Rational Points on Curves, Summer 2021, Problem Set 1

(1) Let $f\colon V \to k$ be a quadratic form on a finite-dimensional vector space V over a field k of characteristic not equal to 2. Show that there is a basis of V in which f is diagonal (equivalently, V has an orthogonal basis for the associated bilinear form).

(2) Let $f \in \mathbb{Z}[X_0, X_1, \ldots, X_n]$ be a homogeneous polynomial. Show that there exists $a = (a_0, a_1, \ldots, a_n) \in \mathbb{Q}^{n+1} \setminus \{0\}$ such that $f(a) = 0$ if and only if there exists $(a_0, a_1, \ldots, a_n) \in \mathbb{Z}^{n+1} \setminus \{0\}$ with $\gcd(a_0, \ldots, a_n) = 1$ such that $f(a) = 0$. Next fix a prime p, and show that the following (for which it suffices to assume the coefficients of f lie in $\mathbb{Z}_p$) are equivalent:
- There is an $a \in \mathbb{Q}_p^{n+1} \setminus \{0\}$ such that $f(a) = 0$.
- There is an $a \in \mathbb{Z}_p^{n+1}$ with some coordinate non-zero mod p such that $f(a) = 0$.
- For all $m \geq 1$, there is an $a \in (\mathbb{Z}/p^m)^n$ with some coordinate non-zero mod p such that $f(a) \equiv 0 \pmod{p^m}$.

(3) Prove the refined form of the single-variable Hensel's Lemma stated in class.

(4) For each prime p, determine the number of roots of unity (elements x such that $x^n = 1$ for some $n \geq 1$) in $\mathbb{Q}_p$. (Hint: use Hensel's Lemma.)

(5) Let $f(X_0, X_1, X_2) \in \mathbb{Z}[X_0, X_1, X_2]$ be a homomogeneous degree 2 polynomial, defining the conic $C_f \subset \mathbb{P}^2$. Show that for all but finitely many primes p, $C_f(\mathbb{Q}_p) \neq \emptyset$. For $f(X_0, X_1, X_2) = X_0^2 + X_1^2 - 3X_2^2$, determine $\{p : C_f(\mathbb{Q}_p) \neq \emptyset\}$.

(6) Consider the affine curve $C \subset \mathbb{A}^2$ given by $2x^2 + 7y^2 = 1$. Parametrize $C(\mathbb{Q})$ as $\{(x(t), y(t)) : t \in \mathbb{Q}\}$ for some rational functions $x(t), y(t) \in \mathbb{Q}(t)$ (analogous to the "Pythagorean triple" parametrization of the rational points on $x^2 + y^2 = 1$).

(7) Prove the two-variable case of the Hasse-Minkowski theorem: a quadratic form $f(X_0, X_1) \in \mathbb{Q}[X_0, X_1]$ represents zero in $\mathbb{Q}$ if and only if it represents zero in $\mathbb{Q}_p$ for all p and represents zero in $\mathbb{R}$ (by "represents zero in a field k" we mean there exists $(a_0, a_1) \in k^2 \setminus \{0\}$ such that $f(a_0, a_1) = 0$).

Rational Points on Curves, Summer 2021, Problem Set 2

Throughout this assignment, unless otherwise indicated, k is a field.

(1) Complete the calculation started in class, using Legendre's proof of the three-variable Hasse-Minkowski theorem, to compute a rational point on the projective curve given by $f(X_0, X_1, X_2) = X_0^2 - 13X_1^2 + 17X_2^2$.

(2) (Some projective geometry)

  (a) Let $V \subset k^{n+1}$ be a vector subspace of dimension $r + 1$, for some $r \leq n$. Show that the image $\mathbb{P}(V) \subset \mathbb{P}^n$ is the vanishing locus of $n - r$ homogeneous linear polynomials. (When $r = 1$, $\mathbb{P}(W)$ is a *line*; when $r = n - 1$, it is a *hyperplane*.)

  (b) Show that any two distinct lines in $\mathbb{P}^2$ intersect in exactly one point.

  (c) Let $P_1, P_2, \ldots, P_{n+2} \in \mathbb{P}^n(k)$ be $(n + 2)$ points such that no $(n + 1)$ of them lie on a hyperplane (we say they are in "general position"). Let $Q_1, \ldots, Q_{n+2} \in \mathbb{P}^n(k)$ be another such set of $n + 2$ points in general position. Show that there is some element $g \in \mathrm{GL}_{n+1}(k)$ such that the induced change of coordinates $g \colon \mathbb{P}^n \to \mathbb{P}^n$ satisfies $g(P_i) = Q_i$ for all i. (If you're having trouble with this, first do it for $n + 1$ points in general position.)

