Advances in Applied Mathematics 应用数学进展, 2024, 13(10), 4669-4673
Published Online October 2024 in Hans. https://www.hanspub.org/journal/aam
https://doi.org/10.12677/aam.2024.1310447

Hans汉斯

整数环的性质与应用研究

金宇驰，邢美慧，鲍佩迪，佟思宏，石玳東妮，田　岩*

辽宁师范大学数学学院，辽宁　大连

收稿日期：2024年9月25日；录用日期：2024年10月17日；发布日期：2024年10月28日

摘　要

整数环作为近世代数中的一个重要代数结构，其相关研究在群、环、域中非常重要。然而，整数环的构造、性质及其应用，有待于进一步的研究。本文主要给出整数环的构造，证明其基本性质。同时，研究整数环的判定、整数环与理想以及其他环类的联系、代数整数环上Ramanujan展开的应用。

关键词

整数环，理想，整数加法环，Ramanujan展开

Research on Properties and Applications of Integer Rings

Yuchi Jin, Meihui Xing, Peidi Bao, Sihong Tong, Daidongni Shi, Yan Tian*

School of Mathematics, Liaoning Normal University, Dalian Liaoning

Received: Sep. 25th, 2024; accepted: Oct. 17th, 2024; published: Oct. 28th, 2024

Abstract

As an important algebraic structure in modern algebra, integer rings are very important in groups, rings, and fields. However, the structure, properties and applications of integer rings await further study. This article mainly gives the construction of integer rings and proves their basic properties. At the same time, the determination of integer rings, the relationship between integer rings and ideals and other ring types, and the application of Ramanujan expansion on algebraic integer rings are studied.

Keywords

Integer Ring, Ideal, Integer Addition Ring, Ramanujan Expansion

*通讯作者。

文章引用: 金宇驰, 邢美慧, 鲍佩迪, 佟思宏, 石玳東妮, 田岩. 整数环的性质与应用研究[J]. 应用数学进展, 2024, 13(10): 4669-4673. DOI: 10.12677/aam.2024.1310447

1. 引言

整数环这一理论的研究在实际应用中具有重要应用，例如：大数据时代下对于身份信息的同态密钥协商，全同态加密算法、多重变量的 Menon 型恒等式等等都与整数环理论具有密切联系。整数环的研究引起了很多专家和学者的关注，取得了很多成果。德国数学家卡尔·弗里德里希·高斯在《数论》中进行了对整数的研究，引入了整系数多项式这一概念，并研究了整数的分解。德国数学家理查德·戴德金和朱斯丁·•索尔维对整数环的理论进行了深入研究，在原有基础上引入了理想和整环的概念。数学家大卫·•希尔伯特和埃米尔·阿廷进一步研究了整数环的结构性质和应用。迄今为止，整数环的研究与其他数学分支，如数论、代数几何和代数拓扑等领域交织在一起。研究者们更关注整数环在更深的数学结构中的应用，如含有整除关系的 Menon 型恒等式、多重变量的 Menon 型恒等式等等[1]，尤其是与计算机和密码学等领域的重要联系[2] [3]。本文受上述文献的启发，主要基于整数环的定义与构造，研究其基本性质，给出整数环的具体应用。

2. 基本理论

下面给出本论文中将用到的基本概念和结论。

定义 2.1 [4] 群定义：一个不空集合 G 对于一个叫做乘法的代数运算来说作成一个群，假如：

1. G 对于乘法来说是闭的；
2. 结合律成立：$a(bc)=(ab)c$；对于 G 的任意三个元 a，b，c 都成立；
3. G 里至少存在一个单位元 e，能让 $ea=a$ 对于 G 的任何元 a 都成立；
4. 对于 G 的每一个元 a，在 G 里至少存在一个左逆元 a^{-1} 能让 $a^{-1}a=e$。

定义 2.2 [4] 一个群叫做交换群，假如 $ab=ba$，对于 G 的任何两个元 a，b 都成立。

定义 2.3 群 G 的左单位元也是右单位元，并且是唯一的，称之为群 G 的单位元。

定义 2.4 群 G 中元素 a 的左逆元也是 a 的右逆元，并且是唯一的，称为元素 a 的逆元。

定义 2.5 一个集合 R 叫做一个环，假如：

1. R 是一个加群，换一句话说，R 对于一个叫做加法的代数运算来说做成一个交换群。
2. R 对于另一个叫做乘法的代数运算来说是闭的。
3. 这个乘法适合结合律。
4. $a(bc)=(ab)c$，任意 R 中三个元素 a，b，c，都有两个分配律都成立：

$a\times(b+c)=ab+ac$　$(b+c)\times a=ba+ca$。

定义 2.6 如果环 R 的乘法满足交换律，即对 R 中任意元素 a，b 都有 $ab=ba$。

则称环 R 为交换环，否则称 R 为非交换环。

定义 2.7 (左零因子、右零因子)若是在一个环里，$a\neq 0, b\neq 0$ 但 $ab=0$，则 a 是这个环的一个左零因子，b 是一个右零因子。

一个环如果为交换环，它的左零因子也是右零因子。

在一个非交换环中，一个零因子未必同时是左零因子和右零因子。

定义 2.8 一个环 R 叫做整环，假如：

1. 乘法适合交换律： $ab=ba$。
2. R 有单位元 1： $1a=a1=a$。
3. R 没有零因子： $ab=0\Rightarrow a=0$ 或 $b=0$ 这里 a，b 可以是 R 的任意元。

