Recall that if \( R \) is a subring of a field \( K \), either a number field or a function field, then an element \( \alpha \in K \) is called integral over \( R \) if \( \alpha \) is a root of some non-zero monic polynomial in \( R[X] \).

The integral closure of \( R \) in \( K \) is the set of all elements of \( K \) that are integral over \( R \).

We've seen that this is a subring of \( K \).

The ring \( R \) is called integrally closed in its quotient field \( K_0 \subseteq K \) if all elements of \( K_0 \) integral over \( R \) are actually elements of \( R \).

An example here would be \( \mathcal{O}_K \subseteq K \).
Recall that if $R$ is a subring of a field $K$, the \textbf{integral closure} of $R$ in $K$ is the set of all elements of $K$ that are integral over $R$. We've seen that this is a subring of $K$. The ring $R$ is called \textbf{integrally closed} in its quotient field $K_0 \subseteq K$ if all elements of $K_0$ integral over $R$ are actually elements of $R$. An example here would be $O_K \subset K$. 
Recall that if \( R \) is a subring of a field \( K \), either a number field or a function field,
Recall that if $R$ is a subring of a field $K$, either a number field or a function field, then an element $\alpha \in K$ is called integral over $R$ if
Recall that if $R$ is a subring of a field $K$, either a number field or a function field, then an element $\alpha \in K$ is called integral over $R$ if $\alpha$ is a root of some non-zero monic polynomial in $R[X]$. The integral closure of $R$ in $K$ is the set of all elements of $K$ that are integral over $R$. We've seen that this is a subring of $K$. The ring $R$ is called integrally closed in its quotient field $K_0 \subseteq K$ if all elements of $K_0$ integral over $R$ are actually elements of $R$. An example here would be $\mathcal{O}_K \subset K$. 

\[ \text{} \]
Recall that if $R$ is a subring of a field $K$, either a number field or a function field, then an element $\alpha \in K$ is called \textit{integral over} $R$ if $\alpha$ is a root of some non-zero monic polynomial in $R[X]$. The \textit{integral closure} of $R$ in $K$ is the set of all elements of $K$ that are integral over $R$. 
Recall that if $R$ is a subring of a field $K$, either a number field or a function field, then an element $\alpha \in K$ is called integral over $R$ if $\alpha$ is a root of some non-zero monic polynomial in $R[X]$. The integral closure of $R$ in $K$ is the set of all elements of $K$ that are integral over $R$. We’ve seen that this is a subring of $K$. 

Recall that if $R$ is a subring of a field $K$, either a number field or a function field, then an element $\alpha \in K$ is called \textit{integral over} $R$ if $\alpha$ is a root of some non-zero monic polynomial in $R[X]$. The \textit{integral closure} of $R$ in $K$ is the set of all elements of $K$ that are integral over $R$.

We’ve seen that this is a subring of $K$.

The ring $R$ is called \textit{integrally closed} in its quotient field $K_0 \subseteq K$ if
Recall that if $R$ is a subring of a field $K$, either a number field or a function field, then an element $\alpha \in K$ is called integral over $R$ if $\alpha$ is a root of some non-zero monic polynomial in $R[X]$. The integral closure of $R$ in $K$ is the set of all elements of $K$ that are integral over $R$. We’ve seen that this is a subring of $K$. The ring $R$ is called integrally closed in its quotient field $K_0 \subseteq K$ if all elements of $K_0$ integral over $R$ are actually elements of $R$. 
Recall that if $R$ is a subring of a field $K$, either a number field or a function field, then an element $\alpha \in K$ is called integral over $R$ if $\alpha$ is a root of some non-zero monic polynomial in $R[X]$. The integral closure of $R$ in $K$ is the set of all elements of $K$ that are integral over $R$. We’ve seen that this is a subring of $K$. The ring $R$ is called integrally closed in its quotient field $K_0 \subseteq K$ if all elements of $K_0$ integral over $R$ are actually elements of $R$. An example here would be $\mathcal{O}_K \subseteq K$. 
Definition

Let $S \subseteq M(K)$ be a proper non-empty set of places contained in the set of all non-archimedian places of $K$. The $S$-integers of $K$ is the subring $O_S = \{ \alpha \in K : |\alpha|_v \leq 1 \text{ all } v \in S \} = \bigcap_{v \in S} R_v$, where $R_v$ is the valuation ring associated with $v$, as usual, and $|\cdot|_v$ is any absolute value in the place $v$.

Examples:
1. Suppose $K$ is a number field and $S$ is the set of all non-archimedean places. Then $O_S = O_K$, the usual ring of algebraic integers of $K$.
2. Suppose $K = \mathbb{F}_q(X)$ is a field of rational functions and $S$ consists of all places except the place corresponding to taking the degree. Then $O_S = \mathbb{F}_q[X]$ is the ring of polynomials in $X$. 

Math 681, Wednesday, April 7

April 9, 2021
### Definition

Let $S \subset M(K)$ be a proper non-empty set of places contained in the set of all non-archimedian places of $K$.

<table>
<thead>
<tr>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Suppose $K$ is a number field and $S$ is the set of all non-archimedean places. Then $O_S = O_K$, the usual ring of algebraic integers of $K$.</td>
</tr>
<tr>
<td>2. Suppose $K = \mathbb{F}_q(X)$ is a field of rational functions and $S$ consists of all places except the place corresponding to taking the degree. Then $O_S = \mathbb{F}_q[X]$ is the ring of polynomials in $X$.</td>
</tr>
</tbody>
</table>
Definition

Let $S \subsetneq M(K)$ be a proper non-empty set of places contained in the set of all non-archimedian places of $K$. The $S$-integers of $K$ is the subring

$$\mathcal{O}_S = \{ \alpha \in K : |\alpha|_v \leq 1 \text{ all } v \in S \} = \bigcap_{v \in S} R_v,$$
Definition

Let \( S \subsetneq M(K) \) be a proper non-empty set of places contained in the set of all non-archimedian places of \( K \). The \( S \)-integers of \( K \) is the subring

\[
\mathcal{O}_S = \{ \alpha \in K : |\alpha|_v \leq 1 \text{ all } v \in S \} = \bigcap_{v \in S} R_v,
\]

where \( R_v \) is the valuation ring associated with \( v \), as usual,
Definition

Let $S \subsetneq M(K)$ be a proper non-empty set of places contained in the set of all non-archimedian places of $K$. The $S$-integers of $K$ is the subring

$$\mathcal{O}_S = \{\alpha \in K : |\alpha|_v \leq 1 \text{ all } v \in S\} = \bigcap_{v \in S} R_v,$$

where $R_v$ is the valuation ring associated with $v$, as usual, and $|\cdot|_v$ is any absolute value in the place $v$. 

Examples:

1. Suppose $K$ is a number field and $S$ is the set of all non-archimedean places. Then $\mathcal{O}_S = \mathcal{O}_K$, the usual ring of algebraic integers of $K$.

