E. Dummit's Math 7315 ∼ Number Theory in Function Fields, Fall 2021 ∼ Homework 2

Problems are worth points as indicated. Solve as many problems as you can (suggestion: at least 30 points' worth). Prepare solutions to these problems so that you may present some of them in lecture on Monday, November 8th. Starred exercises are especially recommended.

0.1 In-Lecture Exercises

0.1.1 Exercises from (Sep 27)

- [2pts] Extend the example from class to describe all monic irreducibles $p \in \mathbb{F}_q[t]$ such that t is a square modulo p for arbitrary finite fields $\mathbb{F}_q$.

0.1.2 Exercises from (Sep 30)

- [1pt] Show that if a is not relatively prime to m, then there are only finitely many primes congruent to a modulo m.
- *[2pt] If S is finite, show that its Dirichlet density is 0.
- [4pts] Show that the set of primes whose leading digit is 1 in base 10 has undefined natural density, but has Dirichlet density $\log_{10} 2$. (The answer works out the same if you use integers with leading digit 1 relative to all integers; this may be a bit easier to work out.)
- [2pts] Show that extended Dirichlet characters modulo m are the same as functions $\chi : \mathbb{Z} \to \mathbb{C}$ (or $A \to \mathbb{C}$) such that (i) $\chi(a+bm) = \chi(a)$ for all a, b, (ii) $\chi(ab) = \chi(a)\chi(b)$ for all a, b, and (iii) $\chi(a) \neq 0$ iff a is relatively prime to m.
- [3pts] If G is a finite abelian group and H is a subgroup, define $H^\perp = \{\chi \in \hat{G} : \chi(H) = 1\}$. Show that $H^\perp \cong \widehat{G/H}$ and that $\hat{G}/H^\perp \cong \hat{H}$. Use these results along with $\hat{G} \cong G$ to conclude that the subgroup lattice of G is the same when turned upside down.
- *[2pts] If G is a finite abelian group, verify that the evaluation map $\varphi : G \to \hat{\hat{G}}$ with $\varphi(g) = \{\chi \mapsto \chi(g)\}$ is an isomorphism from $\hat{\hat{G}}$ to G.
- [3pts] Prove Plancherel's theorem $\langle f_1, f_2 \rangle_G = \dfrac{1}{|G|}\left\langle \hat{f}_1, \hat{f}_2 \right\rangle_{\hat{G}}$ and deduce Parseval's theorem $\sum_{g \in G} |f(g)|^2 = \dfrac{1}{|G|} \sum_{\chi \in \hat{G}} \left|\hat{f}(\chi)\right|^2$.

0.1.3 Exercises from (Oct 14)

- [2pts] Prove that the set $\{x+y, x^2+y^2\}$ is algebraically independent over $\mathbb{R}$ (where x, y are indeterminates).
- [4pts] Show that localization commutes with sums, intersections, quotients, finite direct sums, and is exact. (These are standard facts you can look up in Dummit/Foote and Atiyah/Macdonald.)
- [2pts] Show that the field $F(x, \sqrt{x^2+x})$ is a purely transcendental extension of F. [Hint: Let $t = \sqrt{x^2+x}/x$ and write x and $y = \sqrt{x^2+x}$ in terms of t by using the relation $y^2 = x^2 + x$.]
- [2pts] Show that if I is an ideal of R, then $D = R\backslash I$ is multiplicatively closed if and only if I is prime.
- *[2pts] Show that if P is a prime ideal and $D = R\backslash P$, then $D^{-1}R$ is a local ring with unique maximal ideal $D^{-1}P = \pi(P) = e_P$, the extension of the ideal P to $D^{-1}R$.

0.1.4 Exercises from (Oct 18)

- [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. (This is corollary 8 from Section 16.2 of Dummit/Foote.)
- *[10pts] Let R be a discrete valuation ring with field of fractions F and valuation v. Also $t \in R$ be a uniformizer; i.e., an element with $v(t) = 1$. Show the following:
  1. For any $r \in F^\times$, either r or $1/r$ is in R.
  2. 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 $v(\zeta) = 0$.
  3. 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 $u \in R$.
  4. Every nonzero ideal of R is of the form (t^n) for some $n \geq 0$.
  5. The ring R is a Euclidean domain (hence also a PID and a UFD) and also a local ring.
  6. The ring S is a DVR if and only if it is a PID and a local ring but not a field.
- [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 $\mathbb{Z}$.
- [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.)
- [2pts] For $K = F(t)$, if $a = u\dfrac{p_1^{a_1} \cdots p_k^{a_k}}{q_1^{b_1} \cdots q_l^{b_l}}$ 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 $\mathrm{div}(a) = a_1P_1 + \cdots + a_kP_k - b_1Q_1 - \cdots - b_lQ_l + [\sum_j b_j \deg(q_j) - \sum_i a_i \deg(p_i)]\infty$.
- [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 $F(\frac{f(t)}{g(t)})$.]