(3) Let k be any field, and let $f \in k[X_0, X_1, X_2]$ be a homogeneous polynomial of degree 2. Assume that the projective conic $C_f \subset \mathbb{P}^2$ is nonsingular, and that $C_f(k)$ is non-empty. Fix a point $P_0 \in C_f(k)$ and a linear homogeneous polynomial $L(X_0, X_1, X_2) \in k[X_0, X_1, X_2]$ such that the vanishing locus $C_L \subset \mathbb{P}^2$ does not contain the point P_0.

  (a) Show that the projection map

$$\pi \colon C_f \to C_L$$

  defined by

$$\pi(Q) = \begin{cases} \text{the unique point of intersection } L \cap \overline{QP_0} \text{ if } Q \neq P_0; \\ \text{the unique point of intersection } L \cap T_{C_f, P_0} \text{ if } Q = P_0 \end{cases}$$

  is well-defined, and that it gives a bijection $C_f(K) \to C_L(K)$ for all fields $K \supset k$.

  (b) Show that π is in fact an isomorphism of algebraic varieties over k. (This implies (a); the problems are separate for those who have not necessarily learned what a morphism of varieties is.)

  (c) Show that C_L is isomorphic to $\mathbb{P}^1$, as algebraic varieties over k. Thus any smooth projective conic containing a k-rational point is isomorphic to $\mathbb{P}^1$.

(4) Let $p \equiv 1 \pmod 8$ be a prime such that 2 is not a 4^{th} power in $\mathbb{F}_p$. Let $C^0 \subset \mathbb{A}^2$ be the affine curve over $\mathbb{Q}$ defined by the polynomial $f(w, z) = w^2 - 2 + 2pz^4$. In class we constructed a nonsingular projective curve $C \subset \mathbb{P}^3$ and an isomorphism $C^0 \xrightarrow{\sim} C \setminus \{[0, 0, \pm\sqrt{-2p}, 1])\}$. Show that $C(\mathbb{Q}_2) \neq \emptyset$.

(5) Assume $\mathrm{char}(k) \neq 3$. For each $t \in \bar{k}$, $f_t(X_0, X_1, X_2) = X_0^3 + X_1^3 + X_2^3 - 3tX_0X_1X_2$ defines a projective curve $C_t \subset \mathbb{P}^2$ (over the subfield of $\bar{k}$ generated by t, or just over $\bar{k}$ if you prefer).

  (a) Determine, for all t, the set of singular points of C_t (in particular, determine which C_t are nonsingular).

  (b) Determine $C_0(\mathbb{Q})$.

Rational Points on Curves, Summer 2021, Problem Set 3

(1) Consider the plane curve $C = V(y^2 - x^3 - x) \subset \mathbb{A}^2$ over a field k of characteristic not 2.
  (a) Show that the projective closure $\overline{C} = V(Y^2Z - X^3 - XZ^2) \subset \mathbb{P}^2$ of C is nonsingular (in particular, C is).
  (b) Let $P = (0,0) \in C$, and let v_P be the associated discrete valuation of $k(C)$ (as defined in Monday's class). Compute $v_P(x)$ and $v_P(y)$.
  (c) The affine space $\{Y \neq 0\} \subset \mathbb{P}^2$ has coordinate functions $u = X/Y$ and $v = Z/Y$, i.e., its coordinate ring is the polynomial ring $k[u,v]$. Write in terms of u and v the equation of $C' := \overline{C} \cap \{Y \neq 0\} \subset \{Y \neq 0\} \cong \mathbb{A}^2$. Write down the canonical isomorphism $k(C) \cong k(C')$.
  (d) Let Q be the unique point in $\overline{C} \setminus C$ (you should know from part (a) what Q is). Compute $v_Q(x)$ and $v_Q(y)$, identifying x and y as elements of $k(C')$ as in the last part.

(2) Consider the plane curve $C = V(y^2 - x^3 - x^2) \subset \mathbb{A}^2$. Show that C is singular at $P = (0,0)$, and check that $\mathcal{O}_{C,P}$ is not a DVR.

(3) Let $v \colon \mathbb{Q}^\times \to \mathbb{Z}$ be a surjective discrete valuation. Show that $v = v_p$ for some prime number p.

