E. Dummit's Math 7362 ~ Number Theory in Function Fields, Fall 2025 ~ Homework 2, due Wed Nov 5th

Solve whichever problems you haven't seen before that interest you the most (suggestion: between 30 and 50 points' worth). Starred problems are especially recommended. Prepare to present 2-4 problems in class on the due date.

0.1 In-Lecture Exercises

0.1.1 Exercises from (Oct 6)

- 1. [2pts] If R is a Noetherian integrally-closed domain and P is a minimal nonzero prime ideal of R, show that R_P is a DVR. Deduce in particular that if R is a Dedekind domain and P is a nonzero prime ideal, then R_P is a DVR.
- 2. [6pts*] Let R be a discrete valuation ring with field of fractions F and valuation v. Also $t \in R$ be a uniformizer (an element with v(t) = 1). Prove:
 - (a) For any $r \in F^{\times}$, either r or 1/r is in R.
 - (b) An element $u \in R$ is a unit of R if and only if v(u) = 0. In particular, if $\zeta \in F$ is any root of unity, then $v(\zeta) = 0$.
 - (c) If $x \in R$ is nonzero and v(x) = n, then x can be written uniquely in the form $x = ut^n$ for some unit $u \in R$.
 - (d) Every nonzero ideal of R is of the form (t^n) for some $n \geq 0$.
 - (e) The ring R is a Euclidean domain (hence also a PID and a UFD) and also a local ring.
 - (f) The ring S is a DVR if and only if it is a PID and a local ring but not a field.
- 3. [2pts] If v is a discrete valuation on \mathbb{Q} , show that the set $P = \{n \in \mathbb{Z} : v(n) > 0\}$ is a prime ideal of \mathbb{Z} .
- 4. [3pts] Prove that the p-adic valuations v_p along with v_{∞} are the only discrete valuations on F(t)/F. (Use a similar argument to the one for \mathbb{Q} by identifying all possible uniformizers.)

0.1.2 Exercises from (Oct 15)

- 1. [2pts] For K = F(t), if $a = u \frac{p_1^{a_1} \cdots p_k^{a_k}}{q_1^{b_1} \cdots q_l^{b_l}}$ for $u \in F^{\times}$ and distinct monic irreducibles $p_1, \ldots, p_k, q_1, \ldots, q_l$ having associated primes $P_1, \ldots, P_k, Q_1, \ldots, Q_l$, show that $\operatorname{div}(a) = a_1 P_1 + \cdots + a_k P_k b_1 Q_1 \cdots b_l Q_l + [\sum_i b_i \operatorname{deg}(q_i) \sum_i a_i \operatorname{deg}(p_i)] \infty$.
- 2. [3pts] For any field F, if $f(t), g(t) \in F[t]$ are relatively prime, show that $[F(t): F(\frac{f(t)}{g(t)})] = \max(\deg f, \deg g)$. [Hint: Use Gauss's lemma to show that $q(y) = f(y) \frac{f(t)}{g(t)}g(y) \in F(\frac{f(t)}{g(t)})[y]$ is the minimal polynomial of t over $F(\frac{f(t)}{g(t)})$.]
- 3. [1pt] Verify that the relation $D_1 \sim D_2$ when $D_1 D_2$ is principal is an equivalence relation on divisors and that the equivalence classes are the elements in the quotient group of divisors modulo principal divisors.
- 4. [1pt] Check that the relation $D_1 \leq D_2$ when $D_2 D_1 = \sum_P n_P P$ where all $n_P \geq 0$ is a partial ordering on divisors.
- 5. [2pts] Determine the Riemann-Roch space L(D) when K = F(t) for $D = P_t P_\infty$, $P_t + P_\infty$, and $P_t + P_{t-1}$.
- 6. [1pt] Write down an interesting divisor of positive degree for K = F(t) and then compute a basis for the Riemann-Roch space L(D).

