Збірник праць Ін-ту математики НАН України 2013, том 6, N 6, 148–164

Marek Golasiński, Francisco Gómez Ruiz

Spheres over finite rings and their polynomial maps

The paper [8] grew out of our attempt to describe all polynomial self-maps of the real and complex circle as well.

Introduction. The definition of the n-sphere $\mathbb{S}^n$ with $n \geq 0$ over the reals can be extended to arbitrary commutative and unitary rings R which leads to the n-sphere

$$\mathbb{S}^n(R) = \{(r_0, \ldots, r_n) \in R^{n+1};\ r_0^2 + \cdots + r_n^2 = 1\}$$

over R. If R is finite then it is worthwhile to compute its cardinality $\sharp(\mathbb{S}^n(R))$. More generally, if $V(F_q)$ is an affine variety defined over a finite field F_q, we can not only consider the number $\sharp(V(Fq))$, but also $\sharp(V(F_{q^m}))$ for $m \geq 1$. These can be nicely encoded by the Hasse-Weil zeta function of V: $\zeta(V;X) = \exp(\sum_{m=1}^{\infty} \frac{\sharp(V(F_{q^m}))}{m} X^m) \in \mathbb{Q}[[X]]$ which satisfies a number of fundamental properties, known as the Weil conjectures, which are known to be true mainly by the work [6] of Deligne.

Like for $\mathbb{S}^1$, the circle $\mathbb{S}^1(R)$ is equipped in an abelian group structure. Further, $\mathbb{S}^1(-)$ is a functor from commutative and unitary rings into abelian group. In particular, for the field $\mathbb{Q}$ of rational numbers, points of $\mathbb{S}^1(\mathbb{Q})$ are determined by Pythagorean triples and $\mathbb{S}^1(\mathbb{Q})$ is dense in the circle $\mathbb{S}^1$. If R is a finite ring then $\mathbb{S}^1(R)$ is a finite abelian group and it is a natural problem to determine its structure.

In [9], the author considers the group structure in $\mathbb{S}^1(R)$, with R being a commutative and unitary ring, determines this structure in the case when R is either a finite field or the ring $\mathbb{Z}_m$ of integers modulo m, and describes the group structure on conic sections.

In particular, by [9], the group $\mathbb{S}^1(R)$ is cyclic provided R is a field or the ring $\mathbb{Z}_{p^k}$ of integers modulo p^k for a prime odd number p. Further, in

[9, p. 54] the author has stated: *The case $p = 2$ is particularly interesting* (*or nasty, depending on your point of view* [*oder lästig, je nachdem, wie man es sieht*]).

The aim of Section 1 is to simplify proofs of some results from [9], present their generalizations and state in Theorem 2.5:
If p is a prime and $k \geq 1$ then

$$\mathbb{S}^1(\mathbb{Z}_{p^k}) \cong \begin{cases} \mathbb{Z}^+_{p^{k-1}(p-1)}, & if\ p \equiv 1 \,(\mathrm{mod}\, 4); \\ \mathbb{Z}^+_{p^{k-1}(p+1)}, & if\ p \equiv 3 \,(\mathrm{mod}\, 4); \\ \mathbb{Z}^+_2, & if\ \ k = 1; \\ \mathbb{Z}^+_2 \oplus \mathbb{Z}^+_{2^2} \oplus \mathbb{Z}^+_{2^{k-2}}, & if\ \ k \geq 2. \end{cases}$$

The paper [8] grew out of our attempt to describe all polynomial self-maps of the real and complex circle as well. Then, some results from [11, 14, 15] on spheres and their polynomial maps into spheres over any field has been transfered. In virtue of Wood [14] (see also [5, Chapter 13]) a necessary condition for the existence of a non-constant polynomial map $\mathbb{S}^m \to \mathbb{S}^n$ of spheres for $m \geq n$ is that $2^{k+1} > m \geq n \geq 2^k$ for some $k \geq 0$. It was shown in [15] that from the homotopy point of view nothing is lost by complexifying the problem of which homotopy classes of maps of spheres contain a polynomial representative. Furthermore in virtue of [7] any complex polynomial self-map of $\mathbb{S}^2(\mathbb{C})$ yields a regular self-map of the sphere $\mathbb{S}^2$ in a canonical way. Then Loday [11] using algebraic and topological K-theory proved some results on polynomials maps into $\mathbb{S}^n$. For instance, every polynomial map from the torus $\mathbb{T}^n$ to $\mathbb{S}^n$ is null-homotopic if $n > 1$. For n even those results were extended in [3, 4] to regular and then in [5] to polynomial maps $\mathbb{S}^{n_1} \times \cdots \times \mathbb{S}^{n_k} \to \mathbb{S}^n$ with $n = n_1 + \cdots + n_k$ odd. Certainly, polynomial maps $\mathbb{S}^{m_1}(R) \times \cdots \times \mathbb{S}^{m_k}(R) \to \mathbb{T}^n(R)$ are worth to be studied from the algebraic point of view for any field R. We made use of the abelian group structure on the sphere $\mathbb{S}^1(R)$ to show in [8, Corollary 2.11] that for any polynomial self-map $f : \mathbb{S}^1(R) \to \mathbb{S}^1(R)$ there are $\alpha \in \mathbb{S}^1(R)$ and an integer n such that $f(z) = \alpha z^n$ for any $z \in \mathbb{S}^1(R)$ provided the field R is infinite. All polynomial maps $\mathbb{S}^{m_1}(R) \times \cdots \times \mathbb{S}^{m_k}(R) \to \mathbb{T}^n(R)$ are listed in [8] for any infinite field R.

Section 2 takes up the systematic study of spheres $\mathbb{S}^n(R)$ over a finite field R and polynomial maps $\mathbb{S}^{m_1}(R) \times \cdots \times \mathbb{S}^{m_k}(R) \to \mathbb{S}^{n_1}(R) \times \cdots \times \mathbb{S}^{n_l}(R)$ with $m_1, \ldots, m_k, n_1, \ldots, n_l \geq 0$. Theorem 3.2 shows the cardinality $\sharp(\mathbb{S}^n(R))$ of the n-sphere $\mathbb{S}^n(R)$:

If the characteristic $\chi(R) \neq 2$ then for any number $n \geq 1$ it holds:

$$\sharp\mathbb{S}^n(R) = \begin{cases} (\sharp R)^n - (\sharp R)^{\frac{n}{2}}\eta((-1)^{\frac{n}{2}}), & \textit{if } n \textit{ is even;} \\ (\sharp R)^n - (\sharp R)^{\frac{n-1}{2}}\eta((-1)^{\frac{n+1}{2}}) & \textit{if } n \textit{ is odd,} \end{cases}$$

where

$$\eta(1) = 1 \textit{ and } \eta(-1) = \begin{cases} 1, & \textit{if the equation } X^2+1=0 \textit{ has a solution in} R; \\ -1 & \textit{otherwise} \end{cases}$$

and Corollary 3.4 asserts that any such any map $\mathbb{S}^{m_1}(R)\times\cdots\times\mathbb{S}^{m_k}(R) \to \mathbb{S}^{n_1}(R) \times \cdots \times \mathbb{S}^{n_l}(R)$ is a polynomial one.

1. Circles over a finite ring

1. Circles over a finite ring. Let R be a commutative and unitary ring. The set

$$\mathbb{S}^1(R) = \{(r_0, r_1) \in R \times R;\ r_0^2 + r_1^2 = 1\}$$

is called the 1-*sphere* or the *circle* over R.

