EXPOSITIONES
MATHEMATICAE

Expo. Math 15 (1997), 131-148

Topologies Related to Arithmetical Properties of Integral Domains

John Knopfmacher & Stefan Porubsky

ABSTRACT. Some topologies are defined and investigated for certain subsets and quotient semigroups of commutative domains with identity, and their arithmetical consequences for the underlying ring are studied. In particular (subject to certain assumptions) it is shown that some topological properties have implications for, or are related to, interesting arithmetical properties of prime ideals and prime elements of these rings, such as a generalization of Dirichlet's theorem on the infinity of prime elements in residue classes, etc.

S.W.Golomb [4] showed that certain aspects of the arithmetic of the set of positive integers $\mathbb{N}$ can be described employing some standard topological machinery. Golomb's topology is defined by the arithmetic progressions $\{an+b\}$ with $(a,b)=1$ taken as a basis for the open sets. A cursory inspection of the arguments used in [4] suggests that a similar study might be feasible in relation to other suitable algebraico–arithmetical domains. In fact Golomb himself refers loosely to possible applications to "other rings of algebraic integers", and particularly to the ring $\mathbb{Z}[\sqrt{-1}]$ of Gaussian integers. However $\mathbb{N}$ itself is not a full ring of algebraic integers, and closer examination of Golomb's purported possible application to $\mathbb{Z}[\sqrt{-1}]$ raises some questions, including those of definitions for suitable topologies and of the nature of the sets to be topologized. In addition, it seems desirable to develop such concepts in a context wide enough to at least include examples like the polynomial ring $F[X]$ in a indeterminate X over a given field F (especially when F is finite).

The present paper addresses these questions by introducing some topologies in relation to a general commutative integral domain R (with identity), with emphasis on the semigroup G_R of all associate–classes $\overline{a}$ of non–zero elements in R. Analogues of Golomb's conclusions for $\mathbb{N}$ are then investigated, in many cases subject to extra assumptions on the ring R. However, although various similar results are derived, the proofs are usually somewhat different.

1991 *Mathematics Subject Classification.* 11N80, 11N25, 11A25.
Key words and phrases. topological semigroup, coset topology, topological density, Dirichlet theorem on primes, arithmetical progression.
The research of the first author is supported by Foundation for Research Development, Pretoria
The research was carried out partly while the second author visited the Centre for Applicable Analysis and Number Theory at the University of Witwatersrand, Johannesburg, and he wishes to thank the Centre for its support and hospitality

0723-0869/97/020131-0148$5.10

The extra assumptions on R alluded to above are satisfied by special examples provide by $\mathbb{Z}, \mathbb{Z}[\sqrt{-1}]$ and $F[X]$, in particular. In the case of $\mathbb{Z}$ and $F[X]$, the general derived conclusions carry over quite easily to the natural arithmetical semigroups formed by $\mathbb{N}$ and the set $M_F(X)$ of all *monic* polynomials in $F[X]$. A curious phenomenon here is that the unifying general discussion treated below unexpectedly pulls back to an analogous but *new* topology $\mathfrak{D}^* \subsetneq \mathfrak{D}$ on $\mathbb{N} = \{1, 2, 3, \dots\}$, and *two* analogous topologies $\mathfrak{D}_F^* \subset \mathfrak{D}_F$ on $M_F(X)$, with $\mathfrak{D}_F^* = \mathfrak{D}_F$ if and only if $F = \mathbb{F}_2 = \{0, 1\}$.

Unless the contrary is stated, all rings R under consideration will be supposed to be commutative with an identity $1 = 1_R \neq 0$, and with no proper zero divisors.

Given a commutative integral domain R with the identity, let

$$R^0 = R \setminus \{0\}.$$

Two elements $a, b \in R$ are called *associate* ($a \sim b$) if the principal ideals $(a), (b)$ coincide. Since $\sim$ is an equivalence relation, the set $R/\sim$ of the all classes $\overline{a}$ of associated elements together with multiplication $\overline{a}.\overline{b} = \overline{ab}$ forms a commutative semigroup with zero. Let

$$G_R = R^0/\sim$$

be the set of all associate-classes $\overline{a}$ with $a \neq 0, a \in R$. If $X \subset R^0$, let $\overline{X} = \bigcup\{\overline{x} : x \in X\}$ and $\widetilde{X} = \{\overline{x} : x \in X\}$.

Let

$$\theta : R^0 \to G_R,\ \theta(a) \mapsto \overline{a}$$

be the canonical semigroup epimorphism relative to the ring multiplication and let

$$\rho : G_R \to R^0,\ \overline{a} \mapsto b,$$

with b an element of $\overline{a}$, be a fixed cross-section semigroup homomorphism mapping G_R onto a multiplicative subsemigroup of R^0. Given ρ, G^ρ will denote the set $\rho(G_R)$ endowed with the multiplication naturally induced by the multiplication on G_R. Multiplicative semigroups G_R and semigroups of the type G^ρ take over the role of two specially interesting and important examples which will be referred to repeatedly. For the first example, when $R = \mathbb{Z}$ and $\rho(\overline{a}) = |a|$ we get the multiplicative semigroup of positive integers. In the second, R is a polynomial ring $F[X]$ in an indeterminate X over a field F, with ρ sending each associate-class $\overline{z}$ to its unique *monic* member z^*.

If A, B are two subsets of R then

$$A + B = \{a + b : a \in A, b \in B\},$$
$$AB = A.B = \{ab : a \in A, b \in B\}.$$

If A, B are ideals of R, then so is $A + B$, but not necessarily AB.

1. Basic coset topologies

One way to define a topology on a set T can be based on the notion of the basis of neighborhoods, which is a system $\mathcal{A}$ of subsets of T satisfying the following two conditions [8, Theorem 1.11]:

(I) every point $t \in T$ is contained in some $G \in \mathcal{A}$,

(II) if t is contained in the intersection $G_1 \cap G_2$ of two sets $G_1, G_2 \in \mathcal{A}$ then there exists $G_3 \in \mathcal{A}$ with

$$t \in G_3 \subset G_1 \cap G_2.$$

To ensure that our topology makes the multiplicative semigroup S topological we should further require that

(III) to every $G \in \mathcal{A}$ containing a product ab there exist $G_a, G_b \in \mathcal{A}$ such that $a \in G_a, b \in G_b$ and $G_a.G_b \subset G$.

As mentioned in the introduction we shall mainly investigate a ring theoretic related generalization of Golomb's topology. Before doing this we consider some initial definitions and results which do not require R to be commutative, or not to have proper zero divisors in every case. Firstly we show that two other related topologies can be defined on the multiplicative semigroup of a ring R by systems of cosets of ideals of R. The definitions of the first two of them are based on the following simple result

Lemma 1. *Let $a+A, b+B$ be two cosets of ideals A, B of a ring R. Then their intersection $(a+A) \cap (b+B)$ is either empty or they intersect in a single coset $z + A \cap B$. Moreover, if $a \notin A, b \notin B$, then also $z \notin A \cap B$.*

Proof. Let $z \in (a+A) \cap (b+B)$. Then $a + A = z + A$ and $b + B = z + B$. The inclusion

$$(z + A) \cap (z + B) \supset z + A \cap B$$

is obvious. For the proof of the opposite one take an arbitrary $t \in (z+A) \cap (z+B)$. Then $t = z + a_1$ and $t = z + b_1$ with a suitable $a_1 \in A$ and $b_1 \in B$. Consequently, $a_1 = b_1$, i.e. $t \in z + A \cap B$, as required. Finally, the fact $z \in A \cap B$ with the obvious inclusion $A \cap B \subset A$ would imply $a + A = z + A \subset A$, i.e. $a \in A$, and similarly for b. □

The most common topology on a ring R is the linear topology given through the basis of all cosets of proper ideals of R. We shall use the following part of this result

Proposition 2. *The set of cosets $a + A$ with A running over the all proper ideals of a ring R forms a basis of a topology $\tau_1 = \tau_R$ converting the multiplicative semigroup of the ring R into a topological semigroup.*

Proof. Since the set of all ideals of R is closed under set–theoretical intersection, Lemma 1 shows that the mentioned set of cosets forms a basis. The verification of (III) easily follows from the inclusion

$$(1) \qquad (a + A)(b + B) \subset ab + Ab + aB + AB \subset ab + A + B + AB.$$

For if $ab \in c+C$, then $c+C = ab+C$ and $(a+A)(b+B) \subset ab+C$ whenever $A, B \subset C$. □

Corollary 2.1. *The set R^0 is a topological semigroup relative to the topology τ° induced on R^0 by topology τ_1.*

A related and weaker topology can be defined by non–trivial cosets, i.e. cosets of the form $a + A$ where $a \notin A$.

