

THE EUCLIDEAN CRITERION FOR IRREDUCIBLES

PETE L. CLARK

ABSTRACT. We recast Euclid’s proof of the infinitude of prime numbers as a **Euclidean Criterion** for a domain to have infinitely many atoms. We make connections with Furstenberg’s “*topological*” proof of the infinitude of prime numbers and show that our criterion applies even in certain domains in which not all nonzero nonunits factor into products of irreducibles.

1. INTRODUCTION

This article has its genesis in the first meeting of a graduate *VIGRE research group* taught by Paul Pollack and me in Fall 2015: *Introduction to the Process of Mathematical Research*. Rather than concentrating on a fixed topic preselected by us, this group had the less orthodox goal of guiding students through the process of selecting and performing research on their own. One technique we tried to inculcate is exploitation of the many-to-one relation between theorems and proofs. A good theorem has several proofs, and you will know two proofs are different when can be used to prove further theorems the other cannot.

We presented seven proofs of Euclid’s Proposition IX.20: there are infinitely many prime numbers. Here is the first proof I presented: suppose given a domain R that is not a field, in which each nonzero nonunit factors into irreducibles and whenever $x \in R$ is a nonzero nonunit then $x + 1$ is not a unit; then there is at least one irreducible element f_1 , and given irreducibles f_1, \dots, f_n , by factoring $f_1 \cdots f_n + 1$ we get a new irreducible element. It was pointed out that this argument, though correct, does not imply Euclid’s result: $x = -2$ is a problem. Some salvages were suggested: in \mathbb{Z} it is enough to replace $f_1 \cdots f_n$ by $-f_1 \cdots f_n$, if necessary.

Here we present a general fix – a **Euclidean Criterion** for a domain to have infinitely many nonassociate irreducibles – and explore its consequences. We soon find ourselves on a scenic tour of 20th century mathematics, as we engage with work of Jacobson, Furstenberg, Cohen-Kaplansky and Anderson-Mott, among others.

1.1. Acknowledgments.

Thanks to all members of the 2015-2016 Introduction to Mathematical Research UGA VIGRE group. Conversations with Saurabh Gosavi, Noah Lebowitz-Lockard, Robert Samalis, Lee Troupe and Lori D. Watson were helpful.

My group coleader Paul Pollack made key contributions: first, he emphasized that the Euclidean Criterion automatically yields pairwise comaximality. Second, Theorem 2.9 was inspired by [P, Thm. 1.16], and though I came up with the statement, I could prove it only in various special cases. The proof included here is his.

Date: December 18, 2016.

I am grateful to two anonymous referees for their careful, detail-oriented reports. In particular, Example ?? was suggested by the “first” referee.

2. THE EUCLIDEAN CRITERION

2.1. A primer on factorization in domains.

By a **ring** we will mean a commutative ring with a multiplicative identity. We denote the set of nonzero elements of R by R^\bullet . An element $x \in R$ is a **unit** if there is $y \in R$ such that $xy = 1$. We denote the group of units of R by R^\times . For a subset S of a ring R , we denote by (S) the ideal of R generated by S . (As is standard, we write (x_1, \dots, x_n) for $(\{x_1, \dots, x_n\})$.) Ideals I and J in R are **comaximal** if $I + J = R$. Elements $a, b \in R$ are comaximal if (a) and (b) are comaximal: $(a, b) = R$. An indexed family of ideals $\{I_i\}$ is **pairwise comaximal** if $I_i + I_j = R$ for all $i \neq j$, and similarly for pairwise comaximal elements.

A **domain** is a nonzero ring in which $x, y \neq 0 \implies xy \neq 0$. For $x, y \in R$ we say **x divides y** and write $x \mid y$ if there is $c \in R$ such that $cx = y$. Elements x and y are **associates** if $y = ux$ for some $u \in R^\times$. An element x of a domain is **irreducible** if it is a nonzero nonunit and $x = yz$ implies $y \in R^\times$ or $z \in R^\times$. A **prime element** $p \in R$ is an element $p \in R^\bullet$ for which (p) is a prime ideal. Thus a nonzero nonunit p is prime if and only if $p \mid ab \implies p \mid a$ or $p \mid b$.

An **atom** in a domain R is a principal ideal (x) generated by an irreducible element x . Thus two irreducibles of a domain R determine the same atom if and only if they are associate. (It is more common in the literature for the terms “atom” and “irreducible” to be fully synonymous, but this minor distinction is convenient for our purposes: usually we will count to count irreducibles in a domain *up to associates*, but sometimes we will want to count irreducibles.) A **Furstenberg domain** is a domain R in which every nonzero nonunit has an irreducible divisor.¹ An **atomic domain** is a domain R in which for every nonzero nonunit $x \in R$ there are irreducible elements f_1, \dots, f_n such that $x = f_1 \cdots f_n$. A **unique factorization domain (UFD)** is an atomic domain such that if $f_1, \dots, f_m, g_1, \dots, g_n$ are irreducibles such that $f_1 \cdots f_m = g_1 \cdots g_n$, then $m = n$ and there is a bijection $\sigma : \{1, \dots, m\} \rightarrow \{1, \dots, n\}$ such that $(f_i) = (g_{\sigma_i})$ for all $1 \leq i \leq m$.

Prime elements are irreducible. In general the converse is false! An atomic domain is a UFD iff every irreducible is prime [Co73], [Cl, Thm. 15.8]. The terminology can be confusing in light of the definition of a prime number p as a positive integer not divisible by any $1 < n < p$: this means p is irreducible in \mathbb{Z} . But Euclid showed

$$p \mid ab \implies p \mid a \text{ or } p \mid b.$$

From this one can show the Fundamental Theorem of Arithmetic: \mathbb{Z} is a UFD. A **principal ideal domain (PID)** is a domain in which each ideal is generated by a single element. Every PID is a UFD. It follows from the Euclidean algorithm that \mathbb{Z} is a PID. A **Bézout domain** is a domain in which every finitely generated ideal is principal. A ring is **Noetherian** if all of its ideals are finitely generated. Noetherian domains are atomic [Co73, p. 4], [Cl, Prop. 15.3]. Thus a PID is precisely a Noetherian Bézout domain. A **Dedekind domain** is a domain in which each nonzero proper ideal factors uniquely into prime ideals. A domain is

¹The explanation for the terminology comes in §3.1.

Dedekind iff it is Noetherian, **of dimension at most one** (nonzero prime ideals are maximal) and **integrally closed** (an element of the fraction field satisfying a monic polynomial with coefficients in R lies in R) [J, §10.2], [Cl, Thm. 20.10].

Working in a *domain* rather than a general ring confers certain advantages:

- Fact 1.** a) *Every nonzero ideal in a ring contains a nonzero principal ideal.*
 b) *If R is a domain and $\alpha \in R^\bullet$, $x \in R \mapsto \alpha x$ gives a bijection from R to (α) .*
 c) *Thus for every nonzero ideal I of a domain R we have $\#I = \#R$.*
 d) *For nonzero ideals I and J of R , $I \cap J$ contains IJ and thus is nonzero.*

2.2. The Euclidean Criterion.

A ring R satisfies **Condition (E)** if for all $x \in R^\bullet$, there is $y \in R$ such that $yx + 1 \notin R^\times$. In other words, if $x \neq 0$ then $1 + (x) \not\subset R^\times$. By Fact 1a) this is equivalent to: if I is a nonzero ideal of R then $1 + I \not\subset R^\times$, though we will defer consideration of this restatement until later on.

Example 2.1.

- a) *The ring \mathbb{Z} satisfies Condition (E). Indeed, $\mathbb{Z}^\times = \{\pm 1\}$, so for $x \in \mathbb{Z}^\bullet$, take $y = 1$ if x is positive and $y = -1$ if x is negative; then $yx \geq 1$ so $yx + 1 \geq 2$.*
 b) *For any domain R , the polynomial ring $R[t]$ satisfies Condition (E). Indeed, $(R[t])^\times = R^\times$, so for any $x \in R[t]^\bullet$, take $y = t$.*
 c) *$R = \mathbb{Z}[i]$ satisfies Condition (E). Indeed $\mathbb{Z}[i]^\times = \{1, i, -1, -i\}$, so this is geometrically clear: for any $x \in \mathbb{Z}[i]^\bullet$, if we multiply it by a y with large enough $|y|$, then yx will be much more than 1 unit away from any point on the unit circle.*

Proposition 2.2. *A domain R with $\#R > \#R^\times$ satisfies Condition (E).*

Proof. For $x \in R^\bullet$, the map $\iota : R \rightarrow R$ given by $y \mapsto yx + 1$ is an injection. Thus $\#\iota(R) = \#R > \#R^\times$, so it cannot be that $\iota(R) \subset R^\times$. \square

And here we go:

Theorem 2.3. (The Euclidean Criterion)

Let R be a domain, not a field, satisfying Condition (E).

