FUNCTION FIELDS AND THE CLASS NUMBER

CHAD KLUMB

Abstract. We introduce function fields, defining the class group and building up to a statement of the Riemann-Roch Theorem, which we then use to prove the finiteness of the class number for global function fields, modulo a few technical points (for which we provide references).

Contents

Date: December 14, 2010.

1. Introduction

Consider the rings $\mathbb{Z}$ and $F[t]$, where F is a field and $F[t]$ is the polynomial ring in one variable over F. These rings have many properties in common; for example, both are Euclidean domains. If, in addition, F is finite, then both have finite unit group, and every proper quotient of either is finite.

In algebraic number theory, one studies algebraic number fields, that is, finite extensions of $\mathbb{Q} = \operatorname{Frac} \mathbb{Z}$. Similarly, one can ask questions about finite extensions of $F(t) = \operatorname{Frac} F[t]$; given the similarities between the base rings $\mathbb{Z}$ and $F[t]$, one might expect to get analogous results in many situations.

The first definition we will work with is the following:

Definition. A *function field* is a field extension K/F with the property that some $x \in K$ is transcendental over F and $K/F(x)$ is a finite extension.

It turns out that the closest analogue to the algebraic number fields is the class of global function fields:

Definition. A *global function field* is a function field K/F where F is finite and algebraically closed in K. The field F is called the *constant field of* K.

It is easy to see that if K/F is a global function field, then F is in fact determined by K, namely as the algebraic closure in K of the prime field of K. (Hence, calling F the constant field of K makes sense.)

We will restrict attention to global function fields in Section 3; in the meantime, everything we do will work in an arbitrary function field.

1.1. Primes.

Throughout this subsection, K/F will be a fixed but arbitrary function field.

We begin by recalling a standard definition from algebra:

Definition. A *discrete valuation ring* is a PID with precisely one nonzero maximal ideal (and hence precisely one maximal ideal).

We will, at times, use the abbreviation DVR for discrete valuation ring.

Definition. A *prime* in K/F is a discrete valuation ring R containing F as a subring such that $\operatorname{Frac} R = K$.

It is worth mentioning that there are many equivalent definitions of DVR, and many equivalent definitions of a prime in K/F. The definition of prime used above is that in [2]. If R is a prime in K/F with maximal ideal P, we will sometimes call P a prime in K/F (à la [2]); we will be fairly consistent with using R and S for DVRs, and P and Q for maximal ideals in this situation.

We now compile some results about DVRs and primes, which will be of use later.

Lemma 1. *Suppose R is a DVR with maximal ideal P.*

(1) *P consists precisely of the nonunits of R.*
(2) *Conversely, any ring A with an ideal I consisting precisely of the nonunits in A has a unique maximal ideal (namely, I).*
(3) *The only nonzero prime ideal in R is P.*
(4) *If P is generated by $t \in R$, then every element of R has a unique expression of the form $t^n u$ where $n \geq 0$ and $u \in R^*$.*

Proof. The proofs of (1) and (2) are trivial, and (3) follows easily from (4) and the fact that R is a PID. Item (4) is standard but less trivial; see, for example, theorem 1.1.6 in [5] (such t is sometimes called a *local uniformizing parameter*). □

Lemma 2. *If R is a prime in K/F with maximal ideal P generated by $t \in R$, then every nonzero element of K has a unique expression of the form $t^n u$ where $n \in \mathbb{Z}$ and u is a unit in R. Moreover, the number n does not depend on the choice of generator t.*

Proof. Uniqueness is clear: if $t^n u = t^m v$, then in K we may write $t^{n-m} = vu^{-1}$. Note that t is not a unit in R (as $P = Rt$ is proper) but vu^{-1} is. It follows that $n = m$, and thence that $u = v$.

To see that n is independent of t, suppose r is another generator of P and $x \in K^*$ has been written in the form $x = t^n u$. As $P = Rt = Rr$, it follows that there exists a unit $v \in R$ with $t = rv$, and thus $x = t^n u = (rv)^n u = r^n v^n u$, where $v^n u$ is a unit in R.

