Algorithmic Number Theory in Function Fields
Practice Problems

Renate Scheidler

Most of these questions are facts stated (but not proved) during the lectures. Questions with one or more asterisks reinforce the material covered in the lectures. The number of asterisks indicates the importance of a problem to the material in my (and in some cases the other instructors') lectures. A higher number of asterisks indicates a higher degree of importance. Note that the level of difficulty of a problem has no bearing in its number of asterisks.

Valuations and Places

1. $**$ (Simple properties of valuations)

   Prove the following properties of a valuation v on a field F:

   (a) $v(1) = 0$, $v(-1) = 0$, $v(a) = v(-a)$ for all $a \in F$, $v(a^{-1}) = -v(a)$ for all $a \in F^*$.

   (b) (*Strict triangle inequality*): if $v(a) \neq v(b)$, then $v(a+b) = \min\{v(a), v(b)\}$.

   (c) Suppose that v is discrete. Prove that v is normalized if and only if it is surjective.

2. $***$ (Examples of valuations)

   (a) Let F be any field. For any $a \in F$, define $v(a) = \infty$ when $a = 0$ and $v(a) = 0$ otherwise. Prove that v is a valuation on F. Determine O_v, P_v and F_v.

   (b) Let $p \in \mathbb{N}$ be a fixed prime. For $r \in \mathbb{Q}^*$, write $r = p^n a/b$ with $a, b, n \in \mathbb{Z}$, $b \neq 0$ and $p \nmid ab$. Define $v_p(r) = n$. Prove that v_p is a discrete valuation on $\mathbb{Q}$ with uniformizer p, discrete valuation ring

   $$O_{v_p} = \{r \in \mathbb{Q} \mid r = a/b \text{ with } \gcd(a,b) = 1 \text{ and } p \nmid b\} ,$$

   corresponding place

   $$P_{v_p} = \{r \in \mathbb{Q} \mid r = a/b \text{ with } \gcd(a,b) = 1,\ p \mid a,\ p \nmid b\} ,$$

   and residue field $F_{v_p} = \mathbb{F}_p$.

   (c) Let K be a field and $p(x) \in K[x]$ a fixed monic irreducible polynomial. For $r(x) \in K(x)$ non-zero, write $r(x) = p(x)^n a(x)/b(x)$ with $a(x), b(x) \in K[x]$, $b(x) \neq 0$ and $p(x) \nmid a(x)b(x)$. Define $v_{p(x)}(r(x)) = n$. Prove that $v_{p(x)}$ is a valuation on $K(x)$ with uniformizer $p(x)$, discrete valuation ring

   $$O_{v_{p(x)}} = \{r(x) \in K(x) \mid r(x) = a(x)/b(x) \text{ with } \gcd(a,b) = 1 \text{ and } p(x) \nmid b(x)\} ,$$

corresponding place

$$P_{v_{p(x)}} = \{r(x) \in K(x) \mid (x) = a(x)/b(x) \text{ with } \gcd(a,b) = 1, p(x) \mid f(x), \text{ and } p(x) \nmid g(x)\},$$

and residue field $F_{v_{p(x)}} = K[x]/(p(x))$, where $(p(x))$ is the $K[x]$-ideal generated by $p(x)$.

(d) Let K be a field. For $r(x) = a(x)/b(x) \in K(x)^*$ with $a(x), b(x) \in K[x]$ and $b(x) \neq 0$, define $v_\infty(r(x)) = \deg(b) - \deg(a)$ Prove that v_∞ is a valuation on $K(x)$ with uniformizer x^{-1}, discrete valuation ring

$$O_{v_\infty} = \{r(x) \in K(x) \mid r(x) = a(x)/b(x) \text{ with } \deg(a) \leq \deg(b)\},$$

corresponding place

$$P_{v_\infty} = \{r(x) \in K(x) \mid (x) = a(x)/b(x) \text{ with } \deg(a) < \deg(b)\},$$

and residue field $F_{v_\infty} = K$.

3. (Properties of valuation rings)

Let v be a discrete normalized valuation on some field F. Prove the following properties:

(a) O_v is an integral domain.

(b) O_v is a discrete valuation ring, i.e. $O_v \subsetneq F$ and for $a \in F^*$, we have $a \in O_v$ or $a^{-1} \in O_v$.

(c) O_v^* is the unit group of O_v, i.e. the set of invertible elements in O_v.

(d) P_v is the unique maximal ideal of O_v.

