GEOMETRY AND ARITHMETIC OF LOW GENUS CURVES
2020 ARIZONA WINTER SCHOOL PROBLEM SET

VERSION WITHOUT HINTS

ISABEL VOGT

Using this problem set. The goal of this problem set is to become friends with low genus curves by taking a tour though some constructions and techniques that appear frequently when studying their geometry and arithmetic. The problem set is broken into two chapters as follows:

Chapter I: Geometry. The philosophy of this chapter is that one encounters interesting low genus curves "in nature": as covers of other curves, as divisors on surfaces, and so on. Since we care about arithmetic, in this section we *do not* assume that the ground field is algebraically closed, and pay careful attention to fields of definition.

Chapter II: Arithmetic. The main theme of this section is techniques for understanding the rational points on curves defined over number fields, especially étale descent. We've focused on descent, since it is both a powerful tool to bound the rank of a Jacobian (which is an input to classical Chabauty's method), and can be used in combination with Chabauty arguments to find rational points. We present these ideas in some generality because of their prevalence and usefulness in other contexts.

Date: March 5, 2020.

CHAPTER 1

Geometry

For this section, C denotes a nice (smooth, projective, and geometrically integral) curve of genus g defined over a perfect field k. We will write $\overline{k}$ for an algebraic closure of k. We write $\mathcal{O}_C$ for the structure sheaf on C.

- Given a coherent sheaf $\mathscr{F}$ on C, we write $h^i(C, \mathscr{F})$ for the dimension of the coherent cohomology group $H^i(C, \mathscr{F})$ as a k-vector space.
- We use K_C to denote the canonical line bundle on C; by definition $g = h^0(C, K_C)$.
- We will use divisor notation for line bundles, and write $L_1 + L_2$ for $L_1 \otimes L_2$ and $-L$ for $L^\vee$.
- A curve C is called hyperelliptic if it admits a map of degree 2 to a nice curve of genus 0. (Warning: some authors use a different convention and require that the target is $\mathbb{P}^1_k$. We will use the term $\operatorname{gon}(C) = 2$ for this situation.)
- We write $C(k) = C(\operatorname{Spec} k)$ for the k-rational points on C (i.e., the set of maps $\operatorname{Spec} k \to C$). This is the same as the set of closed points of degree 1. More on this in the next chapter!
- Given a rational function $f \in k(C)$, we write (f) for the (principal) divisor of zeros and poles of that function.
- We write $\operatorname{Pic}(C)$ for the group of line bundles on C over k (equivalently divisors on C over k modulo principal divisors). We write $\operatorname{Pic}_{C/k}$ for the Picard scheme of C/k.
- The Jacobian of C/k is the identity component $\operatorname{Pic}^0_{C/k}$ and will be denoted J_C (or simply J when the curve C is implicit).

1. Background exercises on linear systems and Riemann–Roch

I.1.1 A subspace $V \subseteq H^0(C, L)$ is called p-very ample if for all length $p+1$ subschemes $Z \subseteq C_{\overline{k}}$, the evaluation map

$$V \xrightarrow{\text{ev}} L|_Z$$

is surjective. When $p = 0$, we call it basepoint-free and when $p = 1$, we call it simply very ample. When $H^0(C, L)$ is p-very ample, we say that L itself is p-very ample.

Give a bijection between

$$\{\text{morphisms } \varphi_V \colon C \to \mathbb{P}^r_k\} \qquad \text{and} \qquad \{(L, \sigma_0, \ldots, \sigma_r)\}/\simeq,$$

where L is a line bundle and $\sigma_0, \ldots, \sigma_r \in H^0(C, L)$ span a basepoint-free subspace V. (When $V = H^0(C, L)$, we will write φ_L for the corresponding morphism.)

Show, further, that the associated map is a closed immersion if and only if the sections $\sigma_0, \ldots, \sigma_r \in H^0(C, L)$ span a very ample subspace.

I.1.2 Let L be a line bundle on C.

(a) If $\deg L < 0$, then $h^0(C, L) = 0$.
(b) If $\deg L = 0$, then $h^0(C, L) = 1$ if and only if $L \simeq \mathcal{O}_C$.
(c) If $\deg L = 1$, then $h^0(C, L) > 1$ if and only if $C \simeq \mathbb{P}^1_k$.

I.1.3 Let L be a line bundle on C. By the Riemann–Roch theorem, we have

$$h^0(C, L) - h^1(C, L) = \deg L + 1 - g.$$

Furthermore, as a consequence of the Serre duality theorem, we have

$$h^i(C, L) = h^{1-i}(C, K_C - L).$$

(a) If $h^0(C, L) = r + 1$, give a formula for $h^1(C, L)$.
(b) Prove that $h^0(C, L) \leqslant \deg L + 1$.
(c) Compute the degree of K_C and show that it is the only bundle of that degree with g global sections.
(d) Prove that if $g > 0$, the canonical bundle K_C is basepoint-free.
(e) Show that if $\deg L \geqslant g$, then L is effective (i.e., $h^0(C, L) > 0$).
(f) Show that if $\deg L \geqslant 2g - 1$, then $h^1(C, L) = 0$. (Show that this is sharp: exhibit a bundle L of degree $2g - 2$ for which $h^1(C, L) > 0$.)
(g) Show that if $\deg L \geqslant 2g$, then L is basepoint-free.
(h) Show that if $\deg L \geqslant 2g + 1$, then L is very ample.
(i) A bundle is called ample if there exists some positive integer $n > 0$ such that nL is very ample. Find a necessary and sufficient criterion for a line bundle on C to be ample.

I.1.4 The gonality – denoted $\mathrm{gon}(C)$ – of a curve C is the minimal degree of a dominant map $C \to \mathbb{P}^1_k$.

(a) Prove that if K_C is p-very ample, then $\mathrm{gon}(C) \geqslant p + 2$.
(b) Conversely, show that if K_C is *not* p-very ample, then $\mathrm{gon}(C_{\overline{k}}) \leqslant p + 1$.
(c) * Give an example showing that when K_C is not p-very ample, $\mathrm{gon}(C)$ can be larger than $p + 1$.
(d) In the case $p = 1$, show the stronger statement that K_C is very ample if and only if C is not hyperelliptic.

Therefore, if C is not hyperelliptic, the morphism $\varphi_{K_C} \colon C \to \mathbb{P}^{g-1}_k$ is an embedding called the canonical embedding. The image is called a canonical curve of genus g.

I.1.5 Let D be an effective divisor on a curve C of degree d. Suppose that $h^0(C, \mathcal{O}(D)) = r + 1$. Show that under φ_{K_C}, the image of the points of D span a linear space $\mathbb{P}^{d-1-r}_k$. (This statement is sometimes called geometric Riemann–Roch.)

I.1.6 Compute the following dimensions:

(a) $h^0(C, T_C)$
(b) $h^1(C, T_C)$
(c) $h^2(C, T_C)$

I.1.7 Let C be a curve and L a line bundle on C. Let $p \in C(\overline{k})$ be a geometric point.

(a) Show that $h^0(C, L(-p)) \geqslant h^0(C, L) - 1$. If equality holds, what do we know about p?
(b) Show that if $h^0(C, L) > 0$ and p is a general geometric point, then

$$h^0(C, L(-p)) = h^0(C, L) - 1.$$

(c) If L and M are two line bundles such that $h^0(C, L) > 0$ and $h^0(C, M) > 0$, show that

$$h^0(C, L \otimes M) \geqslant h^0(C, L) + h^0(C, M) - 1.$$

When does equality hold?

I.1.8 (Clifford's Theorem) Let C be a curve of genus g and let L be a line bundle of degree d on the curve C.

(a) If $d > 2g - 2$, what is $h^0(C, L)$?
(b) If $0 \leqslant d \leqslant 2g - 2$, show that

$$h^0(C, L) \leqslant 1 + \frac{d}{2}.$$

(c) * What can you say if equality holds in part (b)?

2. Genus 0 curves

In this section, C is a nice curve of genus 0 defined over a field k.

I.2.1 The simplest example of a curve of genus 0 is $\mathbb{P}^1_k$.

(a) Show that $\mathrm{Pic}(\mathbb{P}^1_k) \simeq \mathbb{Z}$ by the degree. Write $\mathcal{O}(d)$ for the unique (up to isomorphism) line bundle of degree d on $\mathbb{P}^1_k$.
(b) In this notation, what is the canonical bundle?
(c) Determine the cohomology

$$h^0(\mathbb{P}^1_k, \mathcal{O}(d), \qquad \text{and} \qquad h^1(\mathbb{P}^1_k, \mathcal{O}(d)).$$

I.2.2 Choose a coordinate x such that $k(\mathbb{P}^1_k) \simeq k(x)$; write ∞ for the point in $\mathbb{P}^1_k$ where x has a pole so that $(x) = 0 - \infty$.

(a) Let $L = \mathcal{O}_{\mathbb{P}^1}(\infty)$ be the line bundle associated to the divisors ∞. Using the identification

$$H^0(\mathbb{P}^1_k, L) = \{f \in k(\mathbb{P}^1_k) \text{ s.t. } (f) + \infty \text{ is effective}\},$$

give a basis for $H^0(\mathbb{P}^1_k, L)$.
(b) Similarly, give a basis for $H^0(\mathbb{P}^1_k, nL)$ for all n. Compare you answers to those for Exercise (**I.2.1**).
(c) What is the divisor of the meromorphic differential dx?

I.2.3 More generally, show that $\mathrm{Pic}_{C/k}(k) \simeq \mathbb{Z}$. Exhibit a field k and a genus 0 curve C defined over k where $\deg\colon \mathrm{Pic}(C) \to \mathbb{Z}$ is not surjective. In this case, what is $\#\,\mathrm{Pic}_{C/k}(k)/\,\mathrm{Pic}(C)$?

I.2.4 Show that every genus 0 curve admits an embedding $C \hookrightarrow \mathbb{P}^2_k$. What is the degree of the image?

I.2.5 Show that $C(k) \neq \varnothing$ if and only if C has a closed point of odd degree.

I.2.6 Determine the gonality of C.

3. Finite branched covers

Description of the canonical bundle: Riemann–Hurwitz.

Given a finite separable map $\pi\colon X \to Y$ of nice curves, the relative cotangent sheaf $\Omega^1_{X/Y}$ is defined by

$$\Omega^1_{X/Y} = K_X - \pi^* K_Y.$$

Write g_X and g_Y for the genera of X and Y respectively.

I.3.1 Given a closed point $P \in X$ with image $Q = \pi(P) \in Y$, let e_P be such that

$$\mathfrak{m}_Q \cdot \mathcal{O}_{X,P} = \mathfrak{m}_P^{e_P}.$$

Show that if the map π is tamely ramified – i.e., the characteristic of k does not divide e_P for any closed point P – then

$$\Omega^1_{X/Y} = \sum_{\substack{P \in X \\ \text{closed point}}} (e_P - 1)\, P. \tag{1}$$

Deduce the Riemann–Hurwitz formula:

$$2g_X - 2 = (\deg \pi)(2g_Y - 2) + \sum_{P \in X(\overline{k})} (e_P - 1).$$

Closed points $P \in X$ where $e_P > 1$ are called ramification points of π. Closed points $Q \in Y$ such that there exists a ramification point $P \in \pi^{-1}(Q)$ are called branch points of π.

