \in \varphi^{-1}(M'_{\text{tor}}) = M_{\text{tor}}.$$

故φ 诱导同构$M/M_{\text{tor}} \cong M'/M'_{\text{tor}}$. □

注记. 如$\varphi : M \to M'$ 为单同态, 则诱导的同态$M_{\text{tor}} \to M'_{\text{tor}}$ 一定是单同态, 但如φ 是满同态, 诱导的同态不一定是满同态, 因此函子$M \mapsto M_{\text{tor}}$ 不是正合函子. 一个简单的例子是$\mathbb{Z}$-模正合列$0 \to \mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$ 诱导的序列$0 \to 0 \to 0 \to \mathbb{Z}/2\mathbb{Z} \to 0$ 不是正合列.

§1.5.2 有限生成无扭模

下面到本节结束我们都假设R 是主理想整环, 即PID. 在群论学习中, 我们已经知道有限生成阿贝尔群的结构定理, 在线性代数学习中, 我们知道方阵和线性变换的史密斯标准形. 这两个理论的推广, 就是PID 上有限生成模的结构定理. 下面的定理对于结构定理的获得至关重要:

定理1.139. 如R 是PID, 则有限生成无扭R 模都是自由模.

推论1.140. 如R 是PID, F 是有限生成自由R-模, S 是F 的子模, 则S 也是自由模且rank $S \leq$ rank F. 特别地, 有限生成投射R-模是自由模.

推论的证明由下述引理即得.

引理1.141. 设R 为PID, M 是由n 个元素生成的R 模. 则M 的子模S 可由最多n 个元素生成.

证明. 我们对n 作归纳. 当$n = 1$ 时, M 是循环模. 故$M \cong R/I$. 如$S \subseteq M$, 则$S \cong J/I$ 也是循环模.

如$M = \langle x_1, \cdots, x_{n+1} \rangle$, 令$M' = \langle x_1, \cdots, x_n \rangle$. 考虑正合列

$$0 \to S \cap M' \to S \to S/S \cap M' \to 0.$$

则$S \cap M'$ 是M' 的子模. 由归纳假设它可由最多n 个元素生成. 而$S/S \cap M' \cong (S + M')/M' \subseteq M/M'$ 或者是零模, 此时S 是M' 的子模; 或者是循环模, 它由1 个元素$\bar{y}$ 生成. 设$S \cap M' = \langle y_1, \cdots, y_k \rangle$, 其中$k \leq n$. 令$y \in S$ 是$\bar{y}$ 的逆元. 则$k + 1$ 元集合$\{y, y_1, \cdots, y_k\}$ 生成S. □

定理*1.139*的证明. 设M 是有限生成无扭模. 记$\{v_1,\cdots,v_n\}$ 是M 的一组生成元. 我们对n 作归纳来证明定理.

(1) 当$n=1$ 时, M 无扭说明映射$R\to M,\ r\mapsto rv_1$ 是同构, 故M 是自由模.

(2) 如$M=\langle v_1,\cdots,v_{n+1}\rangle$, 令$M'=\{m\in M\mid$ 存在 $0\neq r\in R, rm\in\langle v_{n+1}\rangle\}$. 则容易验证$M'$ 是M 的子模且M/M' 是无扭的. 事实上, 如$x\in M\backslash M'$, 若$r\neq 0$, $r(x+M')=0$, 则$rx\in M'$. 故存在$r'\neq 0$, $rr'x\in\langle v_{n+1}\rangle$, 所以$x\in M'$. 矛盾.

由于$v_{n+1}\in M'$, 故M/M' 是由$\{v_1+M',\cdots,v_n+M'\}$ 生成的无扭模. 由归纳假设, 它是秩$\leq n$ 的自由模. 故正合列$0\to M'\to M\to M/M'\to 0$ 分裂, $M=M'\oplus M/M'$. 我们只要证明若$M'\neq 0$, 则M' 是秩为1 的自由模即可.

对于$x\in M'$, 存在$r\neq 0$, $rx=av_{n+1}$. 我们令

$$\varphi:\ M'\to K=\mathrm{Frac}R,\ x\mapsto\frac{a}{r}.$$

则φ 是良定义的单同态, $D=\varphi(M')$ 是K 中有限生成无扭子模. 记$D=\langle\frac{b_1}{c_1},\cdots,\frac{b_m}{c_m}\rangle$, $c=\prod\limits_{i=1}^{m}c_i$. 则

$$f:\ D\to R,\quad d\mapsto cd.$$

是单同态, $D\cong I=aR$ 是秩1的自由模. □

推论1.142. *设R 是*PID*, M 是有限生成R 模. 则*

(1) $M\cong(M/M_{\mathrm{tor}})\oplus M_{\mathrm{tor}}$, *其中*$M/M_{\mathrm{tor}}$ *是有限生成自由*R *模.*

(2) $M\cong M'$ *当且仅当*$M_{\mathrm{tor}}\cong M'_{\mathrm{tor}}$ *且*$\mathrm{rank}\,(M/M_{\mathrm{tor}})=\mathrm{rank}\,(M'/M'_{\mathrm{tor}})$.

证明. (1) 由于M/M_{tor} 是有限生成无扭模, 故是自由模, 从而是投射模, 故正合列$0\to M_{\mathrm{tor}}\to M\to M/M_{\mathrm{tor}}\to 0$ 分裂. 所以我们有$M\cong(M/M_{\mathrm{tor}})\oplus M_{\mathrm{tor}}$.

(2) 显然. □

注记. 今后对于PID 上有限生成模M, 称M/M_{tor} 的秩为M 的秩, 记为$\mathrm{rank}\,(M)$.

推论1.143. PID*上的平坦模即无扭模.*

我们需要一个引理.

引理1.144. *如模M 的所有有限生成子模都是平坦模, 则M 也是平坦模.*

证明. 对于正合列$0\to N'\xrightarrow{i}N$, 我们要证$0\to M\otimes N'\xrightarrow{i_*}M\otimes N$ 也是正合列. 如$\alpha\in\ker\ i_*$, 令$\alpha=\sum\limits_{i=1}^{k}m_i\otimes n'_i$. 则

$$\begin{aligned}i_*(\alpha)=0=&\sum_j c_j[m_j\otimes(n_j+n'_j)-m_j\otimes n_j-m_j\otimes n'_j]\\&+\sum_s c_s[(m_s+m'_s)\otimes n_s-m_s\otimes n_s-m'_s\otimes n_s]\\&+\sum_t c_t[(r_tm_t)\otimes n_t-m_t\otimes(r_tn_t)],\end{aligned}$$

其中下标j,s,t均过有限集, $m_j,m_s,m'_s,m_t\in M, n_j,n'_j,n_s,n_t\in N, c_j,c_s,c_t,r_t\in R$.

令$M'=\langle m_j,m_s,m'_s,m_t\rangle$. 则$M'$是$M$的有限生成子模, $\alpha\in\ker(M'\otimes N'\xrightarrow{i_*}M'\otimes N)=\{0\}$. 故$\alpha=0$. □

推论 *1.143*的证明. 一方面, 若M是无扭模, 则它的所有有限生成子模都是自由模. 故由引理, M是平坦模.

另一方面, 若M是平坦模. 如M有扭元. 设$0\neq m\in M$, $0\neq r\in R$, $rm=0$. 则$m\otimes 1=m\in\ker(M\otimes_R R\to M\otimes \mathrm{Frac}R)$. 矛盾. □

推论1.140 中的有限生成条件可以去掉:

定理1.145. *设R是PID, F是自由R模, H是F的子模. 则H也是自由模且*rank $H\leq$ rank F. *特别地, 投射模即自由模.*

证明. 设$\{x_k\mid k\in K\}$是F的一组基. 根据选择公理(良序原理), 不妨设K是良序集, 即K上有偏序结构且它的任何非空子集有最小元. 对于$k\in K$, 令$F'_k=\langle x_j\mid j<k\rangle$, $F_k=\langle x_j\mid j\leq k\rangle=F'_k\oplus\langle x_k\rangle$. 则$F=\bigcup\limits_k F_k$. 令$H'_k=H\cap F'_k$, $H_k=H\cap F_k$. 则$H_k/H'_k\subseteq F_k/F'_k\cong R$. 故要么$H_k/H'_k=0$, 要么$H_k/H'_k=\langle\overline{h_k}\rangle$对某个$h_k\in H_k\subseteq H$成立. 我们证明: $H=\langle h_k\mid k\in K\rangle$.

设$H^*=\langle h_k\mid k\in K\rangle$. 自然有$H\supseteq H^*$. 对于$f\in F$, 令$\mu(f)$等于最小的$k$使得$f\in F_k$. 如$H^*\neq H$, 令

$$j=\min\{\mu(h)\mid h\in H,\ h\notin H^*\}.$$

选取$h'\in H$, 使得$\mu(h')=j$. 则$h'\in H\cap F_j$. 故$h'=a+rh_j$对某个$a\in H'_j$和$r\in R$成立. 因此$a\in H$, $a\notin H^*$且$a\in H'_j$与j的最小性矛盾. 故$H=H^*$.

我们只要证明$\{h_k\mid k\in K\}$线性无关. 若

$$r_1h_{k_1}+\cdots+r_nh_{k_n}=0,\ k_1<k_2<\cdots<k_n.$$

则$r_nh_{k_n}\in\langle h_{k_n}\rangle\cap H'_{k_n}=0$. 故$r_n=0$. 同理$r_i=0$, $i=1,\cdots,n-1$. □

§1.5.3 结构定理

由推论1.142, 要得到PID上有限生成模M的结构, 只需知道: (i) M的秩$\mathrm{rank}(M)=\mathrm{rank}(M/M_{\mathrm{tor}})$, (ii) 扭子模$M_{\mathrm{tor}}$的结构. 我们下面研究扭模的结构.

定义1.146. 设$P=(p)$是R的非零素理想(换言之, 即极大理想), M是R-模. 如对任意$m\in M$存在正整数n使得$p^nm=0$. 则称M是**P-准素模**(P-primary module).

对于任意R-模M, M的**P-准素部分**定义为

$$M_P=\{m\in M\mid p^nm=0\text{ 对某正整数 }n\text{ 成立}\}.$$

容易看出M_P 是M 的子模.

命题1.147. *如M 是扭模, 则$M = \bigoplus\limits_{P\neq 0} M_P$.*

证明. 设$m \in M$, $m \neq 0$. 记$\mathrm{ann}(m) = (d)$. 则

$$d = up_1^{e_1} \cdots p_n^{e_n}, \text{ 其中}p_i \text{ 是互不关联的素元, } u\text{是单位.}$$

令$r_i = \frac{d}{p_i^{e_i}}$. 则由$p_i^{e_i} \cdot r_i m = 0$ 知$r_i m \in M_{P_i}$, 其中$P_i = (p_i)$. 由于$\gcd(r_1, \cdots, r_n) = 1$, 故存在$s_i \in R$, $\sum\limits_{i=1}^{n} s_i r_i = 1$. 所以

$$m = \sum_{i=1}^{n} s_i r_i m \in \sum_{i=1}^{n} M_{P_i} \subseteq \langle M_P \mid P \text{ 为非零素理想} \rangle.$$

令$H_P = \langle M_{P'} \mid P' \neq P \rangle$. 要证$M = \bigoplus\limits_{P\neq 0} M_P$, 只要证$H_P \cap M_P = \{0\}$ 即可. 设$m \in H_P \cap M_P$. 一方面由$m \in M_P$, 故存在$l \geq 1$, $p^l m = 0$. 另一方面, 由$m \in H_P$, 故$m = \sum\limits_{i=1}^{t} m_i$, $m_i \in M_{Q_i}$, $Q_i = (q_i)$ 知存在$w = q_1^{l_1} \cdots q_t^{l_t}$, 使得$wm = 0$. 由于$(p^l, w) = 1$, 故$m = 0$. □

推论1.148. *设M 与M' 是扭模. 则$M \cong M'$ 当且仅当对任意非零素理想P, $M_P \cong M'_P$.*

由于$P = (p) \neq 0$ 是R 的极大理想, $k_P = R/P$ 是域. 对于任意有限生成R-模M, M/PM 是有限生成k_P-模, 即有限维k_P-线性空间.

定义1.149. 设M 是有限生成R 模. 定义M 在P 处的**深度**

$$\mathrm{d}_P(M) = \dim_{k_P} M/PM.$$

对于$n \geq 1$, 定义

$$U_P(n, M) = \mathrm{d}_P(P^{n-1}M) - \mathrm{d}_P(P^n M).$$

由定义可知, 当M 是有限生成扭模时, $\mathrm{d}_P(M) = 0$ 当且仅当$M = PM$, 这等价于M 的P-准素部分$M_P = 0$.

命题1.150. *设M 是有限生成P-准素模, 则M 是有限多个循环P-准素模的直和. 即*

$$M \cong \bigoplus_{i=1}^{m} R/P^{e_i}$$

其中R/P^e 分量出现的次数等于$U_P(e, M)$, 它由M 唯一决定.

引理1.151. 设$M \neq 0$ 为有限生成P 准素扭模, $p^{n-1}M \neq 0$, 但$p^nM = 0$. 设$x \in M$ 使得$p^{n-1}x \neq 0$. 令$M_1 = \langle x \rangle$, 则

(1) 对所有$i \geq 1$ 有$M_1 \cap p^iM = p^iM_1$.

(2) $\mathrm{d}_P(M) = \mathrm{d}_P(M_1) + \mathrm{d}_P(M/M_1) = 1 + \mathrm{d}_P(M/M_1)$.

证明. (1) 如$y = mp^tx = p^iu$, $p \nmid m$, $t \geq 0$, $u \in M$, 我们要证$y = p^iu'$ 对某个$u' \in M_1$ 成立. 若$i \geq n$, 则$y = 0$, 取$u' = 0$ 即可. 若$i < n$ 而$t \geq i$, 则$y = p^i \cdot mp^{t-i}x$. 若$i < n$ 且$t < i$, 则

$$p^nu = p^{n-i} \cdot y = mp^{n-i+t}x \neq 0.$$

矛盾.

(2) 由模的同构定理, 我们有

$$\frac{M/M_1}{p(M/M_1)} \cong \frac{M/M_1}{(pM + M_1)/M_1} \cong M/(pM + M_1) \cong \frac{M/pM}{(pM + M_1)/pM},$$

且

$$(pM + M_1)/pM \cong M_1/(pM \cap M_1) = M_1/pM_1,$$

故等式得证. □

命题*1.150*的证明. (1) 首先证明M 是形如R/P^e这样的模的直和. 我们对$\mathrm{d}_P(M)$作归纳.

当$\mathrm{d}_P(M) = 1$ 时, 设$0 \neq x \in M$, 则$\bar{x} \in M/PM$ 生成M/PM. 设$p^nx = 0$ 但$p^{n-1}x \neq 0$. 对任意$y \in M$, $y = a_0x + py_1$, 其中$a_0 \in R$, $y_1 \in M$. 依次递归, 则$y = (a_0 + a_1p + \cdots + a_{n-1}p^{n-1})x$. 故$M$ 由x 生成, $M \cong R/P^n$. 所以命题的存在性成立.

假设存在性对于$\mathrm{d}_P(M) \leq k$ 时成立. 考虑$M_0 = \langle x_0 \rangle$, 其中$p^nx_0 = 0$, 但$p^{n-1}x_0 \neq 0$, $p^nM = 0$. 如引理所示, 则

$$\mathrm{d}_P(M/M_0) \leq \mathrm{d}_P(M) - 1 < \mathrm{d}_P(M),$$

由归纳假设, 我们有

- $M/M_0 \cong \bigoplus_{i=1}^{q} \langle \bar{x}_i \rangle$ 为循环模的直和.
- $M_0 = \langle x_0 \rangle \cong R/P^n$ 是循环模.

设$\bar{x}_i \in M/M_0$ 的阶是p^{n_i}. 即$p^{n_i}\bar{x}_i = 0$, 但$p^{n_i-1}\bar{x}_i \neq 0$. 令$y_i \in M$ 是$\bar{x}_i$ 的一个原像, 则$p^{n_i}y_i \in M_0 \cap p^{n_i}M$. 由引理, 存在$r_ix_0 \in M_0$, $p^{n_i}y_i = p^{n_i}r_ix_0$. 故$x_i = y_i - r_ix_0$ 是$\bar{x}_i$ 的原像, 阶等于p^{n_i}, 即$\bar{x}_i$ 的阶, $M_i = \langle x_i \rangle \cong R/p^{n_i}$. 我们有$M = \langle x_0, x_1, \cdots, x_q \rangle$, 只要证明$M$ 是M_i 的直和即可. 如$r_0x_0 + \cdots + r_qx_q = 0$, 模$M_0$ 即得$r_1\bar{x}_1 + \cdots r_q\bar{x}_q = 0$. 由于$M/M_0$ 是$\langle \bar{x}_i \rangle$ 的直和, 故$r_i\bar{x}_i = 0$ 对

于$1 \le i \le q$ 成立. 由于x_i 与$\bar{x}_i$ 同阶, 故$r_i x_i = 0$ 对于$1 \le i \le q$ 成立. 所以$M = \bigoplus_{i=0}^{q} M_i$ 是直和.

(2) 唯一性. 设$M \cong \bigoplus_{i=1}^{m} R/P^{e_i}$. 对于任意$e \ge 0$, 右边分量中$R/P^{e_i}$ $(e_i \ge e+1)$ 出现的次数即$\mathrm{d}_P(p^e M)$, 所以分量中R/P^{e+1} 出现的次数为$U_P(e, M) = \mathrm{d}_P(p^e M) - \mathrm{d}_P(p^{e+1} M)$, 这个值是由$M$ 决定的. □

归纳前面的结果, 我们就得到本节的主要定理:

定理1.152 (主理想整环上有限生成模的结构定理)**.** 设R 是PID, M 是有限生成R-模, 则

$$M \cong R^r \bigoplus \bigoplus_{0 \ne P \text{ 素}} \bigoplus_{n \ge 1} (R/P^n)^{U_P(n,M)},$$

其中

- $r = \operatorname{rank} M = \lim\limits_{n \to \infty} \mathrm{d}_P(P^n M)$,
- $U_P(n, M) = \dim_{k_P} P^{n-1} M/P^n M - \dim_{k_P} P^n M/P^{n+1} M$

由M 唯一确定. 去掉所有$U_P(n, M) = 0$ 的分量, 则M 唯一同构于有限和

$$R^r \oplus \bigoplus_{i=1}^{s} \bigoplus_{j=1}^{j_i} R/P_i^{e_{i,j}}, \quad P_i = (p_i) \text{ 是非零素理想}, \ e_{i,j} > 0.$$

定义1.153. 模M 的**初等因子组** 是多重集$\{p_i^{e_{i,j}} \mid 1 \le i \le s, \ 1 \le j \le j_i\}$, 其中每个元素$p_i^{e_{i,j}}$称为$M$ 的**初等因子**(elementary divisor). M 的**阶**(order)是初等因子组所有因子之积$\prod\limits_{i,j} p_i^{e_{i,j}}$.

将M 的初等因子按相同素因子, 指数由大到小排列

$$\begin{aligned}
&p_1^{e_{11}}, p_1^{e_{12}}, \cdots, p_1^{e_{1j_1}}, \ e_{11} \ge \cdots \ge e_{1j_1}, \\
&p_2^{e_{21}}, p_2^{e_{22}}, \cdots, p_2^{e_{2j_2}}, \ e_{21} \ge \cdots \ge e_{2j_2}, \\
&\cdots \\
&p_s^{e_{s1}}, p_s^{e_{s2}}, \cdots, p_s^{e_{sj_s}}, \ e_{s1} \ge \cdots \ge e_{sj_s}.
\end{aligned}$$

令c_j' 为对应第j 列所有初等因子的乘积, 则c_j' 总是c_{j-1}' 的因子. 如最小因子为c_t'. 令$c_j = c_{t-j+1}'$, 则$c_1 \mid c_2 \mid \cdots \mid c_t$. c_t 是第1列初等因子之积, c_{t-1} 是第2列初等因子之积, $\cdots$, c_1 是第t 列初等因子之积.

定义1.154. $\{c_1, \cdots, c_t\}$ 称为M 的**不变因子**(invariant factor).

根据中国剩余定理, $R/\langle c_j' \rangle = \bigoplus_{i=1}^{s} R/P_i^{e_{ij}}$, 故

推论1.155. $M_{\mathrm{tor}} \cong R/(c_1) \oplus \cdots \oplus R/(c_t)$.

定义1.156. 设R 是交换环, 设M 是扭R 模. 则M 的**零化子**

$$\mathrm{ann}(M) = \{r \in R \mid rm = 0 \text{ 对任意} m \in M \text{ 成立}\}.$$

由定义, $\mathrm{ann}(M) = \bigcap\limits_{m\in M} \mathrm{ann}(m)$ 是R 的理想. 如R 是PID, 再由于

$$M \cong R/(c_1) \oplus \cdots \oplus R/(c_t),$$

我们有

推论1.157. *如R 是PID, M 是扭R 模, 则*$\mathrm{ann}(M) = (c_t)$.

§1.5.4 从模论观点看史密斯标准形理论

设R 是PID, M 是有限生成R 模, 则我们有正合列

$$0 \to S \to R^n \to M \to 0.$$

根据推论1.140, S 作为R^n 的子模是秩$m \le n$ 的自由模. 设R^n 的一组基是$\{e_1, \cdots, e_n\}$, S 的一组基为$\{f_1, \cdots, f_m\}$. 则

$$f_j = \sum_{i=1}^{n} a_{ij} e_i, \quad a_{ij} \in R.$$

记A 为$n \times m$ 阶矩阵(a_{ij}) $(1 \le i \le n,\ 1 \le j \le m)$. 则上式可以表示为

$$(f_1, \cdots, f_m) = (e_1, \cdots, e_n)A.$$

这个生成关系式和生成矩阵确定了M 的表现

$$M = R^n/S = \langle e_1, \cdots, e_n \mid (f_1, \cdots, f_m) = (e_1, \cdots, e_n)A = 0\rangle.$$

若$\{e_1', \cdots, e_n'\}$ 和$(f_1', \cdots, f_m')$ 分别是R^n 和S 的另外一组基, 记

$$(e_1', \cdots, e_n') = (e_1, \cdots, e_n)P, \quad (f_1', \cdots, f_m') = (f_1, \cdots, f_m)Q.$$

则P 是n 阶可逆阵, Q 是m 阶可逆阵, 且

$$(f_1', \cdots, f_m') = (e_1', \cdots, e_n')P^{-1}AQ.$$

这说明基的不同选取得到的生成矩阵在同一个相抵等价类里. 另一方面, 如果$M = \langle e_1, \cdots, e_n \mid f_1, \cdots, f_m\rangle$, 对应的生成矩阵是$A$, $M' = \langle e_1', \cdots, e_n' \mid f_1', \cdots, f_m'\rangle$, 对应的生成矩阵$A' = P^{-1}AQ$, 令

$$T_P : \langle e_1, \cdots, e_n\rangle \to \langle e_1', \cdots, e_n'\rangle,\ (e_1, \cdots, e_n)X \mapsto (e_1', \cdots, e_n')P^{-1}X,$$

$$T_Q : \langle f_1, \cdots, f_m\rangle \to \langle f_1', \cdots, f_m'\rangle,\ (f_1, \cdots, f_m)Y \mapsto (f_1', \cdots, f_m')Q^{-1}Y.$$

则行正合交换图表

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \langle f_1,\cdots,f_m\rangle & \longrightarrow & \langle e_1,\cdots,e_n\rangle & \longrightarrow & M & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle T_Q} & & \downarrow{\scriptstyle T_P} & & \vdots & & \\ 0 & \longrightarrow & \langle f'_1,\cdots,f'_m\rangle & \longrightarrow & \langle e'_1,\cdots,e'_n\rangle & \longrightarrow & M' & \longrightarrow & 0 \end{array}$$

诱导了M 与M' 的同构. 我们有

命题1.158. PID 上有限生成模M 在同构意义下由生成矩阵A 的相抵等价类唯一确定.

令$E_{ij}=(e_{kl})_{n\times n}$, 其中

$$e_{kl}=\delta_{ki}\delta_{lj}=\begin{cases}1, & \text{如}(k,l)=(i,j),\\ 0, & \text{其他情形.}\end{cases}$$

令

$$\begin{aligned} &P_{ij}=I_n-E_{ii}-E_{jj}+E_{ij}+E_{ji},\\ &D_i(\lambda)=I_n+(\lambda-1)E_{ii},\ \lambda\text{是}R\text{ 中的单位, 即}\lambda\in R^\times,\\ &T_{ij}(\lambda)=I_n+\lambda E_{ij},\ \lambda\in R. \end{aligned}$$

则由线性代数知识, 我们知道P_{ij}, $D_i(\lambda)$ 与$T_{ij}(\lambda)$ 均是R 上的可逆方阵, 它们的逆分别是P_{ij}, $D_i(\lambda^{-1})$ 与$T_{ij}(-\lambda)$. 更进一步地, 对于矩阵的初等行变换,

($R1$) 互换矩阵的i,j 两行, 相当于左乘方阵P_{ij},

($R2$) 将单位$\lambda\in R^\times$乘到矩阵第i行, 相当于左乘方阵$D_i(\lambda)$,

($R3$) 将矩阵第j行的λ倍加到第i行, 相当于左乘方阵$T_{ij}(\lambda)$,

及对应的列变换

($L1$) 互换矩阵的i,j 两列, 相当于右乘方阵P_{ij},

($L2$) 将单位$\lambda\in R^\times$乘到矩阵第i列, 相当于右乘方阵$D_i(\lambda)$,

($L3$) 将矩阵第i列的λ倍加到第j列, 相当于右乘方阵$T_{ij}(\lambda)$.

从现在开始, 本节内我们假设R 是欧几里得整环(ED, Euclidean domain), 例如$R=\mathbb{Z}$ 或$k[X]$.

定理1.159. 设R 为ED, 对任意$n\times m$ 阶矩阵A, 总可以通过初等行(列)变换为

$$\begin{pmatrix} d_1 & & & \\ & \ddots & & \\ & & d_r & \\ & & & O \end{pmatrix}$$

的形式, 其中$d_1\mid d_2\mid\cdots\mid d_r$.

证明. 由R 是ED, 我们知存在函数

$$\varphi : R - \{0\} \to \mathbb{Z}_+$$

使得对任意$a, b \in R$ 且$a \neq 0$, 存在$q, r \in R$ 使得$b = aq + r$ 且满足$r = 0$ 或$\varphi(r) < \varphi(a)$. 我们不妨定义$\varphi(0) = 0$.

如$A = 0$ 则定理显然成立. 如$A \neq 0$, 则总可以通过交换第i 行及第j 列使得$a_{11} \neq 0$. 我们对$\varphi(a_{11})$ 作归纳, 证明如下断言: 可以通过对A 进行初等变换得到矩阵$\widetilde{A} = (\tilde{a}_{ij})$ 使得$\tilde{a}_{11} | \tilde{a}_{ij}$ 对所有i, j 成立.

如$\varphi(a_{11}) = 1$ 则$a_{ij} = q_{ij}a_{11} + r_{ij}$, 知$r_{ij} = 0$, 故无需对$A$ 进行初等变换断言已经成立. 现在设$\varphi(a_{11}) = t \geq 2$, 且假设断言对所有$\varphi(a'_{11}) < t$ 的矩阵$A' = (a'_{ij})$ 且$a'_{11} \neq 0$ 均成立. 如$a_{11} \nmid a_{i1}$, 则$a_{i1} = q_{i1}a_{11} + r_{i1}, \varphi(r_{i1}) < t$. 对$A$ 作两次初等行变换(左乘$T_{1i}(-q_{i1})$ 及P_{i1}), 则得到的矩阵$\widetilde{A} = (\tilde{a}_{ij})$ 中, 满足$\varphi(\tilde{a}_{11}) = \varphi(r_{i1}) < t$. 由归纳假设断言得证. 同理如$a_{11} \nmid a_{1j}$, 断言也成立. 现在假设$a_{11} \mid a_{i1}$ 且$a_{11} \mid a_{1j}$ 对所有i, j 成立. 通过初等行(列)变换, 可设$a_{i1} = a_{1j} = 0$ 对所有$i, j > 1$ 成立. 如$a_{11} \nmid a_{ij}$, 令$a_{ij} = q_{ij}a_{11} + r_{ij}$. 则作列变换(右乘$T_{1j}(1)$), 再作行变换(左乘$T_{1i}(-q_{ij})$), 然后再作行变换(左乘$P_{1i}$), 则得到的矩阵$\widetilde{A} = (\tilde{a}_{ij})$ 中满足$\varphi(\tilde{a}_{11}) = \varphi(r_{ij}) < t$. 由归纳假设断言得证.

由断言, A 经初等行(列)变换后得到$\widetilde{A} = (\tilde{a}_{ij})$ 且$\tilde{a}_{ij}$ 是$\tilde{a}_{11}$ 的倍数, 令$\tilde{a}_{ij} = \tilde{q}_{ij}\tilde{a}_{11}$, 对$\widetilde{A}$ 作初等行变换(左乘$T_{1i}(-q_{i1})$) 和列变换(右乘$T_{1j}(-q_{1j})$), 得到矩阵

$$\widetilde{A} = \begin{pmatrix} \tilde{a}_{11} & 0 \\ 0 & \widetilde{A}_1 \end{pmatrix}$$

且$\widetilde{A}_1$ 中所有元素均是$\tilde{a}_{11}$ 的倍数. 我们再作归纳, 即知A 经初等行(列)变换后会变成如下形式

$$A' = \begin{pmatrix} d_1 & & & \\ & \ddots & & \\ & & d_r & \\ & & & O \end{pmatrix}, \ d_1 \mid d_2 \mid \cdots \mid d_r.$$

定理得证. □

注记. 由定理 1.159容易看出, ED 上的可逆阵均是初等矩阵的乘积, 这与域上可逆阵的情况是一样的.

定理1.160. *设R 为ED, M 是有限生成R-模, A 为其生成矩阵. 若A 经过初等变换得到史密斯标准形矩阵*

$$A' = \begin{pmatrix} d_1 & & & \\ & \ddots & & \\ & & d_r & \\ & & & O \end{pmatrix}.$$

则

$$M \cong R^{n-m} \oplus R/(d_1) \oplus \ldots \oplus R/(d_r).$$

故$\{d_1, \ldots, d_r\}$ 恰为M 的不变因子.

下面我们给出$k[x]$-模M 的一个表现.

设V 是k-线性空间, 基是$\{e_1, \ldots, e_n\}$. 设$T : V \to V$ 是线性变换, A 是T 在基$\{e_1, \ldots, e_n\}$ 下的矩阵. 回忆$k[x]$-模V^T, 即由如下数乘

$$k[x] \times V \to V, \quad (f(x), v) \mapsto f(T)v$$

决定的模.

令$V[x] = \{\sum\limits_{i\geq 0} x^i v_i \mid v_i \in V\}$, 其上数乘为

$$k[x] \times V[x] \longrightarrow V[x], \quad (x^i, \sum_{j\geq 0} x^j v_j) \longmapsto \sum_{j\geq 0} x^{i+j} v_j.$$

则$V[x]$ 是由$\{e_1, \ldots, e_n\}$ 生成的自由$k[x]$-模.

定理1.161. 我们有正合列

$$0 \longrightarrow V[x] \xrightarrow{\lambda} V[x] \xrightarrow{\pi} V^T \longrightarrow 0,$$

其中

$$\lambda(x^i v) = x^{i+1} v - x^i T(v), \quad \pi(x^i v) = T^i(v),$$

且λ 在基$\{e_1, \ldots, e_n\}$ 下的矩阵是$xI - A$.

证明. (1) 先证π 是满射: $T^0(v) = v = \pi(v)$.

(2) 其次$\pi \circ \lambda(x^i v) = \pi(x^{i+1} v) - \pi(x^i T(v)) = T^{i+1}(v) - T^i(T(v)) = 0$. 故$\operatorname{im}\lambda \subseteq \ker\pi$.

(3) 若$u = \sum\limits_{i=0}^{m} x^i v_i \in \ker\pi$, 则$\sum\limits_{i=0}^{m} T^i(v_i) = 0$, 故$u = \sum\limits_{i=0}^{m} (x^i v_i - T^i(v_i))$. 但$x^i v_i - T^i(v_i) = \sum\limits_{j=0}^{i-1} \lambda(x^{i-1-j} T^j(v_i)) \in \operatorname{im}\lambda$, 故$\operatorname{im}\lambda = \ker\pi$.

(4) 最后证明λ 是单射. 设$u = \sum\limits_{i=0}^{m} x^i v_i \in \ker\lambda$. 如$u \neq 0$, 则不妨设$x^m v_m \neq 0$, 故$x^{m+1} v_m \neq 0$. 所以$0 = \lambda(u) = \sum\limits_{i=0}^{m} (x^{i+1} v_i - x^i T(v_i)) = x^{m+1} v_m - x^m T(v_m) + \sum\limits_{i=0}^{m-1} (x^{i+1} v_i - x^i T(v_i)) \neq 0$. 矛盾! 故$u = 0$, 即$\lambda$ 是单射. □

推论1.162. A 和B 相似当且仅当$xI - A$ 与$xI - B$ 相抵.

证明. 如A 和B 相似, 显然有$xI - A$ 与$xI - B$ 相抵.

反之, 若$xI - A$ 与$xI - B$ 相抵, 不妨设

$$xI - B = P(xI - A)Q.$$

设线性变换$T_1 : V \to V$ 在基$\{e_1, \ldots, e_n\}$ 下由矩阵A给出, T_2 在基$\{e_1, \ldots, e_n\}$ 下由矩阵B 给出. 则我们有行正合交换图表

$$\begin{array}{ccccccccc} 0 & \longrightarrow & V[x] & \xrightarrow{\lambda_{T_1}} & V[x] & \xrightarrow{\pi_{T_1}} & V^{T_1} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle Q^{-1}} & & \downarrow{\scriptstyle P} & & \vdots & & \\ 0 & \longrightarrow & V[x] & \xrightarrow{\lambda_{T_2}} & V[x] & \xrightarrow{\pi_{T_2}} & V^{T_2} & \longrightarrow & 0 \end{array}$$

由于图表前两列均是同构, 故我们得到V^{T_1} 到V^{T_2} 的同构映射. 由命题1.9, A 与B 相似. □

由矩阵$xI - A$ 的史密斯标准型即得

推论1.163 (空间分解定理)**.** 作为$k[x]$-模,

$$V^T \cong k[x]/(c_1) \oplus \ldots \oplus k[x]/(c_r),$$

这里:

(1) $c_1 \cdots c_r$ 等于非零常数乘以A 的特征多项式$\det(xI - A)$.

(2) c_r 是A 的最小多项式.

(3) $\{c_1, \ldots, c_r\}$ 是A 的不变因子.

习 题

下面习题中我们都假设R是交换环.

习题1.1. 设X 是模M 的子集. 证明X 所生成的子模$\langle X \rangle$ 是所有包含X 的子模之交.

习题1.2. 设R 是交换环, J 是R的理想. 对于R-模M, 证明M/JM 在数乘

$$(r + J)(m + JM) = rm + JM$$

下是R/J-模. 由此推出如果$JM = \{0\}$, 则M 自身是R/J-模; 特别地, 如果J 是R 的极大理想且$JM = \{0\}$, 则M 是R/J 上的线性空间.

习题1.3. 设A, B 和A' 是M 的子模. 证明: 如$A' \subseteq A$, 则$A \cap (B + A') = (A \cap B) + A'$.

习题1.4. 对于R-模M, 证明

$$\varphi_M : \mathrm{Hom}_R(R, M) \longrightarrow M, \quad f \longmapsto f(1)$$

是R-同构.

习题1.5. 设A 是B 的子模. 如A 与B/A 是有限生成模, 则B 也是有限生成模. 这个命题反过来是否正确?

习题1.6. 设R 为环, $f(x) \in R[x]$ 是次数为n 的首一多项式. 证明$R[x]/(f)$ 是秩n 的自由R-模.

习题1.7. 如序列$0 \to M \to 0$ 是正合列, 证明$M = 0$.

习题1.8. 设 $A \xrightarrow{f} B \xrightarrow{g} C$ 是模同态序列. 证明$gf = 0$ 当且仅当$\operatorname{im} f \subseteq \ker g$. 给出一个非正合这样的序列的例子.

习题1.9. 设$0 \to A \to B \to C \to 0$ 为模的短正合列. 如M 为任意模, 证明存在正合序列

$$0 \to A \oplus M \to B \oplus M \to C \to 0$$

及

$$0 \to A \to B \oplus M \to C \oplus M \to 0.$$

习题1.10. 设V_i $(0 \leq i \leq n)$ 是有限维k-线性空间, $0 \to V_0 \to V_1 \to \cdots \to V_n \to 0$ 是k-线性空间正合列. 证明: $\sum\limits_{i=0}^{n} (-1)^i \dim_k V_i = 0$.

习题1.11. 如$A \xrightarrow{f} B \to C \xrightarrow{h} D$为模正合列, 证明$f$ 为满射当且仅当h 为单射.

习题1.12. 设$A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D \xrightarrow{k} E$ 是模正合列. 证明: 存在短正合列

$$0 \longrightarrow \operatorname{coker} f \xrightarrow{\alpha} C \xrightarrow{\beta} \ker k \longrightarrow 0,$$

其中$\alpha(b + \operatorname{im} f) = g(b)$, $\beta(c) = h(c)$.

习题1.13. 证明模短正合列$0 \to A \xrightarrow{i} B \xrightarrow{p} C \to 0$ 分裂当且仅当存在$q : B \to A$ 使得$qi = 1_A$.

习题1.14. 证明线性空间短正合列都是分裂的.

习题1.15. (1) 证明映射$\varphi : B \to C$ 为单射当且仅当对任意$f, g : A \to B$, $\varphi f = \varphi g$ 给出$f = g$.

(2) 证明映射$\varphi : B \to C$ 为满射当且仅当对任意$h, k : C \to D$, $h\varphi = k\varphi$ 给出$h = k$.

习题1.16 (**中国剩余定理**, Chinese Remainder Theorem)**.** 设A_i $(1 \leq i \leq n)$ 是R 的理想, 且满足对任意$1 \leq i \neq j \leq n$, $A_i + A_j = R$. 设M 是R- 模. 证明映射$\varphi : M \to \prod\limits_{i=1}^{n} M/A_iM$, $m \mapsto (m + A_iM)_{1 \leq i \leq n}$ 诱导同构

$$M \Big/ (\prod_{i=1}^{n} A_i)M \longrightarrow \prod_{i=1}^{n} M/A_iM.$$

习题1.17. 设$\{M_i\}_{i\in I}$ 是一族R-模, 对于每个$i\in I$, N_i 是M_i 的子模. 证明:

$$\left(\bigoplus_{i\in I} M_i\right) / \left(\bigoplus_{i\in I} N_i\right) \cong \bigoplus_{i\in I} (M_i/N_i)\,.$$

习题1.18. 设$f: M\to N$, $g: M\to 0$ 和$h: 0\to N$ 是R-模同态. 试求f与g 的推出和f与h 的拉回.

习题1.19. (1) 给定R-模范畴推出图表

$$\begin{array}{ccc} A & \xrightarrow{g} & C \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle \beta} \\ B & \xrightarrow[\alpha]{} & D, \end{array}$$

证明如g 是单射, 则α 是单射; 如g 是满射, 则α 是满射.

(2) 给定R-模范畴拉回图表

$$\begin{array}{ccc} D & \xrightarrow{\alpha} & C \\ {\scriptstyle \beta}\downarrow & & \downarrow{\scriptstyle g} \\ B & \xrightarrow[f]{} & A, \end{array}$$

证明如f 是单射, 则α 是单射; 如f 是满射, 则α 是满射.

习题1.20. 在R-模范畴中证明: $0\to M'\to M\to M''$ 是正合列当且仅当对任意R-模N, $0\to \mathrm{Hom}(N,M')\to \mathrm{Hom}(N,M)\to \mathrm{Hom}(N,M'')$ 是正合列.

习题1.21 (**五引理**, five lemma)**.** 考虑如下R-模交换图表:

$$\begin{array}{ccccccccc} M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 & \longrightarrow & M_4 & \longrightarrow & M_5 \\ {\scriptstyle f_1}\downarrow & & {\scriptstyle f_2}\downarrow & & {\scriptstyle f_3}\downarrow & & {\scriptstyle f_4}\downarrow & & {\scriptstyle f_5}\downarrow \\ N_1 & \longrightarrow & N_2 & \longrightarrow & N_3 & \longrightarrow & N_4 & \longrightarrow & N_5 \end{array}$$

其中行都是正合列. 证明:

(1) 如果f_1 是满射, 而f_2与f_4 是单射, 则f_3 是单射.

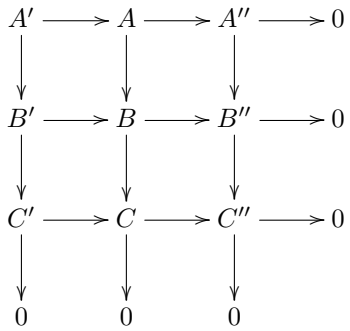
(2) 如果f_5 是单射, 而f_2与f_4 是满射, 则f_3 是满射.

习题1.22. 给出R-模交换图表

$$\begin{array}{ccccccccc} M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 & \longrightarrow & M_4 & \longrightarrow & M_5 \\ {\scriptstyle f_1}\downarrow & & {\scriptstyle f_2}\downarrow & & & & {\scriptstyle f_4}\downarrow & & {\scriptstyle f_5}\downarrow \\ N_1 & \longrightarrow & N_2 & \longrightarrow & N_3 & \longrightarrow & N_4 & \longrightarrow & N_5 \end{array}$$

的例子, 其中中行都是正合列, f_1, f_2, f_4 和f_5 是同构, 但不存在映射$f_3: M_3\to N_3$ 使得图表交换.

习题1.23. 考虑如下R-模交换图表:



其中行与列都是正合列. 证明:

(1) 如果$A'' \to B''$ 和$B' \to B$ 是单射, 则$C' \to C$ 是单射.

(2) 如果$C' \to C$ 和$A \to B$ 是单射, 则$A'' \to B''$ 是单射.

习题1.24. 证明同构一定是双射. 证明在集合范畴$\mathcal{S}$ets中, 双射也是同构.

习题1.25. 设$\mathcal{A}$ 是阿贝尔范畴. $\mathcal{A}$ 的链复形范畴$C(\mathcal{A})$ 如下给出:

- $C(\mathcal{A})$的对象是链复形$A^\bullet = (\cdots \to A^{i-1} \xrightarrow{d_{i-1}} A^i \xrightarrow{d_i} A^{i+1} \to \cdots)$, 其中$d_i \circ d_{i-1} = 0$ 对所有$i \in \mathbb{Z}$ 成立.
- $C(\mathcal{A})$ 的态射$f : A^\bullet \to B^\bullet$ 是态射族$f = (f_i)_{i\in\mathbb{Z}}$, $f_i : A^i \to B^i$, $f_{i+1}d_i = d_i f_i$.

证明$C(\mathcal{A})$ 也是阿贝尔范畴.

习题1.26. 设V 是k-线性空间, V^* 是它的对偶空间. 证明: 函子$V \mapsto V^*$ 是反变正合函子.

