February 24, 2021
From now on we will denote the field $\mathbb{Z}/p\mathbb{Z}$ for a prime $p$ more compactly by $F_p$.

More generally, for $q$ a power of a prime $p$, $F_q$ will denote the finite field with $q$ elements.

**Definition**

A function field is a finite algebraic extension of the field of rational functions $F_p(\mathbb{X})$, where $\mathbb{X}$ is transcendental over $F_p$ (i.e., a "variable").

If $K$ is such a field, then the subset of elements that are algebraic over $F_p$ is clearly an algebraic extension of $F_p$ called the field of constants of $K$.

Note that any element $\alpha$ not in the field of constants is by definition transcendental over $F_p$ and $[K:F_p(\alpha)] < \infty$.

**Definition**

A valuation ring of a field $K$ is a proper subring $R \subseteq K$ such that for all $a \in K$, either $a \in R$ or $a^{-1} \in R$. 
Places of Number Fields and Function Fields

From now on we will denote the field $\mathbb{Z}/p\mathbb{Z}$ for a prime $p$ more compactly by $\mathbb{F}_p$.
From now on we will denote the field $\mathbb{Z}/p\mathbb{Z}$ for a prime $p$ more compactly by $\mathbb{F}_p$. More generally,
From now on we will denote the field $\mathbb{Z}/p\mathbb{Z}$ for a prime $p$ more compactly by $\mathbb{F}_p$. More generally, for $q$ a power of a prime $p$, ...
From now on we will denote the field $\mathbb{Z}/p\mathbb{Z}$ for a prime $p$ more compactly by $\mathbb{F}_p$. More generally, for $q$ a power of a prime $p$, $\mathbb{F}_q$ will denote the finite field with $q$ elements.
From now on we will denote the field $\mathbb{Z}/p\mathbb{Z}$ for a prime $p$ more compactly by $\mathbb{F}_p$. More generally, for $q$ a power of a prime $p$, $\mathbb{F}_q$ will denote the finite field with $q$ elements.

**Definition**

A function field is a finite algebraic extension of the field of rational functions $\mathbb{F}_p(\mathbb{X})$, where $\mathbb{X}$ is transcendental over $\mathbb{F}_p$ (i.e., a "variable"). If $K$ is such a field, then the subset of elements that are algebraic over $\mathbb{F}_p$ is clearly an algebraic extension of $\mathbb{F}_p$ called the field of constants of $K$.

Note that any element $\alpha$ not in the field of constants is by definition transcendental over $\mathbb{F}_p$ and $[K:\mathbb{F}_p(\alpha)]<\infty$. 

**Definition**

A valuation ring of a field $K$ is a proper subring $R \subseteq K$ such that for all $a \in K$, either $a \in R$ or $a^{-1} \in R$. 
From now on we will denote the field $\mathbb{Z}/p\mathbb{Z}$ for a prime $p$ more compactly by $\mathbb{F}_p$. More generally, for $q$ a power of a prime $p$, $\mathbb{F}_q$ will denote the finite field with $q$ elements.

**Definition**

A *function field* is a finite algebraic extension of the field of rational functions $\mathbb{F}_p(X)$,
From now on we will denote the field $\mathbb{Z}/p\mathbb{Z}$ for a prime $p$ more compactly by $\mathbb{F}_p$. More generally, for $q$ a power of a prime $p$, $\mathbb{F}_q$ will denote the finite field with $q$ elements.

**Definition**

A *function field* is a finite algebraic extension of the field of rational functions $\mathbb{F}_p(X)$, where $X$ is transcendental over $\mathbb{F}_p$. 
Places of Number Fields and Function Fields

From now on we will denote the field \( \mathbb{Z}/p\mathbb{Z} \) for a prime \( p \) more compactly by \( \mathbb{F}_p \). More generally, for \( q \) a power of a prime \( p \), \( \mathbb{F}_q \) will denote the finite field with \( q \) elements.

**Definition**

A *function field* is a finite algebraic extension of the field of rational functions \( \mathbb{F}_p(X) \), where \( X \) is transcendental over \( \mathbb{F}_p \) (i.e., a “variable”).
From now on we will denote the field $\mathbb{Z}/p\mathbb{Z}$ for a prime $p$ more compactly by $\mathbb{F}_p$. More generally, for $q$ a power of a prime $p$, $\mathbb{F}_q$ will denote the finite field with $q$ elements.

**Definition**

A *function field* is a finite algebraic extension of the field of rational functions $\mathbb{F}_p(X)$, where $X$ is transcendental over $\mathbb{F}_p$ (i.e., a “variable”). If $K$ is such a field, then the subset of elements that are algebraic over $\mathbb{F}_p$...
From now on we will denote the field $\mathbb{Z}/p\mathbb{Z}$ for a prime $p$ more compactly by $\mathbb{F}_p$. More generally, for $q$ a power of a prime $p$, $\mathbb{F}_q$ will denote the finite field with $q$ elements.

**Definition**

A function field is a finite algebraic extension of the field of rational functions $\mathbb{F}_p(X)$, where $X$ is transcendental over $\mathbb{F}_p$ (i.e., a “variable”). If $K$ is such a field, then the subset of elements that are algebraic over $\mathbb{F}_p$ is clearly an algebraic extension of $\mathbb{F}_p$. 
From now on we will denote the field \( \mathbb{Z}/p\mathbb{Z} \) for a prime \( p \) more compactly by \( \mathbb{F}_p \). More generally, for \( q \) a power of a prime \( p \), \( \mathbb{F}_q \) will denote the finite field with \( q \) elements.

**Definition**

A *function field* is a finite algebraic extension of the field of rational functions \( \mathbb{F}_p(X) \), where \( X \) is transcendental over \( \mathbb{F}_p \) (i.e., a “variable”). If \( K \) is such a field, then the subset of elements that are algebraic over \( \mathbb{F}_p \) is clearly an algebraic extension of \( \mathbb{F}_p \) called the *field of constants* of \( K \).
From now on we will denote the field $\mathbb{Z}/p\mathbb{Z}$ for a prime $p$ more compactly by $\mathbb{F}_p$. More generally, for $q$ a power of a prime $p$, $\mathbb{F}_q$ will denote the finite field with $q$ elements.

**Definition**

A *function field* is a finite algebraic extension of the field of rational functions $\mathbb{F}_p(X)$, where $X$ is transcendental over $\mathbb{F}_p$ (i.e., a “variable”). If $K$ is such a field, then the subset of elements that are algebraic over $\mathbb{F}_p$ is clearly an algebraic extension of $\mathbb{F}_p$ called the *field of constants* of $K$.

Note that any element $\alpha$ not in the field of constants is by definition transcendental over $\mathbb{F}_p$. 
From now on we will denote the field $\mathbb{Z}/p\mathbb{Z}$ for a prime $p$ more compactly by $\mathbb{F}_p$. More generally, for $q$ a power of a prime $p$, $\mathbb{F}_q$ will denote the finite field with $q$ elements.

**Definition**

A *function field* is a finite algebraic extension of the field of rational functions $\mathbb{F}_p(X)$, where $X$ is transcendental over $\mathbb{F}_p$ (i.e., a “variable”). If $K$ is such a field, then the subset of elements that are algebraic over $\mathbb{F}_p$ is clearly an algebraic extension of $\mathbb{F}_p$ called the *field of constants* of $K$.

Note that any element $\alpha$ not in the field of constants is by definition transcendental over $\mathbb{F}_p$ and $[K : \mathbb{F}_p(\alpha)] < \infty$. 
From now on we will denote the field $\mathbb{Z}/p\mathbb{Z}$ for a prime $p$ more compactly by $\mathbb{F}_p$. More generally, for $q$ a power of a prime $p$, $\mathbb{F}_q$ will denote the finite field with $q$ elements.

**Definition**

A function field is a finite algebraic extension of the field of rational functions $\mathbb{F}_p(X)$, where $X$ is transcendental over $\mathbb{F}_p$ (i.e., a “variable”). If $K$ is such a field, then the subset of elements that are algebraic over $\mathbb{F}_p$ is clearly an algebraic extension of $\mathbb{F}_p$ called the field of constants of $K$.

Note that any element $\alpha$ not in the field of constants is by definition transcendental over $\mathbb{F}_p$ and $[K : \mathbb{F}_p(\alpha)] < \infty$.

**Definition**
Places of Number Fields and Function Fields

From now on we will denote the field $\mathbb{Z}/p\mathbb{Z}$ for a prime $p$ more compactly by $\mathbb{F}_p$. More generally, for $q$ a power of a prime $p$, $\mathbb{F}_q$ will denote the finite field with $q$ elements.

**Definition**

A *function field* is a finite algebraic extension of the field of rational functions $\mathbb{F}_p(X)$, where $X$ is transcendental over $\mathbb{F}_p$ (i.e., a “variable”). If $K$ is such a field, then the subset of elements that are algebraic over $\mathbb{F}_p$ is clearly an algebraic extension of $\mathbb{F}_p$ called the *field of constants* of $K$.

Note that any element $\alpha$ not in the field of constants is by definition transcendental over $\mathbb{F}_p$ and $[K : \mathbb{F}_p(\alpha)] < \infty$.

**Definition**

A *valuation ring* of a field $K$ is a proper subring $R \subseteq K$...
From now on we will denote the field $\mathbb{Z}/p\mathbb{Z}$ for a prime $p$ more compactly by $\mathbb{F}_p$. More generally, for $q$ a power of a prime $p$, $\mathbb{F}_q$ will denote the finite field with $q$ elements.

**Definition**

A function field is a finite algebraic extension of the field of rational functions $\mathbb{F}_p(X)$, where $X$ is transcendental over $\mathbb{F}_p$ (i.e., a "variable"). If $K$ is such a field, then the subset of elements that are algebraic over $\mathbb{F}_p$ is clearly an algebraic extension of $\mathbb{F}_p$ called the field of constants of $K$.

Note that any element $\alpha$ not in the field of constants is by definition transcendental over $\mathbb{F}_p$ and $[K : \mathbb{F}_p(\alpha)] < \infty$.

**Definition**

A valuation ring of a field $K$ is a proper subring $R \subsetneq K$ such that for all $a \in K$,
From now on we will denote the field $\mathbb{Z}/p\mathbb{Z}$ for a prime $p$ more compactly by $\mathbb{F}_p$. More generally, for $q$ a power of a prime $p$, $\mathbb{F}_q$ will denote the finite field with $q$ elements.

**Definition**

A *function field* is a finite algebraic extension of the field of rational functions $\mathbb{F}_p(X)$, where $X$ is transcendental over $\mathbb{F}_p$ (i.e., a “variable”). If $K$ is such a field, then the subset of elements that are algebraic over $\mathbb{F}_p$ is clearly an algebraic extension of $\mathbb{F}_p$ called the *field of constants* of $K$.

Note that any element $\alpha$ not in the field of constants is by definition transcendental over $\mathbb{F}_p$ and $[K : \mathbb{F}_p(\alpha)] < \infty$.

**Definition**

A *valuation ring* of a field $K$ is a proper subring $R \subsetneq K$ such that for all $a \in K$, either $a \in R$ or $a^{-1} \in R$. 
Note that any valuation ring $R$ of a field contains $\mathbb{Z}$ in characteristic 0 or $\mathbb{F}_p$ in characteristic $p$, since $\pm 1 \in R$.

Example 1: Suppose $K$ is a number field. Given a non-trivial prime ideal $P \subset \mathcal{O}_K$, the ring $\mathcal{O}_P$ introduced in exercise #4 from week 5 is a valuation ring of the number field $K$.

Example 2: Extend the usual notion of the degree of a polynomial to rational functions by setting the degree of a quotient $P/Q$, $P, Q \in \mathbb{F}_q[X]$, to be $\deg(P) - \deg(Q)$. (Note that this is well-defined.) Then the subset of $\mathbb{F}_q(X)$ consisting of rational functions of degree no more than 0 is a valuation ring.

Lemma (1): All valuation rings are local rings, i.e., have a unique maximal ideal.
Note that any valuation ring $R$ of a field contains $\mathbb{Z}$ in characteristic 0.
Note that any valuation ring $R$ of a field contains $\mathbb{Z}$ in characteristic 0 or $\mathbb{F}_p$ in characteristic $p$. 

Example 1: Suppose $K$ is a number field. Given a non-trivial prime ideal $P \subset \mathcal{O}_K$, the ring $\mathcal{O}_P$ introduced in exercise #4 from week 5 is a valuation ring of the number field $K$. 

Example 2: Extend the usual notion of the degree of a polynomial to rational functions by setting the degree of a quotient $P/Q$, $P, Q \in \mathbb{F}_q[X]$, to be $\deg(P) - \deg(Q)$. (Note that this is well-defined.) Then the subset of $\mathbb{F}_q(X)$ consisting of rational functions of degree no more than 0 is a valuation ring.

Lemma (1) All valuation rings are local rings, i.e., have a unique maximal ideal.
Note that any valuation ring $R$ of a field contains $\mathbb{Z}$ in characteristic 0 or $\mathbb{F}_p$ in characteristic $p$ since $\pm 1 \in R$. 

Example 1: Suppose $K$ is a number field. Given a non-trivial prime ideal $P \subset \mathcal{O}_K$, the ring $\mathcal{O}_P$ introduced in exercise #4 from week 5 is a valuation ring of the number field $K$. 

Example 2: Extend the usual notion of the degree of a polynomial to rational functions by setting the degree of a quotient $P/Q$, $P, Q \in \mathbb{F}_q[\mathbb{X}]$, to be $\deg(P) - \deg(Q)$. (Note that this is well-defined.) Then the subset of $\mathbb{F}_q(\mathbb{X})$ consisting of rational functions of degree no more than 0 is a valuation ring. 

Lemma (1) All valuation rings are local rings, i.e., have a unique maximal ideal.
Note that any valuation ring $R$ of a field contains $\mathbb{Z}$ in characteristic 0 or $\mathbb{F}_p$ in characteristic $p$ since $\pm 1 \in R$.

**Example 1:**
Note that any valuation ring $R$ of a field contains $\mathbb{Z}$ in characteristic 0 or $\mathbb{F}_p$ in characteristic $p$ since $\pm 1 \in R$.

**Example 1:** Suppose $K$ is a number field.
Note that any valuation ring $R$ of a field contains $\mathbb{Z}$ in characteristic 0 or $\mathbb{F}_p$ in characteristic $p$ since $\pm 1 \in R$.

**Example 1:** Suppose $K$ is a number field. Given a non-trivial prime ideal $\mathfrak{P} \subset \mathcal{O}_K$, 

**Example 2:** Extend the usual notion of the degree of a polynomial to rational functions by setting the degree of a quotient $P/Q$, $P, Q \in \mathbb{F}_q[X]$, to be $\deg(P) - \deg(Q)$. (Note that this is well-defined.) Then the subset of $\mathbb{F}_q(X)$ consisting of rational functions of degree no more than 0 is a valuation ring.

**Lemma (1)** All valuation rings are local rings, i.e., have a unique maximal ideal.
Note that any valuation ring $R$ of a field contains $\mathbb{Z}$ in characteristic 0 or $\mathbb{F}_p$ in characteristic $p$ since $\pm 1 \in R$.

**Example 1**: Suppose $K$ is a number field. Given a non-trivial prime ideal $\mathfrak{P} \subset \mathcal{O}_K$, the ring $\mathcal{O}_\mathfrak{P}$ introduced in exercise #4 from week 5 is a valuation ring of the number field $K$. 

**Example 2**: Extend the usual notion of the degree of a polynomial to rational functions by setting the degree of a quotient $\frac{P}{Q}$, $P, Q \in \mathbb{F}_q[X]$, to be $\deg(P) - \deg(Q)$. (Note that this is well-defined.) Then the subset of $\mathbb{F}_q(X)$ consisting of rational functions of degree no more than 0 is a valuation ring.

**Lemma (1)** All valuation rings are local rings, i.e., have a unique maximal ideal.
Note that any valuation ring $R$ of a field contains $\mathbb{Z}$ in characteristic $0$ or $\mathbb{F}_p$ in characteristic $p$ since $\pm 1 \in R$.

**Example 1:** Suppose $K$ is a number field. Given a non-trivial prime ideal $\mathfrak{P} \subset \mathcal{O}_K$, the ring $\mathcal{O}_{\mathfrak{P}}$ introduced in exercise #4 from week 5 is a valuation ring of the number field $K$.

**Example 2:**
Note that any valuation ring $R$ of a field contains $\mathbb{Z}$ in characteristic 0 or $\mathbb{F}_p$ in characteristic $p$ since $\pm 1 \in R$.

**Example 1:** Suppose $K$ is a number field. Given a non-trivial prime ideal $\mathfrak{P} \subset \mathcal{O}_K$, the ring $\mathcal{O}_{\mathfrak{P}}$ introduced in exercise $\#4$ from week 5 is a valuation ring of the number field $K$.

**Example 2:** Extend the usual notion of the degree of a polynomial to rational functions by setting the degree of a quotient $\frac{P}{Q}$, $P, Q \in \mathbb{F}_q[X]$, to be $\deg(P) - \deg(Q)$. (Note that this is well-defined.) Then the subset of $\mathbb{F}_q(X)\,$ consisting of rational functions of degree no more than 0 is a valuation ring.

**Lemma (1)** All valuation rings are local rings, i.e., have a unique maximal ideal.
Note that any valuation ring $R$ of a field contains $\mathbb{Z}$ in characteristic 0 or $\mathbb{F}_p$ in characteristic $p$ since $\pm 1 \in R$.

**Example 1**: Suppose $K$ is a number field. Given a non-trivial prime ideal $\mathfrak{P} \subset \mathcal{O}_K$, the ring $\mathcal{O}_\mathfrak{P}$ introduced in exercise #4 from week 5 is a valuation ring of the number field $K$.

**Example 2**: Extend the usual notion of the degree of a polynomial to rational functions by setting the degree of a quotient $P/Q$, 
Note that any valuation ring $R$ of a field contains $\mathbb{Z}$ in characteristic 0 or $\mathbb{F}_p$ in characteristic $p$ since $\pm 1 \in R$.

**Example 1**: Suppose $K$ is a number field. Given a non-trivial prime ideal $\mathfrak{P} \subset \mathcal{O}_K$, the ring $\mathcal{O}_{\mathfrak{P}}$ introduced in exercise #4 from week 5 is a valuation ring of the number field $K$.

**Example 2**: Extend the usual notion of the degree of a polynomial to rational functions by setting the degree of a quotient $P/Q$, $P, Q \in \mathbb{F}_q[X]$, to be $\deg(P) - \deg(Q)$. (Note that this is well-defined.) Then the subset of $\mathbb{F}_q(X)$ consisting of rational functions of degree no more than 0 is a valuation ring.

**Lemma (1)**: All valuation rings are local rings, i.e., have a unique maximal ideal.
Note that any valuation ring $R$ of a field contains $\mathbb{Z}$ in characteristic 0 or $\mathbb{F}_p$ in characteristic $p$ since $\pm 1 \in R$.

**Example 1**: Suppose $K$ is a number field. Given a non-trivial prime ideal $\mathfrak{p} \subset \mathcal{O}_K$, the ring $\mathcal{O}_{\mathfrak{p}}$ introduced in exercise #4 from week 5 is a valuation ring of the number field $K$.

**Example 2**: Extend the usual notion of the degree of a polynomial to rational functions by setting the degree of a quotient $P/Q$, $P, Q \in \mathbb{F}_q[X]$, to be $\deg(P) - \deg(Q)$.
Note that any valuation ring $R$ of a field contains $\mathbb{Z}$ in characteristic 0 or $\mathbb{F}_p$ in characteristic $p$ since $\pm 1 \in R$.

**Example 1**: Suppose $K$ is a number field. Given a non-trivial prime ideal $\mathfrak{p} \subset \mathcal{O}_K$, the ring $\mathcal{O}_{\mathfrak{p}}$ introduced in exercise #4 from week 5 is a valuation ring of the number field $K$.

**Example 2**: Extend the usual notion of the degree of a polynomial to rational functions by setting the degree of a quotient $P/Q$, $P, Q \in \mathbb{F}_q[X]$, to be $\text{deg}(P) - \text{deg}(Q)$. (Note that this is well-defined.)
Note that any valuation ring $R$ of a field contains $\mathbb{Z}$ in characteristic 0 or $\mathbb{F}_p$ in characteristic $p$ since $\pm 1 \in R$.

**Example 1:** Suppose $K$ is a number field. Given a non-trivial prime ideal $\mathfrak{P} \subset \mathcal{O}_K$, the ring $\mathcal{O}_{\mathfrak{P}}$ introduced in exercise #4 from week 5 is a valuation ring of the number field $K$.

