20MAB143 Rings and Polynomials: Week 11

The material in this document is non-examinable.

1 Euclidean domains and PIDs

This week's lectures will look at various classes of rings with good properties, giving a broader perspective on the examples we have studied throughout the module.

Early in the module we mentioned that the ring of integers $\mathbf{Z}$ and polynomials rings $K[x]$ share many good properties. In this section we will give a conceptual explanation for this: both rings are members of the class of **Euclidean domains**. Here's the definition.

Definition 1.1. *Let* R *be an integral domain. A function*

$$\nu\colon R \setminus \{0\} \to \mathbf{Z}_{\geq 0}$$

is called a **Euclidean valuation** *on* R *if for every element* $a \in R$ *and every nonzero element* $b \in R$ *there exists elements* $q, r \in R$ *such that*

$$a = qb + r$$

and either $r = 0$ *or* $\nu(r) < \nu(b)$*. An integral domain* R *is called a* **Euclidean domain** *if there exists at least one Euclidean valuation on* R*.*

Examples: We have already come across several examples of Euclidean domains.

1. The ring of integers $\mathbf{Z}$ is a Euclidean domain. Here the Euclidean valuation function ν is defined by $\nu(n) = |n|$. The properties of division with remainders in $\mathbf{Z}$ show that this is a Euclidean valuation.

2. The ring of polynomials $K[x]$ is a Euclidean domain, for any field K. Here the Euclidean function ν is defined by $\nu(p) = \deg(p)$ for a polynomial $p \in K[x]$. The Division Theorem (Week 2 Theorem 1.3) shows that this function is a Euclidean valuation.

3. The ring of Gaussian integers $\mathbf{Z}[i]$ is a Euclidean domain. Here the Euclidean valulation ν is defined as follows: for a Gaussian integer $m + ni$, we define

$$\nu(m + ni) = m^2 + n^2$$

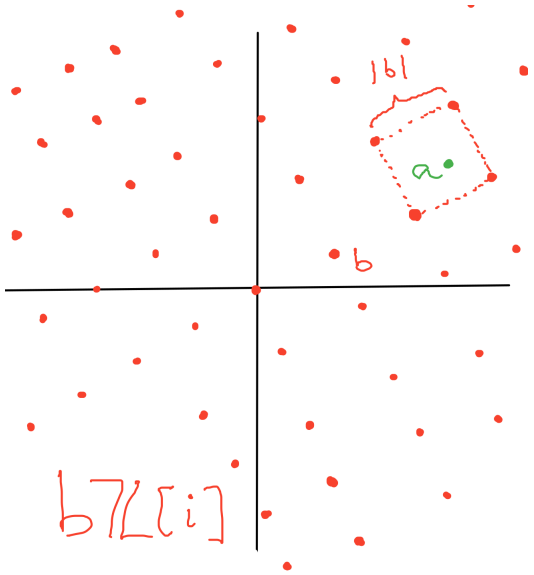

Figure 1: Division in $\mathbf{Z}[i]$

To prove this is a Euclidean valuation requires a bit of work. The idea is as follows: if a and b are Gaussian integers with $b \neq 0$, consider the set

$$b\mathbf{Z}[i] = \{bm + bni \mid m, n \in \mathbf{Z}\}$$

consisting of all multiples of b. This is a rectangular lattice that divides the complex plane $\mathbf{C}$ into "boxes" with sides of length $|b| = \sqrt{\nu(b)}$. Now the number a must sit in one of these "boxes", and hence is at a distance at most $\frac{|b|}{\sqrt{2}}$ from one of the corners. Each corner is a multiple of b, so is of the form qb for some $q \in \mathbf{Z}[i]$. So choosing the corner qb that is closest to a we get

$$\begin{aligned} \nu(a - qb) &\leq \left(\frac{|b|}{\sqrt{2}}\right)^2 \\ &= \frac{\nu(b)}{2} \end{aligned}$$

So choosing q as above and setting $r = a - qb$ we get

$$a = qb + r$$

where either $r = 0$ or $\nu(r) \leq \frac{\nu(b)}{2}$. We can illustrate this process with a picture as in Figure 1.