- a) *There is an infinite sequence $\{a_n\}_{n=1}^\infty$ of pairwise comaximal nonunits.*
 b) *If R is also Furstenberg, it admits an infinite sequence $\{f_n\}_{n=1}^\infty$ of pairwise comaximal irreducibles. Thus $\{(f_n)\}_{n=1}^\infty$ is a sequence of distinct atoms in R .*

Proof. a) By induction on n . Let $a_1 \in R$ be a nonzero nonunit. Having chosen a_1, \dots, a_n pairwise comaximal, by Condition (E) there is $y \in R$ such that $a_{n+1} := ya_1 \cdots a_n + 1 \notin R^\times$. Clearly $(a_i, a_{n+1}) = R$ for all $1 \leq i \leq n$.

b) By induction on n . Since R is Furstenberg and not a field, it has an irreducible f_1 . Having chosen pairwise comaximal irreducibles f_1, \dots, f_n , by Condition (E) there is $y \in R$ such that $x = yf_1 \cdots f_n + 1$ is a nonzero (since $f_1 \notin R^\times$) nonunit, so x has an irreducible factor f_{n+1} . For all $1 \leq i \leq n$ we have

$$1 = (x/f_{n+1})f_{n+1} - (y \prod_{j \neq i} f_j) f_i,$$

so f_i, f_{n+1} are comaximal. Finally, if x and y are pairwise comaximal irreducibles, then $(x), (y) \subsetneq R$ and $(x) + (y) = (x, y) = R$, so we must have $(x) \neq (y)$. \square

Here are two applications of the Euclidean Criterion. The first two are immediate.

Theorem 2.4. a) For any domain R , $R[t]$ has infinitely many atoms.
 b) In particular, let D be a UFD and let $R = D[t_1, \dots, t_n]$. Then R is a UFD satisfying Condition (E), so R has infinitely many nonassociate prime elements.
 c) The Gaussian integers $\mathbb{Z}[i]$ have infinitely many atoms. Since $\mathbb{Z}[i]$ is a PID, there are infinitely many nonassociate prime elements.

Theorem 2.5. Let R be a Furstenberg domain, not a field, such that $\#R > \#R^\times$. Then R has infinitely many atoms.

Theorem 2.6. Let R be a Furstenberg domain, let \mathcal{I} be the set of all irreducible elements of R . Then \mathcal{I} is either empty (if R is a field) or infinite (otherwise).

Proof. Assume $\mathcal{I} \neq \emptyset$ and fix $f \in \mathcal{I}$. If R^\times is finite, Theorem 2.5 yields infinitely many atoms. If R^\times is infinite, then $\{uf \mid u \in R^\times\}$ is an infinite subset of \mathcal{I} . \square

2.3. Supplement: Irreducibles in Residue Classes.

We switch from an ancient theorem to matters of contemporary interest if we ask for infinitely many primes *satisfying certain additional conditions*. Here is a result along these lines, relatively modest over \mathbb{Z} , but of a general algebraic nature.

Lemma 2.7. Let a, b, c be elements of a ring R . If $(a, b) = R$ and $c \mid a + b$, then $(a, c) = (b, c) = R$.

Proof. Let $d \in R$ be such that $cd = a + b$. Then

$$(a, c) \supset (a, cd) = (a, a + b) = (a, b) = R. \quad \square$$

Lemma 2.8. Let R be a domain, not a field, satisfying Condition (E). For any $at + b \in R[t]$ with $a \in R^\bullet$, there is $x \in R$ such that $ax + b$ is a nonzero nonunit.

Proof. Put $P(t) = at + b$. If $b = 0$, take any nonzero nonunit $x \in R$. If $b \in R^\times$, by Condition (E) there is $x \in R$ such that $b^{-1}ax + 1 \notin R^\times$ so $P(x) = b(b^{-1}ax + 1)$ is a nonzero nonunit. If $b \in R$ is a nonzero nonunit, take $x = 0$. \square

The proof of the following result was suggested to me by Paul Pollack.

Theorem 2.9. Let R be an atomic domain satisfying Condition (E), let I be a nonzero ideal of R , and let H be a proper subgroup of $(R/I)^\times$. Then there are infinitely many pairwise comaximal irreducibles f such that the class of f modulo I lies in $(R/I)^\times \setminus H$.

Proof. Let $r : R \rightarrow R/I$ be the quotient map, let $\alpha \in R$ be such that $r(\alpha) \in (R/I)^\times \setminus H$, and let $\beta \in R$ be such that $\alpha\beta - 1 \in I \setminus \{0\}$. Inductively, assume that we have pairwise comaximal irreducibles f_1, \dots, f_n of R such that $(f_i, \alpha) = (f_i, I) = R$ for all i and such that $r(f_i) \notin H$. Let

$$P(t) = (\alpha t + 1)(\alpha\beta - 1)f_1 \cdots f_n + \alpha \in R[t].$$

(We need to include the base case $n = 0$, and in this case $f_1 \cdots f_n = 1$.) By Lemma 2.8 there is $x \in R$ such that

$$y = (\alpha x + 1)(\alpha\beta - 1)f_1 \cdots f_n + \alpha$$

is a nonzero nonunit, so we get an irreducible factorization

$$y = g_1 \cdots g_s$$

with $s \geq 1$. Then

$$r(g_1) \cdots r(g_s) = r(y) = r(\alpha) \in (R/I)^\times \setminus H,$$

so $(g_j, I) = 1$ for all j and there is at least one g_j , say g_1 , such that $r(g_1) \notin H$. Now g_1 cannot be associate to any f_i ; if so g_1 and hence also f_i would divide α : if $\alpha \in R^\times$ this contradicts the irreducibility of f_i ; if not, this contradicts $(f_i, \alpha) = 1$. Moreover $y \equiv -f_1 \cdots f_n \pmod{\alpha}$ so $y \in (R/\alpha)^\times$, hence also $g_1 \in (R/\alpha)^\times$, i.e., $(g_1, \alpha) = R$. Finally, since

$$(\alpha x + 1)(\alpha\beta - 1)f_1 \cdots f_n \equiv -f_1 \cdots f_n \pmod{\alpha},$$

we have $((\alpha x + 1)(\alpha\beta - 1)f_1 \cdots f_n, \alpha) = R$, so by Lemma 2.7 we have

$$(g_1, (\alpha x + 1)(\alpha\beta - 1)f_1 \cdots f_n) = R$$

so $(g_1, f_i) = R$ for all i . Thus we may take $f_{n+1} = g_1$, completing the induction. \square

When $R = \mathbb{Z}$, we get: for any proper subgroup $H \subsetneq (\mathbb{Z}/N\mathbb{Z})^\times$, there are infinitely many prime numbers p such that $\pm p \pmod{N} \notin H$. Moreover, in this classical case one can run the argument with positive integers only and so get rid of the annoying \pm . This is a special case of Dirichlet's theorem on primes in arithmetic progressions. It is an observation of A. Granville – unpublished by him, but reproduced in [P, Thm. 1.16] – that this case can be proved in an elementary “Euclidean” way. The special case of trivial H – for all $N \geq 3$ there are infinitely many primes $p \not\equiv 1 \pmod{N}$ – is older and better known. It is also simpler – just consider $Np_1 \cdots p_{n-1} - 1$. This case does not use that \mathbb{Z} is a UFD, but Granville's argument does. The most auspicious replacement for coprimality arguments is by comaximality, and that is what we've done here.

3. A “TOPOLOGICAL” INTERLUDE

3.1. Furstenberg's Lemma.

In this section we will give several proofs of the following result.

Theorem 3.1. *Let R be a Furstenberg domain with at least one and only finitely many atoms f_1, \dots, f_n . Then:*

- a) *We have $\#R^\times = \#R$.*
- b) *More precisely there is a nonzero ideal I of R such that $1 + I \subset R^\times$.*

Theorem 3.1 is the contrapositive of part b) of the Euclidean Criterion, without the information on comaximality. The proofs that we give here are inspired by the famous paper of H. Furstenberg [Fu55]. The essential core of his argument is the observation that in \mathbb{Z} the set of elements not divisible by any prime number is ± 1 . Notice that has nothing to do with the natural ordering of \mathbb{Z} that underlies most of the classical proofs of Euclid's Theorem. In fact the property of \mathbb{Z} being used is that \mathbb{Z} is a Furstenberg domain.

Lemma 3.2. *(Furstenberg's Lemma)*

- a) *A domain R is a Furstenberg domain iff $R^\times = \bigcap_{f \text{ irreducible}} R \setminus (f)$.*
- b) *In a Furstenberg domain with at least one and only finitely many atoms $(f_1), \dots, (f_n)$, we have $\bigcap_{i=1}^n (R \setminus (f_i)) = R^\times$.*

The proof is virtually immediate and is left to the reader.