习题1.27. 在阿贝尔群范畴$\mathcal{A}$b 中, 定义$G^* = \mathrm{Hom}_{\mathbb{Z}}(G, \mathbb{Q}/\mathbb{Z})$. 证明:

(1) 如果G 是有限阿贝尔群, 则$G \cong G^*$.

(2) 如果$0 \to A \to B \to C \to 0$ 是阿贝尔群正合列, 则$0 \to C^* \to B^* \to A^* \to 0$ 还是正合列.

习题1.28. 设I 是R 的理想. 证明: 如M 是自由R- 模, 则M/IM 是自由R/I-模.

习题1.29. 证明命题*1.91*.

习题1.30. 在阿贝尔范畴中, 证明短正合列$0 \to A \xrightarrow{i} B \xrightarrow{p} C \to 0$分裂当且仅当存在同态$q : B \to A$ 使得$qi = 1_A$.

习题1.31. 在阿贝尔范畴中, 设$A \xrightarrow{f} B \to C \xrightarrow{g} D$ 是正合列. 证明: f 是满射当且仅当g 是单射.

习题1.32. (1) 证明R-模范畴中零模0是零对象.

(2) 证明在集合范畴中, 空集是起始对象, 独点集是终到对象, 但它没有零对象.

习题1.33. 完成例*1.67*的解答.

习题1.34. 证明命题*1.80*.

习题1.35. 设R 是整环, M 是自由R-模. 证明: 如$rm = 0$, 其中$r \in R$ 而$m \in M$, 则$r = 0$或者$m = 0$.

习题1.36. 设R是整环.

(1) 证明: 设I 和J 是R 中非零理想, 则$I \cap J \neq \{0\}$.

(2) 证明: 如果理想I 还是自由R-模, 则I 是主理想.

习题1.37. 证明内射模的直和项还是内射模.

习题1.38. 证明:

(1) 投射模的直和还是投射模.

(2) 投射模的直和项还是投射模.

习题1.39. 设R是整环. 证明:

(1) 如R在R-模范畴中是内射模, 则R是域.

(2) 如R不是域, 则R-模范畴中既是投射模又是内射模的模只能是零模.

习题1.40. 证明: 环$\mathbb{Z}/6\mathbb{Z}$ 作为$\mathbb{Z}/6\mathbb{Z}$-模, 既是投射模又是内射模.

习题1.41. 证明R-模E是内射模当且仅当对R的任意理想I, 正合列$0 \to E \to B \to R/I \to 0$均分裂.

习题1.42. 设$a \in R$不是零除子(即不存在$b \neq 0$, $b \in R$, $ab = 0$). 证明: 对任意平坦R-模F, 不存在非零元$x \in F$, 使得$ax = 0$.

习题1.43. 设R是整环, Q是它的分式域. 证明: $Q/R \otimes_R Q/R = 0$.

习题1.44. 设$(m, n) = 1$, 我们知道$\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} = 0$. 对于一般的$m$ 和n, 有何结论?

习题1.45. 设M, N 是平坦模. 证明$M \otimes N$也是平坦模.

习题1.46. 设R是整环. 证明平坦R-模都是无扭模.

习题1.47. 设$f : R \to S$ 为交换环间的同态, M是R-模, N是S模(故N存在自然R-模结构, 记为N_R). 证明存在典范同构:

$$\mathrm{Hom}_S(S \otimes_R M, N) \cong \mathrm{Hom}_R(M, N_R).$$

习题1.48. 设k 是域, $f(x)$是k上不可约多项式, α 是$f(x)$ 的一个根. 证明: 对于k 的域扩张k', 我们有$k(\alpha)\otimes k'\cong k'[x]/(f(x))$.

习题1.49. 设R 是整环, $0\to M'\to M\to M''\to 0$ 是正合列. 证明: 若M' 可除或者M'' 无扭, 则$0\to M'_{\mathrm{tor}}\to M_{\mathrm{tor}}\to M''_{\mathrm{tor}}\to 0$ 还是正合列.

习题1.50. 设k是域, $R=k[x,y]$ 是k上二元多项式环, $I=(x,y)$ 是R 中的理想.

(1) 求I/I^2 与$(I/I^2)\otimes_R(I/I^2)$ 作为R-模的结构.

(2) 证明$x\otimes y-y\otimes x\in I\otimes_R I$ 非零.

(3) 试求$x\otimes y-y\otimes x$ 的零化子, 从而证明$I\otimes_R I$ 不是无扭模.

(4) 证明I 不是平坦R-模.

习题1.51. 设$G=\prod\limits_p \mathbb{Z}/p\mathbb{Z}$ 为所有素域$\mathbb{Z}/p\mathbb{Z}=\mathbb{F}_p$(即$p$ 过所有素数) 的直积.

(1) 证明: $G_{\mathrm{tor}}=\bigoplus\limits_p \mathbb{Z}/p\mathbb{Z}$.

(2) 证明: G/G_{tor} 是可除群.

(3) 证明: $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q},G)=0$ 但$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q},G/G_{\mathrm{tor}})\neq 0$, 由此证明$G/G_{\mathrm{tor}}$ 不是G 的直和项.

习题1.52. 设R 是PID, M 是R的扭模. 证明:

$$\mathrm{Hom}_R(M,M)\cong\prod_P \mathrm{Hom}_R(M_P,M_P),$$

其中M_P是M的P准素部分.

习题1.53. 设V为2维$\mathbb{F}_p$线性空间. 证明V的所有1维子空间的集合与$\mathbb{P}^1(\mathbb{F}_p)=(\mathbb{F}_p^2-\{(0,0)\})/\sim$一一对应, 其中等价关系$(x,y)\sim(x',y')$ 是指存在$0\neq\lambda\in\mathbb{F}_p$ 使得$(x',y')=(\lambda x,\lambda y)$.

习题1.54. 设M 是有限生成阿贝尔群, 证明加法群$\mathrm{End}_{\mathbb{Z}}(M)$ 也是有限生成阿贝尔群.

习题1.55. 设V是5维实空间, 且通过线性变换$T:V\to V$成为$\mathbb{R}[x]$-模. 给出V作为$\mathbb{R}[x]$-模的结构.

习题1.56. 设R 是PID, p是R的素元, M是R的扭模. 证明: 若$p\in\mathrm{ann}(m)$对某个$0\neq m\in M$成立, 则$\mathrm{ann}(M)\subseteq(p)$.

习题1.57. 设R是PID.

(1) 如A, B, C 是有限生成R模, $A\oplus B\cong A\oplus C$, 证明$B\cong C$.

(2) 如A, B是有限生成R模, $A\oplus A\cong B\oplus B$, 证明$A\cong B$.

习题1.58. 设R是PID, M 是R模. 子模$S \subseteq M$称为**纯子模**是指对任意$r \in R$, 均有$S \cap rM = rS$.

(1) 如p为非零素元, M是准素(p)-模, 证明S是M 的纯子模当且仅当对所有$n \geq 0$, $S \cap p^n M = p^n S$.

(2) 证明M的直和项是M 的纯子模.

(3) 证明M的扭子模M_{tor}是M 的纯子模.

(4) 证明如果M/S无扭, 则S是M 的纯子模.

(5) 设X是M的纯子模构成的集合族, 且满足条件: S, $S' \in X$, 则$S \subseteq S'$或者$S' \subseteq S$. 证明$\bigcup_{S \in X} S$是M 的纯子模.

习题1.59. 设R是PID, M 是有限生成R-模. 证明S是M 的纯子模当且仅当S是M的直和项.

习题1.60. 设R是PID, $P = (p)$ 是R 的一个非零素理想, $k_P = R/P$ 是其商域. 对于R-模M, 定义$M[p] = \{m \in M \mid pm = 0\}$. 对于$n \geq 0$, 定义

$$V_P(n, M) = \dim_{k_P} \left(\frac{p^n M \cap M[p]}{p^{n+1} M \cap M[p]} \right).$$

(1) 证明如果M 是有限生成模, 则$U_P(n, M) = V_P(n, M)$.

(2) 如果M 和N 是形如R/P^e的循环模的直和, 证明$M \cong N$ 当且仅当对任意n, $V_P(n, M) = V_P(n, N)$.

习题1.61. 设k 是域, M 是有限生成$k[x]$-扭模. 如果M的阶是$(x-1)^3(x+1)^2$, 试求M 的所有可能结构, 并给出它的初等因子组和对应的不变因子.

第二章　交换代数初步

本章出现的环均是含幺交换环. 对于环R, $R^\times$是指它的乘法单位群, R 的素谱Spec$R$ 是R中所有素理想构成的集合, R 的极大谱Max$R$ 是R 中所有极大理想构成的集合.

§2.1　诺特环, 诺特模, 阿廷环与阿廷模

§2.1.1　诺特环与诺特模

定义2.1. 如交换环R 的所有理想均是有限生成的, 则称R 是**诺特环**(Noetherian ring).

命题2.2. *设R 是交换环. 则下列条件等价:*

(1) *R 满足**升链条件**(Ascending Chain Condition, 简称ACC), 即R中的理想升链*

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$$

必稳定, 也就是说存在整数N, 当$n \geq N$ 时, $I_n = I_N$.

(2) *R 满足**极大性条件**(Maximality Condition), 即由R 中理想构成的任意非空理想集合族$\mathcal{F}$ 均有极大元, 即存在$I_0 \in \mathcal{F}$ 使得对任意$I \in \mathcal{F}$, $I \neq I_0$, 均有$I_0 \nsubseteq I$.*

(3) *R 是诺特环.*

证明. (1) $\Rightarrow$ (2) 设$\mathcal{F}$ 非空. 如果$\mathcal{F}$ 没有极大元, 任取$I_1 \in \mathcal{F}$, 故存在$I_2 \in \mathcal{F}$, 使得$I_1 \subsetneqq I_2$; 再取$I_3 \in \mathcal{F}$, 使得$I_2 \subsetneqq I_3$; 依此类推, 这样我们得到无穷长不稳定理想升链

$$I_1 \subsetneqq I_2 \subsetneqq I_3 \subsetneqq \cdots \subsetneqq I_n \subsetneqq I_{n+1} \subsetneqq \cdots,$$

与R满足ACC 矛盾.

(2) $\Rightarrow$ (3) 对于R 中任意理想I, 令$\mathcal{F}$ 为所有包含在I 中的有限生成理想构成的集合族, 显然$0 \in \mathcal{F} \neq \emptyset$, 故存在极大元$M \in \mathcal{F}$, $M \subseteq I$为有限生成理想. 如存在$a \in I$, $a \notin M$, 则$I \supseteq M + \langle a \rangle \supsetneqq M$, 而$M + \langle a \rangle$ 还是有限生成的, 这与M 是极大元矛盾, 故$M = I$, 即I 是有限生成的.

(3) $\Rightarrow$ (1) 令$J = \bigcup_{n \geq 1} I_n$, 则$J$ 是有限生成的. 记$J = \langle a_1, \cdots, a_q \rangle$. 设$a_i \in I_{n_i}$. 令$N = \max\{n_i |\ i = 1, \cdots, q\}$, 则$J \subseteq I_N$, 即$J = I_N$. □

例2.3. 我们给出一些诺特环和非诺特环的例子:

(1) 任意域k 都是诺特环, 它只有两个理想: (0) 和(1).

(2) 主理想整环都是诺特环, 特别地, 整数环$\mathbb{Z}$ 和域上的多项式环$k[x]$ 是诺特环.

(3) 设k 是域. 多项式环$k[x_i]_{i \in I}$, 其中指标集I 的阶无限, 不是诺特环.

(4) 设k 是域. 多项式环$k[x,y]$ 的子环$k+xk[x,y]$ 不是诺特环.
(5) 区间$[a,b]$ 上所有实值连续函数构成的环$C([a,b])$ 不是诺特环.
(6) 无限集X到$\mathbb{Z}/2\mathbb{Z}$的函数全体构成的环不是诺特环.

推论2.4. *设R 为诺特环, I 是R 的真理想, 则存在极大理想$\mathfrak{m}$, $\mathfrak{m}\supseteq I$. 特别地, 诺特环的极大理想存在.*

证明. 令$\mathcal{F}=\{J$为R 的真理想且$J\supseteq I\}$, 则$I\in\mathcal{F}$, 故$\mathcal{F}$ 非空. 令$\mathfrak{m}$ 是$\mathcal{F}$ 中的极大元, 则$\mathfrak{m}$ 是R 的极大理想. □

推论2.5. *设R 为诺特环, I 是R 的真理想, 则商环R/I 也是诺特环.*

证明. 由环的对应定理, R/I 中的理想$\bar{J}$ 均有J/I 的形式, 其中J 是R 中包含I 的理想. 由于J 是有限生成的, 自然$\bar{J}$ 也是有限生成的. □

定理2.6 (希尔伯特基定理, Hilbert Basis Theorem)**.** *如R 是诺特环, 则它的多项式环$R[x]$ 也是诺特环.*

证明. 设I 是$R[x]$中的理想. 若I 不是有限生成的, 取$0\neq f_0\in I$ 且其次数最低, 取$f_1\in I-\langle f_0\rangle$ 且其次数最低, 依此类推, 对任意n, 取$f_{n+1}\in I-\langle f_0,f_1,\cdots,f_n\rangle$ 且其次数最低. 令$d_i=\deg f_i$, 则$d_0\leq d_1\leq\cdots\leq d_n\leq\cdots$. 令$a_n$ 为f_n 的首项系数, 则

$$(a_0)\subseteq(a_0,a_1)\subseteq\cdots$$

为R 中的理想升链. 设其在N 处稳定, 故对于$n\geq N$, 均有

$$a_{n+1}\in(a_0,a_1,\cdots,a_n),$$

即存在$r_0,\cdots,r_n\in R$,

$$a_{n+1}=r_0a_0+r_1a_1+\cdots+r_na_n.$$

令

$$f_{n+1}^*=f_{n+1}(x)-\sum_{i=0}^{n}x^{d_{n+1}-d_i}r_if_i(x)$$

则$f_{n+1}^*\in I-\langle f_0,f_1,\cdots,f_n\rangle$, 但

$$\deg f_{n+1}^*<d_{n+1}=\deg f_{n+1}$$

矛盾. □

注记. 上述证明是非构造性的, 我们下面给出一个构造性的证明.

希尔伯特基定理的构造性证明. 设I 是$R[x]$ 的任意理想. 令J 是I 中元素的首项系数生成的R的理想. 它是有限生成的, 故可设$J = \langle a_1, \cdots, a_m\rangle$. 取$f_i \in I$ 使得f_i 的首项系数为a_i, 令$d_0 = \max\{\deg f_i \mid i = 1, \cdots, m\}$. 对于$d \le d_0$, 令$J_d$ 为I 中所有次数为d 的多项式的首项系数生成的理想, 则$J_d = \langle b_{d,1}, \cdots, b_{d,n_d}\rangle$ 也是有限生成的. 对每个$b_{d,j}$, 取$g_{d,j} \in I$, 其次数为d, 首项系数为$b_{d,j}$, 则$I = \langle f_i, g_{d,j} \mid 1 \le i \le m,\ 0 \le d \le d_0,\ 1 \le j \le n_d\rangle$ 是有限生成的. □

推论2.7. 设R 为诺特环, 则n 元多项式环$R[x_1, \cdots, x_n]$ 也是诺特环. 特别地,

(1) 域k上的n元多项式环$k[x_1, \cdots, x_n]$,

(2) 整数环$\mathbb{Z}$上的n元多项式环$\mathbb{Z}[x_1, \cdots, x_n]$,

(3) $k[x_1, \cdots, x_n]$的商环$k[x_1, \cdots, x_n]/I$,

(4) $\mathbb{Z}[x_1, \cdots, x_n]$的商环$\mathbb{Z}[x_1, \cdots, x_n]/I$

均是诺特环.

下面我们介绍诺特模.

命题2.8. 设R 是交换环, M是R 模, 则下列条件等价:

(1) M 的子模都是有限生成模.

(2) **升链条件**(ACC)成立, 即M 的任意子模升链

$$M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n \subseteq \cdots$$

必稳定, 即存在整数N, 对于$n \ge N$ 均有$M_n = M_N$.

(3) **极大性条件**成立, 即M 的子模构成的非空集合族$\mathcal{F}$ 均有极大元, 即存在$N \in \mathcal{F}$, $N \not\subseteq N'$ 对任意的$N' \ne N$ 成立.

证明. 证明与诺特环等价定义的证明一样, 此处从略. □

定义2.9. R 模M 称为诺特模是指它满足前述命题的等价条件.

例2.10. 如R 是诺特环, 则R 作为自身的模是诺特模. 反之亦然.

下面讨论诺特模的性质.

命题2.11. 下列性质成立:

(1) 若M是诺特模, 则M的子模和商模都是诺特模.

(2) 反之, 若$0 \to M' \to M \to M'' \to 0$ 正合, M'与M''都是诺特模, 则M也是诺特模.

证明. (1) 若N 是M 的子模, N' 是N 的子模, 则N' 也是M 的子模, 故它是有限生成的, 所以N是诺特模.

对于$\overline{M'}$ 为M/N 的子模, 由模的对应定理, 存在$N \subseteq M' \subseteq M$ 使得$\overline{M'} = M'/N$. 由于M' 是有限生成的, 故$\overline{M'}$ 也是有限生成的, 所以M/N 是诺特模.

(2) 设N 是M 的子模, $N' = N \cap M'$, $N'' = N/N' \cong (N + M')/M' \subseteq M''$, 故我们有行正合列交换图表

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N' & \longrightarrow & N & \longrightarrow & N'' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0. \end{array}$$

由于M' 与M'' 是诺特模, N' 与N'' 均是有限生成模, 故N 也是有限生成模, 所以M 是诺特模. □

推论2.12. *诺特模的有限直积还是诺特模.*

推论2.13. *如$M = N + N'$, 而N 与N' 均是诺特模, 则M 也是诺特模.*

证明. 由于N 与N' 均是诺特模, 故$N \times N'$ 也是诺特模, 而模同态

$$\begin{aligned} N \times N' &\longrightarrow M, \\ (n, n') &\longmapsto n + n' \end{aligned}$$

是满同态, 故M 作为$N \times N'$ 的商模也是诺特模. □

推论2.14. *设R 是诺特环, M 是有限生成R 模, 则M 是诺特模.*

证明. 设$M = \langle x_1, \cdots, x_n \rangle$, 则模同态

$$f:\ R^n \to M,\ \ (r_1, \cdots, r_n) \mapsto r_1 x_1 + \cdots + r_n x_n$$

是满同态, 故M 作为诺特模R^n 的商模是诺特模. □

§2.1.2 阿廷环与阿廷模

相应于诺特环与诺特模, 我们可以引入阿廷环(Artinian ring) 与阿廷模(Artinian module) 的概念.

定义2.15. 设R 为交换环.

(1) R 称为**阿廷环**, 是指它满足**降链条件** (Descending Chain Condition, 简称DCC), 即R 的理想降链

$$I_1 \supseteq I_2 \supseteq \cdots I_n \supseteq \cdots$$

总稳定, 即存在整数N, 当$n \geq N$时, $I_n = I_N$.

(2) R 模M 称为**阿廷模**, 是指它满足降链条件, 即它的子模降链

$$M_1 \supseteq M_2 \supseteq \cdots \supseteq M_n \supseteq \cdots$$

总稳定.

注记. 由定义知, 环R 是阿廷环, 就是说它作为R-模是阿廷模.

命题2.16. 下列条件等价:

(1) M 是阿廷模.

(2) **极小性条件**成立, 即M 的子模构成的非空集合族均有极小元.

证明. 与诺特环情形类似, 此处从略. □

例2.17. 对于域k, k-模M 是阿廷模当且仅当M 是诺特模当且仅当M 是有限维k- 线性空间.

定理2.18. 设R 是阿廷环, 则

(1) 环R 中只有有限多个极大理想, 即$\mathrm{Max}R = \{\mathfrak{m}_1, \cdots, \mathfrak{m}_n\}$ 为有限集.

(2) 商环$R/\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n \cong R/\mathfrak{m}_1 \times \cdots \times R/\mathfrak{m}_n$ 是有限多个域的直积.

(3) 环R 中的素理想都是极大理想. 理想$J = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n$ 是R 的所有幂零元构成的理想$\mathrm{nil}(R)$, 且存在正整数m, 使得$J^m = 0$.

(4) 我们有环同构

$$R \cong R/\mathfrak{m}_1^m \times \cdots \times R/\mathfrak{m}_n^m,$$

此处$R/\mathfrak{m}_i^m$ 为阿廷环, 且有唯一极大理想$\mathfrak{m}_i/\mathfrak{m}_i^m$.

(5) 阿廷环都是诺特环.

证明. (1) 令S 为R 中有限多个极大理想之交构成的集合族, 则S 中有极小元, 不妨记为$\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n$, 其中$\mathfrak{m}_i$ $(i = 1, \cdots, n)$ 为极大理想. 设$\mathfrak{m}$ 是R 中的任意极大理想, 则

$$\mathfrak{m} \cap \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n.$$

故$\mathfrak{m} \supseteq \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n$. 若对于所有的$i$, 均有$\mathfrak{m}_i \nsubseteq \mathfrak{m}$, 对每个$i$ 取$x_i \in \mathfrak{m}_i$ 但$x_i \notin \mathfrak{m}$. 考虑$x = x_1 \cdots x_n$. 一方面由$x_i \notin \mathfrak{m}$ 和素理想的定义即得$x \notin \mathfrak{m}$, 另一方面由$x_i \in \mathfrak{m}_i$ 即得$x \in \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n \subseteq \mathfrak{m}$, 这就产生了矛盾. 故存在$i$, 使得$\mathfrak{m} \supseteq \mathfrak{m}_i$, 但它们都是极大理想, 所以$\mathfrak{m} = \mathfrak{m}_i$. 因此$\mathfrak{m}_1, \cdots, \mathfrak{m}_n$ 是R 的所有极大理想.

(2) 这由中国剩余定理立得.

(3) 由阿廷环的降链条件(DCC), 我们知道存在$m > 0$, 使得$J^m = J^{m+i}$ 对所有$i > 0$ 成立. 如$J^m \neq 0$, 令S 为R 中所有满足条件$IJ^m \neq 0$ 的真理想I构成的集合族. 则$J \in S$, 故$S \neq \emptyset$. 令I_0 是S 中的极小元. 故存在$x \in I_0$ 使得$xJ^m \neq 0$, 由极小性条件知$I_0 = (x)$. 再由$((x)J)J^m = xJ^m$ 和极小性条件知$(x) = (x)J$. 故$x = xa$ 对某个$a \in J$成立, 即$x(1-a) = 0$. 由于$1-a$ 不在R 的任何极大理想中, $(1-a) = R$, 所以$1-a$ 是单位, 即$x = 0$, 矛盾. 故存在$m \geq 1$, $J^m = 0$.

由于J 是幂零理想, 故$J \subseteq \mathrm{nil}(R) = \{r \mid r^n = 0$对某个$n \geq 0$成立$\}$. 反之, 若$r$ 是幂零元, 故$r^n = 0 \in \mathfrak{p}$, $\mathfrak{p}$ 为任意素理想, 故$r \in \mathfrak{p}$ 对所有的素理想$\mathfrak{p}$ 成立. 所以$\mathrm{nil}(R) \subseteq J$.

我们事实上证明了R 中任何素理想$\mathfrak{p} \supseteq J$, 故它对应$R/J \cong R/\mathfrak{m}_1 \times \cdots \times R/\mathfrak{m}_n = k_1 \times \cdots \times k_n$ 中的一个素理想, 但$R_1 \times R_2$ 的理想总是形如$I_1 \times I_2$的形式, 其中I_1 是R_1 的理想, I_2 是R_2 的理想, 故$k_1 \times \cdots \times k_n$ 的素理想是$k_1 \times \cdots \times 0 \times \cdots \times k_n$的形式, 所以$\mathfrak{p} = \mathfrak{m}_i$ 是极大理想.

(4) 由于$\prod_{i=1}^{n} \mathfrak{m}_i^m \subseteq \left(\prod_{i=1}^{n} \mathfrak{m}_i\right)^m \subseteq J^m = 0$, 故$R = R/\prod_{i=1}^{n} \mathfrak{m}_i^m \cong R/\mathfrak{m}_1^m \times \cdots \times R/\mathfrak{m}_n^m$. 由环的对应定理立得$R/\mathfrak{m}_i^m$ 只有唯一极大理想$\mathfrak{m}_i/\mathfrak{m}_i^m$. 而$R/\mathfrak{m}_i^m$ 是阿廷环由下面的命题 2.19 即得.

(5) 由(4), 只需证$R/\mathfrak{m}^m$ 是诺特环即可. 对于$0 \leq i \leq m-1$ 我们有$R/\mathfrak{m}^m$ 模正合列

$$0 \longrightarrow \mathfrak{m}^{i+1}/\mathfrak{m}^m \longrightarrow \mathfrak{m}^i/\mathfrak{m}^m \longrightarrow \mathfrak{m}^i/\mathfrak{m}^{i+1} \longrightarrow 0.$$

由下面的命题 2.19, 所有$\mathfrak{m}^i/\mathfrak{m}^m$ 及$\mathfrak{m}^i/\mathfrak{m}^{i+1}$ 均是阿廷模. 要证$R/\mathfrak{m}^m$ 是诺特环, 只要证明$\mathfrak{m}^i/\mathfrak{m}^{i+1}$ $(0 \leq i \leq m-1)$ 是诺特模. 但$\mathfrak{m}^i/\mathfrak{m}^{i+1}$ 作为$R/\mathfrak{m}^m$-模是由它作为$R/\mathfrak{m}$-模自然诱导的. 由于$R/\mathfrak{m}$ 是域, 域上的阿廷模与诺特模等价, 均是指域上的有限维线性空间(例 2.17), 故(5)得证. □

注记. 由定理知, 例 2.3 中(3)-(6) 的环由于不是诺特环, 所以也不是阿廷环. 另一方面, 注意到

(1) 诺特环不一定是阿廷环: 整数环$\mathbb{Z}$是诺特环, 但不是阿廷环.

(2) 阿廷模可以不是诺特模: 如设p是素数, $\mathbb{Z}$-模$\mathbb{Z}[\frac{1}{p}]/\mathbb{Z}$ 是阿廷模, 却不是诺特模.

命题2.19. *设$0 \to M' \to M \to M'' \to 0$ 是R 模正合列, 则M 是阿廷模当且仅当M' 与 M'' 是阿廷模.*

证明. 如M 是阿廷模, 视M' 为M 的子模, 则M' 的子模降链也是M 的子模降链, 故一定稳定. 所以M' 是阿廷模. 而根据模的对应定理, $M'' = M/M'$ 的子模降链

$$\overline{N_1} \supseteq \overline{N_2} \supseteq \cdots \supseteq \overline{N_t} \supseteq \cdots$$

对应于M 的子模降链

$$N_1 \supseteq N_2 \supseteq \cdots \supseteq N_t \supseteq \cdots (\supseteq M'),$$

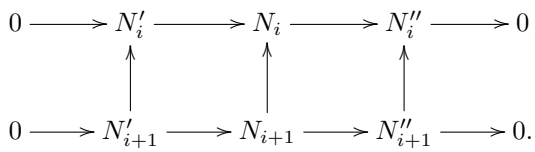
故必稳定. 所以M'' 是阿廷模.

反过来, 设M' 与M'' 是阿廷模. 设

$$N_1 \supseteq N_2 \supseteq \cdots$$

是M 的子模降链. 对于每一个N_i, 令$N_i' = N_i \cap M'$, $N_i'' = (N_i + M')/M'$. 则

我们有行正合交换图表



由降链$N_1' \supseteq \cdots \supseteq N_i' \supseteq \cdots$ 及$N_1'' \supseteq \cdots \supseteq N_i'' \supseteq \cdots$ 稳定知$N_1 \supseteq \cdots \supseteq N_i \supseteq \cdots$ 稳定, 所以M 是阿廷模. □

我们最后给出长度有限模的刻画.

命题2.20. *模M 的长度$\ell(M)$ 有限当且仅当它既是诺特模, 又是阿廷模.*

证明. $\Rightarrow$ 是显然的.

$\Leftarrow$ 现在设M 既是诺特模, 又是阿廷模. 设X 是M 的所有长度有限的子模的集合. 由于$0 \in X$, 故X 非空. 由诺特模的极大性条件, 存在$N \in X$ 是X的极大元. 要证明$M = N$. 如不然, 设Y 是真包含N 的所有M 的子模集合. 由于$M \in Y$, 故Y 非空. 由阿廷模的极小性条件, 设N_0 是Y中的极小元. 则N_0/N是单模, 所以N_0 有长度有限的合成列, 即$N_0 \in X$. 这与N 的极大性矛盾. □

§2.2 局部化

对于交换环R, R 上的乘法含幺半群S 常称为R上的**乘性集**(multiplicative set), 即S 满足条件

(i) $1 \in S$;

(ii) 如$a, b \in S$, 则$ab \in S$.

例2.21. 我们首先给出几个常见的乘性集的例子:

(1) $S = R - \{0\}$.

(2) $S = R^\times$, 即R 的乘法单位集.

(3) $S = R - \mathfrak{p}$, 其中$\mathfrak{p}$ 是R 的素理想.

(4) 更一般地, $S = R - \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_n$, 其中$\mathfrak{p}_1, \cdots, \mathfrak{p}_n$ 是R 的素理想.

引理2.22. *给定交换环R和它上面的乘性集S. 在集合$R \times S$上定义关系*

$$(r_1, s_1) \sim (r_2, s_2) \text{ 当且仅当存在} s \in S, \text{ 使得} s(r_1 s_2 - r_2 s_1) = 0.$$

则此关系是等价关系.

证明. 自反性与对称性显然. 现在设$(r_1, s_1) \sim (r_2, s_2)$, $(r_2, s_2) \sim (r_3, s_3)$. 则存在$s, t \in S$, $sr_1 s_2 = sr_2 s_1$, $tr_2 s_3 = tr_3 s_2$. 故$(sts_2) r_1 s_3 = sts_1 r_2 s_3 = (sts_2) r_3 s_1$. 由于$sts_2 \in S$, 故$(r_1, s_1) \sim (r_3, s_3)$. □

定义2.23. 记(r,s) 所在的等价类为$\frac{r}{s}$. 定义$S^{-1}R = R\times S/\sim$ 为所有等价类构成的集合.

注记. 由定义, $\frac{r_1}{s_1}=\frac{r_2}{s_2}$ 当且仅当存在$s\in S$, $s(r_1s_2-r_2s_1)=0$.

特别地, 如$0\in S$, 则$\frac{r}{s}=\frac{0}{1}$ 对所有$r\in R$, $s\in S$ 成立. 故此时$S^{-1}R=\{0\}$.

以下我们假设$0\notin S$. 我们在$S^{-1}R$ 上定义加法和乘法运算如下:

$$\frac{r_1}{s_1}+\frac{r_2}{s_2}=\frac{r_1s_2+r_2s_1}{s_1s_2},\quad \frac{r_1}{s_1}\cdot\frac{r_2}{s_2}=\frac{r_1r_2}{s_1s_2}.$$

自然需要检查这样的定义是良定义的. 如$\frac{r_1'}{s_1'}=\frac{r_1}{s_1}$, $\frac{r_2'}{s_2'}=\frac{r_2}{s_2}$, 则存在$s,t\in S$, $s(r_1's_1-r_1s_1')=t(r_2's_2-r_2s_2')=0$. 令$s'=st$, 则$s'(r_1's_1-r_1s_1')=s'(r_2's_2-r_2s_2')=0$. 所以

$$\begin{aligned}&s'((r_1s_2+r_2s_1)s_1's_2'-(r_1's_2'+r_2's_1')s_1s_2)\\&=s'r_1s_1's_2s_2'+s'r_2s_2's_1s_1'-s'r_1's_1s_2s_2'-s'r_2's_2s_1s_1'\\&=(s'r_1s_1'-s'r_1's_1)s_2s_2'+(s'r_2s_2'-s'r_2's_2)s_1s_1'=0,\end{aligned}$$

$$\begin{aligned}s'(r_1r_2s_1's_2'-r_1'r_2's_1s_2)&=s'r_1's_1r_2s_2'-s'r_1'r_2's_1s_2\\&=s'r_1s_1r_2's_2-s'r_1'r_2's_1s_2=0.\end{aligned}$$

故

$$\frac{r_1s_2+r_2s_1}{s_1s_2}=\frac{r_1's_2'+r_2's_1'}{s_1's_2'},\quad \frac{r_1r_2}{s_1s_2}=\frac{r_1'r_2'}{s_1's_2'}.$$

命题2.24. 集合$S^{-1}R$ 在上述加法和乘法下构成含幺交换环, 其零元为$0=\frac{0}{1}$, 幺元是$1=\frac{1}{1}$. 映射

$$\varphi_S:\ R\to S^{-1}R,\quad r\to\frac{r}{1}$$

是环同态, 将S映到单位群$(S^{-1}R)^\times$中, 且满足条件:

(1) 若R 为整环, 则φ_S 是单同态, 此时$S^{-1}R$ 也是整环.

(2) 如$S=R^\times$, 则$S^{-1}R=R$.

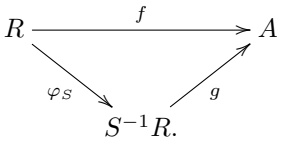
证明. 同态φ_S的核$\ker\varphi_S=\{r\in R\mid \frac{r}{1}=\frac{0}{1}\}=\{r\in R\mid rs=0$对某个$s\in S$成立$\}$. 故当$R$ 为整环时, 由于$0\notin S$, 有$\ker\varphi_S=0$. 其他情形易得. □

定义2.25. 环$S^{-1}R$称为R 在S处的**局部化**(localization).

例2.26. 设R 为交换环. 对于$0\neq f\in R$, 记$S_f=\{f^n\}_{n\geq 0}$, 此处$f^0=1$. 则S_f是R 的乘性集. 记$R_f=S_f^{-1}R$. 如f 为幂零元, 则$R_{f^n}=0$ 对所有正整数n成立. 如f 不是幂零元, 我们有环同构

$$R_f\cong R_{f^n}.$$

定理2.27 (环的局部化泛性质)**.** 设$f : R \to A$ 为环同态且$f(S) \subseteq A^\times$. 则存在唯一的环同态$g : S^{-1}R \to A$ 使得$f = g \circ \varphi_S$, 即有交换图表

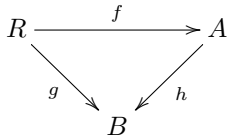


证明. 对于$\frac{r}{s} \in S^{-1}R$, 定义$g(\frac{r}{s}) = f(r)f(s)^{-1}$. 如$\frac{r}{s} = \frac{r'}{s'}$. 则存在$s_1 \in S$, $s_1rs' = s_1r's$. 所以

$$f(s_1)f(r)f(s') = f(s_1)f(r')f(s).$$

由$f(S) \in A^\times$ 知$f(r)f(s)^{-1} = f(r')f(s')^{-1}$. 即$g$ 是良定义的. 定理其他部分的证明易检验. □

注记. 我们可以用范畴论的语言来重新描述一下上述定理. 定义范畴$\mathcal{C}$ 如下: $\mathcal{C}$ 中对象是环同态$f : R \to A$ 且满足条件$f(S) \subseteq A^\times$, $\mathcal{C}$ 的态射是环同态$h : A \to B$, 使得图表



交换. 则定理即是说$\varphi_S : R \to S^{-1}R$ 是范畴$\mathcal{C}$ 的始对象.

例2.28. 设R 为整环, $S = R - \{0\}$. 则$S^{-1}R$ 即R 的分式域K. 它满足如下泛性质: 对任意域L 和环的单同态$f : R \to L$, 存在唯一的域嵌入$g : K \to L$, 使得$f = g\varphi_S$.

现在设R 为交换环, $0 \notin S$ 为R 上的乘性集, M 为R 模. 在集合$M \times S$ 上定义关系

$$(m_1, s_1) \sim (m_2, s_2) \text{ 当且仅当存在 } s \in S,\ s(s_1m_2 - s_2m_1) = 0.$$

则$\sim$ 是$M \times S$上的等价关系. 设其等价类集合为$S^{-1}M$, (m, s) 所在的等价类记为$\frac{m}{s}$. 与$S^{-1}R$ 的情形类似, 可以在$S^{-1}M$ 上定义加法

$$\frac{m_1}{s_1} + \frac{m_2}{s_2} = \frac{s_2m_1 + s_1m_2}{s_1s_2}.$$

它与代表元的选取无关. 由此$S^{-1}M$ 构成阿贝尔群. 定义映射

$$S^{-1}R \times S^{-1}M \longrightarrow S^{-1}M, \quad \left(\frac{r}{s}, \frac{m}{s'}\right) \longmapsto \frac{rm}{ss'}.$$

同样这是良定义的. 并且它满足数乘的基本性质: 恒等元, 结合律和分配律. 故在此意义下, $S^{-1}M$ 构成$S^{-1}R$-模. 更进一步地, R-模同态$f: M \to N$ 诱导$S^{-1}R$-模同态

$$S^{-1}f:\ S^{-1}M \to S^{-1}N, \quad \frac{m}{s} \mapsto \frac{f(m)}{s}.$$

对于模$S^{-1}M$, 定义R-数乘为

$$r \cdot \frac{m}{s} = \varphi_S(r) \cdot \frac{m}{s} = \frac{rm}{s},$$

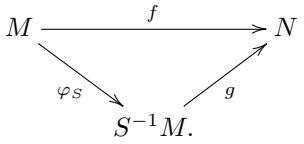
则$S^{-1}M$构成R-模, 映射

$$\varphi_S:\ M \to S^{-1}M, \ \ m \mapsto \frac{m}{1}$$

是R-模同态, 其核$\ker(\varphi_S) = \{m \in M \mid sm = 0 \text{ 对某个 } s \in S \text{ 成立}\}$.

与环的局部化泛性质类似, 有如下的模局部化泛性质:

定理2.29 (模的局部化泛性质)**.** *设M是R-模, N是$S^{-1}R$-模. 如果$f: M \to N$是R-模同态, 则存在唯一的$S^{-1}R$-模同态$g: S^{-1}M \to N$ 使得$f = g \circ \varphi_S$, 即有交换图表*



证明. 对于$\frac{m}{s} \in S^{-1}M$, 定义$g(\frac{m}{s}) = \frac{1}{s}f(m)$. 只要验证$g(\frac{m}{s})$ 与代表元选取无关, 再验证g是$S^{-1}R$-模同态即可. □

推论2.30. *映射$S^{-1}M \to S^{-1}R \otimes_R M$, $\frac{m}{s} \mapsto \frac{1}{s} \otimes m$是$S^{-1}R$-模同构.*

命题2.31. *函子$(M \mapsto S^{-1}M)$ 是R-模到$S^{-1}R$-模的正合函子. 即若$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ 是R-模正合列, 则$0 \to S^{-1}M' \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} S^{-1}M'' \to 0$ 是$S^{-1}R$-模正合列.*

证明. 记$S^{-1}f = f_*$, $S^{-1}g = g_*$. 我们要证f_* 是单射, g_* 是满射且$\operatorname{im} f_* = \ker g_*$.

(1) 如$f_*(\frac{m'}{s}) = \frac{f(m')}{s} = \frac{0}{1}$, 则存在$s_1 \in S$, $s_1 f(m') = f(s_1 m') = 0$. 由$f$ 是单射知$s_1 m' = 0$. 所以$\frac{m'}{s} = \frac{s_1 m'}{s_1 s} = 0$, 即$f_*$ 是单射.

(2) 设$\frac{m''}{s} \in S^{-1}M$, 由$g$ 是满射知存在$m \in M$, $g(m) = m''$, 所以$g_*(\frac{m}{s}) = \frac{m''}{s}$, 即$g_*$ 是满射.

(3) 由$g_* f_*(\frac{m'}{s}) = \frac{gf(m')}{s} = 0$ 知$\operatorname{im} f_* \subseteq \ker g_*$. 另一方面, 若$\frac{m}{s} \in \ker g_*$, 则$\frac{g(m)}{s} = 0$. 故存在$s_1 \in S$, $s_1 g(m) = g(s_1 m) = 0$. 所以$s_1 m \in \ker g = \operatorname{im} f$. 令$f(m') = s_1 m$, 则

$$f_*(\frac{m'}{s_1 s}) = \frac{s_1 m}{s_1 s} = \frac{m}{s} \in \ker g_*.$$

故$\operatorname{im} f_* = \ker g_*$. □

推论2.32. $S^{-1}R$是平坦R-模.

设I 是R 的理想. 由局部化函子的正合性知

$$S^{-1}I = \left\{ \frac{r}{s} \mid r \in I, s \in S \right\} \subseteq S^{-1}R$$

是$S^{-1}R$ 的理想.

反过来, 令J 是$S^{-1}R$ 中的理想, 令

$$J^c = \varphi_S^{-1}(J) = \left\{ r \in R \mid \frac{r}{1} \in J \right\}.$$

则J^c 是R 中理想. 注意到如$\frac{r}{s} \in J$, 则$\frac{r}{1} \cdot \frac{1}{s} \in J$ 知$\frac{r}{1} \in J$, 故$r \in J^c$. 另一方面如$r \in J^c$, 则$\frac{r}{s} = \frac{r}{1} \cdot \frac{1}{s}$ 而$\frac{r}{1} \in J$ 知$\frac{r}{s} \in J$. 因此$S^{-1}J^c = J$.

总结一下, 即有如下命题

命题2.33. *设I 是R 中的理想, J 是$S^{-1}R$ 中的理想, 则*

(1) *$S^{-1}I$ 是$S^{-1}R$ 中的理想, 且满足*

(i) $S^{-1}(I_1+I_2) = S^{-1}I_1+S^{-1}I_2$, $S^{-1}(I_1I_2) = S^{-1}I_1 \cdot S^{-1}I_2$ 且$S^{-1}(I_1 \cap I_2) = S^{-1}I_1 \cap S^{-1}I_2$.

(ii) *存在自然环同构*$S^{-1}(R/I) \cong S^{-1}R/S^{-1}I$. *更进一步地, 如*$I_1 \subseteq I_2$, *则存在自然模同构*$S^{-1}(I_1/I_2) \cong S^{-1}I_1/S^{-1}I_2$.

(2) *J^c 是R 中的理想且*$J = S^{-1}J^c$.

注记. 我们显然有$I \subseteq (S^{-1}I)^c$, 但反方向的包含关系一般不成立. 如I 是R 的真理想且$S \cap I \neq \emptyset$, 则$S^{-1}R = S^{-1}I$.

定义2.34. 对于环R中的理想I, $S^{-1}I$ 称为它的**扩张理想** (extension). 对于环$S^{-1}R$ 中的理想J, J^c 称为它的**收缩理想** (contraction).

定理2.35. 映射

$$\{R\text{中与}S\text{不相交的素理想}\} \longrightarrow \{S^{-1}R\text{中的素理想}\}$$
$$\mathfrak{p} \longmapsto S^{-1}\mathfrak{p}$$

是一一对应, 其逆映射是$\mathfrak{q} \mapsto \mathfrak{q}^c$.