Existence follows immediately from item (4) of the previous lemma, and the fact that $K = \operatorname{Frac} R$. □

It follows that if R is a prime in K/F and $P = Rt$ is the maximal ideal in R, then we have a well-defined map

$$\operatorname{ord}_P : K^* \to \mathbb{Z} : t^n u \mapsto n.$$

The previous lemma shows that this map is independent of the choice of generator t. Note that this map also determines P and R, namely

$$P = \{x \in K^* : \operatorname{ord}_P(x) > 0\}$$

and

$$R = \{x \in K^* : \operatorname{ord}_P(x) \geq 0\}.$$

For future use, we note the following:

Lemma 3. *If R is a prime in K/F with maximal ideal P, then the map $ord_P : K^* \to \mathbb{Z}$ satisfies the following properties:*

1. *$ord_P(xy) = ord_P(x) + ord_P(x)$ for all $x, y \in K^*$*
2. *$ord_P(x) = 0$ for all $x \in F^*$*
3. *$ord_P(x^{-1}) = -ord_P(x)$ for all $x \in K^*$*
4. *$ord_P(x + y) \geq \min\{ord_P(x), ord_P(y)\}$ if $x, y, x + y \in K^*$*

Proof. Proving these is an easy exercise. □

Next, we show that primes in K/F cannot properly contain one another.

Lemma 4. *If R is a prime in K/F and $r \in R$ is nonzero and algebraic over F then $r \in R^*$. In particular, R contains elements which are transcendental over F.*

Proof. Suppose $r \in R$ is nonzero and algebraic over F. Then we may write $p(r) = 0$ for some irreducible $p \in F[x]$. Write

$$p(x) = a_n x^n + \cdots + a_1 x + a_0.$$

As p is irreducible, we have $a_0 \neq 0$. Thus, dividing through by a_0, we have a relation of the form

$$b_n r^n + \cdots + b_1 r + 1 = 0,$$

which shows that
$$r^{-1} = -(b_n r^{n-1} + \cdots + b_1),$$
which lies in R as r does (and R contains F). $\square$

Proposition 1. *If R, S are primes in K/F and $R \subseteq S$ then $R = S$.*

Proof. Choose any nonzero $y \in S$; we must show that $y \in R$. Assume to the contrary that $y \notin R$. Let P be the maximal ideal in R; as observed above, we have
$$R = \{x \in K^* : \mathrm{ord}_P(x) \geq 0\}.$$
It follows that $\mathrm{ord}_P(y) < 0$, and so $\mathrm{ord}_P(y^{-1}) = -\mathrm{ord}_P(y) > 0$. Thus, $y^{-1} \in P$, so in particular $y^{-1} \in R$. As $R \subseteq S$, we also have $y^{-1} \in S$, so y is a unit in S.

Let Q denote the maximal ideal in S. By standard ring theory, the set $Q \cap R$ is a prime ideal in R, being the preimage of the prime ideal Q under the inclusion $R \hookrightarrow S$. Note that we have an injective ring homomorphism
$$R/(R \cap Q) \hookrightarrow S/Q : r + R \cap Q \mapsto r + Q$$
which preserves F (i.e., it sends $\overline{f} \in R/(R \cap Q)$ to $\overline{f} \in S/Q$ for all $f \in F$). By Proposition 2 below, S/Q is finite, hence algebraic, over F. By Lemma 4, R contains an element which is transcendental over F. It follows that $R \cap Q$ cannot be zero (for by the previous two sentences, R does not embed into S/Q via a map preserving F). As the only nonzero prime ideal in R is P, we have $R \cap Q = P$.

We observed above that y is a unit in S, so $y^{-1} \notin Q$. On the other hand, we also observed above that $y^{-1} \in P$. The equality $R \cap Q = P$ is now a contradiction. We conclude that $y \in R$, so $R = S$. $\square$

Definition. Recall that if R is a prime in K/F then F is a subring of R by definition. It follows that if P is the maximal ideal in R, then R/P is a K-vector space. We define the *degree of* P to be the dimension of R/P as a K-vector space, and denote it by $\deg P$.

Proposition 2. *If R is a prime in K/F with maximal ideal P, then* $\deg P < \infty$.

Proof. By definition, there exists $x \in K$, transcendental over F, such that $K/F(x)$ is finite. By Lemma 4, there is an element $y \in P$ which is transcendental over F.