**Example 2:** Extend the usual notion of the degree of a polynomial to rational functions by setting the degree of a quotient $P/Q$, $P, Q \in \mathbb{F}_q[X]$, to be $\deg(P) - \deg(Q)$. (Note that this is well-defined.) Then the subset of $\mathbb{F}_q(X)$ consisting of rational functions of degree no more than 0 is a valuation ring.
Note that any valuation ring $R$ of a field contains $\mathbb{Z}$ in characteristic 0 or $\mathbb{F}_p$ in characteristic $p$ since $\pm 1 \in R$.

**Example 1:** Suppose $K$ is a number field. Given a non-trivial prime ideal $\mathfrak{P} \subset \mathcal{O}_K$, the ring $\mathcal{O}_\mathfrak{P}$ introduced in exercise $\#4$ from week 5 is a valuation ring of the number field $K$.

**Example 2:** Extend the usual notion of the degree of a polynomial to rational functions by setting the degree of a quotient $P/Q$, $P, Q \in \mathbb{F}_q[X]$, to be $\deg(P) - \deg(Q)$. (Note that this is well-defined.) Then the subset of $\mathbb{F}_q(X)$ consisting of rational functions of degree no more than 0 is a valuation ring.

**Lemma (1)**
Note that any valuation ring $R$ of a field contains $\mathbb{Z}$ in characteristic 0 or $\mathbb{F}_p$ in characteristic $p$ since $\pm 1 \in R$.

**Example 1**: Suppose $K$ is a number field. Given a non-trivial prime ideal $\mathfrak{p} \subset \mathcal{O}_K$, the ring $\mathcal{O}_\mathfrak{p}$ introduced in exercise #4 from week 5 is a valuation ring of the number field $K$.

**Example 2**: Extend the usual notion of the degree of a polynomial to rational functions by setting the degree of a quotient $P/Q$, $P, Q \in \mathbb{F}_q[X]$, to be $\deg(P) - \deg(Q)$. (Note that this is well-defined.) Then the subset of $\mathbb{F}_q(X)$ consisting of rational functions of degree no more than 0 is a valuation ring.

**Lemma (1)**

All valuation rings are local rings,
Note that any valuation ring $R$ of a field contains $\mathbb{Z}$ in characteristic 0 or $\mathbb{F}_p$ in characteristic $p$ since $\pm 1 \in R$.

**Example 1:** Suppose $K$ is a number field. Given a non-trivial prime ideal $\mathfrak{p} \subset \mathcal{O}_K$, the ring $\mathcal{O}_\mathfrak{p}$ introduced in exercise #4 from week 5 is a valuation ring of the number field $K$.

**Example 2:** Extend the usual notion of the degree of a polynomial to rational functions by setting the degree of a quotient $P/Q$, $P, Q \in \mathbb{F}_q[X]$, to be $\deg(P) - \deg(Q)$. (Note that this is well-defined.) Then the subset of $\mathbb{F}_q(X)$ consisting of rational functions of degree no more than 0 is a valuation ring.

**Lemma (1)**

All valuation rings are local rings, i.e., have a unique maximal ideal.
Proof:

Let $R$ be a valuation ring of a field and let $M$ denote the non-units of $R$. Note that $M$ consists of more than simply the element 0 since otherwise $R = K$.

Let $\alpha \in M$ and $\beta \in R$. If $\alpha \beta$ is a unit then $\beta (\alpha \beta - 1) = \alpha - 1 \in R$ so that $\alpha$ is a unit, contradicting our hypothesis. Thus $\alpha \beta \in M$.

Now suppose $\beta \in M$ and consider $\alpha + \beta \in R$. If either $\alpha$ or $\beta$ is 0 then clearly $\alpha + \beta \in M$, so suppose otherwise. Since $R$ is a valuation ring we may assume without loss of generality that $\alpha/\beta \in R$. Then $1 + (\alpha/\beta) \in R$ and so $\beta (1 + (\alpha/\beta)) = \alpha + \beta \in M$ by what we have already shown.

Thus $M$ is an ideal. It is clearly the unique maximal ideal of $R$ since any ideal not properly contained in $M$ must contain a unit, whence must be the entire ring.
Proof: Let $R$ be a valuation ring of a field.

Note that $M$ consists of more than simply the element 0 since otherwise $R = K$.

Let $\alpha \in M$ and $\beta \in R$. If $\alpha \beta$ is a unit, then $\beta (\alpha \beta)^{-1} = \alpha^{-1} \in R$ so that $\alpha$ is a unit, contradicting our hypothesis. Thus $\alpha \beta \in M$.

Now suppose $\beta \in M$ and consider $\alpha + \beta \in R$. If either $\alpha$ or $\beta$ is 0, then clearly $\alpha + \beta \in M$, so suppose otherwise. Since $R$ is a valuation ring, we may assume without loss of generality that $\alpha/\beta \in R$. Then $1 + (\alpha/\beta) \in R$ and so $\beta (1 + (\alpha/\beta)) = \alpha + \beta \in M$ by what we have already shown. Thus $M$ is an ideal.

It is clearly the unique maximal ideal of $R$ since any ideal not properly contained in $M$ must contain a unit, whence must be the entire ring.
**Proof:** Let $R$ be a valuation ring of a field and let $M$ denote the non-units of $R$. 

Note that $M$ consists of more than simply the element 0 since otherwise $R = K$.

Let $\alpha \in M$ and $\beta \in R$.

If $\alpha \beta$ is a unit then $\beta (\alpha \beta) - 1 = \alpha - 1 \in R$ so that $\alpha$ is a unit, contradicting our hypothesis. Thus $\alpha \beta \in M$.

Now suppose $\beta \in M$ and consider $\alpha + \beta \in R$.

If either $\alpha$ or $\beta$ is 0 then clearly $\alpha + \beta \in M$, so suppose otherwise.

Since $R$ is a valuation ring we may assume without loss of generality that $\alpha/\beta \in R$.

Then $1 + (\alpha/\beta) \in R$ and so $\beta (1 + (\alpha/\beta)) = \alpha + \beta \in M$ by what we have already shown.

Thus $M$ is an ideal.

It is clearly the unique maximal ideal of $R$ since any ideal not properly contained in $M$ must contain a unit, whence must be the entire ring.
Proof: Let $R$ be a valuation ring of a field and let $\mathcal{M}$ denote the non-units of $R$. Note that $\mathcal{M}$ consists of more than simply the element 0.
Proof: Let $R$ be a valuation ring of a field and let $\mathcal{M}$ denote the non-units of $R$. Note that $\mathcal{M}$ consists of more than simply the element 0 since otherwise $R = K$. 

Let $\alpha \in \mathcal{M}$ and $\beta \in R$. If $\alpha \beta$ is a unit then $\beta(\alpha \beta) - 1 = \alpha - 1 \in R$ so that $\alpha$ is a unit, contradicting our hypothesis. Thus $\alpha \beta \in \mathcal{M}$.

Now suppose $\beta \in \mathcal{M}$ and consider $\alpha + \beta \in R$. If either $\alpha$ or $\beta$ is 0 then clearly $\alpha + \beta \in \mathcal{M}$, so suppose otherwise. Since $R$ is a valuation ring we may assume without loss of generality that $\alpha / \beta \in R$. Then $1 + (\alpha / \beta) \in R$ and so $\beta(1 + (\alpha / \beta)) = \alpha + \beta \in \mathcal{M}$ by what we have already shown. Thus $\mathcal{M}$ is an ideal. It is clearly the unique maximal ideal of $R$ since any ideal not properly contained in $\mathcal{M}$ must contain a unit, whence must be the entire ring.
Proof: Let $R$ be a valuation ring of a field and let $\mathcal{M}$ denote the non-units of $R$. Note that $\mathcal{M}$ consists of more than simply the element 0 since otherwise $R = K$.

Let $\alpha \in \mathcal{M}$ and $\beta \in R$. 

**Proof:** Let $R$ be a valuation ring of a field and let $\mathcal{M}$ denote the non-units of $R$. Note that $\mathcal{M}$ consists of more than simply the element 0 since otherwise $R = K$.

Let $\alpha \in \mathcal{M}$ and $\beta \in R$. If $\alpha \beta$ is a unit
**Proof:** Let $R$ be a valuation ring of a field and let $\mathcal{M}$ denote the non-units of $R$. Note that $\mathcal{M}$ consists of more than simply the element 0 since otherwise $R = K$.

Let $\alpha \in \mathcal{M}$ and $\beta \in R$. If $\alpha \beta$ is a unit then $\beta(\alpha \beta)^{-1} = \alpha^{-1} \in R$
Proof: Let $R$ be a valuation ring of a field and let $\mathcal{M}$ denote the non-units of $R$. Note that $\mathcal{M}$ consists of more than simply the element 0 since otherwise $R = K$.

Let $\alpha \in \mathcal{M}$ and $\beta \in R$. If $\alpha \beta$ is a unit then $\beta(\alpha \beta)^{-1} = \alpha^{-1} \in R$ so that $\alpha$ is a unit,
Proof: Let $R$ be a valuation ring of a field and let $M$ denote the non-units of $R$. Note that $M$ consists of more than simply the element 0 since otherwise $R = K$.

Let $\alpha \in M$ and $\beta \in R$. If $\alpha \beta$ is a unit then $\beta(\alpha \beta)^{-1} = \alpha^{-1} \in R$ so that $\alpha$ is a unit, contradicting our hypothesis.
**Proof:** Let $R$ be a valuation ring of a field and let $\mathcal{M}$ denote the non-units of $R$. Note that $\mathcal{M}$ consists of more than simply the element 0 since otherwise $R = K$.

Let $\alpha \in \mathcal{M}$ and $\beta \in R$. If $\alpha \beta$ is a unit then $\beta(\alpha \beta)^{-1} = \alpha^{-1} \in R$ so that $\alpha$ is a unit, contradicting our hypothesis. Thus $\alpha \beta \in \mathcal{M}$.
Proof: Let $R$ be a valuation ring of a field and let $M$ denote the non-units of $R$. Note that $M$ consists of more than simply the element 0 since otherwise $R = K$.

Let $\alpha \in M$ and $\beta \in R$. If $\alpha \beta$ is a unit then $\beta(\alpha \beta)^{-1} = \alpha^{-1} \in R$ so that $\alpha$ is a unit, contradicting our hypothesis. Thus $\alpha \beta \in M$.

Now suppose $\beta \in M$ and consider $\alpha + \beta \in R$. 

Proof: Let $R$ be a valuation ring of a field and let $\mathcal{M}$ denote the non-units of $R$. Note that $\mathcal{M}$ consists of more than simply the element 0 since otherwise $R = K$.

Let $\alpha \in \mathcal{M}$ and $\beta \in R$. If $\alpha \beta$ is a unit then $\beta(\alpha \beta)^{-1} = \alpha^{-1} \in R$ so that $\alpha$ is a unit, contradicting our hypothesis. Thus $\alpha \beta \in \mathcal{M}$.

Now suppose $\beta \in \mathcal{M}$ and consider $\alpha + \beta \in R$. If either $\alpha$ or $\beta$ is 0
**Proof:** Let $R$ be a valuation ring of a field and let $\mathcal{M}$ denote the non-units of $R$. Note that $\mathcal{M}$ consists of more than simply the element 0 since otherwise $R = K$.

Let $\alpha \in \mathcal{M}$ and $\beta \in R$. If $\alpha \beta$ is a unit then $\beta(\alpha \beta)^{-1} = \alpha^{-1} \in R$ so that $\alpha$ is a unit, contradicting our hypothesis. Thus $\alpha \beta \in \mathcal{M}$.

Now suppose $\beta \in \mathcal{M}$ and consider $\alpha + \beta \in R$. If either $\alpha$ or $\beta$ is 0 then clearly $\alpha + \beta \in \mathcal{M}$,
Proof: Let $R$ be a valuation ring of a field and let $\mathcal{M}$ denote the non-units of $R$. Note that $\mathcal{M}$ consists of more than simply the element 0 since otherwise $R = K$.

Let $\alpha \in \mathcal{M}$ and $\beta \in R$. If $\alpha\beta$ is a unit then $\beta(\alpha\beta)^{-1} = \alpha^{-1} \in R$ so that $\alpha$ is a unit, contradicting our hypothesis. Thus $\alpha\beta \in \mathcal{M}$.

Now suppose $\beta \in \mathcal{M}$ and consider $\alpha + \beta \in R$. If either $\alpha$ or $\beta$ is 0 then clearly $\alpha + \beta \in \mathcal{M}$, so suppose otherwise.
Proof: Let $R$ be a valuation ring of a field and let $\mathcal{M}$ denote the non-units of $R$. Note that $\mathcal{M}$ consists of more than simply the element 0 since otherwise $R = K$.

Let $\alpha \in \mathcal{M}$ and $\beta \in R$. If $\alpha \beta$ is a unit then $\beta(\alpha \beta)^{-1} = \alpha^{-1} \in R$ so that $\alpha$ is a unit, contradicting our hypothesis. Thus $\alpha \beta \in \mathcal{M}$.

Now suppose $\beta \in \mathcal{M}$ and consider $\alpha + \beta \in R$. If either $\alpha$ or $\beta$ is 0 then clearly $\alpha + \beta \in \mathcal{M}$, so suppose otherwise. Since $R$ is a valuation ring we may assume without loss of generality that $\alpha/\beta \in R$. 
**Proof:** Let $R$ be a valuation ring of a field and let $\mathcal{M}$ denote the non-units of $R$. Note that $\mathcal{M}$ consists of more than simply the element 0 since otherwise $R = K$.

Let $\alpha \in \mathcal{M}$ and $\beta \in R$. If $\alpha \beta$ is a unit then $\beta(\alpha \beta)^{-1} = \alpha^{-1} \in R$ so that $\alpha$ is a unit, contradicting our hypothesis. Thus $\alpha \beta \in \mathcal{M}$.

Now suppose $\beta \in \mathcal{M}$ and consider $\alpha + \beta \in R$. If either $\alpha$ or $\beta$ is 0 then clearly $\alpha + \beta \in \mathcal{M}$, so suppose otherwise. Since $R$ is a valuation ring we may assume without loss of generality that $\alpha/\beta \in R$. Then $1 + (\alpha/\beta) \in R$.
Proof: Let $R$ be a valuation ring of a field and let $\mathcal{M}$ denote the non-units of $R$. Note that $\mathcal{M}$ consists of more than simply the element 0 since otherwise $R = K$.

Let $\alpha \in \mathcal{M}$ and $\beta \in R$. If $\alpha \beta$ is a unit then $\beta(\alpha \beta)^{-1} = \alpha^{-1} \in R$ so that $\alpha$ is a unit, contradicting our hypothesis. Thus $\alpha \beta \in \mathcal{M}$.

Now suppose $\beta \in \mathcal{M}$ and consider $\alpha + \beta \in R$. If either $\alpha$ or $\beta$ is 0 then clearly $\alpha + \beta \in \mathcal{M}$, so suppose otherwise. Since $R$ is a valuation ring we may assume without loss of generality that $\alpha/\beta \in R$. Then $1 + (\alpha/\beta) \in R$ and so $\beta \left(1 + (\alpha/\beta)\right) = \alpha + \beta \in \mathcal{M}$.
**Proof:** Let $R$ be a valuation ring of a field and let $\mathcal{M}$ denote the non-units of $R$. Note that $\mathcal{M}$ consists of more than simply the element 0 since otherwise $R = K$.

Let $\alpha \in \mathcal{M}$ and $\beta \in R$. If $\alpha \beta$ is a unit then $\beta(\alpha \beta)^{-1} = \alpha^{-1} \in R$ so that $\alpha$ is a unit, contradicting our hypothesis. Thus $\alpha \beta \in \mathcal{M}$.

Now suppose $\beta \in \mathcal{M}$ and consider $\alpha + \beta \in R$. If either $\alpha$ or $\beta$ is 0 then clearly $\alpha + \beta \in \mathcal{M}$, so suppose otherwise. Since $R$ is a valuation ring we may assume without loss of generality that $\alpha/\beta \in R$. Then $1 + (\alpha/\beta) \in R$ and so $\beta(1 + (\alpha/\beta)) = \alpha + \beta \in \mathcal{M}$ by what we have already shown.
**Proof:** Let $R$ be a valuation ring of a field and let $\mathcal{M}$ denote the non-units of $R$. Note that $\mathcal{M}$ consists of more than simply the element 0 since otherwise $R = K$.

Let $\alpha \in \mathcal{M}$ and $\beta \in R$. If $\alpha \beta$ is a unit then $\beta(\alpha \beta)^{-1} = \alpha^{-1} \in R$ so that $\alpha$ is a unit, contradicting our hypothesis. Thus $\alpha \beta \notin \mathcal{M}$.

Now suppose $\beta \in \mathcal{M}$ and consider $\alpha + \beta \in R$. If either $\alpha$ or $\beta$ is 0 then clearly $\alpha + \beta \notin \mathcal{M}$, so suppose otherwise. Since $R$ is a valuation ring we may assume without loss of generality that $\alpha/\beta \in R$. Then $1 + (\alpha/\beta) \in R$ and so $\beta(1 + (\alpha/\beta)) = \alpha + \beta \in \mathcal{M}$ by what we have already shown. Thus $\mathcal{M}$ is an ideal.
Proof: Let \( R \) be a valuation ring of a field and let \( M \) denote the non-units of \( R \). Note that \( M \) consists of more than simply the element 0 since otherwise \( R = K \).

Let \( \alpha \in M \) and \( \beta \in R \). If \( \alpha \beta \) is a unit then \( \beta(\alpha \beta)^{-1} = \alpha^{-1} \in R \) so that \( \alpha \) is a unit, contradicting our hypothesis. Thus \( \alpha \beta \in M \).

Now suppose \( \beta \in M \) and consider \( \alpha + \beta \in R \). If either \( \alpha \) or \( \beta \) is 0 then clearly \( \alpha + \beta \in M \), so suppose otherwise. Since \( R \) is a valuation ring we may assume without loss of generality that \( \alpha / \beta \in R \). Then \( 1 + (\alpha / \beta) \in R \) and so \( \beta(1 + (\alpha / \beta)) = \alpha + \beta \in M \) by what we have already shown. Thus \( M \) is an ideal.

It is clearly the unique maximal ideal of \( R \).
Proof: Let $R$ be a valuation ring of a field and let $M$ denote the non-units of $R$. Note that $M$ consists of more than simply the element 0 since otherwise $R = K$.

Let $\alpha \in M$ and $\beta \in R$. If $\alpha \beta$ is a unit then $\beta(\alpha \beta)^{-1} = \alpha^{-1} \in R$ so that $\alpha$ is a unit, contradicting our hypothesis. Thus $\alpha \beta \in M$.

Now suppose $\beta \in M$ and consider $\alpha + \beta \in R$. If either $\alpha$ or $\beta$ is 0 then clearly $\alpha + \beta \in M$, so suppose otherwise. Since $R$ is a valuation ring we may assume without loss of generality that $\alpha/\beta \in R$. Then $1 + (\alpha/\beta) \in R$ and so $\beta(1 + (\alpha/\beta)) = \alpha + \beta \in M$ by what we have already shown. Thus $M$ is an ideal.

It is clearly the unique maximal ideal of $R$ since any ideal not properly contained in $M$ must contain a unit,
**Proof:** Let $R$ be a valuation ring of a field and let $\mathcal{M}$ denote the non-units of $R$. Note that $\mathcal{M}$ consists of more than simply the element 0 since otherwise $R = K$.

Let $\alpha \in \mathcal{M}$ and $\beta \in R$. If $\alpha \beta$ is a unit then $\beta(\alpha \beta)^{-1} = \alpha^{-1} \in R$ so that $\alpha$ is a unit, contradicting our hypothesis. Thus $\alpha \beta \in \mathcal{M}$.

Now suppose $\beta \in \mathcal{M}$ and consider $\alpha + \beta \in R$. If either $\alpha$ or $\beta$ is 0 then clearly $\alpha + \beta \in \mathcal{M}$, so suppose otherwise. Since $R$ is a valuation ring we may assume without loss of generality that $\alpha/\beta \in R$. Then $1 + (\alpha/\beta) \in R$ and so $\beta(1 + (\alpha/\beta)) = \alpha + \beta \in \mathcal{M}$ by what we have already shown. Thus $\mathcal{M}$ is an ideal.

It is clearly the unique maximal ideal of $R$ since any ideal not properly contained in $\mathcal{M}$ must contain a unit, whence must be the entire ring.
Lemma (2)

Suppose $R$ is a valuation ring with the property that, given any principal ideal $\alpha R \neq \{0\}$, the number of principal ideals in an ascending chain $\alpha R \subseteq \beta R \subseteq \cdots$ is bounded by a function of $\alpha$. Then $R$ is a principal ideal domain.

