Topology and its Applications 273 (2020) 107101

Contents lists available at ScienceDirect

Topology and its Applications

www.elsevier.com/locate/topol

The Golomb topology on a Dedekind domain and the group of units of its quotients

Dario Spirito

Dipartimento di Matematica e Fisica, Università degli Studi "Roma Tre", Roma, Italy

ARTICLE INFO

Article history:
Received 1 July 2019
Received in revised form 21 January 2020
Accepted 2 February 2020
Available online 5 February 2020

MSC:
54G99
54A10
11A07
13F05

Keywords:
Golomb space
Dedekind domains
Homeomorphism problem

ABSTRACT

We study the Golomb spaces of Dedekind domains with torsion class group. In particular, we show that a homeomorphism between two such spaces sends prime ideals into prime ideals and preserves the P-adic topology on $R \setminus P$. Under certain hypothesis, we show that we can associate to a prime ideal P of R a partially ordered set, constructed from some subgroups of the group of units of R/P^n, which is invariant under homeomorphisms, and use this result to show that the unique self-homeomorphisms of the Golomb space of $\mathbb{Z}$ are the identity and the multiplication by -1. We also show that the Golomb space of any Dedekind domain contained in the algebraic closure of $\mathbb{Q}$ and different from $\mathbb{Z}$ is not homeomorphic to the Golomb space of $\mathbb{Z}$.

1. Introduction

Let R be an integral domain. The *Golomb topology* of R is the topology on $R^\bullet := R \setminus \{0\}$ generated by the coprime cosets; we denote by $G(R)$ the space $R^\bullet$ endowed with this topology, and call it the *Golomb space* of R. The Golomb topology on the set $\mathbb{Z}^+$ of positive integer was introduced by Brown [5] and subsequently studied by Golomb [13,14]. On general domains, the Golomb topology was considered alongside several other coset topologies (see for example [15]), and was shown to provide a way to generalize Furstenberg's "topological" proof of the infinitude of primes in a more general context [11,6]. See [7, Section 4] for a more detailed historical overview of the subject.

Two recent articles have shed more light on the Golomb topology. The first one, due to Banakh, Mioduszewski and Turek [3], deals with the "classical" subject of the Golomb topology on $\mathbb{Z}^+$, with the explicit goal of deciding if this space is *rigid*, i.e., if it does not admit any self-homeomorphism; in particular, they show that any self-homeomorphism of this space fixes 1 [3, Theorem 5.1]. The second one, due to Clark,

E-mail address: spirito@mat.uniroma3.it.

https://doi.org/10.1016/j.topol.2020.107101
0166-8641/

Lebowitz-Lockard and Pollack [7], studies Golomb spaces on general domains, in particular when the ring R is a Dedekind domain with infinitely many maximal ideals: under this hypothesis, they show that $G(R)$ is a Hausdorff space that is not regular, and that it is a connected space that is totally disconnected at each of its points. They also raise the *isomorphism problem*: can two nonisomorphic Dedekind domains with infinitely many maximal ideals (or, more generally, two integral domains with zero Jacobson radical) have homeomorphic Golomb spaces? As a first step in this study, they prove that any homeomorphism of Golomb topologies sends units to units [7, Theorem 13], and thus that two domains with a different number of units have nonhomeomorphic Golomb spaces. We note that the rigidity problem and the isomorphism problem can be unified into a single question:

Problem. Let R, S be two Dedekind domains with infinitely many maximal ideals, and let $h : G(R) \longrightarrow G(S)$ be a homeomorphism. Is it true that there is a ring isomorphism $\sigma : R \longrightarrow S$ and a unit $u \in S$ such that $h(x) = u\sigma(x)$ for all $x \in R$?

In this paper, we show that the only self-homeomorphisms of the Golomb space $G(\mathbb{Z})$ are the identity and the multiplication by -1 (Theorem 7.7), and that if R is a Dedekind domain contained in the algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ such that $G(\mathbb{Z}) \simeq G(R)$ then $R = \mathbb{Z}$, thus giving a complete answer to the above question for $R = S = \mathbb{Z}$ and a partial answer for $R = \mathbb{Z}$. While the method we use works best for the ring of integers, we work as much as possible in a greater generality: the main restrictions we have to put (especially in Sections 6 and 7) are that the class group of the Dedekind domain we consider must be torsion, and that some quotients of the group of units of R/P^n are cyclic.

The structure of the paper is as follows. In Section 3, we generalize [3, Lemma 5.6] to the case of general Dedekind domains; in particular, we show that the partially ordered set $\boldsymbol{\mathcal{V}}(R)$ formed by the subsets of $\operatorname{Max}(R)$ that can be written as $V(x) := \{M \in \operatorname{Max}(R) \mid x \in M\}$ for some $x \in R^\bullet$ is a topological invariant of the Golomb topology (Proposition 3.3). Through this result, we prove that if $G(R) \simeq G(S)$ then the class groups of R and S are either both torsion or both non-torsion (Theorem 3.4) and, if they are torsion, then a homeomorphism between $G(R)$ and $G(S)$ sends prime ideals to prime ideals and radical ideals to radical ideals.

In Section 4, given a prime ideal P of R, we show how to construct from the Golomb topology a new topology on $R \setminus P$ (the *P-topology*), which allows to concentrate on the cosets in the form $a + P^n$. Section 5 collects some results about the groups $H_n(P) := U(R/P^n)/\pi_n(U(R))$.

In Section 6, we study the sets $\operatorname{pow}(a) := \{ua^n \mid u \in U(R)\}$ of powers of the elements $a \in R \setminus P$, and in particular their closure in the P-topology. We relate this closure to the cyclic subgroups of the groups $H_n(P)$; in particular, we show that under some hypothesis (among which that R has torsion class group and that the $H_n(P)$ are cyclic) the closure of $\operatorname{pow}(a)$ is characterized by the index of the subgroup generated by a in $H_n(P)$ for large n. Restricting to almost prime elements (i.e., irreducible elements generating a primary ideal) we show that there is a bijective correspondence between these closures and a set of integers depending on the cardinality of the $H_n(P)$ (Theorem 6.12), and that this structure is preserved under homeomorphisms of Golomb spaces (Propositions 6.5 and 6.14). In Section 7, we make this correspondence explicit enough to characterize completely the self-homeomorphisms of $G(\mathbb{Z})$ (Theorem 7.7).

2. Dedekind domains and the Golomb topology

All unreferenced statements about Dedekind domains are standard; see for example [4, Chapter 7, §2], [2, Chapter 9] or [16, Chapter 1].

Throughout the paper, R will a Dedekind domain, that is, R is a commutative unitary ring with no zerodivisors, and such that every ideal can be written (uniquely) as a product of prime ideals. Equivalently, R is a Dedekind domain if it has no zerodivisors, it is Noetherian (its ideals satisfy the ascending chain condition), one-dimensional (all its nonzero prime ideals are maximal) and integrally closed (if $p(X)$ is a

monic polynomial, then every root of $p(X)$ in the quotient field of R belongs to R). Examples of Dedekind domains are $\mathbb{Z}$, the ring of integers of a number field F and the polynomial ring $K[X]$ over a field K.

For every subset $I \subseteq R$, we set $I^\bullet := I \setminus \{0\}$, and we denote by $U(R)$ the set of units of R.

We denote by $\mathrm{Max}(R)$ the set of maximal ideals of R; if $x \in R^\bullet$, we set $V(x) := \{M \in \mathrm{Max}(R) \mid x \in M\}$; this set is always finite. If I is an ideal of R, the *radical* of I is

$$\mathrm{rad}(I) := \{x \in R \mid x^n \in I \text{ for some } n \in \mathbb{N}\}.$$

The radical of I is an ideal and is also the intersection of all prime ideals containing I. If I is contained in a unique maximal ideal P, then I is called a *primary ideal* (or *P-primary ideal* if we want to underline P); note that this definition is *not* the general definition of a primary ideal, but it is equivalent for a nonzero ideal of a Dedekind domain.

An R-submodule J of the quotient field of R is a *fractional ideal* of R if there is a $d \in R^\bullet$ such that $dJ \subseteq R$ (in particular, dJ is an ideal of R). The set $\mathcal{F}(R)$ of nonzero fractional ideals of R is an abelian group under the product of ideals. The nonzero principal ideals of R form a subgroup $\mathcal{P}(R)$ of $\mathcal{F}(R)$; the quotient $\mathcal{F}(R)/\mathcal{P}(R)$ is called the *class group* (or *ideal class group*) of R, and is denoted by $\mathrm{Cl}(R)$. The class group of R is trivial if and only if R is a unique factorization domain.

Let $I \neq (0)$ be an ideal of R, and let $a \in R$. The coset $a + I$ is a *coprime coset* if $\langle a, I\rangle = R$, i.e., if there is no proper ideal containing both a and I. In particular, any coprime coset is contained in $R^\bullet$. Likewise, two nonzero ideals I and J are *coprime* if $\langle I, J\rangle = R$, i.e., if there is no proper ideal containing both I and J.

The *Golomb topology* on $R^\bullet$ is the topology generated by all coprime cosets $a+I$. We denote by $G(R)$ the set $R^\bullet$ endowed with the Golomb topology, and we call it the *Golomb space* of R. For $X \subseteq R^\bullet$, we denote by $\overline{X}$ the closure of X in the Golomb topology. If R has infinitely many maximal ideals, the Golomb space is an Hausdorff space that is not regular; furthermore, it is not compact and is totally disconnected [7].

The closure of the coprime cosets can be completely described.

Lemma 2.1. *([7, Lemma 15]) Let R be a Dedekind domain, let I be a nonzero ideal of R and let $x \in R^\bullet$ be such that $\langle x, I\rangle = R$. Let $I = P_1^{e_1} \cdots P_n^{e_n}$ be the factorization of I into prime ideals. Then,*

$$\overline{x + I} = \left(\bigcap_{i=1}^{n} P_i \cup (x + P_i^{e_i})\right)^\bullet.$$

In particular, we immediately obtain the following.

Corollary 2.2. *Let R be a Dedekind domain, and let I, J be coprime ideals. For every x such that $\langle x, I\rangle = \langle x, J\rangle = R$, we have $\overline{x + IJ} = \overline{x + I} \cap \overline{x + J}$.*

3. Radical and prime ideals

The purpose of this section is to generalize the results obtained in [3, Section 5] on the relationship between the Golomb topology and the prime divisors of an element $x \in R^\bullet$. Following the methods used therein, we define $\mathcal{F}_x$ as the set of all $F \subseteq R^\bullet$ such that there are a neighborhood U_x of x and a neighborhood U_1 of 1 such that $\overline{U_x} \cap \overline{U_1} \subseteq F$.

Part (b) of the following proposition corresponds to [3, Lemma 5.5(a)], while part (c) corresponds to [3, Lemma 5.6].

Proposition 3.1. *Let R be a Dedekind domain. Let $x, y \in R^\bullet$ and let $M \in \mathrm{Max}(R)$. Then, the following hold.*

(a) $\mathcal{F}_x$ *is a filter.*
(b) $M^\bullet \in \mathcal{F}_x$ *if and only if* $x \notin M$.
(c) $\mathcal{F}_x \subseteq \mathcal{F}_y$ *if and only if* $V(y) \subseteq V(x)$.