Observe that on $\mathbb{S}^1(R)$ there is an abelian group structure defined by $(r_0, r_1) \circ (r_0', r_1') = (r_0r_0' - r_1r_1', r_0r_1' + r_1r_0')$ for any points $(r_0, r_1), (r_0', r_1') \in \mathbb{S}^1(R)$. Writing $SO(2, R)$ for the group of special orthogonal 2×2-matrices over R, we may easily show

Remark 2.1. (1) For any commutative and unitary ring R there is an isomorphism of groups

$$\mathbb{S}^1(R) \cong SO(2, R)$$

determined by the assignment $(r_0, r_1) \mapsto \begin{pmatrix} r_0 & r_1 \\ -r_1 & r_0 \end{pmatrix}$ for $(r_0, r_1) \in \mathbb{S}^1(R)$.

(2) If R_1, R_2 are commutative and unitary rings then there is an isomorphism of groups $\mathbb{S}^1(R_1 \times R_2) \cong \mathbb{S}^1(R_1) \times \mathbb{S}^1(R_2)$.

Next, consider the quotient ring $R[i] = R[X]/(X^2+1)$, where i denotes the class of X in $R[X]/(X^2 + 1)$ and write $U(R)$ for the multiplicative group of R. Let $\chi(R)$ denote the characteristic of R. Then, we may state:

Proposition 2.2. *For any unitary ring R there is a group monomorphism $\mathbb{S}^1(R) \to U(R[i])$. Further:*

(1) *if* $\chi(R) = 2$ *then* $\mathbb{S}^1(R) = \{(1 + r + s, r);\ r, s \in R \,\text{with}\, s^2 = 0\}$ *and there is a splitting short exact sequence*

$$0 \to R^+ \to \mathbb{S}^1(R) \to \tilde{R} \to 1,$$

where R^+ *is the additive group of* R *and the group* $\tilde{R} = \{s \in R; s^2 = 0\}$ *with* $s_1 \circ s_2 = s_1 + s_2 + s_1 s_2$ *for* $s_1, s_2 \in \tilde{R}$*;*

(2) *if* $i \in R$ *with* $i^2 = -1$ *then there is an exact sequence of abelian groups*

$$0 \to R_0 \to \mathbb{S}^1(R) \to U(R),$$

where $R_0 = \{r \in R;\ 2r = 0\}$*;*

(i) *if* $2 \in U(R)$ *then there a group isomorphism*

$$\mathbb{S}^1(R) \xrightarrow{\cong} U(R);$$

(ii) *if* $\chi(R) = 2$ *then there is a splitting short exact sequence*

$$0 \to R \to \mathbb{S}^1(R) \to R_1 \to 1,$$

where $R_1 = \{r \in R;\ r^2 = 1\}$*;*

(3) *if* $i \notin R$ *then there is an exact sequence*

$$1 \to \mathbb{S}^1(R) \to U(R[i]) \xrightarrow{\rho} U(R)$$

of abelian groups, where $\rho(r_0 + r_1 i) = r_0^2 + r_1^2$ *for* $r_0 + r_1 i \in U(R[i])$*. Further, if* R *is a finite field then* $U(R[i]) \xrightarrow{\rho} U(R)$ *is onto.*

Proof. Certainly, the map $\varphi : \mathbb{S}^1(R) \to U(R[i])$ given by $\varphi(r_0, r_1) = r_0 + r_1 i$ for $(r_0, r_1) \in \mathbb{S}^1(R)$ is a group monomorphism.

(1) Let $\chi(R) = 2$. If $r, s \in R$ with $s^2 = 0$ then $(1 + r + s, r) \in \mathbb{S}^1(R)$. Conversely, if $(r_0, r_1) \in \mathbb{S}^1(R)$ then $r_0 = 1 + r_1 + (1 + r_0 + r_1)$ and $(1 + r_0 + r_1)^2 = 0$. Hence, $\mathbb{S}^1(R) = \{(1 + r + s, r);\ r, s \in R \,\text{with}\, s^2 = 0\}$. Further, one can easily see that the map $\phi : R^+ \to \mathbb{S}^1(R)$ given by $\phi(r) = (1 + r, r)$ for $r \in R$ is a group monomorphism. Write $\tilde{R} = \{s \in R; s^2 = 0\}$ and $s_1 \circ s_2 = s_1 + s_2 + s_1 s_2$ for $s_1, s_2 \in \tilde{R}$. Then, $(\tilde{R}, \circ)$ is an abelian group and the map $\rho : \mathbb{S}^1(R) \to \tilde{R}$ given by $\rho(1 + r + s, r) = s$ for $(1 + r + s, r) \in \mathbb{S}^1(R)$ is an epimorphism. The sequence

$$0 \to R^+ \xrightarrow{\phi} \mathbb{S}^1(R) \xrightarrow{\rho} \tilde{R} \to 0$$

is exact and the map $\rho' : \tilde{R} \to \mathbb{S}^1(R)$ given by $\rho'(s) = (1 + s, 0)$ for $s \in \tilde{R}$ determines its splitting.

(2) Write $R_0 = \{r \in R;\, 2r = 0\}$. Then, the maps

$$\alpha : R_0 \to \mathbb{S}^1(R) \ \text{ and } \ \varphi : \mathbb{S}^1(R) \to U(R)$$

given by $\alpha(r) = (1+r, r)$ for $r \in R_0$ and $\varphi(r_0, r_1) = r_0 + r_1 i$ for $(r_0, r_1) \in \mathbb{S}^1(R)$ are group homomorphisms with $\operatorname{Ker}\alpha = \{0\}$ and $\operatorname{Im}\alpha = \operatorname{Ker}\varphi$. Notice that $r \in U(R)$ with $r + r^{-1} = 2s$ for some $s \in R$ implies $(s, -(r-s)i) \in \mathbb{S}^1(R)$ and $\varphi(s, -(r-s)i) = r$. Consequently,

$$\operatorname{Im}\varphi = \{r \in U(R);\, r + r^{-1} \in 2R\}.$$

(i) If $2 \in U(R)$ then $R_0 = \{0\}$ and $r + r^{-1} \in \operatorname{Im}\varphi$ for $r \in U(R)$. Hence, the map

$$\psi : U(R) \to \mathbb{S}^1(R)$$

given by $\psi(r) = (2^{-1}(r^{-1}+r), 2^{-1}(r^{-1}-r)i)$ for $r \in U(R)$ is the inverse of the $\varphi : \mathbb{S}^1(R) \to U(R)$ above.

(ii) If $\chi(R) = 2$ then $R_0 = R$, $\operatorname{Im}\varphi = \{r \in R;\, r^2 = 1\} = R_1$ and the short exact sequence

$$0 \to R^+ \to \mathbb{S}^1(R) \to R_1 \to 1$$

splits as an exact sequence of elementary 2-groups.

(3) Consider the group homomorphism $\rho : U(R[i]) \to U(R)$ given by $\rho(r_0 + r_1 i) = r_0^2 + r_1^2$ for $r_0 + r_1 i \in U(R[i])$. Then, $\operatorname{Ker}\rho = \mathbb{S}^1(R)$ and consequently we get the required short exact sequence $1 \to \mathbb{S}^1(R) \to U(R[i]) \to U(R)$.

Let now R be a finite field and define the group endomorphism $\pi : U(R) \to U(R)$ given by $\pi(r) = r^2$ for $r \in U(R)$. If $\chi(R) = 2$ then π is an automorphism and so $U(R[i]) \xrightarrow{\rho} U(R)$ is onto.