Proof:
Let $R$ be a valuation ring. By Lemma 1 it is a local ring; denote the maximal ideal by $M$ and let $\alpha_1 \in M$. If $M$ is not principal there is an $\alpha_2 \in M$ that isn't in the principal ideal generated by $\alpha_1$. This implies that $\alpha_2 / \alpha_1 \not\in R$, so that its inverse $\alpha_1 / \alpha_2 \in R$. Obviously this element isn't a unit, hence $\alpha_1 R \subset \alpha_2 R$. We repeat this process, getting an infinite ascending chain of principal ideals $\alpha_1 R \subset \alpha_2 R \subset \cdots$ which contradicts the hypothesis on $R$. Thus $M$ is principal. Write $M = \pi R$. 
<table>
<thead>
<tr>
<th>Lemma (2)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Suppose</strong> $R$ is a valuation ring with the property that,</td>
</tr>
</tbody>
</table>

Let $R$ be a valuation ring. By Lemma 1, it is a local ring; denote the maximal ideal by $M$ and let $\alpha_1 \in M$. If $M$ is not principal, there is an $\alpha_2 \in M$ that isn’t in the principal ideal generated by $\alpha_1$. This implies that $\alpha_2/\alpha_1 \not\in R$, so that its inverse $\alpha_1/\alpha_2 \in R$. Obviously, this element isn’t a unit, hence $\alpha_1 \subseteq \alpha_2 \subseteq \cdots$ which contradicts the hypothesis on $R$. Thus $M$ is principal. Write $M = \pi R$. 

Math 681, Wednesday, February 24
Lemma (2)

Suppose $R$ is a valuation ring with the property that, given any principal ideal $\alpha R \neq \{0\}$,
Lemma (2)

Suppose $R$ is a valuation ring with the property that, given any principal ideal $\alpha R \neq \{0\}$, the number of principal ideals in an ascending chain

$$\alpha R \subsetneq \beta R \subsetneq \cdots$$

is bounded by a function of $\alpha$. Then $R$ is a principal ideal domain.

Proof:

Let $R$ be a valuation ring. By Lemma 1 it is a local ring; denote the maximal ideal by $M$ and let $\alpha_1 \in M$. If $M$ is not principal there is an $\alpha_2 \in M$ that isn't in the principal ideal generated by $\alpha_1$. This implies that $\alpha_2/\alpha_1 \not\in R$, so that its inverse $\alpha_1/\alpha_2 \in R$. Obviously this element isn't a unit, hence $\alpha_1 R \subsetneq \alpha_2 R \subsetneq \cdots$ which contradicts the hypothesis on $R$. Thus $M$ is principal. Write $M = \pi R$. 

Math 681, Wednesday, February 24
Lemma (2)

Suppose $R$ is a valuation ring with the property that, given any principal ideal $\alpha R \neq \{0\}$, the number of principal ideals in an ascending chain

$$\alpha R \subsetneq \beta R \subsetneq \cdots$$

is bounded by a function of $\alpha$. 

Proof:
Let $R$ be a valuation ring. By Lemma 1 it is a local ring; denote the maximal ideal by $M$ and let $\alpha_1 \in M$.

If $M$ is not principal there is an $\alpha_2 \in M$ that isn't in the principal ideal generated by $\alpha_1$.

This implies that $\alpha_2/\alpha_1 \not\in R$, so that its inverse $\alpha_1/\alpha_2 \in R$.

Obviously this element isn't a unit, hence $\alpha_1 R \subsetneq \alpha_2 R \subsetneq \cdots$

We repeat this process, getting an infinite ascending chain of principal ideals $\alpha_1 R \subsetneq \alpha_2 R \subsetneq \cdots$ which contradicts the hypothesis on $R$.

Thus $M$ is principal.

Write $M = \pi R$. 

Math 681, Wednesday, February 24 2021
Lemma (2)

Suppose $R$ is a valuation ring with the property that, given any principal ideal $\alpha R \neq \{0\}$, the number of principal ideals in an ascending chain

$$\alpha R \subsetneq \beta R \subsetneq \cdots$$

is bounded by a function of $\alpha$. Then $R$ is a principal ideal domain.
Lemma (2)

Suppose $R$ is a valuation ring with the property that, given any principal ideal $\alpha R \neq \{0\}$, the number of principal ideals in an ascending chain

$$
\alpha R \subsetneq \beta R \subsetneq \cdots
$$

is bounded by a function of $\alpha$. Then $R$ is a principal ideal domain.

Proof:
Lemma (2)

Suppose $R$ is a valuation ring with the property that, given any principal ideal $\alpha R \neq \{0\}$, the number of principal ideals in an ascending chain

$$\alpha R \subsetneq \beta R \subsetneq \cdots$$

is bounded by a function of $\alpha$. Then $R$ is a principal ideal domain.

Proof: Let $R$ be a valuation ring.
Lemma (2)

Suppose $R$ is a valuation ring with the property that, given any principal ideal $\alpha R \neq \{0\}$, the number of principal ideals in an ascending chain

$$\alpha R \subsetneq \beta R \subsetneq \cdots$$

is bounded by a function of $\alpha$. Then $R$ is a principal ideal domain.

**Proof:** Let $R$ be a valuation ring. By Lemma 1 it is a local ring;
Lemma (2)

Suppose \( R \) is a valuation ring with the property that, given any principal ideal \( \alpha R \neq \{0\} \), the number of principal ideals in an ascending chain

\[
\alpha R \subsetneq \beta R \subsetneq \cdots
\]

is bounded by a function of \( \alpha \). Then \( R \) is a principal ideal domain.

Proof: Let \( R \) be a valuation ring. By Lemma 1 it is a local ring; denote the maximal ideal by \( M \) and let \( \alpha_1 \in M \).
Lemma (2)

Suppose $R$ is a valuation ring with the property that, given any principal ideal $\alpha R \neq \{0\}$, the number of principal ideals in an ascending chain

$$\alpha R \subsetneq \beta R \subsetneq \cdots$$

is bounded by a function of $\alpha$. Then $R$ is a principal ideal domain.

**Proof:** Let $R$ be a valuation ring. By Lemma 1 it is a local ring; denote the maximal ideal by $\mathcal{M}$ and let $\alpha_1 \in \mathcal{M}$.

If $\mathcal{M}$ is not principal
Lemma (2)

Suppose \( R \) is a valuation ring with the property that, given any principal ideal \( \alpha R \neq \{0\} \), the number of principal ideals in an ascending chain

\[
\alpha R \subsetneq \beta R \subsetneq \cdots
\]
is bounded by a function of \( \alpha \). Then \( R \) is a principal ideal domain.

Proof: Let \( R \) be a valuation ring. By Lemma 1 it is a local ring; denote the maximal ideal by \( M \) and let \( \alpha_1 \in M \).

If \( M \) is not principal there is an \( \alpha_2 \in M \) that isn’t in the principal ideal generated by \( \alpha_1 \).
Lemma (2)

Suppose $R$ is a valuation ring with the property that, given any principal ideal $\alpha R \neq \{0\}$, the number of principal ideals in an ascending chain

$$\alpha R \subsetneq \beta R \subsetneq \cdots$$

is bounded by a function of $\alpha$. Then $R$ is a principal ideal domain.

Proof: Let $R$ be a valuation ring. By Lemma 1 it is a local ring; denote the maximal ideal by $M$ and let $\alpha_1 \in M$.

If $M$ is not principal there is an $\alpha_2 \in M$ that isn’t in the principal ideal generated by $\alpha_1$. This implies that $\alpha_2/\alpha_1 \notin R$, 

Lemma (2)

Suppose $R$ is a valuation ring with the property that, given any principal ideal $\alpha R \neq \{0\}$, the number of principal ideals in an ascending chain

$$\alpha R \subsetneq \beta R \subsetneq \cdots$$

is bounded by a function of $\alpha$. Then $R$ is a principal ideal domain.

**Proof:** Let $R$ be a valuation ring. By Lemma 1 it is a local ring; denote the maximal ideal by $M$ and let $\alpha_1 \in M$.

If $M$ is not principal there is an $\alpha_2 \in M$ that isn’t in the principal ideal generated by $\alpha_1$. This implies that $\alpha_2/\alpha_1 \notin R$, so that its inverse $\alpha_1/\alpha_2 \in R$. 

Math 681, Wednesday, February 24

February 24, 2021
Lemma (2)

Suppose $R$ is a valuation ring with the property that, given any principal ideal $\alpha R \neq \{0\}$, the number of principal ideals in an ascending chain

$$\alpha R \subsetneq \beta R \subsetneq \cdots$$

is bounded by a function of $\alpha$. Then $R$ is a principal ideal domain.

Proof: Let $R$ be a valuation ring. By Lemma 1 it is a local ring; denote the maximal ideal by $M$ and let $\alpha_1 \in M$.

If $M$ is not principal there is an $\alpha_2 \in M$ that isn’t in the principal ideal generated by $\alpha_1$. This implies that $\alpha_2/\alpha_1 \notin R$, so that its inverse $\alpha_1/\alpha_2 \in R$. Obviously this element isn’t a unit,
Lemma (2)

Suppose $R$ is a valuation ring with the property that, given any principal ideal $\alpha R \neq \{0\}$, the number of principal ideals in an ascending chain

$$\alpha R \subsetneq \beta R \subsetneq \cdots$$

is bounded by a function of $\alpha$. Then $R$ is a principal ideal domain.

**Proof:** Let $R$ be a valuation ring. By Lemma 1 it is a local ring; denote the maximal ideal by $M$ and let $\alpha_1 \in M$.

If $M$ is not principal there is an $\alpha_2 \in M$ that isn’t in the principal ideal generated by $\alpha_1$. This implies that $\alpha_2/\alpha_1 \notin R$, so that its inverse $\alpha_1/\alpha_2 \in R$. Obviously this element isn’t a unit, hence $\alpha_1 R \subsetneq \alpha_2 R$. 
Lemma (2)

Suppose $R$ is a valuation ring with the property that, given any principal ideal $\alpha R \neq \{0\}$, the number of principal ideals in an ascending chain

$$\alpha R \subsetneq \beta R \subsetneq \cdots$$

is bounded by a function of $\alpha$. Then $R$ is a principal ideal domain.

**Proof:** Let $R$ be a valuation ring. By Lemma 1 it is a local ring; denote the maximal ideal by $\mathcal{M}$ and let $\alpha_1 \in \mathcal{M}$.

If $\mathcal{M}$ is not principal there is an $\alpha_2 \in \mathcal{M}$ that isn’t in the principal ideal generated by $\alpha_1$. This implies that $\alpha_2/\alpha_1 \notin R$, so that its inverse $\alpha_1/\alpha_2 \in R$. Obviously this element isn’t a unit, hence $\alpha_1 R \subsetneq \alpha_2 R$.

We repeat this process, getting an infinite ascending chain of principal ideals.
Lemma (2)

*Suppose* \( R \) *is a valuation ring with the property that, given any principal ideal* \( \alpha R \neq \{0\} \), *the number of principal ideals in an ascending chain*

\[
\alpha R \subsetneq \beta R \subsetneq \cdots
\]

*is bounded by a function of* \( \alpha \). *Then* \( R \) *is a principal ideal domain.*

**Proof:** Let \( R \) *be a valuation ring. By Lemma 1 it is a local ring; denote the maximal ideal by* \( \mathcal{M} \) *and let* \( \alpha_1 \in \mathcal{M} \).

If \( \mathcal{M} \) is not principal there is an \( \alpha_2 \in \mathcal{M} \) that isn’t in the principal ideal generated by \( \alpha_1 \). This implies that \( \alpha_2/\alpha_1 \notin R \), so that its inverse \( \alpha_1/\alpha_2 \in R \). Obviously this element isn’t a unit, hence \( \alpha_1 R \subsetneq \alpha_2 R \).

We repeat this process, getting an infinite ascending chain of principal ideals

\[
\alpha_1 R \subsetneq \alpha_2 R \subsetneq \cdots
\]
Lemma (2)

Suppose $R$ is a valuation ring with the property that, given any principal ideal $\alpha R \neq \{0\}$, the number of principal ideals in an ascending chain

$$\alpha R \subsetneq \beta R \subsetneq \cdots$$

is bounded by a function of $\alpha$. Then $R$ is a principal ideal domain.

Proof: Let $R$ be a valuation ring. By Lemma 1 it is a local ring; denote the maximal ideal by $M$ and let $\alpha_1 \in M$.

If $M$ is not principal there is an $\alpha_2 \in M$ that isn’t in the principal ideal generated by $\alpha_1$. This implies that $\alpha_2/\alpha_1 \not\in R$, so that its inverse $\alpha_1/\alpha_2 \in R$. Obviously this element isn’t a unit, hence $\alpha_1 R \subsetneq \alpha_2 R$.

We repeat this process, getting an infinite ascending chain of principal ideals

$$\alpha_1 R \subsetneq \alpha_2 R \subsetneq \cdots$$

which contradicts the hypothesis on $R$. 
Lemma (2)

Suppose $R$ is a valuation ring with the property that, given any principal ideal $\alpha R \neq \{0\}$, the number of principal ideals in an ascending chain

$$\alpha R \subsetneq \beta R \subsetneq \cdots$$

is bounded by a function of $\alpha$. Then $R$ is a principal ideal domain.

Proof: Let $R$ be a valuation ring. By Lemma 1 it is a local ring; denote the maximal ideal by $\mathcal{M}$ and let $\alpha_1 \in \mathcal{M}$.

If $\mathcal{M}$ is not principal there is an $\alpha_2 \in \mathcal{M}$ that isn’t in the principal ideal generated by $\alpha_1$. This implies that $\alpha_2/\alpha_1 \notin R$, so that its inverse $\alpha_1/\alpha_2 \in R$. Obviously this element isn’t a unit, hence $\alpha_1 R \subsetneq \alpha_2 R$.

We repeat this process, getting an infinite ascending chain of principal ideals

$$\alpha_1 R \subsetneq \alpha_2 R \subsetneq \cdots$$

which contradicts the hypothesis on $R$. Thus $\mathcal{M}$ is principal.
Lemma (2)

Suppose $R$ is a valuation ring with the property that, given any principal ideal $\alpha R \neq \{0\}$, the number of principal ideals in an ascending chain

$$\alpha R \subsetneq \beta R \subsetneq \cdots$$

is bounded by a function of $\alpha$. Then $R$ is a principal ideal domain.

**Proof:** Let $R$ be a valuation ring. By Lemma 1 it is a local ring; denote the maximal ideal by $\mathcal{M}$ and let $\alpha_1 \in \mathcal{M}$.

If $\mathcal{M}$ is not principal there is an $\alpha_2 \in \mathcal{M}$ that isn’t in the principal ideal generated by $\alpha_1$. This implies that $\alpha_2/\alpha_1 \notin R$, so that its inverse $\alpha_1/\alpha_2 \in R$. Obviously this element isn’t a unit, hence $\alpha_1 R \subsetneq \alpha_2 R$.

We repeat this process, getting an infinite ascending chain of principal ideals

$$\alpha_1 R \subsetneq \alpha_2 R \subsetneq \cdots$$

which contradicts the hypothesis on $R$. Thus $\mathcal{M}$ is principal. Write $\mathcal{M} = \pi R$. 
We claim that every non-zero \( \alpha \in R \) has a unique representation of the form

\[ \alpha = u \pi^n \]

for some unit \( u \) and non-negative integer \( n \).

This is obvious if \( \alpha \) is a unit itself, so suppose \( \alpha \in M \). Then \( \alpha = \pi^m \beta \) for some \( \beta \in R \) not zero. If \( \beta \) is a unit, then we have such a representation of \( \alpha \), and any such representation is clearly unique.

If \( \beta \in M \), by hypothesis the number of principal ideals in an ascending chain \( \alpha R \subseteq \pi^m R \subseteq \pi^{m-1} R \subseteq \cdots \subseteq \pi R \) is bounded by a function of \( \alpha \) so that there is a maximal exponent \( m \) such that \( \alpha \in \pi^m R \).

Since \( \alpha \not\in \pi^{m+1} R \) we see that \( \alpha = u \pi^m \) for some \( u \not\in \pi R = M \), so that \( u \) is a unit.

Finally, we show that all ideals are principal. Let \( I \) be a non-zero ideal contained in \( M \) (otherwise it is trivially principal). By the above, every non-zero element \( \alpha \in I \) is of the form \( \alpha = u \pi^m \) for some unit and some non-negative integer \( m \).

Let \( m_0 \) be the least such integer occurring here and choose \( \alpha_0 \in I \) of the form \( \alpha_0 = u_0 \pi^{m_0} \) for some unit \( u_0 \).

Then \( \alpha_0 R = \pi^{m_0} R \) and all non-zero \( \alpha \in I \) satisfy \( \alpha = u \pi^m \in \pi^{m_0} R \) since \( m \geq m_0 \) by construction.

Therefore \( I = \alpha_0 R \).
We claim that every non-zero $\alpha \in R$ has a unique representation of the form $\alpha = u \pi^n$ for some unit $u$ and non-negative integer $n$. 
We claim that every non-zero $\alpha \in R$ has a unique representation of the form $\alpha = u\pi^n$ for some unit $u$ and non-negative integer $n$. This is obvious if $\alpha$ is a unit itself,
We claim that every non-zero $\alpha \in R$ has a unique representation of the form $\alpha = u\pi^n$ for some unit $u$ and non-negative integer $n$. This is obvious if $\alpha$ is a unit itself, so suppose $\alpha \in M$. 

Then $\alpha = \pi^m \beta$ for some $\beta \in R$ not zero. If $\beta$ is a unit, then we have such a representation of $\alpha$, and any such representation is clearly unique. If $\beta \in M$, by hypothesis the number of principal ideals in an ascending chain $\alpha R \subseteq \pi^m R \subseteq \pi^{m-1} R \subseteq \cdots \subseteq \pi R$ is bounded by a function of $\alpha$ so that there is a maximal exponent $m$ such that $\alpha \in \pi^m R$. Since $\alpha \not\in \pi^{m+1} R$ we see that $\alpha = u\pi^m$ for some $u \not\in \pi R = M$, so that $u$ is a unit.

Finally, we show that all ideals are principal. Let $I$ be a non-zero ideal contained in $M$ (otherwise it is trivially principal). By the above, every non-zero element $\alpha \in I$ is of the form $u\pi^m$ for some unit and some non-negative integer $m$. Let $m_0$ be the least such integer occurring here and choose $\alpha_0 \in I$ of the form $\alpha_0 = u_0\pi^{m_0}$ for some unit $u_0$. Then $\alpha_0 R = \pi^{m_0} R$ and all non-zero $\alpha \in I$ satisfy $\alpha = u\pi^m \in \pi^{m_0} R$ since $m \geq m_0$ by construction. Therefore $I = \alpha_0 R$. 

Math 681, Wednesday, February 24
We claim that every non-zero $\alpha \in R$ has a unique representation of the form $\alpha = u\pi^n$ for some unit $u$ and non-negative integer $n$. This is obvious if $\alpha$ is a unit itself, so suppose $\alpha \in \mathcal{M}$. Then $\alpha = \pi^m\beta$ for some $\beta \in R$ not zero.
We claim that every non-zero $\alpha \in R$ has a unique representation of the form $\alpha = u\pi^n$ for some unit $u$ and non-negative integer $n$. This is obvious if $\alpha$ is a unit itself, so suppose $\alpha \in \mathcal{M}$. Then $\alpha = \pi^m\beta$ for some $\beta \in R$ not zero. If $\beta$ is a unit,
We claim that every non-zero $\alpha \in R$ has a unique representation of the form $\alpha = u\pi^n$ for some unit $u$ and non-negative integer $n$. This is obvious if $\alpha$ is a unit itself, so suppose $\alpha \in M$. Then $\alpha = \pi^m\beta$ for some $\beta \in R$ not zero. If $\beta$ is a unit, then we have such a representation of $\alpha$,
We claim that every non-zero \( \alpha \in R \) has a unique representation of the form \( \alpha = u\pi^n \) for some unit \( u \) and non-negative integer \( n \). This is obvious if \( \alpha \) is a unit itself, so suppose \( \alpha \in \mathfrak{M} \). Then \( \alpha = \pi^m \beta \) for some \( \beta \in R \) not zero. If \( \beta \) is a unit, then we have such a representation of \( \alpha \), and any such representation is clearly unique.
We claim that every non-zero $\alpha \in R$ has a unique representation of the form $\alpha = u\pi^n$ for some unit $u$ and non-negative integer $n$. This is obvious if $\alpha$ is a unit itself, so suppose $\alpha \in M$. Then $\alpha = \pi^m\beta$ for some $\beta \in R$ not zero. If $\beta$ is a unit, then we have such a representation of $\alpha$, and any such representation is clearly unique. If $\beta \in M$,
We claim that every non-zero $\alpha \in R$ has a unique representation of the form $\alpha = u\pi^n$ for some unit $u$ and non-negative integer $n$. This is obvious if $\alpha$ is a unit itself, so suppose $\alpha \in M$. Then $\alpha = \pi^m \beta$ for some $\beta \in R$ not zero. If $\beta$ is a unit, then we have such a representation of $\alpha$, and any such representation is clearly unique. If $\beta \in M$, by hypothesis the number of principal ideals in an ascending chain

$$\alpha R \subsetneq \pi^m R \subsetneq \pi^{m-1} R \subsetneq \cdots \subsetneq \pi R$$
We claim that every non-zero $\alpha \in R$ has a unique representation of the form $\alpha = u\pi^n$ for some unit $u$ and non-negative integer $n$. This is obvious if $\alpha$ is a unit itself, so suppose $\alpha \in M$. Then $\alpha = \pi^m \beta$ for some $\beta \in R$ not zero. If $\beta$ is a unit, then we have such a representation of $\alpha$, and any such representation is clearly unique. If $\beta \in M$, by hypothesis the number of principal ideals in an ascending chain

$$\alpha R \subsetneq \pi^m R \subsetneq \pi^{m-1} R \subsetneq \cdots \subsetneq \pi R$$

is bounded by a function of $\alpha$
We claim that every non-zero \( \alpha \in R \) has a unique representation of the form \( \alpha = u \pi^n \) for some unit \( u \) and non-negative integer \( n \). This is obvious if \( \alpha \) is a unit itself, so suppose \( \alpha \in \mathcal{M} \). Then \( \alpha = \pi^m \beta \) for some \( \beta \in R \) not zero. If \( \beta \) is a unit, then we have such a representation of \( \alpha \), and any such representation is clearly unique. If \( \beta \in \mathcal{M} \), by hypothesis the number of principal ideals in an ascending chain

\[
\alpha R \subsetneq \pi^m R \subsetneq \pi^{m-1} R \subsetneq \cdots \subsetneq \pi R
\]

is bounded by a function of \( \alpha \) so that there is a maximal exponent \( m \)
We claim that every non-zero $\alpha \in R$ has a unique representation of the form $\alpha = u\pi^n$ for some unit $u$ and non-negative integer $n$. This is obvious if $\alpha$ is a unit itself, so suppose $\alpha \in \mathcal{M}$. Then $\alpha = \pi^m \beta$ for some $\beta \in R$ not zero. If $\beta$ is a unit, then we have such a representation of $\alpha$, and any such representation is clearly unique. If $\beta \in \mathcal{M}$, by hypothesis the number of principal ideals in an ascending chain

$$\alpha R \subsetneq \pi^m R \subsetneq \pi^{m-1} R \subsetneq \cdots \subsetneq \pi R$$

is bounded by a function of $\alpha$ so that there is a maximal exponent $m$ such that $\alpha \in \pi^m R$. 