Proof. (a) By the proof of [7, Theorem 8(a)] (and the discussion in Section 3 therein), for every open sets $V_1, \dots, V_n$ the intersection $\overline{V_1} \cap \dots \cap \overline{V_n}$ is nonempty; the claim follows.

(b) is a direct consequence of [7, Lemma 17], applied with $y = 1$.

(c) Suppose $\mathcal{F}_x \subseteq \mathcal{F}_y$, and let $P \in V(y)$. Then, $y \in P$, so by point (b) $P \notin \mathcal{F}_y$; hence, $P \notin \mathcal{F}_x$ and thus again $x \in P$, i.e., $P \in V_x$.

Conversely, suppose $V(y) \subseteq V(x)$. Let $F \in \mathcal{F}_x$; then, there are ideals I, J of R such that $\langle x, I\rangle = R$ and such that $\overline{x+I} \cap \overline{1+J} \subseteq F$. Without loss of generality, we can suppose that $J \subseteq I$ and that $J = IJ'$ for some J' such that $\langle I, J'\rangle = R$. Let $I = \prod_i P_i^{e_i}$ be the prime decomposition of I; by Corollary 2.2, we have

$$\begin{aligned}\overline{x+I} \cap \overline{1+J} =& \overline{x+I} \cap \overline{1+I} \cap \overline{1+J'} = \\ =& \bigcap_i \overline{x+P_i^{e_i}} \cap \overline{1+P_i^{e_i}} \cap \overline{1+J'}.\end{aligned}$$

For each i, let n_i be an integer such that $y - 1 \notin P_i^{n_i e_i}$. Then, by Lemma 2.1,

$$\overline{y+P_i^{n_i e_i}} \cap \overline{1+P_i^{n_i e_i}} = ((y+P_i^{n_i e_i}) \cup P_i)^\bullet \cap ((1+P_i^{n_i e_i}) \cup P_i)^\bullet = P_i^\bullet.$$

Let $I' := \prod_i P_i^{e_i n_i}$: then,

$$\begin{aligned}\overline{y+I'} \cap \overline{1+I'} =& \bigcap_i \overline{y+P_i^{n_i e_i}} \cap \overline{1+P_i^{n_i e_i}} = \left(\bigcap_i P_i\right)^\bullet \subseteq \\ \subseteq& \bigcap_i \overline{x+P_i^{e_i}} \cap \overline{1+P_i^{e_i}} = \\ =& \overline{x+I'} \cap \overline{1+I'} \subseteq \overline{x+I} \cap \overline{1+I},\end{aligned}$$

and thus

$$\overline{y+I'} \cap \overline{1+I'J'} = \overline{y+I'} \cap \overline{1+I'} \cap \overline{1+J'} \subseteq \overline{x+I} \cap \overline{1+I} \cap \overline{1+J'} \subseteq F.$$

Since the radical of I and I' is the same and $\langle x, I\rangle = R$, also $\langle x, I'\rangle = R$; since $V(y) \subseteq V(x)$, we have $\langle y, I'\rangle = R$, and thus $y + I'$ is an open neighborhood of y. Hence, $F \in \mathcal{F}_y$ and thus $\mathcal{F}_x \subseteq \mathcal{F}_y$, as claimed. □

Let R be a Dedekind domain. We consider two sets associated to R:

$$\boldsymbol{\mathcal{F}}(R) := \{\mathcal{F}_x \mid x \in R^\bullet\}$$

and

$$\boldsymbol{\mathcal{V}}(R) := \{V(x) \mid x \in R^\bullet\}.$$

The previous proposition establishes a relation between them.

Proposition 3.2. *Let R be a Dedekind domain. The map*

$$\begin{aligned}\Psi \colon \boldsymbol{\mathcal{F}}(R) &\longrightarrow \boldsymbol{\mathcal{V}}(R), \\ \mathcal{F}_x &\longmapsto V(x)\end{aligned}$$

is well-defined and an anti-isomorphism (when $\boldsymbol{\mathcal{F}}(R)$ and $\boldsymbol{\mathcal{V}}(R)$ are endowed with the containment order).

Proof. Proposition 3.1(c) guarantees that Ψ is well-defined, injective and order-reversing, while the surjectivity is obvious. □

Proposition 3.3. *Let R, S be Dedekind domains and $h : G(R) \longrightarrow G(S)$ be a homeomorphism. Then, the following hold.*

(a) *If $h(1) = 1$, then $h(\mathcal{F}_x) = \mathcal{F}_{h(x)}$ for every $x \in R^\bullet$.*
(b) *h induces an order isomorphism*

$$\begin{aligned} \overline{h}\colon \boldsymbol{\mathcal{V}}(R) &\longrightarrow \boldsymbol{\mathcal{V}}(S), \\ V(x) &\longmapsto V(h(x)). \end{aligned}$$

Proof. (a) Since h is a homeomorphism and $h(1) = 1$, h sends neighborhoods of x into neighborhoods of $h(x)$, and neighborhoods of 1 into neighborhoods of 1, and analogously for their closures. The claim follows by the definition of $\mathcal{F}_x$.

(b) For every unit v of S, let $\psi_v : G(S) \longrightarrow G(S)$ be the multiplication by v. Clearly, ψ_v is a self-homeomorphism of $G(S)$.

Let $u := h(1)$. By [7, Theorem 13], u is a unit of S, and thus ψ_u is a self-homeomorphism of $G(S)$. Then, $h = \psi_u \circ \psi_{u^{-1}} \circ h$; setting $h' := \psi_{u^{-1}} \circ h$, it is enough to show the claim separately for ψ_u and for h'.

For every $y \in S^\bullet$, $V(uy) = V(y)$; hence, the map

$$\begin{aligned} \widetilde{\psi_u}\colon \boldsymbol{\mathcal{F}}(S) &\longrightarrow \boldsymbol{\mathcal{F}}(S), \\ \mathcal{F}_x &\longmapsto \mathcal{F}_{ux} \end{aligned}$$

is the identity, and in particular it is an order isomorphism. Then, if Ψ is the map of Proposition 3.2, we have that $\Psi \circ \widetilde{\psi_u} \circ \Psi^{-1}$ is an order-isomorphism of $\boldsymbol{\mathcal{V}}(S)$ with itself; unraveling the definition we see that $\overline{\psi_u} = \Psi \circ \widetilde{\psi_u} \circ \Psi^{-1}$, and the claim is proved.

Consider now h'. Then, $h'(1) = u^{-1}h(1) = 1$. By the previous point, $h'(\mathcal{F}_x) = \mathcal{F}_{h'(x)}$; hence, by Proposition 3.1(c), the map

$$\begin{aligned} \widetilde{h'}\colon \boldsymbol{\mathcal{F}}(R) &\longrightarrow \boldsymbol{\mathcal{F}}(R), \\ \mathcal{F}_x &\longmapsto \mathcal{F}_{h'(x)} \end{aligned}$$

is well-defined and an order-isomorphism. As before, we see that $\overline{h'} = \Psi \circ \widetilde{h'} \circ \Psi^{-1}$ and that the right hand side is an order-isomorphism between $\boldsymbol{\mathcal{V}}(R)$ and $\boldsymbol{\mathcal{V}}(S)$, and the claim is proved. □

Since any nonzero element of a Dedekind domain is contained in only finitely many maximal ideals, $\boldsymbol{\mathcal{V}}(R)$ is always a subset of $\mathcal{P}_{\text{fin}}(\text{Max}(R))$, the set of nonzero finite subsets of $\text{Max}(R)$; the two sets are equal if and only if the class group of R is torsion (this is essentially proved in [12, Proposition 3.1]). Indeed, if $\text{Cl}(R)$ is torsion then every nonzero prime ideal P contains an element x_P such that $V(x_P) = \{P\}$, and thus, if $P_1, \dots, P_n$ are nonzero prime ideals then $\{P_1, \dots, P_n\} = V(x_{P_1} \cdots x_{P_n})$. Conversely, if $\text{Cl}(R)$ is not torsion then there is a prime ideal P such that P^k is not principal for every k, and thus $V(x) \neq \{P\}$ for every $x \in R^\bullet$, so $\boldsymbol{\mathcal{V}}(R) \neq \mathcal{P}_{\text{fin}}(\text{Max}(R))$. We can upgrade this difference.

Theorem 3.4. *Let R, S be Dedekind domains such that $G(R)$ and $G(S)$ are homeomorphic. Then, the class group of R is torsion if and only if the class group of S is torsion.*

Proof. Suppose that the class group of R is torsion while the class group of S is not, and let $\mathcal{M}(R)$ (respectively, $\mathcal{M}(S)$) be the set of minimal elements of $\boldsymbol{\mathcal{V}}(R)$ (resp., $\boldsymbol{\mathcal{V}}(S)$).

Since $\mathrm{Cl}(R)$ is torsion, by the reasoning above every member of $\mathcal{M}(R)$ is a singleton; therefore, if $\Delta \subseteq \mathcal{M}(R)$ is finite, say $\Delta = \{\{P_1\}, \dots, \{P_n\}\}$, then $\sup \Delta$ exists and is equal to $\{P_1, \dots, P_n\}$. In particular, $\sup \Delta \neq \sup \Lambda$ for every finite $\Delta \neq \Lambda$.

We claim that this does not hold in $\boldsymbol{\mathcal{V}}(S)$. Indeed, since the class group of S is not torsion there is a maximal ideal P such that no power of P is principal. Let $x \in P \setminus P^2$: then, $xR = PA$ for some ideal A coprime with P. By the approximation theorem for Dedekind domains (see e.g. [4, Chapter 7, §2, Proposition 2]), we can find a $y \in P \setminus P^2$ that is not contained in any prime ideal containing A; then, $yR = PB$ for some ideal B, and by construction B must be coprime with P and A. Since PA and PB are both principal, the classes of A and B in the class group are the same (more precisely, they are both the inverse of the class of P).

Take $b \in P \setminus P^2$: then, $bR = PC$ for some ideal C coprime with P. Again by the approximation theorem, we can choose $c \in C$ such that $c \notin P$ and such that $c \notin CQ$ for every prime ideal Q containing A or B: then, $H := b^{-1}cP$ is a proper ideal of R that is coprime with P, A and B and such that H is in the same class of P. Therefore, HA and HB are principal, say $HA = zR$ and $HB = wR$. Then, $xwR = PAHB = PBHA = yzR$, and in particular $V(xw) = V(yz)$. Let $\mathcal{M}(x)$ be the set of minimal elements of $\boldsymbol{\mathcal{V}}(R)$ containing $V(x)$, and likewise define $\mathcal{M}(y)$, $\mathcal{M}(z)$ and $\mathcal{M}(w)$; then, $\sup(\mathcal{M}(x) \cup \mathcal{M}(w)) = V(x) \cup V(w) = V(xw) = V(yz) = \sup(\mathcal{M}(y) \cup \mathcal{M}(z))$. We claim that $\mathcal{M}(x) \cup \mathcal{M}(w) \neq \mathcal{M}(y) \cup \mathcal{M}(z)$.

