THE GOLOMB TOPOLOGY OF POLYNOMIAL RINGS, II

DARIO SPIRITO

Abstract. We study the interplay of the Golomb topology and the algebraic structure in polynomial rings $K[X]$ over a field K. In particular, we focus on infinite fields K of positive characteristic such that the set of irreducible polynomials of $K[X]$ is dense in the Golomb space $G(K[X])$. We show that, in this case, the characteristic of K is a topological invariant, and that any self-homeomorphism of $G(K[X])$ is the composition of multiplication by a unit and a ring automorphism of $K[X]$.

1. Introduction

Let R be an integral domain, i.e., a commutative unitary ring without zero-divisors. The *Golomb space* $G(R)$ on R is the topological space having $R^\bullet := R \setminus \{0\}$ as its base space and whose topology (the *Golomb topology*) is generated by the cosets $a + I$, where $a \in R$ and I is an ideal such that $a^\bullet$ and I are coprime, i.e., $\langle a, I\rangle = R$. This construction was originally considered on the set $\mathbb{N}$ of natural numbers by Brown [4] and Golomb [7, 8], as part of a series of coset topologies [9], and subsequently extended to arbitrary rings by [5] (following ideas introduced in [1]) with particular focus on what happens when R is a Dedekind domain with infinitely many maximal ideals. In this case, $G(R)$ is a Hausdorff space that is not regular, and is a connected space that is disconnected at each of its points.

An interesting question is how much the topological structure of $G(R)$ reflects the algebraic structure of R: for example, it is an open question whether the fact that $G(R)$ and $G(S)$ are homeomorphic implies that R and S are isomorphic (as rings). Relatedly, one can ask if there are self-homeomorphisms of $G(R)$ besides the one arising from the algebraic structure, i.e., multiplication by units and automorphisims of R (and their compositions).

These problems were studied in [10] for $R = \mathbb{Z}$, showing that the only self-homeomorphisms are the trivial ones (the identity and the multiplication by -1) [10, Theorem 7.7] and that $G(\mathbb{Z}) \simeq G(R)$ cannot happen when $R \neq \mathbb{Z}$ is contained in the algebraic closure of $\mathbb{Q}$ [10, Theorem

Date: September 26, 2022.

2020 *Mathematics Subject Classification.* 54G99; 13F20; 13F05; 12E99.

Key words and phrases. Golomb topology; polynomial rings; Dedekind domains.

7.8]; a variant of its method showed that $\mathbb{N}$, with the Golomb topology, is rigid, i.e., it does not have any nontrivial self-homeomorphism [2]. As a second case, [11] studied the space $G(R)$ when $R = K[X]$ is a polynomial ring over a field K, showing that several algebraic properties of K (for example, having positive or zero characteristic, being algebraically or separably closed) imply different properties on the Golomb space. In particular, it was shown that if K, K' are fields of positive characteristic that are algebraic over their base field, then $G(K[X]) \simeq G(K'[X])$ imply $K \simeq K'$ when one of them is algebraically closed [11, Theorem 5.11 and Corollary 7.2] and when they have the same characteristic [11, Theorem 7.5].

In this paper, we improve these results in two ways. In Section 2, we show that, if the set of irreducible polynomials of $K[X]$ is dense in $G(K[X])$, then the characteristic of K can be detected from the Golomb topology; that is, if K, K' satisfy these hypothesis and $G(K[X]) \simeq G(K'[X])$, then the characteristic of K and K' are equal (Theorem 2.6). As a consequence, we show that if $G(K[X]) \simeq G(K'[X])$ and K is algebraic over $\mathbb{F}_p$, then K and K' must be isomorphic (Theorem 2.7). In Section 3, we concentrate on self-automorphisms of the Golomb space $G(K[X])$ and show that (under the above density hypothesis, and the condition that the characteristic of K is positive) all such self-automorphisms are algebraic in nature, being compositions of a multiplication by a unit and a ring automorphism of $K[X]$ (Theorem 3.9). The key to both results is a variant of the proofs of [1, Lemma 5.10] and [11, Theorem 6.7], which allows to prove that, under appropriate hypothesis, any homeomorphism of Golomb spaces respects powers, i.e., $h(a^n) = h(a)^n$ for every $a \in G(R)$, $n \in \mathbb{N}$.