3.2. Following Furstenberg.

Let R be a domain. By Fact 1d), for each $x \in R$, the family

$$\mathcal{C}(x) = \{x + I \mid I \text{ is a nonzero ideal of } R\}$$

is closed under finite intersections, so $\{\mathcal{C}(x)\}_{x \in X}$ is a system of neighborhood bases for a topology on R – let us call it the **adic topology** – in which $U \subset R$ is open iff for all $x \in U$ there is a nonzero ideal I with $x + I \subset U$. By Fact 1c), every nonempty open has cardinality $\#R$.

Proof of Theorem 3.1: let R be a Furstenberg domain with at least one and only finitely many atoms $(f_1), \dots, (f_n)$. Then each (f_i) is open, hence its complement $R \setminus (f_i)$, being a union of cosets of (f_i) , is also open. By Furstenberg's Lemma $R^\times = \bigcap_{i=1}^n (R \setminus (f_i))$ is open. Since $1 \in R^\times$, we have $\#R^\times = \#R$. More precisely, $R^\times \supset 1 + I$ for some nonzero ideal of R .

3.3. Following Cass-Wildenberg.

Let R be a domain, and let \mathbb{F}_2 be the field of two elements. For an ideal I of R , a function $f : R \rightarrow \mathbb{F}_2$ is **I-periodic** if $f(x + y) = f(x)$ for all $x \in X$ and $y \in I$.

Lemma 3.3. *Let R be a domain, and let I, I_1, \dots, I_n be nonzero ideals of R .*

- a) *If $I_2 \subset I_1$ and $f : R \rightarrow \mathbb{F}_2$ is I_1 -periodic, it is also I_2 -periodic.*
- b) *If for all $1 \leq i \leq n$, $f_i : R \rightarrow \mathbb{F}_2$ is I_i -periodic, then the pointwise product $f_1 \cdots f_n : R \rightarrow \mathbb{F}_2$ is $I_1 \cdots I_n$ -periodic.*
- c) *If $f : R \rightarrow \mathbb{F}_2$ is I -periodic, then for all $x \in R$, we have*

$$\#\{y \in R \mid f(y) = f(x)\} = \#R.$$

Proof. a) This is immediate from the definition.

b) Certainly $f_1 \cdots f_n$ is $\bigcap_{i=1}^n I_i$ -periodic, and $\bigcap_{i=1}^n I_i \supset I_1 \cdots I_n$. Apply part a).

c) Choose a nonzero $\alpha \in I$. Then $f(x + R\alpha) = f(x)$, and $\#R\alpha = \#R$. \square

Proof of Theorem 3.1:

Step 1: For $1 \leq i \leq n$, let $\chi_i : R \rightarrow \mathbb{F}_2$ be the characteristic function of (f_i) ; put

$$\chi = \prod_{i=1}^n (1 - \chi_i).$$

Each χ_i is (f_i) -periodic, hence so too is $1 - \chi_i$, and thus χ is $(f_1 \cdots f_n)$ -periodic. Moreover χ is the characteristic function of $\bigcap_{i=1}^n (R \setminus (f_i)) = R^\times$.

Step 2: Since $\chi(1) = 1$, $\#R^\times = \{x \in R \mid \chi(x) = 1\} = \#R$: part a).

Step 3: More precisely $\chi(1 + Rf_1 \cdots f_n) = 1$, so $Rf_1 \cdots f_n + 1 \subset R^\times$: part b). \square

3.4. Following Mercer.

Let R be a domain. Call a subset $X \subset R$ **lovely** if it is of the form $x + I$ for $x \in R$ and a nonzero ideal I of R , i.e., if it is a coset of a nonzero ideal. Call a subset $X \subset R$ **pleasant** if it is a union of lovely subsets. If I is a nonzero ideal of R , then $R \setminus I$ is a union of cosets of I hence pleasant. If $X, Y \subset R$ are pleasant sets and $x \in X \cap Y$, there are nonzero ideals I, J of R such that $x + I \subset X$ and $x + J \subset Y$. By Fact 1d) $x + (I \cap J) = (x + I) \cap (x + J)$ is a lovely subset of $X \cap Y$ containing x . So $X \cap Y$ is pleasant. By Fact 1c), every nonempty pleasant subset has cardinality $\#R$.

Proof of Theorem 3.1: let R be a Furstenberg domain with at least one and only finitely many atoms $(f_1), \dots, (f_n)$. By Furstenberg's Lemma, R^\times is the finite intersection of complements of nonzero ideals so is pleasant. Since $1 \in R^\times$, we have $\#R^\times = \#R$. More precisely, $R^\times \supset 1 + I$ for some nonzero ideal of R .

3.5. Debriefing.

The three proofs given above are generalizations of the proofs of Euclid's Theorem given by Furstenberg [Fu55], Cass-Wildenberg [CW03] and Mercer [Me09]. The latter two works take the detopologization of Furstenberg's proof as their goal.

Our presentation of the argument of §3.4 differs superficially from Mercer's. We chose the words "lovely" and "pleasant" precisely because they do not have a commonly understood technical mathematical meaning: had we said "basic" and "open" then the reader's attention would have been drawn to the fact that since the basic sets are closed under finite intersections, they form the base of a topology. Mercer's exposition takes pains to point out that the underlying fact here is just that finite intersections of unions are unions of finite intersections. Of course this is a basic logical principle: conjunctions distribute over disjunctions and conversely. Like many basic logical principles it is completely innocuous when used in context (as in our version of the argument). That the pleasant sets form a topology on R is no more and no less than a crisp enunciation of the facts we need to check in the first part of the proof. I find it quite striking (and pleasant!) that the facts can be enunciated in this way, but I must now agree with those who have claimed that there is no *essential topological content* in Furstenberg's argument.²

The use of periodic functions involves slightly more packaging, but of a standard kind: it is well known that the Boolean ring 2^R of subsets of R can be represented as the ring $\text{Maps}(R, \mathbb{F}_2)$ with pointwise addition and multiplication. We recommend wikipedia and Glaymann [Gl67] as references. Glaymann develops this correspondence and applies it to prove such identities as $A\Delta B = C \iff B\Delta C = A \iff C\Delta A = B$...in a manner intended to be used in the high school classroom. This is an interesting snapshot of "the new math" near its zenith.

3.6. The Ubiquitous Theorem.

Here is a result that complements Theorem 3.1. It is not deep, but it will play a recurring role for us as a common intersection of various constructions and themes. The first proof that we give follows the "topological conceit" of this section. We will give other, simpler, proofs later on.

Theorem 3.4. *Let R be a domain, not a field, with only finitely many maximal ideals $\mathfrak{m}_1, \dots, \mathfrak{m}_n$. Then:*

- a) *We have $\#R^\times = \#R$.*
- b) *More precisely there is a nonzero ideal I of R such that $1 + I \subset R^\times$.*

Proof. We endow R with the topology for which, for $x \in R$, $\mathcal{C}(x) = \{x + \mathfrak{m} \mid \mathfrak{m} \text{ is a maximal ideal of } R\}$ is a neighborhood subbase at x : that is, $U \subset R$ is open

²Furstenberg does not claim a *topological proof of the infinitude of the primes* but rather a "topological" proof of the infinitude of the primes.

iff for all $x \in U$ there is a subset $J \subset \{1, \dots, n\}$ such that

$$\bigcap_{i \in J} (x + \mathfrak{m}_i) = x + \bigcap_{i \in J} \mathfrak{m}_i \subset U.$$

Fact 1 gives $\bigcap_{i \in J} \mathfrak{m}_i \supsetneq (0)$, so every nonempty open has cardinality $\#R$. Each $R \setminus \mathfrak{m}_i$, being a union of cosets of \mathfrak{m}_i , is also open. Therefore

$$R^\times = \bigcap_{i=1}^n (R \setminus \mathfrak{m}_i)$$

is open. Since $1 \in R^\times$ we have $\#R^\times = \#R$. More precisely there is a subset $J \subset \{1, \dots, n\}$ such that $1 + \bigcap_{i \in J} \mathfrak{m}_i \subset R^\times$, and thus also $1 + \bigcap_{i=1}^n \mathfrak{m}_i \subset R^\times$. \square

3.7. Supplement: Further Topologies on a Domain.

Here is a common generalization of Theorems 3.1 and 3.4: let \mathcal{J} be a family of nonzero ideals of a domain R , and suppose there are $I_1, \dots, I_n \in \mathcal{J}$ such that $R^\times = \bigcap_{i=1}^n (R \setminus I_i)$. Then $1 + \bigcap_{i=1}^n I_i \subset R^\times$, so in particular $\#R^\times = \#R$.

Look again at Theorem 3.1: instead of taking \mathcal{J} to be the family of all nonzero ideals, we could take $\mathcal{J} = \{(f_1), \dots, (f_n)\}$ and endow R with the unique translation-invariant topology with \mathcal{J} as a neighborhood subbase at 0. This coarsens the adic topology³ so that being open yields the sharper conclusion $1 + \bigcap_{i=1}^n (f_i) \subset R^\times$. In particular $1 + (f_1 \cdots f_n) \subset R^\times$. We are back to a version of Euclid's argument.

