E. Dummit's Math 7362 ~ Number Theory in Function Fields, Fall 2025 ~ Homework 3, due Wed Dec 3rd

Solve whichever problems you haven't seen before that interest you the most (suggestion: between 25 and 40 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 (Nov 3)

1. [1pt] Draw $V(x)$, $V(x^2)$, $V(y-x)$, $V(y-x^2)$, $V(xy)$, $V(x,y)$, and $V(y^2-x^3)$ in $\mathbb{A}^2(\mathbb{R})$.
2. [2pts] Identify $I(S)$ in $\mathbb{R}[x,y]$ for $S = \{(t,0) : t \in \mathbb{R}\}$, $\{(t^2,t) : t \in \mathbb{R}\}$, $\{(1,1)\}$, $\{(0,0),(1,1)\}$, $\{(\cos t, \sin t) : t \in \mathbb{R}\}$, and $\{(t, \sin t) : t \in \mathbb{R}\}$.
3. [1pt] If k is finite, show that the irreducible affine algebraic sets in $\mathbb{A}^n(k)$ are $\emptyset$ and single points.
4. [2pts*] If k is infinite, show that the irreducible affine algebraic sets in $\mathbb{A}^2(k)$ are $\emptyset$, $\mathbb{A}^2(k)$, single points, and curves of the form $V(f)$ for a monic irreducible polynomial $f \in k[x,y]$. [Hint: Show that if $f, g \in k[x,y]$ are relatively prime, then (f,g) contains a nonzero polynomial in $k[x]$ and a nonzero polynomial in $k[y]$.]
5. [2pts] Prove Zariski's lemma: a field L that is finitely generated over k as a ring is finitely generated over k as a module. [Hint: Induct on the number of generators.]
6. [1pt] Suppose k is algebraically closed. Show that $\Gamma(V) = \cap_{P \in V} \mathcal{O}_P(V)$: in other words, that a function with no poles is a polynomial.

0.1.2 Exercises from (Nov 10)

1. [2pts] Suppose k is an infinite field, $P \in \mathbb{A}^{n+1} \backslash \{0\}$, and $f \in k[x_0, \dots, x_n]$. If we write $f = f_0 + f_1 + \cdots + f_d$ for homogeneous polynomials f_i of degree i, show that $f(\lambda P) = 0$ for all $\lambda \in k^\times$ if and only if $f_i(P) = 0$ for all i. [Hint: Use linear algebra and the fact that Vandermonde determinants are nonvanishing.]
2. [2pts] Identify $V(x_0)$, $V(x_0^2)$, $V(x_1 - x_0)$, $V(x_1 - x_0^2)$, $V(x_1^2 - x_0^2)$, $V(x_0, x_1)$, $V(x_0, x_1, x_2)$, and $V(x_0 x_1 - x_2^2)$ in $\mathbb{P}^2(k)$.
3. [3pts] Show that all of the basic properties of the affine operators I and V also hold for the projective I and V (suitably modified).
4. [2pts] Show that an ideal I of $k[x_0, \dots, x_n]$ is homogeneous if and only if I is generated by finitely many homogeneous polynomials.
5. [2pts] When V is a nonempty projective algebraic variety with affine cone $C(V) = \{(x_0, x_1, \dots, x_n) : [x_0 : x_1 : \cdots : x_n] \in V\} \cup \{(0,0,\dots,0)\}$, show that $I_{\text{affine}}(C(V)) = I_{\text{projective}}(V)$, and when I is a homogeneous ideal with $V_{\text{projective}}(I) \neq \emptyset$, show that $C(V_{\text{projective}}(I)) = V_{\text{affine}}(I)$.
6. [1pt] Show that $(FG)_* = F_* G_*$, $(fg)^* = f^* g^*$, $(f^*)_* = f$, $(F_*)^* = F / x_0^{v_{x_0}(f)}$, $(F+G)_* = F_* + G_*$, and $x_0^{\deg(f)+\deg(g)-\deg(f+g)}(f+g)^* = x_0^{\deg(g)} f^* + x_0^{\deg(f)} g^*$.

0.1.3 Exercises from (Nov 12)

1. [1pt] Show that if $f \in k[X_1, \dots, X_n]$ is homogeneous of degree d, then $X_1 f_{X_1} + \cdots + X_n f_{X_n} = df$. (This is a famous result of Euler.) Deduce that for a homogenous $f \in k[X,Y,Z]$, if two of f_X, f_Y, f_Z are zero then the third is as well.

0.1.4 Exercises from (Nov 17)

1. [2pts] Suppose S is an integral extension of the commutative ring R with 1.
   (a) Show that R is a field if and only if S is a field.
   (b) If P is a prime ideal of R, show that there exists a prime ideal Q of S with $P = Q \cap R$, and that P is maximal if and only if Q is maximal.

