DOI: 10.13656/j.cnki.gxkx.2009.02.006
广西科学 Guangxi Sciences 2009, 16(2): 147~150

The Zero-divisors and the Unit Group of Quaternion Algebra $Z_n[i,j,k]$*

Z_n 上四元数代数 $Z_n[i,j,k]$ 的零因子和单位群

WEI Yang-jiang, TANG Gao-hua, LIN Guang-ke
韦扬江,唐高华,林光科

(School of Mathematical Sciences, Guangxi Teachers Education University, Nanning, Guangxi, 530001, China)
(广西师范学院数学科学学院,广西南宁 530001)

Abstract We investigate the zero-divisors and the unit group of quaternion algebra over Z_n which is denoted by $Z_n[i,j,k]$ and obtain the calculating formulas of the number of zero-divisors and the order of the unit group of $Z_n[i,j,k]$. We prove that $Z_n[i,j,k] \cong M_2(Z_n)$ if and only if n is odd. In addition, the structure of the unit group of $Z_n[i,j,k]$ are completely determined.

Key words quaternion algebra, zero-divisor, unit group

摘要:研究 Z_n 上的四元数代数 $Z_n[i,j,k]$ 的零因子和单位群,给出 $Z_n[i,j,k]$ 的零因子个数和 $Z_n[i,j,k]$ 的单位群阶的计算公式,证明 $Z_n[i,j,k] \cong M_2(Z_n)$ 的充分必要条件是 n 为奇数,并且完全决定了 $Z_n[i,j,k]$ 的单位群结构.

关键词:四元数代数 零因子 单位群

中图法分类号: O153.3 文献标识码: A 文章编号: 1005-9164(2009)02-0147-04

Let R be an arbitrary ring, then it is well known that the ring of quaternions over R is denoted by $R[i,j,k]=\{a+bi+cj+dk \mid a,b,c,d\in R\}$, where i,j,k are formal symbols called basic units and $i^2=j^2=k^2=ijk=-1$. Moreover, if R is a commutative ring, then $R[i,j,k]$ is an R-algebra. $Z_n[i,j,k]=\{a+bi+cj+dk \mid a,b,c,d\in Z_n\}$ is the quaternion algebra over Z_n, where Z_n is the modulo n residue class ring.

Throughout the paper, H_n denotes the ring $Z_n[i,j,k]$. Assume $T=a+bi+cj+dk\in Z_n[i,j,k]$, then the scalar $N(T)=a^2+b^2+c^2+d^2$ will be called the norm of T. And the element $\overline{T}=a-bi-cj-dk$ will be called the conjugate element of T. It is easy to know that $T\overline{T}=\overline{T}T=N(T)$. And we put $\mathrm{Re}(T)=a$. If R is a ring, then $D(R)$ denotes the set of all zero-divisors of R. For any subset E of R, $|E|$ denotes the order of E, $U(R)$ is the unit group of R, and the Jacobson radical of R, denoted by $J(R)$, is defined to be the intersection of all the maximal left(right) ideals of R. If $T\in R$, then $\langle T\rangle$ denotes the two-sided ideal which is generated by T. $\langle T\rangle_L$ denotes the left principle ideal generated by T, while the right principle ideal generated by T, is denoted by $\langle T\rangle_R$. $M_n(R)$ denotes the ring of all $n\times n$ matrices over R. Given integers a and b, (a,b) denotes the greatest common divisor of a and b.

In this paper, we obtain the calculating formulas of the number of zero-divisors and the order of unit group of $Z_n[i,j,k]$. And we prove that $H_n \cong M_2(Z_n)$ if and only if $2\nmid n$. And the structure of the unit group of H_n are completely determined.

1 The zero-divisors and the order of unit group of $Z_n[i,j,k]$

Lemma 1.1 [1, P. 443, Example 4] Assume that p is an odd prime, $m\geqslant 1$, and the number of integer solutions of the congruence equation $x_1^2+x_2^2+$

收稿日期: 2008-11-17
作者简介: 韦扬江(1969-),女,副教授,主要从事代数学研究.
* Supported by the National Natural Science Foundation of China (10771095), the Guangxi Science Foundation(0832107, 0640070), the Innovation Project of Guangxi Graduate Education (2007106030701M15) and the Scientific Research Foundation of Guangxi Educational Committee(200707LX233).