证明. 我们首先证明若$\mathfrak{p}$ 是R 中的素理想且$\mathfrak{p} \cap S = \emptyset$, 则$S^{-1}\mathfrak{p} \neq S^{-1}R$ 是$S^{-1}R$ 中的素理想. 若$\frac{a}{s_1}, \frac{b}{s_2} \notin S^{-1}\mathfrak{p}$, 则$a \notin \mathfrak{p}$ 且$b \notin \mathfrak{p}$, 故$ab \notin \mathfrak{p}$. 如$\frac{ab}{s_1s_2} = \frac{c}{s} \in S^{-1}\mathfrak{p}$, 则存在$s' \in S$, $ss'ab = s's_1s_2c \in \mathfrak{p}$. 但$s', s$ 与ab 均不在$\mathfrak{p}$ 中, 不可能. 即$S^{-1}\mathfrak{p}$ 是素理想. 如$1 = \frac{a}{s} \in S^{-1}\mathfrak{p}$, 则存在$s' \in S$, $ss' = s'a \in \mathfrak{p}$, 不可能. 所以$S^{-1}\mathfrak{p} \neq S^{-1}R$.

其次, 若$\mathfrak{q}$ 是$S^{-1}R$ 中素理想, 我们证明$\mathfrak{q}^c$ 是R 中的素理想. 如$r_1, r_2 \notin \mathfrak{q}^c$, 则$\frac{r_1}{1}, \frac{r_2}{1} \notin \mathfrak{q}$, 即$\frac{r_1r_2}{1} \notin \mathfrak{q}$, 故$r_1r_2 \notin \mathfrak{q}^c$.

我们最后证明若$\mathfrak{p} \cap S = \emptyset$, 则$(S^{-1}\mathfrak{p})^c = \mathfrak{p}$. 一方面$\mathfrak{p} \subseteq (S^{-1}\mathfrak{p})^c$ 是显然的. 另一方面, 如$\frac{a}{s} = \frac{r}{1} \in S^{-1}\mathfrak{p}$, 则存在$s_1 \in S$, $rss_1 = s_1a \in \mathfrak{p}$. 由于$s, s_1 \notin \mathfrak{p}$, 故$r \in \mathfrak{p}$, 故$(S^{-1}\mathfrak{p})^c = \mathfrak{p}$. □

命题2.36. *若R 是诺特环, 则$S^{-1}R$ 也是诺特环.*

证明. 设$J \subseteq S^{-1}R$, 则J^c 是R 中理想. 它是有限生成理想, 因此$J = S^{-1}J^c$ 也是有限生成的. 所以$S^{-1}R$ 是诺特环. □

命题2.37. *设M, N 是R 模. 则*

(1) *如M, N 是R-模L 的子模. 则$S^{-1}(M+N) = S^{-1}M + S^{-1}N$, $S^{-1}(M \cap N) = S^{-1}M \cap S^{-1}N$, $S^{-1}L/S^{-1}M \cong S^{-1}(L/M)$.*

(2) $S^{-1}(M \oplus N) \cong S^{-1}M \oplus S^{-1}N$.

(3) $S^{-1}(M \otimes_R N) \cong S^{-1}M \otimes_{S^{-1}R} S^{-1}N$.

证明. (1) 留作练习.

(2) 由函子$(M \to S^{-1}M)$ 的正合性即得.

(3) 映射

$$S^{-1}M \times S^{-1}N \longrightarrow S^{-1}(M \otimes_R N), \quad \left(\frac{m}{s_1}, \frac{n}{s_2}\right) \longmapsto \frac{m \otimes n}{s_1 s_2}$$

是$S^{-1}R$-模双线性映射, 故诱导同态

$$g: \ S^{-1}M \otimes_{S^{-1}R} S^{-1}N \to S^{-1}(M \otimes_R N), \ \ \frac{m}{s_1} \otimes \frac{n}{s_2} \mapsto \frac{m \otimes n}{s_1 s_2}.$$

这显然是满同态.

另一方面, 映射

$$S^{-1}M \times S^{-1}N \to S^{-1}M \otimes_{S^{-1}R} S^{-1}N, \ \ \left(\frac{m}{s_1}, \frac{n}{s_2}\right) \mapsto \frac{m}{s_1} \otimes \frac{n}{s_2}$$

是R-模双线性映射, 故诱导R 模同态

$$\begin{gathered} S^{-1}M \otimes_R S^{-1}N \longrightarrow S^{-1}M \otimes_{S^{-1}R} S^{-1}N, \\ \frac{m}{s_1} \otimes_R \frac{n}{s_2} \longmapsto \frac{m}{s_1} \otimes_{S^{-1}R} \frac{n}{s_2}. \end{gathered}$$

我们得到R 模同态

$$\begin{aligned} f: \ & M \otimes_R N \xrightarrow{\varphi_M \otimes \varphi_N} S^{-1}M \otimes_R S^{-1}N \longrightarrow S^{-1}M \otimes_{S^{-1}R} S^{-1}N, \\ & m \otimes_R n \longmapsto \frac{m}{1} \otimes_R \frac{n}{1} \longmapsto \frac{m}{1} \otimes_{S^{-1}R} \frac{n}{1}. \end{aligned}$$

定义

$$h: \ S^{-1}(M \otimes_R N) \to S^{-1}M \otimes_{S^{-1}R} S^{-1}N, \ \ \frac{m \otimes n}{s} \longmapsto \frac{f(m \otimes n)}{s}.$$

容易验证h 是$S^{-1}R$ 模同态且g 与h 互逆. □

我们下面讨论一类重要的局部化.

设$\mathfrak{p}$ 是R 的素理想. 则$R-\mathfrak{p}$ 是乘性集, 令

$$R_{\mathfrak{p}}=(R-\mathfrak{p})^{-1}R,\quad M_{\mathfrak{p}}=(R-\mathfrak{p})^{-1}M.$$

由定理 2.35, $\mathfrak{p}R_{\mathfrak{p}}=(R-\mathfrak{p})^{-1}\mathfrak{p}$ 是$R_{\mathfrak{p}}$ 的素理想, 且若$\mathfrak{q}$ 是$R_{\mathfrak{p}}$ 的素理想, 则$\mathfrak{q}^c\cap(R-\mathfrak{p})=\emptyset$. 即$\mathfrak{q}^c\subseteq\mathfrak{p}$, $\mathfrak{q}\subseteq\mathfrak{p}R_{\mathfrak{p}}$. 所以$R_{\mathfrak{p}}$ 只有一个极大理想$\mathfrak{p}R_{\mathfrak{p}}$.

定义2.38. 如交换环R 只有唯一的极大理想$\mathfrak{m}$, 则称R 为**局部环**(local ring).

关于局部环的研究是交换代数一项重要内容.

命题2.39. *设R 是交换环, 则下列条件等价:*

(1) *R 是以$\mathfrak{m}$ 为唯一极大理想的局部环.*

(2) *$\mathfrak{m}=R-R^\times$ 是R 的极大理想.*

(3) *存在极大理想$\mathfrak{m}$, 使得$1+\mathfrak{m}\subseteq R^\times$.*

证明. (1) $\Rightarrow$ (2). 如$a\notin\mathfrak{m}$, 则$(a)=R$, 故存在b, $ab=1$, 即$a\in R^\times$.

(2) $\Rightarrow$ (3) 显然.

(3) $\Rightarrow$ (1). 如$a\notin\mathfrak{m}$, 则$(a)+\mathfrak{m}=R$. 故存在$ab+m=1$, 故$ab=1-m\in R^\times$, 所以$a\in R^\times$. $(a)=R$. 即$\mathfrak{m}$ 是唯一极大理想. □

命题2.40. *设M是R-模. 则下面陈述等价:*

(1) *$M=0$.*

(2) *$M_{\mathfrak{p}}=0$ 对任意R 的素理想$\mathfrak{p}$ 成立.*

(3) *$M_{\mathfrak{m}}=0$ 对任意R 的极大理想$\mathfrak{m}$ 成立.*

证明. (1) $\Rightarrow$ (2) $\Rightarrow$ (3) 显然. 要需证(3) $\Rightarrow$ (1).

若$M\neq0$. 令$0\neq m\in M$. 则m 的零化子

$$\mathrm{ann}(m)=\{r\in R\mid rm=0\}\subsetneqq R$$

是R 的真理想. 设它包含在极大理想$\mathfrak{m}$ 中. 则$\frac{m}{1}\in M_{\mathfrak{m}}$ 且$\frac{m}{1}\neq0$. 矛盾. □

命题2.41. *设R 是整环. 视$R_{\mathfrak{p}}$ 为$K=\mathrm{Frac}R$ 的子环, 则有*

$$R=\bigcap_{\mathfrak{p}\in\mathrm{Spec}R}R_{\mathfrak{p}}=\bigcap_{\mathfrak{m}\in\mathrm{Max}R}R_{\mathfrak{m}}.$$

证明. 由于$\varphi_{\mathfrak{p}}:R\to R_{\mathfrak{p}}$ 是单射. 故$R\subseteq\bigcap\limits_{\mathfrak{p}}R_{\mathfrak{p}}\subseteq\bigcap\limits_{\mathfrak{m}}R_{\mathfrak{m}}$. 设$a\in\bigcap\limits_{\mathfrak{m}}R_{\mathfrak{m}}$. 令$I_a=\{d\in R\mid da\in R\}$. 则$I_a$ 是R 的理想, 且$a\in R\Leftrightarrow I_a=(1)$. 若$a\notin R$. 令$\mathfrak{m}$ 为包含I_a 的一个极大理想. 由于$a\in R_{\mathfrak{m}}$, 故$a=\frac{r}{d}$ 对某个$r\in R$ 和$d\in R-\mathfrak{m}$ 成立. 所以$da=r\in R$, 从而$d\in I_a\subseteq\mathfrak{m}$, 矛盾. 故$\bigcap\limits_{\mathfrak{m}}R_{\mathfrak{m}}=R$. □

§2.3 整性

定义2.42. 设R 是环S 的子环.

(1) 元素$s \in S$ 称为**在R 上整**(integral over R)是指存在首一多项式$f(x) \in R[x]$, 使得$f(s) = 0$.

(2) 如S 中所有元素均在R 上整, 则称S **在R 上整**, 或称S 是R 的**整扩张**(integral extension).

(3) R 在S 中的**整闭包**(integral closure)是指S 中所有在R 上整的元素的集合.

(4) 环R 称为在S 中**整闭**(integrally closed)是指R 等于它在S 中的整闭包. 整环R 在其分式域中的整闭包称为它的**正规化**(normalization), R 称为**整闭**是指它在分式域中整闭.

命题2.43. *设$s \in S$, R 是S 的子环. 则下列条件等价:*

(1) *s 在R 上整.*

(2) *$R[s]$ 是有限生成R 模.*

(3) *存在子环$T \ni s$, $R \subseteq T \subseteq S$, 它作为$R$ 模是有限生成的.*

证明. (1) $\Rightarrow$ (2). 设$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ 使得$f(s) = 0$. 则

$$s^n = -(a_{n-1}s^{n-1} + \cdots + a_1 s + a_0).$$

由归纳即知$s^k (k \geq n)$ 由$1, s, \cdots, s^{n-1}$ 生成. 故$R[s]$ 是由$\{1, s, \cdots, s^{n-1}\}$ 生成的R-模.

(2) $\Rightarrow$ (3). 取$T = R[s]$ 即可.

(3) $\Rightarrow$ (1). 假设T作为R-模由$v_1, \cdots, v_n$ 生成. 由于T 是环, 则由$s \in T$ 有$sv_i \in T$. 故

$$sv_i = \sum_{j=1}^{n} a_{ij}v_j,\ a_{ij} \in R.$$

即

$$\sum_{j=1}^{n} (\delta_{ij}s - a_{ij})v_j = 0,\ i = 1, \cdots, n.$$

令$A = (a_{ij})_{1 \leq i,j \leq n}$, $B = sI_n - A$, $v = (v_1, \cdots, v_n)^T$. 则$Bv = 0$. 左乘B 的伴随矩阵B^* 即得

$$B^*Bv = (\det B)v = 0.$$

即$(\det B)v_i = 0$ 对$i = 1, \cdots, n$ 成立.

由于$1 \in R \subseteq T$, 故$1 = r_1v_1 + \cdots + r_nv_n$, 我们得到$\det B = \det(sI_n - A) = 0$. 由于$\det(xI_n - A)$ 是R 上n 次首一多项式, 所以s 在R 上整. □

推论2.44. 设R 是S 的子环. s 与t 是S 中元素. 则

(1) 如s 与t 在R 上整. 则$s \pm t$ 与st 也在R 上整.

(2) R 在S 中的整闭包是S 中包含R 的子环.

(3) 如$R \subseteq S \subseteq T$ 为子环. T 在S 上整, S 在R 上整, 则T 在R 上整. 即整性是传递的.

证明. (1) 设s 与t 在R 上整, 则$R[s]$ 可由$\{s_1, \cdots, s_n\}$ 生成, $R[t]$ 可由$\{t_1, \cdots, t_m\}$ 生成. 故$R[s,t]$ 是由$\{s_i t_j \mid 1 \leq i \leq n,\ 1 \leq j \leq m\}$ 生成的有限生成R 模. 由命题即知它里面所有元素都在R 上整, 这包括$s \pm t$ 和st.

(2) 由(1) 立得.

(3) 设$t \in T$ 在S 上整, 则它是某首一多项式$p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in S[x]$ 的根. 由于$a_i \in S$ 在R 上整, $R[a_i]$ 是有限生成R-模, 所以$R[a_0, \cdots, a_{n-1}]$ 是有限生成R-模, 从而$R[a_0, \cdots, a_{n-1}][t]$ 也是有限生成R-模, 所以t 在R 上整. □

推论2.45. R 在S 上的整闭包在S 上整闭.

定理2.46. 设R 是环S 的子环, 且S 在R 上整.

(1) 如S 是整环, 则R 是域当且仅当S 是域.

(2) 设$\mathfrak{p}$ 是R 的素理想, 则存在$\mathfrak{q}$ 为S 的素理想使得$\mathfrak{p} = \mathfrak{q} \cap R$. 更进一步地, $\mathfrak{p}$ 是R 的极大理想当且仅当$\mathfrak{q}$ 是极大理想.

(3) (上升定理, Going-up Theorem) 如$\mathfrak{p}_1 \subseteq \mathfrak{p}_2 \subseteq \cdots \subseteq \mathfrak{p}_n$ 是R 中素理想升链, 且存在S 中的素理想升链$\mathfrak{q}_1 \subseteq \mathfrak{q}_2 \subseteq \cdots \subseteq \mathfrak{q}_m$, $\mathfrak{q}_i \cap R = \mathfrak{p}_i$, $m < n$. 则可以完备此升链, 即有S 中的素理想升链$\mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_n$, $\mathfrak{q}_i \cap R = \mathfrak{p}_i$.

证明. (1) 如R 是域, $0 \neq s \in S$, 则存在$a_i \in R$,

$$s^n + a_{n-1}s^{n-1} + \cdots + a_1 s + a_0 = 0.$$

不妨设$a_0 \neq 0$. 则

$$-\frac{1}{a_0}(s^{n-1} + \cdots + a_1) \cdot s = 1.$$

即s 可逆. 反过来, 若S 是域, $0 \neq r \in R$. 则$r^{-1} \in S$ 在R 上整. 故存在$b_0, \cdots, b_{m-1} \in R$,

$$r^{-m} + b_{m-1}r^{-m+1} + \cdots + b_0 = 0.$$

故$r^{-1} = -(b_{m-1} + \cdots + b_1 r^{m-2} + b_0 r^{m-1}) \in R$.

(2) 若$\mathfrak{p}$ 是R 中的素理想. 则$R - \mathfrak{p} = D$ 是环R 和环S 中的乘性集. 我们有交换图表

$$\begin{array}{ccc} R & \xrightarrow{\varphi_D} & R_{\mathfrak{p}} \\ {\scriptstyle i}\downarrow & & \downarrow{\scriptstyle \iota} \\ S & \xrightarrow{\varphi_D} & D^{-1}S. \end{array}$$

容易证明$D^{-1}S$ 在$R_{\mathfrak{p}}$ 上整. 令$\mathfrak{m}$ 是$D^{-1}S$ 中任意极大理想. 则$\mathfrak{m}\cap R_{\mathfrak{p}}$ 是$R_{\mathfrak{p}}$ 中的极大理想. 即$D^{-1}\mathfrak{p}$. 故$\mathfrak{p}=(\iota\varphi_D)^{-1}(\mathfrak{m})$. 令$\mathfrak{q}=\varphi_D^{-1}(\mathfrak{m})$. 则$\mathfrak{q}$ 是S 中的素理想且$\mathfrak{q}\cap R=\mathfrak{p}$.

对于第二个断言, 注意到$S/\mathfrak{q}$ 在$R/\mathfrak{p}$ 上整. 故$S/\mathfrak{q}$ 是域当且仅当$R/\mathfrak{p}$ 是域. 即$\mathfrak{q}$ 是极大理想当且仅当$\mathfrak{p}$ 是极大理想.

(3) 只需证明若$\mathfrak{p}_1\subseteq\mathfrak{p}_2$, 且$\mathfrak{q}_1\cap R=\mathfrak{p}_1$. 则存在$S$ 中的$\mathfrak{q}_2$, $\mathfrak{q}_1\subseteq\mathfrak{q}_2$, 且$\mathfrak{q}_2\cap R=\mathfrak{p}_2$. 由于$\overline{S}=S/\mathfrak{q}_1$ 是$\overline{R}=R/\mathfrak{p}_1$ 的整扩张. 故由(2), 存在$\overline{S}$ 中素理想$\overline{\mathfrak{q}_2}$, 使得$\overline{\mathfrak{q}_2}\cap R=\mathfrak{p}_2/\mathfrak{p}_1$. 故$\overline{\mathfrak{q}_2}$ 的原像$\mathfrak{q}_2$ 即S 中包含$\mathfrak{q}_1$ 的素理想且$\mathfrak{q}_2\cap R=\mathfrak{p}_2$. □

注记. 对应上升 定理, 有如下的下降(Going-Down) 定理: 如S 是整环, 在R上整. 设$\mathfrak{p}_1\supseteq\mathfrak{p}_2\supseteq\cdots\supseteq\mathfrak{p}_n$ 是R 中素理想链, 且存在$\mathfrak{q}_1\supseteq\mathfrak{q}_2\supseteq\cdots\supseteq\mathfrak{q}_m$, $m<n$, 使得$\mathfrak{q}_i\cap R=\mathfrak{p}_i$. 则存在$\mathfrak{q}_m\supseteq\mathfrak{q}_{m+1}\supseteq\cdots\supseteq\mathfrak{q}_n$ 为S 中素理想链使得$\mathfrak{q}_i\cap R=\mathfrak{p}_i$, $m<i\leq n$.

定理2.47. *设R 是整闭整环, $F=\mathrm{Frac}R$. 对于F 的有限可分扩张E, R 在E 中的整闭包S 是某秩为$[E:F]$的自由R-模的子模.*

为证明这个定理, 我们需要迹与迹形式的定义和性质.

定义2.48. 设E/F 是有限域扩张. 对于$u\in E$, 令$\Gamma_u: E\to E$ 是F-线性映射$x\mapsto ux$. 定义u 关于E/F 的**迹** (trace) 和**范**(norm) 为Γ_u 的迹与行列式, 即

$$\mathrm{tr}_{E/F}(u)=\mathrm{tr}(\Gamma_u),\quad N_{E/F}(u)=\det(\Gamma_u).$$

E 关于F 的**迹形式**(trace form) 即对称F-双线性映射

$$t: E\times E\to F,\ (u,v)\mapsto \mathrm{tr}(\Gamma_{uv}).$$

命题2.49. *设E/F 是有限可分扩张, 扩张次数为n. (1) 设$u\in E$ 在F 上的最小多项式是$m(x)=x^m-c_{m-1}x^{m-1}+\cdots+(-1)^mc_0$, 则*

$$\mathrm{tr}_{E/F}(u)=\frac{n}{m}c_{m-1},\quad N_{E/F}(u)=c_0^{n/m}.$$

(2) 迹形式t 是非退化双线性型.

证明. 我们将在习题 2.33-2.36中给出证明. □

定理 2.47的证明. 由命题 2.49(1), 我们知道如$u\in S$, 则$\mathrm{tr}_{E/F}(u)\in R$. 其次, 对于$\alpha\in E$, 如$p(x)=x^n+\frac{a_{n-1}}{d_{n-1}}x^{n-1}+\cdots+\frac{a_0}{d_0}$ 是α 在F 上的最小多项式, a_i, $d_i\in R$, $d_i\neq 0$ $(i=0,\cdots,n-1)$. 则$\alpha'=\alpha(d_0d_1\cdots d_{n-1})\in S$. 即存在$0\neq N\in R$, $N\alpha\in S$.

设$\{e_1,\cdots,e_n\}$ 是E 的一组F-基, 同乘以某非零$N\in R$, 我们不妨假设$e_i\in S$. 由命题 2.49(2), t 是非退化双线性型, 我们设$\{f_1,\cdots,f_n\}$ 是$\{e_1,\cdots,e_n\}$ 的对偶基, 即$t(e_i,f_j)=\delta_{ij}$. 对于$\alpha\in S$, 记$\alpha=\sum_i c_if_i$, $c_i\in K$. 由于$\alpha e_i\in S$,

$\mathrm{tr}_{E/F}(\alpha e_i) \in R$. 另一方面, $\mathrm{tr}_{E/F}(\alpha e_i) = t(\alpha, e_i) = \sum_j c_j \delta_{ji} = c_i$, 故$c_i \in R$. 因此, S 中任何元素都是f_i 的R-线性组合, 即S 是由$\{f_1, \cdots, f_n\}$ 生成的自由R-模的子模. □

命题2.50. 设R 是整环. 则下列条件等价:

(1) R 整闭.

(2) 对所有$\mathfrak{p} \in \mathrm{Spec}R$, $R_\mathfrak{p}$ 整闭.

(3) 对所有$\mathfrak{m} \in \mathrm{Max}R$, $R_\mathfrak{m}$ 整闭.

证明. (1) ⇒ (2) 我们视R, $R_\mathfrak{p}$ 为$K = \mathrm{Frac}R$ 的子环. 如R 整闭, $y \in K$ 在$R_\mathfrak{p}$ 上整. 则

$$y^n + \frac{a_{n-1}}{d_{n-1}} y^{n-1} + \cdots + \frac{a_0}{d_0} = 0, a_i \in R, d_i \in R - \mathfrak{p}.$$

故$y' = y d_0 d_1 \cdots d_{n-1}$ 是R 上一个首一多项式的根. 故$y' \in R$. 所以$y \in R_\mathfrak{p}$.

(2) ⇒ (3) 是显然的.

(3) ⇒ (1) 设$y \in K$ 在R 上整. 由于$R \subseteq R_\mathfrak{m}$. 故$y$ 在$R_\mathfrak{m}$ 上整. 所以$y \in R_\mathfrak{m}$ 对每个$\mathfrak{m} \in \mathrm{Max}R$ 成立. 故$y \in \bigcap\limits_\mathfrak{m} R_\mathfrak{m} = R$. □

本节最后我们讨论代数整数的简单性质.

定义2.51. 设K 是有理数域$\mathbb{Q}$ 的扩域.

(1) 元素$\alpha \in K$ 如在有理整数环$\mathbb{Z}$ 上整, 则称α 为K 上的**代数整数**(algebraic integer).

(2) 有理整数环$\mathbb{Z}$ 在K 上的整闭包, 即K上所有代数整数的集合, 称为域K 的**代数整数环**(ring of algebraic integers) 或**整数环**, 记为$\mathcal{O}_K$.

例2.52. 我们来看两个例子.

(1) 有理数域$\mathbb{Q}$ 的代数整数环$\mathcal{O}_\mathbb{Q}$ 即通常的整数环$\mathbb{Z}$.

(2) 令$K = \mathbb{Q}(\sqrt{D})$, D 为无平方因子数, 为二次数域. 则

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{D}], & \text{如} D \equiv 2, 3 (\mathrm{mod} 4); \\ \mathbb{Z}[\frac{1+\sqrt{D}}{2}], & \text{如} D \equiv 1 (\mathrm{mod} 4). \end{cases}$$

命题2.53. 元素$\alpha \in K$ 为代数整数当且仅当α 是代数数且它在$\mathbb{Q}$ 上的最小多项式$\in \mathbb{Z}[x]$.

证明. ⇐ 显然.

⇒ 若α 为代数整数. 则α 显然是代数数. 设首一整系数多项式$f(x)$ 是它的一个化零多项式. 设$p(x) \in \mathbb{Q}[x]$ 是α 在$\mathbb{Q}$ 上的最小多项式. 则$f(x) = g(x)p(x)$对某个首一多项式$g(x) \in \mathbb{Q}[x]$ 成立. 对$p(x)$ 乘以足够大的整数c_p 使得$p^*(x) = c_p p(x)$ 是$\mathbb{Z}[x]$ 中的本原多项式, 对$g(x)$ 乘以足够大的整数c_g 使得$g^*(x) = c_g g(x)$ 是$\mathbb{Z}[x]$ 中的本原多项式, 则由高斯引理知多项式$c_p c_g f(x) =$

$p^*(x)g^*(x)$ 是$\mathbb{Z}[x]$ 中的本原多项式, 故它的容度等于± 1, 也等于$\pm c(c_pc_gf(x)) = \pm c_pc_g$. 所以$c_p = c_f = \pm 1$, $p(x) = \pm p^*(x) \in \mathbb{Z}[x]$. □

命题2.54. *设K 是$\mathbb{Q}$ 的有限扩张, 则$\mathcal{O}_K$ 作为$\mathbb{Z}$ 模是自由模, 秩为$n = [K : \mathbb{Q}]$, 即K在$\mathbb{Q}$上的扩张次数.*

证明. 由于$K/\mathbb{Q}$ 总是可分扩张, 由定理 2.47知$\mathcal{O}_K$ 是秩n的自由$\mathbb{Z}$-模的子模, 故它也是秩$\leq$ n 的自由$\mathbb{Z}$-模. 另一方面, 如$\{e_1, \cdots, e_n\}$ 是K 的一组$\mathbb{Q}$-基, 令$0 \neq N \in \mathbb{Z}$ 使得$Ne_i \in \mathcal{O}_K$ $(i = 0, \cdots, n-1)$, 则$\{Ne_1, \cdots, Ne_n\}$ 生成$\mathcal{O}_K$ 的一个秩为n 的$\mathbb{Z}$-子模, 故$\mathcal{O}_K$ 的秩也是n. □

命题2.55. (1) *设α 是代数整数, 则α 的共轭元也是代数整数.*

(2) *设$\varepsilon_1, \cdots, \varepsilon_n$ 为n 次单位根. 如$\gamma = \frac{\varepsilon_1 + \cdots + \varepsilon_n}{n}$ 是代数整数, 则$\gamma = 0$ 或者$\varepsilon_1 = \varepsilon_2 = \cdots = \varepsilon_n$.*

证明. (1) 这是因为由定义, α 的共轭元与α 有相同的最小多项式.

(2) 若$\gamma \neq 0$, 则$|\gamma| \leq 1$ 且$|\gamma| = 1$ 当且仅当$\varepsilon_1 = \varepsilon_2 = \cdots = \varepsilon_n$. 令$K$ 是γ 的分裂域. 则γ 的共轭元一定是$\sigma(\gamma) : \sigma \in \mathrm{Gal}(K/\mathbb{Q})$ 的形式. 所以

$$|\sigma(\gamma)| = \frac{|\sigma(\varepsilon_1) + \cdots + \sigma(\varepsilon_n)|}{n} \leq 1.$$

故γ 的共轭元之积的绝对值≤ 1.

但由于$\gamma \neq 0$, γ 的共轭元之积的绝对值等于γ 的最小多项式常数项的绝对值, 这是≥ 1 的. 所以

$$\gamma \neq 0,\ \gamma \in \mathcal{O}_K \Leftrightarrow |\gamma| = |\sigma(\gamma)| = 1 \Leftrightarrow \varepsilon_1 = \varepsilon_2 = \cdots = \varepsilon_n.$$ □

§2.4 根式理想和准素理想

§2.4.1 根式理想

命题2.56. *设I 是环R 的理想, 则*

$$\sqrt{I} = \{a \in R \mid \text{存在 } k \geq 1 \text{ 使得 } a^k \in I\}$$

也是R 的理想, 且$\sqrt{I}/I$ 是R/I 中幂零元构成的集合.

证明. 如$a \in \sqrt{I}$, $r \in R$, 则显然有$ra \in \sqrt{I}$. 我们只要证: 如$a, b \in \sqrt{I}$, 则$a+b \in \sqrt{I}$.

设$a^m \in I$, $b^n \in I$, 由二项式定理

$$(a+b)^{m+n} = \sum_{k=0}^{m+n} \binom{m+n}{k} a^k b^{m+n-k},$$

由于总有$k \geq m$ 或$m + n - k \geq n$ 成立, 故$a^k b^{m+n-k} \in I$, 因此$(a+b)^{m+n} \in I$. 所以$a + b \in \sqrt{I}$. 至于$\sqrt{I}/I$ 是R/I 的幂零理想由$\sqrt{I}$ 的定义即得. □

定义2.57. 设I 是环R的理想.

理想$\sqrt{I}=\{a\in R\mid$ 存在 $k\geq 1$ 使得 $a^k\in I\}$ 称为I **的根式理想**(radical ideal of I). 特别地, 取$I=(0)$, 则$\sqrt{(0)}$ 即R 中的幂零元构成的集合, 称为R 的**幂零根**(nilpotent radical), 我们记之为$\mathrm{nil}(R)$.

如$\sqrt{I}=I$, 则I 称为**根式理想**.

例2.58. 素理想均是根式理想.

命题2.59. *设I 是R 的理想, 则*

$$\sqrt{I}=\bigcap_{\text{素理想}\mathfrak{p}\supseteq I}\mathfrak{p}.$$

特别地,

$$\mathrm{nil}(R)=\sqrt{(0)}=\bigcap_{\mathfrak{p}\in\mathrm{Spec}R}\mathfrak{p}.$$

证明. 由命题 2.56, $\sqrt{I}/I=\mathrm{nil}(R/I)$, 故我们只要证$\mathrm{nil}(R)=\bigcap\limits_{\mathfrak{p}\in\mathrm{Spec}(R)}\mathfrak{p}$.

一方面, 若$a^k=0\in\mathfrak{p}$, 则$a\in\mathfrak{p}$. 所以$\mathrm{nil}(R)\subseteq\mathfrak{p}$. 另一方面, 若$a\notin\mathrm{nil}(R)$, 则集合

$$S=\{I\text{为}R\text{中的真理想且 }I\cap\{a^n\mid n\geq 1\}=\emptyset\}$$

是R 中真理想组成的集合. 由于$(0)\in S$, S 是非空集. 令P 是S 中的由包含关系得到的一个极大元. 我们证明P 是素理想. 事实上, 如$x,y\notin P$, 但$xy\in P$, 则有$n,m\geq 1$,

$$a^n\in(x)+P,\ a^m\in(y)+P.$$

所以$a^{m+n}\in(xy)+P=P$, 与$P\in S$ 矛盾. 故P 是素理想. 所以$a\notin\bigcap\limits_{\mathfrak{p}\in\mathrm{Spec}R}\mathfrak{p}$. □

定义2.60. 环R 的**雅各布森根**(Jacobson radical), 记为$\mathrm{Jac}(R)$ 或者$\mathrm{rad}(R)$, 是R 中的所有极大理想之交.

例2.61. 如R 为阿廷环, 则$\mathrm{Spec}R=\mathrm{Max}R=\{\mathfrak{m}_1,\mathfrak{m}_2,\cdots,\mathfrak{m}_n\}$. 此时

$$\mathrm{Jac}(R)=\mathrm{nil}(R)=\mathfrak{m}_1\cap\mathfrak{m}_2\cap\cdots\cap\mathfrak{m}_n.$$

命题2.62. *如R 为诺特环, 对于$I\subseteq R$, 存在$k\geq 1$, $(\sqrt{I})^k\subseteq I\subseteq\sqrt{I}$. 特别地, 存在$N\geq 1$, $\mathrm{nil}(R)^N=0$.*

证明. 这是因为$\sqrt{I}$ 是有限生成的. □

命题2.63. *设J 是R 的雅各布森根, 则*

(1) *如I 是R 的真理想, 则$(I,J)\neq R$.*

(2) *元素$x\in J$ 当且仅当对所有$r\in R$, $1-rx\in R^\times$.*

(3) **中山(*Nakayama*)引理**: *如M 是有限生成R 模且$JM=M$, 则$M=0$.*

证明. (1) 如$I \neq R$, 则$I \subseteq \mathfrak{m}$ 对某个极大理想$\mathfrak{m}$ 成立. 故

$$(I, J) \subseteq \mathfrak{m} \neq R.$$

(2) 如$1 - rx \notin R^\times$, 则$(1 - rx) \subseteq \mathfrak{m}$, $\mathfrak{m}$ 为某极大理想. 如$x \in \mathfrak{m}$, 则$1 \in \mathfrak{m}$, 不可能. 所以$x \notin \mathfrak{m}$. 因此$x \notin J$. 另一方面, 若$x \notin J$, 则存在极大理想$\mathfrak{m}'$, 使得$x \notin \mathfrak{m}'$. 故$R = (x, \mathfrak{m}')$, 即$1 = rx + y$ 对某个$r \in R$, $y \in \mathfrak{m}'$ 成立, 故$1 - rx = y \in \mathfrak{m}'$ 不是单位.

(3) 如$M \neq 0$, 设$M = (m_1, \cdots, m_n)$ 且n 是最小的生成元个数. 由$M = JM$, 故

$$m_n = r_1 m_1 + r_2 m_2 + \cdots + r_n m_n, r_1, r_2, \cdots, r_n \in J.$$

因此$(1 - r_n)m_n = r_1 m_1 + r_2 m_2 + \cdots + r_{n-1} m_{n-1}$. 但由(2), $1 - r_n$ 是单位, 故m_n 由$m_1, \cdots, m_{n-1}$ 表出, $M = (m_1, \cdots, m_{n-1})$. 矛盾. □

§2.4.2 准素理想

定义2.64. 环R 的理想Q 称为**准素理想**(primary ideal) 是指如$ab \in Q$ 且$a \notin Q$, 则存在$n \geq 1$, 使得$b^n \in Q$, 换言之, 即$b \in \sqrt{Q}$.

准素理想有如下基本性质:

命题2.65. (1) *素理想均是准素理想.*

(2) *理想Q 是准素理想当且仅当R/Q 中的零除子均是幂零元.*

(3) *如理想Q 是准素理想, 则$\sqrt{Q}$ 是素理想, 且它是包含Q 的最小素理想.*

(4) *如理想Q 的根式理想$\sqrt{Q}$ 是极大理想, 则Q 是准素理想.*

(5) *如$\mathfrak{m}$ 是极大理想, $\mathfrak{m}^n \subseteq Q \subseteq \mathfrak{m}$. 则$Q$ 是准素理想且$\sqrt{Q} = \mathfrak{m}$.*

证明. (1), (2) 由准素理想的定义立得.

(3) 如$ab \in \sqrt{Q}$, 则存在n, $a^n b^n \in Q$. 若$a^n \in Q$, 则$a \in \sqrt{Q}$; 若$a^n \notin Q$, 则存在$m \leq 1$, $(b^n)^m = b^{nm} \in Q$, 所以$b \in \sqrt{Q}$. 故$\sqrt{Q}$ 是素理想. 由于$\sqrt{I} = \bigcap\limits_{\mathfrak{p} \supseteq I} \mathfrak{p}$ 对所有$I \subseteq R$ 成立(命题 2.59), 所以$\sqrt{Q} = \bigcap\limits_{\mathfrak{p} \supseteq Q} \mathfrak{p}$, 即$\sqrt{Q} \subseteq \mathfrak{p}$ 对所有$\mathfrak{p} \supseteq Q$ 成立.

(4) 由(2), 只要证R/Q 的零除子都是幂零元. 在R/Q 中,

$$\sqrt{Q}/Q = \mathrm{nil}(R/Q) = \bigcap_{\mathfrak{p} \in \mathrm{Spec}(R/Q)} \mathfrak{p}.$$

若$\sqrt{Q}$ 是R 的极大理想, 则$\sqrt{Q}/Q$ 是R/Q 中唯一的素理想和极大理想. 如$d \in R/Q$ 是零除子, 则$R/Q \neq (d) \subseteq \sqrt{Q}/Q$. 即$d$ 是幂零元.

(5) 由$\mathfrak{m}^n \subseteq Q \subseteq \mathfrak{m}$ 知$\sqrt{Q} \subseteq \sqrt{\mathfrak{m}} = \mathfrak{m}$ 且$\sqrt{Q} \supseteq \sqrt{\mathfrak{m}^n} = \mathfrak{m}$. 故$\sqrt{Q} = \mathfrak{m}$. 由(4) 即得$Q$ 是准素理想. □

定义2.66. 如Q 是准素理想. 称$\mathfrak{p} = \sqrt{Q}$ 是Q 的**相伴素理想** (associated prime ideal), 也称Q 是$\mathfrak{p}$-**准素理想**.

定义2.67. (1) R 中的理想I 如果是准素理想的交, 则称I有**准素分解**(primary decomposition), 亦称

$$I = \bigcap_{i=1}^{m} Q_i, \text{ 其中 } Q_i \text{ 为准素理想}$$

为I的准素分解.

(2) I 的准素分解$I = \bigcap\limits_{i=1}^{m} Q_i$ 称为**极小准素分解**(minimal primary decomposition) 是指下列条件成立:

(i) 对于所有$1 \le i \le m$, $Q_i \not\supseteq \bigcap\limits_{j\neq i} Q_j$;

(ii) 对所有$i \neq j$, $\sqrt{Q_i} \neq \sqrt{Q_j}$.

此时称分解式中的Q_i 是I 的**准素分量** (primary component).

定义2.68. 理想$I \subsetneqq R$ 称为**不可约理想**(irreducible ideal) 是指如$I = J \cap K$, 其中J与K是R中理想, 则$I = J$ 或$I = K$ 成立.

例2.69. 素理想是不可约理想.

命题2.70. *设R 是诺特环, 则*

(1) *不可约理想是准素理想.*

(2) *R 中的真理想均是不可约理想的有限交.*

证明. (1) 设I 不可约, $ab \in I$, 且$b \notin I$. 令

$$A_n = \{x \in R \mid a^n x \in I\}.$$

则A_n 是R 中的理想且$A_1 \subseteq A_2 \subseteq \cdots$. 由诺特条件, 故存在$N > 0$, $A_N = A_{N+1} = \cdots$.

设$J = (a^N) + I$, $K = (b) + I$. 令$y \in J \cap K$. 则$y = a^N z + y'$, $z \in R$, $y' \in I$. 由$ab \in I$ 知$aK \subseteq I$. 故$ay \in I$. 故$a^{N+1}z = ay - ay' \in I$. 所以$z \in A_{N+1} = A_N$. 所以$a^N z \in I$. 故$y \in I$. 因此$J \cap K = I$.

由于I 不可约, 而$(b) + I \neq I$. 故$J = (a^N) + I = I$, 故$a^N \in I$. 即I 为准素理想.

(2) 令$S = \{I \subsetneqq R \mid I$ 不是不可约理想的有限交$\}$. 如$S \neq \emptyset$. 则由诺特性质, S 中有极大元, 记为I. 由于I 不是不可约的. 故存在J, K, $I \subsetneqq J$, $I \subsetneqq K$, $I = J \cap K$. 但由于$J \notin S$ 且$K \notin S$. 故J 和K 均是不可约理想的有限交, 这样$I = J \cap K$ 也是不可约理想的有限交. 矛盾. □

引理2.71. *如Q_1 和Q_2 都是交换环R 的$\mathfrak{p}$-准素理想, 则$Q_1 \cap Q_2$ 也是$\mathfrak{p}$-准素理想.*

证明. 如$ab \in Q_1 \cap Q_2$, $b \notin Q_1 \cap Q_2$. 不妨设$b \notin Q_1$, 则存在$m \geq 1$, $a^m \in Q_1$, 即$a \in \sqrt{Q_1} = \mathfrak{p}$. 我们只需证明$\sqrt{Q_1 \cap Q_2} = \sqrt{Q_1} \cap \sqrt{Q_2} = \mathfrak{p}$.

一方面, $\sqrt{Q_1 \cap Q_2} \subseteq \sqrt{Q_1} \cap \sqrt{Q_2}$ 是显然的. 另一方面, 如果$a \in \sqrt{Q_1} \cap \sqrt{Q_2}$, 则存在$m, n \geq 1$, $a^m \in Q_1$, $a^n \in Q_2$, 故$a^{mn} \in Q_1 \cap Q_2$, 我们得到$\sqrt{Q_1 \cap Q_2} \supseteq \sqrt{Q_1} \cap \sqrt{Q_2}$. □

由前面的命题和引理, 我们立刻有如下定理(证明留作练习)

定理2.72. 设R 是诺特环. 则R 的每个真理想I 均有极小准素分解

$$I = \bigcap_{i=1}^{m} Q_i$$

且$\{\sqrt{Q_1}, \sqrt{Q_2}, \cdots, \sqrt{Q_m}\}$ 由I 唯一决定.

命题2.73. 设$I = Q_1 \cap \cdots \cap Q_m$ 为I 的一个准素分解, $\sqrt{Q_i} = \mathfrak{p}_i$. 则

(1) 素理想$\mathfrak{p} \supseteq I \Leftrightarrow$ 存在 i, $1 \leq i \leq m$, $\mathfrak{p} \supseteq \mathfrak{p}_i$.

(2) $\sqrt{I} = \bigcap_{i=1}^{m} \mathfrak{p}_i$.

(3) 如R 是诺特环, 则I 包含有限多个素理想的乘积.

证明. (1) 这是因为$\mathfrak{p} \supseteq I \Leftrightarrow \mathfrak{p} \supseteq Q_1 \cap \cdots \cap Q_m \Leftrightarrow \mathfrak{p} \supseteq Q_i$ 对某个 $1 \leq i \leq m$ 成立 $\Leftrightarrow \mathfrak{p} \supseteq \sqrt{Q_i} = \mathfrak{p}_i$.

(2) $\sqrt{I} = \bigcap_{\mathfrak{p} \supseteq I} \mathfrak{p} = \bigcap_{i=1}^{m} \mathfrak{p}_i$.

(3) 由于R 是诺特环, 故存在$k \geq 1$, 使得$(\bigcap_{i=1}^{m} \mathfrak{p}_i)^k \subseteq I \subseteq \bigcap_{i=1}^{m} \mathfrak{p}_i$. 因此$\mathfrak{p}_1^k \mathfrak{p}_2^k \cdots \mathfrak{p}_m^k \subseteq I$. □

§2.5 仿射代数几何初步

§2.5.1 仿射代数集

定义2.74. 设R 是交换环, A是环(可能非交换). 如$i : R \to A$ 为环同态且R 的像$i(A)$ 包含于A 的中心, 则称A 为R-**代数** (algebra) 且记$r \cdot a = a \cdot r = i(r)a$, 其中$r \in R$, $a \in A$.

如代数A 作为环在子环$i(R)$ 上是有限生成的, 则称A 是**有限生成**R**-代数**.

设A, B 是R-代数. 映射$\varphi : A \to B$ 称为R**-代数同态**是指φ 是环同态且$\varphi(ra) = r\varphi(a)$ 对所有$r \in R$ 和$a \in A$ 成立.