4. $**$ (Uniformizers of rational function fields)

Let $K(x)$ be a rational function field, and let $v = v_{p(x)}$ with $p(x) \in K[x]$ monic and irreducible, or $v = v_\infty$. In the former case, set $u = p(x)$; in the latter case, put $u = x^{-1}$. Prove the following properties:

(a) Every non-zero $a \in K(x)$ has a unique representation $a = \epsilon u^n$ with $\epsilon \in O_v^*$ and $n = v(a) \in \mathbb{Z}$.

(b) P_v is a principal ideal generated by u.

(c) O_v is a principal ideal domain whose ideals are generated by the non-negative powers of u.

5. $*$ (More properties of valuation rings of $\mathbb{Q}$ and $K(x)$)

(a) For any prime $p \in \mathbb{N}$, let v_p denote the corresponding p-adic valuation on $\mathbb{Q}$. Prove that $\bigcap_p O_{v_p} = \mathbb{Z}$, $\bigcap_p O_{v_p}^* = \{\pm 1\}$, and $\bigcap_p P_{v_p} = \{0\}$.

(b) Let $K(x)$ be a rational function field.

i. Prove that $\bigcap_{p(x)} O_{v_{p(x)}} = K[x]$ and $\bigcap_{p(x)} O_{v_{p(x)}} \cap O_{v_\infty} = K$.

ii. Conclude that $\sum_{P \in \mathbb{P}(K(x))} v_P(z) = 0$ for all non-zero $z \in K(x)$.

6. (Correspondence of valuations and places)

   Recall that a *discrete valuation ring* in a field F is a proper sub-ring O of K such that $a \in O$ or $a^{-1} \in O$ for all $a \in F^*$. Prove the *Correspondence Theorem*:

   > There is a one-to-one correspondence between the set of normalized discrete valuations on F and the set $\mathbb{P}(F)$ of places of F, as follows:
   >
   > - If v is a normalized discrete valuation on F, then $P_v \in \mathbb{P}(F)$ is the unique maximal ideal in the discrete valuation ring O_v.
   > - If P is a place of F, i.e. the unique maximal ideal in some discrete valuation ring $O \subset K$, then P defines a discrete normalized valuation on F as follows: if u is any generator of P, then every element $a \in F^*$ has a unique representation $a = \epsilon u^n$ with $n \in \mathbb{Z}$ and ϵ a unit in O, and we define $v(a) = n$ and $v(0) = \infty$. Note that u is a uniformizer for v.

Constant Fields

7. $*$ (Exact constant fields)

   Let F/K be a function field with exact constant field $\tilde{K}$. Show that $K \subseteq \tilde{K} \subsetneq F$, and every element in $F \setminus \tilde{K}$ is transcendental over K.

8. $**$ (Examples of geometric extensions)

   Let K be a field.

   (a) Show that every rational function field $K(x)$ is geometric.

   (b) Show that if K is algebraically closed, then then every function field F/K is geometric.

   (c) Show that a function field $K(x, y)$ is geometric if and only if the minimal polynomial of y over $K(x)$ is absolutely irreducible, i.e. irreducible over $\overline{K}(x)$ where $\overline{K}$ is the algebraic closure of K.

9. (An example of a non-geometric extension)

   Suppose -1 is not a square in K (e.g. $K = \mathbb{R}$ or $K = \mathbb{F}_q$ with $q \equiv 3 \pmod 4$), and let $F = K(x, y)$ where $x^2 + y^4 = 0$. Prove that $\tilde{K} = K(i)$ where $i \notin K$ is a square root of -1. So F/K is not geometric.

10. $*$ (All places contain the exact constant field)

    Let F/K be a function field and P a place of F, i.e. P is the unique maximal ideal in a discrete valuation ring $O = O_P$ in F. Prove that $\tilde{K} \subsetneq O_P$.

    Hint: Let $z \in \tilde{K}$. Then $z \in O_P$ or $z^{-1} \in O_P$. In the latter case, show that $z \in O_P[z^{-1}] \subset O_P$.

Divisors and Class Groups

11. $*$ (Rational function fields have class number one)

    Let $F = K(x)$ be a rational function field.

(a) Let $p(x) \in K[x]$ be monic and irreducible. Prove that the zero divisor of $\operatorname{div}(p(x))$ is $P_{p(x)}$ (the place of $K(x)$ with uniformizer $p(x)$) and the pole divisor of $\operatorname{div}(p(x))$ is P_∞ (the infinite place of $K(x)$). In other words, $\operatorname{div}(p(x)) = P_{p(x)} - \deg(p(x))P_\infty$.