Finally, we show that all ideals are principal. Let $I$ be a non-zero ideal contained in $\mathcal{M}$ (otherwise it is trivially principal). By the above, every non-zero element $\alpha \in I$ is of the form $u\pi^m$ for some unit and some non-negative integer $m$. Let $m_0$ be the least such integer occurring here and choose $\alpha_0 \in I$ of the form $\alpha_0 = u_0\pi^{m_0}$ for some unit $u_0$. Then $\alpha_0 R = \pi^{m_0} R$ and all non-zero $\alpha \in I$ satisfy $\alpha = u\pi^m \in \pi^{m_0} R$ since $m \geq m_0$ by construction. Therefore $I = \alpha_0 R$. 

Math 681, Wednesday, February 24 February 24, 2021
We claim that every non-zero $\alpha \in R$ has a unique representation of the form $\alpha = u\pi^n$ for some unit $u$ and non-negative integer $n$. This is obvious if $\alpha$ is a unit itself, so suppose $\alpha \in \mathcal{M}$. Then $\alpha = \pi^m \beta$ for some $\beta \in R$ not zero. If $\beta$ is a unit, then we have such a representation of $\alpha$, and any such representation is clearly unique. If $\beta \in \mathcal{M}$, by hypothesis the number of principal ideals in an ascending chain

$$\alpha R \subsetneq \pi^m R \subsetneq \pi^{m-1} R \subsetneq \cdots \subsetneq \pi R$$

is bounded by a function of $\alpha$ so that there is a maximal exponent $m$ such that $\alpha \in \pi^m R$. Since $\alpha \notin \pi^{m+1} R$
We claim that every non-zero $\alpha \in R$ has a unique representation of the form $\alpha = u\pi^n$ for some unit $u$ and non-negative integer $n$. This is obvious if $\alpha$ is a unit itself, so suppose $\alpha \in M$. Then $\alpha = \pi^m \beta$ for some $\beta \in R$ not zero. If $\beta$ is a unit, then we have such a representation of $\alpha$, and any such representation is clearly unique. If $\beta \in M$, by hypothesis the number of principal ideals in an ascending chain

$$\alpha R \subsetneq \pi^m R \subsetneq \pi^{m-1} R \subsetneq \cdots \subsetneq \pi R$$

is bounded by a function of $\alpha$ so that there is a maximal exponent $m$ such that $\alpha \in \pi^m R$. Since $\alpha \not\subseteq \pi^{m+1} R$ we see that $\alpha = u\pi^m$ for some $u \not\in \pi R = M$, 


We claim that every non-zero $\alpha \in R$ has a unique representation of the form $\alpha = u\pi^n$ for some unit $u$ and non-negative integer $n$. This is obvious if $\alpha$ is a unit itself, so suppose $\alpha \in \mathbb{M}$. Then $\alpha = \pi^m\beta$ for some $\beta \in R$ not zero. If $\beta$ is a unit, then we have such a representation of $\alpha$, and any such representation is clearly unique. If $\beta \in \mathbb{M}$, by hypothesis the number of principal ideals in an ascending chain

$$\alpha R \not\subseteq \pi^m R \not\subseteq \pi^{m-1} R \not\subseteq \cdots \not\subseteq \pi R$$

is bounded by a function of $\alpha$ so that there is a maximal exponent $m$ such that $\alpha \in \pi^m R$. Since $\alpha \not\in \pi^{m+1} R$ we see that $\alpha = u\pi^m$ for some $u \notin \pi R = \mathbb{M}$, so that $u$ is a unit.
We claim that every non-zero $\alpha \in R$ has a unique representation of the form $\alpha = u\pi^n$ for some unit $u$ and non-negative integer $n$. This is obvious if $\alpha$ is a unit itself, so suppose $\alpha \in \mathcal{M}$. Then $\alpha = \pi^m \beta$ for some $\beta \in R$ not zero. If $\beta$ is a unit, then we have such a representation of $\alpha$, and any such representation is clearly unique. If $\beta \in \mathcal{M}$, by hypothesis the number of principal ideals in an ascending chain

$$\alpha R \subsetneq \pi^m R \subsetneq \pi^{m-1} R \subsetneq \cdots \subsetneq \pi R$$

is bounded by a function of $\alpha$ so that there is a maximal exponent $m$ such that $\alpha \in \pi^m R$. Since $\alpha \notin \pi^{m+1} R$ we see that $\alpha = u\pi^m$ for some $u \notin \pi R = \mathcal{M}$, so that $u$ is a unit.

Finally, we show that all ideals are principal.
We claim that every non-zero $\alpha \in R$ has a unique representation of the form $\alpha = u\pi^n$ for some unit $u$ and non-negative integer $n$. This is obvious if $\alpha$ is a unit itself, so suppose $\alpha \in M$. Then $\alpha = \pi^m \beta$ for some $\beta \in R$ not zero. If $\beta$ is a unit, then we have such a representation of $\alpha$, and any such representation is clearly unique. If $\beta \in M$, by hypothesis the number of principal ideals in an ascending chain

$$\alpha R \subsetneq \pi^m R \subsetneq \pi^{m-1} R \subsetneq \cdots \subsetneq \pi R$$

is bounded by a function of $\alpha$ so that there is a maximal exponent $m$ such that $\alpha \in \pi^m R$. Since $\alpha \not\in \pi^{m+1} R$ we see that $\alpha = u\pi^m$ for some $u \not\in \pi R = M$, so that $u$ is a unit.

Finally, we show that all ideals are principal.

Let $I$ be a non-zero ideal contained in $M$
We claim that every non-zero $\alpha \in R$ has a unique representation of the form $\alpha = u\pi^n$ for some unit $u$ and non-negative integer $n$. This is obvious if $\alpha$ is a unit itself, so suppose $\alpha \in \mathcal{M}$. Then $\alpha = \pi^m \beta$ for some $\beta \in R$ not zero. If $\beta$ is a unit, then we have such a representation of $\alpha$, and any such representation is clearly unique. If $\beta \in \mathcal{M}$, by hypothesis the number of principal ideals in an ascending chain

$$\alpha R \subsetneq \pi^m R \subsetneq \pi^{m-1} R \subsetneq \cdots \subsetneq \pi R$$

is bounded by a function of $\alpha$ so that there is a maximal exponent $m$ such that $\alpha \in \pi^m R$. Since $\alpha \notin \pi^{m+1} R$ we see that $\alpha = u\pi^m$ for some $u \notin \pi R = \mathcal{M}$, so that $u$ is a unit.

Finally, we show that all ideals are principal.

Let $I$ be a non-zero ideal contained in $\mathcal{M}$ (otherwise it is trivially principal).
We claim that every non-zero \( \alpha \in R \) has a unique representation of the form \( \alpha = u\pi^n \) for some unit \( u \) and non-negative integer \( n \). This is obvious if \( \alpha \) is a unit itself, so suppose \( \alpha \in \mathcal{M} \). Then \( \alpha = \pi^m\beta \) for some \( \beta \in R \) not zero. If \( \beta \) is a unit, then we have such a representation of \( \alpha \), and any such representation is clearly unique. If \( \beta \in \mathcal{M} \), by hypothesis the number of principal ideals in an ascending chain

\[
\alpha R \not\subseteq \pi^m R \not\subseteq \pi^{m-1} R \not\subseteq \cdots \not\subseteq \pi R
\]

is bounded by a function of \( \alpha \) so that there is a maximal exponent \( m \) such that \( \alpha \in \pi^m R \). Since \( \alpha \not\in \pi^{m+1} R \) we see that \( \alpha = u\pi^m \) for some \( u \not\in \pi R = \mathcal{M} \), so that \( u \) is a unit.

Finally, we show that all ideals are principal.

Let \( I \) be a non-zero ideal contained in \( \mathcal{M} \) (otherwise it is trivially principal). By the above,
We claim that every non-zero $\alpha \in R$ has a unique representation of the form $\alpha = u\pi^n$ for some unit $u$ and non-negative integer $n$. This is obvious if $\alpha$ is a unit itself, so suppose $\alpha \in \mathcal{M}$. Then $\alpha = \pi^m\beta$ for some $\beta \in R$ not zero. If $\beta$ is a unit, then we have such a representation of $\alpha$, and any such representation is clearly unique. If $\beta \in \mathcal{M}$, by hypothesis the number of principal ideals in an ascending chain

$$\alpha R \subsetneq \pi^m R \subsetneq \pi^{m-1} R \subsetneq \cdots \subsetneq \pi R$$

is bounded by a function of $\alpha$ so that there is a maximal exponent $m$ such that $\alpha \in \pi^m R$. Since $\alpha \not\in \pi^{m+1} R$ we see that $\alpha = u\pi^m$ for some $u \not\in \pi R = \mathcal{M}$, so that $u$ is a unit.

Finally, we show that all ideals are principal.

Let $I$ be a non-zero ideal contained in $\mathcal{M}$ (otherwise it is trivially principal). By the above, every non-zero element $\alpha \in I$ is of the form $u\pi^m$ for some unit and some non-negative integer $m$. 
We claim that every non-zero $\alpha \in R$ has a unique representation of the form $\alpha = u\pi^n$ for some unit $u$ and non-negative integer $n$. This is obvious if $\alpha$ is a unit itself, so suppose $\alpha \in \mathcal{M}$. Then $\alpha = \pi^m \beta$ for some $\beta \in R$ not zero. If $\beta$ is a unit, then we have such a representation of $\alpha$, and any such representation is clearly unique. If $\beta \in \mathcal{M}$, by hypothesis the number of principal ideals in an ascending chain

\[ \alpha R \subsetneq \pi^m R \subsetneq \pi^{m-1} R \subsetneq \cdots \subsetneq \pi R \]

is bounded by a function of $\alpha$ so that there is a maximal exponent $m$ such that $\alpha \in \pi^m R$. Since $\alpha \notin \pi^{m+1} R$ we see that $\alpha = u\pi^m$ for some $u \notin \pi R = \mathcal{M}$, so that $u$ is a unit.

Finally, we show that all ideals are principal.

Let $I$ be a non-zero ideal contained in $\mathcal{M}$ (otherwise it is trivially principal). By the above, every non-zero element $\alpha \in I$ is of the form $u\pi^m$ for some unit and some non-negative integer $m$. Let $m_0$ be the least such integer occurring here.
We claim that every non-zero $\alpha \in R$ has a unique representation of the form $\alpha = u \pi^n$ for some unit $u$ and non-negative integer $n$. This is obvious if $\alpha$ is a unit itself, so suppose $\alpha \in \mathcal{M}$. Then $\alpha = \pi^m \beta$ for some $\beta \in R$ not zero. If $\beta$ is a unit, then we have such a representation of $\alpha$, and any such representation is clearly unique. If $\beta \in \mathcal{M}$, by hypothesis the number of principal ideals in an ascending chain

$$\alpha R \subsetneq \pi^m R \subsetneq \pi^{m-1} R \subsetneq \cdots \subsetneq \pi R$$

is bounded by a function of $\alpha$ so that there is a maximal exponent $m$ such that $\alpha \in \pi^m R$. Since $\alpha \not\in \pi^{m+1} R$ we see that $\alpha = u \pi^m$ for some $u \not\in \pi R = \mathcal{M}$, so that $u$ is a unit.

Finally, we show that all ideals are principal.

Let $I$ be a non-zero ideal contained in $\mathcal{M}$ (otherwise it is trivially principal). By the above, every non-zero element $\alpha \in I$ is of the form $u \pi^m$ for some unit and some non-negative integer $m$. Let $m_0$ be the least such integer occurring here and choose $\alpha_0 \in I$ of the form $\alpha_0 = u_0 \pi^{m_0}$ for some unit $u_0$. 
We claim that every non-zero $\alpha \in R$ has a unique representation of the form $\alpha = u\pi^n$ for some unit $u$ and non-negative integer $n$. This is obvious if $\alpha$ is a unit itself, so suppose $\alpha \in M$. Then $\alpha = \pi^m \beta$ for some $\beta \in R$ not zero. If $\beta$ is a unit, then we have such a representation of $\alpha$, and any such representation is clearly unique. If $\beta \in M$, by hypothesis the number of principal ideals in an ascending chain

$$\alpha R \subsetneq \pi^m R \subsetneq \pi^{m-1} R \subsetneq \cdots \subsetneq \pi R$$

is bounded by a function of $\alpha$ so that there is a maximal exponent $m$ such that $\alpha \in \pi^m R$. Since $\alpha \notin \pi^{m+1} R$ we see that $\alpha = u\pi^m$ for some $u \notin \pi R = M$, so that $u$ is a unit.

Finally, we show that all ideals are principal.

Let $I$ be a non-zero ideal contained in $M$ (otherwise it is trivially principal). By the above, every non-zero element $\alpha \in I$ is of the form $u\pi^m$ for some unit and some non-negative integer $m$. Let $m_0$ be the least such integer occurring here and choose $\alpha_0 \in I$ of the form $\alpha_0 = u_0\pi^{m_0}$ for some unit $u_0$. Then $\alpha_0 R = \pi^{m_0} R$
We claim that every non-zero \( \alpha \in R \) has a unique representation of the form \( \alpha = u\pi^n \) for some unit \( u \) and non-negative integer \( n \). This is obvious if \( \alpha \) is a unit itself, so suppose \( \alpha \in \mathcal{M} \). Then \( \alpha = \pi^m\beta \) for some \( \beta \in R \) not zero. If \( \beta \) is a unit, then we have such a representation of \( \alpha \), and any such representation is clearly unique. If \( \beta \in \mathcal{M} \), by hypothesis the number of principal ideals in an ascending chain

\[
\alpha R \subsetneq \pi^m R \subsetneq \pi^{m-1} R \subsetneq \cdots \subsetneq \pi R
\]

is bounded by a function of \( \alpha \) so that there is a maximal exponent \( m \) such that \( \alpha \in \pi^m R \). Since \( \alpha \not\in \pi^{m+1} R \) we see that \( \alpha = u\pi^m \) for some \( u \not\in \pi R = \mathcal{M} \), so that \( u \) is a unit.

Finally, we show that all ideals are principal.

Let \( I \) be a non-zero ideal contained in \( \mathcal{M} \) (otherwise it is trivially principal). By the above, every non-zero element \( \alpha \in I \) is of the form \( u\pi^m \) for some unit and some non-negative integer \( m \). Let \( m_0 \) be the least such integer occurring here and choose \( \alpha_0 \in I \) of the form \( \alpha_0 = u_0\pi^{m_0} \) for some unit \( u_0 \). Then \( \alpha_0 R = \pi^{m_0} R \) and all non-zero \( \alpha \in I \) satisfy
We claim that every non-zero $\alpha \in R$ has a unique representation of the form $\alpha = u\pi^n$ for some unit $u$ and non-negative integer $n$. This is obvious if $\alpha$ is a unit itself, so suppose $\alpha \in \mathfrak{M}$. Then $\alpha = \pi^m \beta$ for some $\beta \in R$ not zero. If $\beta$ is a unit, then we have such a representation of $\alpha$, and any such representation is clearly unique. If $\beta \in \mathfrak{M}$, by hypothesis the number of principal ideals in an ascending chain

$$\alpha R \subsetneq \pi^m R \subsetneq \pi^{m-1} R \subsetneq \cdots \subsetneq \pi R$$

is bounded by a function of $\alpha$ so that there is a maximal exponent $m$ such that $\alpha \in \pi^m R$. Since $\alpha \notin \pi^{m+1} R$ we see that $\alpha = u\pi^m$ for some $u \notin \pi R = \mathfrak{M}$, so that $u$ is a unit.

Finally, we show that all ideals are principal.

Let $I$ be a non-zero ideal contained in $\mathfrak{M}$ (otherwise it is trivially principal). By the above, every non-zero element $\alpha \in I$ is of the form $u\pi^m$ for some unit and some non-negative integer $m$. Let $m_0$ be the least such integer occurring here and choose $\alpha_0 \in I$ of the form $\alpha_0 = u_0\pi^{m_0}$ for some unit $u_0$. Then $\alpha_0 R = \pi^{m_0} R$ and all non-zero $\alpha \in I$ satisfy $\alpha = u\pi^m \in \pi^{m_0} R$. 


We claim that every non-zero $\alpha \in R$ has a unique representation of the form $\alpha = u\pi^n$ for some unit $u$ and non-negative integer $n$. This is obvious if $\alpha$ is a unit itself, so suppose $\alpha \in M$. Then $\alpha = \pi^m\beta$ for some $\beta \in R$ not zero. If $\beta$ is a unit, then we have such a representation of $\alpha$, and any such representation is clearly unique. If $\beta \in M$, by hypothesis the number of principal ideals in an ascending chain

$$\alpha R \subsetneq \pi^m R \subsetneq \pi^{m-1} R \subsetneq \cdots \subsetneq \pi R$$

is bounded by a function of $\alpha$ so that there is a maximal exponent $m$ such that $\alpha \in \pi^m R$. Since $\alpha \notin \pi^{m+1} R$ we see that $\alpha = u\pi^m$ for some $u \notin \pi R = M$, so that $u$ is a unit.

Finally, we show that all ideals are principal.

Let $I$ be a non-zero ideal contained in $M$ (otherwise it is trivially principal). By the above, every non-zero element $\alpha \in I$ is of the form $u\pi^m$ for some unit and some non-negative integer $m$. Let $m_0$ be the least such integer occurring here and choose $\alpha_0 \in I$ of the form $\alpha_0 = u_0\pi^{m_0}$ for some unit $u_0$. Then $\alpha_0 R = \pi^{m_0} R$ and all non-zero $\alpha \in I$ satisfy $\alpha = u\pi^m \in \pi^{m_0} R$ since $m \geq m_0$ by construction.
We claim that every non-zero $\alpha \in R$ has a unique representation of the form $\alpha = u\pi^n$ for some unit $u$ and non-negative integer $n$. This is obvious if $\alpha$ is a unit itself, so suppose $\alpha \in M$. Then $\alpha = \pi^m \beta$ for some $\beta \in R$ not zero. If $\beta$ is a unit, then we have such a representation of $\alpha$, and any such representation is clearly unique. If $\beta \in M$, by hypothesis the number of principal ideals in an ascending chain

$$\alpha R \subsetneq \pi^m R \subsetneq \pi^{m-1} R \subsetneq \cdots \subsetneq \pi R$$

is bounded by a function of $\alpha$ so that there is a maximal exponent $m$ such that $\alpha \in \pi^m R$. Since $\alpha \notin \pi^{m+1} R$ we see that $\alpha = u\pi^m$ for some $u \notin \pi R = M$, so that $u$ is a unit.

