On Techniques to determine when Quotients of Polynomial Rings Are UFDs

Agaman Banerjee • 5 Jul 2026

One of the most natural questions one can ask about a quotient of a polynomial ring is whether it is a **Unique Factorization Domain (UFD)**. While there is no universal method for answering this question, there are a number of beautiful techniques from commutative algebra and algebraic geometry that often make the problem surprisingly manageable.

We begin with some elementary techniques and standard results from ring theory and commutative algebra that are frequently useful for deciding whether a ring is (or is not) a UFD. Some of the basic facts we shall repeatedly use are:

- **A(i)** A UFD is a normal domain.
- **A(ii)** A Noetherian integral domain is a UFD if and only if every height one prime ideal is principal.
- **A(iii)** In a UFD, irreducible elements are the same as prime elements.

In practice, these results are often more useful for proving that a ring is **not** a UFD. Combined with various techniques for establishing irreducibility—which is typically much subtler than checking primeness—such as the use of **norm maps**, they become extremely effective tools for proving non-UFDness. We shall illustrate these ideas through a number of examples.

There are, however, several powerful methods for proving that a ring *is* a UFD as well. Some of the fundamental results that we shall use are:

- **B(i)** Every Euclidean domain is a PID, and every PID is a UFD.
- **B(ii)** Localizations of UFDs are again UFDs.
- **B(iii)** Nagata's Criterion.

As the article progresses, we shall develop more sophisticated techniques, drawing on ideas from commutative algebra and algebraic geometry, to prove that certain quotients of polynomial rings are UFDs—A theorem that will be of interest to us is the following: if k is a field, $C \subset \mathbb{P}^2_k$ is a nonsingular conic, and U is an affine patch of C, then the absence of k-rational points on C implies that the coordinate ring $\mathcal{O}_C(U)$ is a UFD. This is extremely helpful for

determining when such rings are UFDs—particularly over $\mathbb{Q}$ and, more generally, over number fields. Rather than assuming such results, we shall develop the necessary theory as we proceed. In fact, one of the pleasant surprises is that **B(iii)** Nagata's Criterion will emerge naturally as a corollary of the results we prove.

With the exception of Nagata's Criterion, we shall not prove the bulleted results above. They are standard facts that can be found in almost any textbook on commutative algebra. Our focus will instead be on how these results can be applied effectively, and on developing the additional machinery needed to prove less obvious and more interesting examples of unique factorization.

EXAMPLE 1

In this example we shall prove that the following ring is not a UFD. The proof is a simple application of **A(i)**

$$\frac{\mathbb{R}[x,y]}{(y^2-x^3)}$$

Proof. Showing y^2-x^3 is irreducible in $\mathbb{R}[x,y]$ is pretty easy and hence it is prime by **A(iii)** since $\mathbb{R}[x,y]$ is a UFD, thus the ring (call it A) is an integral domain. We show that a certain element in the quotient field of A that is not in A is integral over A.

Let K be the quotient field of A, consider the monic equation $T^2-X \in A[X]$, then $\frac{y}{x}$ clearly satisfies this monic equation since $y^2-x^3=0$. It remains to show that $\frac{y}{x} \notin A$, so suppose it did, then $\frac{y}{x}=f$ for some $f \in A$, thus $y-fx=0$ in A, which implies $y-fx \in (y^2-x^3)$ which is clearly not possible since $y-fx$ has degree 1 in y, and thus $\frac{y}{x} \notin A$ and is integral over A, thus from **A(i)** we conclude that A is not a UFD! ■

EXAMPLE 2

In this example, we shall prove that the following ring is not a UFD. The proof is an application of **A(iii)** and demonstrates the usefulness of **norm maps** as a tool for proving the irreducibility of elements.

$$\frac{\mathbb{R}[x,y]}{(x^2+y^2-1)}$$

Proof. First we will check that the element $1-y$ is *not* a prime element in this ring (call it A). To show this we quotient A out by $(1-y)$ and check that it's not an integral domain.

$$\frac{\mathbb{R}[x,y]}{(x^2+y^2-1,1-y)} \cong \frac{\mathbb{R}[x,y]}{(x^2,y-1)} \cong \frac{\mathbb{R}[x]}{x^2}$$

which clearly has nonzero nilpotent x in it, hence is not an integral domain, thus $1-y$ is not prime in A.

Now we claim that $1-y$ is irreducible in A, it's not immediately clear to see why it must be irreducible since there are relations in A, one way to do is to pull it back to $\mathbb{R}[x,y]$ and do the computation there but it's ugly, we will instead use the ingenious norm argument.

Firstly observe that any element in A has a unique representative of the form $A(y)+B(y)x$ where $A(y), B(y) \in \mathbb{R}[y]$ (this is fairly easy to see). Now we define the following map.

$$N : A \to \mathbb{R}[y], \qquad A(y)+B(y)x \longmapsto A(y)^2 - B(y)^2(1-y^2).$$

The great thing about this map is that it is multiplicative, that is $N(fg) = N(f)N(g)$.