The adic topology on \mathbb{Z} is not very interesting *as a topological space*: it is countably infinite, metrizable, totally disconnected and without isolated points, hence homeomorphic to the Euclidean topology on \mathbb{Q} . In [Go59], Golomb proved Euclid's Theorem using the topology on \mathbb{Z}^+ with base the one-sided arithmetic progressions $\{an + b \mid n \in \mathbb{Z}^+\}$ for *coprime* $a, b \in \mathbb{Z}^+$. Golomb's topology makes \mathbb{Z}^+ into a countably infinite connected Hausdorff space...which is already interesting.

In a domain R that is not a field, we may consider the **Golomb topology** with neighborhood base at $x \in R$ given by

$$\mathcal{C}(x) = \{x + I \mid I \text{ is a nonzero ideal with } (x, I) = R\}.$$

In this topology every maximal ideal is closed, so in a domain that is not a field with only finitely many maximal ideals $\mathfrak{m}_1, \dots, \mathfrak{m}_n$, R^\times is open and thus contains $1 + I$ for some nonzero ideal I . We get another proof of Theorem 3.4.

The Golomb topology is never Hausdorff: the only open set containing 0 is R . However, the induced topology on R^\bullet can be (it is for \mathbb{Z}). After this paper was first written, jointly with Lebowitz-Lockard and Pollack we further studied the Golomb topology [CLL16]. In particular we show that the induced topology on R^\bullet is Hausdorff if and only if R satisfies Condition (E).

4. CONNECTIONS WITH IDEAL THEORY

For a ring R , we denote by $\text{MaxSpec } R$ the set of all maximal ideals of R .

³The adic topology on a domain is always Hausdorff, but in a Furstenberg domain with finitely many atoms, this new topology is not.

4.1. Comaximal Ideals.

Lemma 4.1. *Let $\{I_n\}_{n=1}^\infty$ be a sequence of pairwise comaximal proper ideals in a ring R . Then $\text{MaxSpec } R$ is infinite.*

Proof. For $n \in \mathbb{Z}^+$, let \mathfrak{m}_n be a maximal ideal containing I_n . If for $n_1 \neq n_2$ we had $\mathfrak{m}_{n_1} = \mathfrak{m}_{n_2}$ then $R = I_{n_1} + I_{n_2} \subset \mathfrak{m}_{n_1}$, contradiction. \square

In particular, part a) of the Euclidean Criterion implies that a domain that is not a field and that satisfies Condition (E) has infinitely many maximal ideals. Thus we get another proof of Theorem 3.4....but by no means our last.

4.2. Euclid Meets Jacobson.

Now is the time to examine the more explicitly ideal-theoretic statement of Condition (E): for all nonzero ideals I , we have $1 + I \not\subset R$. Some readers will now see – or will have already seen – the connection with the Jacobson radical, but we will not assume a prior familiarity. In fact we will use the Euclidean Criterion to motivate a self-contained discussion of this and other ideal-theoretic concepts.

Proposition 4.2. [AM, Prop. 1.9], [Cl, Prop. 4.14] *For a ring R , let*

$$J(R) = \bigcap_{\mathfrak{m} \in \text{MaxSpec } R} \mathfrak{m},$$

*the **Jacobson radical** of R . For $x \in R$, the following are equivalent:*

- (i) $x \in J(R)$.
- (ii) For all $y \in R$, $yx + 1 \in R^\times$.

Proof. (i) \implies (ii): By contraposition: suppose there is $y \in R$ such that $z = yx + 1 \notin R^\times$. Then z lies in some maximal ideal \mathfrak{m} . If also $x \in \mathfrak{m}$, then $yx \in \mathfrak{m}$ and thus also $z - yx = 1 \in \mathfrak{m}$, contradiction. So x does not lie in \mathfrak{m} and thus $x \notin J(R)$. (ii) \implies (i): Again by contraposition: suppose that there is a maximal ideal \mathfrak{m} such that $x \notin \mathfrak{m}$. Then $\mathfrak{m} \subsetneq (\mathfrak{m}, x)$, so $(\mathfrak{m}, x) = R$. It follows that there is $m \in \mathfrak{m}$ and $y \in R$ such that $m + yx = 1$. Thus $(-y)x + 1 = -m \in \mathfrak{m}$ so is not a unit. \square

We get immediately:

Corollary 4.3. *A ring R satisfies Condition (E) iff $J(R) = (0)$.*

This gives a third proof of Theorem 3.4: if R has only finitely many maximal ideals $\mathfrak{m}_1, \dots, \mathfrak{m}_n$, then

$$J(R) = \bigcap_{i=1}^n \mathfrak{m}_i \supset \prod_{i=1}^n \mathfrak{m}_i \supsetneq \{0\}.$$

Apply Corollary 4.3.

A ring with zero Jacobson radical is called **semiprimitive**.⁴

⁴Or **Jacobson semisimple** or **J-semisimple**.

4.3. Some Questions and Some Answers.

We now raise some natural questions...and answer them.

Question 4.4. *In part b) of the Euclidean Criterion, must we assume that R is a Furstenberg domain?*

Question 4.5. *A semiprimitive domain, not a field, has infinitely many maximal ideals. Must a domain with infinitely many maximal ideals be semiprimitive?*

Question 4.6. *Let R be a Furstenberg domain.*

a) *If R is not semiprimitive, can it still have infinitely many atoms?*

b) *Can R have finitely many maximal ideals and infinitely many atoms?*

Example 4.7. *The ring $\overline{\mathbb{Z}}$ of all algebraic integers is not a Furstenberg domain. In fact it is an **antimatter domain**: there are no irreducibles whatsoever: if z is an algebraic integer then so is $z^{1/2}$, so we can always factor $z = z^{1/2}z^{1/2}$. Moreover $\overline{\mathbb{Z}}$ is not a field: for all integers $n \geq 2$, if $n \in \overline{\mathbb{Z}}^\times$ then $\frac{1}{n} \in \overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$, contradiction.*

If I is a nonzero ideal of $\overline{\mathbb{Z}}$ then the constant coefficient of the minimal polynomial of a nonzero element $\alpha \in I$ is a nonzero integer in I . It follows that if $J(\overline{\mathbb{Z}}) \neq 0$ then there is $N \in \mathbb{Z}^+$ that is contained in every $\mathfrak{m} \in \text{MaxSpec } \overline{\mathbb{Z}}$. Choose a prime number $p \nmid N$. Then p is not a unit in $\overline{\mathbb{Z}}$ – otherwise $\frac{1}{p} \in \overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$ – so there is at least one maximal ideal \mathfrak{m}_p of $\overline{\mathbb{Z}}$ containing p . (In fact the set of maximal ideals of $\overline{\mathbb{Z}}$ containing p has continuum cardinality.) Then $\mathfrak{m}_p \supset (N, p) = \overline{\mathbb{Z}}$: contradiction.

So the answer to Question 4.4 is **yes**: a semiprimitive domain that is not a field can have no irreducibles whatsoever.

The following result answers Questions 4.5 and 4.6 for Dedekind domains and shows that the Euclidean Criterion is, in principle, completely efficacious in determining whether a Dedekind domain has infinitely many atoms.

Theorem 4.8.

For a Dedekind domain R that is not a field, the following are equivalent:

- (i) *R is semiprimitive.*
- (ii) *R has infinitely many maximal ideals.*
- (iii) *R has infinitely many atoms.*

Proof. We know (i) \implies (ii) in any domain.

(ii) \implies (i): in a Dedekind domain, any nonzero element is contained in only finitely many maximal ideals. So in fact for any infinite subset $M \subset \text{MaxSpec } R$ we have $\bigcap_{\mathfrak{m} \in M} \mathfrak{m} = (0)$.

(i) \implies (iii): Dedekind domains are Noetherian, hence Furstenberg domains, so the Euclidean Criterion applies.

(iii) \implies (i): By contraposition: a Dedekind domain with finitely many maximal ideals is a PID [J, p. 625], [Cl, Thm. 20.6], and in a PID maximal ideals, principal ideals generated by prime elements, and atoms all coincide. \square

Question 4.9. *Let K be a number field, with ring of integers \mathbb{Z}_K . The set of prime numbers is an infinite sequence of pairwise comaximal nonunits of \mathbb{Z}_K , so (as is well known!) \mathbb{Z}_K has infinitely many prime ideals and thus is semiprimitive. When $K = \mathbb{Q}$ or is imaginary quadratic, the finiteness of \mathbb{Z}_K^\times leads to a direct verification of Condition (E). Is there a similarly direct verification for all K ?*

This is a question we will leave to the reader to address.

