Pure Mathematics 理论数学, 2020, 10(3), 235-243
Published Online March 2020 in Hans. http://www.hanspub.org/journal/pm
https://doi.org/10.12677/pm.2020.103031

Hans汉斯

Function of Ideal in Ring

Fanhong Zhang, Shuxia Yao*

School of Mathematics, Lanzhou City University, Lanzhou Gansu
Email: *yaoshuxia@163.com

Received: Feb. 24th, 2020; accepted: Mar. 10th, 2020; published: Mar. 17th, 2020

Abstract

The role of ideal in ring is similar to the invariant subgroup in group theory. Invariant subgroup plays a very important role in group theory, and is the premise and basis for the conclusion of group homomorphism and isomorphism. This paper analyzes the important role of ideals in characterizing the properties of rings by means of the function of analogous invariant subgroups in group theory, expounds the importance of the properties of ideals in determining the homomorphism and isomorphism of rings, and further illustrates how to construct finite fields by means of ideals, and then establish the homomorphism and isomorphism relations over number fields.

Keywords

Ring, Field, Homomorphism, Ideal

理想在环中的作用

张翻红，姚淑霞*

兰州城市学院(数学学院)，甘肃 兰州
Email: *yaoshuxia@163.com

收稿日期：2020年2月24日；录用日期：2020年3月10日；发布日期：2020年3月17日

摘　要

理想在环中的作用与不变子群在群论中的作用相仿。不变子群在群论中起着非常重要的作用，是群的同态与同构相关结论获得的前提和基础。本文通过类比不变子群在群论中的作用，分析了理想对刻画环的性质所起的重要作用，阐明了理想的性质在决定环的同态与同构关系中的重要性，进一步说明了如何利用理想来构造有限域，进而建立数域上的同态及同构关系。

*通讯作者。

文章引用: 张翻红, 姚淑霞. 理想在环中的作用[J]. 理论数学, 2020, 10(3): 235-243.
DOI: 10.12677/pm.2020.103031

关键词

环，域，同态，理想

1. 引言

1.1. 研究背景

《近世代数》课程主要研究的对象是代数系统，也就是带有运算的集合。群是带有一个运算的代数系统，而环和域是带有两个运算的代数系统。环论起源于 19 世纪关于实数域的扩张和分类的研究。19 世纪早期到 20 世纪二三十年代形成严谨的结构化体系。对环论历史研究，进行不同角度的考察。从思想史角度探讨环论概念的发展，掌握环论与其他相关分支和学科之间的关系，认识在环论发展过程中起主导作用的集合论、公理化、抽象化、结构化等思想[1] [2]。后来在魏得邦(J·H·M·Wedderburn)、诺特(A·E·Noether)、阿廷(E·Artin)、雅各布森(N·Jacobson)等人的不懈努力下，环论的研究不断发展，日渐完善，现已成为代数学研究的一个重要分支[3]。环论的另一起源是代数数论、代数几何学及它们综合而产生的交换环理论。1871 年戴德金(Daidkin)首先引进了理想的概念，开创了理想理论。而环这个名词首先出现在希尔伯特的数论报告中。同时代数几何学的研究也促使希尔伯特证明多项式环的基本定理。在本世纪初英国数学家腊斯克(E·Lasker, 1868~1941)及麦考莱(F·S·Macaulay, 1862~1937)对于多项式环得出了分解定理。对于交换环的一般研究来源于 E • 诺特(A·E·Noether)，他对一般诺特环进行了公理化阐述，并证明了准素分解定理，从而奠定交换环论乃至抽象代数学基础，其后克鲁尔(W·Krull, 1899~1971)给出系统的研究，他还引进了最值得注意的局部环。四十年代，薛华荔、柯恩(I·S·Cohen, 1917~1955)及查瑞斯基(O·Zariski, 1899~1986)对局部环论进行了系统的研究[4]。

