Arithmetic of Curves

Stefan Patrikis (Notes taken by Karthik Prasad)

5/24/2025

Contents

Quick reference

1 Day 1

1.1 Structure of Course

The course will cover three different main topics over the next few weeks.

1. Firstly, we will talk about a specific Local-Global principle via the Hasse-Minkowski Theorem (which we will prove for plane conics). Local-global here refers to this larger idea in number theory of solving a problem in $\mathbf{Z}$ (or $\mathbf{Q}$) by working modulo every n, which is equivalent to working modulo every p^n for every prime p if we have some way of gluing the p^n together. It turns out to be convenient to consider all powers n for a given prime p at once via the p-adics $\mathbf{Z}_p$ (or $\mathbf{Q}_p$). In this case, it turns out that working locally via solving these plane conic equations over $\mathbf{R}$ and over each $\mathbf{Q}_p$, we can solve them globally over the rationals $\mathbf{Q}$. In degree 2 (quadratic forms), this works.

2. Then, we will analyze in some way how this fails in higher dimensions, using some algebraic geometry to understand these higher dimensional spaces.

3. Finally, we will try not to solve these higher-degree curves in $\mathbf{Q}$, but rather modulo p (and generally over finite fields). This is the content of the Weil conjectures (over finite fields).

1.2 Quadratic Forms (Algebraically)

Hasse-Minkowski is actually a general theorem about polynomials in n variables. However, we will prove it only for $n = 1, 2$, as the case of $n = 3$ is tricky. So, what are we really looking at? We are looking at conics in 2 variables, that is, equations of the form $f(X_0, x_1, x_2) = \sum_{i,j=0}^{2} \alpha_{ij} x_i x_j$ where the $\alpha_{ij} \in \mathbf{Q}$. This is a quadratic form.

We can more abstractly define a quadratic form in a general vector space over a field $\mathbf{k}$ by saying $f : V \to \mathbf{k}$ is a quadratic form if $f(av) = a^2 f(v)$ and the map $f' : V \times V \to \mathbf{k}$ by $f'(v, w) = f(v + w) - f(v) - f(w)$ is a (symmetric) bilinear map. We define $\langle v, w \rangle$ to be $\frac{1}{2} f'(v, w)$.

(Convince yourselves that the previous case is indeed a special case of this).

For us, we will deal with char$k \neq 2$. In this case, we will see that just as the quadratic form provides a symmetric bilinear map, any symmetric map provides a bilinear form, therefore giving a correspondence.

Notice when we have f and f':

$$\langle v, v \rangle = \frac{1}{2} \left(f(v + v) - f(v) - f(v) \right) = \frac{1}{2} \left(4f(v) - 2(v) \right) = f(v),$$

and so we can recover $f(v)$ by $f(v) = \langle v, w \rangle$. Any symmetric bilinear form in this characteristic will give a quadratic form in this way.

Choosing a basis $e_1, ..., e_n$ of V (over $\mathbf{k}$), we can define a matrix for f by looking at the associated bilinear form $\langle \cdot, \cdot \rangle$, since:

$$\begin{aligned} f(\sum x_i e_i) &= \langle \sum x_i e_i, \sum x_j e_j \rangle \\ &= \sum_{i,j} x_i x_j \langle e_i, e_j \rangle \end{aligned}$$

and here, we see that $a_{ij} = a_{ji}$ (since $\langle e_i, e_j \rangle$ is symmetric).

Definition 1.1 (Discriminant of a Quadratic Form). The "discrimant" of the form f (in the basis e_i) is the determinant of the matrix A.

It is an exercise to show choosing a different basis C corresponds to transforming C by CAC^T for C the Change-of-Basis matrix.

In particular, wefe see:

$$\det\left(CAC^T\right) = \det(C)^2 \det(A),$$

and hence $\det(A)$ is well defined modulo scalars in $(\mathbf{K}^\times)^2$ (where we can interpret this modulo in terms of the quotient group $\mathbf{K}^\times / (\mathbf{K}^\times)^2$).

Via this fact, we now can say the discriminant is either zero or nonzero everywhere, and hence the following is well-defined:

Definition 1.2 (Non-degeneracy of a Quadratic Form). We say f is non-degenerate if the discriminant of f is not equal to 0. Else f is degenerate.

Now, this is a classically algebraic-kind of construction. We now want to take a dual geometric perspective and see if we can capture this notion of degeneracy clearly.

It is an exercise to show the matrix of the quadratic form f can be diagonalized.

The above example shows in a diagonal basis, non-degeneracy is equivalent to all the a_i not being zero (since the determinant is the product of the a_i). Then, we can interpret non-degeneracy precisely as "having all of our variables".

1.3 Quadratic Forms (Geometrically)

The three-variable case of quadratic forms (as we originally started with) coincide with (projective) plane conics. What do we mean by this?

Let $f(x_0, x_1, x_2) = \sum \alpha_{ij} x_i x_j$ be a quadratic form. Interpreting this as a plane conic, we want to solve $f = 0$ over our field $\mathbf{k}$ (which could be $\mathbf{F}_{p^k}, \mathbf{Q}, \mathbf{R}, \mathbf{Q}_p, \mathbf{C}$, etc). Working in $\mathrm{char}(k) \neq 2$, we will take the α_{ij} to be diagonal.

The equation $f = 0$ can be thought of in two ways:

(a) For any field $\mathbf{K} \supset \mathbf{K}$, we can look for triples $(a_0, a_1, a_2) \in \mathbf{K}^3 \setminus \{(0,0,0)\}$ with $f(a_0, a_1, a_2) = 0$.

There is a kind of redundancy in this in the sense that once we have an initial solution (a_0, a_1, a_2), anything of the form $(\lambda a_0, \lambda a_1, \lambda a_2)$ is a solution, and this is coming from the homogeneity of f (the fact that the polynomial terms are the same degree).

(b) To solve the redundancy from before, we can essentially "cast out" scalars by working in projective space. What is projective space? There are good geometric interpretations (and resources for thse), but algebraically, we want the projective plane $\mathbf{P}^2(\mathbf{K})$ of the space $\mathbf{K^3}$ to be the set:

$$\mathbf{P^2}(\mathbf{K}) = \left(\mathbf{K}^3 \setminus \{(0,0,0)\}\right) / \sim$$

where we say $(a_0, a_1, a_2) \sim (b_0, b_1, b_2)$ if $\frac{a_i}{b_i} = \lambda$ for some $\lambda \in \mathbf{K}^\times$ for all i. Geometrically, we are identifying lines in $\mathbf{K}^3$.

The key idea in this second perspective is going to be to write $[a_0, a_1, a_2]$ to be the equivalence class of (a_0, a_1, a_2) in $\mathbf{P}^2(\mathbf{K})$.

Now, define $C_f \subset \mathbf{P}^2(\mathbf{K})$ to be the zero set (locus) of f in $\mathbf{P}^2(\mathbf{K})$. Homogeneity of f (as discussed before) ensures this is well-defined.

Before proceeding further with C_f, let us think more about this space $\mathbf{P}^2(\mathbf{K})$. Since at least one of the a_i in (a_0, a_1, a_2) is nonzero (since they live in $\mathbf{K}^3 \setminus \{(0,0,0)\}$, we see that the space decomposes by:

$$\mathbf{P}^2 = U_0 \cup U_1 \cup U_2,$$

where $U_i = \{[a_0, a_1, a_2] \mid a_i \neq 0\}$. Notice these unions certainly have overlaps. However, since $a_i \neq 0$ and we are in an equivalence class up to scaling, we see that we can always rescale a_i to 1 and fix it, hence parametrizing U_i in terms of the other a_j. Therefore, we see that U_i is in bijection with $\{(x, y) \in \mathbf{K}^2\}$, by the map (in the case $i = 0$)

$$[a_0, a_1, a_2] \to [1, \frac{a_1}{a_0}, \frac{a_2}{a_0}]$$

We can then figure out how C_f works by looking at its intersection with each of the U_i.

As an example, take the form $X^2 - 13Y^2 + 17Z^2 = f(X, Y, Z)$ and consider $C_f \in \mathbf{P}^2$. We have $U_n \cap C_f = \{x \neq 0\} \cap C_f$, and by our bijection, we are then looking at the solution set of $1 - 13\left(\frac{y}{x}\right)^2 + 17\left(\frac{z}{x}\right)^2 = 0$. This turns out to be simpler to analyze, naturally.

Now, we can finally return to our original question - what is non-degeneracy geometrically? The answer will be that it will correspond to non-singularity of the associated plane algebraic curve.

Suppose $g(x, y) = 0$ is a polynomial over $\mathbf{K}$ in two variables. Let $\mathbf{A}^2$ be the affine 2-space over $\mathbf{K}$, in this case exactly $\mathbf{K}^2$. We are interested in solving $g = 0$ in this space.

What are some such curves? We can take $y^2 = x$, $y^2 = x^2$, $y^2 = x^3$. I won't graph these in these notes, but we see that $y^2 = x$ is nice and smooth everywhere (having a well-defined tangent line), $y^2 = x^2$ has a singularity at $x = 0$, and $y^2 = x^3$ has a singularity at $x = 0$. What is going on here?

The fact in common is that at 0, these functions have gradient $\left(\frac{\partial g}{\partial x}, \frac{\partial g}{\partial y}\right)$. Having a nonzero gradient ensures predictable trajectory and motion, hence, in some sense, a geometric "completeness" of the curve in the sense that at a single point, it is carried elsewhere by the gradient completely. Having zero gradient means this does not happen, meaning somewhere, the geometry of the curve breaks down and doesn't determine a trajectory. We formalize this via the following:

Definition 1.3 (Nonsingularity of a Curve in Affine Space). Given $g(x,y) \in \mathbf{k}[x,y]$ and a point $P = (a,b)$ on C_G in $\mathbf{A}^2$, we say g is non-singular at p if:

$$\nabla g(p) = \left(\frac{\partial g}{\partial x}, \frac{\partial g}{\partial y}\right) \neq (0,0)$$

Else, we say g is singular at p.

We say a curve is non-singular if it is nonsingular at every $p \in C_G$ over every field $\mathbf{K} \supset \mathbf{k}$ (or equivalently in an algebraic closure).

Definition 1.4 (Nonsingularity of a Projective Conic in Projective Space). If f is a homogenous form $f(x_0,x_1,x_2) \in \mathbf{k}[x_0,x_1,x_2]$, take the zero set C_f in $\mathbf{P}^2(\mathbf{k})$, then we say C_f is non-singular at p if $C_f \cap U_i$ is nonsingular at p for each U_i. We say it is non-singular everywhere if $C_f \cap U_i$ is nonsingular everywhere.

Essentially, we define nonsingularity of the projective conic to be nonsingularity in each of the affine subspaces $C_f \cap U_i$.

Now, let us return to our prior example. Here, we have that $U_0 \cap C_f$ is $1 - 13w^2 - 17v^2 = 0 = g(w,v)$. The gradient here is:

$$\nabla(g)(p) = \begin{pmatrix} -26w & 34v \end{pmatrix}$$

The question is of course, when is this singular?

In characteristic 2, this is always singular. In characteristic 0 or characteristic not 13, 17, this is not singular since $\nabla(g)(p) = 0$ implies $(w,v) = 0$ and this is not in the zero set C_f. In characteristic 13, $\nabla(g)(p)$ only when $v = 0$, but then at such p, f is not zero, hence it is nonsingular, and a similar analysis holds for characteristic 17.

We also can similarly check this for $U_1 \cap C_f$, and $U_2 \cap C_f$. We will check U_2 first. Here, the right equivalence class of curves to study is $h(s,t)s^2 - 13t^2 + 17 = 0$, which gives gradient 13, this is nonsingular since $s = 0$ gives $f \neq 0$, and in characteristic 17, the point $(0,0)$ will in-fact be singular.

Similarly, in $U_1 \cap C_f$, we observe a singular point at $(0,0)$ in characteristic 13.

What is the general result? We have:

Lemma 1.5. Given $\mathbf{k} \subset \mathbf{K}$ not of characteristic 2, the quadratic form $f(x,y,z) = ax^2 + bY^2 + cZ^2$ is non-degenerate if and only if the projective curve $C_f \subset \mathbf{P}^2$ is non-singular.

The proof is exactly analagous to the before case, as essentially we observe non-singularity if and only if one of the a,b,c is zero in our characteristic (corresponding in the example to working in char p where p was one of the coeffieints), which is equivalence to non-degeneracy of this quadratic form in diagonal form.

1.4 Hasse-Minkowski

This approach to looking at C_f may seem sort of "haywire". We will revisit this more formally via formally defining objects of algebraic geometry in the future, which may make some ideas more clear. Now, we turn to our actual local global-principle, stating the result in full.

Theorem 1.6 (Hasse-Minkowski Theorem). Let $f(x_0, ..., x_n)$ be a quadratic form over $\mathbf{Q}$ (which we take to be non-degenerate). Then, there exists a nonzero solution $(a_0, ..., a_n) \in \mathbf{Q}^{n+1} \setminus \{(0, ..., 0)\}$ such that $f(a_0, ..., a_n) = 0$ if and only if for all primes p there exist $(a_0, ..., a_n) \in \mathbf{Q}_p^{n+1} \setminus \{(0, ..., 0)\}$ such that $f(a_0, ..., a_n) = 0$ and there exists $(a_0, ..., a_n) \in \mathbf{R}^{n+1} \setminus \{(0, ..., 0)\}$ such that $f(a_0, ..., a_n) = 0$.

Informally, there exists a solution in $\mathbf{Q}$ if and only if there exists a solution in each $\mathbf{Q}_p$ for all p and in $\mathbf{R}$.

We will prove this for the case of $n = 3$ (the case of $n = 2$ is left as an exercise). The case of $n = 4$ is the hardest case (we will not discuss this), at which point an induction argument proves the result in general. It turns out this can be done more generally when we replace $\mathbf{Q}$ with a number field (a finite extension of $\mathbf{Q}$).

So, how do we solve such equations over $\mathbf{R}$? The answer is simple - an affine change of variables diagonalizes the quadratic form by $\lambda_0 x_0^2 + \lambda_1 x_1^2 + ... + \lambda_r x_r^2 + -(\lambda_{r+s} x_{r+s}^2 + ... + \lambda_n x_n^2)$. However, this is easy to solve, as we can obtain any $r \in \mathbf{R}_{\geq 0}$ via any nonempty sum of this form $\lambda_0 x_0^2 + \lambda_1 x_1^2 + ... + \lambda_r x_r^2$.

Therefore, the $\lambda_0 x_0^2 + \lambda_1 x_1^2 + ... + \lambda_r x_r^2$ allows us to obtain an arbitrary positive real when it isn't empty (no positive coefficients), and the $(\lambda_{r+s} x_{r+s}^2 + ... + \lambda_n x_n^2)$ provide a negative term when (again) this is not empty (meaning no negative coefficients. Therefore, we can get zero if and only if we have both a positive and a negative term, and this is found via diagonalization. This is somewhat easy in the sense that the continuity of $\mathbf{R}$ lets us solve everything in a straightforward manner.

