SUPPLEMENTARY LECTURE NOTES ON ELLIPTIC CURVES

PETE L. CLARK

Contents

WARNING: These are the *supplementary* lecture notes for a first graduate course on elliptic curves (Math 8430) I taught at UGA in Fall 2012. The word "supplementary" here is key: unlike most graduate courses I've taught in recent years, there was an official course text, namely [AEC]. Thus although the notes include what was discussed in the lectures, in their detailed coverage they tend to focus on slightly different material and/or a slightly different perspective than what is given in [AEC]. I want to emphasize that to read these notes without having the wonderful, classic text [AEC] in hand would be rather strange and is not recommended.

1. What is an elliptic curve?

An elliptic curve is an object defined over a **ground field** K. As a sign of the inherent richness of the theory, there are (at least!) four apparently different definitions of an elliptic curve $E_{/K}$, of various degrees of concreteness and/or abstraction. These four definitions turn out to be equivalent – i.e., they all specify the same class (or, I suppose, equivalent categories) of mathematical objects – but seeing the

equivalence is not trivial.

I. An **elliptic curve** $E_{/K}$ is given by a **Weierstrass equation**

$$E : y^2 = x^3 + ax + b$$

with $a, b \in K$ and

$$\Delta(E) = -16(4a^3 + 27b^2) \neq 0.$$

Remark: In fact this is a "short Weierstrass equation", which is adequate for elliptic curves over fields of characteristic diferent from 2 and 3. Notice that, because of the factor -16 in the definition of $\Delta(E)$, according to this definition there are no elliptic curves in characteristic 2. The official definition, valid in all characteristics, is that an elliptic curve is given by a **long Weierstrass equation**

$$E : y^2 + a_1xy + a_3y = x^3 + a_4x + a_6$$

with $a_1, a_3, a_4, a_5, a_6 \in K$ and $\Delta(E) \neq 0$; here $\Delta(E)$ is something of a mess:

$$\Delta(E) = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_8,$$

where (wait for it!)

$$b_2 = a_1^2 + 4a_4,$$

$$b_4 = 2a_4 + a_1a_3,$$

$$b_6 = a_3^2 + 4a_6,$$

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2.$$

This definition is "correct" in the sense that it is equivalent to the other definitions to come. Further, it is useful: certainly for calculations, and even for theoretical reasons (e.g. the theory of "good reduction" of elliptic curves is simpler than the corresponding theory for arbitrary algebraic curves largely because of the existence of Weierstrass equations). However, it is a distressingly unenlightening definition: we are being asked to consider an algebraic curve defined by a certain type of equation. But for any polynomial $P(x, y) \in K[x, y]$, we could study the equation $P(x, y) = 0$. What's so special about the choice $P(x, y) = y^2 - x^3 - ax - b$? This is hard to answer without recourse to some of the other definitions, so let's move on.

II. An **elliptic curve** $E_{/K}$ is a smooth, projective plane cubic curve

$$E(X, Y, Z) = a_1X^3 + a_2X^2Y + \ldots + a_{10}Z^3 = 0$$

endowed with a K-rational point O.

Every word in this definition will receive careful scrutiny in due course, but let us make a few remarks now: we think of E as being embedded in the **projective plane** $\mathbb{P}^2$. The set of K-rational points $E(K)$ is then the set of all $[X : Y : Z] \in \mathbb{P}^2(K)$ such that $E(X, Y, Z) = 0$. The smoothness is a natural generalization of what smoothness means in multivariable calculus: it means that there is no point $P \in E(\overline{K})$ at which the partial derivatives $\frac{\partial E}{\partial X}$, $\frac{\partial E}{\partial Y}$, $\frac{\partial E}{\partial Z}$ all vanish. And "endowed with a K-rational point" means that we are postulating the existence of a point $O \in E(K)$ and considering it as part of the data of an elliptic curve.

Example 1.1: Let $a, b, c \in K$, and consider the *diagonal* plane cubic

$$C : aX^3 + bY^3 + cZ^3 = 0.$$

When is E the plane cubic of an elliptic curve? First, we check the smoothness:

$$\frac{\partial C}{\partial X} = 3aX^2, \ \frac{\partial C}{\partial Y} = 3bY^2, \ \frac{\partial C}{\partial Z} = 3cZ^2.$$

If $\operatorname{char} K = 3$, these expressions vanish identically and we definitely do not get smoothness...so we assume $\operatorname{char} K \neq 3$. Then the three equations have a common zero in $\mathbb{P}^2(\overline{K})$ iff $abc = 0$. So assuming $abc \neq 0$, we get a smooth curve.