$\cdots + x_m^2 \equiv 0 \pmod p$ is denoted by $T(m,p)$.

(Ⅰ) If m is even, $p \equiv 1 \pmod 4$, then $T(m,p) = p^{m-1} + (p-1)p^{\frac{m}{2}-1}$.

(Ⅱ) If m is even, $p \equiv 3 \pmod 4$, then $T(m,p) = p^{m-1} + (-1)^{\frac{m}{2}}(p-1)p^{\frac{m}{2}-1}$.

(Ⅲ) If m is odd, then $T(m,p) = p^{m-1}$.

Theorem 1.1 (Ⅰ) If $n = 2^t, t \geq 1$, then $|D(H_n)| = |U(H_n)| = 2^{4t-1}$.

(Ⅱ) If $n = p^t, t \geq 1, p$ is an odd prime, then $|D(H_n)| = (p^2 + p - 1)p^{4t-3}$, $|U(H_n)| = p^{4t}(1 - \frac{1}{p})(1 - \frac{1}{p^2})$.

(Ⅲ) If $n = p_1^{t_1}p_2^{t_2}\cdots p_m^{t_m}, m \geq 2$, and $p_1, p_2, \cdots, p_m$ are distinct odd primes, $t_1, t_2, \cdots, t_m \geq 1$, then $|D(H_n)| = n^4[1 - \prod_{e=1}^{m}(1 - \frac{1}{p^e})(1 - \frac{1}{p^{e^2}})]$, $|U(H_n)| = n^4\prod_{e=1}^{m}(1 - \frac{1}{p^e})(1 - \frac{1}{p^{e^2}})$.

(Ⅳ) If $n = 2^f p_1^{t_1}p_2^{t_2}\cdots p_m^{t_m}, f \geq 1, m \geq 1$, and $p_1, p_2, \cdots, p_m$ are distinct odd primes, $t_1, t_2, \cdots, t_m \geq 1$, then $|D(H_n)| = n^4[1 - \frac{1}{2}\prod_{e=1}^{m}(1 - \frac{1}{p^e})(1 - \frac{1}{p^{e^2}})]$, $|U(H_n)| = \frac{n^4}{2}\prod_{e=1}^{m}(1 - \frac{1}{p^e})(1 - \frac{1}{p^{e^2}})$.

Proof (Ⅰ) It is a direct conclusion of [2, Theorem 4.3].

(Ⅱ) Assume $n = p^t, t \geq 1, p$ is an odd prime. Then we have two cases to argument.

Case 1 Suppose $t = 1$, and $V = a + bi + cj + dk \in H_p$ with $0 \leq a,b,c,d \leq p - 1$. Then $V = a + bi + cj + dk \in D(H_p) \Leftrightarrow p \mid N(V) \Leftrightarrow \{a,b,c,d\}$ is a solution of the congruence equation

$$a^2 + b^2 + c^2 + d^2 \equiv 0 \pmod p. \quad (1)$$

Moreover, by Lemma 1.1, the number of solutions of equation (1) is $T(4,p) = p^3 + p^2 - p$. So $|D(H_n)| = p^3 + p^2 - p$. And therefore $|U(H_n)| = p^4 - |D(H_n)| = p^4 - p^3 - p^2 + p = p(1 - \frac{1}{p})(1 - \frac{1}{p^2})$.

Case 2 Suppose $t \geq 2$, and $V = a + bi + cj + dk \in H_{p^t}$ with $0 \leq a,b,c,d \leq p^t - 1$. Then $V = a + bi + cj + dk \in D(H_{p^t}) \Leftrightarrow p \mid N(V) \Leftrightarrow \{a,b,c,d\}$ is a solution of the congruence equation (1).

If $i = (a_0, b_0, c_0, d_0)$ with $0 \leq a_0, b_0, c_0, d_0 \leq p - 1$ is an integer solution of equation (1), and $a \equiv a_0 \pmod p, b \equiv b_0 \pmod p, c \equiv c_0 \pmod p, d \equiv d_0 \pmod p$, it is easy to see that $\{a,b,c,d\}$ is also a solution of the congruence equation (1). Therefore, for any $W_1, W_2, W_3, W_4 \in \{0, 1, 2, \cdots, p^{t-1}\}$, $(a_0 + W_1 p) + (b_0 + W_2 p)i + (c_0 + W_3 p)j + (d_0 + W_4 p)k \in D(H_n)$.