2. Suppose $K = \mathbb{F}_q(X)$ is a field of rational functions and $S$ consists of all places except the place corresponding to taking the degree. Then $\mathcal{O}_S = \mathbb{F}_q[X]$ is the ring of polynomials in $X$. 

Definition

Let $S \subset M(K)$ be a proper non-empty set of places contained in the set of all non-archimedian places of $K$. The $S$-integers of $K$ is the subring

$$\mathcal{O}_S = \{ \alpha \in K : |\alpha|_v \leq 1 \text{ all } v \in S \} = \bigcap_{v \in S} R_v,$$

where $R_v$ is the valuation ring associated with $v$, as usual, and $|\cdot|_v$ is any absolute value in the place $v$.

Examples:
Definition

Let \( S \subsetneq M(K) \) be a proper non-empty set of places contained in the set of all non-archimedian places of \( K \). The \( S \)-integers of \( K \) is the subring

\[
\mathcal{O}_S = \{ \alpha \in K : |\alpha|_v \leq 1 \text{ all } v \in S \} = \bigcap_{v \in S} R_v,
\]

where \( R_v \) is the valuation ring associated with \( v \), as usual, and \( |\cdot|_v \) is any absolute value in the place \( v \).

Examples: 1. Suppose \( K \) is a number field and \( S \) is the set of all non-archimedean places.
Definition

Let $S \subsetneq M(K)$ be a proper non-empty set of places contained in the set of all non-archimedean places of $K$. The $S$-integers of $K$ is the subring

$$\mathcal{O}_S = \{ \alpha \in K : |\alpha|_v \leq 1 \text{ all } v \in S \} = \bigcap_{v \in S} R_v,$$

where $R_v$ is the valuation ring associated with $v$, as usual, and $|\cdot|_v$ is any absolute value in the place $v$.

Examples: 1. Suppose $K$ is a number field and $S$ is the set of all non-archimedean places. Then $\mathcal{O}_S = \mathcal{O}_K$, the usual ring of algebraic integers of $K$. 

Definition

Let $S \subset M(K)$ be a proper non-empty set of places contained in the set of all non-archimedean places of $K$. The $S$-integers of $K$ is the subring

$$\mathfrak{O}_S = \{ \alpha \in K : |\alpha|_v \leq 1 \text{ all } v \in S \} = \bigcap_{v \in S} R_v,$$

where $R_v$ is the valuation ring associated with $v$, as usual, and $|\cdot|_v$ is any absolute value in the place $v$.

Examples: 1. Suppose $K$ is a number field and $S$ is the set of all non-archimedean places. Then $\mathfrak{O}_S = \mathfrak{O}_K$, the usual ring of algebraic integers of $K$.
2. Suppose $K = \mathbb{F}_q(X)$ is a field of rational functions
Definition

Let $S \subset M(K)$ be a proper non-empty set of places contained in the set of all non-archimedian places of $K$. The $S$-integers of $K$ is the subring

$$\mathcal{O}_S = \{ \alpha \in K : |\alpha|_v \leq 1 \text{ all } v \in S \} = \bigcap_{v \in S} R_v,$$

where $R_v$ is the valuation ring associated with $v$, as usual, and $|\cdot|_v$ is any absolute value in the place $v$.

Examples: 1. Suppose $K$ is a number field and $S$ is the set of all non-archimedean places. Then $\mathcal{O}_S = \mathcal{O}_K$, the usual ring of algebraic integers of $K$.

2. Suppose $K = \mathbb{F}_q(X)$ is a field of rational functions and $S$ consists of all places except the place corresponding to taking the degree.
**Definition**

Let \( S \subset M(K) \) be a proper non-empty set of places contained in the set of all non-archimedean places of \( K \). The **\( S \)-integers** of \( K \) is the subring

\[
\mathfrak{O}_S = \{ \alpha \in K : |\alpha|_v \leq 1 \text{ all } v \in S \} = \bigcap_{v \in S} R_v,
\]

where \( R_v \) is the valuation ring associated with \( v \), as usual, and \( |\cdot|_v \) is any absolute value in the place \( v \).

**Examples:** 1. Suppose \( K \) is a number field and \( S \) is the set of all non-archimedean places. Then \( \mathfrak{O}_S = \mathfrak{O}_K \), the usual ring of algebraic integers of \( K \).
2. Suppose \( K = \mathbb{F}_q(X) \) is a field of rational functions and \( S \) consists of all places except the place corresponding to taking the degree. Then \( \mathfrak{O}_S = \mathbb{F}_q[X] \) is the ring of polynomials in \( X \).
Lemma (1)

The quotient field of the ring of $S$-integers is all of $K$ and $O_S$ is integrally closed.

Proof:
Clearly $O_S \supseteq O_K$ in the number field case, so that the quotient field of $O_S$ is the quotient field of $O_K$, which is $K$.

In the function field case, an application of the Strong Approximation Theorem shows that for all non-zero $\alpha \in K$ there is a $\beta \in K$ with $\operatorname{ord}_v(\beta) \geq \max\{0, \operatorname{ord}_v(\alpha - 1)\}$, $v \in S$.

Notice that $\beta \in O_S$, as is $\alpha \beta$, so that $\alpha$ is in the quotient field of $O_S$.

Now suppose $\alpha \in K$ is integral over $O_S$ and write $\alpha^n + \beta^n - 1 \alpha^{n-1} + \cdots + \beta_1 \alpha + \beta_0 = 0$, where the $\beta_i$'s are all in $O_S$.

If $\operatorname{ord}_v(\alpha) < 0$ for some place $v \in S$, then $\operatorname{ord}_v(\alpha^n) = n \operatorname{ord}_v(\alpha) < \min\{0, \operatorname{ord}_v(\alpha - 1)\}$ for all $i = 0, \ldots, n-1$.

But this can't happen by the ultra-metric inequality!

Therefore $\alpha \in O_S$. 

Lemma (1)

The quotient field of the ring of S-integers is all of $K$
Lemma (1)

The quotient field of the ring of $S$-integers is all of $K$ and $\mathcal{O}_S$ is integrally closed.

Proof:

Clearly $\mathcal{O}_S \supseteq \mathcal{O}_K$ in the number field case, so that the quotient field of $\mathcal{O}_S$ is the quotient field of $\mathcal{O}_K$, which is $K$.

In the function field case, an application of the Strong Approximation Theorem shows that for all non-zero $\alpha \in K$ there is a $\beta \in K$ with $\text{ord}_v(\beta) \geq \max\{0, \text{ord}_v(\alpha - 1)\}$, $v \in S$.

Notice that $\beta \in \mathcal{O}_S$, as is $\alpha \beta$, so that $\alpha$ is in the quotient field of $\mathcal{O}_S$.

Now suppose $\alpha \in K$ is integral over $\mathcal{O}_S$ and write $\alpha n + \beta n - 1\alpha n - 1 + \cdots + \beta 1\alpha + \beta 0 = 0$, where the $\beta_i$'s are all in $\mathcal{O}_S$.

