DOI: 10.26485/0459-6854/2017/67.1/4 PL ISSN 0459-6854

B U L L E T I N

DE LA SOCIÉTÉ DES SCIENCES ET DES LETTRES DE ŁÓDŹ

2017 Vol. LXVII

Recherches sur les déformations no. 1

pp. 49–70

Jan Jakóbowski

SOME NONCOMMUTATIVE RINGS CONSTRUCTED ON THE BASE OF POLYNOMIALS $x^2 + tx + 1$ AND THEIR ZERO DIVISORS

Summary

For any Galois field $F = GF(p^n)$ we construct some ring extension $\mathfrak{R}(F)$ of order p^{4n}. Such construction may be applied also for any infinite field F with $\operatorname{char} F \neq 0$. Then, for any element of $\mathfrak{R}(F)$ we give necessary and sufficient condition to be a zero divisor. With additional assumptions, we make some variations on this condition. In special cases we are able to calculate easily the number of all zero divisors and of idempotents and nilpotents of degrre 2. The method used to construct $\mathfrak{R}(F)$ is the following. First we find $t \in F$, such that the polynomial $x^2 + tx + 1$ does not have roots in F (such t-s exist!). Then we take the 4-dimensional F-vector space with basic elements 1, i, j, k, where i, j, k not belonging to F are roots of $x^2 + tx + 1$ in the ring extension, and $ji = -k - t$. Thus multiplication of i, j, k (and hence in all ring) is some generalization of multiplication in the real Hamilton quaternions.

In consequence, we have got wide class of noncommutative rings. It is known very much on noncommutative rings of smaller order, e.g. in 1994 J. B. Derr, G. F. Orr, and P. S. Peck classified all noncommutative rings of order p^4, using radical as a helpful tool. Thus, in the particular case $n = 1$, each of the rings constructed here must be of one kind given by Derr and the others. Our consideration is more general. It turns out that selected properties of $\mathfrak{R}(F)$ depend on $\operatorname{char} F$ and on $t^2 - 2^2$ is a square in F or not. To get these and other results, we use some properties of multiplicative subgroup of nonzero squares in $GF(p^n)$ and of the polynomial x^2+tx+1. All contents is provided with examples illustrating general situation or special cases.

Keywords and phrases: Galois field, polynomial, noncommutative ring, zero divisor, vector space, skew field of quaternions

1. Introduction

Let F be any field with $\operatorname{char} F = p$, where p is prime (eg. [6, p. 83]). It is obvious that there exists $t \in F$ such that the polynomial $x^2 + tx + 1$ is irreducible in F. Our construction of the ring (denoted by $\mathfrak{R}(F)$) is based on the following foundations:

$$i, j, k \notin F;\ i^2 + ti + 1 = 0,\ j^2 + tj + 1 = 0,\ k^2 + tk + 1 = 0;\ ji + k + t = 0.$$

Therefore, for $t = 0$, the construction is almost a copy of Hamilton algebra of all real quaternions [6, p. 380]; for $t = 1$ all general formulae become simpler and we are able to determine quickly some combinatorial properties. To vary and apply quaternions construction to a field F with $\operatorname{char} F \neq 0$, some authors assume that $\operatorname{char} F \neq 2$ and put $i^2 = a$, $j^2 = b$, $ij = -ji = k$, where a, b are not squares in F (cf. [1] and [7, p. 1314]). This way they usually obtain either infinite division ring or a ring isomorphic with the ring of matrices $M_{2\times 2}(F)$ [8, p. 16, 19]. Note that the Hamilton algebra of all real quaternions is isomorphic to some subring of matrices $M_{4\times 4}(R)$ [5, p. 16].

Our construction is much more general. We regard every nonzero characteristic p and some properties of the ring depends on what this characteristic is.
On the other hand, J. B. Derr and the others in [2] have described all the isomorphism classes of noncommutative rings of order p^4. Their classification depends only on the radical of a ring. The most of their classes consists of special type of matrices and seemingly has no connection with our construction. However, in the case of order p^4 the rings constructed here must belong to classes given in [2].

More examples of not-division rings based on quaternions construction, are given in [5, §1].

1.1. Preliminaries useful for farther consideration

Remark 1.1.
- *For every field F, the multiplicative subgroup of all nonzero squares will be denoted by S.*
- *In this paper a nilpotent (resp. idempotent) z of degree 2 (i.e. $z^2 = 0$ or $z^2 = z$, respectively) will be shortly called a nilpotent (resp. idempotent).*

From Fermat's two squares theorem [3] the following is immediate.

Proposition 1.2. [4, p. 251–252] *Let $GF(p^n)$ be the Galois field with odd p. Then $p^n = 4m + 1$ for some positive integer m, if and only if for every $a \in GF(p^n)$ we have $a \in S \Leftrightarrow -a \in S$. In particular, the element -1 is a square iff $p^n = 4m + 1$.*

We apply properties of polynomial $x^2 + tx + 1$, e.g. the following:

Remark 1.3. *If a is a root of the polynomial $x^2 + tx + 1$ over a field F, then $a^{-1} = -a - t$ is the second root. Moreover, if $t = 1$, then $a^{-1} = a^2$. If a is a root of $x^2 + tx + 1$ then $x^2 - tx + 1$ has the roots $-a$ and $a + t$.*

The following property (proved in further part of the work) is very useful for our consideration: the equation $x^2 + y^2 - txy = 0$ over F, where $\operatorname{char} F > 3$, has a nonzero solution if and only if $t^2 - 2^2$ is a square in F. Using this condition we are able to evaluate, more or less precisely, the numbers of all zero divisors, idempotents and nilpotents.

2. Construction of the ring and its selected properties

Let us take any field F of nonzero characteristic and $t \in F$, such that the polynomial $x^2 + tx + 1$ has no roots in F. Then $-2 \neq t \neq 2$ for $\operatorname{char} F \neq 2$. Let i, j, k are elements not belonging to F, and assume:

$$i^2 + ti + 1 = 0, \quad j^2 + tj + 1 = 0, \quad k^2 + tk + 1 = 0, \quad ji + k + t = 0. \tag{2.1}$$

Then we take the standard vector space $V = \{a + bi + cj + dk;\ a, b, c, d \in F\}$ over F with the base 1, i, j, k and we have to define multiplication so that to get a ring. In particular, we require multiplication to be associative and both-side distributive with respect to addition. Therefore, by (2.1), we obtain subsequently:

$$\begin{aligned} -i = (j^2 + tj)i = (j + t)(ji) = (j + t)(-k - t) = -jk - tj - tk - t^2, \\ \text{i.e.} \quad jk = i - t(j + k + t)]; \\ -j = j(k^2 + tk) = (jk)(k + t) = (jk)k + tjk = \\ = (i - tj - tk - t^2)k + tjk = ik - tjk - tk^2 - t^2k + tjk = \\ = ik - t(k^2 + tk) = ik + t \quad \text{i.e.} \quad ik = -j - t. \end{aligned}$$

In the same way we subsequently obtain ij, kj and ki; thus multiplication on basic elements is defined as follows.

Definition 2.1. *Multiplication of basic elements is given in Table 1, where an element from heading column is taken as the first, from heading row – as the second one.*

Tab. 1: Multiplication of basic elements

$\cdot$	1	i	j	k
1	1	i	j	k
i	i	$-1 - ti$	$k - t(i + j + t)$	$-j - t$
j	j	$-k - t$	$-1 - tj$	$i - t(j + k + t)$
k	k	$j - t(k + i + t)$	$-i - t$	$-1 - tk$

Corollary 2.2. *Multiplication on any two elements of our algebraic structure is defined as*

$$\begin{aligned}
&(a+bi+cj+dk)(p+qi+rj+sk) =\\
&= [ap-(bq+cr+ds)-t(bs+cq+dr)+\\
&- t^2(br+cs+dq)]+\\
&+ [aq+bp+cs-dr-t(bq+br+dq)]i+\\
&+ [ar-bs+cp+dq-t(br+cr+cs)]j+\\
&+ [as+br-cq+dp-t(cs+dq+ds)]k.
\end{aligned} \tag{2.2}$$

Corollary 2.3. **a)** *If* $\operatorname{char} F \neq 2$*, then*

$$\begin{aligned}
&(a+bi+cj+dk)^2 = \{a^2-[(b+c+d)^2+\\
&+ (t^2+t-2)(bc+cd+db)]\}+\\
&+ [2a-t(b+c+d)](bi+cj+dk);
\end{aligned}$$

b) *if* $\operatorname{char} F = 2$*, then*

$$\begin{aligned}
&(a+bi+cj+dk)^2 = [a^2+b^2+c^2+d^2]+\\
&+ (t^2+t)(bc+cd+db)+\\
&+ t(b+c+d)(bi+cj+dk);
\end{aligned}$$

c) *If* $t^2+t=2$ *or* $bc+bd+cd=0$*, then*

$$(a+bi+cj+dk)^2 = 0 \Leftrightarrow a=0 \wedge b+c+d=0\ .$$

If the former assumption is the case, then $t=1$.