Proposition 3. *The set of non–trivial cosets $a + A$ with $a \notin A$ and A running over the all proper ideals of ring R forms a basis of a topology τ_2 converting the multiplicative semigroup of ring R into a topological semigroup.*

The proof runs along similar lines to the proof of Proposition 2, and yields

Corollary 3.1. *The set R^0 is a topological semigroup relative to the topology $\tau^\times$ induced on R^0 by topology τ_2.*

Two ideals A, B of a commutative ring R with identity are said to be *coprime* if

$$A + B = \{a + b \,:\, a \in A, b \in B\} = R,$$

or equivalently, if and only if

$$a + b = 1$$

for some $a \in A$ and $b \in B$.

A coset $a + A$ is called *invertible* provided (a) and A are coprime. This definition does not depend on the choice of the representative a of the class $a + A$. Also note that a coset $a + A$ is invertible if and only if this coset is an invertible element in the residue class ring R/A. This immediately implies the next two results.

Lemma 4. *If $x + A$ and $y + A$ are two invertible cosets then so is $xy + A$.*

Lemma 5. *Let M be a maximal (proper) ideal of a ring R. Then for every $x \notin M$ the coset $x + M$ is invertible.*

Lemma 6. *Let $x + A$ be an invertible coset. Then also the coset $x + A^n$ is invertible for every $n = 1, 2, \ldots$.*

Proof. Since $(x) + A = R$, we have $xt + a = 1$ for a suitable $t \in R$ and $a \in A$. Then

$$1 = (xt + a)^n = \sum_{k=0}^{n} \binom{n}{k} (xt)^k a^{n-k} = x \sum_{k=1}^{n} \binom{n}{k} x^{k-1} t^k + a^n.$$

Here $\sum_{k=1}^{n} \binom{n}{k} x^{k-1} t^k$ is an element of the ring R and $a^n \in A^n$, and the conclusion follows. □

The next lemma plays a role of Lemma 1 in our third topology

Lemma 7. *If $a + A$ and $b + B$ are two invertible cosets with a non-empty intersection, then also $(a + A) \cap (b + B)$ is invertible.*

Proof. Let $z \in (a + A) \cap (b + B)$. Then

$$a + A = z + A, \quad \text{and} \quad b + B = z + B.$$

Since $z + A$ is invertible, $zt + a_1 = 1$ for some $t \in R$ and $a_1 \in A$. Similarly $zv + b_1 = 1$ for some $v \in R$ and $b_1 \in B$. Consequently,

$$1 = (zt + a_1)(zv + b_1) = z(tzv + a_1 v + b_1 t) + a_1 b_1,$$

where $z(tzv + a_1 v + b_1 t) \in (z)$ and $a_1 b_1 \in AB \subset A \cap B$, i.e. $z + A \cap B$ is invertible. □

Proposition 8. *The set of invertible cosets $a + A$ with A running over the all proper ideals of ring R forms a basis of a topology τ_3 converting the multiplicative semigroup of ring R into a topological semigroup.*

Proof. The proof runs along similar lines as proofs of Propositions 2 and 3. For the proof that multiplication is continuous note that if $ab + C$ is invertible then so is $a + C$ for $(a) \supset (ab)$, and from similar reasons $b + C$ is invertible, too. The conclusion follows from the obvious inclusion $(a + C)(b + C) \subset ab + C$. □

Now assume again that R is a commutative integral domain, for short a "domain".

Corollary 8.1. *The set R^0 is a topological semigroup relative to the topology τ^* induced on R^0 by topology τ_3.*

The set G_R can be endowed with the quotient topology Δ with respect to the canonical epimorphism θ and a given topology τ on R^0 where

$$\Delta = \left\{X \subset G_R \ : \ \theta^{-1}(X) = \bigcup\{\overline{x} : \overline{x} \in X\} \text{ belongs to } \tau\right\}. \tag{2}$$

This quotient topology is the greatest topology with respect to which the canonical epimorphism θ is continuous. However more is true for our topologies. Let $\Delta^\circ, \Delta^\times$, and Δ^* be the quotient topologies on G_R corresponding to $\tau^\circ, \tau^\times$, and τ^*, resp. Then we have

Lemma 9. *The canonical epimorphism $\theta : R^0 \to G_R$ is continuous and open for every couple of topologies $\tau^\circ, \Delta^\circ; \tau^\times, \Delta^\times$; or τ^*, Δ^*.*

Proof. Due to the previous remarks only the openness is to be proved. Using Theorem 3.10 of [8] it is sufficient to prove that given an open set O in any of the mentioned topologies on R^0, the set $\overline{O} = \bigcup\{\overline{x} \ : \ x \in O\}$ is also open in the same topology. To see this it is enough to note that

(1) if $a \sim b$, i.e. if $b = au$, where u is a unit (i.e. a divisor of 1) on R, and $(a+A)\setminus\{0\} \subset O$ then $b + A = au + Au = \{\overline{x} \ : \ x \in a + A\}$ with zero removed, if necessary, is also a subset of $\overline{O}$,
(2) if $a + A$ is non–trivial or invertible then so is $au + A$ provided u is a unit of R. □

Proposition 10. *G_R forms a topological semigroup relative to each of quotient topologies $\Delta^\circ, \Delta^\times$, or Δ^*.*

Proof. It remains to prove that the multiplication of G_R is continuous. To do this it is sufficient to show that θ maps the defining bases for $\tau^\circ, \tau^\times$, and τ^* onto corresponding bases for $\Delta^\circ, \Delta^\times$, and Δ^*, resp. But this follows from the just proved fact that θ is open and continuous. □

Golomb's topology [4] is most closely related to the following subspace topology defined on G^ρ. On G^ρ two topologies can be defined:

- the subspace topology $\mathfrak{D}$ induced by the topology τ^* on R^0 because $G^\rho \subset R^0$.
- the quotient topology $\mathfrak{D}^*$ relative to the topology Δ^* and cross–section mapping ρ.

From the definition of the subspace topology we get

$$\mathfrak{D} = \{X \subset G^\rho \ : \ \underset{Y \in \tau^*}{\exists} \ X = G^\rho \cap Y\} = \{X \subset G^\rho \ : \ \underset{Z \in \tau_3}{\exists} \ X = G^\rho \cap Z\}.$$

Here $Y = Z \setminus \{0\}$.