(b) Let $f(x) \in K[x] \setminus K$, and let $f(x) = ap_1(x)^{n_1}p_2(x)^{n_2}\cdots p_r(x)^{n_r}$ be the factorization of $f(x)$ into distinct powers of monic irreducible polynomials $p_i(x) \in K[x]$ (with $a \in K^*$). Prove that

$$\operatorname{div}(f(x)) = \sum_{i=1}^{r} n_i P_{p_i(x)} - \left(\sum_{i=1}^{r} n_i \deg(p_i(x))\right) P_\infty$$

(c) Prove that every divisor of $K(x)$ is principal; in other words, $K(x)$ has class number one.

12. $**$ (Effective divisors of degree 0 and 1)

Let F/K be a function field. A divisor $D \in \operatorname{Div}(F)$ is *effective* if $v_P(D) \geq 0$ for all $P \in \mathbb{P}(F)$.

(a) Characterize all effective degree zero divisors of F.

(b) Characterize all effective degree one divisors of F.

13. $*$ (Properties of principal divisors)

Let F/K be a function field.

(a) Let $z \in F^*$. Show that $\operatorname{div}(z) = 0$ if and only if $z \in K^*$.

(b) Conclude that $\bigcap_{P \in \mathbb{P}(F)} O_P = K$.

(c) Prove that the map $\operatorname{div} : F^* \to \operatorname{Prin}(F)$ via $z \mapsto \operatorname{div}(z)$ is a surjective homomorphism with kernel K^*.

14. Show that linear equivalence is an equivalence relation on the set of divisors of a function field.

15. $***$ (Embedding degree one places into the class group)

Let F/K be a non-rational function field that has a rational place, denoted Q.

(a) Prove that the map $\Phi_Q : \mathbb{P}_1(F) \to \operatorname{Cl}^0(F)$ via $P \mapsto [P - Q]$ is injective. Here, $[D]$ denotes the divisor class of D in $\operatorname{Cl}(F)$.

Hint: Use that fact that $[F : K(x)] = \deg(\operatorname{div}(x)_0)$ for all $x \in F \setminus K$.

(b) Explain how the injection Φ_Q can be used to impose a group structure on $\mathbb{P}_1(F)$. What is the group identity? (Note that this group structure is *not* canonical as it depends on the choice of Q.)

Genus and Riemann-Roch

16. $**$ (Properties of Riemann-Roch spaces)

Let F/K be a function field and $D, D' \in \operatorname{Div}(F)$. Prove the following:

(a) $x \in L(D)$ if and only if $v_P(x) \geq -v_P(D)$ for all $P \in \mathbb{P}(F)$.

(b) $L(D)$ is a K-vector space.

(c) If $[D] = [D']$, then $L(D)$ and $L(D')$ are isomorphic as K-vector spaces.

(d) $L(0) = K$, where 0 is the trivial divisor.

(e) If $\deg(D) < 0$ or $D \in \mathrm{Div}^0(F) \setminus \mathrm{Prin}(F)$, then $L(D) = \{0\}$.

(f) $L(D) \neq \{0\}$ if and only if the class $[D]$ contains an effective divisor.

17. $**$ (Examples of Riemann-Roch spaces)

(a) Let $K(x)$ be a rational function field.

i. Prove that if $D = -3P_{x-1} + 2P_{x-2} + 4P_{x-7}$, then

$$L(D) = \left\{ \frac{(x-1)^3}{(x-2)^2(x-7)^4} r(x) \;\mid\; r(x) \in K(x), \deg(r) \leq 3 \right\}.$$

ii. Prove that $L(nP_\infty) = \{f(x) \in K[x] \;\mid\; \deg(f) \leq n\}$ for all $n \geq 0$.

(b) Let F/K be any function field and $P \in \mathbb{P}(F)$. Prove that

$$L(nP) \setminus L((n-1)P) = \{x \in F \;\mid\; \mathrm{div}(x)_\infty = nP\}$$

for all $n \in \mathbb{N}$.

18. $*$ (Consequences of the Riemann-Roch Theorem)

Let F/K be a function field. Prove the following:

(a) $\deg(W) = 2g - 2$ and $\ell(W) = g$ for any canonical divisor W of F.
Hint: Apply the Riemann-Roch Theorem first to $D = 0$ and then to $D = W$.

(b) If $D \in \mathrm{Div}(F)$ with $\deg(D) \geq 2g - 1$, then $\ell(D) = \deg(D) - g + 1$.
Hint: Apply the Riemann-Roch Theorem first to $D - W$ were W is any canonical divisor, and then to D.

19. $*$ (Rational function fields have genus zero)

(a) Let $F = K(x)$ be a rational function field and $n \geq 0$. Prove that $\{1, x, x^2, \ldots, x^n\}$ is a basis of $L(nP_\infty)$, so $\ell(nP_\infty) = n + 1$.
Hint: Part (a) ii of Problem 17.