整环即无零因子的幺环。

整数环定义

由以上环与整环相关定义，我们可以得到整数环定义：

全体整数做成的集合中有两种运算(×；+)。

(I) R 对于一个叫做加法的代数运算来说做成一个交换群。

(II) R 对于一个叫做乘法的代数运算来说封闭、满足结合律、有单位元 1、乘法适合交换律。

(III) R 没有零因子。

(IV) R 对于加法和乘法来说满足分配律。

那么 R 就叫做整数环。

3. 整数环的性质

性质 1. 整数环是无零因子环

整数环的特征或是无限大或是一个素数 P 且一个环有无零因子这一性质在经过一个同态满射是不一定可以保持的。例如：R 为整数环， R^* 为模 n 的剩余类环，那么 ϕ：

$$a\to[a]$$

显然， ϕ 是 R 到 R^* 的一个同态满射，但 R 没有零因子， R^* 有零因子。

性质 2. 整数环是主理想环

(1) 整数环 R 关于加法做成循环群，因为循环群的子群是其生成子群，设

$$\mu=(a)\ a\in R$$

由生成子群定义 $(a)=\{ka|k\in a\}$，所以 $\mu=\{ka|k\in a\}$。

(2) 整数环 R 是有理想的交换环，所以 R 的由元素 a 确定的主理想为 $\{ka|k\in a\}$，即整数环 R 的每一个理想都是他的主理想，故 μ 是 R 的主理想。

性质 3. 整数环是完备环

设有一个整数环中的柯西序列 $\{a_n\}$，即对于任意给定的正数 ε，存在一个正整数 N，使得当 $m,n>N$ 时，

$$|a_m-a_n|<\varepsilon$$

由于整数环中任意两个整数的差的绝对值是一个非负整数，因此对于柯西序列 $\{a_n\}$，随着序列元素的增加，差值不会无限增大，从而这个差值序列也会收敛到一个整数。即整数环中的任意柯西序列都有一个极限，整数环满足柯西序列收敛条件，说明整数环是一个完备环。

性质 4. 整数环是唯一分解整环或高斯整环

因为整数环 R 是一个整环，整数环的每一个既不是零也不是单位的元 a 都有一个分解 $a=p_1p_2p_3\cdots p_r$ (p_r 是 R 的素元)。并且 R 的一个素元 p 若能整除 ab，那么 p 能整除 a 或 b，所以整数环是唯一分解环。

性质 5. 整数环是一个欧式环

定义：

$$\varphi:a\to\left|a=\varphi(a)\left(|a|\text{表示整数 }a\text{ 的绝对值}\right)\right|$$

是一个适合条件有一个从整环 I 的非零元所做成的集合到 ≥ 0 的整数集合的映射 φ 存在的映射，给了整数 $a\neq 0$，任何整数 b 是可以写成 $b=qa+r$ 的形式，这里 $r\neq 0$ 或 $\varphi(r)<|a|=\varphi(a)$。因此整数环是欧式环。任何欧式环一定是一个主理想环，也是一个唯一分解环。

4. 整数环的构造

1. 整数加法群的结构

整数及整数上的加法运算构成了群 $\langle Z,+\rangle$，称之为整数加法群。其中 0 是群的单位元，每一个元素的逆元是它的相反数。

整数与整数上的乘法运算不能构成群，因为除了元素 1 和−1 外，所有元素都不存在逆元。类似地，$\langle Q,+\rangle$，$\langle R,+\rangle$ 都是群，而 $\langle Q,\times\rangle$，$\langle R,\times\rangle$ 都不是群，因为元素 0 没有逆元。$\langle Q-\{0\},\times\rangle$，$\langle R-\{0\},\times\rangle$ 都是群，两个群的单位元均为 1，元素 a 的逆元是该元素的倒数。

整数加法群 $\langle Z,+\rangle$，是由整数 Z 和整数加法运算(+)组成。其单位元 0；

封闭性：$\forall a,b\in Z, a+b\in Z$；

结合律：$\forall a,b,c\in Z,(a+b)+c=a+(b+c)$；

逆元：$\forall a\in Z, a^{-1}=-a$。

2. 整数加法群的性质

(1) 子群

设 G 是群，$\varnothing\neq H\subseteq G$，若 H 具封闭性、单位元、逆元，称 H 是 G 的一个子群，记号 $H\leq G$。换句话说，若 $1_G=1_H\in H$；$\forall a,b\in H$，$a\cdot b\in H$；$\forall a\in H$，$a^{-1}\in H$，则 H 是 G 的一个子群。作为群公理之一的结合律，因为 H 继承了 G 的运算，所以自然成立，因此，子群也是群。