If $\text{ord}_v(\alpha) < 0$ for some place $v \in S$, then $\text{ord}_v(\alpha n) = n\text{ord}_v(\alpha) < i\text{ord}_v(\beta_i\alpha^i) \leq \text{ord}_v(\beta_i\alpha^i)$ for all $i = 0, \ldots, n - 1$.

But this can't happen by the ultra-metric inequality!

Therefore $\alpha \in \mathcal{O}_S$. 
Lemma (1)

The quotient field of the ring of $S$-integers is all of $K$ and $\mathfrak{D}_S$ is integrally closed.

Proof:
Lemma (1)

The quotient field of the ring of $S$-integers is all of $K$ and $\mathcal{O}_S$ is integrally closed.

Proof: Clearly $\mathcal{O}_S \supseteq \mathcal{O}_K$ in the number field case,
Lemma (1)

The quotient field of the ring of $S$-integers is all of $K$ and $\mathcal{O}_S$ is integrally closed.

Proof: Clearly $\mathcal{O}_S \supseteq \mathcal{O}_K$ in the number field case, so that the quotient field of $\mathcal{O}_S$ is the quotient field of $\mathcal{O}_K$,
Lemma (1)

The quotient field of the ring of $S$-integers is all of $K$ and $\mathcal{O}_S$ is integrally closed.

**Proof**: Clearly $\mathcal{O}_S \supseteq \mathcal{O}_K$ in the number field case, so that the quotient field of $\mathcal{O}_S$ is the quotient field of $\mathcal{O}_K$, which is $K$. 
Lemma (1)

The quotient field of the ring of $S$-integers is all of $K$ and $\mathcal{O}_S$ is integrally closed.

**Proof:** Clearly $\mathcal{O}_S \supseteq \mathcal{O}_K$ in the number field case, so that the quotient field of $\mathcal{O}_S$ is the quotient field of $\mathcal{O}_K$, which is $K$. In the function field case, an application of the Strong Approximation Theorem
Lemma (1)

The quotient field of the ring of $S$-integers is all of $K$ and $\mathfrak{O}_S$ is integrally closed.

Proof: Clearly $\mathfrak{O}_S \supseteq \mathfrak{O}_K$ in the number field case, so that the quotient field of $\mathfrak{O}_S$ is the quotient field of $\mathfrak{O}_K$, which is $K$.

In the function field case, an application of the Strong Approximation Theorem shows that for all non-zero $\alpha \in K$ there is a $\beta \in K$ with
Lemma (1)

The quotient field of the ring of $S$-integers is all of $K$ and $\mathcal{O}_S$ is integrally closed.

Proof: Clearly $\mathcal{O}_S \supseteq \mathcal{O}_K$ in the number field case, so that the quotient field of $\mathcal{O}_S$ is the quotient field of $\mathcal{O}_K$, which is $K$.

In the function field case, an application of the Strong Approximation Theorem shows that for all non-zero $\alpha \in K$ there is a $\beta \in K$ with

$$\text{ord}_v(\beta) \geq \max\{0, \text{ord}_v(\alpha^{-1})\}, \quad v \in S.$$
Lemma (1)

The quotient field of the ring of $S$-integers is all of $K$ and $\mathfrak{O}_S$ is integrally closed.

Proof: Clearly $\mathfrak{O}_S \supseteq \mathfrak{O}_K$ in the number field case, so that the quotient field of $\mathfrak{O}_S$ is the quotient field of $\mathfrak{O}_K$, which is $K$.

In the function field case, an application of the Strong Approximation Theorem shows that for all non-zero $\alpha \in K$ there is a $\beta \in K$ with

$$\text{ord}_v(\beta) \geq \max\{0, \text{ord}_v(\alpha^{-1})\}, \quad v \in S.$$ 

Notice that $\beta \in \mathfrak{O}_S$, ...
Lemma (1)

*The quotient field of the ring of $S$-integers is all of $K$ and $\mathcal{O}_S$ is integrally closed.*

**Proof:** Clearly $\mathcal{O}_S \supseteq \mathcal{O}_K$ in the number field case, so that the quotient field of $\mathcal{O}_S$ is the quotient field of $\mathcal{O}_K$, which is $K$.

In the function field case, an application of the Strong Approximation Theorem shows that for all non-zero $\alpha \in K$ there is a $\beta \in K$ with

$$\text{ord}_v(\beta) \geq \max\{0, \text{ord}_v(\alpha^{-1})\}, \quad v \in S.$$ 

Notice that $\beta \in \mathcal{O}_S$, as is $\alpha \beta$, 

Lemma (1)

The quotient field of the ring of $S$-integers is all of $K$ and $\mathcal{O}_S$ is integrally closed.

Proof: Clearly $\mathcal{O}_S \supseteq \mathcal{O}_K$ in the number field case, so that the quotient field of $\mathcal{O}_S$ is the quotient field of $\mathcal{O}_K$, which is $K$.

In the function field case, an application of the Strong Approximation Theorem shows that for all non-zero $\alpha \in K$ there is a $\beta \in K$ with

$$\text{ord}_v(\beta) \geq \max\{0, \text{ord}_v(\alpha^{-1})\}, \quad v \in S.$$ 

Notice that $\beta \in \mathcal{O}_S$, as is $\alpha \beta$, so that $\alpha$ is in the quotient field of $\mathcal{O}_S$. 
Lemma (1)

The quotient field of the ring of $S$-integers is all of $K$ and $\mathcal{O}_S$ is integrally closed.

Proof: Clearly $\mathcal{O}_S \supseteq \mathcal{O}_K$ in the number field case, so that the quotient field of $\mathcal{O}_S$ is the quotient field of $\mathcal{O}_K$, which is $K$.

In the function field case, an application of the Strong Approximation Theorem shows that for all non-zero $\alpha \in K$ there is a $\beta \in K$ with

$$\operatorname{ord}_v(\beta) \geq \max\{0, \operatorname{ord}_v(\alpha^{-1})\}, \quad v \in S.$$ 

Notice that $\beta \in \mathcal{O}_S$, as is $\alpha \beta$, so that $\alpha$ is in the quotient field of $\mathcal{O}_S$.

Now suppose $\alpha \in K$ is integral over $\mathcal{O}_S$ and write

$$\alpha^n + \beta_{n-1}\alpha^{n-1} + \cdots + \beta_1\alpha + \beta_0 = 0,$$
Lemma (1)

The quotient field of the ring of $S$-integers is all of $K$ and $\mathfrak{O}_S$ is integrally closed.

Proof: Clearly $\mathfrak{O}_S \supseteq \mathfrak{O}_K$ in the number field case, so that the quotient field of $\mathfrak{O}_S$ is the quotient field of $\mathfrak{O}_K$, which is $K$.

In the function field case, an application of the Strong Approximation Theorem shows that for all non-zero $\alpha \in K$ there is a $\beta \in K$ with

$$\text{ord}_v(\beta) \geq \max\{0, \text{ord}_v(\alpha^{-1})\}, \quad v \in S.$$  

Notice that $\beta \in \mathfrak{O}_S$, as is $\alpha \beta$, so that $\alpha$ is in the quotient field of $\mathfrak{O}_S$.