We claim that $K/F(y)$ is finite. First, it is clear that $F(y)$ is algebraic over $F(x)$ (as K is algebraic over $F(x)$), so there is a nonzero polynomial $g \in F[X, Y]$ in two variables such that $g(x, y) = 0$. Since y is transcendental over F, we cannot have $g \in F[Y]$. It follows immediately that x is algebraic over $F(y)$. Obviously K is finite over $F(x, y)$ (as it is finite over $F(x)$), and we have just shown that $F(x, y)$ is finite over $F(y)$ (as x is algebraic over $F(y)$), so K is finite over $F(y)$.

Now, we claim that $\deg P \leq |K : F(y)|$. Suppose $r_1, \ldots, r_n \in R$ are chosen so that $r_1 + P, \ldots, r_n + P \in R/P$ are F-linearly independent. We claim that $r_1, \ldots, r_n \in K$ are $F(y)$-linearly independent. If not, there exist rational functions $q_1, \ldots, q_n$ of y with coefficients in F such that
$$r_1 q_1 + \cdots + r_n q_n = 0.$$
Clearing denominators and cancelling any common factors of y, this gives us a relation
$$r_1 p_1 + \cdots + r_n p_n = 0$$
where the p_i are polynomials in y with coefficients in F, and not every p_i is divisible by y.

Note that mod P, each $\overline{p}_i$ lies in F, as $y \in P$. Moreover, any p_i not divisible by y does not lie in P: the monomials cy^k ($k > 0$, $c \in F$) lie in P (as $y \in P$ and $F \subseteq R$), but the constant term of any such p_i is a nonzero element of F, and as F is a field contained in R and P consists precisely of the nonunits of R, it follows that $F \cap P = \{0\}$. Thus, $p_i \notin P$. It follows that reducing mod P gives us a nontrivial F-linear relation

$$\overline{r}_1\overline{p_1} + \cdots + \overline{r}_n\overline{p}_n = 0$$

amongst the $\overline{r}_i$, which is a contradiction. We conclude that $r_1, \dots, r_n$ are $F(y)$-linearly independent over K, so the assertion $\deg P \leq |K : F(y)|$ follows. □

1.2. **The Rational Function Field.** In this subsection, we illustrate the definitions made above in the special case of the function field $F(x)/F$ (where x is transcendental over F), called the *rational function field*. These considerations will also be used in Section 3, when we consider how primes behave with respect to extensions of function fields.

Our goal here is to classify primes in $F(x)/F$, and determine the degree of (most of) them. We first describe a family of primes in $F(x)/F$, naturally indexed by the monic irreducible polynomials in $F[x]$ (or, equivalently, the nonzero prime ideals in $F[x]$). We then show that these primes, and one additional exceptional prime, are the only primes in $F(x)/F$.

Let $p \in F[x]$ be a given monic irreducible polynomial. Define

$$\mathcal{O}_p = \{\frac{f}{g} : f, g \in F[x],\ p \nmid g\} \subseteq F(x)$$

and

$$P_p = \{\frac{f}{g} \in \mathcal{O}_p : p \mid f\}.$$

It is immediate that $\mathcal{O}_p$ is a ring, and it is easy to see that P_p is an ideal consisting precisely of the nonunits of $\mathcal{O}_p$ (note also that P_p is the principal ideal generated by $\frac{p}{1}$).

Thus, in order to show that $\mathcal{O}_p$ is a DVR (with maximal ideal P_p), we need only show that $\mathcal{O}_p$ is a PID. Suppose $I = (\{\frac{f_\alpha}{g_\alpha}\}_\alpha)$ is an ideal in $\mathcal{O}_p$, where the generators are normalized so that no g_α is divisible by p. By unique factorization in $F[x]$, we can multiply each $\frac{f_\alpha}{g_\alpha}$ by a unit u_α (in $\mathcal{O}_p$) such that $u_\alpha \frac{f_\alpha}{g_\alpha} = \frac{p^{n_\alpha}}{1}$ where p^{n_α} is the largest power of p dividing f_α. It follows that $I = (\frac{p^m}{1})$ where $m = \inf_\alpha n_\alpha$, so $\mathcal{O}_p$ is a DVR.