Throughout the paper, K is a field, and if R is an integral domain then $G(R)$ denotes the Golomb space as defined above. Given a set $X \subseteq R$, we set $X^\bullet := X \setminus \{0\}$. By a "polynomial ring", we always mean a polynomial ring in one variable. We denote by $U(R)$ the set of the units of R, so that $U(K[X]) = K^\bullet$.

If $h : G(R) \longrightarrow G(S)$ is a homeomorphism, then h sends units to units [5, Theorem 13] and prime ideals to prime ideals (i.e., if P is a prime ideal of R, then $h(P^\bullet) \cup \{0\}$ is a prime ideal of S; equivalently, $h(P^\bullet) = Q^\bullet$ for some prime ideal Q of S) [11, Theorem 3.6].

If x is a prime element of R, we set $\mathrm{pow}(x) := \{ux^n \mid u \in U(R), n \in \mathbb{N}\}$. If $h : G(R) \longrightarrow G(S)$ is a homeomorphism, then $h(\mathrm{pow}(x)) = \mathrm{pow}(h(x))$ (see [11, Section 2]).

If P is a prime ideal of R, the *P-topology* on $R \setminus P$ is just the P-adic topology, i.e., the topology having the sets $a + P^n$, for $n \in \mathbb{N}$, as a local basis for a. The P-topology can be recovered from the Golomb topology, and thus, for any prime ideal P of R, a homeomorphism $h : G(R) \longrightarrow G(S)$ restricts to a homeomorphism between $R \setminus P$

endowed with the P-topology and $S \setminus Q$ endowed with the Q-topology (where $h(P^\bullet) = Q^\bullet$) [10, Theorem 4.3].

We say that R is *Dirichlet* if the set of irreducible elements of R is dense, with respect to the Golomb topology. If $R = K[X]$ is Dirichlet, where K is a field, we say for brevity that K itself is Dirichlet. This happens, for example, when K is pseudo-algebraically closed and admits separable irreducible polynomials of arbitrary large degree [3, Theorem A]; in particular, it happens when K is an algebraic extension of a finite field that is not algebraically closed [6, Corollary 11.2.4].

2. Detecting the characteristic

In this section, we show how to detect the characteristic of a polynomial ring from its Golomb topology.

Given an element $t \in R^\bullet$, we denote by σ_t the multiplication by t, i.e.,

$$\begin{aligned} \sigma_t\colon G(R) &\longrightarrow G(R),\\ y &\longmapsto ty. \end{aligned}$$

It is easy to see that the map σ_t is always continuous, and that it is a homeomoprhism if t is a unit of R.

If R is a polynomial ring over a Dirichlet field, and $h : G(R) \longrightarrow G(R)$ is a self-homeomorphism such that $h(P^\bullet) = P^\bullet$ for every prime ideal P, then h must be equal to σ_u for some unit u [11, Proposition 7.4]; this result can be improved in the following way.

Proposition 2.1. *Let R, S be polynomials rings over Dirichlet fields. If $h : G(R) \longrightarrow G(S)$ is a homeomorphism such that $h(1) = 1$, then $h(uz) = h(u)h(z)$ for every $u \in U(R)$ and $z \in R^\bullet$.*

Proof. Let u be a unit of R. Consider the map $h' := h^{-1} \circ \sigma_{h(u)} \circ h$, that is,

$$h'(z) = h^{-1}(h(u)h(z))$$

for every $z \in R^\bullet$. Since u is a unit, so is $h(u)$, and thus $\sigma_{h(u)}$ is a self-homeomorphism of $G(S)$; therefore, h' is a homeomorphism of $G(R)$.

Let now P be a prime ideal of R; then, $h(P^\bullet) = Q^\bullet$ for some prime ideal Q of S. For every $z \in P$, we have $h(u)h(z) \in Q$, and thus $h'(z) = h^{-1}(h(u)h(z)) \in P$. Hence, $h'(P) \subseteq P$, i.e., h fixes every prime ideal of R; by [11, Proposition 7.4], $h' = \sigma_t$ for some unit t of R. However, since $h(1) = 1$,

$$h'(1) = h^{-1}(h(u)h(1)) = h^{-1}(h(u)) = u,$$

and thus it must be $t = u$, i.e., $h'(z) = uz$ for every $z \in R^\bullet$; it follows that, $h(uz) = h(u)h(z)$ for every $z \in R^\bullet$. $\square$

We now want to study the relationship between a homeomorphism of Golomb topologies and powers of elements. For an element $z \in R^\bullet$, we denote by $z^{\mathbb{N}}$ the set of powers of z, i.e., $z^{\mathbb{N}} := \{z^n \mid n \in \mathbb{N}\}$.