Now suppose $\alpha \in K$ is integral over $\mathfrak{O}_S$ and write

$$\alpha^n + \beta_{n-1}\alpha^{n-1} + \cdots + \beta_1 \alpha + \beta_0 = 0,$$

where the $\beta_i$’s are all in $\mathfrak{O}_S$. 
Lemma (1)

The quotient field of the ring of $S$-integers is all of $K$ and $\mathfrak{O}_S$ is integrally closed.

Proof: Clearly $\mathfrak{O}_S \supseteq \mathfrak{O}_K$ in the number field case, so that the quotient field of $\mathfrak{O}_S$ is the quotient field of $\mathfrak{O}_K$, which is $K$.

In the function field case, an application of the Strong Approximation Theorem shows that for all non-zero $\alpha \in K$ there is a $\beta \in K$ with

$$\text{ord}_v(\beta) \geq \max\{0, \text{ord}_v(\alpha^{-1})\}, \quad v \in S.$$ 

Notice that $\beta \in \mathfrak{O}_S$, as is $\alpha \beta$, so that $\alpha$ is in the quotient field of $\mathfrak{O}_S$.

Now suppose $\alpha \in K$ is integral over $\mathfrak{O}_S$ and write

$$\alpha^n + \beta_{n-1}\alpha^{n-1} + \cdots + \beta_1\alpha + \beta_0 = 0,$$

where the $\beta_i$'s are all in $\mathfrak{O}_S$. If $\text{ord}_v(\alpha) < 0$ for some place $v \in S$, 

Lemma (1)

The quotient field of the ring of \( S \)-integers is all of \( K \) and \( \mathcal{O}_S \) is integrally closed.

**Proof:** Clearly \( \mathcal{O}_S \supseteq \mathcal{O}_K \) in the number field case, so that the quotient field of \( \mathcal{O}_S \) is the quotient field of \( \mathcal{O}_K \), which is \( K \).

In the function field case, an application of the Strong Approximation Theorem shows that for all non-zero \( \alpha \in K \) there is a \( \beta \in K \) with

\[
\text{ord}_v(\beta) \geq \max\{0, \text{ord}_v(\alpha^{-1})\}, \quad v \in S.
\]

Notice that \( \beta \in \mathcal{O}_S \), as is \( \alpha \beta \), so that \( \alpha \) is in the quotient field of \( \mathcal{O}_S \).

Now suppose \( \alpha \in K \) is integral over \( \mathcal{O}_S \) and write

\[
\alpha^n + \beta_{n-1}\alpha^{n-1} + \cdots + \beta_1\alpha + \beta_0 = 0,
\]

where the \( \beta_i \)'s are all in \( \mathcal{O}_S \). If \( \text{ord}_v(\alpha) < 0 \) for some place \( v \in S \), then

\[
\text{ord}_v(\alpha^n) = n\text{ord}_v(\alpha) < i\text{ord}_v(\alpha) \leq \text{ord}_v(\beta_i\alpha^i)
\]

for all \( i = 0, \ldots, n-1 \).
Lemma (1)

The quotient field of the ring of $S$-integers is all of $K$ and $\mathfrak{O}_S$ is integrally closed.

Proof: Clearly $\mathfrak{O}_S \supseteq \mathfrak{O}_K$ in the number field case, so that the quotient field of $\mathfrak{O}_S$ is the quotient field of $\mathfrak{O}_K$, which is $K$.
In the function field case, an application of the Strong Approximation Theorem shows that for all non-zero $\alpha \in K$ there is a $\beta \in K$ with

$$\text{ord}_v(\beta) \geq \max\{0, \text{ord}_v(\alpha^{-1})\}, \quad v \in S.$$  

Notice that $\beta \in \mathfrak{O}_S$, as is $\alpha \beta$, so that $\alpha$ is in the quotient field of $\mathfrak{O}_S$.
Now suppose $\alpha \in K$ is integral over $\mathfrak{O}_S$ and write

$$\alpha^n + \beta_{n-1}\alpha^{n-1} + \cdots + \beta_1\alpha + \beta_0 = 0,$$

where the $\beta_i$’s are all in $\mathfrak{O}_S$. If $\text{ord}_v(\alpha) < 0$ for some place $v \in S$, then

$$\text{ord}_v(\alpha^n) = n \text{ord}_v(\alpha) < i \text{ord}_v(\alpha) \leq \text{ord}_v(\beta_i\alpha^i)$$

for all $i = 0, \ldots, n - 1$. But this can’t happen by the ultra-metric inequality!
Lemma (1)

The quotient field of the ring of $S$-integers is all of $K$ and $\mathcal{O}_S$ is integrally closed.

Proof: Clearly $\mathcal{O}_S \supseteq \mathcal{O}_K$ in the number field case, so that the quotient field of $\mathcal{O}_S$ is the quotient field of $\mathcal{O}_K$, which is $K$.

In the function field case, an application of the Strong Approximation Theorem shows that for all non-zero $\alpha \in K$ there is a $\beta \in K$ with

$$\text{ord}_v(\beta) \geq \max\{0, \text{ord}_v(\alpha^{-1})\}, \quad v \in S.$$  

Notice that $\beta \in \mathcal{O}_S$, as is $\alpha\beta$, so that $\alpha$ is in the quotient field of $\mathcal{O}_S$.

Now suppose $\alpha \in K$ is integral over $\mathcal{O}_S$ and write

$$\alpha^n + \beta_{n-1}\alpha^{n-1} + \cdots + \beta_1\alpha + \beta_0 = 0,$$

where the $\beta_i$’s are all in $\mathcal{O}_S$. If $\text{ord}_v(\alpha) < 0$ for some place $v \in S$, then

$$\text{ord}_v(\alpha^n) = n\text{ord}_v(\alpha) < i\text{ord}_v(\alpha) \leq \text{ord}_v(\beta_i\alpha^i)$$

for all $i = 0, \ldots, n-1$. But this can’t happen by the ultra-metric inequality! Therefore $\alpha \in \mathcal{O}_S$. 
Lemma (2)

The ring \( O \) is always a Dedekind domain.

Proof:
The proof here (along with recalling the definition of Dedekind domain) will be a week #10 exercise.

Lemma (3)

Suppose \( S \) is finite.

Then \( O \) is a principal ideal domain.

Proof:
Actually something more general is true: a Dedekind domain with a finite number of prime ideals is a principal ideal domain.
Lemma (2)

The ring $\mathcal{O}_S$ is always a Dedekind domain.
Lemma (2)

*The ring $\mathcal{O}_S$ is always a Dedekind domain.*

**Proof:**
Lemma (2)

The ring $\mathcal{O}_S$ is always a Dedekind domain.

Proof: The proof here (along with recalling the definition of Dedekind domain) will be a week #10 exercise.
Lemma (2)

The ring $\mathcal{O}_S$ is always a Dedekind domain.

Proof: The proof here (along with recalling the definition of Dedekind domain) will be a week #10 exercise.