There is an element of $\mathcal{M}(x)$ containing P: since the class of P is not torsion, such element cannot be $\{P\}$, and thus it must be equal to $\Theta := \{P, Q_1, \dots, Q_n\}$ for some prime ideals $Q_1, \dots, Q_n$ containing A. Since $z \notin P$, no element of $\mathcal{M}(z)$ contains P, and in particular $\Theta \notin \mathcal{M}(z)$. If $\Theta' \in \mathcal{M}(y)$ contains P then $\Theta' = \{P, L_1, \dots, L_m\}$ for some prime ideals $L_1, \dots, L_m$ containing B; since A and B are coprime, each Q_i is different from each L_j, and thus $\Theta' \neq \Theta$, and so $\Theta \notin \mathcal{M}(y)$. Hence, there are finite subsets $\Delta \neq \Lambda$ of $\mathcal{M}(S)$ such that $\sup \Delta = \sup \Lambda$; since this property is purely order-theoretic, it follows that $\boldsymbol{\mathcal{V}}(R)$ and $\boldsymbol{\mathcal{V}}(S)$ are not isomorphic. By Proposition 3.3(a), neither $G(R)$ and $G(S)$ are homeomorphic. □

It would be interesting to know how much further this method can be pushed: for example, is it possible to recover the rank of the class group of R from the order structure of $\boldsymbol{\mathcal{V}}(R)$?

We now consider more in detail the case where the class group of R is torsion. Given $\Delta \subseteq \mathrm{Max}(R)$, we define

$$G_\Delta(R) := \{x \in R^\bullet \mid V(x) = \Delta\}.$$

By the discussion before Theorem 3.4, if $\mathrm{Cl}(R)$ is torsion then $G_\Delta(R) \neq \emptyset$ for every finite $\Delta \subseteq \mathrm{Max}(R)$.

The following is an analogue of [3, Lemmas 5.8 and 5.9].

Proposition 3.5. *Let R, S be Dedekind domains with torsion class group, and let $h : G(R) \longrightarrow G(S)$ be a homeomorphism. Then, there is a bijection $\sigma : \mathrm{Max}(R) \longrightarrow \mathrm{Max}(S)$ such that $h(G_\Delta(R)) = G_{\sigma(\Delta)}(S)$.*

Proof. By [7, Theorem 13], $h(1)$ is a unit of S. The multiplication by u is a homeomorphism of S which sends every $G_\Lambda(S)$ into itself; hence, passing to $h' : G(R) \longrightarrow G(S)$, $x \mapsto h(1)^{-1}h(x)$, we can suppose without loss of generality that $h(1) = 1$.

We claim that $|V(x)| = |V(h(x))|$ for every $x \in R^\bullet$. Indeed, since $\mathrm{Cl}(R)$ is torsion $\boldsymbol{\mathcal{V}}(R) \simeq \mathcal{P}_{\mathrm{fin}}(\mathrm{Max}(R))$, and thus $|V(x)|$ is equal to 1 plus the length of a descending chain of $\boldsymbol{\mathcal{V}}(R)$ starting from $V(x)$. By Proposition 3.3(b), this property passes to $\boldsymbol{\mathcal{V}}(S)$, and thus $|V(x)| = |V(h(x))|$.

Let $\overline{\sigma}$ be the restriction to $\mathcal{M}(R)$ (the set of minimal elements of $\boldsymbol{\mathcal{V}}(R)$) of the isomorphism $\overline{h}$ of Proposition 3.3(b). Since $\mathcal{M}(R)$ is in natural bijective correspondence with $\mathrm{Max}(R)$ (just send $\{P\}$ into P) we

get a bijection $\sigma : \mathrm{Max}(R) \longrightarrow \mathrm{Max}(S)$, such that if $P \in \mathrm{Max}(R)$ and xR is P-primary then $\sigma(P)$ is the unique maximal ideal of S containing $h(x)$.

If now $x \in G_\Delta(R)$, then $\Delta = \{P \in \mathrm{Max}(R) \mid P \notin \mathcal{F}_x\}$; hence, $\sigma(\Delta) = \{Q \in \mathrm{Max}(S) \mid Q \notin \mathcal{F}_{h(x)}\}$, and thus $h(x) \in G_{\sigma(\Delta)}(S)$, so $h(G_\Delta(R)) \subseteq G_{\sigma(\Delta)}(S)$. Applying the same reasoning to h^{-1} gives the opposite inclusion, and thus $h(G_\Delta(R)) = G_{\sigma(\Delta)}(S)$. □

If $h : G(R) \longrightarrow G(S)$, we denote by $h_e : R \longrightarrow S$ the extension of h sending 0 to 0.

Theorem 3.6. *Let R, S be Dedekind domains with torsion class group, and let $h : G(R) \longrightarrow G(S)$ be a homeomorphism. Let I be a radical ideal of R. Then, the following hold.*

(a) *$h_e(I)$ is a radical ideal of S.*
(b) *The number of prime ideals of R containing I is equal to the number of prime ideals of S containing $h_e(I)$.*
(c) *If I is prime, $h_e(I)$ is prime.*

Proof. Since I is radical, $I = \bigcup\{G_\Delta(R) \mid V(I) \supseteq \Delta\} \cup \{0\}$; hence, applying Proposition 3.5,

$$\begin{aligned} h_e(I) =& h\left(\bigcup\{G_\Delta(R) \mid V(I) \supseteq \Delta\}\right) \cup \{0\} = \\ =& \bigcup\{h(G_\Delta(R)) \mid V(I) \supseteq \Delta\} \cup \{0\} = \\ =& \bigcup\{G_\Lambda(S) \mid V(I) \subseteq \sigma^{-1}(\Lambda)\} \cup \{0\} = \\ =& \bigcup\{G_\Lambda(S) \mid \sigma(V(I)) \subseteq \Lambda\} \cup \{0\} = J \end{aligned}$$

where J is the radical ideal such that $V(J) = \Delta$, i.e., $J = \bigcap_{Q\in\Lambda} Q$. (a) is proved.

(b) follows from the fact that the number of prime ideals containing I is the least n such that there is a subset $\Delta \subseteq \mathrm{Max}(R)$ of cardinality n such that $G_\Delta(R) \subseteq I$. (c) is immediate from (b). □

4. The P-topology

The Golomb topology on a Dedekind domain R is a very "global" structure: that is, it depends at the same time on all the prime ideals of R. In this section, we show a way to "isolate" the neighborhoods relative to a single prime ideal P, i.e., in the form $a + P^n$. The main idea is the following.

Proposition 4.1. *Let R be a Dedekind domain and let P be a prime ideal of R; take $\Omega \subseteq R \setminus P$. If Ω is clopen in $R \setminus P$, then for every $x \in \Omega$ there is an $n \geq 1$ such that $x + P^n \subseteq \Omega$.*

Proof. Fix Ω clopen in $R \setminus P$ and let $x \in \Omega$. Since $R \setminus P$ is open, Ω is also an open set of $G(R)$, and thus there is an ideal I such that $x + I \subseteq \Omega$; since $(x + I) \cap P = \emptyset$, we can write $I = P^n J$ for some $n \geq 1$ and some ideal J coprime with P. We claim that $x + P^n \subseteq \Omega$.

Otherwise, let $y \in (x + P^n) \setminus \Omega$; then, $y \in R \setminus P$, and since $(R \setminus P) \setminus \Omega$ is clopen in $R \setminus P$ we can find, as in the previous paragraph, an integer $m \geq 1$ and an ideal L coprime with P such that $y + P^m L \subseteq (R \setminus P) \setminus \Omega$. Since Ω is clopen in $R \setminus P$, we have $\overline{\Omega} \cap (R \setminus P) = \Omega$; hence, $\overline{x + P^n J} \cap (R \setminus P) \subseteq \Omega$. Likewise, $\overline{y + P^m L} \cap (R \setminus P) \subseteq (R \setminus P) \setminus \Omega$, and thus in particular $\overline{x + P^n J} \cap \overline{y + P^m L} = \emptyset$. However,

$$\overline{x + P^n J} = \overline{x + P^n} \cap \overline{x + J} = ((x + P^n) \cup P)^\bullet \cap \overline{x + J} \supseteq (x + P^n) \cap \mathrm{rad}(J)^\bullet$$

and likewise $\overline{y+P^mL} \supseteq (y+P^m)\cap \mathrm{rad}(L)^\bullet$. Since $y \in x+P^n$, the intersection $(x+P^n)\cap(y+P^m)$ is nonempty, and thus it contains a coset $z+P^t$. Since J and L are coprime with P, we have $(x+P^t)\cap\mathrm{rad}(J)^\bullet\cap\mathrm{rad}(L)^\bullet \neq \emptyset$; this contradicts the construction of J and L, and thus y cannot exist, i.e., $x + P^n \subseteq \Omega$. The claim is proved. □

Corollary 4.2. *Let R, S be Dedekind domain with torsion class group, let $h : G(R) \longrightarrow G(S)$ be a homeomorphism, and let P be a prime ideal of R. For every $x \in R\setminus P$, there is an n such that $h(x)+h_e(P)^n \subseteq h(x+P)$.*

Proof. Since $\overline{x+P} = (x+P)\cup P^\bullet$, the set $x+P$ is a clopen set of $R\setminus P$. Hence, $h(x+P)$ is clopen in $S\setminus h_e(P)$; we now apply the previous proposition. □

Let P be a prime ideal of R. We define the *P-topology* on $R\setminus P$ as the topology generated by the $\Omega \subseteq R\setminus P$ that are clopen in $R\setminus P$, with respect to the Golomb topology. Since every coprime coset $a+P^n$ is clopen in $R\setminus P$, Proposition 4.1 implies that the P-topology is generated by $a+P^n$, for $a \in R\setminus P$ and arbitrary n. Therefore, the P-topology on $R\setminus P$ actually coincides with the restriction of the P-adic topology.

In our context, the most useful property of the P-topology is that it depends uniquely on the Golomb topology, in the following sense.

Theorem 4.3. *Let R, S be Dedekind domain with torsion class group, and let $h : G(R) \longrightarrow G(S)$ be a homeomorphism of Golomb topologies. Then the restriction of h to $R\setminus P$ is a homeomorphism between $R\setminus P$ with the P-topology and $S\setminus h_e(P)$ with the $h_e(P)$-topology.*

Proof. If $\Omega \subseteq R\setminus P$ is clopen in $R\setminus P$, then $h(\Omega)$ is clopen in $S\setminus h_e(P)$. Hence, the basic open sets of the P-topology go to open sets in the $h_e(P)$-topology; since the same holds for h^{-1}, the restriction of h is a homeomorphism between the P-topology and the $h_e(P)$-topology. □

We end this section by determining the closure of a subset in the P-topology.

Proposition 4.4. *Let $Y \subseteq R\setminus P$, and let X be the closure of Y in the P-topology. For every $n \geq 1$, let $\pi_n : R \longrightarrow R/P^n$ be the canonical quotient map. Then,*

$$X = \bigcap_{n\geq 1} \pi_n^{-1}(\pi_n(Y)).$$

Proof. Let g be in the intersection: then, for every n, there is $a_n \in Y$ such that $\pi_n(g) = \pi_n(a_n)$, that is, $g - a_n \in P^n$. Hence, $g \in X$. Conversely, if g is in the closure then for every n there is $a_n \in Y$ such that $g - a_n \in P^n$; that is, $\pi_n(g) \in \pi_n(Y)$, as claimed. □

5. The groups $H_n(P)$

Let R, S be Dedekind domain with torsion class group, and let P be a prime ideal of R. Let $h : G(R) \longrightarrow G(S)$ be a homeomorphism. By Theorem 3.6, $h_e(P) = h(P)\cup\{0\}$ is a prime ideal of S. A natural question is whether this result can be generalized to cosets: that is, if $a \in R\setminus P$, does $h(a+P) = h(a)+h_e(P)$? In particular, if $h(1) = 1$, does $h(1+P) = 1+h_e(P)$? We are not able to prove this result; therefore, our strategy will be to use Proposition 3.5, the P-topology and the group structure of $U(R/P^n)$ to obtain "approximate" results. We collect in this section some technical lemmas which will be useful in the following sections.