Lemma 2.2. *Let R, S be polynomial rings over Dirichlet fields, and let $h : G(R) \longrightarrow G(S)$ be a homeomorphism such that $h(1) = 1$. The set*
$$\mathcal{X}_h := \{z \in R \mid z \text{ is irreducible and } h(z^{\mathbb{N}}) = h(z)^{\mathbb{N}}\}$$
is dense in $G(R)$.

Proof. Let Q be a prime ideal of S, and let P be the prime ideal of R such that $h(P^\bullet) = Q^\bullet$. Then, h restricts to a homeomorphism between the P-topology on $R \setminus P$ and the Q-topology on $S \setminus Q$; it follows that for every $m \in \mathbb{N}$ there is an n such that $h(1 + P^n) \subseteq 1 + Q^m$. Let z be any irreducible element in $1 + P^n$ (which exists since R is Dirichlet); then, for every $t \in \mathbb{N}$, we have $z^t \in 1 + P^n$ too, and thus also $h(z^t) \in 1 + Q^m$. Moreover, $z^t \in \mathrm{pow}(z)$, and thus there are a unit u of S and an integer $\alpha(t)$ such that $h(z^t) = uh(z)^{\alpha(t)}$. Since $U(S) \longrightarrow S/Q$ is injective, it follows that $u = 1$ for every t. Hence, $h(z^{\mathbb{N}}) = h(z)^{\mathbb{N}}$.

Let now $\Omega = c + I$ be a subbasic open set of $G(R)$, and let $d + J$ be a subbasic open set contained in $h(\Omega)$. Let Q be a prime ideal of S that is coprime with J; then, the prime P such that $h(P^\bullet) = Q^\bullet$ is coprime with I. Since R is Dirichlet, $(c + I) \cap (1 + P^n)$ contains irreducible elements for every n; in particular, is n is large enough, every irreducible polynomial in $1 + P^n$ is in $\mathcal{X}_h$, and thus $\mathcal{X}_h \cap (c + I)$ is nonempty. Thus $\mathcal{X}_h$ is dense. $\square$

The following proof follows the one of [11, Theorem 6.8], which in turn was based on the one of [1, Lemma 5.10].

Lemma 2.3. *Let R, S be polynomial rings over Dirichlet fields, and let $h : G(R) \longrightarrow G(S)$ be a homeomorphism such that $h(1) = 1$. For every $a \in R$, we have $h(a^{\mathbb{N}}) = h(a)^{\mathbb{N}}$.*

Proof. If a is a unit, the statement follows from Proposition 2.1. Take any $a \in R$, $a \notin U(R)$, and let $b := h(a)$. We first claim that $h(a^{\mathbb{N}}) \subseteq b^{\mathbb{N}}$. Take any $n \in \mathbb{N}$ and let $f : G(R) \longrightarrow G(R)$ be defined as $f(y) = y^n$, and let $\phi := h \circ f \circ h^{-1}$. Then, $\phi : G(S) \longrightarrow G(S)$ is continuous (since f is continuous) and $\phi(P^\bullet) \subseteq P^\bullet$ for every prime ideal P of R. Let
$$c := \phi(b) = h(f(a)) = h(a^n),$$
and suppose that $c \notin b^{\mathbb{N}}$. Take an integer k such that $\deg b^k > \deg h(a^n) = \deg c$; then, since b and $b^k - 1$ are coprime, so are c and $b^k - 1$ (since c and b belong to the same prime ideals, by [10, Theorem 3.6]), and thus $\Omega := c + (b^k - 1)S$ is an open set. Since ϕ is open, there is a neighborhood $b + dS$ of b such that $\phi(b + dS) \subseteq \Omega$.