Now, suppose that $\chi(R) \neq 2$ and write $\sharp X$ for the cardinality of a finite set X. Notice that the group endomorphism $U(R) \to U(R)$ given by $r \mapsto r^2$ for $r \in U(R)$ leads to $\ker\pi \cong \mathbb{Z}_2$ and $\sharp\{r^2;\, r \in U(R)\} = \frac{\sharp U(R)}{2}$. Given $r \in U(R)$, we follow [10, Remark 6.25] to consider the sets $A = \{r_0^2;\, r_0 \in U(R) \cup \{0\}\}$ and $B = \{r - r_1^2;\, r_1 \in U(R) \cup \{0\}\}$. Then, $\sharp A = \sharp B = \frac{\sharp U(R)}{2} + 1$ and consequently $A \cap B \neq \emptyset$ which implies that $\rho(r_0 + r_1 i) = r$.

$\square$

Writing $\mathbb{Z}_m^+$ for the cyclic group with order m, we deduce (see [9, Korollar 6]):

Corollary 2.3. *If R is a finite field then there is an isomorphism of groups:*

(1) $\mathbb{S}^1(R) \simeq (\mathbb{Z}_2^+)^k$ *provided* $\sharp R = 2^k$ *and* $\chi(R) = 2$*;*

(2) $\mathbb{S}^1(R) \simeq \begin{cases} \mathbb{Z}^+_{\sharp R-1}, & if\ \sharp R \equiv 1 \pmod 4; \\ \mathbb{Z}^+_{\sharp R+1}, & if\ \sharp R \equiv 3 \pmod 4. \end{cases}$ *provided* $\chi(R) \neq 2$.

Proof. (1) follows directly from Proposition 2.2(2)(ii).

(2) If $\sharp R \equiv 1 \pmod 4$ then $i \in R$ and by Proposition 2.2(2), we get an isomorphism $\mathbb{S}^1(R) \cong U(R)$. Hence, the well-known isomorphism $U(R) \cong \mathbb{Z}^+_{\sharp R-1}$ yields $\mathbb{S}^1(R) \cong \mathbb{Z}^+_{\sharp R-1}$.

If $\sharp R \equiv 3 \pmod 4$ then, by Fermat Theorem on Sums of Two Squares, $i \notin R$. Then, by Proposition 2.2(3), there is an exact sequence $1 \to \mathbb{S}^1(R) \to U(R[i]) \to U(R) \to 1$ of abelian groups. Because R and $R[i]$ are finite fields, there are isomorphisms $U(R) \cong \mathbb{Z}_{\sharp R-1}$ and $U(R[i]) \cong \mathbb{Z}_{(\sharp R)^2-1}$. Consequently, we deduce $\mathbb{S}^1(R) \cong \mathbb{Z}^+_{\sharp R+1}$ and the proof is complete.

□

Let now $R = \mathbb{Z}_m$, the ring of integers modulo m. The primary factorization $m = p_1^{k_1} \cdots p_t^{k_t}$ yields an isomorphism of rings $\mathbb{Z}_m \xrightarrow{\cong} \mathbb{Z}_{p_1^{k_1}} \times \cdots \times \mathbb{Z}_{p_t^{k_t}}$. Because $\mathbb{S}^1(-)$ is a product preserving functor from unitary rings to abelian groups, we get an isomorphism

$$\mathbb{S}^1(\mathbb{Z}_m) \xrightarrow{\cong} \mathbb{S}^1(\mathbb{Z}_{p_1^{k_1}}) \times \cdots \times \mathbb{S}^1(\mathbb{Z}_{p_t^{k_t}})$$

and $\sharp\mathbb{S}^1(\mathbb{Z}_m) = \sharp\mathbb{S}^1(\mathbb{Z}_{p_1^{k_1}}) \cdots \sharp\mathbb{S}^1(\mathbb{Z}_{p_t^{k_t}})$. Hence, the problem of determining the structure of $\mathbb{S}^1(\mathbb{Z}_m)$ and $\sharp\mathbb{S}^1(\mathbb{Z}_n)$ has been reduced to the case of prime powers p^k. By the claim in [9, p. 54], the group $\mathbb{S}^1(\mathbb{Z}_{p^k})$ is cyclic provided p is an odd prime. A proof of that is presented below.

Lemma 2.4. *If p is a prime and $k \geq 1$ then*

$$U(\mathbb{Z}_{p^k}[i]) \cong \begin{cases} \mathbb{Z}^+_{p^{k-1}(p-1)} \oplus \mathbb{Z}^+_{p^{k-1}(p-1)}, & if\ p \equiv 1 \pmod 4; \\ \mathbb{Z}^+_{p^{k-1}} \oplus \mathbb{Z}^+_{p^{k-1}(p^2-1)}, & if\ p \equiv 3 \pmod 4; \\ \mathbb{Z}^+_2, & if\ p = 2\, and\, k = 1; \\ \mathbb{Z}^+_{2^2} \oplus \mathbb{Z}^+_{2^{k-2}} \oplus \mathbb{Z}^+_{2^{k-1}}, & if\ p = 2\, and\, k \geq 2. \end{cases}$$

Proof. First, let p be an odd prime. Recall the well-known the isomorphism $U(\mathbb{Z}_{p^k}) \cong ((p)+1) \oplus U(\mathbb{Z}_p) \cong \mathbb{Z}^+_{p^{k-1}(p-1)}$ stated in [13, Theorem 6.7], where (p) is the nilpotent principal ideal of $\mathbb{Z}_{p^k}$ generated by p.

Let $p \equiv 1 \,(\mathrm{mod}\ 4)$ and $i \in U(\mathbb{Z}_{p^k})$ with order four. Because $i \in \mathbb{Z}_{p-1}$ and -1 is the only element in $\mathbb{Z}_{p-1}$ with order two, we deduce that $i^2 = -1$. Consequently, $\mathbb{Z}_{p^k}[i] \cong \mathbb{Z}_{p^k} \times \mathbb{Z}_{p^k}$ and $U(\mathbb{Z}_{p^k}[i]) \cong U(\mathbb{Z}_{p^k}) \times U(\mathbb{Z}_{p^k}) \cong \mathbb{Z}^+_{p^k(p-1)} \oplus \mathbb{Z}^+_{p^k(p-1)}$.

If $p \equiv 3 \,(\bmod\ 4)$ then, by Fermat's Theorem on Sums of Two Squares, $i \notin \mathbb{Z}_{p^k}$. Given $r_0 + r_1 i \in \mathbb{Z}_{p^k}[i]$, we see that $r_0 + r_1 i \in U(\mathbb{Z}_{p^k}[i])$ if and only if $r_0^2 + r_1^2 \in U(\mathbb{Z}_{p^k})$ or equivalently, if and only if $r_0 \in U(\mathbb{Z}_{p^k})$ or $r_1 \in U(\mathbb{Z}_{p^k})$. Hence, $\mathbb{Z}_{p^k}[i]$ is a p-primary ring with the nilpotent principal prime ideal (p) and $\sharp(p) = p^{2(k-1)}$. Then, the residue filed $\mathbb{Z}_{p^k}[i]/(p) \cong \mathbb{Z}_{p^2}$ and in view of [2, Proposition 1], we deduce that $U(\mathbb{Z}_{p^k}[i]) \cong ((p)+1) \oplus U(\mathbb{Z}_{p^2})$. Following the proof of [13, Theorem 6.7], we get $(1+p)^{p^{l-2}}, (1+pi)^{p^{l-2}} \not\equiv 1 \,(\bmod\ p^l)$ and $(1+p)^{p^{l-1}}, (1+pi)^{p^{l-1}} \equiv 1 \,(\bmod\ p^l)$ for $l \geq 2$. Because $\langle 1+p \rangle \cap \langle 1+pi \rangle = \{1\}$, we deduce a group isomorphism $((p)+1) \cong \langle 1+p \rangle \oplus \langle 1+pi \rangle \cong \mathbb{Z}^+_{p^{k-1}} \oplus \mathbb{Z}^+_{p^{k-1}}$. Consequently, we get that $U(\mathbb{Z}_{p^k}[i]) \cong \mathbb{Z}^+_{p^{k-1}} \oplus \mathbb{Z}^+_{p^{k-1}(p^2-1)}$.