As $\mathcal{O}_p$ contains $\frac{f}{1}$ for all $f \in F[x]$, and $\mathcal{O}_p \subseteq F(x)$, it is clear that $\operatorname{Frac}\mathcal{O}_p = F(x)$. We conclude that $\mathcal{O}_p$ is a prime in $F(x)/F$. Note that if p and q are distinct monic irreducible polynomials in $F[x]$, then $\mathcal{O}_p \neq \mathcal{O}_q$ (for example, $\frac{1}{q} \in \mathcal{O}_p \setminus \mathcal{O}_q$). Also, we can explicitly describe the ord maps ord_{P_p} (or ord_p for short), specifically

$$\operatorname{ord}_p(p^n \frac{f}{g}) = n \qquad\qquad (p \nmid f, g)$$

As for the exceptional prime, we define

$$\mathcal{O}_\infty = \{\frac{f}{g} : f, g \in F[x],\ \deg f \leq \deg g\}$$

and

$$P_\infty = \{\frac{f}{g} \in \mathcal{O}_\infty : \deg f < \deg g\}.$$

It is not hard to see that $\mathcal{O}_\infty$ is a ring, and that P_∞ is an ideal in $\mathcal{O}_\infty$ consisting precisely of the nonunits. Also, observe that P_∞ is generated by $\frac{1}{x}$: if $\frac{f}{g} \in P_\infty$, so that $\deg f < \deg g$, then we may write $\frac{f}{g} = \frac{1}{x}\frac{xf}{g}$ where $\deg xf \leq \deg g$.

Now, we claim that $\mathcal{O}_\infty$ is a PID, so that it is in fact a DVR with maximal ideal P_∞. Observe that if $\frac{f}{g}$ is any nonzero element of $\mathcal{O}_\infty$, then

$$\frac{f}{g} \cdot \frac{g}{fx^{\deg g - \deg f}} = x^{\deg f - \deg g},$$

where $\frac{g}{fx^{\deg g - \deg f}}$ is a unit in $\mathcal{O}_\infty$ (to obtain its inverse, interchange the numerator and denominator). It follows that any nonzero ideal I in $\mathcal{O}_\infty$ is generated by x^m where $m = \sup_{\frac{f}{g} \in I} \deg f - \deg g$, so $\mathcal{O}_\infty$ is a DVR. It is also the case that $\operatorname{Frac} \mathcal{O}_\infty = F(x)$, as $\mathcal{O}_\infty \subseteq F(x)$ and $\frac{1}{f} \in \mathcal{O}_\infty$ for all nonzero $f \in F[x]$. It particular, $\mathcal{O}_\infty$ is a prime in $F(x)$. Note also that $\mathcal{O}_\infty \neq \mathcal{O}_p$ for any monic irreducible p in $F[x]$; e.g., $x \in \mathcal{O}_p \setminus \mathcal{O}_\infty$. Also, our discussion above shows that the ord function $\operatorname{ord}_{P_\infty}$ (or $\operatorname{ord}_\infty$ for short) is given by

$$\operatorname{ord}_\infty(\frac{f}{g}) = \deg g - \deg f.$$

Proposition 3. *The primes in $F(x)/F$ are precisely $\mathcal{O}_\infty$ and $\mathcal{O}_p$ for monic irreducible $p \in F[x]$.*

Proof. We need only show that if R is a given prime in $F(x)/F$ then R is either $\mathcal{O}_\infty$ or $\mathcal{O}_p$ for some p. We proceed via two cases. First, suppose $x \in R$. In this case, $F[x] \subseteq R$. If we let P be the maximal ideal in R, then we have an injection

$$F[x]/(P \cap F[x]) \hookrightarrow R/P : f + P \cap F[x] \mapsto f + P.$$

As proven in Proposition 2, R/P is finite, hence, algebraic, over F. As x is not algebraic over F, the above injection implies that $P \cap F[x]$ is nonzero. As P is prime, so too is $P \cap F[x]$, so we may write $P \cap F[x] = (p)$ for some (uniquely determined) monic irreducible p in $F[x]$. Thus, if $g \in F[x]$ is not divisible by p, then $g \notin P$. Our previous remarks about ord functions imply that $\operatorname{ord}_P(g) \leq 0$, so $\operatorname{ord}_P(g^{-1}) = -\operatorname{ord}_P(g) \geq 0$, and thus $g^{-1} \in R$. Since $F[x] \subseteq R$ was observed above, it follows immediately that any $\frac{f}{g} \in F(x)$ with $p \nmid g$ lies in R. By definition, R contains $\mathcal{O}_p$, and so by Proposition 1, we have $R = \mathcal{O}_p$.