任何一门学科，就其本质来说，关键的内容、核心的概念，往往就不过那么几条；而发挥出来，就成了洋洋大观的巨著。理解了这些核心和关键，并通过严格的训练将其真正学到手，就掌握了这门课程的精髓，就能得心应手地加以应用和发挥，也就达到了学习这门课程的目的，并为培养创新人才打下了基础。近世代数也不例外，要让学生把主要的精力集中在那些最基本、最主要的内容上，真正学深学透，一生受用不尽。同时，任何一门学科的产生与发展，都离不开外界的推动，数学也是如此。19 世纪关于实数域的扩张和分类的研究使得环论应用而生，直到今天，理想这个威力无比的武器仍在各方面不断发挥着重要的作用。这不仅为近世代数增添了色彩，而且也为近世代数以后的发展提供了丰富的原材料。再次，任何一门课程的内容不应该是故步自封的，而应顺应时代的发展和科技的进步。学习的目的在于应用。只有将所学知识与现实生活联系起来并加以应用，才能够发挥数学的威力。19 世纪初，见证了纯数学向抽象代数学的变化。以 18 世纪末的方程的可解性研究为开端，到 19 世纪 40 年代，虽然那个时候还没有完全弄清楚群，但群的概念已明显地出现在多个独立的数学领域(包括置换理论)。由于对规律的渴求以及对新概念的需求，到 20 世纪我们有了对群的本质属性的公理化。走在这场变革前沿的有 3 个人分别是：Evariste Galois (方程可解性的先锋)；Augustin-Louis Cauchy (置换理论的奠基人)；Arthur Cayley (把群抽象化的先驱)。自从 1968 年 A.L. Kostrikin 的相关文章发表以后，模李代数(即素特征域上的李代数)的研究有了长足的发展，经过多位数学家几十年的共同努力，特别是 H Strade 的杰出工作，最终于 1989 年完成了特征数大于 7 的代数闭域上单的有限维李代数的分类。至今，模李代数已经有了丰富的理论[4]。

近世代数又名抽象代数，它是近代数学的基础学科。近世代数主要研究对象是具有代数运算的集合所做成的代数系统中元素之间的关系，从而将其推广到普通意义下的群、环、域中。环作为带有两个代数运算中最简单的一例，自然成为我们主要的研究对象。通过理想的若干等价命题能够帮助我们快速找到环中元素之间的关系，从而能够大大减少繁琐的证明过程。加深学生对知识的理解和掌握。不变子群是近世代数中为数不多的重要概念之一，熟练应用不变子群的性质有利于我们对群论产生更直观、更简明的认识和了解。那么，理想对环论而言，又起着怎样的重要意义，理想本身的特殊性质又会带给我们怎样的学习体会？这将是本论文要解决的主要问题。近世代数又名抽象代数，它是近代数学的基础学科。近世代数主要研究对象是具有代数运算的集合所做成的代数系统中元素之间的关系，从而将其推广到普通意义下的群、环、域中。为培养学生良好的逻辑思维能力。环作为带有两个代数运算中最简单的一例，自然成为我们主要的研究对象。通过理想的若干等价命题能够帮助我们快速找到环中元素之间的关系，从而能够大大减少繁琐的证明过程。加深学生对知识的理解和掌握。

1.2. 基础知识

定义 1 [5] 环(Ring)：设非空集合 R 有两个代数运算，一个叫做加法(常用+表示)，另一个叫做乘法。如果对于 R 中的任意三个元 a,b,c 来说，满足：

1) R 对加法作成一个加群；

2) R 对乘法满足结合律：

$$(ab)c = a(bc).$$

3) 乘法对加法满足左右分配律：

$$a(b+c) = ab + ac,\ (b+c)a = ba + ca.$$

则称 R 对这两个代数运算做成一个环。

定义 2 [6] 除环(Division ring)：一个环 R满足：

1) R 至少包含一个不等于零的元；

2) R 中有一个单位元；

3) R 的每一个不等于零的元有一个逆元。

则称 R 是一个除环(或体)；一个可交换的除环叫做域。

定义 3 [7] 理想(Ideals)：设 N 是环 R 的一个子加群，即对 N 中任意元素 a,b， $a-b$ 仍属于 N。如果还满足：

$$\forall r \in R,\ a \in N \Rightarrow ra \in N.$$

则称 N 是环 R 的一个左理想；并称 N 满足左吸收率。

如果：

$$\forall r \in R,\ a \in N \Rightarrow ar \in N.$$

则称 N 是环 R 的一个右理想；并称 N 满足右吸收率。

如果 N 即是环 R 的左理想，又是环 R 的右理想，则称 N 是环 R 的一个双边理想，简称理想(Ideals)。并用符号 $N \trianglelefteq R$ 表示。

定义 4 [8] 商环(Quotient Ring)：设 μ 是 R 的一个理想， R/μ 表示 μ 的所有左(右)陪集构成的集合，则 R/μ 关于集合的乘法构成一个环，称其为 R 关于 μ 的商环，记为 R/μ 。

