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. A function field for us will mean some 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 $\pm 1 \in R$.

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

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 $\mathfrak{M}$ denote the non-units of $R$. Note that $\mathfrak{M}$ consists of more than simply the element $0$ since otherwise $R = K$. Let $\alpha \in \mathfrak{M}$ 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 $\alpha \beta \in \mathfrak{M}$. Now suppose $\beta \in \mathfrak{M}$ and consider $\alpha + \beta \in R$. If either $\alpha$ or $\beta$ is $0$ then clearly $\alpha + \beta \in \mathfrak{M}$, 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 $\beta(1 + (\alpha/\beta)) = \alpha + \beta \in \mathfrak{M}$ by what we have already shown. Thus $\mathfrak{M}$ is an ideal. It is clearly the unique maximal ideal of $R$ since any ideal not properly contained in $\mathfrak{M}$ 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

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

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 $\mathfrak{M}$ and let $\alpha_1 \in \mathfrak{M}$. If $\mathfrak{M}$ is not principal there is an $\alpha_2 \in \mathfrak{M}$ 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 $\mathfrak{M}$ is principal.

Write $\mathfrak{M} = \pi R$. 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 $\alpha \in \mathfrak{M}$. Then $\alpha = \pi^n \beta$ 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
\[ \alpha R \subseteq \pi^m R \subseteq \pi^{m-1} R \subseteq \cdots \subseteq \pi R \]
is bounded by a function of \( \alpha \) so that there is a maximal exponent \( m \) such that \( \alpha \in \pi^m R \). Since \( \alpha \notin \pi^{m+1} R \) 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 \( \alpha = u \pi^m \in \pi^{m_0} R \) since \( m \geq m_0 \) by construction. Therefore \( I = \alpha_0 R \).

**Definition:** A valuation rings 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 \( \mathfrak{M} = \pi R \). 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 \( \mathfrak{M} \).

**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 \( \alpha \notin R \), 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 \( \mathfrak{M} \) 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 \( n, m \in \mathbb{Z} \), so that \( \alpha \beta = uu' \pi^{n+m} \) and \( v_R(\alpha \beta) = v_R(\alpha) + v_R(\beta) \). 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 \(| \cdot |_1 \neq | \cdot |_2^\rho \) for any \( \rho > 0 \). By exercise \#2 from homework \#7 these two absolute values are inequivalent.

**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 \( R \supset \mathbb{Z} \) in characteristic \( 0 \), which is certainly the case for number fields, and \( R \supset \mathbb{F}_p \) 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

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

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

Since either $\alpha \in R$ or $\alpha^{-1} \in R$, we must have $\alpha \in R$. We remark that the same argument shows $R \supset \mathfrak{O}_K$ in the number field case.

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

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

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

Now $\alpha_i, P_i(\alpha_1) \in R$ for all $i$, $\alpha_i / \alpha_{i_0} \in \mathfrak{M}$ for all $i < i_0$ by hypothesis, and $P_i(\alpha_1) / \alpha_{i_0} \in \mathfrak{M}$ 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 $P_{i_0}(\alpha_1) \in \mathfrak{M}$. Since $\alpha_1 | (P_i(\alpha_1) - a_{i_0})$, we see that $a_{i_0} \in \mathfrak{M}$, too. But clearly $\mathfrak{M} \cap F = \{0\}$. This contradiction shows that $\alpha_1, \ldots, \alpha_n$ are linearly independent over $F(\alpha_1)$.

Now 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 $\mathfrak{M}$, 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 $\alpha_1$.

**Remark:** In the case of number fields we have a slightly more direct argument for Proposition 1 as follows. Let $\mathfrak{M}$ denote the unique maximal ideal of $R$. Since $R \supset \mathfrak{O}_K$ we may restrict the canonical map $R \rightarrow R/\mathfrak{M}$ to $\mathfrak{O}_K$ and get a kernel $\mathfrak{P} = \mathfrak{M} \cap \mathfrak{O}_K \subsetneq \mathfrak{O}_K$ (1 $\not\in \mathfrak{M}$, for example). Since $R/\mathfrak{M}$ 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 so that $R$ is the entire quotient field of $\mathfrak{O}_K$, i.e., $K$. Thus $\mathfrak{P}$ is a maximal ideal of $\mathfrak{O}_K$. It is now almost trivial to show that $R = \mathfrak{O}_K/\mathfrak{P}$, which was shown to be a principal ideal domain in an exercise. That relied on the Fundamental Theorem, however, whereas our proof above is 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. Then $|\alpha| = \exp (-\rho v_R(\alpha))$ for some valuation ring $R$ of $K$ and $\rho > 0$.