Proposition 4.10. *Let R be a Noetherian domain of dimension at most one (nonzero prime ideals are maximal). If $\text{MaxSpec } R$ is infinite, then R is semiprimitive and thus has infinitely many pairwise comaximal irreducibles.*

Proof. If R is not semiprimitive, then every maximal ideal \mathfrak{m} of R is a minimal prime ideal of $R/J(R)$. Since R is Noetherian, so is $R/J(R)$, and a Noetherian ring has only finitely many minimal prime ideals [J, p. 439], [Cl, Thm. 10.13]. \square

A **Jacobson ring** is a ring in which every prime ideal is the intersection of the maximal ideals containing it. Since in a domain (0) is prime, a Jacobson domain must be semiprimitive. Any quotient of a Jacobson ring is again a Jacobson ring. If R is a Jacobson ring and S is a commutative, finitely generated R -algebra then S is a Jacobson ring [K, p. 18], [Cl, Thm. 12.15, 12.21]. So:

Theorem 4.11. *a) A Jacobson Furstenberg domain that is not a field has infinitely many pairwise comaximal irreducibles.*

b) Let F be a field, and let \mathfrak{p} be a prime but not maximal ideal of $F[t_1, \dots, t_n]$. Then the ring $R = F[t_1, \dots, t_n]/\mathfrak{p}$ – i.e., a coordinate ring of an integral affine variety of positive dimension – has infinitely many pairwise comaximal irreducibles.

c) A domain R that is finitely generated over \mathbb{Z} and not a field has infinitely many pairwise comaximal irreducibles.

To sum up: if we want to see a domain that has infinitely many maximal ideals but is not semiprimitive, it cannot be finitely generated over a field, and if Noetherian it must have a nonzero prime ideal that is not maximal. This cues us up for the following example, which gives a negative answer to Question 4.5.

Example 4.12. *Consider the ring $\mathbb{Z}[[t]]$ of formal power series with integral coefficients. It is not hard to show that $\mathbb{Z}[[t]]$ is an atomic domain. In fact $\mathbb{Z}[[t]]$ is a Noetherian UFD [K, p. 48, Thm. 72], [Cl, Thm. 15.32]. Since $1+(t) \subset \mathbb{Z}[[t]]^\times$, the Jacobson radical $J(\mathbb{Z}[[t]])$ contains (t) and is thus nonzero. Since $J(\mathbb{Z}[[t]]) \neq (0)$, the hypotheses of the Euclidean Criterion do not apply. Nevertheless there are infinitely many pairwise comaximal prime elements, namely the prime numbers! Hence there are infinitely many maximal ideals.*

Here we could have replaced \mathbb{Z} with any PID with infinitely many maximal ideals.

Thus the answer to Question 4.6a) is **yes**: moreover a nonsemiprimitive domain can have infinitely many comaximal irreducibles.

Example 4.13. *Let k be a field. Recall that $k[x, y]$ is a UFD, and let $K = k(x, y)$ be its fraction field. Let R be the subring of $k(x, y)$ consisting of rational functions $\frac{f(x, y)}{g(x, y)}$ that, when written in lowest terms, have $g(0, 0) \neq 0$. Then R is itself a UFD – factorization in R proceeds as in $k[x, y]$ except that the prime elements $p(x, y) \in k[x, y]$ such that $p(0, 0) \neq 0$ become units in R – in which an element is a unit iff $f(0, 0) \neq 0$. Thus $\mathfrak{m} = \left\{ \frac{f(x, y)}{g(x, y)} \mid f(0, 0) = 0 \right\}$ is the unique maximal ideal, so $J(R) = \mathfrak{m}$ and R is very far from being semiprimitive. Nevertheless it has infinitely many prime elements, e.g. $\{y - x^n\}_{n=1}^\infty$. In more geometric language, the atoms correspond to irreducible curves in the affine plane passing through $(0, 0)$.*

Thus the answer to Question 4.6b) is **yes**. However, there is more to say. The preceding example can be vastly generalized using the following striking result.

Theorem 4.14. (Cohen-Kaplansky [CK46])

Let R be an atomic domain with finitely many atoms. Then:

- a) R has only finitely many prime ideals.
- b) R is Noetherian.
- c) Every nonzero prime ideal of R is maximal.

Proof. a) In an atomic domain R , whenever a prime ideal \mathfrak{p} of R contains a nonzero element x , we may factor $x = f_1 \cdots f_r$ into irreducibles and thus see that \mathfrak{p} contains some irreducible element f dividing x . Thus, given any set of generators of a prime ideal \mathfrak{p} we can replace it with a set of irreducible generators. In a set of generators of an ideal, replacing each element by any one of its associates does not change the ideal generated, and thus if we have only finitely many nonassociate irreducibles we can only generate finitely many prime ideals.

b) The proof of part a) shows that every prime ideal of R is finitely generated. By a result of Cohen [Co50, Thm. 2], [Cl, Thm. 4.26], all ideals are finitely generated. (This is an instance of the **prime ideal principle** of Lam-Reyes [LR08].)

c) If not, there are prime ideals $(0) \subsetneq \mathfrak{p}_1 \subsetneq \mathfrak{p}_2$. As R is Noetherian, there are then infinitely many prime ideals [K, Thm. 144], [Cl, Cor. 8.46]. \square

A **Cohen-Kaplansky domain** is an atomic domain with finitely many atoms. The work [CK46] does not give a complete classification: we are left with the case of a Noetherian domain R with finitely many nonzero prime ideals, all of which are maximal. If R is a Dedekind domain, then by Theorem 4.8 there are only finitely many atoms. So the remaining case is when R is not integrally closed in its fraction field, in which case the integral closure \overline{R} is a Dedekind domain with finitely many prime ideals [M, Thm. 11.7], [Cl, Cor. 18.8]. One might expect that this forces R to be Cohen-Kaplansky. This need not be the case!

Example 4.15. Let k be a field, and consider the subring

$$R = k[[t^2, t^3]] = k + t^2k[[t]]$$

of the formal power series ring $k[[t]]$. For $0 \neq f = \sum_{n=0}^{\infty} a_n t^n \in k[[t]]$, we define $v(f)$ to be the least n such that $a_n \neq 0$. Then v is a discrete valuation on $k[[t]]$, and the only nonzero prime ideal of $k[[t]]$ is $(t) = \{f \in R \mid v(f) > 0\} \cup \{0\}$. In particular, $k[[t]]$ is a PID. So is the (isomorphic!) subring $k[[t^2]]$, and $\{1, t^3\}$ is a generating set for R as a $k[[t^2]]$ -module, so by standard PID structure theory, every ideal of R can be generated by two elements. Thus R is Noetherian, hence atomic. For $f = a_0 + \sum_{n=2}^{\infty} a_n t^n \in R$, we have $f \in R^\times \iff a_0 \neq 0$, and thus

$$\mathfrak{m} = \left\{ \sum_{n=2}^{\infty} a_n t^n \right\} = (t^2, t^3)$$

is the unique maximal ideal of R . We will give a complete description of the atoms of R . First we claim that $f \in R$ is irreducible iff $v(f) \in \{2, 3\}$. Indeed a nontrivial factorization $f = xy$ involves $v(x), v(y) \geq 2$ hence $v(f) \geq 4$; conversely, if $v(f) \geq 4$ then $f = t^2 \frac{f}{t^2}$ is a nontrivial factorization. Since $k^\times \subset R^\times$, every irreducible is associate to one of the form

$$t^2 + \sum_{n \geq 3} a_n t^n, \quad (v(f) = 2 \text{ case})$$

or one of the form

$$t^3 + \sum_{n \geq 4} a_n t^n, \quad (v(f) = 3 \text{ case}).$$

Associate elements have the same valuation, so certainly no irreducible of the first type is associate to an irreducible of the second type. We claim that $t^2 + \sum_{n \geq 3} a_n t^n$ is associate to $t^2 + \sum_{n \geq 3} b_n t^n$ iff $a_3 = b_3$ and $t^3 + \sum_{n \geq 3} a_n t^n$ is associate to $t^3 + \sum_{n \geq 3} b_n t^n$ iff $a_4 = b_4$. This can be done by direct computation:

$$\begin{aligned} & (t^2 + a_3 t^3 + a_4 t^4 + a_5 t^5 + \dots)(1 + u_2 t^2 + u_3 t^3 + \dots) \\ &= t^2 + a_3 t^3 + (a_4 + u_2) t^4 + (a_5 + a_3 u_2 + u_3) t^5 + \dots, \end{aligned}$$

so $a_3 = b_3$ and there is a unique choice of u_2, u_3, \dots leading to $a_n = b_n$ for all $n \geq 4$. The $v(f) = 3$ case is similar. Thus there are precisely $2\#k$ atoms, and R is Cohen-Kaplansky iff k is finite.

Example 4.16. (Anderson-Mott [AM92, Cor. 7.2]) For a prime power q and $d, e \in \mathbb{Z}^+$, the ring $R = \mathbb{F}_q + t^e \mathbb{F}_{q^d}[[t]]$ is a Cohen-Kaplansky domain with exactly one nonzero prime ideal and exactly $e \frac{q^d - 1}{q - 1} q^{d(e-1)}$ atoms, none of which are prime unless $(d, e) = (1, 1)$.