For the quotient topology $\mathfrak{D}^*$ we have

$$\begin{aligned}\mathfrak{D}^* &= \{X \subset G^\rho \ : \ \rho^{-1}(X) = \{\overline{x} : x \in X\} \in \Delta^*\} \\ &= \{X \subset G^\rho \ : \ \underset{X_1 \in \Delta^*}{\exists} X = \{\rho(\overline{x}) : \overline{x} \in X_1\}\}.\end{aligned}$$

Proposition 11. *The topology $\mathfrak{D}$ is bigger than topology $\mathfrak{D}^*$.*

Proof. Given $X \in \mathfrak{D}^*$, let $X_1 \subset G_R$ be defined by $X = \{\rho(\overline{x}) : \overline{x} \in X_1\}$ and $Y = \theta^{-1}(X_1) = \overline{X_1} = \bigcup\{\overline{x} \ : \ \overline{x} \in X_1\}$. As noticed above $X_1 \in \Delta^*$ and also $Y \in \tau^*$. We claim that $X = G^\rho \cap Y$.

If $x \in X \subset G^\rho$ then $\overline{x} \in X_1$ and consequently $x \in \theta^{-1}(X_1) = Y$, i.e. $X \subset G^\rho \cap Y$. For the proof of the reverse inclusion let $x \in G^\rho \cap Y$. Then $x \in G^\rho$ and $\overline{x} \in X_1$. The last relation implies that $\rho(\overline{x})$ belongs to $X \subset G^\rho$. Together with the first relation this gives that $x = \rho(\overline{x})$ because one and only one element of every equivalence class belongs to G^ρ, which is in this case $x \in \overline{x}$.

This together yields that $G^\rho \cap Y \subset X$, and the proof is finished. □

Example 11.1. *The topology $\mathfrak{D}^* \subsetneqq \mathfrak{D}$ on $\mathbb{N}$.*

As mentioned in the introduction Golomb [4] studied topology having as a basis all arithmetical progressions $\{x + an\}$ with $(x, a) = 1$. Although this is not explicitly stated in [4], we shall assume that $1 \leq x < a$ and $n = 0, 1, 2, \ldots$. Under these assumptions Golomb's topology can be identified with our topology $\mathfrak{D}$.

Given $S \subset \mathbb{Z}^0$, let S^* denote the set of all positive members of $S \cup (-S)$. Since $\rho : G_{\mathbb{Z}} \to \mathbb{N}$ is a bijection, it is both open and continuous, and $\mathfrak{D}^*$ is a homeomorphic topology to Δ^*. Hence a basis for the open sets in $\mathfrak{D}^*$ is given by the sets $\rho(\theta(x + A)) = (x + A)^*$, where $x + A$ denotes an invertible coset of a nonzero ideal A of $\mathbb{Z}$. Since $\mathbb{Z}$ is a principal ideal domain, any of these basic sets can be rewritten in the form

$$(x + A)^* = \{x + a_1 n \ : \ n \in \mathbb{Z}\}^* \quad \text{for some } a_1 \in \mathbb{N}$$

coprime to x. If $a_1 \geq 2$ then we may write

$$(x + A)^* = \{x_1 + a_1 n \ : \ 0 \leq n \in \mathbb{Z}\} \cup \{a_1 - x_1 + a_1 n \ : \ 0 \leq n \in \mathbb{Z}\},$$

where $1 \leq x_1 < a_1$. Thus $(x + A)^*$ is a union of two disjoint $\mathfrak{D}$–basic progressions if $a_1 > 2$, while $(x + A)^* = \mathbb{N}$ if $a_1 = 1$. If $a_1 = 2$, then the invertibility of the coset implies $x_1 = 1$, and both progressions on the right hand side coincide.

For example,

$$(-7 + (3))^* = (1 + (3))^* = \{1, 4, 7, \ldots\} \cup \{2, 5, 8, \ldots\}.$$

However $\{1, 4, 7, \ldots\} = \{1 + 3n \ : \ n \geq 0\}$ is *not* a union of $\mathfrak{D}^*$–basic open sets; otherwise it would contain a set $(x_1 + (a_1))^*$ with $1 \leq x_1 < a_1$ and $(a_1, x_1) = 1$. Then, in particular

$$x_1 = 1 + 3n_0, \quad x_1 + a_1 = 1 + 3n_1, \quad a_1 - x_1 = 1 + 3m_0,$$

say, thus

$$a_1 = 3(n_1 - n_0) \quad \text{and} \quad a_1 = 3(m_0 + n_0) + 2,$$

giving $a_1 \equiv 0$ and $2 \pmod 3$, which is impossible. ◊

In number theory and elsewhere the multiplicative semigroup $M_F(X)$ of all *monic* polynomials in a given polynomial ring $F[X]$ over a field F is often taken as a natural analogue of the semigroup $\mathbb{N}$ of positive integers, especially when F is finite. It is therefore reasonable to investigate the possibility of finding arithmetically interesting topologies for $M_F(X)$. One such topology is the quotient $\mathfrak{D}_F^*$ induced on $M_F(X)$ by the cross–section homomorphism $\rho : G_{F[X]} \to M_F(X)$ which sends each associate–class $\overline{z}$ to its monic member z^*. Since ρ is a bijection, it is an open map and $\mathfrak{D}_F^*$ is a homeomorphic topology to Δ^* on $G_{F[X]}$. In view of the defining basis for open sets in Δ^* on $G_{F[X]}$, it turns out that a basis for the open sets in $\mathfrak{D}_F^*$ is provided by the sets $\rho(\theta(x+A)) = (x+A)^*$, say, where now S^* denotes the set of all monic associates of the elements in a given set $S \subset F[X]^0$.

Apart from $\mathfrak{D}_F^*$ which is analogous to $\mathfrak{D}^*$ on $\mathbb{N}$, the subspace topology $\mathfrak{D}_F$ for $M_F(X)$ relative to τ^* on $F[X]^0$ *also* provides an analogue of Golomb's topology $\mathfrak{D}$ for $\mathbb{N}$.

Example 11.2. *We have $\mathfrak{D}_F^* = \mathfrak{D}_F$ on $M_F(X)$ if and only if $F = \mathbb{F}_2 = \{0,1\}$.*

A basis for the subspace topology $\mathfrak{D}_F$ for $M_F(X)$ is provided by sets $(x+(a))^M = (x+(a)) \cap M_F(X)$, where it may be assumed that a is monic and $0 \leq \deg(x) < \deg(a)$, $(a,x) = 1$. So

$$(x+(a))^M = \begin{cases} \{x\} \cup \{x+ra \ : \ r \in M_F(X)\} & \text{if } x \text{ is monic,} \\ \{x+ra \ : \ r \in M_F(X)\} & \text{otherwise.} \end{cases}$$

Also, if y^* denotes the unique monic associate of $y \neq 0$,

$$\begin{aligned} (x+(a))^* &= \{x^*\} \cup \{(x+ra)^* \ : \ 0 \neq r \in F(X)\} \\ &= \{x^*\} \cup \{(x+ura)^* \ : \ 0 \neq u \in F, r \in M_F(X)\} \\ &= \{x^*\} \bigcup_{0 \neq w \in F} \{wx+ra \ : \ r \in M_F(X)\}, \end{aligned}$$

since $\deg(x) < \deg(a)$. (It follows, again from here, that every $\mathfrak{D}_F^*$–basic open set is open in $\mathfrak{D}_F$, i.e. that $\mathfrak{D}_F^* \subset \mathfrak{D}_F$.)

If $F = \mathbb{F}_2 = \{0,1\}$, then $x^* = x$ for $x \neq 0$, and $(x+(a))^* = (x+(a))^M$, and conversely every $\mathfrak{D}_F$–open set is open in $\mathfrak{D}_F^*$, and consequently $\mathfrak{D}_F^* = \mathfrak{D}_F$ *when* $F = \mathbb{F}_2$.

