第24卷 第4期 湖 南 工 业 大 学 学 报 Vol.24 No.4
2010年7月 Journal of Hunan University of Technology July 2010

$Z_n[\omega]$的代数结构

徐承杰

（湖南工业大学 理学院，湖南 株洲 412008）

摘　要：对n的素分解式分类，利用数论及环论知识，讨论了代数整数环的模n剩余类环$Z_n[\omega]$的素谱、单位乘群的阶、局部环直和分解。

关键词：$Z_n[\omega]$；素谱；零因子；单位；局部环

中图分类号：O153.3　　**文献标志码**：A　　**文章编号**：1673-9833(2010)04-0032-04

On the Structure of $Z_n[\omega]$

Xu Chengjie

（School of Science，Hunan University of Technology，Zhuzhou Hunan 412008，China）

Abstract: Classifies the prime decomposition of n. With the theory of numbers and rings, discusses the spectrium, the order of unit multiplication group and direct sum of local rings of $Z_n[\omega]$.

Keywords: $Z_n[\omega]$；spectrium；zero divisor；unit；local ring

0　引言

$Z[\mathrm{i}]=\{a+b\mathrm{i}|a,b\in\mathbf{Z}\}$和$Z[\omega]=\{a+b\omega|a,b\in\mathbf{Z}\}$（其中i为虚数单位，$\omega=-\frac{1}{2}+\frac{\sqrt{3}}{2}\mathrm{i}$为$x^3=1$的根，并且有$1+\omega+\omega^2=0$）是抽象代数环论中的2个重要环，常见于各种抽象代数教材及论文中。文献[1]讨论了代数整数环$Z[\omega]$的素元及剩余类环，并且证明了$Z[\omega]$为欧氏环，从而是主理想整环，因此是唯一分解整环。文献[2]讨论了$Z[\mathrm{i}]$的模n剩余类环$Z_n[\mathrm{i}]$的素谱和零因子。本文讨论代数整数环$Z[\omega]$的模n剩余类环$Z_n[\omega]$的零因子集合、单位群、素谱以及$Z_n[\omega]/J$的局部环直和分解。在不致混淆的前提下，文中用a表示Z_n中的$\bar{a}$，$a+b\omega$代替$\bar{a}+\bar{b}\omega$表示$Z_n[\omega]$中的元素，为了书写方便，没有把$Z_n[\omega]$中的理想写成剩余类的形式（例如：I是$Z[\omega]$的理想，若$(n)\subseteq I$，仍用I表示$Z_n[\omega]$的理想$I+(n)$）。此外，除非特别说明，文中所指环均为有限含幺交换环。p表示一个素数，Spec$R$表示环的素谱，Max$R$表示环的极大谱，J表示环的Jacbson根，即环的所有极大理想的交，用(a)表示由a生成的主理想，用$D(R)$表示环R的零因子集合，$U(R)$则是环R的单位乘群。

1　预备知识

引理1　关于$Z_n[\omega]$有以下结论：

1）$Z_n[\omega]\cong Z[\omega]/(n)$；

2）$Z_n[\omega]\cong Z_n[x]/\left(x^2+x+1\right)$；

3）$Z_n[\omega]$为主理想环；

4）$n\equiv 2(\mathrm{mod}3)$且n为素数$\Leftrightarrow Z_n[\omega]$为域。

证明　1）定义对应$f:Z[\omega]\to Z_n[\omega]$，对任意$a+b\omega\in Z[\omega]$，有

$f(a+b\omega)=\bar{a}+\bar{b}\omega,\ a,\ b\in\mathbf{Z},\ \bar{a},\bar{b}\in Z_n$，

收稿日期：2010-04-19

基金项目：国家自然科学基金资助项目（60874025）

通信作者：徐承杰（1982-）湖北汉川人，湖南工业大学教师，硕士，主要研究方向为代数学及其应用，稳定性理论，E-mail：Xu-chengjie@163.com

易知f为映射，且为满的环同态。又因为

$$\ker f=\left\{a+b\omega \,\middle|\, f(a+b\omega)=\bar{a}+\bar{b}\omega=0\right\},$$