我们考虑域k 上的代数情况. 若A 是有限生成交换k-代数(即A 是交换环和有限生成k-代数), 由于此时i是单射, 我们视k 为A 的子环. 设$r_1, \cdots, r_n$ 生成A. 则由多项式环的泛性质, 存在环的满同态

$$\varphi : k[x_1, \cdots, x_n] \longrightarrow A,$$
$$x_i \mapsto r_i,\ a \mapsto a,\ \forall\, a \in k.$$

则φ 是k-代数满同态, 它诱导同构

$$\bar{\varphi}:\ k[x_1,\cdots,x_n]/I \xrightarrow{\sim} A,\ \text{其中}\ I=\ker\varphi.$$

由希尔伯特基定理知A 是诺特环. 我们有

命题2.75. *有限生成交换k-代数均同构于$k[x_1,\cdots,x_n]/I$ 的形式, 它是诺特环.*

定义2.76. 域k 上的n 维**仿射空间** (affine space) 是指集合

$$\mathbb{A}^n_k=\mathbb{A}^n=\{(a_1,\cdots,a_n)\mid\ a_i\in k\}.$$

它的**坐标环**(coordinate ring)

$$k[\mathbb{A}^n]=k[x_1,\cdots,x_n]$$

是k上的n元多项式环.

注意到每个n 元多项式$f(x_1,\cdots,x_n)\in k[x_1,\cdots,x_n]$ 均对应映射

$$f:\ \mathbb{A}^n\ \to k,\ (a_1,\cdots,a_n)\ \mapsto\ f(a_1,\cdots,a_n).$$

定义2.77. 设S 是环$k[x_1,\cdots,x_n]$ 的子集合. S 的**零点集**(zero locus, 零轨迹)定义为

$$\mathcal{Z}(S)=\{a\in\mathbb{A}^n\mid f(a)=0\ \text{对任意}\ f(x_1,\cdots,x_n)\in S\ \text{成立}\}.$$

如$S=\{f_1,\cdots,f_m\}$ 为有限集, 记

$$\mathcal{Z}(S)=\mathcal{Z}(f_1,\cdots,f_m).$$

如$\mathbb{A}^n$ 的子集合$V=\mathcal{Z}(S)$ 对某个$S\ \subseteq k[\mathbb{A}^n]$ 成立, 则称V 是**仿射代数集**(affine algebraic set).

例2.78. (1) $\mathcal{Z}(0)=\mathbb{A}^n$, $\mathcal{Z}(1)=\emptyset$.

(2) $\mathcal{Z}(x_1-a_1,\cdots,x_n-a_n)=\{(a_1,\cdots,a_n)\}$ 是独点集.

(3) 对于$f\in k[\mathbb{A}^n]$, $\deg f>0$, 称$\mathcal{Z}(f)$ 是$\mathbb{A}^n$ 上的**超曲面**(hypersurface).

(4) 如$n=1$, 则$\mathcal{Z}(f)$ 是f 在k 中的零点的集合. 如$f\neq 0$, 则$\mathcal{Z}(f)$ 是有限集. 故$\mathbb{A}^1$ 中的仿射代数集包括三种形式: 空集$\emptyset$, 有限点集及全集合$k=\mathbb{A}^1$.

命题2.79. *仿射代数集有如下性质;*

(1) *如$S\subseteq T$, 则$\mathcal{Z}(S)\supseteq\mathcal{Z}(T)$.*

(2) *令$\langle S\rangle$ 为$k[\mathbb{A}^n]$ 中由S 生成的理想, 则$\langle S\rangle=\langle f_1,\cdots,f_m\rangle$, $\mathcal{Z}(S)=\mathcal{Z}(\langle S\rangle)=\mathcal{Z}(f_1,\cdots,f_m)$.*

(3) *任意多个仿射代数集之交是仿射代数集: 如$(S_i)_{i\in I}$ 是$\mathbb{A}^n$ 的子集合族, 则$\bigcap\limits_{i\in I}\mathcal{Z}(S_i)=\mathcal{Z}(\bigcup\limits_{i\in I}S_i)$ 还是仿射代数集.*

(4) *若I,J 是$k[\mathbb{A}^n]$ 中的理想, 则$\mathcal{Z}(I)\cup\mathcal{Z}(J)=\mathcal{Z}(IJ)$. 故有限多个仿射代数集之并还是仿射代数集.*

(5) *$\mathcal{Z}(0)=\mathbb{A}^n$ 及$\mathcal{Z}(1)=\emptyset$ 是仿射代数集.*

由性质(2), 我们有映射

$$\mathcal{Z}:\ \{k[\mathbb{A}^n]\text{ 中的理想}\}\ \longrightarrow\ \{\mathbb{A}^n\text{ 上的仿射代数集}\}$$
$$I\ \longmapsto\ \mathcal{Z}(I).$$

如$I=\langle f_1,\cdots,f_m\rangle$, 则 $\mathcal{Z}(I)=\mathcal{Z}(f_1,\cdots,f_m)=\mathcal{Z}(f_1)\cap\cdots\cap\mathcal{Z}(f_m)$.

反过来, 设A 是$\mathbb{A}^n$ 的子集. 令

$$\mathcal{I}(A)=\{f\in k[\mathbb{A}^n]\mid f(a)=0\text{ 对任意 }a\in A\text{ 成立}\}.$$

则$\mathcal{I}(A)$ 是$k[\mathbb{A}^n]$ 中的理想, 且是在A 上取值为0 的所有理想的极大元, 称为A的**化零理想**.

命题2.80. 映射

$$\mathcal{I}:\ \{\mathbb{A}^n\text{ 中的子集合}\}\ \longrightarrow\ \{k[\mathbb{A}^n]\text{ 中的理想}\}$$
$$A\ \longmapsto\ \mathcal{I}(A)$$

满足条件:

(1) $\mathcal{I}(A)$ 是根式理想.

(2) 如$A\subseteq B$, 则$\mathcal{I}(A)\supseteq\mathcal{I}(B)$.

(3) $\mathcal{I}(A\cup B)=\mathcal{I}(A)\cap\mathcal{I}(B)$.

(4) $\mathcal{I}(\emptyset)=k[\mathbb{A}^n]$, 且如$k$ 是无限域, 则$\mathcal{I}(\mathbb{A}^n)=0$.

更进一步地, 映射$\mathcal{Z}$ 与$\mathcal{I}$ 有如下联系

(i) 如I 是理想, 则$I\subseteq\mathcal{I}(\mathcal{Z}(I))$; 如$A\subseteq\mathbb{A}^n$, 则$A\subseteq\mathcal{Z}(\mathcal{I}(A))$.

(ii) 如$V=\mathcal{Z}(I)$ 是仿射代数集, 则$V=\mathcal{Z}(\mathcal{I}(V))$.

证明. 只证(ii). $V\subseteq\mathcal{Z}(\mathcal{I}(V))$ 由定义立知. 反之, 由$I\subseteq\mathcal{I}(\mathcal{Z}(I))$ 知$\mathcal{Z}(I)\supseteq\mathcal{Z}(I\mathcal{Z}(I))$, 故$V\supseteq\mathcal{Z}(\mathcal{I}(V))$. □

定义2.81. 仿射空间$\mathbb{A}^n$ 里的仿射代数集V 的**坐标环** $k[V]$ 定义为商环$k[\mathbb{A}^n]/\mathcal{I}(V)$.

注记. 如k 是无限域, $V=\mathbb{A}^n$, 则$\mathcal{I}(V)=0$. 则上述定义与前述定义是一致的.

我们注意到

(1) 对于$f\in k[\mathbb{A}^n]$, 考虑映射

$$f:\ \mathbb{A}^n\ \longrightarrow\ k$$

在V 上的限制$f|_V$. 则 $f|_V=g|_V$ 当且仅当$f-g\ \in\mathcal{I}(V)$. 故对任意$\bar{f}\in k[V]$, 令 $f\in k[\mathbb{A}^n]$ 为它的一个原像, 映射

$$\bar{f}:\ V\ \longrightarrow\ k,\ a\ \mapsto\ f(a)$$

是定义良好的映射.

(2) $k[V]$ 是有限生成 k-代数, 因此是诺特环.

定义2.82. 设$V \subseteq \mathbb{A}^n$ 和$W \subseteq \mathbb{A}^m$ 为仿射代数集. 如存在多项式$\varphi_1, \cdots, \varphi_m \in k[x_1, \cdots, x_n]$ 使得映射$\varphi: V \to W$ 满足等式

$$\varphi(a) = (\varphi_1(a), \varphi_2(a), \cdots, \varphi_m(a))$$

对所有$a = (a_1, \cdots, a_n) \in V$ 成立, 称φ 为代数集V 到W 的**态射**.

态射$\varphi: V \to W$ 称为**同构**, 是指存在态射$\psi: W \to V$ 使得$\varphi \circ \psi = 1_W$ 且$\psi \circ \varphi = 1_V$.

注记. 对于态射φ, 多项式$\varphi_1, \cdots, \varphi_m$ 不是唯一确定的.

设$\varphi: V \to W$ 是态射. 定义

$$\begin{aligned} \tilde{\varphi}: k[W] &\longrightarrow k[V], \\ f + \mathcal{I}(W) &\longmapsto f(\varphi_1, \cdots, \varphi_m) + \mathcal{I}(V). \end{aligned}$$

我们证明$\tilde{\varphi}$ 是定义良好的k-代数同态. 如

$$f_1 = f_2 \bmod \mathcal{I}(W), \text{ 则 } F = f_1 - f_2 \in \mathcal{I}(W)$$

故$F(\varphi_1, \cdots, \varphi_m) \in \mathcal{I}(V)$, 即$\tilde{\varphi}$ 是良定义的. 至于$\tilde{\varphi}$ 是k-代数同态容易证明.

反过来, 设 $\Phi: k[W] \to k[V]$ 是k-代数同态. 设

$$\Phi(x_i + \mathcal{I}(W)) = F_i(x_1, \cdots, x_n) + \mathcal{I}(V), \text{ 其中 } 1 \leq i \leq m.$$

如$g(x_1, \cdots, x_m) \in \mathcal{I}(W)$, 则$\Phi(g(x_1, \cdots, x_m) + \mathcal{I}(W)) = g(F_1, \cdots, F_m) \in \mathcal{I}(V)$. 若$(a_1, \cdots, a_n) \in V$, 则$g(F_1(a), \cdots, F_m(a)) = 0$. 所以

$$(F_1(a), \cdots, F_m(a)) \in \mathcal{Z}(\mathcal{I}(W)) = W.$$

这样$\varphi: V \to W$, $a = (a_1, \cdots, a_n) \mapsto (F_1(a), \cdots, F_m(a))$ 是V 到W 的态射. 它与F_i 的选取无关且$\tilde{\varphi} = \Phi$.

总结一下上面的讨论, 即有如下定理.

定理2.83. 设$V \subseteq \mathbb{A}^n$ 和$W \subseteq \mathbb{A}^m$ 为仿射代数集. 则存在一一对应

$$\begin{aligned} \{V \text{ 到 } W \text{ 的态射}\} &\to \{k[W] \text{ 到 } k[V] \text{ 的} k\text{-代数同态}\} \\ \varphi &\mapsto \tilde{\varphi}, \end{aligned}$$

满足如下条件:

(1) 对任意k-代数同态 $\Phi: k[W] \to k[V]$, 存在唯一态射$\varphi: V \to W$ 使得$\Phi = \tilde{\varphi}$.

(2) $\widetilde{\psi \circ \varphi} = \tilde{\varphi} \circ \tilde{\psi}$.

(3) φ 是同构当且仅当 $\tilde{\varphi}$ 是同构.

§2.5.2 希尔伯特零点定理

希尔伯特零点定理(Hilbert's Nullstellensatz) 是交换代数一个伟大定理.

定理2.84 (希尔伯特零点定理). *设k 是代数封闭域. 则*

$$\mathcal{I}(\mathcal{Z}(I)) = \sqrt{I}$$

对所有理想$I \subseteq k[x_1, \cdots, x_n]$ 成立. 故$\mathcal{I}$ 与$\mathcal{Z}$ 给出互逆的一一对应:

$$\{\mathbb{A}^n\text{中的仿射代数集}\} \underset{\mathcal{Z}}{\overset{\mathcal{I}}{\rightleftarrows}} \{k[\mathbb{A}^n]\text{中的根式理想}\}.$$

特别地, 如I 是$k[\mathbb{A}^n]$ 的真理想, 则$\mathcal{Z}(I)$ 非空.

为证明此定理, 我们先证明如下的诺特正规化引理(Noether's Normalization Lemma)

定理2.85 (诺特正规化引理). *设k 是域, $A = k[r_1, \cdots, r_m]$ 是有限生成k-代数, 则存在整数q, $0 \leq q \leq m$, 以及元素$y_1, \cdots, y_q \in A$, 它们在k上代数独立, 使得A 在$k[y_1, \cdots, y_q]$ 上整.*

证明. 我们对m 作归纳. 当$m = 1$ 时定理是显然的.

对于一般的m, 如$r_1, \cdots, r_m$ 代数独立, 令$q = m$, $y_i = r_i$ $(i = 1, \cdots, m)$ 即可.

否则, 存在多项式$f(x_1, \cdots, x_m) \in k[x_1, \cdots, x_m]$, 次数$\deg f = d > 0$ 使得$f(r_1, \cdots, r_m) = 0$. 我们不妨假设f 是系数在$k[x_1, \cdots, x_{m-1}]$ 中关于未定元x_m 的非常值多项式.

对于$1 \leq i \leq m-1$, 令

$$\alpha_i = (1+d)^i, \ X_i = x_i - x_m^{\alpha_i}.$$

则

$$\begin{aligned} g(X_1, \cdots, X_{m-1}, x_m) &= f(X_1 + x_m^{\alpha_1}, \cdots, X_{m-1} + x_m^{\alpha_{m-1}}, x_m) \\ &\in k[X_1, \cdots, X_{m-1}, x_m] \end{aligned}$$

可以写成

$$cx_m^N + \sum_{i=0}^{N-1} h_i(X_1, \cdots, X_{m-1}) x_m^i$$

的形式, 其中$c \in k$, $c \neq 0$. 令$s_i = r_i - r_m^{\alpha_i}$, 则

$$\frac{1}{c} g(s_1, \cdots, s_{m-1}, r_m) = \frac{1}{c} f(r_1, \cdots, r_m) = 0.$$

故r_m 在环$B = k[s_1, \cdots, s_{m-1}]$ 上整. 又由于$r_1, \cdots, r_{m-1}$ 在$B[r_m]$ 上整, 故A 在B 上整. 由于B 是由 $m-1$ 个元素生成的$k-$代数, 由归纳假设以及整性的传递性, 定理得证. □

定理2.86 (希尔伯特零点定理的弱形式)**.** 设k 是代数封闭域. 理想$\mathfrak{m}$ 是多项式环$k[x_1,\cdots,x_m]$ 的极大理想当且仅当$\mathfrak{m}=(x_1-a_1,\cdots x_n-a_n)$. 特别地, 如$I$ 是 $k[x_1,\cdots,x_n]$ 的真理想, 则$\mathcal{Z}(I)$ 非空.

证明. $\Leftarrow$ 满同态$k[x_1,\cdots,x_n]\to k$, $f(x_1,\cdots,x_n)\mapsto f(a_1,\cdots,a_n)$ 的核是$\mathfrak{m}$. 故$\mathfrak{m}$ 是极大理想.

$\Rightarrow$ 如$\mathfrak{m}$ 是极大理想, 令$E=k[x_1,\cdots,x_n]/\mathfrak{m}=k[\tilde{x_1},\cdots,\tilde{x_n}]$. 这是有限生成$k-$代数, 故由诺特正规化引理, E 在多项式环$k[y_1,\cdots,y_q]$ 上整. 由E 是域, 故$k[y_1,\cdots,y_q]$ 也是域. 故$q=0$, E 在代数封闭域上整, 故$E=k$. 这就是说$\tilde{x_i}=a_i\in k$, 即$x_i-a_i\in\mathfrak{m}$ $(i=1,\cdots,m)$. 故$\mathfrak{m}=(x_1-a_1,\cdots,x_n-a_n)$.

如I 是$k[x_1,\cdots,x_n]$ 上的真理想. 设$\mathfrak{m}\supseteq I$ 是极大理想. 则$\mathfrak{m}=(x_1-a_1,\cdots,x_n-a_n)$, $(a_1,\cdots,a_n)\in\mathcal{Z}(I)\neq\emptyset$. □

希尔伯特零点定理的证明. 设$I=(f_1,\cdots,f_m)$, $g\in\mathcal{I}(\mathcal{Z}(I))$. 令$I'$ 是多项式环$k[x_1,\cdots,x_n,x_{n+1}]$ 中由$\{f_1,\cdots,f_m,x_{n+1}g-1\}$生成的理想. 则$\mathcal{Z}(I')=\emptyset$. 故由希尔伯特零点定理的弱形式, $1\in I'$, 即存在$a_i=a_i(x_1,\cdots,x_{n+1})$ $(i=1,\cdots,m+1)$, 使得

$$1=a_1f_1+\cdots+a_mf_m+a_{m+1}(x_{n+1}g-1).$$

令$y=\frac{1}{x_{n+1}}$, 则存在N 使得

$$y^N=c_1f_1+\cdots+c_mf_m+c_{m+1}(g-y),\ c_i\in k[x_1,\cdots,x_n,y]\ (i=1,\cdots,m+1).$$

取$y=g$ 代入上述恒等式. 则有$g^N=y^N\in I$, 故$g\in\sqrt{I}$. □

§2.5.3 仿射代数集上的拓扑

设X 为集合. 回忆一下X 上的**拓扑**是指X 的一些子集构成的集合族T, 其元素称为**闭集**, 满足如下公理:

(1) $X\in T$, $\emptyset\in T$. 即全集X 与空集$\emptyset$ 均是闭集.

(2) 闭集的任意交还是闭集. 即若$\{X_i\}_{i\in I}\subseteq T$, 则$\bigcap\limits_{i\in I}X_i\in T$.

(3) 闭集的有限并是闭集. 即若$\{X_i\}_{i=1}^n\subseteq T$, 则$\bigcup\limits_{i=1}^nX_i\in T$.

此时, X 称为**拓扑空间**.

闭集的余集称为**开集**. 故开集满足公理:

(1′) X 与 $\emptyset$ 是开集.

(2′) 开集的任意并是开集.

(3′) 开集的有限交是开集.

由仿射代数集的性质, 它满足闭集的三个条件.

定义2.87. 仿射空间$\mathbb{A}^n$ 以其上仿射代数集作为闭集决定的拓扑称为$\mathbb{A}^n$ 上的**扎里斯基拓扑** (Zariski topology).

例2.88. 如$n=1$, $\mathbb{A}^1=k$ 的扎里斯基 拓扑即是说除去全空间k 外, 其余闭集均是有限集. 这与通常所谓的有限补空间一致. 如$k=\mathbb{R}$ 或$\mathbb{C}$, 它的扎里斯基拓扑比我们在分析中学习到的欧氏距离空间拓扑要粗糙得多. 如k 是无限集, 则k 的扎里斯基 拓扑总是T_1 的但不是T_2 (豪斯多夫) 的.

定义2.89. 设V 是非空仿射代数集. 如对于$V=V_1\cup V_2$, 其中V_1, V_2 为仿射代数集, 必有$V=V_1$ 或$V=V_2$ 成立, 我们称V 是**不可约**的, 否则称V 是**可约**的. 不可约仿射代数集称为**仿射簇**.

命题2.90. *设V 是非空仿射代数集.*

(1) *V 不可约当且仅当$\mathcal{I}(V)$ 是素理想. 换言之, V 是代数簇当且仅当其坐标环$k[V]$ 是整环.*

(2) *V 可以唯一表示成如下形式;*

$$V=V_1\cup V_2\cup\cdots\cup V_q$$

其中V_i 不可约且$V_i\not\subseteq V_j$ 对于任意$j\neq i$ 成立.

证明. (1) 设$I=\mathcal{I}(V)$. 如 $V=V_1\cup V_2$ 是可约的, 可设V_1 与V_2 均是V 的真闭子集. 由于$V_i\neq V$. 故存在$f_i\in\mathcal{I}(V_i)-I$, 但f_1f_2 在$V_1\cup V_2=V$ 上取值为0. 故$f_1f_2\in I$. 即I 不是素理想. 反之, 若I 不是素理想, 则存在$f_1f_2\in k[x_1,\cdots,x_n]$, 且$f_1$ 和$f_2\notin I$. 令$V_1=\mathcal{Z}(f_1)\cap V$, $V_2=\mathcal{Z}(f_2)\cap V$. 则 $V=V_1\cup V_2$ 且 $V_i\neq V$, 即V 可约.

(2) 设S 是由所有不能写为不可约代数集有限并的非空代数集构成的集合族. 假设$S\neq\emptyset$. 由于$k[\mathbb{A}^n]$ 是诺特环, 集合$\{\mathcal{I}(V)\mid V\in S\}$ 有最大元I_0, 故$V_0=\mathcal{Z}(I_0)$ 是S 中的极小元. 由于$V_0\in S$, 故 V_0 是可约的, 即有$V_0=V_1\cup V_2$, V_1 与V_2 是V_0 的真闭子集. 但由V_0 的极小性, V_1 与V_2 不在S 中, 故均是有限多不可约代数集之并. 所以V_0 也是有限多不可约代数集之并, 即$V_0\notin S$. 矛盾. 所以$S=\emptyset$, 即任意代数集均是不可约代数集的有限并.

要证唯一性. 设

$$V=V_1\cup V_2\cup\cdots\cup V_r=U_1\cup U_2\cup\cdots\cup U_s$$

为 V 的两个分解, V_i, U_j 不可约, 且$V_i\not\subseteq V_{i'}$, $U_j\not\subseteq U_{j'}$ $(i,i'=1,\cdots,r,$ $j,j'=1,\cdots,s)$. 则

$$V_1=V_1\cap V=(V_1\cap U_1)\cup\cdots\cup(V_1\cap U_s).$$

由V_1 的不可约性知, 存在j, 使得$V_1=V_1\cap U_j$. 即$V_1\subseteq U_j$. 同样可知, 对U_j 存在i', 使得$U_j\subseteq V_{i'}$ 对某个i' 成立. 所以$V_1\subseteq U_j\subseteq V_{i'}$, 故$i'=1$ 且$V_1=U_j$. 同样道理有$V_i=U_{\sigma(i)}$ 对某个$1\leq\sigma(i)\leq s$ 成立. 故$r=s$ 且$\{V_1,\cdots,V_r\}=\{U_1,\cdots,U_s\}$. □

§2.5.4 交换环素谱上的拓扑

设R 是含幺交换环. 回忆一下Spec R 是R 的素谱, 即R 中所有素理想的集合, Max $R \subseteq$ Spec R 是R 的极大谱, 即R 中极大理想的集合.

例2.91. 设k 是域.

(1) Spec k = Max $k = \{0\}$.

(2) Spec $\mathbb{Z} = \{(0)\} \cup$ Max $\mathbb{Z} = \{(0)\} \cup \{p\mathbb{Z} \mid p$ 是素数$\}$.

(3) Spec $k[x] = \{(0)\} \cup$ Max $k[x] = \{0\} \cup \{(f) \mid f \in k[x],$ 首一不可约$\}$.

(4) Spec $\mathbb{Z}[x]$ 由如下四类素理想组成:

(i) 零理想(0).

(ii) (p), 其中p 为素数.

(iii) (f), 其中$f(x)$ 在$\mathbb{Z}[x]$ 上不可约($\Leftrightarrow f$本原且在 $\mathbb{Q}[x]$ 上不可约).

(iv) 极大理想(p, g), 其中p 为素数, $g(x) \in \mathbb{Z}[x]$ 为首一多项式且$g \mod p$ 在$\mathbb{F}_p[x]$ 中不可约.

定义2.92. 设$f \in R$, $\mathfrak{p} \in$ Spec R. 则f 在点$\mathfrak{p}$ 处的值为$f(\mathfrak{p}) = f \bmod \mathfrak{p} \in R/\mathfrak{p}$. 故$f(\mathfrak{p}) = 0 \Leftrightarrow f \in \mathfrak{p}$.

定义2.93. 设A 是R 的子集. A的**零点集**定义为素谱Spec$R$ 的子集

$$\begin{aligned}\mathcal{Z}(A) &= \{\mathfrak{p} \in \text{Spec } R \mid A \subseteq \mathfrak{p}\} \\ &= \{\mathfrak{p} \in \text{Spec } R \mid a(\mathfrak{p}) = 0 \text{ 对任意 } a \in A \text{ 成立}\}.\end{aligned}$$

设Y 是Spec R 的子集. Y的**化零理想** 定义为环R 的理想

$$\mathcal{I}(Y) = \bigcap_{\mathfrak{p} \in Y} \mathfrak{p} = \{a \in R \mid a(\mathfrak{p}) = 0 \text{ 对任意 } \mathfrak{p} \in Y \text{ 成立}\}.$$

由于$\mathcal{Z}(A) = \mathcal{Z}(\langle A \rangle)$, 我们下面只需考虑$A = I$ 是R 的理想的情形.

命题2.94. 映射$\mathcal{Z}$ 与$\mathcal{I}$ 满足如下性质

(1) 对R 的理想I, $\mathcal{Z}(I) = \mathcal{Z}(\sqrt{I})$ 而$\mathcal{I}(\mathcal{Z}(I)) = \sqrt{I}$.

(2) 对任意理想I, J 有$\mathcal{Z}(I \cap J) = \mathcal{Z}(IJ) = \mathcal{Z}(I) \cup \mathcal{Z}(J)$.

(3) $\mathcal{Z}(\bigcup\limits_j I_j) = \bigcap\limits_j \mathcal{Z}(I_j)$.

证明. (1) 如$\mathfrak{p} \supseteq I$, 则$\mathfrak{p} \supseteq \sqrt{I}$. 故$\mathcal{Z}(I) = \mathcal{Z}(\sqrt{I})$. 类似地, $\mathcal{I}(\mathcal{Z}(I)) = \bigcap\limits_{\mathfrak{p} \in \mathcal{Z}(I)} \mathfrak{p} = \bigcap\limits_{I \subseteq \mathfrak{p}} \mathfrak{p} = \sqrt{I}$.

(2) $\mathcal{Z}(I \cap J) = \mathcal{Z}(I) \cup \mathcal{Z}(J)$ 显然. 如$\mathfrak{p} \supseteq IJ$, 则$\mathfrak{p} \supseteq I$ 或$\mathfrak{p} \supseteq J$. 故$\mathcal{Z}(IJ) = \mathcal{Z}(I) \cup \mathcal{Z}(J)$.

(3) 易验证. □

由上述命题

$$T = \{\mathcal{Z}(I) \mid I\text{为 } R\text{中理想}\}$$

满足Spec R 中拓扑闭集三公理.

定义2.95. 以$\mathcal{Z}(I)$ 作为闭集定义的拓扑称为Spec R 上的**扎里斯基拓扑**.

由定义, 如独点集$\{\mathfrak{p}\}$ 是Spec R 的闭集, 则

$$\{\mathfrak{p}\} = \overline{\{\mathfrak{p}\}} = \bigcap_{I:\ \mathfrak{p}\in\mathcal{Z}(I)} \mathcal{Z}(I) = \{\mathfrak{q} \in \text{Spec } R \mid \mathfrak{q} \supseteq \mathfrak{p}\}.$$

故$\{\mathfrak{p}\}$ 是闭集当且仅当$\mathfrak{p} \in \text{Max } R$ 是极大理想, 即Max R 是Spec R 中的闭点构成的集合.

同样, 可以定义Spec R 上的不可约闭集: Y不可约 $\Leftrightarrow$ 若$Y = Y_1 \cup Y_2$. 则$Y = Y_1$ 或$Y = Y_2$. 可以证明$Y = \mathcal{Z}(I)$ 不可约当且仅当$\mathcal{I}(Y) = \sqrt{I}$ 是素理想.

命题2.96. *映射$\mathcal{I}$ 与$\mathcal{Z}$ 定义互逆双射*

$$\{\text{Spec } R\text{中的扎里斯基闭子集}\} \underset{\mathcal{Z}}{\overset{\mathcal{I}}{\rightleftarrows}} \{R\text{中的根式理想}\}.$$

*此对应将*Spec R *中的闭点集对应到*R *中的极大理想,* Spec R *中的不可约闭集对应到*R *中的素理想.*

§2.6 格罗布纳基

设k是域, I是多项式环$k[X] := k[x_1, \cdots, x_n]$ 中的理想. 由希尔伯特基定理, $k[X]$ 是诺特环, 故I 是有限生成的. 那么如何寻找I 的一组合适的生成元呢? 布赫伯格(Buchberger) 发明一种算法, 得到I的一组合适生成元, 即它的格罗布纳基, 并由此回答如下问题:

(1) 判断多项式$h(X)$ 是否在I 中.

(2) 判断多项式$g(X)$ 是否在$\sqrt{I}$ 中.

(3) 判断两个理想是否相等.

格罗布纳基在计算数学领域有巨大应用. 在本节, 我们将介绍布赫伯格的理论.

§2.6.1 域上多元多项式环上的带余除法

在本节, 我们总是假设$I = (f_1, \cdots, f_r)$ 是n 元多项式环$k[X] = k[x_1, \cdots, x_n]$ 的理想.

多项式环$k[X]$ 中的单项式可以记为$X^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, 其中$\alpha = (\alpha_1, \cdots \alpha_n) \in \mathbb{N}^n$, α 的**权** $|\alpha| = \alpha_1 + \cdots + \alpha_n$. 注意到$\mathbb{N}^n$ 是加法含幺半群,单项式的乘法与$\mathbb{N}^n$ 加法相容:

$$X^\alpha X^\beta = X^{\alpha+\beta}.$$

定义2.97. 集合S称为**偏序集**(partially ordered set)是指S上有二元关系$\leq$满足自反性, 反对称性和传递性, 此时关系$\leq$称为**偏序**(partial order). 我们称$x < y$或$y > x$如$x \leq y$且$x \neq y$, 称$x \geq y$如$y \leq x$.

偏序集称为**良序集**(well ordered set)是指它的非空子集均有最小元.

定义2.98. 集合$\mathbb{N}^n$中的偏序$\leq$若是良序且与$\mathbb{N}^n$的加法相容, 即

$$\alpha \leq \beta \ \Rightarrow \alpha + \gamma \leq \beta + \gamma, \text{ 对任意 } \gamma \text{ 成立.}$$

则称此序为**单项式序**(monomial order).

定义2.99. 给定$\mathbb{N}^n$中的单项式序. 对于$0 \neq f(X) = f(x_1, \cdots, x_n) \in k[X]$, 则

$$f(X) = c_\alpha X^\alpha + \sum_{\beta < \alpha} c_\beta X^\beta.$$

我们称$\mathrm{LT}(f) = c_\alpha X^\alpha$是$f$的**首项**, $\mathrm{Deg}\, f = \alpha$是$f$的**次数**. 如$\mathrm{LT}(f) = X^\alpha$, 则称$f(X)$是首一多项式.

定义2.100. 集合$\mathbb{N}^n$的**字典序**(lexicographic order)是指如下定义的偏序:

$$\alpha \leq_{\mathrm{lex}} \beta \text{ 如 } \alpha = \beta \text{ 或} \beta - \alpha \text{ 的第一个非零分量为正.}$$

命题2.101. *字典序是单项式序.*

证明. 要证字典序满足:

(i) 自反性, 反对称性和传递性.

(ii) 良序性.

(iii) 单项式序条件.

这里(i) 和(iii) 都是很显然的. 对于(ii), 令$S \subseteq \mathbb{N}^n$为非空集. 令

$$\begin{aligned} \delta_1 &= \min\{\alpha_1 \mid \alpha = (\alpha_1, \cdots, \alpha_n) \in S\}, \\ C_1 &= \min\{\alpha \in S \mid \alpha_1 = \delta_1\}. \end{aligned}$$

归纳定义

$$\begin{aligned} \delta_i &= \min\{\alpha_i \mid \alpha \in C_{i-1}\}, \\ C_i &= \min\{\alpha \in C_{i-1} \mid \alpha_i = \delta_i\}. \end{aligned}$$

则$(\delta_1, \delta_2, \cdots, \delta_n)$是$S$中的最小元. □

下面这两个命题是显然的:

命题2.102. *设$\leq$是$\mathbb{N}^n$的一个单项式序. 对于多项式$f(X)$, $g(X) \in k[X]$, 如$f(X)$中存在单项式$c_\beta X^\beta$, 使得$\mathrm{LT}(g) \mid c_\beta X^\beta$, 令*

$$h(X) = f(X) - \frac{c_\beta X^\beta}{\mathrm{LT}(g)} g(X).$$

则

(1) 如$\beta = \mathrm{Deg}\, f$, 则$h(X) = 0$ 或$\mathrm{Deg}\, h < \mathrm{Deg}\, f$.

(2) 如$\beta < \mathrm{Deg}\, f$, 则$\mathrm{Deg}\, h = \mathrm{Deg}\, f$ 且$\mathrm{LT}(h) = \mathrm{LT}(f)$.

命题2.103. 设$\leq$ 为$\mathbb{N}^n$ 的一个单项式序, $\mathrm{Deg}\, f \in \mathbb{N}^n$. 则

(1) 如$\mathrm{Deg}\, f = \mathrm{Deg}\, g$, 则$\mathrm{LT}(f) = c\mathrm{LT}(g)$, $c \in k$, $c \neq 0$.

(2) $\mathrm{LT}(hg) = \mathrm{LT}(h)\mathrm{LT}(g)$, 故$\mathrm{Deg}\,(fg) = \mathrm{Deg}\, f + \mathrm{Deg}\, g$.

(3) 如$\mathrm{Deg}\, f = \mathrm{Deg}\,(hg)$, 则$\mathrm{LT}(g) \mid \mathrm{LT}(f)$.

(4) $\mathrm{Deg}\,(f+g) \leq \max(\mathrm{Deg}\, f, \mathrm{Deg}\, g)$.

定义2.104. 集合$\mathbb{N}^n$ 上的**次数-字典序** (degree-lexicographic order) 是指序$\leq_{\mathrm{dlex}}$, 对于α, $\beta \in \mathbb{N}^n$, $\alpha \leq_{\mathrm{dlex}} \beta$ 当且仅当下列三情形之一成立:

(1) $\alpha = \beta$;

(2) $|\alpha| < |\beta|$;

(3) $|\alpha| = |\beta|$ 但$\alpha \leq_{\mathrm{lex}} \beta$.

换言之,

$$\alpha >_{\mathrm{dlex}} \beta \Leftrightarrow |\alpha| > |\beta|, \text{ 或 } |\alpha| = |\beta| \text{ 且 } \alpha >_{\mathrm{lex}} \beta.$$

命题2.105. 次数-字典序$\leq_{\mathrm{dlex}}$ 是$\mathbb{N}^n$ 上的单项式序.

证明. 显然. 留作练习. □

定义2.106. 设$\{g_1, \cdots, g_m\} \subseteq k[X]$. 多项式$r(X) \in k[X]$ 称为模$\{g_1, \cdots, g_m\}$ 是**约化的**(reduced)是指$r(X)$ 或者等于0 或者它中间不存在被某个$\mathrm{LT}(g_i)$ 整除的非零项.

定理2.107 (多元多项式环上的带余除法)**.** 设$\leq$ 是$\mathbb{N}^n$ 的一个单项式序. 对于$f(X) \in k[X]$, $G = [g_1, \cdots, g_m]$ 为$k[X]$ 中m 元多项式组, 则存在算法, 给出$r(X)$, $a_1(X), \cdots, a_m(X) \in k[X]$,

$$f = a_1 g_1 + a_2 g_2 + \cdots + a_m g_m + r,$$

使得

(1) $r(X)$ 模$\{g_1, \cdots, g_m\}$ 是约化的.

(2) $\mathrm{Deg}\,(a_i g_i) \leq \mathrm{Deg}\, f$ 对任意$1 \leq i \leq m$ 成立.

证明. 我们的算法如下:

输入 $f(X) = \sum_{\beta} c_\beta X^\beta$, $G = [g_1, \cdots, g_m]$.

输出 r, a_1, $\cdots, a_m$.

(1) 设$r = f$, $a_i = 0$.

(2) 如r 模$\{g_1,\cdots,g_m\}$ 不是约化的. 则找到最小的i 使得$\mathrm{LT}(g_i)\mid c_\beta X^\beta$ 对$r(X)$ 某单项式成立. 令

$$r := r - \frac{c_\beta X^\beta}{\mathrm{LT}(g_i)} g_i,$$
$$a_i := a_i + \frac{c_\beta X^\beta}{\mathrm{LT}(g_i)},\ a_j := a_j,\ \text{如}j \neq i.$$

然后循环.

我们须证明上述算法一定会在有限步终止. 对于$f(X)\in k[X]$, $f(X)\neq 0$. 则$f(X)=c_\alpha X^\alpha + c_\beta X^\beta + c_\gamma X^\gamma + \cdots$, $\alpha>\beta>\gamma>\cdots$. 记$W(f)=\alpha\beta\gamma\cdots$, 它是以$\mathbb{N}^n$ 为字母表的一个字. 令$W(\mathbb{N}^n)$ 是以$\mathbb{N}^n$ 为字母表的字的集合. 并采用字典序$\leq_{\mathrm{lex}}$. 则$\leq_{\mathrm{lex}}$ 是$W(\mathbb{N}^n)$ 的一个良序. 如$r(X)$ 中有非零项$c_\beta X^\beta$, 使得$\mathrm{LT}(g_i)\mid c_\beta X^\beta$. 我们有$W(r) > W\big(r - \frac{c_\beta X^\beta}{\mathrm{LT}(g_i)} g_i\big)$. 故每经过一次循环$W(r)$ 必降低. 如得到的$W(r) < \min\limits_{1\leq i\leq m}\{W(\mathrm{LT}(g_i))\}$, 则$r$ 必是约化的. 而从$W(f)$ 到$\min\limits_{1\leq i\leq m}\{W(\mathrm{LT}(g_i))\}$ 之间只有有限步.

由算法给出的r 自然是模$\{g_1,\cdots,g_m\}$ 约化的, 而每个a_i 是形如$\frac{c_\beta X^\beta}{\mathrm{LT}(g_i)}$ 的单项式之和. 故$\mathrm{Deg}\,(a_i g_i)\leq \mathrm{Deg}\, f$. □

注记. 上述算法给出的$r(X)$ 与$g_1,\cdots,g_m$ 的次序有关, 即是由n 元有序组$G=[g_1,\cdots,g_m]$ 决定, 我们称之为$f(X)$ **模**G **的余数**.

例2.108. 设在多项式环$k[x,y,z]$ 中$z<y<x$ 并采用次数- 字典序. 设$f(x,y,z)=x^2y^2+xy$, $g_1=y^2+z^2$, $g_2=x^2y+yz$, $g_3=z^3+xy$. 则对于$G=[g_1,g_2,g_3]$, $r=-x^2z^2+xy$; 而对于$G=[g_2,g_1,g_3]$, $r=0$.

§2.6.2 格罗布纳基和布赫伯格算法

定义2.109. 设I是$k[X]$的理想. $\{g_1,\cdots,g_m\}$ 称为I 的**格罗布纳基**(Gröbner basis)是指$\{g_1,\cdots,g_m\}$ 生成I, 且对任意$f\in I$, 存在i, 使得$\mathrm{LT}(g_i)\mid \mathrm{LT}(f)$.

例2.110. 继续讨论例 2.108的理想I. 由例 2.108可知$r(x,y,z)=-x^2z^2+xy\in I$, 但$\mathrm{LT}(r)=-x^2z^2$ 不整除$\mathrm{LT}(g_1)=y^2$, $\mathrm{LT}(g_2)=x^2y$ 和$\mathrm{LT}(g_3)=z^3$, 故由定义知$\{g_1=y^2+z^2, g_2=x^2y+yz, g_3=z^3+xy\}$ 不是$I=(g_1,g_2,g_3)$ 的格罗布纳基. 当然, 由例 2.108的计算和下面的命题也可得出这个结论.

命题2.111. *集合$\{g_1,\cdots,g_m\}$ 是$I=(g_1,\cdots,g_m)$ 的格罗布纳基当且仅当对任意$\sigma\in S_m$, 对任意$f\in I$, f 模$G_\sigma=[g_{\sigma(1)},\cdots,g_{\sigma m}]$ 的余数$r_\sigma=0$.*

证明. 若对$\sigma\in S_m$, 存在$f\in I$, f 模G_σ 的余数不等于0. 取满足这样条件且次数最低的f. 若$\{g_1,\cdots,g_m\}$ 是I 的格罗布纳基, 存在i, $\mathrm{LT}(g_i)\mid \mathrm{LT}(f)$. 取最小的$i$ 使得$\mathrm{LT}(g_{\sigma(i)})\mid \mathrm{LT}(f)$. 则$h=f-\frac{\mathrm{LT}(f)}{\mathrm{LT}(g_{\sigma(i)})}\mathrm{LT}(g_{\sigma(i)})$ 是求f 模$G_{\sigma(i)}$余数的算法的第一步, 故f 模G_σ 的余数等于$h \bmod G_\sigma$ 的余数. 但$\mathrm{Deg}\, h < \mathrm{Deg}\, f$,

由f的次数最低性, $h \bmod G_\sigma$ 的余数等于0, 矛盾. 故$\{g_1, \cdots, g_m\}$ 不是I 的格罗布纳基.

反之, 若对任意$\sigma \in S_m$, f 模G_σ 的余数$r_\sigma = 0$, 但$\{g_1, \cdots, g_m\}$ 不是I 的格罗布纳基, 则存在$0 \neq f \in I$ 使得$\mathrm{LT}(g_i) \nmid \mathrm{LT}(f)$ 对任意i 成立. 故在求f模G 的余数时, 每一次约化得到的r 与前面的r 的次数不变均为$\mathrm{Deg}\, f \neq 0$, 这与$r = 0$ 矛盾. □

推论2.112. 如$\{g_1, \cdots, g_m\}$ 是理想$I = (g_1, \cdots, g_m)$ 的格罗布纳基, 则对于任意$f(X) \in k[X]$, 存在唯一的$r(X) \in k[X]$, $r(X)$ 模$\{g_1, \cdots, g_m\}$ 是约化的且$f - r \in I$. 事实上r 是f 模G_σ 的余数, 其中σ 为S_m 中任意元.

证明. $k[X]$ 上的带余除法算法给出$r(X)$ 模$\{g_1, \cdots, g_m\}$ 是约化的, 且$f - r = a_1 g_1 + \cdots + a_m g_m \in I$, 故存在性成立.

设r 和r' 均模$\{g_1, \cdots, g_m\}$ 约化且$f - r \in I$, $f - r' \in I$. 则$r - r' \in I$. 如$r - r' \neq 0$. 由约化的性质, $r - r'$ 中任意单项式均不被任何$\mathrm{LT}(g_i)$ 整除. 这与$r - r' \in I$ 且$\{g_1, \cdots, g_m\}$ 是格罗布纳基矛盾. 故$r = r'$. 唯一性成立. □

推论2.113. 如$\{g_1, \cdots, g_m\}$ 是$I = (g_1, \cdots, g_m)$ 的格罗布纳基, 则

(1) 对任意$\sigma \in S_m$, f 模G_σ 的余数是一样的;

(2) $f \in I$ 当且仅当f 模G 的余数是0.