However, when $F \neq \mathbb{F}_2$, it turns out that $\mathfrak{D}_F^* \subsetneq \mathfrak{D}_F$. In order to see this, consider the $\mathfrak{D}_F$–open set

$$(1+(X))^M = \{1\} \cup \{1+rX \ : \ r \in M_F(X)\}.$$

If this set was open in $\mathfrak{D}_F^*$ it would contain some $\mathfrak{D}_F^*$–basic open set $(x+(a))^*$. In that case the above expressions for $(1+(X))^M$ and $(x+(a))^*$ would in particular yield $x^* = 1$, $1+a = 1+r_0X$ and $w+a = 1+r_1X$ for any unit $w \neq 1$ in F. Then $a = r_0X$ and $X \mid (w-1)$, which is impossible. $\Diamond$

2. Ring arithmetics and topologies τ^*, Δ^*

From now on it will be convenient to consider a domain R which is *not* a field (for which τ^* and Δ^* would be trivial). Since it seems rare for the canonical epimorphism $\theta : R^0 \to G_R$ to admit a "natural" cross–section homomorphism ρ, it is probably more natural to study the canonical topological space G_R relative to Δ^* than to generally investigate spaces G^ρ homeomorphic to G_R under an arbitrary non–algebraic, injective cross–section mapping $\rho : G_R \to R^0$. Although in principle *one could* work with the images G^ρ of arbitrarily

We are interested in proving some extensions of classical number–theoretical results on primes to general commutative domains with identity. Thus, that every arithmetical progression $a + b\mathbb{Z}$ with $(a, b) = 1$ contains at least one rational prime can be reformulated in our topology τ^* that the set of rational primes is dense in topology τ^* on $\mathbb{Z}^0$. Since every irreducible element in R is a non–unit, every invertible coset necessarily should contain a non–unit in this case. A necessary condition to this is that the set U of units of R is not open. The next theorem shows that this is at least sufficient for the existence of infinity of prime elements in many natural cases.

Theorem 14. *If the set U of units is not open in topology τ^* on R^0 then the set of maximal ideals in R is infinite.*

Proof. Every element of R which is not a unit belongs to some maximal ideal of R. If U is the set of units of R then

$$R^0 = U \bigcup_{P \in \mathfrak{M}} (P \setminus \{0\})$$

where $\mathfrak{M}$ is the set of maximal ideals of R. By the assumption, U is not open and so

$$Y = \bigcup_{P \in \mathfrak{M}} (P \setminus \{0\})$$

is not closed. On the other hand, each $P \setminus \{0\}, P \in \mathfrak{M}$, is closed, because

$$R^0 = W \cup (P \setminus \{0\})$$

where

$$W = \bigcup_{x \in R \setminus P} (x + P)$$

is the union of invertible cosets $x + P$ (c.f. Lemma 5) and thus W is open in R.

Since Y is not closed, it cannot be a finite union of the closed sets $P \setminus \{0\}, P \in \mathfrak{M}$. Consequently $\mathfrak{M}$ must be infinite. □

Corollary 14.1. *Under the assumptions of Proposition* 14 *the set of prime ideals of R is infinite.*

To the proof note that every maximal ideal in a commutative integral domain with identity is prime. Also note that [3, Exercise 3, p.220] for every positive integer n, there exists a principal ideal domain with exactly n maximal ideals.

To the class of rings to which Theorem 14 is applicable belong certainly infinite rings with finite groups of units. Typical examples of such rings are $\mathbb{Z}$, $\mathbb{F}_q[X]$, and $\mathbb{Z}[\sqrt{-k}]$, $\mathbb{Z}[\frac{1}{2} + \frac{1}{2}\sqrt{-k}]$ with $k \in \mathbb{N}$.

Corollary 14.2. *If R is a principal ideal domain and the set U of units of R is not open in topology τ^*, then the set of non–associate prime elements of R is infinite.*

Here note that in a unique factorization domain every irreducible element is prime and that every principal ideal domain is a unique factorization domain in which every (proper) prime ideal is maximal, and conversely ([27, Cor. 1]).

The rings $\mathbb{Z}$, $R[X]$ with R a unique factorization domain and $\mathbb{Z}[\sqrt{-k}]$ for certain $k \in \mathbb{N}$ are examples of unique factorization domains for which the hypothesis of Corollary14.2 about the set of units is valid. This Corollary thus provides a "topological" approach to the infinity of primes in these cases (for $\mathbb{Z}$, actually for $\mathbb{N}$, Golomb [4] gave a similar proof

selected maps ρ, this seems less natural even for an interesting concrete domain like the ring $\mathbb{Z}[\sqrt{-1}]$ of all Gaussian integers. Even here there seems to be no "best possible" choice of an injective (not necessarily algebraic) cross–section ρ, although reasonable ad hoc choices could be made for this particular ring: for example one could choose $G^{\rho}_{\mathbb{Z}[\sqrt{-1}]}$ to be the "semi–closed first quadrant" of all numbers $a + b\sqrt{-1}$ with $a \in \mathbb{N}, 0 \leq b \in \mathbb{Z}$.

Theorem 12. *The topological spaces* (R^0, τ^*) *and* (G_R, Δ^*) *are connected.*

Proof. Let V, W be two non-empty disjoint open sets in the topology τ^*. We show that their union cannot be R^0. To do this we show the existence of two ideals A, B such that $AB \nsubseteq V \cup W$.

The openness of V and (I) implies the existence of an invertible coset, say, $a + A$ such that $a + A \subset V$. We claim that $A \cap W = \emptyset$. If $x \in A \cap W$, then according to (I) there exists an invertible coset $b + B$ containing x and contained in W. Since the invertibility of a coset does not depend on the representative of this coset, $(x) + B = R$. However $x \in (x) \subset A$, and therefore the ideals A, B are coprime. Then the Chinese Remainder Theorem implies that $(x + A) \cap (b + B) \neq \emptyset$. This contradicts the assumption $V \cap W = \emptyset$.

Along symmetric lines it can be proved that there exists an invertible coset $c + C$ with $C \cap V = \emptyset$. But $AC \subset A \cap C$ and thus $AC \cap (V \cup W) = \emptyset$. □

A system of cosets

$$a_i + A_i, \quad i \in I \tag{4}$$

is called a *disjoint cover* of R if every element of R belongs to exactly one coset of (4). There is a rich bibliography on disjoint covers, we refer the reader to [Poru1981] for more details. Disjoint covers of the whole ring R consisting only from invertible cosets can be trivially excluded because the zero element cannot be covered by an invertible coset. For covering of R^0 we get from the previous Theorem

Corollary 12.1. *There is no disjoint cover on* R^0 *consisting only of invertible cosets. In other words, if* (4) *is a disjoint cover on* R^0 *then we have* $(a_i) + A_i \neq R$ *at least for one* $i \in I$.

If $R = \mathbb{Z}$, the ring of integers, then a disjoint cover can be described in terms of arithmetic progressions or congruences. Corollary 12.1 shows that it is not possible to split nonzero integers into (finite or not) system of disjoint arithmetic progressions

$$a_i + b_i\mathbb{Z}, \; i \in I$$

with $(a_i, b_i) = 1$ for every $i \in I$.

If R is a unique factorization domain, then arithmetically G_R is a *unique factorization* semigroup, with a set of *primes* consisting of the associate–classes $\overline{p}$ of the all *irreducible* elements $p \in R$. Note that in the general situation a non–unit p is irreducible if and only if the principal ideal (p) is prime and $\neq R$.

Rather trivial algebraico–topological arguments show that

Lemma 13. *Let* $Q \subset R$. *The set* $\bigcup\{\overline{x} : x \in Q\}$ *is dense in the topology* τ_3 *if and only if* Q *meets every invertible coset in* R.

via his topology $\mathfrak{D}$ which does not equal to $\mathfrak{D}^*$ as we saw in Example 11.1). However the ring $\mathbb{Z}_p$ *of all p–adic integers* is a unique factorization domain for which the hypothesis about units as well as the conclusion of Corollary 14.2 fail: in fact $\mathbb{Z}_p$ has p as its *unique* prime element (up to associates), and $G_{\mathbb{Z}_p} = \{\overline{1}, \overline{p}, \overline{p}^2, \dots\}$.