一方面，由$x\in(n)\Rightarrow x=(a+b\omega)n\Rightarrow f(x)=0$知

$$(n)\subseteq\ker(f);$$

另一方面，由$a+b\omega\in\ker(f)$知

$$f(a+b\omega)=\bar{a}+\bar{b}\omega=0。$$

而$\bar{a}+\bar{b}\omega=0\Rightarrow a|n$，且$b|n\Rightarrow a+b\omega\in n\cdot Z[\omega]=(n)$，故$\ker(f)\subseteq(n)$，所以$\ker(f)=(n)$。

由同态基本定理知1）成立。

2）定义对应$\varphi:Z_n[x]\to Z_n[\omega]$，对任意$f(x)\in Z_n[x]$，有$\varphi(f(x))=f(\omega)$，易知$\varphi$为映射且为满的环同态。考察$\varphi$的核：

$$\ker\varphi=\left\{f(x)\in Z_n[x]\,\middle|\,\varphi(f(x))=f(\omega)=0\right\},$$

在$Z_n[\omega]$中，若ω为$f(x)$的根，则$f(x)$必含有因子x^2+x+1或其同余式，从而ω的共轭复数ϖ也是$f(x)$的根，因此

$$f(\omega)=0\Leftrightarrow(x-\omega)|f(x)\Leftrightarrow$$
$$x^2+x+1|f(x)\Leftrightarrow f(x)\in\left(x^2+x+1\right),$$

故$\ker\varphi=\left(x^2+x+1\right)$。再由同态基本定理有：

$$Z_n[\omega]\cong Z_n[x]/\left(x^2+x+1\right)。$$

3）由文献[1]知$Z[\omega]$为欧氏环，因而是主理想整环，即$Z[\omega]$中的每一个理想都是主理想，从而$Z_n[\omega]$的理想都为主理想，所以$Z_n[\omega]$为主理想环。

4）由文献[1]的定理1可知，$n\equiv2(\text{mod}\,3)$且n为素数$\Leftrightarrow n$为$Z[\omega]$的素元。若$n\equiv2(\text{mod}\,3)$且n为素数，则n为$Z[\omega]$的素元，故(n)为$Z[\omega]$的非零素理想，从而是极大理想，因此$Z_n[\omega]\cong Z[\omega]/(n)$为域，所以$n\equiv2(\text{mod}\,3)$且$n$为素数$\Rightarrow Z_n[\omega]$为域。

反之，若$Z_n[\omega]$为域，则(n)为$Z[\omega]$的极大理想，从而(n)为$Z[\omega]$的非零素理想，故n为$Z[\omega]$的素元，因此$n\equiv2(\text{mod}3)$且(n)为素数。所以4）成立。

引理2[3-4]　设R为有限环，则

1）$D(R)=\bigcup\limits_{p\in\text{Spec}R}P$，且$U(R)=R-D(R)$；

2）$\text{Max}R=\text{Spec}R$。

引理3　设p为素数，$R=Z_{p^k}[\omega]$，$I=(p)$是R的p生成的主理想，则$|I|=p^{2k-2}$。

证明　因为$(p)=pR=\left\{pr\,|\,r\in R\right\}$，

$$\forall\alpha=a+b\mathrm{i}\in(p)\Leftrightarrow\begin{cases}a\equiv0(\text{mod}\,p),\\ b\equiv0(\text{mod}\,p),\end{cases}$$

a,b仅可从$0,p,2p,\cdots,p^k-2p,p^k-p$中取值，从而$a,b$各有$p^{k-1}$种取法，所以$|I|=p^{2k-2}$。

引理4[5]　1）$Z_{mn}\cong Z_m\oplus Z_n\Leftrightarrow(m,n)=1$;

2）设$n=p_1^{k_1}p_2^{k_2}\cdots p_s^{k_s}$是$n$的标准素分解式，则$Z_n\cong Z_{p_1^{k_1}}\oplus\cdots\oplus Z_{p_s^{k_s}}$。

引理5[5]　设$R\cong R_1\oplus\cdots\oplus R_m$，则

$$U(R)=U(R_1)\times U(R_2)\times\cdots\times U(R_m),$$

又若$|U(R_i)|=k_i$，则

$$|U(R)|=k_1\cdots k_m,\ 1\le i\le m,\ i\in\mathbf{N}。$$

2　主要结果及证明

定理1　设$R=Z_n[\omega]$，

1）当$n=3^k$时，R为局部环，其唯一的极大理想为$(1-\omega)$，且$|D(R)|=3^{2k-1},|U(R)|=2\times3^{2k-1},R/J\cong Z_3$；