0.1.3 Exercises from (Oct 20)

- 1. [1pt] Show that when K = F(x), the canonical class contains every divisor of K of degree -2.
- 2. [2pts] If R is the valuation ring of P and σ is an endomorphism of K, show that σR is also a valuation ring with maximal ideal σP , and that σ gives an isomorphism of R/P with $\sigma R/\sigma P$. Show also that for any $a \in K$, $v_{\sigma P}(a) = v_P(\sigma^{-1}a)$.
- 3. [1pt] Show that the number of primes of degree $\leq n$ in K is at most $[K:F(x)]q^n$ for any $x \in K \setminus F$.
- 4. [1pt] Give an explicit upper bound in terms of [K:F(x)], q, and n for the number of effective divisors of degree n in K.

0.1.4 Exercises from (Oct 22)

- 1. [1pt] Suppose X is a compact Riemann surface. For any nonzero meromorphic f on X, show that $\deg(\operatorname{div}(f)) = 0$. [Hint: Use Cauchy's argument principle: for any contour C, $\frac{1}{2\pi i} \int_C \frac{f'}{f} dz = Z P$ is the number of zeroes minus the number of poles in C.]
- 2. [1pt] Explain why saying that the dimension of the space of holomorphic differentials on X has dimension g is equivalent to saying $\ell(C) = g$.

0.1.5 Exercises from (Oct 27)

- 1. [2pts] Let P be a prime of the function field K with valuation ring R and residue field E = R/P. Show that the power series expansion method yields a one-to-one ring homomorphism of the metric space R (under the metric induced by the discrete valuation v_P) into the formal power series ring E[[t]] (under the metric induced by the order valuation v_t , giving the lowest-degree term with a nonzero coefficient).
- 2. [3pts*] Suppose $D: K \to M$ is a derivation of K/F into M. Show the following:
 - (a) D(c) = 0 for all $c \in F$.
 - (b) (Quotient Rule) $D(a/b) = [bD(a) aD(b)]/b^2$ for all $a \in K, b \in K^{\times}$.
 - (c) (Chain Rule 1) For any $f(x) \in F[x]$ and any $a \in K$, we have D(f(a)) = f'(a)D(a) where f' is the usual formal derivative of f.
- 3. [2pts] Suppose K/F is a function field with $x \in K \setminus F$ and where K/F(x) is separable. If D_1 and D_2 are derivations from K/F to M and $D_1(x) = D_2(x)$, show that $D_1(a) = D_2(a)$ for all $a \in K$. [Hint: First show D_1 and D_2 agree on F(x). Then for any $y \in K$, apply D_1 and D_2 to its minimal polynomial m(y) = 0 over F(x); separability ensures that m'(y) is not the zero polynomial.]
- 4. [2pts] For a function field K/F, let Der_K denote the space of derivations $D:K\to K$.
 - (a) Show that Der_K is a K-vector space under pointwise addition and scalar multiplication.
 - (b) Show that for any derivation $D \in \operatorname{Der}_K$ and any $a \in K^{\times}$ we have $D = D(x) \cdot D_x$. Deduce that Der_K is 1-dimensional (as a K-vector space).
- 5. [2pts] If x and y are separating elements of a function field K/F, show the chain rule: that $D_x = D_x(y) \cdot D_y$ as functions on K. Deduce that the relation $(a, x) \sim (b, y)$ when $b = a \cdot D_y(x)$ is in fact an equivalence relation.
- 6. [1pt] Show that the map $d: K \to \text{Diff}_K$ via d(a) = 1 da when a is a separating element and d(a) = 0 when a is non-separating is a derivation of K/F.
- 7. [2pts] If K/F is a function field and F is algebraically closed, show that all nonzero differentials lie in the same divisor class.

0.1.6 Exercises from (Oct 29)

- 1. [2pts] Show using the divisor-counting results from earlier that the zeta function $\zeta_K(s) = \sum_{A\geq 0} q^{-s \deg A}$ converges absolutely for Re(s) > 1. (We will later improve those estimates, but the weak ones in the earlier exercises are good enough here.)
- 2. [2pts*] Show that $\zeta_{\mathbb{F}_q(t)}(s) = (1 q^{-s})^{-1} \zeta_{\mathbb{F}_q[t]}(s) = \frac{1}{(1 q^{1-s})(1 q^{-s})}$.
- 3. [3pts*] Using the explicit formula $\zeta_{\mathbb{F}_q(t)}(s) = \frac{1}{(1-q^{-s})(1-q^{1-s})}$, verify the Weil conjectures for $K = \mathbb{F}_q(t)$.