Do we have an elliptic curve? Not yet: we still need a K-rational point O. A little thought shows that, in general, we cannot just stare at the equation

$$aX^3 + bY^3 + cZ^3 = 0$$

and write down a K-rational point (other than $(0,0,0)$, of course, which does not count as a point in $\mathbb{P}^2$). Well, some examples will surely help.

Example 1.2: Let $K = \mathbb{Q}$, let p be a prime, and consider

$$C_p : X^3 + pY^3 + p^2Z^3 = 0.$$

I claim that $C(\mathbb{Q}) = \varnothing$. Indeed, if there is a rational point, then there are $x, y, z \in \mathbb{Z}$ with $\gcd(x, y, z) = 1$ and $x^3 + py^3 + p^2z^3 = 0$. But since $x^3 = -p(y^3 + pz^3)$, $p \mid x^3$ and thus (by uniqueness of factorization in $\mathbb{Z}$!) $p \mid x$, so we may write $x = pX$ for $X \in \mathbb{Z}$. Doing so, we get $(pX)^3 + py^3 + p^2z^3 = 0$, which simplifies to

$$y^3 + pz^3 + p^2X^3 = 0.$$

But now we see that $p \mid y^3$ and thus we may write $y = pY$ and substitute and simplify to get

$$z^3 + pX^3 + p^2Y^3 = 0.$$

Once again we see that $p \mid z^3$ and thus $p \mid z$...and this is a contradiction, since we assumed $\gcd(x, y, z) = 1$.

Exercise 1.3: Show that in fact $C_p(\mathbb{Q}_p) = \varnothing$.

This was a very easy example. Here is a much more famous, deep example:

Example 1.4 (Selmer): The cubic curve

$$C_S : 3X^3 + 4Y^3 + 5Z^3 = 0$$

has no $\mathbb{Q}$-rational points.

What makes this example deep is that in this case we have $C_S(\mathbb{Q}_p) \neq \varnothing$ for all primes p (and of course $C_S(\mathbb{R}) \neq \varnothing$, as for any cubic curve). Justifying these claims is not trivial! I hope to cover them later in the course.

Finally, a favorable case is when $a = b = 1$: the curve

$$C : X^3 + Y^3 + cZ^3 = 0$$

evidently does have a $\mathbb{Q}$-rational point, namely $[1 : -1 : 0]$. In fact, it will turn out that over any field K of characteristic different from 3, whenever the diagonal

plane cubic $aX^3 + bY^3 + cZ^3 = 0$ has a K-rational point – so is an elliptic curve – then it is **isomorphic** over K to the elliptic curve

$$J(C) : X^3 + Y^3 + abcZ^3 = 0.$$

Here "isomorphic" means something more general than just "projectively equivalent". Indeed, it turns out that C is projectively equivalent to $J(C)$ iff C has a K-rational **flex point**. More on this later (including the definition of a flex point!).

I claim that I. is essentially a special case of II.: given a Weierstrass equation, we can naturally associate a smooth plane cubic endowed with a rational point. I'll ask you to think about this on your own for now; we'll certainly come back to it later.

III. An **elliptic curve** $E_{/K}$ is a **nice** (= smooth, projective, geometrically integral) genus one curve over K endowed with a K-rational point C.

This definition is significantly more sophisticated: it is couched in the language of "abstract" algebraic curves, rather than algebraic curves as subsets of some particular affine or projective space. The algebraic geometry *cognoscenti* will know that a smooth plane curve of degree d has genus $\frac{(d-1)(d-2)}{2}$, and thus a smooth plane curve has genus one iff it is a cubic curve. Thus II. is again a special case of III. Conversely, any smooth plane curve endowed with a rational point O is *isomorphic* to a smooth plane cubic curve (in fact, to a **Weierstrass cubic**, a concept we have not yet quite defined). This requires the **Riemann-Roch Theorem** and will be discussed later. So definitions I., II. and III. are all equivalent.

IV. An **elliptic curve** $E_{/K}$ is a one-dimensional **abelian variety**, i.e., a nice one-dimensional **group variety**.

Again, some algebraic geometry shows that a curve which carries a group law must have genus one: e.g. the canonical bundle must be trivial. Conversely, for any nice algebraic curve $C_{/K}$ we have the **Picard group** $\operatorname{Pic} C$ of K-rational divisor classes (or isomorphism classes of K-rational line bundles) on C, and its subgroup $\operatorname{Pic}^0(C)$ of degree zero divisors. When C has genus one and a K-rational point O, an application of the Riemann-Roch Theorem gives a canonical bijection $C(K) \to \operatorname{Pic}^0(C)$. This will show the equivalence of III. and IV.