推论：一个环 R 同它的每一个商环 R/μ 同态。

定义 5 [6] 子环(Subloop)：如果环 R 的非空子集 N 对于环 R 的加法和乘法运算也作成一个环，那么

称 N 为 R 的子环，记作 $N \le R$。

特别的，我们把一个阶为素数的零乘环叫做素阶零乘环。

定理(子环的判定定理) [9]：一个环 R 的一个不空子集 N 作成 R 的一个子环的充要条件是：

(i) $a,b \in N \Rightarrow ab \in N$；

(ii) $a \in N \Rightarrow a^{-1} \in N$；

推论：一个环 R 的一个不空子集 N 作成 R 的一个子环的充要条件是：

$$\forall a,b \in N \Rightarrow ab^{-1} \in N.$$

为方便叙述，常用符号 $|R|$ 表示环 R 的阶。

2. 不变子群在群论中的作用

我们知道，群论是近世代数的基础，下面对群论中的相关理论做一个简单的介绍，并以此为依据引出理想在环论中的重要应用。

在群论的研究中，由一个群 G 获得一个相应的商群的思路是：首先，找到群 G 的一个非空子集 S，进一步由非空子集 S 作成子群 H；再做子群 H 的陪集：

$$\bar{H} = H \circ a = \{h \circ a \mid h \in H\};$$

进一步利用子群 H 的陪集 $\bar{H}$ 得到一个不变子群 N；紧接着，将不变子群 N 的所有左(右)陪集找出来构成集合 G/N 表示；最后，将 G/N 中元素所在的类找出来，做成一个剩余类记为 $\bar{G}$。这样，我们得到了以下结论：

1) G/N 也是一个群，我们把它叫做商群，并且有 $G \sim G/N$ [3]；

2) $\bar{G}$ 是群，且有：$G \sim \bar{G}$ [7]；

3) (群同态基本定理[4])：若有 $G \sim \bar{T}$，则这个同态满射的核 K 是 G 的一个不变子群，并且

$$G/K \cong \bar{T};$$

4) (群第二同构定理[3])：设 G 是群，若有 $H \le G$，并有 $N \trianglelefteq G$ 则

(i) $H \cap N \trianglelefteq H$；

(ii) $HN/N \cong H/(H \cap N)$，

如图 1 所示：

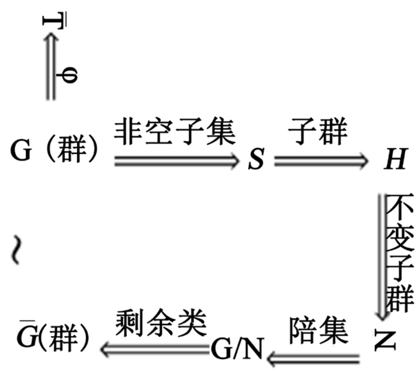

Figure 1. Graph of invariant subgroups and homomorphisms of groups
图 1. 不变子群及群的同态关系图

3. 理想在环中的作用

接下来我们将利用群论中由群到商群的研究思路及不变子群在群的同态与同构中所起的作用，来阐明理想在环中所处的地位，并通过对一些定理及例题的证明向揭示理想在环中的重要意义。

设 R 是一个环，我们先找到环 R 的一个理想 μ，这样，μ 关于我们所规定的加法自然能够做成一个加群，因而 μ 是一个关于加法构成的不变子群。接下来，我们将 μ 的所有左(右)陪集拿出来做成集合 R/μ。我们希望能够得到一个与环 R 同态的环，因此，将 R/μ 中元素所在的类找出来，做成一个剩余类。我们发现 R/μ 中元素所在的类其实就是对整数集的一个分类。为方便起我们将其记为 $\bar{R}$。同样，我们可以得到以下结论：