Now, suppose instead that $x \notin R$. Thus, $\operatorname{ord}_P(x) < 0$, so $\operatorname{ord}_P(x^{-1}) = -\operatorname{ord}_P(x) > 0$, so $x^{-1} \in P$ (where, as above, P denotes the maximal ideal in R). It follows that R contains $F[x^{-1}]$, and that $P \cap F[x^{-1}]$ is a prime ideal in $F[x^{-1}]$ containing x^{-1}. As x^{-1} is irreducible in $F[x^{-1}]$, we must have that $P \cap F[x^{-1}]$ is the ideal generated by x^{-1}. Thus, as R contains $F[x^{-1}]$ and P consists precisely of the nonunits in R, we have $\frac{1}{g} \in R$ for any $g \in F[x^{-1}]$ with $x^{-1} \nmid g$. Thus, we have $\frac{f}{g} \in R$ for all $f, g \in F[x^{-1}]$ with $x^{-1} \nmid g$. Now, recall that

$$\mathcal{O}_\infty = \{\frac{u}{v} : u, v \in F[x],\ \deg u \leq \deg v\}.$$

Given such $\frac{u}{v} \in \mathcal{O}_\infty$, set $f = ux^{-\deg v}$ and $g = vx^{-\deg v}$, so that $f, g \in F[x^{-1}]$, $x^{-1} \nmid g$, and $\frac{u}{v} = \frac{f}{g}$. It follows that $\frac{u}{v} \in R$, so $\mathcal{O}_\infty \subseteq R$. By Proposition 1, we have $\mathcal{O}_\infty = R$. $\square$

Finally, we claim that $\deg P_p = \deg p$ for monic irreducible $p \in F[x]$. Set $n = \deg p$. We claim that $\frac{1}{1}, \ldots, \frac{x^{n-1}}{1}$ is an F-basis for $\mathcal{O}_p/P_p$. First, observe that any $\frac{f}{g} \in \mathcal{O}_p$ is equivalent (mod P_p) to some $\frac{h}{1} \in \mathcal{O}_p$. To see this, note that as p is irreducible and $p \nmid g$ we have $(g, p) = 1$ so $ag + bp = 1$ for some $a, b \in F[x]$. Then $\frac{1}{g} - \frac{a}{1} = \frac{1-ag}{g} = \frac{bp}{g}$ which is equivalent to 0 mod P_p. Therefore, $\frac{1}{g}$ is equivalent to $\frac{a}{1}$, so $\frac{f}{g}$ is equivalent to $\frac{af}{1}$.

Next, we have a relation of the form $\frac{x^n}{1} \equiv -\frac{\sum_{i=0}^{n-1} c_i x^i}{1}$ (mod P_p), where the c_i are the coefficients of p. Thus, every element of $\mathcal{O}_p/P_p$ has a representative of the form $\frac{u}{1}$ where $u = 0$ or $\deg u < \deg p$. Moreover, it is easy to see that if u and v are distinct and satisfy $u = 0$ or $\deg u < \deg p$ and $v = 0$ or $\deg v < \deg p$, then $\frac{u}{1} \not\equiv \frac{v}{1}$ (mod P_p), for the difference $\frac{u-v}{1}$ is nonzero and cannot lie in P_p as $\deg u - v < \deg p$. Thus, every element of $\mathcal{O}_p/P_p$ has a unique representative of the above form, and it follows immediately that $\frac{1}{1}, \ldots, \frac{x^{n-1}}{1}$ is an F-basis for $\mathcal{O}_p/P_p$, so $\deg P_p = n = \deg p$.

1.3. **Divisors.** We now return to the case of a general function field.

Definition. The group of *divisors* $\mathcal{D}_K$ of a function field K/F is the free abelian group on the primes in K/F. Thus a divisor in K/F is of the form $\sum_P a_P P$ where the sum is taken over all primes P in K/F and the a_P are integers, only finitely many of which are nonzero.