Finally, we show that all ideals are principal.

Let $I$ be a non-zero ideal contained in $M$ (otherwise it is trivially principal). By the above, every non-zero element $\alpha \in I$ is of the form $u\pi^m$ for some unit and some non-negative integer $m$. Let $m_0$ be the least such integer occurring here and choose $\alpha_0 \in I$ of the form $\alpha_0 = u_0\pi^{m_0}$ for some unit $u_0$. Then $\alpha_0 R = \pi^{m_0} R$ and all non-zero $\alpha \in I$ satisfy $\alpha = u\pi^m \in \pi^{m_0} R$ since $m \geq m_0$ by construction. Therefore $I = \alpha_0 R$. 
Definition

A valuation ring that is also a principal ideal domain is called a **discrete valuation ring**.

**Lemma (3)**

Suppose $R$ is a discrete valuation ring of a field $K$ with maximal ideal $M$ and write $M = \pi R$. Then every non-zero ideal is of the form $\pi^n R$ for some non-negative integer $n$ and every non-zero $\alpha \in K$ is uniquely expressible as a product $u \pi^n$, where $u$ is a unit and $n \in \mathbb{Z}$. This integer $n$ is called the valuation of the element $\alpha$ and is denoted $v_R(\alpha)$. It is independent of the choice of the generator $\pi$ of $M$. 
Definition

A valuation ring that is also a principal ideal domain is called a discrete valuation ring.
Definition
A valuation ring that is also a principal ideal domain is called a \textit{discrete valuation ring}.

Lemma (3)
Suppose $R$ is a discrete valuation ring of a field $K$ with maximal ideal $M$ and write $M = \pi R$. Then every non-zero ideal is of the form $\pi^n R$ for some non-negative integer $n$ and every non-zero $\alpha \in K$ is uniquely expressible as a product $u \pi^n$, where $u$ is a unit and $n \in \mathbb{Z}$. This integer $n$ is called the valuation of the element $\alpha$ and is denoted $v_R(\alpha)$. It is independent of the choice of the generator $\pi$ of $M$. 

Definition
A valuation ring that is also a principal ideal domain is called a *discrete valuation ring*.

Lemma (3)
Suppose $R$ is a discrete valuation ring of a field $K$ with maximal ideal $M$ and write $M = \pi R$. Then every non-zero ideal is of the form $\pi^n R$ for some non-negative integer $n$ and every non-zero $\alpha \in K$ is uniquely expressible as a product $u \pi^n$, where $u$ is a unit and $n \in \mathbb{Z}$. This integer $n$ is called the valuation of the element $\alpha$ and is denoted $v_R(\alpha)$. It is independent of the choice of the generator $\pi$ of $M$. 

*Math 681, Wednesday, February 24, 2021*
Definition
A valuation ring that is also a principal ideal domain is called a discrete valuation ring.

Lemma (3)
Suppose $R$ is a discrete valuation ring of a field $K$ with maximal ideal $\mathfrak{M}$ and write $\mathfrak{M} = \pi R$. Then every non-zero ideal is of the form $\pi^n R$ for some non-negative integer $n$ and every non-zero $\alpha \in K$ is uniquely expressible as a product $u \pi^n$, where $u$ is a unit and $n \in \mathbb{Z}$. This integer $n$ is called the valuation of the element $\alpha$ and is denoted $v_R(\alpha)$. It is independent of the choice of the generator $\pi$ of $\mathfrak{M}$. 
Definition
A valuation ring that is also a principal ideal domain is called a *discrete valuation ring*.

Lemma (3)
*Suppose* $R$ *is a discrete valuation ring of a field* $K$ *with maximal ideal* $\mathcal{M}$ *and write* $\mathcal{M} = \pi R$. *Then every non-zero ideal is of the form* $\pi^n R$ *for some non-negative integer* $n$. *Then every non-zero* $\alpha \in K$ *is uniquely expressible as a product* $u \pi^n$, *where* $u$ *is a unit and* $n \in \mathbb{Z}$. *This integer* $n$ *is called the valuation of the element* $\alpha$ *and is denoted* $v_R(\alpha)$. *It is independent of the choice of the generator* $\pi$ *of* $\mathcal{M}$. 
Definition
A valuation ring that is also a principal ideal domain is called a discrete valuation ring.

Lemma (3)
Suppose $R$ is a discrete valuation ring of a field $K$ with maximal ideal $\mathfrak{M}$ and write $\mathfrak{M} = \pi R$. Then every non-zero ideal is of the form $\pi^n R$ for some non-negative integer $n$ and every non-zero $\alpha \in K$ is uniquely expressible as a product $u \pi^n$, where $u$ is a unit.
Definition

A valuation ring that is also a principal ideal domain is called a discrete valuation ring.

Lemma (3)

Suppose $R$ is a discrete valuation ring of a field $K$ with maximal ideal $\mathfrak{M}$ and write $\mathfrak{M} = \pi R$. Then every non-zero ideal is of the form $\pi^n R$ for some non-negative integer $n$ and every non-zero $\alpha \in K$ is uniquely expressible as a product $u \pi^n$, where $u$ is a unit and $n \in \mathbb{Z}$. 
Definition
A valuation ring that is also a principal ideal domain is called a *discrete valuation ring*.

Lemma (3)
Suppose $R$ is a discrete valuation ring of a field $K$ with maximal ideal $\mathcal{M}$ and write $\mathcal{M} = \pi R$. Then every non-zero ideal is of the form $\pi^n R$ for some non-negative integer $n$ and every non-zero $\alpha \in K$ is uniquely expressible as a product $u\pi^n$, where $u$ is a unit and $n \in \mathbb{Z}$. This integer $n$ is called the valuation of the element $\alpha$. 
Definition
A valuation ring that is also a principal ideal domain is called a discrete valuation ring.

Lemma (3)
Suppose $R$ is a discrete valuation ring of a field $K$ with maximal ideal $\mathfrak{M}$ and write $\mathfrak{M} = \pi R$. Then every non-zero ideal is of the form $\pi^n R$ for some non-negative integer $n$ and every non-zero $\alpha \in K$ is uniquely expressible as a product $u \pi^n$, where $u$ is a unit and $n \in \mathbb{Z}$. This integer $n$ is called the valuation of the element $\alpha$ and is denoted $v_R(\alpha)$. 
Definition

A valuation ring that is also a principal ideal domain is called a discrete valuation ring.

Lemma (3)

Suppose $R$ is a discrete valuation ring of a field $K$ with maximal ideal $\mathcal{M}$ and write $\mathcal{M} = \pi R$. Then every non-zero ideal is of the form $\pi^n R$ for some non-negative integer $n$ and every non-zero $\alpha \in K$ is uniquely expressible as a product $u \pi^n$, where $u$ is a unit and $n \in \mathbb{Z}$. This integer $n$ is called the valuation of the element $\alpha$ and is denoted $v_R(\alpha)$. It is independent of the choice of the generator $\pi$ of $\mathcal{M}$. 
Proof:

Since $R$ is a principal ideal domain, it is a unique factorization domain. Suppose $\alpha$ is an irreducible element (not a unit). Then $\alpha \in M$ so that $\alpha = \beta \pi$. But $\pi$ is clearly irreducible so that $\beta$ must be a unit. Thus, all irreducible elements are associates of $\pi$.

Let $I$ be a non-zero ideal of $R$ and write $I = \alpha R$ (possible since $R$ is a principal ideal domain). Then by the above $\alpha = u \pi^n$ for some unique unit $u$ and non-negative integer $n$, so that $I = \alpha R = \pi^n R$.

Let $\alpha$ be a non-zero element of the field. If $\alpha \in R$ then the principal ideal $\alpha R = \pi^n R$ for a unique non-negative integer $n$ (if $n = 0$ if $\alpha$ is a unit) so that $\alpha = u \pi^n$ for some unit $u$.

If $\alpha \not\in R$, then $\alpha^{-1} \in R$ so that $\alpha^{-1} = u \pi^{-n}$ for some unit $u$ and negative integer $n$, whence $\alpha = u^{-1} \pi^n$. 


**Proof:** Since $R$ is a principal ideal domain, it is a unique factorization domain.
**Proof:** Since $R$ is a principal ideal domain, it is a unique factorization domain.
Suppose $\alpha$ is an irreducible element.
**Proof**: Since $R$ is a principal ideal domain, it is a unique factorization domain.
Suppose $\alpha$ is an irreducible element (not a unit).
Proof: Since $R$ is a principal ideal domain, it is a unique factorization domain.
Suppose $\alpha$ is an irreducible element (not a unit). Then $\alpha \in \mathbb{M}$
**Proof:** Since $R$ is a principal ideal domain, it is a unique factorization domain.

Suppose $\alpha$ is an irreducible element (not a unit). Then $\alpha \in \mathcal{M}$ so that $\alpha = \beta \pi$.
Proof: Since $R$ is a principal ideal domain, it is a unique factorization domain.
Suppose $\alpha$ is an irreducible element (not a unit). Then $\alpha \in M$ so that $\alpha = \beta \pi$. But $\pi$ is clearly irreducible
Proof: Since $R$ is a principal ideal domain, it is a unique factorization domain.

Suppose $\alpha$ is an irreducible element (not a unit). Then $\alpha \in M$ so that $\alpha = \beta \pi$. But $\pi$ is clearly irreducible so that $\beta$ must be a unit.
**Proof:** Since $R$ is a principal ideal domain, it is a unique factorization domain.
Suppose $\alpha$ is an irreducible element (not a unit). Then $\alpha \in \mathcal{M}$ so that $\alpha = \beta \pi$. But $\pi$ is clearly irreducible so that $\beta$ must be a unit. Thus, all irreducible elements are associates of $\pi$. 
Proof: Since $R$ is a principal ideal domain, it is a unique factorization domain.
Suppose $\alpha$ is an irreducible element (not a unit). Then $\alpha \in \mathcal{M}$ so that $\alpha = \beta \pi$. But $\pi$ is clearly irreducible so that $\beta$ must be a unit. Thus, all irreducible elements are associates of $\pi$.

Let $I$ be a non-zero ideal of $R$ and write $I = \alpha R$
Proof: Since $R$ is a principal ideal domain, it is a unique factorization domain.

Suppose $\alpha$ is an irreducible element (not a unit). Then $\alpha \in M$ so that $\alpha = \beta \pi$. But $\pi$ is clearly irreducible so that $\beta$ must be a unit. Thus, all irreducible elements are associates of $\pi$.

Let $I$ be a non-zero ideal of $R$ and write $I = \alpha R$ (possible since $R$ is a principal ideal domain).
Proof: Since $R$ is a principal ideal domain, it is a unique factorization domain.
Suppose $\alpha$ is an irreducible element (not a unit). Then $\alpha \in \mathcal{M}$ so that $\alpha = \beta \pi$. But $\pi$ is clearly irreducible so that $\beta$ must be a unit. Thus, all irreducible elements are associates of $\pi$.

Let $I$ be a non-zero ideal of $R$ and write $I = \alpha R$ (possible since $R$ is a principal ideal domain). Then by the above $\alpha = u \pi^n$ for some unique unit $u$ and non-negative integer $n$, 
**Proof**: Since $R$ is a principal ideal domain, it is a unique factorization domain.

Suppose $\alpha$ is an irreducible element (not a unit). Then $\alpha \in \mathcal{M}$ so that $\alpha = \beta \pi$. But $\pi$ is clearly irreducible so that $\beta$ must be a unit. Thus, all irreducible elements are associates of $\pi$.

Let $I$ be a non-zero ideal of $R$ and write $I = \alpha R$ (possible since $R$ is a principal ideal domain). Then by the above $\alpha = u \pi^n$ for some unique unit $u$ and non-negative integer $n$, so that $I = \alpha R = \pi^n R$. 
Proof: Since $R$ is a principal ideal domain, it is a unique factorization domain.
Suppose $\alpha$ is an irreducible element (not a unit). Then $\alpha \in M$ so that $\alpha = \beta \pi$. But $\pi$ is clearly irreducible so that $\beta$ must be a unit. Thus, all irreducible elements are associates of $\pi$.

Let $I$ be a non-zero ideal of $R$ and write $I = \alpha R$ (possible since $R$ is a principal ideal domain). Then by the above $\alpha = u \pi^n$ for some unique unit $u$ and non-negative integer $n$, so that $I = \alpha R = \pi^n R$.

Let $\alpha$ be a non-zero element of the field.
**Proof:** Since $R$ is a principal ideal domain, it is a unique factorization domain.

Suppose $\alpha$ is an irreducible element (not a unit). Then $\alpha \in \mathcal{M}$ so that $\alpha = \beta \pi$. But $\pi$ is clearly irreducible so that $\beta$ must be a unit. Thus, all irreducible elements are associates of $\pi$.

Let $I$ be a non-zero ideal of $R$ and write $I = \alpha R$ (possible since $R$ is a principal ideal domain). Then by the above $\alpha = u\pi^n$ for some unique unit $u$ and non-negative integer $n$, so that $I = \alpha R = \pi^n R$.

Let $\alpha$ be a non-zero element of the field. If $\alpha \in R$ then the principal ideal $\alpha R = \pi^n R$ for a unique non-negative integer $n$. 
**Proof:** Since $R$ is a principal ideal domain, it is a unique factorization domain.

Suppose $\alpha$ is an irreducible element (not a unit). Then $\alpha \in \mathcal{M}$ so that $\alpha = \beta \pi$. But $\pi$ is clearly irreducible so that $\beta$ must be a unit. Thus, all irreducible elements are associates of $\pi$.

Let $I$ be a non-zero ideal of $R$ and write $I = \alpha R$ (possible since $R$ is a principal ideal domain). Then by the above $\alpha = u \pi^n$ for some unique unit $u$ and non-negative integer $n$, so that $I = \alpha R = \pi^n R$.

Let $\alpha$ be a non-zero element of the field. If $\alpha \in R$ then the principal ideal $\alpha R = \pi^n R$ for a unique non-negative integer $n$ ($n = 0$ if $\alpha$ is a unit).
**Proof:** Since $R$ is a principal ideal domain, it is a unique factorization domain.

Suppose $\alpha$ is an irreducible element (not a unit). Then $\alpha \in \mathcal{M}$ so that $\alpha = \beta \pi$. But $\pi$ is clearly irreducible so that $\beta$ must be a unit. Thus, all irreducible elements are associates of $\pi$.

Let $I$ be a non-zero ideal of $R$ and write $I = \alpha R$ (possible since $R$ is a principal ideal domain). Then by the above $\alpha = u\pi^n$ for some unique unit $u$ and non-negative integer $n$, so that $I = \alpha R = \pi^n R$.

Let $\alpha$ be a non-zero element of the field. If $\alpha \in R$ then the principal ideal $\alpha R = \pi^n R$ for a unique non-negative integer $n$ ($n = 0$ if $\alpha$ is a unit) so that $\alpha = u\pi^n$ for some unit $u$. 
**Proof:** Since $R$ is a principal ideal domain, it is a unique factorization domain.

Suppose $\alpha$ is an irreducible element (not a unit). Then $\alpha \in \mathcal{M}$ so that $\alpha = \beta \pi$. But $\pi$ is clearly irreducible so that $\beta$ must be a unit. Thus, all irreducible elements are associates of $\pi$.

Let $I$ be a non-zero ideal of $R$ and write $I = \alpha R$ (possible since $R$ is a principal ideal domain). Then by the above $\alpha = u \pi^n$ for some unique unit $u$ and non-negative integer $n$, so that $I = \alpha R = \pi^n R$.

Let $\alpha$ be a non-zero element of the field. If $\alpha \in R$ then the principal ideal $\alpha R = \pi^n R$ for a unique non-negative integer $n$ ($n = 0$ if $\alpha$ is a unit) so that $\alpha = u \pi^n$ for some unit $u$. If $\alpha \notin R$, then $\alpha^{-1} \in R$.
**Proof:** Since $R$ is a principal ideal domain, it is a unique factorization domain.

Suppose $\alpha$ is an irreducible element (not a unit). Then $\alpha \in \mathcal{M}$ so that $\alpha = \beta \pi$. But $\pi$ is clearly irreducible so that $\beta$ must be a unit. Thus, all irreducible elements are associates of $\pi$.

Let $I$ be a non-zero ideal of $R$ and write $I = \alpha R$ (possible since $R$ is a principal ideal domain). Then by the above $\alpha = u \pi^n$ for some unique unit $u$ and non-negative integer $n$, so that $I = \alpha R = \pi^n R$.

Let $\alpha$ be a non-zero element of the field. If $\alpha \in R$ then the principal ideal $\alpha R = \pi^n R$ for a unique non-negative integer $n$ ($n = 0$ if $\alpha$ is a unit) so that $\alpha = u \pi^n$ for some unit $u$. If $\alpha \not\in R$, then $\alpha^{-1} \in R$ so that $\alpha^{-1} = u \pi^{-n}$ for some unit $u$ and negative integer $n$, ...
**Proof:** Since $R$ is a principal ideal domain, it is a unique factorization domain.
Suppose $\alpha$ is an irreducible element (not a unit). Then $\alpha \in \mathcal{M}$ so that $\alpha = \beta \pi$. But $\pi$ is clearly irreducible so that $\beta$ must be a unit. Thus, all irreducible elements are associates of $\pi$.

Let $I$ be a non-zero ideal of $R$ and write $I = \alpha R$ (possible since $R$ is a principal ideal domain). Then by the above $\alpha = u \pi^n$ for some unique unit $u$ and non-negative integer $n$, so that $I = \alpha R = \pi^n R$.

Let $\alpha$ be a non-zero element of the field. If $\alpha \in R$ then the principal ideal $\alpha R = \pi^n R$ for a unique non-negative integer $n$ ($n = 0$ if $\alpha$ is a unit) so that $\alpha = u \pi^n$ for some unit $u$. If $\alpha \not\in R$, then $\alpha^{-1} \in R$ so that $\alpha^{-1} = u \pi^{-n}$ for some unit $u$ and negative integer $n$, whence $\alpha = u^{-1} \pi^n$. 
**Proof:** Since $R$ is a principal ideal domain, it is a unique factorization domain.

Suppose $\alpha$ is an irreducible element (not a unit). Then $\alpha \in \mathfrak{M}$ so that $\alpha = \beta \pi$. But $\pi$ is clearly irreducible so that $\beta$ must be a unit. Thus, all irreducible elements are associates of $\pi$.

Let $I$ be a non-zero ideal of $R$ and write $I = \alpha R$ (possible since $R$ is a principal ideal domain). Then by the above $\alpha = u \pi^n$ for some unique unit $u$ and non-negative integer $n$, so that $I = \alpha R = \pi^n R$.

Let $\alpha$ be a non-zero element of the field. If $\alpha \in R$ then the principal ideal $\alpha R = \pi^n R$ for a unique non-negative integer $n$ ($n = 0$ if $\alpha$ is a unit) so that $\alpha = u \pi^n$ for some unit $u$. If $\alpha \not\in R$, then $\alpha^{-1} \in R$ so that $\alpha^{-1} = u \pi^{-n}$ for some unit $u$ and negative integer $n$, whence $\alpha = u^{-1} \pi^n$. 
Clearly all generators of $\mathcal{M}$ are irreducible elements of $R$
Clearly all generators of $M$ are irreducible elements of $R$ which are associates of $\pi$ as shown above,
Clearly all generators of \( \mathfrak{M} \) are irreducible elements of \( R \) which are associates of \( \pi \) as shown above, which shows that the valuation \( \nu_R \) doesn’t depend on the choice of the generator.
Clearly all generators of $\mathcal{M}$ are irreducible elements of $R$ which are associates of $\pi$ as shown above, which shows that the valuation $\nu_R$ doesn’t depend on the choice of the generator.

Lemma (4)
Clearly all generators of $\mathfrak{M}$ are irreducible elements of $R$ which are associates of $\pi$ as shown above, which shows that the valuation $\nu_R$ doesn’t depend on the choice of the generator.

**Lemma (4)**

*Let $R$ be discrete valuation ring of a field $K$*
Clearly all generators of $\mathcal{M}$ are irreducible elements of $R$ which are associates of $\pi$ as shown above, which shows that the valuation $v_R$ doesn’t depend on the choice of the generator.

**Lemma (4)**

Let $R$ be discrete valuation ring of a field $K$ and for $\alpha \in K$ set

$$|\alpha| = \begin{cases} \exp(-v_R(\alpha)) & \text{if } \alpha \neq 0, \\ 0 & \text{otherwise.} \end{cases}$$

Then $|\cdot|$ is a non-archimedean absolute value on $K$. Moreover, any two distinct discrete valuation rings yield inequivalent absolute values.