2. [3pts] Let L/K be an extension of function fields. Suppose that $\tilde{P}$ is a prime of L with associated valuation ring $\mathcal{O}_{\tilde{P}}$ in L and P is a prime of K with associated valuation ring $\mathcal{O}_P$ in K. Show that the following are equivalent:
   (a) $P \subseteq \tilde{P}$.
   (b) $\mathcal{O}_P \subseteq \mathcal{O}_{\tilde{P}}$.
   (c) There exists an integer $e \geq 1$ such that $v_{\tilde{P}}(a) = e \cdot v_P(a)$ for all $a \in K$.

3. [2pts] Show that the relative degree and ramification index compose in towers; explicitly, that if $\tilde{\tilde{P}}|\tilde{P}$ and $\tilde{P}|P$ in a tower of extensions $M/L/K$, then $e(\tilde{\tilde{P}}|P) = e(\tilde{\tilde{P}}|\tilde{P}) \cdot e(\tilde{P}|P)$ and $f(\tilde{\tilde{P}}|P) = f(\tilde{\tilde{P}}|\tilde{P}) \cdot f(\tilde{P}|P)$.

4. [1pt*] For the cubic extension $\mathbb{R}(t)/\mathbb{R}(t^3)$, determine all primes lying over P_{t^3-0}, P_{t^3-1}, and P_{t^3+8} and determine their relative degrees and ramification indices.

5. [1pt] In the quadratic extension $\mathbb{Q}(\sqrt{11})/\mathbb{Q}$ with ring of integers $\mathbb{Z}[\sqrt{11}]$, use Dedekind's factorization theorem to determine whether the primes (2), (3), (5), (7), and (11) are split, inert, or ramified.

6. [1pt] Show that the norm and conorm of divisors compose in towers.

7. [1pt] Show that for any $a \in K^\times$, it is true that $\mathrm{Con}_{L/K}[\mathrm{div}_K a] = \mathrm{div}_L(a)$.

8. [1pt] Show that the conorm also respects the positive and negative parts of divisors: explicitly, that for $a \in K^\times$ we have $\mathrm{Con}_{L/K}(\mathrm{div}_{-,K} a) = \mathrm{div}_{-,L}(a)$ and $\mathrm{Con}_{L/K}(\mathrm{div}_{+,K} a) = \mathrm{div}_{+,L}(a)$.

9. [1pt] When L/K is separable, show that for any $\tilde{a} \in L$, it is true that $N_{L/K}[\mathrm{div}_L \tilde{a}] = \mathrm{div}_K[N_{L/K}\tilde{a}]$. (In fact the norm also respects positive and negative parts of divisors.)

0.1.5 Exercises from (Nov 19)

1. [3pts] Suppose that $\mathcal{O}_{\tilde{P}} = \mathcal{O}_P[\alpha]$ has integral basis $\{1, \alpha, \dots, \alpha^{n-1}\}$ where α has minimal polynomial $f(t) = (t-\alpha)(c_{n-1}t^{n-1} + \cdots + c_0)$ over K.
   (a) Show that the dual basis is $\{\frac{c_0}{f'(\alpha)}, \frac{c_1}{f'(\alpha)}, \dots, \frac{c_{n-1}}{f'(\alpha)}\}$. [Hint: Use the identity $\sum_{i=1}^n \frac{r_i^k}{f'(r_i)} \frac{f(t)}{t - r_i} = t^k$ where the r_i are the roots of f.]
   (b) Show that $C_{B/A} = f'(\alpha) \cdot B$. [This connection between the different and the derivative $f'(\alpha)$ is why it has the name "different".]

2. [2pts] Suppose that K/F is a separable extension of the function field $F(x)/F$ and that $[K : F(x)] > 1$. Show that $F(x)$ has at least one prime that ramifies in K. (This generalizes the classical result that the only unramified extension of $\mathbb{Q}$ is $\mathbb{Q}$ itself.)

0.1.6 Exercises from (Dec 1)

1. [2pts] Verify that if $q = p^{2b}$ and $q > (g+1)^4$, then taking $e = b$, $m = p^b + 2g$, and $l = \lfloor \frac{g}{g+1} p^b \rfloor$ satisfies all of the required relations and yields the bound $N_1(K) \leq 1 + p^b + (p^b + 2g)q = 1 + q + (2g+1)\sqrt{q}$.

2. [2pts] Show that if $K_n/\mathbb{F}_{q^n}$ is the constant-field extension of $K/\mathbb{F}_q$ of degree n, then $\zeta_{K_n}(s^n) = \zeta_K(s)\zeta_K(\omega s) \cdots \zeta_K(\omega^{n-1}s)$ where $\omega = e^{2\pi i/n}$. Deduce in particular that $\zeta_K(-1) = h_{K_2}/h_K$, a fact we needed to finish the proof of the prime number theorem for K.

