M.B.J. Zwaan

On commutative rings with only finitely many ideals

Bachelorscriptie, June 22, 2014

Scriptiebegeleider: dr. M. Kosters

Mathematisch Instituut, Universiteit Leiden

Contents

1. Abstract

In this thesis we take a closer look at the ideal structure of non-principal ideal rings with only finitely many ideals. I this thesis rings are assumed to be commutative.

We wish to show that for every natural number, strictly greater than five, there is a non-principal local ideal ring with exactly that many ideals. We succeeded for all natural numbers up to 1050. After quickly repeating some useful lemmas in the first segment we explore some of the more general structure of rings with only finitely many ideals in the second. In particular we prove that every ring with only finitely many ideals can be written as a finite product of principal ideal rings and finite rings.

In the third segment, aptly named bounds, we find an upper and a lower bound for the number of ideals of certain rings:

Theorem 1.1. *Take any finite local non-principal ideal ring* $(R, \mathfrak{m})$*. Let* $n \in \mathbf{Z}_{\geq 1}$ *its number of ideals.*

Take the smallest $d \in \mathbf{Z}_{\geq 0}$ *such that the number of subspaces of a d-dimensional vector space over the residue field is greater than or equal to* $n-1$*. Then one has that* $(R/\mathfrak{m})^{d+1} \leq \#R \leq \#(R/\mathfrak{m})^{n-3}$*.*

Furthermore we find that the finite local rings with the most ideals for a fixed length are rings of which the maximal ideal is a vector space over the residue field. Then in the fourth section we take a closer look at the general ideal structure of rings proving amongst other things that the number of ideals of fixed length is 1 modulo the cardinality of the residue field.

In the last part we study three families of rings in an attempt to find a non-principal ring local ring with precisely n ideals for every $n \in \mathbf{Z}_{>5}$:

Theorem 1.2. *For every* $n \in \mathbf{Z}_{\geq 0}$ *such that* $n \leq 5$ *there are no non-principal ideal rings with exactly* n *ideals. For every* $n \in \mathbf{Z}_{>5}$ *such that* $n < 1051$ *there is a local non-principal ideal ring with exactly* n *ideals.*

2. Preliminaries

Most statements in this section will not be proven, but we will provide references. We will only work with commutative rings in this thesis.

Definition 2.1. An ideal J of a ring R is called maximal in an ideal $I \subseteq R$ if $J \subsetneq I$ and for every ideal $J \subseteq K \subseteq I$ we have $K = J$ or $I = K$. An ideal is called maximal if it is maximal in the ideal (1).

Definition 2.2. A ring R is called noetherian if for every ascending chain $I_1 \subseteq I_2 \subseteq \ldots$ of ideals of R there is an $n \in \mathbf{Z}_{>0}$ such that $I_n = I_{n+1} = \ldots$. Equivalently a ring is noetherian if and only if all of its ideals are finitely generated (see chapter 7 of [1]).

Definition 2.3. A ring R is called artin if for every descending chain $I_1 \supseteq I_2 \supseteq \ldots$ of ideals of R there is an $n \in \mathbf{Z}_{>0}$ such that $I_n = I_{n+1} = \ldots$.

Definition 2.4. A 0-dimensional ring is a non-zero ring such that every prime ideal is maximal.

Proposition 2.5. *A non-zero ring* R *is artin if and only if it is noetherian and 0-dimensional.*

Proof. See [1] thm. 8.5. □

Lemma 2.6. *Every finite domain R is a field.*

Proof. Take $a \neq 0$ in R. The map from R to R that sends x to ax is injective because R is a domain. This map is therefore a bijection as R is finite. Hence there is an $x \in R$ such that $ax = 1$, meaning a has an inverse. Hence R is a field. □

Definition 2.7. A ring R is called local when it has a unique maximal ideal $\mathfrak{m}$. Notation: $(R, \mathfrak{m})$.

Theorem 2.8. *An artin ring A is uniquely (up to isomorphism) a finite direct product of local artin rings.*

Proof. See [1] Prop. 8.6. □

Lemma 2.9 (Nakayama's lemma)**.** *For R a ring and M a finitely generated R-module and $\mathfrak{a}$ an ideal in the intersection of all maximal ideals of R, we have that*

i. $\mathfrak{a}M = M \iff M = 0$*;*
ii. *let N be a submodule of M then $N + \mathfrak{a}M = M \iff N = M$.*

Proof. See [1, thm 2.6, 2.7]. □

Lemma 2.10. *For any ring R and finite decreasing sequence of ideals ending at zero $R = I_0 \supseteq I_1 \supseteq I_2 \supseteq \ldots \supseteq I_n = 0$ we have $|R| = |I_0| = \prod_{i=1}^{n} |I_{i-1}/I_i|$.*

Proof. For $I \supseteq J$ ideals $|I| = |J| \cdot |I/J|$ holds. The result follows. □

Corollary 2.11. *In an artin local ring $(R, \mathfrak{m})$ there is an $n \in \mathbf{Z}_{>0}$ such that $0 = \mathfrak{m}^n = \mathfrak{m}^{n+1} = \ldots$.*

Proof. The decreasing sequence $R \supseteq \mathfrak{m} \supseteq \mathfrak{m}^2 \supseteq \ldots$ must become constant after a finite number of steps by 2.3. So there is an $n \in \mathbb{Z}_{>0}$ such that $\mathfrak{m}^n = \mathfrak{m}^{n+1} = \ldots$. The ideal $\mathfrak{m}$ is the only maximal ideal and so it is contained in the intersection of all maximal ideals of R. Hence we can apply Nakayama's lemma 2.9 (i). We have $\mathfrak{m}^n = \mathfrak{m}\mathfrak{m}^n$ so by 2.9 we get $0 = \mathfrak{m}^n = \mathfrak{m}^{n+1} = \ldots$. □

Definition 2.12. The length of a finite strictly decreasing chain of modules over a ring R is defined to be the number of modules in this chain minus 1. Let M be an R-module, if every descending chain of submodules starting with the module M is finite then the length of that module is defined to be the maximum length of such a chain.
We write $\text{length}_R(M)$ for the length of M as an R-module.

Note that there may be several paths to calculate the length, however they all have the same value, for the proof see [1] pg. 76.

Definition 2.13. Let $n, k, q \in \mathbf{Z}_{\geq 0}$ such that q is a prime power, which is not one, and $k \leq n$. Define $\binom{n}{k}_q$ to be

$$\binom{n}{k}_q := \frac{(q^n - 1)(q^n - q)\ldots(q^n - q^{k-1})}{(q^k - 1)(q^k - q)\ldots(q^k - q^{k-1})}.$$

Note that

$$\frac{(q^n-1)(q^n-q)\dots(q^n-q^{k-1})}{(q^k-1)(q^k-q)\dots(q^k-q^{k-1})} =$$
$$\frac{(q^n-1)q(q^{n-1}-1)\dots q^{k-1}(q^{n-k+1}-1)}{(q^k-1)q(q^{k-1}-1)\dots q^{k-1}(q^1-1)} =$$
$$\frac{(q^n-1)(q^{n-1}-1)\dots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\dots(q^1-1)}$$

which is congruent to $\frac{(-1)^k}{(-1)^k} \pmod q = 1 \pmod q$.