For further applications of Corollary 14.2 also note that in [13, Proposition 1.2] it is proved that if R is a Noetherian domain in which every maximal ideal is the radical of a principal ideal, then Krull dimension of R is 1.

Now consider an inter–relationship between Δ^* and a deep property of primes known to hold for very special domains R, the most famous case being given by Dirichlet's classical theorem about primes in an arithmetical progression. In order to describe this in a wider setting, consider the next definition.

A domain R will be said to satisfy *Dirichlet's condition* for a subset P of R if every invertible coset in R contains infinitely many pairwise non–associate elements from P.

P.G. Lejeune Dirichlet's famous theorem of 1837, which has never been proved in full generality without the aid of real or complex analysis (or at least limiting processes of analysis), amounts to the assertion that $\mathbb{Z}$ satisfies the preceding condition. Similar non–trivial theorems, depending again on analytic methods and going back to H.Kornblum (1919) and E.Artin (1924) (see [1, 6, 9]), imply that $\mathbb{F}_q[X]$ (for a *finite field* $\mathbb{F}_q$) and certain other domains related to such polynomial domains also satisfy Dirichlet's condition. However it does not seem to be well known at present exactly how much more widely Dirichlet's condition may be applicable.

The objective of the following proposition is to show, subject to certain further hypotheses on R, that Dirichlet's condition is equivalent to a certain *strong* form of density of the set $\overline{P}$ of prime elements in G_R. This type of density[1] is as follows:

Given a subset W of an arbitrary topological space Y, call W *strongly dense* in Y if every non–empty open set in Y contains at least two elements of W.

Proposition 15. *(1) A set is strongly dense in topology τ_3 if and only if it is dense in τ_3.*
(2) A set is strongly dense in topology τ^* if and only if it is dense in τ^*.
(3) If (G_R, Δ^*) is a T_1–space then a set is strongly dense in Δ^* if and only if it is dense in Δ^*.

Proof. What is to prove are the sufficient conditions. Their proofs in cases (1) and (2) can be based on ideas of [5]. Let Q be dense, and $x + A$ an invertible coset. (There is no necessity to do this, but we may suppose that $A \neq R$. In that case $t \neq 0$ below.) Then there exist $t \in R$ and $a \in A$ such that

$$tx + a = 1, \tag{3}$$

and so $x + (a)$ is also invertible. Without loss of generality we can suppose that $a \neq 0$ here. For if $a = 0$ in (3) then x is a unit of R. However if x is a unit with inverse s in R, and $0 \neq b \in A$, then $tx + a = 1$ for $a = bx \neq 0$ in A, and $t = s - b$. Now

$$1 = tx + a = t(x + a) + (1 - t)a$$

[1] which might perhaps be known by another name in general topology, but which could not be traced anywhere by the present authors

which implies that $x+a+(a)$ is again invertible. Clearly $(a^2)=(a)^2$ and Lemma 6 implies that the cosets

$$x+(a^2), \quad x+a+(a^2)$$

are invertible, too. They are disjoint because $x+t_1a^2=x+a+t_2a^2$ implies that a is a unit or zero, which is impossible. Since both of these cosets are subsets of $x+A$, the conclusion of (1) and (2) follows.

For the proof of (3) note that we proved in Theorem 12 that (G_R,Δ^*) is connected. Consequently there is no singleton in (G_R,Δ^*) which can be simultaneously open and closed. Then the next Lemma implies that if (G_R,Δ^*) is T_1 then a set is strongly dense in Δ^* if and only if it is dense in Δ^*. □

Lemma 16. [2] *Let W be a dense set in a T_1–space Y, such that no singleton subset of W is open in Y. Then W is strongly dense in Y.*

In order to derive the next proposition, and also certain other aspects of the topologies τ^* and Δ^*, we first list *some possible assumptions about R:*

(i) R admits an non–negative integer–value *norm* mapping N with the properties:
  (a) $N(x)=0$ if and only if $x=0$,
  (b) $N(x)=1$ if and only if x is a unit,
  (c) $N(ab)=N(a)N(b)$ for all $a,b\in R$.

(ii) for any fixed $x,y\in R$ and any units u,v of R, $N(ux+vy)$ is bounded uniformly relative to $N(x),N(y)$,

(iii) G_R contains only finitely many elements $\overline{a}$ for which $N(a)$ takes any given, fixed value $k\in\mathbb{N}$.

Note that assumptions (i), (ii) and (iii) are not generally independent. To demonstrate this introduce the following concepts. If I is a non–zero ideal of a ring R such that the ring R/I is finite, then I is said to be *residually finite* and the positive integer $\mathcal{N}(I)=\mathrm{card}(R/I)$ is called the *norm* of I. A ring R is said to be *residually finite* if every non–zero ideal of R is residually finite. Then we have

a) If R is a Noetherian ring and A,B are two residually finite non–zero ideals of R then [2, Lemma 2.1] AB is also residually finite. If moreover R is Dedekind then [3, Ex.8(i),p.467] $\mathcal{N}(AB)=\mathcal{N}(A)\mathcal{N}(B)$. Thus if R is a residually finite Dedekind domain then (i)(b) and (i)(c) are mere consequences of the properties of the norm function $\mathcal{N}$, provided we choose $N=\mathcal{N}$.

b) Assuming (ii) is more special but can easily be verified for the above choice $N=\mathcal{N}$ in an arbitrary residually finite ring R, since the ideal $(ux+vy)$ does not depend on the units u,v in these cases. Another class of rings satisfying (ii) independently of the choice of N is given by the rings with only finitely many units.

c) Assumption (iii) is fulfilled for all residually finite rings provided $N=\mathcal{N}$, as Theorem 6 of [7] shows.

It is proved in [2, Corollary 2.2] that a commutative ring R with identity is residually finite if and only if every non–zero prime ideal of R is finitely generated and of finite index in R. Thus residually finite rings include the polynomial rings $\mathbb{F}_q[X]$, the formal power series ring $\mathbb{F}_q[[X]]$ over a finite field $\mathbb{F}_q$, and others listed below.

[2] This simple lemma, essentially, was kindly suggested to the first author by Dr.R.Fenn of the University of Sussex.

We have also proved:

Lemma 17. *Every residually finite Dedekind domain satisfies assumptions (i), (ii) and (iii) with $N = \mathcal{N}$ and $N(0) = 0$.*

It follows from the next result that the rings of all algebraic integers and maximal orders of algebraic number fields K are covered by previous Lemma 17

Lemma 18 ([2, Corollary 4.6]). *Let R be a residually finite domain with quotient field F and let K be a finite algebraic extension of F. Then the integral closure R' of R in K is residually finite and so is every ring between R and R'.*

Now consider:

Theorem 19. *Suppose that either*

a) *R satisfies the assumptions (i) and (ii), or*
b) *R is noetherian.*

If P is a subset of R such that $\widetilde{P} = \{\overline{x} : x \in P\}$ is infinite. Then Dirichlet's condition for $\widetilde{P}$ is valid if and only if $\widetilde{P}$ is strongly dense in G_R.

Proof. In the one direction, it is trivial from the definition of Δ^* that Dirichlet's condition implies the strong density of $\widetilde{P}$.

a) Conversely, suppose that $\widetilde{P}$ is strongly dense in G_R. Then every invertible coset $x + A$ with $A \neq \{0\}$ contains at least one element $p \in P$ with $p \nsim x$.

If $A = R$, the assertion is implied by the assumption that $\widetilde{P}$ is infinite. Suppose that $A \subsetneqq R$ and that $x + A$ is invertible. Then as in (3) we can suppose that there exist $t \in R$ and $a \in A, a \neq 0$ such that

$$xt + a = 1.$$

This means that also $x + (a)$ is an invertible coset, and Lemma 6 shows that this is true also for $x + (a)^n$ for every $n \geq 1$. Moreover a is *not* a unit, since $A \neq R$.