Lemma (3)
Lemma (2)

The ring $\mathfrak{O}_S$ is always a Dedekind domain.

**Proof:** The proof here (along with recalling the definition of Dedekind domain) will be a week #10 exercise.

Lemma (3)

Suppose $S$ is finite.
Lemma (2)

The ring $\mathcal{O}_S$ is always a Dedekind domain.

**Proof**: The proof here (along with recalling the definition of Dedekind domain) will be a week #10 exercise.

Lemma (3)

Suppose $S$ is finite. Then $\mathcal{O}_S$ is a principal ideal domain.
Lemma (2)

*The ring $\mathcal{O}_S$ is always a Dedekind domain.*

**Proof:** The proof here (along with recalling the definition of Dedekind domain) will be a week #10 exercise.

Lemma (3)

*Suppose $S$ is finite. Then $\mathcal{O}_S$ is a principal ideal domain.*

**Proof:**
Lemma (2)

The ring $\mathcal{O}_S$ is always a Dedekind domain.

Proof: The proof here (along with recalling the definition of Dedekind domain) will be a week #10 exercise.

Lemma (3)

Suppose $S$ is finite. Then $\mathcal{O}_S$ is a principal ideal domain.

Proof: Actually something more general is true:
Lemma (2)

*The ring $\mathfrak{O}_S$ is always a Dedekind domain.*

**Proof:** The proof here (along with recalling the definition of Dedekind domain) will be a week #10 exercise.

Lemma (3)

*Suppose $S$ is finite. Then $\mathfrak{O}_S$ is a principal ideal domain.*

**Proof:** Actually something more general is true: a Dedekind domain with a finite number of prime ideals is a principal ideal domain.
Indeed, suppose $R$ is a Dedekind domain with only finitely many prime ideals and let $I$ be a non-zero ideal.
Indeed, suppose $R$ is a Dedekind domain with only finitely many prime ideals and let $I$ be a non-zero ideal. Write

$$I = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r},$$
Indeed, suppose $R$ is a Dedekind domain with only finitely many prime ideals and let $\mathcal{I}$ be a non-zero ideal. Write

$$\mathcal{I} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r},$$

where $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are the non-zero prime ideals of $R$. 
Indeed, suppose $R$ is a Dedekind domain with only finitely many prime ideals and let $\mathcal{I}$ be a non-zero ideal. Write

$$\mathcal{I} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r},$$

where $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ are the non-zero prime ideals of $R$. Choose $\pi_i \in \mathfrak{P}_i \setminus \mathfrak{P}_i^2$.
Indeed, suppose $R$ is a Dedekind domain with only finitely many prime ideals and let $\mathcal{I}$ be a non-zero ideal. Write

$$\mathcal{I} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r},$$

where $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are the non-zero prime ideals of $R$. Choose $\pi_i \in \mathfrak{p}_i \setminus \mathfrak{p}_i^2$ and via the Chinese Remainder Theorem find an element $\alpha$ with $\alpha \equiv \pi_i^{e_i} \mod \mathfrak{p}_i^{e_i+1}$ for all $i = 1, \ldots, r$. 

The we readily see that the principal ideal $\alpha R = \mathcal{I}$. 

From now on we will consider the case where $F \supseteq K$ is a finite and separable extension of $K$ (it need not have the same field of constants as $K$ in the function field case). Obviously separability is only an issue in the function field case. Since $F$ is a separable extension, it is a primitive extension and we readily get a well-behaved trace and norm from $F$ down to $K$. We'll denote these by $\text{Tr}_{F/K}$ and $N_{F/K}$, respectively.
Indeed, suppose $R$ is a Dedekind domain with only finitely many prime ideals and let $\mathcal{I}$ be a non-zero ideal. Write

$$\mathcal{I} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r},$$

where $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ are the non-zero prime ideals of $R$. Choose $\pi_i \in \mathfrak{P}_i \setminus \mathfrak{P}_i^2$ and via the Chinese Remainder Theorem find an element $\alpha$ with $\alpha \equiv \pi_i^{e_i} \mod \mathfrak{P}_i^{e_i+1}$ for all $i = 1, \ldots, r$. The we readily see that the principal ideal $\alpha R = \mathcal{I}$.
Indeed, suppose $R$ is a Dedekind domain with only finitely many prime ideals and let $I$ be a non-zero ideal. Write

$$ I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}, $$

where $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are the non-zero prime ideals of $R$. Choose $\pi_i \in \mathfrak{p}_i \setminus \mathfrak{p}_i^2$ and via the Chinese Remainder Theorem find an element $\alpha$ with $\alpha \equiv \pi_i^{e_i} \mod \mathfrak{p}_i^{e_i+1}$ for all $i = 1, \ldots, r$. The we readily see that the principal ideal $\alpha R = I$.

From now on we will consider the case where $F \supseteq K$ is a finite and separable extension of $K$. 
Indeed, suppose \( R \) is a Dedekind domain with only finitely many prime ideals and let \( \mathcal{I} \) be a non-zero ideal. Write

\[
\mathcal{I} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r},
\]

where \( \mathfrak{P}_1, \ldots, \mathfrak{P}_r \) are the non-zero prime ideals of \( R \).

Choose \( \pi_i \in \mathfrak{P}_i \setminus \mathfrak{P}_i^2 \) and via the Chinese Remainder Theorem find an element \( \alpha \) with \( \alpha \equiv \pi_i^{e_i} \mod \mathfrak{P}_i^{e_i+1} \) for all \( i = 1, \ldots, r \). The we readily see that the principal ideal \( \alpha R = \mathcal{I} \).

From now on we will consider the case where \( F \supseteq K \) is a finite and separable extension of \( K \) (it need not have the same field of constants as \( K \) in the function field case).
Indeed, suppose $R$ is a Dedekind domain with only finitely many prime ideals and let $\mathcal{I}$ be a non-zero ideal. Write

$$\mathcal{I} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r},$$

where $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are the non-zero prime ideals of $R$. Choose $\pi_i \in \mathfrak{p}_i \setminus \mathfrak{p}_i^2$ and via the Chinese Remainder Theorem find an element $\alpha$ with $\alpha \equiv \pi_i^{e_i} \mod \mathfrak{p}_i^{e_i+1}$ for all $i = 1, \ldots, r$. The we readily see that the principal ideal $\alpha R = \mathcal{I}$.

From now on we will consider the case where $F \supseteq K$ is a finite and separable extension of $K$ (it need not have the same field of constants as $K$ in the function field case). Obviously separability is only an issue in the function field case.
Indeed, suppose $R$ is a Dedekind domain with only finitely many prime ideals and let $\mathcal{I}$ be a non-zero ideal. Write

$$\mathcal{I} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r},$$

where $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ are the non-zero prime ideals of $R$. Choose $\pi_i \in \mathfrak{P}_i \setminus \mathfrak{P}_i^2$ and via the Chinese Remainder Theorem find an element $\alpha$ with $\alpha \equiv \pi_i^{e_i} \mod \mathfrak{P}_i^{e_i+1}$ for all $i = 1, \ldots, r$. The we readily see that the principal ideal $\alpha R = \mathcal{I}$.