(b) Prove that every rational function field has genus zero.
Hint: Part (a), and part (b) of Problem 18.

20. (Genus zero function fields have class number one)

Let F/K be a function field of genus 0 and $D \in \mathrm{Div}^0(F)$.

(a) Prove that $L(D) = K$.
Hint: Part (b) of Problem 18.

(b) Prove that D is principal.
Hint: Part (e) of Problem 16.

Extensions

Throughout, let K be a perfect field.

21. (Extensions and constant fields)

    Let F/K and F'/K' be geometric function fields with $F \subseteq F'$ and $K \subseteq K'$. Prove hat K'/K is algebraic, $F \cap K' = K$, and F'/K' is a finite geometric extension of the composite field FK'/K'.

22. $**$ (Degree in extensions, norm and co-norm)

    Let F/K and F'/K' be geometric function fields with $F \subseteq F'$ and $K \subseteq K'$. Prove the following:

    (a) $\deg(P') = \dfrac{f(P'|P)}{[K' : K]} \deg(P)$ for all $P \in \mathbb{P}(F)$, $P' \in \mathbb{P}(F')$ with $P'|P$.

    (b) $\deg(\mathrm{Con}_{F'/F}(D)) = \dfrac{[F' : F]}{[K' : K]} \deg(D)$ for all $D \in \mathrm{Div}(F)$.

    (c) $N_{F'/F}(\mathrm{Con}_{F'/F}(D)) = [F' : F]\, D$ for all $D \in \mathrm{Div}(F)$.

23. $*$ (Finite places as prime ideals)

    Let F/K be a function field, and let $x \in F$ be transcendental over K, so $F/K(x)$ is finite algebraic. A place P' of F is *finite* if it lies above a finite place of $K(x)$ and *infinite* otherwise. Let $y \in F$ and suppose that y is integral over $K[x]$, i.e. the minimal polynomial of y has coefficients in $K[x]$.

    (a) Prove that $v_{P'}(y) > 0$ for all finite places P' of F.

    (b) Conclude that $\displaystyle\bigcap_{P' \in \mathbb{P}(F) \text{ finite}} O_{P'} \supseteq K[x, y]$.

    (c) Let $P' \in \mathbb{P}(F)$ be finite and set $\mathfrak{p} = P' \cap K[x, y]$. Prove that $\mathfrak{p}$ is a prime ideal of $K[x, y]$.

Quadratic Extensions

Throughout, let K be a perfect field.

24. (Characterization of hyperelliptic function fields)

    (a) Prove that every hyperelliptic function field F/K has a divisor $D \in \mathrm{Div}(F)$ with $\deg(D) = 2$ and $\ell(D) \geq 2$.
    Hint: let $x \in F$ with $[F : K(x)] = 2$ and put $D = \mathrm{div}(x)_0$.

    (b) Prove that if a function field F/K of genus $g \geq 2$ has a divisor $D \in \mathrm{Div}(F)$ with $\deg(D) = 2$ and $\ell(D) \geq 2$, then F/K is hyperelliptic.
    Hint: Let E be an effective divisor that is linearly equivalent to D (why does such a divisor exist?), and consider $x \in L(E) \setminus K$.

    (c) Prove that every genus 2 function field is hyperelliptic.
    Hint: consider a canonical divisor.

25. $***$ (Decomposition of places)

Let K have characteristic different from 2, and let $F = K(x, y)$ where $x \in F$ is transcendental over K and $y^2 = f(x)$ with $f(x) \in K[x] \setminus K$ square-free. In this problem, you will use Kummer's Theorem to establish a simple characterization of the decomposition of places of $K(x)$ in F.

(a) Let $p(x) \in K[x]$ be monic and irreducible, and denote by $P_{p(x)}$ the place of $K(x)$ with uniformizer $p(x)$.

i. Prove that $\phi_y(T) \in O_{P_{p(x)}}[T]$ and $\{1, y\}$ is a basis of $\overline{O}_{Pp(x)}$.

ii. Prove that if $p(x)$ divides $f(x)$, then $P_{p(x)}$ is totally ramified in F.

iii. Prove that if $f(x)$ is a non-zero square modulo $p(x)$, then $P_{p(x)}$ splits completely in F.

iv. Prove that if $f(x)$ is a not a square modulo $p(x)$, then $P_{p(x)}$ is inert in F.