定义2.114. 对$\alpha, \beta \in \mathbb{N}^n$, 定义$\alpha \vee \beta = \mu = (\mu_1, \cdots, \mu_n)$, 其中$\mu_i = \max\{\alpha_i, \beta_i\}$.

定义2.115. 设$f, g \in k[X]$, $\mathrm{LT}(f) = a_\alpha X^\alpha$, $\mathrm{LT}(g) = b_\beta X^\beta$. 定义

$$\mathrm{LT}(f, g) = X^{\alpha \vee \beta},$$
$$S(f, g) = \frac{\mathrm{LT}(f, g)}{\mathrm{LT}(f)} f - \frac{\mathrm{LT}(f, g)}{\mathrm{LT}(g)} g.$$

后者称为f 与g 的**S-多项式**(S-polynomial), 它可以写为

$$S(f, g) = a_\alpha^{-1} X^{\mu - \alpha} f(X) - b_\beta^{-1} X^{\mu - \beta} g(X) = -S(g, f).$$

例2.116. 如f 和g 均是单项式, 则$S(f, g) = 0$.

引理2.117. 对于$j = 1, \cdots, l$, 给定$g_j \in k[X]$ 及单项式$c_j X^{\alpha(j)}$. 令$h(X) = \sum_{j=1}^{l} c_j X^{\alpha(j)} g_j(X)$. 如$\mathrm{Deg}\, h < \delta$, 但对于任意$1 \leq j \leq l$, 均有$\mathrm{Deg}\,(X^{\alpha(j)} g_j(X)) = \delta$, 则对于$1 \leq j \leq l - 1$, 存在$d_j \in k$, 使得

$$h(X) = \sum_{j=1}^{l-1} d_j X^{\delta - \mu(j)} S(g_j, g_{j+1}),$$

这里$\mu(j) = \mathrm{Deg}\,(g_j) \vee \mathrm{Deg}\,(g_{j+1})$, 且

$$\mathrm{Deg}\,(X^{\delta - \mu(j)} S(g_j, g_{j+1})) < \delta.$$

证明. 令$\mathrm{LT}(g_j) = b_j X^{\beta(j)}$. 则

$$\mathrm{LT}(c_j X^{\alpha(j)} g_j) = c_j b_j X^{\alpha(j)+\beta(j)} = c_j b_j X^{\delta}.$$

由$\mathrm{Deg}\, h < \delta$ 知$\sum\limits_j c_j b_j = 0$. 令$u_j(X) = b_j^{-1} X^{\alpha(j)} g_j(X)$. 则由阿贝尔求和公式(分部求和公式),

$$\begin{aligned} h(X) &= \sum_{j=1}^{l} c_j b_j u_j \\ &= \sum_{j=1}^{l-1} (\sum_{k=1}^{j} c_k b_k)(u_j - u_{j+1}) + (\sum_{k=1}^{l} c_k b_k) u_l \\ &= \sum_{j=1}^{l-1} (u_j - u_{j+1}) \cdot \sum_{k=1}^{j} c_k b_k. \end{aligned}$$

注意到$u_j - u_{j+1}$ 即$X^{\delta-\mu(j)} S(g_j, g_{j+1})$. 由于$u_j$ 和u_{j+1} 都是首一多项式且次数为δ, 故多项式$X^{\delta-\mu(j)} S(g_j, g_{j+1})$ 的次数$< \delta$. 令$d_j = \sum\limits_{k=1}^{j} c_k b_k$, 则引理得证. □

定理2.118. 集合$\{g_1, \cdots, g_m\}$ 是$I = (g_1, \cdots, g_m)$ 的格罗布纳基当且仅当对任意$1 \le p, q \le m$, $S(g_p, g_q)$ 模$G = [g_1, \cdots, g_m]$ 的余数都是0.

证明. $\Rightarrow$ 显然, 因为$S(g_p, g_q) \in I$.

$\Leftarrow$ 设$S(g_p, g_q)$ 模G 的余数均为0. 对于$f \neq 0$, $f \in I$, 记$f = \sum\limits_{i=1}^{m} h_i g_i$. 则

$$\mathrm{Deg}\, f \le \max_{1 \le i \le m} \{\mathrm{Deg}\,(h_i g_i)\}.$$

若等式成立, 则$\mathrm{Deg}\, f = \mathrm{Deg}\,(h_i g_i)$ 对某个i 成立, 故$\mathrm{LT}(g_i) \mid \mathrm{LT}(f)$. 所以我们不妨假设$\mathrm{Deg}\, f < \max\limits_i \{\mathrm{Deg}\,(h_i g_i)\} = \delta$ 且选取表达式$f = \sum\limits_i h_i g_i$ 使得δ 最小. 记

$$f = \sum_{\mathrm{Deg}\,(h_j g_j) = \delta} h_j g_j + \sum_{\mathrm{Deg}\,(h_{j'} g_{j'}) < \delta} h_{j'} g_{j'}.$$

对于满足条件$\mathrm{Deg}\,(h_j g_j) = \delta$的$j$, 不妨设为$j = 1, \cdots, l$, 则$\mathrm{Deg}\,(\sum\limits_{j=1}^{l} \mathrm{LT}(h_j) g_j) < \delta$. 故由引理, 存在$d_j \in k$, $\mu(j) \in \mathbb{N}^n$, $1 \le j \le l-1$, 使得

$$\sum_{j=1}^{l} \mathrm{LT}(h_j) g_j = \sum_{j=1}^{l-1} d_j X^{\delta-\mu(j)} S(g_j, g_{j+1}),$$

而$X^{\delta-\mu(j)} S(g_j, g_{j+1})$ 的次数小于δ. 由已知条件和带余除法, $X^{\delta-\mu(j)} S(g_j, g_{j+1})$ 可以写成$h'_{1j} g_1 + \cdots + h'_{mj} g_m$的形式, 其中$\mathrm{Deg}\,(h'_{ij} g_i) < \delta$. 故$f = \sum\limits_{i=1}^{m} \tilde{h}_i g_i$, 其中$\mathrm{Deg}\,(\tilde{h}_i g_i) < \delta$ 对每个$1 \le i \le m$ 均成立. 这与δ 的最小性矛盾. 故假设不成立. □

推论2.119. 如$I=(f_1,\cdots,f_s)$ 且f_i 均是单项式, 则$\{f_1,\cdots,f_s\}$ 是I 的格罗布纳基.

定理2.120 (布赫伯格)**.** 由I 的一组生成元, 存在算法求I 的一组格罗布纳基.

证明. 算法如下. 首先设$I=(f_1,\cdots,f_s)$. 循环计算: 令$B=\{f_1,\cdots,f_s\}$, $G=[f_1,\cdots,f_s]$. 对于$g,g'\in B$, $g\neq g'$. 计算$S(g,g') \bmod G$. 如$S(g,g') \bmod G$ 为$r(X)\neq 0$. 则令

$$B=B\cup\{r\},\ G=[f_1,\cdots,f_s,r],$$

并循环. 如$S(g,g') \bmod G$ 全为0, 则输出B 为I 的格罗布纳基.

我们需要证明上述算法不会无限循环下去. 事实上, 对于集合$B'\subseteq B$. 则

$$\langle \mathrm{LT}(g') \mid g'\in B'\rangle \ \subseteq\ \langle \mathrm{LT}(g)\mid g\in B\rangle.$$

在算法中, 如r 是$S(g,g') \bmod G$ 的余数, 则

$$\mathrm{LT}(r)\notin \langle \mathrm{LT}(g)|\ g\in B\rangle.$$

故每经过一次循环

$$\langle \mathrm{LT}(g)|\ g\in B\rangle \subsetneqq \langle \mathrm{LT}(g)|\ g\in B\cup\{r\}\rangle.$$

这样就得到$k[X]$ 中的理想严格升链. 由希尔伯特基定理, $k[X]$是诺特环, 这样的升链只能是有限长的. □

例2.121. 我们还是回到例 2.108的例子. 对于$I=(y^2+z^2,x^2y+yz,z^3+xy)$, 由于$S(y^2+z^2,x^2y+yz)=x^2z^2-y^2z\neq 0$ 模$[y^2+z^2,x^2y+yz,z^3+xy]$. 故$\{y^2+z^2,x^2y+yz,z^3+xy\}$ 不是I 的格罗布纳基, 但$\{y^2+z^2,x^2y+yz,z^3+xy,x^2z^2-y^2z\}$ 是I 的格罗布纳基.

下面的推论回答了本节开篇提出的问题.

推论2.122. (1) 如$I=(f_1,\cdots,f_s)$ 是$k[X]$ 的理想, 则可通过算法判定$h(X)$ 是否在I 中.

(2) 如$I=(f_1,\cdots,f_s)$ 是$k[X]$ 的理想, 则可通过算法判定$g(X)$ 是否在$\sqrt{I}$ 中.

(3) 如$I=(f_1,\cdots,f_s)$, $I'=(f'_1,\cdots,f'_{s'})$, 则可通过算法判定I 与I' 是否相等.

证明. (1) 先求出I 的一组格罗布纳基$\{g_1,\cdots,g_m\}$, 然后计算$h(X) \bmod [g_1,\cdots,g_m]$, 看其是否为0.

(2) 这等价于判定$k[X,y]$ 中的理想$(f_1,\cdots,f_s,1-yg)$ 是否包含1.

(3) 先求出I 与I' 的格罗布纳基$\{g_1,\cdots,g_m\}$ 与$\{g'_1,\cdots,g'_{m'}\}$, 然后求$g'_i \bmod [g_1,\cdots,g_m]$ 及$g_i \bmod [g'_1,\cdots,g'_{m'}]$. 如全为零, 则$I=I'$, 否则不是. □

定义2.123. 设k 为域, I 是$k[X,Y]=k[x_1,\cdots,x_n,y_1,\cdots,y_m]$ 的理想. $I_X=I\cap k[X]$ 称为I 关于$k[X]$ 的**消去理想**(elimination ideal).

例2.124. 如$I=(x^2,xy)$, 则$I_x=(x^2)$, $I_y=(0)$.

命题2.125. 设$k[X]$ 中的单项式序满足$x_1>x_2>\cdots>x_n$. 固定$p>1$, $Y=\{x_p,\cdots,x_n\}$. 如$I\subseteq k[X]$ 的格罗布纳基$G=[g_1,\cdots,g_m]$, 则$G\cap I_Y$ 是$I_Y=I\cap k[x_p,\cdots,x_n]$ 的格罗布纳基.

证明. 设$\{g_1,\cdots,g_m\}$ 是I 的格罗布纳基. 对于$0\neq f\in I$, 存在i, 使得$\mathrm{LT}(g_i)\mid \mathrm{LT}(f)$. 设$f(x_p,\cdots,x_n)\in I_Y\subseteq I$. 若$\mathrm{LT}(g_i)\mid\mathrm{LT}(f)$, 则$g_i\in k[x_p,\cdots,x_n]$, 故$g_i\in I_Y$. 又此时$f'=f-\frac{\mathrm{LT}(f)}{\mathrm{LT}(g_i)}g_i\in I_Y$, 但$\mathrm{Deg}\,f'<\mathrm{Deg}\,f$, 由归纳可知$I_Y$ 由$G\cap I_Y$ 生成. 故$G\cap I_Y$ 是I_Y 的格罗布纳基. □

命题2.126. 设$I_1,\cdots,I_t$ 是$k[X]=k[x_1,\cdots,x_n]$ 中的理想.

(1) 对于多项式环$k[X,y_1,\cdots,y_t]=k[x_1,\cdots,x_n,y_1,\cdots,y_t]$, 令

$$J=\langle 1-(y_1+\cdots+y_t),y_jI_j\mid 1\leq j\leq t\rangle.$$

则$\bigcap\limits_{j=1}^{t}I_j=J_X$.

(2) 给定$I_1,\cdots,I_t$ 的格罗布纳基, 可以计算$\bigcap\limits_{j=1}^{t}I_j$ 的格罗布纳基.

证明. 如$f(X)\in J_X=J\cap k[X]$. 记

$$f(X)=g(X,Y)(1-\sum_{j=1}^{t}y_j)+\sum_{j=1}^{t}h_j(X,y_1,\cdots,y_t)y_jq_j(X).$$

其中$q_j(X)\in I_j$ $(1\leq j\leq t)$. 对于给定的j, 取$y_j=1$, 且对于$l\neq j$ 取$y_l=0$. 则

$$f(X)=h_j(X,0,\cdots,0,1,\cdots,0)q_j(X)\in I_j.$$

所以$f(X)\in\bigcap\limits_{j=1}^{t}I_j$ 即$J_X\subseteq\bigcap\limits_{j=1}^{t}I_j$.

反之, 若$f\in\bigcap\limits_{j=1}^{t}I_j$, 则

$$f(X)=f(X)\cdot(1-\sum_{j=1}^{t}y_j)+\sum_{j=1}^{t}y_jf(X)\in J_X.$$

故$J_X=\bigcap\limits_{j=1}^{t}I_j$.

(2) 定义单项式的序: $x_1<x_2<\cdots<x_n<y_1<\cdots<y_t$. 则先由$I_j$ 的基得到J 的生成元, 求出J 的格罗布纳基G, 再由前面命题$G\cap J_X$ 即$J_X=\bigcap\limits_{j=1}^{t}I_j$ 的格罗布纳基. □

例2.127. 设$I=(x)\cap(x^2,xy,y^2)\subseteq k[x,y]$. 则

$$J=(1-u-v,ux,vx^2,vxy,vy^2)\subseteq k[x,y,u,v].$$

取$x<y<u<v$, 求得J 的格罗布纳基为

$$G=\{v+u-1,x^2,yx,ux,uy^2-y^2\}.$$

故$G\cap I=\{x^2,xy\}$ 是I 的格罗布纳基.

§2.7 结式

设R 是交换环,

$$f(x)=a_dx^d+a_{d-1}x^{d-1}+\cdots+a_0,\ a_d\neq 0 \text{ 和}$$
$$g(x)=b_ex^e+b_{e-1}x^{e-1}+\cdots+b_0,\ b_e\neq 0$$

是R 上的多项式. 设$\mathcal{P}_i$ 是R 上次数$<i$ 的多项式集合. 则$\mathcal{P}_i$ 是秩为i 的自由R-模, $\{1,x,\cdots,x^{i-1}\}$ 是它的一组基. 所以$\mathcal{P}_d\times P_e$ 与$\mathcal{P}_{d+e}$ 均是秩为$d+e$ 的自由R-模. 映射

$$\begin{aligned}\varphi=\varphi(f,g):\ \mathcal{P}_e\times\mathcal{P}_d&\longrightarrow\mathcal{P}_{d+e}\\(P,Q)&\longmapsto fP+gQ\end{aligned}$$

是R-模同态.

定义2.128. 多项式f 和g 的**结式**(resultant) 即

$$\mathrm{Res}(f,g)=\det\varphi(f,g)\in R.$$

令

$$e_i=\begin{cases}(x^i,0), & 0\leq i<e;\\(0,x^{i-e}), & e\leq i<d+e,\end{cases}$$
$$\tilde{e}_i=x^i,\ 0\leq i<d+e.$$

则$\{e_i\}$ 是$\mathcal{P}_e\times\mathcal{P}_d$ 的一组基, $\{\tilde{e}_i\}$ 是$\mathcal{P}_{e+d}$ 的一组基. 线性映射φ 在这 两组基下的矩阵为

$$A=\begin{pmatrix}a_0 & & & b_0 & & \\ a_1 & \ddots & & b_1 & \ddots & \\ \vdots & \ddots & a_0 & \vdots & \ddots & b_0\\ a_d & & a_1 & b_e & & b_1\\ & \ddots & \vdots & & \ddots & \vdots\\ & & a_d & & & b_e\end{pmatrix},$$

即$\varphi(e_0,e_1,\cdots,e_{d+e-1})=(\tilde{e}_0,\tilde{e}_1,\cdots,\tilde{e}_{d+e-1})A$.

故由线性代数知识, 我们有

引理2.129. $\mathrm{Res}(f,g)=\det A$.

定理2.130. *设R 为整环,*

$$f(x)=a_d(x-\alpha_1)\cdots(x-\alpha_d),$$
$$g(x)=b_e(x-\beta_1)\cdots(x-\beta_e),$$

其中$\alpha_1,\cdots,\alpha_d$ 和$\beta_1,\cdots,\beta_e$ 分别是f 和g 在R 的分式域K 的代数闭包$\overline{K}$ 中的根. 则

$$\mathrm{Res}(f,g)=a_d^e b_e^d\cdot\prod_{\substack{1\le i\le d\\1\le j\le e}}(\alpha_i-\beta_j).$$

证明. 令$W=(w_{ij})$, 其中

$$w_{ij}=\begin{cases}\beta_i^j, & \text{如}i\le e;\\ \alpha_{i-e}^j, & \text{如}e<i\le d+e.\end{cases}$$

则

$$WA=\begin{pmatrix} f(\beta_1) & \beta_1 f(\beta_1) & \cdots & \beta_1^{e-1}f(\beta_1) & & & & \\ f(\beta_2) & \beta_2 f(\beta_2) & \cdots & \beta_2^{e-1}f(\beta_2) & & & & \\ \vdots & \vdots & & \vdots & & & & \\ f(\beta_e) & \beta_e f(\beta_e) & \cdots & \beta_e^{e-1}f(\beta_e) & & & & \\ & & & & g(\alpha_1) & \alpha_1 g(\alpha_1) & \cdots & \alpha_1^{d-1}g(\alpha_1)\\ & & & & g(\alpha_2) & \alpha_2 g(\alpha_2) & \cdots & \alpha_2^{d-1}g(\alpha_2)\\ & & & & \vdots & \vdots & & \vdots\\ & & & & g(\alpha_d) & \alpha_d g(\alpha_d) & \cdots & \alpha_d^{d-1}g(\alpha_d)\end{pmatrix}$$

由范德蒙行列式的计算, 我们知

$$\begin{aligned}\det WA&=f(\beta_1)\cdots f(\beta_e)g(\alpha_1)\cdots g(\alpha_d)\prod_{i<j}(\beta_i-\beta_j)\prod_{i<j}(\alpha_i-\alpha_j)\\&=\det W\cdot\det A,\end{aligned}$$

及

$$\det W=\prod_{i<j}(\beta_i-\beta_j)\prod_{i<j}(\alpha_i-\alpha_j)\prod_{\substack{1\le i\le d\\1\le j\le e}}(\beta_j-\alpha_i).$$

若α_i,β_j 两两不同, 则

$$\det A\cdot\prod_{\substack{1\le i\le d\\1\le j\le e}}(\beta_j-\alpha_i)=f(\beta_1)\cdots f(\beta_e)g(\alpha_1)\cdots g(\alpha_d).$$

但

$$f(\beta_1)\cdots f(\beta_e) = a_d^e \prod_{\substack{1\le i\le d\\ 1\le j\le e}} (\beta_j - \alpha_i),$$
$$g(\alpha_1)\cdots g(\alpha_d) = b_e^d \prod_{\substack{1\le i\le d\\ 1\le j\le e}} (\alpha_i - \beta_j).$$

故

$$\begin{aligned}\mathrm{Res}(f,g) = \det A &= a_d^e g(\alpha_1)\cdots g(\alpha_d)\\ &= (-1)^{ed} b_e^d f(\beta_1)\cdots f(\beta_e)\\ &= a_d^e b_e^d \prod_{\substack{1\le i\le d\\ 1\le j\le e}} (\alpha_i - \beta_j).\end{aligned}$$

如α_i, β_j 均等于α, 则可将其中一个换为$\alpha + \delta a$, 其中a是某固定的非零数, δ变化. 则A 中元素是δ 的多项式, 故$\det A$ 也是δ的多项式. 当$\delta \neq 0$ 时定理成立, 故等式两边作为多项式是一样的, 所以$\delta = 0$时定理也成立. □

推论2.131. *如R 是整环, 结式由如下性质刻画:*

(1) *如$d = 0$, 则*$\mathrm{Res}(f,g) = a_d^e$, *如$e = 0$, 则*$\mathrm{Res}(f,g) = b_e^d$.

(2) $\mathrm{Res}(x - a_1)(x - b_1) = a_1 - b_1$.

(3) $\mathrm{Res}(g,f) = (-1)^{de}\mathrm{Res}(f,g)$.

(4) $\mathrm{Res}(fg,h) = \mathrm{Res}(f,h)\mathrm{Res}(g,h)$.

证明. 一方面由定理知结式满足(1)-(4). 反过来, 若

$$f(x) = a(x - \alpha_1)\cdots(x - \alpha_d),$$
$$g(x) = b(x - \beta_1)\cdots(x - \beta_e),$$

$R'(f,g)$为满足(1)-(4) 的函数, 则

$$R'(f,g) = a^e b^d \prod_{\substack{1\le i\le d\\ 1\le j\le e}} (\alpha_i - \beta_j) = \mathrm{Res}(f,g).$$ □

推论2.132. *设R 是唯一因子分解环*(UFD). *则f 与g 有公因子当且仅当它们的结式*$\mathrm{Res}(f,g) = 0$.

证明. 这是定理的直接推论。 □

设R 是整环, $K = \mathrm{Frac}\ R$ 是它的分式域. 令V_i是次数$< i$ 的K 上多项式的集合, 则V_i 是i 维K-线性空间, $\varphi(f,g)$ 可以自然看成K-线性映射

$$\begin{aligned}V_e \times V_d &\longrightarrow V_{d+e},\\ (P,Q) &\longmapsto fP + gQ.\end{aligned}$$

仍记此映射为$\varphi(f,g)$.

故由线性代数知识, 我们知

$$\mathrm{Res}(f,g)\neq 0 \Leftrightarrow \ker\varphi = 0.$$

即有

命题2.133. *设R 是整环, $f(x)$ 和$g(x)\in R[x]$ 是正次数多项式.*

(1) $\mathrm{Res}(f,g)=0$ *当且仅当存在非零多项式$P_0(x)\in\mathcal{P}_e$ 和$Q_0(x)\in\mathcal{P}_d$, 使得$fP_0+gQ_0=0$.*

(2) *存在多项式$P_1(x)\in\mathcal{P}_e$, $Q_1(x)\in\mathcal{P}_d$, 使得*

$$fP_1(x)+gQ_1(x)=\mathrm{Res}(f,g).$$

更进一步地, 总可以假设$P_1(x)$ 和$Q_1(x)$ 的系数是f和g 的系数的整系数多项式.

证明. $\mathrm{Res}(f,g)=0$ 等价于存在非零$p(x)\in V_e$, $q(x)\in V_d$ 使得

$$f(x)p(x)+g(x)q(x)=0.$$

将$p(x)$, $q(x)$ 的系数进行通分, 即得$P_0(x)\in\mathcal{P}_e$, $Q_0(x)\in\mathcal{P}_d$, 使得$fP_0+gQ_0=0$.

(2) 如$\mathrm{Res}(f,g)=0$, 只要取$P_1=Q_1=0$ 即可. 如$\mathrm{Res}(f,g)\neq 0$, 取定$V_e\times V_d$的基$\{e_i\}$和V_{d+e}的基$\{\tilde{e}_i\}$ 如同本节开始时$\mathcal{P}_e\times\mathcal{P}_d$和$\mathcal{P}_{d+e}$的基, 则

$$\varphi(f,g)(e_0,\cdots,e_{d+e-1})=(\tilde{e}_0,\cdots,\tilde{e}_{d+e-1})A.$$

此时$\mathrm{Res}(f,g)=\det A\neq 0$, 故$K$ 上的线性方程组

$$A\begin{pmatrix} c_0\\ c_1\\ \vdots\\ c_{d+e-1}\end{pmatrix}=\begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix}$$

有唯一解. 由克莱姆法则, 此唯一解即

$$\left(c_i=\frac{\det A_i}{\det A}:\ 0\le i<d+e\right),$$

其中A_i 是将矩阵A 的第i 列替换为$(1,0,\cdots,0)^T$ 得到. 故$c_i=\frac{a_s,b_t\text{ 的整系数多项式}}{\mathrm{Res}(f,g)}$.
令

$$p_1(x)=\sum_{i=0}^{e-1}c_ix^i=\frac{P_1(x)}{\mathrm{Res}(f,g)},\quad q_1(x)=\sum_{j=0}^{d-1}c_{e+j}x^j=\frac{Q_1(x)}{\mathrm{Res}(f,g)}.$$

则$P_1(x), Q_1(x)$ 的系数是f和g 系数的整系数多项式, 且

$$fp_1 + gq_1 = 1,$$

即$fP_1 + gQ_1 = \mathrm{Res}(f, g)$. □

习 题

习题2.1. 设R 是诺特环. 证明M 是诺特R-模当且仅当M是有限生成R-模.

习题2.2. 设R 是诺特环. 证明R^n是诺特R-模.

习题2.3. 设k是域. 证明多项式环$k[x]$中包含k的子环都是诺特环.

习题2.4. 证明: R 是诺特环当且仅当R中每个素理想都是有限生成的.

习题2.5. 给出例子, 对交换环R 及真理想$I \subsetneq J \subsetneq R$, J 是有限生成的但I 不是有限生成的.

习题2.6. 设R 是诺特环. 证明幂级数环$R[[x]]$是诺特环.

习题2.7. 设R 是诺特环, 且对任意$a, b \in R$, 存在a 和b 的公因子是它们的线性组合. 证明: R 是PID.

习题2.8. 设M是诺特R-模, 则$R/\mathrm{ann}(M)$是诺特环.

习题2.9. 证明希尔伯特基定理的逆定理, 即若$R[x]$是诺特环, 则R也是诺特环.

习题2.10. 证明例 *2.3*(3)-(6)中出现的环不是诺特环, 即

(1) 设k 是域. 多项式环$k[x_i]_{i\in I}$, 其中I 是无限集, 不是诺特环.

(2) 设k 是域. 多项式$k[x, y]$ 的子环$k + xk[x, y]$ 不是诺特环.

(3) 区间$[a, b]$ 上所有实值连续函数构成的环$C([a, b])$ 不是诺特环.

(4) 无限集X到$\mathbb{Z}/2\mathbb{Z}$的函数全体构成的环.

习题2.11. 证明: R 是诺特环当且仅当任意有限生成R-模的子模都是有限生成的.

习题2.12. 设$f : R \to T$ 和$g : S \to T$ 是环的满同态, $R \times_T S = \{(r, s) \mid f(r) = g(s)\}$ 为其纤维积. 证明: 若R 与S 是诺特环, 则$R \times_T S$ 也是诺特环.

习题2.13. 设p是素数. 证明$\mathbb{Z}$-模$\mathbb{Z}[\frac{1}{p}]/\mathbb{Z}$ 是阿廷模, 不是诺特模.

习题2.14. 证明有限生成阿廷模是诺特模.

习题2.15. 设M 是阿廷模, $\varphi : M \to M$ 是单同态. 证明: φ 是同构.

习题2.16. 设M是诺特R-模, $\varphi : M \to M$是R-模同态. 证明当n足够大时, $\ker \varphi^n \cap \operatorname{im} \varphi^n = \{0\}$. 由此证明如$\varphi$为满射, 则$\varphi$是同构.

习题2.17. 设S是交换环R的乘法集, M是有限生成R-模. 证明$S^{-1}M = 0$ 当且仅当$sM = 0$ 对某个$s \in S$成立.

习题2.18. 证明: M 是平坦R-模当且仅当对所有$\mathfrak{p} \in \operatorname{Spec}(R)$, $M_{\mathfrak{p}}$ 是平坦$R_{\mathfrak{p}}$-模. 将素理想换为极大理想, 此结论仍然成立.

习题2.19. 设N与N'是模M的子模. 证明$N = N'$当且仅当对所有R的素理想$\mathfrak{p}$, $N_{\mathfrak{p}} = N'_{\mathfrak{p}}$. 将素理想换为极大理想, 此结论仍然成立.

习题2.20. 设$\varphi : M \to N$是R-模同态. 证明φ是单射或满射当且仅当对每个素理想$\mathfrak{p}$, 诱导映射$\varphi_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ 是单射或满射. 将素理想换为极大理想, 此结论仍然成立.

习题2.21. 设$\mathfrak{p} \subseteq \mathfrak{q}$是$R$上的两个素理想. 证明: $R_{\mathfrak{p}} \cong (R_{\mathfrak{q}})_{\mathfrak{p}R_{\mathfrak{q}}} = (R_{\mathfrak{q}} - \mathfrak{p}R_{\mathfrak{q}})^{-1}R_{\mathfrak{q}}$.

习题2.22. 对于模M, 定义M 的支集$\operatorname{Supp}(M) = \{\mathfrak{p} \in \operatorname{Spec}R \mid M_{\mathfrak{p}} \neq 0\}$. 证明:

(1) $M = 0$ 当且仅当$\operatorname{Supp}(M) = \emptyset$.

(2) 如$0 \to L \to M \to N \to 0$ 是R-模正合列, 则$\operatorname{Supp}(M) = \operatorname{Supp}(L) \cup \operatorname{Supp}(N)$.

(3) 设$\mathfrak{p} \subseteq \mathfrak{q}$ 为素理想. 如$\mathfrak{p} \in \operatorname{Supp}(M)$, 则$\mathfrak{q} \in \operatorname{Supp}(M)$.

习题2.23. 设S是交换环R的乘法集, M, N是R-模. 证明存在唯一的$S^{-1}R$-模同构$\varphi : (S^{-1}M) \otimes_{S^{-1}R} (S^{-1}N) \cong S^{-1}(M \otimes_R N)$, 使得$\varphi((m/s) \otimes (n/s')) = (m \otimes n)/ss'$对任意$m \in M$, $n \in N$和$s, s' \in S$成立.

习题2.24. 设R是整环, F是它的分式域. 证明: F是有限生成R-模当且仅当$R = F$.

习题2.25. 设$D \neq 0$是无平方因子整数. 试求二次域$\mathbb{Q}(\sqrt{D})$的代数整数环.

习题2.26. 设R 是整闭整环, S 是R 上的乘法集且$0 \notin S$. 证明$S^{-1}R$ 也是整闭整环.

习题2.27. 设S/R 是整扩张, $s_1, \cdots, s_m \in S$. 证明$R[s_1, \cdots, s_m]$ 是有限生成R-模.

习题2.28. 设S/R 是整扩张.

(1) 如果元素$a \in R$ 在S 中是单位, 证明a 在R 中也是单位.

(2) 证明对于雅各布森根, 有等式: $\operatorname{Jac}(R) = R \cap \operatorname{Jac}(S)$.

习题2.29. 设R 是整环, S/R 是整扩张. 证明如R 中非零素理想均是极大理想, 则S 中非零素理想也都是极大理想.

习题2.30. 设k 是域, $R=k[\bar{x},\bar{y}]=k[x,y]/(x^2-y^3)$, $t=\bar{x}/\bar{y}\in \mathrm{Frac}(R)$. 证明: $\mathrm{Frac}(R)=k(t)$, 且R 在其中的整闭包是$k[t]$.

习题2.31. 设$E/\mathbb{Q}$ 是伽罗瓦扩张, $\alpha\in E$ 是代数整数. 证明对任意$\sigma\in \mathrm{Gal}(E/\mathbb{Q})$, $\sigma(\alpha)$ 是代数整数.

习题2.32. 设R是整闭整环, F是它的分式域.

(1) 如K为F的扩域且$a\in K$, 证明: a在R上整当且仅当a在F上代数且其最小多项式系数在R中.

(2) 由(1), 证明: 如$f(x)$是R上首一多项式, $f(x)=a(x)b(x)$, 其中$a(x),b(x)\in F[x]$且首一, 则$a(x)$和$b(x)$均在$R[x]$中.

下面四道习题证明命题 2.49.

习题2.33. 设E/F 是n 次有限域扩张, $u\in E$ 在F 上的最小多项式是$m(x)=x^m-c_{m-1}x^{m-1}+\cdots+(-1)^m c_0$, 设$u_1,\cdots,u_m$ 是$m(x)$ 的根. 证明

$$\mathrm{tr}_{E/F}(u)=\frac{n}{m}c_{m-1}=\frac{n}{m}\sum_i u_i,\quad N_{E/F}(u)=c_0^{n/m}=(\prod_i u_i)^{n/m}.$$

习题2.34. 更进一步地, 假设E/F 是可分扩张, $\tilde{E}$ 是E 在F 上的正规闭包. 令$G=\mathrm{Gal}(\tilde{E}/F)$, $H=\mathrm{Gal}(\tilde{E}/E)$, T 是G 关于H 的左陪集代表元系. 证明:

$$\prod_{\sigma\in T}(x-\sigma(u))=m(x)^{n/m},$$

从而

$$\mathrm{tr}_{E/F}(u)=\sum_{\sigma\in T}\sigma(u),\quad N_{E/F}(u)=\prod_{\sigma\in T}\sigma(u).$$

习题2.35. 假设同前. 设$\{e_1,\cdots,e_n\}$ 是E 的F-基, 设$T=\{\sigma_1,\cdots,\sigma_n\}$. 证明:

$$\det(t(e_i,e_j)_{i,j})=\det(\sigma_\ell(e_i)_{\ell,i})^2.$$

习题2.36. 设E/F 是域扩张, $\sigma_1,\cdots,\sigma_n$ 是E的F-自同构群$\mathrm{Gal}(E/F)$ 中的不同元. 证明若$\sum_i c_i\sigma_i(x)=0$ $(c_i\in E)$ 对所有$x\in E$ 成立, 则c_i 恒等于0. 由此得出习题 *2.35* 中$\det(t(e_i,e_j))\neq 0$, 从而迹形式t 是非退化双线性型.

习题2.37. 设I,J是环R的理想. 证明:

(1) $\sqrt{IJ}=\sqrt{I\cap J}=\sqrt{I}\cap\sqrt{J}$.

(2) $\sqrt{\sqrt{I}}=\sqrt{I}$.

(3) $\sqrt{\sqrt{I}+\sqrt{J}}=\sqrt{I+J}$.

习题2.38. 证明理想(x^3-y^2)是环$\mathbb{F}_2[x,y]$中的根式理想.

习题2.39. 设$\mathfrak{p}$为素理想且$\mathfrak{p}\supseteq I$, 证明: $\mathfrak{p}\supseteq\sqrt{I}$.

习题2.40. 设R 是诺特环. 证明: 理想I 是根式理想当且仅当I 是有限多个素理想之交.

习题2.41. 试举例, 使得:

(1) $\mathfrak{p}$ 是素理想, 但$\mathfrak{p}^2$ 不是准素理想.

(2) Q 是准素理想, 但Q 不是$\mathfrak{p}=\sqrt{Q}$ 的幂次.

(3) I 不是准素理想但$\sqrt{I}$ 是素理想.

习题2.42. 证明定理 *2.72:* 设R 是诺特环. 则R 的每个真理想I 均有极小准素分解

$$I=\bigcap_{i=1}^{m} Q_i$$

且$\{\sqrt{Q_1},\sqrt{Q_2},\cdots,\sqrt{Q_m}\}$ 由I 唯一决定.

习题2.43. 证明对任意域k, $\mathbb{A}^1$中的仿射代数集为$\mathbb{A}^1$, $\emptyset$ 和k 的有限子集.

习题2.44. 如果$k=\mathbb{F}_2$, $V=\{(0,0),(1,1)\}\subseteq\mathbb{A}^2$, 证明$\mathcal{I}(V)$是极大理想$\mathfrak{m}_1=(x,y)$与$\mathfrak{m}_2=(x-1,y-1)$ 的乘积$\mathfrak{m}_1\mathfrak{m}_2$.

习题2.45. 试举例说明当k 不是代数封闭域时, 零点定理可能不成立.

习题2.46. 设V是$\mathbb{A}^n$的有限仿射代数集. 证明: 如V 的元素个数是m, 则$k[V]$作为k-代数同构于k^m.

习题2.47. 设k 是有限域. 证明$\mathbb{A}^n$ 的任意子集均是仿射代数集.

习题2.48. 设f是域k上的一元多项式, 次数≥ 1. 证明: $\mathcal{I}(\mathcal{Z}(f))=(f)$ 当且仅当f 是$k[x]$ 中不同线性因子的乘积.

习题2.49. 设$f,g\in k[x,y]$ 为不可约多项式且互不关连, 即$(f)\neq(g)$. 证明: $\mathcal{Z}((f,g))$或者是空集, 或者是$\mathbb{A}^2$ 中的有限集.

习题2.50. 设$V\subseteq\mathbb{A}^n$是仿射代数集, $f\in k[V]$. f的图是指集合

$$\{(a_1,\cdots,a_n,f(a_1,\cdots,a_n))\mid(a_1,\cdots,a_n)\in V\}.$$

证明f的图是$\mathbb{A}^{n+1}$上的仿射代数集.

习题2.51. 设V,W 是仿射代数集. 证明$V\times W$ 也是仿射代数集, 且$k[V\times W]\cong k[V]\otimes_k k[W]$.

习题2.52. 设$f:A\to B$ 是环同态. 令$f^*:\mathrm{Spec}(B)\to\mathrm{Spec}(A)$ 为映射$\mathfrak{p}\mapsto f^{-1}(\mathfrak{p})$. 证明$f^*$ 在扎里斯基拓扑下是连续映射.

习题2.53. 证明: 自然同态$\varphi:R\to R/\mathrm{nil}(R)$ 诱导的映射$\varphi^*:\mathrm{Spec}(R/\mathrm{nil}(R))\to\mathrm{Spec}(R)$ 是同胚.

习题2.54. 证明: 有限生成$\mathbb{Z}$-代数如果是域, 则一定是有限域.

习题2.55. (1) 分别写出$k[x,y]$ 中以字典序和次数-字典序前10 个单项式.

(2) 以字典序和次数-字典序写出$k[x,y,z]$ 中所有权≤ 2 的单项式.

习题2.56. 使用次数-字典序求:

(1) $x \mod [x-y, x-z]$ 与$x \mod [x-z, x-y]$.

(2) $x^7y^2+x^3y^2-y+1 \mod [xy^2-x, x-y^3]$ 和$x^7y^2+x^3y^2-y+1 \mod [x-y^3, xy^2-x]$.

习题2.57. 设$c_\alpha X^\alpha$ 是非零单项式, $f(X), g(X)$ 是$k[X]$ 中的多项式且它们的每一项都不被$c_\alpha X^\alpha$ 整除. 证明$f(X)-g(X)$的每一项都不被$c_\alpha X^\alpha$ 整除.

习题2.58. 设$k[X]$ 中的理想I是**单项式理想** *(monomial ideal)*, 即是指它由单项式$X^{\alpha(1)}, \cdots, X^{\alpha(q)}$ 生成.

(1) 证明$f(X) \in I$ 当且仅当f 的每一项均被某$X^{\alpha(i)}$ 生成.

(2) 如$G=[g_1, \cdots, g_m]$ 而r 模G 约化, 则$r \notin [\mathrm{LT}(g_1), \cdots, \mathrm{LT}(g_m)]$.

习题2.59. 给定$k[X]$中一个单项式序. 设I是$k[X]$中的理想, $\{g_1, \cdots, g_m\} \subseteq I$. 如对任意非零$f \in I$, 存在$g_i$使得$\mathrm{LT}(g_i) \mid \mathrm{LT}(f)$, 证明$I=(g_1, \cdots, g_m)$. 这说明在格罗布纳基的定义中, 不需要假设$I$ 由$g_1, \cdots, g_m$ 生成.

以下三题采用次数-字典单项式序.

习题2.60. 试求$I=(x^2-y, y^2-x, x^2y^2-xy)$的格罗布纳基并判断$x^4+x+1$是否在$I$中.

习题2.61. 设$I=(y-x^2, z-x^3)$.

(1) 设$x<y<z$, 令$\leq_{\mathrm{lex}}$是对应的次数-字典单项式序. 证明$\{y-x^2, z-x^3\}$不是I 的格罗布纳基.

(2) 设$y<z<x$, 令$\leq_{\mathrm{lex}}$是对应的次数-字典单项式序. 证明$\{y-x^2, z-x^3\}$不是I 的格罗布纳基.

习题2.62. 试求$I=(xz, xy-z, yz-x)$的格罗布纳基并判断x^3+x+1是否在I中.

习题2.63. 设$f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_0$ 的根为$\alpha_1, \cdots, \alpha_n$. 令$f'(x)=nx^{n-1}+(n-1)a_{n-1}x^{n-2}+\cdots+a_1$ 是$f(x)$的形式微分. 证明:

$$\mathrm{Res}(f, f') = \prod_{i=1}^{n} f'(\alpha_i).$$

更进一步地, 回顾$f(x)$ 的判别式(见《代数学基础》)

$$D(f) = \prod_{1 \leq i < j \leq n} (\alpha_j - \alpha_i).$$

证明:

$$D(f) = (-1)^{n(n-1)/2} \mathrm{Res}(f, f').$$

第三章　半单代数和有限群表示

§3.1　一般环上的模

在本书第一部分学习模论时, 我们一般假设环是含幺交换环. 事实上, 模的理论可以建立在一般环的情形, 即环可以是非交换的.

定义3.1. 设R 是含幺环, 加法阿贝尔群M 称为**左R-模**是指存在**左乘映射**

$$R \times M \longrightarrow M,\ (r, m) \longmapsto rm,$$

满足如下性质

(1) **恒等元**: 对任意的$m \in M$, 均有$1m = m$;

(2) **分配律**: 对于$r, s \in R$ 和$m, n \in M$, 等式$(r + s)m = rm + sm$和$r(m + n) = rm + rn$成立;

(3) **结合律**: 对于$r, s \in R$, $m \in M$, $(rs)m = r(sm)$ 成立.

同样地, M称为**右R-模**是指存在**右乘映射**

$$M \times R \longrightarrow M,\ (m, r) \mapsto mr$$

满足如下性质

(1)′ **恒等元**: 对任意的$m \in M$, 均有$m1 = m$;

(2)′ **分配律**: 对于$r, s \in R$, $m, n \in M$, 等式$m(r+s) = mr+ms$和$(m+n)r = mr + nr$成立;

(3)′ **结合律**: 对于$r, s \in R$, $m \in M$, $m(rs) = (mr)s$ 成立.

定义3.2. 设R为环, R的**反环**(opposite ring) R^{op} 是指作为集合$R^{\mathrm{op}} = R$, 它的加法与R的加法一样, 但它的乘法$\circ$ 如下定义：$r \circ s = sr$.

对于反环, 我们有如下简单性质:

命题3.3. *设R 是含幺环, R^{op}是它的反环. 则*

(1) *R为交换环当且仅当$R^{\mathrm{op}} = R$.*

(2) *$R = (R^{\mathrm{op}})^{\mathrm{op}}$.*

(3) *若R是域F上的代数, 则R^{op}也是.*

例3.4. 设R 为环, M为左R-模, 定义映射

$$M \times R^{\mathrm{op}} \longrightarrow M,\ (m, r) \longmapsto m \circ r = rm.$$

则此映射是右乘映射, M可以视作右R^{op}-模. 特别地, 若R是交换环, 由于$R^{\mathrm{op}} = R$, 故此时左模=右模= 模.

类似地, 若M是右R-模, 我们可以自然定义M上的左R^{op}-模结构. 由于$R = (R^{\mathrm{op}})^{\mathrm{op}}$, 我们通常只需考虑左模的情形. 今后如不特殊说明, 我们讨论的模都是左模, 我们常常称模的左乘映射为数乘映射.

定义3.5. 设R与S为环, M为加法阿贝尔群. M称为(R,S)-**双模** 是指M 既是左R-模, 也是右S-模, 且对任意的$r\in R$, $s\in S$, $m\in M$, 等式$r(ms)=(rm)s$ 恒成立.