Proposition 2.4. *The structure* $(V,+,\cdot)$ *with multiplication defined by* (2.2) *is a noncommutative ring.*

Proof. $(V,+)$ is a group since addition is the same as in the vector space V. We have to verify associativity of multiplication and both-side distributivity. Easy but lengthy calculations, omitted here, give the following final results confirming these properties.

- Multiplication is associative:

$$\begin{aligned}
&[(a+bi+cj+dk)(p+qi+rj+sk)](u+vi+wj+zk) =\\
&= \{[ap-(bq+cr+ds)-t(bs+cq+dr)-t^2(br+cs+dq)]u+\\
&+ [-aq-bp-cs+dr+t(-ar+bq+br+bs-cp)+\\
&+ t^2(-as+cq+cr+cs-dp)+t^3(cs+dq+ds)]v+\\
&+ [-ar+bs-cp-dq+t(-as+cq+cr+cs-dp)+
\end{aligned}$$

$$\begin{aligned}
&+ t^2(-aq - bp + dq + dr + ds) + t^3(bq + br + dq)]w+\\
&+ [-as - br + cq - dp + t(-aq - bp + dq + dr + ds)+\\
&+ t^2(-ar + bq + br + bs - cp) + t^3(br + cr + cs)]z\}+\\
&+ \{[aq + bp + cs - dr - t(bq + br + dq)]u+\\
&+ [ap - (bq + cr + ds) - t(aq + as + bp + br + bs + cs + dp)+\\
&+ t^2(bq + dq + ds)]v+\\
&+ [-as - br + cq - dp + t(-aq - bp + dq + dr + ds) + t^2(bq + br + dq)]w+\\
&+ [ar - bs + cp + dq - t(br + cr + cs)]z\}i+\\
&+ \{[ar - bs + cp + dq - t(br + cr + cs)]u+\\
&+ [as + br - cq + dp - t(cs + dq + ds)]v+\\
&+ [ap - (bq + cr + ds) - t(aq + ar + bp + cp + cq + cs + dq)+\\
&+ t^2(bq + br + cr)]w+\\
&+ [-aq - bp - cs + dr + t(-ar + bq + br + bs - cp) + t^2(br + cr + cs)]z\}j+\\
&+ \{[as + br - cq + dp - t(cs + dq + ds)]u+\\
&+ [-ar + bs - cp - dq + t(-as + cq + cr + cs - dp) + t^2(cs + dq + ds)]v+\\
&+ [aq + bp + cs - dr - t(bq + br + dq)]w + [ap - (bq + cr + ds)-\\
&- t(ar + as + br + cp + dp + dq + dr) + t^2(cr + cs + ds)]z\}k =\\
&= (a + bi + cj + dk)[(p + qi + rj + sk)(u + vi + wj + zk)].
\end{aligned}$$

- Law of left distributivity:

$$\begin{aligned}
&(a + bi + cj + dk)[(p + qi + rj + sk) + (u + vi + wj + zk)] =\\
&= \{a(p + u) - [b(q + v) + c(r + w) + d(s + z)] - t[b(s + z) + c(q + v)+\\
&+ d(r + w)] - t^2[b(r + w) + c(s + z) + d(q + v)]\} + \{a(q + v) + b(p + u)+\\
&+ c(s + z) - d(r + w) - t[b(q + v) + b(r + w) + d(q + v)]\}i + \{a(r + w)-\\
&- b(s + z) + c(p + u) + d(q + v) - t[b(r + w) + c(r + w) + c(s + z)]\}j+\\
&+ \{a(s + z) + b(r + w) - c(q + v) + d(p + u) - t[c(s + z) + d(q + v)+\\
&+ d(s + z)]\}k = (a + bi + cj + dk)(p + qi + rj + sk)+\\
&+ (a + bi + cj + dk)(u + vi + wj + zk).
\end{aligned}$$

- Law of right distributivity:

$$\begin{aligned}
&[(a + bi + cj + dk) + (p + qi + rj + sk)](u + vi + wj + zk) =\\
&= \{(a + p)u - [(b + q)v + (c + r)w + (d + s)z] - t[(b + q)z + (c + r)v+\\
&+ (d + s)w] - t^2[(b + q)w + (c + r)z + (d + s)v]\} + \{(a + p)v + (b + q)u+\\
&+ (c + r)z - (d + s)w - t[(b + q)v + (b + q)w + (d + s)v]\}i + \{(a + p)w-\\
&- (b + q)z + (c + r)u + (d + s)v - t[(b + q)w + (c + r)w + (c + r)z]\}j+
\end{aligned}$$

$$+\,\{(a+p)z+(b+q)w-(c+r)v+(d+s)u-t[(c+r)z+(d+s)v+$$
$$+\,(d+s)z]\}k=(a+bi+cj+dk)(u+vi+wj+zk)+$$
$$+\,(p+qi+rj+sk)(u+vi+wj+zk). \qquad \square$$

We shall denote the ring constructed above by $\mathfrak{R}(F)$. Since multiplication in $\mathfrak{R}(F)$ is associative, it follows that the left inverse (if exists) of any element is equal to the right one. It is obvious that char $\mathfrak{R}(F) = \operatorname{char} F$.

Example 2.5. Let us consider possible irreducible polynomials x^2+tx+1 in small prime fields (cf. Remark 1.3). In $GF(2)$ there is only x^2+x+1; in $GF(3)$ only x^2+1; in $GF(5)$ x^2+x+1, and x^2+4x+1; in $GF(7)$, x^2+1, x^2+3x+1 and x^2+4x+1; in $GF(11)$ x^2+1, x^2+x+1, x^2+5x+1, x^2+6x+1, and $x^2+10x+1$; in $GF(13)$ x^2+3x+1, x^2+5x+1, x^2+6x+1, x^2+7x+1, x^2+8x+1, and $x^2+10x+1$.

Tab. 2: Addition and multiplication in $GF(2^3)$

$+$	0	1	A	B	C	D	E	F
0	0	1	A	B	C	D	E	F
1	1	0	B	A	D	C	F	E
A	A	B	0	1	E	F	C	D
B	B	A	1	0	F	E	D	C
C	C	D	E	F	0	1	A	B
D	D	C	F	E	1	0	B	A
E	E	F	C	D	A	B	0	1
F	F	E	D	C	B	A	1	0

$\cdot$	0	1	A	B	C	D	E	F
0	0	0	0	0	0	0	0	0
1	0	1	A	B	C	D	E	F
A	0	A	C	E	B	1	F	D
B	0	B	E	D	F	C	1	A
C	0	C	B	F	E	A	D	1
D	0	D	1	C	A	F	B	E
E	0	E	F	1	D	B	A	C
F	0	F	D	A	1	E	C	B

Now, take the fields $GF(2^2)$ with elements $0,\ 1,\ A,\ B$ where $A+1=A^2=B$, $AB=A+B=1$, and $GF(2^3)$. In the former case x^2+Ax+1, and x^2+Bx+1 are the irreducible polynomials. In the latter case polynomials over $GF(2)$ of degree less than 3, i.e.

0, 1, $A=x$, $B=x+1$, $C=x^2$, $D=x^2+1$, $E=x^2+x$, $F=x^2+x+1$, may be used as elements of $GF(2^3)$. Results of multiplication are residuals of division by irreducible polynomial $x^3 + x + 1$. Thus Table 2 presents addition and multiplication. One can easily check that polynomials $x^2 + x + 1$, $x^2 + Ax + 1$, $x^2 + Cx + 1$, and $x^2 + Ex + 1$ are irreducible. The polynomial $x^2 + 1$ has a double root 1, and each of the polynomials $x^2 + Bx + 1$, $x^2 + Dx + 1$, $x^2 + Fx + 1$ has two distinct roots, C and F, B and E, A and D, respectively.