(4) Let $v \colon \bar{k}(t)^\times \to \mathbb{Z}$ be a surjective discrete valuation trivial on $\bar{k}$ (here $\bar{k}$ is an algebraically closed field). Show that either there exists $a \in \bar{k}$ such that $v = v_{t-a}$ or $v = v_\infty$. (See the class notes for these examples of valuations.) How would you describe the discrete valuations on $k(t)$ (trivial on k) when k is not necessarily algebraically closed?

(5) Let $X \subset \mathbb{A}^n$ be an affine variety over an algebraically closed field $\bar{k}$. Exhibit a bijection between the points of X and the maximal ideals of $\bar{k}[X]$.

(6) The most concrete definition of an elliptic curve over a field k of characteristic not 2 or 3 is the following: it is a nonsingular projective curve $C = V(F) \subset \mathbb{P}^2$ where

$$F(X,Y,Z) = Y^2Z - X^3 - AXZ^2 - BZ^3$$

for some $A, B \in k$, along with its evident k-rational point $[0,1,0]$. Show that such an equation in fact defines a *nonsingular* curve if and only if $\Delta(A,B) = -16(4A^3 + 27B^2)$ is non-zero in k. (Of course, the factor of -16 does not affect—in characteristic not 2!—whether Δ is zero; this normalization is conventional, and it also reflects the fact that such a curve is always singular in characteristic 2.)

Rational Points on Curves, Summer 2021, Problem Set 4

(1) Let k be a field of characteristic not 2, and consider the projective nonsingular curve over k associated to the affine curve $y^2 = f(x)$, where $f(x) \in k[x]$ is a cubic polynomial with distinct roots.
  (a) Show that the (rational) differential $\omega = \frac{dx}{y} \in \Omega_{k(C)/k}$ satisfies $\operatorname{div}(\omega) = 0$. Deduce from the Riemann-Roch theorem that $g(C) = 1$.
  (b) *Without* assuming the Riemann-Roch theorem, show that the dimension of the space of everywhere regular differentials on C is 1. (Hint: which $h\omega$ can be everywhere regular, for $h \in k(C)$?)

(2) Carry out a version of the arguments in Problem 1 to show that the nonsingular projective curve $C \subset \mathbb{P}^3$ (an intersection of two quadrics) we studied to produce a counterexample to the local-global principle for rational points is in fact of genus 1. What is a natural class of curves that your argument applies to?

(3) (Galois descent of vector spaces) Let L/K be a finite Galois extension, and let V be an L-vector space equipped with an L-semilinear action of $\mathrm{Gal}(L/K)$: that is, $\mathrm{Gal}(L/K)$ acts on the abelian group V, and this action satisfies $\sigma(cv) = \sigma(c)\sigma(v)$ for all $\sigma \in \mathrm{Gal}(L/K)$, $c \in L$, $v \in V$. Let $W \subset V$ be the subset of $\mathrm{Gal}(L/K)$-invariant vectors:

$$W = \{v \in V : \sigma(v) = v \text{ for all } \sigma \in \mathrm{Gal}(L/K)\}.$$

  (a) Check that W is a K-vector subspace of V.
  (b) Show that for all $v \in V$, $\mathrm{tr}(v) := \sum_{\sigma \in \mathrm{Gal}(L/K)} \sigma(v)$ lies in W; and show that for $v \neq 0$, $\mathrm{tr}(cv) \neq 0$ for some $c \in L$.
  (c) Show that the natural L-linear map $\alpha \colon W \otimes_K L \to V$ is an isomorphism. (Hint: apply the last part to $V/\operatorname{im}(\alpha)$; how is this quotient space equipped with an L-semilinear action of $\mathrm{Gal}(L/K)$?) Concretely, W admits a K-basis that is an L-basis of V.
  (d) Let $\overline{K}$ be a separable closure of K. Generalize the result of (c) to the case of a *continuous* $\overline{K}$-semilinear action of $G_K := \mathrm{Gal}(\overline{K}/K)$ on a $\overline{K}$-vector space V, where the continuity condition means that for every $v \in V$, the stabilizer $\{\sigma \in G_K : \sigma(v) = v\}$ is $\mathrm{Gal}(\overline{K}/L)$ for some finite extension L/K (i.e., the map $\sigma \mapsto \sigma(v)$ is continuous for the discrete topology on V and the Krull topology on G_K).