Reason (click on it)
Since all elements in A have a unique representative of the form $A(y)+B(y)x$ and none of them are the same in A, we can view A as a free $\mathbb{R}[y]$-module of rank 2 with basis $\{1,x\}$. Now consider the following map

$$N : A \to \mathbb{R}[y]$$

given by

$$z \longmapsto \det(\lambda_z),$$

where $\lambda_z : A \to A$ is an $\mathbb{R}[y]$-module homomorphism which takes $x \mapsto xz$. Now since determinant is multiplicative, we get that N is a multiplicative map.

Now why is it relevant in our case? You see that the map N defined above is the same as the one that we have defined. To see this, abbreviate $A(y), B(y)$ as a, b respectively. Then the matrix defined by $a+bx$ is

$$\begin{pmatrix} a & b(1-y^2) \\ b & a \end{pmatrix}$$

and the determinant is exactly what we have defined above, hence the above defined map is indeed multiplicative.

From this we immediately see that if $f \in A$ is a unit then $N(f)$ is a unit in $\mathbb{R}[y]$ and hence $N(f) \in \mathbb{R}^\times$. From this we can characterize all the units of A, so

$$A(y) + B(y)x \text{ is a unit in } A \iff A(y)^2 - B(y)^2(1-y^2) \text{ is constant.}$$

From this characterization and the fact that $A(y), B(y) \in \mathbb{R}[y]$ it's easy to see that $A(y)$ is a constant and $B(y) = 0$.

Remark (click on it)
Over $\mathbb{C}$ this conclusion would not hold! So be careful with the conclusions, here it holds simply because after squaring, all the coefficients are nonnegative and as a result the leading terms don't cancel off.

So the units in A are precisely $\mathbb{R}^\times$. Now suppose

$$1 - y = fg,$$

where f, g are non-units in A, then via the multiplicative property of norm we get

$$N(1-y) = N(f)N(g) = 1 - y^2,$$

but since f, g are non-units, $N(f)$ and $N(g)$ both have at least degree 2, thus we arrive at a contradiction! So $1 - y$ is irreducible.

We get $1 - y$ is irreducible but not prime in A, thus from **A(iii)** we conclude that

$$\frac{\mathbb{R}[x,y]}{(x^2+y^2-1)}$$

is not a UFD! ■

EXAMPLE 3

In this example we shall prove that the following ring is a UFD.

$$\frac{\mathbb{C}[x,y]}{(x^2+y^2-1)}$$

Proof. Notice that since $x^2 + y^2 = 1$ in this ring, it motivates us to think of x, y as the coordinates of the unit circle. Call the ring A. We define the map

$$\phi : A \longrightarrow \mathbb{C}[z, z^{-1}]$$

by sending

$$x \longmapsto \frac{z + z^{-1}}{2}, \qquad y \longmapsto \frac{z - z^{-1}}{2i}.$$

Notice first of all that the map is well defined since

$$\phi(x^2 + y^2 - 1) = 0,$$

then clearly the map is surjective as

$$\phi(x + iy) = z.$$

Construct the inverse

$$\psi : \mathbb{C}[z, z^{-1}] \longrightarrow A$$

by

$$z \longmapsto x + iy.$$

It's easy to verify that $\phi \circ \psi$ is the identity. Thus we get that

$$A \cong \mathbb{C}[z, z^{-1}].$$

Now we already know that $\mathbb{C}[z]$ is a UFD, and from **B(ii)** we get that $\mathbb{C}[z, z^{-1}]$ is a UFD, thus A is a UFD!

Remark. For those who already know some basic algebraic geometry, the assertion that

$$\frac{\mathbb{C}[x, y]}{(x^2 + y^2 - 1)} \cong \mathbb{C}[x, x^{-1}] \cong \frac{\mathbb{C}[x, y]}{(xy - 1)}$$

should almost be immediate since over $\mathbb{C}$, the two conics given by $x^2 + y^2 - 1$ and $xy - 1$ are affinely equivalent, i.e., they are isomorphic as affine varieties, and hence their coordinate rings are isomorphic.

EXAMPLE 4

In this example we shall prove that the following ring is a UFD. The proof is computational and we will use Nagata's Criterion **B(iii)** along with some other commutative algebraic results. In fact this ring is a PID but not an ED. The ring we consider is the following

$$\frac{\mathbb{R}[x,y]}{(x^2+y^2+1)}$$

Proof. We shall characterize all the prime ideals in this ring (call it A). First we observe that $(ax+by+c)$ where $(a,b) \neq (0,0)$ is a prime ideal in A. To see this we do some computation. Assume WLOG $b \neq 0$. Then in the ring

$$\frac{\mathbb{R}[x,y]}{(x^2+y^2+1, ax+by+c)}$$

we have

$$y = -\frac{ax+c}{b},$$

thus

$$x^2+y^2+1 = 0 \Longrightarrow (a^2+b^2)x^2 + 2acx + (b^2+c^2) = 0,$$

and the discriminant of this quadratic equation is < 0. Hence we see that

$$\frac{\mathbb{R}[x,y]}{(x^2+y^2+1, ax+by+c)} \cong \mathbb{C}.$$

Thus we see that $(ax+by+c)$ are prime ideals, even maximal.