Recall that the group of fractional ideals in a Dedekind domain is a free abelian group on the prime ideals, so the above definition of $\mathcal{D}_K$ is at least superficially similar to what we proved for fractional ideals. (Of course, we haven't said much in the way of why primes in K/F as we defined them are the appropriate analogues of prime ideals in a Dedekind domain.)

Definition. The *degree* of a divisor $\sum_P a_P P \in \mathcal{D}_K$ is defined to be the integer $\sum_P a_P \deg P$. This clearly gives us a group homomorphism $\deg : \mathcal{D}_K \to \mathbb{Z}$ sending a divisor to its degree.

Definition. A divisor $D = \sum_P a_P P \in \mathcal{D}_K$ is called *effective* if $a_P \geq 0$ for all P. We write this as $D \geq 0$.

Definition. If K/F is a function field and $a \in K^*$, define the *principal divisor of* a to be the divisor $(a) = \sum_P \mathrm{ord}_P(a) P$.

It is important to note that principal divisors are well-defined as divisors of K/F. By considering how the ord functions behave with respect to taking inverses, and recalling that $a \in K^*$ satisfies $\mathrm{ord}_P(a) > 0$ iff $a \in P$, it is easy to see that principal divisors are well-defined if and only if each nonzero element of K lies in only finitely many primes P in K/F. (In this case, prime refers to the maximal ideal, not the DVR.) If $a \in K$ is transcendental over F, then it is easy to see that there are only finitely many primes in $F(a)/F$ containing a (using our classification above), and so by the theorem on extensions of primes in Section 3, there are only finitely many primes in K/F containing a. For the general case, see page 47 of [2].

We will also need the following fact: if (a) is a principal divisor, then $\deg(a) = 0$. The proof is contained in the same proposition on page 47 of [2].

Definition. If K/F is a function field, the set of all principal divisors in $\mathcal{D}_K$ is denoted by $\mathcal{P}_K$. It is easy to see that if $a, b \in K^*$ then $(ab) = (a) + (b)$ (as

$\mathrm{ord}_P(ab) = \mathrm{ord}_P(a) + \mathrm{ord}_P(b)$ for all P) and $(c) = 0$ for any $c \in F^*$ (as any prime R contains c, and its maximal ideal P does not). It follows that $(x^{-1}) = -(x)$, and so $\mathcal{P}_K$ is in fact a subgroup of $\mathcal{D}_K$. We define $Cl_K = \mathcal{D}_K/\mathcal{P}_K$ to be the *class group of* K/F. Elements of Cl_K are called *divisor classes*. As principal divisors have degree zero, we have a well-defined induced map $\deg : Cl_K \to \mathbb{Z}$ sending $D + \mathcal{P}_K$ to $\deg D$. Denote by Cl_K^o the kernel of this map deg. We set $h_K = |Cl_K^o|$, called the *class number of* K/F.

Definition. If D is a divisor in K/F, define $L(D) = \{x \in K^* : (x) + D \geq 0\} \cup \{0\}$. Properties of the ord maps compiled above immediately imply that $L(D)$ is an F-vector space. We let $l(D)$ denote the dimension of $L(D)$ as an F-vector space.

Lemma 5. *If D is a divisor in K/F, then $l(D) < \infty$.*

Proof. This result follows easily from a few simple lemmas, but since we will not need the details of the proof, we direct the reader to page 19 of [5]. □

2. The Riemann-Roch Theorem

We can now state the Riemann-Roch Theorem:

Theorem 1 (The Riemann-Roch Theorem). *If K/F is a function field then there exists an integer $g \geq 0$ and a divisor class $\mathcal{C} \in Cl_K$ such that for all $C \in \mathcal{C}$ and all $A \in \mathcal{D}_K$ we have*

$$l(A) = \deg(A) - g + 1 + l(C - A).$$

Moreover, the integer g and the divisor class $\mathcal{C}$ are uniquely determined by K/F, and are called the genus *and* canonical class*, respectively.*

For a proof, see Chapter 6 of [2].

A useful corollary is the following:

Corollary 1 (Riemann's Inequality). *For $A \in \mathcal{D}_K$ we have $l(A) \geq \deg A - g + 1$.*

Proof. $l(C - A) \geq 0$. □

3. Finiteness of the Class Number

We now consider a global function field K/F. The goal is to show that the class number, h_K, is finite. Fix $x \in K$, transcendental over F, with $K/F(x)$ finite.