**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.
\[ \mathfrak{M} = \{ \alpha \in K : |\alpha| < 1 \}. \text{ Write } \mathfrak{M} = \pi R \text{ and set } \rho = \log |\pi^{-1}| > 0. \text{ For any non-zero } \alpha \in K \text{ we have } \alpha = u \pi^{\nu_R(\alpha)} \text{ for some unit } u \text{ by Lemma 3, so that } |\alpha| = |\pi^{\nu(\alpha)}| = \exp \left( -\rho \nu(\alpha) \right). \]

**Theorem 1:** Let \( K \) be a number field and \(| \cdot |\) be a non-trivial absolute value on \( K \).

If it is archimedean, then \( |\alpha| = |\sigma(\alpha)|_\infty \) for all \( \alpha \in K \), where \( \sigma : K \to \mathbb{C} \) is an embedding of \( K \) into \( \mathbb{C} \). \( |\cdot|_\infty \) is the usual complex modulus, and \( \rho \in (0, 1] \).

If it is non-archimedean, then \( |\alpha| = \exp \left( -\rho v_R(\alpha) \right) \) for some \( \rho > 0 \), where \( R = \mathcal{O}_K \) for some maximal ideal \( \mathfrak{P} \subset \mathcal{O}_K \).

**Proof:** The non-archimedean case follows directly from Proposition 2 and the Remark above.

Suppose the absolute value is archimedean. Note that we get an archimedean absolute value on \( \mathbb{Q} \) by simply restricting to rational numbers. By exercise #2 and Ostrowski’s Theorem this restriction must be of the form \( |\cdot|^\rho \) for some \( \rho \in (0, 1] \), where the absolute value here is the usual one on \( \mathbb{Q} \). Without loss of generality we may assume \( \rho = 1 \). We now extend the number field \( K \) topologically to get a complete field (i.e., all Cauchy sequences converge) and denote it \( \overline{K} \). Of course we can do the same with \( \mathbb{Q} \) and get the real numbers. The compositum field \( K \mathbb{R} \) is contained in \( \overline{K} \). On the other hand, \( K \mathbb{R} \) is necessarily a finite extension of \( \mathbb{R} \), hence either \( \mathbb{R} \) or \( \mathbb{C} \). But either of these are topologically complete, so that \( \overline{K} \) is either \( \mathbb{R} \) or \( \mathbb{C} \). Thus there must be some embedding \( \sigma : K \to \mathbb{C} \) with \( |\alpha| = |\sigma(\alpha)|_\infty \) for all \( \alpha \in K \).

**Theorem 2:** For a number field \( K \), the archimedean places are in one-to-one correspondence with the \( r_1 + r_2 \) real embeddings and pairs of complex conjugate embeddings of \( K \) into \( \mathbb{C} \). The non-archimedean places are in one-to-one correspondence with the valuation rings of \( K \), which in turn are in one-to-one correspondence with the maximal ideals \( \mathfrak{P} \subset \mathcal{O}_K \).

**Proof:** By Lemma 4 we have a non-archimedean place for every \( \mathcal{O}_K \) and by Theorem 1 and exercise #2 from the seventh homework assignment this accounts for all non-archimedean places. Obviously \( |\cdot| := |\sigma(\alpha)|_\infty \) is an archimedean absolute value for all embeddings \( \sigma : K \to \mathbb{C} \) and by Theorem 1 and exercise #2 all archimedean absolute values on \( K \) are equivalent to one of these.

If \(|\cdot|_1\) is non-archimedean but \(|\cdot|_2\) is not, then let \( p \) be the unique rational prime contained in the maximal ideal of the valuation ring associated with \(|\cdot|_1\). Then \( |p|_1 < 1 < |p|_2 \) since \(|\cdot|_2\) restricted to \( \mathbb{Q} \) is equivalent to the usual absolute value on \( \mathbb{Q} \) by Ostrowski’s Theorem.

Obviously complex conjugate embeddings yield the exact same absolute values. We just need to show that the absolute values derived from distinct embeddings not complex conjugates are inequivalent.