Let now $p = 2$. First, it is obvious that $U(\mathbb{Z}_2[i]) = \{1, i\} \cong \mathbb{Z}_2$. Hence, we can assume that $k \geq 2$. Recall form [13, Theorem 5.44] that $U(\mathbb{Z}_{2^k}) \cong \langle 5 \rangle \oplus \langle -1 \rangle \cong \mathbb{Z}^+_{2^{k-2}} \oplus \mathbb{Z}^+_2$ for $k \geq 2$. Because $r_0 + r_1 i \in U(\mathbb{Z}_{2^k}[i])$ if any only if r_0 is odd and r_1 is even or *vise versa*, we get $\sharp U(\mathbb{Z}_{2^k}[i]) = 2^{2k-1}$. Further, $(1+2i)^{2^{l-2}} \equiv 2^{l-1} + 1 + 2^{l-1} i \,(\mathrm{mod}\, 2^l)$ for $l > 2$. This implies that 2^{k-1} is the order of $1+2i$. Next, the intersection of any two of the subgroups $\langle i \rangle$, $\langle 5 \rangle$ and $\langle 1+2i \rangle$ is the trivial group and $\sharp U(\mathbb{Z}_{2^k}[i]) = 2^{2k-1}$. Thus, we deduce that $U(\mathbb{Z}_{2^k}[i]) \cong \langle i \rangle \oplus \langle 5 \rangle \oplus \langle 1+2i \rangle \cong \mathbb{Z}_{2^2} \oplus \mathbb{Z}_{2^{k-2}} \oplus \mathbb{Z}_{2^{k-1}}$ for $k \geq 2$ and the proof is complete.

□

Now, we are in a position to show the main result of this Section:

Theorem 2.5. *If p is a prime and $k \geq 1$ then*

$$\mathbb{S}^1(\mathbb{Z}_{p^k}) \cong \begin{cases} \mathbb{Z}^+_{p^{k-1}(p-1)}, & if\ p \equiv 1 \,(\mathrm{mod}\, 4); \\ \mathbb{Z}^+_{p^{k-1}(p+1)}, & if\ p \equiv 3 \,(\mathrm{mod}\, 4); \\ \mathbb{Z}^+_2, & if\ \ k = 1; \\ \mathbb{Z}^+_2 \oplus \mathbb{Z}^+_{2^2} \oplus \mathbb{Z}^+_{2^{k-2}}, & if\ \ k \geq 2. \end{cases}$$

Proof. (1) If $p \equiv 1 \,(\mathrm{mod}\ 4)$ then $i \in \mathbb{Z}_{p^k}$. Because $2 \in U(\mathbb{Z}_{p^k})$, by Proposition 2.2(2), the map $\rho : \mathbb{S}^1(\mathbb{Z}_{p^k}) \to U(\mathbb{Z}_{p^k})$ given by $\rho(r_0, r_1) = r_0 + r_1 i$ for $(r_0, r_1) \in \mathbb{S}^1(\mathbb{Z}_{p^k})$ is an isomorphism of groups. Thus,

$$\mathbb{S}^1(\mathbb{Z}_{p^k}) \cong U(\mathbb{Z}_{p^k}) \cong \mathbb{Z}^+_{p^{k-1}(p-1)}.$$

(2) If $p \equiv 3 \,(\mathrm{mod}\ 4)$ then $i \notin \mathbb{Z}_{p^k}$. Further, $U(\mathbb{Z}_{p^k}) \cong \mathbb{Z}^+_{p^{k-1}(p-1)}$ and, in view of Lemma 2.4, it holds $U(\mathbb{Z}_{p^k}[i]) \cong \mathbb{Z}^+_{p^{k-1}} \oplus \mathbb{Z}^+_{p^{k-1}(p^2-1)}$. Next, consider the map $\rho : U(\mathbb{Z}_{p^k}[i]) \to U(\mathbb{Z}_{p^k})$ defined in Proposition 2.2(2). Then, the restriction $\rho|_{\mathbb{Z}^+_{p^{k-1}}}$ is an isomorphism and, in view of Proposition 2.2(3), the restriction $\rho|_{\mathbb{Z}^+_{p^2-1}}$ is onto. Consequently, $\rho : U(\mathbb{Z}_{p^k}[i]) \to U(\mathbb{Z}_{p^k})$ is onto and the short exact sequence $1 \to \mathbb{S}^1(\mathbb{Z}_{p^k}) \to U(\mathbb{Z}_{p^k}[i]) \xrightarrow{\rho} U(\mathbb{Z}_{p^k}) \to 1$ from Proposition 2.2(3) yields $\mathbb{S}^1(\mathbb{Z}_{p^k}) \cong \mathbb{Z}^+_{p^{k-1}(p+1)}$.

(3) For the group homomorphism $\rho : U(\mathbb{Z}_{2^k}[i]) \to U(\mathbb{Z}_{2^k})$ given by $\rho(r_0 + r_1 i) = r_0^2 + r_1^2$ for $r_0 + r_1 i \in U(\mathbb{Z}_{2^k}[i])$, by Proposition 2.2(3), we get the short exact sequence

$$1 \to \mathbb{S}^1(\mathbb{Z}_{2^k}) \to U(\mathbb{Z}_{2^k}[i]) \xrightarrow{\rho} U(\mathbb{Z}_{2^k})$$

of abelian groups with $k \geq 1$.

Because $U(\mathbb{Z}_2) = \{1\}$, Lemma 2.4 yields that $\mathbb{S}^1(\mathbb{Z}_2) \cong U(\mathbb{Z}_2[i]) \cong \mathbb{Z}^+_2$. If $k \geq 2$ then by the proof of Lemma 2.4, we have that $U(\mathbb{Z}_{2^k}[i]) \cong \langle i \rangle \oplus \langle 5 \rangle \oplus \langle 1+2i \rangle \cong \mathbb{Z}_{2^2} \oplus \mathbb{Z}_{2^{k-2}} \oplus \mathbb{Z}_{2^{k-1}}$. Because $\rho(i) = 1$, $\rho(5) = 5^2$, $\rho(1+2i) = 5$ and $U(\mathbb{Z}_{2^k}) \cong \langle 5 \rangle \oplus \langle -1 \rangle \cong \mathbb{Z}^+_{2^{k-2}} \oplus \mathbb{Z}^+_2$, we deduce that $\mathrm{Im}\,\rho = \langle 5 \rangle \cong \mathbb{Z}^+_{2^{k-2}}$. Consequently, the exact sequence

$$1 \to \mathbb{S}^1(\mathbb{Z}_{2^k}) \to U(\mathbb{Z}_{2^k}[i]) \xrightarrow{\rho} \mathbb{Z}_{2^{k-2}} \to 1$$

yields $\mathbb{S}^1(\mathbb{Z}_{2^k}) \cong \mathbb{Z}^+_2 \oplus \mathbb{Z}^+_{2^2} \oplus \mathbb{Z}^+_{2^{k-2}}$ for $k \geq 2$ and the proof is complete. □

2. Spheres over finite fields and their polynomial maps

Let R be a commutative and unitary ring. Then, we notice:

Remark 3.1. For any commutative and unitary ring R there is a bijection $\mathbb{S}^3(R) \cong SU(R[i])$ determined by the assignment

$$(r_0, r_1, r_2, r_3) \mapsto \begin{pmatrix} r_0 + r_1 i & r_2 + r_3 i \\ -r_2 + r_3 i & r_0 - r_1 i \end{pmatrix}$$

for $(r_0, r_1, r_2, r_3) \in \mathbb{S}^3(R)$. Consequently, $\mathbb{S}^3(R)$ inherits the group structure from $SU(R[i])$. Notice that $\mathbb{S}^2(R) \cong \{A \in SU(R[i]);\, \mathrm{tr}\,(A) = 0\}$ provided $2R = 0$, where $tr : SU(R[i]) \to R[i]$ is the trace function.