Thus from every solution $i = \{a_0, b_0, c_0, d_0\}$ with $0 \leq a_0, b_0, c_0, d_0 \leq p - 1$ of the equation (1), we can get $(p^{t-1})^4$ different zero-divisors of H_n. From case 1 we know that the equation (1) has $p^3 + p^2 - p$ different solutions $i = \{a_0, b_0, c_0, d_0\}$ with $0 \leq a_0, b_0, c_0, d_0 \leq p - 1$. Thus the equation (1) has $(p^3 + p^2 - p)(p^{t-1})^4$ different solutions $\{a,b,c,d\}$ with $0 \leq a,b,c,d \leq p^t - 1$. Hence, in this case, $|D(H_n)| = (p^2 + p - 1)p^{4t-3}$, and therefore $|U(H_n)| = p^{4t} - |D(H_n)| = p^{4t-3}(p^3 - p^2 - p + 1) = p^{4t}(1 - \frac{1}{p})(1 - \frac{1}{p^2})$.

(Ⅲ) Suppose $n = p_1^{t_1}p_2^{t_2}\cdots p_m^{t_m}, m \geq 2$. From [2, Lemma 3.6], we have $H_n \cong H_{p_1^{t_1}} \oplus H_{p_2^{t_2}} \oplus \cdots \oplus H_{p_m^{t_m}}$. Thus $|U(H_n)| = |U(H_{p_1^{t_1}})| \times \cdots \times |U(H_{p_m^{t_m}})| = p_1^{4t_1}(1 - \frac{1}{p_1})(1 - \frac{1}{p_1^2})\cdots p_m^{4t_m}(1 - \frac{1}{p_m})(1 - \frac{1}{p_m^2}) = n^4\prod_{e=1}^{m}(1 - \frac{1}{p^e})(1 - \frac{1}{p^{e^2}})$, and $|D(H_n)| = |H_n| - |U(H_n)| = n^4[1 - \prod_{e=1}^{m}(1 - \frac{1}{p^e})(1 - \frac{1}{p^{e^2}})]$.

(Ⅳ) Suppose $n = 2^f p_1^{t_1}p_2^{t_2}\cdots p_m^{t_m}, f \geq 1, m \geq 1$. By [2, Lemma 3.6], we have $H_n \cong H_{2^f} \oplus H_{p_1^{t_1}} \oplus H_{p_2^{t_2}} \oplus \cdots \oplus H_{p_m^{t_m}}$. Thus $|U(H_n)| = |U(H_{2^f})| \times |U(H_{p_1^{t_1}})| \times \cdots \times |U(H_{p_m^{t_m}})| = 2^{4f-1}p_1^{4t_1}(1 - \frac{1}{p_1})(1 - \frac{1}{p_1^2})\cdots p_m^{4t_m}(1 - \frac{1}{p_m})(1 - \frac{1}{p_m^2}) = \frac{n^4}{2}\prod_{e=1}^{m}(1 - \frac{1}{p^e})(1 - \frac{1}{p^{e^2}})$, and $|D(H_n)| = |H_n| - |U(H_n)| = n^4[1 - \frac{1}{2}\prod_{e=1}^{m}(1 - \frac{1}{p^e})(1 - \frac{1}{p^{e^2}})]$.

2 The structure of $Z_n[i,j,k]$

In the next, we use $H(F)$ to denote the quaternion algebra over field F.

Lemma 2.1 [3, Theorem 7.4.6] Assume that $\mathrm{char}(F) \neq 2$. Then the quaternion algebra $H(F)$ is either a division ring or being isomorphic to $M_2(F)$, the ring of 2×2 matrices over F. The last possibility if and only if the equation $x^2 + y^2 = -1$ can be solved in F, and the map $\theta: H(F) \to M_2(F)$ given by

$\theta(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \theta(i) = \begin{pmatrix} x & y \\ y & -x \end{pmatrix}, \theta(j) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \theta(k) = \begin{pmatrix} -y & x \\ x & y \end{pmatrix}$.

It is an isomorphism of rings.

Lemma 2.2 If p is an odd prime and $t \geqslant 1$, then the congruence equation $x^2 + y^2 \equiv -1 \pmod{p^t}$ has an integer solution x_0, y_0 such that $(x_0, y_0, p) = 1$.