(b) Let P_∞ denote the infinite place of $K(x)$. Put $k = \lceil \deg(f)/2 \rceil$, let s be the coefficient of x^{2k} in $f(x)$ (note that $s = 0$ when $\deg(f)$ is odd), and set $z = y/x^k$.

i. Prove that the minimal polynomial of z over $K(x)$ is $\phi_z(T) = T^2 - f(x)/x^{2k}$.

ii. Prove that $\phi_z(T) \in O_{P_\infty}[T]$ and $\{1, z\}$ is a basis of $\overline{O}_{P_\infty}$.

iii. Prove that if $\deg(f)$ is odd, then P_∞ is totally ramified in F.

iv. Prove that if $\deg(f)$ is even and s is a square in K^*, then P_∞ splits completely in F.

v. Prove that if $\deg(f)$ is even and s is not a square in K^*, then P_∞ is inert in F.

26. $**$ (Genus and different degree)

Let F/K have characteristic $\neq 2$, and let $x \in F$ with $[F : K(x)] = 2$. Write $F = K(x, y)$ where $y^2 = f(x)$ with $f(x) \in K[x] \setminus K$ square-free.

(a) Prove that F has genus $g = \lfloor (\deg(f) - 1)/2 \rfloor$.

(b) Conclude that $\deg(f) = 2g + 1$ or $2g + 2$, and hence $\deg(\mathrm{Diff}(F/K(x)) = 2g + 2$.

27. (An example of a non-rational genus 0 function field)

Let K be a field that does not contain a square root of -1, and let $F = K(x, y)$ where x and y are transcendental over K with $x^2 + y^2 = -1$.

(a) Prove that F is a quadratic extension of $K(x)]$. Conclude that F has genus 0.

(b) Prove that F/K is geometric (i.e. has full constant field K).

(c) Prove that every place of $K(x)$ is inert in F.

(d) Conclude that no place of F is rational, and hence F/K is not rational.

28. (An example of a non-elliptic genus 1 function field)

Let K be a field that does not contain a square root of -1, and let $F = K(x, y)$ where x and y are transcendental over K with $x^4 + y^2 = -1$.

(a) Prove that F is a quadratic extension of $K(x)]$. Conclude that F has genus 1.

(b) Prove that F/K is geometric (i.e. has full constant field K).

(c) Prove that every place of $K(x)$ is inert in F.

(d) Conclude that no place of F is rational, and hence F/K is not elliptic.

29. Set of rational places of an elliptic function field as a group)

Let F/K be an elliptic function field and Q a rational place of F. Prove that the injection $\Phi_Q : \mathbb{P}_1(F) \to \mathrm{Cl}^0(F)$ via $P \mapsto [P - Q]$ of Problem 15 is a bijection.

Hint: Let $[D] \in \mathrm{Cl}^0(F)$. Prove that $\ell(D + Q) = 1$. Conclude that the class $[D + Q]$ contains a prime divisor that gives rise to a rational place $P \in \mathbb{P}_1(F)$ with $\Phi_Q(P) = [D]$.

30. ** (Bijection between rational points and finite rational places)

Let K be a field of characteristic different from 2, and let $F = K(x, y)$ where $x \in F$ is transcendental over K and $C : y^2 = f(x)$ with $f(x) \in K[x]$ square-free.

(a) Let $(x_0, y_0) \in K \times K$ be a point on C. Let $P_{x-x_0} \in \mathbb{P}_1(K(x))$ be the place corresponding to $x - x_0$, and P' a place of F lying above P_{x-x_0}.

Suppose first that $y_0 = 0$.

i. Show that P_{x-x_0} ramifies as $2P'$ in F.

ii. Show that $v_{P'}(y) = 1$.

iii. Prove that $P' \in \mathbb{P}_1(F)$ is the unique place Q' of F with $v_{Q'}(x - x_0) > 0$ and $v_{Q'}(y - y_0) = v_{Q'}(y) > 0$.

Suppose now that $y_0 \neq 0$.

i. Show that P_{x-x_0} splits in F.

ii. Prove that there exists again a unique finite place $Q' \in \mathbb{P}_1(F)$ with $v_{Q'}(x - x_0) > 0$ and $v_{Q'}(y - y_0) > 0$, namely P' or the other place of F lying above P_{x-x_0}.

(b) Conversely, let P' be any rational finite place of F.

i. Show that $P' \cap K(x)$ is a finite rational place of $K(x)$, so $P' \cap K(x) = P_{x-x_0}$ for some $x_0 \in K$.

ii. If $f(x_0) = 0$, show that $(x_0, 0)$ is a point on C and $v_{P'}(y) = 1$.

iii. Suppose $f(x_0) \neq 0$. Prove that there is a unique $y_0 \in K^*$ such that $v_{P'}(y - y_0) > 0$.

iv. Let y_0 be as in part iii. Prove that (x_0, y_0) is a point on C.