Definition. If R is a prime in $F(x)/F$ with maximal ideal P and S is a prime in K/F with maximal ideal Q, we say that Q lies over P if $Q \cap F(x) = P$ and $S \cap F(x) = R$.

Remark. The conditions in the above definition are somewhat redundant, and the notion of one prime lying over another can be generalized to cases other than the extension K/F of $F(x)/F$, but the above will suffice for our purposes.

Lemma 6 (Strict Triangle Inequality). *If P is a prime in K/F and $x, y \in K^*$ satisfy $ord_P(x) \neq ord_P(y)$ then $ord_P(x + y) = \min\{ord_P(x), ord_P(y)\}$.*

Proof. Given x and y as above, take $\mathrm{ord}_P(x) < \mathrm{ord}_P(y)$ without loss of generality. Note that $\mathrm{ord}_P(-y) = \mathrm{ord}_P(y)$ by previously compiled properties of ord functions (as $-1 \in F^*$). In particular, $x + y \neq 0$.

Now, if $\mathrm{ord}_P(x+y) \neq \min\{\mathrm{ord}_P(x), \mathrm{ord}_P(y)\}$, then $\mathrm{ord}_P(x+y) > \mathrm{ord}_P(x)$. We then have

$$\mathrm{ord}_P(x) = \mathrm{ord}_P((x+y)-y) \geq \min\{\mathrm{ord}_P(x+y), \mathrm{ord}_P(-y)\} > \mathrm{ord}_P(x),$$

which is a contradiction. Thus, $\mathrm{ord}_P(x+y) = \min\{\mathrm{ord}_P(x), \mathrm{ord}_P(y)\}$. □

Proposition 4.

(1) *Each prime in K/F lies over a prime in $F(x)/F$.*
(2) *Each prime in $F(x)/F$ has at least one but only finitely many primes lying over it in K/F.*
(3) *If Q lies over P, then $\deg Q \geq \deg P$.*

Proof. We first prove (1). Let S be a prime in K/F with maximal ideal Q, and let $R = S \cap F(x)$ and $P = Q \cap F(x)$. As Q consists precisely of the nonunits in S and as $F(x)$ is a field, it is clear that P consists precisely of the nonunits in R. Moreover, as $\mathrm{Frac}\, S = K$ and K contains $F(x)$, we have $\mathrm{Frac}\, R = \mathrm{Frac}\,(S \cap F(x)) = F(x)$. Thus, to show that R is a prime in P, we need only show that R is a PID and P is a nonzero ideal in R. Note that $R = \{y \in F(x)^* : \mathrm{ord}_Q(y) \geq 0\} \cup \{0\}$ and $P = \{y \in F(x)^* : \mathrm{ord}_Q(y) > 0\} \cup \{0\}$.

We first show that P is nonzero. Clearly it suffices to show that there is some element $y \in F(x)^*$ with $\mathrm{ord}_Q(y) > 0$. Suppose to the contrary that $\mathrm{ord}_Q(y) = 0$ for all $y \in F(x)^*$. Choose any $t \in K$ with $\mathrm{ord}_Q(t) > 0$. Since K is finite (hence algebraic) over $F(x)$, we may choose $c_0, \ldots, c_{n-1} \in F(x)$, with $c_0 \neq 0$, such that

$$t^n + c_{n-1}t^{n-1} + \cdots + c_0 = 0.$$

For any i such that c_i is nonzero, we have

$$\mathrm{ord}_Q(c_i t^{n-i}) = \mathrm{ord}_Q(c_i) + \mathrm{ord}_Q(t^{n-i}) = 0 + (n-i)\mathrm{ord}_Q(t).$$

An easy application of the Strict Triangle Inequality now shows that $\mathrm{ord}_Q(t^n + c_{n-1}t^{n-1} + \cdots + c_0)$ exists and is positive, which is impossible, as $\mathrm{ord}_Q(0)$ is undefined. We conclude that some $y \in F(x)^*$ has $\mathrm{ord}_Q(y) \neq 0$.