**Proof:** Let $\pi$ generate the maximal ideal of $R$.

First suppose $\alpha$ and $\beta$ are non-zero with $v_R(\alpha) = n$ and $v_R(\beta) = m$. Then $\alpha = u\pi^n$ and $\beta = u'\pi^m$ for units $u, u' \in R$ and $n, m \in \mathbb{Z}$, so that $\alpha\beta = uu'\pi^{n+m}$ and $v_R(\alpha\beta) = v_R(\alpha) + v_R(\beta)$.
Clearly all generators of $\mathfrak{M}$ are irreducible elements of $R$ which are associates of $\pi$ as shown above, which shows that the valuation $v_R$ doesn’t depend on the choice of the generator.

**Lemma (4)**

Let $R$ be discrete valuation ring of a field $K$ and for $\alpha \in K$ set

$$|\alpha| = \begin{cases} \exp (- v_R(\alpha)) & \text{if } \alpha \neq 0, \end{cases}$$
Clearly all generators of $\mathfrak{M}$ are irreducible elements of $R$ which are associates of $\pi$ as shown above, which shows that the valuation $\nu_R$ doesn’t depend on the choice of the generator.

**Lemma (4)**

Let $R$ be discrete valuation ring of a field $K$ and for $\alpha \in K$ set

$$|\alpha| = \begin{cases} \exp (- \nu_R(\alpha)) & \text{if } \alpha \neq 0, \\ 0 & \text{otherwise.} \end{cases}$$
Clearly all generators of $\mathfrak{M}$ are irreducible elements of $R$ which are associates of $\pi$ as shown above, which shows that the valuation $\nu_R$ doesn’t depend on the choice of the generator.

**Lemma (4)**

Let $R$ be discrete valuation ring of a field $K$ and for $\alpha \in K$ set

$$|\alpha| = \begin{cases} \exp(-\nu_R(\alpha)) & \text{if } \alpha \neq 0, \\ 0 & \text{otherwise.} \end{cases}$$

Then $|\cdot|$ is a non-archimedean absolute value on $K$. 
Clearly all generators of $\mathcal{M}$ are irreducible elements of $R$ which are associates of $\pi$ as shown above, which shows that the valuation $\nu_R$ doesn’t depend on the choice of the generator.

**Lemma (4)**

Let $R$ be discrete valuation ring of a field $K$ and for $\alpha \in K$ set

$$
|\alpha| = \begin{cases} 
\exp(-\nu_R(\alpha)) & \text{if } \alpha \neq 0, \\
0 & \text{otherwise.}
\end{cases}
$$

Then $|\cdot|$ is a non-archimedean absolute value on $K$. Moreover, any two distinct discrete valuation rings yield inequivalent absolute values.
Clearly all generators of $\mathcal{M}$ are irreducible elements of $R$ which are associates of $\pi$ as shown above, which shows that the valuation $v_R$ doesn’t depend on the choice of the generator.

**Lemma (4)**

Let $R$ be discrete valuation ring of a field $K$ and for $\alpha \in K$ set

$$|\alpha| = \begin{cases} 
\exp \left( - v_R(\alpha) \right) & \text{if } \alpha \neq 0, \\
0 & \text{otherwise}.
\end{cases}$$

Then $|\cdot|$ is a non-archimedean absolute value on $K$. Moreover, any two distinct discrete valuation rings yield inequivalent absolute values.

**Proof:**
Clearly all generators of $\mathfrak{M}$ are irreducible elements of $R$ which are associates of $\pi$ as shown above, which shows that the valuation $v_R$ doesn’t depend on the choice of the generator.

**Lemma (4)**

Let $R$ be discrete valuation ring of a field $K$ and for $\alpha \in K$ set

$$|\alpha| = \begin{cases} 
\exp(-v_R(\alpha)) & \text{if } \alpha \neq 0, \\
0 & \text{otherwise}.
\end{cases}$$

Then $|\cdot|$ is a non-archimedean absolute value on $K$. Moreover, any two distinct discrete valuation rings yield inequivalent absolute values.

**Proof:** Let $\pi$ generate the maximal ideal of $R$. 
Clearly all generators of $\mathfrak{M}$ are irreducible elements of $R$ which are associates of $\pi$ as shown above, which shows that the valuation $v_R$ doesn’t depend on the choice of the generator.

**Lemma (4)**

Let $R$ be discrete valuation ring of a field $K$ and for $\alpha \in K$ set

$$|\alpha| = \begin{cases} 
\exp (-v_R(\alpha)) & \text{if } \alpha \neq 0, \\
0 & \text{otherwise}.
\end{cases}$$

Then $|\cdot|$ is a non-archimedean absolute value on $K$. Moreover, any two distinct discrete valuation rings yield inequivalent absolute values.

**Proof:** Let $\pi$ generate the maximal ideal of $R$.

First suppose $\alpha$ and $\beta$ are non-zero with $v_R(\alpha) = n$ and $v_R(\beta) = m$. 
Clearly all generators of $\mathfrak{M}$ are irreducible elements of $R$ which are associates of $\pi$ as shown above, which shows that the valuation $v_R$ doesn’t depend on the choice of the generator.

**Lemma (4)**

Let $R$ be discrete valuation ring of a field $K$ and for $\alpha \in K$ set

$$|\alpha| = \begin{cases} \exp(-v_R(\alpha)) & \text{if } \alpha \neq 0, \\ 0 & \text{otherwise.} \end{cases}$$

Then $|\cdot|$ is a non-archimedean absolute value on $K$. Moreover, any two distinct discrete valuation rings yield inequivalent absolute values.

**Proof:** Let $\pi$ generate the maximal ideal of $R$.

First suppose $\alpha$ and $\beta$ are non-zero with $v_R(\alpha) = n$ and $v_R(\beta) = m$. Then $\alpha = u\pi^n$ and $\beta = u'\pi^m$ for units $u, u' \in R$ and $n, m \in \mathbb{Z}$,
Clearly all generators of $\mathcal{M}$ are irreducible elements of $R$ which are associates of $\pi$ as shown above, which shows that the valuation $\nu_R$ doesn’t depend on the choice of the generator.

Lemma (4)

Let $R$ be discrete valuation ring of a field $K$ and for $\alpha \in K$ set

$$|\alpha| = \begin{cases} \exp(-\nu_R(\alpha)) & \text{if } \alpha \neq 0, \\ 0 & \text{otherwise.} \end{cases}$$

Then $|\cdot|$ is a non-archimedean absolute value on $K$. Moreover, any two distinct discrete valuation rings yield inequivalent absolute values.

Proof: Let $\pi$ generate the maximal ideal of $R$.

First suppose $\alpha$ and $\beta$ are non-zero with $\nu_R(\alpha) = n$ and $\nu_R(\beta) = m$. Then $\alpha = u\pi^n$ and $\beta = u'\pi^m$ for units $u, u' \in R$ and $n, m \in \mathbb{Z}$, so that $\alpha\beta = uu'\pi^{n+m}$ and $\nu_R(\alpha\beta) = \nu_R(\alpha) + \nu_R(\beta)$. 

For the ultra-metric inequality,
For the ultra-metric inequality, by what we have already shown
For the ultra-metric inequality, by what we have already shown
\[ v_R(\alpha + \beta) = v_R(\alpha) + v_R(1 + \beta/\alpha) \]
For the ultra-metric inequality, by what we have already shown
\( v_R(\alpha + \beta) = v_R(\alpha) + v_R(1 + \beta/\alpha) \) (assuming \( \alpha \neq 0 \), of course).
For the ultra-metric inequality, by what we have already shown
\( v_R(\alpha + \beta) = v_R(\alpha) + v_R(1 + \beta/\alpha) \) (assuming \( \alpha \neq 0 \), of course). Exercise
#3 from homework #7 is to show that
For the ultra-metric inequality, by what we have already shown \( v_R(\alpha + \beta) = v_R(\alpha) + v_R(1 + \beta/\alpha) \) (assuming \( \alpha \neq 0 \), of course). Exercise #3 from homework #7 is to show that \( v_R(1 + \gamma) \geq \min\{0, v_R(\gamma)\} \) for all \( \gamma \),
For the ultra-metric inequality, by what we have already shown

$$v_R(\alpha + \beta) = v_R(\alpha) + v_R(1 + \beta/\alpha)$$

(assuming \(\alpha \neq 0\), of course). Exercise #3 from homework #7 is to show that

$$v_R(1 + \gamma) \geq \min\{0, v_R(\gamma)\}$$

for all \(\gamma\), whence we get the ultra-metric inequality.
For the ultra-metric inequality, by what we have already shown $v_R(\alpha + \beta) = v_R(\alpha) + v_R(1 + \beta/\alpha)$ (assuming $\alpha \neq 0$, of course). Exercise #3 from homework #7 is to show that $v_R(1 + \gamma) \geq \min\{0, v_R(\gamma)\}$ for all $\gamma$, whence we get the ultra-metric inequality.

Let $R_1$ and $R_2$ be distinct valuation rings of $K$.
For the ultra-metric inequality, by what we have already shown
\[ \nu_R(\alpha + \beta) = \nu_R(\alpha) + \nu_R(1 + \beta/\alpha) \] (assuming \( \alpha \neq 0 \), of course). Exercise
\#3 from homework \#7 is to show that \( \nu_R(1 + \gamma) \geq \min\{0, \nu_R(\gamma)\} \) for all \( \gamma \), whence we get the ultra-metric inequality.

Let \( R_1 \) and \( R_2 \) be distinct valuation rings of \( K \) and denote the corresponding absolute values \( |\cdot|_1 \) and \( |\cdot|_2 \), respectively.
For the ultra-metric inequality, by what we have already shown
\( v_R(\alpha + \beta) = v_R(\alpha) + v_R(1 + \beta/\alpha) \) (assuming \( \alpha \neq 0 \), of course). Exercise #3 from homework #7 is to show that \( v_R(1 + \gamma) \geq \min\{0, v_R(\gamma)\} \) for all \( \gamma \), whence we get the ultra-metric inequality.

Let \( R_1 \) and \( R_2 \) be distinct valuation rings of \( K \) and denote the corresponding absolute values \( |\cdot|_1 \) and \( |\cdot|_2 \), respectively. Without loss of generality there is an \( \alpha \in R_1 \setminus R_2 \).
For the ultra-metric inequality, by what we have already shown
\( v_R(\alpha + \beta) = v_R(\alpha) + v_R(1 + \beta/\alpha) \) (assuming \( \alpha \neq 0 \), of course). Exercise #3 from homework #7 is to show that \( v_R(1 + \gamma) \geq \min\{0, v_R(\gamma)\} \) for all \( \gamma \), whence we get the ultra-metric inequality.

Let \( R_1 \) and \( R_2 \) be distinct valuation rings of \( K \) and denote the corresponding absolute values \( |\cdot|_1 \) and \( |\cdot|_2 \), respectively. Without loss of generality there is an \( \alpha \in R_1 \setminus R_2 \). Then \( |\alpha|_1 \leq 1 < |\alpha|_2 \),
For the ultra-metric inequality, by what we have already shown
\[ v_R(\alpha + \beta) = v_R(\alpha) + v_R(1 + \beta/\alpha) \] (assuming \( \alpha \neq 0 \), of course). Exercise
#3 from homework #7 is to show that \( v_R(1 + \gamma) \geq \min\{0, v_R(\gamma)\} \) for all
\( \gamma \), whence we get the ultra-metric inequality.

Let \( R_1 \) and \( R_2 \) be distinct valuation rings of \( K \) and denote the
corresponding absolute values \( |\cdot|_1 \) and \( |\cdot|_2 \), respectively. Without loss of
generality there is an \( \alpha \in R_1 \setminus R_2 \). Then \( |\alpha|_1 \leq 1 < |\alpha|_2 \), so that the
sequence \( \alpha^{-n} \rightarrow 0 \) in the topology given by \( |\cdot|_2 \), but not for that
given by \( |\cdot|_1 \).
For the ultra-metric inequality, by what we have already shown \( v_R(\alpha + \beta) = v_R(\alpha) + v_R(1 + \beta/\alpha) \) (assuming \( \alpha \neq 0 \), of course). Exercise \#3 from homework \#7 is to show that \( v_R(1 + \gamma) \geq \min\{0, v_R(\gamma)\} \) for all \( \gamma \), whence we get the ultra-metric inequality.

Let \( R_1 \) and \( R_2 \) be distinct valuation rings of \( K \) and denote the corresponding absolute values \( |\cdot|_1 \) and \( |\cdot|_2 \), respectively. Without loss of generality there is an \( \alpha \in R_1 \setminus R_2 \). Then \( |\alpha|_1 \leq 1 < |\alpha|_2 \), so that the sequence \( \alpha e^{-n} \rightarrow 0 \) in the topology given by \( |\cdot|_2 \), but not for that given by \( |\cdot|_1 \). Thus these are inequivalent absolute values.
For the ultra-metric inequality, by what we have already shown
\( v_R(\alpha + \beta) = v_R(\alpha) + v_R(1 + \beta/\alpha) \) (assuming \( \alpha \neq 0 \), of course). Exercise 
\#3 from homework \#7 is to show that \( v_R(1 + \gamma) \geq \min\{0, v_R(\gamma)\} \) for all
\( \gamma \), whence we get the ultra-metric inequality.

Let \( R_1 \) and \( R_2 \) be distinct valuation rings of \( K \) and denote the
corresponding absolute values \( |\cdot|_1 \) and \( |\cdot|_2 \), respectively. Without loss of
generality there is an \( \alpha \in R_1 \setminus R_2 \). Then \( |\alpha|_1 \leq 1 < |\alpha|_2 \), so that the
sequence \( \alpha 2^{-n} \rightarrow 0 \) in the topology given by \( |\cdot|_2 \), but not for that
given by \( |\cdot|_1 \). Thuse these are inequivalent absolute values.

Proposition (1)
For the ultra-metric inequality, by what we have already shown
\[ v_R(\alpha + \beta) = v_R(\alpha) + v_R(1 + \beta/\alpha) \] (assuming \( \alpha \neq 0 \), of course). Exercise #3 from homework #7 is to show that \( v_R(1 + \gamma) \geq \min\{0, v_R(\gamma)\} \) for all \( \gamma \), whence we get the ultra-metric inequality.

Let \( R_1 \) and \( R_2 \) be distinct valuation rings of \( K \) and denote the corresponding absolute values \( |\cdot|_1 \) and \( |\cdot|_2 \), respectively. Without loss of generality there is an \( \alpha \in R_1 \setminus R_2 \). Then \( |\alpha|_1 \leq 1 < |\alpha|_2 \), so that the sequence \( \alpha_2^{-n} \to 0 \) in the topology given by \( |\cdot|_2 \), but not for that given by \( |\cdot|_1 \). Thuse these are inequivalent absolute values.

**Proposition (1)**

*If \( K \) is a number field or a function field,*
For the ultra-metric inequality, by what we have already shown $v_R(\alpha + \beta) = v_R(\alpha) + v_R(1 + \beta/\alpha)$ (assuming $\alpha \neq 0$, of course). Exercise #3 from homework #7 is to show that $v_R(1 + \gamma) \geq \min\{0, v_R(\gamma)\}$ for all $\gamma$, whence we get the ultra-metric inequality.

Let $R_1$ and $R_2$ be distinct valuation rings of $K$ and denote the corresponding absolute values $|\cdot|_1$ and $|\cdot|_2$, respectively. Without loss of generality there is an $\alpha \in R_1 \setminus R_2$. Then $|\alpha|_1 \leq 1 < |\alpha|_2$, so that the sequence $\alpha 2^{-n} \to 0$ in the topology given by $|\cdot|_2$, but not for that given by $|\cdot|_1$. Thuse these are inequivalent absolute values.

**Proposition (1)**

*If $K$ is a number field or a function field, then all valuation rings $R$ of $K$ satisfy the hypothesis of Lemma 2*
For the ultra-metric inequality, by what we have already shown
\[ v_R(\alpha + \beta) = v_R(\alpha) + v_R(1 + \beta/\alpha) \] (assuming \( \alpha \neq 0 \), of course). Exercise #3 from homework #7 is to show that \( v_R(1 + \gamma) \geq \min\{0, v_R(\gamma)\} \) for all \( \gamma \), whence we get the ultra-metric inequality.

Let \( R_1 \) and \( R_2 \) be distinct valuation rings of \( K \) and denote the corresponding absolute values \( |\cdot|_1 \) and \( |\cdot|_2 \), respectively. Without loss of generality there is an \( \alpha \in R_1 \setminus R_2 \). Then \( |\alpha|_1 \leq 1 < |\alpha|_2 \), so that the sequence \( \alpha_2^{-n} \to 0 \) in the topology given by \( |\cdot|_2 \), but not for that given by \( |\cdot|_1 \). Thus these are inequivalent absolute values.

**Proposition (1)**

*If \( K \) is a number field or a function field, then all valuation rings \( R \) of \( K \) satisfy the hypothesis of Lemma 2 and are hence discrete valuation rings.*
Proof:

As remarked above $R \supseteq \mathbb{Z}$ in characteristic $0$, which is certainly the case for number fields, and $R \supseteq \mathbb{F}_p$ in characteristic $p$, which is the case for function fields. We claim that in fact $R$ contains the entire field of constants for a function field $K$.

Indeed, let $\alpha$ be a non-zero element of the field of constants with minimal polynomial $z_0 + z_1 Y + \cdots + Y^n \in \mathbb{F}_p[Y]$. Then

\[
\alpha^n = -z_0 - \cdots - z_{n-1} - \frac{1}{\alpha^{n-1}} \in \mathbb{F}_p[\alpha^{-1}].
\]

Since either $\alpha \in R$ or $\alpha^{-1} \in R$, we must have $\alpha \in R$.

We remark that the same argument shows $R \supseteq \mathcal{O}_K$ in the number field case.
**Proof:** As remarked above
Proof: As remarked above $R \supseteq \mathbb{Z}$ in characteristic 0,
Proof: As remarked above $R \supseteq \mathbb{Z}$ in characteristic 0, which is certainly the case for number fields,
Proof: As remarked above $R \supseteq \mathbb{Z}$ in characteristic 0, which is certainly the case for number fields, and $R \supseteq \mathbb{F}_p$ in characteristic $p$, 
**Proof:** As remarked above $R \supseteq \mathbb{Z}$ in characteristic 0, which is certainly the case for number fields, and $R \supseteq \mathbb{F}_p$ in characteristic $p$, which is the case for function fields.
**Proof**: As remarked above $R \supseteq \mathbb{Z}$ in characteristic 0, which is certainly the case for number fields, and $R \supseteq \mathbb{F}_p$ in characteristic $p$, which is the case for function fields. We claim that in fact $R$ contains the entire field of constants for a function field $K$. 

Indeed, let $\alpha$ be a non-zero element of the field of constants with minimal polynomial $z_0 + z_1 \alpha Y + \cdots + Y^n \in \mathbb{F}_p[Y]$. Then $\alpha^n = -z_0 - \cdots - z_n - 1 \alpha_{n-1} \in \mathbb{F}_p[\alpha - 1]$. Since either $\alpha \in R$ or $\alpha - 1 \in R$, we must have $\alpha \in R$. We remark that the same argument shows $R \supseteq \mathcal{O}_K$ in the number field case.
Proof: As remarked above $R \supseteq \mathbb{Z}$ in characteristic 0, which is certainly the case for number fields, and $R \supseteq \mathbb{F}_p$ in characteristic $p$, which is the case for function fields. We claim that in fact $R$ contains the entire field of constants for a function field $K$.

Indeed, let $\alpha$ be a non-zero element of the field of constants for a function field $K$.
Proof: As remarked above $R \supseteq \mathbb{Z}$ in characteristic 0, which is certainly the case for number fields, and $R \supseteq \mathbb{F}_p$ in characteristic $p$, which is the case for function fields. We claim that in fact $R$ contains the entire field of constants for a function field $K$.

Indeed, let $\alpha$ be a non-zero element of the field of constants with minimal polynomial $z_0 + z_1 Y + \cdots + Y^n \in \mathbb{F}_p[Y]$. 
Proof: As remarked above \( R \supseteq \mathbb{Z} \) in characteristic 0, which is certainly the case for number fields, and \( R \supseteq \mathbb{F}_p \) in characteristic \( p \), which is the case for function fields. We claim that in fact \( R \) contains the entire field of constants for a function field \( K \).

Indeed, let \( \alpha \) be a non-zero element of the field of constants with minimal polynomial \( z_0 + z_1 Y + \cdots + Y^n \in \mathbb{F}_p[Y] \). Then

\[
\alpha^n = -z_0 - \cdots - z_{n-1}\alpha^{n-1},
\]
Proof: As remarked above $R \supseteq \mathbb{Z}$ in characteristic 0, which is certainly the case for number fields, and $R \supseteq \mathbb{F}_p$ in characteristic $p$, which is the case for function fields. We claim that in fact $R$ contains the entire field of constants for a function field $K$.