From now on we will consider the case where $F \supseteq K$ is a finite and separable extension of $K$ (it need not have the same field of constants as $K$ in the function field case). Obviously separability is only an issue in the function field case. Since $F$ is a separable extension, it is a primitive extension.
Indeed, suppose $R$ is a Dedekind domain with only finitely many prime ideals and let $\mathfrak{I}$ be a non-zero ideal. Write

$$\mathfrak{I} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r},$$

where $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ are the non-zero prime ideals of $R$. Choose $\pi_i \in \mathfrak{P}_i \setminus \mathfrak{P}_i^2$ and via the Chinese Remainder Theorem find an element $\alpha$ with $\alpha \equiv \pi_i^{e_i} \mod \mathfrak{P}_i^{e_i+1}$ for all $i = 1, \ldots, r$. The we readily see that the principal ideal $\alpha R = \mathfrak{I}$.

From now on we will consider the case where $F \supseteq K$ is a finite and separable extension of $K$ (it need not have the same field of constants as $K$ in the function field case). Obviously separability is only an issue in the function field case. Since $F$ is a separable extension, it is a primitive extension and we readily get a well-behaved trace and norm from $F$ down to $K$. 

Indeed, suppose $R$ is a Dedekind domain with only finitely many prime ideals and let $\mathcal{I}$ be a non-zero ideal. Write

$$\mathcal{I} = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_r^{e_r},$$

where $\mathcal{P}_1, \ldots, \mathcal{P}_r$ are the non-zero prime ideals of $R$. Choose $\pi_i \in \mathcal{P}_i \setminus \mathcal{P}_i^2$ and via the Chinese Remainder Theorem find an element $\alpha$ with $\alpha \equiv \pi_i^{e_i} \mod \mathcal{P}_i^{e_i+1}$ for all $i = 1, \ldots, r$. Then we readily see that the principal ideal $\alpha R = \mathcal{I}$.

From now on we will consider the case where $F \supseteq K$ is a finite and separable extension of $K$ (it need not have the same field of constants as $K$ in the function field case). Obviously separability is only an issue in the function field case. Since $F$ is a separable extension, it is a primitive extension and we readily get a well-behaved trace and norm from $F$ down to $K$. We’ll denote these by $\text{Tr}_{F/K}$ and $\text{N}_{F/K}$, respectively.
Lemma (4)

Let $O_S \subset K$ be a ring of $S$-integers of $K$ and let $\alpha \in F \times$. Then $\alpha$ is integral over $O_S$ if and only if its minimal polynomial $P(X) \in O_S[X]$. In particular, if $\alpha$ is integral over $O_S$ then $\text{Tr}_{F/K}(\alpha) \in O_S$. 

Proof: Obviously if $P(X) \in O_S[X]$ then $\alpha$ is integral over $O_S$. Suppose $\alpha$ is integral over $O_S$. Then the coefficients of its minimal polynomial $P(X)$ are also integral over $O_S$. Since $O_S$ is integrally closed by Lemma 1, we see that $P(X) \in O_S[X]$. 
Lemma (4)

Let $\mathcal{O}_S \subset K$ be a ring of $S$-integers of $K$ and let $\alpha \in F^\times$. Then $\alpha$ is integral over $\mathcal{O}_S$ if and only if its minimal polynomial $P(X) \in \mathcal{O}_S[X]$.

Proof:
Obviously if $P(X) \in \mathcal{O}_S[X]$ then $\alpha$ is integral over $\mathcal{O}_S$.

Suppose $\alpha$ is integral over $\mathcal{O}_S$. Then the coefficients of its minimal polynomial $P(X)$ are also integral over $\mathcal{O}_S$. Since $\mathcal{O}_S$ is integrally closed by Lemma 1, we see that $P(X) \in \mathcal{O}_S[X]$. 
Lemma (4)

Let $\mathcal{O}_S \subset K$ be a ring of $S$-integers of $K$ and let $\alpha \in F^\times$. Then $\alpha$ is integral over $\mathcal{O}_S$ if and only if its minimal polynomial $P(X) \in \mathcal{O}_S[X]$. 

Proof: Obviously if $P(X) \in \mathcal{O}_S[X]$ then $\alpha$ is integral over $\mathcal{O}_S$. Suppose $\alpha$ is integral over $\mathcal{O}_S$. Then the coefficients of its minimal polynomial $P(X)$ are also integral over $\mathcal{O}_S$. Since $\mathcal{O}_S$ is integrally closed by Lemma 1, we see that $P(X) \in \mathcal{O}_S[X]$. 

Lemma (4)

Let $\mathcal{O}_S \subset K$ be a ring of $S$-integers of $K$ and let $\alpha \in F^\times$. Then $\alpha$ is integral over $\mathcal{O}_S$ if and only if its minimal polynomial $P(X) \in \mathcal{O}_S[X]$. In particular, if $\alpha$ is integral over $\mathcal{O}_S$ then $\text{Tr}_{F/K}(\alpha) \in \mathcal{O}_S$. 

Proof: Obviously if $P(X) \in \mathcal{O}_S[X]$ then $\alpha$ is integral over $\mathcal{O}_S$. Suppose $\alpha$ is integral over $\mathcal{O}_S$. Then the coefficients of its minimal polynomial $P(X)$ are also integral over $\mathcal{O}_S$. Since $\mathcal{O}_S$ is integrally closed by Lemma 1, we see that $P(X) \in \mathcal{O}_S[X]$. 

Lemma (4)

Let $\mathcal{O}_S \subset K$ be a ring of $S$-integers of $K$ and let $\alpha \in F^\times$. Then $\alpha$ is integral over $\mathcal{O}_S$ if and only if its minimal polynomial $P(X) \in \mathcal{O}_S[X]$. In particular, if $\alpha$ is integral over $\mathcal{O}_S$ then $\text{Tr}_{F/K}(\alpha) \in \mathcal{O}_S$.

Proof:
Lemma (4)

Let $\mathcal{O}_S \subset K$ be a ring of $S$-integers of $K$ and let $\alpha \in F^\times$. Then $\alpha$ is integral over $\mathcal{O}_S$ if and only if its minimal polynomial $P(X) \in \mathcal{O}_S[X]$. In particular, if $\alpha$ is integral over $\mathcal{O}_S$ then $\text{Tr}_{F/K}(\alpha) \in \mathcal{O}_S$.

Proof: Obviously if $P(X) \in \mathcal{O}_S[X]$ then $\alpha$ is integral over $\mathcal{O}_S$. 
Lemma (4)

Let $\mathcal{O}_S \subset K$ be a ring of $S$-integers of $K$ and let $\alpha \in F^\times$. Then $\alpha$ is integral over $\mathcal{O}_S$ if and only if its minimal polynomial $P(X) \in \mathcal{O}_S[X]$. In particular, if $\alpha$ is integral over $\mathcal{O}_S$ then $\text{Tr}_{F/K}(\alpha) \in \mathcal{O}_S$.