By Lemma 2.2, we can find an irreducible polynomial $z \in h^{-1}(b + d(b^k - 1)S)$ such that $h(z^{\mathbb{N}}) = h(z)^{\mathbb{N}}$; setting $y := h(z)$, we have
$$\phi(y) = (h \circ f \circ h^{-1})(h(z)) = h(z^n) = h(z)^l$$
for some integer l. Thus, we have
$$\phi(y) \in \phi(b + dS) \subseteq \Omega = c + (b^k - 1)S$$

and

$$\phi(y) = h(z)^l \in (b + d(b^k - 1)S)^l \subseteq b^l + (b^k - 1)S;$$

hence, $c \equiv b^l \mod (b^k-1)S$. If $l = ik+j$, we have $b^j \equiv b^l \bmod (b^k-1)S$; hence, we have $c \equiv b^j \mod (b^k - 1)S$ for some $0 \leq j < k$. However, by hypothesis, $c \neq b^j$, and the degree of both c and b^j is less than the degree of $b^k - 1$; this is a contradiction, and thus we must have $h(a^{\mathbb{N}}) \subseteq b^{\mathbb{N}}$.

The opposite inclusion is obtained using the homeomorphism h^{-1}. Thus, $h(a^{\mathbb{N}}) = b^{\mathbb{N}} = h(a)^{\mathbb{N}}$, as claimed. □

Lemma 2.4. *Let R be an integral domain. If $U(R)$ is infinite, then its exponent is infinite.*

Proof. Suppose that the exponent of $U(R)$ is finite, say equal to n. Since R is a domain, there can be at most n units of order divisible by n (the roots of $X^n - 1 = 0$); however, this is impossible since $U(R)$ is infinite. Hence, the exponent is infinite. □

Proposition 2.5. *Let R, S be polynomial rings over infinite Dirichlet fields, and let $h : G(R) \longrightarrow G(S)$ be a homeomorphism such that $h(1) = 1$. For every $a \in R$ and every $n \in \mathbb{N}$, we have $h(a^n) = h(a)^n$.*

Proof. If a is a unit the claim follows from Proposition 2.1. Take $a \in R \setminus U(R)$ and $n \in \mathbb{N}$; by Lemma 2.3, we have $h(a^n) = h(a)^s$ for some $s \in \mathbb{N}$. By hypothesis, R has infinitely many units, and thus by Lemma 2.4 there is a unit u whose order is larger than n and s; then, using Proposition 2.1 we have

$$h((ua)^n) = (h(ua))^t = (h(u)h(a))^t = h(u)^t h(a)^t$$

for some t and

$$h((ua)^n) = h(u^n a^n) = h(u^n)h(a^n) = h(u)^n h(a)^s.$$

The equality

$$h(u)^t h(a)^t = h(u)^n h(a)^s$$

can only hold if $n = t = s$; in particular, $n = s$ and $h(a^n) = h(a)^n$, as claimed. □

Theorem 2.6. *Let K, K' be infinite Dirichlet fields. If $G(K[X])$ and $G(K'[X])$ are homeomorphic, then they have the same characteristic.*

Proof. If one of K and K' has characteristic 0, the claim follows from [11, Corollary 4.2]. Suppose thus that $\operatorname{char} K = p$ and $\operatorname{char} K' = q$, with $p, q > 0$.

Let $h : G(K[X]) \longrightarrow G(K'[X])$ be a homeomorphism such that $h(1) = 1$, and let a be an irreducible element. Let f be a factor of $a - 1$. By [11, Proposition 5.5], the sequence a^{p^n} converges to 1 in the (f)-topology, and thus also $h(a^{p^n})$ converges to 1 in the $h((f))$-topology. By Proposition 2.5, $h(a^{p^n}) = h(a)^{p^n}$. By [11, Proposition 5.5], it follows that $v_q(p^n) \longrightarrow \infty$, where v_q is the q-adic valuation; thus, it must be $q = p$. The claim is proved. □

We note that the proof of the previous theorem actually needs only *one* irreducible element a such that $h(a^n) = h(a)^n$ for every n.

Theorem 2.7. *Let K, K' be fields. If K is algebraic over $\mathbb{F}_p$ and $G(K[X]) \simeq G(K'[X])$, then $K \simeq K'$.*

Proof. If K is finite then $|U(K[X])| = |K| - 1$. Since the set of units is preserved by homeomorphisms of the Golomb topology, K and K' must have the same cardinality, and thus they are isomorphic. Suppose K, K' are infinite.

By [11, Corollary 4.2], K' has positive characteristic, and by [11, Corollary 7.2] K' must be algebraic over its base field $\mathbb{F}_q$.