Indeed, let $\alpha$ be a non-zero element of the field of constants with minimal polynomial $z_0 + z_1 Y + \cdots + Y^n \in \mathbb{F}_p[Y]$. Then

$$\alpha^n = -z_0 - \cdots - z_{n-1} \alpha^{n-1},$$

$$\alpha = -z_0 \alpha^{-(n-1)} - \cdots - z_{n-1} \in \mathbb{F}_p[\alpha^{-1}].$$
**Proof:** As remarked above $R \supseteq \mathbb{Z}$ in characteristic 0, which is certainly the case for number fields, and $R \supseteq \mathbb{F}_p$ in characteristic $p$, which is the case for function fields. We claim that in fact $R$ contains the entire field of constants for a function field $K$.

Indeed, let $\alpha$ be a non-zero element of the field of constants with minimal polynomial $z_0 + z_1 Y + \cdots + Y^n \in \mathbb{F}_p[Y]$. Then

\[ \alpha^n = -z_0 - \cdots - z_{n-1} \alpha^{n-1}, \]
\[ \alpha = -z_0 \alpha^{-(n-1)} - \cdots - z_{n-1} \in \mathbb{F}_p[\alpha^{-1}]. \]

Since either $\alpha \in R$ or $\alpha^{-1} \in R$, 

...
Proof: As remarked above $R \supseteq \mathbb{Z}$ in characteristic 0, which is certainly the case for number fields, and $R \supseteq \mathbb{F}_p$ in characteristic $p$, which is the case for function fields. We claim that in fact $R$ contains the entire field of constants for a function field $K$.

Indeed, let $\alpha$ be a non-zero element of the field of constants with minimal polynomial $z_0 + z_1 Y + \cdots + Y^n \in \mathbb{F}_p[Y]$. Then

$$\alpha^n = -z_0 - \cdots - z_{n-1} \alpha^{n-1},$$

$$\alpha = -z_0 \alpha^{-(n-1)} - \cdots - z_{n-1} \in \mathbb{F}_p[\alpha^{-1}].$$

Since either $\alpha \in R$ or $\alpha^{-1} \in R$, we must have $\alpha \in R$. 
Proof: As remarked above $R \supseteq \mathbb{Z}$ in characteristic 0, which is certainly the case for number fields, and $R \supseteq \mathbb{F}_p$ in characteristic $p$, which is the case for function fields. We claim that in fact $R$ contains the entire field of constants for a function field $K$.

Indeed, let $\alpha$ be a non-zero element of the field of constants with minimal polynomial $z_0 + z_1 Y + \cdots + Y^n \in \mathbb{F}_p[Y]$. Then

$$\alpha^n = -z_0 - \cdots - z_{n-1}\alpha^{n-1},$$

$$\alpha = -z_0\alpha^{-(n-1)} - \cdots - z_{n-1} \in \mathbb{F}_p[\alpha^{-1}].$$

Since either $\alpha \in R$ or $\alpha^{-1} \in R$, we must have $\alpha \in R$.

We remark that the same argument shows $R \supseteq \mathcal{O}_K$ in the number field case.
Let $F$ denote the prime field
Let $F$ denote the prime field ($\mathbb{Q}$ in characteristic 0 and $\mathbb{F}_p$ in characteristic $p$).
Let $F$ denote the prime field ($\mathbb{Q}$ in characteristic 0 and $\mathbb{F}_p$ in characteristic $p$).

Suppose $\alpha_1, \ldots, \alpha_n \in M$
Let $F$ denote the prime field ($\mathbb{Q}$ in characteristic 0 and $\mathbb{F}_p$ in characteristic $p$).

Suppose $\alpha_1, \ldots, \alpha_n \in M$ with $\alpha_i \in \alpha_{i+1}M$ for all $i < n$,
Let $F$ denote the prime field ($\mathbb{Q}$ in characteristic 0 and $\mathbb{F}_p$ in characteristic $p$).

Suppose $\alpha_1, \ldots, \alpha_n \in M$ with $\alpha_i \in \alpha_{i+1}M$ for all $i < n$, i.e.,

$$\alpha_1 R \subsetneq \alpha_2 R \subsetneq \cdots \subsetneq \alpha_n R.$$
Let $F$ denote the prime field ($\mathbb{Q}$ in characteristic 0 and $\mathbb{F}_p$ in characteristic $p$).

Suppose $\alpha_1, \ldots, \alpha_n \in \mathcal{M}$ with $\alpha_i \in \alpha_{i+1}\mathcal{M}$ for all $i < n$, i.e.,

$$\alpha_1 R \subsetneq \alpha_2 R \subsetneq \cdots \subsetneq \alpha_n R.$$ 

We claim that these elements are linearly independent over $F(\alpha_1)$. 

Let $F$ denote the prime field ($\mathbb{Q}$ in characteristic 0 and $\mathbb{F}_p$ in characteristic $p$).

Suppose $\alpha_1, \ldots, \alpha_n \in \mathcal{M}$ with $\alpha_i \in \alpha_{i+1} \mathcal{M}$ for all $i < n$, i.e.,

$$\alpha_1 R \subsetneq \alpha_2 R \subsetneq \cdots \subsetneq \alpha_n R.$$ 

We claim that these elements are linearly independent over $F(\alpha_1)$.

To see why, suppose

$$\sum_{i=1}^n P_i(\alpha_1) \alpha_i = 0$$
Let $F$ denote the prime field ($\mathbb{Q}$ in characteristic 0 and $\mathbb{F}_p$ in characteristic $p$).

Suppose $\alpha_1, \ldots, \alpha_n \in \mathcal{M}$ with $\alpha_i \in \alpha_{i+1}\mathcal{M}$ for all $i < n$, i.e.,

$$\alpha_1 R \subsetneq \alpha_2 R \subsetneq \cdots \subsetneq \alpha_n R.$$

We claim that these elements are linearly independent over $F(\alpha_1)$.

To see why, suppose

$$\sum_{i=1}^{n} P_i(\alpha_1)\alpha_i = 0$$

with $P_i(\alpha_1) \in F[\alpha_1]$ for all $i$. 
Let $F$ denote the prime field ($\mathbb{Q}$ in characteristic 0 and $\mathbb{F}_p$ in characteristic $p$).

Suppose $\alpha_1, \ldots, \alpha_n \in M$ with $\alpha_i \in \alpha_{i+1}M$ for all $i < n$, i.e.,

$$\alpha_1 R \subsetneq \alpha_2 R \subsetneq \cdots \subsetneq \alpha_n R.$$ 

We claim that these elements are linearly independent over $F(\alpha_1)$.

To see why, suppose

$$\sum_{i=1}^{n} P_i(\alpha_1) \alpha_i = 0$$

with $P_i(\alpha_1) \in F[\alpha_1]$ for all $i$. Without loss of generality $P_i(\alpha_1) \in \mathbb{Z}[\alpha_1]$ in characteristic 0,
Let $F$ denote the prime field ($\mathbb{Q}$ in characteristic 0 and $\mathbb{F}_p$ in characteristic $p$).

Suppose $\alpha_1, \ldots, \alpha_n \in M$ with $\alpha_i \in \alpha_{i+1}M$ for all $i < n$, i.e.,

$$\alpha_1 R \subsetneq \alpha_2 R \subsetneq \cdots \subsetneq \alpha_n R.$$ 

We claim that these elements are linearly independent over $F(\alpha_1)$.

To see why, suppose

$$\sum_{i=1}^{n} P_i(\alpha_1) \alpha_i = 0$$

with $P_i(\alpha_1) \in F[\alpha_1]$ for all $i$. Without loss of generality $P_i(\alpha_1) \in \mathbb{Z}[\alpha_1]$ in characteristic 0, so that in all cases $P_i(\alpha_1) \in R[\alpha_1] \subset R$. 

Let $F$ denote the prime field ($\mathbb{Q}$ in characteristic 0 and $\mathbb{F}_p$ in characteristic $p$).

Suppose $\alpha_1, \ldots, \alpha_n \in \mathcal{M}$ with $\alpha_i \in \alpha_{i+1} \mathcal{M}$ for all $i < n$, i.e.,

$$\alpha_1 R \subsetneq \alpha_2 R \subsetneq \cdots \subsetneq \alpha_n R.$$ 

We claim that these elements are linearly independent over $F(\alpha_1)$.

To see why, suppose

$$\sum_{i=1}^{n} P_i(\alpha_1) \alpha_i = 0$$

with $P_i(\alpha_1) \in F[\alpha_1]$ for all $i$. Without loss of generality $P_i(\alpha_1) \in \mathbb{Z}[\alpha_1]$ in characteristic 0, so that in all cases $P_i(\alpha_1) \in R[\alpha_1] \subset R$.

If not all $P_i(\alpha_1) = 0$, 

Let $F$ denote the prime field ($\mathbb{Q}$ in characteristic 0 and $\mathbb{F}_p$ in characteristic $p$).

Suppose $\alpha_1, \ldots, \alpha_n \in M$ with $\alpha_i \in \alpha_{i+1}M$ for all $i < n$, i.e.,

$$\alpha_1R \subsetneq \alpha_2R \subsetneq \cdots \subsetneq \alpha_nR.$$ 

We claim that these elements are linearly independent over $F(\alpha_1)$.

To see why, suppose

$$\sum_{i=1}^{n} P_i(\alpha_1)\alpha_i = 0$$

with $P_i(\alpha_1) \in F[\alpha_1]$ for all $i$. Without loss of generality $P_i(\alpha_1) \in \mathbb{Z}[\alpha_1]$ in characteristic 0, so that in all cases $P_i(\alpha_1) \in R[\alpha_1] \subset R$.

If not all $P_i(\alpha_1) = 0$, then without loss of generality they aren’t all divisible by $\alpha_1$, 

Math 681, Wednesday, February 24 February 24, 2021
Let $F$ denote the prime field ($\mathbb{Q}$ in characteristic 0 and $\mathbb{F}_p$ in characteristic $p$).

Suppose $\alpha_1, \ldots, \alpha_n \in \mathcal{M}$ with $\alpha_i \in \alpha_{i+1} \mathcal{M}$ for all $i < n$, i.e.,

$$\alpha_1 R \subsetneq \alpha_2 R \subsetneq \cdots \subsetneq \alpha_n R.$$

We claim that these elements are linearly independent over $F(\alpha_1)$.

To see why, suppose

$$\sum_{i=1}^{n} P_i(\alpha_1) \alpha_i = 0$$

with $P_i(\alpha_1) \in F[\alpha_1]$ for all $i$. Without loss of generality $P_i(\alpha_1) \in \mathbb{Z}[\alpha_1]$ in characteristic 0, so that in all cases $P_i(\alpha_1) \in R[\alpha_1] \subset R$.

If not all $P_i(\alpha_1) = 0$, then without loss of generality they aren’t all divisible by $\alpha_1$, so that there is a maximal index $i_0$ where $P_{i_0}(0) := a_{i_0} \neq 0$. 
We have

\[-P_{i_0}(\alpha_1)\alpha_{i_0} = \sum_{i \neq i_0} P_i(\alpha_1)\alpha_i\]
We have

\[-P_{i_0}(\alpha_1)\alpha_{i_0} = \sum_{i \neq i_0} P_i(\alpha_1)\alpha_i\]

\[-P_{i_0}(\alpha_1) = \sum_{i < i_0} P_i(\alpha_1)\alpha_i/\alpha_{i_0} + \sum_{i > i_0} P_i(\alpha_1)\alpha_i/\alpha_{i_0}.\]
We have

\[-P_{i_0}(\alpha_1)\alpha_{i_0} = \sum_{i \neq i_0} P_i(\alpha_1)\alpha_i\]

\[-P_{i_0}(\alpha_1) = \sum_{i < i_0} P_i(\alpha_1)\frac{\alpha_i}{\alpha_{i_0}} + \sum_{i > i_0} P_i(\alpha_1)\frac{\alpha_i}{\alpha_{i_0}}.\]

Now \(\alpha_i, P_i(\alpha_1) \in R\) for all \(i\),
We have

\[-P_{i_0}(\alpha_1)\alpha_{i_0} = \sum_{i \neq i_0} P_i(\alpha_1)\alpha_i\]

\[-P_{i_0}(\alpha_1) = \sum_{i < i_0} P_i(\alpha_1)\alpha_i/\alpha_{i_0} + \sum_{i > i_0} P_i(\alpha_1)\alpha_i/\alpha_{i_0}.\]

Now \(\alpha_i, P_i(\alpha_1) \in R\) for all \(i\), \(\alpha_i/\alpha_{i_0} \in \mathcal{M}\) for all \(i < i_0\) by hypothesis,
We have

\[-P_{i_0}(\alpha_1)\alpha_{i_0} = \sum_{i \neq i_0} P_i(\alpha_1)\alpha_i\]

\[-P_{i_0}(\alpha_1) = \sum_{i < i_0} P_i(\alpha_1)\alpha_i/\alpha_{i_0} + \sum_{i > i_0} P_i(\alpha_1)\alpha_i/\alpha_{i_0}.\]

Now \(\alpha_i, P_i(\alpha_1) \in R\) for all \(i\), \(\alpha_i/\alpha_{i_0} \in M\) for all \(i < i_0\) by hypothesis, and \(P_i(\alpha_1)/\alpha_{i_0} \in M\) for all \(i > i_0\).
We have

\[ -P_i(\alpha_1)\alpha_{i_0} = \sum_{i \neq i_0} P_i(\alpha_1)\alpha_i \]

\[ -P_i(\alpha_1) = \sum_{i < i_0} P_i(\alpha_1)\alpha_i/\alpha_{i_0} + \sum_{i > i_0} P_i(\alpha_1)\alpha_i/\alpha_{i_0}. \]

Now \( \alpha_i, P_i(\alpha_1) \in R \) for all \( i \), \( \alpha_i/\alpha_{i_0} \in M \) for all \( i < i_0 \) by hypothesis, and \( P_i(\alpha_1)/\alpha_{i_0} \in M \) for all \( i > i_0 \) since \( \alpha_1 | P_i(\alpha_1) \) for \( i > i_0 \) by construction.
We have

\[-P_{i_0}(\alpha_1)\alpha_{i_0} = \sum_{i \neq i_0} P_i(\alpha_1)\alpha_i\]

\[-P_{i_0}(\alpha_1) = \sum_{i < i_0} P_i(\alpha_1)\alpha_i/\alpha_{i_0} + \sum_{i > i_0} P_i(\alpha_1)\alpha_i/\alpha_{i_0}.\]

Now \(\alpha_i, P_i(\alpha_1) \in R\) for all \(i\), \(\alpha_i/\alpha_{i_0} \in M\) for all \(i < i_0\) by hypothesis, and \(P_i(\alpha_1)/\alpha_{i_0} \in M\) for all \(i > i_0\) since \(\alpha_1|P_i(\alpha_1)\) for \(i > i_0\) by construction and \(\alpha_{i_0}|\alpha_1\) by hypothesis.
We have

$$-P_{i_0}(\alpha_1)\alpha_{i_0} = \sum_{i \neq i_0} P_i(\alpha_1)\alpha_i$$

$$-P_{i_0}(\alpha_1) = \sum_{i < i_0} P_i(\alpha_1)\alpha_i/\alpha_{i_0} + \sum_{i > i_0} P_i(\alpha_1)\alpha_i/\alpha_{i_0}.$$ 

Now $\alpha_i, P_i(\alpha_1) \in R$ for all $i$, $\alpha_i/\alpha_{i_0} \in M$ for all $i < i_0$ by hypothesis, and $P_i(\alpha_1)/\alpha_{i_0} \in M$ for all $i > i_0$ since $\alpha_1 | P_i(\alpha_1)$ for $i > i_0$ by construction and $\alpha_{i_0} | \alpha_1$ by hypothesis. Thus $P_{i_0}(\alpha_1) \in M$. 


We have

\[-P_{i_0}(\alpha_1)\alpha_{i_0} = \sum_{i \neq i_0} P_i(\alpha_1)\alpha_i\]

\[-P_{i_0}(\alpha_1) = \sum_{i < i_0} P_i(\alpha_1)\alpha_i/\alpha_{i_0} + \sum_{i > i_0} P_i(\alpha_1)\alpha_i/\alpha_{i_0}.\]

Now \(\alpha_i, P_i(\alpha_1) \in R\) for all \(i\), \(\alpha_i/\alpha_{i_0} \in \mathcal{M}\) for all \(i < i_0\) by hypothesis, and \(P_i(\alpha_1)/\alpha_{i_0} \in \mathcal{M}\) for all \(i > i_0\) since \(\alpha_1|P_i(\alpha_1)\) for \(i > i_0\) by construction and \(\alpha_{i_0}|\alpha_1\) by hypothesis. Thus \(P_{i_0}(\alpha_1) \in \mathcal{M}\). Since \(\alpha_1|(P_i(\alpha_1) - a_{i_0})\),
We have

\[-P_{i_0}(\alpha_1)\alpha_{i_0} = \sum_{i \neq i_0} P_i(\alpha_1)\alpha_i\]

\[-P_{i_0}(\alpha_1) = \sum_{i < i_0} P_i(\alpha_1)\alpha_i/\alpha_{i_0} + \sum_{i > i_0} P_i(\alpha_1)\alpha_i/\alpha_{i_0}.\]

Now \(\alpha_i, P_i(\alpha_1) \in R\) for all \(i\), \(\alpha_i/\alpha_{i_0} \in M\) for all \(i < i_0\) by hypothesis, and \(P_i(\alpha_1)/\alpha_{i_0} \in M\) for all \(i > i_0\) since \(\alpha_1|P_i(\alpha_1)\) for \(i > i_0\) by construction and \(\alpha_{i_0}|\alpha_1\) by hypothesis. Thus \(P_{i_0}(\alpha_1) \in M\). Since \(\alpha_1|(P_i(\alpha_1) - a_{i_0})\), we see that \(a_{i_0} \in M\), too.
We have

\[-P_{i_0}(\alpha_1)\alpha_{i_0} = \sum_{i \neq i_0} P_i(\alpha_1)\alpha_i\]

\[-P_{i_0}(\alpha_1) = \sum_{i < i_0} P_i(\alpha_1)\alpha_i / \alpha_{i_0} + \sum_{i > i_0} P_i(\alpha_1)\alpha_i / \alpha_{i_0}.\]

Now $\alpha_i, P_i(\alpha_1) \in R$ for all $i$, $\alpha_i / \alpha_{i_0} \in \mathcal{M}$ for all $i < i_0$ by hypothesis, and $P_i(\alpha_1) / \alpha_{i_0} \in \mathcal{M}$ for all $i > i_0$ since $\alpha_1 | P_i(\alpha_1)$ for $i > i_0$ by construction and $\alpha_{i_0} | \alpha_1$ by hypothesis. Thus $P_{i_0}(\alpha_1) \in \mathcal{M}$. Since $\alpha_1 | (P_i(\alpha_1) - a_{i_0})$, we see that $a_{i_0} \in \mathcal{M}$, too.

But clearly $\mathcal{M} \cap F = \{0\}$. 
We have

\[-P_{i_0}(\alpha_1)\alpha_{i_0} = \sum_{i \neq i_0} P_i(\alpha_1)\alpha_i\]

\[-P_{i_0}(\alpha_1) = \sum_{i < i_0} P_i(\alpha_1)\alpha_i/\alpha_{i_0} + \sum_{i > i_0} P_i(\alpha_1)\alpha_i/\alpha_{i_0}.\]

Now \(\alpha_i, P_i(\alpha_1) \in R\) for all \(i\), \(\alpha_i/\alpha_{i_0} \in M\) for all \(i < i_0\) by hypothesis, and \(P_i(\alpha_1)/\alpha_{i_0} \in M\) for all \(i > i_0\) since \(\alpha_1 | P_i(\alpha_1)\) for \(i > i_0\) by construction and \(\alpha_{i_0} | \alpha_1\) by hypothesis. Thus \(P_{i_0}(\alpha_1) \in M\). Since \(\alpha_1 | (P_i(\alpha_1) - a_{i_0})\), we see that \(a_{i_0} \in M\), too.

But clearly \(M \cap F = \{0\}\). This contradiction shows that \(\alpha_1, \ldots, \alpha_n\) are linearly independent over \(F(\alpha_1)\).
In the number field case $n \leq [K : \mathbb{Q}(\alpha_1)] \leq [K : \mathbb{Q}]$. 
In the number field case \( n \leq [K : \mathbb{Q}(\alpha_1)] \leq [K : \mathbb{Q}] \).

In the function field case \( \alpha_1 \) is not in the field of constants.
In the number field case $n \leq [K : \mathbb{Q}(\alpha_1)] \leq [K : \mathbb{Q}]$. 

In the function field case $\alpha_1$ is not in the field of constants (it’s a non-zero element of $\mathcal{M}$, after all),
In the number field case \( n \leq [K : \mathbb{Q}(\alpha_1)] \leq [K : \mathbb{Q}] \).

In the function field case \( \alpha_1 \) is not in the field of constants (it’s a non-zero element of \( \mathcal{M} \), after all), whence it must be transcendental over \( \mathbb{F}_p \).
In the number field case $n \leq [K : \mathbb{Q}(\alpha_1)] \leq [K : \mathbb{Q}]$.