In Week 3 we showed how to compute the greatest common divisor of two polynomials in $K[x]$ using the Euclidean algorithm. The key point in showing that this algorithm works is that,

at each step, the degree of the remainder term decreases. If now R is any Euclidean domain, we can do the same process of repeated division, and by Definition 1.1 we know that at each step the value of the Euclidean valulation ν will decrease. So the algorithm will work in exacltly the same way, and we have:

Theorem 1.2. *Let* R *be a Euclidean domain and let* r, s *be two elements of* R. *Then we can compute* $\gcd(r, s)$ *by running the Euclidean algorithm.*

Example: Let us give an example to illustrate how the Euclidean algorithm works in the Gaussian integers $\mathbf{Z}[i]$. So let

$$a = 10,\ b = 6 + 3i.$$

Let's use the Euclidean algorithm to calculate $\gcd(a, b)$.

The first step is to divide a by b. As described above, to find the quotient q we need to find the multiple qb which is closest to a. With a little searching we find

$$10 = (6 + 3i)(1 - i) + (1 + 3i)$$

so here $r = 1 + 3i$. Note that $\nu(b) = 6^2 + 3^2 = 49$, while $\nu(r) = 1^2 + 3^2 = 10 \leq \frac{1}{2}\nu(b)$ as needed.

The second step is to divide b by r. Doing this we get

$$6 + 3i = (1 + 3i)(1 - i) + (2 + i)$$

so putting $r_2 = 2 + i$, again we have $\nu(r_2) = 5 \leq \frac{1}{2}\nu(r)$.

Finally we divide r by r_2 to get

$$1 + 3i = (2 + i)(1 + i)$$

with remainder 0.

To find the gcd we look at the last nonzero remainder: we get

$$\gcd(a, b) = 2 + i.$$

Note one difference between this case and the case of polynomials: in $\mathbf{Z}[i]$ there is no such thing as a "monic" element. In fact the gcd is not uniquely defined in $\mathbf{Z}[i]$; we could multiply the above result by any unit in $\mathbf{Z}[i]$, namely any of $\pm 1, \pm i$, and the answer would be equally valid.

1.1 Principal Ideal Domains

There is a broader class of rings that include Euclidean domains, but whose definition is purely in terms of ideals:

Definition 1.3. *An integral domain* R *is called a* **principal ideal domain** *or PID if every ideal* $I \subseteq R$ *is generated by a single element: that is, for every ideal* I *there exists an element* $r \in R$ *such that*

$$I = \langle r \rangle = \{rs \mid s \in R\}.$$

Theorem 1.4. *Every Euclidean domain is a PID.*

Sketch of proof. The proof is a direct generalisation of that of Week 2 Theorem 2.5, where we proved that $K[x]$ is a PID.

So let R be a Euclidean domain with Euclidean valuation ν, and let I be an ideal in R. Among the nonzero elements of I, choose an element a for which $\nu(a)$ is minimal. Then I claim that $I = \langle a \rangle$.

To see this, let b be any element of I. We need to show that $b \in \langle a \rangle$; in other words, $a \mid b$. Since R is a Euclidean domain we can write

$$b = qa + r$$

where $\nu(r) < \nu(a)$. Now since $r = s - qa$ we see that $r \in I$. Since a has minimal valuation among nonzero elements, we conclude that $r = 0$, and therefore $a \mid b$ as required. □

All the examples of PIDs that we have seen in this module are in fact Euclidean domains. There are examples of PIDs which are not Euclidean domains, but they are not so easy to come up with. If you are curious, you can consult [W] for an example.

2 Unique Factorisation Domains

In Week 10 Lemma 1.1 we used a certain property of irreducible polynomials: if f is irreducible and $f \mid gh$ then $f \mid g$ or $f \mid h$. To justify this, we introduce the following important class of rings.

Definition 2.1. *An integral domain* R *is called a* **unique factorisation domain** *or UFD if every element* $r \in R$ *which is not zero and not a unit can be factorised as*

$$r = p_1 \cdots p_n$$

where each p_i *is irreducible in* R*, and moreover this factorisation is unique in the sense that if also*

$$r = q_1 \cdots q_m$$

for irreducible elements $q_i \in R$*, then* $m = n$ *and for each* i *there exists a* j *such that* $p_i = uq_j$ *for some unit* $u \in R$*.*

Example: The ring of integers $\mathbf{Z}$ is a UFD. To see this, note that the irreducible elements in $\mathbf{Z}$ are exactly the prime numbers and their negatives. The so-called **Fundamental Theorem of Arithmetic** says that any integer m can be factored uniquely as

$$m = p_1^{k_1} \cdots p_n^{k_n}$$

for some primes p_i and powers k_i, and this is exactly the condition in Definition 2.1 above.