1) R/μ 也是一个环，我们把它叫做商环，并且有 $R\sim R/\mu$ [4]；

2) $\bar{R}$ 是环，且有：$R\sim\bar{R}$ [7]；

3) (环同态基本定理[4])：若记 $R\xrightarrow{\varphi}\bar{T}$，则

$$K=Ker(\varphi)\{x\mid\varphi(x)=\bar{0}\}$$

是 R 的理想，且有：

$$R/K\cong\bar{T};$$

4) (环第二同构定理[10])：设 R 是环，S 是其子环，$\mu\trianglelefteq R$，则：

$$(S+\mu)/\mu\cong S/(S\cap\mu).$$

如图 2 所示：

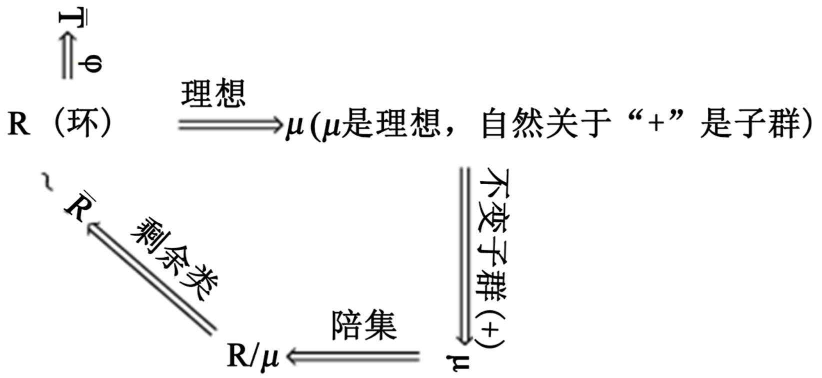

Figure 2. Diagram of ring isomorphism
图 2. 环同构的关系图

3.1. 有关理想的重要结论

定理 1 [3]：设 N 是环 R 的一个理想，则 R/N 对陪集的加法和乘法作成一个环，称为 R 关于 N 的或称为剩余类环)，且 $R\sim R/N$。

定理 2 [7]：设 U 是环 R 的理想，若“+”和“x”是 $\bar{R}$ 的二元运算，则 $(\bar{R},+,X)$ 是环，且有 $R\sim\bar{R}$。

定理 3 [4]：(环同态基本定理)：设 R 与 $\bar{R}$ 是两个环，且 $R\sim\bar{R}$，则

1) 这个同态满射的核 N，即零元的全体逆像是 R 的一个理想；

2) $R/N\cong\bar{R}$。

定理 4 [10]：(环第二同构定理)：设 R 是环，S 是其子环，$\mu\trianglelefteq R$，则：

$$(S+\mu)/\mu\cong S/(S\cap\mu).$$

3.2. 理想在环中的应用

下面我们通过对具体例题的分析和证明来阐明理想在环论中的广泛应用及重要作用。

3.2.1. 理想在循环环中的应用

结论 1：N 是循环环 $R=\langle a\rangle$ 的一个理想，当且仅当 N 是 R 的子加群(子环)。

证明：$\Rightarrow$) 理想当然是子加群；

$\Leftarrow$) 设 N 是循环环 $R=\langle a\rangle$ 的一个子加群，则：$\forall b\in N, r\in R$，有

$$b=sa,\ r=ta,\ a^2=ka.$$

其中 s,t,k 为整数，则：

$$rb=(ta)(sa)=(ts)(a^2)=(ts)(ka)=(tk)(sa)=(tk)b\in N.$$

又循环环必是可交换环，故 $N\trianglelefteq R$。

3.2.2. 理想的可加性

结论 2：若 $N_1,N_2,\cdots,N_m$ 是环 R 的 m 个(子环)理想，则 $N_1+N_2+\cdots+N_m$ 也是环 R 的(子环)理想。

证明：对 m 采用数学归纳法。

1) 当 $m=1$ 时结果显然成立；

2) 当 $m=2$ 时，N_1+N_2 显然作为 R 的子加群。又设 $r\in R$，且：

$$x=x_1+x_2\in N_1+N_2,\ x_i\in N_i,$$

则由于 N_1,N_2 是 R 的理想，故

$$rx=r(x_1+x_2)=rx_1+rx_2\in N_1+N_2;$$

$$xr=(x_1+x_2)r=x_1r+x_2r\in N_1+N_2.$$

它们都属于 N_1+N_2 从而 $N_1+N_2\trianglelefteq R$，即 $m=2$ 时结论成立。

3) 假定对 $m-1$ 时结论成立，则由于

$$N_1+N_2+\cdots+N_{m-1}+N_m=(N_1+N_2+\cdots+N_{m-1})+N_m.$$

故由 $m=2$ 时的结论知此结果对于 m 也成立。

则 $N_1+N_2+\cdots+N_m$ 也是环 R 的(子环)理想。

3.2.3. 理想在除环中的应用

结论 3：R 是一个阶大于 1 的环，并且除了单位理想和零理想外无其它左或右理想，则当 R 有单位元时，R 为除环；当 R 无单位元时，R 为素阶零乘环。

为方便起见，我们先证明一个引理。

引理[7]：若 R 是环且 $|R|>1$，则 R 是除环当且仅当对 R 中任意元素 $a\neq 0,b$，方程 $ax=b$ 或 $(ya=b)$ 在 R 中有解。