In some sense IV. is the "best" definition, because it places the most important feature of an elliptic curve front and center: the group law on the set of K-rational points. The principal disadvantage of IV. is that it requires some sophisticated algebraic geometric ideas. Historically first was a down-to-earth description of the group law on a plane cubic endowed with a rational point O, which we turn to next.

2. Mordell-Weil Groups

2.1. The Group Law on a Smooth, Plane Cubic Curve.

Namely, let (E, O) be our plane cubic endowed with a rational point, and let $P, Q \in E(K)$. Consider the line L joining P to Q. It cuts the cubic E in three

points (over $\overline{K}$, and counted with multiplicities), of which two are K-rational. Essentially then we have a cubic polynomial with K-coefficients and two K-rational roots, so the third root must also be K-rational, and thus the third intersection point, R, of L with E, is K-rational. Now consider the line L' joining R to O; again its third intersection point S with E is K-rational, and we put

$$P + Q = S.$$

Notice that there is a unique line L joining any two *distinct* points in $\mathbb{P}^2$, but of course this is not the case if $P = Q$. In that case, thinking about what happens as a distinct point Q approaches a fixed point Q immediately suggests that in the case $P = Q$ we should take L to be the **tangent line** at P. All in all this geometric construction is known as the **chord and tangent process**.

Let us check that the binary operation ("addition law")

$$+ : E(K) \times E(K) \to E(K)$$

that we have defined is commutative, has O as an identity, and is such that every element has an inverse.

Since "the line from P to Q" is "the line from Q to P", commutativity is clear.

For any $A \in E(K)$, to get $A + O$ we form the line from A to O and take the third intersection point, say B, and then take the line from B to O and take the third intersection point. But the second line is the same as the first, so the third intersection point is A.

For $A \in E(K)$, we construct a point A' as follows: let L be the tangent line to O, and let K be its third intersection point with E. Let L' be the line from K to O, and let A' be its third intersection point. Then $A + A' = O$.

Exercise 2.1: Show that the following are equivalent:
(i) O is a flex point of the cubic curve E: i.e., the tangent line to O intersects O with multiplicity at least 3 (and thus, here, exactly 3).
(ii) For all $A \in E(K)$, the inverse A' of A lies on the line from A to O.

In treatments of the group law on a cubic, it is often assumed that the endowed point O is a flex point. This slightly simplifies the geometry of the addition law according to the above exercise, but is not necessary for any of the results to hold. I find it enlightening to do the general case.

In order to know that our addition law on $E(K)$ is a group law, it remains to show that the operation is associative, i.e., for all $A, B, C \in E(K)$,

$$(A + B) + C = A + (B + C).$$

Somewhat frustratingly, this is not obvious! In fact the literature contains several proofs. We give a proof which is directly inspired by [LEC, §7], but with some expanded details. Note that it is no loss of generality to assume that $K = \overline{K}$ (why?).

We will need – or so it seems to me, at least – the following basic geometric fact.

FACT: Let K be an algebraically closed field, and let E be a nonsingular plane cubic curve over K. Then E is *not* isomorphic to the projective line $\mathbb{P}^1$.

Let me rephrase the FACT in the following slightly more concrete form, which is how it will be used: let $f : E \to \mathbb{P}^1$ be a morphism, i.e., a rational function on E. Then f does not have degree 1: i.e., the preimage of a point $P \in \mathbb{P}^1$ cannot consist of a single, simple point.

A student of algebraic geometry will be very familiar with this fact. For instance, it can be proved as a consequence of a much more general fact that if $C(X, Y, Z) = 0$ is a smooth, homogeneous polynomial of degree d, then the *genus* of C is $\frac{(d-1)(d-2)}{2}$. Thus a smooth plane cubic has genus 1, whereas a line in the plane has genus 0.

To someone unfamiliar with geometry, the previous paragraph probably raises more questions than it answers, e.g. 1) Why is the above genus formula valid? and indeed 2) What is the genus of a plane curve?

These questions will be addressed in due course, the key idea being the divisor associated to a meromorphic differential. For now, let us press on: recall that (E, O) is a smooth plane cubic over an algebraically closed field K, endowed with $O \in E(K)$.