(c) Prove that the above correspondence is a bijection between the points $(x_0, y_0) \in K \times K$ on C and the finite rational places of F.

31. *** (Semi-reduced divisors)

Let F/K be a function field, and let $x \in F$ be such that $[F : K(x)]$ is algebraic. A divisor of F is *finite* if all the places in its support are finite (see Exercise 23). A divisor of F is *semi-reduced* if is is finite, effective (see Exercise 12) and co-norm-free, i.e. it cannot be written as $\mathrm{Con}_{F/K(x)}(D) + E'$ where $D \in \mathrm{Div}(K(x))$ and $E' \in \mathrm{Div}(F)$. Assume that $[F : K(x)] = 2$.

(a) Let D' be a finite effective divisor of F. Prove that D' is semi-reduced if and only if for all finite places P' of F, the following hold:

- If $P' \cap K(x)$ is inert in F, then $v_{P'}(D') = 0$.

- If $P' \cap K(x)$ is ramified in F, then $v_{P'}(D') = 1$.
- If $P' \cap K(x)$ splits in F, say as $P' + Q'$, then $v_{P'}(D') = 0$ or $v_{Q'}(D') = 0$.

(b) Recall from Problem 11 that every finite place $P_{p(x)}$ of $K(x)$ is equivalent to $\deg(p)P_\infty$. Suppose the infinite place of $K(x)$ ramifies in F, i.e. $\mathrm{Con}_{F/K(x)}(P_\infty) = 2\infty$. Let P' be a placer of F. Use the fact that the co-norm map preserves principality of divisors to prove the following:

- If $P' \cap K(x)$ is inert in F, then $P' - 2\infty$ is principal.
- If $P' \cap K(x)$ is ramified in F, then $2P' - 2\infty$ is principal.
- If $P' \cap K(x)$ splits in F, say as $P' + Q'$, then $P' + \infty$ is equivalent to $-(Q' + \infty)$.

(c) Assume again that the infinite place of $K(x)$ ramifies in F. Prove that every degree divisor $D' \in \mathrm{Div}^0(F)$ is equivalent to a degree zero divisor of F of the form $D'_0 - \deg(D'_0)\infty$ where D_0 is semi-reduced.

Models of Quadratic Extensions

Throughout, let K be a perfect field.

32. $**$ (Weierstrass models of elliptic curves)

If F/K be an elliptic function field and P a rational place of F.

(a) Prove that $\ell(nP) = n$, and conclude that $L(P) = K$ and $L(nP) \subsetneq L((n+1)P)$, for all $n \geq 0$.

(b) Let $s \in L(2P) \setminus K$ and $t \in L(3P) \setminus L(2P)$. Prove that $1, s, t, s^2, st, s^3$ have pole divisors $0, 2P, 3P, 4P, 5P, 6P$, respectively.

(c) Prove that $1, s, t, s^2, st, s^3$ form a basis of $L(6P)$.

(d) Prove that $t^2 \in L(6P)$. Conclude that there exist $c_0, c_1, c_2, c_3, c_4, c_6 \in K$, with $c_0 \neq 0$, such that $t^2 + c_1 st + c_3 t = c_0 s^3 + c_2 s^2 + c_4 s + c_6$.

(e) Put $x = c_0 s$ and $y = c_0 t$. Conclude that there exist $a_1, a_2, a_3, a_4, a_6 \in K$ such that

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \ .$$

(f) Prove that $[F : K(x)] = 2$ and $[F : K(y)] = 3$. Conclude that $y \notin K(x)$ and hence $F = K(x, y)$.

33. $***$ (Defining curves in characteristic $\neq 2$)

Let K have characteristic different from 2, F/K a function field, and $x \in F$ such that $[F : K(x)] = 2$.

(a) Prove that there exists a square-free polynomial $f(x) \in K[x]$ such that $F = K(x, y)$ with $y^2 = f(x)$.

(b) Prove that $F/K(x)$ is geometric if and only if the polynomial $f(x)$ of part (a) is non-constant.

(c) If $f(x)$ is constant, what is $\tilde{K}$?

34. ** (From ramified to split models and vice versa)

Let F/K be a function field of characteristic $\neq 2$. and let $x \in F$ with $[F : K(x)] = 2$. Write $F = K(x, y)$ where $y^2 = f(x)$ with $f(x) \in [x]$ square-free and non-constant.