2）当$n=p^k$，$p\equiv1(\text{mod}3)$时，R为半局部环，R有2个极大理想(α)和$(\bar{\alpha})$，且$p=\alpha\cdot\bar{\alpha}$为$p$在$Z[\omega]$中的分解，$J(R)=(p)$，$|D(R)|=2p^{2k-1}-p^{2k-2}$，$|U(R)|=p^{2k}-2p^{2k-1}+p^{2k-2}$，$R/J\cong Z_p\oplus Z_p$；

3）当$n=p^k$，$p\equiv2(\text{mod}3)$时，R为局部环，其唯一的极大理想为(p)，$|D(R)|=|(p)|=p^{2k-2}$，$|U(R)|=p^{2k}-p^{2k-2}$，$R/J\cong Z_p[\omega]$。

证明　1）由文献[1]知$Z[\omega]$为欧氏环，从而是唯一分解环。在复数域中，x^2+x+1有因式分解：

$$x^2+x+1=(x-\omega)\left(x-\varpi\right)。$$

令$x=1$得：

$$3=(1-\omega)(1-\varpi)=(1-\omega)\left(1-\omega^2\right)=$$
$$(1+\omega)(1-\omega)^2=-\omega^2(1-\omega)^2,$$

从而$3^k=(-1)^k\omega^{2k}(1-\omega)^{2k}$。

再由文献[1]知ω为$Z[\omega]$的单位，$1-\omega$为$Z[\omega]$的素元，因此$(1-\omega)$为$Z[\omega]$的素理想，即极大理想。

由于$Z_n[\omega]$的素理想与$Z[\omega]$中包含(n)的素理想是一一对应的，而由$3^k=(-1)^k\omega^{2k}(1-\omega)^{2k}$可知，$Z[\omega]$中包含$(n)$唯一的极大理想为$(1-\omega)$，故$(1-\omega)$为$Z_{3^k}[\omega]$的唯一极大理想，因此$Z_{3^k}[\omega]$为局部环。由引理2知$D(R)=(1-\omega)$，所以$|D(R)|=|(1-\omega)|$。

以下证明$|(1-\omega)|=3^{2k-1}$。

记集合$A=\left\{x+y\omega\,|\,x,y\in Z_n,x+y\equiv0(\text{mod}\,3)\right\}$。

任取$r=a+b\omega\in R$，则

$$(1-\omega)\cdot r=(1-\omega)(a+b\omega)=(a+b)+(2b-a)\omega。$$

因$(a+b)+(2b-a)=3b\equiv0$，故$(1-\omega)\cdot r\in A$，即$(1-\omega)\subseteq A$。

反之，$\forall x+y\omega\in A$，由$x+y\equiv0(\text{mod}3)$知

$\dfrac{2x-y}{3},\dfrac{x+y}{3}\in Z_n$，从而

$$x+y\omega=\left(\frac{2x-y}{3}+\frac{x+y}{3}\omega\right)\cdot(1-\omega)\in(1-\omega),$$

故$A\subseteq(1-\omega)$。

综上所述$A=(1-\omega)$。

在R中，若$x+y\omega$满足$x+y\equiv0(\text{mod}3)$，则在$Z_n[\omega]$

$\left(n=3^k\right)$中，(x,y)的所有选择方法数为 3^{2k} 种。当 $n=3^k$ 时，$x+y\equiv 0(\mathrm{mod}3)$的选取种数与 $x+y\equiv 1(\mathrm{mod}3)$及 $x+y\equiv 2(\mathrm{mod}3)$的选取种数相等。因此 R 中满足 $x+y\equiv 0(\mathrm{mod}3)$的元素个数为$\frac{3^{2k}}{3}=3^{2k-1}$，所以$|D(R)|=|(1-\omega)|=\frac{3^{2k}}{3}=3^{2k-1}$，

$|U(R)|=|R|-|D(R)|=3^{2k}-3^{2k-1}=2\cdot 3^{2k-1}$。

又因为

$$J=(1-\omega),\ |R/J|=\frac{|R|}{|J|}=\frac{|R|}{|(1-\omega)|}=\frac{3^{2k}}{3^{2k-1}}=3,$$