Definition 2.14. Define

$$N(n,q) := \sum_{k=0}^{n} \binom{n}{k}_q.$$

Lemma 2.15. *Let V be a vector space of dimension $n \in \mathbf{Z}_{\geq 0}$ over $\mathbf{F}_q$, a field of cardinality $q \in \mathbf{Z}_{\geq 0}$, then the number of k-dimensional subspaces of V equals $\binom{n}{k}_q$.The total number of subspace is $N(n,q) = \sum_{k=0}^{n}\binom{n}{k}_q$.*

Proof. Let $i \in \{1,\dots,k\}$. If we have i many linearly independent vectors they span a i-dimensional subspace. There are $q^n - q^i$ elements outside of this subspace. If we take such an element it is clear that it is linearly independent with the i-dimensional subspace as together they span a bigger subspace. Any element in the i-dimensional subspace is clearly not linearly independent. This means by induction that there are $(q^n-1)(q^n-q)\dots(q^n-q^{k-1})$ ways to choose a basis for a i-dimensional subspace of V. Note that we are counting the ways in which we can choose such vectors and not the number of different bases.
Therefore the number of ways we can choose k independent vectors in a n-dimensional vector space is $(q^n-1)(q^n-q)\dots(q^n-q^{k-1})$.
We have now also shown that the number of ways we can choose a basis that would span the same subspace is $(q^k-1)(q^k-q)\dots(q^k-q^{k-1})$. In conclusion the number of subspaces of dimension k of a vector space of dimension n over a finite field of size q is equal to

$$\frac{(q^n-1)(q^n-q)\dots(q^n-q^{k-1})}{(q^k-1)(q^k-q)\dots(q^k-q^{k-1})} = \binom{n}{k}_q.$$

The number of subspaces of such a vector space is therefore

$$N(n,q) = \sum_{k=0}^{n} \binom{n}{k}_q.$$

□

3. Rings with only finitely many ideals

In this chapter we will gain some more insight in the structure of rings with finitely many ideals.

Lemma 3.1. *Let $(R,\mathfrak{m})$ be a local artin ring. The following are equivalent:*
(i) R is a principal ideal ring;
(ii) $\mathfrak{m}$ is a principal ideal;
(iii) $\dim_{R/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 \leq 1$;
(iv) For all ideals $I \subset R$ there is a $i \in \{0,1,\dots,\mathrm{length}_R(R)\}$ such that $I = \mathfrak{m}^i$.

Proof. (i)⇒(ii): The ring R is a principal ideal ring so all its ideals are principal; $\mathfrak{m}$ is an ideal of R, so it is a principal ideal.
(ii)⇒(iv): Let $\pi \in R$ be such that $\mathfrak{m} = (\pi)$, such an element exists as $\mathfrak{m}$ is generated by one element. By 2.11 the sequence $R \supseteq \mathfrak{m} \supseteq \mathfrak{m}^2 \dots$ is constantly zero after finitely many steps. Let $\mathfrak{a}$ be an ideal such that $\mathfrak{a} \subseteq \mathfrak{m}$. If $\mathfrak{a} = 0$, then $i = \text{length}_R(R)$ suffices, so we assume $\mathfrak{a} \neq 0$. Now let j be the largest integer such that $\mathfrak{a} \subseteq \mathfrak{m}^j$. There is an element $a \in \mathfrak{a}$ such that $a \in \mathfrak{m}^j \setminus \mathfrak{m}^{j+1}$. Therefore $a = s\pi^j$ for some unit s. After all if s is not a unit, then s would be of the form πt for some $t \in R$. This would mean that $a = \pi^{j+1}t \notin \mathfrak{m}^j \setminus \mathfrak{m}^{j+1}$, which is a contradiction. Hence $\mathfrak{m}^j = (\pi^j) = (a) \subseteq \mathfrak{a} \subseteq \mathfrak{m}^j$ so $\mathfrak{m}^j = \mathfrak{a}$. This means that in such a ring all ideals are of the form $\mathfrak{m}^i$ for some $i \in \{0, 1, \dots, \text{length}_R(R)\}$.
(iv)⇒(i) Take R a ring such that for all ideals $I \subset R$ there is an integer $i \in \{0, \dots, \text{length}_R(R)\}$ such that $I = \mathfrak{m}^i$. Then the ideals are linearly ordered by inclusion. So if an ideal has 2 generators a, b we can assume without loss of generality that $(a) \subseteq (b)$. From this it follows that b generates the ideal on its own. Hence R is a principal ideal ring.
(ii)⇒(iii): The ideal $\mathfrak{m}$ is generated by one element so we can take $\pi \in R$ such that $\mathfrak{m} = (\pi)$. The homomorphism $R \to \mathfrak{m}/\mathfrak{m}^2$ that maps 1 to $\overline{\pi} \in \mathfrak{m}/\mathfrak{m}^2$ is surjective. As this map has kernel a kernel contained in $\mathfrak{m}$ the quotient map $R/\mathfrak{m} \to \mathfrak{m}/\mathfrak{m}^2$ is a surjective homomorphism as well. Therefore the dimension of $\mathfrak{m}/\mathfrak{m}^2$ is less than or equal to the dimension of $R/\mathfrak{m}$ over $R/\mathfrak{m}$, which is 1.
(iii)⇒(ii)
The vector space $\mathfrak{m}/\mathfrak{m}^2$ is of dimension 1 or 0 over $R/\mathfrak{m}$. So there is an element $\pi \in R$ such that $(R/\mathfrak{m})\overline{\pi} = \mathfrak{m}/\mathfrak{m}^2$ and so $R\pi + \mathfrak{m}^2 = \mathfrak{m}$. We can apply 2.9 (ii), because $\mathfrak{m}$ is contained in the intersection of all maximal ideals and is finitely generated, this gives us $\mathfrak{m} = R\pi$.

□

Lemma 3.2. *A local ring* $(R, \mathfrak{m})$ *is finite if and only if* $R/\mathfrak{m}$ *is finite and R is artin.*

Proof. ⇒: The ring R is finite so the residue field $R/\mathfrak{m}$ is finite and R is obviously artin.
⇐: The ring R is an artin ring so by 2.11 there is a $n \in \mathbf{Z}_{\geq 0}$ such that

$$R \supseteq \mathfrak{m} \supseteq \mathfrak{m}^2 \supseteq \dots \supseteq \mathfrak{m}^n = 0.$$

The dimension of $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ over $R/\mathfrak{m}$ is finite because $\mathfrak{m}$ is finitely generated and every generator of $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ is the image of some generator of $\mathfrak{m}$ under the natural projection. The cardinality of R, which is $\prod_{i=0}^{n} |\mathfrak{m}^i/\mathfrak{m}^{i+1}|$ by 2.10, must then also be finite.

□

Theorem 3.3. *A ring R has only finitely many ideals if and only if R is the product of an artin principal ideal ring and a finite ring.*

Proof. The ideals of products of rings are products of the ideals of those rings. If the rings in product all have only finitely many ideals then the product has only finitely many ideals.
⇐: Let Q be a 0-dimensional principal ideal ring. We can write Q as the product of local rings by 2.8. By 3.2 we know that all of these local rings are finite. Clearly

finite rings have only finitely many ideals, as they have only finitely many subsets, concluding this part of the proof. ⇒:
The ring R is artin therefore it can be seen as the product of local artin rings by 2.8. The implication holds if these local artin rings are either principal ideal rings or finite rings. Assume this is not the case and one of these rings $(Q, \mathfrak{m})$ is an infinite artin local non-principal ideal ring. Then by 3.2 we see $Q/\mathfrak{m}$ is infinite as Q is local and artin. We can apply 3.1, as Q is not a principal ideal ring and is artin and local, yielding that $\mathfrak{m}/\mathfrak{m}^2$ has dimension greater than 1 over $Q/\mathfrak{m}$. As $Q/\mathfrak{m}$ is infinite and $\mathfrak{m}/\mathfrak{m}^2$ has a dimension higher than 1. The vector space $\mathfrak{m}/\mathfrak{m}^2$ has infinitely many submodules. These submodules can be lifted to ideals of R, therefore this is in contradiction with the assumption that R has only finitely many ideals. Hence Q is finite. This means that R is the product of artin local principal ideal rings and finite rings. So we can write R as product of an artin principal ideal ring and a finite ring.