例3.6. 以环的乘法作为左乘和右乘映射, 则R具备自然的左R-模, 右R-模和(R,R)-双模结构.

定义3.7. 设R为环, M为左R-模. M的加法子群N称为M的**子模** 是指N 对于数乘封闭, 即对任意的$r\in R$ 和$n\in N$, 均有$rn\in N$.

例3.8. 我们给出子模的一些例子:

(1) 对于任意模M, $0=\{0\}$和M是M的子模, 称为**平凡子模**.

(2) 环R作为左R模时的子模I称为R的**左理想**(left ideal), 此时对任意的$r\in R$, 均有$rI\subseteq I$; R作为右R模时的子模J 称为R的**右理想**(right ideal), 此时对任意的$r\in R$, 均有$Jr\subseteq J$. 如果I既是左理想又是右理想, 则称I 是**双边理想**(two-sided ideal), 即通常定义的理想, 此时I 是(R,R)-双模R 的子模.

定义3.9. 非零模M称为**单模**(simple module)或**不可约模**(irreducible module)是指它没有非平凡的子模.

定义3.10. 如N是M的子模, 在商群M/N上通过数乘映射

$$R\times M/N\longrightarrow M/N,\ (r,m+N)\mapsto rm+N$$

得到的模M/N称为M对N的**商模**(quotient module).

定义3.11. 设M,N是R模. 映射$f:M\to N$ 称为**模同态**(homomorphism of modules) 如f 为加法群同态, 且对任意$r\in R$, $m\in M$, 均有$f(rm)=rf(m)$.

如同态f是单射(满射, 双射), 则称f为单同态(满同态, 同构).

注意到如f 为同构, 则f^{-1}也是同构.

与交换环上模的情形, 我们有如下模的同构定理和对应定理**:**

定理3.12 (同态基本定理)**.** *设$f:M\longrightarrow N$为R模同态, 则$\ker f=f^{-1}(0)$是M的子模, $\operatorname{im}f=f(M)$ 是N的子模, 且f诱导R 模同构*

$$\bar f:M/\ker f\xrightarrow{\sim}\operatorname{im}f, m+\ker f\longmapsto f(m).$$

定理3.13 (第二同构定理)**.** *如S 和T 是模M 的子模, 则存在R-模同构*

$$S/(S\cap T)\xrightarrow{\sim}(S+T)/T,\ s+(S\cap T)\longmapsto s+T.$$

定理3.14 (第三同构定理)**.** *设模$T\subseteq S\subseteq M$, 则存在R-模同构*

$$\frac{M/T}{S/T}\xrightarrow{\sim}M/S,\ \ \overline{m+T}\longmapsto m+S.$$

定理3.15 (对应定理). 设T 是模M 的子模, $\pi : M \to M/T$ 是自然商映射. 则存在一一对应

$$\begin{aligned}\varphi : \{\text{中间模} S \mid T \subseteq S \subseteq M\} &\longrightarrow \{M/T\text{的子模}\},\\ S &\longmapsto S/T,\end{aligned}$$

其逆映射为$\overline{S} \mapsto \pi^{-1}(\overline{S})$.更进一步地, $S \subseteq S'$ 当且仅当$S/T \subseteq S'/T$.

下面定理(舒尔引理, Schur Lemma)在表示论研究中起到了至关重要的作用.

定理3.16 (舒尔引理). 单模间的任意非零同态均是同构.

证明. 设$f : M_1 \to M_2$为单模间的非零同态. 则一方面$\ker f \neq M_1$ 为M_1的子模, 故$\ker f = 0$. 另一方面$\operatorname{im} f \neq 0$ 为M_2的子模, 故$\operatorname{im} f = M_2$. 由同态基本定理, 故得$f$ 为同构. □

定义3.17. 设M, N是R模. 记$\mathrm{Hom}_R(M, N)$为M到N 的模同态集合, 记$\mathrm{End}_R(M) = \mathrm{Hom}_R(M, M)$ 为M 的R-模自同态集合.

在$\mathrm{Hom}_R(M, N)$中定义加法

$$f + g : M \to N,\ m \mapsto f(m) + g(m).$$

由此加法, $\mathrm{Hom}_R(M, N)$ 构成加法群.

在$\mathrm{End}_R(M)$中, 定义乘法

$$f \cdot g = f \circ g : M \xrightarrow{g} M \xrightarrow{f} M.$$

由此加法和乘法, $\mathrm{End}_R(M)$构成环, 称为M的**自同态环**(Endomorphism ring).

舒尔引理的一个直接推论是

推论3.18. 若M是单模, 则$\mathrm{End}_R(M)$是可除环.

对于$\mathrm{Hom}_R(R, M)$, 可以在其上定义左乘

$$r\varphi(u) = \varphi(ur),\ r \in R,\ \varphi \in \mathrm{Hom}_R(R, M).$$

则$\mathrm{Hom}_R(R, M)$是R模, 且容易得出

引理3.19. 映射$\mathrm{Hom}_R(R, M) \to M$, $\varphi \mapsto \varphi(1)$是模同构.

定义3.20. (1)设M是R模, $(M_\alpha)_{\alpha \in I}$是$M$的子模集合, 则它们的**和**

$$\sum_{\alpha \in I} M_\alpha = \{\sum_{\alpha \in I} m_\alpha \mid m_\alpha \in M_\alpha,\ \text{且} m_\alpha \text{只在有限个} \alpha \text{ 非零}\}$$

是M的子模.

(2)设$(M_\alpha)_{\alpha\in I}$是R模集合, 则它们的**直积**定义为R模

$$\prod_{\alpha\in I} M_\alpha = \{(m_\alpha)_{\alpha\in I} \mid m_\alpha \in M_\alpha\}.$$

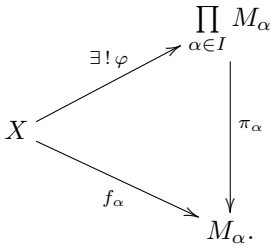
它们的**直和**定义为

$$\bigoplus_{\alpha\in I} M_\alpha = \{(m_\alpha)_{\alpha\in I} \mid m_\alpha \in M_\alpha\text{且只在有限个}\alpha\text{ 处非零}\}.$$

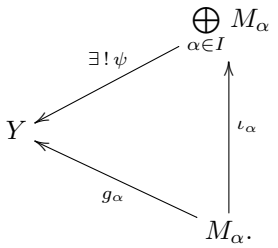
命题3.21. (1) 若I是有限集, 则直和与直积相同.

(2) 若N_1和N_2是M的子模, 则N_1+N_2是直和, 即$N_1+N_2\cong N_1\bigoplus N_2$, 当且仅当$N_1\cap N_2=0$.

(3) 令$\pi_k:\ \prod_{\alpha\in I} M_\alpha \to M_k,\ (m_\alpha)_{\alpha\in I}\mapsto m_k$. 则$\pi_k$ 是满同态, 且满足**泛性质:** 如对任意$\alpha\in I$, 均给定模同态$f_\alpha: X\to M_i$, 则存在唯一的模同态$\varphi:\ X\to\prod_{\alpha\in I} M_\alpha$, 使得$f_\alpha=\pi_\alpha\circ\varphi$. 也就是说, 我们有如下的交换图表:



(4) 令$\iota_k:\ M_k\to\bigoplus_{\alpha\in I} M_\alpha,\ m_k\mapsto(0,\cdots,m_k,\cdots,0)$. 则$\iota_k$ 是单同态, 且满足**泛性质:** 如对任意$\alpha\in I$, 均给定模同态$g_\alpha: M_\alpha\longrightarrow Y$, 则存在唯一的模同态$\psi:\bigoplus_{\alpha\in I} M_\alpha\to Y$, 使得$g_\alpha=\psi\circ\iota_\alpha$. 也就是说, 我们有如下的交换图表:



注记. 今后π_α称为$\prod_{\alpha\in I} M_\alpha$到$M_\alpha$的**典范投射**, ι_α 称为M_α到$\bigoplus_{\alpha\in I} M_\alpha$ 的**典范嵌入映射**, 命题 3.21(3) 与(4) 即通常意义下直积直和的定义.

注记. 如I是有限指标集, 我们将不区分直积与直和, 直接记它们为$\bigoplus_{\alpha\in I} M_\alpha$. 我们记$n$个$M$的直和$M\oplus\cdots\oplus M=nM$.

§3.2 群的表示

本章自此以后各节, 如无特别说明, 我们均假设F是域, G是群.

定义3.22. 群G在域F上的**群环**(group ring), 记作$F[G]$, 是由所有形如

$$\sum_{g\in G} a_g g \ (a_g \in F,\ g \in G且a_g只在有限个g\ 处非零)$$

的形式和构成的集合, 并配备加法

$$\sum_{g\in G} a_g g + \sum_{g\in G} b_g g = \sum_{g\in G}(a_g + b_g)g$$

和乘法

$$\sum_{g\in G} a_g g \cdot \sum_{g\in G} b_g g = \sum_{g\in G}\sum_{h\in G} a_g b_h gh = \sum_{g\in G}(\sum_{h\in G} a_h b_{h^{-1}g})g$$

构成的环.

我们首先注意到
(1) $F[G]$是F-代数;
(2) $F[G]$是交换环当且仅当G是阿贝尔群;
(3) $F[G]$是以G为基的F-线性空间, 故它的维数有限当且仅当G是有限群.

引理3.23. *设G是有限群, V是$F[G]$-模. 则V是有限生成$F[G]$-模当且仅当V作为F-线性空间维数有限.*

证明. 显然. □

定义3.24. 设V是F-线性空间. 群G在V上的群作用称为**线性作用**(linear action)是指对于任意$v, w \in V$, $g \in G$, $\lambda \in F$, 有

$$g(v + w) = gv + gw,\ g(\lambda v) = \lambda gv.$$

对于线性空间V, 记$\mathrm{GL}(V)$是所有V到V的可逆线性变换构成的群, 它是自同态环$\mathrm{End}_F(V)$的单位群.

命题3.25. *群G在线性空间V上的线性作用集合与G到$\mathrm{GL}(V)$的群同态集合一一对应.*

证明. 如$\rho : G \longrightarrow \mathrm{GL}(V)$是群同态, 定义群作用$g \cdot v = \rho(g)(v)$, 则此作用是线性作用. 反过来, 给定$G$在$V$上的线性作用, 定义$\rho(g)(v) = gv$. 则$\rho(g)$是$V$到自身的线性变换, 且由于$\rho(g)\rho(g^{-1})v = v$知$\rho(g)$可逆. □

定义3.26. 设G是群, F为域. 则(V, ρ) 称为G**的**F**-线性表示**(linear representation)或者简称G**的**F**-表示** 是指V 是F-线性空间并配备群同态$\rho : G \to \mathrm{GL}(V)$, 该表示的**维数**是$V$作为$F$-线性空间的维数$\dim_F V$.

命题3.27. 设G是有限群, F是域. 则下列集合存在自然双射:

(1) G的有限维F-表示集合;

(2) 有限维F-线性空间并配备G线性作用的集合;

(3) 有限生成$F[G]$-模集合.

证明. (1)和(2)间的双射即前面的命题. 如V是有限生成$F[G]$-模, 则由引理 3.23 知$\dim_F V < \infty$, 且

$$G \times V \longrightarrow V,\ (g, v) \longmapsto gv$$

是G在V上的线性作用.

反之, 对于有限维F-表示(V, ρ), 定义数乘

$$F[G] \times V \longrightarrow V,\quad \left(\sum_g a_g g, v\right) \longmapsto \sum_g a_g \rho(g)(v).$$

则V是$F[G]$模, 且是有限生成的. □

命题3.28. 设G是有限群, F是域. 设(V_1, ρ_1)与(V_2, ρ_2)是G的有限维表示. 则下列条件等价:

(1) V_1与V_2作为有限生成$F[G]$-模同构.

(2) 存在可逆F-线性变换$\varphi : V_1 \to V_2$使得对所有$g \in G$, 均有$\rho_2(g) = \varphi \circ \rho_1(g) \circ \varphi^{-1}$.

(3) 存在可逆F-线性变换

$$\varphi : V_1 \longrightarrow V_2,\ g \cdot \varphi(v) = \varphi(g \cdot v),$$

这里等式左边$g \cdot \varphi(v)$是G在V_2上的线性作用, 右边$g \cdot v$是G在V_1上的线性作用.

证明. 显然. 留作练习. □

定义3.29. 设$n \geq 1$. 称群同态$\rho :\ G \to \mathrm{GL}_n(F)$为$G$的$n$维**矩阵表示**.

对n维矩阵表示ρ_1和ρ_2, 如存在可逆矩阵P 使得$\rho_1(g) = P^{-1}\rho_2(g)P$对任意$g \in G$成立, 则称矩阵表示$\rho_1$与$\rho_2$**同构**.

命题3.30. 设G是有限群, F是域. 则存在一一对应:

(1) G的n维表示同构类集合,

(2) G的n维矩阵表示同构类集合.

证明. 令F^n是F的n维列向量空间. 一方面, 如$\rho :\ G \to \mathrm{GL}_n(F)$为群同态, 由于$\mathrm{GL}(F^n) = \mathrm{GL}_n(F)$, 我们得到$G$ 的表示(F^n, ρ).

反过来, 如(V, ρ)是n维表示, 设$\{e_1, \cdots, e_n\}$是V 的一组基, 对于$g \in G$, 令$A(g) \in \mathrm{GL}_n(F)$是线性变换$v \mapsto gv$ 在基$\{e_1, \cdots, e_n\}$下的矩阵, 即

$$g(e_1, \cdots, e_n) = (e_1, \cdots, e_n)A(g).$$

则$\widetilde{\rho} :\ G \to GL_n(F),\ g \mapsto A(g)$ 是群同态. 如另选一组基, 则得到等价的矩阵表示. 这样定义的对应将(1)中的同构类与(2)中的同构类等同起来. □

从现在开始, 我们假设F为域, G为有限群. G的F-表示是指如下的三种等价定义:

(1) (V,ρ): V是有限维F-线性空间, 且配备群同态$\rho:\ G\to \mathrm{GL}(V)$,

(2) 有限维F-线性空间V, 并配备G的一个线性作用,

(3) 有限生成$F[G]$-模.

如取定V的一组基, 则(V,ρ)给出矩阵表示$\widetilde{\rho}:\ G\to \mathrm{GL}_n(F)$, 其中$n=\dim_F V$. 不同基给出的矩阵表示等价, 即存在可逆阵$P$, $P\widetilde{\rho}(g)P^{-1}=\widetilde{\rho'}(g)$ 对任意$g\in G$成立.

定义3.31. (1) W是表示V的**子表示**(sub-representation)是指W 是V的$F[G]$-子模, 或等价地说, G 在V上的线性作用对W 封闭, 即$gW\subseteq W$ 对任意$g\in G$ 成立.

(2)表示V称为**不可约表示**(irreducible representation) 是指V作为$F[G]$-模是单模.

例3.32. (1) $V=F$并配备平凡作用, 此表示称为**平凡表示** (trivial representation). 平凡表示自然是不可约表示. 更进一步地, 任何1维表示都是不可约表示.

(2) 设X是有限G-集. 令

$$F[X]=\left\{\text{形式和}\sum_{x\in X}a_x x\mid a_x\in F,\ x\in X\right\},$$

并定义

$$g\big(\sum_{x\in X}a_x x\big)=\sum_{x\in X}a_x(gx)=\sum_{x\in X}a_{g^{-1}x}x.$$

则$F[X]$是维数为$|X|$的G表示, 称为X的**置换表示** (permutation representation).

(3) 在上例中令$X=G$, 则群环$F[G]$是G的F表示, 称为G的**正则表示** (regular representation). 它有两个子表示:

$$N=\big\langle\sum_{g\in G}g\big\rangle\cong F\quad\text{和}\quad I=\big\{\sum_{g\in G}a_g g\mid\sum_g a_g=0\big\}.$$

这里I是同态$\deg:\ F[G]\to F,\ \sum_g a_g g\mapsto\sum_g a_g$的核, 称为$F[G]$的**增广理想** (augmentation ideal).

设U和V是G的F-表示, 则$\mathrm{Hom}_F(U,V)$和$U\otimes_F V$均是F-线性空间. 对于$\varphi\in\mathrm{Hom}_F(U,V)$, 定义

$$(g\varphi)(u)=g(\varphi(g^{-1}u)).$$

则$(g,\varphi)\mapsto g\varphi$是$G$在$\mathrm{Hom}_F(U,V)$ 上的线性作用. 考虑映射

$$\alpha_g:\ U\times V\longrightarrow U\otimes_F V,\ (u,v)\longmapsto(gu)\otimes(gv).$$

则α_g 是F-双线性映射, 它诱导F-线性映射

$$\widetilde{\alpha_g}:\ U\otimes_F V\longrightarrow U\otimes_F V,\ u\otimes v\longmapsto (gu)\otimes(gv).$$

定义$g.(u\otimes v)=\widetilde{\alpha_g}(u\otimes v)=(gu)\otimes(gv)$, 则我们得到$G$在$U\otimes_F V$上的线性作用. 故$\mathrm{Hom}_F(U,V)$ 与$U\otimes_F V$ 均是G 的F-表示.

定义3.33. 对于G的F-表示U, $\mathrm{Hom}_F(U,F)$ 称为U 的**对偶表示**(dual representation), 记为U^*.

命题3.34. *设U,V是G的F-表示. 则映射*

$$\Gamma:\ U^*\otimes_F V\longrightarrow \mathrm{Hom}_F(U,V),\ \varphi\otimes v\longmapsto (u\mapsto\varphi(u)v)$$

是表示间的同构.

证明. 首先映射

$$U^*\times V\longrightarrow \mathrm{Hom}_F(U,V),\ (\varphi,v)\longmapsto(u\mapsto\varphi(u)v)$$

是F-双线性映射, 故它诱导的映射Γ 是定义良好的F-线性映射. 我们要证明Γ是单射和满射, 且是$F[G]$-模同态.

设$\{u_1,\cdots,u_n\}$是U的一组基, $\{u_1^*,\cdots,u_n^*\}$是U^* 的对偶基, 即$u_i^*(u_j)=\delta_{ij}$. 故$U^*\otimes_F V$中元素可以写为

$$\sum_k(\sum_{i=1}^n\beta_{ik}u_i^*)\otimes v_k=\sum_{i=1}^n u_i^*\otimes(\sum_k\alpha_{ik}v_k)$$

的形式, 即$\sum_i u_i^*\otimes v_i$的形式, 其中$v_i\in V$. 由于

$$\Gamma(\sum_i u_i^*\otimes v_i)(u_j)=v_j,$$

故若$\Gamma(\sum_i u_i^*\otimes v_i)=0$, 则$v_i=0$, 所以$\sum_i u_i^*\otimes v_i=0$. 即$\Gamma$ 为单射. 如$\sigma\in\mathrm{Hom}_F(U,V)$, 则对任意$u_j,\Gamma(\sum_i u_i^*\otimes\sigma(u_i))(u_j)=\sigma(u_j)$. 故$\Gamma$ 为满射.

由于

$$\begin{aligned}\Gamma(g(\varphi\otimes v))(u)=&\Gamma(g\varphi\otimes gv)(u)=(g\varphi)(u)\cdot(gv)\\=&g(\varphi(g^{-1}u))\cdot(gv)=\varphi(g^{-1}u)\cdot(gv),\end{aligned}$$

而

$$\begin{aligned}(g\Gamma(\varphi\otimes v))(u)=&g(\Gamma(\varphi\otimes v)(g^{-1}u))=g(\varphi(g^{-1}u)v)\\=&\varphi(g^{-1}u)\cdot(gv),\end{aligned}$$

故Γ是模同态. □

定理3.35 (马施克, Maschke)**.** *设域F的特征为0或与G的阶互素. 对于任意表示V, 如U 是V 的真子表示, 则存在子表示W, 使得$V = U \oplus W$. 换言之, G的任意F表示的子表示均是直和项.*

证明. 设$\pi : V \to U$为F 线性空间间的一个投射. 令

$$\pi' : \ V \longrightarrow V, \ v \longmapsto \frac{1}{|G|}\sum_{g\in G} g\pi(g^{-1}v).$$

由$\pi(g^{-1}v) \in U$知$\pi'(v) \in U$, 即π'是V到U的线性映射. 对于$u \in U$, $\pi(g^{-1}u) = g^{-1}u$, 故$\pi'(u) = u$, 即$\pi'|_U = \mathrm{Id}$. 特别地, π'为满射. 作为F-线性空间, 我们有直和$V = U \oplus \ker\pi'$. 只要证明$\ker\pi'$ 为V的子表示即可, 这等价于证明π'是$F[G]$-模同态, 即证对任意$x \in G$ 和$v \in V$, 均有$\pi'(xv) = x\pi'(v)$. 但

$$\begin{aligned}\pi'(xv) =& \frac{1}{|G|}\sum_{g\in G} g\pi(g^{-1}xv) = \frac{1}{|G|}x(\sum_{g\in G}(x^{-1}g)\pi(g^{-1}xv))\\ =& x(\frac{1}{|G|}\sum_{h=x^{-1}g\in G} h\pi(h^{-1}v)) = x\pi'(v),\end{aligned}$$

故定理得证. □

定义3.36. 如模M是单模的直和, 则称M为**半单模**(semisimple module).

推论3.37. *如F的特征为0或与$|G|$互素, 则G 的非零F-表示均是不可约表示的直和. 等价地说, 任意有限生成非零$F[G]$模是半单模.*

§3.3 半单代数

在本节, 设F是域, A是有限维F-代数. 设所有A模均是有限生成的, 即是有限维F-线性空间.

引理3.38. *设M是A模. 则下列断言等价:*

(1) *M的任意子模均是M的直和项.*

(2) *M是半单模.*

(3) *M是单子模之和.*

证明. (1)⇒ (2) ⇒ (3) 显然. 下证(3) ⇒ (1).

设N是M的子模. 令V是M的子模, 且是与N之交平凡的所有子模中的极大元. 我们要证$M = N \oplus V = N + V$. 如不然, 由于M是单子模之和, 故存在单子模S, $S \nsubseteq N + V$. 但由于S是单模, 故$S \cap (N + V) \subsetneqq S$, 故它只能是0, 这说明$N \cap (V + S) = 0$. 由于$V \subsetneqq V + S$, 这与$V$的极大性矛盾. □

引理3.39. *半单模的子模和商模都是半单模.*

证明. 如N是半单模M的子模, 则存在W, $M = N \oplus W$, 故$N \cong M/W$ 是M的商模. 故只要对商模是半单模证明即可.

如M半单, 则$M = S_1 + \cdots + S_n$. 其中S_i为单模. 令$\pi : M \longrightarrow M/N$为自然映射, 则$\pi(S_i) = (S_i + N)/N \cong S_i/S_i \cap N$. 故$\pi(S_i)$同构于$S_i$或者$\pi(S_i) = 0$. 所以$M/N = \pi(S_1) + \cdots + \pi(S_n)$ 是单模之和. 由前面引理即知M/N是半单模. □

定义3.40. 如代数A的非零A模均是半单模, 则称A是**半单代数**(semisimple algebra).

例3.41. 如G为有限群, $\mathrm{char}F = 0$或与$|G|$ 互素, 马施克定理即是说群环$F[G]$是半单F-代数.

引理3.42. *A是半单代数当且仅当它作为A模是半单模.*

证明. 一方面, 如A是半单代数, 由定义即知它作为A模是半单模. 另一方面, 如A模是半单模, 则对于任意正整数n, 自由模A^n 也是半单模, 而任意有限生成A 模是A^n 的商模, 故也是半单模. □

命题3.43. *设A是半单代数, 且作为A模, $A \cong S_1 \oplus \cdots \oplus S_r$, 其中$S_i$为单模. 则任意单$A$模均同构于某个$S_i$.*

证明. 设S为单模, $0 \neq s \in S$. 令$\varphi : A \to S$, $a \mapsto as$. 则φ 为满同态. 令$\varphi_i = \varphi|_{S_i} : S_i \to S$. 则$\varphi_i$ 不全为0. 由Schur引理, 如$\varphi_i \neq 0$, 则$\varphi_i : S_i \cong S$. □

命题3.44. *如$\{S_1, \cdots, S_r\}$是半单代数A的所有非同构单模的集合. 对于A-模M, 如$M \cong n_1S_1 \oplus \cdots \oplus n_rS_r$, 则$\{n_i\}_{i=1}^r$ 是唯一确定的.*

证明. 设$\varphi : n_1S_1 \oplus \cdots \oplus n_rS_r \cong m_1S_1 \oplus \cdots \oplus m_rS_r$. 要证$m_i = n_i$ 对于$1 \leq i \leq r$均成立. 令

$$\varphi_{ij} : \ n_iS_i \xrightarrow{\beta_i} n_1S_1 \oplus \cdots \oplus n_rS_r \xrightarrow{\varphi} m_1S_1 \oplus \cdots \oplus m_rS_r \xrightarrow{\alpha_j} m_jS_j,$$

其中α_j, β_i分别是直积和直和定义的投射和内射. 则若$i \neq j$, 由于任何$\psi : S_i \to S_j$为零同态. 由直和与直积的泛性质, 知$\varphi_{ij} = 0$. 故$\varphi = \bigoplus_{i=1}^{r} \varphi_{ii}$. 由于$\varphi$是同构, 故$\varphi_{ii} : n_iS_i \to m_iS_i$也是同构. 比较维数即知$m_i = n_i$. □

定义3.45. 如可除环D是F-代数, 称D为**F-可除代数**(division algebra).

我们下面设D是可除代数. 对于$n > 0$, D上的n阶矩阵构成的环$M_n(D)$ 也是F-代数. 令$D^n = \{(v_1, \cdots, v_n)^T \mid v_i \in D\}$ 表示D上的n维列向量空间. 则通过矩阵乘法, D^n是自然的$M_n(D)$-模.

令$E_{ij} \in M_n(D)$, 它在(i, j)位置为1, 其余位置为0. 令$P_{ij} = I_n - E_{ii} - E_{jj} + E_{ji} + E_{ij}$为对换$(i, j)$对应的置换矩阵. 令$e_i \in D^n$, 它在第$i$个位置为1, 其余位置为0.

定理3.46. 设D是可除代数, $n>0$, 则环$M_n(D)$是半单代数, 它的单模均同构于D^n, 而$M_n(D)$ 作为$M_n(D)$-模同构于nD^n.

证明. 先证D^n是单$M_n(D)$模. 设N是D^n的非零子模. 若$v=(v_1,\cdots,v_n)^T\in N$, $v\neq 0$, 不妨令$v_j\neq 0$, 则$(v_j^{-1}E_{ij})\cdot v=e_j\in N$. 再由于$P_{ij}e_j=e_i\in N$, 所以$N=D^n$. 故$D^n$是单$M_n(D)$模.

对于$1\leq k\leq n$, 令C_k是$M_n(D)$中在第k列外均为零的矩阵集合. 则C_k是$M_n(D)$ 的子模, $C_k\cong D^n$, 且$M_n(D)\cong\bigoplus\limits_{k=1}^{n}C_k\cong nD^n$. 故$M_n(D)$是半单代数, 且$D^n$ 是唯一的单$M_n(D)$模. □

定义3.47. 如代数只有平凡的双边理想, 即它作为环是单环, 则称该代数为**单代数**(simple algebra).

引理3.48. 单代数都是半单代数.

证明. 设A是单代数, Σ是A的所有单子模之和. 如S为A的单子模, $a\in A$. 则$\varphi: S\to Sa,\ s\mapsto sa$为模的满同态, 故或者$Sa=0$或$Sa\cong S$为单模. 所以总有$Sa\subset\Sigma$, 即$\Sigma$是$A$的双边理想. 由于$A$是单代数而$\Sigma\neq 0$, 故$\Sigma=A$. 所以$A$是半单模, 故为半单代数. □

定理3.49. 设D为可除代数, 则$M_n(D)$是单代数.

证明. 只要证对任意$0\neq M\in M_n(D)$, M生成的理想$J=M_n(D)$. 这等价于证明对任意$1\leq i,j\leq n$, 都有$E_{ij}\in J$. 设$M=(m_{ij})$且$m_{rs}=a\neq 0$. 则

$$E_{ss}=(a^{-1}E_{sr})\cdot M\cdot E_{ss}\in J.$$

对于一般情况,

$$E_{ij}=P_{is}E_{ss}P_{sj}\in J.$$

定理得证. □

引理3.50. 代数B的反代数B^{op}与它的自同态代数$\mathrm{End}_B(B)=\mathrm{Hom}(B,B)$ 同构.

证明. 设$\varphi\in\mathrm{End}_B(B)$, $a=\varphi(1)$. 则$\varphi(b)=b\varphi(1)=ba$对任意$b\in B$成立. 即$\varphi=\rho_a=(b\mapsto ba)$. 所以$\mathrm{End}_B(B)=\{\rho_a\mid a\in B\}$. 映射$\rho: B^{\mathrm{op}}\to\mathrm{End}_B(B)$, $a\mapsto\rho_a$ 满足

(1) $\rho_1=\mathrm{Id}$;

(2) $\rho_a+\rho_b=\rho_{a+b}$;

(3) $\rho_a\rho_b=\rho_{a\circ b}$ (这是由于$\rho_a\rho_b(x)=\rho_a(xb)=xba=\rho_{ba}(x)=\rho_{a\circ b}(x)$);

(4) ρ为双射且保持代数结构.

故ρ为代数同构. □

引理3.51. (1) 设S是单模, 则$D = \mathrm{End}_A(S)$是可除代数且$\mathrm{End}_A(nS) \cong M_n(D)$.

(2) 如$S_1, \cdots, S_r$是互不同构的单模, $U_i = n_iS_i$, $D_i = \mathrm{End}_A(S_i)$. 则

$$\mathrm{End}_A(U_1 \oplus \cdots \oplus U_r) \cong M_{n_1}(D_1) \oplus \cdots \oplus M_{n_r}(D_r).$$

证明. (1) D是可除代数是舒尔引理的结论.

将nS看作n维列向量空间S^n. 对于$\Phi = (\varphi_{ij}) \in M_n(D)$, 令

$$\Gamma(\Phi)\begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} = \Phi\begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} = \begin{pmatrix} \varphi_{11}(s_1) + \cdots + \varphi_{1n}(s_n) \\ \vdots \\ \varphi_{n1}(s_1) + \cdots + \varphi_{nn}(s_n) \end{pmatrix}.$$

则$\Gamma(\Phi) \in \mathrm{End}_A(nS)$. 我们得到代数同态

$$\Gamma: \ M_n(D) \longrightarrow \mathrm{End}_A(nS).$$

如$\Gamma(\Phi) = 0$, 取$s_i \neq 0$而对于$j \neq i$ 取$s_j = 0$. 则

$$(\varphi_{1i}(s_i), \cdots, \varphi_{ni}(s_i))^T = 0.$$

由s_i的任意性, $\varphi_{1i} = \cdots = \varphi_{ni} = 0$. 故$\Phi = 0$, Γ 为单射.

若$\Psi \in \mathrm{End}_A(nS)$, 对于$1 \leq i \leq n$, 令

$$\Psi((0, \cdots, s_i, \cdots, 0)^T) = (\psi_{1i}(s_i), \cdots, \psi_{ni}(s_i))^T.$$

则$\psi_{ij} \in \mathrm{End}_A(S) = D$. 令$\Phi = (\psi_{ij})$. 则$\Gamma(\Phi) = \Psi$. 故$\Gamma$为满射.

(2) 令$U = U_1 \oplus \cdots \oplus U_r$. 对于$\phi \in \mathrm{End}_A(U)$, 令

$$\phi_{ij} = (U_i \longrightarrow U \xrightarrow{\phi} U \longrightarrow U_j).$$

则对任意$i \neq j$, $\phi_{ij} = 0$. 故$\phi = \bigoplus_{i=1}^{r} \phi_{ii}$. 由(1)即得欲证. □

引理3.52. 如F是代数封闭域, S是单模, 则$\mathrm{End}_A(S) \cong F$.

证明. 如$\phi \in \mathrm{End}_A(S)$, 取$\lambda_\phi$为$\phi$作为线性变换的一个特征值, 则$\phi - \lambda_\phi \mathrm{Id}_S \in \mathrm{End}_A(S)$, 且它有非零核, 故不可能为同构. 由舒尔引理知$\phi - \lambda_\phi \mathrm{Id}_S = 0$, 即$\phi = \lambda_\phi \mathrm{Id}_S$. 这样$\phi \mapsto \lambda_\phi$ 定义了$\mathrm{End}_A(S)$ 到F的同构. □

引理3.53. $M_n(B)^{\mathrm{op}} \cong M_n(B^{\mathrm{op}})$.

证明. 定义映射

$$\psi: M_n(B)^{\mathrm{op}} \longrightarrow M_n(B^{\mathrm{op}}), \ X \longmapsto X^T.$$

则ψ显然是双射, 且保持加性. 令$X=(x_{ij})$, $Y=(y_{ij})$, 则

$$\begin{aligned}(\psi(X)\psi(Y))_{ij} =&(X^TY^T)_{ij}=\sum_{k=1}^{n}x_{ki}\circ y_{jk}\\ =&\sum_{k=1}^{n}y_{ik}x_{ki}=(YX)_{ji}\\ =&(YX)_{ij}^T=(X\circ Y)_{ij}^T\\ =&\psi(X\circ Y)_{ij}.\end{aligned}$$

故ψ是代数同构. □

定理3.54 (韦德伯恩, Wedderburn)**.** *代数A是半单代数当且仅当$A\cong\bigoplus_{i=1}^{r}M_{n_i}(D_i)$, 其中$D_i$是可除代数.*

证明. $\Longleftarrow$ 已证.

$\Longrightarrow$ 如A半单, 则$A\cong U_1\oplus\cdots\oplus U_r$, $U_i=n_iS_i$, S_i是互不同构的单模. 故

$$A^{\mathrm{op}}\cong\mathrm{End}_A(A)\cong M_{n_1}(\mathrm{End}_A(S_1))\oplus\cdots\oplus M_{n_r}(\mathrm{End}_A(S_r)).$$

故

$$A=(A^{\mathrm{op}})^{\mathrm{op}}\cong M_{n_1}(\mathrm{End}_A(S_1)^{\mathrm{op}})\oplus\cdots\oplus M_{n_r}(\mathrm{End}_A(S_r)^{\mathrm{op}}).$$

再由可除代数的反代数还是可除代数即得. □

命题3.55. *设$A_1,A_2,\cdots,A_n$是半单代数, $\{S_{i1},\cdots,S_{it_i}\}$ 是A_i的所有单子模同构类代表元. 则$A_1\oplus A_2\oplus\cdots\oplus A_n$也是半单代数, 它的单子模同构类代表元为$\{\widetilde{S_{ij}}=(0,\cdots,S_{ij},\cdots,0)\mid 1\le i\le n,\ 1\le j\le t_i\}$.*

证明. 由归纳法, 只要证$n=2$的情形即可.

设J为$A_1\oplus A_2$的子模. 视$A_1=A_1\oplus\{0\}, A_2=\{0\}\oplus A_2$ 令$J_i=J\cap A_i$. 则J_i为A_i的子模, 且$J_1\oplus J_2\subset J$. 另一方面, 若$(a_1,a_2)\in J$, 则$(1,0)\cdot(a_1,a_2)\in J$, 知$(a_1,0)\in J_1$. 同理$(0,a_2)\in J_2$. 故$(a_1,a_2)\in J_1\oplus J_2$. 故$A_1\oplus A_2$的子模均有$J_1\oplus J_2$的形式. 任何这样形式的集合也是$A_1\oplus A_2$ 的子模, 所以$A_1\oplus A_2$ 的单子模均有$S_1\oplus\{0\}$ 或$\{0\}\oplus S_2$ 这样的形式, 其中S_1 和S_2 分别为A_1与A_2 的单子模. 由于A_1 和A_2 均为自身的单子模之和, $A_1\oplus A_2$也是它自己的单子模之和. 故$A_1\oplus A_2$ 是半单代数.

现在只需证如S_1,S_2分别为A_1与A_2的单子模, 则$S_1\oplus\{0\}$ 与$\{0\}\oplus S_2$不同构. 如不然, 设$\phi:S_1\oplus\{0\}\longrightarrow\{0\}\oplus S_2$为$A_1\oplus A_2$-模的同构. 故存在$s_1\in S_1, s_1\neq 0$, 使得$\phi((s_1,0))=(0,s_2)\neq 0$. 但另一方面,

$$\phi((s_1,0))=\phi((1,0)(s_1,0))=(1,0)\phi((s_1,0))=(1,0)(0,s_2)=0.$$

矛盾. 至于S_1与S_1'为A_1的不同构单子模, 显然$S_1\oplus\{0\}$ 与$S_1'\oplus\{0\}$作为$A_1\oplus A_2$-模也不同构. □

推论3.56. 设$A \cong M_{n_1}(D_1) \oplus \cdots \oplus M_{n_r}(D_r)$是半单代数. 则$A$ 的单子模同构类恰有r个. 令$S_i = D_i^{n_i}$为$M_{n_i}(D_i)$的唯一的单子模, 则$\{\widetilde{S_1}, \cdots, \widetilde{S_r}\}$是$A$的单子模同构类代表元, 其中

$$\widetilde{S_i} = \{0\} \oplus \cdots \oplus S_i \oplus \cdots \{0\}.$$

故$\dim_F \widetilde{S_i} = \dim_F S_i$总是$n_i$的倍数, 且当$F$为代数封闭域时, $\dim_F \widetilde{S_i} = n_i$.

§3.4 有限群的特征标理论

在本节, 我们设G为有限群. $F = \mathbb{C}$为复数域.

由韦德伯恩定理及其推论,

定理3.57. 作为$\mathbb{C}$-代数,

$$\mathbb{C}[G] \cong M_{f_1}(\mathbb{C}) \oplus \cdots \oplus M_{f_r}(\mathbb{C}).$$

它恰好有r个单模同构类(即不可约子表示的同构类). 如令$\{V_1, \cdots, V_r\}$ 为其代表元, 令$V_1 = \mathbb{C}$是平凡表示, 则

$$\mathbb{C}[G] \cong f_1 V_1 \oplus \cdots \oplus f_r V_r, \qquad \dim V_i = f_i.$$

任何G的$\mathbb{C}$表示V均可唯一写成如下形式

$$V \cong a_1 V_1 \oplus \cdots \oplus a_r V_r, \qquad a_i \in \mathbb{Z}_{\geq 0}.$$

注记. 由于$V_1 = \mathbb{C}$, $f_1 = 1$.

推论3.58. $|G| = f_1^2 + \cdots + f_r^2 = 1 + f_2^2 + \cdots + f_r^2$.

下面我们确定互不同构的不可约表示的个数r的确切值.

定理3.59. r等于G的共轭类个数.

证明. 令Z是$\mathbb{C}[G]$的中心, 则

$$Z \cong \bigoplus_{i=1}^{r} Z(M_{f_i}(\mathbb{C})).$$

但由线性代数, 我们知道

$$Z(M_{f_i}(\mathbb{C})) = \{\lambda I_{f_i} \mid \lambda \in \mathbb{C}\} \cong \mathbb{C}.$$

故$Z \cong \mathbb{C}^r$, $\dim_{\mathbb{C}} Z = r$.

另一方面. 设$K_1, \cdots, K_s$为G的所有共轭类. 如$x = \sum_g \lambda_g g \in Z$, 由$hx = xh$知$\lambda_g = \lambda_{hgh^{-1}}$对任意$h \in G$成立. 故对于$g \in K_i$, $\lambda_g = c_i$为常值. 所以

$$x = c_1 \sum_{g \in K_1} g + \cdots + c_s \sum_{g \in K_s} g.$$

反过来, 这样的形式的x总在Z中. 故Z是以$\{\sum_{g \in K_1} g, \cdots, \sum_{g \in K_s} g\}$为基的$s$维复线性空间, 故$r = s = G$ 的共轭类个数. □

定义3.60. 设(V,ρ)是G的表示. V的**特征**(character) 是指函数

$$\chi_V:\ G\longrightarrow \mathbb{C},\ \chi_V(g)=\mathrm{tr}(\widetilde{\rho}(g))=\mathrm{tr}\rho(g),$$

其中$\widetilde{\rho}$为V对应的矩阵表示.

注记. 尽管$\widetilde{\rho}$的形式与V的基的选取有关, 但不同的$\widetilde{\rho}(g)$相似, 故迹$\mathrm{tr}(\widetilde{\rho}(g))$与基的选取以及$\widetilde{\rho}$的具体形式没有关系.

如$(V,\rho)\cong(V',\rho')$, 则$\rho'(g)=\varphi\rho(g)\varphi^{-1}$, 其中$\varphi:V\to V'$是可逆线性变换, 因此$\chi_V(g)=\chi_{V'}(g)$. 故同构的表示有相同的特征.

基于同样的理由, 我们知道$\chi_V(g)=\chi_V(hgh^{-1})$, 故$\chi_V$在$G$的共轭类上取值为常数.

定义3.61. 如函数$f:G\to\mathbb{C}$在G的共轭类上取值为常值, 则称f为**类函数**(class function).

所有类函数集合构成的r维复线性空间, 称为G的**类函数空间**, 记作$\mathfrak{Cl}$.

定义3.62. 记$\chi_i=\chi_{V_i}$ $(i=1,\cdots,r)$, 其中$V_1,\cdots,V_r$是G的所有不同构不可约表示. 特别地, 平凡表示的特征记为χ_1, 称为G的**主特征**(principal character).

正则表示的特征称为G的**正则特征** (regular character).

1维表示的特征称为**线性特征**(linear character).

引理3.63. *每个线性特征是G到乘法群$\mathbb{C}^\times$的同态. 不同构的1维表示对应不同的线性特征. 所有线性特征的集合即*$\mathrm{Hom}(G,\mathbb{C}^\times)\cong\mathrm{Hom}(G/G',\mathbb{C}^\times)=\mathrm{Hom}(G/G',S^1)$, *这里$G'$是$G$的换位子群, S^1是单位圆.*

证明. 若$V=\mathbb{C}x$是1 维表示, 则$gx=\lambda_g x$对某个$\lambda_g\in\mathbb{C}^\times$成立. 由$(gh)(x)=g(h(x))$ 即得$\lambda_g\lambda_h=\lambda_{gh}$. 因此函数$\chi_V:g\mapsto\lambda_g$是$G$到$\mathbb{C}^\times$的群同态.

若$\chi_V=\chi_{V'}$, 令$\varphi:V=\mathbb{C}x\to V'=\mathbb{C}x'$为线性映射, 使得$\varphi(x)=x'$. 则

$$\varphi(gx)=\varphi(\lambda_g x)=\lambda_g\varphi(x)=\lambda_g x'=g\varphi(x)$$

故φ是表示V到V'的同构.