I.3.2 Let G be a finite group. A finite branched cover $\pi\colon X \to Y$ is called a Galois cover with Galois group G (or simply a G-Galois cover) if $k(X)/k(Y)$ is a Galois extension of function fields with Galois group G.

(a) Interpret G as a constant finite group scheme over k. Show that if $\pi\colon X \to Y$ is a G-Galois cover, then X admits a right G-action

$$X \times G \to X,$$
$$(x, g) \mapsto xg$$

that respects $\pi\colon X \to Y$; i.e., such that for all $g \in G$, the diagram

(2)
$$\begin{array}{ccc} X & \xrightarrow{\quad g \quad} & X \\ & {\scriptstyle\pi}\searrow \quad \swarrow{\scriptstyle\pi} & \\ & Y & \end{array}$$

commutes.

(b) Given an action of a group G on a scheme X, a scheme Y is called the scheme-quotient of X by G if it is universal for schemes fitting into diagram (2). We write $Y = X/G$. Phrase this precisely and show that π is a G-Galois cover if and only if $Y = X/G$.

(c) If $\pi\colon X \to Y$ is a G-Galois cover, what can you say about the ramification indices e_P for $P \in X$?

(d) Suppose further now that $\pi\colon X \to Y$ is a G-Galois *étale* cover (i.e., all $e_P = 1$). Show that

$$X \times G \to X \times_Y X,$$
$$(x, g) \mapsto (x, xg)$$

is an isomorphism of k-varieties.

I.3.3 If the genus g of C is at least 2, then the group of automorphisms $\mathrm{Aut}(C)$ is finite.[1] Assuming this fact, this exercise will lead you through the proof of the 84(g-1) theorem: if $g \geqslant 2$ and the characteristic of k is 0, then $\#\,\mathrm{Aut}(C) \leqslant 84(g-1)$.

Let $K := k(C)^{\mathrm{Aut}(C)}$ denote the fixed field of the $\mathrm{Aut}(C)$-action on $k(C)$.

(a) Show that K is a finitely-generated extension of k of transcendence degree 1 that contains no finite extensions of K, and therefore the function field of a nice curve Y over k. By Exercise (**I.3.2**), $\pi\colon C \to Y$ is a $\mathrm{Aut}(C)$-Galois cover and $Y = C/\mathrm{Aut}(C)$.

(b) Give a formula for $\#G$ in terms of g, g_Y, and the ramification of $\pi\colon C \to Y$ over its branch points.

(c) If the genus of Y is at least 1, derive an upper bound on $\#\,\mathrm{Aut}(C)$.

(d) If the genus of Y is 0, show that $\#\,\mathrm{Aut}(C) \leqslant 84(g-1)$.

(e) * Where did you use that the characteristic of the ground field was 0?

I.3.4 Suppose that $f\colon X \to Y$ is a G-cover of curves over k and assume that $\#G$ is coprime to the characteristic of k.

(a) Show that the subspace of differentials pulled back from Y lies in $H^0(X, K_X)^G$.

(b) Conversely, show that every G-invariant differential on X gives rise to a differential on Y.

(c) Show that the genus g_Y of Y can be computed as

$$g_Y = \dim H^0(X, K_X)^G.$$

[1] Compare this to Exercise (**I.1.6**), which computed the infinitessimal automorphisms.

Hyperelliptic curves. For this section, let Y be a nice curve of genus 0 and assume that C admits a degree 2 map to Y.

I.3.5 For what genera do there exist hyperelliptic curves?

I.3.6 For this problem, C is a nice hyperelliptic curve of genus at least 2.

(a) Suppose that L is a line bundle of degree 2 on C with $h^0(C, L) = 2$. Determine $h^0(C, nL)$ as a function of n.
(b) What can you say about $(g-1)L$? Describe $\varphi_{(g-1)L}$.
(c) If C is hyperelliptic of genus at least 2, show that the hyperelliptic map $C \to Y$ is unique.

The next two problems do these calculations (and more) explicitly.

I.3.7 Suppose that C has gonality 2. Let L be such that φ_L is a degree 2 map onto $\mathbb{P}^1_k$.

(a) Let $D_\infty = \varphi_L^*(\infty) \in \mathrm{Div}(C)$. Write $x \in k(C)$ for the pullback of a coordinate function such that $\{1, x\}$ form a basis for $H^0(C, D_\infty)$ (as in Exercise (**I.2.2**)). What is the relationship between D_∞ and L?
(b) Give a basis for $H^0(C, nD_\infty)$ for $n \leqslant g$.
(c) What does an explicit basis for $H^0(C, (g+1)D_\infty)$ look like?
(d) In terms of your previous answer, give a basis for $H^0(C, nD_\infty)$ for $g < n \leqslant 2g+1$. What happens when $n = 2g+2$?
(e) Assume that the characteristic of the ground field is not 2. Show that every nice curve of gonality 2 is birational to a plane curve with affine equation

$$y^2 = f(x) = a_{2g+2}x^{2g+2} + a_{2g+1}x^{2g+1} + \cdots + a_0. \tag{3}$$

Show that we may further assume that f is monic, square-free, and of degree $2g+2$ or $2g+1$. What happens in arbitrary characteristic?

I.3.8 Suppose that C_i is birational to the plane curve with equation

$$C_1 : y^2 = f_1(x) = x^{2g+2} + a_{2g+1}x^{2g+1} + \cdots + a_0,$$
$$C_2 : y^2 = f_2(x) = x^{2g+1} + b_{2g}x^{2g} + \cdots + b_0$$

for $g \geqslant 1$, where f_i is squarefree. We will refer to a curve of type C_1 as gonality 2 of even degree and type C_2 as gonality 2 of odd degree. (Or we will drop the pedantic "gonality 2" and simply refer to them as hyperellitpic of even/degree.) As in the previous problem, write $D_\infty := \varphi_L^*(\infty)$.

(a) Compute the ramification of the x-coordinate map using (1) and the equations of C_1 and C_2. Comment on the difference between these two situations. The closed points $P \in C$ for which $e_P > 1$ are called Weierstrass points of the hyperelliptic curve C.
(b) Compute the ramification divisor of the x-coordinate map using Riemann–Hurwitz by comparing the divisor of dx to the pullback of the divisor of the corresponding differential on $\mathbb{P}^1$.
(c) Show that the divisor of the differential dx/y is $(g-1)D_\infty$. Compare this to Exercise ((b)).
(d) Show that

$$\frac{dx}{y}, \frac{xdx}{y}, \frac{x^2dx}{y}, \ldots, \frac{x^{g-1}dx}{y}$$

form a basis for the space of regular differentials on C_i.

I.3.9 Assume that $g \geqslant 1$.

(a) Show that C is hyperelliptic if and only if $\mathrm{gon}(C_{\overline{k}}) = 2$.
(b) Show that if g is even, then $\mathrm{gon}(C) = 2$.

I.3.10 More generally, can you find (birational) equations for any hyperelliptic curve over k?

I.3.11 (Mumford coordinates on the Jacobian) Let $\pi\colon C \to \mathbb{P}^1_k$ be a gonality 2 curve of odd degree with affine equation $y^2 = f(x)$ and let L be a degree 0 line bundle on C. Write $\infty \in C$ for the unique point of C over $\infty \in \mathbb{P}^1_k$.

(a) Show that for some $d \leqslant g$, we have that $h^0(C, L(d\infty)) > 0$.
(b) Show that for the minimal such d, $h^0(C, L(d\infty)) = 1$. Call D the unique effective divisor linearly equivalent to $L(d\infty)$. Show:
   i. $\infty \notin \operatorname{supp}(D)$.
   ii. If $P \in \operatorname{supp}(D)$, then $\iota(P) \notin \operatorname{supp}(D)$ (where ι is the hyperelliptic involution).

   We will refer to such an effective divisor as general relative to π.
(c) Let D be an effective divisor of degree d on C that is general relative to π. Show that there exist unique polynomials $a(x), b(x) \in k[x]$ with a monic of degree d and $\deg(b) < d$ such that
   i. a divides $f - b^2$,
   ii. For all $P = (x_0, y_0) \in \operatorname{supp}(D)$,

$$a(x_0) = 0, \qquad b(x_0) = y_0.$$

   And the multiplicity of P in $\operatorname{supp}(D)$ is the order of vanishing of $a(x)$ at x_0.

   The pair $(a(x), b(x))$ are called Mumford coordinates for the divisor D. When $d \leqslant g$, the pair $(a(x), b(x))$ are caled the Mumford representation for the point $[\mathcal{O}(D - d\infty)] \in J(k)$.
(d) Suppose that (a, b) are Mumford coordinates for a divisor D. Describe the principal divisor $(y - b)$ on C.

I.3.12 (Group law on hyperelliptic Jacobians) In this problem we will explicitly see the group law on the Jacobian J of an odd degree gonality 2 curve $\pi\colon C \to \mathbb{P}^1$ using Mumford coordinates.

(a) Let L_1 and L_2 be line bundles on C, and suppose that D_1 and D_2 are the unique divisors of minimal degrees $d_1, d_2 \leqslant g$ such that $L_i \simeq \mathcal{O}(D_i - d_i\infty)$. By Exercise (**I.3.11**), these are general relative to π. Describe the line bundle

$$L = L_1 +_J L_2.$$

(b) Is the divisor $D = D_1 + D_2$ general relative to π? If not, how can you make it so?
(c) Let (a_i, b_i) be the Mumford coordinates of D_i (and hence the Mumford representation for L_i). Show that the following is an algorithm which terminates with the Mumford representation of $L_1 +_J L_2$:
   i. Let $e = \gcd(a_1, a_2, b_1 + b_2)$. Let $a = \frac{a_1 a_2}{e^2}$. Let b the unique polynomial of degree less than $\deg(a)$ such that

$$\frac{a_i}{e} \text{ divides } b - b_i, \qquad \text{and} \qquad a \text{ divides } f - b^2.$$

   ii. While $\deg(a) > g$:
      - Write $f - b^2 = \lambda ac$ for some $\lambda \in k^\times$ and c monic. Replace a with c.
      - Replace b with $-b$ modulo a.

I.3.13 (Explicit arithmetic in a hyperelliptic Jacobian) Let C be the odd degree hyperelliptic curve of genus 2 with affine equation

$$y^2 = x(x-1)(x-2)(x^2-3)$$

over $\mathbb{F}_5$.

(a) What are the Mumford coordinates of every point in $J(\mathbb{F}_5)[2]$?

(b) Let $P = (3, 1)$ be a point in $J(\mathbb{F}_5)$. What are the Mumford coordinates of P? What are the Mumford coordinates of $2P$? What are the Mumford coordinates of $3P$? What is the order of P in $J(\mathbb{F}_5)[2]$?