So, what is it like to solve in $\mathbf{Q}_p$? We cannot answer this question just yet, but we can consider a "warm-up" in $\mathbf{F}_p$, by asking "does $a_0 x_0^2 + a_1 x_1^2 + a_2 x_2^2 = 0$ have a solution in $\mathbf{P^2 F}_p$. This will give $(a_0, a_1, a_2) \in \mathbf{F}_p$ not all zero, and working in each $U_i \cap C_f$ really sort of tells us we are asking if there exist x, y such that:

$$ax^2 + by^2 = -1 \pmod{p}.$$

The answer is yes, via the sets. It is an exercise to generalize this to finite fields.

1.5 P-Adics (Analytically)

Now, we will want to actually construct this space $\mathbf{Q}_p$, and perhaps explain what we meant earlier when we said this allows us to work modulo all p^n.

Analytically, we construct $\mathbf{Q}_p$ as an analog with $\mathbf{R}$. $\mathbf{R}$ is the Cauchy completion of $\mathbf{Q}$ with respect to the regular absolute-value norm $|\cdot|$ (we can consider it an equivalence classes of Cauchy serquences). The space $\mathbf{Q}_p$ is the Cauchy completion of $\mathbf{Q}$ with respect to the p-norm. But, what is the p-norm?

Recall that any $q \in \mathbf{Q}$ can be uniquely written as $q = p^r \cdot \frac{a}{b}$ with a, b both coprime to p (pulling p-powers out of both numerator and denominator). The p-norm aims to consider something very small if it is divisible by p, in the following sense

Definition 1.7 (p-norm). Define the p-adic absolute value $|\cdot|_p : \mathbf{Q} \to \mathbf{R}_{\geq 0}$ by sending $q \in \mathbf{Q}$ to $|q|_p = p^{-r}$ where r is the power of p in the $p^r \frac{a}{b}$ decomposition described above.

In this sense, p^{100} is "tiny" since it has norm p^{-100}, and p^{-100} is "large" since it has norm p^{100}.

It turns out we can use any a^{-r} with a a positive real greater than 1, but the p turn out to be useful for normalization facts.

In what sense is this a good metric? Well, notice:

$$|ab|_\infty = |a||b|, |a+b|_\infty \leq |a|_\infty + |b|_\infty, |a|_\infty \text{ if and only if } a = 0.$$

These properties similarly hold for $|\cdot|_p$, and indeed, we have a strengthened or non-Archimedian triangle inequality $|q_1 + q_2|_p \leq \max(|q_1|_p, |q_2|_p)$. Therefore, this gives us a sort of natural metric on $\mathbf{Q}$ by $d(r,s) = |r_s|_p$, although this is not quite a true norm.

We define the p-adic field $\mathbf{Q}_p$ to be the completion of $\mathbf{Q}$ with respect to the $|\cdot|_p$. It is an exercise to show $\mathbf{Q}_p$ is a (topological) field with $+, \cdot$ extending the old operations on $\mathbf{Q}$ and the norm $|\cdot|_p : \mathbf{Q}_p \to \mathbf{R}_{\geq 0}$ extending $|\cdot|_p$ on $\mathbf{Q}$.

Inside $\mathbf{Q}_p$, there is a distinguished subring $\mathbf{Z}_p$ defined as the unit ball in $\mathbf{Q}_p$, equivalently, $\{x \in \mathbf{Q}_p \mid |x|_p \leq 1\}$. This has a unique maximal ideal given by $p\mathbf{Z}$, the open unit ball in $\mathbf{Q}_p$. It is an exercise to check $\mathbf{Z}_p$ is a subring with $\text{Frac}(\mathbf{Z}_p) = \mathbf{Q}_p$.

1.6 P-Adics (Algebraically)

As we said before, we want to think of p-adics as solving something modulo p^n simultaenously for all n. To do this, then, it turns out to be convenient to consider the following:

$$\mathbf{Z}_p = \left\{(a_0, a_1, ...,) \mid a_n \in \mathbf{Z}/p^{n+1}\mathbf{Z}, a_n \equiv a_{n-1} \pmod{p^n}\right\}.$$

For example, consider the sequence $(1, 1+p, 1+p+p^2, ...)$ modulo p. Such sequences form a ring under component-wise operations as usual. This is going to be $\mathbf{Z}_p$ again, with a unique maximal ideal by $p\mathbf{Z}_p = \{(0, a, ...,) \in \mathbf{Z}_p\}$.

The ring $\mathbf{Z}_p$ is naturally equipped with projection or reduction maps (homomorphisms) modulo p^n from $\mathbf{Z}_p \to \mathbf{Z}/p^n\mathbf{Z}$ via $(a_0, ...,) \to a_{n-1}$.

It is an exercise to show $\mathbf{Z}_p$ has no nonzero zero divisors.

Then, define $\mathbf{Q}_p = \text{Frac}(\mathbf{Z}_p)$, just as in $\mathbf{Z}$.

It is an exercise to identify these analytic and algebraic descriptions.

1.7 Failure in $\mathbf{Q}_p$

Unlike the case of $\mathbf{F}_p$ where we had a solution every prime, quadratic forms must not have a nontrivial solution over $\mathbf{Q}_p$. Here, we will provide an example.

Consider $f(x,y,z) = x^2 + 3y^2 - 15z^2$ in $\mathbf{Q}_3$. Certainly in characteristic 3, this has no solutions. So, suppose there is some nonzero $(a_0, a_1, a_2) \in \mathbf{Q}_3 \setminus \{(0,0,0)\}$ a root of $f(x,y,z)$ in 3-space. Then, any element of $\mathbf{Q}_p$ can be written as $p^r \cdot u$ with $r \in \mathbf{Z}$, and $|u|_p = 1$ and hence $u \in \mathbf{Z}_p^*$.

Consequently, we may assume our solution is primitive, meaning of them must lie in $\mathbf{Z}_3$, but cannot be all divisible by p. Choosing this as $i = 1$ without loss of generality, we see:

$$a_0^2 = -3a_1^2 + 15q_2^2$$

and writing $|a|_p = p^{-\nu_p(a)}$ where $\nu_{p(a)}$ is a shorthand for the p-adic valuation at a, we see this is a multiplicative to additive law, specifically:

$$\nu_p(a \cdot b) = \nu_p(a) + \nu_p(b)$$

In particular, $\nu_p(a_0^2) > 0$ implies $a_0(a_0) > 0$, but notice $\nu_p(-3a_1^3 + 15a_2^3) \geq 2$ by this strong Archimedian law, and hence $\nu_p(-a_1^2 + 5a_2^2) \geq 1$ by the triangle inequality, and hence $a_1^2 \equiv 5a_2^2 \pmod 3$, but since 5 is not a square modulo 3, this is a contradiction.

1.8 Day 1 Exercises

(In-Text not on Set):

Exercise 1.1. Let $f : V \to \mathbf{k}$ 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).

Exercise 1.2. In class, we gave two constructions of the ring $\mathbf{Z}_p$ of p-adic integers: algebraically, by:

$$\mathbf{Z}_p = \left\{ (a_1, a_2, ...,) \in \prod_{n=1}^{\infty} \mathbf{Z}/p^n\mathbf{Z} \mid a_{n+1} \equiv a_n \pmod{p^n} \text{ for all } n \right\}$$

and analytically:

$$\mathbf{Z}_p = \{x \in \mathbf{Q}_p \mid |x|_p \leq 1\}$$

having first constructed $\mathbf{Q}_p$ as the completion of $\mathbf{Q}$ with respect to the p-adic absolute value $|\cdot|_p$. Show the equivalence of these definitions, i.e, produce a ring homomorphism between the two constructions.

Exercise 1.3. (a) Show (using either perspective on $\mathbf{Z}_p$) that an element $x \in \mathbf{Z}_p$ is invertible if and only if it is not divisible by p (in the ring $\mathbf{Z}_p$). Deduce that $p\mathbf{Z}_p$ is the unique maximal ideal of $\mathbf{Z}_p$ (a ring with a unique maximal ideal is called a local ring).

(b) Show that every element $x \in \mathbf{Q}_p$ can be written uniquely as $x = p^r \cdot u$ where $r = \nu_p(x)$ is an integer and $u \in \mathbf{Z}_p^\times$ (the multiplicative group of invertible element of $\mathbf{Z}_p$).

Exercise 1.4. Let $f \in \mathbf{Z}[X_0, X_1, ..., X_n]$ be a homogenous polynomial. Show that there exists $a = (a_0, a_1, ..., a_n) \in \mathbf{Q}^{n+1} \setminus \{0\}$ with $\gcd(a_0, ..., a_n) = 1$ 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 $\mathbf{Z}_p$) are equivalent:

- There is an $a \in \mathbf{Q}_p^{n+1} \setminus \{0\}$ such that $f(a) = 0$.
- There is an $a \in \mathbf{Z}_o^{n+1}$ with some coordinate non-zero mod p such that $f(a) = 0$.
- For all $m \geq 1$, there is an $a \in (\mathbf{Z}/p^m\mathbf{Z})$ with some coordinate non-zero $\pmod{p}$ such that $f(a) \equiv 0 \pmod{p^m}$.

Exercise 1.5. Consider the affine curve $C \subset \mathbf{A}^2$ given by $2x^2 + 7y^2 = 1$. Parametrize $C(\mathbf{Q})$ as $\{(x(t), y(t)) \mid t \in \mathbf{Q}\}$ for some rational functions $x(t), y(t) \in \mathbf{Q}(t)$ (analagous to the Pythagorean triple parametrization of the rational points on $x^2 + y^2 = 1$).

Exercise 1.6. Prove the $n = 2$ case of the Hasse-Minkowski theorem: a quadratic form $f(X_0, X_1) \in \mathbf{Q}[X_0, X_1]$ represents zero in $\mathbf{Q}$ if and only if it represents zero in $\mathbf{Q}_p$ for all p and represents zero in $\mathbf{Q}$ if and only if it represents zero in $\mathbf{Q}_p$ for all p and represents zero in $\mathbf{R}$, where by "represents zero in a field $\mathbf{k}$" we mean there exists $(a_0, a_1) \in \mathbf{k}^2 \setminus \{0\}$ such that $f(a_0, a_1) = 0$).

2 Day 2

2.1 Review/Overview

Our first goal is to understand the idea of a local-global principle via thinking about this Hasse-Minkowski theorem:

Theorem 2.1 (Hasse-Minkowski Theorem). Let $f(x_0, ..., x_n)$ be a quadratic form over $\mathbf{Q}$ (which we take to be non-degenerate). Then, there exists a nonzero solution $(a_0, ..., a_n) \in \mathbf{Q}^{n+1} \setminus \{(0, ..., 0)\}$ such that $f(a_0, ..., a_n) = 0$ if and only if for all primes p there exist $(a_0, ..., a_n) \in \mathbf{Q}_p^{n+1} \setminus \{(0, ..., 0)\}$ such that $f(a_0, ..., a_n) = 0$ and there exists $(a_0, ..., a_n) \in \mathbf{R}^{n+1} \setminus \{(0, ..., 0)\}$ such that $f(a_0, ..., a_n) = 0$.

We saw the case of $n = 1$ on the problem set, where sort of trivially the modulo p condition extended to all p^n. The case of $n = 2$ is slightly more advanced, requiring the Hensel lemma to lift from modulo p to modulo p^n for all n. The case of $n = 3$ (which we will not do) involves quaternionic algebras over $\mathbf{Q}_p$. The case of $n \geq 4$ is essentially trivial for complicated-to-state reasons (ask Patrikis for more, he wouldn't tell me!).

Last time, we ended by looking at a curve in which we could not solve in $\mathbf{Q}_p$, and so, the condition that we can solve an equation locally modulo all p^n is somehow nontrivial to analyze (unlike $\mathbf{R}$). So, we need to develop some tools to solve these things.

The relevant method is Hensel's lemma, which essentially given a function f with "good" behavior, we can lift a solution modulo p to a unique solution modulo p^n satisfying the reduction maps in $\mathbf{Z}_p$.

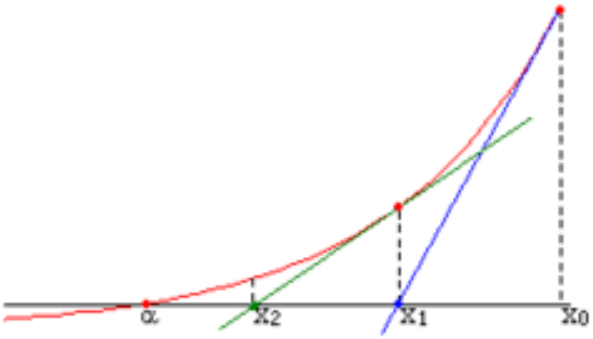

Figure 1: Pictorial Description of Newton's Method for Approximating Roots

2.2 Hensel's Lemma

The version on the Ross sets of Hensel's lemma (here rephrased as to utilize the language of $\mathbf{Z}_p$):

Theorem 2.2 (Standard Hensel's Lemma). Let $f(x) \in \mathbf{Z}_p[x]$ be the p-adic integers. Let $a \in \mathbf{Z}_p$ such that $f(a) \equiv 0 \pmod{p}$ and $f'(a) \neq 0 \pmod{p}$. Then, there exists a unique $a \in \mathbf{Z}_p$ such that $a' \equiv a \pmod{p}$ and $f(a') = 0$ in $\mathbf{Z}_p$.

The proof of this is left as an exercise. A sketch is as follows, "intuitively". Essentially, apply Newthon's method for roots in $\mathbf{R}$. When we have a root with a nonzero derivative around it, we can guess a root b, evaluate f take an approximation to find a "closer" point to a. This approximation is made formal by the Taylor decomposition of $f(x)$ a polynomial using formal derivatives.

To get an intuition for how this works, consider the following :

Example 2.3. $x^{p-1} - 1 = f(x)$. In this, $f(\bar{a}) = 0$ for every $\bar{a} \in (\mathbf{Z}/p\mathbf{Z})^{\times}$. Thus, Hensel tells us that $x^{p-1} - 1$ has $p - 1$ distinct solutions in $\mathbf{Z}_p$.

It turns out that perhaps even when $f'(a) \equiv 0 \pmod{p}$, we can salvage the Hensel lifting method to obtain a refined method when $f(a)$ is a root not modulo a, but modulo p^n with $n > 2\nu_p f'(a)$ to still find a unique $a \in \mathbf{Z}_p$ with $a' \equiv a \pmod{p^{n-\nu_p(f'(a))}}$ and $f(a') = 0$ in $\mathbf{Z}_p$.