Now in the next half of the proof we use certain results from commutative algebra. First observe that

$$\operatorname{Dim}_{\text{Krull}} A = \operatorname{Dim}_{\text{Krull}} \mathbb{R}[x,y] - \operatorname{ht}(x^2+y^2+1) = 2-1 = 1.$$

So A is a one-dimensional integral domain, thus every nonzero prime ideal P is maximal, and therefore A/P is a field. Now let

$$A/P = \mathbb{R}[x', y'],$$

where x', y' are the residue classes of x, y in A/P, respectively. Then A/P is a finitely generated $\mathbb{R}$-algebra which is also a field. Now we use the following result from commutative algebra.

> **Zariski's Lemma.** If L is a finitely generated k-algebra such that L is also a field, then L/k is a finite field extension.

So the above lemma tells us that since A/P is a field which is a finitely generated $\mathbb{R}$-algebra, then $A/P = \mathbb{R}[x', y']$ is a finite field extension of $\mathbb{R}$, and thus

$$[A/P : \mathbb{R}] \leq 2.$$

In particular we observe that $\{1, x', y'\}$ is linearly dependent over $\mathbb{R}$, which implies

$$ax + by + c \in P$$

for some $(a, b) \neq (0, 0)$. Thus

$$(ax + by + c) \subset P,$$

and we proved earlier that $(ax + by + c)$ is a prime ideal. Since P has height 1, we immediately get

$$P = (ax + by + c).$$

From this we can immediately conclude that A is a PID, hence a UFD by **B(i)**, from this result.

But we take a different path and prove that A is a UFD via Nagata's Criterion.

Let $S \subset A$ be the multiplicative set generated by all prime elements $ax + by + c$ with $(a, b) \neq (0, 0)$. The localization $S^{-1}A$ has no nonzero prime ideals, and therefore $S^{-1}A$ is a field, hence a UFD. Now Nagata's Criterion tells us that A is a UFD. ■

> **Remark.** In this example, we have seen that the fact that $\mathbb{R}$ has only one nontrivial finite algebraic extension, namely $\mathbb{C}$, plays a crucial role in the proof. If the base field is replaced by $\mathbb{Q}$, or more generally by a number field, the situation changes dramatically: these fields admit infinitely many finite algebraic extensions, and consequently none of the arguments above carry over directly. Later in this article, we shall study quotients of polynomial rings over $\mathbb{Q}$ and number fields, and develop criteria that determine when such rings are UFDs and when they are not.

EXAMPLE 5

In this example we prove that the following ring is a UFD using Nagata's Criterion **B(iii)** and a very useful dimension argument technique. We show that the following ring is a UFD.

$$\frac{\mathbb{R}[x,y,z]}{(x^2+y^2+z^2-1)}$$

Proof. Checking that $x^2+y^2+z^2-1$ is irreducible, and hence prime by **A(iii)** since $\mathbb{R}[x,y,z]$ is a UFD, is pretty easy. Thus the ring (call it A) is an integral domain. We check that $z-1$ is a prime element in A. To do this we quotient out by $(z-1)$ and see that the resulting ring is an integral domain.

$$\frac{\mathbb{R}[x,y,z]}{(x^2+y^2+z^2-1,z-1)} \cong \frac{\mathbb{R}[x,y,z]}{(x^2+y^2,z-1)} \cong \frac{\mathbb{R}[x,y]}{(x^2+y^2)}.$$

Now it's easy to check that x^2+y^2 is irreducible in $\mathbb{R}[x,y]$ and hence prime by **A(iii)** since $\mathbb{R}[x,y]$ is a UFD. Therefore the resulting quotient is an integral domain, and we conclude that $z-1$ is prime in A.

Now to use Nagata's Criterion we localize at $z-1$. Let

$$t := \frac{1}{z-1},$$

so that

$$z = 1 + \frac{1}{t}.$$

Then in A we have

$$x^2+y^2+z^2-1=0 \Longrightarrow (tx)^2+(ty)^2 = -2t-1. \qquad (\star)$$

We now claim that

$$A[t] = \mathbb{R}\left[tx, ty, \frac{1}{t}\right].$$

Indeed,

$$A[t] \subset \mathbb{R}\left[tx, ty, \frac{1}{t}\right]$$

since clearly x,y,z,t all belong to the right-hand side using $(\star)$, while the reverse inclusion is immediate. Hence

$$A_{z-1} := A[t] = \mathbb{R}\left[tx, ty, \frac{1}{t}\right] \cong \mathbb{R}[tx,ty]\left[\frac{1}{t}\right].$$

Now we claim that tx, ty are algebraically independent over $\mathbb{R}$. Let

$$u = tx, \qquad v = ty,$$

and let K be the quotient field of A. Then

$$K = \mathbb{R}(x, y, z),$$

and from $(\star)$ one can clearly see that x, y, z are all rational functions of u, v. Thus

$$K = \mathbb{R}(u, v).$$

Now we use the following theorem from commutative algebra.