Then the invertible coset $x + (a^k)$ $\left(= x + (a)^k\right)$ contains at least one element $p_k = x + r_k a^k \in P$ with $p_k \nsim x$. In that case, if $p_h = p_k$ for some $h < k$, then

$$r_h a^h = r_k a^k \,. \tag{4}$$

and consequently

$$N(r_k) = \frac{N(r_h)}{N(a)^{k-h}}.$$

Since $r_h, r_k \neq 0$ and $N(a) \geq 2$, it then follows that

$$1 \leq N(r_k) \leq \frac{N(r_h)}{2^{k-h}} < 1$$

for any fixed $h \geq 1$ if k is sufficiently large. This shows that at most a finite number of the elements p_k could coincide with a given p_h as above. Therefore, out of the elements $p_k = x + r_k a^k \nsim x$, one may inductively select a sequence of *distinct* ones $p_{h(1)} = p_1, p_{h(2)}, p_{h(3)}, \ldots$. If $p_{h(i)} \sim p_{h(j)}$ for $h(i) < h(j)$, then

$$x + r_{h(i)} a^{h(i)} = ux + u r_{h(j)} a^{h(j)}$$

for a unit $u \neq 1$. Hence

$$0 \neq (u-1)x = r'a^{h(i)} \tag{5}$$

for $0 \neq r' \in R$, and this implies that $N((u-1)x) \geq N(a)^{h(i)} \geq 2^{h(i)}$.

Now the assumption (ii) about N implies that $N((u-1)x)$ is bounded for units u and fixed x. Therefore the preceding inequalities are impossible for large $h(i)$. Thus the distinct elements $p_{h(i)} \in x + (a)$ are pairwise *non-associate* for all large enough indices $h(i)$. This establishes Dirichlet's condition for R in case a), when $\widetilde{P}$ is strongly dense in G_R.

b) In this case we employ a consequence of the Krull's intersection theorem [27, Corollary 1 of Theorem 12] that if R is a noetherian domain and $A \subsetneq R$ is an ideal of R then $\cap_n A^n = (0)$.

It follows from (4) that

$$r_h = r_k a^{k-h} \in (a)^k$$

which is impossible for infinitely many k due to the result above. Therefore again at most a finite number of the elements p_k could coincide with a given p_h. Similarly (5) implies

$$(u-1)x \in (a)^{h(i)}$$

which is again impossible for infinitely many $h(i)$'s. □

3. Further properties of the topologies

Lastly we give a small selection of further results about the topologies τ^* and Δ^*, subject to special assumptions on R, and in certain cases we deal only with $\mathbb{Z}$ and $F[X]$. It might be interesting to investigate how far the special assumptions could possibly be weakened, and also to look into other special properties of topological spaces in the present context.

Theorem 20. *If R satisfies the assumptions (i) and (ii), then the set P of irreducible elements in R has empty interior in R^0, and similarly for $\widetilde{P}$ in G_R.*

Proof. If $P \neq R^0$ had nonempty interior in R^0, then there would be an invertible coset $x+A$ consisting entirely of irreducible elements, therefore $x \neq 0$. As in the proof of Theorem 19 we can show that there is an invertible coset $x + (a) \subset x + A$ with $a \in A, a \neq 0$. Since all elements of $x + (a)$ are irreducible, $x + ra$ is irreducible for all $r \in R$. Then x is an irreducible element not dividing a since in the opposite case $a = x\epsilon$ and $x + ra = x(1 + r\epsilon)$. Consequently, $u(r) = 1 + r\epsilon$ is a unit for all $r \in R$. Then $N(r\epsilon) = N(u(r) - 1)$ is bounded, by (ii) with $x = 1, y = -1$, and so $N(\epsilon) = 0$, which is impossible. Moreover a is not a unit since that would imply $R = x + (a)$. It follows that, for any $k \in \mathbb{N}$, both $x + a^k$ and

$$x + (a^k + x + 1)a^k = (x + a^k)(1 + a^k)$$

are irreducible. Thus $1 + a^k = u_k$ is a unit, and

$$2^k \leq N(a^k) = N(u_k - 1).$$

Since $k \in \mathbb{N}$ and the values $N(u-1)$ are bounded for units u by (ii), we obtain a contradiction. Hence P must have empty interior in R^0, and the same follows for $\widetilde{P}$ in G_R. □

Theorem 21. *Let P_1 be the set of the all irreducible elements p of R for which the principal ideals (p) are maximal. Suppose that the set $\widetilde{P_1}$ is infinite.*

(1) *If R satisfies (i) and (iii), then R^0 is a Hausdorff space.*

(2) *If R satisfies (i), (ii) and (iii), then G_R is a Hausdorff space.*

Proof. (1) For fixed $x \neq y$ in R^0, there is an irreducible element $p \in P_1$ with $N(p)$ larger that $N(x), N(y)$ and $N(x-y)$, because $\widetilde{P_1}$ is infinite, and at most a finite of elements $\overline{p'}$ have $N(p') \leq$ any *fixed* bound, by (iii). Since (p) is maximal, $x+(p)$ and $y+(p)$ are disjoint open neighbourhoods of x and y, respectively, in R^0, because $x, y \in (p) \Rightarrow p|x \Rightarrow N(p) \leq N(x)$, $p|y \Rightarrow N(p) \leq N(y)$, and $x + r_1 p = y + r_2 p \Rightarrow p|(x-y) \Rightarrow N(p) \leq N(x-y)$. Thus R^0 is a Hausdorff space.

(2) Next, for fixed $\alpha \neq \beta$ in G_R, (ii) implies that the norms $N(ux+vy)$ are bounded for any fixed pair $x \in \alpha, y \in \beta$. Since $\widetilde{P_1}$ is infinite, (iii) then implies that there is an irreducible $p \in R$ with $N(p)$ larger than $N(x), N(y)$ and all the preceding norms $N(ux+vy)$. In that case, as before, p does not divide x, y or any of the elements $xu + yv$ for units u, v. It follows from this that no element of $x + (p)$ is an associate of any element of $y + (p)$, since $x + r_1 p = u(y + r_2 p)$ for a unit u implies $0 \neq x - uy = r_3 p$, i.e. $p|(x - uy)$, and that is impossible. Thus $\theta(x + (p)), \theta(y + (p))$ are disjoint open neighbourhoods of $\alpha = \overline{x}, \beta = \overline{y}$. Hence G_R is Hausdorff. □

One wide class of rings in which the ideals generated by irreducible elements are maximal are Dedekind domains. A wider class is formed by the so–called Bezout domains and still wider are the GCD–domains, integral domains R with identity in which each finite set of elements has a GCD in R. Should an ideal (p) generated by an irreducible element p not be maximal in R, then there would be a maximal ideal $M \subsetneqq R$. Let $x \in M \setminus (p)$ and $a = \mathrm{GCD}(p, x)$. Then on one hand $(p) \subset (p, x) \subset (a)$; on the other $a|p$, and since a is not a unit ($(a) \subset M \neq R$), $p \sim a$, i.e. $(p) = (a)$; a contradiction with $x \notin (p)$.