Theorem 2.4 (Refined Hensel's Lemma). Let $f(x) \in \mathbf{Z}_p[x]$. Let $a \in \mathbf{Z}_p$ such that $f(a) \equiv 0 \pmod{p^n}$ such that $n > 2\nu_p(f'(a))$. Then, there exists unique $a' \in \mathbf{Z}_p$ such that $a' \equiv a \pmod{p - \nu_p(f'(a))}$ and $f(a') = 0$ in $\mathbf{Z}_p$.

For an example when we can apply this, see the following:

Example 2.5. Let $p = 2$ and consider $f(x) = x^2 + 7 \in \mathbf{Z}_2[x]$. We have $f(1) = 0 \pmod{8 = 2^3}$, but $\nu_2(f'(1)) = 1$, hence since $3 > 2 \cdot 1$, we have that there exists a unique $a \in \mathbf{Z}_2$ with $a \equiv 1 \pmod{4}$ such that $a^2 = -7$ in $\mathbf{Z}_2$.

Quadratic forms are not a function of a single variable, but indeed functions of multiple (for all nontrivial forms). Hence, we need to somehow extend this Hensel tool to

multiple variables. We can do this easily, but we lose uniqueness.

Theorem 2.6 (Multivariable Hensel's Lemma). Let $f \in \mathbf{Z}_p[X_0, ..., X_n]$ and suppose there exists $a = (a_0, ..., a_r)$ and $j \in \{0, ..., r\}$ such that $f(a) \equiv 0 \pmod{p^n}$ and $n > 2\nu_p\left(\frac{\partial f}{\partial x_j}\right)$. Then, there exists a' not necessarily unique such that $a' \equiv a \pmod{p^{n-\nu_p(\frac{\partial f}{\partial x_j})}}$ in $\mathbf{Z}_p^{r+1}$ such that $f(a') = 0$ in $\mathbf{Z}_p$.

Proof. The $r = 0$ version is the single-variable result. In general, given a and j as in the statement, fix the a_i with $i \neq j$, such that we are instead considering $f(a_0, a_1, ..., a_{j-1}, x_j, a_{j+1}, ..., a_0) \in \mathbf{Z}_p[x_j]$. This is a one-variable function of x_j and hence we can solve the congruence via the one-dimensional Hensel argument. □

2.3 Solvability in $\mathbf{Q}_p$

The ultimate goal of developing these various Hensel lifting methods is to apply this concretely to quadratic forms. How do we do this? Recall that we are interested in studying $f(x) = a_{ij}x_ix_j \in \mathbf{Z}_p[x_0, ..., x_n]$ non-degenerate with $\det(a_{ij}) \in \mathbf{Z}_p^\times$. It turns out this non-degeneracy condition will imply some $\frac{\partial f}{\partial x_j}$ cannot go to zero modulo p, and then this will allow us to apply multivariable Hensel.

Corollary 2.7. For $p \neq 2$, consider a general quadratic form $f(x) = a_{ij}x_ix_j \in \mathbf{Z}_p[X_0, ..., X_n]$ that is non-degenerate. Suppose there is some primitive solution $a = (a_0, ..., a_p) \in \mathbf{Z}p^{n+1}$ is a primitive solution (meaning it does not lie in $p\mathbf{Z}_p^{n+1}$, and equivalently not all a_i are divisible by p) to $f(a) \equiv 0 \pmod{p}$. Then there exists a' with $a' \equiv a \pmod{p}$ such that $f(a') = 0$.

Proof. We see that $\frac{\partial f}{\partial x_i} = \sum_{j=0}^{n} 2a_{ij}x_j$ (for $i = j$, this is clear, for $i \neq j$, symmetry of the a_{ij} for a quadratic form provides the factor of 2). In particular, this means $\frac{\partial f}{\partial x_i} = 2\sum j = 0 a_{ij}a_j = 2A(a)_i$.

We want to obtain some $\frac{\partial f}{\partial x_i} \neq 0 \pmod{p}$, such that then $\nu_p\left(\frac{\partial f}{\partial x_i}\right) = 0$, as this will allow us to apply multivariate Hensel.

So, consider the case with all the $\frac{\partial f}{\partial x_i} \equiv 0 \pmod{p}$. This is equivalent to $2A(a)_i = 0$ everywhere, hence we see:

$$A(a) = \begin{pmatrix} a_{11} & a_{12} & ... & a_{1n} \\ a_{21} & a_{22} & ... & a_{2n} \\ \vdots & \ddots & & \vdots \\ a_{n1} & a_{n2} & ... & a_{nn} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ ... \\ a_n \end{pmatrix} = 0$$

This contradicts non-degeneracy of the form (since non-degeneracy tells us $\det(A) \in (\mathbf{Z}_p)^\times$ which means A is invertible).

Therefore, given this solution a, we must have some j with $\frac{\partial f}{\partial x_i} \neq 0 \pmod{p}$, and applying multivariable Hensel gives the result. □

There exists a similar test for $p = 2$. To see this, see Dr. Patrikis's Ross 2021 notes. Now that we have all this machinery, how do we actually go about testing local solvability in the various $\mathbf{Q}_p$?

Example 2.8. Take the quadratic form $f(X, Y, Z) = X^2 - 13Y^2 + 17Z^2$. The astute reader may see $10, 3, 1)$ works, but this is certainly not immediately apparent.

So now, we will illustrate this general idea. Consider $C_f \subset \mathbf{P}^2$. It is clear by the general method for checking solvability in $\mathbf{R}$ that there are solutions. So, we must analyze when $C_f(\mathbf{Q}_p)$ is nonempty.

The matrix of our form is:

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -13 & 0 \\ 0 & 0 & 11 \end{pmatrix}$$

So, for $p \neq 2, 13, 17$, the question reduces by Corollary 2.7 to the question of "does there exist a primitive solution modulo p", and we have already seen this is true by **??**.

Hence, we only need to analyze these primes $p = 13, 17, 2$.

- For $p = 13$, $f \pmod{13}$ reduces to $x^2 + 4z^2$. We can quickly see $(3, 1)$ is a solution (in projective space, $f([3, 0, 1]) \equiv 0 \pmod{13}$ would be the $C_f \cap U_2$), and $\frac{\partial f}{\partial x_0} = 6 \neq 0 \pmod{13}$, so we apply single-variable Hensel to find a solution in $\mathbf{Z}_{13}^3 \setminus \{(0, 0, 0)\}$.
- Similarly for $p = 17$, we see $f([8, 1, 0]) = 0 \pmod{17}$ is a solution in $C_f \cap U_1$ and $\frac{\partial f}{\partial x_0} = 16 \neq 0 \pmod{17}$, hence single-variable Hensel lifts to a solution in $\mathbf{Z}_{17}^3 \setminus \{(0, 0, 0)\}$.
- In the case of $p = 2$, we have a little more work, but it is still relatively straightforward. Essentially, $f([2, 1, 1]) \equiv 0 \pmod{8 = 2^3}$, and $\nu_2(\frac{\partial f}{\partial x_1}) = 1$, and hence the refined Hensel suffices to lift.

So, we can conclude $C_f(\mathbf{Q}_p)$ is nonempty for every prime p, and $C_f(\mathbf{R})$ is nonempty. So, applying this Hasse-Minkowski theorem allows us to include $C_f(\mathbf{Q}) \neq 0$, and as we saw before this point $(10, 3, 1)$ works.

This method works extremely well in general. Essentially, given $f(x) = a_0X_0^2 + a_1X_1^2 + ... + a_nX_N^2$, the non-degeneracy condition allows us to find solutions for all primes except those dividing $a_0, ..., a_n$. Then, this is a finite set of primes which we can easily analyze since finite-fields (in particular $\mathbf{Z}_p$) are well-behaved. This algorithm then allows us to conclude solvability of quadratic forms in a straightforward manner.

2.4 Hasse-Minkowski for $n = 3$

We have already seen that the Hasse-Minkowski theorem is true in $n = 2$ via Exercise 1.6 via a sort-of-trivial argument.

SPOILERS FOR THE EXERCISE. Essentially, $ax^2 + by^2 = 0$ is solved for $\frac{a}{b}$ a square of a rational, but thinking p-adically, working every prime tells us we have a square modulo

the p^i if the p-adic valuation is divisible by 2. If the p-adic valuation is divisible by 2 for all primes p, then it is possible to show this happens only for $\frac{a}{b}$ a rational prime. Alternatively, the question $\frac{a}{b}$ a rational square can be phrased as an integer problem, and then Set 23 Problem 4 provides a solution (which can be proven elementarily via Jacobi symbols).

However, we will see the condition in $n = 3$ is much deeper and in-fact has to do with the algebraic number theory and the geometry of the curve. This connection will allow us to invoke powerful facts about norms of quadratic extensions providing a natural proof (whereas in $n = 2$ the relevant "extension" is trivial). This argument is due to Legendre, and relies on the following lemma.

Lemma 2.9. Let $\mathbf{k}$ be any field, with $\text{char}(\mathbf{k}) \neq 2$. Let $a, b \in \mathbf{k}^\times$. The equation $z^2 - ax^2 - by^2 = 0$ has a nonzero solution in $\mathbf{k}^3 \setminus \{(0,0,0)\}$ if and only if $a \in N_{\mathbf{k}[\sqrt{b}]/\mathbf{k}}\left(\mathbf{k}[\sqrt{b}]^\times\right)$.

(For those not used to algebraic number theory, $N_{\mathbf{k}[\sqrt{b}]/\mathbf{k}}$ is trivial for $\sqrt{b} \in \mathbf{k}$ and satisfies $N(x + y\sqrt{b}) = x^2 - by^2$ for $\sqrt{b} \notin \mathbf{k}$)

Proof. Firstly, if $\sqrt{b} \in \mathbf{k}$, the norm is trivial, and so this set $N_{\mathbf{k}[\sqrt{b}]/\mathbf{k}}\left(\mathbf{k}[\sqrt{b}]^\times\right)$ is simply $\mathbf{k}^\times$, and then $(\sqrt{b})^2 = a \cdot 0^2 - b \cdot 1^2 = 0$ is a solution.

So, we now reduce to the case $b \notin (\mathbf{k}^\times)^2$. Then, suppose $a \in N(\mathbf{k}[\sqrt{b}]^\times)$, meaning $a = a_1^2 - ba_2^2$, meaning $0 = a_1^2 - a \cdot 1^2 - b \cdot a_2^2$. Conversely, if $z^2 - ax^2 - by^2 = 0$, we can realize a as a norm of the element $\frac{z}{x} + \frac{y}{x}\sqrt{b}$ if $xyz \neq 0$, which must be true since any of these implies b is a square. □

Now, we are equipped for cubic Hasse-Minkowski.

Theorem 2.10 (Hasse-Minkowski Theorem for Conics). Let $f(x_0, x_1, x_2)$ be a quadratic form over $\mathbf{Q}$ (which we take to be non-degenerate). Then, there exists a nonzero solution $(a_0, ..., a_n) \in \mathbf{Q}^{n+1} \setminus \{(0, ..., 0)\}$ such that $f(a_0, ..., a_n) = 0$ if and only if for all primes p there exist $(a_0, ..., a_n) \in \mathbf{Q}_p^{n+1} \setminus \{(0, ..., 0)\}$ such that $f(a_0, ..., a_n) = 0$ and there exists $(a_0, ..., a_n) \in \mathbf{R}^{n+1} \setminus \{(0, ..., 0)\}$ such that $f(a_0, ..., a_n) = 0$.

Proof. The forward direction is trivial. So, consider such a $f \in \mathbf{Q}[X_0, X_1, X_2]$ is a non-degenerate quadratic form with $C_f(\mathbf{R})$ is nonempty and $C_f(\mathbf{Q}_p)$ is nonempty for every prime p. We must show that $C_f(\mathbf{Q})$ is nonempty.

We know the equation has two terms of the same-sign and one of opposite-sign (via the condition for $\mathbf{R}$). By a change of variables, we can diagonalize f and rescale (and re-order the terms) so that the leading coefficient is 1 and the successive terms have negative coefficient, i.e we can write $f(X_0, X_1, X_2) = X_0^2 - aX_1^2 - bX_2^2$ with a, b square free and $0 \neq |a| \leq |b|$.

Now, we will apply induction on the quantity $m = |a| + |b|$. The base case of $|m| = 2$ gives us an equation of the form $f = x_0^2 - x_1^2 - x_2^2$, which clearly has rational solutions in the same manner that we have real solutions. Hence, for $m > 2$, we see $|b| \geq 2$, and so $b = \pm p_1, ..., p_r$ for $p_1, ..., p_r$ distinct (since b is square-free).

We claim that a is a square modulo b. To see this, notice a is a square modulo b if and only if it is a square modulo each p_i, but by assumption, we have a solution in each $\mathbf{Q}_{p_i}$ to this equation, and in-particular we recover a p_i-adic primitive solution in $\mathbf{Z}_{p_i}$, meaning $(x, y, z) \in \mathbf{Z}_{p_i}^3 \setminus p_i\mathbf{Z}_{p_i}^3$ with $z^2 - ax^2 - by^2 = 0$ in $\mathbf{Z}_{p_i}^\times$. Since $p_i \mid b$, this then tells us as long $p_i \nmid x$, $a \equiv z^2x^{-2} \pmod{p_i}$ and hence a is a square modulo each p_i.

So, we need to check $p_i \nmid x$. If $p_i \mid x$, then$p_i \mid b$, $p_i \mid x$, and $z^2 - ax^2 - by^2 \equiv 0 \pmod{p_i}$ tells us $p_i \mid z$, so $p_i^2 \mid z^2$ and $p_i^2 \mid x^2$, hence $p_i^2 \mid by^2$, and since b is square-free this allows us to conclude $p_i \mid y^2$ and hence $p_i \mid y$. This shows the solution is not primitive, a contradiction. Hence, we have $p_i \nmid x$ as desired.

Now that we know a is a square mod b, we know $a \equiv t^2 \pmod{b}$, hence $b \mid t^2 - a$, and $t^2 - a = bb'$. Working mod b tells us we can choose some $t \in \mathbf{Z}$ with $|t| \leq \frac{|b|}{2}$. The key observation is as follows:

$$\begin{aligned} |b'| = \frac{|t^2 - a|}{|b|} &\leq \frac{|t^2|}{|b|} + \frac{|a|}{|b|} \\ &\leq \frac{|b^2|}{4|b|} + \frac{|a|}{|b|} \\ &< \frac{|b|}{4} + 1, \end{aligned}$$

where in the last step we use the fact that $|a| < |b|$. Thus, we see for $|b| \geq 4$ (♣ Our base case was only $m = 2$? I don't see how 3 and 4 are obvious), we have $|b'| < |b|$.