Tab. 3: Addition and multiplication in $GF(3^2)$

$+$	0	1	2	A	B	C	D	E	F
0	0	1	2	A	B	C	D	E	F
1	1	2	0	B	C	A	E	F	D
2	2	0	1	C	A	B	F	D	E
A	A	B	C	D	E	F	0	1	2
B	B	C	A	E	F	D	1	2	0
C	C	A	B	F	D	E	2	0	1
D	D	E	F	0	1	2	A	B	C
E	E	F	D	1	2	0	B	C	A
F	F	D	E	2	0	1	C	A	B

$\cdot$	0	1	2	A	B	C	D	E	F
0	0	0	0	0	0	0	0	0	0
1	0	1	2	A	B	C	D	E	F
2	0	2	1	D	F	E	A	C	B
A	0	A	D	2	C	F	1	B	E
B	0	B	F	C	D	1	E	2	A
C	0	C	E	F	1	A	B	D	2
D	0	D	A	1	E	B	2	F	C
E	0	E	C	B	2	D	F	A	1
F	0	F	B	E	A	2	C	1	D

Similarly, consider $GF(3^2)$ with elements 0, 1, 2, $A = \alpha$, $B = \alpha + 1$, $C = \alpha + 2$, $D = 2\alpha$, $E = 2\alpha + 1$, $F = 2\alpha + 2$, where $\alpha \notin GF(3)$, $\alpha^2 = 2$ (see Table 3) Now, polynomials $x^2 + Bx + 1$, $x^2 + Cx + 1$, $x^2 + Ex + 1$, $x^2 + Fx + 1$ are irreducible. The polynomials $x^2 + x + 1$ and $x^2 + 2x + 1$ have double roots 1 and 2, respectively. Each of the polynomials $x^2 + 1$, $x^2 + Ax + 1$, $x^2 + Dx + 1$ has two distinct roots A and D, B and C, E and F, respectively.

Proposition 2.6. *In* $\mathfrak{R}(F)$ *every left zero divisor is also a right zero divisor and vice versa.*

Proof. An element $a+bi+cj+dk$ is a left zero divisor if there exists nonzero $p+qi+rj+sk \in \mathfrak{R}(F)$ such that $(a+bi+cj+dk)(p+qi+rj+sk)=0$. Then, by (2.2), the equations

$$\left\{\begin{array}{rcl} ap-(b+tc+t^2d)q-(c+td+t^2b)r-(d+tb+t^2c)s &=& 0,\\ bp+(a-tb-td)q-(d+tb)r+cs &=& 0,\\ cp+dq+(a-tb-tc)r-(b+tc)s &=& 0,\\ dp-(c+td)q+br+(a-tc-td)s &=& 0 \end{array}\right. \tag{2.3}$$

must have a nonzero solution (p,q,r,s). Therefore the determinant of the main matrix must be equal to 0. Analogously, $a+bi+cj+dk$ is a right zero divisor if there exists nonzero $p+qi+rj+sk \in \mathfrak{R}(F)$ such that $(p+qi+rj+sk)(a+bi+cj+dk)=0$. Now, the equations

$$\left\{\begin{array}{rcl} pa-q(b+td+t^2c)-r(c+tb+t^2d)-s(d+tc+t^2b) &=& 0,\\ pb+q(a-tb-tc)+rd-s(c+tb) &=& 0,\\ pc-q(d+tc)+r(a-tc-td)+sb &=& 0,\\ pd+qc-r(b+td)+s(a-tb-td) &=& 0 \end{array}\right. \tag{2.4}$$

must have a nonzero solution (p,q,r,s), i.e. the determinant of their main matrix must be equal to 0.

But the both determinants (of (2.3) and of (2.4)) have the same value:

$$\begin{vmatrix} a & -[b+t(c+td)] & -[c+t(d+tb)] & -[d+t(b+tc)] \\ b & a-t(b+d) & -(d+tb) & c \\ c & d & a-t(b+c) & -(b+tc) \\ d & -(c+td) & b & a-t(c+d) \end{vmatrix} =$$

$$= \begin{vmatrix} a & -[b+t(d+tc)] & -[c+t(b+td)] & -[d+t(c+tb)] \\ b & a-t(b+c) & d & -(c+tb) \\ c & -(d+tc) & a-t(c+d) & b \\ d & c & -(b+td) & a-t(b+d) \end{vmatrix}.$$

. □

Theorem 2.7. *An element $a+bi+cj+dk$ is a zero divisor if and only if*

$$a^2-ta(b+c+d)+(b+c+d)^2+(t^2+t-2)(bc+bd+cd)=0.$$

The set of solutions $p+qi+rj+sk$ of the equations (2.3) *constitute the right annihilator of an element $a+bi+cj+dk$.*

Proof. We simply have to calculate the determinant of (2.3) as follows:

$$\begin{vmatrix} a & -[b+t(c+td)] & -[c+t(d+tb)] & -[d+t(b+tc)] \\ b & a-t(b+d) & -(d+tb) & c \\ c & d & a-t(b+c) & -(b+tc) \\ d & -(c+td) & b & a-t(c+d) \end{vmatrix} =$$

$$= a \cdot \begin{vmatrix} a-t(b+d) & -(d+tb) & c \\ d & a-t(b+c) & -(b+tc) \\ -(c+td) & b & a-t(c+d) \end{vmatrix} +$$

$$+[b+t(c+td)] \cdot \begin{vmatrix} b & -(d+tb) & c \\ c & a-t(b+c) & -(b+tc) \\ d & b & a-t(c+d) \end{vmatrix} +$$

$$-[c+t(d+tb)] \cdot \begin{vmatrix} b & a-t(b+d) & c \\ c & d & -(b+tc) \\ d & -(c+td) & a-t(c+d) \end{vmatrix} +$$

$$+[d+t(b+tc)] \cdot \begin{vmatrix} b & a-t(b+d) & -(d+tb) \\ c & d & a-t(b+c) \\ d & -(c+td) & b \end{vmatrix} =$$

$$\begin{array}{r}
= a \cdot \{[a-t(b+d)][a-t(b+c)][a-t(c+d)] + bcd + \\
-(c+td)(d+tb)(b+tc) + (c+td)[a-t(b+c)]c + \\
+b(b+tc)[a-t(b+d)] + [a-t(c+d)](d+tb)d\} + \\
+[b+t(c+td)] \cdot \{b[a-t(b+c)][a-t(c+d)] + c^2b + \\
+d(d+tb)(b+tc) - c[a-t(b+c)]d + b^2(b+tc) + \\
+[a-t(c+d)]c(d+tb)\} - [c+t(d+tb)] \cdot \{bd[a-t(c+d)] + \\
-c^2(c+td) - d[a-t(b+d)](b+tc) - cd^2 - (b+tc)(c+td)b + \\
-[a-t(c+d)]c[a-t(b+d)]\} + [d+t(b+tc)] \cdot \{b^2d + \\
+c(c+td)(d+tb) + d[a-t(b+d)][a-t(b+c)] + \\
+d^2(d+tb) + [a-t(b+c)](c+td)b - bc[a-t(b+d)]\} = \\
= a \cdot \{a^3 + ac^2 + ab^2 + ad^2 - t[2a^2(b+c+d) - a(bc+bd+cd) + \\
+c^2d + b^2c + bd^2 + bc^2 + c^3 + b^3 + b^2d + cd^2 + d^3] + \\
+t^2[3a(bc+bd+cd) + a(b^2+c^2+d^2) - (c^2b + cd^2 + b^2d + c^2d + \\
+b^2c + bd^2 + 3bcd)] - t^3[b^2c + bc^2 + c^2d + b^2d + bd^2 + cd^2 + 3bcd]\} + \\
+[b+t(c+td)] \cdot \{a^2b + c^2b + d^2b + b^3 + t[-ab(b+c+d) + \\
+b^2d + bcd + b^2c] + t^2[b^2c + b^2d + bcd]\} - [c+t(d+tb)]\{-c^3 - cd^2 + \\
-b^2c - a^2c + t[ac(b+c+d) - (bcd + c^2d + bc^2)] - t^2[bc^2 + c^2d + bcd]\} + \\
+[d+t(b+tc)]\{b^2d + c^2d + a^2d + d^3 + t[-ad(b+c+d) + \\
+cd^2 + bd^2 + bcd] + t^2[bcd + bd^2 + cd^2]\} =
\end{array}$$