If K is algebraically closed, then the set $G_1(K[X]) := \{z \in K[X] \mid z$ is contained in a unique prime ideal$\}$ is not dense in $G(K[X])$ [11, Proposition 5.2(a)]; conversely, if K is not algebraically closed then $G_1(K[X])$ is dense since it contains the irreducible polynomials. The same holds for K'. Since a homeomorphism of Golomb topologies sends $G_1(K[X])$ to $G_1(K'[X])$ [10, Theorem 3.6(b)], it follows that if K is algebraically closed then so is K', and in this case $p = q$ by [11, Theorem 5.11]; hence $K \simeq K'$.

If K and K' are not algebraically closed, they are pseudo-algebraically closed fields containing separable irreducible polynomials of arbitrarily large degree [3, Theorem A]; by Theorem 2.6, it follows that $p = q$. By [11, Theorem 7.5], it follows that $K \simeq K'$. □

3. Self-homeomorphisms and automorphisms

In this section, we concentrate on the study of self-homeomorphisms of the Golomb space $G(K[X])$. We shall work under the following assumptions:

Hypothesis 3.1.
- K is an infinite field of characteristic $p > 0$;
- $R := K[X]$;
- R is Dirichlet, i.e., the set of irreducible polynomials is dense in $G(R)$;
- $h : G(R) \longrightarrow G(R)$ is a self-homeomorphism such that $h(1) = 1$.

In particular, under these hypothesis, we have $h(a^n) = h(a)^n$ for every $a \in R$ and $n \in \mathbb{N}$, by Proposition 2.5.

Given a set $X \subseteq R$, we define the *p-radical* of X as

$$\mathrm{rad}_p(X) := \{f \in R \mid f^{p^n} \in X \text{ for every large } n\}.$$

This construction is invariant under h, in the following sense.

Lemma 3.2. *Assume Hypothesis 3.1. For every $X \subseteq R^\bullet$, we have* $h(\mathrm{rad}_p(X)) = \mathrm{rad}_p(h(X))$.

Proof. If $f \in \mathrm{rad}_p(X)$, then $f^{p^n} \in X$ for every $n \geq N$, and thus $h(f^{p^n}) \in h(X)$. By Proposition 2.5, it follows that $h(f)^{p^n} \in h(X)$ for $n \geq N$, and thus $h(f) \in \mathrm{rad}_p(h(X))$. Conversely, if $g = h(f) \in \mathrm{rad}_p(h(X))$, then $g^n = h(f)^{p^n} = h(f^{p^n})$ belongs to $h(X)$ for large n, and thus applying h^{-1} we have $f^{p^n} \in X$ for large n. Thus $f \in \mathrm{rad}_p(X)$ and $g \in h(\mathrm{rad}_p(X))$. □

Lemma 3.3. *Let P a prime ideal of a ring R of characteristic p. For every $m \in \mathbb{N}^+$, we have* $\mathrm{rad}_p(1 + P^m) = 1 + P$.

Proof. If $t \in 1 + P$, then $t = 1 + x$ with $x \in P$; if $p^n \geq m$, then $t^{p^n} = (1 + x)^{p^n} = 1 + x^{p^n} \in 1 + P^m$, and thus $t \in \mathrm{rad}_p(1 + P^m)$. Conversely, if $t \in \mathrm{rad}_p(1 + P^m)$ then $t^{p^n} \in 1 + P^m$ for some m; in particular, $t^{p^n} \in 1 + P$, and thus $t^{p^n} - 1 = (t - 1)^{p^n} \in P$. Hence $t - 1 \in P$, i.e., $t \in 1 + P$. □

Proposition 3.4. *Assume Hypothesis 3.1, and let P, Q be prime ideals of R with $h(P^\bullet) = Q^\bullet$. Then, $h(1 + P) = 1 + Q$.*

Proof. Since $h(1) = 1$, $h(1 + P)$ is open in the Q-topology, and thus $1 + Q^m \subseteq h(1 + P)$ for some m. Therefore,

$$1 + Q = \mathrm{rad}_p(1 + Q^m) \subseteq \mathrm{rad}_p(h(1 + P)) = h(\mathrm{rad}_p(1 + P)) = h(1 + P)$$

using Lemmas 3.2 and 3.3. Applying the same reasoning to h^{-1} gives $1 + P \subseteq h^{-1}(1 + Q)$, i.e., $h(1 + P) \subseteq 1 + Q$. Hence, $h(1 + P) = 1 + Q$, as claimed. □