Notice that there is an embedding $R_0^n \hookrightarrow \mathbb{S}^n(R)$ given by

$$(r_0, \dots, r_{n-1}) \mapsto (1 + r_0 + \cdots + r_{n-1}, r_0, \dots, r_{n-1})$$

for $(r_0, \dots, r_{n-1}) \in R_0^n$, where $R_0 = \{r \in R;\, 2r = 0\}$. In particular, $R^n \hookrightarrow \mathbb{S}^n(R)$ provided $\chi(R) = 2$. If R is a field with $\chi(R) = 2$ then certainly there is a bijection $\mathbb{S}^n(R) \cong R^n$ and $\sharp\mathbb{S}^n(R) = (\sharp R)^n$.

Now, suppose that R is a finite field with $\chi(R) \neq 2$. Basing on [10, Theorems 6.26 and 6.27], we obtain:

Theorem 3.2. *If R is a finite field with $\chi(R) \neq 2$ then for any number $n \geq 1$ it holds:*

$$\sharp\mathbb{S}^n(R) = \begin{cases} (\sharp R)^n + (\sharp R)^{\frac{n}{2}}\eta((-1)^{\frac{n}{2}}), & \text{if } n \text{ is even;} \\ (\sharp R)^n - (\sharp R)^{\frac{n-1}{2}}\eta((-1)^{\frac{n+1}{2}}), & \text{if } n \text{ is odd,} \end{cases}$$

where $\eta(1) = 1$ *and* $\eta(-1) = \begin{cases} 1, & \text{if the equation } x^2 + 1 = 0 \\ & \text{has a solution in } R; \\ -1, & \text{otherwise.} \end{cases}$

Let $\sharp R = p^k$ for an odd prime p. Notice that $\eta(-1) = 1$ if and only if $p \equiv 1\,(\mathrm{mod}\,4)$ or k is an even number.

To examine polynomial maps $P = (P_0, \dots, P_n) : \mathbb{S}^m(R) \to \mathbb{S}^n(R)$ in that case a general result would be useful.

Proposition 3.3. *Let R be a field and $S \subseteq R^{m+1}$, $T \subseteq R^{n+1}$ finite subsets. Then any map $f : S \to T$ is a polynomial one for $m, n \geq 0$.*

Proof. Given a finite subset $S \subseteq R^{m+1}$ there is obviously a finite subset $S_0 = \{r_1, \dots, r_k\} \subseteq R$ with $S \subseteq S_0^{m+1}$. It is well-know that there are interpolation polynomials $P_{r_1}(X), \dots, P_{r_k}(X) \in R[X]$ with $P_{r_i}(x_j) =$

$\delta_{r_i r_j}$ for $i, j = 0, \ldots, k$. Next for any $s = (r_{i_0}, \ldots, r_{i_m}) \in S_0^{m+1}$ consider the polynomial

$$P_s(X_0, \ldots, X_m) = P_{r_{i_0}}(X_0) \cdots P_{r_{i_m}}(X_m) \in R[X_0, \ldots, X_m].$$

Then $P_s(s') = \delta_{ss'}$ for any $s, s' \in S_0^{m+1}$.

Now, given a map $f : S \to T$ write $f(s) = (f_0(s), \ldots, f_n(s))$ for any point $s \in S$. Then, the polynomial map $S \to T$ determined by polynomials:

$$Q_0(X_0, \ldots, X_m) = \sum_{s \in S} f_0(s) P_s(X_0, \ldots, X_m),$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$Q_n(X_0, \ldots, X_m) = \sum_{s \in S} f_n(s) P_s(X_0, \ldots, X_m)$$

coincides with $f : S \to T$ and the proof is complete. $\square$

In particular, the following conclusion follows.

Corollary 3.4. *Let R be a finite field. Then any map $\mathbb{S}^{m_1}(R) \times \cdots \times \mathbb{S}^{m_k}(R) \to \mathbb{S}^{n_1}(R) \times \cdots \times \mathbb{S}^{n_l}(R)$ is a polynomial one for $m_1, \ldots, m_k, n_1, \ldots, n_l \geq 0$.*

Let $\mathrm{End}_R(R[X_1, \ldots, X_n])$ be the set of all R-homomorphisms of $R[X_1, \ldots, X_n]$ and $\mathrm{Aut}_R(R[X_1, \ldots, X_n])$ the group of all its R-automorphisms. Write $T(R, n)$ for the tame polynomial automorphism subgroup of $\mathrm{Aut}_R(R[X_1, \ldots, X_n])$ generated by $(X_1 + F(X_2, \ldots, X_n), X_2, \ldots, X_n)$ for all $F(X_2, \ldots, X_n) \in R[X_2, \ldots, X_n]$, $\mathcal{P}(R^n)$ for the set of all self-maps of R^n and $\mathcal{B}(R^n)$ the group of all bijections of R^n. Then, we get an obvious map

$$\mathcal{E} : \mathrm{End}_R(R[X_1, \ldots, X_n]) \longrightarrow \mathcal{P}(R^n).$$

Theorem 3.5. ([12]) *Let R be a finite field and F_p the simple field, where p is a prime. Then:*

(1) $\sharp\mathcal{E}(T(R,1)) = \sharp\mathcal{B}(R)/\sharp R - 2)!$, so $\mathcal{E}(T(R,1)) = \mathcal{B}(R)$ only if $R = F_2, F_3$;

(2) if $n \geq 2$ and $\chi(R) \neq 2$ or $R = F_2$ then $\mathcal{E}(T(R,n)) = \mathcal{B}(R^n)$;

(3) if $n \geq 2$, $\chi(R) = 2$ and $\sharp R > 2$ then $\sharp\mathcal{E}(T(R,n) = \sharp\mathcal{B}(R^n)/2$. In fact,

$\mathcal{E}(T(R,n))$ is the alternating subgroup $\mathcal{A}(R^n)$ of the group $\mathcal{B}(R^n)$.

Now, any bijection of $\mathbb{S}^{n_1}(R)\times\cdots\times\mathbb{S}^{n_l}(R)$ yields an bijection of $R^{m_1+\cdots+m_k+k}$. Furthermore, for $\chi(R)=2$ there is an obvious polynomial isomorphism $\mathbb{S}^n(R)\to R^n$. Consequently, Theorem 3.5 leads to:

Corollary 3.6. *Let R be a finite field. Then:*

(1) if $\chi(R)\neq 2$ or $R=F_2$ then any bijection of $\mathcal{B}(\mathbb{S}^{n_1}(R)\times\cdots\times\mathbb{S}^{n_l}(R))$ is an invertible polynomial map;

(2) if $\sharp R>2$ and $\chi(R)=2$ then any bijection of $\mathcal{A}(\mathbb{S}^{n_1}(R)\times\cdots\times\mathbb{S}^{n_l}(R))$ is an invertible polynomial map.