An example of a different approach to the deduction of separation properties T_0, T_1 and T_2 is given by the next proposition (whose proof is omitted):

Theorem 22. *If $\widetilde{P_1}$ is infinite, then G_R will be a T_0–, T_1–, or T_2–space according respectively as R satisfies the corresponding assumptions:*

- (δ_0) *any non–associate pair in R^0 can be written as (x, y) where only finitely many non–associate irreducibles of R divide the elements $x + uy$ for arbitrary units $u \in R$, or*
- (δ_1) *any non–associate pair x, y in R^0 satisfies (δ_0) relative to both orderings $(x, y), (y, x)$, or*
- (δ_2) *for any non–associate pair x, y in R, only finitely many non–associate irreducibles of R divide the element $ux + vy$ for arbitrary units $u, v \in R$.*

Finally we consider a few conclusions for $\mathbb{N}$ and $M_F(X)$ alone. Firstly, corresponding to Golomb's result [4] that $\mathbb{N}$ is not compact relative to D, we have:

Theorem 23. *(i) $\mathbb{N}$ is not compact relative to $\mathfrak{D}^*$.*
(ii) $M_F(X)$ is not compact relative to $\mathfrak{D}_F^*$ or $\mathfrak{D}_F$.
Hence $\mathbb{Z}^0$ and $F[X]^0$ are not compact under τ^*.

Proof. (i) Since $\mathfrak{D}^* \subsetneqq \mathfrak{D}$ on $\mathbb{N}$, Golomb's argument for D does not completely embrace $\mathfrak{D}^*$. However a very similar argument works: Simply note that the sets $(-1 + (p))^*$ for prime $p \in \mathbb{N}$ provide a $\mathfrak{D}^*$–open covering of $\mathbb{N}$ such that $(-1 + (p))^*$ contains $q - 1$ for a prime

$q \in \mathbb{N}$ if and only if $p = q$. Thus covering has no proper subcovering at all. Hence $\mathfrak{D}^*$ is also not compact.

(ii) For $M_F(X)$ it is sufficient to consider $\mathfrak{D}_F^*$ alone. Then, for $1 \neq a \in M_F(X)$, $\deg(a-1) \geq 1$ and $a = 1 + (a-1)$ lies in one or more $\mathfrak{D}^*$–open sets $(1+(p))^*$ for primes $p \in M_F(X)$. Thus these sets provide a $\mathfrak{D}_F^*$–open covering of $M_F(X)$ such that $(1+(p))^*$ contains $1+q$ for a prime $q \in M_F(X)$ if and only if $p = q$. Hence the covering has no proper subcoverings at all, and so $\mathfrak{D}_F^*$ is not compact. □

Some further negative conclusions are provided by:

Theorem 24. *Both $\mathbb{N}$ and $M_F(X)$ are neither compact nor T_3–spaces relative to $\mathfrak{D}^*$ and $\mathfrak{D}_F^*$, respectively.*

Proof. Since $\mathfrak{D}^* \subsetneq \mathfrak{D}$, the conclusion about $\mathfrak{D}^*$ are consequences of Golomb's results [4] that $\mathbb{N}$ is neither locally compact nor a T_3–space under $\mathfrak{D}$. Since $\mathfrak{D}_F^*$ is Hausdorff, it will suffice here to show that $\mathfrak{D}_F^*$ is not a T_3–topology:

For this purpose, now note that from the proof of Theorem 14 earlier it follows that $\langle \overline{p} \rangle = \theta((p) \setminus \{0\})$ is closed in G_R, for any prime element p in a principal ideal domain R, since in a principal ideal domain (PID) the maximal ideals are the ideals generated by prime singletons. Therefore $(p)^* = \rho(\langle \overline{p} \rangle)$ is $\mathfrak{D}_F^*$–closed in $M_F(X)$, if $R = F[X]$. Next suppose that V, W are disjoint $\mathfrak{D}_F^*$–open sets containing 1 and $(X)^*$, respectively.

In that case $1 \in (x+(a))^* \subset V$ for some invertible coset $x+(a)$ with $0 \leq \deg(x) < \deg(a)$. Thus $x = 1$. Also $X|a$, because *otherwise* $a = \gamma_0 + \gamma_1 X + \ldots$ for $\gamma_i \in F, \gamma_0 \neq 0$, which implies that some multiple of X lies in $(1+(a))^* \subset V$, and hence $V \cap W \neq \emptyset$. It follows that $a \in (X)^* \subset W$, and so $a \in (y+(b))^* \subset W$ for some invertible coset $y+(b)$. This implies that $(a,b) = 1$. Therefore the Chinese Remainder Theorem implies that there is an element $z \in F[X]^0$ with $z \equiv 1 \pmod{a}$ and $z \equiv y \pmod{b}$. So $z^* \in (1+(a))^* \cap (y+(b))^*$ and $V \cap W \neq \emptyset$, which is false. Hence $\{1\}$ cannot be separated from the $\mathfrak{D}_F^*$–closed set $(X)^*$ by any open set V, W.

Thus $\mathfrak{D}_F^*$ is not a T_3–topology. □

4. Selected applications

Lemma 17 shows that the assumptions about the ring R in Theorems 19 and 21 are satisfied if R is a residually finite Dedekind domain with infinite set $\widetilde{\mathcal{P}_1}$ of the non–associate prime elements. Proposition 15(3) allows density to replace strong density in Theorem 19 whenever G_R is T_1. Using this and the fact that G_R is Hausdorff when assumption (iii) above is also true, which we proved in Theorem 21, one may deduce the next result

Theorem 25. *Suppose that R is a residually finite Dedekind domain with infinite set $\widetilde{\mathcal{P}_1}$ of the non–associate prime elements and let P be a subset of R such that $\widetilde{P} = \{\overline{x} : x \in P\}$ is infinite. Then Dirichlet's condition for $\widetilde{P}$ is valid if and only if $\widetilde{P}$ is dense in G_R.*

For $P = \mathcal{P}_1$, the set of prime elements of R we get the following result

Corollary 25.1. *Suppose that R is a residually finite PID with infinite set $\widetilde{\mathcal{P}_1}$ of associate–classes of prime elements. Then R satisfies Dirichlet's condition for $\mathcal{P}_1$ if and only if $\widetilde{\mathcal{P}_1}$ is dense in G_R.*

The following reformulation of the conclusion of Dirichlet's theorem on primes in arithmetic progressions appears repeatedly in the literature (c.f. [20, p.526](or [23, p.129]) or [24]).[3]

Corollary 25.2. *Let $(a,b) = 1$ with $0 \leq b < a$. Then $ax + b$ assumes for $x = 0, 1, 2, \ldots$ infinitely many prime values if and only if $ax + b$ assumes here at least one prime value.*

The proofs of this statement are sometimes faulty if x is not restricted to positive integers. For example, if b itself is a prime then the arguments used may reproduce b. Thus by exploiting the simple density only it is theoretically possible that the argument used does not ensure that the next constructed prime will "get on". This was the reason for introducing our concept of strong density. To complete the proof of the Corollary 25.2 using Theorem 19 instead of Theorem 25 note that the cases $a = 1, b = 0$ and $a = 2, b = 1$ can be trivially excluded from the rest of the proof. If $a > 2$ then we saw in the proof of Example 11.1 that $(b + a\mathbb{Z})^*$ splits into two progressions

$$b + a\mathbb{N} \quad \text{and} \quad a - b + a\mathbb{N}.$$

Either of these progressions contains at least one prime owing to the assumption of the Corollary. If $a > 2$ these primes are distinct, i.e. the set $(b + a\mathbb{Z})^*$ is strongly dense in $\mathfrak{D}^*$ and Theorem 19 applies.

Golomb [4] also claims to show that Dirichlet's theorem for $\mathbb{N}$ is equivalent to ordinary density of prime numbers in $\mathbb{N}$ relative to his topology $\mathfrak{D}$. However his proof actually employs *strong* density, via the use of a certain incompletely quoted auxiliary theorem on arithmetical progressions. Nevertheless as we saw, Golomb's conclusion can be retrieved with the aid of the fact that $\mathfrak{D}$ is Hausdorff.