$$\begin{aligned}
&= a^4 + a^2(b^2+c^2+d^2) - t[2a^3(b+c+d) - a^2(bc+bd+cd)+ \\
&+a(b+c+d)(b^2+c^2+d^2)] + t^2[3a^2(bc+bd+cd) + a^2(b^2+c^2+d^2)- \\
&-a(bc+bd+cd)(b+c+d)] - t^3a(bc+bd+cd)(b+c+d)+ \\
&+[b+t(c+td)]b\cdot\{a^2+b^2+c^2+d^2+t[-a(b+c+d)+bc+bd+cd]+ \\
&+t^2(bc+bd+cd)\} - [c+t(d+tb)]c\cdot\{-c^2-d^2- \\
&-b^2-a^2+t[a(b+c+d)-(bd+cd+bc)]-t^2[bc+cd+bd]\}+ \\
&+[d+t(b+tc)]d\cdot\{b^2+c^2+a^2+d^2+t[-a(b+c+d)+ \\
&+cd+bd+bc]+t^2[bc+bd+cd]\} = \\
&= a^4 - 2ta^3(b+c+d) + (t+3t^2)a^2(bc+bd+cd)- \\
&-(t^2+t^3)a(bc+bd+cd)(b+c+d)+ \\
&+[a^2-ta(b+c+d)+t^2a^2](b^2+c^2+d^2)+ \\
&+[b^2+c^2+d^2+(t+t^2)(bc+bd+cd)][a^2+b^2+c^2+d^2-ta(b+c+d)+ \\
&+(t+t^2)(bc+bd+cd)] = \\
&= a^4 - 2ta^3(b+c+d) + (t+3t^2)a^2(bc+bd+cd)- \\
&-(t^2+t^3)a(bc+bd+cd)(b+c+d)+ \\
&+[a^2-ta(b+c+d)+t^2a^2][(b+c+d)^2-2(bc+bd+cd)]+ \\
&+[(b+c+d)^2+(t+t^2-2)(bc+bd+cd)][a^2+(b+c+d)^2- \\
&-ta(b+c+d)+(t^2+t-2)(bc+bd+cd)] = \\
&= a^4 - 2ta^3(b+c+d) + (t+3t^2)a^2(bc+bd+cd)- \\
&-(t^2+t^3)a(bc+bd+cd)(b+c+d)+ \\
&+a^2(b+c+d)^2 - ta(b+c+d)^3 + t^2a^2(b+c+d)^2- \\
&-2a^2(bc+bd+cd) + 2ta(b+c+d)(bc+bd+cd)- \\
&-2t^2a^2(bc+bd+cd) + (b+c+d)^2a^2 + (b+c+d)^4- \\
&-ta(b+c+d)^3 + (t^2+t-2)(bc+bd+cd)(b+c+d)^2+ \\
&+(t+t^2-2)(bc+bd+cd)a^2 + (t+t^2-2)(bc+bd+cd)(b+c+d)^2- \\
&-(t+t^2-2)(bc+bd+cd)ta(b+c+d+[(t^2+t-2)(bc+bd+cd)]^2 = \\
&= a^4 + t^2a^2(b+c+d)^2 + (b+c+d)^4 + [(t^2+t-2)(bc+bd+cd)]^2- \\
&-2ta^3(b+c+d) + 2a^2(b+c+d)^2 + 2a^2(t^2+t-2)(bc+bd+cd)- \\
&-2ta(b+c+d)^3 - 2ta(b+c+d)(t^2+t-2)(bc+bd+cd)+ \\
&+2(t^2+t-2)(bc+bd+cd)(b+c+d)^2 = \\
&= [a^2 - ta(b+c+d) + (b+c+d)^2 + (t^2+t-2)(bc+bd+cd)]^2.
\end{aligned}$$

The last part of the Theorem follows from the definition of annihilator. □

Corollary 2.8. *a) Let* $t = 1$ *or* $bc+bd+cd = 0$*. Then* $a+bi+cj+dk$ *is a zero divisor iff* $a^2 - ta(b+c+d) + (b+c+d)^2 = 0$*. If it is the case then* $a = 0 \Leftrightarrow b+c+d = 0$*.*

b) *Let $t \neq 1$ and $b + c + d = 0$. Then $a + bi + cj + dk$ is a zero divisor iff* $a^2 + (t^2 + t - 2)(bc + bd + cd) = 0$.
If it is the case then: $a = 0 \Leftrightarrow bc + bd + cd = 0$; for $a \neq 0$ the element $(t^2 + t - 2)(b^2 + c^2 + bc)$ *must be a square.*

c) *If $b + c + d = 0$ and $bc + bd + cd = 0$, then $bc = d^2$, $bd = c^2$, $cd = b^2$. Hence $b^3 = c^3 = d^3$ and either $b, c, d \in S$ or $b, c, d \notin S$. Every element $z = bi + cj + dk$ satisfying the both assumptions is a nilpotent, i.e. $z^2 = 0$* (see *Corollary* 2.3).

d) *Let $t = -1$ and* $\operatorname{char} F \neq 2$. *Then $a + bi + cj + dk$ is a zero divisor iff* $a^2 + b^2 + c^2 + d^2 + a(b + c + d) = 0$.
If it is the case and $a = 0$ then $b + c + d = 0 \Leftrightarrow bc + bd + cd = 0$. Hence every element $z = bi + cj + dk$ satisfying the condition $b + c + d = 0$ is a nilpotent.

Remark 2.9. *Note that the possibility $b = c = d \neq 0$ is excluded if* $\operatorname{char} F \neq 3$ *and $b+c+d = 0 \vee bc+bd+cd = 0$. Otherwise $b+c+d = 3b = 0$ or $bc+bd+cd = 3b^2 = 0$, and zero divisors would exist in the field.*

Remark 2.10. *If $bc + bd + cd = 0$, then either one of elements b, c, d is arbitrary and the remaining two are equal to* 0, *or $b + c \neq 0$, $b + d \neq 0$, and $c + d \neq 0$.*

Although $\mathfrak{R}(F)$ may be infinite (e.g. if F is the field of rational functions over $GF(2)$), the following condition holds.

Proposition 2.11. *An element in $\mathfrak{R}(F)$ is invertible if and only if it is not a zero divisor.*

Proof. A nonzero element $a+bi+cj+dk$ is invertible if there exists $p+qi+rj+sk \in \mathfrak{R}(F)$ such that $(a + bi + cj + dk)(p + qi + rj + sk) = 1$. Equivalently, we have obtained the equations like (2.3) with a unique difference: in the 1-st equation on the right side there is 1 instead of 0. But this time we have Cramer equations, so the determinant is different from zero. Summarizing, $a + bi + cj + dk$ is invertible (resp. a zero divisor) if the determinant of the main matrix of (2.3) is different from (resp. equal to) zero. □

The following Remark 2.12 and Lemma 2.13 will be used in further study.

Remark 2.12. *In every field F $x^2 - txy + y^2 = 0 \Rightarrow (x = 0 \Leftrightarrow y = 0)$.*

Lemma 2.13. *Let* $\operatorname{char} F > 2$. *Then:*

a) *There exists a nonzero solution (x, y) of the equation $x^2 - txy + y^2 = 0$ over F if and only if $t^2 - 2^2$ is a square in F.*

b) If $t^2 - 2^2 = \alpha^2$ for some $0 \neq \alpha \in F$, then for every $x \neq 0$ there exist exactly two y-s such that $x^2 - txy + y^2 = 0$: $y_1 = 2^{-1}(\alpha + t)x$ and $y_2 = 2^{-1}(-\alpha + t)x$. Then $y_2 = -y_1 + tx$, $y_1 \neq y_2$, and $y_1 \neq x \neq y_2$.