0.1.5 Exercises from (Oct 21)

- [2pts] Verify that the relation $D_1 \sim D_2$ if $D_1 - D_2$ is principal is an equivalence relation, and that the equivalence classes are the elements in the quotient group of divisors modulo principal divisors.
- [1pt] Check that the relation $D_1 \leq D_2$ is a partial ordering on divisors.
- *[2pts] Determine $L(D)$ when $K = F(t)$ for $D = P_t - P_\infty$, $P_t + P_\infty$, and $P_t + P_{t-1}$.
- [2pts] Show that when $K = F(x)$, the canonical class contains every divisor of K of degree -2.

0.1.6 Exercises from (Oct 25)

- [2pts] For any nonzero meromorphic f on X, show that $\deg(\mathrm{div}(f)) = 0$. [Hint: Use Cauchy's argument principle: for any contour C, $\dfrac{1}{2\pi i}\int_C \dfrac{f'}{f}\,dz = Z - P$ is the number of zeroes minus the number of poles in C.]
- [2pts] Explain why saying that the dimension of the space of holomorphic differentials on X has dimension g is equivalent to saying $\ell(C) = g$.
- [3pts] If R is the valuation ring of P, 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 $a \in K$, $v_{\sigma P}(a) = v_P(\sigma^{-1}a)$.
- [2pts] Show that the number of primes of degree $\leq n$ in K is at most $[K : F(x)]q^n$ for any $x \in K \backslash F$.
- [2pts] 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.
- [1pt] If $A, B \geq 0$, show that $N(A + B) = NA \cdot NB$.

0.1.7 Exercises from (Oct 28)

- [2pts] Show that $\zeta_{\mathbb{F}_q(t)}(s) = (1-q^{-s})^{-1}\zeta_{\mathbb{F}_q[t]}(s) = \dfrac{1}{(1-q^{1-s})(1-q^{-s})}$.
- *[3pts] Using the explicit formula $\zeta_{\mathbb{F}_q(t)}(s) = \dfrac{1}{(1-q^{-s})(1-q^{1-s})}$, verify the Weil conjectures for $K = \mathbb{F}_q(t)$.
- [2pts] Show that if $q \geq 4g^2$, then there must exist primes of degree 1 in K.
- [2pts] Show that if $q > 4$ and $g > 0$, then the class number of K is greater than 1.

0.2 Additional Exercises

- [15pts] 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 $S \subseteq R$.

  1. 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.
  2. 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 $x^{-1} \in \mathcal{O}$. [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.]
  3. Suppose that Σ is a subring of K containing F, with $\Sigma \neq F, K$, and such that every element $a \in K$ has $a \in \Sigma$ or $a^{-1} \in \Sigma$. Show that Σ is a valuation ring of K. [Hint: Show that Σ is a local ring and that its maximal ideal is principal, and use this to write down the discrete valuation.]
  4. Show that for any $a \in K\backslash F$, a has at least one zero and one pole. [Hint: Take the ring $F[z]$ and the ideal $I = zF[z]$ to get a zero.]
  5. 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.)

- [10pts] 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 $\text{div}_-(a) = -nP$, and otherwise (if there is no such a) we say n is a <u>gap number</u> for P.

  1. Show that the set of pole numbers for P is an additive semigroup (i.e., it is closed under addition and contains 0).
  2. Show that if $n \geq 2g$, then $L((n-1)P) < L(nP)$. Deduce that there exists an element $a \in K$ such that $\text{div}_-(a) = -nP$ and conclude that each $n \geq 2g$ is a pole number.
  3. Show that there are exactly g gap numbers $i_1 < i_2 < \cdots < i_g$ for P, and that $i_1 = 1$ and $i_g \leq 2g - 1$.