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 Thursday, December 9th. Starred exercises are especially recommended.

0.1 In-Lecture Exercises

0.1.1 Exercises from (Nov 1)

- *[2pts] If K is a function field over $\mathbb{F}_q$ of genus g where $q > 4$ and $g > 0$, show that the class number of K is greater than 1.
- *[2pts] 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 $\mathbb{A}^2(\mathbb{R})$.
- [3pts] 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 $\{(t, \sin t) : t \in \mathbb{R}\}$.
- [2pts] If k is finite, show that the irreducible affine algebraic sets in $\mathbb{A}^n(k)$ are $\emptyset$ and single points.
- *[3pts] 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 $k[y]$.]

0.1.2 Exercises from (Nov 4)

- [2pts] Let $\mathcal{F}(V,k)$ be the ring of k-valued functions on an affine variety V. We say $f \in \mathcal{F}(V,k)$ is a polynomial function if there exists $g \in k[x_1,\dots,x_n]$ such that $f(P) = g(P)$ for all $P \in V$. Show that $\Gamma(V)$ is the set of equivalence classes of polynomial functions under the relation $g_1 \sim g_2$ if $g_1(P) = g_2(P)$ for all $P \in V$.
- [3pts] Let V be an affine variety. Show that $\Gamma(V) = \cap_{P \in V} \mathcal{O}_P(V)$: in other words, that a function with no poles is a polynomial. (Note of course that k is algebraically closed!)

0.1.3 Exercises from (Nov 8)

- [3pts] Suppose k is an infinite field, $P \in \mathbb{A}^{n+1}\backslash\{0\}$, and suppose $f \in k[x_0,\dots,x_n]$ has homogeneous $f = f_0 + f_1 + \cdots + f_d$ 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.]
- *[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 $\mathbb{P}^2(k)$.
- [3pts] An ideal I of $k[x_0,\dots,x_n]$ is homogeneous if, for any $f \in I$ with homogeneous decomposition $f = f_0 + f_1 + \cdots + f_d$, it is true that each component $f_i \in I$. Show that I is homogeneous if and only if I is generated by finitely many homogeneous polynomials.
- [3pts] Let V be a nonempty projective variety in $\mathbb{P}^n$ and $C(V)$ be its cone in $\mathbb{A}^{n+1}$. 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 $C(V_{\text{projective}}(I)) = V_{\text{affine}}(I)$.
- [2pts] Show that $(FG)_* = F_* G_*$, $(fg)^* = f^* g^*$, $(f^*)_* = f$, $(F_*)^* = F / x_0^{v_{x_0}(f)}$, $(F+G)_* = F_* + G_*$, and $x_0^{\deg(f)+\deg(g)-\deg(f+g)} (f+g)^* = x_0^{\deg(g)} f^* + x_0^{\deg(f)} g^*$.

0.1.4 Exercises from (Nov 11)

- [3pts] Show that the isomorphisms $\varphi : \mathbb{A}^n \to \mathbb{A}^n$ are the invertible affine linear transformations, of the form $\varphi(x) = Ax + b$ where A is an invertible $n \times n$ matrix and b is any vector of constants. (Hint: First show that the degree of each coordinate in φ and ψ must be 1.)

0.1.5 Exercises from (Nov 18)

- [3pts] 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 at a point $P \in V(f)$, then the third is as well.

0.1.6 Exercises from (Nov 22)

- [3pts] 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 $f(\tilde{\tilde{P}}|P) = f(\tilde{\tilde{P}}|\tilde{P}) \cdot f(\tilde{P}|P)$.
- [2pts] 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.
- *[3pts] 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.

0.1.7 Exercises from (Nov 29)

- [2pts] Show that the norm and conorm of divisors compose in towers.
- [2pts] Show that for any $a \in K^\times$, it is true that $\mathrm{Con}_{L/K}[\mathrm{div}_K a] = \mathrm{div}_L(a)$.
- [2pts] When L/K is separable, show that for any $\tilde{a} \in L$, it is true that $N_{L/K}[\mathrm{div}_L \tilde{a}] = \mathrm{div}_K[N_{L/K}\tilde{a}]$.
- [3pts] If $\mathcal{O}_{\tilde{P}} = \mathcal{O}_P[\alpha]$ 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, 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.]
- [3pts] Show that if $\mathcal{O}_{\tilde{P}} = \mathcal{O}_P[\alpha]$ has integral basis $\{1, \alpha, \dots, \alpha^{n-1}\}$ where α has minimal polynomial $f(t)$ over K, then $C_{B/A} = f'(\alpha) \cdot B$. [This connection between the different and the derivative $f'(\alpha)$ is why it has the name "different".]

0.1.8 Exercises from (Dec 6)

- [3pts] Verify that if $q = p^{2b}$ and $q > (g+1)^4$, then taking $e = b$, $m = p^b + 2g$, and $l = \lfloor \frac{g}{g+1} p^b \rfloor$ has $lp^e < q$, and $l, m \geq g$, and $(l - g + 1)(l - m + 1) > lp^e + m - g + 1$, and converts the bound $N_1(K) \leq 1 + l + mq/p^e$ into $N_1(K) \leq 1 + q + (2g+1)\sqrt{q}$.

0.2 Additional Exercises

- *[10pts] We say an algebraic function field $K/\mathbb{F}$ 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 $K/\mathbb{F}$ is elliptic then there exist $x, y \in K$ such that $K = \mathbb{F}(x, y)$ and $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ for some $a_1, a_2, a_3, a_4, a_6 \in \mathbb{F}$.

  1. 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.]
  2. 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.
  3. 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.
  4. 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 $\mathrm{div}(g/h)$.]

- [10pts] Let Λ be a 2-dimensional lattice inside of $\mathbb{C}$ (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 $f(z + \alpha) = f(z + \beta) = f(z)$ for all z.

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

- [3pts] 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.)