One way to get more examples of UFDs is the following:

Theorem 2.2. *Every PID is a UFD.*

So for example the Gaussian integers $\mathbf{Z}[i]$ and polynomial rings $K[x]$ in one variable are UFDs.

Sketch of proof. Let R be a PID. We need to show first that every element of R can be factorised into irreducible elements, and secondly that factorisations are unique.

For the first point, let $r \in R$. If r is irreducible, we are done. If not, it can be factored as $r = r_1 r_2$ where neither r_1 nor r_2 is a unit. If both are irreducible, we are done; if not keep going. The issue is to show that this process terminates, in other words we get a factorisation into irreducibles after finitely many steps. If not, then at each step we have a factorisation

$$r = r_1 \cdots r_n$$

in which at least one factor r_k cannot be factored into irreducibles. So we get an infinite chain of elements r_k such that $r_{k+1} \mid r_k$ for each k. If we let $I_k = \langle r_k \rangle$, this gives an infinite chain of ideals $I_1 \subsetneq \cdots \subsetneq I_k \subsetneq \cdots$ in which each ideal is strictly larger than the preceding ones. On the other hand, one can show that the union $I = \cup_k I_k$ is an ideal. Since R is a PID, I must be generated by a single element c; since $c \in I$ there exists an N such that $c \in I_N$, therefore $I = \langle c \rangle \subseteq I_N$, which shows that $I_N = I$ and therefore $I_k = I_N$ for all $k \geq N$. This is a contradiction, showing that every element in R has a factorisation into irreducibles.

We omit the proof of the uniqeness part. □

Examples: Here are two examples of rings which are **not** UFDs,

1. The ring

$$\mathbf{Z}[\sqrt{-5}] = \left\{ a + b\sqrt{-5} \mid a,\, b \in \mathbf{Z} \right\}$$

is not a UFD: in this ring we can factor the element 6 in two different ways as

$$\begin{aligned} 6 &= 2 \cdot 3 \\ &= (1 + \sqrt{-5})(1 - \sqrt{-5}) \end{aligned}$$

One can show that each of 2, 3, $1 \pm \sqrt{-5}$ is an irreducble element in $\mathbf{Z}[\sqrt{-5}]$, but there is no unit u such that $2 = u \cdot (1 \pm \sqrt{-5})$. So we do not have uniqueness of factorisation into irreducibles in this ring.

2. The quotient ring

$$R = \frac{\mathbf{C}[x, y, z, w]}{I}$$

where I is the ideal $I = \langle xy - zw \rangle$ is not a UFD. To see this, notice that in R we have

$$\begin{aligned}(I + x)(I + y) &= I + xy \\ &= I + zw \\ &= (I + z)(I + w)\end{aligned}$$

Again one can show that the factors in these two factorisations do not differ by a unit, so again unique factorisation fails. Examples of this kind are closely connected to te study of higher-dimensional singularities in algebraic geometry.

The most important result about the class of UFDs in the following; for us it is important because of its consequence for factorisation of polynomials.

Theorem 2.3. *If R is a UFD, then the polynomial ring $R[x]$ is a UFD.*

We will not say much about the proof. The basic idea is to consider the so-called **field of fractions** of the ring R: this is a field K whose elements are fractions $\frac{r}{s}$ where r and s are elements of R and s is nonzero, and where addition and multiplication work in the usual way for fractions. Since K is a field we know that $K[x]$ is a PID, in particular a UFD, and then the key point is to relate factorisations in $K[x]$ to factorisations in $R[x]$ using a generalisation of the Gauss Lemma (which is the case where $R = \mathbf{Z}$ and $K = \mathbf{Q}$).