Proof First, by [1, P. 443, Example 4], the congruence equation in x, y: $x^2 + y^2 \equiv -1 \pmod{p}$ must has integer solutions. Assume that integers x_0, y_0 satisfy $x_0^2 + y_0^2 \equiv -1 \pmod{p}$, let $x_0^2 + y_0^2 = m_1 p - 1$, where m_1 is an integer. Then it is easy to see that $(x_0, y_0, p) = 1$.

Second, we claim that the congruence equation

$$(x_0 + xp)^2 + (y_0 + yp)^2 \equiv -1 \pmod{p^2} \quad (2)$$

must has integer solutions. In fact, by simple computations, the equation (2) can be written as

$$2p(x_0 x + y_0 y) \equiv -m_1 p \pmod{p^2}. \quad (3)$$

Since $(2px_0, 2py_0, p^2) = p$ and $p \mid m_1 p$, the equation (3) has integer solutions. Assume that integers x_1, y_1 satisfy $(x_0 + x_1 p)^2 + (y_0 + y_1 p)^2 \equiv -1 \pmod{p^2}$, let $(x_0 + x_1 p)^2 + (y_0 + y_1 p)^2 = m_2 p^2 - 1$, where m_2 is an integer. Then it is certainly that $(x_0 + x_1 p, y_0 + y_1 p, p) = 1$.

Third, we claim that the congruence equation

$$(x_0 + x_1 p + x p^2)^2 + (y_0 + y_1 p + y p^2)^2 \equiv -1 \pmod{p^3} \quad (4)$$

has integer solutions. In fact, by simple computations, the equation (4) can be written as

$$2p^2((x_0 + x_1 p)x + (y_0 + y_1 p)y) \equiv -m_2 p^2 \pmod{p^3}. \quad (5)$$

Since $(2p^2(x_0 + x_1 p), 2p^2(y_0 + y_1 p), p^3) = p^2$ and $p^2 \mid m_2 p^2$, the equation (5) has integer solution x_2, y_2 such that $(x_0 + x_1 p + x_2 p^2, y_0 + y_1 p + y_2 p^2, p) = 1$.

Therefore, by the similar argument, we can conclude that for any odd prime p and integer $t \geqslant 1$, the congruence equation $x^2 + y^2 \equiv -1 \pmod{p^t}$ must has an integer solution x_0, y_0 such that $(x_0, y_0, p) = 1$.

Theorem 2.1 $Z_n[i,j,k] \cong M_2(Z_n) \Leftrightarrow 2 \nmid n$, for $n \geqslant 1$.

Proof "$\Leftarrow$". Assume $2 \nmid n$, we need to prove that $H_n \cong M_2(Z_n)$.

Case 1 Assume that $n = p$ is an odd prime. Since Z_p is a field, by Lemma 2.1 and Lemma 2.2, we have $Z_p[i,j,k] \cong M_2(Z_p)$.

Case 2 Assume that $n = p^t$, where p is an odd prime and $t \geqslant 2$. By Lemma 2.2, there exist two non-zero integers x, y such that $x^2 + y^2 \equiv -1 \pmod{p^t}$ and $(x, y, p) = 1$. Without loss of generality, we may assume that $(p, y) = 1$. Let $\theta: Z_{p^t}[i,j,k] \to M_2(Z_{p^t})$ be a map defined as Lemma 2.1. It is easy to verify that θ is a ring homomorphism. We claim that θ is injective. To prove our claim, it suffices to show that the kernel of θ is equal to 0. For an element $T = a + bi + cj + dk \in Z_{p^t}[i,j,k]$ such that

$$\theta(T) = a\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b\begin{pmatrix} x & y \\ y & -x \end{pmatrix} + c\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + d\begin{pmatrix} -y & x \\ x & y \end{pmatrix} = 0,$$

we have the following system of linear homogenous equations in a, b, c, and d.