Let R be a commutative and unitary ring. Then, we could consider the non-commutative and unitary ring $R\{i,j,k\}$ with $i^2=j^2=k^2=-1, ij=k, jk=i, ki=j$. Given $q=r_0+r_1i+r_2j+r_3k\in R\{i,j,k\}$, we write $|q|^2=r_0^2+r_1^2+r_2^2+r_3^2$ and $\bar{q}=r_0-r_1i-r_2j-r_3k$. Then, $q\bar{q}=|q|^2$, $|q_1q_2|^2=|q_1|^2|q_2|^2$ for $q,q_1,q_2\in R\{i,j,k\}$ and

$$\mathbb{S}^3(R)\cong\{q\in R\{i,j,k\};\ |q|^2=1\}.$$

Hence, $\mathbb{S}^3(R)$ inherits the group structure which coincides with the previous one. Further, we have a group monomorphism

$$\varphi:\mathbb{S}^3(R)\to U(R\{i,j,k\})$$

given by $\varphi(r_0,r_1,r_2,r_3)=r_0+r_1i+r_2j+r_3k$ for $(r_0,r_1,r_2,r_3)\in\mathbb{S}^3(R)$. Notice that $r_0+r_1i+r_2j+r_3k\in U(R\{i,j,k\})$ if and only if $r_0^2+r_1^2+r_2^2+r_3^2\in U(R)$. Hence, the map

$$\rho:U(R\{i,j,k\})\to U(R)$$

given by $\rho(r_0+r_1i+r_2j+r_3k)=r_0^2+r_1^2+r_2^2+r_3^2$ for $r_0+r_1i+r_2j+r_3k\in U(R\{i,j,k\})$ is a well-defined group homomorphism and the sequence

$$1\to\mathbb{S}^3(R)\xrightarrow{\varphi}U(R\{i,j,k\})\xrightarrow{\rho}U(R)$$

is exact.

Next, we consider the non-associative and unitary ring $R\{e_1,e_2,e_3,e_4,e_5,e_6,e_7\}$, where products e_se_t are defined by the Cayley algebra rules for $s,t=1,2,3,4,5,6,7$. Given $c=r_0+r_1e_1+r_2e_2+r_3e_3+r_4e_4+r_5e_5+r_6e_6+r_7e_7\in R\{e_1,e_2,e_3,e_4,e_5,e_6,e_7\}$, write $|c|^2=r_0^2+r_1^2+r_2^2+r_3^2+r_4^2+r_5^2+r_6^2+r_7^2$. Then, $|c_1c_2|^2=|c_1|^2|c_2|^2$ for $c_1,c_2\in R\{e_1,e_2,e_3,e_4,e_5,e_6,e_7\}$ and

$$\mathbb{S}^7(R)\cong\{c\in R\{e_1,e_2,e_3,e_4,e_5,e_6,e_7\};\ |c|^2=1\}$$

inherits a non-associative group structure.

Notice that we have a non-associative group monomorphism

$$\varphi : \mathbb{S}^7(R) \to U(R\{e_1, e_2, e_3, e_4, e_5, e_6, e_7\})$$

given by $\varphi(r_0, r_1, r_2, r_3, r_4, r_5, r_6, r_7) = r_0 + r_1e_1 + r_2e_2 + r_3e_3 + r_4e_4 + r_5e_5 + r_6e_6 + r_7e_7$ for $(r_0, r_1, r_2, r_3, r_4, r_5, r_6, r_7) \in \mathbb{S}^7(R)$. Notice that $r_0 + r_1e_1 + r_2e_2 + r_3e_3 + r_4e_4 + r_5e_5 + r_6e_6 + r_7e_7 \in U(R\{e_1, e_2, e_3, e_4, e_5, e_6, e_7\})$ if and only if $r_0^2 + r_1^2 + r_2^2 + r_3^2 + r_4^2 + r_5^2 + r_6^2 + r_7^2 \in U(R)$. Hence, the map

$$\rho : U(R\{e_1, e_2, e_3, e_4, e_5, e_6, e_7\}) \to U(R)$$

given by $\rho(r_0 + r_1e_1 + r_2e_2 + r_3e_3 + r_4e_4 + r_5e_5 + r_6e_6 + r_7e_7) = r_0^2 + r_1^2 + r_2^2 + r_3^2 + r_4^2 + r_5^2 + r_6^2 + r_7^2$ for $r_0 + r_1e_1 + r_2e_2 + r_3e_3 + r_4e_4 + r_5e_5 + r_6e_6 + r_7e_7 \in U(R\{e_1, e_2, e_3, e_4, e_5, e_6, e_7\})$ is a well-defined non-associative group homomorphism and the sequence

$$1 \to \mathbb{S}^7(R) \overset{\varphi}{\to} U(R\{e_1, e_2, e_3, e_4, e_5, e_6, e_7\}) \overset{\rho}{\to} U(R)$$

is exact.

If R_1, R_2 are commutative and unitary rings then there is a bijection $\mathbb{S}^n(R_1 \times R_2) \cong \mathbb{S}^n(R_1) \times \mathbb{S}^n(R_2)$ for $n \geq 0$. Because the primary factorization $m = p_1^{k_1} \cdots p_t^{k_t}$ yields an isomorphism of rings $\mathbb{Z}_m \overset{\cong}{\to} \mathbb{Z}_{p_1^{k_1}} \times \cdots \times \mathbb{Z}_{p_t^{k_t}}$, we derive a bijection

$$\mathbb{S}^n(\mathbb{Z}_m) \cong \mathbb{S}^n(\mathbb{Z}_{p_1^{k_1}}) \times \cdots \times \mathbb{S}^n(\mathbb{Z}_{p_t^{k_t}}).$$

Thus, the study of $\mathbb{S}^n(\mathbb{Z}_m)$ reduces to $\mathbb{S}^n(\mathbb{Z}_{p^k})$ for any prime p and $k \geq 1$.

Proposition 3.7. *If p is a prime and $k \geq 1$ then:*

$$(1)\ \sharp\mathbb{S}^3(\mathbb{Z}_{p^k}) = \begin{cases} p^{3k-2}(p^2-1), & \textit{if } p \textit{ is an odd prime};\\ 2^{3k}, & \textit{if } p = 2; \end{cases}$$

$$(2)\ \sharp\mathbb{S}^7(\mathbb{Z}_{p^k}) = \begin{cases} p^{7k-4}(p^2-1)(p^2+1), & \textit{if } p \textit{ is an odd prime};\\ 2^{7k}, & \textit{if } p = 2. \end{cases}$$

Proof. (1) First, notice that $r_0 + r_1i + r_2j + r_3k \notin U(\mathbb{Z}_{p^k}\{i, j, k\})$ if only if $r_0^2 + r_1^2 + r_2^2 + r_3^2 \equiv 0 \pmod p$ or equivalently, $r_0^2 + r_1^2 + r_2^2 + r_3^2 = 0$ in the field $\mathbb{Z}_p$.

If p is an odd prime then, in view of [10, Theorem 6.26], the equation $r_0^2 + r_1^2 + r_2^2 + r_3^2 = 0$ has $p^3 + (p-1)p$ solutions in $\mathbb{Z}_p$. Consequently, the equation $r_0^2+r_1^2+r_2^2+r_3^2 \equiv 0 \,(\mathrm{mod}\, p)$ has $p^{4(k-1)}(p^3+(p-1)p) = p^{4k-3}(p^2+p-1)$ solutions in $\mathbb{Z}_{p^k}$. This implies that $\sharp U(\mathbb{Z}_{p^k}\{i,j,k\}) = p^{4k} - p^{4k-3}(p^2+p-1) = p^{4k-3}(p^2-1)(p-1)$.