Corollary 3.5. *Assume Hypothesis 3.1,and let P, Q be prime ideals of R with $h(P^\bullet) = Q^\bullet$. If $u \in K^\bullet$, then $h(u+P) = h(u)+Q$. In particular, if $f \equiv u \bmod P$ for some unit u, then $h(f) \equiv h(u) \bmod Q$.*

Proof. By Propositions 2.1, we have $u + P = u(1 + P)$; by Proposition 3.4, it follows that

$$h(u + P) = h(u)h(1 + P) = h(u)(1 + Q) = h(u) + Q,$$

as claimed. The “in particular” statement follows from the fact that $f \equiv u \bmod P$ is equivalent to $f \in u + P$. □

Corollary 3.6. *Assume Hypothesis 3.1. If f is a linear polynomial, so is $h(f)$.*

Proof. Since f is linear, (f) is prime and every polynomial $g \notin (f)$ is equivalent to a unit modulo (f). By Corollary 3.5, it follows that every $g \notin (h(f))$ is equivalent to a unit modulo $(h(f))$; hence, $h(f)$ must be linear too. □

In particular, by Corollary 3.6, $h(X)$ is a linear polynomial; it follows that there is an automorphism σ of R sending $h(X)$ to h. Since σ restricts to a self-homeomorphism of $G(R)$, passing from h to $H := \sigma\circ h$ we obtain a self-homeomorphism of $G(R)$ that fixes both 1 and X. Thus, it is not restrictive to assume also that $h(X) = X$, as we do in the remaining part of the section.

Lemma 3.7. *Assume Hypothesis 3.1 and suppose $h(X) = X$. For every $u \in K^\bullet$, we have $h(X + u) = X + h(u)$.*

Proof. We have

$$\begin{cases} X + u \equiv u \bmod (X) \\ X \equiv -u \bmod (X + u). \end{cases}$$

Applying h to both equivalences, using $h(X) = X$ and Corollary 3.5, we have

$$\begin{cases} h(X + u) \equiv h(u) \bmod (X) \\ X \equiv -h(u) \bmod (h(X + u)). \end{cases}$$

The first equation implies that X divides $h(X+u)-h(u)$; since $h(X+u)$ is linear, it follows that $h(X + u) = vX + h(u)$ for some $v \in K^\bullet$. The second equation implies that $vX + h(u)$ divides $X + h(u)$; the only possibility is $v = 1$, i.e., $h(X+u) = X+h(u)$. The claim is proved. □

Lemma 3.8. *Assume Hypothesis 3.1 and suppose $h(X) = X$. Then, the map*

$$H\colon K \longrightarrow K,$$

$$a \longmapsto \begin{cases} h(a) & \text{if } a \neq 0 \\ 0 & \text{if } a = 0 \end{cases}$$

is an automorphism of K.

Proof. Let $a, b \in K$. If $a = 0$ or $b = 0$ then clearly $H(ab) = H(a)H(b)$ and $H(a + b) = H(a) + H(b)$.

Suppose $a \neq 0 \neq b$. Then, $H = h$ on these values, and $h(ab) = h(a)h(b)$ by Proposition 2.1. Furthermore,

$$X + a + b \equiv b \bmod (X + a);$$

applying h and using Lemma 3.7, we have

$$X + h(a + b) \equiv h(b) \bmod (X + h(a)),$$

that is, $X + h(a)$ divides $X + h(a + b) - h(b)$. Thus, it must be $X + h(a) = X + h(a + b) - h(b)$ and $h(a) = h(a + b) - h(b)$, that is, $h(a) + h(b) = h(a + b)$. It follows that H is an automorphism of K, as claimed. □

Theorem 3.9. *Let K is an infinite Dirichlet field of positive characteristic, and let h be a self-homeomorphism of $G(K[X])$. Then, there are a unit $u \in K^\bullet$ and an automorphism σ of $K[X]$ such that $h(f) = u\sigma(f)$ for every $f \in K[X]^\bullet$.*

Proof. By [5, Theorem 13], $h(1) = u$ is a unit of R; since the multiplication σ_u is a self-homeomorphism of $G(R)$, the map $h_1 := \sigma_u^{-1} \circ h$ is a self-homeomorphism such that $h_1(1) = 1$.