Let P be a prime ideal of R and let $n \geq 1$ be an integer. Let $\pi_n : R \longrightarrow R/P^n$ be the canonical quotient; then, $\pi_n(U(R))$ is a subgroup of the (abelian) group $U(R/P^n)$ of the units of R/P^n. Therefore, we can define $H_n(P)$ as the quotient group

$$H_n(P) := U(R/P^n)/\pi_n(U(R)),$$

and we denote by $\theta_n : U(R/P^n) \longrightarrow H_n(P)$ the canonical quotient. We also denote by $\widetilde{\pi}_n = \theta_n \circ \pi_n : R \setminus P \longrightarrow H_n(P)$ the composition of the two quotients. The reason for considering $H_n(P)$ instead of $U(R/P^n)$ is that we want to "factor out" the self-homeomorphisms of $G(R)$ given by the multiplications by the units of R.

If $m > n$, there is a natural map from R/P^m to R/P^n, obtained by taking the quotient by P^n/P^m. An analogous connection holds for the groups $H_n(P)$.

Lemma 5.1. *For every $n \geq 1$, there is a surjective map $\lambda_n : H_{n+1}(P) \longrightarrow H_n(P)$ such that the following diagram commutes:*

$$\begin{array}{ccccc} R \setminus P & \xrightarrow{\pi_{n+1}} & U(R/P^{n+1}) & \xrightarrow{\theta_{n+1}} & H_{n+1}(P) \\ \| & & \downarrow & & \downarrow \lambda_n \\ R \setminus P & \xrightarrow{\pi_n} & U(R/P^n) & \xrightarrow{\theta_n} & H_n(P). \end{array}$$

Proof. If $u + P^n$ is a unit of R/P^n, then $u \notin P$, and thus $u + P^{n+1}$ is a unit of R/P^{n+1}. Hence, the natural map $R/P^{n+1} \longrightarrow R/P^n$ restricts to a surjective map $\lambda' : U(R/P^{n+1}) \longrightarrow U(R/P^n)$ between the unit groups; thus, the left square commutes. Furthermore, λ' sends $\pi_{n+1}(U(R))$ onto $\pi_n(U(R))$, and thus λ' induces a map λ_n which remains surjective. □

Let L be a subgroup of $H_n(P)$. By the previous lemma, we can lift L to $H_{n+1}(P)$ by λ_n and, subsequently, use the maps λ_{n+i} to lift it to all groups $H_{n+i}(P)$; therefore, we obtain a sequence

$$L \xleftarrow{\lambda_n} L_1 := \lambda_n^{-1}(L) \xleftarrow{\lambda_{n+1}} L_2 := \lambda_{n+1}^{-1}(L_1) \xleftarrow{\lambda_{n+2}} \cdots \tag{1}$$

where each L_i is a subgroup of $H_{n+i}(L)$. Since every λ_k is surjective, the index $[H_{n+i}(P) : L_i]$ is always equal to the index $[H_n(P) : L]$ of L, and in particular does not depend on i; on the other hand, the cardinality of these subgroups may grow, as $|L_{i+1}| = |L_i| \cdot |\ker \lambda_{n+i}|$. We call the sequence $\{L, L_1, \dots, \}$ the *telescopic sequence* of L. When $L = H_1(P)$, the telescopic sequence of L is just the sequence $\{H_1(P), H_2(P), \dots\}$.

We distinguish two classes of behavior.

One case is when the maps λ_n are isomorphisms for every $n \geq N$: in this case, all the information about the $H_n(P)$ "stops at N". If R/P is finite (and thus also $U(R/P^n)$ and $H_n(P)$ are finite for every $n \geq 1$) then in particular the sequence of the cardinalities of the $H_n(P)$ is bounded.

The second case is when there are infinitely many λ_n that are not isomorphisms: in this case, to study $H_n(P)$ we need to consider all the groups. If R/P is finite, this implies that the sequence of the cardinalities of the $H_n(P)$ is not bounded.

Example 5.2. Consider the ring of integers $\mathbb{Z}$, and let p be a prime number. If $p > 2$, then $U(\mathbb{Z}/p^n\mathbb{Z})$ is a cyclic group of cardinality $p^{n-1}(p-1)$, while $\pi_n(U(\mathbb{Z}))$ is always its two-elements subgroup. Hence, $H_n(p\mathbb{Z})$ is a cyclic group of cardinality $\frac{p^{n-1}(p-1)}{2}$. In particular, none of the maps $\lambda_n : H_{n+1}(p\mathbb{Z}) \longrightarrow H_n(p\mathbb{Z})$ is an isomorphism.

When $p = 2$, then $U(\mathbb{Z}/2^n\mathbb{Z})$ is not cyclic, but it is isomorphic (as a group) to $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{n-2}\mathbb{Z})$ (for $n \geq 2$), with the class of -1 corresponding to the element $(1, 0)$ of the direct product. Hence, $H_n(2\mathbb{Z})$ is again a cyclic group, of cardinality 2^{n-2}, and λ_n is not an isomorphism for every $n \geq 2$.

Let now $R := \mathbb{Z}[1/2]$: then, the units of R are 2^z and -2^z, with $z \in \mathbb{Z}$. Let $p \neq 2$ be a prime number; then, pR is a prime ideal of R, and $R/p^nR \simeq \mathbb{Z}/p^n\mathbb{Z}$, so $U(R/p^nR)$ is a cyclic group of cardinality $p^{n-1}(p-1)$.

The subgroup $\pi_n(U(R))$ is generated by 2 and -1, and for every $n \geq 2$ the index of this subgroup is equal to the index of $\pi_2(U(R))$ in $U(R/p^2R)$ (this is a standard result, and can be proved essentially in the same way of Proposition 6.3, (iv) $\implies$ (i) below); thus, λ_n is an isomorphism for every $n \geq 2$.

For example, if $p = 5$ then 2 and -1 generate the whole unit group $U(R/p^2R)$, and thus $H_n(pR)$ is the trivial group for every $n \geq 1$. On the other hand, if $p = 17$, then the order of 2 in $U(R/p^2R)$ is $8 \cdot 17$, and the subgroup generated by 2 contains -1, so that $H_n(pR)$ is cyclic of order 2 for every n.

A similar reasoning shows that, if p is a prime number and $R_p := \mathbb{Z}[1/p]$, then for every prime ideal Q of R_p the maps λ_n between the groups $H_n(Q)$ are isomorphisms for $n \geq 2$.

Even when the cardinality of the $H_n(P)$ grows unbounded, however, a part of their structure is still bounded. Given an abelian group L and a prime number p, the *non-p-component* of L is the subgroup of L formed by the elements whose order is coprime with p.

Lemma 5.3. *Let R be a Dedekind domain and let P be a prime ideal such that R/P is finite; let p be the characteristic of R/P. Then, there is an integer $\eta(P)$, coprime with p, such that, for all $n \geq N$, the non-p-component of $H_n(P)$ has order $\eta(P)$.*

Proof. Let $H'_k(P)$ be non-p-component of $H_k(P)$, and let $\eta_k(P)$ be its cardinality. Then, λ_k maps $H'_{k+1}(P)$ onto $H'_k(P)$, so that $\eta_k(P)$ divides $\eta_{k+1}(P)$. Hence, $\{\eta_k(P)\}_{k\in\mathbb{N}}$ is an ascending chain with respect to the divisibility order. Set $|R/P| = p^e$. Then, $|U(R/P^n)| = p^{e(n-1)}(p^e - 1)$, and thus $\eta_k(P)$ divides $p^e - 1$; hence, the chain is bounded above and thus finite. It follows that it stabilizes at some value $\eta(P)$. □

When $R = \mathbb{Z}$, using Example 5.2, it is not hard to see that $\eta(p\mathbb{Z})$ is equal to 1 if $p = 2$, while it is equal to $\frac{p-1}{2}$ if p is odd. For $R = \mathbb{Z}[1/p]$, on the other hand, there is no easy formula for $\eta(P)$.

Several results in the following sections will be valid only under the assumption that the groups $H_n(P)$ are cyclic. This forces a rather severe limit on the cardinalities of the residue fields.

Lemma 5.4. *Let R be a Dedekind domain, and let P be a prime ideal of R. If $U(R)$ is discrete in the P-topology, and $H_n(P)$ is cyclic for every n, then $|R/P|$ is a prime number.*

Proof. Since $U(R)$ is discrete in the P-topology, there is an $N \geq 2$ such that $1 + P^{N-1}$ contains no units different from 1. Fix $p \in P^{N-1} \setminus P^N$, and define

$$\begin{aligned} \sigma\colon R &\longrightarrow H_N(P), \\ a &\longmapsto \widetilde{\pi}_N(1 + ap). \end{aligned}$$

Since $p^2 \in P^N$, we have

$$\sigma(a)\sigma(b) = \widetilde{\pi}_N((1 + ap)(1 + bp)) = \widetilde{\pi}_N(1 + (a + b)p) = \sigma(a + b).$$

Hence, σ is a group homomorphism from $(R, +)$ to $H_N(P)$. Furthermore,

$$\begin{aligned} \ker\sigma =& \{a \in R \mid \widetilde{\pi}_N(1 + ap) = \widetilde{\pi}_N(1)\} = \\ =& \{a \in R \mid 1 + ap \in U(R) + P^N\} = P \end{aligned}$$

by the choice of N and p. Therefore, σ factors into an embedding of $(R/P, +)$ inside $H_N(P)$; since $H_N(P)$ is cyclic, it follows that also $(R/P, +)$ is cyclic. Since R/P is a field, it follows that R/P must be isomorphic to the field $\mathbb{F}_p$ with p elements for some prime number p. In particular, $|R/P|$ is prime. □

Note that the fact that $|R/P|$ is a prime number does not guarantee that $H_n(P)$ is cyclic: for example, if $R = \mathbb{F}_p[X]$, where $p > 2$ is a prime number, and $P = (X)$, then $H_3(P)$ has p^2 elements, but every element has order p.

6. Closure of powers

In isolation, the P-topology is not very interesting: indeed, since it coincides with the P-adic topology, it makes $R \setminus P$ into a metric space with no isolated points. In particular, if R is countable then $R \setminus P$ is homeomorphic to $\mathbb{Q}$ [17,9], and thus a homeomorphism between the P-topology of $R \setminus P$ and the Q-topology of $S \setminus Q$ does not give much information. However, by Proposition 3.5, a homeomorphism h between Golomb spaces carries a lot more structure.

In the following, we shall mostly restrict ourselves to Dedekind domains with torsion class group; indeed, many of our proofs are generalizations and abstractions of arguments that can be carried more concretely in the ring $\mathbb{Z}$ of integers. The hypothesis we put on R (for example, R being Dirichlet at P and P being almost cyclic, see Definitions 6.6 and 6.7) are, as well, formalizations of the properties of $\mathbb{Z}$ that are needed to carry out the proofs.