The paper [CK46] was mostly forgotten for many years, until the breakthrough work of Anderson and Mott [AM92] gave a complete characterization of Cohen-Kaplansky domains. In fact they give 14 characterizations! Here is one:

Theorem 4.17. (Anderson-Mott [AM92])

For an atomic domain R , the following are equivalent:

- (i) R is a Cohen-Kaplansky domain.
- (ii) R is Noetherian of dimension at most one (nonzero prime ideals are maximal), has finitely many prime ideals, the integral closure \bar{R} of R is finitely generated as an R -module, $\# \text{MaxSpec } \bar{R} = \# \text{MaxSpec } R$, and for all nonprincipal ideals $\mathfrak{m} \in \text{MaxSpec } R$, R/\mathfrak{m} is finite.

Example 4.18. Let k be a field of characteristic different from 2 or 3, and consider:

- R_1 : the localization of $k[x, y]/(y^2 - x^3 - x)$ at $\mathfrak{m}_0 = (x, y)$.
- R_2 : the localization of $k[x, y]/(y^2 - x^3 - x^2)$ at $\mathfrak{m}_0 = (x, y)$.
- R_3 : the localization of $k[x, y]/(y^2 - x^3)$ at $\mathfrak{m}_0 = (x, y)$.

Then:

- R_1 is always Cohen-Kaplansky (it is a Dedekind domain with one maximal ideal).
- R_2 is never Cohen-Kaplansky ($\# \text{MaxSpec } \bar{R}_2 = 2 > 1 = \# \text{MaxSpec } R_2$).
- R_3 is Cohen-Kaplansky iff k is finite.

4.4. Euclid Beyond Atomicity.

In the case of an atomic domain, the part of the Euclidean Criterion that yields infinitely many maximal ideals is much weaker than the Cohen-Kaplansky Theorem. However, there is life beyond atomic domains.

Example 4.19. Let $\text{Hol}(\mathbb{C})$ be the ring of entire functions $f : \mathbb{C} \rightarrow \mathbb{C}$. For $f \in \text{Hol}(\mathbb{C})$, put $Z(f) = \{z \in \mathbb{C} \mid f(z) = 0\}$. If $f, g \in \text{Hol}(\mathbb{C})^\bullet$, then $Z(f)$ and $Z(g)$ are countable sets, hence so is $Z(fg) = Z(f) \cup Z(g)$, so $fg \neq 0$. Thus $H(\mathbb{C})$ is a domain. The map $z_0 \in \mathbb{C} \mapsto (z - z_0)$ gives a bijection from \mathbb{C} to the atoms of $\text{Hol}(\mathbb{C})$. An element $f \in \text{Hol}(\mathbb{C})$ is a unit iff $Z(f) = \emptyset$, and a nonzero nonunit f

is a (finite!) product of atoms iff $Z(f)$ is finite and nonempty.

So $\text{Hol}(\mathbb{C})$ is not atomic – consider e.g. $f(z) = \sin z$ – but it is Furstenberg: if f is a nonzero nonunit, then f vanishes at some $z_0 \in \mathbb{C}$ and thus is divisible by the irreducible element $z - z_0$. Moreover $\text{Hol}(\mathbb{C})$ satisfies Condition (E): if $f \in \text{Hol}(\mathbb{C})^\bullet$ then there is $w \in \mathbb{C}$ such that $f(w) \neq 0$. Let $g = z - w - \frac{1}{f(w)}$. Then $(gf+1)(w) = 0$, so $gf+1 \notin \text{Hol}(\mathbb{C})^\times$. Thus the Euclidean Criterion applies in $\text{Hol}(\mathbb{C})$.

Theorem 4.20. *Let $1 \leq \alpha \leq \beta \leq \gamma$ be cardinal numbers. There is a domain R satisfying all of the following properties:*

- (i) R is a Bézout domain: every finitely generated ideal is principal.
- (ii) R has exactly α atoms, each of which is a maximal ideal.
- (iii) R has exactly β maximal ideals.
- (iv) R has exactly γ nonzero prime ideals.
- (v) R is an atomic domain iff $\alpha = \beta = \gamma < \aleph_0$.
- (vi) R is a Furstenberg domain iff $\alpha = \beta$.
- (vii) R is semiprimitive iff $\beta \geq \aleph_0$.

We postpone the proof of Theorem 4.20 in order to discuss its significance. By taking $\alpha = \beta$ and $\gamma \geq \aleph_0$ we get Furstenberg domains with any number $\alpha \geq 1$ of atoms and any number $\gamma \geq \max(\alpha, \aleph_0)$ nonzero prime ideals. In particular, a Furstenberg domain can have any finite, positive number of atoms and any infinite number of prime ideals, so the Cohen-Kaplansky Theorem does not extend from atomic domains to Furstenberg domains. For any $\alpha = \beta \geq \aleph_0$ and $\gamma \geq \alpha$ we get a semiprimitive Furstenberg domain that is not an atomic domain.

Now we come to the proof of Theorem 4.20, which requires somewhat more specialized results. A completely self-contained presentation would require more space than we want to devote here. So we will make use of the material of [FS, Ch. II and III], and our treatment will be at the level of a detailed sketch.

Let R be a domain with fraction field K . To $x \in K^\bullet$ we attach the **principal fractional ideal** $(x) = \{ax \mid a \in R\}$. When $x \in R$, this coincides with the usual notion of a principal ideal. For $x, y \in K^\bullet$ we have $(x) = (y)$ iff there is $u \in R^\times$ such that $y = ux$. The principal fractional ideals of K form a commutative group under pointwise multiplication: we have $(x)(y) = (xy)$. We call this the **group of divisibility** of R and denote it $G(R)$. It is partially ordered by reverse inclusion: that is, for $x, y \in K^\bullet$ we put $(x) \leq (y)$ iff $(y) \supset (x)$. This order reversal is actually rather familiar: for $x, y \in K^\times$, we write $x \mid y \iff \frac{y}{x} \in R$, and then we have $x \mid y$ if $(x) \supset (y)$: *to contain is to divide*.

Let $\{G_i\}_{i \in I}$ be an indexed family of nonzero totally ordered commutative groups, and let $G = \bigoplus_{i \in I} G_i$ be the direct sum endowed with the pointwise partial ordering: $x \leq y$ iff $x_i \leq y_i$ for all $i \in I$. Let $\pi_i : G \rightarrow G_i$ be projection onto the i th coordinate. By the Kaplansky-Jaffard-Ohm Theorem [FS, Thm. III.5.3] there is a Bézout domain R and an isomorphism $\varphi : G(R) \xrightarrow{\sim} G$ of partially ordered commutative groups. See [FS, Example III.5.4]. Let v be the composite $K^\times \rightarrow K^\times/R^\times \xrightarrow{\varphi} \bigoplus_{i \in I} G_i$. Then the maximal ideals of R are precisely $\mathfrak{m}_i = \{x \in R \mid (\pi_i \circ v)(x) > 0\} \cup \{0\}$ for $i \in I$. Thus no element of R^\bullet lies in infinitely many maximal ideals, so R is semiprimitive iff I is infinite.

An **atom** in a partially ordered commutative group is a minimal positive element. This is a direct generalization of our previous use of the term: if R is a

domain, the minimal positive elements of the group of divisibility $G(R)$ are precisely the principal fractional ideals (x) for an irreducible element $x \in R$. For every atom $x \in G$, there is $i \in I$ such that x_i is an atom of G_i and $x_j = 0$ for all $j \neq i$, and conversely all such elements give atoms of G . Since each G_i is totally ordered, it has at most one atom, the *least* positive element of G_i if such an element exists. It follows that R is Furstenberg iff each G_i has a least positive element. Similarly, a nonzero nonunit $x \in R$ factors into irreducibles iff $v(x) \in G$ is a sum of atoms iff for all $i \in I$, G_i has a least positive element a_i and $v_i(r) = na_i$ for some $n \in \mathbb{Z}^+$. Thus R is an atomic domain iff each $G_i \cong \mathbb{Z}$.

The domain R is **h-local**: each nonzero prime ideal is contained in a unique maximal ideal [FS, *loc. cit.*]. The nonzero prime ideals contained in \mathfrak{m}_i correspond bijectively to the proper convex subgroups of G_i . (A subset Y of a totally ordered set X is convex if for all $x < y < z \in X$, if $x, z \in Y$ then also $y \in Y$.) We will take each G_i to be a lexicographic product of copies of subgroups of $(\mathbb{R}, +)$ indexed by an ordinal η . Then the convex subgroups of G_i are precisely $\{H_\delta\}_{0 \leq \delta \leq \eta}$, where H_δ is the set of all elements of G_i with j -coordinate zero for all $j < \delta$. So there are $\#\eta$ nonzero prime ideals in \mathfrak{m}_i .