Proof. Ad. a) Because of Remark 2.12, the values x and y are different from 0 since we seek nonzero solutions (x, y). Dividing the equation by y^2, we have

$$\left(\frac{x}{y}\right)^2 - t \cdot \frac{x}{y} + 1 = 0 \quad \text{or equivalently} \quad \left[2\left(\frac{x}{y} - 2^{-1}t\right)\right]^2 = t^2 - 2^2.$$

The left side of the last equation is a square and so must be the right one, if the equation has a solution $\frac{x}{y}$.

Ad. b) The equation $x^2 - txy + y^2 = 0$ may be written as

$$\left(y - \frac{tx}{2}\right)^2 = (t^2 - 2^2)\left(\frac{x}{2}\right)^2. \quad \text{Hence} \quad y_1 = \frac{(\alpha + t)x}{2}, \quad y_2 = \frac{(-\alpha + t)x}{2}.$$

The conditions $y_2 = -y_1 + tx$ and $y_1 \neq y_2$ are obvious. If e.g. $y_1 = x$ then $2x = (\alpha + t)x$, whence $\alpha^2 = t^2 - 2^2 = (2 - t)^2$, $t = 2$ and $\alpha = 0$, a contradiction. □

Corollary 2.14. *Assume that* $\operatorname{char} F > 2$, $t^2 - 2^2 = \alpha^2$ *for some* $\alpha \in F$, $b, c, d \in F$, $x = b + c + d \neq 0$, *and let* $a = \frac{(\alpha+t)x}{2}$ *or* $a = \frac{(-\alpha+t)x}{2}$. *If* $t = 1$ *or* $bc + bd + cd = 0$, *then* $a + bi + cj + dk$ *is a zero divisor which is not a nilpotent.*

Proof. It suffices to put $x = b + c + d$ in Lemma 2.13 b) and then use Corollary 2.8 a), where $y = a$. □

The following proposition generalizes Corollary 2.14.

Proposition 2.15. *Let* $\operatorname{char} F > 2$ *and* $b, c, d \in F$ *are chosen so as*

$$(t^2 - 2^2)(b + c + d)^2 - 2^2(t^2 + t - 2)(bc + bd + cd) = \alpha^2 \in S \cup \{0\}$$

for some $\alpha \in F$. *Then* $a + bi + cj + dk$ *is a zero divisor in* $\mathfrak{R}(F)$ *iff* $a = 2^{-1}[t(b + c + d) \pm \alpha]$.

Proof. We use the same method as in Lemma 2.13. Because of Theorem 2.7, $a + bi + cj + dk$ is a zero divisor iff

$$a^2 - ta(b + c + d) + (b + c + d)^2 + (t^2 + t - 2)(bc + bd + cd) = 0.$$

Hence

$$2^2[a - 2^{-1}t(b + c + d)]^2 = (t^2 - 2^2)(b + c + d)^2 - 2^2(t^2 + t - 2)(bc + bd + cd),$$

i.e.

$$2^2[a - 2^{-1}t(b + c + d)]^2 = \alpha^2$$

and we get

$$a = 2^{-1}[t(b + c + d) \pm \alpha].$$

□

Corollary 2.16. *If* $\operatorname{char} F > 2$*,* $b, c, d \in F$ *and*

$$(t^2 - 2^2)(b+c+d)^2 - 2^2(t^2+t-2)(bc+bd+cd)$$

is not a square in F*, then, for every* $a \in F$*,* $a+bi+cj+dk$ *is not a zero divisor in* $\mathfrak{R}(F)$*.*

Example 2.17. Let us consider $\mathfrak{R}(GF(7))$ and take $t = 3$ (see Example 2.5). Then $S = \{1,\ 4,\ 2\}$ and

$$\begin{aligned}\beta = (t^2 - 2^2)(b+c+d)^2 - 2^2(t^2+t-2)(bc+bd+cd) =\\ = 5 \cdot [(b+c+d)^2 - (bc+(b+c)d)].\end{aligned}$$

Let us fix $b = 2$, $c \in \{3, 4, 5\}$, and in accordance with Proposition 2.15 and Corollary 2.16, select all $d, a \in F$, such that $a+bi+cj+dk$ is a zero divisor. If $\beta \in S$ then $\beta = \alpha^2$ and we can determine the two values of a. We have got the results in Table 4.

We see in Table 4 that the set of zero divisors satisfying all conditions listed in Corollary 2.8 c) is not empty ($b = 2$, $c = 4$, $d = 1$). Yet, Corollary 2.8 c) also implies that $z = bi + cj + dk$ is a nilpotent either for $\{b, c, d\} = \{1, 2, 4\}$ or for $\{b, c, d\} = \{6, 5, 3\}$. One can easily find the annihilator of such an element. Taking e.g. $b = 1$, $c = 2$, $d = 4$, we get $(i + 2j + 4k) \cdot [(5r + s) + (5r + 3s)i + rj + sk] = 0$ for every $r, s \in GF(7)$. Note that there exist other nilpotents. It suffices to take $a = 1$, $\{b, c, d\} = \{0, 1, 2\}$, and using Corollary 2.3 a), we obtain

$$\begin{aligned}(a+bi+cj+dk)^2 =\\ = \{1^2 - [(0+1+2)^2 + (3^2+3-2)(0\cdot 1 + 0\cdot 2 + 1\cdot 2)]\}+\\ +[2\cdot 1 - 3(0+1+2)](bi+cj+dk) =\\ = \{1 - [2 + 3\cdot 2]\} + [2 - 3\cdot 3](bi+cj+dk) = 0.\end{aligned}$$

Example 2.18. Consider $\mathfrak{R}(GF(3^2))$ (cf. Example 2.5 and Remark 2.9). Then the polynomial $x^2 + tx + 1$ is irreducible exactly for $0 \neq t \notin S$. Since $B^2 - 2^2 \notin S$, $C^2 - 2^2 \notin S$, $E^2 - 2^2 \notin S$, and $F^2 - 2^2 \notin S$, every element $a+bi+cj+dk$, such that $bc+bd+cd = 0$ and $b+c+d \neq 0$ is invertible (*see* Corollary 2.16). Since $\operatorname{char} F = 3$, for every $b \in GF(3^2)$ we have $b+b+b = 0$ and $bb+bb+bb = 0$. Hence every element $bi + bj + bk$ is a zero divisor. There exist many zero divisors $a + bi + cj + dk$ for which $bc + bd + cd \neq 0$. Like in Example 2.17, put e.g. $b = A$, $c = B = t$. Then

$$\begin{aligned}\beta = (B^2 - 2^2)(A+B+d)^2 - 2^2(B^2+B-2)(AB+Ad+Bd) =\\ = F\cdot(E+d)^2 - (1-2)\cdot[C + (A+B)d] = F\cdot(E+d)^2 + C + Ed\end{aligned}$$

and β is a square for $d \in \{0,\ 2,\ B,\ C,\ D,\ E\}$ as it has been shown in Table 5. Because of Corollary 2.16, elements $a+Ai+Bj+k$, $a+Ai+Bj+Ak$, $a+Ai+Bj+Fk$

Tab. 4: Zero divisors for $c \in \{3, 4, 5\}$ in Example 2.17

$c = 3$						
d	$(b+c+d)^2$	$bc+(b+c)d$	β	α	a_1	a_2
0	4	6	4	2	5	3
1	1	4	$6 \notin S \cup \{0\}$			
2	0	2	4	2	1	6
3	1	0	$5 \notin S \cup \{0\}$			
4	4	5	2	4	5	1
5	2	3	2	4	3	6
6	2	1	$5 \notin S \cup \{0\}$			

$c = 4$						
d	$(b+c+d)^2$	$bc+(b+c)d$	β	α	a_1	a_2
0	1	1	0	0	2	2
1	0	0	0	0	0	0
2	1	6	$3 \notin S \cup \{0\}$			
3	4	5	2	4	5	1
4	2	4	4	2	2	0
5	2	3	2	4	1	4
6	4	2	$3 \notin S \cup \{0\}$			

$c = 5$						
d	$(b+c+d)^2$	$bc+(b+c)d$	β	α	a_1	a_2
0	0	3	$6 \notin S \cup \{0\}$			
1	1	3	4	2	6	4
2	4	3	$5 \notin S \cup \{0\}$			
3	2	3	2	4	3	6
4	2	3	2	4	1	4
5	4	3	$5 \notin S \cup \{0\}$			
6	1	3	4	2	3	1

are invertible for every $a \in GF(3^2)$.