Given $a \in R \setminus P$, set

$$\operatorname{pow}(a) := \{ua^t \mid u \in U(R), t \in \mathbb{N}^+\}.$$

We want to study the closure of $\operatorname{pow}(a)$ in the P-topology.

Proposition 6.1. *Let R be a Dedekind domain, P a prime ideal, $a \in R \setminus P$; let X be the closure of* $\operatorname{pow}(a)$ *in the P-topology. Then, the following hold.*

(a) *If $\pi_n(a)$ is torsion in $U(R/P^n)$ for every $n \geq 1$ then*

$$X = \bigcap_{n \geq 1} \pi_n^{-1}\big(\langle \pi_n(a), \pi_n(U(R)) \rangle\big).$$

(b) *If $\widetilde{\pi}_n(a)$ is torsion in $H_n(P)$ for every $n \geq 1$ then*

$$X = \bigcap_{n \geq 1} \widetilde{\pi}_n^{-1}(\langle \widetilde{\pi}_n(a) \rangle).$$

Proof. (a) If $\pi_n(a)$ is torsion with order k, then

$$\begin{aligned}\pi_n(\operatorname{pow}(a)) =& \{\pi_n(u)\pi_n(a)^t + P^n \mid u \in U(R), t \in \mathbb{N}^+\} = \\ =& \{\pi_n(u)\pi_n(a)^t + P^n \mid u \in U(R), t \in \{1, \dots, k\}\}\end{aligned}$$

is exactly the subgroup generated by $\pi_n(a)$ and $\pi_n(U(R))$. The claim now follows from Proposition 4.4.

(b) follows as the previous point, noting that $\widetilde{\pi}_n$ sends all of $U(R)$ into the identity. □

The sets $\widetilde{\pi}_n^{-1}(\langle \widetilde{\pi}_n(a) \rangle)$ form a descending sequence of subsets of $R \setminus P$; if such sequence stabilizes at N, then we can study $\operatorname{pow}(a)$ by studying the subgroup $\langle \widetilde{\pi}_N(a) \rangle$ of $H_N(P)$. In general, this does not happen: for example, if $a = 1$ (so $\operatorname{pow}(a) = U(R)$ and $U(R)$ is finite), then $\widetilde{\pi}_n^{-1}(\langle \widetilde{\pi}_n(a) \rangle) = U(R) + P^n$ and thus the sequence is strictly decreasing (at least for large n). However, we can characterize this case; we distinguish the two behaviors of the λ_n in the next two propositions.

Proposition 6.2. *Let R be a Dedekind domain, P a prime ideal, $X \subseteq R \setminus P$. Suppose that the canonical surjections $\lambda_n : H_{n+1}(P) \longrightarrow H_n(P)$ are isomorphisms for $n \geq N$. Then, the following are equivalent.*

(i) *X is the closure of* $\operatorname{pow}(a)$ *for some $a \in R \setminus P$;*
(ii) *$X = \widetilde{\pi}_N^{-1}(L)$ for some cyclic subgroup L of $H_N(P)$.*

Proof. Take any $a \in R \setminus P$. For every $k \geq 0$, we have $\lambda_{N+k}(\widetilde{\pi}_{N+k+1}(a)) = \widetilde{\pi}_{N+k}(a)$, and thus the subgroup generated by $\widetilde{\pi}_{N+k+1}(a)$ in $H_{N+k+1}(P)$ is mapped onto the subgroup generated by $\widetilde{\pi}_{N+k}(a)$. Hence, $\widetilde{\pi}_N^{-1}(\langle \widetilde{\pi}_N(a) \rangle) = \widetilde{\pi}_{N+k}^{-1}(\langle \widetilde{\pi}_{N+k}(a) \rangle)$ for every $k \geq 0$. The claim follows. □

When the canonical surjections are not isomorphisms, the picture is more complicated. For simplicity, we restrict to the case where R/P is finite.

Proposition 6.3. *Let R be a Dedekind domain, P a prime ideal, $a \in R \setminus P$; let X be the closure of* $\operatorname{pow}(a)$ *in the P-topology. Suppose that R/P is finite and that there are infinitely many n such that $\lambda_n : H_{n+1}(P) \longrightarrow H_n(P)$ is not an isomorphism. Then, the following are equivalent:*

(i) *the chain $\{\widetilde{\pi}_n^{-1}(\langle \widetilde{\pi}_n(a) \rangle)\}_{n \in \mathbb{N}}$ stabilizes;*
(ii) *$X = \widetilde{\pi}_N^{-1}(L)$ for some $N \geq 1$ and some subgroup L of $H_N(P)$;*
(iii) *there is an $N \geq 1$ such that every element of the telescopic sequence of $\langle \widetilde{\pi}_N(a) \rangle$ is generated by the image of a;*
(iv) *there is an $N \geq 1$ such that every element of the telescopic sequence of $\langle \widetilde{\pi}_N(a) \rangle$ is cyclic, and the order of $\widetilde{\pi}_n(a)$ goes to infinity as $n \to \infty$.*

Proof. (i) $\implies$ (ii) If the chain stabilizes at N, that is, if $\widetilde{\pi}_N^{-1}(\langle \widetilde{\pi}_N(a) \rangle) = \widetilde{\pi}_{N+k}^{-1}(\langle \widetilde{\pi}_{N+k}(a) \rangle)$ for all $k \geq 0$, then $X = \widetilde{\pi}_N^{-1}(L)$ with $L := \langle \widetilde{\pi}_N(a) \rangle$.

(ii) $\implies$ (iii) If $X = \widetilde{\pi}_N^{-1}(L)$, then $\widetilde{\pi}_N(X) = L$, and thus by Proposition 6.1(a) $L = \langle \widetilde{\pi}_N(a) \rangle$. We have a commutative diagram

$$\begin{array}{ccc} X & \xrightarrow{\widetilde{\pi}_N} & L \\ \| & & \uparrow{\scriptstyle \lambda_N} \\ X & \xrightarrow{\widetilde{\pi}_{N+1}} & \lambda_N^{-1}(L); \end{array}$$

however, we also have $\widetilde{\pi}_{N+1}(X) = \langle \widetilde{\pi}_{N+1}(a) \rangle$, and thus the telescopic sequence of L is formed by the subgroups is generated by (the image of) a in the various $H_{N+k}(P)$.

(iii) $\implies$ (iv) Since there are infinitely many n such that λ_n is not an isomorphism, the cardinality of $H_n(P)$ goes to infinity; since the index remains fixed among the elements of a telescopic sequence, it follows that the cardinality of the $\langle \widetilde{\pi}_n(a) \rangle$ is unbounded, as claimed.

(iv) $\implies$ (i) Let σ_n be the order of $\widetilde{\pi}_n(a)$.

By Lemma 5.3, $\sigma_n = p^{k(n)} d_n$ for some $k(n) \geq 0$ and some d_n dividing $\eta(P)$; since the sequence $\{\sigma_n\}_{n \in \mathbb{N}}$ is unbounded, we can find N' such that $d_{N'} = d_{N'+k}$ for every $k \geq 0$. Furthermore, by the hypothesis, we can find $N \geq N'$ such that every element of the telescopic sequence $\{L, L_1, \dots, \}$ of $L := \langle \widetilde{\pi}_N(a) \rangle$ is cyclic. We claim that each L_i is generated by the image of a.

Indeed, by construction we have $|L_k| = p^{s(k)}|L| = p^{s(k)}\sigma_N$ for every $k \geq 0$ (and some nonnegative function $k \mapsto s(k)$). If ϕ is the Euler totient, the number of generators of L_k is

$$\phi(|L_k|) = \phi(\sigma_{N+k}) = \phi(p^{s(k)}\sigma_N) = p^{s(k)}\phi(\sigma_N),$$

since p does not divide σ_N. Hence, every generator of L lifts to a generator of L_k; therefore, $\widetilde{\pi}_N^{-1}(\langle\widetilde{\pi}_N(a)\rangle) = \widetilde{\pi}_{N+k}^{-1}(\langle\widetilde{\pi}_{N+k}(a)\rangle)$ for all $k \geq 0$, as claimed. □

One problem in applying the previous proposition to the Golomb topology is that we don't know if the sets $\mathrm{pow}(a)$ are invariant with respect to homeomorphisms. However, if R, S are principal ideal domains, and $q \in R$ is a prime element (i.e., if qR is a prime ideal) then $\mathrm{pow}(q) = G_{\{qR\}}(R)$, and thus by Proposition 3.5 a homeomorphism $h : G(R) \longrightarrow G(S)$ carries $\mathrm{pow}(q)$ to $\mathrm{pow}(q')$, for some prime element q' of S. Therefore, it carries the closure of $\mathrm{pow}(q)$ in the P-topology to the closure of $\mathrm{pow}(q')$ in the $h_e(P)$-topology (where P is any prime ideal of R distinct from qR).

More generally, suppose R is a Dedekind domain with torsion class group. Take a maximal ideal Q of R. If $Q^t = qR$ is the smallest power of Q that is a principal ideal, we say that q is an *almost prime* element; equivalently, an almost prime element is an irreducible element generating a primary ideal. In this case, we still have $\mathrm{pow}(q) = G_Q(R)$, since if xR is a Q-primary ideal then xR must be in the form $(Q^t)^k$ for some k. In particular, we must still have $h(\mathrm{pow}(q)) = \mathrm{pow}(q')$ for some almost prime element q' of S. More precisely, the unique prime ideal containing q' will be $h_e(Q)$, since Q is the only prime ideal containing q.

Definition 6.4. Let P be a prime ideal. We define $\mathcal{X}(P)$ as the set of closures of $\mathrm{pow}(q)$, as q ranges among the almost prime elements of R outside P.

The previous discussion shows the following.

Proposition 6.5. *Let R, S be two Dedekind domains with torsion class group, and let $h : G(R) \longrightarrow G(S)$ be a homeomorphism. Let P be a maximal ideal of R. Then, the map*

$$\begin{aligned} \overline{h}\colon \mathcal{X}(P) &\longrightarrow \mathcal{X}(h_e(P)), \\ X &\longmapsto h(X) \end{aligned}$$

is an order isomorphism (when $\mathcal{X}(P)$ and $\mathcal{X}(h_e(P))$ are endowed with the containment order).

We are now interested in studying the order structure of $\mathcal{X}(P)$; since we will need to have plenty of almost prime elements, we introduce the following definition.

Definition 6.6. Let R be a principal ideal domain and P a prime ideal of R. We say that R is *Dirichlet at* P if, for every $a \in R \setminus P$ and every $n \geq 1$ the coset $a + P^n$ contains at least one almost prime element.

For example, by Dirichlet's theorem on primes in arithmetic progressions (see e.g. [10, Chapter 4] or [1, Chapter 7]), $\mathbb{Z}$ is Dirichlet at each of its primes. An equivalent condition is that the set of almost prime elements of R is dense in $R \setminus P$ under the P-topology. Note that it is not known if a homeomorphism of Golomb spaces sends almost prime elements to almost prime elements, and thus this condition may not be a topological invariant.

We shall use the following terminology.