**Proof:** Obviously if $P(X) \in \mathcal{O}_S[X]$ then $\alpha$ is integral over $\mathcal{O}_S$. Suppose $\alpha$ is integral over $\mathcal{O}_S$. 

Lemma (4)

Let $\mathcal{O}_S \subset K$ be a ring of $S$-integers of $K$ and let $\alpha \in F^\times$. Then $\alpha$ is integral over $\mathcal{O}_S$ if and only if its minimal polynomial $P(X) \in \mathcal{O}_S[X]$. In particular, if $\alpha$ is integral over $\mathcal{O}_S$ then $\text{Tr}_{F/K}(\alpha) \in \mathcal{O}_S$.

**Proof:** Obviously if $P(X) \in \mathcal{O}_S[X]$ then $\alpha$ is integral over $\mathcal{O}_S$.

Suppose $\alpha$ is integral over $\mathcal{O}_S$.

Then the coefficients of its minimal polynomial $P(X)$ are also integral over $\mathcal{O}_S$. 
Lemma (4)

Let $\mathfrak{O}_S \subset K$ be a ring of $S$-integers of $K$ and let $\alpha \in F^\times$. Then $\alpha$ is integral over $\mathfrak{O}_S$ if and only if its minimal polynomial $P(X) \in \mathfrak{O}_S[X]$. In particular, if $\alpha$ is integral over $\mathfrak{O}_S$ then $\text{Tr}_{F/K}(\alpha) \in \mathfrak{O}_S$.

**Proof:** Obviously if $P(X) \in \mathfrak{O}_S[X]$ then $\alpha$ is integral over $\mathfrak{O}_S$.
Suppose $\alpha$ is integral over $\mathfrak{O}_S$.
Then the coefficients of its minimal polynomial $P(X)$ are also integral over $\mathfrak{O}_S$.
Since $\mathfrak{O}_S$ is integrally closed by Lemma 1,
Lemma (4)

Let $\mathcal{O}_S \subset K$ be a ring of $S$-integers of $K$ and let $\alpha \in F^\times$. Then $\alpha$ is integral over $\mathcal{O}_S$ if and only if its minimal polynomial $P(X) \in \mathcal{O}_S[X]$. In particular, if $\alpha$ is integral over $\mathcal{O}_S$ then $\text{Tr}_{F/K}(\alpha) \in \mathcal{O}_S$.

Proof: Obviously if $P(X) \in \mathcal{O}_S[X]$ then $\alpha$ is integral over $\mathcal{O}_S$.
Suppose $\alpha$ is integral over $\mathcal{O}_S$. Then the coefficients of its minimal polynomial $P(X)$ are also integral over $\mathcal{O}_S$.
Since $\mathcal{O}_S$ is integrally closed by Lemma 1, we see that $P(X) \in \mathcal{O}_S[X]$. 
Lemma (5)

Let \(\{\alpha_1, \ldots, \alpha_n\}\) be a basis of \(F\) over \(K\). Then there are uniquely determined elements \(\alpha^*_1, \ldots, \alpha^*_n \in F\) such that
\[
\text{Tr}_{F/K}(\alpha_i \alpha^*_j) = \begin{cases} 
1 & \text{if } i = j, \\
0 & \text{otherwise.}
\end{cases}
\]
The set \(\{\alpha^*_1, \ldots, \alpha^*_n\}\) is also a basis for \(F\) over \(K\), called the dual basis with respect to the trace.
Lemma (5)

Let \( \{ \alpha_1, \ldots, \alpha_n \} \) be a basis of \( F \) over \( K \).
Lemma (5)

Let \( \{\alpha_1, \ldots, \alpha_n\} \) be a basis of \( F \) over \( K \). Then there are uniquely determined elements \( \alpha_1^*, \ldots, \alpha_n^* \in F \) such that

\[
\text{Tr}_{F/K}(\alpha_i \alpha_j^*) = \begin{cases} 
1 & \text{if } i = j, \\
0 & \text{otherwise}.
\end{cases}
\]

The set \( \{\alpha_1^*, \ldots, \alpha_n^*\} \) is also a basis for \( F \) over \( K \), called the dual basis with respect to the trace.
Lemma (5)

Let \( \{\alpha_1, \ldots, \alpha_n\} \) be a basis of \( F \) over \( K \). Then there are uniquely determined elements \( \alpha_1^*, \ldots, \alpha_n^* \in F \) such that

\[
\text{Tr}_{F/K}(\alpha_i \alpha_j^*) = \begin{cases} 
1 & \text{if } i = j, \\
0 & \text{otherwise.}
\end{cases}
\]

The set \( \{\alpha_1^*, \ldots, \alpha_n^*\} \) is also a basis for \( F \) over \( K \), called the dual basis with respect to the trace.
Lemma (5)

Let \( \{ \alpha_1, \ldots, \alpha_n \} \) be a basis of \( F \) over \( K \). Then there are uniquely determined elements \( \alpha_1^*, \ldots, \alpha_n^* \in F \) such that

\[
\text{Tr}_{F/K}(\alpha_i \alpha_j^*) = \begin{cases} 
1 & \text{if } i = j, \\
0 & \text{otherwise.}
\end{cases}
\]
Lemma (5)

Let \( \{\alpha_1, \ldots, \alpha_n\} \) be a basis of \( F \) over \( K \). Then there are uniquely determined elements \( \alpha_1^*, \ldots, \alpha_n^* \in F \) such that

\[
\text{Tr}_{F/K}(\alpha_i \alpha_j^*) = \begin{cases} 
1 & \text{if } i = j, \\
0 & \text{otherwise.}
\end{cases}
\]

The set \( \{\alpha_1^*, \ldots, \alpha_n^*\} \) is also a basis for \( F \) over \( K \),
Lemma (5)

Let \( \{\alpha_1, \ldots, \alpha_n\} \) be a basis of \( F \) over \( K \). Then there are uniquely determined elements \( \alpha_1^*, \ldots, \alpha_n^* \in F \) such that

\[
\text{Tr}_{F/K}(\alpha_i \alpha_j^*) = \begin{cases} 
1 & \text{if } i = j, \\
0 & \text{otherwise.}
\end{cases}
\]

The set \( \{\alpha_1^*, \ldots, \alpha_n^*\} \) is also a basis for \( F \) over \( K \), called the dual basis with respect to the trace.
Proof:

Consider the dual space $F^*$ of $F$ over $K$, i.e., the $K$-vector space of all linear maps from $F$ to $K$. From linear algebra $F^*$ is isomorphic to $F$ as $K$-vector spaces.

For $\alpha \in F$ and $\theta \in F^*$ define $\alpha \theta \in F^*$ by $\alpha \theta(\beta) := \theta(\alpha \beta)$.

One easily verifies that this turns $F^*$ into an $F$-vector space of dimension 1.

Now $\text{Tr}_{F/K}$ is not identically zero, so that any $\theta \in F^*$ has a unique representation $\theta = \alpha \text{Tr}_{F/K}$.