$$a + bx - dy \equiv 0 \pmod{p^t}, \quad (6)$$

$$c + by + dx \equiv 0 \pmod{p^t}, \quad (7)$$

$$-c + by + dx \equiv 0 \pmod{p^t}, \quad (8)$$

$$a - bx + dy \equiv 0 \pmod{p^t}. \quad (9)$$

From (6) + (9) and (7) − (8), we derive $2a \equiv 0 \pmod{p^t}$, $2c \equiv 0 \pmod{p^t}$. Since $2 \nmid p$, we have $a = 0$, $c = 0$. Substituting these values into formula (6) and formula (7), we obtain

$$bx \equiv dy \pmod{p^t}, \quad (10)$$

$$by \equiv -dx \pmod{p^t}. \quad (11)$$

Since $x \neq 0, y \neq 0$, by (10) $\times x$ + (11) $\times y$, we derive $b(x^2 + y^2) \equiv 0 \pmod{p^t}$, and then $b \equiv 0 \pmod{p^t}$. On the other hand, substituting $a = b = 0$ into formula (6), we have $dy \equiv 0 \pmod{p^t}$. Since $(p, y) = 1$, we get $d = 0$. Therefore $\theta(T) = 0 \Leftrightarrow T = 0$. Thus θ is injective. Moreover, since $|Z_n[i,j,k]| = |M_2(Z_n)|$ is finite, θ is bijective. Therefore, θ is a ring isomorphism, which implies that $Z_{p^t}[i,j,k] \cong M_2(Z_{p^t})$.

Case 3 Assume that $n = p_1^{t_1} p_2^{t_2} \cdots p_m^{t_m}$, where $p_1, \cdots, p_m$ are distinct odd primes and $m \geqslant 2, t_1, \cdots, t_m \geqslant 1$. Then

$$Z_n[i,j,k] \cong Z_{p_1^{t_1}}[i,j,k] \oplus \cdots \oplus Z_{p_m^{t_m}}[i,j,k] \cong M_2(Z_{p_1^{t_1}}) \oplus \cdots \oplus M_2(Z_{p_m^{t_m}}) \cong M_2(Z_{p_1^{t_1}} \oplus \cdots \oplus Z_{p_m^{t_m}}) \cong M_2(Z_{p_1^{t_1} \cdots p_m^{t_m}}) = M_2(Z_n).$$

"$\Rightarrow$". Assume that $Z_n[i,j,k] \cong M_2(Z_n)$, we need

to prove $2 \nmid n$.

If $n = 2^t$ with $t \geq 1$, then it is easy to verify that $M_2(Z_n)$ is not a local ring. In fact, both of $A = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ are zero-divisors in $M_2(Z_n)$ but $A + B = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ is a unit of $M_2(Z_n)$, so $M_2(Z_n)$ is not a local ring. On the other hand, by [2, Theorem 3.7], $Z_n[i,j,k]$ is a local ring, thus $Z_n[i,j,k] \ncong M_2(Z_n)$, which implies that $n \neq 2^t$.

If $n = 2^f p_1^{t_1} \cdots p_m^{t_m}$, where $f \geq 1, m \geq 1, p_1, \cdots, p_m$ are distinct odd primes and $t_1, \cdots, t_m \geq 1$. By [2, Lemma 3.6], we have $H_n \cong H_{2^f} \oplus H_{p_1^{t_1}} \oplus \cdots \oplus H_{p_m^{t_m}} \ncong M_2(Z_{2^f}) \oplus M_2(Z_{p_1^{t_1}}) \oplus \cdots \oplus M_2(Z_{p_m^{t_m}}) \cong M_2(Z_{2^f} \oplus Z_{p_1^{t_1}} \oplus \cdots \oplus Z_{p_m^{t_m}}) \cong M_2(Z_n)$. Therefore $H_n \ncong M_2(Z_n)$. This completes the proof.

3 The unit group of $Z_n[i,j,k]$

From [2, Theorem 3.8], we know that the ideal $M = \langle 1+i, 1+j, 1+k \rangle = \langle 1+i, 1+j, 1+k \rangle_L = \langle 1+i, 1+j, 1+k \rangle_R$ is a maximal ideal in $Z_n[i,j,k]$ if $2 \mid n$.

Lemma 3.1 Suppose $2 \mid n$. Let $M = \langle 1+i, 1+j, 1+k \rangle$ in H_n and $N = \{a_1(1+i) + a_2(1-i) + b_1(1+j) + b_2(1-j) + c_1(1+k) + c_2(1-k) \mid a_\alpha, b_\alpha, c_\alpha \in Z_n, \lambda = 1, 2\}$. Then $M = N$.