证明：必要性显然成立，下证充分性。

1) 先证环 R 中无零因子；

在 R 中任取元素 $a\neq 0, b\neq 0$。因为方程 $ax=b$ 在 R 中有解，设为 c。即有：$ac=b$；

又因方程 $bx=c$，在 R 中有解，设为 d，即有：$bd=c$。

于是 $abd=ac=b\neq 0$。从而 $ab\neq 0$，即证环 R 中无零因子。

2) 再证 R 中有单位元。

在 R 中任取元素 $a \neq 0$ 因为方程 $ax = a$ 在R中有解，设为 e，即 $ae = a$，从而有：

$$ae^2 = ae,\ ae^2 - e = 0.$$

但 $a \neq 0$，又无零因子，故 $e^2 - e = 0$， $e^2 = e \neq 0$。

再任取 $b \in R$，则有：

$$(be - b)e = 0,\ e(eb - b) = 0.$$

但 $e \neq 0$，故 $be - b = eb - b = 0$。从而：

$$be = eb = b.$$

即 R 中有单位元 e。

3) 最后证 R 中每个非零元都有逆元。

在 R 中任取元素 $a \neq 0$，因为方程 $ax = e$ 在 R 中有解，设为 a'，即有 $aa' = e$，下证 $a'a = e$。

由于：

$$(a'a - e)a' = a'aa' - ea' = a'e - a' = a' - a' = 0.$$

但 $a' \neq 0$，故必有 $a'a - e = 0$， $a'a = e$。因此：

$$a'a = aa' = e.$$

即 a 在 R 中有逆元。

综上所述，R 是一个除环。

接下来我们借用该引理证明结论 3。

证明：首先，证明当 R 除了单位理想和零理想外无其他左理想时，结论成立。

设 R 除了单位理想和零理想外无其他左理想。在 R 中任取元素 $a \neq 0$，则显然 $Ra = \{ra \mid r \in R\}$ 是 R 的一个左理想。

当 R 有单位元时， $a \in Ra$，从而 $Ra \neq 0$。于是 $Ra = R$，即方程 $ya = b(b \in R)$ 在 R 中有解。于是由以上引理知，R 是除环；

当 R 无单位元时，若对 R 中任意元素 $a \neq 0$，都有 $Ra = R$，则同样可知 R 是除环，这与 R 中无单位元相矛盾(除环中必有单位元)。因此，总存在元素 $a \neq 0$ 使得 $Ra = 0$，于是 $a^2 = 0$，而且：

$$N = \{\cdots, -2a, -a, 0, a, 2a, \cdots\}.$$

是环 R 的一个左理想，也是循环零乘环，故 $N = R$，再由假设以及结论 1 知，R 只能为素阶零乘环。

当 R 除了单位理想和零理想外无其他右理想时，同理可证。

3.2.4. 理想在多项式环中的应用

结论 4 [11]：设 P 为数域， $P[x]$ 是 P 上的一元多项式环，称 $P[x]$ 的非空子集合 I 为 $P[x]$ 的理想，如果对任意的 $f(x), g(x) \in I$， $h(x) \in P[x]$，有

$$f(x) \mp g(x) \in I,\ h(x)f(x) \in I.$$

证明：1) 对于 $P[x]$ 的任意理想 I，存在 $d_I(x)$ 使得对任意 $f(x) \in I$，有

$$d_I(x) \mid f(x).$$

2) 对任意的 $f(x), g(x) \in P[x]$，有：

$$J=\{u(x)f(x)+v(x)g(x)\mid u(x),v(x)\in P[x]\}.$$

是 $P[x]$ 的理想，且 $d_J(x)$ 是 $f(x),g(x)$ 的最大公因式。

证明：1) 当 $I=\{0\}$ 时：

$$d_I(x)=0,\ \forall f(x)\in I,0\mid f(x).$$

$I=\{0\}$ 显然是 $P[x]$ 的理想。

当 $I\neq\{0\}$ 时，取 I 中次数最小的多项式为 $d_I(x)$。下证 $\forall f(x)\in I$， $d_I(x)\mid f(x)$。设