Let \( K = \mathbb{Q}(\alpha) \) and take two embeddings \( \sigma_1, \sigma_2 \) not complex conjugates. Then \( \sigma_1(\alpha) = \alpha_1 \) and \( \sigma_2(\alpha) = \alpha_2 \) are distinct roots of the minimal polynomial of \( \alpha \). If \( |\alpha_1|_\infty = |\alpha_2|_\infty \), then they both lie on the same circle in the complex plane centered at the origin, and since they are not conjugates, there is a rational number \( a \) such that \( |\alpha_1 + a|_\infty \neq |\alpha_2 + a|_\infty \). Thus there is a \( \beta \in K (\beta = \alpha \text{ or } a + \alpha) \) with \( |\sigma_1(\beta)|_\infty < |\sigma_2(\beta)|_\infty \). Now since \( \mathbb{Q} \) is dense in \( \mathbb{R} \) there is a rational number \( b \) with \( |\sigma_1(\beta)|_\infty < b < |\sigma_2(\beta)|_\infty \). Letting \( \gamma = \beta/b \), we have \( \gamma \in K \) with \( |\sigma_1(\gamma)|_\infty < 1 < |\sigma_2(\gamma)|_\infty \). By exercise #2 from homework #7 the two absolute values are inequivalent.

**Theorem 3:** The places of a function field \( K \) are in one-to-one correspondence with the valuation rings of \( K \).

**Proof:** Exercise #1 from homework #7 implies that all places here are non-archimedean. The exact same reasoning as in the number field case shows that the non-archimedean places are in one-to-one correspondence with the valuation rings of the field.

With this in mind we often abuse notation somewhat and identify places with the associated valuation rings. The only problem here is that, unlike the number field case, we haven’t actually shown that there are any such valuation rings! We’ll fix that right away.

**Lemma 5:** Suppose \( K \) is a function field and \( S \) is a proper subring of \( K \). If \( I \) is a proper
non-zero ideal of $S$, then there is a maximal element of this set; denote it by $R$ (totally ordered subset) has a maximal element which is simply the union. Thus by Zorn’s Lemma there is a maximal element of this set; denote it by $R$. We claim that $R$ is a valuation ring of $K$.

First, since $I \neq \{0\}$ and $IR \neq R$, we obviously have $R \subseteq K$ and $I$ is contained in the subset of non-units of $R$. Suppose $\alpha \in K$ is not in $R$ and neither is $\alpha^{-1}$. By construction the rings $R[\alpha]$ and $R[\alpha^{-1}]$ are not in our set above, so that $IR[\alpha] = R[\alpha]$ and $IR[\alpha^{-1}] = R[\alpha^{-1}]$. Thus there are elements $a_0, \ldots, a_n, b_0, \ldots, b_m \in IR$ satisfying

$$1 = a_0 + a_1 \alpha + \cdots + a_n \alpha^n$$
$$1 = b_0 + b_1 \alpha^{-1} + \cdots + b_m \alpha^{-m}.$$

Obviously both $n, m \geq 1$ here, and without loss of generality they are chosen minimally and also $m \leq n$ (trade $\alpha$ with $\alpha^{-1}$ if necessary). Now some simple manipulations give

$$1 - b_0 = (1 - b_0)a_0 + \cdots + (1 - b_0)a_n \alpha^n$$
$$0 = (b_0 - 1)a_0 \alpha^n + b_1 a_0 \alpha^{n-1} + \cdots + b_m a_0 \alpha^{n-m}$$
$$1 = c_0 + c_1 \alpha + \cdots + c_{n-1} \alpha^{n-1}$$

for some $c_0, \ldots, c_{n-1} \in IR$. This contradicts the minimality of $n$, so that $R$ is a valuation ring. Since $I$ is contained in the subset of non-units of $R$ as remarked above, $I \subseteq \mathfrak{M}$.

**Lemma 6:** Let $K$ be a function field and $\alpha \in K$ be transcendental over $\mathbb{F}_p$. Then there are valuation rings $R_1$ and $R_2$ of $K$ with corresponding maximal ideals $\mathfrak{M}_1$ and $\mathfrak{M}_2$ such that $\alpha \in \mathfrak{M}_1$ and $\alpha^{-1} \in \mathfrak{M}_2$. In particular, the set of places $M(K) \neq \emptyset$.

**Proof:** Consider the proper subring $\mathbb{F}_p[\alpha] \subset K$ and the ideal $\alpha \mathbb{F}_p[\alpha]$. Clearly this ideal is a proper non-zero ideal of the subring so that Lemma 5 applies, yielding the desired valuation ring $R_1$. The same argument applied to $\mathbb{F}_p[\alpha^{-1}]$ works to get $R_2$.