The general idea of the induction is as follows: since $t^2 - a$ is a norm, we will be able to divide out by it to pass from an equation to $|b|$ to an equation in $|b'|$. Formally, we have the following:

For $\mathbf{k} = \mathbf{Q}, \mathbf{Q}_p, \mathbf{R}$, f has a nonzero solution in $\mathbf{k}^3$ if and only if $b \in N(\mathbf{k}[\sqrt[\alpha]{}])^\times$. But, this has a solution if and only if $b' \in N(\mathbf{k}[\sqrt{\alpha}])^\times$ since $t^2 - \alpha$ is a norm and hence can be divided out by. But, $|b'| \leq |b|$, and hence we can look at this equation $f_{b'}(X_0, X_1, X_2) = z^2 - aX_1^2 - b'X_2^2$. Pulling out the square part of b' to get b'' square-free and absorbing this into X_2^2, this equation $f_{b''}(X_0, X_1, X_2) = z^2 - aX_1^2 - b''X_2^2$ has a nonzero solution by induction (since it is solvable in every $\mathbf{Q}_p$ and $\mathbf{R}$, we apply Hasse-Minkowski inductively), and this provides a solution for the equation in $|b|$ in the obvious way. □

2.5 Takeaways

What can we take away from the proof? Although there are a few technical arguments inside of this (which all vaguely feel local-global in scope but for finitely-many primes p_i), the argument rests really upon this inductive step working via the norms. Furthermore, this proof is constructive, in the sense that that we can pass down to b_i small until we are in a case with trivial solutions, at which point these pass back "up" to the original b.

Example 2.11. Take $X^2 - 13Y^2 + 17Z^2$. We first need to find a specific t with $a \equiv t^2 \pmod{b = 17}$, and indeed $t = 8$ will work and satisfies $\frac{8}{17} \leq \frac{1}{2}$, so $8^2 = 13 = (-17)(-3)$, and using $b' = -3$, we reduce to $z^2 - 13x^2 - 3y^2$, at which point we can reduce the 13

term until we arrive at the trivial case with coefficients in $\{-1, 0, 1\}$ which is solvable in the same manner as in $\mathbf{R}$. Actually working this out is reserved for the exercises.

It turns out the Hasse-Minkowski theorem holds not just in $\mathbf{Q}$, but in arbitrary number fields (finite extensions of $\mathbf{Q}$) $\mathbf{K} \supset \mathbf{Q}$. The inductive step is essentially just a question of taking an extension $\mathbf{K}[\sqrt{d}]$ (for $d \in \mathbf{K}$) that is either trivial or quadratic in $\mathbf{K}$, at which point working with squares lets us apply this same "find a norm and divide" method. More generally, for quadratic (or trivial) extensions this kind of statement about norms is a kind of local-global principle in-and-of-itself, which pairs with the rest of this to obtain a proof of the local-global principle for quadratic forms, since the form of a quadratic form resembles a norm.

The problem here lies in unique factorization, since the decomposition $b_1 = \pm p_1, ..., p_r$ cannot hold, and hence it is not possible to check these finitely-many points of failure and stitch them together. It is more complicated in a general number field to come up with a decomposition like this.

2.6 General Method and Failure in Higher Degrees

To solve a conic in $\mathbf{Q}$, we do the following:

1. We solve in $\mathbb{F}_p$ (and we can always do this via **??**).
2. We lift from (1) to $\mathbf{Q}_p$ via Hensel's lemma, or check failure (which is not terribly difficult, as we see via the argument in Section 1.7).
3. Check solvability in $\mathbf{R}$ via signs (this is always easy).
4. If $2 + 3$ work, apply Hasse-Minkowski to find a solution in $\mathbf{Q}$.

However, the conic case is the simplest nontrivial case. We would like to extend this method to higher-degree plane curves $C_f \in \mathbf{P}^2$ by taking a form in $\mathbf{Q}[X, Y, Z]$ of degree d. In general, steps 2 and 3 roughly look the same. It is hard to show this, but it is well-understood. However, at larger degree d, step 1 is no longer guaranteed, and then it can become extraordinarily difficult to identify solutions.

Example 2.12. Fix a prime p. Consider the form $X^{p-1} + Y^{p-1} + Z^{p-1}$ in $\mathbf{Q}[X, Y, Z]$. For $x, y, z \in \mathbf{Z}/p\mathbf{Z}$, $f(x, y, z) \in \{0, 1, 2, 3\}$ and when not all X, Y, Z are zero, this is in $\{1, 2, 3\}$, hence there are no nontrivial solutions modulo p and we cannot raise to modulo p^n and find roots in $\mathbf{Z}_p$ for $p \geq 5$.

So, roughly the last three lectures (the "second half" of this course) will be dedicated to solving higher-degree curves over finite fields (in essence, solving (1) in the higher-degree class), and the next lecture will be dedicated to setting up the algebraic geometry necessary to talk about these objects. This is the content of the Weil conjectures over finite fields, which helped inspire a great deal of modern algebraic geometry. Indeed, a big driving question in modern algebraic geometry is, "Why do these local-global principles fail in higher-degree?"

2.7 Explicit Failure of Hasse-Minkowski

In fact, even if we can solve (2) and (3) despite the difficulties with (1), the Hasse-Minkowski principle will not necessarily guarantee that this will give a rational solution. Hence, the local-global principle does not simply become difficult due to trouble in the base case, but can fail regardless.

Example 2.13 (Famous Example due to Selner). Take $f(X_0, X_1, X_2) = 3X_0^3 + 4X_1^3 + 5X_2^3 \in \mathbf{Q}[X_0, X_1, X_2]$. This has $\mathbf{C}_f(\mathbf{k}) \neq 0$ for $\mathbf{k} = \mathbf{R}, \mathbf{F}_p, \mathbf{Q}$ (this is an exercise), but we have $C_f(\mathbf{Q}) =$.

Showing this is empty is quite tricky and so we will instead show explicit failure of Hasse-Minkowski via a more elementary example.

Example 2.14 (Easier Example(s)). Let p be a prime (hence, we obtain a family of examples parametrized by primes) with $p \equiv 1 \pmod 8$ and $\left(\frac{2}{p}\right)_4 \neq 1$ (meaning $x^4 - 2 \pmod p$ has no solution). For example, $p = 17$ satisfies these properties.

Now, consider the affine (over $\mathbf{Q}$) plane curve $C^0 \subset \mathbf{A}^2$ defined by $\{W^2 = 2 - 2pZ^4\}$. C^0 is nonsingular.

Form a projective curve $\bar{C^0} \in \mathbf{P}^2$ by $\{W^2T^2 = 2T^4 - 2pZ^4$. It is not hard to check that $\bar{C^0} \cap \{T \neq 0\} \cong C^0$, and $\bar{C^0} \cap \{T = 0\} = [0, 1, 0]$, but this point $[0, 1, 0]$ is (a) singular point of $\bar{C^0}$ where here we are working in an affine subspace of $\mathbf{P}^2$. This singularity prevents us from solving in $\mathbf{Q}^2$.

While this example fails to "really" embed C^0 in a curve since the resultant curve has a singular point, the following is a general result saying it is possible to embed C^0 in a space where the embedded curve can have higher degree.

Theorem 2.15. Let C^0 be any nonsingular affine curve. Them, there exists a non-singular projective curve in possibly-higher-dimension-than-C^0 such that $C^0 \cong C \setminus \{$ finitely-many primes $\}$. In the meaning up to isomorphism, this construction maybe finitely-many points in C^2 works better.

Example 2.16. From this curve, $\bar{C^0}$ is still an equation in $\mathbf{P}^2$, and to solve this in this manner, we would have to solve in $\mathbf{P^n}$ (essentially requring some higher m) and would have to reduce to $n = 2$ norm.

Define $C \subset \mathbf{P}^3$ to be the intersection of $X_1X_3 = X_1^2$ and $0 = X_2^2 - 2X_0^2 + 2pX_3^2$. Then, take $C^{(0)} \subset \{x_0 \neq 0\}$ by f, and we can identify (w, z) with $[1, z, w, z^2]$, hence C $C^0 = C \cap \{X_0 = 0\}$, and this last set can be parametrized by $[0, 0 \pm \sqrt{p}]$.

The exercises involve a great deal of checking claims in this example. The ideas and results here may seem wildly motivated, but once we survey some basic ideas in geometry next time, it will be very clear. Next time, we will continue on with places where the Hasse principle fails, then develop the language of algebraic geometry.

2.8 Day 2 Exercises

Exercise 2.1. Prove the refined-version of the single-variable Hensel's lemma stated in class.

Exercise 2.2. For each prime p, determine the number of roots of unity (elements x such that $x^n = 1$ for some $n \geq 1$) in $\mathbf{Q}_p$. (Hint: Use Hensel's lemma)

Exercise 2.3. Let $f(X_0, X_1, X_2) \in \mathbf{Z}[X_0, X_1, X_2]$ be a homogenerous degree 2 polynomial, defining the conic $C_f \subset \mathbf{P}^2$. Assume f is non-degenerate (C_f is nonsingular). Show that for all but finitely-many primes p, $C_f(\mathbf{Q}_p) \neq \emptyset$. For $f(X_0, X_1, X_2) = X_0^2 + X_1^2 - 3X_2^2$, determine $\{p : C_f(\mathbf{Q}_p)\} \neq \emptyset$.

Exercise 2.4. Legendre's proof of the three-variable Hasse-Minkowski theorem is effective: follow the proof to compute a rational point on the projective curve given by $f(X_0, X_1, X_2) = X_0^2 - 13X_1^2 + 17X_2^2$.

Exercise 2.5. Let k be any field, and let $f \in \mathbf{k}[X_1, X_2, X_3]$ be a homogeneous polynomial of degree 2. Assume that the projective conic $C_f \subset \mathbf{P}^2$ is nonsingular, and that $C_f(\mathbf{k})$ is nonempty. Fix a point $P_0 \in C_f(\mathbf{k})$ and a linear homogeneous polynomial $L(X_0, X_1, X_2) \in \mathbf{k}[X_0, X_1, X_2]$ such that the vanishing locus $C_L \subset \mathbf{P}^2$ does not contain the point P_0.

1. Show that the projection map

$$\pi : C_f \to C_L$$

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 gives a bijection $C_f(K) \to C_L(K)$ for all $\mathbf{K} \supset \mathbf{k}$.

2. If you know what this means, show that π is in-fact an isomorphism of algebraic varieties over $\mathbf{k}$. This implies (a) (this problem is a separate approach from the other one for those who have not necessarily learned what a morphism of vareties is). If you don't know what this means, still try to write algebraic formulae for π: what kinds of functions are required?

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

Exercise 2.6. Let $p \equiv 1 \pmod 8$ be a prime such that 2 is not a 4th power in $\mathbf{F}_p$. Let $C^0 \subset \mathbf{A}^2$ be the affine curve over $\mathbf{Q}$ defined by the polynomial $f(w, z) = w^2 - 2 + 2pz^4$. In class we constructed a nonsingular projective curve $C \subset \mathbf{P}^3$ and an isomorphism $C^0 \to C \setminus \{[0, 0, \pm\sqrt{-2p}, 1]\}$. Show that $C(\mathbf{Q}_2) \neq \emptyset$.

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

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

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

3 Day 3

3.1 Overview

Last time, we discussed the curve $C_0 = \{w^2 = 2 - 2pz^4\}$ in $\mathbf{A}^2$, which we could embed in a "projective closure" C by taking $C = \{X_1X_3 = X_1^2\} \cap \{0 = X_2^2 - 2X_0^2 + 2pX_3^2\} \subset \mathbf{P}^3$, in which-case $C^{(0)}$ arises as the subset of C with the condition $X_0 \neq 0$, where we can identify $[1, z, w, z^2]$, and the complement $C \setminus C_0 = C \cap \{X_0 = 0\}$, which is parametrized by $[0, 0, \pm\sqrt{p}, 1]$.

We claimed that this curve C_0 was a higher-degree curve with solutions in every $\mathbf{Q}_p$ and in $\mathbf{R}$, but not in $\mathbf{Q}$. Now, of course, we should actually justify this, as to illustrate failure of the local-global principle. In the process of this, we will begin to define some general notions in algebraic geometry.

Mathematically, the natural question after examples like this showed that the Hasse principle failed for higher-degree terms is "how can we salvage it"? This led to the development of the Weil conjectures for finite fields. Using the algebraic-geometric language described before, we will be able to state the Weil conjectures, and assuming the Riemann-Roch theorem, be able to prove many of them.

3.2 Failure in Q

Proposition 3.1. The curve $C_0 = \{w^2 = 2 - 2pz^4\}$ for $p \equiv 1 \pmod 8$ and 2 not a fourth power of p (equivalently, $\left(\frac{2}{p}\right)_4 \neq 1$) has no solutions in $\mathbf{Q}$, equivalently, $C_0(\mathbf{Q}) = 0$.

Proof. Suppose there exists $(w, z) \in C^0(\mathbf{Q})$ such that $w^2 = 2 - 2pz^4$. We aim to turn this into an integer equation so we can work modulo p in a straightforward manner. Write z as $z = \frac{r}{t}$ with r, t coprime in $\mathbf{Z}$ to get:

$$w^2 = 2 - 2p\frac{r^4}{z^4},$$

which gives:

$$t^4w^2 = 2t^4 - 2pr^r$$

. Now, write $w = \frac{a}{b}$ as a ratio of coprime integers, such that the left-hand-side becomes $\frac{t^4a^2}{b^2}$ and since the right-hand-side is already integral, $b^2 \mid t^4a^2$, but since a, b were already corpiem, this tells us $b^2 \mid t^4$ which tells us $b \mid t^2$, so we can write $t^2 = b \cdot u$ for u in $\mathbf{Z}$, and then we see $w = \frac{au}{t^2}$. Plugging in, we get:

$$a^2u^2 = 2(t^4 - pr)$$

and so $2 \mid a \cdot u$, hence $w = 2 \cdot \frac{s}{t}$, and now plugging this in gives:

$$4s^2 = 2t^4 - 2pr^4$$

and dividing gives:

$$2s^2 = t^4 - pr$$

and this is an equation in $\mathbf{Z}$. Now, we do the obvious thing - take the equation modulo p. We get:

$$2s^2 \equiv t^4 \pmod{p}$$

So, if we can show s is a square modulo p, we can plug this in, we will then see 2 is a fourth power modulo p, a contradiction of our assumptions.

So, consider any odd prime q dividing s. Take the equation $2s^2 = t^4 - pr^4$ modulo q to see:

$$0 \equiv 2s^2 \equiv t^4 - pr^4 \pmod{q}$$

and hence:

$$p \equiv \frac{t^4}{r^4} \pmod{q}$$

and so $\left(\frac{p}{q}\right) = 1$. Since $p \equiv 1 \pmod 4$, reciprocity tells us $\left(\frac{q}{p}\right) = 1$. Since $p \equiv 1 \pmod 8$, we have $\left(\frac{2}{p}\right), \left(\frac{-1}{p}\right) = 1$, and therefore we multiply to get that $\left(\frac{s}{p}\right) = 1$.