> **Theorem.** If A is a finitely generated k-algebra which is an integral domain and K is its quotient field, then
>
> $$\operatorname{trdeg}_k K = \operatorname{Dim}_{\text{Krull}} A.$$

Applying the theorem gives

$$\operatorname{trdeg}_{\mathbb{R}} K = \operatorname{Dim}_{\text{Krull}} A = \operatorname{Dim}_{\text{Krull}} \mathbb{R}[x, y, z] - \operatorname{ht}(x^2 + y^2 + z^2 - 1) = 3 - 1 = 2.$$

Thus $K = \mathbb{R}(u, v)$ has transcendence degree 2, which implies that $\{u, v\}$ is algebraically independent over $\mathbb{R}$. Consequently,

$$\mathbb{R}[tx, ty] \cong \mathbb{R}[X, Y],$$

where X, Y are indeterminates, and hence $\mathbb{R}[tx, ty]$ is a UFD.

Now A_{z-1} is a localization of a UFD, so by **B(ii)** it is again a UFD. Therefore, by Nagata's Criterion **B(iii)**, we conclude that A is a UFD. ■

In the remark following **Example 4**, we saw that verifying whether a quotient of a polynomial ring is a UFD becomes significantly more subtle when the ground field is $\mathbb{Q}$, or more generally, a number field. The elementary techniques developed so far are no longer sufficient, and a deeper understanding of the underlying commutative algebra and algebraic geometry becomes necessary. In this section, we shall develop the required background from scratch and build up the theory needed to tackle such problems. As a pleasant by-product of this development, we shall recover Nagata's Criterion as a corollary of the more general results that we prove.

Weil divisor class group and the Excision sequence

Throughout this section **all rings and schemes are assumed to be Noetherian**. Our goal in this section is to define the divisor class group of a scheme. We begin with the notion of Weil divisors in complete generality, and then impose additional hypotheses that allow us to define principal divisors.

> **Definition.** Let X be a Noetherian integral scheme and $k(X)$ be its function field. A **Weil divisor** on X is a formal finite integral linear combination of integral closed subschemes of codimension one. Thus a Weil divisor has the form

$$D = \sum_{Y} n_Y Y,$$

where the sum ranges over the integral codimension one closed subschemes of X, each $n_Y \in \mathbb{Z}$, and all but finitely many of the coefficients are zero.

To define principal divisors we shall now assume that X is **regular in codimension one**, which is defined below.

Recall that a point $x \in X$ is said to have codimension one if its closure $\overline{\{x\}}$ is an integral closed subscheme of codimension one (for an affine scheme it consists of all the height one prime ideals). We say that X is regular in codimension one if, for every codimension one point $x \in X$, the local ring $\mathcal{O}_{X,x}$ is a discrete valuation ring (DVR).

> **Definition.** Let $y \in X$ be a codimension one point. Since $\mathcal{O}_{X,y}$ is a discrete valuation ring, it induces a discrete valuation

$$v_y : k(X)^\times \longrightarrow \mathbb{Z}.$$

The integer $v_y(f)$ is called the **order of f at the point y**.

> **Proposition.** Let X be an integral Noetherian scheme which is regular in codimension one, and let $f \in k(X)^\times$. Then $v_y(f) = 0$ for all but finitely many codimension one points $y \in X$.

Proof. Since f is a rational function, there exists a dense open subset $U \subseteq X$ on which f is a regular invertible function, that is,

$$f \in \mathcal{O}_X(U)^\times.$$

Now let $y \in U$ be a codimension one point. The germ of f at y is then a unit in the local ring $\mathcal{O}_{X,y}$. Since units in a discrete valuation ring have valuation zero, it follows that $v_y(f) = 0$. Hence, if $v_y(f) \neq 0$, then necessarily $y \in X \setminus U$.

At this point the Noetherian hypothesis becomes essential. Since X is Noetherian, every closed subset has only finitely many irreducible components. Thus the closed subset $X \setminus U$ has only finitely many irreducible components, and therefore contains only finitely many codimension one irreducible components. Their generic points are precisely the codimension one points contained in $X \setminus U$. Consequently $v_y(f) \neq 0$ for only finitely many codimension one points y. ■

> **Definition.** Let $f \in k(X)^\times$. The **principal divisor** associated to f, denoted by $\operatorname{div}(f)$, is defined by

$$\operatorname{div}(f) = \sum_{\operatorname{codim}(y)=1} v_y(f)\,\overline{\{y\}},$$

where $\overline{\{y\}}$ denotes the integral codimension one closed subscheme whose generic point is y.

Since discrete valuations satisfy

$$v_y(fg) = v_y(f) + v_y(g),$$

it follows immediately that

$$\operatorname{div}(fg) = \operatorname{div}(f) + \operatorname{div}(g).$$

Hence the set of principal divisors forms a subgroup of $\operatorname{Div}(X)$.