By Corollary 3.6, $h_1(X)$ is a linear polynomial, and thus there is an automorphism σ_1 of R such that $h_1(X) = \sigma_1(X)$. Thus, $h_2 := \sigma_1^{-1} \circ h_1$ is again a self-homeomorphism of $G(R)$, and furthermore both 1 and X are fixed points of h_2.

By Lemma 3.8, the restriction of h_2 to K is an automorphism H; this map can be extended to an automorphism σ_2 of R by setting $\sigma_2\left(\sum_i a_i X^i\right) = \sum_i H(a_i)X^i$. Thus, $h_3 := \sigma_2^{-1} \circ h_2$ is a self-homeomorphism of $G(R)$ such that $h_3(u) = u$ for every $u \in K^\bullet$ and $h_3(X) = X$. By Lemma 3.7, it follows that $h_3(X + u) = X + u$ for every $u \in K^\bullet$.

Let now $f \in R$, and take any $t \in K$. Then,

$$\begin{cases} f \equiv f(t) \bmod (X - t) \\ h_3(f) \equiv h_3(f)(t) \bmod (X - t). \end{cases}$$

Since $h_3((X - t)) = (X - t)$, by Corollary 3.5 the first equivalence also implies $h_3(f) \equiv h_3(f(t)) \bmod (X - t)$. Hence, $h_3(f)(t) = h_3(f(t)) = f(t)$. Since this happens for every $t \in K$, and K is infinite, it follows that $f = h_3(f)$, that is, h_3 is the identity on $G(R)$.

Going back to the definition,

$$h_3 = \sigma_2^{-1} \circ h_2 = \sigma_2^{-1} \circ \sigma_1^{-1} \circ h_1 = \sigma_2^{-1} \circ \sigma_1^{-1} \circ \sigma_u^{-1} \circ h,$$

i.e., $h = \sigma_u \circ \sigma_1 \circ \sigma_2$. Since $\sigma_u(x) = ux$ for every x, setting $\sigma := \sigma_1 \circ \sigma_2$ (which is still an automorphism of R), we obtain $h(f) = u\sigma(f)$ for every $f \in G(R)$, as claimed. $\square$

References

[1] Taras Banakh, Jerzy Mioduszewski, and Sławomir Turek. On continuous self-maps and homeomorphisms of the Golomb space. *Comment. Math. Univ. Carolin.*, 59(4):423–442, 2018.

[2] Taras Banakh, Dario Spirito, and Sł awomir Turek. The Golomb space is topologically rigid. *Comment. Math. Univ. Carolin.*, 62(3):347–360, 2021.

[3] Lior Bary-Soroker. Dirichlet's theorem for polynomial rings. *Proc. Amer. Math. Soc.*, 137(1):73–83, 2009.

[4] Morton Brown. A countable connected Hausdorff space. In L.W. Cohen, editor, *The April meeting in New York*, volume 4, pages 330–371. Bull. Amer. Math. Soc., 1953. Abstract 423.

[5] Pete L. Clark, Noah Lebowitz-Lockard, and Paul Pollack. A note on Golomb topologies. *Quaest. Math.*, 42(1):73–86, 2019.

[6] Michael D. Fried and Moshe Jarden. *Field arithmetic*, volume 11 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]*. Springer-Verlag, Berlin, second edition, 2005.

[7] Solomon W. Golomb. A connected topology for the integers. *Amer. Math. Monthly*, 66:663–665, 1959.

[8] Solomon W. Golomb. Arithmetica topologica. In *General Topology and its Relations to Modern Analysis and Algebra (Proc. Sympos., Prague, 1961)*, pages 179–186. Academic Press, New York; Publ. House Czech. Acad. Sci., Prague, 1962.
[9] John Knopfmacher and Stefan Porubsky. Topologies related to arithmetical properties of integral domains. *Exposition. Math.*, 15(2):131–148, 1997.
[10] Dario Spirito. The Golomb topology on a Dedekind domain and the group of units of its quotients. *Topology Appl.*, 273:107101, 20, 2020.
[11] Dario Spirito. The Golomb topology of polynomial rings. *Quaest. Math.*, 44(4):447–468, 2021.

Dipartimento di Scienze Matematiche, Informatiche e Fisiche, Università degli Studi di Udine, Udine, Italy
Email address: `dario.spirito@uniud.it`