In the function field case $\alpha_1$ is not in the field of constants (it’s a non-zero element of $\mathcal{M}$, after all), whence it must be transcendental over $\mathbb{F}_p$. Therefore $n \leq [K : \mathbb{F}_p(\alpha_1)]$, which is a finite integer depending only on $\alpha_1$. 
In the number field case $n \leq [K : \mathbb{Q}(\alpha_1)] \leq [K : \mathbb{Q}]$.

In the function field case $\alpha_1$ is not in the field of constants (it’s a non-zero element of $\mathcal{M}$, after all), whence it must be transcendental over $\mathbb{F}_p$. Therefore $n \leq [K : \mathbb{F}_p(\alpha_1)]$, which is a finite integer depending only on $\alpha_1$.

We remark that in the case of number fields we have a slightly more direct argument for the Proposition as follows.
In the number field case \( n \leq [K : \mathbb{Q}(\alpha_1)] \leq [K : \mathbb{Q}] \).

In the function field case \( \alpha_1 \) is not in the field of constants (it’s a non-zero element of \( \mathcal{M} \), after all), whence it must be transcendental over \( \mathbb{F}_p \). Therefore \( n \leq [K : \mathbb{F}_p(\alpha_1)] \), which is a finite integer depending only on \( \alpha_1 \).

We remark that in the case of number fields we have a slightly more direct argument for the Proposition as follows.

Let \( \mathcal{M} \) denote the unique maximal ideal of \( R \).
In the number field case $n \leq [K : \mathbb{Q}(\alpha_1)] \leq [K : \mathbb{Q}]$.

In the function field case $\alpha_1$ is not in the field of constants (it’s a non-zero element of $\mathcal{M}$, after all), whence it must be transcendental over $\mathbb{F}_p$. Therefore $n \leq [K : \mathbb{F}_p(\alpha_1)]$, which is a finite integer depending only on $\alpha_1$.

We remark that in the case of number fields we have a slightly more direct argument for the Proposition as follows.

Let $\mathcal{M}$ denote the unique maximal ideal of $R$. Since $R \supset \mathfrak{O}_K$
In the number field case \( n \leq [K : \mathbb{Q}(\alpha_1)] \leq [K : \mathbb{Q}] \).

In the function field case \( \alpha_1 \) is not in the field of constants (it’s a non-zero element of \( \mathcal{M} \), after all), whence it must be transcendental over \( \mathbb{F}_p \). Therefore \( n \leq [K : \mathbb{F}_p(\alpha_1)] \), which is a finite integer depending only on \( \alpha_1 \).

We remark that in the case of number fields we have a slightly more direct argument for the Proposition as follows.

Let \( \mathcal{M} \) denote the unique maximal ideal of \( R \). Since \( R \supset \mathcal{O}_K \) we may restrict the canonical map \( R \to R/\mathcal{M} \) to \( \mathcal{O}_K \).
In the number field case \( n \leq [K : \mathbb{Q}(\alpha_1)] \leq [K : \mathbb{Q}] \).

In the function field case \( \alpha_1 \) is not in the field of constants (it’s a non-zero element of \( \mathcal{M} \), after all), whence it must be transcendental over \( \mathbb{F}_p \). Therefore \( n \leq [K : \mathbb{F}_p(\alpha_1)] \), which is a finite integer depending only on \( \alpha_1 \).

We remark that in the case of number fields we have a slightly more direct argument for the Proposition as follows.

Let \( \mathcal{M} \) denote the unique maximal ideal of \( R \). Since \( R \supset \mathcal{O}_K \) we may restrict the canonical map \( R \to R/\mathcal{M} \) to \( \mathcal{O}_K \) and get a kernel \( \mathfrak{P} = \mathcal{M} \cap \mathcal{O}_K \subseteq \mathcal{O}_K \).
In the number field case \( n \leq [K : \mathbb{Q}(\alpha_1)] \leq [K : \mathbb{Q}] \).

In the function field case \( \alpha_1 \) is not in the field of constants (it’s a non-zero element of \( \mathcal{M} \), after all), whence it must be transcendental over \( \mathbb{F}_p \). Therefore \( n \leq [K : \mathbb{F}_p(\alpha_1)] \), which is a finite integer depending only on \( \alpha_1 \).

We remark that in the case of number fields we have a slightly more direct argument for the Proposition as follows.

Let \( \mathcal{M} \) denote the unique maximal ideal of \( R \). Since \( R \supset \mathcal{O}_K \) we may restrict the canonical map \( R \to R/\mathcal{M} \) to \( \mathcal{O}_K \) and get a kernel \( \mathfrak{P} = \mathcal{M} \cap \mathcal{O}_K \subsetneq \mathcal{O}_K \) (\( 1 \notin \mathcal{M} \), for example).
In the number field case \( n \leq [K : \mathbb{Q}(\alpha_1)] \leq [K : \mathbb{Q}] \).

In the function field case \( \alpha_1 \) is not in the field of constants (it’s a non-zero element of \( \mathcal{M} \), after all), whence it must be transcendental over \( \mathbb{F}_p \). Therefore \( n \leq [K : \mathbb{F}_p(\alpha_1)] \), which is a finite integer depending only on \( \alpha_1 \).

We remark that in the case of number fields we have a slightly more direct argument for the Proposition as follows.

Let \( \mathcal{M} \) denote the unique maximal ideal of \( R \). Since \( R \supset \mathcal{O}_K \) we may restrict the canonical map \( R \to R/\mathcal{M} \) to \( \mathcal{O}_K \) and get a kernel \( \mathfrak{p} = \mathcal{M} \cap \mathcal{O}_K \subsetneq \mathcal{O}_K \) (1 \( \notin \mathcal{M} \), for example). Since \( R/\mathcal{M} \) is a field,
In the number field case $n \leq [K : \mathbb{Q}(\alpha_1)] \leq [K : \mathbb{Q}]$.

In the function field case $\alpha_1$ is not in the field of constants (it’s a non-zero element of $\mathcal{M}$, after all), whence it must be transcendental over $\mathbb{F}_p$. Therefore $n \leq [K : \mathbb{F}_p(\alpha_1)]$, which is a finite integer depending only on $\alpha_1$.

We remark that in the case of number fields we have a slightly more direct argument for the Proposition as follows.

Let $\mathcal{M}$ denote the unique maximal ideal of $R$. Since $R \supset \mathfrak{O}_K$ we may restrict the canonical map $R \to R/\mathcal{M}$ to $\mathfrak{O}_K$ and get a kernel $\mathfrak{P} = \mathcal{M} \cap \mathfrak{O}_K \subseteq \mathfrak{O}_K \not\subseteq \mathfrak{O}_K$ ($1 \not\in \mathcal{M}$, for example). Since $R/\mathcal{M}$ is a field, the image of the canonical map restricted to $\mathfrak{O}_K$ is necessarily an integral domain,
In the number field case $n \leq [K : \mathbb{Q}(\alpha_1)] \leq [K : \mathbb{Q}]$.

In the function field case $\alpha_1$ is not in the field of constants (it’s a non-zero element of $\mathcal{M}$, after all), whence it must be transcendental over $\mathbb{F}_p$. Therefore $n \leq [K : \mathbb{F}_p(\alpha_1)]$, which is a finite integer depending only on $\alpha_1$.

We remark that in the case of number fields we have a slightly more direct argument for the Proposition as follows.

Let $\mathcal{M}$ denote the unique maximal ideal of $R$. Since $R \supset \mathfrak{O}_K$ we may restrict the canonical map $R \to R/\mathcal{M}$ to $\mathfrak{O}_K$ and get a kernel $\mathfrak{P} = \mathcal{M} \cap \mathfrak{O}_K \subsetneq \mathfrak{O}_K$ ($1 \notin \mathcal{M}$, for example). Since $R/\mathcal{M}$ is a field, the image of the canonical map restricted to $\mathfrak{O}_K$ is necessarily an integral domain, so that $\mathfrak{P}$ is a prime ideal.
In the number field case \( n \leq [K : \mathbb{Q}(\alpha_1)] \leq [K : \mathbb{Q}] \).

In the function field case \( \alpha_1 \) is not in the field of constants (it’s a non-zero element of \( \mathcal{M} \), after all), whence it must be transcendental over \( \mathbb{F}_p \).

Therefore \( n \leq [K : \mathbb{F}_p(\alpha_1)] \), which is a finite integer depending only on \( \alpha_1 \).

We remark that in the case of number fields we have a slightly more direct argument for the Proposition as follows.

Let \( \mathcal{M} \) denote the unique maximal ideal of \( R \). Since \( R \supset \mathcal{O}_K \) we may restrict the canonical map \( R \rightarrow R/\mathcal{M} \) to \( \mathcal{O}_K \) and get a kernel \( \mathfrak{P} = \mathcal{M} \cap \mathcal{O}_K \subseteq \mathcal{O}_K \) (\( 1 \notin \mathcal{M} \), for example). Since \( R/\mathcal{M} \) is a field, the image of the canonical map restricted to \( \mathcal{O}_K \) is necessarily an integral domain, so that \( \mathfrak{P} \) is a prime ideal. It certainly isn’t the zero ideal,
In the number field case $n \leq [K : \mathbb{Q}(\alpha_1)] \leq [K : \mathbb{Q}]$.

In the function field case $\alpha_1$ is not in the field of constants (it’s a non-zero element of $\mathcal{M}$, after all), whence it must be transcendental over $\mathbb{F}_p$. Therefore $n \leq [K : \mathbb{F}_p(\alpha_1)]$, which is a finite integer depending only on $\alpha_1$.

We remark that in the case of number fields we have a slightly more direct argument for the Proposition as follows.

Let $\mathcal{M}$ denote the unique maximal ideal of $R$. Since $R \supset \mathcal{O}_K$ we may restrict the canonical map $R \to R/\mathcal{M}$ to $\mathcal{O}_K$ and get a kernel $\mathfrak{P} = \mathcal{M} \cap \mathcal{O}_K \subseteq \mathcal{O}_K$ ($1 \notin \mathcal{M}$, for example). Since $R/\mathcal{M}$ is a field, the image of the canonical map restricted to $\mathcal{O}_K$ is necessarily an integral domain, so that $\mathfrak{P}$ is a prime ideal. It certainly isn’t the zero ideal, since then all non-zero elements of $\mathcal{O}_K$ would be units.
In the number field case $n \leq [K : \mathbb{Q}(\alpha_1)] \leq [K : \mathbb{Q}]$.

In the function field case $\alpha_1$ is not in the field of constants (it’s a non-zero element of $\mathcal{M}$, after all), whence it must be transcendental over $\mathbb{F}_p$. Therefore $n \leq [K : \mathbb{F}_p(\alpha_1)]$, which is a finite integer depending only on $\alpha_1$.

We remark that in the case of number fields we have a slightly more direct argument for the Proposition as follows.

Let $\mathcal{M}$ denote the unique maximal ideal of $R$. Since $R \supset \mathcal{O}_K$ we may restrict the canonical map $R \to R/\mathcal{M}$ to $\mathcal{O}_K$ and get a kernel $\mathfrak{P} = \mathcal{M} \cap \mathcal{O}_K \subseteq \mathcal{O}_K$ ($1 \notin \mathcal{M}$, for example). Since $R/\mathcal{M}$ is a field, the image of the canonical map restricted to $\mathcal{O}_K$ is necessarily an integral domain, so that $\mathfrak{P}$ is a prime ideal. It certainly isn’t the zero ideal, since then all non-zero elements of $\mathcal{O}_K$ would be units implying that $R$ is the entire quotient field of $K$ of $\mathcal{O}_K$. 
In the number field case \( n \leq [K : \mathbb{Q}(\alpha_1)] \leq [K : \mathbb{Q}] \).

In the function field case \( \alpha_1 \) is not in the field of constants (it’s a non-zero element of \( \mathcal{M} \), after all), whence it must be transcendental over \( \mathbb{F}_p \). Therefore \( n \leq [K : \mathbb{F}_p(\alpha_1)] \), which is a finite integer depending only on \( \alpha_1 \).

We remark that in the case of number fields we have a slightly more direct argument for the Proposition as follows.

Let \( \mathcal{M} \) denote the unique maximal ideal of \( R \). Since \( R \supseteq \mathfrak{O}_K \) we may restrict the canonical map \( R \to R/\mathcal{M} \) to \( \mathfrak{O}_K \) and get a kernel \( \mathfrak{P} = \mathcal{M} \cap \mathfrak{O}_K \subseteq \mathfrak{O}_K \) (\( 1 \notin \mathcal{M} \), for example). Since \( R/\mathcal{M} \) is a field, the image of the canonical map restricted to \( \mathfrak{O}_K \) is necessarily an integral domain, so that \( \mathfrak{P} \) is a prime ideal. It certainly isn’t the zero ideal, since then all non-zero elements of \( \mathfrak{O}_K \) would be units implying that \( R \) is the entire quotient field of \( K \) of \( \mathcal{O}_K \).

Thus \( \mathfrak{P} \) is a maximal ideal of \( \mathfrak{O}_K \).
In the number field case \( n \leq [K : \mathbb{Q}(\alpha_1)] \leq [K : \mathbb{Q}] \).

In the function field case \( \alpha_1 \) is not in the field of constants (it’s a non-zero element of \( \mathcal{M} \), after all), whence it must be transcendental over \( \mathbb{F}_p \).

Therefore \( n \leq [K : \mathbb{F}_p(\alpha_1)] \), which is a finite integer depending only on \( \alpha_1 \).

We remark that in the case of number fields we have a slightly more direct argument for the Proposition as follows.

Let \( \mathcal{M} \) denote the unique maximal ideal of \( R \). Since \( R \supset \mathcal{O}_K \) we may restrict the canonical map \( R \to R/\mathcal{M} \) to \( \mathcal{O}_K \) and get a kernel \( \mathfrak{p} = \mathcal{M} \cap \mathcal{O}_K \subsetneq \mathcal{O}_K \) (\( 1 \notin \mathcal{M} \), for example). Since \( R/\mathcal{M} \) is a field, the image of the canonical map restricted to \( \mathcal{O}_K \) is necessarily an integral domain, so that \( \mathfrak{p} \) is a prime ideal. It certainly isn’t the zero ideal, since then all non-zero elements of \( \mathcal{O}_K \) would be units implying that \( R \) is the entire quotient field of \( K \) of \( \mathcal{O}_K \).

Thus \( \mathfrak{p} \) is a maximal ideal of \( \mathcal{O}_K \).

It is now almost trivial to show that \( R = \mathcal{O}_{\mathfrak{p}} \),
In the number field case $n \leq [K : \mathbb{Q}(\alpha_1)] \leq [K : \mathbb{Q}]$.

In the function field case $\alpha_1$ is not in the field of constants (it’s a non-zero element of $\mathcal{M}$, after all), whence it must be transcendental over $\mathbb{F}_p$. Therefore $n \leq [K : \mathbb{F}_p(\alpha_1)]$, which is a finite integer depending only on $\alpha_1$.

We remark that in the case of number fields we have a slightly more direct argument for the Proposition as follows.

Let $\mathcal{M}$ denote the unique maximal ideal of $R$. Since $R \supset \mathcal{O}_K$ we may restrict the canonical map $R \to R/\mathcal{M}$ to $\mathcal{O}_K$ and get a kernel $\mathfrak{P} = \mathcal{M} \cap \mathcal{O}_K \subseteq \mathcal{O}_K$ (1 $\not\in \mathcal{M}$, for example). Since $R/\mathcal{M}$ is a field, the image of the canonical map restricted to $\mathcal{O}_K$ is necessarily an integral domain, so that $\mathfrak{P}$ is a prime ideal. It certainly isn’t the zero ideal, since then all non-zero elements of $\mathcal{O}_K$ would be units implying that $R$ is the entire quotient field of $K$ of $\mathcal{O}_K$.

Thus $\mathfrak{P}$ is a maximal ideal of $\mathcal{O}_K$.

It is now almost trivial to show that $R = \mathcal{O}_\mathfrak{P}$, which was shown to be a principal ideal domain in an exercise.
The argument above relies on the Fundamental Theorem, however,
The argument above relies on the Fundamental Theorem, however, whereas our proof of Proposition 1 is more self-contained.
The argument above relies on the Fundamental Theorem, however, whereas our proof of Proposition 1 is more self-contained.

**Proposition (2)**

Let \(|·|\) be a non-trivial non-archimedean absolute value on \(K\), where \(K\) is either a number field or a function field. Then

\[ |\alpha| = \exp\left(-\rho v_R(\alpha)\right) \]

for some valuation ring \(R\) of \(K\) and \(\rho > 0\).
The argument above relies on the Fundamental Theorem, however, whereas our proof of Proposition 1 is more self-contained.

Proposition (2)

Let $|\cdot|$ be a non-trivial non-archimedean absolute value on $K$, 

The argument above relies on the Fundamental Theorem, however, whereas our proof of Proposition 1 is more self-contained.

**Proposition (2)**

Let \( |\cdot| \) be a non-trivial non-archimedean absolute value on \( K \), where \( K \) is either a number field or a function field.
The argument above relies on the Fundamental Theorem, however, whereas our proof of Proposition 1 is more self-contained.

**Proposition (2)**

Let $|·|$ be a non-trivial non-archimedean absolute value on $K$, where $K$ is either a number field or a function field. Then $|α| = \exp\left(-ρ v_R(α)\right)$ for some valuation ring $R$ of $K$ and $ρ > 0$. 
Proof: By exercise #4 from the seventh homework assignment,
Proof: By exercise #4 from the seventh homework assignment, 
\[ R := \{ \alpha \in K : |\alpha| \leq 1 \} \] 
is a valuation ring on \( K \).
**Proof:** By exercise #4 from the seventh homework assignment, \( R := \{ \alpha \in K : |\alpha| \leq 1 \} \) is a valuation ring on \( K \).

By Proposition 1 this must be a discrete valuation ring
Proof: By exercise #4 from the seventh homework assignment, \( R := \{ \alpha \in K : |\alpha| \leq 1 \} \) is a valuation ring on \( K \).

By Proposition 1 this must be a discrete valuation ring with maximal ideal \( \mathcal{M} = \{ \alpha \in K : |\alpha| < 1 \} \).
Proof: By exercise #4 from the seventh homework assignment, 

\( R := \{ \alpha \in K : |\alpha| \leq 1 \} \) is a valuation ring on \( K \).

By Proposition 1 this must be a discrete valuation ring with maximal ideal

\[ \mathcal{M} = \{ \alpha \in K : |\alpha| < 1 \} . \]

Write \( \mathcal{M} = \pi R \)
**Proof:** By exercise #4 from the seventh homework assignment, 
\[ R := \{ \alpha \in K : |\alpha| \leq 1 \} \] is a valuation ring on \( K \).

By Proposition 1 this must be a discrete valuation ring with maximal ideal

\[ \mathcal{M} = \{ \alpha \in K : |\alpha| < 1 \}. \]

Write \( \mathcal{M} = \pi R \) and set \( \rho = \log |\pi^{-1}| > 0 \).
**Proof:** By exercise #4 from the seventh homework assignment, 
\[ R := \{ \alpha \in K : |\alpha| \leq 1 \} \] is a valuation ring on \( K \).

By Proposition 1 this must be a discrete valuation ring with maximal ideal

\[ \mathcal{M} = \{ \alpha \in K : |\alpha| < 1 \}. \]

Write \( \mathcal{M} = \pi R \) and set \( \rho = \log |\pi^{-1}| > 0 \).

For any non-zero \( \alpha \in K \) we have
**Proof:** By exercise #4 from the seventh homework assignment, 
\[ R := \{ \alpha \in K : |\alpha| \leq 1 \} \] is a valuation ring on \( K \).

By Proposition 1 this must be a discrete valuation ring with maximal ideal 
\[ \mathcal{M} = \{ \alpha \in K : |\alpha| < 1 \}. \]

Write \( \mathcal{M} = \pi R \) and set \( \rho = \log |\pi^{-1}| > 0 \).

For any non-zero \( \alpha \in K \) we have \( \alpha = u\pi^{v_R(\alpha)} \) for some unit \( u \) by Lemma 3,
Proof: By exercise #4 from the seventh homework assignment, 
\( R := \{ \alpha \in K : |\alpha| \leq 1 \} \) is a valuation ring on \( K \).

By Proposition 1 this must be a discrete valuation ring with maximal ideal 
\[ \mathfrak{M} = \{ \alpha \in K : |\alpha| < 1 \}. \]

Write \( \mathfrak{M} = \pi R \) and set \( \rho = \log |\pi^{-1}| > 0 \).

For any non-zero \( \alpha \in K \) we have \( \alpha = u\pi^{v_R(\alpha)} \) for some unit \( u \) by Lemma 3, so that \( |\alpha| = |\pi^{v(\alpha)}| = \exp (-\rho v(\alpha)) \).