> **Definition.** The **Weil divisor class group** of X, denoted by $\operatorname{Cl}(X)$, is the quotient group

$$\operatorname{Cl}(X) = \frac{\operatorname{Div}(X)}{\{\text{principal divisors}\}}.$$

> **Excision/Localization Sequence.** Let X be a Noetherian integral scheme, and let $Z \subset X$ be a closed subset each of whose irreducible components have codimension one. Suppose Z has n irreducible components. Then we have the following exact sequence of groups:

$$\bigoplus_n \mathbb{Z} \longrightarrow \mathrm{Cl}(X) \longrightarrow \mathrm{Cl}(X \setminus Z) \longrightarrow 0.$$

The map

$$\bigoplus_n \mathbb{Z} \longrightarrow \mathrm{Cl}(X)$$

sends each irreducible component Y of Z to its divisor class $[Y]$, while the map

$$\mathrm{Cl}(X) \longrightarrow \mathrm{Cl}(X \setminus Z)$$

is simply the natural restriction map.

Although the exactness of this sequence at each stage is straightforward to verify, it will play a crucial role in many of the arguments that follow later on.

UFD Characterization via Cl(X) and Nagata's Criterion

We now present a fundamental characterization of Unique Factorization Domains in terms of the Weil divisor class group $\mathrm{Cl}(X)$ introduced previously. As an immediate application, we shall also prove Nagata's Criterion, which was used earlier in **Example 4** and **Example 5**. Before proceeding with the proof, we briefly state the celebrated Algebraic Hartogs' Lemma, which will play a key role in the argument. We shall state the lemma without proof.

> **Algebraic Hartogs' Lemma.** Let A be a normal Noetherian integral domain. Then

$$A = \bigcap_{\mathrm{ht}\, P = 1} A_P.$$

> **Remark.** This says that any element which belongs to the localization A_P for every height one prime ideal P of A must already belong to A. It is easy to see that this statement is immediate for one-dimensional rings, since in that case all nonzero prime ideals are maximal and we have
>
> $$A = \bigcap_m A_m,$$
>
> where m ranges over the maximal ideals of A. This is analogous to the elementary fact that if a rational number $\frac{a}{b}$ has denominator divisible by no prime number, then $\frac{a}{b} \in \mathbb{Z}$.

> **Proposition.** Let A be an integral domain. Then
>
> $$A \text{ is normal and } \mathrm{Cl}(A) = 0 \iff A \text{ is a UFD.}$$

Proof. Assume first that A is a UFD. Then from **A(i)** we already know that A is normal, so it remains to show that every divisor is principal.

Let $D = \sum_{\mathrm{ht}\, P=1} n_P P$ be a divisor. Since A is a UFD, we know from **A(ii)** that every height one prime ideal P is principal, so let $P = (p)$ where p is a prime element. Define

$$f := \prod p^{n_P} \in K^\times.$$

We claim that $\mathrm{div}(f) = D$. Indeed, if $P \neq Q$ are height one prime ideals generated by distinct prime elements, then $v_P(q) = 0$.

Therefore,

$$\mathrm{div}(f) = \sum_{\mathrm{ht}\, P=1} v_P\Big(\prod p^{n_P}\Big)\, P = \sum_{\mathrm{ht}\, P=1} n_P P = D.$$

Conversely, assume that A is normal and $\mathrm{Cl}(A) = 0$. We show that every height one prime ideal is principal, and hence A is a UFD by **A(ii)**.

Let P be a height one prime ideal. Since $\mathrm{Cl}(A) = 0$, there exists $x \in K^\times$ such that $\mathrm{div}(x) = P$.

By definition, $v_P(x) = 1$, so $x \in P$, and therefore $(x) \subseteq P$.Now let $y \in P$. Then for every height one prime ideal Q,

$$v_Q\left(\frac{y}{x}\right) = v_Q(y) - v_Q(x) \geq 0.$$

Indeed, if $Q = P$, then $v_P(y) \geq 1$, while if $Q \neq P$, then $v_Q(x) = 0$ and $v_Q(y) \geq 0$ since $y \in A$. Hence

$$v_Q\left(\frac{y}{x}\right) \geq 0 \qquad \text{for every height one prime } Q,$$

which implies

$$\frac{y}{x} \in A_Q \qquad \text{for every height one prime } Q.$$

Since A is normal, Algebraic Hartogs' Lemma gives $\frac{y}{x} \in A$.

Thus $y \in (x)$, so $P \subseteq (x)$. Together with $(x) \subseteq P$, we conclude that

$$P = (x).$$

Hence every height one prime ideal is principal, and therefore A is a UFD by **A(ii)**. ■

> **Nagata's Criterion.** Let A be a Noetherian domain and let $x \in A$ be a prime element. If
>
> $$A_x = A\left[\frac{1}{x}\right]$$
>
> is a UFD, then A is a UFD.

Proof. We first prove that A is normal.

Since A_x is a UFD, **A(i)** implies that A_x is normal.

Suppose

$$T^n + a_{n-1}T^{n-1} + \cdots + a_1T + a_0 = 0,$$

where $T \in Q(A)$ and $a_i \in A$. It suffices to prove that $T \in A$.