If $p=2$ then the equation $r_0^2+r_1^2+r_2^2+r_3^2 = 0$ has 2^3 solutions in $\mathbb{Z}_2$. Consequently, the equation $r_0^2+r_1^2+r_2^2+r_3^2 \equiv 0 \,(\mathrm{mod}\, 2)$ has $2^{4(k-1)}2^3 = 2^{4k-1}$ solutions in $\mathbb{Z}_{2^k}$. This implies that $\sharp U(\mathbb{Z}_{2^k}\{i,j,k\}) = 2^{4k} - 2^{4k-1} = 2^{4k-1}$.

Next, by Lagrange Four-Square Theorem, the map $\rho : U(\mathbb{Z}_{p^k}\{i,j,k\}) \to U(\mathbb{Z}_{p^k})$ is onto for any prime p and $k \geq 1$. Hence, the short exact sequence

$$1 \to \mathbb{S}^3(\mathbb{Z}_{p^k}) \xrightarrow{\varphi} U(\mathbb{Z}_{p^k}\{i,j,k\}) \xrightarrow{\rho} U(\mathbb{Z}_{p^k}) \to 1$$

and $U(\mathbb{Z}_{p^k}) \cong \begin{cases} \mathbb{Z}_{p^{k-1}(p-1)}, & \text{if } p \text{ is an odd prime;} \\ \{1\}, & \text{if } p=2 \text{ and } k=1; \\ \mathbb{Z}_2 \oplus \mathbb{Z}_{2^{k-2}}, & \text{if } p=2 \text{ and } k\geq 2 \end{cases}$

lead to (1).

(2) If p is an odd prime then, in view of [10, Theorem 6.26], the equation $r_0^2+r_1^2+r_2^2+r_3^2+r_4^2+r_5^2+r_6^2+r_7^2 = 0$ has $p^7+(p-1)p^3$ solutions in $\mathbb{Z}_p$. Consequently, the equation $r_0^2+r_1^2+r_2^2+r_3^2+r_4^2+r_5^2+r_6^2+r_7^2 \equiv 0 \,(\mathrm{mod}\, p)$ has $p^{8(k-1)}(p^7+(p-1)p^3) = p^{8k-5}(p^4+p-1)$ solutions in $\mathbb{Z}_{p^k}$. This implies that $\sharp U(\mathbb{Z}_{p^k}\{e_1,e_2,e_3,e_4,e_5,e_6,e_7\}) = p^{8k} - p^{8k-5}(p^4+p-1) = p^{8k-5}(p^2-1)(p-1)(p^2+1)$.

If $p=2$ then the equation $r_0^2+r_1^2+r_2^2+r_3^2+r_4^2+r_5^2+r_6^2+r_7^2 = 0$ has 2^7 solutions in $\mathbb{Z}_2$. Consequently, the equation $r_0^2+r_1^2+r_2^2+r_3^2+r_4^2+r_5^2+r_6^2+r_7^2 \equiv 0 \,(\mathrm{mod}\, 2)$ has $2^{8(k-1)}2^7 = 2^{8k-1}$ solutions in $\mathbb{Z}_{2^k}$. This implies that $\sharp U(\mathbb{Z}_{2^k}\{e_1,e_2,e_3,e_4,e_5,e_6,e_7\}) = 2^{8k} - 2^{8k-1} = 2^{8k-1}$.

Then, we follow *mutatis mutandis* the procedure presented in (1) and the proof is completed. $\square$

Now, for $z = r_0 + r_1 i \in R[i]$, we write $|z|^2 = r_0^2 + r_1^2$ and $\bar{z} = r_0 - r_1 i$. Then, $z\bar{z} = |z|^2$, $z \in U(R[i])$ if and only if $|z|^2 \in U(R)$ and

$$\mathbb{S}^3(R) \cong \{(z_0,z_1) \in R[i] \times R[i];\, |z_0|^2 + |z_1|^2 = 1\}.$$

Notice that there is an action

$$\circ : \mathbb{S}^1(R) \times \mathbb{S}^3(R) \longrightarrow \mathbb{S}^3(R)$$

such that $\lambda \circ (z_0,z_1) = (\lambda z_0, \lambda z_1)$ for $\lambda \in \mathbb{S}^1(R)$ and $(z_0,z_1) \in \mathbb{S}^3(R)$.

Next, $q \in U(R\{i,j,k\})$ if and only if $|q|^2 \in U(R)$ for $q \in R\{i,j,k\}$, and

$$\mathbb{S}^7(R) \cong \{(q_0,q_1) \in R\{i,j,k\} \times R\{i,j,k\};\ |q_0|^2 + |q_1|^2 = 1\}.$$

Further, there is an action

$$\circ : \mathbb{S}^3(R) \times \mathbb{S}^7(R) \longrightarrow \mathbb{S}^7(R)$$

such that $\lambda \circ (q_0,q_1) = (\lambda q_0, \lambda q_1)$ for $\lambda \in \mathbb{S}^3(R)$ and $(q_0,q_1) \in \mathbb{S}^7(R)$.

Now, we mimic the Hopf maps $h : \mathbb{S}^3 \longrightarrow \mathbb{S}^2$ and $H : \mathbb{S}^7 \longrightarrow \mathbb{S}^4$ to define

$$h(R) : \mathbb{S}^3(R) \longrightarrow \mathbb{S}^2(R)$$

by $h(R)(z_0,z_1) = (|z_0|^2 - |z_1|^2, 2z_0\bar{z}_1)$ for $(z_0,z_1) \in \mathbb{S}^3(R)$ and

$$H(R) : \mathbb{S}^7(R) \longrightarrow \mathbb{S}^4(R)$$

by $H(R)(q_0,q_1) = (|q_0|^2 - |q_1|^2, 2q_0\bar{q}_1)$ for $(q_0,q_1) \in \mathbb{S}^7(R)$.

Proposition 3.8. *Let R be a local commutative and unitary ring such that 2 is not a zero divisor of R. Then:*

$$(1)\ \ h(R)^{-1}(h(R)(z_0,z_1)) = \{(\lambda z_0, \lambda z_1);\ for\, \lambda \in \mathbb{S}^1(R)\} \cong \mathbb{S}^1(R)$$

for any $(z_0,z_1) \in \mathbb{S}^3(R)$;

$$(2)\ \ H(R)^{-1}(h(R)(q_0,q_1)) = \{(\lambda q_0, \lambda q_1);\ for\, \lambda \in \mathbb{S}^3(R)\} \cong \mathbb{S}^3(R)$$

for any $(q_0,q_1) \in \mathbb{S}^7(R)$.

Proof. (1) Let $(z_0,z_1) \in \mathbb{S}^3(R)$. Then, certainly it holds $\{(\lambda z_0, \lambda z_1); \text{for}\, \lambda \in \mathbb{S}^1(R)\} \subseteq h(R)^{-1}(h(R)(z_0,z_1))$.