0.2 Additional Exercises

1. [8pts*] We say an algebraic function field K/F is an elliptic function field if $g_K = 1$ and there exists at least one prime P_0 of degree 1. As proven in class, if K/F is elliptic then there exist $x, y \in K$ such that $K = F(x, y)$ and $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ for some $a_1, a_2, a_3, a_4, a_6 \in F$.

   (a) Show that for any degree-0 divisor D, there exists a unique degree-1 prime P of K such that $D \sim P - P_0$. [Hint: Write down a generator of $l(D + P_0)$ and consider its positive part.]

   (b) Show that the mapping φ : [degree-1 primes] $\to \mathrm{Pic}^0(K)$ via $\varphi(P) = [P - P_0]$ (the class of $P - P_0$) is a bijection.

   (c) Show that the binary operation $P \oplus Q = \varphi^{-1}(\varphi(P) + \varphi(Q))$ is a group operation on degree-1 primes with identity element P_0, and that $P \oplus Q = R$ is equivalent to saying $P + Q \sim R + P_0$ in the divisor group of K.

   (d) Show that the operation $P \oplus Q$ from (3) is the same as the "geometric" group law on the corresponding elliptic curve C defined by saying $P \oplus Q \oplus R = 0$ precisely when P, Q, R lie on the same line. [Hint: Let f be the line through P, Q, R, g be the line through R and P_0, and h be the tangent line at P_0 which passes through P_0 with multiplicity 3. Compare $\mathrm{div}(f/h)$ to $\mathrm{div}(g/h)$.]

2. [8pts] Let Λ be a 2-dimensional lattice in $\mathbb{C}$ (i.e., $\Lambda = \mathbb{Z}\alpha + \mathbb{Z}\beta$ where $\alpha, \beta \in \mathbb{C}^\times$ and β/α is not real). An elliptic function with respect to Λ is a meromorphic function f with $f(z + \lambda) = f(z)$ for all $z \in \mathbb{C}$ and all $\lambda \in \Lambda$. Equivalently, f is a "doubly periodic function" with $f(z + \alpha) = f(z) = f(z + \beta)$ for all z.

   (a) Show that the elliptic functions with respect to Λ form a field.

   (b) Show that the only elliptic functions with no poles are constant. [Hint: Liouville.]

   (c) Show that the Weierstrass $\wp$-function $\wp(z) = \dfrac{1}{z^2} + \sum_{\gamma \in \Lambda, \gamma \neq 0} \left[\dfrac{1}{(z-\gamma)^2} - \dfrac{1}{\gamma^2} \right]$ is an elliptic function with respect to Λ, as is its derivative $\wp'(z) = -\dfrac{2}{z^3} - \sum_{\gamma \in \Lambda, \gamma \neq 0} \dfrac{2}{(z-\gamma)^3}$. [Hint: It is perhaps easier to start with $\wp'$ since its sum is absolutely convergent.]

   (d) Show that $\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$ for some constants g_2 and g_3. [Hint: Consider Laurent series centered at $z = 0$.]

   (e) Show that every elliptic function with respect to Λ is an element of $K = \mathbb{C}(\wp(z), \wp'(z))$ and that K is an elliptic function field (as defined above).

   Remark: The primes of this elliptic function field K correspond to the points in $\mathbb{C}/\Lambda$, which is topologically a torus (a genus 1 surface). The group law on this elliptic function field as defined in problem 1 agrees with the natural additive group structure on $\mathbb{C}/\Lambda$.

3. [2pts] In $\mathbb{P}^2(k)$, a line is the vanishing locus of a homogeneous linear polynomial $l \in k[X, Y, Z]$ such as $X + Y = 0$ or $2X - Y - Z = 0$. Show that any two distinct lines in $\mathbb{P}^2(k)$ intersect in exactly one point. (Compare to the affine statement that any two lines are either parallel or intersect in exactly one point.)

4. [3pts] Let K be a function field and suppose $f(t) = a_nt^n + \cdots + a_1t + a_0 \in K[t]$. Generalize Eisenstein's criterion: if there exists a prime P of K such that $v_P(a_n) = 0$, $v_P(a_i) \geq v_P(a_0)$ for each $1 \leq i \leq n-1$, and $v_P(a_0) > 0$ is relatively prime to n, then $f(t)$ is irreducible in $K[t]$: moreover, for $L = K(\alpha)$ where $f(\alpha) = 0$, show that P is totally ramified in L. [Hint: Write $-a_n\alpha^n = a_0 + \cdots + a_{n-1}\alpha^{n-1}$; with $\tilde{P}|P$, use valuations to show that $n \cdot v_{\tilde{P}}(y) = e \cdot v_P(a_0)$ and deduce $n = e = [L : K]$.]