Since A_x is normal, $T = \frac{r}{x^m}$ for some $r \in A$.

Assume $T \notin A$.

Without loss of generality, assume $r \notin (x), \qquad m > 0$.

Multiplying the integral equation by x^{mn} gives

$$\left(\frac{r}{x^m}\right)^n + a_{n-1}\left(\frac{r}{x^m}\right)^{n-1} + \cdots + a_1\left(\frac{r}{x^m}\right) + a_0 = 0 \Longrightarrow r^n \in (x).$$

Since (x) is prime,$r \in (x)$, a contradiction. Hence $T \in A$, proving that A is normal.

Now apply the Excision Sequence:

$$\mathbb{Z}[(x)] \longrightarrow \mathrm{Cl}(A) \longrightarrow \mathrm{Cl}(\mathrm{Spec}\, A \setminus V(x)) = \mathrm{Cl}(A_x) \longrightarrow 0.$$

Since A_x is a UFD, the previous proposition implies $\mathrm{Cl}(A_x) = 0$. Hence

$$\mathrm{Cl}(A) = \mathbb{Z}[(x)].$$

Thus it suffices to show that (x) represents the trivial divisor class.

We claim that $\mathrm{div}(x) = (x)$. Indeed, $v_{(x)}(x) = 1$. Moreover, if P is any other height one prime ideal and $v_P(x) > 0$, then $x \in P$, which implies

$$(x) \subseteq P.$$

Since (x) itself is a height one prime ideal, this forces $P = (x)$, a contradiction.

Hence $\mathrm{div}(x) = (x)$, so (x) is principal in the divisor class group, and therefore $\mathrm{Cl}(A) = 0$.

Since we have already proved that A is normal, the proposition above yields that A is a UFD. ■

Riemann–Roch and Bézout for Curves over Arbitrary Fields

The celebrated theorems of **Riemann–Roch** and **Bézout** are usually presented over algebraically closed fields in most introductory textbooks on algebraic geometry. In this article, however, we shall require these theorems over arbitrary fields. Since our applications involve only curves (by which we shall always mean integral schemes of dimension one), we restrict ourselves to stating these results in the setting of curves over arbitrary fields.

One important point to keep in mind is that some of the familiar notions require slight modifications in this more general setting. We begin by recalling the relevant definitions.

Throughout this section, whenever we refer to a **closed point** of a curve C, we mean a maximal ideal of the scheme C. If P is a closed point, its **residue field** is defined by

$$k(P) := \mathcal{O}_{C,P}/\mathfrak{m}_P,$$

where $\mathcal{O}_{C,P}$ denotes the local ring of C at P, and $\mathfrak{m}_P$ is its unique maximal ideal.

> **Definition.** Let D be a Weil divisor
>
> $$D = \sum_P n_P P.$$

Then we define

$$\deg D = \sum_P n_P [k(P) : k].$$

As usual, for a divisor D, we define

$$L(D) = \{\, f \in k(C)^\times : \operatorname{div}(f) + D \geq 0 \,\} \cup \{0\}.$$

It is easy to verify that $L(D)$ is a finite-dimensional vector space over k. We denote its dimension by

$$\ell(D) := \dim_k L(D),$$

and let K_C denote a canonical divisor on C.

We may now state the Riemann–Roch theorem.

> **Riemann–Roch.** Let C be a smooth projective geometrically integral curve over a field k with genus g, and let D be a Weil divisor on C. Then
>
> $$\ell(D) - \ell(K_C - D) = \deg(D) + 1 - g.$$

> **Corollary (Riemann–Roch, genus 0).** If C has genus 0, then
>
> $$\ell(D) = \deg(D) + 1 + \ell(K_C - D) \geq \deg(D) + 1.$$

We now state Bézout's theorem in the setting of curves over arbitrary fields. We use the same notions as before.

> **Bézout's Theorem.** Let X and Y be two projective plane curves over k with degrees d_1 and d_2. Assume they share no common irreducible components. Then

$$d_1 d_2 = \sum_{P \in |X \cap Y|} i(X, Y; P)\,[k(P) : k],$$

where

- $|X \cap Y|$ is the set of all closed points in the scheme-theoretic intersection of X and Y.
- $i(X, Y; P)$ is the intersection multiplicity at P, defined by

$$i(X, Y; P) = \dim_{k(P)} \frac{\mathcal{O}_{\mathbb{P}^2_k, P}}{(f_P, g_P)},$$

where f_P, g_P are the local equations of X and Y, respectively.

Worked out example to gain some familiarity

The UFD Property of Coordinate Rings of Conics over Arbitrary Fields

> **Theorem.** Let k be a field and let $C \subset \mathbb{P}^2_k$ be a nonsingular conic. Let

$$U = C \cap \mathbb{A}^2_k.$$

Suppose that there is no k-rational point on C. Then

$$A := \mathcal{O}_C(U)$$

is a UFD.

Proof. We make use of all the results that we have seen before in this proof.