We will take a family of nonzero totally ordered commutative groups G_i parameterized by $i \in \beta$: this gives us β maximal ideals, and R is semiprimitive iff $\beta \geq \aleph_0$. We are left to choose the groups G_i in terms of α and γ so as to attain the other assertions. We define an ordinal η : if γ is finite, it is the positive integer $\gamma - \beta + 1$; if γ is infinite, it is the successor ordinal to γ (what matters in this case is that η is a well-ordered set of cardinality γ and with a largest element). There are cases:

- If $\alpha = \beta = \gamma < \aleph_0$, we take R to be a PID with γ nonzero prime ideals.
- If $\alpha = \beta$ and $\gamma \geq \min(\beta + 1, \aleph_0)$ we take $G_i = \mathbb{Z}$ for all $0 < i \in \beta$. We take G_0 to be the Cartesian product of copies of \mathbb{Z} indexed by η , endowed with the lexicographic ordering. Then G_0 has a least positive element: the element that is 0 in all factors but the last and 1 in the last factor. So all G_i have least elements and R is a Furstenberg domain. Moreover $\eta \geq 2$ so $G_0 \not\cong \mathbb{Z}$ and R is not an atomic domain. It has $(\beta - 1) + \#\eta = \gamma$ nonzero prime ideals.
- If $\alpha < \beta$, we take G_0 to be the Cartesian product of copies of \mathbb{Z} indexed by η , for $1 \leq i < \alpha$ we take $G_i = \mathbb{Z}$, and for $i \geq \alpha$ we take $G_i = \mathbb{R}$.

4.5. Supplement: Rings With Infinitely Many Maximal Ideals.

Let us briefly consider the case of an arbitrary commutative ring. Though others have done so (see e.g. [AVL96]), it is beyond our ambitions to pursue a factorization theory in the presence of zero divisors. But we can still ask for criteria under which there are infinitely many maximal ideals. In this more general context $J(R) = (0)$ is no longer sufficient: e.g. $J(\mathbb{C} \times \mathbb{C}) = 0$ and there are only two maximal ideals. Nevertheless both Euclid and Jacobson have a role to play.

Proposition 4.21. *Let I be an ideal of R contained in the Jacobson radical. Then for all $x \in R$, if the image of x in R/I is a unit, then x is a unit. In particular the natural map $R^\times \rightarrow (R/I)^\times$ is surjective.*

Proof. If the image of x in R/I is a unit, then there is $y \in R$ such that $xy \equiv 1 \pmod{I}$, i.e., $xy - 1 \in I \subset J(R)$. Thus for every maximal ideal \mathfrak{m} of R , $xy - 1 \in \mathfrak{m}$ so we cannot have $x \in \mathfrak{m}$. So x lies in no maximal ideal of R and thus $x \in R^\times$. \square

Theorem 4.22. (*Dubuque [Du10]*) *Let R be an infinite ring. If $\#R > \#R^\times$, then $\text{MaxSpec } R$ is infinite.*

Proof. We will show by induction on n that for all $n \in \mathbb{Z}^+$, R has n maximal ideals. Base Case: Since R is infinite, it is nonzero and thus it has a maximal ideal \mathfrak{m}_1 . Induction Step: Let $\mathfrak{m}_1, \dots, \mathfrak{m}_m$ be maximal ideals, and put

$$I = \prod_{i=1}^m \mathfrak{m}_i.$$

Case 1: Suppose $I + 1 \subset R^\times$. Then $\#I \leq \#R^\times$. Moreover $I \subset J(R)$, so by Proposition 4.21 $R^\times \rightarrow (R/I)^\times$ is surjective. It follows that $\#(R/I)^\times \leq \#R^\times < \#R$: by the Chinese Remainder Theorem, $R/I \cong \prod_{i=1}^m R/\mathfrak{m}_i$, hence there is an injection $(R/\mathfrak{m}_i)^\times \rightarrow (R/I)^\times$. Putting the last two sentences together we conclude $\#(R/\mathfrak{m}_i)^\times < \#R$, and thus, since R/\mathfrak{m}_i is a field and R is infinite, $\#R/\mathfrak{m}_i = \#(R/\mathfrak{m}_i)^\times + 1 < \#R$. Finally this gives the contradiction

$$\#R = \#I \cdot \#R/I = \#I \cdot \prod_{i=1}^m \#R/\mathfrak{m}_i < (\#R)^{m+1} = \#R.$$

Case 2: So there is $x \in I + 1 \setminus R^\times$. Let \mathfrak{m}_{m+1} be a maximal ideal containing x . For all $1 \leq i \leq m$ we have $x - 1 \in I \subset \mathfrak{m}_i$, so

$$1 = x + (1 - x) \in \mathfrak{m}_{m+1} + \mathfrak{m}_i.$$

So \mathfrak{m}_{m+1} is an $(m + 1)$ st maximal ideal of R , completing the induction step. \square

A special case of Theorem 4.22 appears in [K, § 1.1, Exc. 8].

For a ring R , consider the quotient $R/J(R)$. The maximal ideals of $R/J(R)$ correspond to the maximal ideals of R containing $J(R)$ – that is, to the maximal ideals of R . Thus $R/J(R)$ is semiprimitive. Thus we can replace any ring with a semiprimitive ring without changing its MaxSpec . However this “Jacobson semisimplification” need not carry domains to domains: e.g. if R is a domain with $2 \leq n < \aleph_0$ maximal ideals $\mathfrak{m}_1, \dots, \mathfrak{m}_n$, then $R/J(R) \cong \prod_{i=1}^n R/\mathfrak{m}_i$. Here is a generalization.

Theorem 4.23. *a) For a ring R , the following are equivalent.*

- (i) *R has only finitely many maximal ideals.*
 - (ii) *$R/J(R)$ is a finite product of fields.*
 - (iii) *$R/J(R)$ has only finitely many ideals.*
 - (iv) *$R/J(R)$ is Artinian (i.e., there are no infinite descending chains of ideals).*
- b) A semiprimitive ring with finitely many maximal ideals has finitely many ideals.*

Proof. a) (i) \implies (ii): If the maximal ideals of R are $\mathfrak{m}_1, \dots, \mathfrak{m}_n$, then by the Chinese Remainder Theorem [AM, Prop. 1.10], [Cl, Thm. 4.18] we have

$$R/J(R) = R / \bigcap_{i=1}^n \mathfrak{m}_i \cong \prod_{i=1}^n R/\mathfrak{m}_i.$$

(ii) \implies (iii) \implies (iv) immediately. (iv) \implies (i): Maximal ideals of $R/J(R)$ are in bijection with maximal ideals of R , and an Artinian ring has finitely many maximal ideals [AM, Thm. 8.10], [Cl, Thm. 8.31]. b) Apply part a). \square

5. BUT WHAT ABOUT PRIMES?

Our take on Euclid's argument has been as a criterion for the existence of *irreducibles*. The distinction evaporates in a UFD. A PID with only finitely many prime ideals is a UFD with only finitely many principal prime ideals. It turns out that the converse is also true.⁵

Theorem 5.1. *Let R be a UFD, not a field, with only finitely many atoms. Then R is a PID with finitely many prime ideals and $\#R = \#R^\times$.*

Proof. A UFD with finitely many nonassociate prime elements is a Cohen-Kaplansky domain, so $\text{MaxSpec } R$ is finite and $\#R = \#R^\times$ by Theorem 3.4. By Theorem 4.14 every nonzero prime ideal of R is maximal. The proof of Theorem 4.14a shows: every nonzero prime ideal \mathfrak{p} contains a prime element p . Since (p) is maximal, we have $\mathfrak{p} = (p)$. Thus every prime ideal is principal, so R is a PID [K, p. 8], [Cl, Thm. 4.25]. (This is another case of the Lam-Reyes Prime Ideal Principle.) \square

Let us now move away from UFDs. From Example 4.15, we deduce:

Theorem 5.2. *Let $\kappa \geq \aleph_0$ be a cardinal. There is a Noetherian domain R with exactly one nonzero prime ideal, exactly κ atoms and no prime elements.*

Proof. Let k be a field of cardinality κ , e.g. $k = \mathbb{Q}(\{t_\alpha \mid \alpha \in \kappa\})$. By Example 4.15, $R = k[[t^2, t^3]]$ is a Noetherian domain with one nonzero prime ideal $\mathfrak{m} = (t^2, t^3)$ and $2\kappa = \kappa$ atoms. Since \mathfrak{m} is not principal, R has no prime elements. \square

Cohen-Kaplansky showed that an atomic domain that is neither a field nor a UFD must have at least 3 atoms [CK46, p. 469]. Their argument is a nice one: we must have at least one nonprime irreducible f_1 . Since (f_1) is not prime, it is properly contained in some prime ideal \mathfrak{p} , which must therefore contain a nonassociate irreducible f_2 . Since $f_1 + f_2 \in \mathfrak{p}$, $f_1 + f_2$ is not a unit and therefore it is divisible by an irreducible f_3 , which cannot be associate to either f_1 or f_2 .

Finally, we consider Dedekind domains.

Question 5.3. *Let R be a Dedekind domain with infinitely many prime ideals. Must R have infinitely many atoms?*

In an important classical case the answer is **yes**, as most number theorists know.