A perhaps surprising facet of the previous analysis of the classical Dirichlet's theorem on primes in arithmetical progressions is the fact that the set P in the hypotheses of Theorem 19 does not consist necessarily of primes or irreducible elements. So our general treatment allows us to deduce some other instances of a not immediately related nature.

Using the Dirichlet theorem on primes in arithmetic progressions one can inductively show (c.f. [21, solution of Exercise 61] or [22, Exercise 69]) that every arithmetical progression $an + b$ with $(a,b) = 1$ contains at least one product of s distinct primes. Analogically we get

Corollary 25.3. *Suppose that R is a residually finite PID and that the set $\widetilde{\mathcal{P}}_1$ of associate-classes of prime elements in R is infinite. Let $\mathcal{P}_s$ for $s \in \mathbb{N}$ denote the set of products of s non-associate primes of R. Then $\widetilde{\mathcal{P}}_s$ satisfies Dirichlet's condition for $\widetilde{\mathcal{P}}_s$ for every $s \in \mathbb{N}$ if and only if $\widetilde{\mathcal{P}}_1$ is dense in G_R.*

Let us mention other applications connected with various forms of pseudoprimes. The proofs of their infiniteness in arithmetical progressions $an + b$ are mostly based on the fact that such progressions contain at least one of these pseudoprimes.

Thus for instance a composite positive integer n is called *pseudoprime* if $n|2^n - 2$. Rotkiewicz [15] based his proof that there exist infinitely many pseudoprimes of the form $an + b$ with $n \in \mathbb{N}$ on the fact that it is enough to show that an invertible arithmetical progression contains one pseudoprime. In our terminology this means that odd pseudoprimes

[3] A. Schinzel has kindly drawn our attention to two further references [19], [26], which cover special cases.

are dense in $\mathbb{N}$ and Corollary 25.1 may be applied to show the infinity of pseudoprimes. The same technigue was used for odd strong pseudoprimes in [11], or for certain odd strong Lehmer pseudoprimes in [17], etc. (see also [11], [14], [15], [16], [17], [18] for more details).

Szymiczek [25] proved (see also [10, p.10]) that there exist (squarefree) pseudoprimes with arbitrarily many prime factors. Since in view of the previous results primes and pseudoprimes behave in a certain sense similarly a natural question is whether a parallel result is true with pseudoprimes instead of primes. Corollary 25.3 gives a result which we did not find elsewhere

Corollary 25.4. *Given $a, b, s \in \mathbb{N}$, $(a, b) = 1$, the arithmetical progression $an + b, n \in \mathbb{N}$ contains infinitely many products of s pseudoprimes.*

Due to the result mentioned above the same conclusion is true for odd strong pseudoprimes, odd strong Lehmer pseudoprime, etc. instead of pseudoprimes.

One possible question induced by previous results may ask which topologies allow the conclusion of Theorems 19 or 25. The impossibility of extending Dirichlet's theorem on primes to sequences with $(a, b) \neq 1$ is apparent. In [10] it is shown that if $(a, b) \neq 1$ the same conclusion is also true for the pseudoprimes.

References

1. Artin,E.: *Quadratische Körper in Gebiete der höheren Kongruenzen, I-II*, Math. Z. **19**, 1924, 153–246
2. Chew,L.–K. and Lawn,Sh.: *Residually finite fields*, Canad. J. Math. **22**, 1970, 92–101
3. Gilmer,R.: *Multiplicative Ideal Theory*, M.Dekker, Inc., 1972
4. Golomb,S.W.: *Arithmetica topologica*, In: Proc. 1961 Prague Symp. on *General Topology and its Relations to Modern Analysis and Algebra*, pp. 179–186 (Academic Press, 1962)
5. Hanly,S.: *Solution of problem E1218*, Amer. Math. Monthly **64**, 1957, 742
6. Hayes,D.R.: *The distribution of irreducibles in $GF[q, x]$*, Trans. Amer. Math. Soc. **117**, 1965, 101–112
7. Hirano,Y.: *On residually finite rings*, Math. J. Okayama Univ. **35**, 1993, 155–167
8. Kelley,J.L.: *Topology*, van Nostrand Inc. Toronto – London – New York 1957
9. Kornblum,H.: *Über die Primfunktionen in einer arithmetischen Progression*, Math. Z. **5**, 1919, 100–111
10. Pomerance,C. and Selfridge,J.L. and Wagstaff,S.jr.: *The pseudoprimes to 25.10^9*, preprint
11. van der Poorten,A.J. and Rotkiewicz, A.: *On strong pseudoprimes in arithmetic progressions*, J. Austral. Math. Soc. **29**, 1980, 316–321
12. Porubský,Š.: *Results and problems on covering systems of residue classes*, Mitt. Math. Sem. Giessen, Heft 150, 1981, 1–85
13. Reis,C.M. and Viswanathan,T.M.: *A compactness property for prime ideals in Noetherian ring*, Proc. Amer. Math. Soc. **25**, 1970, 353–356
14. Rotkiewicz, A.: *Sur les nombres pseudopremiers de la forme $ax + b$*, C. R. Acad. Sci. Paris **257**, 1963, 2601–2604
15. Rotkiewicz, A.: *On the pseudoprimes of the form $ax+b$*, Proc. Cambridge Phil. Soc. **63**, 1967, 389–392
16. Rotkiewicz, A.: *On the pseudoprimes of the form $ax+b$ with respect to the sequences of Lehmer*, Bull. Acad. Polonaise de Sci., Serie des sci. math. astr. et phys. **20**, 1972, 349–354
17. Rotkiewicz, A.: *On Euler Lehmer pseudoprimes and strong pseudoprimes with parameters L, Q in arithmetic progressions*, Math. Comp. **39**, 1982, 239–247
18. Rotkiewicz, A.: *On strong Lehmer pseudoprimes in the case of negative discriminant in arithmetic progressions*, Acta Arith. **68**, 1994, 145–151
19. Schur,I.: *Über die Existenz unendlich vieler Primzahlen in einigen speziellen arithmetischen Progressionen*, S.–B.Berlin Math. Ges. **11**, 1912, 40–50
20. Sierpiński,W.: *Teoria liczb*, (Polish) [Theory of numbers], 3rd ed., Monografie Matematyczne, Vol. XIX, Warsaw–Wrocław, 1950

21. Sierpiński,W.: *200 zadań z elementarnej teorii liczb*, (Polish) [200 problems in the elementary theory of numbers], Biblioteczka Matematyczna, Vol. 17, Panstwowe Zakłady Wydawnictw Szkolnych, Warsaw 1964
22. Sierpiński,W.: *250 Problems in Elementary Number Theory*, American Elsevier & PWN, New York–Warsaw 1970
23. Sierpiński,W.: *Elementary Theory of Numbers*, North–Holland Math. Libr., Vol.31, North–Holland, PWN (Polish Scientific Publishers), Amsterdam–Warsaw, 1988
24. Spira,R.: *Problem E 1218*, Amer. Math. Monthly **63**, 1956, p.342
25. Szymiczek,K.: *On pseudoprimes which are products of distinct primes*, Amer. Math. Monthly **74**, 1967, 35–37
26. Wójcik,J.: *A refinement of a theorem of Schur on primes in arithmetic progressions*, Acta Arith. **11**, 1966, 433–436
27. Zariski,O. and Samuel,P.: *Commutative Algebra I*, GTM Vol.28, Springer Verlag, New York–Heidelberg–Berlin, 1979

John Knopfmacher
Department of Mathematics
University of Witwatersrand
P.O. Wits 2050
Johannesburg
South Africa
E-mail: 036knj@cosmos.wits.ac.za

Stefan Porubsky
Department of Mathematics
Institute of Chemical Technology
Technická 5
166 28 Prague
Czech Republik
E-mail: porubsks@vscht.cz

Received: 20.06.96
Revised: 18.09.96