Hence, we see 2 is indeed a 4th power, contradicting the assumption that $\left(\frac{2}{p}\right)_4 = -1$, and hence there are no rational points on this curve. □

3.3 Solvability in R, $\mathbf{Q}_k$ for $l = 2, p$

Now that we have shown there are no rational solutions, to demonstrate failure of Hasse-Minkowski, we need to check there are solutions in $\mathbf{R}$ and $\mathbf{Q}_p$. There are of-course solutions in $\mathbf{R}$ simply by taking $w = \sqrt{2}$, $z = 0$. So, we need to check solvability in $\mathbf{Q}_l$, which by Hensel's Lemma, is essentially equivalent to checking solvability modulo l, for all primes l. There are three different kinds of primes:

1. $l = p$
2. $l = 2$
3. $l \neq p, 2$

So, let us start with Case 1: $l = p$. The equation modulo p just becomes:

$$w^2 = 2$$

and hence we just take w equal to a square root of p (which exists since $p \equiv 1 \pmod 8$) and z to be anything. We have:

$$\begin{pmatrix} \frac{\partial f}{\partial w} & \frac{\partial f}{\partial z} \end{pmatrix} = \begin{pmatrix} 2w & 0 \end{pmatrix}$$

and this is not equal to zero for $w_0, *$ as chosen before, hence by Hensel, we get a solution in $\mathbf{Z}_l$.

Case 2 is $l = 2$. We leave this as an exercise. In particular, we claim that C^0 and even $(C \subset \mathbf{P}^3)$ are nonsingular and hence Hensel allows us to reduce the problem to checking if there exists a modulo l solution.

3.4 General-Case for $l \neq 2, p$

There are two ways to approach checking case 3 of l a prime not equal to 2, p. The first is a more-general machine in algebraic geometry. Essentially, it is as follows:

Let C be a projective $(C \subset \mathbf{P}^n)$ be a nonsingular curve, and $\mathbf{F}_q$ a finite field of order q (q is a prime power):

Assume $\bar{C} = C_{\bar{\mathbf{F}}_q}$ is irreducible, considering the curve in an algebraic closure of $\mathbf{F}_q$. Let g be the genius of $\bar{C}$. Then, the following bound holds:

$$|\#C(\mathbf{F}_q) - (q+1)| \leq 2g\sqrt{q}$$

How does this give the result? Recall C is the intersection of 2 quadrics in $\mathbf{P}^3$. This tells us that $g = 1$, and then plugging in, we see:

$$|\#C(\mathbf{F}_q) - (l+1)| \leq 2\sqrt{l}$$

but in particular, we see $\#C(\mathbf{F}_q) \neq 0$, as otherwise we would obtain $l - 2\sqrt{l} + 1 = (\sqrt{l} - 1)^2 \leq 0$, which is not possible for $l > 1$.

Example 3.2. Take the projective line over $\mathbf{F}_q$ $\mathbf{P}^1 = \frac{\mathbf{F}_q \backslash 0}{\mathbf{F}_q}$ and consider this as a curve itself. We have that there are exactly $q + 1$ solutions in $\mathbf{P}^1$ to the curve $\mathbf{P}^1$, and this arises exactly from the fact that the genus of $\mathbf{P}^1$ is 0 (hence making the difference $\#C(\mathbf{F}_q) - (q+1)$ an exact equality).

At this point, it is easy to check the curve is non-singular, and hence we can apply Hensel to see $C(\mathbf{Q}_k) \neq$ for l prime not equal to 2, p. This arises from the Riemann hypothesis over finite fields (this is one of the Weil conjectures). Elliptic curves are curves with genius 1, and this bound for elliptic curves over finite fields was proven by Hasse. Weil proved this bound for general curves and formulated his conjectures, which were left unsolved until Grothendieck's theory of schemes allowed Pierre Deligne (one of Grothendieck's students) to prove the Weil conjectures.

Now, this general technique is very powerful, but we have not even defined a large number of the terms in the preceding paragraphs, nor do we have any idea how to even begin proving this theorem. A large part of the remainder of the course is dedicated to building up the necessary geometry to actually talk about this (which we start in the next subsection). However, for completeness, we will also provide a more technical, but elementary, solution for the case of the curve $C^0 = \{w^2 = 2 - 2pz^4\}$ leveraging reciprocity relations.

3.5 Basic Notions in Algebraic Geometry

For this section, take $\mathbf{k}$ a field and consider $\bar{\mathbf{k}}$ an algebraic closure of $\mathbf{k}$.

Definition 3.3 (Affine Variety). An affine variety $X \subset \mathbf{A}^n$ (over $\bar{\mathbf{k}}$) is the zero set:

$$X = V(S) = \{p \in \mathbf{A}^n(\mathbf{k}) \mid f(p) = 0 \text{ for every } f \in S\}$$

for some subset $S \subset \bar{\mathbf{k}}[x_1, ..., x_n]$.

Put plainly, an affine variety in $\mathbf{A}_n$ is simply the zero set of some set of polynomials in the variables $x_0, x_1, ..., x_n$.

Definition 3.4 (Ideal of a Subset of Affine Space). The ideal $I(X)$ of a subset X of Affine Space is the set:

$$I(x) = \{g \in \bar{\mathbf{k}}[x_1, ..., x_n] \mid g(p) = 0 \text{ for every } p \in X$$

The definition of the ideal of a set X is essentially the converse of the definition of a variety - instead of taking the zero set of a given set of polynomial, we take the polynomials who are zero on a fixed set. It can be readily checked this is indeed an ideal.

Definition 3.5 (Affine Coordinate Ring of a Variety). Given X a variety, the affine coordinate ring of X is the ring:

$$\bar{\mathbf{k}}[X] = \bar{\mathbf{k}}[x_1, ..., x_n]/O(X)$$

This ring is essentially the equivalence classes of nontrivial functions on affine space up to the variety X.

Definition 3.6 (Irreducible Variety). We say X is an irreducible variety if $I(X)$ is a prime ideal.

(For those unfamliar, a prime ideal is an ideal J such that if $ab \in J$, $a \in J$ or $b \in J$).

It will be an exercise to check that a curve C is irreducible if and only if X is not "reducible" in the sense that X is not $V(S_1) \cup V(S_2)$ for proper subsets $V(S_1), V(S_2)$ of X.

Example 3.7. Let $f(x) \in \mathbf{k}[x, y]$ be an irreducible polynomial. Then, define $X = V(f)$ to be the zero set of V in affine 2-space $\mathbf{A}^n$. This will be a variety, and it is true that $I(V(f)) = \langle f \rangle$. This claim needs to be checked, but is an instance of a more general theorem called Hilbert's Nullstellensatz, which is fundamental to studying algebraic geometry.

Then, since we are in a polynomial ring, an irreducible polynomial generates a prime ideal, and as such, the affine coordinate ring of X will be an integral domain. More specifically, we will see:

$$\bar{\mathbf{k}}[X] = \bar{\mathbf{k}}[x, y]/\langle f \rangle \cong \bar{\mathbf{k}}[x]$$

is an integral domain.

Definition 3.8 (Field of Rational Functions on X). Let X be an irreducible affine variety. Consider the affine coordinate ring $\bar{\mathbf{k}}[X]$, and consider its fraction field $\bar{\mathbf{k}}(X) = \text{frac}\left(\bar{\mathbf{k}}[X]\right)$. This is the field of rational functions on X.

Since X is irreducible, the affine coordinate ring is a domain, and hence forming this field of fractions is justified.

Example 3.9. Let X be all of affine n-space, $\mathbf{A}^n$. Then, $\mathbf{k}(X) = \bar{\mathbf{k}}(X_1, ..., X_n)$.

Definition 3.10 (Dimension of an Irreducible Variety). Given an irreducible variety X, define dim X to be the transcendence degree of $\bar{\mathbf{k}}(X)$ over $\bar{\mathbf{k}}$.

Example 3.11. Consider the variety $\mathbf{A}^n$ (take it on faith that this is irreducible). We have already seen its coordinate ring is $\bar{\mathbf{k}}[x_1, ..., x_n]$, and hence its transcendence degree over $\mathbf{k}$ is n, hence $\dim(\mathbf{A}^n) = n$.

Example 3.12. As before, take $f \in \mathbf{k}[x, y]$ to be an irreducible polynomial with $X = V(f)$. Then,

$$\bar{\mathbf{k}}[X] = \bar{\mathbf{k}}[x, y]/\langle f \rangle.$$

We claim $\dim(f) = 1$. Clearly, $\dim(f) \leq 1$ since $\langle f \rangle$ is not trivial for f a nontrivial irreducible polynomial. How do we know it is not zero? Since f is nontrivial, at least one of x, y appears in f. Without loss of generality, let this be x. Then, we claim $\bar{y}$, the image of y in $\mathbf{k}[X]$ under the natural projection $\bar{\mathbf{k}}[x_1, ..., x_n] \to \bar{\mathbf{k}}[X] = \bar{\mathbf{k}}[x_1, ..., x_n]/I(X)$, is transcendental over $\bar{\mathbf{k}}$.

Otherwise, since $\bar{\mathbf{k}}$ is algebraically closed, $\bar{y}$ is a root of some polynomial in $\bar{\mathbf{k}}[x]$, and then we have $\bar{y} \in \bar{\mathbf{k}}$, but then since $\langle f \rangle$ contains x already, $\langle f \rangle$ would consist of all of $\bar{\mathbf{k}}[x, y]$, contradicting nontriviality of f. Hence, $\bar{\mathbf{k}}[X]$ is generated by at least one transcendental element $\bar{y}$ and hence has transcendence degree ≥ 1, but we have already seen it has transcendence degree ≤ 1, so it is exactly 1.

All of this work with the variety generated by an irreducible polynomial $f \in \mathbf{k}[x, y]$ has revolved around our assumption that $I(V(f)) = \langle f \rangle$. Now, we will attempt to prove this fact. First, though, we need some lemmas.

Lemma 3.13. Given f irreducible and g in $\bar{\mathbf{k}}[x, y]$ with $f \nmid g$, the variety $X(f, g)$ of simultaenous solutions to f and g is finite.

More plainly, the intersection of an irreducible curve with a curve not a multiple of it has finitely-many points.

Proof. By Gauss's lemma, since f is irreducible, we may embed into $\bar{\mathbf{k}}(x)[y] = \left(\text{Frac}\, \bar{\mathbf{k}}[x]\right)[y]$ to see that f and g are coprime. Since we are now working over a field, Bézout's identity guarantees the existence of $u, v \in \bar{\mathbf{k}}(x)[y]$ such that

$$u \cdot f + v \cdot g = 1.$$

We can clear denominators by multiplying through by a common denominator $w \in \bar{\mathbf{k}}[x]$ to obtain:

$$(wu) \cdot f + (wv) \cdot g = w,$$

where $wu, wv \in \bar{\mathbf{k}}[x, y]$ and $w \in \bar{\mathbf{k}}[x]$.

Now, at any point $(a, b) \in V(f, g)$, the left-hand-side vanishes, hence $w(a, b) = 0$, but w is a polynomial only of x, hence a is a root of w, but there are finitely-many roots of

w, so there are finitely-many choices for a. An analagous argument working in $\bar{\mathbf{k}}(Y)$ tells us the values of b are roots of some polynomial w' , and then this is also a finite-set, so there are finitely-many choices for b, so there are finitely-many (a, b) (not all of which are necessarily even roots to begin with), proving the claim. □

Lemma 3.14. Given f an irreducible polynomial in $\mathbf{k}[x, y]$, $V(f)$ is infinite.

Proof. Since at least one of x, y is in x, we can write $f(x, y) = \sum_{i=0}^{n} x^i c_i(y)$ with at least one of the $C_i(y) \neq 0$, $i \neq 0$ for some $i \neq 0$.

Then, $c_{i_0}(y)$ would have finitely-many roots $S_{i_0} \in \bar{\mathbf{k}}$, so for any $t \in \bar{\mathbf{k}} \setminus \{0\}$, $f(x, t)$ is non-constant in $\bar{\mathbf{k}}[x]$, hence it will have roots in $\bar{\mathbf{k}}$ (since it is algebraically closed), and so $V(f) \supset \bigcup_{t \in \bar{\mathbf{k}}} \{((\text{a root of } f(x, t), t)\}$ is going to be an infinite set (since it is an infinite union of disjoint sets). □

Proposition 3.15. Given f an irreducible polynomial in $\mathbf{k}[x, y]$ with $\langle f \rangle$ with $X(f)$ the variety of f, then $I(X(f)) = \langle f \rangle$.

Proof. Consider $g \in I(V(f))$. By the lemma, if $f \nmid g$, we can conclude $V(f) = V(f, g)$ is finite, but this is of course a contradiction of the lemma. □

More generally, given an ideal $J \subset \bar{\mathbf{k}}[x_1, ..., x_n]$ and the associated variety $V(J)$, one may ask, what is $I(V(J))$? Certainly, this contains J, and as we have seen just now, for irreducible curves f, this is exactly $\langle f \rangle$. The following example illustrates this is not always the case:

Example 3.16. Cosnider $\bar{\mathbf{k}}[x]$ and the ideal $J = \langle x^2 \rangle$. Then, $V(J) = \{0\}$ (as $x^2 = 0$ if and only if x is zero), but then $I(V(J)) = \langle x \rangle$ which strictly contains $\langle x^2 \rangle$.

This illustrates the prior question is actually nontrivial. This was solved by Hilbet.

Definition 3.17 (Radical of an Ideal). If I is an ideal in a ring R, define $\text{Rad}(I)$ to be the set of all "nth roots" of elements in I, that is, $\{a \in R \mid a^n \in I \text{ for some } n \in \mathbf{Z}^+\}$.

Theorem 3.18 (Hilbert's Nullstellensatz). Let I be an ideal in $\bar{\mathbf{k}}[x_1, ..., x_n]$. Then,

$$I(V(I)) = \text{Rad}(I)$$

Conceretely, this says if $f_1, f_2, ..., f_r$ and g are polynomials in $\mathbf{k}[x_1, ..., x_n]$ such that g vanishes when the f_i vanish, then there exists n such that $g^n = a_1 f_1 + a_1 f_2 + ... + a_n f_n$ for some $a_i \in \mathbf{k}[x_1, ..., x_n]$.

The Nullstellensatz is a critical result and is very important elsewhere in algebraic geometry.

3.6 Solvability for $l \neq 2, p$

Now, we will attempt to provide an elementary argument for showing the curve $C^0 = \{w^2 = 2 - 2pz^4\}$ has solutions in $\mathbf{Q}_l$ for l a prime not 2 or p. In fact, we will be able to show there are solutions in the set $C(\mathbf{F}_l)$ as opposed to the smaller set $C^0(\mathbf{F}_l)$. As discussed before, via nonsingularity and Hensel it suffices to find a solution in $\mathbf{Z}/l\mathbf{Z}$.

Essentially, we will look for non-zero solutions (w, x, z) to the equation $w^2 = 2x^4 - 2pz^4$ in $\mathbf{F}_l$. If $x \neq 0$, dividing by x gives a rational solution $W^2 = 2 - 2pZ^4$ with $W = \frac{w}{x}$ and $Z = \frac{z}{x}$ to $C^0 \subset C$.