Tab. 5: β for $b = A$, $c = B = t$ in Example 2.18

d	0	1	2	A	B	C	D	E	F
β	0	$C \notin S$	D	$C \notin S$	A	2	A	A	$E \notin S$
α	0		B		C	A	C	C	
$-\alpha$	0		F		E	A	E	E	

It is obvious that all our consideration becomes simpler if the last component of $a^2 - ta(b+c+d) + (b+c+d)^2 + (t^2+t-2)(bc+bd+cd)$ disappears. In particular, the number of all zero divisors, idempotents and nilpotents may be evaluated more or less precisely. The case $t^2+t-2=0$ (i.e. $t=1$) is very simple. We have no additional restriction in the fields where x^2+x+1 is irreducible, and we take it to construct the ring. Similarly, cases $t=0$, $\operatorname{char} F=2$ are easy to investigate. Yet the condition $bc+bd+cd=0$ implies additional restrictions.

3. Special case $bc+bd+cd=0$

Theorem 3.1. *Let* $\operatorname{char} F>2$, $|F|=q$ *(*$|F|$ *denotes cardinality of* F*), and consider zero divisors* $a+bi+cj+dk\in\mathfrak{R}(F)$ *satisfying the condition* $bc+bd+cd=0$ *in* F*. Then:*

1. *If* $\operatorname{char} F=3$ *then there exist at least* $q-1$ *proper nilpotents;*
2. *If* $\operatorname{char} F>3$ *then there exist exactly* $2(q-1)$ *proper nilpotents if* $-3\in S$ *and there is no proper nilpotent if* $-3\notin S$*;*
3. *If* $t^2-2^2\notin S$ *then all zero divisors in* $\mathfrak{R}(F)$ *are nilpotents;*
4. *If* $t^2-2^2\in S$ *and* $\operatorname{char} F>3$*, then there exist at least* $4(q-1)$ *zero divisors which are not nilpotents.*

Proof. The expression $a^2-ta(b+c+d)+(b+c+d)^2$ used in Proposition 2.7 may be written as $x^2-txy+y^2$, where $x=a$, $y=b+c+d$.

Assume that $x=a=0$, $y=b+c+d=0$ (see Remark 2.12). By the assumption $bc+bd+cd=0$ and Remark 2.10, we obtain $c\neq -b\neq d$ for $b\neq 0$, and

$$d=-(b+c)=-\frac{bc}{b+c},\quad \text{i.e.}\quad b^2+bc+c^2=0.$$

If $\operatorname{char} F=3$ then every pair (b,c) with $b=c\neq 0$ satisfies the latter equation, whence every element $bi+bj-2bk$ is a nilpotent (see Corollary 2.8 c)), which ends the proof of item *1*.

If $\operatorname{char} F>3$, then by Lemma 2.13 a) with $x=c$, $y=b$, $t=-1$, this equation has nonzero solutions if -3 is a square in F. Let $u\in F$ be an element such that $u^2=-3$. Because of Lemma 2.13 b), for every $c\neq 0$ there exist exactly two distinct values of b and then the values of $d=-(b+c)$ are uniquely determined: $b_1=2^{-1}c(u-1)=d_2$, $b_2=-2^{-1}c(u+1)=d_1$. If $c=0$ then $d=-b$, a contradiction. Therefore we have got exactly $2(q-1)+1$ quadruples (a,b,c,d) (together with $(0,0,0,0)$), satisfying the conditions $a=0$, $b+c+d=0$. By Corollary 2.3 c), such elements and only such elements are nilpotents. Thus item *2* is proved.

If t^2-2^2 is not a square in F then the equation $x^2-txy+y^2=0$ has only zero solution (see Lemma 2.13 a)): $x=a=0$ and $y=b+c+d=0$. The assumption $bc+bd+cd=0$ and Corollary 2.8 c) imply that all such elements are nilpotents. So item *3* is proved.

Now let $t^2 - 2^2$ be a square in F. Then the equation $x^2 - txy + y^2 = 0$ has also nonzero solutions. Using Lemma 2.13 b), we know that for every nonzero $a = x \in F$, there exist exactly two nonzero y-s such that $x^2 - txy + y^2 = 0$: for $t^2 - 2^2 = \beta^2$ we obtain $y_1 = 2^{-1}a(t + \beta)$, $y_2 = 2^{-1}a(t - \beta)$. If one of two y-s is fixed, then we put $y = b + c + d$. But we have to recall the assumption $bc + bd + cd = 0$. Hence

$$d = y - b - c = -\frac{bc}{b+c}, \quad \text{i.e.} \quad c^2 + (b - y)(b + c) = 0,$$

$$\text{or, equivalently,} \quad \left[2 \cdot \left(c + 2^{-1}(b - y)\right)\right]^2 = -3b^2 + 2by + y^2.$$

Like before, the latter equation has solutions (b, c) if and only if the right side is a square in F. It depends on the kind of the field for which relations between b and y is $-3b^2 + 2by + y^2 \in S \cup \{0\}$. Yet for every field F, if $y = b \vee y = -3b$; then $-3b^2 + 2by + y^2 = 0$. For $b = y$ Remark 2.10 yields $c = d = 0$. If $b = (-3^{-1})y$ then $0 = c + 2^{-1}(b - y)$, whence $c = -2^{-1}(b - y) = -2^{-1}(-3^{-1}y - y) = 2 \cdot 3^{-1}y$, and $d = y - b - c = y + 3^{-1}y - 2 \cdot 3^{-1}y = 2 \cdot 3^{-1}y$. Summarizing, for every $a \neq 0$ the following elements are zero divisors and they are not nilpotents:

$$a[1 + 2^{-1}(t + \beta)i], \quad a[1 + 2^{-1}(t - \beta)i],$$
$$a\{1 + 2^{-1}3^{-1}(t + \beta)(-i + 2j + 2k)\},$$
$$a\{1 + 2^{-1}3^{-1}(t - \beta)](-i + 2j + 2k)\}.$$

This ends the proof of item *4*. □

Corollary 3.2. *If there exist $y, b, c, d \in F$ such that $y = b+c+d$ and $bc+bd+cd = 0$, then $-3b^2 + 2by + y^2 = (c - d)^2$.*

Proposition 3.3. *Let $bc + bd + cd = 0$, where $0 \notin \{b, c, d\}$. Then $a + bi + cj + dk$ is an idempotent if and only if*

$$t^2 - 2^2 \in S, \text{ and } t(b + c)^2 - (2a - 1)(b + c) - tbc = 0.$$

Proof. Let $(a + bi + cj + dk)^2 = a + bi + cj + dk$. By Corollary 2.3 we have

$$\begin{cases} a^2 - (b + c + d)^2 = a, \\ 2a - t(b + c + d) = 1. \end{cases} \tag{3.1}$$

Hence

$$\left[2(a - 2^{-1})\right]^2 = t^2(t^2 - 2^2)^{-1}.$$

The left side is a square and so must be the right one if the equation has a solution a. From the latter equation of (3.1) we have the value $b + c + d = \frac{2a-1}{t}$, i.e. $d = -b - c + \frac{2a-1}{t}$.