We apply this to the linear forms $\theta_1, \ldots, \theta_n \in F^*$ given by $\theta_i(\alpha_j) = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{otherwise.} \end{cases}$

Writing $\theta_i = \alpha^*_i \text{Tr}_{F/K}$ completes the proof.

**Proof:** Consider the dual space $F^*$ of $F$ over $K$, 

...
Proof: Consider the dual space $F^*$ of $F$ over $K$, i.e., the $K$-vector space of all linear maps from $F$ to $K$. 

One easily verifies that this turns $F^*$ into an $F$-vector space of dimension 1. Now $\text{Tr}_{F/K}$ is not identically zero, so that any $\theta \in F^*$ has a unique representation $\theta = \alpha \text{Tr}_{F/K}$. We apply this to the linear forms $\theta_1, \ldots, \theta_n \in F^*$ given by $\theta_i(\alpha_j) = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{otherwise.} \end{cases}$ Writing $\theta_i = \alpha^*_i \text{Tr}_{F/K}$ completes the proof.
**Proof**: Consider the dual space $F^*$ of $F$ over $K$, i.e., the $K$-vector space of all linear maps from $F$ to $K$. From linear algebra $F^*$ is isomorphic to $F$ as $K$-vector spaces.
Proof: Consider the dual space $F^*$ of $F$ over $K$, i.e., the $K$-vector space of all linear maps from $F$ to $K$. From linear algebra $F^*$ is isomorphic to $F$ as $K$-vector spaces. For $\alpha \in F$ and $\theta \in F^*$ define $\alpha \theta \in F^*$ by
**Proof:** Consider the dual space $F^*$ of $F$ over $K$, i.e., the $K$-vector space of all linear maps from $F$ to $K$. From linear algebra $F^*$ is isomorphic to $F$ as $K$-vector spaces. For $\alpha \in F$ and $\theta \in F^*$ define $\alpha \theta \in F^*$ by

$$\alpha \theta(\beta) := \theta(\alpha \beta).$$
Proof: Consider the dual space $F^*$ of $F$ over $K$, i.e., the $K$-vector space of all linear maps from $F$ to $K$. From linear algebra $F^*$ is isomorphic to $F$ as $K$-vector spaces. For $\alpha \in F$ and $\theta \in F^*$ define $\alpha \theta \in F^*$ by

$$\alpha \theta(\beta) := \theta(\alpha \beta).$$

One easily verifies that this turns $F^*$ into an $F$-vector space of dimension 1.
Proof: Consider the dual space $F^*$ of $F$ over $K$, i.e., the $K$-vector space of all linear maps from $F$ to $K$. From linear algebra $F^*$ is isomorphic to $F$ as $K$-vector spaces. For $\alpha \in F$ and $\theta \in F^*$ define $\alpha \theta \in F^*$ by

$$\alpha \theta(\beta) := \theta(\alpha \beta).$$

One easily verifies that this turns $F^*$ into an $F$-vector space of dimension 1. Now $\text{Tr}_{F/K}$ is not identically zero,
**Proof:** Consider the dual space $F^*$ of $F$ over $K$, i.e., the $K$-vector space of all linear maps from $F$ to $K$. From linear algebra $F^*$ is isomorphic to $F$ as $K$-vector spaces. For $\alpha \in F$ and $\theta \in F^*$ define $\alpha \theta \in F^*$ by

$$\alpha \theta(\beta) := \theta(\alpha \beta).$$

One easily verifies that this turns $F^*$ into an $F$-vector space of dimension 1. Now $\text{Tr}_{F/K}$ is not identically zero, so that any $\theta \in F^*$ has a unique representation $\theta = \alpha \text{Tr}_{F/K}$. 
Proof: Consider the dual space $F^*$ of $F$ over $K$, i.e., the $K$-vector space of all linear maps from $F$ to $K$. From linear algebra $F^*$ is isomorphic to $F$ as $K$-vector spaces. For $\alpha \in F$ and $\theta \in F^*$ define $\alpha \theta \in F^*$ by

$$\alpha \theta(\beta) := \theta(\alpha \beta).$$

One easily verifies that this turns $F^*$ into an $F$-vector space of dimension 1. Now $\text{Tr}_{F/K}$ is not identically zero, so that any $\theta \in F^*$ has a unique representation $\theta = \alpha \text{Tr}_{F/K}$.

We apply this to the linear forms $\theta_1, \ldots, \theta_n \in F^*$ given by
**Proof:** Consider the dual space $F^*$ of $F$ over $K$, i.e., the $K$-vector space of all linear maps from $F$ to $K$. From linear algebra $F^*$ is isomorphic to $F$ as $K$-vector spaces. For $\alpha \in F$ and $\theta \in F^*$ define $\alpha \theta \in F^*$ by

$$\alpha \theta(\beta) := \theta(\alpha \beta).$$

One easily verifies that this turns $F^*$ into an $F$-vector space of dimension $1$. Now $\text{Tr}_{F/K}$ is not identically zero, so that any $\theta \in F^*$ has a unique representation $\theta = \alpha \text{Tr}_{F/K}$.

We apply this to the linear forms $\theta_1, \ldots, \theta_n \in F^*$ given by

$$\theta_i(\alpha_j) = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{otherwise.} \end{cases}$$
Proof: Consider the dual space $F^*$ of $F$ over $K$, i.e., the $K$-vector space of all linear maps from $F$ to $K$. From linear algebra $F^*$ is isomorphic to $F$ as $K$-vector spaces. For $\alpha \in F$ and $\theta \in F^*$ define $\alpha \theta \in F^*$ by

$$\alpha \theta(\beta) := \theta(\alpha \beta).$$

One easily verifies that this turns $F^*$ into an $F$-vector space of dimension 1. Now $\text{Tr}_{F/K}$ is not identically zero, so that any $\theta \in F^*$ has a unique representation $\theta = \alpha \text{Tr}_{F/K}$.

We apply this to the linear forms $\theta_1, \ldots, \theta_n \in F^*$ given by

$$\theta_i(\alpha_j) = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{otherwise}. \end{cases}$$
Proof: Consider the dual space $F^*$ of $F$ over $K$, i.e., the $K$-vector space of all linear maps from $F$ to $K$. From linear algebra $F^*$ is isomorphic to $F$ as $K$-vector spaces. For $\alpha \in F$ and $\theta \in F^*$ define $\alpha \theta \in F^*$ by

$$\alpha \theta(\beta) := \theta(\alpha \beta).$$

One easily verifies that this turns $F^*$ into an $F$-vector space of dimension 1. Now $\text{Tr}_{F/K}$ is not identically zero, so that any $\theta \in F^*$ has a unique representation $\theta = \alpha \text{Tr}_{F/K}$.

We apply this to the linear forms $\theta_1, \ldots, \theta_n \in F^*$ given by

$$\theta_i(\alpha_j) = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{otherwise.} \end{cases}$$

Writing $\theta_i = \alpha_i^* \text{Tr}_{F/K}$ completes the proof.