If $x = 0$, then $w^2 = -2pz^4$, but this means $\left(\frac{-2p}{l}\right) = 1$, so we have a square root of $2 - p$. Hence, since $C \setminus C^0$ consists of the points $[0, 0, \pm\sqrt{-2p}, 1]$, these points indeed lie in $\mathbf{F}_l$, showing $C(\mathbf{F}_l)$ is non-empty as desired.

Proposition 3.19. For any $l \neq 2$, $a, b \in \mathbf{F}_l^\times$, $aX^4 + bY^2 = Z^2$ has a nonzero $\mathbf{F}_l$ solution.

Proof. The curve $aX_0^2 + bX_1^2 = X_2^2$ has a non-zero solution in $\mathbf{F}_l$ (via counting), so we can can find a family of rational points on $aX_0^2 + bY_0^2 = Z_0^2$ (in the same manner as Exercise 5 from Day 1) paramterized by t of the form $(x_0(t), x_1(t), x_2(t)$ with $x_i(t) \in \mathbf{F}_l[t]$ all nonzero, of degree ≤ 2, and pairwise nonassociate. Additionally, at least 2 must actually be degree 2.

It will be an exercise to explicitly work out the following via the chord parametrization from Day 1 Exercise 5. We get:

$$a(bx_0t^2 - 2bx_1 - ax_0)^2 + b(-bx_1, t^2 - 2ax_0t + ay_1)^2 = (bt + a)^2.$$

We want a point on this conic $ax_0^2 + by_0^2 = z_0^2$ such that we can actually obtain a point on the conic $ax_0^4 + by_0^4 = z_0^2$. The way we will obtain this point is essentially via taking a solution to the conic and using reciprocity to find new points with x_0', y_0' squares, hence giving us a solution to the quartic equation.

Since $x_0(t), x_1(t)$ are not associate, there must exist some $t_0 \in \mathbf{F}_k$ such that

$$\left(\frac{x_0(t_0)}{l}\right) \neq \left(\frac{x_1(t_0)}{l}\right)$$

Why? If not, $\left(\frac{x_o(t_0)}{l}\right) = \left(\frac{x_1(t_0}{l}\right)$ for every $t_0 in \mathbf{F}_l$, but then $x_0(t)^{\frac{l-1}{2}} - x_1(t)^{\frac{l-1}{2}}$ will be a polynomial in t of degree at most $l - 1$ that vanishes at all $t \in \mathbf{F}_l$, but then this is either the zero polynomial or a multiple of the degree l polynomial given by $x(x-1)...(x-(l-1))$. The latter case contradicts unique factorization since the polynomial is of degree $l - 1$, so we must be in the zero case $x_0(t)^{\frac{l-1}{2}} = x_1(t)^{\frac{l-1}{2}}$ as polynomials, but this implies they are indeed associate, a contradiction.

The same argument works when we take $x_1(t)'$ to be $x_1(t) \cdot c$ for c a non-square in $\mathbf{F}_k$ (since this is a unit). Then, this tells us there exists some t_0 with:

$$\left(\frac{x_0(t_0)}{l}\right) \neq \left(\frac{x_1(t_0)'}{l}\right) = \left(\frac{cx_1(t_0)}{l}\right) = \left(\frac{c}{l}\right)\left(\frac{x_1(t_0)}{l}\right) = -\left(\frac{c}{l}\right)\left(\frac{x_1(t_0)}{l}\right).$$

So, in all cases, we can find a t_0 such that either x_0 and x_1 are both squares or both non-squares (technically, there is some ambiguity due to zero case, but these cases can manually be sorted out). Then, no matter what, we can choose these in such a way that $(x_0)(t_0) \cdot (x_1)(t_0)$ is a square c not zero. More explicitly, the cases are $x_0(t_0) = 0$ with

$x_1(t_0)$ is not zero and $c = 0$, $x_0(t_0)$ nonzero with $x_1(t_0) = 0$ and $c = 0$, or $x_0(t_0)$ and $x_1(t_0)$ nonzero with the same legendre symbol $c \neq 0$.

So, now, consider the case of $x_0(t_0) \neq 0$. Then, $(x_0(t_0), c, x_0(t_0)x_2(t_0))$ is a solution to $aX^4 + bY^4 + Z^2$ since:

$$a(x_0(t_0))^4 + bc^4 = x_0(t_0)^2 x_2(t_0)^2$$

happens if and only if we can divide out by $x_0(t)^2$, which we can by this construction.

In the case of $x_1(t_0) = 0$, $(c_1 x_1(t_0), x_1(t_0), x_1(t_0)x_2(t_))$ is a solution. □

This very-long-winded (but quite-pretty!) argument has given us failure of the local-global principle of the Hasse-Minkowski Theorem. Next time, we will move towards building the language necessary to discuss the Weil conjecture about finite fields, which will essentially amount to shifting from a concrete example-driven approach to curves here to a more abstract approach, which will allow us to (assume) the Riemann-Roch theorem for curves and provide proofs of most of the Weil conjectures (although not quite a proof of the Riemann hypothesis).

3.7 Exercises

Exercise 3.1. Let $\mathbf{k}$ be an algebraically closed field, and let $X \subset \mathbf{A}^n$ and $Y \subset \mathbf{A}^m$ be affine varieties over $\mathbf{k}$. We define a morphism (or regular map) of affine varieties $f : XtoY$ to be an m-tuple $f = (f_1, ..., f_m)$ of elements $f_i \in \mathbf{k}[X]$ (the affine coordinate ring: recall $\mathbf{k}[X] = \mathbf{k}[x_1, ..., x_n]/I(x)$ such that for all $p \in X$, $f(p) \in Y \subset \mathbf{A}^m$.

1. Verify the following are morphisms:
   (a) $f : \mathbf{A}^1 \to Y = V(y^2 - x^3) \subset \mathbf{A}^2$ given by $f(t) = (t^2, t^3)$.
   (b) When $\mathbf{k}$ has characteristic $p > 0$, and $X \subset \mathbf{A}^n$ is defined over the finite field $\mathbf{F}_q$ (q is a power of p), i.e $I(X)$ is generated by polynomials in $\mathbf{F}_q$, the map $F : X \to X$ given by $F(a_1, ..., a_n) = (a_1^q, ..., a_n^q)$ (Extra: if X is not defined over $\mathbf{F}_q$, can you describe an affine variety $X^{(q)}$ such that the above formula defines a morphism $F : X \to X^{(q)}$?) Also, verify that:
   $$\{p \in X(\bar{\mathbf{F}}_q) \mid F(p) = p\} = X(\mathbf{F}_q).$$
2. Show that a morphism $f : X \to Y$ as above defines a $\mathbf{k}$-algebra homomorphism (i.e a ring-morphism that is $\mathbf{k}$-linear) $f^\# : \mathbf{k}[Y] \to \mathbf{k}[X]$.
3. Conversely, explain how any $\mathbf{k}$-algebra homomorphism $\varphi : \mathbf{k}[Y] \to \mathbf{k}[X]$ has the form $\varphi = f^\#$ for some morphism $f : X \to Y$.
4. Deduce that the last two parts induce a bijection between $\mathbf{k}$-algebra homomorphisms $\mathbf{k}[Y] \to \mathbf{k}[X]$ and morphisms $X \to Y$ of affine varieties.

Exercise 3.2. Let $X \subset \mathbf{A}^n$ be an affine variety over an algebraically closed field $\bar{k}$. Exhibit a bijection between points of X and maximal ideals of $\bar{k}[X]$.

Exercise 3.3. The most concrete definition of an elliptic curve over a field $\mathbf{k}$ of characteristic not $2, 3$ is the following: it is a nonsingular projective curve $C = V(F) \subset \mathbf{P}^2$ where:

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

for some $A, B \in \mathbf{k}$, along with its evident $\mathbf{k}$-rational point $[0, 1, 0]$. Show such an equation in-fact defines a *nonsingular* curve if and only if $\Delta(A, B) = -16(4A^3 + 27B^2)$ is nonzero in $\mathbf{k}$.

(Of course, the factor of -16 does not affect - in characteristic not equal to 2 - whether Δ is zero. This normalization factor is conventional and reflects the fact that such a curve is always singular in characteristic 2.

Exercise 3.4. Consider the plane curve $C = V(y^2 - x^3 - x) \subset \mathbf{A}^2$ over a field $\mathbf{k}$ of characteristic not 2.

1. Show that the projective closure $\bar{C} = V(Y^2Z - X^3 - XZ^2) \subset \mathbf{P}^2$ of C is nonsingular (in particular, C is).

2. Let $P = (0, 0) \in C$, and let v_p be the associated discrete valuation of $\mathbf{k}(C)$ (as defined in Monday's class). Compute $v_P(x)$ and $v_P(y)$.

3. The affine space $\{Y \neq 0\} \subset \mathbf{P}^2$ has coordinate functions $u = X/Y$ and $z = Z/Y$, i.e, its coordinate ring is the polynomial ring $k[u, v]$. Write in terms of u and v the equation of $C' = \bar{C} \cap \{Y \neq 0\} \subset \{Y \neq 0\} \cong \mathbf{A}^2$. Write down the canonical isomorphism $\mathbf{k}(C) \cong \mathbf{k}(C')$.

4. Let Q be the unique point in $\bar{C} \setminus C$ (you should know from part a what Q is). Compute $v_Q(x)$ and $v_Q(y)$, identifying x and y as elements of $\mathbf{k}(C')$ as in the last part.

Exercise 3.5. Consider the plane curve $C = V(y^2 - x^3 - X^2) \subset \mathbf{A}^2$. Show that C is singular at $P = (0, 0)$ and check $\mathcal{O}_{C,P}$ is not a DVR.

Exercise 3.6. Let $v : \mathbf{Q}^\times \to \mathbf{Z}$ be a surjective discrete valuation. Show that $v = v_P$ for some prime number p.

Exercise 3.7. Let $v : \bar{\mathbf{k}}(t)^\times \to \mathbf{Z}$ be a surjective discrete valuation trivial on $\bar{\mathbf{k}}$ (here $\bar{\mathbf{k}}$ is algebraically closed). Show either there exists $a \in \bar{\mathbf{k}}$ such that $v = v_{t-a}$ or $v = v_\infty$. (See the appendix for definitions of these valuations). How would you describe the discrete valuations on $\mathbf{k}(t)$ (trivial on $\mathbf{k}$) when $\mathbf{k}$ is not necessarily algebraically closed?

A Preliminary Algebra

A.1 Transcendence Degree

The exposition here is primarily from Brian Conrad's Graduate Algebra Course, and is taken almost word-for-word (but included for completeness).

Definition A.1 (Algebraically Independent Set). Let $L \supset \mathbf{k}$ be an arbitrary field extension. A subset $S \subset L$ is called algebraically independent over $\mathbf{k}$ if for all finite sets of elements $a_1, ..., a_n \in S$, no nonzero $f \in \mathbf{k}[X_1, ..., X_n]$ satisfies $f(a_1, ..., a_n) = 0$ in L. If a subset S is not algebraically independent, we call it algebraically dependent.

Equivalently, this says that the evaluation map $\mathbf{k}[X_1, ..., X_n]$ given by $f(X_1, ..., X_n) \to f(a_1, ..., a_n)$ has trivial kernel. However, the map is surjective by construction, meaning:

Proposition A.2. A subset $S \subset L$ is algebraically independent if and only if for all finite sets of elements $a_1, ..., a_n \in S$, $\mathbf{k}[X_1, ..., X_n] \cong \mathbf{k}[a_1, ..., a_n$.

There are close analogies between algebraically independent subsets of a field extension $L \supset \mathbf{k}$ and linearly independent subsets of a vector space V over $\mathbf{k}$.

Definition A.3 (Maximal Algebraically Independent Subset). We say an algebraically independent subset $S \subset L$ over $\mathbf{k}$ is maximal if it is not a proper subset of another algebraically independent set $S' \subset L$.

Proposition A.4. An algebraically independent subset $S \subset L$ over $\mathbf{k}$ is maximal if and only if the extension $L \sup \mathbf{k}(S)$ is an algebraic extension.

Proof. For $L \sup \mathbf{k}(S)$ to be algebraic means for all $a \in L$ there is some nonzero $f \in \mathbf{k}(S)[X]$ such that $f(a) = 0$. Indeed, if such an f exists (for a given $a \in L$), it involves just a finite set of elements $s_1, ..., s_n \in S$ in its coefficients (relative to X), so by scaling against a nonzero common denominator in $\mathbf{k}[s_1, ..., s_n]$ we can conclude:

$$f \in \mathbf{k}[s_1, ..., s_n][x] = \mathbf{k}[s_1, ..., s_n, X]$$

and hence the relation $f(a)$ with $\deg_X(f) > 0$ shows $S \cup \{a\}$ is not algebraically independent for any a, so S is maximal.

Conversely, suppose S is maximal as an algebraically independent set in L over $\mathbf{k}$. We must show L is algebraic over $\mathbf{k}(S)$. For any $a \in L - S$, maximality tells us $S \cup \{a\}$ is algebraically dependent, and so for some $s_1, ..., s_n \in S$, there is a nonzero $f \in \mathbf{k}[X_1, ..., X_n, X_{n+1}]$ such that $f(s_1, ..., s_n, a) = 0$. But, f must involve X_{n+1}. Otherwise, this would be a polynomial in $f(s_1, ..., s_n)$ equalling zero, violating the algebraic independence of $\{s_1, ..., s_n\} \subset S$ over $\mathbf{k}$. Hence, we see that:

$$f = h_d X_{n+1}^d + ... + h_1 X + h_0$$

for $h_j \in [X_1, ..., X_n]$ with $d > 0$ and $h_d \neq 0$. Then:

$$0 = f(s_1, ..., s_n, a) = \sum_j h_j(s_1, ..., s_d) a^j$$

and so $h_d(s_1, ..., s_n) \neq 0$ in L since $h_d \neq 0$ and $\{s_1, ..., s_n\}$ is algebraically independent over $\mathbf{k}$ as desired. □

The following theorem will allow us to define the transcendence degree of a finitely-generated field extension:

Theorem A.5. Let $L \supset \mathbf{k}$ be a finitely-generated field extension, with $\{a_1, ..., a_n\}$ a finite subset of L generating L over $\mathbf{k}$.

1. Every algebraically independent subset of $\{a_1, ..., a_n\}$ (relative to k) that is maximal as such is also maximal as a algebraically independent subset of L over $\mathbf{k}$.

2. Every algebraically independent subset of L is finite, and all such subsets live inside maximal algebraically independent subsets. All maximal algebraically independent subsets have the same size.

3. Every subfield $F \subset L$ is finitely-generated over $\mathbf{k}$. In particular, the subfield $\mathbf{k}' \subset L$ consisting of all $a \in L$ algebraic over $\mathbf{k}$ is of finite-degree over $\mathbf{k}$.