(4) Consider the elliptic curve $y^2 = x^3 - 2$ over $\mathbb{Q}$. Let $P = (3, 5)$. Compute $[2]P$.

(5) Let (E, O) be an elliptic curve over a field of characteristic not 2 or 3 given by a homogeneous Weierstrass equation $F(X_0, X_1, X_2) = 0$.
  (a) For $P \in E$, show that $[3]P = O$ if and only if the tangent line to E at P intersects E only at P.
  (b) Next show that $[3]P = 0$ if and only if the "Hessian" matrix $(\partial^2 F/\partial X_i \partial X_j(P))_{i,j}$ is singular.
  (c) Conclude that $\#(E[3]) = 9$.
  (d) Describe $E[3]$ when E is given by a cubic equation $F(X_0, X_1, X_2) = X_0^3 + X_1^3 + X_2^3 - 3tX_0X_1X_2$ as in PSet 2, Problem 5 (for any t such that this curve is nonsingular), and the origin $O \in E$ is taken to be $[1, -1, 0]$.

Rational Points on Curves, Summer 2021, Problem Set 5

(1) Let k be a field of characteristic not 2, and let E/k be an elliptic curve. In this exercise, you will prove that for all non-zero $m \in \mathbb{Z}$, $[m]\colon E \to E$ is an isogeny.
  (a) Show that (for any k), $[m]$ is a morphism.
  (b) Show that $[2]$ is not constant by writing down in terms of a Weierstrass equation for E a necessary condition for $P = (x, y) \in E$ to satisfy $[2]P = O$. (This should lead you to a cubic equation in x; if you prefer to simplify the calculations, you may also assume $\mathrm{char}(k) \neq 3$, in order to have a Weierstrass equation of the form $y^2 = x^3 + ax + b$.)
  (c) Continue the analysis of the previous part and check that $E[2]$ strictly contains $\{O\}$. Deduce that for m odd, $[m]$ is non-constant.
  (d) Combine the previous two parts to show that $[m]$ is non-constant for all $m \neq 0$.

(2) Consider the elliptic curve $E/\mathbb{Q}$ given by the Weierstrass equation $y^2 = x^3 + 3$.
  (a) For what primes p does this Weierstrass equation have good reduction modulo p?
  (b) For any prime p such that E has good reduction modulo p, and any m coprime to p, we have shown that $E(\mathbb{Q}_p)[m]$ injects (as a group) into $\tilde{E}(\mathbb{F}_p)$. Use this to show that the torsion subgroup $E(\mathbb{Q})_{\mathrm{tor}}$ is trivial.
  (c) Show that $E(\mathbb{Q})$ is infinite.

(3) Let F be a number field, and let E/F be an elliptic curve. Prove, as in the last problem using our results on elliptic curves over local fields, that the torsion subgroup $E(F)_{\mathrm{tor}}$ of $E(F)$ is finite.

(4) Let K be a finite extension of $\mathbb{Q}_p$, and let E/K be an elliptic curve with good reduction. In our proof that $[m]$ is an automorphism of $E_1(K)$, for m coprime to p, we used that a certain reduction map $E_n(k) \to C(k)_{\mathrm{ns}}$ to the non-singular points of the cuspidal cubic $C : y^2 = x^3$ over the residue field k of K, was in fact a group homomorphism. Precisely, we wrote $P \in E_n(K)$ as $[\varpi^n x_0, y_0, \varpi^{3n} z_0]$ with $y_0 \in \mathcal{O}_K^\times$ and $x_0, z_0 \in \mathcal{O}_K$ (with x_0 and z_0 also units if $P \notin E_{n+1}(K)$), and that map was $[x, y, z] \mapsto [x_0, y_0, z_0] \pmod{\varpi}$. Verify the claim that this is a surjective homomorphism.

(5) Let G be a (discrete) group. Prove that to any short exact sequence

$$0 \to M \xrightarrow{\alpha} N \xrightarrow{\beta} P \to 0$$

of G-modules, there is an associated long exact sequence

$$0 \to M^G \to N^G \to P^G \xrightarrow{\delta} H^1(G, M) \to H^1(G, N) \to H^1(G, P)$$

of abelian groups, with $\delta(p)\colon G \to M$ given by $g \mapsto g \cdot n - n$ for any $n \in N$ such that $\beta(n) = p$. Check that your proof also works when $G = G_k$ is the absolute Galois group of a field k, and M, N, and P are discrete G_k-modules. (If you know what it means, replace G_k by any profinite group here.)