By the assumptions $bc+bd+cd=0$, $0\notin\{b,c,d\}$ and Remark 2.10, we obtain $d=-\frac{bc}{b+c}$. Hence we have got the equality

$$t(b+c)^2-(2a-1)(b+c)-tbc=0.$$

Now, assume that $t(b+c)^2-(2a-1)(b+c)-tbc=0$. By the assumption $bc+bd+cd=0$, for $d\neq 0$ we obtain $b+c=-bcd^{-1}$. Then $bc\neq 0$ and

$$\begin{aligned} t(bc)^2d^{-2}+(2a-1)bcd^{-1}-tbc&=0;\\ tbc+(2a-1)d-td^2&=0;\\ (2a-1)d=t(d^2-bc)&=t(d^2+bd+cd);\\ 2a-1&=t(d+b+c). \end{aligned}$$

The last equality coincides with the latter one of (3.1). It remains to verify that $a^2-(b+c+d)^2=a$. We already have $b+c+d=(2a-1)t^{-1}$. Thus

$$\begin{gathered} a^2-(b+c+d)^2=a\Leftrightarrow a^2-[(2a-1)t^{-1}]^2=a\Leftrightarrow\\ (a^2-a)(t^2-2^2)=1\Leftrightarrow(2a-1)^2=t^2(t^2-2^2)^{-1}. \end{gathered}$$

□

Corollary 3.4. *If $t^2-2^2\in S\subset F$ and $\beta^2=t^2-2^2$, then the following elements are idempotents in $\mathfrak{R}(F)$:*

$$\begin{array}{ccc} \dfrac{t+\beta}{2\beta}+\beta^{-1}i\ ; & \dfrac{-t+\beta}{2\beta}-\beta^{-1}i\ ; & \dfrac{t+\beta}{2\beta}+\beta^{-1}j\ ;\\ \dfrac{-t+\beta}{2\beta}-\beta^{-1}j\ ; & \dfrac{t+\beta}{2\beta}+\beta^{-1}k\ ; & \dfrac{-t+\beta}{2\beta}-\beta^{-1}k\ . \end{array}$$

4. Special cases: $\operatorname{char}F=2$, $t=0$, and $t=1$

Example 4.1. $\mathfrak{R}(GF(2))$ is the smallest ring among $\mathfrak{R}(F)$. Its all invertible elements are presented in Table 6.

One can easily prove that the group of invertible elements contains the following proper subgroups:
3 groups of order 2: $(\{1,1+i+j\},\ \{1,1+i+k\},\ \{1,1+j+k\})$;
4 groups of order 3: $(\{1,i,1+i\},\ \{1,j,1+j\},\ \{1,k,1+k\},\ \{1,i+j+k,1+i+j+k\})$.

Tab. 6: Invertible elements in $\mathfrak{R}(GF(2))$

x	1	i	j	k	$1+i+j$	$1+i+k$	$1+j+k$	$i+j+k$
x^{-1}	1	$1+i$	$1+j$	$1+k$	$1+i+j$	$1+i+k$	$1+j+k$	$1+i+j+k$

There are exactly three proper both-side zero divisors $i+j$, $i+k$, $j+k$, multiplication of which is presented in Table 7.

Tab. 7: Multiplication of zero divisors in $\mathfrak{R}(GF(2))$

$\cdot$	$i+j$	$i+k$	$j+k$
$i+j$	0	0	0
$i+k$	0	0	0
$j+k$	0	0	0

This means that there exists a unique annihilator.

From Proposition 2.7 the following is immediate:

Proposition 4.2. *a) If $t=0$ then $a+bi+cj+dk$ is a zero divisor if and only if $a^2+b^2+c^2+d^2=0$;*

b) If $t=1$ then $a+bi+cj+dk$ is a zero divisor if and only if $a^2-a(b+c+d)+(b+c+d)^2=0$.

Proposition 4.3. *Let $t=1$.*

1. *An element $z=a+bi+cj+dk$ is a nilpotent (i.e. $z^2=0$) in $\mathfrak{R}(F)$ if and only if $a=0$ and $b+c+d=0$;*

2. *An element $z=a+bi+cj+dk$ is a nontrivial idempotent (i.e. $z^2=z$ and $1\neq z\neq 0$) in $\mathfrak{R}(F)$ if and only if the following conditions hold:*

$$3\neq \operatorname{char} F\neq 2, \quad 3a^2-3a+1=0, \quad b+c+d=2a-1.$$

Proof. From Corollary 2.3 **c)** item *1.* is immediate. To prove item *2.* we have to consider $a+bi+cj+dk$ such that $(a+bi+cj+dk)^2=a+bi+cj+dk$. Using Corollary 2.3 **a)** and **b)**, we obtain the following equations:

$$[a^2-(b+c+d)^2]+[2a-(b+c+d)](bi+cj+dk)=a+bi+cj+dk \qquad \text{if}\operatorname{char} F\neq 2;$$

$$[a^2+(b+c+d)^2]+(b+c+d)(bi+cj+dk)=a+bi+cj+dk \qquad \text{if}\operatorname{char} F=2.$$

If $b=c=d=0$, then $a^2=a$, whence $z=0$ or $z=1$. Assume that $(a,b,c)\neq(0,0,0)$. If $\operatorname{char} F=2$ then $b+c+d=1$ and we have $a^2+1=a$, i.e. $a^2+a+1=0$, which contradicts the assumption that the polynomial $x^2+x+1=0$ does not have a root. If $\operatorname{char} F\neq 2$ then $2a-(b+c+d)=1$, whence $a^2-(2a-1)^2=a$, i.e. $1=0$ (a contradiction) for $\operatorname{char} F=3$ and $3a^2-3a+1=0$ for $\operatorname{char} F\neq 3$.

Assume that $3 \neq \operatorname{char} F \neq 2$, $3a^2 - 3a + 1 = 0$ and $b + c + d = 2a - 1$. Then the last condition implies:

$$a^2 - (b + c + d)^2 = a \Leftrightarrow a^2 - (2a - 1)^2 = a \Leftrightarrow 3a^2 - 3a + 1 = 0;$$

$$2a - (b + c + d) = 2a - (2a - 1) = 1.$$

□

Remark 4.4. *The condition $3a^2 - 3a + 1 = 0$ yields $-3 \in S$ since the equation $3x^2 - 3x + 1 = 0$, or equivalently $[2 \cdot (a - 2^{-1})]^2 = (-3)^{-1}$, has a solution.*

Example 4.5. It follows from Proposition 4.3 that proper idempotents exist neither in $\mathfrak{R}(GF(2))$ nor in $\mathfrak{R}(GF(2^3))$ where we take $t = 1$ (see Example 2.5). We already know from Example 4.1 that in $\mathfrak{R}(GF(2))$ all three zero divisors are nilpotents. One can also easily find the number of nilpotents in $\mathfrak{R}(GF(2^3))$. By Corollary 2.3 c), we have to put $a = 0$ and find all b, c, d, such that $b+c+d = 0$, where $(b, c, d) \neq (0, 0, 0)$. We have 7^3 ordered triples (b, c, d) without 0, $3 \cdot 7^2$ triples with one 0, and $3 \cdot 7$ triples with two 0-s. Together there is 511 such triples. Let us try to find in $\mathfrak{R}(GF(2^3))$ zero divisors $a + bi + cj + dk$ which are not nilpotents (by Proposition 4.3 *2.*, idempotents either). Then, by Theorem 2.7 and the assumptions $t = 1$, $\operatorname{char} F = 2$, the following condition holds

$$a^2 + a(b + c + d) + (b + c + d)^2 = 0, \qquad a \neq 0 \neq b + c + d.$$

Denote $b + c + d = y$ and obtain $a^2 + ay + y^2 = 0$, i.e. $(a + y)^2 = ay$. Yet, this equation has no solutions (a, y) in $F(2^3)$. Therefore all zero divisors in $\mathfrak{R}(GF(2^3))$ are nilpotents. If we change the assumption $t = 1$ by $bc + bd + cd = 0$ and $t \in \{A, C, E\}$, then we have to solve the equation $(a + y)^2 = tay$. Yet, for $t \in \{A, C, E\}$ such equation has no solution (a, y) again.

Theorem 4.6. *Let $t = 1$, $\operatorname{char} F > 3$ and $|F| = q$. Then:*

1. *The number of all proper zero divisors in $\mathfrak{R}(F)$ is equal to:*
   - *a) $q^2 - 1$ if -3 is not a square in F. Then all zero divisors are nilpotents;*
   - *b) $2q^3 - q^2 - 1$ (and $q^2 - 1$ nilpotents among them) if -3 is a square in F.*
2. *a) 0 and 1 are the only idempotents in $\mathfrak{R}(F)$ if -3 is not a square in F;*
   - *b) The number of all idempotents in $\mathfrak{R}(F)$ is equal to $2 \cdot q^2 + 2$ if -3 is a square in F.*

Proof. Ad. 1. We have to determine how many quadruples (a, b, c, d) are solutions of the equation $a^2 - a(b + c + d) + (b + c + d)^2 = 0$. As before, we use Lemma 2.13 and Remark 2.12, where $x = a$, $y = b + c + d$.