Definition 6.7. Let R be a Dedekind domain, and let P be a prime ideal of R. We say that P is *almost cyclic* if R/P is finite and $H_n(P)$ is cyclic for every $n \geq 1$.

The main example of almost cyclic prime ideals are the prime ideals of $\mathbb{Z}$ (see Example 5.2). Note that, if R is a Dedekind domain, it is possible that some prime ideals are almost cyclic and some are not: for example, if $R = \mathbb{Z}[i]$ is the ring of Gaussian integers, then $H_n(P)$ is cyclic if P is generated by the factor of a prime number congruent to 1 modulo 4 (since in this case $U(R/P^n)$ is cyclic [8, Theorem 3]), while if P

is generated by a prime number $q \equiv 3 \bmod 4$ then $|R/P| = q^2$ is not prime and thus P is not almost cyclic by Lemma 5.4.

Our next step is to link $\mathcal{X}(P)$ with the subgroups of the $H_n(P)$. We first show how to compare subgroups living in different $H_n(P)$.

Lemma 6.8. *Let R be a Dedekind domain, and let P be an almost cyclic prime ideal. Let L and L' be, respectively, subgroups of $H_n(P)$ and $H_m(P)$. Then, $\widetilde{\pi}_n^{-1}(L) \subseteq \widetilde{\pi}_m^{-1}(L')$ if and only if $[H_m(P) : L']$ divides $[H_n(P) : L]$; in particular, $\widetilde{\pi}_n^{-1}(L) = \widetilde{\pi}_m^{-1}(L')$ if and only if $[H_m(P) : L'] = [H_n(P) : L]$.*

Proof. Without loss of generality, suppose $n \geq m$. Composing the canonical maps λ_k, we get a surjective map $\lambda := \lambda_{n-1} \circ \cdots \circ \lambda_m$ from $H_n(P)$ to $H_m(P)$. Then, $\lambda(L)$ is a subgroup of $H_m(P)$ of the same index of L in $H_n(P)$, i.e., $[H_n(P) : L] = [H_m(P) : \lambda(L)]$. Since $H_m(P)$ is cyclic, we have $\lambda(L) \subseteq L'$ if and only if $[H_n(P) : L]$ is a multiple of $[H_m(P) : L']$, as claimed.

The "in particular" part follows immediately. □

Proposition 6.9. *Let R be a Dedekind domain with torsion class group, and let P be an almost cyclic prime ideal. Then, the following hold.*

(a) *Let X be the closure of* $\mathrm{pow}(q)$ *in the P-topology. If* $\mathrm{pow}(q)$ *is disjoint from the closure of $U(R)$ (with respect to the P-topology), then there is an $n \geq 1$ and a subgroup H of $H_n(P)$ such that $X = \widetilde{\pi}_n^{-1}(H)$.*
(b) *If R is Dirichlet at P, then $\widetilde{\pi}_n^{-1}(H) \in \mathcal{X}(P)$ for every subgroup H of $H_n(P)$.*

Proof. Let p be the characteristic of R/P.

(a) If the cardinality of the $H_n(P)$ is bounded, the claim follows from Proposition 6.2.

If the cardinality is unbounded, let q be an almost prime element such that X is the closure of $\mathrm{pow}(q)$, and let σ_n be the order of $\widetilde{\pi}_n(q)$. Suppose that $\{\sigma_n\}_{n\in\mathbb{N}}$ is bounded, and let σ be its maximum; then, $\widetilde{\pi}_n(q)^\sigma$ is the identity in $H_n(P)$ for all n, i.e., $\pi_n(q)^\sigma \in U(R) + P^n$ for every n. However, this implies that q^σ is in the closure of $U(R)$ in the P-topology, a contradiction. Therefore, σ_n becomes arbitrary large and the claim follows from Proposition 6.3.

(b) If the cardinality of the $H_n(P)$ is bounded, then there is an $a \in R\setminus P$ and an N such that $X := \widetilde{\pi}_N^{-1}(H)$ is the closure of $\mathrm{pow}(a)$ in the P-topology; since R is Dirichlet at P there is an almost prime element $q \in a + P^N$, and X is the closure of $\mathrm{pow}(q)$ in the P-topology, as claimed.

Suppose that the cardinality of the $H_n(P)$ is not bounded. Let $N \geq n$ be big enough such that the non-p-component of $H_N(P)$ has cardinality $\eta(P)$, and choose $k > N$ such that $|H_k(P)| > |H_N(P)|$. Let L be the element of the telescopic sequence of H that is contained in $H_k(P)$. Then, L is cyclic, and thus there is an $a \in R \setminus P$ such that $\widetilde{\pi}_k(a)$ generates L; as in the proof of Proposition 6.3, the fact that p divides the cardinality of L implies that every element of the telescopic sequence of L is generated by the image of a. Since R is Dirichlet at P, we can find an almost prime element $q \in a + P^k$; then, X is the closure of $\mathrm{pow}(q)$, and in particular $X \in \mathcal{X}(P)$, as claimed. □

Corollary 6.10. *Let R be a Dedekind domain with torsion class group, and let P be a prime ideal of R. Suppose that $U(R)$ is closed in the P-topology. Then, the following hold.*

(a) *If $R \setminus P \in \mathcal{X}(P)$, then P is almost cyclic.*
(b) *If R is Dirichlet at P and P is almost cyclic, then $R \setminus P \in \mathcal{X}(P)$.*

Proof. If $R \setminus P \in \mathcal{X}(P)$, then there is an almost prime element q such that $R \setminus P$ is the closure of $\mathrm{pow}(q)$. By Proposition 6.1, each $H_n(P)$ is generated by the image of q, and in particular they are all cyclic.

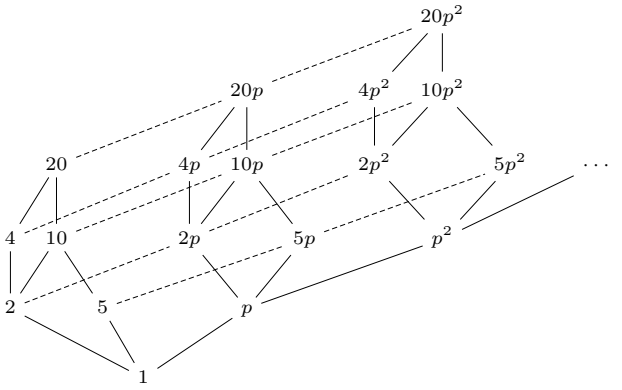

Fig. 1. The structure of $\mathcal{D}(p\mathbb{Z})$ for $p = 41$. In this case, $\eta(p\mathbb{Z}) = 20 = 2^2 \cdot 5$.

Conversely, suppose P is almost cyclic. By Proposition 6.9(b), $\widetilde{\pi}_n^{-1}(H) \in \mathcal{X}(P)$ for every subgroup of the $H_n(P)$; in particular, this holds for $H = H_n(P)$, for which we have $\widetilde{\pi}_n^{-1}(H) = R \setminus P$. □

Corollary 6.11. *Let R, R' be Dedekind domains with torsion class group and let P be a prime ideal of R; suppose that $U(R)$ is closed in the P-topology. Let $h : G(R) \longrightarrow G(R')$ be a homeomorphism and let $P' := h_e(P)$.*

(a) *If R is Dirichlet at P and P is almost cyclic then P' is almost cyclic.*
(b) *If also R' is Dirichlet at P', then P is almost cyclic if and only if P' is almost cyclic.*

Proof. If R is Dirichlet at P and P is almost cyclic, then by Corollary 6.10 $R \setminus P \in \mathcal{X}(P)$; hence, $R' \setminus P' = h(R \setminus P) \in h(\mathcal{X}(P)) = \mathcal{X}(P')$. Applying again the corollary we see that P' is almost cyclic.

The second part follows by considering the inverse $h^{-1} : G(R') \longrightarrow G(R)$. □

Set now

$$\mathcal{D}(P) := \{d \in \mathbb{N} \mid d \text{ divides } |H_n(P)| \text{ for some } n\};$$

then, $\mathcal{D}(P)$ has a natural order structure given by the divisibility relation (i.e., $a \leq b$ if and only if $a|b$). See Fig. 1 for an example. From a structural point of view, the previous proposition implies the following result.

Theorem 6.12. *Let R be a Dedekind domain with torsion class group, P an almost cyclic prime ideals, and suppose that $U(R)$ is closed in the P-topology. Let Θ_P be the map*

$$\Theta_P \colon \mathcal{X}(P) \longrightarrow \mathcal{D}(P),$$
$$X = \widetilde{\pi}_n^{-1}(L) \longmapsto [H_n(P) : H].$$

Then, the following hold.

(a) *Θ_P is well-defined, injective and order-reversing.*
(b) *If R is Dirichlet at P, then Θ_P is surjective, and thus Θ_P is an order-reversing isomorphism.*

Proof. For simplicity of notation, let $\Theta := \Theta_P$.

Since $U(R)$ is closed in the P-topology, and every $\mathrm{pow}(q)$ is disjoint from $U(R)$, by Proposition 6.9(a) every $X \in \mathcal{X}(P)$ is in the form $\widetilde{\pi}_n^{-1}(L)$; by Lemma 6.8, if it is also equal to $\widetilde{\pi}_{n'}^{-1}(L')$ then the index of L and L' are the same, and thus Θ is well-defined. The same Lemma 6.8 implies also that Θ is injective and order-reversing.

If R is Dirichlet at P, we can apply Proposition 6.9(b), and thus Θ is also surjective. It follows that Θ is an order-reversing isomorphism. □

The previous theorem implies that, under good hypothesis, the structure of $\mathcal{D}(P)$ is a topological invariant of the Golomb topology; in particular, if $h : G(R) \longrightarrow G(S)$ is a homeomorphism, then Proposition 6.5 can be extended to a chain of bijections

$$\mathcal{D}(P) \xrightarrow{\Theta_P^{-1}} \mathcal{X}(P) \xrightarrow{\overline{h}} \mathcal{X}(h_e(P)) \xrightarrow{\Theta_{h_e(P)}} \mathcal{D}(h_e(P)) \tag{2}$$

whose composition gives an order isomorphism between $\mathcal{D}(P)$ and $\mathcal{D}(h_e(P))$.

We shall use the following shorthand.

Definition 6.13. Let $z, z' \in \mathbb{N}$, and let $z = p_1^{e_1} \cdots p_k^{e_k}$ and $z' = q_1^{f_1} \cdots q_r^{f_r}$ be their factorizations. We say that z and z' *have the same factorization structure* if $k = r$ and, after a permutation, $e_i = f_i$ for every i.

Proposition 6.14. *Let R, R' be two Dedekind domains with torsion class group, and suppose there is a homeomorphism $h : G(R) \longrightarrow G(R')$. Let P be an almost cyclic prime ideal of R, and let $P' := h_e(P)$; suppose that R'/P' is finite, that $U(R)$ is closed in the P-topology, that R is Dirichlet at P and that R' is Dirichlet at P'. Then, the following hold.*

(a) *The sequence $\{|H_n(P)|\}_{n\in\mathbb{N}}$ is bounded if and only if $\{|H_n(P')|\}_{n\in\mathbb{N}}$ is bounded.*
(b) *If $|H_n(P)| = z$ and $|H_n(P)| = z'$ for all $n \geq N$, then z and z' have the same factorization structure.*
(c) *If $\{|H_n(P)|\}_{n\in\mathbb{N}}$ and $\{|H_n(P')|\}_{n\in\mathbb{N}}$ are unbounded, then $\eta(P)$ and $\eta(P')$ have the same factorization structure.*

Proof. Since h is a homeomorphism in the P-topology, $U(R') = h(U(R))$ is closed in the P'-topology; furthermore, by Corollary 6.11, P' is almost cyclic. By Proposition 6.5, there is an order isomorphism between $\mathcal{D}(P)$ and $\mathcal{D}(P')$.