□

4. Bounds

It will in general be useful to have an upper and lower bound for the number of elements in a finite local non-principal ideal ring $(R, \mathfrak{m})$ ring based on its number of ideals.

Lemma 4.1. *Let R be a ring. Let M be an R-module with a maximal submodule $N \subsetneq M$. Then there is a maximal ideal $\mathfrak{m} \subset R$ such that $M/N \cong R/\mathfrak{m}$.*

Proof. Take $a \in M \setminus N$ then $N \subsetneq N + aR \subseteq M$ and so by maximality we have $N + aR = M$. Therefore the map $R \to M/N : r \mapsto ra$ is a surjection. If we divide out by the kernel of this map, call it K, this reduces to an isomorphism. The ideal K must be maximal in R as every ideal between R and K can be lifted to a submodule of M/N . Therefore one has $I/J \cong_R R/\mathfrak{m}$, for some maximal ideal $\mathfrak{m}$. □

Lemma 4.2. *For $(R, \mathfrak{m})$ a finite local non principal ideal ring with exactly n ideals and $d \in \mathbf{Z}_{\geq 2}$ such that $d = \dim_{R/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2)$. We have the following:*

$$\#R = \#(R/\mathfrak{m})^{\text{length}_R(R)} \leq \#(R/\mathfrak{m})^{n-N(d,\#R/\mathfrak{m})+d} \leq$$
$$\#(R/\mathfrak{m})^{n-N(2,\#R/\mathfrak{m})+2} \leq \#(R/\mathfrak{m})^{n-3}.$$

Proof. Combining 2.12, 2.10 and 4.1 gives us the first equality.
By 2.13 there are at least $N(d, \#R/\mathfrak{m})$ subspaces of $\mathfrak{m}/\mathfrak{m}^2$. Hence for a local non-principal ring we have at least

$$N(d, \#R/\mathfrak{m})$$

modules in between $\mathfrak{m}$ and $\mathfrak{m}^2$ whilst $\text{length}_R(\mathfrak{m}/\mathfrak{m}^2) = d$. Note that

$$\begin{aligned} n &\geq \text{length}_R(R/\mathfrak{m}) + N(d, \#R/\mathfrak{m}) + \text{length}_R(\mathfrak{m}^2) \\ &\geq \text{length}_R(R/\mathfrak{m}) + \text{length}_R(\mathfrak{m}/\mathfrak{m}^2) + (N(d, R/\mathfrak{m}) - d) + \text{length}_R(\mathfrak{m}^2) \\ &= \text{length}_R(R) + N(d, \#R/\mathfrak{m}) - d. \end{aligned}$$

Therefore
$n - N(d, \#R/\mathfrak{m}) + d \geq \text{length}_R(R)$ which gives us the second inequality.

Note that $N(d, \#R/\mathfrak{m}) - d \geq N(2, \#R/\mathfrak{m}) - 2$ as a vector space of dimension $m \in \mathbf{Z}_{\geq 0}$ has more than one subspace of any dimension r if $0 < r < m$. Therefore the third inequality holds. Then $n - N(2, \#R/\mathfrak{m}) + 2 \leq n - 3$ gives us the last equality. □

For a finite local non-principal ideal ring R this gives us an upper bound for $\#R$ based on the number of of ideals it has and the cardinality of its residue field $R/\mathfrak{m}$.

We will now give a lower bound by showing that:

Lemma 4.3. *Let $(R, \mathfrak{m})$ be a finite local ring. Let V be an $R/\mathfrak{m}$-vector space of length $n \in \mathbf{Z}_{\geq 0}$. Take any $k \in \{1, \ldots, n-1\}$. Then for M any non-isomorphic R-module of length n we have that V has more submodules of length k than M has.*

Let R be an artin ring. For any finitely generated R-module M take a submodule N. We can make the following exact sequence:

$$\begin{tikzcd} 0 \arrow[r] & N \arrow[r] & M \arrow[r] & M/N \arrow[r] & 0. \end{tikzcd}$$

If we then take another submodule B_0 of M we get the following commutative diagram with exact rows:

$$\begin{tikzcd} 0 \arrow[r] & N \arrow[r] & M \arrow[r] & M/N \arrow[r] & 0 \\ 0 \arrow[r] & A = N \cap B_0 \arrow[r] \arrow[u] & B_0 \arrow[r] \arrow[u] & C = B_0/A \arrow[r] \arrow[u] & 0 \end{tikzcd}$$

If we can find out how many submodules B fit this diagram at the place of B_0 for certain A, C we have a way of counting the number of submodules of M.

Lemma 4.4. *Let $(R, \mathfrak{m})$ be a finite local ring. Take V a 1-dimensional $R/\mathfrak{m}$-vector space, and N a finite R-module.*
Then the following are equivalent:
(i) For for all R-modules $A \subseteq N$ we have $\#\mathrm{Hom}_R(V, N/A) \cong \#N/A$;
(ii) $N = N[\mathfrak{m}]$, where $N[\mathfrak{m}]$ are the elements of N which are annihilated by $\mathfrak{m}$ (which means N is an $R/\mathfrak{m}$ module).

Proof. $(ii) \Rightarrow (i)$: Note that we can see V as an R-module which is annihilated by $\mathfrak{m}$. For every generator $v \in V$ module homomorphisms from V to N/A are uniquely determined by its image. Let $A \subset N$ be a submodule. The image of v under any R-module homomorphism from V to N/A is annihilated by $\mathfrak{m}$, as v is annihilated by $\mathfrak{m}$. Hence v is an element of $(N/A)[\mathfrak{m}]$, and can be any element of $(N/A)[\mathfrak{m}]$. Therefore we have $\mathrm{Hom}_R(V, N/A) \cong N/A[m] = N/A$, because $N[\mathfrak{m}] = N$.
$(i) \Rightarrow (ii)$: Take $A = 0 \subseteq N$ then we have $\#\mathrm{Hom}_R(V, N/A) = \#\mathrm{Hom}_R(V, N)$ which, with the same reasoning as before, is $\#N[m]$. □

Lemma 4.5. *Let $(R, \mathfrak{m})$ be a local ring. Let M be a R-module with submodule N. Let $A \subseteq N$ respectively $C \subseteq M/N$ be submodules of N respectively M/N. Let $S_{N,A,C}$ be the set of submodules B of M making the following commutative diagram with exact rows.*

The arrows in this diagram represent the natural maps:

$$\begin{tikzcd}
0 \arrow[r] & N \arrow[r] & M \arrow[r] & M/N \arrow[r] & 0 \\
0 \arrow[r] & A \arrow[r] \arrow[u] & B \arrow[r] \arrow[u] & C \arrow[r] \arrow[u] & 0.
\end{tikzcd}$$

For every $B \in S_{N,C,A}$ define $\sigma(B) \in \mathrm{Hom}_R(C, M/A)$ as the composition of the natural maps $C \overset{\sim}{\to} B/A$ and $B/A \to M/A$. Suppose $B_0 \in S_{N,A,C}$. Then the map

$$\begin{array}{rcl} \phi : S_{N,C,A} & \to & \mathrm{Hom}_R(C, N/A) \\ B & \mapsto & \sigma(B) - \sigma(B_0) \end{array}$$

is a bijection.