考虑整数加法群 $(Z,+,0)$，自然可以想到，在偶整数上做加法可以成群，如 0 + 2 = 2，2 + 4 = 6……定义为整数上的所有偶数，则 $(2Z,+,0)$ 是 $(Z,+,0)$ 的子群。对任意整数 b，定义 $bZ=\{bx:x\in Z\}$，则 $(bZ,+,0)$ 是 $(Z,+,0)$ 的子群。

整数加法群 $\langle Z,+\rangle$ 是 $\langle R,+\rangle$ 的子群。

(2) 循环群

设 g 是群 G 中一个取定的元素，若群 G 的任意一个元素 a 可以写成 $a=g^n, n\in Z$ 的形式，则称 G 循环群，称 g 为群 G 的一个生成元，可写成 $G=\langle g\rangle$。

循环群分为两类：一类是有限循环群，n 个元的有限循环群与模 n 的剩余类加群同构；另一类是无限循环群，它与整数加法群同构，循环群是特殊的阿贝尔群，循环群的子群和商群仍是循环群。

整数加法群 $\langle Z,+\rangle$ 中，任意元素 a 都可以表示成 1 或−1 的幂，因此 $\langle Z,+\rangle$ 是循环群。在整数加法群上做一些小修改可以做出另一个有意思的循环群 $\langle Z_n,\tilde{+},0\rangle$，其中 $Z_n=\{0,1,\cdots,n-1\}$，同余加法 $\tilde{+}$ 定义为 $\forall a,b\in Z_n, a\tilde{+}b=(a+b)\bmod n$。在这里 $1^n=0$，也就是说 $1\tilde{+}1\tilde{+}1\tilde{+}\cdots\tilde{+}1=0$（$n$ 个 1 相加模 n 余 0)。所以，$\langle Z_n,\tilde{+},0\rangle=\langle 1\rangle$ 是 n 阶循环群。

(3) 交换群

具有交换性的群称为交换群。交换性：$\forall a,b\in G, ab=ba$。

整数加法群 $(Z,+,0)$ 是交换群，因为整数加法满足交换律。一般线性群 $GL(n)$ 由所有 $n\times n$ 的可逆矩阵和矩阵乘法组成，它不是交换群，因为矩阵乘法不满足交换律。在整数加法群 $(Z,+,0)$ 中，0 的周期是 1，除 0 以外的其他元素的周期都是无限的。

5. 整环的应用

代数整数环上的 Ramanujan 展开有：代数整数环上的 Ramanujan 和与酉 Ramanujan 和[5]。

对于次数 $d \geq 2$ 的数域 L/Q，我们把它的代数整数环记作 D_L。对于 D_L 中的任意非零理想 M、N，将 D_L 上的 Ramanujan 和与酉 Ramanujan 和分别定义为

$$C(M,N)=\sum_{J\mid(M,N)} N(J)\mu(N/J)$$

$$C^*(M,N)=\sum_{J\mid(M,N)^*} N(J)\mu^*(N/J)$$

特别地，对于二次域 $K=Q(\sqrt{d})$，当 $d\equiv 2$ 或 $3(\mathrm{mod}\,4)$ 时，K 的代数整数环为 $Z+Z\sqrt{d}$；当 $K=Q(\sqrt{i})$ 时，K 的代数整数环为 $Z[i]$。

Ramanujan 展开提供了一种计算模形式 Fourier 系数的有效方法，为研究整数的性质、素数的性质等数论问题提供了重要工具。总的来说，代数整数环上的 Ramanujan 展开在数学理论研究以及应用领域都有着重要的意义，为多个数学领域的发展提供了重要的理论支持和数学工具。

6. 小结

本文主要讨论整数环的构造，给出整数环的性质，整数环与其他理想环的关系、整数加法群的结构和性质，进而给出整数环在高等代数等其他数学学科的具体应用。如代数整数环上的 Ramanujan 展开、含有整除关系的 Menon 型恒等式、多重变量的 Menon 型恒等式。研究近世代数中的整数环，从环论、域论、反证等思想进行了研究，为高等代数等其他数学学科的学习提供了借鉴和参考。

基金项目

辽宁师范大学教师指导本科生科研训练项目，名称《整数环的性质与应用研究》，项目编号：CX202302013。

参考文献

[1] 王凌云. 代数整数环上 Menon 型恒等式的推广[D]: [硕士学位论文]. 南京: 南京师范大学, 2022.

[2] 董学东, 张妍. 二次整数环上的 ElGamal 密码体制和签名方案[J]. 计算机工程与应用, 2013, 49(19): 73-74.

[3] 徐鹏. 基于整数环的全同态加密算法设计及应用[D]: [硕士学位论文]. 郑州: 解放军信息工程大学, 2012.

[4] 张禾瑞. 近世代数基础(1978 年修订本) [M]. 北京: 高等教育出版社, 1978.

[5] 刘旭瑞. 代数整数环上的 Ramanujan 展开[D]: [硕士学位论文]. 广州: 华南理工大学, 2021.