I.3.14 (Jacobian arithmetic in Magma) Given a hyperelliptic curve of odd degree, Magma represents points on the Jacobian via thier Mumford coordinates $P = (a, b, d)$, where a and b are the polynomials giving the Mumford representation of the effective divisor general with respect to the hyperelliptic map (c.f., Exercise (**I.3.11**)), and d records the (negative) multiple of ∞ (i.e., the degree of this divisor). For example, to create the previous curve and point P, one could type:

```
R<x> := PolynomialRing(GF(5));
C := HyperellipticCurve(x*(x-1)*(x-2)*(x^2-3));
J := Jacobian(C);
P := elt<J|x + 2, 1, 1>;
```

Using this, redo the previous problem in Magma.

I.3.15 Let $\pi\colon C \to \mathbb{P}^1$ be a gonality 2 curve.

(a) A line bundle L on a curve is called special if $h^1(C, L) > 0$. Show that every special line bundle on C is of the form

$$L = r \cdot \pi^* \mathcal{O}_{\mathbb{P}^1}(1) + L_0,$$

where $h^0(C, L_0) = 0$ and $r + 1 = h^0(C, L)$. Conclude that if L is special, then φ_L is never an embedding.

(b) Show that the smallest degree of an embedding of C into $\mathbb{P}^r$ is $g + r$ ($r \geqslant 3$ if $g \geqslant 2$).

Bielliptic curves.

A curve C is called bielliptic if it admits a degree 2 map to a nice curve of genus 1.

I.3.16 Let C be a nice curve. Show that C is bielliptic if and only if there exists an involution $\alpha \in \mathrm{Aut}(C)$ such that the induced action of α on the regular differential $H^0(C, K_C)$ has a 1-dimensional $+1$-eigenspace.

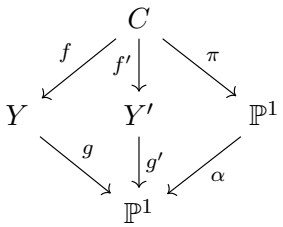
I.3.17 (Bielliptic genus 2 curves – adapted from Exercise 5.8 of [Poo]) Let C be a nice genus 2 curve over a field k of characteristic not 2. Write $\iota \in \mathrm{Aut}(C)$ for the hyperelliptic involution. Suppose that C has another involution $\alpha \in \mathrm{Aut}(C)$.

(a) Show that α and ι commute.

(b) Write $Y := C/\langle\alpha\rangle$ and $Y' := C/\langle\alpha\iota\rangle$ for the nice curves corresponding to the fixed fields of α and $\alpha\iota$ acting on $k(C)$ (c.f. Exercise (**I.3.2**)).

(c) Show that Y and Y' are of genus 1.

(d) Show that there is a diagram of finite covers:



(e) What is the ramification of the map $g' \circ f'\colon C \to \mathbb{P}^1$?

(f) Compute the ramification of g, g' and α. Show that there is a unique point in $\mathbb{P}^1$ that is a branch point of g and α. Show that this is a k-point.

(g) Prove that Y has affine equation

$$y^2 = h(x) = h_3x^3 + h_2x^2 + h_1x + h_0,$$

for some polynomial $h(x)$ of degree 3.

(h) Prove that C has affine equation $y^2 = h(x^2)$.

(i) Prove that Y' has affine equation

$$y^2 = h^{\mathrm{rev}}(x) = h_0x^3 + h_1x^2 + h_2x + h_3.$$

(j) Explicitly, what is the action of ι and α on the vector space $H^0(C, K_C)$? Verify the genus calculations you did.

(k) * Show that J_C is isogenous to $Y \times Y'$.

4. Curves on surfaces

Description of the canonical bundle: Adjunction.

The adjunction formula says that if $C \subseteq X$ is a nice curve on a nice surface, then

$$K_C = (K_X + C)|_C.$$

Smooth plane curves. In this section, unless otherwise stated, let $C \subseteq \mathbb{P}^2_k$ be a smooth plane curve of degree

$$\deg C = \deg \mathcal{O}_{\mathbb{P}^2}(1)|_C = d.$$

I.4.1 Show that $K_{\mathbb{P}^2} = \det \Omega^1_{\mathbb{P}^2/k} = \mathcal{O}_{\mathbb{P}^2}(-3)$.

I.4.2 (a) Give a formula for the canonical bundle K_C in terms of line bundles on $\mathbb{P}^2_k$.

(b) Prove the degree-genus formula

$$g = \frac{(d-1)(d-2)}{2}.$$

(c) When $d \geqslant 3$, prove that the canonical bundle K_C is $(d-3)$-very ample.

I.4.3 Compute the gonality of C.

I.4.4 (Explicit Adjuction) Suppose that the characteristic of k does not divide d and that $C \subseteq \mathbb{P}^2_k$ is the vanishing of a single homogeneous equation $F(X, Y, Z)$ of degree d.

(a) Show that symbolically

$$\frac{X \cdot dY - Y \cdot dX}{\partial F/\partial Z} = \frac{Y \cdot dZ - Z \cdot dY}{\partial F/\partial X} = \frac{Z \cdot dX - X \cdot dZ}{\partial F/\partial Y}.$$

(b) Using this, give an explicit basis for the space of global regular differentials on C.

I.4.5 Show that the smooth curve C in $\mathbb{P}^2_k$ with equation

$$X^4 + Y^4 = Z^4$$

is bielliptic.

I.4.6 For what degrees $d \leqslant 4$ do all automorphisms of a smooth plane curve of degree d come from automorphisms of $\mathbb{P}^2_k$?

I.4.7 If C is a smooth plane curve, write $\mathcal{O}_C(k)$ for the restriction of $\mathcal{O}_{\mathbb{P}^2}(k)$ to C. Show that every section of $\mathcal{O}_C(k)$ is the restriction of a section of $\mathcal{O}_{\mathbb{P}^2}(k)$. (This means that C is what is called projectively normal.)

Curves on Hirzebruch surfaces. In this section we make a brief foray into the geometry of surfaces, for the eventual purpose of understanding the curves on these surfaces. For that reason, this section requires a bit more background in algebraic geometry.

A Hirzebruch surface over Y is a surface S that is isomorphic (over k) to the projectivization of a rank 2 vector bundle on a nice genus 0 curve Y. (We use the Grothendieck convention for projective space: the fiber of $\mathbb{P}(E)$ over point $y \in Y$ is $\mathbb{P}(E_y)$, the space of codimension 1 subspaces in E_y.)

I.4.8 Show that every Hirzebruch surface over $\mathbb{P}^1_k$ is isomorphic to $\mathbb{F}_n$, the projective bundle $\mathbb{P}\left(\mathcal{O}_{\mathbb{P}^1} \oplus \mathcal{O}_{\mathbb{P}^1}(n)\right)$ over $\mathbb{P}^1_k$.

I.4.9 (a) Describe all maps of a curve C to the Hirzebruch surface $\mathbb{P}(E)$. (This should be, in part, reminiscent of the case of maps to projective space as in Exercise (**I.1.1**).)

(b) A section of a Hirzebruch surface S is a map $Y \xrightarrow{\sigma} S$, such that post-composition with the projection to Y is the identity. Describe all sections.

(c) Let $\sigma(Y)$ be a the image of a section of $S \to Y$. In terms of your description above, what is the self-intersection $\sigma(Y)^2$?

(d) For $n > 0$, show that the Hirzebruch surface $\mathbb{F}_n$ over $\mathbb{P}^1_k$ has a unique section with negative self-intersection. What is the self-intersection?

I.4.10 Let $n > 0$ and let C_n be the image of the unique section with negative self-intersection on $\mathbb{F}_n$. Let F be a fiber of $\mathbb{F}_n \to \mathbb{P}^1_k$ over a k-point of $\mathbb{P}^1_k$.

(a) Show that the Picard group of $\mathbb{F}_n$ is a free abelian group of rank 2 with generators C_n and F.

(b) What is the self-intersection of a curve in class $aC_n + bF$?

(c) Use adjunction on $\mathbb{F}_n$ to determine the canonical class $K_{\mathbb{F}_n}$.

I.4.11 Show that $\mathbb{F}_0 \simeq \mathbb{P}^1_k \times \mathbb{P}^1_k$.

(a) Show that the Picard group of $\mathbb{F}_0$ is the free abelian group with generators F_1 and F_2, the fibers over rational points under the two natural projections. Write $\mathcal{O}(a, b)$ for the line bundle $aF_1 + bF_2$.

(b) Let C be a smooth curve on $\mathbb{P}^1 \times \mathbb{P}^1$ with $\mathcal{O}(C) \simeq \mathcal{O}(a, b)$. What is the genus of C?

(c) What is the canonical class $K_{\mathbb{F}_0}$?

(d) What is $h^0(\mathbb{P}^1 \times \mathbb{P}^1, \mathcal{O}(a, b))$?

(e) Show that the line bundle $\mathcal{O}(1, 1)$ is very ample and describe the embedding into projective space this gives.

I.4.12 (a) (Castelnuovo–Severi inequality) Suppose that C has two independent maps to $\mathbb{P}^1$ of degrees d_1 and d_2. Then show that the genus g of C satisfies

$$g \leqslant (d_1 - 1)(d_2 - 1).$$

(b) Use the Castelnuovo–Severi inequality to give another proof that if $g \geqslant 1$, the hyperelliptic map on a curve of genus g is unique (up to obvious post-compositions with automorphisms on $\mathbb{P}^1$).

I.4.13 Consider $\mathbb{F}_1$.

(a) Show that the linear system associated to $C_1 + F$ is basepoint-free and describe the associated map.

(b) Show that $\mathbb{F}_1 \simeq \mathrm{Bl}_p \mathbb{P}^2_k$ for some point $p \in \mathbb{P}^2(k)$. What is the exceptional divisor of the blowup?

I.4.14 Consider $\mathbb{F}_2$. Show that the linear system associated to $C_2 + 2F$ is basepoint-free and describe the associated map.

I.4.15 Suppose that $Y(k) = \varnothing$. (However, $Y_{\overline{k}} \simeq \mathbb{P}^1_{\overline{k}}$, see Exercise (**I.2.6**).)

(a) Show that there exists a rank 2 vector bundle E on Y fitting in the exact sequence

$$0 \to \mathcal{O}_Y \to E \to T_Y \to 0,$$

which is indecomposable over k, but for which the base change $E_{\overline{k}} \simeq \mathcal{O}_{\mathbb{P}^1_{\overline{k}}}(1) \oplus \mathcal{O}_{\mathbb{P}^1_{\overline{k}}}(1)$.

(b) Show that every Hirzebruch surface over Y is isomorphic to $\mathbb{P}(E)$ or $\mathbb{P}(\mathcal{O}_Y \oplus (mK_Y))$. Which $\mathbb{F}_n$ are these isomorphic to over $\overline{k}$?

(c) Give a more down-to-earth description of $\mathbb{P}(E)$.