Proof. Assume that there is $B_0 \in S_{N,A,C}$. Note that for any $B \in S_{N,A,C}$ we have the following diagram:

$$\begin{tikzcd}
 & & M/N \\
C \arrow[r, "\sim"] \arrow[urr] & B/A \arrow[r] & M/A \arrow[u, hook]
\end{tikzcd}$$

We will call this diagram D. In this diagram the arrows between C and B/A represent the isomorphisms and the rest the natural injections.

By the commutativity of the diagram from the lemma the diagram D is commutative as well. For every B this gives us an induced map, call it $\sigma(B) \in \mathrm{Hom}_R(C, M/A)$, from C to M/A. Note that for all such B the map $\sigma(B) - \sigma(B_0)$ is a homomorphism from C to M/A. The induced map from C to M/N is the same for all possible modules B. Hence $\sigma(B) - \sigma(B_0)$ can be viewed as a homomorphism from C to N/A. We have hereby constructed the map ϕ.

We will now construct the inverse. Let f be an element of $\mathrm{Hom}_R(C, N/A)$. Note that f can be seen as an element of $\mathrm{Hom}_R(C, M/A)$. The map $g := f + \sigma(B_0)$ is then a homomorphsim from C to M/A as sum of two such homomorphisms. Let π be the map from M to M/A. Then, as both π and g are homomorphisms, $\pi^{-1}(g(C))$ is a submodule of M. We have $A \subset B$, as $A = \pi^{-1}(0)$. Now we need to show that there is a surjective map from B to C such that A is its kernel. In other words we need to prove that there is an isomorphism from $\pi(B) = B/A$ to C, note that $B/A = g(C)$ as $g(C) \subset M/A$ and $\pi^{-1}(g(C)) = B$. We already have a surjective homomorphism from C to $g(C)$, namely g. We will now show that g is injective. Take $c \in C$ such that $g(c) = 0$ then

$$f(c) + \sigma(B_0)(c) = g(c) = 0.$$

Note that $f(c) \in N/A$ and $\sigma(B_0)(c) \in B_0/A$ as such $f(c), \sigma(B_0)(c) \in B_0 \cap N/A = 0$. Therefore $\sigma(B_0)(c) = 0$ and as $\sigma(B_0)$ is injective this means that $c = 0$. Hence g is an isomorphism and $g^{-1} \circ \pi$ is a surjective map to C from B which has the image of A as a kernel. Call the map that sends an element $f \in \mathrm{Hom}_R(C, N/A)$ to such a submodule ψ.

For $x \in C$ we have

$$\phi(\psi(f))(x) = \phi(\pi^{-1}(f + \sigma(B_0)(C))(x) =$$
$$\sigma(\pi^{-1}((f(C) + \sigma(B_0)(C)))(x) - \sigma(B_0)(x) = f(x) + \sigma(B_0)(x) - \sigma(B_0)(x).$$

The third equality holds because π^{-1} sends an element to its inverse image under the natural mapping from M to M/A whilst σ practically mods out by A. Note that

$$\psi(\phi(B)) = \psi(\sigma(B) - \sigma(B_0)) =$$
$$\pi^{-1}(\sigma(B) - \sigma(B_0) + \sigma(B_0)(C)) = \pi^{-1}(\sigma(B))(C)) = \pi^{-1}(B/A) = B.$$

We get the last equality as B is the only submodule of M that is mapped to B/A by π. Therefore ϕ and ψ are each others two sided inverses. Hence the map ϕ is the bijection we were looking for. □

Proof of lemma 4.3. Let $N \subset M$ be a maximal module in M. Let A be the set of submodules of N and let B be $\{0, M/N\}$. Set $T_k \subset A \times B$ to be the set of pairs of which the lengths sum to k. Then it suffices to show that $\sum_{(C,D)\in T_k} \#S_{N,C,D} \leq \binom{n-1}{k-1}_{\#(R/\mathfrak{m})}(\#(R/\mathfrak{m}))^{n-k} + \binom{n-1}{k}_{\#(R/\mathfrak{m})} = \binom{n}{k}_{\#(R/\mathfrak{m})}$ with equality if and only if $k = 0$ or if M is a vector space. Afterall $\sum_{(C,D)\in T_k} \#S_{N,C,D}$ is the number of submodules of M of length k by a combination of 4.4 and 4.5. We will prove this by induction on the length n of the module M.
For any $n \in \mathbf{Z}_{\geq 0}$ there is always one module of length k for $k \in \{0, n\}$.
The lemma is true for $n = 1$ as for $k \in \{0, \ldots, n-1\} = \{0\}$ the only module that can possibly have length k is 0.
Take $m \in \mathbf{Z}_{\geq 1}$. Assume the lemma holds for all $n < m$. Let M be a module of length m. Take any $k \in \{1, \ldots, m-1\}$. By 4.1 M/N is a 1-dimensional vector space over $R/\mathfrak{m}$. Note that every submodule of M of length k is an element of $S_{N,C,D}$ for a unique pair $(C, D) \in T$, because of the additivity of the length over exact sequences. We then have that the number of submodules of M of length k equals $\sum_{(C,D)\in T_k} \#S_{N,C,D}$. Furthermore by 4.5 we have $\sum_{(C,D)\in T_k} \#S_{N,C,D} \leq \sum_{(C,D)\in T_k} \#\mathrm{Hom}_R(D, N/C)$ where this is an equality if and only if for all the combinations of A and C the set $S_{N,A,C}$ is non-empty. It is clear that if M is a vector space $S_{N,A,C}$ is non-empty. Note that by 4.4 we have

$$\begin{aligned}
&\sum \quad {}_{(A,C)\in T_k}\#\mathrm{Hom}_R(C, N/A) = \\
&\sum \quad {}_{A\subset N:\mathrm{length}_R(A)=k-1}\#\mathrm{Hom}_R(M/N, N/A) + \\
&\sum \quad {}_{A\subset N:\mathrm{length}_R(A)=k}\#\mathrm{Hom}_R(0, N/A) \leq \\
&\sum \quad {}_{A\subset N:\mathrm{length}_R(A)=k-1}\#(N/A) + \\
&\sum \quad {}_{A\subset N:\mathrm{length}_R(A)=k}1
\end{aligned}$$

with equality if $N = N[\mathfrak{m}]$.
By induction $\forall i \in \{0, \ldots, m-1\}$ we have that N has the most ideals of length i iff it is a vector space or $i = 0$, in both cases it has $\binom{n-1}{i}_{\#(R/\mathfrak{m})}$ of them, call this result (1). Furthermore for a submodule A of N of length k we have that $\#N/A = (\#(R/\mathfrak{m}))^{n-k}$. Therefore from our induction hypothesis it follows that

$$\sum_{A\subset N:\mathrm{length}_R(A)=k-1} \#(N/A) \leq \binom{n-1}{k-1}_{\#(R/\mathfrak{m})} (\#(R/\mathfrak{m}))^{n-k},$$

$$\sum_{A\subset N:\mathrm{length}_R(A)=k} 1 \leq \binom{n-1}{k}_{\#(R/\mathfrak{m})}$$

with equality iff N is a vector space. This is last part follows from the fact that if N is a vector space we clearly have equality and if N is not a vector space then by result (1) we have

$$\sum_{A\subset N:\mathrm{length}_R(A)=k-1} \#(N/A) \leq \binom{n-1}{k-1}_{\#(R/\mathfrak{m})} (\#(R/\mathfrak{m}))^{n-k},$$

$$\sum_{A\subset N:\mathrm{length}_R(A)=k} 1 < \binom{n-1}{k}_{\#(R/\mathfrak{m})}$$