所以$R/J\cong Z_3$。

2）由文献[1]知，当$p\equiv 1(\mathrm{mod}3)$时，p在$Z[\omega]$中的唯一素因子分解为$p=\alpha\cdot\bar{\alpha}$，其中$\alpha$与$\bar{\alpha}$都是$p$的互素的素因子。因此$p^k$在$Z[\omega]$中的唯一素因子分解为$p^k=\alpha^k\cdot\overline{\alpha^k}$，所以$Z[\omega]$中包含$(p)$的极大理想为$m_1=(\alpha)$，$m_2=(\bar{\alpha})$，故$R$仅有2个极大理想，从而为半局部环。又$m_1, m_2$极大，故必有$m_1+m_2=R$，即$m_1=(\alpha)$，$m_2=(\bar{\alpha})$在$Z_n[\omega]$中是互素的。

由I_1, I_2互素$\Rightarrow I_1\cap I_2=I_1I_2$[8]得：

$J=m_1\cap m_2=m_1m_2=(\alpha\bar{\alpha})=(p)$。

由引理3可知$|J|=p^{2k-2}$，而作为群，有$J\le m_i\le R(i=1,2)$，所以$|J|$整除$|m_i|$，$|m_i|$整除$|R|(i=1,2)$。因p是一个素数，$|m_i|(i=1,2)$必为p^{2k-1}，则

$|D(R)|=|m_1\cup m_2|=|m_1|+|m_2|-|J|=2p^{2k-1}-p^{2k-2}$，

$|U(R)|=|R|-|D(R)|=p^{2k}-2\cdot p^{2k-1}+p^{2k-2}$。

由引理4知$R/J\cong R/m_1\oplus R/m_2$，而$R/m_1$为域，且$|R/m_i|=p(i=1,2)$，故$R/m_i\cong Z_p(i=1,2)$，所以$R/J\cong Z_p\oplus Z_p$。

3）当$k=1$时，由引理1的4）可知，R为域，从而是局部环。

当$k\ge 2$时，由文献[1]知，p在$Z[\omega]$中不可约，故(p)是$Z[\omega]$中包含(n)的唯一极大理想，从而(p)是$Z_n[\omega]$的唯一极大理想，因此R为局部环。

由引理3知

$|J|=|(p)|=p^{2k-2}$，$|U(R)|=|R|-|D(R)|=p^{2k}-p^{2k-2}$。

从而$|R/J|=p^2$，所以R/J为p^2阶有限域。

又由引理1的4）知，当$p\equiv 2(\mathrm{mod}3)$时，$Z_p[\omega]$为p^2阶域，故$R/J\cong Z_p[\omega]$。

由文献[2]中定理3的2）有：

定理2 $Z_n[\omega]\cong Z_{p_1^{k_1}}[\omega]\oplus\cdots\oplus Z_{p_s^{k_s}}[\omega]$，且$n$的素分解式为$n=p_1^{k_1}p_2^{k_2}\cdots p_s^{k_s}$。

定理3 设$R=Z_n[\omega]$，$n=3^{k_0}p_1^{k_1}\cdots p_s^{k_s}q_1^{l_1}\cdots q_t^{l_t}$，$p_i\equiv 1(\mathrm{mod}3)$，$q_j\equiv 2(\mathrm{mod}3)$，$k_i, l_j\ge 1$，则

1）当$k_0=0$时，

$\mathrm{Spec}R=\left\{(\alpha_1),(\overline{\alpha_1}),\cdots,(\alpha_s),(\overline{\alpha_s}),(q_1),\cdots,(q_t)\right\}$，

当$k_0\ge 1$时，

$\mathrm{Spec}R=\left\{(1-\omega),(\alpha_1),(\overline{\alpha_1}),\cdots,(\alpha_s),(\overline{\alpha_s}),(q_1),\cdots,(q_t)\right\}$；

2）当$k_0=0$时，$|\mathrm{Spec}R|=|\mathrm{Max}R|=2s+t$，

当$k_0\ge 1$时，$|\mathrm{Spec}R|=|\mathrm{Max}R|=2s+t+1$；

3）当$k_0=0$时，$J=(p_1\cdots p_sq_1\cdots q_t)$，

当$k_0\ge 1$时，$J=((1-\omega)p_1\cdots p_sq_1\cdots q_t)$；

4）当$k_0=0$时，

$R/J\cong Z_{p_1}\oplus\cdots\oplus Z_{p_s}\oplus Z_{q_1}[\omega]\oplus\cdots\oplus Z_{q_t}[\omega]$，