Step 1: For $A, B, P \in E(K)$, the following are equivalent:
(i) $P = A + B$.
(ii) There is a rational function $f : E \to \mathbb{P}^1$ with

$$\operatorname{div} f = [A] + [B] - [O] - [P].$$

Proof: (i) $\implies$ (ii): Let L_1 be the line through A and B – here and henceforth, in this context "the line through A and B" means the unique one if $A \neq B$ and the tangent line to the curve at A if $A = B$ – call the third intersection point C. Let L_2 be the line through C and O; by definition, the third intersection point is $A + B = P$. Now $f = \frac{L_1}{L_2}$ is a rational function on $\mathbb{P}^2$ hence restricts to a rational function on E. We have

$$\operatorname{div}(f) = [A] + [B] + [C] - [C] - [O] - [P] = [A] + [B] - [O] - [P].$$

(ii) $\implies$ (i): Let $f : E \to \mathbb{P}^1$ be such that

$$\operatorname{div} f = [A] + [B] - [0] - [P].$$

Let L_1 be the line through A and B, and let C_1 be its third intersection point with E. Let L_2 be the line through O and P, and let C_2 be its third intersection point with E. Then

$$\operatorname{div}(fL_2/L_1) = [C_2] - [C_1].$$

But if C_1 and C_2 were distinct, we would then have a degree one rational function on E, contradicting the fact above. So in fact $C_1 = C_2$ and thus $P = A + B$.
Step 2: Now we prove associativity: for $A, B, C \in E(K)$, put

$$X = (A + B) + C,\ Y = A + (B + C).$$

By Step 1, there are $f_1, g_1, f_2, g_2 \in K(E)$ with

$$\operatorname{div} f_1 = [A + B] + [C] - [O] - [X],$$

$$\operatorname{div} g_1 = [A] + [B+C] - [O] - [Y],$$
$$\operatorname{div} f_2 = [A] + [B] - [O] - [A+B],$$
$$\operatorname{div} g_2 = [B] + [C] - [O] - [B+C].$$

Then

$$\operatorname{div}\left(\frac{f_1 f_2}{g_1 g_2}\right) = [Y] - [X],$$

which, as above, implies

$$(A+B)+C = X = Y = A+(B+C).$$

In summary:

Theorem 2.1. *For any smooth plane cubic E endowed with a rational point O, the chord and tangent process gives $E(K)$ the structure of a commutative group with identity element O. We call this group the* ***Mordell-Weil group*** *of E.*

Note that the Mordell-Weil group is defined in terms of the pair (E, O). It may well be the case that O is the only K-rational point on E, but of course the case of interest is when there is more than one point. In this case one may wonder about the group law defined in terms of the pair (E, O') for a different K-rational point O'.

Exercise 2.2: Construct a canonical isomorphism from the group law defined via (E, O) to the group law defined via (E, O').

In other words, the specific choice of "endowed rational point" is immaterial: another way to say this is that any two K-rational points on E are conjugate under the automorphism group of the underlying algebraic curve. The key is that there is *at least one* K-rational point, which as we have seen above, there need not be.

2.2. **Reminders on Commutative Groups.**

For any elliptic curve (E, O), we have defined on $E(K)$ the structure of a commutative group. A highly interesting question is to determine the structure of $E(K)$ as a function of K and/or E.

For any commutative group $(G, +)$ the elements of finite order form a subgroup, called the **torsion subgroup**, and written as $G[\text{tors}]$. For instance, if G is finite, then $G[\text{tors}] = G$, whereas $\mathbb{Z}[\text{tors}] = \mathbb{Q}[\text{tors}] = \mathbb{R}[\text{tors}] = 0$. A group with trivial torsion subgroup is said to be **torsionfree**.

Exercise 2.3: Show that for any commutative group G, $G/G[\text{tors}]$ is torsionfree.

Thus for any commutative group G we have a short exact sequence

$$0 \to G[\text{tors}] \to G \to H \to 0, \tag{1}$$

with $G[\text{tors}]$ a torsion group and $H = G/G[\text{tors}]$ a torsionfree group. The best case scenario for understanding the structure of G occurs when (1) is a *split* exact sequence, i.e., if the map $q : G \to H$ has a section $\sigma : H \to G$: a homomorphism such that $q \circ \sigma = 1_H$. When this occurs, we have

$$G \cong G[\text{tors}] \oplus H,$$

and we say that G is **torsion-split**.

When is this the case? Well, for an R-module M_1, *every* short exact sequence

$$0 \to M_1 \to M_2 \to M_3 \to 0$$

is split iff M_1 is **injective**. When $R = \mathbb{Z}$, the injective modules are precisely the **divisible** commutative groups, namely the groups having the property that

$$[n] : G \to G,\ x \mapsto nx$$

is surjective for all $n \in \mathbb{Z}^+$.[1] Thus if $G[\text{tors}]$ is divisible, G is torsion-split.