Theorem 5.4. *For each number field K , the ring of integers \mathbb{Z}_K has infinitely many nonassociate prime elements.*

Proof. Step 1: For any number field L , the number of rational primes that split completely in L is infinite. This is a special case of the Chebotarev Density Theorem, which however can be proved in a more elementary way, as was shown in [Po10]. Using some basic algebraic number theory which we omit here, it comes down to showing that for every nonconstant polynomial $f \in \mathbb{Z}[t]$, the set of prime numbers p dividing $f(n)$ for some $n \in \mathbb{Z}$ is infinite. If $f(0) = 0$ this is trivial. If $f(0) \neq 0$, let p_1, \dots, p_k be the prime divisors of $f(0)$ (we allow $k = 0$) and let q_1, \dots, q_ℓ be any finite set of primes not dividing $f(0)$. For $1 \leq i \leq k$, let a_i be such that $p_i^{a_i} \mid f(0)$ and $p_i^{a_i+1} \nmid f(0)$. For $N \in \mathbb{Z}^+$ consider

$$x_N = f(Np_1^{a_1+1} \cdots p_k^{a_k+1} q_1 \cdots q_\ell).$$

⁵Theorem 5.1 is known to the experts: see e.g. [Za08].

Then for all $1 \leq i \leq k$, $p_i^{a_i+1} \nmid x_N$ and for all $1 \leq j \leq \ell$, $q_j \nmid x_N$, so the set of N for which x_N is not divisible by some prime other than $p_1, \dots, p_k, q_1, \dots, q_\ell$ is finite.

Step 2: A prime ideal \mathfrak{p} of a number field is principal iff it splits completely in the Hilbert class field K^1 of K . So every prime ideal \mathfrak{p} of K lying above any one of the infinitely many prime numbers p that split completely in K^1 is principal. \square

Looking at the above argument, one wonders: were we working too hard? Perhaps some simple argument gives a general affirmative answer to Question 5.3.

In fact Question 5.3 was answered negatively by Claborn [Cl65, Example 1.5]. The construction is impressively direct: start with a Dedekind domain A that is not a PID, let \mathcal{P} be the set of prime elements of R and pass to $R = A[\{\frac{1}{p}\}_{p \in \mathcal{P}}]$. The prime ideals of R are precisely the nonprincipal prime ideals of A , which remain nonprincipal in R ! This **prime-killing construction** also appears in a work of Samuel [Sa64, p. 17, Thm. 6.3] and is therein attributed to Nagata (cf. [N57, Lemma 2]). For a Dedekind domain A , write $\text{Cl}A$ for its ideal class group: the quotient of the monoid of nonzero ideals of A under the equivalence relation $I \sim J$ iff there are $\alpha, \beta \in A^\bullet$ with $(\alpha)I = (\beta)J$. In the setting of the prime-killing construction – i.e., R is the localization of A at the multiplicative subset generated by the prime elements – we have [Sa64], [Cl65] that $\text{Cl}R \cong \text{Cl}A$.

Theorem 5.5. *Let κ be an infinite cardinal. There is a Dedekind domain R with exactly κ atoms and no prime elements.*

Proof. We will use some properties of “elliptic Dedekind domains”: for more details, see [Cl09, §2.4]. Let k be an algebraically closed field of characteristic 0 and cardinality κ , and put $R = k[x, y]/(y^2 - x^3 - x)$. Then R is a Dedekind domain, and by the Nullstellensatz the nonzero prime ideals of R are all of the form $\mathfrak{p}_{(x_0, y_0)} = (x - x_0, y - y_0, y^2 - x^3 - x)$ for pairs $(x_0, y_0) \in k^2$ such that $y_0^2 = x_0^3 + x_0$. In other words, they are the k -rational points on the projective elliptic curve $E : y^2z = x^3 + xz^2$, excluding the point at infinity $O = [0 : 1 : 0]$. Moreover, by the Riemann-Roch Theorem, since $[x_0 : y_0 : 1] \neq O$, the prime ideal $\mathfrak{p}_{(x_0, y_0)}$ is not principal. Thus R is a Dedekind domain with $\#\text{MaxSpec} R = \#R = \kappa$ and without prime elements. Because R is Dedekind, every ideal can be generated by two elements [J, p. 630], [Cl, Thm. 20.12]. Since Dedekind domains are atomic domains, this implies that for all $\mathfrak{p} \in \text{MaxSpec} R$ there are irreducibles $p_{\mathfrak{p}}, q_{\mathfrak{p}}$ such that $\mathfrak{p} = (p_{\mathfrak{p}}, q_{\mathfrak{p}})$. Thus if λ is the number of atoms of R we have

$$\kappa = \#\text{MaxSpec} R \leq \lambda^2 \leq (\#R)^2 = \kappa^2 = \kappa,$$

so $\lambda^2 = \kappa$. Since κ is infinite, so is λ and thus $\lambda = \lambda^2 = \kappa$. \square

REFERENCES

- [AM] M.F. Atiyah and I.G. Macdonald, *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading Mass.-London-Don Mills, Ont. 1969.
- [AM92] D.D. Anderson and J.L. Mott, *Cohen-Kaplansky domains: integral domains with a finite number of irreducible elements*. J. Algebra 148 (1992), 17-41.
- [AVL96] D.D. Anderson and S. Valdes-Leon, *Factorization in commutative rings with zero divisors*. Rocky Mountain J. Math. 26 (1996), 439-480.
- [CK46] I.S. Cohen and I. Kaplansky, *Rings with a finite number of primes. I*. Trans. Amer. Math. Soc. 60 (1946), 468-477.
- [Cl] P. L. Clark, *Commutative Algebra*, <http://math.uga.edu/~pete/integral.pdf>.
- [Cl65] L.E. Claborn, *Dedekind domains and rings of quotients*. Pacific J. Math. 15 (1965), 59-64.

- [Cl09] P.L. Clark, *Elliptic Dedekind domains revisited*. Enseignement Math. 55 (2009), 213–225.
- [CLL16] P.L. Clark, N. Lebowitz-Lockard and P. Pollack, *A note on Golomb topologies*. http://alpha.math.uga.edu/~pete/CLLP16_November_14.pdf
- [Co50] I.S. Cohen, *Commutative rings with restricted minimum condition*. Duke Math. J. 17 (1950), 27–42.
- [Co73] P.M. Cohn, *Unique factorization domains*. Amer. Math. Monthly 80 (1973), 1–18.
- [CS12] J. Coykendall and C. Spicer, *Cohen-Kaplansky domains and the Goldbach conjecture*. Proc. Amer. Math. Soc. 140 (2012), 2227–2233.
- [CW03] D. Cass and G. Wildenberg, *Math Bite: A Novel Proof of the Infinitude of Primes, Revisited* Mathematics Magazine, Vol. 76 (2003), 203.
- [Du10] W.G. Dubuque, <http://math.stackexchange.com/questions/201>
- [FS] L. Fuchs and L. Salce, *Modules over non-Noetherian domains*. Mathematical Surveys and Monographs, 84. American Mathematical Society, Providence, RI, 2001.
- [Fu55] H. Furstenberg, *On the infinitude of primes*, Amer. Math. Monthly 62 (1955), 353.
- [Gl67] M. Glaymann, *Characteristic Functions and Sets*. Mathematics Teacher, 60 (1967), 775–778.
- [Go59] S.W. Golomb, *A connected topology for the integers*. Amer. Math. Monthly 66 (1959), 663–665.
- [J] N. Jacobson, *Basic Algebra II*. Second edition. W.H. Freeman and Company, New York, 1989.
- [K] I. Kaplansky, *Commutative rings*. Allyn and Bacon, Inc., Boston, Mass. 1970.
- [LR08] T.Y. Lam and M. Reyes, *A prime ideal principle in commutative algebra*. J. Algebra 319 (2008), 3006–3027.
- [M] H. Matsumura, *Commutative ring theory*. Translated from the Japanese by M. Reid. Second edition. Cambridge Studies in Advanced Mathematics, 8. Cambridge University Press, Cambridge, 1989.
- [Me09] I.D. Mercer, *On Furstenberg’s Proof of the Infinitude of Primes*. Amer. Math. Monthly 116 (2009), 355–356.
- [N57] M. Nagata, *A remark on the unique factorization theorem*. J. Math. Soc. Japan 9 (1957), 143–145.
- [P] P. Pollack, *Not always buried deep. A second course in elementary number theory*. American Mathematical Society, Providence, RI, 2009.
- [Po10] B. Poonen, <http://mathoverflow.net/q/15221>
- [Sa64] P. Samuel, *Lectures on unique factorization domains*. Notes by M. Pavman Murthy. Tata Institute of Fundamental Research Lectures on Mathematics, No. 30 Tata Institute of Fundamental Research, Bombay 1964.
- [Za08] M. Zafrullah, <http://mathforum.org/kb/message.jspa?messageID=6451774>