A proof can be found in Conrad's notes. The common finite size of all algebraically independent subsets of L over $\mathbf{k}$ is called the transcendence degree of L over $\mathbf{k}$, and such maximal subsets are called transcendence bases of L over $\mathbf{k}$.

If $B \subset L = \mathbf{k}(a_1, ..., a_n)$ is a transcendence basis over $\mathbf{k}$, every element of L not in B is algebraic over $\mathbf{k}(B)$ due to maximality, as are elements of B (trivially). Hence, the a_i are algebraic over $\mathbf{k}(B)$, meaning L is finitely-generated over $\mathbf{k}(B)$.

This is the general structure of $L/\mathbf{k}$: a finite extension of $\mathbf{k}(B)$ will be isomorphic to $\mathbf{k}(Y_1, ..., Y_d)$ where d is the transcendence degree of L over $\mathbf{k}$, and this in-turn is isomorphic to the ring of polynomials $\mathbf{k}[X_1, ..., X_n]$.

In this context, the theorem simply asserts that transcendence degree is finite (for finitely-generated extensions) and well-defined. Transcendence degree is necessary for defining the dimension of a variety, as seen in the main body.

A.2 Basic Ring Notions

Definition A.6 (Noetherian Ring). A ring A is Noetherian if every ideal in A is finitely-generated.

Proposition A.7 (Characterization of Noetherian Rings). The following conditions on a ring A are equivalent:

1. A is Noetherian.

2. Every ascendending chain of ideals

$$I_1 \subset I_2 \subset ... \subset I_n \subset$$

eventually becomes constant, i.e, for some n, $I_n = I_{n+1} = ...$

3. Every nonempty set S of ideals of A has a maximal element, i.e, there exists an ideal in S not properly contained in any other ideal in S.

The following theorem tells us that any Noetherian ring has factorization (not necessarily unique) into irreducibles.

Proposition A.8. Every nonzero non-unit element of a Noetherian integral domain can be written as a product of irreducible elements.

In the case where the factorization is unique up to units, R is a unique factorization domain.

Definition A.9 (Local Ring). A ring is local if it has exactly one maximal ideal m. In this case, $A^\times = A \setminus m$.

Example A.10. Let $\mathbf{k} = \mathbf{Q}$. Take any prime p. As in the construction of the p-adics, we can write any nonzero $x \in \mathbf{Q}$ by $p^a y$, with $a \in \mathbf{Z}$ and the numerator and denominator of y are relatively prime to p. The ring $\mathbf{Z}_{(p)}$ is the the ring of quotients $(\mathbf{Z} \setminus p\mathbf{Z})^{-1}\mathbf{Z}$, or equivalently:

$$\mathbf{Z}_{(p)} = \{\frac{a}{b} \mid a, b \in \mathbf{Z} \text{ and } \gcd(b, p) = 1\}.$$

It will be justified this is in-fact a local ring in the exercises.

Example A.11. The ring $\mathbf{Z}_p$ is a local ring.

Definition A.12 (Integral Over a Ring). Let A be an integrally closed domain contained in another ring B. An element $b \in B$ is integral over A if it is a root of a monic polynomial in A.

Proposition A.13. Let L be a field containing A. An element α of L is integral over A if and only if there exists a nonzero finitely-generated A-submodule of L such that $\alpha M \subset M$ (in-fact, it suffices to take $M = A[\alpha]$).

Definition A.14 (Integrally Closed Ring). A ring A is integrally closed if it is its own integral closure in its field of fractions K, meaning if α is a root in K of a monic polynomial with coefficients in A, then α is in A.

B Commutative Algebra for Arithmetic Geometry

B.1 Discrete Valuation Rings

The following conditions on a principal ideal domain are equivalent:

1. A has exactly one nonzero prime ideal:
2. Up to associated, A has exactly one prime element.
3. A is a local ring but not a field.

We have already seen the first condition is equivalent to the third in the special case of the ring $\mathbf{Z}_p$, and the proof generalizes.

Definition B.1 (Discrete Valuation Ring). A ring satisfying the above conditions is called a discrete valuation ring, and so justifies the name.

Example B.2. $\mathbf{Z}_{(p)}$ is a discrete valuation ring as it is a local ring that is not a field.

Example B.3. We have seen that the p-adic integers $\mathbf{Z}_p$ are a local ring, yet not a field, and hence the p-adic integers are a discrete valuation ring.

In a discrete valuation ring A with prime element π, we can write nonzero elements of A as $u\pi^m$ with u a unit and $m \geq 0$ (and $m > 0$ unless the element itself is a unit). Every nonzero ideal of A is then of the form (π^m) for a unique $m \in \mathbf{N}$. Thus, if I is an ideal in A and $\mathbf{p}$ is the unique maximal ideal of A, then $a = p^m$ for a well-defined integer $m \geq 0$.

Definition B.4 (Annihilator). Given an A-module M and $m \in M$, the annihilator of m is the set:

$$\mathrm{Ann}(m) = \{a \in A \mid am = 0\}$$

This is an ideal in A, proper if $m \neq 0$. Suppose A is a discrete valuation ring, and let c be nonzero in A. Let $M = A/(c)$. What is the annihilator of a nonzero element $b + (c)$ of M? Fix a prime element π of A, and let $c = u\pi^m$, $b = v\pi^n$ with u and v units. Then $n < m$ as otherwise $b + (c) = 0$ in M, and then:

$$\mathrm{Ann}(b + (c)) = (\pi^{m-n})$$

Hence, any b where $\mathrm{Ann}(b + (c))$ is a maximal ideal, is of the form $v\pi^{m-1}$, and furthermore for such a b this is a prime ideal generated by $\frac{c}{b}$. These will be key in the next proof, which gives a criterion to check if a ring is a DVR.

Proposition B.5. An integral domain A is a discrete valuation ring if and only if:

1. A is noetherian.
2. A is integrally closed.
3. A has exactly one nonzero prime ideal.

Proof. The necessity of the conditions is obvious, so consider A a domain satisfying the three conditions. It suffices to show A is a principal ideal domain. Notice the third condition implies A is a local ring, since maximal ideals are prime.

As a first step, we prove that the nonzero prime ideal is principal. Consider $c \in A$ with c not a unit, and consider the module $M = A/(c)$. For each nonzero element m of M,

$$\text{Ann}(m) = \{a \in A \mid am = 0\}$$

is a proper ideal in A, and since A is noetherian, we can choose m with $\text{Ann}(m)$ maximal. Write $m = b + (c)$ and $\mathbf{p} = \text{Ann}(b + (c))$. Notice that $c \in \mathbf{p}$, and hence, $\mathbf{p} \neq 0$, and then:

$$\mathbf{p} = \{a \in A \mid c \mid ab\}$$

I claim $\mathbf{p}$ is prime. If it is not, there exist $x, y \in A$ with $xy \in \mathbf{p}$ but niether $x, y \in \mathbf{p}$, but then $yb + (c)$ is a nonzero element of M since $y \notin \mathbf{p}$. Take $\text{Ann}(yb + (c))$. Obviously it contains $\mathbf{p}$ and it contains x, but this contradicts maximality of $\mathbf{p}$ among ideals of the form $\text{Ann}(m)$, so $\mathbf{p}$ must be prime.

Now, we must have $\frac{b}{c} \notin A$, as otherwise $b = c \cdot \frac{b}{c} \in (c)$ and so $m = 0$.

Then, we must have $\frac{c}{b} \in A$, and further that $\mathbf{p} = (\frac{c}{b})$. By definition, $\mathbf{p}b \subset (c)$, and so $\mathbf{p} \cdot \frac{b}{c} \subset A$, and this is an ideal in A. If $\mathbf{p} \cdot \frac{b}{c} \subset \mathbf{p}$, then $\frac{b}{c}$ is integral over A (by Proposition A.13) and so $\frac{b}{c} \in A$ (by condition 2), but we know $\frac{b}{C} \notin A$. Hence, $\mathbf{p}\frac{b}{c} = A$ by condition 3, and this implies $\mathbf{p} = (\frac{c}{b})$.

Let $\pi = \frac{c}{b}$, such that $\mathbf{p} = (\pi)$. Let $\mathbf{a}$ be a proper ideal of A, and consider the sequence:

$$\mathbf{a} \subset \mathbf{a}\pi^{-1} \subset \mathbf{a}\pi^{-2} \subset ...$$

If $\mathbf{a}\pi^{-r} = \mathbf{a}\pi^{-r-1}$, then $\pi^{-1}(\mathbf{a}\pi^{-r}) = \mathbf{a}\pi^{-r}$ and so π^{-1} is integral over A (by Proposition A.13), hence lying in A. But, this is impossible as π is not a unit. Therefore, this sequence is strictly increasing, and since A is noetherian, this tells us it is not contained in A. Let m be the smallest integer such that $\mathbf{a}\pi^{-m} \subset A$, but $\mathbf{a}\pi^{-m-1} \notin A$. Then, $\mathbf{a}\pi^{-m} \notin \mathbf{p}$, hence $\mathbf{a}\pi^{-m} = A$, so $\mathbf{a} = (\pi^m)$. □

B.2 Discrete Valuation

Now, we can define discrete valuations on a field $\mathbf{k}$.

Definition B.6 (Discrete Valuation). A discrete valuation on $\mathbf{k}$ is a nonzero homomorphism $v : \mathbf{K}^\times \to \mathbf{Z}$ such that $v(a + b) \geq \min(v(a), v(b))$.

As v is not the zero homomorphism, its image is a nonzero subgroup of $\mathbf{Z}$ and is hence of the form $m\mathbf{Z}$ for some $m \in \mathbf{Z}$. If $m = 1$, the map is surjective and we call v normalized. Otherwise, $x \to m^{-1}v(x)$ will be a normalized discrete valuation.

We can extend v to a map $\mathbf{Z} \cup \{\infty\}$ by setting $v(0) = \infty$, where ∞ is a point at infinity with $\infty \geq n$ for all $n \in \mathbf{Z}$.

Example B.7. Let A be a principal ideal domain with field of fractions K and a singular prime ideal π in A. Then each element $c \in \mathbf{k}^\times$ can be expressed uniquely in the form $c = \pi^m \frac{a}{b}$ with $m \in \mathbf{Z}$ and a and b elements of A relatively prime to π. Define $v(c) = m$. Then v is a normalized discrete valuation on K.

Example B.8. More generally, let A be a Dedekind domain and let $\mathbf{p}$ be the prime ideal in A. For any $c \in \mathbf{K}^\times$, let $\mathbf{p}^{v(c)}$ be the power of $\mathbf{p}$ in the factorization of the ideal (c) as a power of $\mathbf{p}$. Then v is a normalized discrete valuation on K.

In all these examples, we have $v(a+b) = v(b)$ if $v(a) > v(b)$. This is a more general property of discrete valuations:

Definition B.9. A discrete valuation satisfies $v(a+b) = \min(v(a), v(b))$ for $v(a) \neq v(b)$.

Proof. Assume $v(a) > v(b)$. Notice $v(\zeta) = 0$ for any element $\zeta \in \mathbf{K}^\times$ for any element $\mathbf{K}^\times$ of finite-order since v is a homomorphism and $\mathbf{Z}$ has no elements of finite order, so $v(-a) = v(-1) + v(a) = v(a)$. Then, if $v(a) > v(b)$, we have:

$$v(b) = v(a+b-a) \geq \min(v(a+b), v(a)) \geq \min(v(a), v(b)) = v(b),$$

and hence we must have an equality, implying $v(a+b) = v(b)$. □

An example showed every discrete valuation ring gave a discrete valuation on its field of fractions. We show the converse:

Proposition B.10. Let v be a discrete valuation on K. Then the set $A = \{a \in \mathbf{k} \mid v(a) \geq 0\}$ is a principal ideal domain with maximal ideal:

$$\mathbf{m} = \{a \in \mathbf{K} \mid v(a) > 0\}$$

If $v(\mathbf{k}^\times) = m\mathbf{Z}$, then the ideal $\mathbf{m}$ is generated by every element π such that $v(\pi) = m$.

Proof. Left as an exercise. □

This construction should look very similar to the construction of the integers localized at p $\mathbf{Z}_{(p)}$ and the p-adic integers $\mathbf{Z}_p$.

B.3 Basic Appearance in Algebraic Geometry

Definition B.11. Let $\mathbf{k}$ be any field. Let $L \supset \mathbf{k}$ be a field extension. We say a valuation $v : \mathbf{L}^\times \to \mathbf{Z}$ is trivial on $\mathbf{k}$ if $v(\mathbf{k}^\times) = \{0\}$. We let $\mathcal{V}(L/\mathbf{k})$ denote the set of surjective valuations $v : \mathbf{L}^\times \to \mathbf{Z}$ trivial on $\mathbf{k}$.

Definition B.12. A projective line over $\mathbf{k}$ is a nonsingular complete curve $\mathbf{P}^1$ such that the field of functions $\mathbf{k}(\mathbf{P}^1)$ is isomorphic as a $\mathbf{k}$-algebra to the field of rational functions in one variable.

We have already discussed in the main body how $\mathbf{P}^1$ is a nonsingular curve.

Definition B.13 (f-adic valuation). Given an monic irreducible polynomial in $\mathbf{k}[x]$, define an f-adic valuation v_f on $\mathbf{k}(x)^\times$ by the following. For any nonzero rational function $\frac{g(x)}{h(x)}$, write:

$$\frac{g(x)}{h(x)} = f(x)^a \frac{p(x)}{q(x)}$$

with $p(x), q(x)$ relatively prime to f. Then define:

$$v_f\left(\frac{g(x)}{h(x)}\right) = a$$

Define $v_\infty = \deg(g) - \deg(h)$.

It is an exercise to show this is actually a valuation.

Proposition B.14. Let $\mathbf{k}$ be any field, and let $\mathbf{P}^1$ be the projective line associated to $\mathbf{k}(x)$ over $\mathbf{k}$. Then:

$$\mathbf{P}^1 = \{v_{g(x)} \mid g(x) \in \mathbf{k}[x], \text{ with } g \text{ irreducible and monic } \} \cup \{v_\infty\}$$

Proof. Here is a sketch of a proof (the details are left as an exercise). Let $v \in \mathcal{V}(\mathbf{k}(x)/\mathbf{k})$. Because v is surjective, there exists $h(x) \in \mathbf{k}[x]$ with $v(h(x)) \neq 0$.

Show if $v(h(x)) < 0$, then $v = v_\infty$, and if $v(h(x)) > 0$, then $v = v_{g(x)}$ where $g(x)$ is an irreducible factor of $h(x)$. □

In particular, for $\mathbf{k}$ algebraically closed, the only irreducible polynomials in $\mathbf{k}[x]$ are the linear polynomials, at which point we denote v_{x-a} by a. Then, we see $\mathbf{P}^1$ is in bijection with $\mathbf{k} \cup \{\infty\}$.