设$\chi\in\mathrm{Hom}(G,\mathbb{C}^\times)$. 令$V=\mathbb{C}e$为1 维复空间. 对任意$\lambda\in\mathbb{C}$, 定义$g(\lambda e)=\lambda\chi(g)e$. 容易验证$G$在$V$上的作用是线性作用, 故$V$是$G$的复表示且$\chi_V=\chi$. □

命题3.64. *设(V,ρ)是G的n维表示, g是G中m阶元. 则*

(1) *$\rho(g)$可对角化, 特征值均为m次单位根.*

(2) *$\chi_V(g)$是n个m次单位根之和.*

(3) *$\chi_V(g^{-1})=\overline{\chi_V(g)}$.*

(4) *$|\chi_V(g)|\le n$.*

(5) *$\{g\in G\mid\chi_V(g)=n\}$是$G$的正规子群.*

证明. (1) 由$g^m = 1$知$\rho(g)^m - \mathrm{Id}_V = 0$, 故$\rho(g)$有零化多项式$X^m - 1 = 0$, 而此多项式无重根, 所以$\rho(g)$可对角化, 且其特征值均为$m$次单位根.

(2) 由(1)立得.

(3) 这是由于如$\lambda \in \mathbb{C}$, $|\lambda| = 1$. 则$\lambda^{-1} = \bar{\lambda}$, 再由(2)即得.

(4) 显然.

(5) 这个集合即$\ker(\rho)$. □

命题3.65. *设U, V是G的两个表示, 则*

(1) $\chi_{U\oplus V} = \chi_U + \chi_V$.

(2) $\chi_{U\otimes V} = \chi_U \cdot \chi_V$.

(3) $\chi_{U^*} = \overline{\chi_U}$, *其中$U^*$是$U$的对偶表示*$\mathrm{Hom}_{\mathbb{C}}(U, \mathbb{C})$.

(4) $\chi_{\mathrm{Hom}(U,V)} = \overline{\chi_U} \cdot \chi_V$.

证明. (1) 取U的一组基$\{e_1, \cdots, e_m\}$, V的一组基$\{f_1, \cdots, f_n\}$. 则$\{e_1 \oplus 0, \cdots, e_m \oplus 0, 0 \oplus f_1, \cdots, 0 \oplus f_n\}$ 是$U \oplus V$的基. 在此基下

$$\rho_{U\oplus V}(g) = \begin{pmatrix} \rho_U(g) & 0 \\ 0 & \rho_V(g) \end{pmatrix}.$$

故$\chi_{U\oplus V} = \chi_U + \chi_V$.

(2) 由于$\rho_U(g)$与$\rho_V(g)$可对角化, 故可取U 的基$\{e_1, \cdots, e_m\}$, 其中e_i 是$\rho_U(g)$ 的以λ_i 为特征值的特征向量, 取V 的基$\{f_1, \cdots, f_n\}$, 其中f_j 是$\rho_V(g)$ 以μ_j 为特征值的特征向量. 则$\{e_i \otimes f_j \mid 1 \le i \le m,\ 1 \le j \le n\}$是$U \otimes V$的基, 且$e_i \otimes f_j$ 是$\rho_{U\otimes V}(g)$ 以$\lambda_i\mu_j$ 为特征值的特征向量. 所以

$$\chi_{U\otimes V}(g) = \sum_{1\le i\le m} \sum_{1\le j\le n} \lambda_i\mu_j = \chi_U(g) \cdot \chi_V(g).$$

(3) 设$\{e_1, \cdots, e_m\}$是U的一组由$\rho_U(g)$的特征向量组成的基, $\rho_U(g)(e_i) = \lambda_i e_i$. 令$\{e_1^*, \cdots, e_m^*\}$是$U^*$的对偶基. 故由

$$(ge_i^*)(e_j) = e_i^*(g^{-1}e_j) = \lambda_j^{-1}\delta_{ij}$$

知$\rho_{U^*}(g)(e_i^*) = ge_i^* = \lambda_i^{-1}e_i^*$. 所以

$$\chi_{U^*}(g) = \sum_{i=1}^m \lambda_i^{-1} = \sum_{i=1}^m \overline{\lambda_i} = \overline{\chi_U(g)}.$$

(4) 这是由于$\mathrm{Hom}(U, V) \cong U^* \otimes V$. □

推论3.66. *群G的任意表示V的特征χ_V是不可约特征$\chi_i = \chi_{V_i}$ $(i = 1, \cdots, r)$的非负整数线性组合.*

对于类函数$\alpha, \beta \in \mathfrak{Cl}$, 定义

$$(\alpha, \beta) = \frac{1}{|G|} \sum_{g\in G} \alpha(g)\overline{\beta(g)}.$$

命题3.67. $(\ ,\ )$是复线性空间$\mathfrak{C}$上的内积, 即满足

(1) 正定性: $(\alpha,\alpha)\geq 0$对所有$\alpha\in\mathfrak{C}$ 成立, 且等号成立当且仅当$\alpha=0$.

(2) 共轭对称性: $(\alpha,\beta)=\overline{(\beta,\alpha)}$.

(3) 线性性: $(\lambda\alpha_1+\mu\alpha_2,\beta)=\lambda(\alpha_1,\beta)+\mu(\alpha_2,\beta)$对所有$\lambda,\mu\in\mathbb{C}$ 和$\alpha,\beta\in\mathfrak{C}$成立.

证明. 简单验证. □

引理3.68. 设V是G的复表示, $V^G=\{v\in V\mid gv=v$对所有$g\in G$成立$\}$. 则

$$\dim_{\mathbb{C}} V^G=\frac{1}{|G|}\sum_{g\in G}\chi_V(g).$$

证明. 记$a=\frac{1}{|G|}\sum_{g\in G}g\in\mathbb{C}[G]$, 则$ga=a$对所有$g\in G$ 成立, 故$a^2=a$. 线性变换

$$\rho_a:\ V\to V,\ v\mapsto av$$

满足$\rho_a^2-\rho_a=0$, 故可以对角化, 且它最多有两个特征值: 0 和1. 故$V=V_1\oplus V_0$, 其中V_1是1的特征子空间, V_0是0的特征子空间. 若$v\in V_1$, 则$av=v$, $gv=gav=av=v$, 故$v\in V^G$. 反过来, 如$v\in V^G$, 自然有$av=v$. 所以$V_1=V^G$. 我们知

$$\mathrm{tr}(\rho_a)=\dim_{\mathbb{C}} V_1=\dim_{\mathbb{C}} V^G.$$

另一方面$\rho_a=\frac{1}{|G|}\sum_{g\in G}\rho(g)$, 故$\mathrm{tr}(\rho_a)=\frac{1}{|G|}\sum_{g\in G}\chi_V(g)$. 引理得证. □

定理3.69. 设U 和V是G的复表示, 则

$$(\chi_U,\chi_V)=\dim_{\mathbb{C}}\mathrm{Hom}_{\mathbb{C}[G]}(U,V).$$

证明. 视$\mathrm{Hom}_{\mathbb{C}[G]}(U,V)$为$\mathrm{Hom}_{\mathbb{C}}(U,V)$的子空间. 若$\varphi\in\mathrm{Hom}_{\mathbb{C}[G]}(U,V)$, $g\in G$, 则

$$(g\varphi)(u)=g(\varphi(g^{-1}u))=gg^{-1}\varphi(u)=\varphi(u).$$

故$\varphi\in\mathrm{Hom}_{\mathbb{C}}(U,V)^G$. 反过来这也是对的. 因此

$$\mathrm{Hom}_{\mathbb{C}[G]}(U,V)=\mathrm{Hom}_{\mathbb{C}}(U,V)^G.$$

由引理 3.68即得

$$\begin{aligned}\dim_{\mathbb{C}}\mathrm{Hom}_{\mathbb{C}[G]}(U,V)=&\dim_{\mathbb{C}}\mathrm{Hom}_{\mathbb{C}}(U,V)^G\\ =&\frac{1}{|G|}\sum_{g\in G}\chi_{\mathrm{Hom}_{\mathbb{C}}(U,V)}(g)\\ =&\frac{1}{|G|}\sum_{g\in G}\overline{\chi_U}(g)\chi_V(g)\\ =&(\chi_V,\chi_U).\end{aligned}$$

故$(\chi_U,\chi_V)=\overline{(\chi_V,\chi_U)}=\dim_{\mathbb{C}}\mathrm{Hom}_{\mathbb{C}[G]}(U,V)$. □

	1	k_2	$\cdots$	k_r
	1	g_2	$\cdots$	g_r
χ_1	1	1	$\cdots$	1
χ_2	f_2	$\chi_2(g_2)$	$\cdots$	$\chi_2(g_r)$
$\vdots$	$\vdots$			
χ_r	f_r	$\chi_r(g_2)$	$\cdots$	$\chi_r(g_r)$

表 3.1: 特征标表$\mathfrak{X}$

定理3.70. *$\{\chi_1,\cdots,\chi_r\}$是内积空间$\mathfrak{cl}$的标准正交基. 故每个特征χ_V写为χ_1, $\cdots$, χ_r的非负整系数线性组合的方式唯一, 表示V是由它的特征χ_V唯一确定.*

证明. 只要证$(\chi_i,\chi_j)=\delta_{ij}$ 即可. 但由Schur引理,

$$(\chi_i,\chi_j)=\dim_{\mathbb{C}}\operatorname{Hom}_{\mathbb{C}[G]}(V_i,V_j)=\begin{cases}1, & \text{若}V_i=V_j,\\ 0, & \text{否则.}\end{cases}$$

故定理得证. □

§3.5 特征标表

§3.5.1 基本性质

由上节我们知道任何一个表示V是由它的特征χ_V(在同构意义下)唯一确定, 而每个χ_V均是不可约特征χ_i的非负整系数线性组合. 因此如果我们能确定所有不可约特征, 我们对G的表示就有了比较深刻的认识.

定义3.71. 设G是有限群, G 的共轭类记为$K_1=\{1\}$, $K_2,\cdots,K_r$, 其中K_i的阶是k_i, g_i 是它的一个代表元. G 的不可约特征集合记为$\{\chi_1,\chi_2,\cdots,\chi_r\}$, 其中$\chi_1$是主特征. 则$G$的**特征标表**(character table) 即$r\times r$图表$\mathfrak{X}=(\chi_i(g_j))_{1\le i,j\le r}$, 如表3.1 所示. 我们约定$\chi_i$所在的行是特征标表的第$i$行, g_j 所在的列是它的第j 列.

注记. 可以看出$f_i=\dim V_i$即V_i的维数, $k_i=(G:Z_G(g_i))$即g_i 的中心化子$Z_G(g_i)$ 在群G中的指数.

首先, 上节最后一个定理(定理3.70)可以表述为

定理3.72 (行正交关系, Row Orthogonality Relation)**.**

$$(\chi_i,\chi_j)=\frac{1}{|G|}\sum_{g\in G}\chi_i(g)\overline{\chi_j(g)}=\frac{1}{|G|}\sum_{t=1}^{r}k_t\chi_i(g_t)\overline{\chi_j(g_t)}=\delta_{ij}.$$

推论3.73. 如$\alpha=\sum_i a_i\chi_i$, $\beta=\sum_i b_i\chi_i$是类函数, 其中$a_i,b_j\in\mathbb{C}$, 则

$$(\alpha,\beta)=\sum_i a_i\bar{b}_i.$$

推论3.74. 设V 是G 的复表示, 令$n_i=(\chi_V,\chi_i)$, 则

$$\chi_V=\sum_{i=1}^r n_i\chi_i,$$

故$V\cong\bigoplus_{i=1}^r n_iV_i$.

推论3.75. 如α是G的特征, 且$(\alpha,\alpha)=n\leq 3$, 则α是n个互异不可约特征之和. 反之, 对任意n, 如α是n个互异不可约特征之和, 则$(\alpha,\alpha)=n$.

证明. 如$\alpha=\sum_{i=1}^r a_i\chi_i$, 则$\sum_{i=1}^r a_i^2=n\leq 3$. 由$a_i$为非负整数知$a_i=0$或1, α为n个不可约特征之和. 反之显然. □

命题3.76. 如α是线性特征, χ是不可约特征, 则$\alpha\chi$也是不可约特征.

证明. 只要证$(\alpha\chi,\alpha\chi)=1$. 事实上

$$\begin{aligned}(\alpha\chi,\alpha\chi)=&\frac{1}{|G|}\sum_{g\in G}\alpha(g)\chi(g)\overline{\alpha(g)\chi(g)}\\=&\frac{1}{|G|}\sum_{g\in G}\alpha(g)\chi(g)\alpha(g)^{-1}\overline{\chi(g)}\\=&(\chi,\chi)=1.\end{aligned}$$

□

定理3.77 (列正交关系, Column Orthogonality Relation)**.**

$$\sum_{t=1}^r\chi_t(g_i)\overline{\chi_t(g_j)}=\frac{|G|}{k_i}\delta_{ij}=|Z_G(g_i)|\delta_{ij}.$$

证明. 视$\mathfrak{X}=(\chi_i(g_j))_{1\leq i,j\leq r}$为$r\times r$矩阵. 则行正交关系说明

$$\mathfrak{X}\begin{pmatrix}\frac{k_1}{|G|}&&0\\&\ddots&\\0&&\frac{k_r}{|G|}\end{pmatrix}\overline{\mathfrak{X}}^T=I_r.$$

所以

$$\mathfrak{X}^{-1}=\begin{pmatrix}\frac{k_1}{|G|}&&0\\&\ddots&\\0&&\frac{k_r}{|G|}\end{pmatrix}\overline{\mathfrak{X}}^T.$$

故

$$\begin{pmatrix} \frac{k_1}{|G|} & & 0 \\ & \ddots & \\ 0 & & \frac{k_r}{|G|} \end{pmatrix} \overline{\mathfrak{X}}^T \mathfrak{X} = I_r.$$

展开即得列正交关系. □

§3.5.2 计算实例

上面小节的结果给出了我们求G的特征标表的一些最基本方法.

(1) 由关系式$|G| = \sum_{i=1}^{r} f_i^2$求得维数$f_i$的信息;

(2) 通过$\mathrm{Hom}(G, \mathbb{C}^\times)$得到线性特征的信息;

(3) 利用行和列正交关系;

(4) 从一些容易得到的表示的特征求它满足的关系式;

(5) 由不可约特征乘以线性特征得到新的不可约特征.

我们来看一些例子

例3.78 (循环群)**.** 设$G \cong \mathbb{Z}/n\mathbb{Z}$, g是它的一个生成元. 设ζ_n为n次本原单位根. 令

$$\chi : G \to \mathbb{C}^\times,\ g \mapsto \zeta_n.$$

则χ^i $(0 \le i \le n-1)$ 是G 的n 个不同的线性特征, 而$r \le n$, 故G的所有不可约特征为$\{\chi^i \mid 0 \le i \le n-1\}$, 其中$\chi^i(g^j) = \zeta_n^{ij}$.

例3.79 (有限阿贝尔群)**.** 由有限阿贝尔群结构定理

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \bigoplus \cdots \bigoplus \mathbb{Z}/n_s\mathbb{Z}.$$

它共有$|G| = n_1 \cdots n_s$个共轭类. 故$f_1 = \cdots = f_r = 1$, 即G的所有不可约特征都是线性特征, 即$\mathrm{Hom}(G, \mathbb{C}^\times)$的元素. 如令$G = \langle g_1 \rangle \times \cdots \times \langle g_s \rangle$, 其中$g_i$的阶为$n_i$. 则$G$的所有线性特征有如下形式$\chi = \chi_{i_1, \cdots, i_s}$:

$$\chi(g_1^{t_1} \cdots g_s^{t_s}) = \zeta_{n_1}^{i_1 t_1} \cdots \zeta_{n_s}^{i_s t_s}.$$

例3.80 (有限群的直积)**.** 设$G = G_1 \times G_2$. 设χ为G_1的不可约特征, 对应的表示是V_χ, ψ 为G_2 的不可约特征, 对应的表示是V_ψ. 则G 如下作用于$V_\chi \otimes_{\mathbb{C}} V_\psi$:

$$(g_1, g_2)(v_1 \otimes v_2) = (g_1 v_1) \otimes (g_2 v_2),$$

从而$V_\chi \otimes_{\mathbb{C}} V_\psi$ 是G-表示, 它的特征是

$$\alpha(g_1, g_2) = \chi(g_1)\psi(g_2) : G \to \mathbb{C}.$$

	1 1	3 (12)	2 (123)
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

表 3.2: S_3 的特征标表

又由于

$$\begin{aligned}(\alpha,\alpha) &= \tfrac{1}{|G_1\times G_2|}\textstyle\sum_{(g_1,g_2)\in G}\chi(g_1)\psi(g_2)\overline{\chi(g_1)\psi(g_2)}\\ &= \tfrac{1}{|G_1|}\sum_{g_1\in G_1}\chi(g_1)\overline{\chi(g_1)}\cdot\tfrac{1}{|G_2|}\sum_{g_2\in G_2}\psi(g_2)\overline{\psi(g_2)}\\ &= 1,\end{aligned}$$

故α为G的不可约特征. 同样可知如$(\chi,\psi)\neq(\chi',\psi')$, 则$(\alpha(\chi,\psi),\alpha(\chi',\psi'))=0$, 故$\alpha(\chi,\psi)$ 是两两不同的不可约特征.

如令G_1的不可约特征为$\{\chi_1,\cdots,\chi_r\}$, G_2的不可约特征为$\{\psi_1,\cdots,\psi_s\}$. 由上述讨论, 我们得到G的rs个互相正交的不可约特征$\{\alpha(\chi_i,\psi_j)\mid 1\le i\le r,\ 1\le j\le s\}$. 若$\{K_1,\cdots,K_r\}$为$G_1$的共轭类, $\{H_1,\cdots,H_s\}$ 为G_2的共轭类, 则$\{K_i\times H_j\mid 1\le i\le r, 1\le j\le s\}$是$G$的共轭类集合. 故$\{\alpha(\chi_i,\psi_j)\mid 1\le i\le r,\ 1\le j\le s\}$ 是G的所有不可约特征.

例3.81 ($G=S_3$)**.** 此时G有三个共轭类: $K_1=\{1\}$, $K_2=\{(12),(13),(23)\}$, $K_3=\{(123),(132)\}$. 由$1+f_2^2+f_3^2=6$, 不妨设$f_2\le f_3$, 知$f_2=1$, $f_3=2$. 对任意对称群S_n,

$$S_n\to\{\pm1\}\hookrightarrow\mathbb{C}^\times,\ \sigma\mapsto\mathrm{sgn}(\sigma)$$

是群同态, 故给出S_n 的一个线性特征, 此处即χ_2. 故$\chi_2((12))=-1$, $\chi_2((123))=1$.

由于χ_3与$\chi_2\cdot\chi_3$均是S_3的2维不可约特征, 故$\chi_3=\chi_2\cdot\chi_3$. 所以$\chi_3((12))=0$. 由行正交关系知$\chi_3((123))=-1$. 故我们得到表3.2.

例3.82 ($G=S_4$)**.** 由于S_4中元素共轭当且仅当它们的型相同, 故它共有5个共轭类: $\{1\}$, {两个不相交对换之积} , {三轮换}, {对换} 和{四轮换}. 它们元素个数分别为1, 3, 8, 6, 6. 由于$g\in S_4$ 与g^{-1} 同型, 故对任意特征χ, $\chi(g)=\chi(g^{-1})=\overline{\chi(g)}$, 因此$\chi(g)\in\mathbb{R}$.

与S_n的情形一样, χ_2是线性特征: χ_2(偶置换) $=1$, χ_2(奇置换) $=-1$. 故我们有$1+1+f_3^2+f_4^2+f_5^2=24$. 不妨设$f_3\le f_4\le f_5$. 则有$f_3=2$, $f_4=3$, $f_5=3$. 由于χ_3 是唯一的2 维不可约特征, $\chi_3=\chi_2\cdot\chi_3$, 故$\chi_3((12))=\chi_3((1234))=0$. 令$\chi_3((12)(34))=a$, $\chi_3((123))=b$. 则由行正交关系

$$2+3a+8b=0,\ 4+3a^2+8b^2=24.$$

	1 1	3 (12)(34)	8 (123)	6 (12)	6 (1234)
χ_1	1	1	1	1	1
χ_2	1	1	1	-1	-1
χ_3	2	2	-1	0	0
χ_4	3	-1	0	1	-1
χ_5	3	-1	0	-1	1

表 3.3: S_4 的特征标表

故$b=-1$或$b=7/11$. 但b是两个单位根之和, 它一定是代数整数, 所以$b=-1$, $a=1$.

最后要求出χ_4与χ_5. 考虑集合$X=\{1,2,3,4\}$ 生成的4 维G表示$V=\mathbb{C}[X]$: 对任意$\sigma\in S_4$, $i\in X$, $\sigma\cdot i=\sigma(i)$. 则

$$\chi_V(g)=\mathrm{tr}(\rho(g))=\sharp\{x\in X\mid gx=x\}=\begin{cases}4, & \text{若}g\in K_1,\\ 0, & \text{若}g\in K_2,\\ 1, & \text{若}g\in K_3,\\ 2, & \text{若}g\in K_4,\\ 0, & \text{若}g\in K_5.\end{cases}$$

计算$(\chi_V-\chi_1,\chi_V-\chi_1)$知其值为1. 故$\chi_V-\chi_1$ 是不可约特征, 它的维数是3. 不妨设其为χ_4. 由于$\chi_2\chi_4\neq\chi_4$, 故$\chi_2\chi_4=\chi_5$为它的另一个不可约特征. 故我们得到表3.3.

事实上, 我们还可以用其他办法求χ_4与χ_5.

若$\chi_2\chi_4=\chi_4$, 则χ_4所在行最后两个数都是0. 令$\chi_4((12)(34))=a$, $\chi_4((123))=b$. 由行正交关系知

$$\begin{cases}3+3a+8b &= 0,\\ 9+3a^2+8b^2 &= 24.\end{cases}$$

解出来的a 和b 不是代数整数, 故不可能. 所以$\chi_2\chi_4=\chi_5\neq\chi_4$. 设$\chi_4$所在行取值为3, a, b, c, d. 则χ_5所在行取值必为3, a, b, $-c$, $-d$. 由列正交关系(第一列分别与第二, 三列作运算) 知$a=-1$, $b=0$. 再由行正交关系知

$$(\chi_4,\chi_4)=1\Rightarrow 9+3+6c^2+6d^2=24,$$
$$(\chi_1,\chi_4)=0\Rightarrow c+d=0.$$

故$c=1,d=-1$或$c=-1,d=1$. 这样就求得S_4的特征标表3.3.

例3.83 ($G=A_5$)**.** 此时A_5中的元素在S_5中共有4个共轭类, 代表元分别为1, (12)(34), (123) 和(12345), 个数分别为1, 15, 20 和24. 由于(分别)存在奇置

换与1, (12)(34) 及(123) 交换, 故它们所在S_5 的共轭类还是A_5共轭类. 对于$x = (12345)$ 所在的S_5 共轭类中的元素, 它要么与x 在A_5 中共轭. 要么与$(12)x(12) = (13452)$ 在A_5 中共轭, 故此S_5共轭类中最多两个A_5 共轭类. 但由于$24 \nmid 60$, 故x 在A_5 中的共轭类(元素个数是60 的因子) 不可能等于x在S_5 的共轭类, 所以x在S_5中的共轭类恰好分为两个A_5 共轭类, 它们通过$y \mapsto (12)y(12)$一一对应. 即各有12个元素.

设$f_2 \leq f_3 \leq f_4 \leq f_5$. 由于$A_5$是单群, $\mathrm{Hom}(A_5, \mathbb{C}^\times) = \{1\}$, 知$f_2 \neq 1$. 所以$f_2 \geq 2$. 等式$1 + f_2^2 + f_3^2 + f_4^2 + f_5^2 = 60$ 有唯一解$f_2 = 3$, $f_3 = 3$, $f_4 = 4$和$f_5 = 5$.

考虑$X = \{1, 2, 3, 4, 5\}$, $V = \mathbb{C}[X]$为5维表示, 则

$$\chi_V(g) = \sharp\{x \in X | gx = x\} = \begin{cases} 5, & g = 1, \\ 1, & g = (12)(34), \\ 2, & g = (123), \\ 0, & g = (12345), \\ 0, & g = (13452). \end{cases}$$

我们计算得到$(\chi_V, \chi_V) = 2$, 故χ_V是两个不同的不可约特征之和. 由$(\chi_V, \chi_1) = 1$ 而$\dim V = 5$, 故只能是$\chi_V = \chi_1 + \chi_4$.

考虑$Y = \{\{i, j\} | \ \{i, j\} \subseteq X\}$, 则$U = \mathbb{C}[Y]$为10维表示

$$\chi_U(g) = \sharp\{y \in Y | gy = y\} = \begin{cases} 10, & g = 1, \\ 2, & g = (12)(34), \\ 1, & g = (123), \\ 0, & g = (12345), \\ 0, & g = (13452). \end{cases}$$

计算知$(\chi_U, \chi_U) = 3$, χ_U为三个不同的不可约特征之和. 再由于$(\chi_U, \chi_1) = 1$, 故$\chi_U = \chi_1 + \chi_4 + \chi_5$. 我们得到表3.4.

注意到对于K_2与K_3, a, a^{-1}同在共轭类中. 故$\chi(\sigma) = \chi(\sigma^{-1}) = \overline{\chi(\sigma)}$知$\chi(\sigma)$为实数. 现在设$\chi_2((12)(34)) = a$, $\chi_3((12)(34)) = b$. 对表3.4第2列与第1列作列正交有

$$0 = 6 + 3a + 3b;$$

第2列自身作列正交, 则有

$$4 = 1 + 1 + a^2 + b^2.$$

联立求解得$a = b = -1$.

	1 1	15 (12)(34)	20 (123)	12 (12345)	12 (13452)
χ_1	1	1	1	1	1
χ_2	3	-1	0	?	?
χ_3	3	-1	0	?	?
χ_4	4	0	1	-1	-1
χ_5	5	1	-1	0	0

表 3.4: A_5 的特征标表

	1 1	15 (12)(34)	20 (123)	12 (12345)	12 (13452)
χ_1	1	1	1	1	1
χ_2	3	-1	0	$\frac{1+\sqrt{5}}{2}$	$\frac{1-\sqrt{5}}{2}$
χ_3	3	-1	0	$\frac{1-\sqrt{5}}{2}$	$\frac{1+\sqrt{5}}{2}$
χ_4	4	0	1	-1	-1
χ_5	5	1	-1	0	0

表 3.5: A_5 的特征标表

令$\chi_2((123)) = s$, $\chi_3((123)) = t$. 同样用列正交关系, 注意到$s, t \in \mathbb{R}$, 得到$s = t = 0$.

令$\chi_2((12345)) = c$, $\chi_2((13452)) = d$. 由行正交关系. 则

$$\begin{aligned} 0 =& 3 - 15 + 12c + 12d, \\ 60 =& 9 + 15 + 12|c|^2 + 12|d|^2. \end{aligned}$$

注意到$(25)(34)x(25)(34) = x^{-1}$, 即$x, x^{-1}$在$A_5$的同一共轭类中. 故$c$与$d$均为实数. 所以

$$c + d = 1,\ c^2 + d^2 = 3.$$

解得$c = \frac{1\pm\sqrt{5}}{2}$, $d = 1 - c = \frac{1\mp\sqrt{5}}{2}$. 由于$\chi_2$与$\chi_3$的地位对称, 我们得到特征标表3.5.

§3.5.3 特征标表的更多性质与应用

引理3.84. *设N 是G 的正规子群. 设V是商群G/N的表示. 则V具有自然的G表示结构, 且V的子空间U是G-子模当且仅当U是G/N-子模. 如ψ是V作为G/N表示的特征, 则V作为G表示的特征是$\psi \circ \pi$, 其中$\pi : G \to G/N$为自然映射.*

证明. 对于$g \in G$, $v \in V$, 只要定义$gv = (gN)v$即可. 其他易验证. □

例3.85. 克莱因群$K_2 = \{1, (12)(34), (14)(23), (13)(24)\}$是$S_4$ 的正规子群, 且$S_4/K_2 \cong S_3$, 故S_4的特征标表中的χ_3可由S_3特征标表中的χ_3获得.

定义3.86. 对G的特征χ, 令$N_\chi = \{x \in G \mid \chi(x) = \chi(1)\} = \ker(\rho)$, 称为$\chi$的**核**或称为对应表示$(V, \rho)$ 的核.

特别地, 令$N_i = N_{\chi_i}$.

注记. (1) 正则表示的核平凡.

(2) $N_i = G$当且仅当$i = 1$, 即χ为主特征.

注意到N_χ 作为群同态的核, 都是G 的正规子群. 更进一步地, 我们有

命题3.87. *G的正规子群均有$\bigcap\limits_{i\in I} N_i$的形式, 其中$I$ 是$\{1, \cdots, r\}$ 的子集.*

证明. 如$N \lhd G$, 令$U = \mathbb{C}[G/N]$, 令ψ为U作为G/N表示的特征, χ为U作为G表示的特征. 由于正则表示的核平凡, 故$\chi(g) = \chi(1)$ 当且仅当$gN = N$即$g \in N$. 故$N_\chi = N$.

记$\chi = \sum\limits_{i\in I} a_i\chi_i$, 其中$a_i > 0$. 则

$$|\chi(g)| \le \sum_{i\in I} a_i|\chi_i(g)| \le \sum_i a_i\chi_i(1) = \chi(1).$$

故$g \in N_\chi$当且仅当对所有的$i \in I$, 均有$\chi_i(g) = \chi_i(1)$, 即$g \in N_i$. 故我们得到$N = N_\chi = \bigcap_{i\in I} N_i$.

反过来, $\bigcap_{i\in I} N_i$自然是G的正规子群. □

注记. 我们知道正则表示的核是平凡群, 另一方面它又是所有N_i 的交, 故$\bigcap\limits_{i=1}^{r} N_i = \{1\}$.

推论3.88. *下列条件等价:*

(1) *G是单群.*

(2) *对$i = 2, \cdots, r$, $N_i = \{1\}$.*

(3) *如存在$g \neq 1$, $\chi_i(g) = \chi_i(1)$, 则χ_i是主特征χ_1.*

证明. 显然. □

推论3.89. *G的特征标表可以用来决定G是否是可解群.*

证明. G 的特征标表决定了它的所有正规子群, 以及正规子群的包含关系, 从而决定了所有正规子群列. □

定义3.90. 设χ为G的特征. 定义$Z_\chi = \{x \in G \mid |\chi(x)| = \chi(1)\}$. 特别地, 记$Z_i = Z_{\chi_i}$.

引理3.91. (1) Z_χ是G的子群.

(2) 如$\chi=\chi_i$不可约, 则$Z_i/N_i=Z(G/N_i)$, 即群G/N_i 的中心.

(3) 特别地, 如G是非阿贝尔单群, 则对于$i>1$均有$Z_i=1$.

证明. (1) 令$\chi=\chi_V$. 由于$\chi(g)$是$\chi(1)$个单位根之和, 故$g\in Z_\chi$ 当且仅当这些单位根均相等. 等价地说, $g\in Z_\chi$即是说它对应的线性变换$\rho(g)=\lambda_g\mathrm{Id}_V$, 其中$\lambda_g$为单位根. 故若$g,\ h\in Z_\chi$, 则$\rho(gh^{-1})=\lambda_g\lambda_h^{-1}\mathrm{Id}_V$知$gh^{-1}\in Z_\chi$. 所以$Z_\chi$是$G$的子群.

(2) 如$\chi=\chi_i=\chi_{V_i}$, $gN_i\in Z(G/N_i)$, 则对所有$x\in G$, $\rho(g)\rho(x)=\rho(x)\rho(g)$. 故$\rho(g):v\mapsto gv$是$\mathbb{C}[G]$-模同态. 但由舒尔引理, $\mathrm{End}_{\mathbb{C}[G]}(V_i)\cong\mathbb{C}$. 故$\rho(g)=\mu\mathrm{Id}_V$, 所以$g\in Z_i$. 即$Z_i/N_i\supseteq Z(G/N_i)$. 另一方面的包含关系是显然的.

(3) 最后, 若G是非阿贝尔单群, 则对于$i>1$有$N_i=1$, 所以Z_i是G 的中心也只能是1. □

命题3.92. 群G的中心$Z(G)=\bigcap\limits_{i=1}^{r}Z_i$.

证明. 对于任意i, $Z(G)N_i/N_i\le Z(G/N_i)$, 故$Z(G)\le Z_i$对所有i 成立. 反过来, 如$g\in Z_i$对所有i成立, 则由

$$Z_i/N_i=Z(G/N_i),$$

故对所有$x\in G$, 换位子$[g,x]\in N_i$. 故$[g,x]\in\bigcap\limits_{i=1}^{r}N_i=\{1\}$, 即$g\in Z(G)$. □

引理3.93. 如$N\lhd G$. 则G/N的不可约特征由G的不可约特征决定.

证明. 设$\chi=\chi_V$为G的不可约特征, 且$N\le N_\chi$, 则N作用在V上平凡. 故

$$(G/N)\times V\to V,\ (gN,v)\mapsto gv$$

是良好定义的线性作用. 所以V可以视为G/N-模, 其特征$\psi(gN)=\chi_V(g)$.

另一方面, G/N 的不可约特征ψ 都可以提升到G 的不可约特征χ, 且$\chi(g)=\psi(gN)$. □

推论3.94. G的特征标表可以用来决定G是否是幂零群.

证明. 考虑上中心序列

$$1\le G_1\le G_2\le\cdots$$

其中$G_i\lhd G$, $G_i/G_{i-1}=Z(G/G_{i-1})$. 首先特征标表可以决定$Z(G)=G_1=\bigcap\limits_{i=1}^{r}Z_i$. 再由上面命题, $G/G_1=G/Z(G)$的不可约特征由G的不可约特征给出, 故特征标表可以决定

$$Z(G/Z(G))=G_2.$$

以此类推, 特征标表可以决定所有的G_i, 从而决定G是否是幂零群. □

§3.5.4 伯恩赛德定理

伯恩赛德(Burnside)定理的证明是有限群表示论的成功应用.

定理3.95 (伯恩赛德). *对于任意素数p 和q, p^aq^b阶群都是可解群.*

下面的引理即命题2.55:

引理3.96. *设$\varepsilon_1,\cdots,\varepsilon_n$为单位根. 如*

$$\gamma=\frac{\varepsilon_1+\cdots+\varepsilon_n}{n}\neq 0$$

是代数整数, 则$\varepsilon_1=\cdots=\varepsilon_n=\gamma$.

命题3.97. *设χ为G的特征. 设$g\in G$所在的共轭类K_g元素个数为$k_g=(G:Z_G(g))$. 则*

(1) *$\chi(g)$是代数整数.*

(2) *如χ不可约, 则$\dfrac{k_g\chi(g)}{\chi(1)}$ 是代数整数.*

证明. (1) 因为$\chi(g)$是单位根之和.

(2) 令$\alpha=\sum_{x\in K_g}x$, 则对于任意$h\in G$, 有$h\alpha=\alpha h$. 令χ对应的不可约表示为V. 则对任意$h\in G$, $\varphi:V\to V$, $\varphi(v)=\alpha v$ 满足$\varphi(hv)=\alpha hv=h\alpha v=h\varphi(v)$, 所以$\varphi\in \mathrm{End}_{\mathbb{C}[G]}(V)\cong\mathbb{C}$. 故存在$\lambda\in\mathbb{C}$, 使得$\alpha v=\lambda v$对任意$v\in V$成立.

现在考虑线性变换$\tau:\mathbb{C}[G]\to\mathbb{C}[G]$, $\tau(z)=z\alpha$. 则$\tau\in\mathrm{End}_{\mathbb{C}[G]}(\mathbb{C}[G])$. 视$V$为$\mathbb{C}[G]$的子模. 则对于$v\in V$, $\tau(v)=v\alpha=\alpha v=\lambda v$, 故$\lambda$是$\tau$的特征值. 令$A$是$\tau$在基$G$下的矩阵, 则

$$\det(\lambda I-A)=0.$$

由于A是$(0,1)$矩阵, 故$f(x)=\det(\lambda I-A)$是首一整系数多项式, 因此λ 是代数整数. 但

$$\begin{aligned}\lambda\chi(1)=&\mathrm{tr}(\varphi)=\sum_{x\in K_g}\mathrm{tr}(\rho(x))\\ =&\sum_{x\in K_g}\chi(x)=(G:Z_G(g))\chi(g),\end{aligned}$$

故$\lambda=\frac{k_g\chi(g)}{\chi(1)}$. □

命题3.98. *如χ为不可约特征, 则$\chi(1)\mid|G|$.*

证明. 由行正交关系, 有理数

$$\begin{aligned}\frac{|G|}{\chi(1)}=&\frac{1}{\chi(1)}\sum_{i=1}^{r}k_{g_i}\chi(g_i)\overline{\chi(g_i)}\\ =&\sum_{i=1}^{r}\frac{k_{g_i}\chi(g_i)}{\chi(1)}\cdot\overline{\chi(g_i)}\end{aligned}$$

是代数整数之和, 因此也是代数整数, 但有理代数整数就是通常的整数. □

定理3.99. *如群G中存在元素个数为素数正幂次的共轭类, 则G不是单群.*

证明. 设$g \in G$所在共轭类的阶为p^n, 其中p是素数, $n \geq 1$. 则由列正交关系

$$0 = \frac{1}{p}\sum_{i=1}^{r} \chi_i(g)\chi_i(1) = \frac{1}{p} + \sum_{i=2}^{r} \chi_i(g) \cdot \frac{\chi_i(1)}{p}.$$

故一定存在$2 \leq i \leq r$, 使得$\chi_i(g)\cdot\frac{\chi_i(1)}{p}$ 不是代数整数, 所以$p \nmid \chi_i(1)$且$\chi_i(g) \neq 0$. 对于这个i, 由于$k_g = p^n$ 与$\chi_i(1)$ 互素, 由贝祖(Bezout)等式, 故存在$a, b \in \mathbb{Z}$, 使得

$$ak_g + b\chi_i(1) = 1.$$

由命题3.97, 故$\frac{\chi_i(g)}{\chi_i(1)} = ak_g\frac{\chi_i(g)}{\chi_i(1)} + b\chi_i(g)$ 是代数整数. 由引理3.96, $|\chi_i(g)| = \chi_i(1)$, 即$Z_i \neq \{1\}$. 根据引理3.91, 当G为非交换单群时$Z_i = \{1\}$. □

伯恩赛德定理的证明. 我们对$a+b$作归纳. 如$a+b=1$, 则G是素数阶群, 自然是可解群. 故设$a+b \geq 2$.

设Q是G的Sylow q-子群. 如$Q = 1$, 则G是素数幂次群, 它不是单群. 如$Q \neq 1$, 则$Z(Q) \neq 1$. 令$1 \neq g \in Z(Q)$, 则$Q \leq Z_G(g)$. 故$k_g = (G : Z_G(g)) = p^n$对某个$n \leq a$成立. 如$n = 0$. 则$g \in Z(G)$, G不是单群; 如$n > 0$, 由上面定理, G也不是单群. 故G有非平凡真子群N. 由归纳假设, N与G/N均可解, 故G也是可解群. □

§3.6 诱导表示

§3.6.1 诱导表示和诱导特征

在构建群G的特征标表时, 常常需要构造一些表示, 并通过求它们的内积得到不可约特征的关系式. 这些表示里, 有一部分是通过商群的不可约特征提升到群G得来, 但是商群往往是很少的(比如非阿贝尔单群), 这样得到的表示常常不足以构建完整的特征标表. 诱导表示则通过子群的表示来构造新的表示.

设H是G的子群, T是H的左陪集代表元系, 即有不交并

$$G = \bigsqcup_{t\in T} tH.$$

设F是域, 对于群H的F-表示V, 则$F[G]\bigotimes_{F} V$是F-线性空间, 维数等于$|G| \cdot \dim_F V$. 视V为平凡$F[G]$-模, 则$F[G]\bigotimes_{F} V$ 上有$F[G]$模结构:

$$g(x \otimes v) = gx \otimes v.$$

令Y是$F[G]\bigotimes_F V$的F-子空间, 由

$$\{gh\otimes v-g\otimes hv\mid g\in G,h\in H,v\in V\}$$

生成. 由于对于$x\in G$,

$$x(gh\otimes v-g\otimes hv)=(xg)h\otimes v-(xg)\otimes hv,$$

故Y是$F[G]\bigotimes_F V$的$F[G]$-子模.

定义3.100. V到G上的**诱导表示**(induced representation), 记为$\mathrm{Ind}_H^G V$, 即商模$(F[G]\bigotimes_F V)/Y$.

记$g\otimes v$为$g\otimes v\in F[G]\bigotimes_F V$在$\mathrm{Ind}_H^G V$上的像.

引理3.101. *作为G的F-表示, $\mathrm{Ind}_H^G V$的维数等于$[G:H]\dim_F V$, 且若$\{e_1,\cdots,e_n\}$是V的一组F基, 则$\{t\otimes e_i\mid t\in T,\ i=1,\cdots,n\}$是$\mathrm{Ind}_H^G V$的一组基.*

证明. 设$\{e_i\}_{i=1}^n$为是V的一组基, 则Y是由

$$\{th\otimes e_i-t\otimes he_i\mid t\in T,h\in H,h\neq 1,i=1,\cdots,n\}$$

生成, 故它的维数$\leq |T|\cdot(|H|-1)\dim_F V$. 所以

$$\dim_F \mathrm{Ind}_H^G V\geq [G:H]\dim_F V.$$

另一方面, 如$g=th$, 则$g\otimes v=th\otimes v=t\otimes(hv)$是$t\otimes e_i$的线性组合. 故

$$\dim_F \mathrm{Ind}_H^G V\leq [G:H]\dim_F V.$$

所以等号成立, 且$\{t\otimes e_i\mid t\in T,\ i=1,\cdots,n\}$是$\mathrm{Ind}_H^G V$的一组基. □

注记. 也可以通过定义张量积$F[G]\bigotimes_{F[H]} V$来得到$\mathrm{Ind}_H^G V$. 这里张量积的定义需要用到$(F[G],F[H])$-双模的性质.

定义3.102. 设U是G 的F-表示(即$F[G]$-模). 视U为$F[H]$-模(即H 的F-表示), 记为$\mathrm{Res}_H^G U$, 称为U 在H 上的**限制表示**(restriction).

定理3.103 (弗罗贝尼乌斯互反律, Frobenius reciprocity law)**.** *设H是G 的子群. 设U是$F[G]$表示, V为$F[H]$表示, 则作为F-线性空间有同构*

$$\mathrm{Hom}_{F[H]}(V,\mathrm{Res}_H^G U)\cong \mathrm{Hom}_{F[G]}(\mathrm{Ind}_H^G V,U).$$

证明. 设$\varphi\in \mathrm{Hom}_{F[H]}(V,\mathrm{Res}_H^G U)$. 考虑映射

$$f_\varphi: F[G]\times V\to U,(g,v)\mapsto g\varphi(v),$$

这是F-双线性映射, 故诱导F-线性映射:

$$\widetilde{\varphi}:\ F[G]\bigotimes_F V\to U, g\otimes v\mapsto g\varphi(v).$$

由φ的性质知$Y\subset\ker\widetilde{\varphi}$, 故诱导映射$\Gamma(\varphi):\mathrm{Ind}_H^G V\to U, g\otimes v\mapsto g\varphi(v)$. 此映射保持$F[G]$-结构. 我们得到映射

$$\Gamma:\mathrm{Hom}_{F[H]}(V,\mathrm{Res}_H^G U)\to\mathrm{Hom}_{F[G]}(\mathrm{Ind}_H^G V,U),\ \varphi\mapsto\Gamma(\varphi).$$

很容易看出Γ是线性映射, 且如$\Gamma(\varphi)=0$, 则$\varphi=0$, 即Γ为单射.