当$k_0\ge 1$时，

$R/J\cong Z_3\oplus Z_{p_1}\oplus\cdots\oplus Z_{p_s}\oplus Z_{q_1}[\omega]\oplus\cdots\oplus Z_{q_t}[\omega]$。

证明 1）当$k_0=0$时，n在$Z[\omega]$中的不可约分解为$n=\left(\alpha_1\overline{\alpha_1}\right)^{k_1}\cdots\left(\alpha_s\overline{\alpha_s}\right)^{k_s}q_1^{l_1}\cdots q_t^{l_t}$，其中$p_i=\alpha_i\overline{\alpha_i}$。由交换代数知识容易得到：

$\mathrm{Spec}R=\left\{(\alpha_1),(\overline{\alpha_1}),\cdots,(\alpha_s),(\overline{\alpha_s}),(q_1),\cdots,(q_t)\right\}$；

同理，当$k_0\ge 1$时，有：

$\mathrm{Spec}R=\left\{(1-\omega),(\alpha_1),(\overline{\alpha_1}),\cdots,(\alpha_s),(\overline{\alpha_s}),(q_1),\cdots,(q_t)\right\}$。

2）由1）直接观察可得。

3）$k_0=0$时，R为有限环，则

$\mathrm{Spec}R=\mathrm{Max}R$，$J=\cap\mathrm{Max}R\cap\mathrm{Spec}R$。

由文献[8]知，若$I_1,I_2,\cdots,I_n$两两互素，则

$I_1\cap I_2\cap\cdots\cap I_n=I_1I_2\cdots I_n$。

再由文献[1]知：

$\mathrm{Spec}R=\left\{(\alpha_1),(\overline{\alpha_1}),\cdots,(\alpha_s),(\overline{\alpha_s}),(q_1),\cdots,(q_t)\right\}$，

其中$\alpha_i,\overline{\alpha_i},q_j,1\le i\le s,1\le j\le t$是极大理想，因而是两两互素的。所以：

$$J=\cap\mathrm{Spec}R=(\alpha_1)\cdot(\overline{\alpha_1})\cdot\cdots\cdot(\alpha_s)\cdot(\overline{\alpha_s})\cdot(q_1)\cdot\cdots\cdot(q_t)=\left(\alpha_1\cdot\overline{\alpha_1}\cdot\cdots\cdot\alpha_s\cdot\overline{\alpha_s}\cdot q_1\cdot\cdots\cdot q_t\right)=(p_1\cdots p_sq_1\cdots q_t)。$$

当$k_0\ge 1$时，证明与$k_0=0$相同。

4）由中国剩余定理，定理1及1）可得4），即R的局部环直和分解定理成立。

定理4 设$R=Z_n[\omega]$，$n=3^{k_0}p_1^{k_1}\cdots p_s^{k_s}q_1^{l_1}\cdots q_t^{l_t}$，$p_i\equiv 1(\mathrm{mod}3)$，$q_j\equiv 2(\mathrm{mod}3)$，$k_i, l_j\ge 1$，则

1）当$k_0=0$时，

$$|D(R)|=n^2-n^2\left(1-\frac{1}{p_1}\right)^2\cdots\left(1-\frac{1}{p_s}\right)^2\left(1-\frac{1}{q_1^2}\right)\cdots\left(1-\frac{1}{q_t^2}\right),$$

$$|U(R)|=n^2\left(1-\frac{1}{p_1}\right)^2\cdots\left(1-\frac{1}{p_s}\right)^2\left(1-\frac{1}{q_1^2}\right)\cdots\left(1-\frac{1}{q_t^2}\right)。$$

2）当$k_0\ge 1$时，

$$|D(R)|=n^2-\frac{2}{3}n^2\left(1-\frac{1}{p_1}\right)^2\cdots\left(1-\frac{1}{p_s}\right)^2\left(1-\frac{1}{q_1^2}\right)\cdots\left(1-\frac{1}{q_t^2}\right),$$

$$|U(R)|=\frac{2}{3}n^2\left(1-\frac{1}{p_1}\right)^2\cdots\left(1-\frac{1}{p_s}\right)^2\left(1-\frac{1}{q_1^2}\right)\cdots\left(1-\frac{1}{q_t^2}\right)。$$