(Fun but unnecessary exercise: can you explicitly show that we cannot construct any other indecomposable bundles other than E (and its twists) as extensions of nT_Y by $\mathcal{O}_Y$ by showing that the subvarities of $\mathrm{Ext}^1(nT_Y, \mathcal{O}_Y)$ parameterizing such a splitting types have no rational points? For example: there are no rank 2 vector bundles on Y that geometrically split as $\mathcal{O}(1) \oplus \mathcal{O}(3)$ coming from $\mathrm{Ext}^1(2T_Y, \mathcal{O}_Y)$.)

5. Canonical curves of low genus

In this section, we will assume that C is a nice curve over a field k. Since we already know that if C is hyperelliptic, the canonical map is $2:1$ onto a degree $g-1$ and genus 0 curve in $\mathbb{P}^{g-1}$, we will also assume that C is not hyperelliptic.

I.5.1 Show that every nice curve C over a field k has:

(a) A closed point of degree at most $2g-2$ over k.

(b) Gonality at most $2g-2$.

(c) Infinitely many closed points of degree at most $2g-2$ over k.

Genus 3 curves.

I.5.2 Show that every non-hyperelliptic curve of genus 3 is a smooth plane quartic curve in $\mathbb{P}^2_k$ and conversely that every smooth plane quartic is a canonical curve of genus 3. What is the gonality of C?

I.5.3 * Can you match an "expected" dimension count for the moduli space of genus 3 curves with earlier calculations? Compare this with Exercise (**I.1.6**). What should be the codimension of the locus of hyperelliptic curves?

Genus 4 curves.

I.5.5 Suppose that C is a nice non-hyperelliptic curve of genus 4.

(a) Show that the canonical map is an embedding

$$\varphi_K : C \hookrightarrow \mathbb{P}^3_k.$$

(b) Show that C lies on a unique quadric surface Q. Show that this quadric has rank at least 3 (i.e., it is smooth or a quadric cone).

(c) Show that C lies on a cubic surface S over k. How unique is this surface?

(d) Show that C is the complete intersection of Q and S.

I.5.6 Show that every smooth complete intersection of a quadric surface and a cubic surface in $\mathbb{P}^3_k$ is a canonical curve of genus 4.

I.5.7 Suppose that C is a nice non-hyperelliptic curve of genus 4. If

$$f : C \to \mathbb{P}^1$$

is a map of degree 3, show that the fibers of f are 3 collinear points in $\mathbb{P}^3$ (i.e., in the canonical embedding). Show that the line through these points must be contained in the unique quadric containing C.

I.5.8 Suppose that the unique quadric Q containing C is a quadric cone (i.e., Q is the cone over a smooth plane conic X).

(a) Show that C admits a unique map of degree 3 to a genus 0 curve (over k and over $\overline{k}$). When is the gonality of C equal to 3?

(b) * Show that the blow up of Q at the cone point is a projective bundle over X. When X is $\mathbb{P}^1$, do you recognize Q as the image of a map from a Hirzebruch surface?

(c) * What is the class of C on this Hirzebruch surface?

I.5.9 Suppose that the unique quadric Q containing C is a smooth quadric.

(a) Over $\overline{k}$, $Q_{\overline{k}} \simeq \mathbb{P}^1 \times \mathbb{P}^1 = \mathbb{F}_0$. What is the class of $C_{\overline{k}}$ on this surface?

(b) Show that over $\overline{k}$, C admits two maps of degree 3 to a genus 0 curve. Describe these maps geometrically.

(c) Let L/k be the discriminant extension of the quadric Q over k; i.e., if Q is represented by a symmetric 4×4 matrix A, then

$$L = k\left(\sqrt{\det(A)}\right).$$

Show that over L, C_L admits two maps of degree 3 to genus 0 curves.

(d) Conversely show that if C admits a degree 3 map to a genus 0 curve over k, then $L = k$.

I.5.10 * Can you match an "expected" dimension count for the moduli space of genus 4 curves with earlier calculations? Compare this with Exercise (**I.1.6**). What should be the codimension of the locus of hyperelliptic curves?

Genus 5 curves.

I.5.11 Suppose that C is a nice non-hyperelliptic curve of genus 5.

(a) Show that the canonical map is an embedding

$$\varphi_K \colon C \hookrightarrow \mathbb{P}^4_k,$$

and exhibits C as a smooth curve of degree 8 and genus 5 in $\mathbb{P}^4_k$.

(b) Show that there is a 3-dimensional vector space of quadratic polynomials on $\mathbb{P}^4_k$ that vanish along C. Let Q_1, Q_2 and Q_3 be a choice of three independent quadrics spanning this space.

(c) Show that the complete intersection of three quadrics in $\mathbb{P}^4_k$ is always a canonical curve of genus 5.

(d) If $C_{\overline{k}}$ admits a degree 3 map to $\mathbb{P}^1_{\overline{k}}$, show that the ideal of C is *not* generated by Q_1, Q_2 and Q_3 (i.e., it is not the complete intersection).

I.5.12 Let C be a canonical curve of genus 5. Let Q_1, Q_2 and Q_3 be a choice of three independent quadrics spanning the space of quadrics vanishing along C.

(a) If $C \subsetneq V(Q_1, Q_2, Q_3)$, then show that $V(Q_1, Q_2, Q_3)$ has dimension 2.

(b) Let $S = V(Q_1, Q_2)$ be the surface cut out by the first two quadrics. If S is irreducible, show that any other quadric containing S must be a linear combination of Q_1 and Q_2.

(c) Conclude that if S is irreducible, $C = V(Q_1, Q_2, Q_3)$ is a complete intersection.

(d) Show that if S is reducible, it must be the union of a surface of degree 3 and a surface of degree 1. Which one contains C?

(e) A degree 3 surface is a minimal degree surface T called a cubic scroll. Such a surface is the image of a map from $\mathbb{F}_1$ or $\mathbb{F}_3$. What is this map?

(f) Give an intrinsic description of T in $\mathbb{P}^4$.

(g) Show that if C lies on T, then $\mathrm{gon}(C_{\overline{k}}) = 3$. Conclude that $C_{\overline{k}}$ does not admit a degree 3 map to $\mathbb{P}^1_{\overline{k}}$, then C is the complete intersection of three quadrics in $\mathbb{P}^3$.

I.5.13 Suppose that $\mathrm{gon}(C_{\overline{k}}) = 3$.

(a) Show that C lies on a cubic scroll T and find its class on T.
(b) Show that the degree 3 map $C_{\overline{k}} \to \mathbb{P}^1$ is unique.
(c) Show that $\mathrm{gon}(C) = 3$. (This should be somewhat surprising!)

I.5.14 Now suppose that $\mathrm{gon}(C_{\overline{k}}) > 3$. Then we know that C is the complete intersection of three quadrics in $\mathbb{P}^4_k$.

(a) Let Q be a singular quadric cone containing C. Show that a 2-plane in Q meets C in 4 geometric points. Show that the divisor of these four points defines a map of degree 4 from $C_{\overline{k}}$ to $\mathbb{P}^1_{\overline{k}}$.
(b) Show that if the locus of singular quadrics in the projective space $\mathbb{P}^2$ of quadrics containing C is smooth, then the variety parameterizing degree 4 maps from C to $\mathbb{P}^1$ is a curve of genus 11.
(c) * Explicitly, what is this curve? (E.g., can you write down equations for its function field in terms of equations for C?)

I.5.15 * Can you match an "expected" dimension count for the moduli space of genus 5 curves with earlier calculations? Compare this with Exercise (**I.1.6**). What should be the codimension of the locus of hyperelliptic curves? What should be the codimension of the locus of trigonal curves?

Genus at least 6 curves.

I.5.16 Show that a canonical curve $C \subseteq \mathbb{P}^{g-1}$ with $g \geqslant 6$ is never a complete intersection.

I.5.17 * (If you know something about del Pezzo surfaces) Descriptions of *general* canonical curves of genus up to 10 are known, partly worked out in a series of papers Mukai [Muk92, Muk95, Muk10].

(a) Fill in the details for the following: a general canonical curve of genus 6 is a transverse quadric section of a del Pezzo surface of degree 5 in $\mathbb{P}^5$.
(b) What does general mean in the previous sentence?
(c) Can you give a description of *every* canonical curve of genus 6?

I.5.18 * Try to generalize the results about geometrically trigonal curves: is it true that if $\mathrm{gon}(C_{\overline{k}}) = 3$ and the genus of C is odd and at least 5, then $\mathrm{gon}(C) = 3$?

CHAPTER 2

Arithmetic

For this section, we focus on the technique of descent for understanding the rational points on a variety. Most of the exercises in the first part of this chapter are done is greater generality than needed in the second part, since this is a robust technique that appears in other contexts. We assume familiarity with (non-abelian) Galois cohomolgy, for example as in [Ser97].

- As in the first chapter, k will denote a perfect field, and $\overline{k}$ an algebraic closure.

1. Twists and Torsors

Twists.

- We always use the left action of $\mathrm{Gal}(\overline{k}/k)$ on k, giving a right action on $\operatorname{Spec} k$.

II.1.1 Let X be a k-scheme and let $\sigma \in \mathrm{Aut}(k)$, which induces a map $\operatorname{Spec} k \xrightarrow{\sigma} \operatorname{Spec} k$. Write ${}^{\sigma}X$ for the pullback of X over $\operatorname{Spec} k$ under this map:

$$\begin{array}{ccc} {}^{\sigma}X & \longrightarrow & X \\ \downarrow & & \downarrow \\ \operatorname{Spec} k & \xrightarrow{\sigma} & \operatorname{Spec} k \end{array}$$

(The left vertical map is *not* an morphism of k-schemes if σ is nontrivial!)

(a) Suppose that X is an affine variety cut out by equations $g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_m)$. Give equations for ${}^{\sigma}X$.

(b) Show that ${}^{\sigma}X(k)$ is in bijection with $X(k)$. (In the affine case, as above, can you make this explicit?)

(c) More generally, let S be any k-scheme. Give a bijection

$$\begin{aligned} X(S) &\to {}^{\sigma}X(S) \\ f &\mapsto {}^{\sigma}f \end{aligned}$$

(d) * While ${}^{\sigma}X$ and X are isomorphic as abstract schemes, give an example of X and σ for which ${}^{\sigma}X$ and X are *not* isomorphic as k-schemes.

II.1.2 Let k'/k be a finite Galois extension. Suppose that X is a k-scheme. Show that there exists a collection of isomorphisms $(f_\sigma)_{\sigma \in \mathrm{Gal}(k'/k)}$ of k'-varieties

$$f_\sigma \colon {}^{\sigma}X_{k'} \to X_{k'},$$

such that for all $\sigma, \tau \in \mathrm{Gal}(k'/k)$

$$f_{\sigma\tau} = f_\sigma {}^{\sigma}(f_\tau). \tag{4}$$

In other words, such that the following diagram commutes.

$$\begin{array}{ccccc} {}^{\sigma\tau}X_{k'} & \xrightarrow{{}^{\sigma}(f_\tau)} & {}^{\sigma}X_{k'} & \xrightarrow{f_\sigma} & X_{k'} \\ & \searrow & & \nearrow & \\ & & f_{\sigma\tau} & & \end{array}$$

II.1.3 (Necessity of Condition (4) – adapted from Exercise 4.1 of [Poo17]) Let $\sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ be complex conjugation. Suppose that $a_0, \ldots, a_6 \in \mathbb{C}$ are such that

$$^{\sigma}a_{6-j} = (-1)^{j+1}a_j.$$

Let X be the hyperelliptic curve with affine equation

$$y^2 = f(x) = a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0,$$

over $\mathbb{C}$. Assume that $f(x)$ is separable and $\mathrm{Aut}(X) = \mathbb{Z}/2\mathbb{Z}$ generated by the hyperelliptic involution.