B.4 Exercises

Exercise B.1. Let R be a commutative ring with identity. We define a multiplicative subset of R to be a subset with $1 \in S$ and $ab \in S$ if $a, b \in S$.

1. Define a relation $\sim$ on $R \times S$ by $(a, s) \sim (a', s')$ if there exists an $s^* \in S$ such that $s^*(s'a - sa') = 0$. Show that $\sim$ is an equivalence relation on $R \times S$.

2. Let a/s denote the equivalence class of $(a, s) \in R \times S$ and let $S^{-1}R$ be the set of all equivalence classes with respect to $\sim$. Define operations of addition and multiplication on $S^{-1}R$ by:

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}, \frac{a}{s}\frac{b}{t} = \frac{ab}{st}$$

respectively. Prove that these operations are well-defined on $S^{-1}R$ and that $S^{-1}R$ is a ring with identity under these operations. The ring $S^{-1}R$ is called the ring of quotients of R with respect to S.

3. Show that the map $\psi : R \to S^{-1}R$ defined by $\psi(a) = \frac{a}{1}$ is a ring homomorphism.
4. If R has no zero divisors and $0 \notin S$, show ψ is one-to-one.
5. Prove that P is a prime ideal if and only if $S = R \setminus P$ is a multiplicative subset of R.
6. If P is a prime ideal of R and $S = R \setminus P$, show that the ring of qutoients $S^{-1}R$ has a unique maximal ideal. such a ring is called local.

Exercise B.2. Consider an integral domain A and a multiplicative subset S of A. For an ideal $\mathbf{a}$ of A, write $\mathbf{a}^e$ for the ideal it generates in $S^{-1}A$, for an ideal $\mathbf{a}$ of $S^{-1}A$, write $\mathbf{a}^c$ for $\mathbf{a} \cap A$. Then:

$$\mathbf{a}^{ce} = \mathbf{a} \text{ for all ideals } \mathbf{a} \subset S^{-1}A \mathbf{a}^{ec} \qquad = \mathbf{a} \text{if } \mathbf{a} \text{ is a prime ideal of } A \text{disjoint from} S.$$

Exercise B.3. Let A be an integral domain, S a multiplicative subset. The map $\mathbf{p} \to \mathbf{p}^e = \mathbf{p} \cdot S^{-1}A$ is a bijection from a set of prime ideals in A such that $\mathbf{p} \cap S = \emptyset$ to the set of prime ideals in $S^{-1}A$; the inverse map is $\mathbf{p} \to \mathbf{p} \cap A$.

Exercise B.4. Show the v_f as described above are actually valuations.

Exercise B.5. Fill in the details to the proof of Proposition B.14.

C Unique Factorization in Dedekind Domains

Most of this section is copied nearly-word-for-word out of Milne's Algebraic Number Theory notes.

C.1 Dedekind Domains

Definition C.1 (Dedekind Domain). A Dedekind domain is an integral domain A such that:

1. A is noetherian.
2. A is integrally closed.
3. every nonzero prime ideal is maximal.

The above work tells us that a local integral domain is a Dedekind domain if and only if it is a discrete valuation ring.

Proposition C.2. Let A be a Dedekind domain, and let S be a multiplicative subset of A. Then S^{-1} is a Dedekind domain.

Proof. The third condition says there is no containment relation between prime ideals, and then Exercise B.3 shows the lack of containment holds for $S^{-1}A$. The first and second condition follows from the following: □

Proposition C.3. Let A be an integral domain and let S be a multiplicative subset of A.

1. If A is noetherian, then so is $S^{-1}A$.
2. If A is integrally closed, so is $S^{-1}A$.

Proof.
1. Let $\mathbf{a}$ be an ideal in $S^{-1}A$. Then $\mathbf{a} = S^{-1}(\mathbf{a} \cap A)$ (see the exercises) and so $\mathbf{a}$ is finitely-generated by every (finite) set of generators for $\mathbf{a} \cap A$.
2. Let α be an element of the field of fractions of A (the same as the field of fractions of $S^{-1}A$) such that this is integral over $S^{-1}A$. Then

$$\alpha^m + a_1\alpha^{m-1} + ... + a_m = 0$$

for some $a_i \in S^{-1}A$. For each i, there exists an $s_i \in S$ with $s_i a_i \in A$, and let $s = s_1, ..., s_m \in S$, and multiply through by s^m:

$$(s\alpha)^m + sa_1(s\alpha)^{m-1} + ... + s^m a_m = 0$$

and so $s\alpha$ is integral over A and lies in A (since A is integrally closed), hence $\alpha = \frac{s\alpha}{s} \in S^{-1}A$.

□

Now, we are equipped to prove the following:

Proposition C.4. A Noetherian integral domain A is a Dedekind domain if and only if for each nonzero prime ideal $\mathbf{p}$ in A, the localization $\mathbf{A}_p$ is a discrete valuation ring.

Proof. For the forward definition, it is an exercise that the localization of a ring A at a prime ideal is local, and the above proposition tells us $A_{\mathbf{p}}$ is a discrete valuation ring (since it is not a field).

For the reverse direction, we must show A is integrally closed. Let x be an element of the field of fractions integral over A, and let $\mathbf{a}$ be the set of elements a of A such that $ax \in A$. For each nonzero prime ideal $\mathbf{p}$ in A, $x \in A_{\mathbf{p}}$, so there exists $s \in A \setminus \mathbf{p}$ such that $sx \in A$. Then, $\mathbf{a}$ is an ideal not contained in a maximal ideal of A, hence $\mathbf{a} = A$. In particular, $1 \in \mathbf{a}$. □

C.2 Unique Factorization of Ideals in Dedekind Domains

The main result of interest in Dedekind domains is the following.

Theorem C.5. Let A be a Dedekind domain. Every proper nonzero ideal $\mathbf{a}$ of A can be written in the form:

$$\mathbf{a} = \mathbf{p}_1^{r_1}\mathbf{p}_2^{r_2}....\mathbf{p}_n^{r_n}$$

with the $\mathbf{p}_i$ distinct prime ideals and the $r_i > 0$; the $\mathbf{p}_i$ and the r_i are uniquely determined.

The proof of this will require a great deal of work.

Lemma C.6. Let A be a Noetherian ring; then every ideal $\mathbf{a}$ in A is a product of nonzero prime ideals.

Proof. Suppose the statement is false for A, and choose a maximal counterexample $\mathbf{a}$. Then $\mathbf{a}$ is not prime, so there exist $x, y \in A$ such that $xy \in \mathbf{a}$ but neither $x, y \in \mathbf{a}$. Then, take the ideals $\mathbf{a} + (x)$ and $\mathbf{a} + (y)$, which strictly contain $\mathbf{a}$, but whose product is a subset of $\mathbf{a}$. Since $\mathbf{a}$ is a maximal counterexample to the lemma, each of $\mathbf{a} + (x)$ and $\mathbf{a} + (y)$ contains a product of prime ideals, and it follows that $\mathbf{a}$ contains a product of prime ideals. □

Lemma C.7. Let A be a ring, and let $\mathbf{a}$ and $\mathbf{b}$ be relatively-prime ideals in A. Then, for all $m, n \in \mathbf{N}$, $\mathbf{a}^m, \mathbf{b}^n$ are relatively prime.

Proof. If $\mathbf{a}^m$ and $\mathbf{b}^n$ are not relatively prime, then they are both contained in some (even maximal) ideal $\mathbf{p}$. But then, if a prime ideal contains a power of an element, it contains the element, so $\mathbf{p} \supset \mathbf{a}^m, \mathbf{b}^n$ implies $\mathbf{a}, \mathbf{b} \subset \mathbf{p}$ and this contradicts the hypothesis that $\mathbf{a}, \mathbf{b}$ are relatively prime. □

Another (more concrete) proof is as follows:

Proof. We know there exist $a \in A, b \in B$ such that $a + b = 1$. Consider:

$$1 = (a+b)^r = a^r + \binom{r}{1}a^{r-1} + ... + b^r.$$

If $r \geq m + n - 1$, the term on the right is a sum of an element of $\mathbf{a}^m$ with an element of $\mathbf{b}^n$. □

If $\mathbf{p}, \mathbf{p}'$ are distinct prime ideals of a Dedekind domain, the fact that every nonzero prime ideal is maximal tells us that $\mathbf{p}, \mathbf{p}'$ are relatively prime, and then the lemma shows $\mathbf{p}^m$ and $\mathbf{p}'^n$ are also relatively prime for all $m, n \geq 1$.

Lemma C.8. Let $\mathbf{p}$ be a maximal ideal of a domain A, and let $\mathbf{q}$ be the ideal it generates in $A_\mathbf{p}$, given by $\mathbf{q} = \mathbf{p}A_\mathbf{p}$. The map:

$$a + \mathbf{p}^m \to \mathbf{a} + q^m : A/A/\mathbf{p}^m \to A_\mathbf{p}/\mathbf{q}^m$$

is an isomorphism for $m \in \mathbf{N}$.

Proof. First, we show the map is injective, meaning $\mathbf{q}^m \cap A = \mathbf{p}^m$. But $\mathbf{q}^m = S^{-1}\mathbf{p}^m$ and $S = A - \mathbf{p}$, so we must show $\mathbf{p}^m = (S^{-1}\mathbf{p}^m) \cap A$. An element of $(S^{-1}\mathbf{p}^m) \cap A$ can be written as $a = \frac{b}{s}$ with $b \in \mathbf{p}^m, s \in S$, and $a \in A$. Then $sa \in \mathbf{p}^m$, and so $sa = 0$ in $A/\mathbf{p}^m$. The only maximal ideal containing $\mathbf{p}^m$ is $\mathbf{p}$ (since $\mathbf{m} \supset \mathbf{p}^m$ implies $\mathbf{m} \supset \mathbf{p}$), so the only maximal ideal in $A/\mathbf{p}$ is $\mathbf{p}/\mathbf{p}^m$, meaning $A/\mathbf{p}^m$ is local. Since $s + \mathbf{p}^m$ is not in $\mathbf{p}/\mathbf{p}^m$, it is a unit in $A/\mathbf{p}^m$, and so $sa = 0$ in $A/\mathbf{p}^m$ implies $a = 0 \in A/\mathbf{p}^m$, hence, $a \in \mathbf{p}^m$ as desired.

So, we now show the map is surjective. Let $\frac{a}{s} \in A_\mathbf{p}$. Since $s \notin \mathbf{p}$ and $\mathbf{p}$ is maximal, we have $(s) + \mathbf{p} = A$, meaning (s) and $\mathbf{p}$ are relatively prime. Therefore (s) and $\mathbf{p}^m$ are relatively prime, so there exist $b \in A$ and $q \in \mathbf{p}^m$ such that $bs + q = 1$, and so b maps to s^{-1} in $A_\mathbf{p}/\mathbf{q}^m$, so ba maps to $\frac{a}{s}$.

More precisely, since s is invertible in $A_\mathbf{p}/\mathbf{q}^m$, $\frac{a}{s}$ is the unique element of the ring such that $s\frac{a}{s} = a$. Since $s(ba) = a(1 - q)$, the image of ba in $A_\mathbf{p}$ also has this property and therefore equals $\frac{a}{s}$. □

Proposition C.9. A nonzero ideal $\mathbf{a}$ of A can be factored into a product of prime ideals.

Proof. Applying the first lemma, the ideal $\mathbf{a}$ contains a product of nonzero prime ideals:

$$\mathbf{b} = \mathbf{p}_1^{r_1} ... \mathbf{p}_m^{r_m}$$

We may suppose the $\mathbf{p}_i$ are distinct. Then:

$$A/\mathbf{b} \cong A/\mathbf{p}_1^{r_1} \times ... \times A/\mathbf{p}_m^{r_m} \cong A_{\mathbf{p}_1}/\mathbf{q}_1^{r_1} \times ... \times A_{\mathbf{p}_m}/\mathbf{q}_m^{r_m}$$

where $\mathbf{q}_i = \mathbf{p}_i A_{\mathbf{p}_i}$ is the maximal ideal of $A_{\mathbf{p}_i}$. The first isomorphism theorem is given by the Chinese Remainder theorem and the second lemma, while the second isomorphism is given by the third lemma. Under this isomorphism, the, $\mathbf{a}/\mathbf{b}$ corresponds to $\mathbf{q}_1^{s_1}/\mathbf{q}_1^{r_1} \times ... \times \mathbf{q}_m^{s_m}/\mathbf{q}_m^{r_m}$ for some $s_i \leq r_i$ (recall the rings $A_{\mathbf{p}_i}$ are all discrete valuation rings). Since this ideal is the image of $\mathbf{p}_1^{s_1} ... \mathbf{p}_m^{s_m}$ under this isomorphism, we see that:

$$\mathbf{a} = \mathbf{p}_1^{s_1} .... \mathbf{p}_m^{s_m} \text{ in } A/\mathbf{b}$$

Both ideals contain $\mathbf{b}$, and so we have:

$$\mathbf{a} = \mathbf{p}_1^{s_1} ... \mathbf{p}_m^{s_m}$$

in A, because there is a one-to-one correspondence between the ideals of $A/\mathbf{b}$ and the ideals of A containing $\mathbf{b}$. □

Now that we have existence of a factorization, we must show any such factorization is unique.

Proposition C.10. Any such factorization of an ideal $\mathbf{a}$ in A is unique.

Proof. Suppose we have two factorizations of the ideal $\mathbf{a}$. After adding factors with zero exponent, we may suppose the same prime ideals occur in each factorization, such that:

$$\mathbf{p}_1^{s_1} ... \mathbf{p}_m^{s_m} = \mathbf{a}A = \mathbf{p}_1^{t_1} ... \mathbf{p}_m^{t_m}$$

In the course of the above proof, we showed that:

$$\mathbf{q}_i^{s_i} = \mathbf{a}A_{\mathbf{p}_i} = \mathbf{q}_i^{t_i}$$

where $\mathbf{q}_i$ is maximal in $A_{\mathbf{p}_i}$. Hence, $s_i = t_i$ for all i, showing factorization is indeed unique. □

One more theorem (which we will not prove) provides a converse to the classical proof that A is a principal ideal domain implies A is a unique factorization domain.

Theorem C.11. A Dedekind domain with unique factorization is a principal ideal domain.

Proof. In a UFD, an irreducible element π divides bc if and only if b divides b or c. This is exactly equivalent to (π) being a prime ideal.

Now let A be a Dedekind domain with UFT. It suffices to show each nonzero prime ideal $\mathbf{p}$ of A is principal. Let a be nonzero in $\mathbf{p}$. Then a factors into a product of irreducibles (by unique factorization) and since $\mathbf{p}$ is prime, it contains at least one of these irreducible prime factors π. Then $\mathbf{p} \supset (\pi) \supset (0)$, and since $\mathbf{p}$ is prime, it is maximal, and hence equals $\mathbf{p}$. □