We remark that $M(K)$ is, in fact, infinite. We can see this rather easily in the case of a field of rational functions.

**Examples:** 1. Consider the field of rational functions $\mathbb{F}_p(X)$. Just as we have the Fundamental Theorem of Arithmetic for $\mathbb{Z}$, we have unique factorization in the polynomial ring $\mathbb{F}_p[X]$. For each irreducible monic $P(X) \in \mathbb{F}_p[X]$ (i.e., a “prime”) we have a valuation ring

$$R_P = \{ f(X)/g(X) \in \mathbb{F}_p[X] : f(X), g(X) \in \mathbb{F}_p[X] \text{ relatively prime}, \ P(X) \nmid g(X) \}$$

The analogy with the case $\mathbb{Q}$ and a prime $p \in \mathbb{Z}$ should be obvious. Here the unique maximal ideal consists of those $f(X)/g(X) \in R_P$ where $P(X)|f(X)$.

2. There is another valuation ring $R_\infty$ of $\mathbb{F}_p(X)$ consisting of those elements of degree no greater than 0, as we mentioned above. We can call this the “prime at infinity,” though unlike the number field case, this place is non-archimedean. In fact, segregating this place from the others is entirely artificial.

**Lemma 7:** The set of valuation rings of $\mathbb{F}_p(X)$ above is precisely the set of all valuation rings of $\mathbb{F}_p(X)$. In other words the set of places of the field of rational functions $\mathbb{F}_p(X)$ is in one-to-one correspondence with the set of monic irreducible polynomials and the “prime at infinity.”
Proof: Let $R$ be a valuation ring of $F_p(X)$ and suppose $X \in R$. Then $F_p[X] \subset R$ and just as we did above with number fields, we may restrict the canonical map $R \to R/\mathfrak{M}$ to the polynomial ring $F_p[X]$, yielding a maximal ideal $\mathfrak{M}$ which is necessarily a principal ideal generated by a unique monic irreducible polynomial $P(X)$. We easily verify that $R = R_p$.

Now suppose $R$ is a valuation ring and $X \notin R$. Then $X^{-1} \in R$ so that $F_p[X^{-1}] \subset R$. Since $X \notin R, X^{-1} \in \mathfrak{M}$ and $\mathfrak{M} = X^{-1}F_p[X^{-1}]$. We see that $R$ contains all rational functions $f(X^{-1})/g(X^{-1}), f(X^{-1}), g(X^{-1}) \in F_p[X^{-1}]$ where $X^{-1} \not| g(X^{-1})$. Let $f/g$ be such a rational function, say $n = \deg(f)$ and $m = \deg(g)$. Then

$$\frac{f(X^{-1})}{g(X^{-1})} = \frac{X^{m+n}f(X^{-1})}{X^{m+n}g(X^{-1})} = \frac{h(X)}{k(X)}$$

for some $h(X), k(X) \in F_p[X]$ and $\deg(h) \leq \deg(k)$ since the constant coefficient of $g$ is non-zero. Therefore $R \supset R_\infty$. Clearly we must have equality here since otherwise $R$ is the entire field.

Lemma 8: Let $K$ be a number field or function field and let $\cdot |_1, \ldots, \cdot |_n$ be inequivalent non-trivial absolute values on $K$, $\alpha_1, \ldots, \alpha_n \in K$, and $\epsilon_1, \ldots, \epsilon_n > 0$. Then there is an $\alpha \in K$ with $|\alpha - \alpha_i| < \epsilon_i$ for all $i = 1, \ldots, n$.

Proof: We first claim that there is a $\beta \in K$ with $|\beta|_1 > 1$ and $|\beta|_i < 1$ for all $i = 2, \ldots, n$. We prove this claim by induction on $n$. The case $n = 2$ follows directly from exercise #2 from homework #7. Now suppose $n > 2$ and we have $\beta_1, \beta_2 \in K$ with $|\beta_1|_1 > 1$, $|\beta_1|_i < 1$ for $i = 2, \ldots, n - 1$, $|\beta_2|_1 > 1$ and $|\beta_2|_n < 1$. If $|\beta_1|_n \leq 1$ then $\beta = \beta_1^m \beta_2$ will do for sufficiently large $m$. If $|\beta_1|_n > 1$ then $\beta = \beta_1^m \beta_2/(1 + \beta_1^m)$ will do for sufficiently large $m$.