(a) Suppose first that $\deg(f) = 2g + 1$ is odd, so the infinite place of $K(x)$ ramifies in F.

i. Show that there exist a *monic* square-free non-constant polynomial $h(x) \in K[x]$ of degree $2g + 1$ such that $F = K(x, z)$ with $z^2 = h(x)$.

ii. Let $a \in K$ with $f(a) \neq 0$ and put $t = (x - a)^{-1}$ and $w = z(x - a)^{-(g+1)}$. Prove that $F = (t, w)$ where $w^2 = m(t)$ with $m(t) \in K[t]$ square-free,non-constant and of degree $2g + 2$, and the infinite place of $F/K(w)$ splits in F.

(b) Suppose first that $\deg(f) = 2g + 2$ is even, so the infinite place of $K(x)$ is unramified in F. Suppose there exists $a \in K$ with $f(a) = 0$ (note that this is a much stronger assumption than that of part (a) (ii)).

i. Show that $f'(a) \neq 0$ where $f'(x)$ is the formal derivative with respect to x.

ii. Put $t = (x - a)^{-1}$ and $w = z(x - a)^{-(g+1)}$. Prove that $F = (t, w)$ where $w^2 = m(t)$ with $m(t) \in K[t]$ square-free, non-constant and of degree $2g+1$ (so the infinite place of $F/K(w)$ is ramified in F).

35. * (Inert models become split over quadratic constant field extensions)

Let F/K be a function field of characteristic $\neq 2$, and let $x \in F$ with $[F : K(x)] = 2$. Write $F = K(x, y)$ where $y^2 = f(x)$ with $f(x) \in [x]$ square-free and non-constant. Assume that the infinite place of $K(x)$ is inert in F, so $\deg(f)$ is even and the leading coefficient $\operatorname{sgn}(f)$of $f(x)$ is a non-square in K^*.

Let $a \notin K$ be a square root of $\operatorname{sgn}(f)$ in some algebraic closure of K. Put $L = K(a)$ and $E = FL = F(a)$. Prove that $[E : L(x) = 2]$, $E = L(x, y)$, and the infinite place of $L(x)$ splits in E.

Divisor Arithmetic in Quadratic Extensions

Throughout, let K be a perfect field.

36. *** (Mumford representation)

Let K be a field of characteristic $\neq 2$, and let $F = K(x, y)$ where $x \in F$ is transcendental over K and $y^2 = f(x)$ with $f(x) \in K[x] \setminus K^2$ square-free.

(a) Let $D' = \sum_{i=1}^{r} n_i P_i'$ be a semi-reduced divisor of F. For each P_i', let $P_{p_i(x)}$ denote the place of $K(x)$ lying below P_i', and set $u(x) = p_1(x)^{n_1} p_2(x)^{n_2} \cdots p_r(x)^{n_r} \in K[x]$.

i. Let $i \in \{1, 2, \ldots, r\}$. Prove that there exists a unique polynomial $v_i(x) \in K[x]$ such that $v_{P_i'}(v_i + y) > 0$.
Hint: by Exercise 25, $f(x)$ is a square (possibly zero) modulo $p_i(x)$. Now pick a suitable square root.

ii. Prove that there exists a polynomial $v(x) \in K[x]$, unique modulo $u(x)$, such that $u(x)$ divides $f(x) - v(x)^2$ and $v_{P_i'}(v_i(x) + y) > 0$ for $1 \leq i \leq r$.

The pair $(u(x), v(x) \pmod{u(x)})$ us called the *Mumford representation* of D'.

(b) Conversely, let $u(x), v(x) \in \mathbb{F}_q[x]$ with $u(x)$ monic, non-zero, and dividing $f(x) - v(x)^2$. Let $u(x) = p_1(x)^{n_1} p_2(x)^{n_2} \cdots p_r(x)^{n_r}$ be the factorization of $u(x)$ into monic irreducible polynomials in $\mathbb{F}_q[x]$, and let $P_{p_i(x)}$ be the place of $K(x)$ corresponding to $p_i(x)$.

i. Prove that no $p_i(x)$ is inert.

ii. Prove that for every i, there is a unique place $P_i' \in \mathbb{P}(F)$ lying above $P_{p_i(x)}$ such that $v_{P_i'}(v + y) > 0$.

iii. Put $D' = \sum_{i=1}^{r} n_i P_i'$ where the P_i' are the unique places determined in part (b) ii. Prove that D' is a semi-reduced divisor of F with Mumford representation $(u(x), v(x))$.

37. $***$ (Semi-reduced divisors and $K[x, y]$-ideals)

Let K be a field of characteristic different from 2, and let $F = K(x, y)$ where $x \in F$ is transcendental over K and $y^2 = f(x)$ with $f(x) \in K[x]$ square-free. Let $u(x), v(x) \in K[x]$ with $u(x)$ monic, and consider the $K[x]$-module $M \subseteq K[x, y]$ of rank 2 generated by $u(x)$ and $v(x) + y$.