as $k \neq 0$. This means we have equality if and only if $N = N[\mathfrak{m}]$. Note that $N = N[\mathfrak{m}]$ means that N is a vector space. Now all we need to prove is that if M has such a maximal submodule N which is a $R/\mathfrak{m}$-vector space then M is a $R/\mathfrak{m}$-vector space. Take M a module with such a submodule N. Take $C = 0$ then there is an $N' \in S_{N,C,M/N}]$ such that:

$$\begin{tikzcd}
0 \arrow[r] & N \arrow[r] & M \arrow[r] & M/N \arrow[r] & 0 \\
0 \arrow[r] & 0 \arrow[r] \arrow[u] & N' \arrow[r] \arrow[u] & M/N \arrow[r] \arrow[u, leftrightarrow] & 0
\end{tikzcd}$$

is a commutative diagram where the rows are exact sequences. Note that the arrow between M/N and M/N as well as the arrow between N' and M/N are isomorphsims. Therefore by the commutativity of the diagram the sequence:

$$\begin{tikzcd}
0 \arrow[r] & N \arrow[r] & M \arrow[r] & M/N \arrow[r] & 0
\end{tikzcd}$$

Hence we find that the diagram is split. Hence we have $M = N \oplus M/N$. Which is therefore an $R/\mathfrak{m}$-vector space as sum of two such vector spaces. If M is a vector space we know that the number of ideals of length i equals $\sum_{(C,D)\in T_k} \#S_{N,C,D}$ by 4.4 and 4.5 and by 2.14 it equals $\binom{n-1}{k-1}_{\#(R/\mathfrak{m})}(\#(R/\mathfrak{m}))^{n-k} + \binom{n-1}{k}_{\#(R/\mathfrak{m})} = \binom{n}{k}_{\#(R/\mathfrak{m})}$. Therefore we have

$$\sum_{(C,D)\in T_k} \#S_{N,C,D} \leq \binom{n-1}{k-1}_{\#(R/\mathfrak{m})} (\#(R/\mathfrak{m}))^{n-k+1} + \binom{n-1}{k}_{\#(R/\mathfrak{m})}$$

with equality if and only if M is a vector space or $k = 0$. □

Lemma 4.6. *Take any finite local ring $(R, \mathfrak{m})$ which has precisely n ideals. Take the smallest $d \in \mathbf{Z}_{\geq 0}$ such that $N(d, \#R/\mathfrak{m}) + 1 \geq n$. Then one has that $(R/\mathfrak{m})^{d+1}$ is a lower bound for the number of elements in that ring. The maximal ideal of any ring that reaches this lower bound is a vector space over its residue field.*

Proof. To prove this we need to show that for a finite local ring with maximal ideal $\mathfrak{m}$ and length $d+1$, where $d \in \mathbf{Z}_{\geq 0}$, the maximal ideal $\mathfrak{m}$ cannot have more than $N(d, \#R/\mathfrak{m})$ sub-ideals. This is a result of 6.9 as $\mathfrak{m}$ is, like all ideals, an R-module, and 6.9 states that $\mathfrak{m}$ has the maximal number of submodules if it is a vector space. By definition $N(d, \#R/\mathfrak{m})$ is the number of submodules of a vector space this size. □

Proof of Theorem 1.1. The first part holds by 4.6. The second by 4.2. □

This, given $R/\mathfrak{m}$, gives us a lower bound for the number of elements of any finite local ring.

Note that from the upper and lower bound it follows that there are no non principal local artin rings with less than 6 ideals, as the lowerbound exeeds the upperbound. Hence, to give more of an idea what these bounds mean, I will demonstrate the lower and upper bounds for rings with 6 to 10 ideals. As both the bounds are dependent on the residue field of the local ring we will give the upper and lower bound as function of number of ideals and number of elements in the residue field. Note that the residue fields are finite fields and therefore their cardinality is a prime power. We will later see a family of rings that reaches the lower bound.

$\#R/\mathfrak{m}$	Number of ideals	Lower bound	Upper bound
2	6	2^3	2^3
2	7	2^4	2^4
3	7	3^3	3^3
2	8	2^4	2^4
3	8	3^4	3^4
4	8	4^3	4^3
2	9	2^4	2^5
3	9	3^4	3^5
4	9	4^4	4^4
5	9	5^3	5^3
2	10	2^4	2^7
3	10	3^4	3^6
4	10	4^4	4^5
5	10	5^4	5^4

5. Diagrams

Definition 5.1. Let $(R, \mathfrak{m})$ be a local ring. We define $(J : \mathfrak{m}) := \{x \in R$ such that $x\mathfrak{m} \subseteq J\}$. This is clearly an ideal.

Lemma 5.2. *In a local ring $(R, \mathfrak{m})$ for any ideal I we have that:*

i. *$I/\mathfrak{m}I$ is a vector space over $R/\mathfrak{m}$.*

ii. *$(I : \mathfrak{m})/I$ is a vector space over $R/\mathfrak{m}$*

Proof. (i): It is clearly a module over R and $\mathfrak{m}$ is in the kernel of the module action as for all $x \in I$ we have $\mathfrak{m}x \subseteq \mathfrak{m}I$.
(ii): Note that $I \subseteq (I : \mathfrak{m})$ as $I\mathfrak{m} \subset I$. Therefore $(I : \mathfrak{m})/I$ is well defined. It is clearly a module over R and $\mathfrak{m}$ is in the kernel of the module action by definition of $(I : \mathfrak{m})$. □

It would be ideal for us if for some ideal structure we could determine whether there is a ring with that structure or not. We cannot do this, however we can derive quite a lot of other information from diagrams of ideals.

Lemma 5.3. *Let $(R, \mathfrak{m})$ be a local noetherian ring. Then the following hold for any ideal $I \subseteq R$.*

i. *There is a bijection between the set of ideals $\{J : J \subseteq I$ such that J is maximal in $I\}$ and hyperplanes in $I/\mathfrak{m}I$, which is given by $J \mapsto J/\mathfrak{m}I$.*
ii. *There is a bijection between the set of ideals $\{J : I \subseteq J$ such that I is maximal in $J\}$ and 1-dimensional sub-vector spaces of $(I : \mathfrak{m})/I$, which is given by $J \mapsto J/I$.*

Proof. (i): For such a maximal ideal J we have $\mathfrak{m}I \subseteq J$, because $J + \mathfrak{m}I \neq I$ by 2.9 as $J \neq I$. The module $I/\mathfrak{m}I$ is a vector space over $R/\mathfrak{m}$ by 5.2. Our bijection is the one that sends an ideal J to $J/\mathfrak{m}I \subseteq I/\mathfrak{m}I$. If we have two different such ideals then when dividing out by $\mathfrak{m}I$ they will be mapped to two different hyperplanes, they are mapped to hyperplanes because there can not be anything in between their image and $I/\mathfrak{m}I$.
(ii): For an ideal J in which I is maximal we have $\mathfrak{m}J \subseteq I$, because if this were not the case by maximality of I in J we have $\mathfrak{m}J + I = J$ and by 2.9 (ii) we would have $J = I$ which is a contradiction. Hence we have $J \subseteq (I : \mathfrak{m})$. The module $(I : \mathfrak{m})/I$ is a vector space over $R/\mathfrak{m}$ by 5.2. Our bijection is the one that sends an ideal J to $J/I \subseteq (I : \mathfrak{m})/I$. If we have two different such ideals then as they both contain I they are mapped to different subspaces if we divide out by I they are also mapped to 1-dimensional subspaces because I is maximal in them.