To start off, let

$$\mathbb{P}^2_k = \mathrm{Proj}(k[X, Y, Z])$$

and let $H_\infty = \mathrm{Proj}\left(\frac{k[X,Y,Z]}{(Z)}\right)$, which is the line at infinity of $\mathbb{P}^2_k$. Let $U = \mathbb{P}^2_k \setminus H_\infty$.

Now consider the **Excision Sequence**

$$\bigoplus_n \mathbb{Z} \longrightarrow \mathrm{Cl}(C) \longrightarrow \mathrm{Cl}(U) \longrightarrow 0,$$

where n is the number of irreducible components of $C \cap H_\infty$.

By **Bézout's Theorem** we get that $n \leq 2$. We shall show that $n = 1$. Suppose $|C \cap H_\infty| = \{P, Q\}$.

Now by **Bézout's Theorem** we know that

$$2 \cdot 1 = 2 = i(C, H_\infty; P)[k(P) : k] + i(C, H_\infty; Q)[k(Q) : k].$$

This forces both $[k(P) : k] = 1, \qquad [k(Q) : k] = 1$, which implies that P and Q are k-rational points on C, contradicting our hypothesis.

Thus the Excision Sequence becomes

$$\mathbb{Z} \longrightarrow \mathrm{Cl}(C) \longrightarrow \mathrm{Cl}(U) \longrightarrow 0.$$

To show that $\mathcal{O}_C(U)$ is a UFD, it suffices by the **Proposition** proved earlier to show that

$$\mathrm{Cl}(U) = 0,$$

or equivalently, that the map

$$\mathbb{Z} \longrightarrow \mathrm{Cl}(C)$$

is surjective. Since C is nonsingular, it already follows that $\mathcal{O}_C(U)$ is normal.

Since $Z = C \cap H_\infty$ is the only closed point at infinity, it follows from **Bézout's Theorem** that $\deg[Z] = 2$. Let D be a Weil divisor on C with $\deg D = 2n$.

Since C is a nonsingular conic, it has genus 0. Therefore two divisors are linearly equivalent if and only if they have the same degree. Hence $D \sim n[Z]$.

It remains to show that there is no divisor on C of degree 1. Suppose D is a divisor of degree 1. Then by the genus 0 case of **Riemann–Roch** we have

$$\ell(D) \geq \deg(D) + 1 = 2.$$

Therefore there exists a nonzero rational function $f \in k(C)^\times$ such that $\mathrm{div}(f) + D \geq 0$. Let $E := D + \mathrm{div}(f)$. Then E is effective, and

$$\deg(E) = \deg(D) + \deg(\operatorname{div}(f)) = 1.$$

Hence $E = [P]$ for some closed point P, and

$$[k(P) : k] = 1,$$

which implies that P is a k-rational point on C, contradicting our assumption.

Thus there are no divisors of odd degree on C, and every divisor of even degree is linearly equivalent to $n[Z]$ for some $n \in \mathbb{Z}$.

Therefore $\mathbb{Z} \longrightarrow \mathrm{Cl}(C)$ is surjective.

Finally, from the Excision Sequence

$$\mathbb{Z} \longrightarrow \mathrm{Cl}(C) \longrightarrow \mathrm{Cl}(U) \longrightarrow 0$$

we conclude that

$$\mathrm{Cl}(U) = 0.$$

Since $\mathcal{O}_C(U)$ is normal, the Proposition proved earlier implies that $\mathcal{O}_C(U)$ is a UFD. ■

A careful refinement of the above proof leads to even stronger results, three of which we state below.

> **Theorem (Stronger versions).**

- If C has no k-rational points, then $\mathcal{O}_C(U)$ is a UFD.
- If C has k-rational points at infinity, then $\mathcal{O}_C(U)$ is a UFD.
- If C has k-rational points but none at infinity, then $\mathcal{O}_C(U)$ is **not** a UFD.

Applications

Application 1

Let us revisit **Example 4**, where we proved that

$$\frac{\mathbb{R}[x, y]}{(x^2 + y^2 + 1)}$$

is a UFD. This now follows almost immediately from the theorem above.

Let C be the projective closure of the affine curve, namely

$$x^2 + y^2 + z^2 = 0.$$

On the affine patch $z = 1$, this becomes

$$x^2 + y^2 + 1 = 0.$$

It is immediate that

$$x^2 + y^2 + z^2 = 0$$

has no solution in $\mathbb{P}^2_{\mathbb{R}}$, and hence C has no $\mathbb{R}$-rational point. Therefore, by the theorem above,

$$\frac{\mathbb{R}[x, y]}{(x^2 + y^2 + 1)}$$

is a UFD.

For the $\mathbb{C}$ counterpart, we observe that

$$x^2 + y^2 + z^2 = 0$$

does have a point at infinity; for example,

$$[1 : i : 0]$$

lies on the conic. Hence, from the stronger version of the theorem,

$$\frac{\mathbb{C}[x, y]}{(x^2 + y^2 + 1)}$$

is also a UFD.