$$f(x)=d_I(x)q(x)+r(x).$$

此时 $r(x)=0$ 或者 $r(x)\neq 0$ 且 $\partial^{\circ}[r(x)]<\partial^{\circ}d_I(x)$。

而当 $\partial^{\circ}[r(x)]<\partial^{\circ}d_I(x)$ 时，这与 $d_I(x)\in I$ 且次数最小相矛盾。故：

$$I=r(x)=f(x)-d_I(x)q(x)=0.$$

即：

$$f(x)=d_I(x)q(x)\Rightarrow d_I(x)\mid f(x).$$

综上，对于 $P[x]$ 的任意理想 I，存在 $d_I(x)$ 使得对任意 $f(x)\in I$，有 $d_I(x)\mid f(x)$。

2) 设 $\forall h_1(x),h_2(x)\in J$， $u_1(x),u_2(x),v_1(x),v_2(x)\in P[x]$。

$$h_1(x)=u_1(x)f(x)+v_1(x)g(x),\ h_2(x)=u_2(x)f(x)+v_2(x)g(x).$$

$$\begin{aligned}h_1(x)+h_2(x)&=u_1(x)f(x)+v_1(x)g(x)+u_2(x)f(x)+v_2(x)g(x)\\&=(u_1(x)+u_2(x))f(x)+(v_1(x)+v_2(x))g(x)\in J.\end{aligned}$$

$$\begin{aligned}h_1(x)h_2(x)&=[u_1(x)f(x)+v_1(x)g(x)][u_2(x)f(x)+v_2(x)g(x)]\\&=u_1(x)u_2(x)f^2(x)+v_1(x)v_2(x)g^2(x)\\&\quad+u_1(x)v_2(x)f(x)g(x)+v_1(x)u_2(x)f(x)g(x)\\&=[u_1(x)u_2(x)f(x)+u_1(x)v_2(x)g(x)]f(x)\\&\quad+[v_1(x)u_2(x)f(x)+v_1(x)v_2(x)g(x)]g(x)\\&\in J.\end{aligned}$$

故对任意 $f(x),g(x)\in P[x]$， $J=\{u(x)f(x)+v(x)g(x)\mid u(x),v(x)\in P[x]\}$ 是 $P[x]$ 的理想。

又 $d_J(x)\mid f(x),d_J(x)\mid g(x)$，即 $d_J(x)$ 是 $f(x)$ 与 $g(x)$ 的公因式。

因为 $\forall h(x)\mid f(x),h(x)\mid g(x)$，由最小数原理知：$h(x)\mid d_J(x)$。即得 $d_J(x)$ 是 $f(x)$ 与 $g(x)$ 的最大公因式。

本文通过对一些定理和结论的分析证明，以便让读者发现理想在环中的地位与群论中不变子群的地位相类似，熟练应用这些知识及定理可使得读者对群论和环论有更清楚、更直观的认识。让读者对近世代数有一个整体的认识和把握。由于学识，编者水平能力有限，谬误之处在所难免，恳请广大读者提出宝贵的批评意见和建议。

基金项目

本论文得到姚淑霞老师国家自然科学基金项目(31960273)的支持。

参考文献

[1] 李冰. 关于欧氏环定义中单位元的讨论[J]. 唐山师专学报, 1999(21): 6.

[2] 朱德高. 整数的整除性[J]. 高等函授学报: 自然科学版, 1996(6): 9-11.

[3] 杨子胥. 近世代数[M]. 第三版. 北京: 高等教育出版社, 1998.

[4] 刘培杰, 刘丽娟. Lie 群与 Lie 代数[M]. 哈尔滨: 哈尔滨工业大学出版社, 2016.

[5] 杨子胥. 近世代数[M]. 北京: 中国矿业大学出版社, 2008.

[6] 谢邦杰. 抽象代数学[M]. 上海: 上海科学技术出版社, 1984.

[7] 邓胜兰. 抽象代数基础[M]. 北京: 机械工业出版社, 2011.

[8] 滕加俊. 近世代数辅导与习题精解[M]. 第二版. 大连: 大连理工大学出版社, 2006.

[9] 张禾瑞. 近世代数基础[M]. 修订版. 北京: 高等教育出版社, 1978.

[10] 胡冠章. 应用近世代数[M]. 第二版. 北京: 清华大学出版社, 1999.

[11] 王丽, 李永军. 高等代数选讲[M]. 上海: 同济大学出版社, 2014.