Corollary 2.4. *For any field K and any positive integer n, the polynomial ring $K[x_1, \ldots, x_n]$ is a UFD.*

Proof. A field K is a PID, since the only ideals in K are $\{0\}$ and K, generated by the elements 0 and 1 respectively. By Theorem 2.2 this implies K is a UFD. Using Theorem 2.3, we then see by induction that $K[x_1, \ldots, x_n]$ is a UFD for any positive integer n. □

Finally returning to Week 10 Lemma 1.1, let $f \in K[x_1, \ldots, x_n]$ be an irreducible polynomial and suppose $f \mid gh$. So there exists a polynomial p such that $fp = gh$. Since $K[x_1, \ldots, x_n]$ is a UFD, we can write both sides out as products of irreducible polynomials, and the irreducible factors on both sides must be the same up to multiplication by a unit. Snce f appears among the irreducible factors on the left-hand side, it must appear on the right-hand side too. So either g or h must have f among its irreducible factors, meaning that $f \mid g$ or $f \mid h$.

3 Noetherian rings

In this final section we introduce another class of rings called **Noetherian** rings. This class contains all polynomial rings over fields, as well as their quotients, while retaining good general properties. This flexibility makes it perhaps the most important and useful class of rings in modern algebra and algebraic geometry.

Definition 3.1. *A commutative ring* R *is called* **Noetherian** *if every ideal in* R *is finitely generated: that is, for every ideal* $I \subset R$ *there exist elements* $r_1, \ldots, r_n$ *such that*

$$\begin{aligned} I &= \langle r_1, \ldots, r_n \rangle \\ &= \{r_1 s_1 + \cdots + r_n s_n \mid s_1, \ldots, s_n \in R\}. \end{aligned}$$

There is an alternative characterisation of Noetherian rings that is often very useful in practice. It is based on the following definition:

Definition 3.2. *Let* R *be a commutative ring. We say that* R *has the* **ascending chain condition** *(ACC) if and only if every ascending chain of ideals*

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

stabilises, that is, there exists an N *such that* $I_n = I_N$ *for all* $n \geq N$.

With this notion we can now prove the alternive characterisation of Noetherian rings:

Proposition 3.3 (Ascending Chain Condition)**.** *A commutative ring* R *is Noetherian if and only it satisfies the ACC.*

Proof. First let R be Noetherian, and let $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ be an ascending chaing of ideals. Then one can check that the union $I = \cup_n I_n$ is an ideal. Since R is Noetherian, the ideal I is finitely generated: say $I = \langle r_1, \ldots, r_n \rangle$ for some elements $r_i \in R$. Each of the r_i belongs to one of the ideals in the chain, and since there are finitely many of them, we can choose a single ideal I_N containing all of the r_i. Then

$$I = \langle r_1, \ldots, r_n \rangle \subseteq I_N \subseteq I$$

which proves that $I_N = I$. Since $I_N \subseteq I_n \subseteq I$ for all $n \geq N$, this also shows $I_n = I_N$ for all $n \geq N$.

Conversely suppose that R satisfies the ACC, and let $I \subseteq R$ be an ideal. Suppose for contradiction that I is not finitely generated Let $I_0 = \{0\}$ and for each n, let $I_n = I_{n-1} + \langle r_n \rangle$ where r_n is any element in $I \setminus I_{n-1}$. (Since I is not finitely generated but each I_n is, we can always pick such an r_n.) Then $I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots$, so we get an infinite ascending chain of ideals in R which does not stabilise, contradicting the ACC. □

Examples: Every PID is Noetherian, since in a PID every ideal is generated by a **single** element, so Definition 3.1 is certainly satisfied. After Theorem 3.5 we will have lots more examples.

For an example of a non-Noetherian ring, consider $C[0,1]$, the ring of continuous functions on the unit interval. Define

$$I_n = \left\{ f \in C[0,1] \mid f(x) = 0 \ \forall\, x \in \left[0, \frac{1}{n}\right] \right\}.$$

Then one can check that I_n is an ideal for every n, and that $I_n \subsetneq I_{n+1}$ for every n. So $I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots$ is an ascending chain of ideals in $C[0,1]$ which does not stabilise. By Proposition 3.3 this shows $C[0,1]$ is not Noetherian.

Now we start to prove the important properties of the class of Noetherian rings.

Proposition 3.4. *Let R be a Noetherian ring. Then for any ideal $I \subseteq R$, the quotient ring R/I is Noetherian.*

Sketch of proof. Let $J \subseteq R/I$ be an ideal. We need to prove that J is finitely generated.