□

Theorem 5.4. *Let $(R, \mathfrak{m})$ be a local ring with finitely many ideals. Let $q = \#R/\mathfrak{m}$ if $R/\mathfrak{m}$ is finite and 0 otherwise. Then for $i \in \{0, 1, \ldots, \text{length}_R(R)\}$ we have $\#\{I \subseteq R : \text{length}_R(I) = i\} \equiv 1 \pmod{q}$.*

Proof. Note that $\text{length}_R(R)$ is finite as R has only finitely many ideals. For $q = 0$ we know that $R/\mathfrak{m}$ is infinite. Then by 3.2 the ring is infinite and then because it is local by 3.3 it is a principal ideal ring. Utilising 3.1 we know all its ideals are of the form $\mathfrak{m}^i$ and so the theorem holds in this case.
For $q \neq 0$ we will prove it by induction on $i \in \{0, 1, \ldots, \text{length}_R(R)\}$. For $i = 0$ it is clear as (0) is the only one of that length. Let $N \in \{0, \ldots n\}$. Assume the theorem holds for all $n < N$. With 2.13, 2.15 and 5.3 for every ideal of length N there are $1 \pmod{q}$ of length $N - 1$ contained in it and for every ideal of length $N - 1$ there are $1 \pmod{q}$ ideals of length N which contain it. Hence we have:

$$\begin{aligned} 1 \pmod{q} &\equiv \#\{I : I \subseteq R,\ \text{length}_\text{R}(I) = N - 1\} \\ &\equiv \#\{(I, J) : I \subseteq R,\ \text{length}_R(I) = N - 1,\ \text{length}_R(J) = N, I \subseteq J\} \\ &\equiv \#\{J : J \subseteq R,\ \text{length}_R(J) = N\}. \end{aligned}$$

Therefore the theorem holds for N as well, so by induction it holds for all $N \in \{0, 1, \ldots, \text{length}(R)\}$. □

We also know that two rings with the same diagrams do not necesarily have to be isomorphic. For example $\mathbb{Z}[X, Y]/(2, X^2, Y^2, XY)$ and $\mathbb{Z}[X]/(4, X^2, 2X)$ are not isomorphic and both of them have the following diagram:

$$\begin{tikzcd}
 & R \arrow[d, dash] & \\
 & (a,b)=\mathfrak{m} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
(a) \arrow[dr, dash] & (b) \arrow[d, dash] & (a+b) \arrow[dl, dash] \\
 & 0 &
\end{tikzcd}$$

where for the first ring we take $a = X$ en $b = Y$ and for the second one we take $a = X$ en $b = 2$. These rings are not isomorphic as in the first ring we have $1+1 = 0$ and in the second we have $1 + 1 = 2 \neq 0$.

6. Families of rings

Let $n \in \mathbf{Z}_{\geq 0}$. We will try to create a finite local non-principal ideal ring with exactly n ideals. For this reason we will study certain families of rings.

6.1. **Family 1.**

Definition 6.1. For $p \in \mathbf{N}$ prime and $n, d \in \mathbf{Z}_{\geq 1}$, where $d > 1$ if $n = 1$, let V_d signify a vector space over $\mathbb{Z}/p\mathbb{Z}$ of dimension d. Define the commutative group $R_{n,p,d}$ to be $\mathbb{Z}/p^n\mathbb{Z} \oplus V_d$. Then define a commutative multiplication $\cdot : R_{n,p,d} \times R_{n,p,d} \to R_{n,p,d}$ by setting it to be the normal multiplication on the subset $\mathbb{Z}/p^n\mathbb{Z} \times \mathbb{Z}/p^n\mathbb{Z}$, the module action on $\mathbb{Z}/p\mathbb{Z} \times V_d$ and the trivial map, sending all elements to 0, on $V_d \times V_d$.

It will soon become clear that this is a ring and that the generators of the maximal ideal of this ring are p and the generators of V_d as a vectorspace. Therefore if we had allowed $d = 1, n = 1$, which would imply that $p = 0$, the maximal ideal would only have one generator, wich would mean the ring is a principal ideal ring which we are not interested in.

Lemma 6.2. *The group $R_{n,p,d}$ with the multiplication defined in this way is a finite local ring with maximal ideal $\mathfrak{m} = (p) \oplus V_d$ and residue field $\mathbf{Z}/p\mathbf{Z}$.*

Proof. First we will check the ring axioms. The requirements for addition are met by definition. The multiplication is associative on the three sets it is defined on therefore the multiplication must be associative. Take $a, b, c \in R_{n,p,d}$. If $a, b \in V_d$ or $a, b \in \mathbf{Z}/p^n\mathbf{Z}$ then we have $c(a + b) = ca + cb$, because $\mathbf{Z}/p^n\mathbf{Z}$ and V_d work distributively on V_d and $\mathbf{Z}/p^n\mathbf{Z}$. If $a \in \mathbf{Z}/p^n\mathbf{Z}, b \in V_d$ the product $c(a + b)$ is defined to be $ca + cb$. Therefore the addition is distribitive.
The ideal $\mathfrak{m} := (p) \oplus V_d$ is maximal as $R_{n,p,d}/((p) \oplus V_d) = \mathbb{F}_p$ which is a field. Note that every element not contained in this ideal is of the form $a \oplus v$ where $a \in (\mathbf{Z}/p^n\mathbf{Z})^*$ and $v \in V_d$ which has $a^{-1} \oplus -a^{-2}v$ as its inverse. This means that every element outside of $\mathfrak{m}$ is a unit. Therefore $\mathfrak{m}$ is the unique maximal ideal. □

Lemma 6.3. *The ring $R_{n,p,d}$ is a non-principal ideal ring with precisely $(N(d+1,p)-N(d,p))\cdot(n-1)+N(d,p)+1$ ideals.*

Proof. Take a non-zero element $a \in \mathfrak{m}$. By definition of $R_{n,p,d}$ there is a unique $i \in \{1,\dots,n\}$ such that there are $b \in (\mathbf{Z}/p^n\mathbf{Z})^*$, $c \in V_d$ for which $a = bp^i + c$.
Let $I \subsetneq R_{n,p,d}$ and then let $a \in I$ be an element of which the corresponding $i \in \{1,\cdots,n\}$ is minimal amongst the elements of I. Then we have $I \subset (p^i) \oplus V_d$ by minimalitly of i, note that this would not hold for any larger i. We also get $(p^{i+1}) \subsetneq (a)$, as long as $a \neq 0$ as in that case $p^{i+1} = p^{n+1} = 0$. Note that therefore $(p)^{i+1} \subsetneq I \subset (p)^i \oplus V_d$. Note that $(p^{i-1}) \not\subset I$ as then $i-1$ would be the minimal i found. This means for an ideal there are at most two elements $i, j \in \{1,\cdots,n-1\}$ such that $(p)^{i+1} \subsetneq I \subset (p)^i \oplus V_d$, $(p)^{j+1} \subsetneq I \subset (p)^j \oplus V_d$.
This means that if $i \in \{1,\cdots n-1\}$ the ideals J such that $(p)^{i+1} \subsetneq J \subset (p)^i \oplus V_d$ for which $(p)^j \subsetneq J \subset (p)^j \oplus V_d$ does not hold for any $j \in \{i+1,\dots,n\}$ correspond to the subspaces of $(p)^i \oplus V_d/(p)^{i+1}$ which are not contained in $(p)^{i+1} \oplus V_d/(p)^{i+1}$. Note that $(p)^{i+1} \oplus V_d/(p)^{i+1} = 0 \oplus V_d$ which is a d dimensional subspace of $(p)^i \oplus V_d/(p)^{i+1} = (p)^i/p^{i+1} \oplus V_d$ which is a $d+1$ dimensional subspace. So the number of all the ideals $I \subsetneq R_{n,p,d}$ not contained in V_d is $(n-1)(N(d+1,p)-N(d,p))$. For $i = n$ the set $\{i+1,\dots,n\}$ is empty so here we need to simply count all the subspaces of $(p)^i \oplus V_d/(p)^{i+1} = (0) \oplus V_d/(0) = 0 \oplus V_d$.
Therefore this ring has precisely $(N(d+1,p)-N(d,p))\cdot(n-1)+N(d,p)+1$ ideals. Note that $(p)^1 \oplus V_d/(p)^2$ is a $d+1$ dimensional vector space as $d>0$ its dimension is more than 2 therefore this ring is not a principal-ideal ring.