It is easy to see that P is an ideal: if $p \in P$ and $r \in R$ are nonzero then $\mathrm{ord}_Q(pr) = \mathrm{ord}_Q(p) + \mathrm{ord}_Q(r) \geq \mathrm{ord}_Q(p) > 0$, so $pr \in P$. Similarly, if $p, r \in P$ and $p \neq -r$ then $\mathrm{ord}_Q(p+r) \geq \min\{\mathrm{ord}_Q(p), \mathrm{ord}_Q(r)\} > 0$, so $p + r \in P$.

Finally, we must show that R is a PID. We proceed as follows. Let $I = (\{i_\alpha\}_\alpha)$ be a proper, nonzero ideal in R, where the i_α are nonzero generators; choose n to be the smallest positive integer with $\mathrm{ord}_Q(i) = n$ for some $i \in I$. Let t be a local uniformizing parameter for Q, so $i = t^n u$ for some unit u in K. We claim that every element of I is a multiple of $t^n u$ by an element of R. It suffices to show that for each α there exists $c_\alpha \in R$ with $i_\alpha = c_\alpha i$. As $\mathrm{ord}_Q(i_\alpha) \geq n$, we have $i_\alpha = t^m v$ for some $m \geq n$ and some unit v in K. As i and i_α both lie in $F(x)$, so too does $c_\alpha \equiv i_\alpha i_\alpha^{-1} = t^{m-n}vu^{-1}$. Moreover, as $m \geq n$ we clearly have $\mathrm{ord}_Q(c_\alpha) \geq 0$, so $c_\alpha \in R$. It follows that I is generated by i, so R is a PID.

The proof of (2) seems to involve some concepts we haven't introduced here; see for example page 71 of [5].

Finally, we prove (3). Let S be the prime with maximal ideal Q, and R the prime with maximal ideal P. By definition, we have an equality

$$R/P = (S \cap F(x))/(Q \cap F(x)).$$

On the other hand, by standard ring theory we have an injective ring-homomorphism

$$(S \cap F(x))/(Q \cap F(x)) \hookrightarrow S/Q : s + Q \cap F(x) \mapsto s + Q,$$

and it is easy to see that this map is F-linear. Therefore, R/P embeds into S/Q as F-vector spaces, so $\dim_F R/P \leq \dim_F S/Q$, i.e., $\deg P \leq \deg Q$. □

Lemma 7. *For each $n \geq 0$, there are finitely many effective divisors in K/F of degree n.*

Proof. By the definition of effective divisor, it suffices to show that there are finitely many primes in K/F of degree at most n. By our classification of primes in $F(x)/F$, the number of primes of degree at most n in $F(x)/F$ is bounded by the number of monic irreducible polynomials of degree at most n in $F[x]$, plus 1. As F is finite, there are finitely many monic irreducible polynomials of degree at most n in $F[x]$, and thus there are finitely many primes of degree at most n in $F(x)/F$. By Proposition 4, there are finitely many primes of degree at most n in K/F. □

We can now prove the following

Theorem 2. *The class number h_K is finite.*

Proof. Fix a divisor D in K/F of degree at least g, the genus of K/F. (For example, $D = gP$ for any prime P will work.) Given a divisor $A \in \mathcal{D}_K$ of degree 0, we have $\deg(D + A) = \deg D + \deg A = \deg D \geq g$. By Riemann's inequality, $l(D + A)$ is at least 1, so there is a nonzero $h \in L(D + A)$. Set $B = (h) + D + A$, so by the definition of h we have $B \geq 0$. Recall that $\deg(h) = 0$, so $\deg B = \deg D$. Also, we have $B - D = (h) + A$, so $A \equiv B - D \bmod \mathcal{P}_K$. It follows that h_K is bounded by the number of effective degree $\deg D$ divisors in K/F, which we showed above was finite. □

References

[1] Koch, Helmut. *Number Theory: Algebraic Numbers and Functions.* AMS, 2000.

[2] Rosen, Michael. *Number Theory in Function Fields.* Springer, 2002.

[3] Schmidt, F.K. Analytischen Zahlentheorie in Körpern der Characteristik p, *Math Zeit.* **33** (1931), 668-678.

[4] Spalk, Henrik Gadegaard. *Curves, Function Fields, and the Riemann Hypothesis.* 2001.

[5] Stichtenoth, Henning. *Algebraic Function Fields and Codes.* Springer, 2009.