Consider the quotient map $q : R \to R/I$. Then one can prove that the set

$$q^{-1}(J) = \{r \in R \mid q(r) \in J\}$$

is an ideal in R. Since R is Noetherian, the ideal $q^{-1}(J)$ is finitely generated, say $q^{-1}(J) = \langle r_1, \ldots, r_n \rangle$.

Now let $I + r$ be any element of the ideal J. Then $r \in q^{-1}(J)$, so there exist elements $s_1, \ldots, s_n \in R$ such that

$$r = s_1 r_1 + \cdots + s_n r_n.$$

Applying q to both sides, we get

$$\begin{aligned} I + r = q(r) &= q(s_1)q(r_1) + \cdots + q(s_n)q(r_n) \\ &= (I + s_1)(I + r_1) + \cdots (I + s_n)(I + r_n) \end{aligned}$$

This shows that $J = \langle I + r_1, \ldots, I + r_n \rangle$ as required. □

Next comes perhaps the key theorem about the class of Noetherian rings. Hilbert's proof of this theorem in 1890 was a landmark in the development of modern mathematics; in contrast to the established "constructive" method of proof at the time, Hilbert gave a "non-constructive" proof, proving that that a set of generating elements for an ideal exists without actually producing one.

Theorem 3.5 (Hilbert basis theorem)**.** *If R is a Noetherian ring, then $R[x]$ is a Noetherian ring.*

Proof. Let $I \subseteq R[x]$ be an ideal. We have to prove that I is finitely generated. Suppose for the sake of contradiction that it is not. Let $f_0 \in I$ be any element, and for $n \geq 1$ let f_n be an element of smallest degree in $I \setminus \langle f_0, \ldots, f_{n-1} \rangle$. (We can choose such f_n because we are assuming I is not finitely generated.) Write I_n to denote the ideal $\langle f_0, \ldots, f_n \rangle$.

Now let $a_n \in R$ be the leading coefficient of f_n, and define a sequence of ideals $(J_n)_n$ of R by

$$J_n = \langle a_0, \ldots, a_n \rangle .$$

This is an ascending chain of ideals in the Noetherian ring R, so by Proposition 3.3 it stabilises: for some N we have $\cup_n J_n = J_N$. This implies that $a_{N+1} \in J_N$ and so

$$a_{N+1} = \sum_{i \leq N} r_i a_i$$

for some elements $r_i \in R$.

Now let d_i denote the degree of f_i and consider the polynomial

$$f = \sum_{i \leq N} r_i x^{(d_{N+1} - d_i)} f_i$$

This is an element of I_N with degree d_{N+1} and its leading term is $\sum_{i \leq N} r_i a_i = a_{N+1}$, the same as the leading term of f_{N+1}. Therefore the difference $f - f_{N+1}$ is a polynomial of degree strictly less than d_{N+1}. However, since $f \in I_N$ but $f_{N+1} \notin I_N$, we must have that $f - f_{N+1} \notin I_N$. Therefore we have found an element of $I \setminus I_N$ of degree strictly less than that of f_{N+1}. This contradicts our choice of f_{N+1} as an element of minimal degree in $I \setminus I_{N+1}$.

□

Corollary 3.6. *For any field* K *and any positive integer* n*, the polynomial ring* $K[x_1, \ldots, x_n]$ *is Noetherian. Moreover, if* I *is any ideal in the ring* $K[x_1, \ldots, x_n]$*, then the quotient ring* $K[x_1, \ldots, x_n]/I$ *is also Noetherian.*

Proof. Any field K is Noetherian since its only ideals are $\{0\}$ and K. The first statement then follows by induction, using Theorem 3.5.

The second statement then follows from Proposition 3.4. □

Remark: Rings of the form $K[x_1, \ldots, x_n]/I$ are of central importance in algebraic geometry. The basic idea is that if I is a "good" ideal defining an algebraic set $V(I)$, then $R = K[x]/I$ is the ring of "polynomial functions" on the set $V(I)$. The geometry of $V(I)$ can then be studied by means of the ring R. For example, the Noetherian property of R can be used to prove that any decreasing chain $V_0 \supseteq V_1 \supseteq \cdots$ of algebraic subsets of $V(I)$ stabilises after finitely many steps: there is some N such that $V_n = V_N$ for all $n \geq N$. This kind of finiteness property is a key element of algebraic geometry that distinguishes it from other kinds of geometry.