(a) What is the equation of $^{\sigma}X$? Show that $^{\sigma}X$ is isomorphic to X as curves over $\mathbb{C}$.
(b) Show that X is not the base-change of a curve from $\mathbb{R}$ to $\mathbb{C}$.
(c) Show that the hypotheses on f and $\mathrm{Aut}(X)$ can be satisfied for some choice of parameters $a_0, \ldots, a_6 \in \mathbb{C}$.

II.1.4 Let k'/k be a finite Galois extension and let X' be a quasi-projective k'-variety. A k'/k-descent datum on X' is a collection of k'-isomorphisms $(f_\sigma)_{\sigma\in\mathrm{Gal}(k'/k)}$ satisfying (4).

(a) Formulate what a morphism of k'-schemes with k'/k-descent data is. What is an *iso*morphism?
(b) By Weil's Galois descent, there is an equivalence of categories

$$\left\{\begin{array}{c}\text{quasi-projective}\\ k\text{-varieties}\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{quasi-projective } k'\text{-varieties}\\ \text{with } k'/k\text{-descent data}\end{array}\right\}.$$

If X is a k-variety, what should be the corresponding k'-variety with k'/k-descent data corresponding to it?
(c) Given that k'/k-descent data for X' exists, show that the set of all k'/k-descent data is *non-canonically* isomorphic to $H^1(\mathrm{Gal}(k'/k), \mathrm{Aut}(X'))$.

II.1.5 Varieties X and Y over k are called twists (or forms) of each other if $X_{\overline{k}} \simeq Y_{\overline{k}}$. Given an extension k'/k, we say that X and Y are k'/k-twists of each other if $X_{k'} \simeq Y_{k'}$. A twist Y of X *together with* a choice of isomorphism $\varphi\colon X_{k'} \to Y_{k'}$ will be called a rigidified twist.

(a) Let k'/k be a finite Galois extension. Explicitly show that the set of rigidified k'/k-twists of a k-variety X are in bijection with 1-cocycles

$$\mathrm{Gal}(k'/k) \to \mathrm{Aut}(X_{k'}).$$

(b) Show that isomorphism classes of twists of X are *canonically* isomorphic to the pointed set $H^1(k, \mathrm{Aut}(X_{k'}))$.

Classification of torsors under smooth algebraic groups over a field.

- For this section, let G be a smooth algebraic group over the perfect field k. Every such group is quasiprojective.
- Recall that a morphism of algebraic groups is a morphism of the underlying varieties that respects the structure morphisms (multiplication, inversion, and identity).
- The trivial G-torsor over k, denoted $\underline{\mathbf{G}}$, is the variety G together with the right action of G on itself by translation.
- A G-torsor is a twist of $\underline{\mathbf{G}}$, i.e., a variety X over k with a right G-action such that $X_{\overline{k}}$ with the right action of $G_{\overline{k}}$ is isomorphic to $\underline{\mathbf{G}}_{\overline{k}}$.

II.1.6 Show that if X is a G-torsor over k, then $X(\overline{k})$ is a set with a simply transitive right $G(\overline{k})$-action.

II.1.7 Show that a G-torsor X over k is isomorphic to $\underline{\mathbf{G}}$ if and only if $X(k) \neq \varnothing$.

II.1.8 Show that the automorphism group scheme of $\underline{\mathbf{G}}$ over k is isomorphic to G acting on $\underline{\mathbf{G}}$ by translation on the left. Conclude that $\mathrm{Aut}(\underline{\mathbf{G}}) \simeq G(k)$.

II.1.9 (a) Show that the set of isomorphism classes of G-torsors over k are in bijection with the pointed set
$$H^1(k, G) := H^1(k, G(\overline{k})).$$
(In addition, can you explicitly write down a cocycle representing the cohomology class of a given torsor? Exercise (**II.1.6**) might be helpful.)
(b) Show that a torsor is isomorphic to $\underline{\mathbf{G}}$ if and only if its cohomology class is the neutral element of $H^1(k, G)$.

II.1.10 Show that every $\mathbb{G}_m$- or $\mathbb{G}_a$-torsor over k is trivial.

II.1.11 Let L/k be a finite Galois extension with Galois group G. Show that $\operatorname{Spec} L$ is a G-torsor over $\operatorname{Spec} k$.

II.1.12 Let C be a nice curve over k, and assume, to make technical issues with the Picard functor disappear, that $C(k) \neq \varnothing$. Show that the degree e component $\mathrm{Pic}^e_{C/k}$ is a $\mathrm{Pic}^0_{C/k}$-torsor.

II.1.13 (Twists arising from torsors) Let G be an algebraic group over k and let X be a nice variety over k. Suppose that G acts on X on the left.
(a) First, describe "abstractly" a map $H^1(k, G) \to H^1(k, \operatorname{Aut} X_{\overline{k}})$.
(b) Given a G-torsor T, the contracted product $T \times^G X$ is the quotient of $T \times_k X$ by the free G-action
$$(t, x) \mapsto (tg^{-1}, gx).$$
Show that $[T \times^G X]$ is the image of $[T]$ under the map you described above.
(c) G acts on $\underline{\mathbf{G}}$ on the left by Exercise (**II.1.8**). Describe the map from the first part in this case.

II.1.14 (Inner twists) Let G be an algebraic group over k with the action on itself by conjugation.
(a) Using the action of inner automorphisms, describe a map of pointed sets
$$H^1(k, G) \to H^1(k, \operatorname{Aut} G_{\overline{k}}).$$
The twist G^τ corresponding to a class $\tau \in H^1(k, G)$ is called an inner twist of G.
(b) In terms of a cocycle in $Z^1(k, G)$, write down a cocycle representing the corresponding inner twist of G.
(c) Is G^τ a G-torsor?
(d) What happens if G is commutative?

II.1.15 (Left actions) If T is a (right) G-torsor with class $[T] = \tau \in H^1(k, G)$, show that T is a left G^τ-torsor. (So it is a G^τ, G-bitorsor.)

II.1.16 (Inverse torsors) Given a (right) G-torsor T with class τ, how can you produce a (right) G^τ-torsor? This will be called T^{-1}. (This will be a G, G^τ-bitorsor.) What happens if G is commutative?

II.1.17 (Contraction product) As you saw in Exercise (**II.1.13**), if T is a (right) G-torsor and X has a left-action of G, we can define the contraction product $T \times^G X$ as the quotient of $T \times X$ by the G-action $(t, x) \mapsto (tg^{-1}, gx)$. Similarly, if T is a left G-torsor, and X has a right action of G, we define $X \times^G T$ as the quotient by $(x, t) \mapsto (xg, g^{-1}t)$.

Show that if Z is a right G-torsor, and T is a G, H-bitorsor, then $Z \times^G T$ is a right H-torsor.

II.1.18 (a) Show that $T^{-1} \times_k^{G^\tau} T$ is the trivial right G-torsor. (And similarly, $T \times_k^G T^{-1}$ is the trivial G^τ-torsor.)

(b) Show that the contraction product map

$$H^1(k,G) \to H^1(k,G^\tau)$$
$$[Z] \mapsto [Z \times_k^G T]$$

is a bijection of pointed sets. What is the inverse?

Torsors over more general bases.

- More generally, we can consider families of torsors under a smooth algebraic group G over a field; i.e., a torsor over a base scheme S.
- For the problems in this problem set, it will suffice to consider group schemes over S that are of the form $G_S := G \times_k S$ for G a (smooth) algebraic group over k. We will also assume that G is affine or an abelian variety (and S is sufficiently nice) to do away with technical representability problems.
- A (right) G-torsor over S (also called by some authors an S-torsor under G_S) is an S-scheme X with a right action of G

$$X \times G \to X$$
$$(x,g) \mapsto xg$$

(as S-schemes!) such that there exists an étale cover $\{S_i\} \to S$ and an isomorphism

$$X \times_S S_i \quad \simeq \quad G \times_k S_i$$

of S_i-schemes.
- Under our assumptions the first Cech étale cohomology

$$H^1(S,G) := \check{H}^1_{\text{ét}}(S,G)$$

parameterizes G-torsor over S up to isomorphisms. (If you aren't familiar with this, use your intuition from the case k a field and take this as a working definition of this pointed set.)

II.1.19 How does the definition of a G-torsor over S square with the definition of a torsor over a field?

II.1.20 (Étale Galois covers, compare with Exercise (**II.1.11**))

(a) Let G be a finite group and suppose that $Y \to X$ is an étale G-cover of curves (c.f. Exercise (**I.3.2**)). Show that Y is a G-torsor over X for the constant algebraic group G.

(b) * Why is the étale assumption necessary?

(c) What if $Y \to X$ is defined over k, but is only *geometrically* a G-cover, for some constant group G?

II.1.21 (Homogeneous spaces) Let G be a (smooth) algebraic group over k and let H be a closed (smooth) algebraic subgroup. Suppose that the quotient $X = G/H$ exists. (This is guaranteed if G is affine or H is finite.) Show that G is an H-torsor over X.

II.1.22 (Twisted torsor) Let G be an algebraic group over k and let $Z \to S$ be a (right) G-torsor over S. Suppose that T is a right G-torsor over k with class τ. Define

$$Z^\tau := Z \times_k^G T^{-1},$$

where $Z \times_k^G T^{-1}$ is the quotient of $Z \times_k T^{-1}$ by the free action of G acting on the right on Z by g and acting on the left on T^{-1} by g^{-1}.

(a) Using the way that G acts on the left on T^{-1}, show that, explicitly, Z^τ is quotient of $Z \times_k T$ by $(z,t) \mapsto (zg, tg)$.

(b) Show that Z^τ is a right G^τ-torsor over S.

(c) Let $s\colon \operatorname{Spec} k \to S$ be a point. Show that the fiber Z_s^τ is the trivial G^τ-torsor if and only $[Z_s] = \tau \in H^1(k, G)$.

II.1.23 (n-coverings of abelian varieties) Let A be an abelian variety, and assume that the characteristic of k is coprime to n. A n-covering of A is a pair (X, ψ), where X is an A-torsor over k, and $\psi\colon X \to A$ is a map such that $\psi(xa) = \psi(x) + na$.