如$\theta:\mathrm{Ind}_H^G V\longrightarrow U$是$F[G]$-模同态, 令

$$\varphi:V\longrightarrow\mathrm{Res}_H^G U,\ \varphi(v):=\theta(1\otimes v).$$

则φ是$F[H]$-模同态, 且

$$\Gamma(\varphi)(g\otimes v)=g\varphi(v)=g\cdot\theta(1\otimes v)=\theta(g\otimes v).$$

即$\Gamma(\varphi)=\theta$. 故Γ为满射. □

现在设$F=\mathbb{C}$. 如V作为$\mathbb{C}[H]$模的特征为φ, 我们记φ^G为$\mathbb{C}[G]$模Ind_H^G的特征, 称为φ的**诱导特征**(induced character). 如χ是$\mathbb{C}[G]$模U的特征, 记$\chi|_H$为$\mathbb{C}[H]$-模$\mathrm{Res}_H^G U$的特征, 称为χ 在H 上的**限制特征**.

定理3.104. *设H是G的子群. 设φ是$\mathbb{C}[H]$-模V的特征, χ是$\mathbb{C}[G]$模U的特征. 则*

$$(\varphi,\chi|_H)_H=(\varphi^G,\chi)_G.$$

证明. 由弗罗贝尼乌斯互反律, 及

$$(\varphi,\chi|_H)_H=\dim_{\mathbb{C}}\mathrm{Hom}_{\mathbb{C}[H]}(V,\mathrm{Res}_H^G U),\ \ (\varphi^G,\chi)_G=\dim_{\mathbb{C}}\mathrm{Hom}_{\mathbb{C}[G]}(\mathrm{Ind}_H^G V,U)$$

即得. □

命题3.105. *设$H\le G$, T是H的左陪集代表元系. 设V是H的复表示, 特征为χ. 则*

$$\chi^G(g)=\sum_{t\in T,t^{-1}gt\in H}\chi(t^{-1}gt).$$

证明. 令$\{e_i\}_{i\in I}$为V的一组基, 则$\{t\otimes e_i\mid t\in T,i\in I\}$ 是$\mathrm{Ind}_H^G V$的一组基. 令$\rho^G(g)$为线性变换$\mathrm{Ind}_H^G V\to\mathrm{Ind}_H^G V$, $t\otimes v\mapsto gt\otimes v$. 则$\chi^G(g)=\mathrm{tr}(\rho^G(g))$.

对于$t\in T$, $g\in G$, 记$gt=sh$, 其中$s\in T$, $h\in H$. 则$g(t\otimes V)=s\otimes hV\subseteq s\otimes V$.

若$s\neq t$, 即$t^{-1}gt\notin H$, 则$\rho^G(g)(t\otimes V)\subseteq s\otimes V\neq t\otimes V$. 它不贡献$\chi^G(g)$.

若$s=t$, 即$t^{-1}gt\in H$, 则

$$\rho^G(g)(t\otimes v)=g(t\otimes v)=gt\otimes v=t\cdot(t^{-1}gt)\otimes v=t\otimes(t^{-1}gt)v.$$

故$g:t\otimes v\to t\otimes v$相当于$t^{-1}gt:V\to V$. 它对$\chi^G(g)$产生的贡献是$\chi(t^{-1}gt)$. 综合起来故命题得证. □

推论3.106. 设$H \leq G$, 设χ为H的特征, $g \in G$. 则

$$\chi^G(g) = \frac{1}{|H|} \sum_{x \in G, x^{-1}gx \in H} \chi(x^{-1}gx).$$

证明. 若$x = th$, $t \in T$而$h \in H$, 则

$$x^{-1}gx = h^{-1}(t^{-1}gt)h.$$

则$x^{-1}gx \in H$ 当且仅当$t^{-1}gt \in H$. 此时它们在同一H-共轭类中. 故

$$\begin{aligned}\chi^G(g) =& \sum_{t \in T, t^{-1}gt \in H} \chi(t^{-1}gt) \\ =& \sum_{t \in T, t^{-1}gt \in H} \frac{1}{|H|} \sum_{x \in tH} \chi(x^{-1}gx) \\ =& \frac{1}{|H|} \sum_{x \in G, x^{-1}gx \in H} \chi(x^{-1}gx).\end{aligned}$$

□

命题3.107. 设χ是$H \leq G$的特征. 对于$g \in G$, 令s为g所在的G共轭类中H共轭类的个数. 如$s = 0$, 则$\chi^G(g) = 0$. 如$s > 0$, 设l为g所在的G共轭类元素个数, 设$h_1, \cdots, h_s$为这s个H共轭类的代表元, 设$k_1, \cdots, k_s$ 为共轭类中元素的个数. 则

$$\chi^G(g) = \sum_{i=1}^{s} \frac{|Z_G(g)|}{|Z_H(h_i)|} \chi(h_i) = \sum_{i=1}^{s} (G : H) \cdot \frac{k_i}{l} \chi(h_i).$$

证明. 如$s = 0$. 则不存在$x \in G$, 使得$x^{-1}gx \in H$, 由上面推论知$\chi^G(g) = 0$.

如$s > 0$. 令$X_i = \{x \in G \mid x^{-1}gx \in H,\ x^{-1}gx$与$h_i$共轭$\}$. 则$\coprod_{i=1}^{s} X_i = \{x \in G \mid x^{-1}gx \in H\}$. 故

$$\begin{aligned}\chi^G(g) =& \frac{1}{|H|} \sum_{x \in G, x^{-1}gx \in H} \chi(x^{-1}gx) \\ =& \frac{1}{|H|} \sum_{i=1}^{s} \sum_{x \in X_i} \chi(x^{-1}gx) \\ =& \frac{1}{|H|} \sum_{i=1}^{s} |X_i| \cdot \chi(h_i).\end{aligned}$$

只要求出$|X_i|$即可.

设$t_i^{-1}gt_i = h_i$. 则对于$c \in Z_G(g)$, $h \in H$, $(ct_ih)^{-1}g(ct_ih) = h^{-1}h_ih$ 在h_i所在的H-共轭类中, 故$Z_G(g)t_iH \subset X_i$. 另一方面, 如$x \in X_i$, 则存在$h \in H$,

$$x^{-1}gx = h^{-1}h_ih = (t_ih)^{-1}g(t_ih).$$

故$xh^{-1}t_i^{-1} \in Z_G(g)$. 所以$x \in Z_G(g)t_iH$. 故我们得到$X_i = Z_G(g)t_iH$. 因此

$$|X_i| = |Z_G(g)t_iH| = \frac{|Z_G(g)| \cdot |t_iHt_i^{-1}|}{|Z_G(g) \bigcap t_iHt_i^{-1}|} = \frac{|Z_G(g)| \cdot |H|}{|H \bigcap t_i^{-1}Z_G(g)t_i|}.$$

	1 1	3 (12)	2 (123)
ψ_1	1	1	1
ψ_2	1	-1	1
ψ_3	2	0	-1

表 3.6: S_3 的特征标表

	1 1	3 (12)(34)	8 (123)	6 (12)	6 (1234)
χ_1	1	1	1	1	1
χ_2	1	1	1	-1	-1
χ_3	2	2	-1	0	0
χ_4	3	-1	0	1	-1
χ_5	3	-1	0	-1	1

表 3.7: S_4 的特征标表

但$t_i^{-1}Z_G(g)t_i = Z_G(t_igt_i^{-1}) = Z_G(h_i)$, $H\bigcap Z_G(h_i) = Z_H(h_i)$, 因此我们得到第一个等式. 第二个等式是由于$|Z_G(g)| = \frac{|G|}{l}$, 而$|Z_H(h_i)| = \frac{|H|}{k_i}$. 故命题得证. □

§3.6.2 利用诱导特征计算特征标表

例3.108 ($G = S_4$)**.** 取$H = S_3$. 我们知H的特征标表为表3.6. S_4有5个共轭类, 2个1维表示. 由

$$(\psi_1^G, \chi_1)_G = (\psi_1, \chi_1|_H)_H = 1,\ (\psi_1^G, \chi_2)_G = (\psi_1, \psi_2)_H = 0,$$

知$\psi_1^G - \chi_1$的维数是3, 且是χ_3, χ_4, χ_5的和. 故$\psi_1^G - \chi_1 = \chi_4$或$\chi_5$, 不妨设为$\chi_4$. 由于没有$h \in H$与(12)(34)或(1234)共轭, 故$\chi_4((12)(34)) = \chi_4((1234)) = -1$

由于(123)所在的G共轭类有8个元素, 只包含1个H共轭类, 有2个元素. (12)所在G共轭类阶为6, 只包含1个H共轭类, 阶为3. 则由命题3.107,

$$\psi_1^G((123)) = 4 \cdot \frac{2}{8}\psi_1((123)) = \psi_1((123)) = 1,$$

故$\chi_4((123)) = 0$;

$$\psi_1^G((12)) = 4 \cdot \frac{3}{6}\psi_1((12)) = 2,$$

故$\chi_4((12)) = 1$. 这样$\chi_2\chi_4 \neq \chi_4$, 故$\chi_2\chi_4 = \chi_5$.

由$\chi_2\chi_3 = \chi_3$ 知$\chi_3((1234)) = \chi_3((12)) = 0$. 再由列正交关系知$\chi_3((12)(34)) = 2$, $\chi_3((123)) = -1$. 这样我们就完成了S_4 的特征标表3.7.

	1 1	10 (12)	15 (12)(34)	20 (123)	20 (123)(45)	30 (1234)	24 (12345)
χ_1^G	5	3	1	2	0	1	0
χ_2^G	5	-3	1	2	0	-1	0
χ_3^G	10	0	2	-2	0	0	0
χ_4^G	15	3	-1	0	0	-1	0
χ_5^G	15	-3	-1	0	0	1	0

表 3.8: $H = S_4$在$G = S_5$中的诱导表示

例3.109. 我们再由$H = S_4$的特征标表来看$G = S_5$的特征标表. S_5有7个共轭类.

设$\chi_1, \chi_2, \chi_3, \chi_4, \chi_5$由$S_4$的特征标表 3.7 给出. 对于$g_2 = (12)$, $g_3 = (12)(34)$, $g_4 = (123)$和$g_6 = (1234)$, 它们在H上均只有1个共轭类, 阶分别为6, 3, 8 和6. 故由命题3.107, 可得

$$\chi_i^G(g_2) = 5 \cdot \frac{6}{10}\chi_i(g_2) = 3\chi_i(g_2),$$

$$\chi_i^G(g_3) = 5 \cdot \frac{3}{15}\chi_i(g_3) = \chi_i(g_3),$$

$$\chi_i^G(g_4) = 5 \cdot \frac{8}{20}\chi_i(g_4) = 2\chi_i(g_4),$$

$$\chi_i^G(g_6) = 5 \cdot \frac{6}{30}\chi_i(g_6) = \chi_i(g_6).$$

由$(\chi_1^G, \varphi_1) = 1$, $(\chi_1^G, \chi_1^G) = 2$, 知$\chi_1^G - \varphi_1$ 为不可约特征. 不妨设为φ_3. 由$(\chi_1^G, \varphi_2) = 1$ 而$(\chi_2^G, \chi_2^G) = 2$, 知$\chi_2^G - \varphi_1$为不可约特征, 且经计算不是φ_3, 不妨设为φ_4.

由

$$1 + 1 + 16 + 16 + f_5^2 + f_6^2 + f_7^2 = 120,$$

知$f_5^2 + f_6^2 + f_7^2 = 86$. 再由$f_i \mid |G|$, 知$f_i \neq 7$. 故$f_5 = 5$, $f_6 = 5$, $f_7 = 6$.

由$(\chi_3^G, \chi_3^G) = 2$, 而$(\chi_3^G, \varphi_3) = (\chi_3^G, \varphi_4) = 0$, 知$\chi_3^G = \varphi_5 + \varphi_6$. 由$\varphi_2\varphi_7 = \varphi_7$知$\varphi_7(g_2) = \varphi_7(g_5) = \varphi_7(g_6) = 0$. 再由列正交关系知$\varphi_5(g_2) = \pm 1$, $\varphi_6(g_2) = \mp 1$. 故$\varphi_6 = \varphi_2\varphi_5$. 从而得出$\varphi_5$与$\varphi_6$的值. 再由列正交关系即得$\varphi_7$的所有取值, 见表3.9.

例3.110 (二面体群)**.** 设G是正n边形的二面体群$D_n = \langle \sigma, \tau \mid \sigma^n = \tau^2 = 1, \tau\sigma\tau = \sigma^{-1} \rangle$. 它是$2n$阶群, 有1个$n$阶正规子群$H = \langle \sigma \rangle$, $T = \{1, \tau\}$ 是H的陪集代表元系.

如n是奇数, G的共轭类为$\{1\}$, $\{\sigma^i, \sigma^{n-i}\}_{1 \leq i \leq \frac{n-1}{2}}$, $\{\tau, \cdots, \tau\sigma^{n-1}\}$, 阶分别为1, 2(共$\frac{n-1}{2}$个)和$n$, 共$\frac{n+3}{2}$个共轭类. 如$n$是偶数, G的共轭类为$\{1\}$, $\{\sigma^{\frac{n}{2}}\}$, $\{\sigma^i, \sigma^{n-i}\}_{1 \leq i < \frac{n}{2}}$, $\{\tau, \tau\sigma^2, \cdots, \tau\sigma^{n-2}\}$ 和$\{\tau\sigma, \tau\sigma^3, \cdots, \tau\sigma^{n-1}\}$, 阶分别为1, 1, 2(共$\frac{n}{2} - 1$个), $\frac{n}{2}$ 和$\frac{n}{2}$, 共$\frac{n}{2} + 3$个共轭类.

	1 1	10 (12)	15 (12)(34)	20 (123)	20 (123)(45)	30 (1234)	24 (12345)
φ_1	1	1	1	1	1	1	1
φ_2	1	-1	1	1	-1	-1	1
φ_3	4	2	0	1	-1	0	-1
φ_4	4	-2	0	1	1	0	-1
φ_5	5	1	1	-1	1	-1	0
φ_6	5	-1	1	-1	-1	1	0
φ_7	6	0	-2	0	0	0	1

表 3.9: S_5的特征标表

令$\zeta_n = \exp(\frac{2\pi i}{n})$. 我们知$H$的不可约特征是线性特征$\chi^j$ $(0 \le j < n)$, 其中$\chi^j(\sigma) = \zeta_n^j$. 对于$0 \le j < n$,

$$(\chi^j)^G(x) = \begin{cases} \zeta_n^{ij} + \zeta_n^{-ij}, & \text{如} x = \sigma^i, \\ 0, & \text{如} x = \tau\sigma^i. \end{cases}$$

当n为奇数, $1 \le j \le \frac{n-1}{2}$时; 或$n$为偶数, $1 \le j \le \frac{n}{2} - 1$时

$$((\chi^j)^G, (\chi^j)^G) = 1.$$

故$(\chi^j)^G$是D_n的2维不可约特征.

对于线性特征, 若n为奇数, 则G/H为2阶群, 对应两个线性特征: 主特征χ_1 及χ_2, 这里$\chi_2(\sigma^i) = 1$ 而$\chi(\tau\sigma^i) = -1$. 若n 为偶数, 则$\langle\sigma^2\rangle$是G的正规子群, $G/\langle\sigma^2\rangle$ 同构于克莱因群K_2, 它生成四个线性特征

$$\chi_1 : \sigma \mapsto 1,\ \tau \mapsto 1,$$
$$\chi_2 : \sigma \mapsto 1,\ \tau \mapsto -1,$$
$$\chi_3 : \sigma \mapsto -1,\ \tau \mapsto 1,$$
$$\chi_4 : \sigma \mapsto -1,\ \tau \mapsto -1.$$

我们构造的这些不可约特征两两不同, 个数恰好是D_n的共轭类个数, 故得到了D_n的所有不可约特征构成的集合: $\{\chi_1, \chi_2, \chi^j | \ 1 \le j \le \frac{n-1}{2}\}$ (如n 为奇数) 或者$\{\chi_1, \chi_2, \chi_3, \chi_4, \chi^j | \ 1 \le j \le \frac{n}{2} - 1\}$ (如n 为偶数). 由此自然写出D_n 的特征标表, 我们不再赘述.

习 题

下面习题中我们都假设F是域, G 是有限群, A 是有限维含幺F代数, 所有的模都是有限生成的.

习题3.1. 设A是n维F-代数. 证明: A可以嵌入为矩阵代数$M_n(F)$的F-子代数.

习题3.2. (1) 证明: 群环$F[G] \cong F[G]^{\mathrm{op}}$.

(2) 证明: 四元数体$\mathbb{H} \cong \mathbb{H}^{\mathrm{op}}$.

(3) 给出一个环R的例子, 使得$R \ncong R^{\mathrm{op}}$.

习题3.3. 设A和B是F-代数, 证明$(A \otimes_F B)^{\mathrm{op}} \cong A^{\mathrm{op}} \otimes_F B^{\mathrm{op}}$.

习题3.4. 设U和V是有限生成$F[G]$模, 它们作为F线性空间的维数均是n. 分别取定U和V的基,则它们对应的表示即可视为群同态$\rho : G \to \mathrm{GL}_n(F)$与$\tau : G \to \mathrm{GL}_n(F)$. 证明: $U \cong V$当且仅当存在$M \in \mathrm{GL}_n(F)$, 使得对任意$g \in G$, $\tau(g) = M^{-1}\rho(g)M$.

习题3.5. 证明命题*3.28*.

习题3.6. 对于正则表示$F[G]$, 令$N = F\sum_g g = \{\sum_g \lambda g : \lambda \in F\}$, $I = \{\sum_g n_g g \mid \sum_g n_g = 0\}$.

(1) 证明N是$F[G]$的子模, $N \cong F$, 且如果$F[G]$的子模M同构与F, 则$M = N$.

(2) 证明I是$F[G]$的子模, $F[G]/I \cong F$, 且如果$F[G]$的子模M的商模$F[G]/M \cong F$, 则$M = I$.

(3) 如果$\mathrm{char}F \mid |G|$, 证明$N \subseteq I$, 并说明I不是$F[G]$的直和项.

习题3.7. 设n是正整数, B是A-模, U是B的一个n维F-子空间. 若M是任意A-模, U到M的任意F-线性变换均可扩充为B到M的A-模同态, 证明: $B \cong A^n$.

习题3.8. 设$T_n(F)$是上三角形n阶方阵构成的F-代数. 试求$T_n(F)$的最大幂零理想.

习题3.9. 设U是A-模. 则U的n-维列向量空间U^n是$M_n(A)$-模. 证明:

(1) U是单A-模当且仅当U^n是单$M_n(A)$-模.

(2) 对任意A-模U和V, $\mathrm{Hom}_A(U, V) \cong \mathrm{Hom}_{M_n(A)}(U^n, V^n)$.

(3) 如果M是$M_n(A)$-模, 则存在A-模U, $M \cong U^n$.

习题3.10. 证明A是单A-模当且仅当A是可除代数.

习题3.11. 证明M是单A-模当且仅当M是单$A/\mathrm{Jac}(A)$-模, 此处$\mathrm{Jac}(A)$指A的雅各布森根, 即A的最大幂零理想.

习题3.12. 设S是单$\mathbb{C}[G]$-模, U是1维$\mathbb{C}[G]$模, 证明: $S \otimes U$也是单模.

习题3.13. 证明$\mathbb{C}$是唯一的可除单$\mathbb{C}$-代数.

习题3.14. 设k 是域, V 是k-线性空间, $T : V \to V$ 是线性变换, $m(x)$ 是T 的最小多项式. 证明: 环$k[x]/(m(x))$ 是半单环当且仅当线性变换T 可对角化, 也就是说$m(x)$ 是不同线性因子的乘积.

习题3.15. 对于域F, 设$\mathrm{sgn} : S_n \to \{\pm 1\} \leq F$ 是符号映射. 令$\mathrm{Sig}(F) = F$, 且对$\gamma \in S_n$ 和$a \in F$, 令$\gamma a = \mathrm{sgn}(\gamma)a$, 这样$\mathrm{Sig}(F)$ 构成$F[S_n]$-模. 证明$\mathrm{Sig}(F)$是$F[S_n]$-模.

习题3.16. 设G 是有限群, k 与K 分别是特征p 与特征q的代数封闭域, 且p与q 与$|G|$ 互素.

(1) 证明$k[G]$ 与$K[G]$ 有相同数目的不可约分量.

(2) 证明: G在k 与K 上的不可约表示有相同的次数.

习题3.17. 设U是$\mathbb{C}[G]$模, 证明: U 是单模当且仅当它的对偶U^* 是单模.

习题3.18. 设χ是G的不可约特征, $\mu_{|G|}$是$|G|$-次单位根构成的群. 证明: $\{g \in G \mid \chi(g)/\chi(1) \in \mu_{|G|}\}$ 是G 的正规子群.

下面习题中我们都假设G 是有限群, $\mathfrak{X}$ 是G的特征标表, H 为G 的子群, F 为域. 我们假设所有出现的$F[G]$-模和$F[H]$-模是有限生成的.

习题3.19. 试求$\mathfrak{X}$的行列式, 并证明$\mathfrak{X}$ 中每行的和是非负整数.

习题3.20. 设G的阶是奇数. 证明: 如χ是G的实值不可约特征, 则$\chi = \chi_1$为主特征.

习题3.21. 设χ 是2 维表示的特征, $x \in G$ 是2 阶元. 证明: $\chi(x)$ 等于2, 0 或者-2. 试将此结论推广到n 维表示.

习题3.22. 决定正5边形的二面体群$D_5 = \langle \sigma, \tau \mid \sigma^5 = \tau^2 = 1, \tau\sigma\tau = \sigma^{-1} \rangle$ 的特征标表.

习题3.23. 决定对称群S_5的特征标表.

习题3.24. 设W是$F[G]$-模, 它由$F[H]$-模V生成, 并设$\dim_F W = (G : H) \dim_F V$. 证明: $W = \mathrm{Ind}_H^G V$.

习题3.25. 设g 是有限群G 中的m 阶元. 设k 与m 互素. 如果g 与g^k 在G 的同一个共轭类里, 证明对于任意特征χ, $\chi(g) \in \mathbb{Z}$.

习题3.26. 设$\rho : G \to \mathrm{GL}(V)$ 是G 的复表示, 对应的特征是ψ. 令$W = \{v \in V \mid \rho(g)(v) = v\}$ 是V 中所有G-作用不动点构成的子空间. 证明$\dim W = (\psi, \chi_1)$, 这里χ_1 是主特征.

习题3.27. 设V是G的复表示, ψ是对应的特征. 设$\mathcal{B}$是V的一组基, 且G作用保持$\mathcal{B}$不变. 令$\mathcal{B}_1, \cdots, \mathcal{B}_t$是$\mathcal{B}$的轨道, 令$V_i$是$\mathcal{B}_i$生成的子空间. 令$W = \{v \in V \mid \rho(g)(v) = v\}$是$V$中所有$G$-作用不动点构成的子空间. 证明:

(1) 作为G的表示, $V = V_1 \oplus \cdots \oplus V_t$.

(2) 每个V_i有唯一一个一维子表示.

(3) $\dim W = t$.

习题3.28. 证明作为F-线性空间, 映射

$$\mathrm{Hom}_{F[H]}(\mathrm{Res}^G_H U, V) \to \mathrm{Hom}_{F[G]}(U, \mathrm{Ind}^G_H V),\ \varphi \mapsto (u \mapsto \sum_{t \in T} t \otimes \varphi(t^{-1}u))$$

是同构映射, 其中T是H关于G的左陪集代表元系.

习题3.29. 设p, q为素数且$p \equiv 1 \bmod q$. 证明存在唯一的pq阶非阿贝尔群G, 并求它的特征标表.

习题3.30. 设S是有限集并配备G的作用, 令$\mathbb{C}[S]$为S生成的$\mathbb{C}$-线性空间, ψ为对应的特征. 设S的G-轨道个数是m. 证明: $(\psi, \chi_1)_G = m$.

习题3.31. 定义函数$\psi : G \to \mathbb{C}$, $\psi(g) = |\{(x, y) \in G \times G \mid [x, y] = xyx^{-1}y^{-1} = g\}|$. 证明:

$$\psi = \sum_{i=1}^{r} \frac{|G|}{\chi_i(1)} \chi_i.$$

故ψ是G的一个特征.

习题3.32. 试将交错群A_4中所有不可约特征在A_5上的诱导特征分解为A_5上不可约特征之和的形式.

习题3.33. 设$x, y \in G$. 证明x与y共轭当且仅当对G的所有不可约特征χ均有$\chi(x) = \chi(y)$.

习题3.34. 设G是有限群, N是G的正规子群, T是G关于N的陪集表示. 设χ是N的不可约特征. 给定元素$t \in T$, 定义N上的函数$\chi_t(x) = \chi(t^{-1}xt)$.

(1) 证明χ_t是N的不可约特征.

(2) 证明: 诱导特征χ^G是G的不可约特征当且仅当χ_t $(t \in T)$两两不同.

习题3.35. 设H是G的指数为2的子群, $\rho : G \to \mathrm{GL}(V)$为$G$的表示. 令$\rho' : G \to \mathrm{GL}(V)$为映射, 取值如下: 对于$g \in H$, $\rho'(g) = \rho(g)$; 对于$g \notin H$, $\rho'(g) = -\rho(g)$.

(1) 证明: ρ'也是G的表示.

(2) 试确定ρ, ρ'与$\rho|_H$的关系.

习题3.36. 对于$g \in G$, 证明: g的中心化子$Z_G(g)$的阶等于$\sum_{i=1}^{r} |\chi_i(g)|^2$.

习题3.37. 设$\rho : G \to \mathrm{GL}_n(\mathbb{C})$ 是表示. 证明

(1) $\rho^* : G \to \mathrm{GL}_n(\mathbb{C})$, $g \mapsto \rho(g^{-1})^T$ 是G 的表示. 此表示称为ρ 的**逆步表示**(*contragredient representation*).

(2) 证明$\chi_{\rho^*}(g) = \overline{\chi_\rho(g)}$.

习题3.38. 对于四元数群$Q_8 = \langle \sigma, \tau \mid \sigma^4 = 1,\ \sigma^2 = \tau^2,\ \tau\sigma\tau^{-1} = \sigma^{-1} \rangle$, 证明存在表示$\rho : Q \to \mathrm{GL}_2(\mathbb{C})$, 使得

$$\sigma \mapsto \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}, \quad \tau \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

并证明ρ是不可约表示.

习题3.39. 求Q_8 的特征标表.

习题3.40. 设有限域$\mathbb{F}_5$上的矩阵群

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \mid a, b \in \mathbb{F}_5,\ a \neq 0 \right\},$$

子群

$$H = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \mid a \in \mathbb{F}_5^\times \right\}, \quad N = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{F}_5 \right\}.$$

(1) 求群H和群N的所有不可约特征.

(2) 求群G的所有不可约特征.

习题3.41. 设$\rho : G \to \mathrm{GL}(V)$ 和$\rho' : G \to \mathrm{GL}(W)$ 是表示.

(1) 证明$\rho \otimes \rho' : G \to \mathrm{GL}(V \otimes W)$, $(\rho \otimes \rho')g = \rho(g) \otimes \rho'(g)$ 是表示.

(2) 求$\rho \otimes \rho'$ 的特征.

参考文献

[1] 冯克勤, 余红兵. **整数与多项式**. 北京: 高等教育出版社, 施普林格出版社, 1999.

[2] 冯克勤, 李尚志, 查建国, 章璞. **近世代数引论**. 合肥: 中国科学技术大学出版社, 2002.

[3] 欧阳毅, 申伊塊. **代数学I: 代数学基础**. 北京: 高等教育出版社, 2016年.

[4] 欧阳毅, 叶郁, 陈洪佳. **代数学II: 近世代数**. 北京: 高等教育出版社, 2017.

[5] Alperin J.L., Bell R. B., **Groups and Representations**. Graduate Texts in Mathematics **162**, Berlin-New York-Heidelberg, Springer, 1995.

[6] Artin M., **Algebra, 2nd ed**. Boston, Addison Wesley, 2010. (中译本: 郭晋云译. 代数. 北京: 机械工业出版社, 2009)

[7] Buchberger B., **An Algorithm for Finding the Basis Elements of the Residue Class Ring of a Zero Dimensional Polynomial Ideal**. Ph.D. dissertation, University of Innsbruck, 1965. English translation by Michael Abramson in Journal of Symbolic Computation **41** (2006): 471-511.

[8] Buchberger B., **An Algorithmic Criterion for the Solvability of a System of Algebraic Equations**. Aequationes Mathematicae **4** (1970): 374 – 383. English translation by M. Abramson and R. Lumbert in Gröbner Bases and Applications (B. Buchberger, F. Winkler, eds.). London Mathematical Society Lecture Note Series **251**, Cambridge University Press, 1998, 535-545.

[9] Cartan H., Ellenberg S., **Hoomological Algebra**. Princeton Mathematical Series **19**, Princeton, Princeton University Press, 1999.

[10] Cox D., Little J., O'Shea D., **Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra, 2nd ed.** New York, Springer, 2004.

[11] Dummit D. S., Foote R. M., **Abstract Algebra, 3rd ed.** New York, John Wiley & Sons Inc., 2003.

[12] Hungerford T. W., **Algebra**. Graduate Texts in Mathematics **73**, Berlin-New York-Heidelberg, Springer, 1980.

[13] Jacobson N., **Basic Algebra I & II, 2nd ed.** New York, W. H. Freeman and Co., 1985, 1989.

[14] Kostrikin A. I., **Exercises in Algebra: A Collection of Exercises in Algebra, Linear Algebra and Geometry, 2nd revised ed.** Algebra, Logic and Applications Series, Vol. 6. Amsterdam, Gordon and Breach Publishers, 1996.

[15] Lang S., **Algebra, revised 3rd ed**. Graduate Texts in Mathematics **211**. Berlin-New York, Springer, 2002.

[16] Rotman J.J., **Advanced Modern Algebra, revised 2nd ed.** Providence, American Mathematical Society, 2003.

[17] Rotman J.J., **Advanced Modern Algebra, 3rd ed., Part 1**, Graduate Studies in Mathematics, Vol. **165**; **Part 2**, Graduate Studies in Mathematics, Vol. **180**, Providence, American Mathematical Society, 2015.

[18] Rotman J.J., **An Introduction to Homological Algebra, 2nd ed.** Universitext, Berlin-New York, Springer, 2008.

[19] Serre J.-P., **Linear Representations of Finite Groups, Corr. 5th printing.** Graduate Texts in Mathematics **42**, Berlin-New York, Springer, 1996.

[20] van der Waerden B. L., **Algebra, Vol I. and II**. Berlin-New York, Springer, 1991. (世界图书出版公司经典英文数学教材系列再版, 2007 年).

[21] Weibel C., **An Introduction to Homological Algebra**. Cambridge Studies in Advanced Mathematics **38**, Cambridge, Cambridge University Press, 1995.

索 引

(R,S)-双模, 108
$(k^n)^A$, 2
1_A: 恒等态射, 17
$C^0(X)$: X 上的连续函数范畴, 18
$C^\infty(X)$: X 上的C^∞函数范畴, 18
C_A: 常函子, 22
$F[G]$: 群G在域F上的群环, 111
$F[X]$: 集合X在域F上的置换表示, 113
$H(U)$: U 上的全纯映射范畴, 18
I_X: I 关于$k[X]$ 的消去理想, 97
JM, 2
J^c: 理想$J \subseteq S^{-1}R$ 在R 上的收缩, 71
M: 模, 1
M_P: M 的P-准素部分, 46
$M_{\mathfrak{p}}$: M 在素理想$\mathfrak{p}$ 处的局部化, 73
M_{tor}: M 的扭子集, 43
N_χ: χ的核, 131
R: 含幺交换环, 1
$R[x]$: 环R的多项式环, 2
$R^\times$: 环R 的乘法单位群, 61
$R_{\mathfrak{p}}$: R 在素理想$\mathfrak{p}$ 处的局部化, 73
R_f: R 在f 处的局部化, 68
S-多项式, 94
$S(f,g)$: f 和g 的S-多项式, 94
$S+T$: S与T的和, 3
$S \oplus T$: S 与T 的直和, 9
$S \times T$: S 与T 的直积, 9
$S^{-1}I$: 理想$I \subseteq R$ 在$S^{-1}R$ 上的扩张, 71
$S^{-1}M$: M 在S处的局部化, 70
$S^{-1}R$: R 在S处的局部化, 68
T'_A: 函子$B \mapsto \mathrm{Hom}(B,A)$, 22
T_A: 函子$B \mapsto \mathrm{Hom}(A,B)$, 22
U^*: U 的对偶表示, 114
$U_P(n,M) = \mathrm{d}_P(P^{n-1}M) - \mathrm{d}_P(P^nM)$, 47
V^*: 线性空间V的对偶空间, 5
V^T, 2
$V_1, \cdots, V_r$: G 的不可约表示, 120
$X \amalg Y$: X 和Y 的上乘积, 19
$X \amalg_Z Y$: X 与Y 在Z 上的纤维上积, 21
$X \times Y$: X 和Y 的乘积, 19
$X \times_Z Y$: X 与Y 在Z 上的纤维积, 21
Z_χ, 131
$\mathcal{A}$b: 阿贝尔群范畴, 18
$\mathrm{Ar}(\mathcal{C})$: 范畴(C) 的态射集类, 17
$\mathcal{C}$omRings: 交换环范畴, 18
$\mathrm{Deg}\, f$: f 的次数, 91
$\mathrm{End}(A)$: A 到自身的态射集, 17
$\mathrm{End}_F(V)$: V上的F-线性变换环, 111
$\mathrm{End}_R(M)$, 109
$\mathrm{End}_R(M)$: M的R- 模自同态环, 5
$\mathrm{GL}(V)$: V上的可逆线性变换群, 111
$\mathcal{G}$roups: 群范畴, 18
$\mathrm{Hom}(A,B)$: A 到B的态射集, 17
$\mathrm{Hom}_R(M,N)$, 109
$\mathrm{Hom}_R(M,N)$: M到N的R- 模同态集, 5
Id: 恒等函子, 22
$\mathrm{Ind}_H^G V$: H 上的表示V 到G 上的诱导表示, 135
$\mathrm{Jac}(R)$ 或者$\mathrm{rad}(R)$: R 的雅各布森根, 79
$\mathrm{LT}(f)$: f 的首项, 91
$\mathrm{LT}(f,g)$, 94
$\mathrm{Max}R$: 环R 的极大谱, 61
$\mathbb{R}$: 实数域, 5
$\mathrm{Res}(f,g)$: f 和g 结式, 98
$\mathrm{Res}_H^G U$: G 上的表示U 到H 上的限制表示, 135

$\mathcal{R}$ings: 环范畴, 18
$\mathcal{R}$-mod: R- 模范畴, 18
$\mathcal{S}$ets: 集合范畴, 18
Spec$R$: 环R 的素谱, 61
$\mathbb{Z}$: 整数环, 1
$\alpha \vee \beta$, 94
ann(M): M 的零化子, 50
ann(m): m 的零化子, 43
$\bigcap\limits_{i\in I} S_i$: $\{S_i : i \in I\}$的和, 3
$\bigoplus\limits_{\alpha\in I} S_\alpha$: $\{S_\alpha\}_{\alpha\in I}$ 的直和, 12
$\mathcal{C}_X$, 18
$\mathcal{Z}(A)$: $A \subseteq \mathbb{A}^n$ 的零化理想, 84
$\mathcal{Z}(S)$: $S \subseteq k[x_1, \cdots, x_n]$ 的零点集, 83
$\chi, {}_H$: χ 在H 上的限制特征136
χ_1: 主特征, 121
χ_V: 表示V 的特征, 121
coim f: 态射f的上像, 24
coker f: 态射f的余核, 24
coker f: 同态f 的余核, 15
$\coprod\limits_{\alpha\in I} X_\alpha$: $\{X_\alpha\}_{\alpha\in I}$ 的上乘积, 20
d$_P(M)$: M 在P 处的深度, 47
$\ell(M)$: 模M的长度, 9
im f: 态射f的像, 24
im f: 同态f 的像, 5
ker f: 态射f 的核, 24
ker f: 同态f 的核, 5
$\langle X\rangle$: X 生成的子模, 3
$\langle m\rangle$: m 生成的子模, 3
$\leq_{\text{dlex}}$: 次数字典序, 92
$\leq_{\text{lex}}$: 字典序, 91
$\mathbb{A}^n_k = \mathbb{A}^n$: k 上的n 维**仿射空间**, 83
$\mathcal{C}$: 范畴, 17
$\mathcal{C}^{\text{op}}$: 范畴$\mathcal{C}$ 的反范畴, 18
$\mathcal{O}_K$: K 的代数整数环, 77
$\mathfrak{CI}$: 类函数空间, 121
$\mathfrak{X}$: 特征标表, 124
μ_r: r 乘映射, 4
nil(R): R的幂零根, 79
ob$(\mathcal{C})$: 范畴(C) 的对象类, 17
$\prod\limits_{\alpha\in I} X_\alpha$: $\{X_\alpha\}_{\alpha\in I}$ 的乘积, 21
$\prod\limits_{\alpha\in I} S_\alpha$: $\{S_\alpha\}_{\alpha\in I}$ 的直积, 12
rank (M): 自由模M 的秩, 27
$\sqrt{I}$: I 的根式理想, 78
Supp(M): M 的支集, 103
φ^G: φ 在G 上的诱导特征, 136
f_i, χ_i: 不可约表示V_i 的次数和特征, 120
k: 域, 1
$k[V]$: 仿射代数集V的坐标环, 84
$k[\mathbb{A}^n] = k[x_1, \cdots, x_n]$: $\mathbb{A}^n$ 的坐标环, 83
r: G的不可约表示个数, 120
rM, 2

ACC, 61

DCC, 64

阿贝尔范畴, 25
阿廷环, 64
阿廷模, 64
白尔判别法, 31
半单代数, 116
半单模, 115

保核收缩, 12
闭集, 87
标量乘法, 1
表示, 111
　维数, 111

伯恩赛德定理, 133
不变因子, 49
不可约表示, 113
不可约理想, 81
不可约模, 8, 108

布赫伯格算法, 96

常函子, 22
超曲面, 83
乘积, 19
    两个对象, 19
    任意多个对象, 21
乘性集, 67
初等因子, 49
初等因子组, 49

纯子模, 60
次数-字典序, 92
代数, 82
代数同态, 82
代数整数, 77
代数整数环, 77

单代数, 117
单模, 8, 108
单射
    态射, 23
单同态, 108
单项式理想, 106
单项式序, 91
第二同构定理, 6, 108
第三同构定理, 6, 108
第一同构定理, 6
典范投射, 110
典范嵌入映射, 11, 110
典范投射, 11

短正合列, 14, 25
    分裂, 14
对偶表示, 114
对偶空间, 5
对应定理, 7, 109
多元多项式环上的带余除法, 92
多重线性映射, 32

反范畴, 18
范: $N_{E/F}$, 76
范畴, 17
    对象, 17
    态射, 17
仿射簇, 88
仿射代数集, 83
    不可约, 88
    可约, 88
    态射, 85
    同构, 85
    坐标环, 84
仿射空间, 83
分配率, 1

弗罗贝尼乌斯互反律, 135
复形, 13
格罗布纳基, 93
根式理想, 79

函子
    反变函子, 22
    共变函子, 22
    逆变函子, 22
    协变函子, 22
    右正合, 25
    正合, 25
    左正合, 25
核
    表示, 131
    态射, 24
    特征, 131
合成列, 8
恒等函子, 22
恒等态射, 17

环
    反环, 107
环的局部化泛性质, 69
基, 26
基变换, 42

迹: $\mathrm{tr}_{E/F}$, 76
迹形式, 76
极大性条件, 61
极小性条件, 65
极小准素分解, 81
加性范畴, 23

降链条件, 64
阶, 49
结合律, 1
结式, 98

局部化, 68
局部环, 73
矩阵表示, 112

开集, 87
可除代数, 116
可除模, 31
空间分解定理, 54

扩张理想, 71
拉回, 21
类函数, 121
类函数空间, 121

良序集, 91
两两不交性, 17
列正交关系, 125
零点集, 83
零对象, 18
零化理想, 84
零化子, 43
    模, 50

马施克定理, 115
满射
    态射, 23
满同态, 108

幂零根, 79

模, 1
    分配律, 107
    结合律, 107
    有限生成, 3
    右模, 107
    真子模, 2
    直和, 110
    直积, 110
    子模, 2
    左模, 107
模的长度, 9
模的局部化泛性质, 70
模同构, 3
    自同构, 3
模同态, 3, 108
    单, 3
    核, 5
    满, 3
    像, 5
    自同态, 3
挠模, 43
挠元, 43
内射模, 30
逆步表示, 144

扭模, 43
扭元, 43
诺特模, 63
诺特环, 61
诺特正规化引理, 86

偏序, 91
偏序集, 91
平凡表示, 113
平凡子模, 108
平坦模, 38

群环, 111

商模, 6, 108

上乘积, 19
　两个对象, 19
　任意多个对象, 20
上升定理, 75
蛇形引理, 16, 26
深度, 47
升链条件, 61

史密斯标准形
　矩阵, 51
　模, 52
始对象, 18
收缩, 12
收缩理想, 71
舒尔引理, 109
舒尔引理
　代数封闭域情形, 118
数乘, 1

双射
　态射, 23

态射
　仿射代数集, 85
　同构, 17
特征, 121
特征标表, 124

同构, 108
　仿射代数集, 85
同态基本定理, 6, 108
投射模, 28
推出, 21
拓扑, 87
拓扑空间, 87

韦德伯恩定理, 119
无挠模, 43
无扭模, 43
五引理, 56

希尔伯特基定理, 62
希尔伯特零点定理, 86
　弱形式, 87
下降定理, 76
纤维和, 21
纤维积, 21
纤维上积, 21
限制表示, 135
限制特征, 136
线性表示, 111
线性特征, 121
线性作用, 111
相伴素理想, 81
消去理想, 97

行正交关系, 124

循环模, 3
雅各布森根, 79

有限阶元, 43
有限生成代数, 82
有限生成模, 3
右乘映射, 107
右理想, 108
右正合函子, 25
诱导表示, 135
诱导特征, 136
余核
　态射, 24
余数
　模G, 93

约化, 92
　模I, 41
增广理想, 113
扎里斯基拓扑, 87
　素谱, 90

张量积, 33

整
    环, 74
    元素, 74
整闭, 74
整闭包, 74
整扩张, 74
正规化, 74
正合, 13, 25
正合函子, 25
正合列, 13
正则表示, 113
正则特征, 121

直和, 9, 11
直和项, 12
直积, 9, 10
置换表示, 113
秩, 27
中国剩余定理, 55
中山引理, 79
终对象, 18
主理想整环上有限生成模结构定理, 49
主特征, 121

准素部分, 46
准素分解, 81
准素分量, 81
准素理想, 80
准素模, 46
子表示, 113
子模, 108
    和, 3
    集合生成的子模, 3
    交, 3
    平凡子模, 2
    循环子模, 3
子模的和, 109
自同态环, 5, 109
自由模, 26
    秩, 27
字典序, 91
    次数, 92
左乘映射, 107
左理想, 108
左正合函子, 25
坐标环, 83