The sequence $\{|H_n(P)|\}_{n\in\mathbb{N}}$ is bounded if and only if it is finite, which happens if and only if $\mathcal{D}(P)$ is finite. Since $\mathcal{D}(P)$ and $\mathcal{D}(P')$ are isomorphic, $\mathcal{D}(P')$ is finite and thus $\{|H_n(P)|\}_{n\in\mathbb{N}}$ is bounded if and only if $\{|H_n(P')|\}_{n\in\mathbb{N}}$ is bounded.

If $|H_n(P)| = z$ for all large n, then $\mathcal{D}(P)$ is just the set of divisors of z; in particular, the minimal elements of $\mathcal{D}(P) \setminus \{1\}$ correspond to the distinct prime factors of z. Since the same happens for $\mathcal{D}(P')$, the number of distinct prime factors of z and z' is the same. Furthermore, the exponent of p in z is equal to the number of elements of $\mathcal{D}(P)$ that are divisible only by p; hence, it depends only on the structure of $\mathcal{D}(P)$, and thus it doesn't change passing from $\mathcal{D}(P)$ to $\mathcal{D}(P')$.

On the other hand, if $\{|H_n(P)|\}_{n\in\mathbb{N}}$ is unbounded, the minimal elements of $\mathcal{D}(P)$ correspond to p (the cardinality of R/P) and the prime factors of $\eta(P)$. The elements of $\mathcal{D}(P)$ that are larger than exactly one minimal element are the powers of p and of the prime factors of $\eta(P)$; hence, there are infinitely many such elements larger than p, while there are only finitely many of them above the factors of $\eta(P)$. Hence, in the chain of bijections (2) p gets sent to p', the cardinality of R'/P'. Similarly, the divisors of $\eta(P)$ are the elements of $\mathcal{D}(P)$ that are not divisible by p, i.e., that are not above p; hence, the chain of bijection sends them to the elements of $\mathcal{D}(P')$ that are not above p', i.e., to the divisors of $\eta(P')$. As in the previous case, this implies that $\eta(P)$ and $\eta(P')$ have the same factorization structure. □

7. The correspondence at powers of p

Proposition 6.14 gives a very strong restriction for the image of a prime ideal under a homeomorphism of Golomb spaces. For example, suppose $R = \mathbb{Z}$. Then, every prime ideal is almost cyclic, and by Example 5.2 we have

$$\eta(p\mathbb{Z}) = \begin{cases} 1 & \text{if } p = 2 \\ \frac{p-1}{2} & \text{if } p > 2. \end{cases}$$

Thus, the only prime ideals $p\mathbb{Z}$ such that $\eta(p\mathbb{Z}) = 1$ (and so $\eta(p\mathbb{Z})$ has an empty factorization) are 2 and 3; it follows that, for every self-homeomorphism h of $G(\mathbb{Z})$, $h(2\mathbb{Z}^\bullet)$ can be equal only to $2\mathbb{Z}^\bullet$ or $3\mathbb{Z}^\bullet$. Likewise, $\eta(5\mathbb{Z}) = 2$ is prime, and thus $h(5\mathbb{Z}^\bullet)$ must be equal to $(2q+1)\mathbb{Z}^\bullet$ for some prime number q such that $2q+1$ is prime.

In this section, we use a finer analysis of the structure of $\mathcal{D}(P)$ to obtain even more. We concentrate on sets in the form

$$Y_k(P) := \Theta_P^{-1}(\eta(P)p^k)$$

where Θ_P is the map of Theorem 6.12.

Proposition 7.1. *Preserve the hypothesis and the notation of Proposition 6.14, and suppose that $\{|H_n(P)|\}_{n\in\mathbb{N}}$ is unbounded; let $p := |R/P|$ and $p' := |R'/P'|$. Then, the following hold.*

(a) *Let $h^\star := \Theta_{P'} \circ h \circ \Theta_P^{-1}$. Then, $h^\star(\eta(P)p^k) = \eta(P')(p')^k$ for every $k \geq 0$.*
(b) *$h(Y_k(P)) = Y_k(P')$.*

Proof. As we saw in the proof of Proposition 6.14, the minimal elements of $\mathcal{D}(P) \setminus \{1\}$ correspond to p and the prime factors of $\eta(P)$; moreover, p is the unique minimal element of $\mathcal{D}(P) \setminus \{1\}$ with infinitely many multiples that are not divisible by any other prime. Hence, $h^\star(p) = p'$. Furthermore, $\eta(P)$ is the largest element of $\mathcal{D}(P)$ that is not a multiple in p, and thus $h^\star(\eta(P))$ is the largest element of $\mathcal{D}(P')$ that is not a multiple of $h^\star(p) = p'$; that is, $h^\star(\eta(P)) = \eta(P')$.

Consider now the multiples of $\eta(P)$ in $\mathcal{D}(P)$: they are all in the form $\eta(P)p^k$ for some $k \geq 0$. The map $h^\star$ restricts to an order isomorphism between the multiples of $\eta(P)$ and the multiples of $\eta(P')$; hence, it must be $h^\star(\eta(P)p^k) = \eta(P')(p')^k$, as claimed.

By turning (2) inside-out and using the previous part of the proof, we see that

$$\begin{aligned} h(Y_k(P)) =& (\Theta_{P'}^{-1} \circ h^\star \circ \Theta_P)(Y_k(P)) = \\ =& (\Theta_{P'}^{-1} \circ h^\star)(\eta(P)p^k) = \Theta_{P'}^{-1}(\eta(P')(p')^k) = Y_k(P'). \end{aligned}$$

The claim is proved. □

Proposition 7.1 is rather close to our hope that a homeomorphism sends cosets into cosets, since both $Y_k(P)$ and $Y_k(P')$ are union of cosets. Further improvements of this result hinge on the explicit determination of the sets $Y_k(P)$; however, this will depend closely on the actual structure of the prime ideals and the units of R, and in particular on the image of $U(R)$ in R/P^n.

Proposition 7.2. *Let R be a Dedekind domain with torsion class group, and let P be an almost cyclic prime ideal; let $p := |R/P|$. Suppose that $U(R)$ is finite. Then, the following hold.*

(a) *There are $m \geq 0$ and $t \geq 1$ such that, for every $N \geq m$, we have $Y_N(P) = U(R) + P^{N+t}$.*
(b) *If $|U(R)|$ is coprime with p, then we can take $m = t = 1$. Furthermore, in this case*

$$\eta(P) = |H_1(P)| = \frac{p-1}{|\pi_1(U(R))|}.$$

Proof. (a) By Lemma 5.4, the cardinality p of R/P is a prime number.

Since $U(R)$ is finite, we can find M' such that the kernel of the map $\widetilde{\pi}_n : U(R) \longrightarrow H_n(P)$ is equal to the kernel of $\widetilde{\pi}_{M'}$ for every $n \geq M'$. Furthermore, by Lemma 5.3 there is an M'' such that $\eta(P)$ divides $|H_{M''}(P)|$. Take $M := \max\{M', M''\}$; then, $|H_M(P)| = p^m\eta(P)$ for some $0 \leq m < M$, and thus $|H_{M+k}(P)| = p^{m+k}\eta(P)$ for every $k \geq 0$.

By Theorem 6.12, $Y_N(P)$ correspond to the subgroup of index $p^N\eta(P)$ in $H_k(P)$, for $k \gg 0$. If $N \geq m$, let $N := m + k$; then, $|H_{M+k}(P)| = p^N\eta(P)$, and thus $Y_N(P)$ corresponds exactly to the identity subgroup of $H_{M+k}(P)$, i.e., $Y_N = U(R) + P^{M+k}$. However, $M + k = M + N - m$; setting $t := M - m$ we have our claim.

(b) If the cardinality of $U(R)$ is coprime with p, then for every $n \geq 1$ the natural map from $H_n(P)$ to $H_1(P)$ reduces to an isomorphism between their non-p-components, and the image of $U(R)$ in $H_1(P)$ is sent onto the image of $U(R)$ in $H_n(P)$; in particular, $|\pi_n(U(R))| = |\pi_1(U(R))|$ and the formula holds.

With the notation of the previous part of the proof, we have $M' = M'' = 1$, $m = 0$ and $t = 1 - 0 = 1$. The claim is proved. □

We now restrict to the case $R = \mathbb{Z}$; we first specialize the previous proposition.

Proposition 7.3. *Let p be a prime number, and let $k \geq 0$. Then, the following hold.*

(a) *If $p = 2$, then $Y_k(2\mathbb{Z}) = (1 + 2^{k+2}\mathbb{Z}) \cup (-1 + 2^{k+2}\mathbb{Z})$.*
(b) *If $p > 2$, then $Y_k(p\mathbb{Z}) = (1 + p^{k+1}\mathbb{Z}) \cup (-1 + p^{k+1}\mathbb{Z})$*

Proof. For $p > 2$ the claim is exactly the one in Proposition 7.2(b). For $p = 2$, we can take $M = 2$, so $m = 0$, $t = 1$ and thus $Y_k = \pm 1 + 2^{k+2}\mathbb{Z}$, as claimed. □

A different way to express the previous proposition is the following.

Proposition 7.4. *Let p be a prime number, a an integer coprime with p, and $k \geq 0$. Then:*

(a) *if a is even, then $a \in Y_k(p\mathbb{Z})$ if and only if p^{k+1} divides $a^2 - 1$;*
(b) *if a is odd, then $a \in Y_k(p\mathbb{Z})$ if and only if p^{k+1} divides $\frac{a^2-1}{4}$.*

Proof. If a is even, then p is odd. Then, $a \in Y_k(p\mathbb{Z})$ if and only if p^{k+1} divides $a-1$ or $a+1$. Since p cannot divide $a - 1$ and $a + 1$ at the same time, this happens if and only if p^{k+1} divides $a^2 - 1$.

If a is odd and p is odd, the same reasoning applies (noting that p^{k+1} divides $a^2 - 1$ if and only if it divides $\frac{a^2-1}{4}$). If $p = 2$, then one of $a - 1$ and $a + 1$ is in the form $2b$ for b odd, while the other is in the form $2^j c$ with c odd and $j \geq 2$. Hence, $a \in Y_k(2\mathbb{Z})$ if and only if $j \geq k + 2$, i.e., if and only if 2^{k+3} divides $a^2 - 1$. Dividing by 4 we have our claim. □

For any $n \in \mathbb{Z}$, let now

$$n^\star := \begin{cases} n^2 - 1 & \text{if } n \text{ is even,} \\ \frac{n^2-1}{4} & \text{if } n \text{ is odd.} \end{cases}$$

This notation allows to simplify the previous proposition.