We have

$$\lim_{m \to \infty} \left| \frac{\beta^m}{1 + \beta^m} \right| = \begin{cases} 1 & \text{if } i = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Hence there is a $\gamma_1$ with $|\gamma_1|_1 \approx 1$ and $|\gamma_1|_i \approx 0$ for $i \neq 1$. Repeating the process with other absolute values in place of $|\cdot|_1$ above, we may construct $\gamma_1, \ldots, \gamma_n \in K$ where $\gamma_i$ is arbitrarily close to 1 with the $i$th absolute value and arbitrarily close to 0 for the others. In particular, we can find an $\alpha = \alpha_1 \gamma_1 + \cdots + \alpha_n \gamma_n$ that satisfies the conclusion of the lemma.

Theorem (Weak Approximation Theorem): Let $K$ be a function field, let $R_1, \ldots, R_n$ be distinct valuation rings of $K$, and denote the corresponding valuations by $v_1, \ldots, v_n$. Let $\alpha_1, \ldots, \alpha_n \in K$ and $z_1, \ldots, z_n \in \mathbb{Z}$. There is an $\alpha \in K$ with $v_i(\alpha - \alpha_i) = z_i$ for all $i = 1, \ldots, n$.

Proof: Choose $\delta_i \in K$ with $v_i(\delta_i) = z_i$ for all $i$ and get $\delta, \delta' \in K$ via Lemma 8 above with $v_i(\delta - \alpha_i) > z_i$ and $v_i(\delta' - \delta) > z_i$ for all $i = 1, \ldots, n$. One readily verifies via exercise #5 from homework #7 that $\alpha = \delta + \delta'$ does the trick.

Corollary: A function field has infinitely many places.

Proof: Suppose not and get an $\alpha \in K$ with $0 < |\alpha|_v < 1$ for all places $v \in M(K)$ by the Weak Approximation Theorem. As noted in the proof of Proposition 1, all valuation rings contain the entire field of constants of $K$. Therefore $\alpha^{-1}$ can’t be in any of our valuation rings, so certainly must be transcendental over $F_p$. But now by Lemma 6 there is a valuation ring containing $\alpha^{-1}$.

Definition: For a function field $K$ and valuation ring $R$, the residue class field of $R$ is $R/\mathfrak{M}$. This is an extension of $F_p$ and we say $[R/\mathfrak{M}: F_p]$ is the degree of the valuation/place of $K$.

Note that we may identify any element of the field of constants as an element of the residue class field since all valuation rings contain the field of constants as shown in the proof of Proposition 1. We can say more.

Lemma 9: If $K$ is a function field and $v \in M(K)$, then $\deg(v) \leq [K: F_p(\alpha)] < \infty$ for all non-zero $\alpha \in \mathfrak{M}$. 


Proof: As noted above, such an $\alpha$ is transcendental over $\mathbb{F}_p$ so that the degree $[K: \mathbb{F}_p(\alpha)]$ is necessarily finite. Let $\alpha_1, \ldots, \alpha_n \in R$ with $\alpha_i + \mathcal{M}$ linearly independent over $\mathbb{F}_p$. We claim that the $\alpha_i$'s are linearly independent over $\mathbb{F}_p(\alpha)$. To see why, suppose we have a non-trivial linear combination

$$\alpha_1 P_1(\alpha) + \cdots + \alpha_n P_n(\alpha) = 0$$

where the $P_i(\alpha) \in \mathbb{F}_p[\alpha]$ are polynomials in the variable $\alpha$. If not all $P_i$ are zero, then without loss of generality not all $P_i(\alpha)$ are divisible by $\alpha$, i.e., not all of the constant terms are zero. Denoting these constant terms by $a_i \in \mathbb{F}_p$ we readily see that $P_i(\alpha) + \mathcal{M} = a_i + \mathcal{M}$ for all $i$. But now

$$a_1(\alpha_1 + \mathcal{M}) + \cdots + a_n(\alpha_n + \mathcal{M}) = 0 + \mathcal{M},$$

contradicting our hypothesis.

Corollary: The field of constants of a function field is a finite extension of $\mathbb{F}_p$.

From now on we denote the field of constants by $\mathbb{F}_{q_K}$. Here $q_K$ is some power of the characteristic $p$. Note that one way to extend a function field is to “cheat” and merely extend the field of constants. This can be a terribly handy notion to exploit for function fields, something not available for number fields.