0.2 Additional Exercises

- 1. [6pts] Suppose K/F is a function field and suppose R is a proper subring of K containing F with the property that $a \in R$ or $a^{-1} \in R$ for all $a \in K^{\times}$.
 - (a) Show that R is a local ring and that the maximal ideal P of R consists of the elements $a \in K$ such that $a^{-1} \notin R$.
 - (b) Suppose $x_1 \in P$ is nonzero and x_2, \ldots, x_n have $x_i \in x_{i+1}P$ for $1 \le i \le n-1$. Show that $n \le [K: F(x_1)]$. [Hint: Adapt the proof that R/P is a finite-dimensional F-vector space to show that x_1, \ldots, x_n are linearly independent over $F(x_1)$.]
 - (c) Show that P is principal. [Hint: If not, pick a nonzero $x_1 \in P$ and $x_2 \in P \setminus (x_1)$ and show $x_1/x_2 \in P$ so $x_1 \in x_2P$. If x_2 does not generate P, repeat until a generator is obtained.]
 - (d) Letting P = (t), show that every nonzero $x \in R$ can be written in the form $x = ut^n$ for a unique unit $u \in R$ and unique nonnegative integer n. Deduce that the function $v : R \to \mathbb{Z}$ with v(x) = n (and $v(0) = \infty$) is a discrete valuation on R, and conclude that R is a valuation ring of K.

Remark: Since all valuation rings of K have the property that $a \in R$ or $a^{-1} \in R$ for all $a \in K^{\times}$, this gives a way to identify valuation rings of function fields without explicitly needing to reference the valuation.

- 2. [5pts] Our discussion of primes of a function field K/F is predicated on the assumption that there are actually DVRs inside K. The goal of this problem is to show this is indeed the case by establishing the following result: if S is a subring of K containing F and I is a nonzero proper ideal of S, then there is a prime P of K with valuation ring R such that $I \subseteq P$ and $S \subseteq R$.
 - (a) Let \mathcal{F} be the set of subrings T of K containing R such that $IT \neq T$. Show that \mathcal{F} contains a maximal element.
 - (b) Suppose that \mathcal{O} is a maximal element under the conditions of (1). Show that for any element $x \in K$, either $x \in \mathcal{O}$ or $x^{-1} \in \mathcal{O}$; deduce that \mathcal{O} is a valuation ring of K. [Hint: If not, then $I\mathcal{O}[x] = \mathcal{O}[x]$ and $I\mathcal{O}[x^{-1}] = \mathcal{O}[x^{-1}]$. Pick m, n minimal with $1 = a_0 + a_1x + \cdots + a_nx^n$ and $1 = b_0 + b_1x^{-1} + \cdots + b_mx^{-m}$ with $a_i, b_i \in I\mathcal{O}$. Use these relations to eliminate a power and obtain a contradiction.]
 - (c) Show that for any $a \in K \setminus F$, a has at least one zero and one pole. [Hint: Take the ring F[a] and the ideal I = aF[a] to get a zero.]
 - (d) Conclude that K/F has at least two primes P. (In fact, every function field has infinitely many primes, though this is a bit harder to extract.)
- 3. [4pts*] The goal of this problem is to prove a result known as the Weierstrass gap theorem. Let P be a prime of K and suppose that the genus of K is g. The main task is to investigate the spaces L(nP) for various n: we say that an integer n is a <u>pole number</u> for P if there exists $a \in K$ such that $\operatorname{div}_{-}(a) = -nP$, and otherwise (if there is no such a) we say n is a gap number for P.
 - (a) Show that the set of pole numbers for P is an additive semigroup (i.e., it is closed under addition and contains 0).
 - (b) Show that if $n \ge 2g$, then L((n-1)P) < L(nP). Deduce that there exists an element $a \in K$ such that $\operatorname{div}_{-}(a) = -nP$ and conclude that each $n \ge 2g$ is a pole number.
 - (c) Show that there are exactly g gap numbers $i_1 < i_2 < \cdots < i_g$ for P, and that $i_1 = 1$ and $i_g \le 2g 1$.