□

6.2. **Family 2.**

Definition 6.4. Let q be a prime power. Let $m, n \in \mathbf{Z}_{\geq 2}$. Let $\mathbf{F}_q$ be a field of cardinality q and let $\mathbf{F}_{q^m}$ be a field extension over $\mathbf{F}_q$ of degree m. Define $P_{q,m,n}$ as the inverse image of $\mathbf{F}_q$ of the morphism π from $\mathbf{F}_{q^m}[X]/(X^n)$ to $\mathbf{F}_{q^m}$ that mods out by the unique maximal ideal (X).

Lemma 6.5. *The set $P_{q,m,n}$ is a finite local ring with maximal ideal*

$$\mathfrak{m} := X \cdot \mathbf{F}_{q^m}[X]/(X^n) \cap P_{q,m,n}.$$

Proof. Since $P_{q,m,n}$ is the inverse image of a ring under a ring homomorphism, it is a ring itself.
The ring $\mathbf{F}_{q^m}[X]/(X^n)$ is finite so $P_{q,m,n}$ is finite too.
It is clear that $\mathfrak{m} = (X \cdot \mathbf{F}_{q^m}[X]/(X^n)) \cap P_{q,m,n}$ is an ideal in $P_{q,m,n}$ as it is equal to $X \cdot \mathbf{F}_{q^m}[X]/(X^n)$ as set which is an ideal in $\mathbf{F}_{q^m}[X]/(X^n)$. All the elements outside of the maximal ideal are units in $\mathbf{F}_{q^m}[X]/(X^n)$ and the first coordinate of their inverses map is the inverse of their first coordinates which are therefore in $\mathbf{F}_q$ so they are units in $P_{q,m,n}$ as well. Therefore $\mathfrak{m} = X \cdot \mathbf{F}_{q^m}[X]/(X^n) \cap P_{q,m,n}$ is the unique maximal ideal. □

Proposition 6.6. *The ring $P_{q,m,n}$ is a non-principal ideal ring and has precisely $(n-1)(N(m,q)-1)+2$ ideals. By taking quotients of rings of this form we can create non-principal ideal rings which have precisely $(n-2)(N(m,q)-1)+2+(N(d,q)-1)$ ideals for any $d \in \mathbf{Z}_{\geq 0}$ such that $d \leq m$ and $d > 1$ if $n = 2$.*

Proof. Define $F := \mathbf{F}_{q^m}[X]/(X^n)$. Note that as the maximal ideals of $P_{q,m,n}$ and F are the same sets their powers must be the same as well. Hence $\mathfrak{m}^i = X^i F$. We have:

$$XF \subseteq P_{q,m,n} \subseteq F$$

and so for any ideal $I \subsetneq P_{q,m,n}$ we have:

$$XFI \subseteq I \subseteq FI.$$

There is an $i \in \{1, \dots n\}$ such that

$$FI = X^i F$$

as F is a local principal ideal ring. Then

$$XFI = XX^i F = X^{i+1} F$$

follows. Combining this information gives us that for every non-zero ideal $I \subsetneq R_{q,o,n}$ there is a unique $i \in \{1, \dots, n-1\}$ such that $\mathfrak{m}^{i+1} \subsetneq I \subseteq \mathfrak{m}^i$ as for two different such i_1, i_2 we have $\mathfrak{m}^{i_1} \setminus \mathfrak{m}^{i_1+1} \cap \mathfrak{m}^{i_2} \setminus \mathfrak{m}^{i_2+1} = \emptyset$. So every ideal apart from $P_{q,m,n}$ and 0 can uniquely represented as a non-zero subspace of a vector space of the form $\mathfrak{m}^i/\mathfrak{m}^{i+1}$, for some $i \in \{1, \dots, n-1\}$. Note that $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ is a 1 dimensional vector space over $\mathbf{F}_{q^m}$ so $\#\mathfrak{m}^i/\mathfrak{m}^{i+1} = \#\mathbf{F}_{q^m} = \#(\mathbf{F}_q)^m = \#P_{q,m,n}/\mathfrak{m}$. We note that this implies that $P_{q,m,n}$ is not a principal ideal ring. Note that there are $n-1$ vector spaces of the form $\mathfrak{m}^i/\mathfrak{m}^{i+1}$, for some $i \in \{1, \dots, n-1\}$. So the number of ideals this ring has is $(n-1)(N(m,q)-1)+2$. We can divide out by any ideal $I \subsetneq \mathfrak{m}$ such that $\dim(\mathfrak{m}/(\mathfrak{m}^2+I)) > 1$, which means the resulting ring is still a non principal-ideal ring. Note that any ideal $I \subset \mathfrak{m}^2$ satisfies $\mathfrak{m}/(\mathfrak{m}^2+I) > 1$ and any ideal which corresponds to a subspace in $\mathfrak{m}/\mathfrak{m}$ which is not $\mathfrak{m}^2$ and of which the dimension is 2 lower than that of $\mathfrak{m}/\mathfrak{m}^2$. In this way we can effectively vary the dimension of $\mathfrak{m}^{n-1}/\mathfrak{m}^n$ anywhere from 0 to m as long as $\mathfrak{m}^{n-1}$ is not the maximal ideal in which case the dimension must be at least 2. Therefore we can create rings with exactly $(n-2)(N(m,q)-1)+2+(N(d,q)-1)$ ideals for every $d \leq m$ such that $d > 1$ if $n = 2$. □

6.3. **Family 3.**

Lemma 6.7. *Take $n \in \mathbf{Z}_{>0}, q \in \mathbf{N}$ with q a prime power. Let V be a n dimensional vector space over $\mathbf{F}_q$, for $\mathbf{F}_q$ some field of cardinality q. Let H_i, $i \in \{1, \dots n\}$, be hyperspaces such that $V \cap \bigcap_{i \in S \subset \{1,\dots,n\}} H_i$ is a $n - \#S$ dimensional vector space. Then the number of subspaces of V which are not contained in any of the H_i is $\sum_{i=0}^n (-1)^i \binom{n}{i} N(n-i,q)$.*

Proof. In this proof for $W \subseteq V$ a subspace we write $N(W)$ for the number of subspaces of W. By the inclusion-exclusion principle $|\{W \subseteq : \exists i : W \subseteq H_i\}| = \sum_{i=1}^n N(H_j) - \sum_{1=i1<j}^n N((H_i \cap H_j)) + \dots + (-1)^n N(\bigcap_{i=1}^{n+1} H_i)$ note that the intersection of m of such hyperplanes is a vector space of co-dimension m by choice of H_i. Therefore $N(\bigcup_{i=1}^n H_i) = \sum_{i=1}^n N(n-1,q) - \sum_{1=i1<j}^n N(n-2,q) + \dots + (-1)^{n+1} N(0,q) = \sum_{i=1}^n (-1)^{i+1} \binom{n}{i} N(n-i,q)$. Therefore all the subspaces of a vector space not contained in such subspaces is $N(n,q) - |\{W \subseteq : \exists i : W \subseteq H_i\}| = \sum_{i=0}^n (-1)^i \binom{n}{i} N(n-i,q)$. □