(6) Let k be a field. One form of Hilbert's Theorem 90 asserts that $H^1(G_k, \bar{k}^\times) = \{1\}$ (if k is not perfect, $\bar{k}$ here means a separable closure of k). Assuming this, prove that $\mathbb{P}^n(\bar{k})^{G_k} = \mathbb{P}^n(k)$. (The analogous statement for $\mathbb{A}^n$ is obvious; this is not!)

(7) Combine problems 5 and 6 to prove the fundamental isomorphism of *Kummer theory*: for any field k and integer n coprime to $\mathrm{char}(k)$, there is an isomorphism

$$k^\times/(k^\times)^n \xrightarrow{\sim} H^1(G_k, \mu_n(\bar{k}))$$

given by the boundary map in the long-exact sequence in G_k-cohomology associated to the short-exact sequence

$$1 \to \mu_n(\bar{k}) \to \bar{k}^\times \xrightarrow{z \mapsto z^n} \bar{k}^\times \to 1.$$

(Here $\mu_n(\bar{k})$ is the set of n^{th} roots of unity in $\bar{k}$. In the classical form of Kummer theory, one assumes k contains all n^{th} roots of 1, so that $\mu_n(\bar{k})$ is a G_k-module with trivial action, and $k^\times/(k^\times)^n \xrightarrow{\sim} \mathrm{Hom}_{\mathrm{cts}}(G_k, \mu_n)$. One easily translates this isomorphism into a correspondence between finite abelian exponent n extensions of k (inside $\bar{k}$) and finite subgroups A of $k^\times/(k^\times)^n$, a subgroup A corresponding to the "Kummer extension" $k[A^{1/n}]$. Work out the details of this correspondence as an optional exercise.)

Rational Points on Curves, Summer 2021, Problem Set 6

(1) Let F be a number field, with $|F|$ its set of places. For each $v \in |F|$, let $|\cdot|_v$ be the associated *normalized* absolute value as defined in class. Prove the product formula: for all $a \in F$,

$$\prod_{v \in |F|} |a|_v = 1.$$

(2) Let α be an algebraic integer (that is, α satisfies some monic polynomial with integer coefficients) such that for every embedding $\tau \colon \mathbb{Q}[\alpha] \to \mathbb{C}$, $|\tau(\alpha)| \leq 1$. Prove that α is a root of unity. (Note this is not true if we only assume α is an algebraic number.) More generally, if F is a number field and $P = [x_0, \dots, x_n] \in \mathbb{P}^n(F)$ with some $x_i \neq 0$, show that $H(P) = 1$ if and only if $\frac{x_j}{x_i}$ is either zero or a root of unity for every $0 \leq j \leq n$.

(3) Suppose that $y^2 = x^3 + Ax + B$ is a non-singular Weierstrass equation over a field F of characteristic not 2. Show that the rational map $g \colon \mathbb{P}^2 \to \mathbb{P}^2$ defined by

$$g([t, u, v]) = [u^2 - 4tv, 2u(At + v) + 4Bt^2, (v - At)^2 - 4Btu]$$

is a morphism. (Recall that we use this for $F = \overline{\mathbb{Q}}$ in our proof of the Mordell-Weil theorem.)

(4) Let $\alpha_1, \alpha_2 \in \overline{\mathbb{Q}}$, and let h denote the absolute logarithmic height on $\mathbb{P}^n$ (for n to be understood from the context). Prove the lower bound

$$h[1, \alpha + \beta, \alpha\beta]) \geq h([\alpha_1, 1]) + h([\alpha_2, 1]) - \log 4.$$

(5) Let F be a number field, and let M be a discrete G_F-module with $|M|$ finite. Let S be any finite set of primes of F. In class we proved that

$$\{\varphi \in H^1(G_F, M) : \varphi \text{ is unramified outside } S\}$$

is finite, using the Hermite-Minkowski theorem. Give another proof of this fact without using Hermite-Minkowski, but instead using (a) finiteness of the class group; (b) finite-generation of the unit group; and (c) Kummer theory.

(6) Fix a number field F and an integer n. Show that there is a uniform bound on $\mathrm{rk}(E(F))$ as E ranges over all elliptic curves over F having good reduction outside a set of most n primes (we do not fix the set, just its size!). (Remark: it is unknown whether $\mathrm{rk}(E(F))$ is (un)bounded as E ranges over all elliptic curves over F.)