(a) Show that by the map $\psi\colon X \to A$, the variety X is an $A[n]$-torsor over A.
(b) Let τ be the class of $\psi^{-1}(e)$ in $H^1(k, A[n])$, for the identity point $e \in A$. Show that the twisted torsor X^τ is isomorphic to A.
(c) The group A acts on itself by translations (we don't need to be careful about left/right because it is abelian!) In this way, under the multiplication-by-n map $A \to A$, the first copy of A acts on the second copy of A (an element g acts as translation by ng). As in Exercise (**II.1.17**), show that the resulting contraction product $X \times_k^A A$, i.e., defined as the quotient of $X \times_k A$ by the $g \in A$ action

$$(x, a) \mapsto (xg^{-1}, a + ng)$$

is an A-torsor over k. In fact, show that

$$\begin{aligned} X \times_k^A A &\to A \\ (x, a) &\mapsto \psi(x) + a, \end{aligned} \tag{5}$$

is an isomorphism of A-torsors (and hence it is the trivial torsor). Let e be the identity element of A. Show that the following is a map of A-torsors

$$\begin{aligned} X &\to X \times_k^A A \\ x &\mapsto (x, e), \end{aligned}$$

and that composition with the isomorphism (5) is the n-covering map ψ.

Unramified torsors. In this section, we make the following simplifying/necessary assumptions.

- Let k be a number field and let $v \in \Omega_k$ be a place. Write $\mathcal{O}_v$ for the valuation ring of k_v.
- Let G be a *finite étale* algebraic group over k. Assume that $S \subset \Omega_k$ is a finite subset of places such that G spreads out to a finite étale group scheme $\mathscr{G}$ over $\mathcal{O}_{k,S}$.
- For a prime $v \notin S$, we say that $\tau \in H^1(k, G)$ is unramified at v if the restriction $\operatorname{res}_v(\tau)$ to k_v is in the image of the map

$$H^1(\mathcal{O}_v, \mathscr{G}) \to H^1(k_v, G)$$

restricting to the generic point.
- Using descent, one can show that if τ is unramified at all $v \notin S$ (i.e., unramified outside S), then τ is in the image of

$$H^1(\mathcal{O}_{k,S}, \mathscr{G}) \to H^1(k, G).$$

- Write $H^1_S(k, G) \subset H^1(k, G)$ for the set of τ that are unramified outside S.

II.1.24 Show that if a $\tau \in H^1(k, G)$ is unramified at v, then

$$\operatorname{res}_v(\tau) \in \ker\left(H^1(k_v, G) \to H^1(k_v^{\mathrm{nr}}, G)\right),$$

where k_v^{nr} is the maximal unramified extension of k_v.

II.1.25 Let S be a finite subset of Ω_k. Show that $H^1_S(k, G)$ is finite:

(a) As a k-scheme, what is a class $\tau \in H^1(k, G)$? (c.f. Exercise (**II.1.11**))
(b) For $v \notin S$, as an $\mathcal{O}_v$-scheme what is a class in $H^1(\mathcal{O}_v, \mathscr{G})$? What does it tell you about part (a) to know that $\operatorname{res}_v(\tau)$ is in the image of $H^1(\mathcal{O}_v, \mathscr{G})$?

(c) Show that the fibers of the map

$$H^1_S(k,G) \to \prod_{v\in S} H^1(k_v,G)$$

are finite.

(d) Show that $H^1(k_v,G)$ is finite.

II.1.26 Let $S=\{\infty,2,p_1,\dots,p_n\}$ be a finite set of rational primes. Describe the set $H^1(\mathbb{Q},\mu_2)$ and the (finite!) subset $H^1_S(\mathbb{Q},\mu_2)$.

2. Descent

Evaluation.

Given a morphism, $\varphi\colon T\to S$, we have by functoriality a map

$$H^1(S,G)\xrightarrow{\varphi^*} H^1(T,G)$$

defined by sending the class $[X]$ of a G-torsor over S to the class $[X_T]$ is called evaluation along T.

II.2.1 (Soft question) Describe the evaluation map along rational points $s\colon \operatorname{Spec} k\to S$:

(a) First, in words, for any G-torsor over S.

(b) If G is a constant finite group scheme over S (c.f., Exercise (**II.1.20**)).

(c) When G is an algebraic group, H is a finite subgroup, and $X=G$, considered as an H-torsor over $S=G/H$. (It might also be helpful to first think through the case that S is a *(finite) group* and G is a finite subgroup.)

II.2.2 Suppose that H is a finite étale subgroup of the algebraic group G.

(a) Since

$$1\to H(\overline{k})\to G(\overline{k})\to G/H(\overline{k})\to 1$$

is an exact sequence of $\mathrm{Gal}(\overline{k}/k)$-sets, show that we have an exact sequence in Galois cohomology

$$1\to H(k)\to G(k)\to G/H(k)\xrightarrow{\delta} H^1(k,H(\overline{k}))\to H^1(k,G(\overline{k}))$$

(b) Show that the boundary map δ agrees with the evaluation map at k-points you described in Exercise (**II.2.1**).

II.2.3 (Descent partition of rational points) Let G be a (smooth) algebraic group over k and suppose that Z is a G-torsor over a base scheme X. Then evaluation gives a partition of the rational points $X(k)$: write $X^\tau(k)$ for the subset of points

$$X^\tau(k)\colon \left\{x\in X(k) : [Z_x]=\tau\in H^1(k,G)\right\}.$$

(a) Show that equivalently $X^\tau(k)=f^\tau(Z^\tau(k))$, for $f^\tau\colon Z^\tau\to X$ the twisted torsor $Z\times_k^G T^{-1}$ (c.f. Exercise (**II.1.22**)). Therefore

$$X(k)=\bigcup_{\tau\in H^1(k,G)} f^\tau(Z^\tau(k)).$$

(b) Show that if X is proper over a number field k, then every rational point on X is the image of a rational point on one of a *finite* number of twists of Z.

II.2.4 (Chevalley-Weil Theorem) Suppose that

$$f\colon Z \to X$$

is a finite étale cover of proper varieties over a field k. Show that there exists a finite extension k'/k such that

$$X(k) \subseteq f(Z(k')).$$

Classical descent by n-isogeny.

Let A be an abelian variety over a number field k. Write

$$A[n] := \ker\left(A \xrightarrow{n} A\right)$$

for the finite group scheme of n-torsion points on A. We will write $A[n](k')$ for the points of $A[n]$ over k' (i.e., the n-torsion points defined over k').

II.2.6 (You may have already done this exercise in various parts in previous problems!)

(a) Show that there is an exact sequence of G_k-modules

$$0 \to A[n](k) \to A(k) \xrightarrow{n} A(k) \xrightarrow{\delta} H^1(k, A[n](\overline{k}))$$

(b) Show that $A \xrightarrow{n} A$ is an $A[n]$-torsor over A.

(c) Show that δ is the "evaluation map" of the previous section (c.f., (**II.2.2**)).

II.2.7 (The weak Mordell–Weil Theorem) Show that $A(K)/nA(K)$ is finite for every n.

II.2.8 (The descent lemma) Let Γ be a $\mathbb{Z}$-module and let V be a $\mathbb{Q}$-vector space containing $\Gamma/\Gamma_{\text{tors}}$. Let $x \mapsto Q(x)^2 \in \mathbb{R}$ be a positive quadratic form on V. For some $n \geqslant 2$, let $\gamma_i \in \Gamma$ be representatives of $\Gamma/n\Gamma$. Suppose that $Q(\gamma_i)$ is at most a positive constant C for all i.

(a) Given an element y and suppose that $Q(y) \leqslant mC$. If we write $y = nx + \gamma_i$, give a bound on $Q(x)$.

(b) Show that Γ is generated by elements x with $Q(x) \leqslant 2C$.

(c) (If you know about heights...) Let A be an abelian variety over a number field K. Show that an appropriate height function on $\Gamma = A(K)$ gives the quadratic form Q. (Or assume this.) Show that $A(K)$ is finitely generated.

Explicit 2-descent on hyperelliptic Jacobians.

The questions in this section will lead you through a proof that a *bound* for the rank of the Jacobian of a hyperelliptic curve over a number field k of odd degree is computable. For this reason, the questions are intended to be done in order.

- For this section J denotes the Jacobian of an odd degree hyperelliptic curve C over k with affine equation
$$y^2 = f(x), \qquad \deg(f) = 2g + 1.$$
Since $C(k) \neq \varnothing$, we have that $J(k) = \mathrm{Pic}^0(C)$ is the set of line bundles on C.
- Write ∞ for the unique place of C over ∞ in $\mathbb{P}^1$ under the hyperelliptic x-coordinate map.
- Recall that for a finite set of places $S \subseteq \Omega_k$, the set $H^1_S(k, J[2])$ denotes the isomorphism classes of torsors for $J[2]$ unramified outside S.

II.2.9 (Warmup: 2-descent on an elliptic curve with rational 2-torsion) For this problem, let E be an elliptic curve over $\mathbb{Q}$ with full rational 2-torsion, i.e., with Weierstrass equation

$$E\colon y^2 = (x - e_1)(x - e_2)(x - e_3), \qquad e_1, e_2, e_3 \in \mathbb{Q}.$$

(a) Describe the group scheme $E[2]$. Show that

$$H^1(\mathbb{Q}, E[2]) \simeq \mathbb{Q}^\times/\mathbb{Q}^{\times 2} \times \mathbb{Q}^\times/\mathbb{Q}^{\times 2}.$$

For some prime p, explicitly, what classes are unramified at p?

(b) What is the Galois cohomology $H^1(\mathbb{Q}_p, E[2])$ for each prime $p \leqslant \infty$? (The prime ∞ is to be interpreted as the Archimedean place, so that $\mathbb{Q}_\infty = \mathbb{R}$.)

(c) Show that the multiplication-by-2 map $E \xrightarrow{2} E$ corresponds to the function field extension

$$\begin{array}{c} \mathbb{Q}(x,y,z,w)/y^2 - (x-e_1)(x-e_2)(x-e_3), z^2 - (x-e_1), w^2 - (x-e_2) \\ \big\downarrow \\ \mathbb{Q}(x,y)/y^2 - (x-e_1)(x-e_2)(x-e_3) \end{array}$$

(Warning: this is easier to prove over an algebraically closed field. Over $\mathbb{Q}$, how do you know that the field extension is not $z^2 - \lambda(x-e_1)$ for some $\lambda \in \mathbb{Q}^\times \smallsetminus \mathbb{Q}^{\times 2}$, for example?)

(d) Can you explicitly give equations for all 2-covers of E? (These correspond to classes in $H^1(\mathbb{Q}, E[2])$ by Exercise (**II.1.23**), so the answer should depend on how you answered part (a).)

(e) Show that the descent map δ from the previous section is explicitly given by

$$\begin{array}{ll} E(\mathbb{Q}) \to H^1(\mathbb{Q}, E(\mathbb{Q})) \simeq \mathbb{Q}^\times/\mathbb{Q}^{\times 2} \times \mathbb{Q}^\times/\mathbb{Q}^{\times 2} \\ (x_0, y_0) \qquad\qquad\qquad \mapsto (x_0 - e_1, x_0 - e_2) \end{array} \tag{6}$$

for all affine points with $y_0 \neq 0$. What happens for the remaining points on E?

(f) Describe the descent partition of rational points on E.