Suppose that $h(R)(w_0,w_1) = h(R)(z_0,z_1)$ for some $(w_0,w_1) \in \mathbb{S}^3$. Then, $|w_0|^2 - |w_1|^2 = |z_0|^2 - |z_1|^2$ and $2w_0\bar{w}_1 = 2z_0\bar{z}_1$. Because $|w_0|^2 + |w_1|^2 = 1 = |z_0|^2 + |z_1|^2$ and $2 \in R$ is not a zero divisor, we get $|w_0|^2 = |z_0|^2$, $|w_1|^2 = |z_1|^2$ and $w_0\bar{w}_1 = z_0\bar{z}_1$. Further, R is a local ring, so $|w_0|^2 + |w_1|^2 = 1 = |z_0|^2 + |z_1|^2$ implies $|w_0|^2 \in U(R)$ or $|w_1|^2 \in U(R)$ and $|z_0|^2 \in U(R)$ or $|z_1|^2 \in U(R)$. Hence, $w_0 \in U(R)$ or $w_1 \in U(R)$ and $z_0 \in U(R)$ or $z_1 \in U(R)$.

If $z_0 \in U(R)$ then we set $\lambda = z_0^{-1}w_0$; if $z_1 \in U(R)$ then we set $\lambda = z_1^{-1}w_1$. Thus, $\lambda \in \mathbb{S}^1(R)$ and $(w_0,w_1) = (\lambda z_0, \lambda z_1)$. Because $(z_0,z_1) \in$

$\mathbb{S}^3(R)$ implies $z_0 \in U(R)$ or $z_1 \in U(R)$, we get $h(R)^{-1}(h(R)(z_0, z_1)) \cong \mathbb{S}^1(R)$.

(2) Given $(q_0, q_1) \in \mathbb{S}^7(R)$, we follow *mutatis mutandis* (1) to complete the proof.

□

By [1, Theorem 8.7], any commutative Artinian and unitary ring (in particular, any finite commutative and unitary ring) is a finite product of commutative Artinian local rings. Further, $\mathbb{S}^n(R_1 \times R_2) \cong \mathbb{S}^n(R_1) \times \mathbb{S}^n(R_2)$ for any commutative and unitary rings R_1, R_2 and $n \geq 0$. Consequently, in view of Proposition 3.8, for a commutative Artinian and unitary ring R, and such that 2 is not a zero divisor in R, we get embeddings

$$\bar{h}(R) : \mathbb{S}^3(R)/\mathbb{S}^1(R) \longrightarrow \mathbb{S}^2(R) \text{ and } \bar{H}(R) : \mathbb{S}^7(R)/\mathbb{S}^3(R) \longrightarrow \mathbb{S}^4(R).$$

In particular:

if R is a finite field with $\chi(R) \neq 2$ then Corollary 2.3 and Theorem 3.2 imply that $\bar{h}(R) : \mathbb{S}^3(R)/\mathbb{S}^1(R) \longrightarrow \mathbb{S}^2(R)$ and $\bar{H}(R) : \mathbb{S}^7(R)/\mathbb{S}^3(R) \longrightarrow \mathbb{S}^4(R)$ are bijections;

if $R = \mathbb{Z}_{p^k}$ for an odd prime p and $k \geq 1$ then Theorem 2.5 and Proposition 3.7 lead to:

$$\sharp\mathbb{S}^2(\mathbb{Z}_{p^k}) \geq \begin{cases} p^{3k-2}(p+1), & \text{if } p \equiv 1 \,(\mathrm{mod}\, 4); \\ p^{3k-2}(p-1), & \text{if } p \equiv 3 \,(\mathrm{mod}\, 4) \end{cases}$$

and

$$\sharp\mathbb{S}^4(\mathbb{Z}_{p^k}) \geq p^{4k-2}(p^2+1).$$

Remark 3.9. Because

$\mathbb{S}^{15}(R) \cong \{(c_0, c_1) \in R\{e_1, e_2, e_3, e_4, e_5, e_6, e_7\} \times R\{e_1, e_2, e_3, e_4, e_5, e_6, e_7\};$

$|c_0|^2 + |c_1|^2 = 1\},$

we make use the Hopf map $\mathcal{H} : \mathbb{S}^{15} \to \mathbb{S}^8$ to consider $\mathcal{H}(R) : \mathbb{S}^{15}(R) \to \mathbb{S}^8(R)$ for a commutative and unitary ring R, and state a result as in Proposition 3.8 as well.

We close the paper with:

Conjecture 3.10. If p is an odd prime and $k \geq 1$ then:

$$(1)\ \sharp\mathbb{S}^2(\mathbb{Z}_{p^k}) = \begin{cases} p^{3k-2}(p+1), & \text{if } p \equiv 1 \,(\mathrm{mod}\, 4); \\ p^{3k-2}(p-1), & \text{if } p \equiv 3 \,(\mathrm{mod}\, 4); \end{cases}$$

$$(2)\ \sharp\mathbb{S}^4(\mathbb{Z}_{p^k}) = p^{4k-2}(p^2+1).$$

and

Problem 3.11. Let p be an odd prime and $k \geq 1$. Find:
(1) $\sharp(\mathbb{S}^n(\mathbb{Z}_{p^k}))$ for $n > 4$ with $n \neq 7$;
(2) the group structure of $\mathbb{S}^3(\mathbb{Z}_{p^k})$.

References

[1] M.F. Atiyah and I.G. MacDonald, *Introduction to commutative algebra*, Addison-Wesley Publishing Company, Reading, Massachusetts (1969).

[2] Ch.W. Ayoub, *On finite primary rings and their groups of units*, Compos. Math. vol. 21 (3), (1966), 247-252.

[3] J. Bochnak, *On real algebraic morphisms into even-dimensional spheres*, Ann. of Math. 128 (1988), 415-433.

[4] J. Bochnak and W. Kucharz, *Realization of homotopy classes by algebraic mappings*, J. Reine Angew. Math. 377 (1987), 159-169.

[5] J. Bochnak, M. Coste and M.-F. Roy, *Real Algebraic Geometry*, Erg. der Math. 36, Springer-Verlag, Berlin-Heidelberg-New York (1998).

[6] P. Deligne, *La conjecture de Weil, I*, Publ. Math. IHES 43 (1974), 273-307.

[7] M. Golasiński and F. Gómez Ruiz, *Polynomial and regular maps into Grassmannians*, K-Theory 26(1) (2002), 51-68.

[8] M. Golasiński and F. Gómez Ruiz, *On maps of tori*, Bull. Belg. Math. Soc. Simon Stevin 13, no. 1 (2006), 139-148.

[9] F. Lemmermeyer, *Kreise und Quadrate modulo p*, Math. Semesterber. 47 (2000), no. 1, 51-73.

[10] R. Lidl and H. Niederreiter, *Finite fields*, Addis-Wesley Publishing Company, London-Amsterdam-Don Mills, Ontario-Sydney-Tokyo (1983).

[11] J.-L. Loday, *Applications algébriques du tore dans la sphere et de* $\mathbb{S}^p \times \mathbb{S}^q$, in Algebraic K-theory II, Lect. Notes in Math. 342 (1973), 79-91.

[12] S. Maubach, *Polynomial automorphisms over finite fields*, Serdica Math. J. 27 (2001), 343-350.

[13] J.J. Rotman, *An Introduction to the Theory of Groups*, Springer-Verlag, New York (1995).

[14] R. Wood, *Polynomial maps from spheres to spheres*, Invent. Math. 5 (1968), 163-168.

[15] R. Wood, *Polynomial maps of affine quadrics*, Bull. London Math. Soc. 25 (1993), 491-497.

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

Departamento de Álgebra, Geometría y Topología
Facultad de Ciencias, Universidad de Málaga
Campus Universitario de Teatinos
29071 Málaga, España
e-mail: gomez_ruiz@uma.es