Corollary 7.5. *Let h be a self-homeomorphism of $G(\mathbb{Z})$, and let $n \in \mathbb{Z}$ such that $|n| > 1$. If $n^\star$ factors as $p_1^{e_1} \cdots p_t^{e_t}$, then $h(n)^\star$ factors as $q_1^{e_1} \cdots q_t^{e_t}$, where $h(p_i\mathbb{Z}^\bullet) = q_i\mathbb{Z}^\bullet$.*

Proof. For every n, let $X(n)$ be the set of all pairs (p,k) where p is a prime factor of $n^\star$ and k is the largest integer such that p^{k+1} divides $n^\star$. By the previous proposition, $(p,k) \in X(n)$ if and only if $n \in Y_k(p\mathbb{Z})$; hence, $X(n) = \{(p_1, e_1 - 1), \dots, (p_t, e_t - 1)\}$.

Since h is a homeomorphism, $h(Y_k(p_i\mathbb{Z})) = Y_k(q_i\mathbb{Z})$; thus, $X(h(n)) = \{(q_1, e_1 - 1), \dots, (q_t, e_t - 1)\}$. It follows that $h(n)^\star = q_1^{e_1} \cdots q_t^{e_t}$, as claimed. □

Note that the previous corollary is similar to Proposition 6.14, in the sense that both compare the factorization structures of two elements linked by a homeomorphism h. However, this result is much more precise, since it applies to every integer (instead of only the $\eta(P)$) and, more importantly, the relationship between the corresponding factors p_i and q_i does not depend on n.

Lemma 7.6. *Let $n, m \in \mathbb{Z}$.*

(a) *If n and m are both even or both odd, then $n^\star = m^\star$ if and only if $|n| = |m|$.*
(b) *If $|n| > 1$ and $n^\star$ is prime, then $|n| \in \{2, 3\}$.*

Proof. The first claim follows directly from the definition. For the second one, since $n^\star = |n|^\star$ we can suppose without loss of generality that $n > 0$. If $n > 3$ is even, then both $n-1$ and $n+1$ have an odd prime factor, and thus $n^\star = n^2 - 1 = (n-1)(n+1)$ has at least two factors. If $n > 3$ is odd, then one of $n-1$ and $n+1$ is divisible by 4 and the other one by 2, so that $n^\star$ is even; however, since $n - 1 > 2$, there is at least one odd prime dividing $n-1$ or $n+1$, and thus $n^\star$ has at least two prime factors. The claim is proved. □

Theorem 7.7. *The unique self-homeomorphisms of $G(\mathbb{Z})$ are the identity and the multiplication by -1.*

Proof. Let $h : G(\mathbb{Z}) \longrightarrow G(\mathbb{Z})$ be a self-homeomorphism of $G(\mathbb{Z})$. We first claim that, for every $n \in \mathbb{Z}^\bullet$, $|h(n)| = n$; we proceed by induction on n.

If $|n| = 1$ then n is a unit and thus $h(n) \in U(\mathbb{Z}) = \{\pm 1\}$.

Suppose $|n| = 2$. Then, $n^\star = 3$, and thus $h(n)^\star$ must be a prime number; by the previous lemma, $h(n) \in \{\pm 2, \pm 3\}$. Suppose that $|h(n)| = 3$, so in particular $h(2\mathbb{Z}^\bullet) = 3\mathbb{Z}^\bullet$ and $h(3\mathbb{Z}^\bullet) = 2\mathbb{Z}^\bullet$. Consider $m = 7$: then, $m^\star = 12 = 2^2 \cdot 3$, and thus by Corollary 7.5 $h(m)^\star$ must be equal to $3^2 \cdot 2 = 18$. Since $h(m) \notin 2\mathbb{Z}^\bullet = h(3\mathbb{Z}^\bullet)$, we have $m^2 = 18 \cdot 4 + 1 = 73$, a contradiction. Hence $h(n) \in \{\pm 2\}$, and at the same time $h(\pm 3) \in \{\pm 3\}$.

Suppose now the claim holds for $|m| < |n|$, with $|n| \geq 4$. In particular, $h(p\mathbb{Z}^\bullet) = p\mathbb{Z}^\bullet$ for all prime numbers p with $p < |n|$; since $h(2\mathbb{Z}^\bullet) = 2\mathbb{Z}^\bullet$, n and $h(n)$ are either both even or both odd. Let $a := |n| + 1$ and $b := |n| - 1$; then, $n^\star = ab$ or $n^\star = \frac{ab}{4}$ (according to whether n is even or odd). If a is not prime, then all prime factors of a and b are smaller than $|n|$; hence, if $n^\star = p_1^{e_1} \cdots p_n^{e_n}$ by Corollary 7.5 then also $h(n)^\star = p_1^{e_1} \cdots p_n^{e_n}$, and thus $n^\star = h(n)^\star$; by Lemma 7.6, $|n| = |h(n)|$.

Suppose that a is prime: then, n must be even. Hence, $n^\star = (|n|-1)a$, and by Corollary 7.5 and inductive hypothesis we have $h(n)^\star = (|n|-1)a'$ for some prime number a'. If $|h(n)| \neq |n|$, then $|h(n)| > |n|$ (since all m with $|m| < |n|$ are image of m or $-m$), and in particular $|h(n)| - 1$ and $|h(n)| + 1$ are both greater than $|n| - 1$. Since $h(n)^\star = (|h(n)| - 1)(|h(n)| + 1) = (|n| - 1)a'$ and a' is prime, it follows that a' must divide at least one of $|h(n)|-1$ and $|h(n)|+1$. In the former case, $|h(n)|-1 \geq a'$ and $(|h(n)|-1)(|h(n)|+1) > a'(|n|-1)$, a contradiction; in the latter case, $|h(n)| + 1 \geq a'$ and thus $(|h(n)| - 1)(|h(n)| + 1) > (|n| - 1)a'$, again a contradition. Thus, $|h(n)| = |n|$.

Set now $X := \{n \in \mathbb{Z}^\bullet \mid h(n) = n\}$ and $Y := \{n \in \mathbb{Z}^\bullet \mid h(n) = -n\}$: by the previous part of the proof, $X \cup Y = \mathbb{Z}^\bullet$, and since $0 \notin \mathbb{Z}^\bullet$ they are disjoint.

Both sets are closed in $G(\mathbb{Z})$: indeed, X is the set of fixed points of h, which is closed since $G(\mathbb{Z})$ is Hausdorff, while Y is the set of fixed point of $-h$ (i.e., the homeomorphism that sends n to $-h(n)$). Since $G(\mathbb{Z})$ is connected [7, Theorem 8(b)], they can't be both nonempty: hence, either $X = \emptyset$ (and thus h is the multiplication by -1) or $Y = \emptyset$ (and thus h is the identity). The claim is proved. □

Theorem 7.8. *Let K be an algebraic extension of $\mathbb{Q}$, and let R be a Dedekind domain with quotient field K. If $G(R) \simeq G(\mathbb{Z})$, then $R = \mathbb{Z}$.*

Proof. By [7, Theorem 13], the number of units is an invariant of the Golomb topology, and thus $|U(R)| = 2$. Since R is a Dedekind domain (and thus in particular integrally closed), it contains the ring of integers $\mathcal{O}_K$ of K; hence, by Dirichlet's Unit Theorem (see e.g. [16, Chapter 1, §7]), $[K : \mathbb{Q}] \leq 2$. Furthermore, if $R \neq \mathcal{O}_K$, then there is a prime ideal of $\mathcal{O}_K$ such that $PR = R$; since $\mathcal{O}_K$ has torsion class group, there are elements of $\mathcal{O}_K$ generating a $(P \cap \mathcal{O}_K)$-primary ideal, and they would be units of R, a contradiction. Hence $R = \mathcal{O}_K$.

If $K \neq \mathbb{Q}$, then (since $[K : \mathbb{Q}] = 2$) there exists a field automorphism σ of K, which reduces to a ring automorphism of $\mathcal{O}_K$. Therefore, the restriction σ_0 of σ to $\mathcal{O}_K^\bullet$ is a self-homeomorphism of $G(\mathcal{O}_K)$ which fixes all elements of $\mathbb{Z}$. In particular, $G(\mathcal{O}_K)$ has at least four distinct self-homeomorphisms: the identity, the multiplication by -1, σ_0 and the composition of the latter two. By Theorem 7.7, $G(\mathcal{O}_K)$ cannot be homeomorphic to $\mathbb{Z}$; thus we must have $K = \mathbb{Q}$ and $R = \mathbb{Z}$, as claimed. □

References

[1] Tom M. Apostol, Introduction to Analytic Number Theory, Undergraduate Texts in Mathematics, Springer-Verlag, New York-Heidelberg, 1976.
[2] M.F. Atiyah, I.G. Macdonald, Introduction to Commutative Algebra, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.
[3] Taras Banakh, Jerzy Mioduszewski, Sławomir Turek, On continuous self-maps and homeomorphisms of the Golomb space, Comment. Math. Univ. Carol. 59 (4) (2018) 423–442.
[4] Nicolas Bourbaki, Commutative Algebra. Chapters 1–7, Elements of Mathematics (Berlin), Springer-Verlag, Berlin, 1989, translated from the French, reprint of the 1972 edition.
[5] Morton Brown, A countable connected Hausdorff space, in: L.W. Cohen (Ed.), The April Meeting in New York, in: Bull. Amer. Math. Soc., vol. 4, 1953, pp. 330–371, Abstract 423.
[6] Pete L. Clark, The Euclidean criterion for irreducibles, Am. Math. Mon. 124 (3) (2017) 198–216.
[7] Pete L. Clark, Noah Lebowitz-Lockard, Paul Pollack, A note on Golomb topologies, Quaest. Math. 42 (1) (2019) 73–86.
[8] James T. Cross, The Euler φ-function in the Gaussian integers, Am. Math. Mon. 90 (8) (1983) 518–528.
[9] Abhijit Dagupta, Countable metric spaces without isolated points, in: Topology Atlas, 2005.
[10] Harold Davenport, Multiplicative Number Theory, third edition, Graduate Texts in Mathematics, vol. 74, Springer-Verlag, New York, 2000, revised and with a preface by Hugh L. Montgomery.
[11] Harry Furstenberg, On the infinitude of primes, Am. Math. Mon. 62 (1955) 353.
[12] Robert Gilmer, Jack Ohm, Integral domains with quotient overrings, Math. Ann. 153 (1964) 97–103.
[13] Solomon W. Golomb, A connected topology for the integers, Am. Math. Mon. 66 (1959) 663–665.
[14] Solomon W. Golomb, Arithmetica topologica, in: General Topology and Its Relations to Modern Analysis and Algebra, Proc. Sympos., Prague, 1961, Academic Press/Publ. House Czech. Acad. Sci., New York/Prague, 1962, pp. 179–186.
[15] John Knopfmacher, Stefan Porubsky, Topologies related to arithmetical properties of integral domains, Expo. Math. 15 (2) (1997) 131–148.
[16] Jürgen Neukirch, Algebraic Number Theory, Grundlehren der Mathematischen Wissenschaften (Fundamental Principles of Mathematical Sciences), vol. 322, Springer-Verlag, Berlin, 1999, translated from the 1992 German original and with a note by Norbert Schappacher, with a foreword by G. Harder.
[17] Wacław Sierpiński, Sur une propriété topologique des ensembles denombrables denses en soi, Fundam. Math. 1 (1920) 11–16.