Definition 6.8. Let $n \in \mathbf{Z}_{>1}, m_1, \dots, m_n \in \mathbf{Z}_{>1}$, where $m_i \neq 1$ for at least two $i \in \{1, \dots n\}$, and let q be a prime power in $\mathbf{N}$. Define $O_{q,n,m_1,m_2,\dots,m_n}$ as the subring of $F := \mathbf{F}_q[X]/(X)^{m_1} \times \mathbf{F}_q[X]/(X^{m_2}) \times \dots \times \mathbf{F}_q[X]/(X^{m_n})$ consisting of the elements $a \in F$ such that $\pi_1(a) = \pi_2(a) = \dots = \pi(a)$. Here $\pi_i : F \to \mathbf{F}_q$ is the map that takes the i-th coordinate, which can be written as $a_0 + a_1X^1 + \ldots + a_{m_i-1}X^{m_i-1}$, to $a_0 \in \mathbf{F}_q$.

Lemma 6.9. *The ring $O_{q,n,m_1,m_2,\ldots,m_n}$ is a non-principal ideal ring and has exactly*

$$1 + \sum_{S\subseteq\{1,\ldots,n\}} (\sum_{i=0}^{\#S}(-1)^i\binom{\#S}{i}N(\#S-i,q))\prod_{e\in S}(m_e-1)$$

ideals.

Proof. Fix $q, n, m_1, \ldots m_n$ and define $O = O_{q,n,m_1,m_2,\ldots,m_n}$. For $i \in \{1,\ldots,n\}$ define X_i to be the element which is zero on every coordinate but i where it is X. It is clear that $(X_1,\ldots,X_n) \subset O$ is the unique maximal ideal of O. Call it $\mathfrak{m}$.
For $i \in \{1,\ldots n\}$ define p_i to be the function from O to $\mathbf{Z}$ which sends the i-th coordinate of an element in O which can be written as $a_0+a_1X^1+\ldots+a_{m_i-1}X^{m_i-1}$ to the first interger $j \in \mathbf{Z}_{\geq 0}$ such that $a_j \neq 0$, if there is no such element (that is if $a_0 + a_1X^1 + \ldots + a_{m_i-1}X^{m_i-1} = 0$) we define the image to be m_i.
Let $I \subsetneq O$ be an ideal. Define $d_i := \min(p_i(I))$. Note that for any element $a \in O$ such that $p_i(a) = 0$ we get that $\pi_i(a)$ is non-zero. This means that $\pi_1(a) \neq 0, \pi_2(a) \neq 0, \ldots, \pi_n(a) \neq 0$. Therefore a must be a unit and so $(a) = O$. Hence we have $d_i \in \{1,\ldots m_i\}$.
For every $a \in I$ we have that $a \in (X_1^{d_1},\ldots,X_n^{d_n})$ as $a = \sum_i c_iX_i^{d_i}X_i^{p_i(a)-d_i}$ for $c_i \in \mathbf{F}_q[X]/(X)^{m_i}$ units, this is an element of $(X_1^{d_1},\ldots,X_n^{d_n})$ as $p_i(a) - d_i \geq 0$. Therefore we have $I \subseteq (X_1^{d_1},\ldots,X_n^{d_n})$. Note that for every $i \in \{1,\ldots,n\}$ we have an $a \in I$ such that $p_i(a) = d_i$ and so $a \cdot c_i^{-1}X_i = X_i^{d_i+1}$ where $c_i \in \mathbf{F}_q[X]/(X)^{m_i}$ is any unit such that $c_iX_i^{d_i}$ is the i-th coordinate of a. Hence we have

$$\mathfrak{m}(X_1^{d_1},\ldots,X_n^{d_n}) = (X_1^{d_1+1},\ldots,X_n^{d_n+1}) \subsetneq I \subseteq (X_1^{d_1},\ldots,X_n^{d_n}),$$

this gives us a map which sends an ideal $I \subsetneq O$ to a tuple d_i. Note that for such a sequence of d_i's and an ideal $(X_1^{d_1+1},\ldots,X_n^{d_n+1}) \subsetneq I \subseteq (X_1^{d_1},\ldots,X_n^{d_n})$ such that I is mapped to d_i we get that

$$I/(X_1^{d_1+1},\ldots,X_n^{d_n+1})$$

is not contained in any hyperspace of the form

$$(X_1^{d_1+1},X_2^{d_2},\ldots,X_n^{d_n})/(X_1^{d_1+1},\ldots,X_n^{d_n+1}),\ldots,$$
$$(X_1^{d_1},\ldots X_{n-1}^{d_{n-1}},X_n^{d_n+1})/(X_1^{d_1+1},\ldots,X_n^{d_n+1}),$$

(here we only count these spaces if they are in fact hyperspaces and not the whole vector space which can happen if for some $i \in \{1,\ldots,n\}$ we have $d_i = m_i$) moreover any subspace outside of all such hyperspaces corresponds to an ideal which gets mapped to this tuple d_i. This means that we can count the number of non-zero ideals $I \subsetneq O$ by counting all the subspaces of the vector spaces of the form $(X_1^{b_1},\ldots,X_n^{b_n})/\mathfrak{m}(X_1^{b_1},\ldots,X_n^{b_n})$ where $b_i \in \{1,\ldots m_i\}$, which are not contained in subspaces of the form

$$(X_1^{b_1+1},X_2^{b_2},\ldots,X_n^{b_n})/(X_1^{b_1+1},\ldots,X_n^{b_n+1}),\ldots,$$
$$(X_1^{b_1},\ldots X_{n-1}^{b_{n-1}},X_n^{b_n+1})/(X_1^{b_1+1},\ldots,X_n^{b_n+1}).$$

The dimension of a vector space of this form over the residue field $\mathbf{F}_q$ is equal to the number of b_i such that $b_i \neq m_i$.
For $S \subset \{1,\ldots n\}$ the number of such vector spaces for which $b_i \neq m_i$ for all $i \in S$

is $\prod_{e\in S}(m_e-1)$ by 6.7, the requirements for 6.7 are clearly met, the number of subspaces we have to count for all such vector spaces is $\sum_{i=0}^{n}(-1)^i\binom{n}{i}N(n-i,q)$. This means that there are

$$\sum_{S\subseteq\{1,\dots,n\}}(\sum_{i=0}^{\#S}(-1)^i\binom{\#S}{i}N(\#S-i,q))\prod_{e\in S}(m_e-1).$$

in $\mathfrak{m}$ so there are

$$1+\sum_{S\subseteq\{1,\dots,n\}}(\sum_{i=0}^{\#S}(-1)^i\binom{\#S}{i}N(\#S-i,q))\prod_{e\in S}(m_e-1)$$

ideals in total.

□

Proof of theorem 1.2. The case $n<5$ follows from the fact that the lowerbound exceeds the upperbound for this n which means it is impossible to make such a ring.

We have come to this interval for local non-principal ideal rings by simply letting a computer grind the possibilities we have gotten from our three families of rings. Because of the time required to run the program only numbers up to a 1200 were checked. Furthermore we couldn't actually calculate all the possiblilities because that would take too long. □

References

[1] Atiyah, M. F., and Macdonald, I. G. *Introduction to commutative algebra.* Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.