Assume that $a = 0, \quad b+c+d = 0$. The value d is uniquely determined for every fixed pair b, c. Therefore we have got exactly q^2 quadruples (a, b, c, d) (together with $(0, 0, 0, 0)$) satisfying the conditions $a = 0$, $b + c + d = 0$. By Corollary 2.3 c), such elements and only such elements are nilpotents.

If -3 is not a square in F then the equation $x^2 - xy + y^2 = 0$ has only the solution $(0, 0)$ and there is no other zero divisor.

Now let $-3 \in S$. By Lemma 2.13 b), for every nonzero $a = x \in F$ there exist exactly two nonzero y-s such that $x^2 - xy + y^2 = 0$. If one of two y-s is fixed, then for every pair $(b, c) \in F^2$, the value of d is uniquely determined from the equality $y = b + c + d$. Hence we obtain $(q - 1) \cdot 2 \cdot q^2$ quadruples (a, b, c, d) with $a \neq 0$, $b + c + d \neq 0$. The total number of proper zero divisors in this case is equal to $q^2 - 1 + (q - 1) \cdot 2 \cdot q^2 = 2q^3 - q^2 - 1$.

Ad. 2. Using Corollary 2.3, the condition $(a + bi + cj + dk)^2 = a + bi + cj + dk$ may be written as the following equations in F:

$$\text{(4.1)} \qquad \left\{ \begin{array}{llcl} a^2 & -(b+c+d)^2 & = & a, \\ b & (2a-b-d-c-1) & = & 0, \\ c & (2a-c-b-d-1) & = & 0, \\ d & (2a-d-b-c-1) & = & 0. \end{array} \right.$$

If $b + c + d \neq 2a - 1$ then $b = c = d = 0$, whence $a^2 = a$, i.e. $a = 0$ or $a = 1$. Now we use Proposition 4.3. If $b + c + d = 2a - 1$ and $-3 \in S$ then the equation $3a^2 - 3a + 1 = 0$ (or equivalently $[2 \cdot (a - 2^{-1})]^2 = (-3)^{-1}$) has two distinct solutions. Let $(a - 2^{-1})^2 = v^2 = (-3)^{-1} \cdot 2^{-2}$ for some $v \in F$. Thus $a = 2^{-1} + v$ or $a = 2^{-1} - v$. For each such a and every pair $(b, c) \in F \times F$, the value of d is uniquely determined. Therefore we have got exactly $2q^2$ idempotents different from 0 and 1. □

From Proposition 2.11 and Theorem 4.6 *1.* the following is immediate.

Corollary 4.7. *Let $t = 1$ and $|F| = q$. Then the group of all invertible elements in $\mathfrak{R}(F)$ consists of $q^2(q^2 - 1)$ elements if -3 is not a square in F, and of $q^2(q - 1)^2$ elements if -3 is a square.*

Example 4.8. Assume that $t = 1$. We know from Example 2.5 that $x^2 + x + 1$ is irreducible in $GF(2)$, $GF(5)$ and $GF(11)$. This polynomial is also irreducible in $GF(17)$, $GF(19)$, $GF(23)$, $GF(29)$, ... In $GF(5)$, $GF(11)$, $GF(17)$, $GF(23)$ and $GF(29)$, -3 is not a square (Proposition 1.2 is helpful here). So, in $\mathfrak{R}(GF(5))$, $\mathfrak{R}(GF(11)$, $\mathfrak{R}(GF(17))$, $\mathfrak{R}(GF(23))$, $\mathfrak{R}(GF(29))$ only 1 and 0 are idempotents and total number of zero divisors is equal to 5^2, 11^2, 17^2, 23^2, 29^2, respectively. Now, consider $GF(19)$. This time the subgroup of nonzero squares consists of: 1, 4, 9, 16, 6, 17, 11, 7, 5. Note that $-3 = 16$ is a square. Since $[2(a - 2^{-1})]^2 = (4^{-1})^2$, we obtain $2(a - 10) = 5$ or $2(a - 10) = -5 = 14$, i.e. $a = 3$ or $a = 17$. There exist exactly $2 \cdot 19^2 + 2 = 724$ idempotents, e.g. $3 + 2i + 4j + 18k$ and $17 + 5i + 7j + 2k$ are idempotents. Total number of zero divisors is equal to $2 \cdot 19^3 - 19^2 = 13357$. There exist exactly 361 nilpotents among them. In the same way, one can study $GF(37)$, where $-3 = 34 = 16^2$ is a square.

References

[1] M. Aristidou, A. Demetre, *A note on quaternion rings*, International Journal of Algebra, **3**, no. 15 (2009), 725–728.

[2] J. B. Derr, G. F. Orr. P. S. Peck, *Noncommutative rings of order p^4*, Journal of Pure and Applied Algebra **97** (1994), 109–116.

[3] J. A. Ewell, *A simple proof of Fermat's two squares theorem*, American Mathematical Monthly 90 (1983), 635–637.

[4] J. Jakóbowski *Some examples of denumerable pseudo-ordered fields and their application to geometry*, Demonstratio Mathematica **46**, no. 2 (2013), 247–256.

[5] T. Y. Lam, *A First Course in Noncommutative Rings* Springer–Verlag New York 1991.

[6] S. Lang, *Algebra*, Addison–Wesley Publishing Company, 1970.

[7] C. J. Miguel, R. Serôdio, *On the structure of quaternion rings over Z_p*, International Journal of Algebra **5**, no. 27 (2011), 1313–1325.

[8] R. S. Pierce, *Associative Algebras*, Springer, 1982.

Faculty of Mathematics and Computer Science
University of Warmia and Mazury in Olsztyn
Słoneczna 54, PL-10-710 Olsztyn, Poland
e-mail: jjakob@matman.uwm.edu.pl

Presented by Adam Paszkiewicz at the Session of the Mathematical-Physical Commission of the Łódź Society of Sciences and Arts on March 23, 2017.

PEWNE PIERŚCIENIE NIEPRZEMIENNE KONSTRUOWANE NA PODSTAWIE WIELOMIANÓW $x^2 + tx + 1$ ORAZ ICH DZIELNIKI ZERA

Streszczenie

W pracy konstruujemy pewne rozszerzenie pierścieniowe dla dowolnego ciała Galois $F = GF(p^n)$. Najpierw znajdujemy $t \in F$, takie że wielomian x^2+tx+1 nie ma pierwiastków w F (takie t zawsze istnieją!). Następnie bierzemy 4-wymiarową przestrzeń wektorową nad F z elementami bazowymi 1, i, j, k, gdzie i, j, k nie należą do F i zakładamy, że są one pierwiastkami wielomianu x^2+tx+1 w konstruowanym rozszerzeniu. Ponadto przyjmujemy $ji = -k - t$. Te warunki wystarczają do zdefiniowania mnożenia na elementach bazowych i w konsekwencji w całej algebraicznej strukturze tak, by otrzymać pierścień. Taka konstrukcja jest podobna do konstrukcji Hamiltona kwaternionów rzeczywistych, ale jest ona dużo bardziej ogólna i zastosowana do ciał skończonych. Najpierw w celu samej konstrukcji, a potem do badania własności pierścieni $\mathfrak{R}(F)$, używamy wybranych własności ciał oraz wielomianów $x^2 + tx + 1$.

Wśród otrzymanych wyników, w szczególności podajemy warunek konieczny i dostateczny dla dowolnego elementu z $\mathfrak{R}(F)$, aby był on dzielnikiem zera, w tym nilpotentem lub idempotentem rzędu 2. Rozważono wiele wersji tego warunku w szczególnych przypadkach i opisano przykłady. Zbadano także własności kombinatoryczne. Pewne ważne własności badanych w pracy pierścieni zależą od charakterystyki ciała i od tego, czy pewne elementy są kwadratami w danym ciele. Podsumowując, w pracy skonstruowano szeroką klasę pierścieni nieprzemiennych i zbadano ich wybrane własności. Ta konstrukcja może być zastosowana dla dowolnych ciał (także nieskończonych) o charakterystyce różnej od zera.

Słowa kluczowe: ciało Galois, wielomian, pierścień nieprzemienny, dzielnik zera, przestrzeń wektorowa, skośne ciało kwaternionów