Proof It is certainly that $N \subseteq M$. On the other hand, assume that $T = T_1(1+i) + T_2(1+j) + T_3(1+k) \in M$, where $T_1 = a_1 + a_2 i + a_3 j + a_4 k$, $T_2 = b_1 + b_2 i + b_3 j + b_4 k$, , $T_3 = c_1 + c_2 i + c_3 j + c_4 k \in H_n$. Then

$$T = (a_1 - a_2 + b_1 - b_3 + c_1 - c_4) + (a_1 + a_2 + b_2 - b_4 + c_2 + c_3)i + (a_3 + a_4 + b_1 + b_3 + c_3 - c_2)j + (a_4 - a_3 + b_2 + b_4 + c_1 + c_4)k = (a_1 + b_2 + c_3)(1+i) + (b_4 - a_2 - c_2)(1-i) + (a_3 + b_1)(1+j) + (c_2 - a_4 - b_3 - c_3)(1-j) + (a_4 - a_3 + c_1)(1+k) + (-b_2 - b_4 - c_4)(1-k) \in N.$$

Hence, we must have $M = N$.

In the following, G_{2^t} denotes the unit group of $Z_{2^t}[i,j,k]$, $GL_m(R)$ denotes the group of invertible $m \times m$ matrices over a given ring R.

Theorem 3.1 (Ⅰ) Suppose $n = 2$, then $G_2 \cong Z_2 \oplus Z_2 \oplus Z_2$.

(Ⅱ) Suppose $n = 2^t$ while $t \geq 2$, then $G_{2^t} = \{1 + T \mid T \in N\}$, where N is presented in Lemma 3.1.

(Ⅲ) Suppose $n = p_1^{t_1} \cdots p_m^{t_m}$, where $m \geq 1, p_1, \cdots, p_m$ are distinct odd primes and $t_1, \cdots, t_m \geq 1$. Then $U(H_n) \cong GL_2(Z_{p_1^{t_1}}) \oplus \cdots \oplus GL_2(Z_{p_m^{t_m}})$.

(Ⅳ) Suppose $n = 2^f p_1^{t_1} \cdots p_m^{t_m}$, where $f \geq 1, m \geq 1, p_1, \cdots, p_m$ are distinct odd primes and $t_1, \cdots, t_m \geq 1$. Then $U(H_n) \cong G_{2^f} \oplus GL_2(Z_{p_1^{t_1}}) \oplus \cdots \oplus GL_2(Z_{p_m^{t_m}})$.

Proof (Ⅰ) It is easy to verify that $G_2 \cong Z_2 \oplus Z_2 \oplus Z_2$.

(Ⅱ) By Lemma 3.1, $\forall U = 1 + T$ where $T \in N$, it is easy to verify that $2 \nmid N(U)$, thus by [2, Corollary 4.4], we have $U \in G_{2^t}$. On the contrary, by [2, Corollary 4.4], we have $H_{2^t}/M \cong Z_2$. Thus $\forall V \in G_{2^t}$, we must have $V = 1 + T$, where $T \in M = N$. Therefore $G_{2^t} = \{1 + T \mid T \in N\}$.

(Ⅲ) By Theorem 2.1, we have $H_n \cong H_{p_1^{t_1}} \oplus \cdots \oplus H_{p_m^{t_m}} \cong M_2(Z_{p_1^{t_1}}) \oplus \cdots \oplus M_2(Z_{p_m^{t_m}})$, thus $U(H_n) \cong GL_2(Z_{p_1^{t_1}}) \oplus \cdots \oplus GL_2(Z_{p_m^{t_m}})$.

(Ⅳ) By Theorem 2.1, we have $H_n \cong H_{2^t} \oplus H_{p_1^{t_1}} \oplus \cdots \oplus H_{p_m^{t_m}} \cong H_{2^t} \oplus M_2(Z_{p_1^{t_1}}) \oplus \cdots \oplus M_2(Z_{p_m^{t_m}})$, thus $U(H_n) \cong G_{2^t} \oplus GL_2(Z_{p_1^{t_1}}) \oplus \cdots \oplus GL_2(Z_{p_m^{t_m}})$.

References

[1] Pan C D, Pan C B. Elementary number theory[M]. Beijing: Beijing university publishing company, 2005.

[2] Wei Y J, Tang G H. The spectra and radicals of quaternion algebra $Z_n[i,j,k]$. Journal of Guangxi Teachers Education University, 2009, 26(1): 1-10.

[3] Milies C P, Sehgal S K. An introduction to group rings[M]. Kluwer Academic Publishers: Springer, 2002.

(责任编辑: 尹 闯)