4 Conclusion

We have introduced various classes of rings and explained some of the relations between them. Let us repeat some of what we know and mention some more relations here:

- Every Euclidean domain is a PID.
- Every PID is a UFD.
- Every PID is Noetherian.
- Not every Noetherian ring is an integral domain, hence not every Noetherian ring is a UFD. Here are a couple of examples to show this:
  (a) Any ring with finitely many elements is Noetherian, because it has only finitely many ideals. So for example $\mathbf{Z}_6$ is Noetherian, but it is not an integral domain.

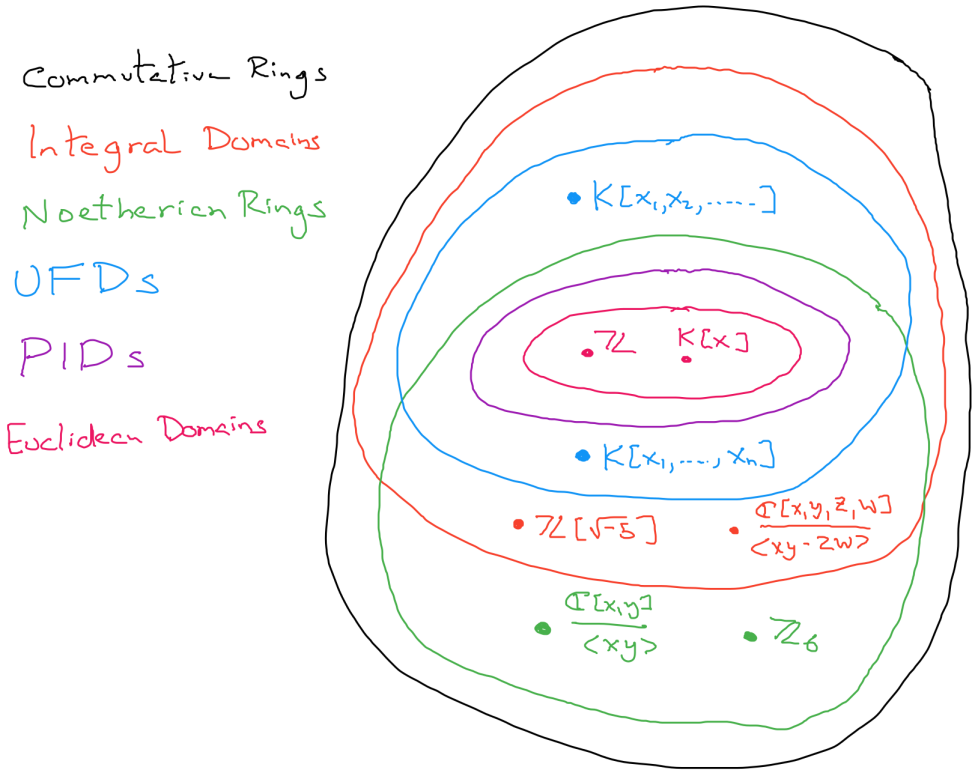

Figure 2: Relations between different types of rings in this module

(b) The quotient ring $\mathbf{C}[x, y]/\langle xy\rangle$ is Noetherian by Corollary 3.6, but the ideal $\langle xy\rangle$ is not prime, so by Week 9 Theorem2.5 this ring is not an integral domain.

- Even among integral domains, there are examples of Noetherian rings which are not UFDs. Both examples of non-UFDs from Section 2 are Noetherian integral domains.
- Not every UFD is Noetherian. One example is the ring $K[x_1, x_2, x_3, \ldots]$ of polynomials over a field K with infinitely many variables. (This is the only time we will mention this ring in this module!) To see it is not Noetherian, just observe that there is an infinite strictly ascending chain of ideals

$$\langle x_1\rangle \subsetneq \langle x_1, x_2\rangle \subsetneq \langle x_1, x_2, x_3\rangle \subsetneq \cdots$$

So this ring does not satisfy the ACC, and hence is not Noetherian.

Figure 2 is an attempt to depict the relationships between the various classes of rings we have seen in the module.

References

[W] Wikipedia contributors, Principal ideal domain. Wikipedia, The Free Encyclopedia, https://en.wikipedia.org/w/index.php?title=Principal_ideal_domain&oldid=992377154 (accessed December 10, 2020).