证明　1）当$k_0=0$时，由定理2知：

$$R\cong Z_{p_1^{k_1}}[\omega]\times\cdots\times Z_{p_s^{k_s}}[\omega]\times Z_{q_1^{l_1}}[\omega]\times\cdots\times Z_{q_t^{l_t}}[\omega],$$

再由引理5知：

$$|U(R)|=\left|U\left(Z_{p_1^{k_1}}[\omega]\right)\right|\times\cdots\times\left|U\left(Z_{p_s^{k_s}}[\omega]\right)\right|\times\left|U\left(Z_{q_1^{l_1}}[\omega]\right)\right|\times\cdots\times\left|U\left(Z_{q_t^{l_t}}[\omega]\right)\right|=$$
$$\left(p_1^{2k_1}-2p_1^{2k_1-1}+p_1^{2k_1-2}\right)\cdots\left(p_s^{2k_s}-2p_s^{2k_s-1}+p_s^{2k_s-2}\right)\cdot\left(q_1^{2k_1}-q_1^{2k_1-2}\right)\cdots\left(q_t^{2k_t}-q_t^{2k_t-2}\right)=$$
$$p_1^{2k_1}\cdots p_s^{2k_s}q_1^{2l_1}\cdots q_t^{2l_t}\left(1-\frac{1}{p_1}\right)^2\cdots\left(1-\frac{1}{p_s}\right)^2\cdot\left(1-\frac{1}{q_1^2}\right)\cdots\left(1-\frac{1}{q_t^2}\right)=$$
$$n^2\left(1-\frac{1}{p_1}\right)^2\cdots\left(1-\frac{1}{p_s}\right)^2\left(1-\frac{1}{q_1^2}\right)\cdots\left(1-\frac{1}{q_t^2}\right)。$$

从而

$$|D(R)|=n^2-n^2\left(1-\frac{1}{p_1}\right)^2\cdots\left(1-\frac{1}{p_s}\right)^2\left(1-\frac{1}{q_1^2}\right)\cdots\left(1-\frac{1}{q_t^2}\right)。$$

2）的证明与1）类似。

参考文献：

[1] 于　萍,欧晓斌. 代数整数环$Z[\omega]$的素元及剩余类环[J]. 西安文理学院学报：自然科学版，2007，10(3)：111-113.
Yu Ping，Ou Xiaobin. The Prime Elements and Factor Ring of Algebrical Integral Ring $Z[\omega]$[J]. Journal of Xi’an University of Arts and Science：Natural Science Edition，2007，10(3)：111-113.

[2] 苏华东,唐高华. Z_n[i]的素谱和零因子[J]. 广西师范学院学报：自然科学版，2006，23(4)：1-4.
Su Huadong，Tang Gaohua. The Prime Spectrium and Zero Divisors of Z_n[i][J]. Journal of Guangxi Teachers Education University：Natural Science Edition，2006，23(4)：1-4.

[3] 冯克勤. 交换代数基础[M]. 北京：高等教育出版社，1985.
Feng Keqing. Basic Communicative Algebra[M]. Beijing：Higher Education Press，1985.

[4] 宋光天. 交换代数导引[M]. 合肥：中国科学技术大学出版社，2002.
Song Guangtian. Introduction to Communicative Algebra[M]. Hefei：University of Science and Technology of China Press，2002.

[5] 杨子胥. 近世代数[M]. 北京：高等教育出版社，2003.
Yang Zixu. Abstract Algebra[M]. Beijing：Higher Education Press，2003.

[6] Jacobson N. Basic Algebra[M]. New York：W. H. Freeman and co.，1980.

[7] 潘承洞，潘承彪. 初等数论[M]. 北京：北京大学出版社，2005.
Pan Chengdong，Pan Chengbiao. Elementary Number Theory [M]. Beijing：Peking University Press，2005.

[8] 王芳贵. 交换环与星型算子理论[M]. 北京：科学出版社，2006.
Wang Fanggui. Theory of Commutative Rings and Star-Operator[M]. Beijing：Science Press，2006.

（责任编辑：邓光辉）