As an exercise, apply this theorem to **Exercise 3**. ■

Application 2

The true strength of the theorem becomes apparent when the ground field is $\mathbb{Q}$, or more generally, a number field. In this setting, the arithmetic question of whether the conic admits a rational point completely governs the algebraic question of whether its coordinate ring is a UFD. It is in these cases that the theorem reveals its full power.

Consider the ring

$$\frac{\mathbb{Q}[x,y]}{(x^2+2y^2+1)}.$$

Let C be the projective closure of the conic, namely

$$x^2+2y^2+z^2=0.$$

Clearly this has no point in $\mathbb{P}^2_{\mathbb{Q}}$. Hence, by the theorem,

$$\frac{\mathbb{Q}[x,y]}{(x^2+2y^2+1)}$$

is a UFD.

Now consider the same ring over $\mathbb{Q}(i)$:

$$\frac{\mathbb{Q}(i)[x,y]}{(x^2+2y^2+1)}.$$

The projective conic

$$x^2+2y^2+z^2=0$$

has the rational point

$$[\,1:0:i\,].$$

However, if $z=0$, then

$$x^2+2y^2=0,$$

so

$$\left(\frac{x}{y}\right)^2=-2,$$

which has no solution in $\mathbb{Q}(i)$ since

$$\sqrt{2}\notin\mathbb{Q}(i).$$

Thus C has a rational point, but none at infinity. Therefore, by the stronger version of the theorem,

$$\frac{\mathbb{Q}(i)[x,y]}{(x^2+2y^2+1)}$$

is **not** a UFD. ■

Exercises

1. Show that

$$\frac{\mathbb{Q}[x,y]}{(x^2+2y^2-1)}$$

is **not** a UFD.

2. Show that

$$\frac{\mathbb{Q}(i)[x,y]}{(x^2+2y^2-1)}$$

is a UFD.

Bonus!

Here is an extra example illustrating the usefulness of the preceding theory for the coordinate ring of the elliptic curve

$$y^2 = x^3 - x$$

over the algebraically closed field $\mathbb{C}$.

We shall prove that

$$\frac{\mathbb{C}[x,y]}{(y^2-x^3+x)} \quad \text{is not a UFD.}$$

Proof. Let C be the projective closure of the affine curve

$$y^2 = x^3 - x$$

inside $\mathbb{A}^2_{\mathbb{C}}$.

Its homogeneous equation is

$$Y^2Z = X^3 - XZ^2.$$

When $Z = 0$, we obtain

$$X = 0,$$

so there is exactly one point at infinity. Let the corresponding affine open subset be denoted by U.

The Excision Sequence therefore becomes

$$\mathbb{Z} \longrightarrow \mathrm{Cl}(C) \longrightarrow \mathrm{Cl}(U) \longrightarrow 0.$$

Since

$$\mathrm{Cl}(C) = \mathrm{Pic}(C) \cong \mathbb{Z} \oplus \mathrm{Pic}^0(C),$$

we obtain the exact sequence

$$\mathbb{Z} \longrightarrow \mathbb{Z} \oplus \mathrm{Pic}^0(C) \longrightarrow \mathrm{Cl}(U) \longrightarrow 0.$$

Hence

$$\mathrm{Cl}(U) \cong \mathrm{Pic}^0(C).$$

A deep theorem of algebraic geometry, whose proof ultimately relies on the **Riemann–Roch Theorem**, states that

$$\mathrm{Pic}^0(C) \cong E(\mathbb{C}).$$

Since $E(\mathbb{C})$ is an infinite group, it follows that

$$\mathrm{Cl}(U) \neq 0.$$

Therefore, by the Proposition proved earlier,

$$\frac{\mathbb{C}[x, y]}{(y^2 - x^3 + x)}$$

is not a UFD. ■

> **Remark.** There is nothing special about the above example. More generally, the affine coordinate ring of any elliptic curve is never a UFD. Indeed, quotienting the group
>
> $$E(\mathbb{C}) \cong \mathrm{Pic}^0(C)$$
>
> by the image of a finitely generated free abelian group still leaves a large nontrivial group. Consequently,
>
> $$\mathrm{Cl}(U) \neq 0,$$
>
> so the coordinate ring cannot be a UFD. This illustrates the broader principle that affine coordinate rings of positive genus curves almost always fail to be unique factorization domains.

Conclusion

In this article, we explored a variety of techniques for determining whether quotients of polynomial rings are unique factorization domains. We began with elementary tools from commutative algebra, which are often effective in proving that a ring is not a UFD, before developing the geometric machinery of the Weil divisor class group to obtain powerful criteria for proving that a ring is a UFD. Along the way, we recovered Nagata's Criterion as a natural consequence of this theory.

The final examples on affine conics beautifully illustrate the philosophy behind these ideas: over number fields, the arithmetic question of whether a conic has a rational point completely determines whether its coordinate ring is a UFD. This striking interplay between arithmetic, algebraic geometry, and commutative algebra is one of the many reasons why the study of unique factorization remains such a rich and fascinating subject.

Signing off!