(g) Let S be the set consisting of the infinite place ∞ and all finite p which divide $e_i - e_j$ for some $i \neq j \in \{1, 2.3\}$. (Since at least two e_i have the same parity, the prime 2 is always in S!) Show that the image of δ lies in $H^1_S(\mathbb{Q}, E[2])$.

(h) Using part (e), give a bound on the rank of any elliptic curve with full 2-torsion in terms of the number of primes in S.

II.2.10 (Explicit 2-descent on an elliptic curve) For this question, let E be the elliptic curve with Weierstrass equation

$$E\colon y^2 = x(x-1)(x+1).$$

(This curve is one of first examples of congruent number elliptic curves. The calculation you are about to do shows that 1 is not a congruent number.)

(a) Look for some points on E by testing x and y values in a box.

(b) Show that $S = \{\infty, 2\}$. Describe $H^1_S(\mathbb{Q}, E[2])$ as explicitly as you can.

(c) Now consider the real place. Show that $\mathbb{R}^\times/\mathbb{R}^{\times 2} \simeq \{\pm 1\}$. Show that $E(\mathbb{R})/2E(\mathbb{R})$ has cardinality two. Identify its image under δ_∞:

$$E(\mathbb{R})/2E(\mathbb{R}) \xrightarrow{\delta_\infty} H^1(\mathbb{R}, E[2]) \simeq \{\pm 1\} \oplus \{\pm 1\}.$$

(d) Using the diagram,

$$\begin{array}{ccc} E(\mathbb{Q})/2E(\mathbb{Q}) & \xhookrightarrow{\delta} & H^1_S(\mathbb{Q}, E[2]) \\ \big\downarrow & & \big\downarrow \\ E(\mathbb{R})/2E(\mathbb{R}) & \xhookrightarrow{\delta_\infty} & \{\pm 1\} \oplus \{\pm 1\} \end{array}$$

what are the local conditions coming from ∞?

(e) Now consider the place 2. Find representatives for $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$. $E(\mathbb{Q}_2)/2E(\mathbb{Q}_2)$ has cardinality 8. Identify its image under δ_2:

$$E(\mathbb{Q}_2)/2E(\mathbb{Q}_2) \xrightarrow{\delta_2} H^1(\mathbb{Q}_2, E[2])$$

in terms of your generators. What are the analogous local conditions coming from 2?

(f) Show using your local conditions that E has rank 0. (Can you compute the torsion points also to determine $E(\mathbb{Q})$?)

II.2.11 As you can see, in the previous problem two problems, it was very helpful to know the size of $E(\mathbb{Q}_p)/2E(\mathbb{Q}_p)$ to determine the image of δ_p.

(a) Show that the dimension of $E(\mathbb{R})/2E(\mathbb{R})$ as an $\mathbb{F}_2$-vector space is given by $\dim_{\mathbb{F}_2} E(\mathbb{R})[2]-1$. What happens in general for a Jacobian J at a real place?

(b) If $p \neq 2$, show that the dimension of $E(\mathbb{Q}_p)/2E(\mathbb{Q}_p)$ as an $\mathbb{F}_2$-vector space is $\dim_{\mathbb{F}_2} E(\mathbb{Q}_p)[2]$. What happens in general for a Jacobian J at a finite place not dividing 2?

(c) Show that the dimension of $E(\mathbb{Q}_2)/2E(\mathbb{Q}_2)$ as an $\mathbb{F}_2$-vector space is $\dim_{\mathbb{F}_2} E(\mathbb{Q}_2)[2]+1$. What happens in general for a Jacobian J at a place above 2?

II.2.12 (Another 2-descent) Let E be the elliptic curve with Weierstrass equation

$$E\colon y^2 = x(x-5)(x+5).$$

(E is another congruent number curve.) Repeat Exercise (**II.2.10**) with this curve. What can you say about its rank?

We're now ready to start doing this is general, for Jacobians of odd degree hyperelliptic curves!

II.2.13 ($J[2](\overline{k})$ as a G_k-module) Let $w_1, \dots, w_{2g+1}$ denote the zeros of $f(x)$ and let $W_i = (w_i, 0)$ be the corresponding Weierstrass point on C. Write $\mathscr{W} = \{W_1, \dots, W_{2g+1}\}$ for the set of all such points. Let $L = k[T]/f(T)$ denote the étale algebra determined by the polynomial f.

(a) Describe the étale algebra L. What happens if f splits completely? What happens if f is irreducible over k? Describe the norm map $N_{L/k}$. What does $\overline{L} = L \otimes_k \overline{k}$ look like?

(b) Write $\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{\mathscr{W}}$ for the trivial Galois-module $\mathbb{Z}/2\mathbb{Z}$ induced from L to k. (As an $\mathbb{F}_2$-vector space, what is the dimension of this module?) Show that there is a surjective map of G_k-modules

$$\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{\mathscr{W}} \to J[2]$$

sending W_i to the line bundle $\mathcal{O}_C(W_i - \infty)$.

(c) Identify the kernel to give an exact sequence of G_k-modules

$$0 \to \frac{\mathbb{Z}}{2\mathbb{Z}} \to \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{\mathscr{W}} \to J[2] \to 0$$

Show that this sequence splits.

(d) Give a formula for the $\mathbb{F}_2$-dimension of $J(k)[2]$.

(e) Show that

$$H^1(k, \mathbb{Z}/2\mathbb{Z}) \simeq k^\times/{k^\times}^2, \qquad \text{and} \qquad H^1\left(k, \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{\mathscr{W}}\right) \simeq \frac{L^\times}{{L^\times}^2}.$$

(f) Show that

$$H^1(k, J[2]) \simeq \ker\left(\frac{L^\times}{{L^\times}^2} \xrightarrow{N_{L/k}} \frac{k^\times}{{k^\times}^2}\right),$$

where $N_{L/k}$ is the norm map from L to k.

(g) Think through how the computations in this problem specialize when $J = E$ is an elliptic curve with full 2-torsion over $\mathbb{Q}$.

II.2.14 (The $x - T$ map) Write T for the image of T from $\overline{k}[T]$ in $\overline{L}$.

(a) Write $\mathrm{Div}_\perp C$ for the group of divisors on C whose support is disjoint from $\mathscr{W} \cup \{\infty\}$. Show that the map

$$\begin{array}{rcl} C(\overline{k}) \smallsetminus (\mathscr{W} \cup \{\infty\}) & \to & \overline{L}^\times \\ P & \mapsto & x(P) - T \end{array} \tag{7}$$

gives rise to a homomorphism

$$\mathrm{Div}_\perp C \to L^\times.$$

We call this map the $x - T$ map (for obvious reasons!)

(b) Show that if $D \in \mathrm{Div}_\perp C$ is principal, then $(x-T)(D) \in {L^\times}^2$.

(c) Show that the $x - T$ map extends to a well-defined map on all of $\mathrm{Pic}^0(X)$

$$J(k) = \mathrm{Pic}^0(X) \to \frac{L^\times}{{L^\times}^2}.$$

(d) Suppose that f is reducible with factors f_1 and f_2. Write $D_1 = W_1 + \cdots + W_r$ for the sum of Weierstrass points with x coordinate a root of f_1. Can you say where the line bundle $\mathcal{O}(D_1 - r\infty)$ is sent under this map?

(e) In fact, show that the image of $x - T$ is contained in

$$\ker\left(\frac{L^\times}{{L^\times}^2} \xrightarrow{N_{L/k}} \frac{k^\times}{{k^\times}^2}\right).$$

(f) (If you did the problem earlier about Mumford coordinates) Explicitly, what is the image of point in $J(k)$ under the $x - T$ map whose Mumford coordinates are (a, b).

(g) * Show that the $x-T$ map agrees with the descent map δ (c.f. Equation (6) for elliptic curves with full 2-torsion).

II.2.15 (The 2-Selmer group) Let Ω_k denote the set of places of k (including Archimedean places). By restriction to the decomposition group for a place, we have a commutative diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & \frac{J(k)}{2J(k)} & \xrightarrow{\delta} & H^1(k, J[2]) \\ & & \downarrow & & \downarrow \prod_v \mathrm{res}_v \\ 0 & \longrightarrow & \displaystyle\prod_{v \in \Omega_k} \frac{J(k_v)}{2J(k_v)} & \xrightarrow{\prod_v \delta_v} & \displaystyle\prod_{v \in \Omega_k} H^1(k_v, J[2]) \end{array}$$

Define the 2-Selmer set

$$\mathrm{Sel}_J(k, J[2]) := \left\{\tau \in H^1(k, J[2]) : \mathrm{res}_v(\tau) \in \mathrm{im}\left(\delta_v \colon J(k_v) \to H^1(k_v, J[2])\right) \text{ for all } v \in \Omega_k\right\}$$

(a) If v is a finite place of good reduction of J that is not above 2, show that

$$\mathrm{res}_v(\tau) \in \mathrm{im}\left(\delta_v \colon J(k_v) \to H^1(k_v, J[2])\right)$$

if and only if τ is unramified at v.

(b) Let $S \subset \Omega_k$ denote the set of all Archimedean places, all places above 2, and all places of bad reduction for J. Show that we have the following containments

$$\mathrm{im}\left(\frac{J(k)}{2J(k)} \xrightarrow{\delta} H^1(k, J[2])\right) \subseteq \mathrm{Sel}_J(k, J[2]) \subseteq H^1_S(k, J[2]),$$

and the simpler definition

$$\mathrm{Sel}_J(k, J[2]) = \left\{\tau \in H^1_S(k, J[2]) : \mathrm{res}_v(\tau) \in \mathrm{im}\,(\delta_v) \text{ for all } v \in S\right\}.$$

(c) Rephrase the definition of the 2-Selmer group using the concrete explicit descriptions of $H^1(k, J[2])$ and the descent maps δ and δ_v. (Along the way, explicitly describe in words the set $H^1_S(k, J[2])$ and why it is finite in terms of L above.)
(d) * Give an algorithm to compute the $\mathbb{F}_2$-dimension of $\mathrm{Sel}_J(k, J[2])$.