(a) Prove that M is an ideal in $K[x, y]$ if and only if $u(x)$ divides $v(x)^2 - f(x)$.
Hint: Convince yourself that M is an ideal if and only if $(v(x) + y)y \in M$.

(b) Prove that the $K[x, y]$-ideals M of the form described above are in one-to-one correspondence with the semi-reduced divisors of F.[1]

38. $***$ (Divisor addition)

Let K be a field of characteristic different from 2, and let $F = K(x, y)$ where $x \in F$ is transcendental over K and $y^2 = f(x)$ with $f(x) \in K[x]$ square-free.

(a) Let $D_1 = (u_1, v_1$ and $D_2 = (u_2, v_2)$ be two semi-reduced divisors of F in Mumford representation. Prove that $D_1 + D_2$ is semi-reduced if and only if $\gcd(u_1, u_2, v_1 + v_2) = 1$.

(b) Under the assumption of part (a), prove that the Mumford representation of $D_1 + D_2$ is (u, v) where

$$u = u_1 u_2 \quad \text{and} \quad v \equiv \begin{cases} v_1 \pmod{u_1} \\ v_2 \pmod{u_2} \end{cases}.$$

39. $***$ (Divisor reduction)

Let K be a field of characteristic different from 2, and let $F = K(x, y)$ have where $x \in F$ is transcendental over K and $y^2 = f(x)$ with $f(x) \in K[x]$ square-free. Let g be the genus of F.

Let $D = (u, v)$ be a semi-reduced divisor in Mumford representation. Put

$$u' = \frac{f + hv - v^2}{u}, \qquad v \equiv h - v \pmod{u'}.$$

(a) Prove that $D' = (u', v')$ is a semi-reduced divisor in Mumford representation. Prove the following:

[1] In fact, this bijection extends to a group isomorphism from the ideal class group of $K[x, y]$ onto the degree zero class group of F. More generally, these two groups are isomorphic for any function field F/K for which there exists $x \in F$ transcendental over K such that $F = K(x, y)$ and the infinite place of $K(x)$ is totally ramified in F.

(b) D' is equivalent to D.

(c) If $\deg(u) \geq g+2$, then $deg(u') \leq \deg(u) - 2$.

(d) If $\deg(u) = g+1$, then $\deg(D) \leq g$.

(e) Starting with $D = (u, v)$, the above substitution $(u, v) \to (u', v')$ applied at most $\lceil \deg(u) - g/2 \rceil$ times yields the unique reduced divisor equivalent to D.

Miscellaneous

40. (2-torsion of the class group over an algebraically closed field)

This problem is tangential to the material in the lectures.

Let F be a function field over an an algebraically closed field K, and let $x \in F$ such that $[F : K(x)] = 2$. Write $F = K(x, y)$ where $y^2 = f(x)$ with $f(x) \in \mathbb{F}_q[x]$ square-free and of odd degree, so $f(x)$ splits into an odd number of distinct linear factors. Recall that the ramified places of $K(x)$ are the infinite place P_∞ and the places P_i, $1 \leq i \leq \deg(f)$, that correspond to the linear factors of $f(x)$. Write $\mathrm{Con}_{F/K(x)}(P_\infty) = 2P'_\infty$, $\mathrm{Con}_{F/K(x)}(P_i) = 2P'_i$, and put $D'_i = P'_i - P'_\infty$ for $1 \leq i \leq \deg(f)$. For $D' \in \mathrm{Div}^0(F)$, let $[D']$ denote the class of D' in $\mathrm{Cl}^0(F)$.

(a) Show that $[D'_i] \neq 0$ and $2[D'_i] = [0]$ for $1 \leq i \leq \deg(f)$.

(b) Show that $[D'_1] + [D'_2] + \cdots + [D'_{\deg(f)}] = [0]$.

(c) Let G be the subgroup of $\mathrm{Div}^0(F)$ generated by $[D'_1]$, $[D'_2]$, $\ldots$, $[D'_{\deg(f)}]$. Prove that G is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{\deg(f)-1}$.

(d) Let $\mathrm{Cl}^0(F)[2]$ denote the 2-torsion of $\mathrm{Cl}^0(F)$, i.e. the collection of divisor classes of order dividing 2. Prove that $\mathrm{Cl}^0(F)[2] = G$, so the number of 2-torsion elements of $\mathrm{Cl}^0(F)$ is $2^{\deg(f)-1}$.