II.2.16 (Rank calculation for the Jacobian of a genus 3 hyperelliptic curve) This problem leads you through the computation in [Sch95] of the rank of the Jacobian of a genus 3 curve over $\mathbb{Q}$. Let C be the odd degree hyperelliptic curve with affine equation

$$y^2 = x(x-2)(x-3)(x-4)(x-5)(x-7)(x-10).$$

(a) Verify that $(1, \pm 36)$ and $(6, \pm 24)$ are rational points on C. We will verify that these two points together with the 8 rational 2-torsion points generate the 2-Selmer group $\mathrm{Sel}_J(\mathbb{Q}, J[2])$.
(b) Show that the set S from the previous problem is $\{\infty, 2, 3, 5, 7\}$. Describe $H^1_S(\mathbb{Q}, J[2])$ explicitly.
(c) Show/recall that the descent map is explicitly

$$\frac{J(\mathbb{Q})}{2J(\mathbb{Q})} \xrightarrow{(x-0, x-2, x-3, x-4, x-5, x-7, x-10)} \ker\left(\left(\frac{\mathbb{Q}^\times}{\mathbb{Q}^{\times 2}}\right)^7 \xrightarrow{N} \frac{\mathbb{Q}^\times}{\mathbb{Q}^{\times 2}}\right).$$

Recall how to evaluate on a Weierstrass point.
(d) From your answers to Exercise (**II.2.11**), you should know that $\dim_{\mathbb{F}_2} J(\mathbb{R})/2J(\mathbb{R}) = 3$. Show that the known rational points generate the image

$$\delta_\infty\left(\frac{J(\mathbb{R})}{2J(\mathbb{R})}\right) \subseteq H^1(\mathbb{R}, J[2]).$$

Write down these "real constraints" explicitly.
(e) Find generators for $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$. From your answers to Exercise (**II.2.11**), you should know that $\dim_{\mathbb{F}_2} J(\mathbb{Q}_2)/2J(\mathbb{Q}_2) = 9$. In terms of your generators, find the images of the known rational points under

$$\delta_\infty\left(\frac{J(\mathbb{Q}_2)}{2J(\mathbb{Q}_2)}\right) \subseteq H^1(\mathbb{Q}_2, J[2]).$$

Do these generate the image? If not, can you find another independent 2-adic point on J?
(f) For each of the primes $p = 2, 5, 7$, from your answers to Exercise (**II.2.11**), you should know that $\dim_{\mathbb{F}_2} J(\mathbb{Q}_p)/2J(\mathbb{Q}_p) = 3$. Show that the images of the known rational points generate the image of δ_p.
(g) Combine the local information to conclude that the image of δ is generated by the known rational points on J.

II.2.17 (Rank calculation for the Jacobian of a genus 2 curve without full 2-torsion) Let C be the odd degree hyperelliptic curve over $\mathbb{Q}$ with affine equation

$$y^2 = x^5 + 1$$

(a) Compute $J[2](\mathbb{Q})$.
(b) Show that the set S can be taken to be $S = \{\infty, 2, 5\}$.
(c) Let ζ be a primitive 5th root of unity. Show that

$$H^1(\mathbb{Q}, J[2]) \simeq \frac{\mathbb{Q}(\zeta)^\times}{\mathbb{Q}(\zeta)^{\times 2}}.$$

Show that in terms of this δ is the map of $x + \zeta$.

(d) Show that $\{-1, 1+\zeta, 2, 1-\zeta\}$ are representatives for the elements of $\frac{\mathbb{Q}(\zeta)^\times}{\mathbb{Q}(\zeta)^{\times 2}}$ that give rise to extensions unramified away from S.
(e) Does δ_∞ give any information?
(f) (Local information at 5)
  (a) What is $\dim_{\mathbb{F}_2} J(\mathbb{Q}_5)[2]$?
  (b) Find representatives for $\frac{\mathbb{Q}_5(\zeta)^\times}{\mathbb{Q}_5(\zeta)^{\times 2}}$.
  (c) In terms of your representatives, what is the map from $H^1_S(\mathbb{Q}, J[2])$ to $H^1(\mathbb{Q}_5, J[2])$?
  (d) Can you determine the image of δ_5?
  (e) What does this tell you about $\mathrm{Sel}_J(\mathbb{Q}, J[2]) \subset H^1_S(\mathbb{Q}, J[2])$?
(g) (Local information at 2)
  (a) What is $\dim_{\mathbb{F}_2} J(\mathbb{Q}_2)[2]$? What is $\dim_{\mathbb{F}_2} J(\mathbb{Q}_2)/2J(\mathbb{Q}_2)$?
  (b) Find representatives for $\frac{\mathbb{Q}_2(\zeta)^\times}{\mathbb{Q}_2(\zeta)^{\times 2}}$.
  (c) In terms of your representatives, what is the map from $H^1_S(\mathbb{Q}, J[2])$ to $H^1(\mathbb{Q}_2, J[2])$?
  (d) By generating 2-adic points on J, can you determine the image of δ_2?
  (e) What does this tell you about $\mathrm{Sel}_J(\mathbb{Q}, J[2]) \subset H^1_S(\mathbb{Q}, J[2])$?
(h) Show that $\mathrm{Sel}_J(\mathbb{Q}, J[2])$ is spanned by the image of the 2-torsion point $(-1, 0)$ under δ. Conclude that J has rank 0.

II.2.18 * Repeat your calculation of the previous example with the curve

$$y^2 = x^5 - 1.$$

What happens in this case?

II.2.19 (Genus 1 curves and pencils of quadrics) In this problem, we'll combine some of the arithmetic and geometric theory to "see" the 2-covers of an elliptic curve E as genus 1, degree 4 space curves. Assume for simplicity that E has full 2-torsion over $\mathbb{Q}$, and hence has Weierstrass equation

$$y^2 = (x - e_1)(x - e_2)(x - e_3).$$

(a) If C is a 2-cover of E (c.f. Exercise (**II.1.23**)), show that there exists a line bundle $L \in \mathrm{Pic}^4(C)$ giving $\varphi_L \colon C \hookrightarrow \mathbb{P}^3$. Show that under this embedding C is the base locus of a pencil of quadric hypersurfaces.
(b) On the other hand, 2-covers of E correspond to twists of $E \xrightarrow{2} E$ by classes in $H^1(\mathbb{Q}, E[2])$. Using your understanding of this group, give another proof that C is an intersection of two quadrics in $\mathbb{P}^3$ by writing down two quadrics generating the pencil.
(c) Show with your explicit equations that E is also the discriminant curve of your pencil of quadrics. Namely, if quadrics Q_1 and Q_2 generate your pencil, and A_1 and A_2 are symmetric 3×3 matrices representing Q_1 and Q_2, show that the curve with equation

$$y^2 = \det(xA_1 - A_2)$$

is isomorphic to E over $\mathbb{Q}$.
(d) More geometrically, the discriminant curve parameterizes the rulings on the pencil of quadrics. (Make this precise). Assume that Q_1 and Q_2 generate a pencil of quadrics over k whose discriminant scheme (vanishing of $\det(xA_1 - A_2)$ in $\mathbb{P}^1_k$) is smooth, and write X for the discriminant curve (which may not be an elliptic curve!) Write $B = V(Q_1, Q_2)$ for the base locus curve. Show that X is canonically isomorphic to $\mathrm{Pic}^2_{B/k}$ and that if X has a k-point, then the map $B \to X$ is a 2-covering.

Descent with étale Galois covers.

In this section, we work directly with étale G-covers of curves and the descent partition of rational points, c.f., Exercise (**II.2.3**). This can be a powerful technique, since the twists Z^τ may map to lower-genus curves whose rational points are easier to understand.

II.2.20 (Translating previous exercises into this setup) Suppose that $f\colon Y \to X$ is a G-Galois cover of nice curves over k (c.f. Exercise (**I.3.2**)).

(a) Explain why it suffices to find the rational points on finitely many curves Y^τ corresponding to twists $f^\tau\colon Y^\tau \to X$ in order to determine $X(k)$.
(b) What do these finite set of twists correspond to?

II.2.21 (Example with $G = \mathbb{Z}/2\mathbb{Z}$) Suppose that C is a hyperelliptic curve of genus at least 2 over $\mathbb{Q}$ with affine equation

$$y^2 = f_1(x)f_2(x),$$

with $\deg f_1 \geqslant \deg f_2$, and f_1 and f_2 square-free with no common factors over $\mathbb{Q}$.

(a) Show that the curve D with (affine) equations

$$y^2 = f_1(x)f_2(x)$$
$$w^2 = f_1(x)$$

is an étale $\mathbb{Z}/2\mathbb{Z}$-cover of C. Compute the genus of D.
(b) Show that D maps to the curve X with affine equation

$$w^2 = f_1(x).$$

Compute the genus of X.
(c) Describe a finite set S such that the images of the rational points on twists D^τ corresponding to elements $\tau \in H^1_S(\mathbb{Q}, \mathbb{Z}/2\mathbb{Z})$ cover the rational points on C. Describe the equations for the covers $f^\tau\colon D^\tau \to C$.
(d) Show that D^τ covers an analogous twisted curve X^τ as in part (b). If $X^\tau(\mathbb{Q})$ is finite for every $\tau \in H^1_S(\mathbb{Q}, \mathbb{Z}/2\mathbb{Z})$, how can you compute $C(\mathbb{Q})$?
(e) Carry out this strategy when, as in [RZB15], one wants to find the rational points on the hyperelliptic curve

$$y^2 = x^6 - 5x^4 - 5x^2 + 1,$$

whose Jacobian has rank 2 (and therefore classical Chabauty does not suffice.)
(f) Show that every hyperelliptic curve whose Jacobian has a nontrivial rational 2-torsion point is of this form.

II.2.22 (Chabauty in Magma) Chabauty's method (combined with a Mordell-Weil seive to combine information at different primes) is implemented in Magma; you can read about it here: `https://magma.maths.usyd.edu.au/magma/handbook/text/1534`.

(a) Let C be the hyperelliptic curve with affine model

$$y^2 = x^5 + 1$$

that we encountered in Exercise (**II.2.17**). In that exercise, you showed *explicitly by hand* that the Jacobian has rank 0. Find all of the rational points on C using the magma function `Chabauty0`.
(b) Let C be the hyperelliptic curve with affine model

$$y^2 = x^5 - 1$$

that we encountered in Exercise (**II.2.18**). In that exercise, you showed *explicitly by hand* that the Jacobian has rank 1. Find all of the rational points on C using the magma function `Chabauty`.

(c) Here is a list of all genus 2 curves over $\mathbb{Q}$ in the LMFBD that have good reduction away from 2: `https://www.lmfdb.org/Genus2Curve/Q/?hst=List&bad_quantifier=exactly&bad_primes=2&search_type=List`
You can download this list in a format readable by magma with a link at the bottom of the page. For which of these curves can you use magma's built in Chabauty methods to compute the rational points?

References

[Muk92] Shigeru Mukai. Curves and symmetric spaces. *Proc. Japan Acad. Ser. A Math. Sci.*, 68(1):7–10, 1992.

[Muk95] Shigeru Mukai. Curves and symmetric spaces. I. *Amer. J. Math.*, 117(6):1627–1644, 1995.

[Muk10] Shigeru Mukai. Curves and symmetric spaces, II. *Ann. of Math. (2)*, 172(3):1539–1558, 2010.

[Poo] Bjorn Poonen. Lectures on rational points on curves. Available at `http://math.mit.edu/~poonen/papers/curves.pdf`.

[Poo17] Bjorn Poonen. *Rational points on varieties*, volume 186 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2017.

[RZB15] Jeremy Rouse and David Zureick-Brown. Elliptic curves over $\mathbb{Q}$ and 2-adic images of Galois. *Res. Number Theory*, 1:Art. 12, 34, 2015.

[Sch95] Edward F. Schaefer. 2-descent on the Jacobians of hyperelliptic curves. *J. Number Theory*, 51(2):219–232, 1995.

[Ser97] Jean-Pierre Serre. *Galois cohomology*. Springer-Verlag, Berlin, 1997. Translated from the French by Patrick Ion and revised by the author.