Dually, for an R-module M_3, *every* short exact sequence

$$0 \to M_1 \to M_2 \to M_3 \to 0$$

is split iff M_3 is **projective**. When $R = \mathbb{Z}$ (or any PID), an R-module is projective iff it is free, i.e., a direct sum of copies of $\mathbb{Z}$. Thus another sufficient condition for G to be torsion-split is for $G/G[\text{tors}]$ to be free.

Exercise 2.4: Let $(G, +)$ be a commutative group.
a) Show (or recall) that if G is finitely generated and torsionfree, then it is free.
b) Conclude that any finitely generated commutative group is torsion-split and thus isomorphic to $\mathbb{Z}^n \oplus T$, with $n \in \mathbb{N}$ and T a finite group.
c) Show that a nonzero divisible group is not free.
d) Show that G is torsionfree and divisible iff it can be endowed with the structure of a $\mathbb{Q}$-vector space.
e) Deduce that $\mathbb{Q}$ and $\mathbb{R}$ are torsionfree but not free.

Actually in asking that $G[\text{tors}]$ be injective, we are asking for more than we need: we have not used the fact that $G/G[\text{tors}]$ is torsionfree. Thus for instance it can be shown that although $\mathbb{Z}/2\mathbb{Z}$ is not injective – consider e.g.

$$0 \to \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0,$$

any short exact sequence

$$0 \to \mathbb{Z}/2\mathbb{Z} \to M_2 \to M_3 \to 0$$

with M_3 torsionfree does split. More generally, one says that a torsion group has G **bounded order** if there is $n \in \mathbb{Z}^+$ such that $nx = 0$ for all $x \in G$. In particular a finite group has bounded order, but not conversely.

Theorem 2.2. *(Baer* [Ba36]*) For a torsion commutative group T, TFAE:*
(i) Every commutative group G with $G[\text{tors}] \cong T$ is torsion-split.
(ii) Every short exact sequence of commutative groups

$$0 \to T \to M_2 \to M_3 \to 0$$

with M_3 torsionfree is split.
(ii) T is the direct sum of a subgroup of bounded order and a divisible subgroup.

[1] More generally, an integral domain R has the property that every divisible R-module is injective iff it is a Dedekind domain.

Exercise 2.5: Let G be a commutative group with a finite index torsionfree subgroup. Show that G is torsion-split.

Exercise 2.6: Show that the commutative group $\prod_p \mathbb{Z}/p\mathbb{Z}$ (the product extends over all prime numbers p) is not torsion-split.

2.3. **Some Elementary Results on Mordell-Weil Groups.**

Proposition 2.3. *Let $E_{/K}$ be an elliptic curve.*
a) We have $\#E(K) \leq 2\#K + 1$.
b) If K is algebraically closed, then $\#E(K) = \#K$.

Exercise 2.7:
a) Prove Proposition 2.3.
b) Show that there is an elliptic curve $E_{/\mathbb{F}_2}$ with $\#E(\mathbb{F}_2) = 5$.
c) Show that there is an elliptic curve $E_{/\mathbb{F}_3}$ with $\#E(\mathbb{F}_3) = 7$.
d) Show that there is an elliptic curve $E_{/\mathbb{F}_4}$ with $\#E(\mathbb{F}_4) = 9$.
e) Show that there is *no* elliptic curve $E_{/\mathbb{F}_5}$ with $\#E(\mathbb{F}_5) = 11$.

Remark: Later we will show that the bound $\#E(\mathbb{F}_q) \leq 2q + 1$ cannot be attained for any $q \geq 5$, and we will give the best possible bound.

Exercise 2.8: For a prime power q, it is known – by work of Hasse, Deuring and Waterhouse – exactly which positive integers N are the order of $\mathbb{E}(\mathbb{F}_q)$ for some elliptic curve $E_{/\mathbb{F}_q}$. For instance, when $q = p$ is prime, the answer is especially simple: it is necessary and sufficient that $|N - (p+1)| < 2\sqrt{p}$.
a) Compare this bound with Exercise 2.6.
b) Assuming the above result, show that every integer $N \leq 10^6$ (say) is the order of a Mordell-Weil group of some elliptic curve over some finite field.
c) It is in fact a folk conjecture (especially in crypographic circles) that every positive integer is the order of a Mordell-Weil group of an elliptic curve over $\mathbb{F}_p$ for some prime p. Discuss how it is posible to have complete information about the sizes of Mordell-Weil groups $E(\mathbb{F}_p)$ and still not be able to resolve this conjecture.

The following will be proved later using properties of the multiplication-by-n maps.

Theorem 2.4. *If K is an algebraically closed field and $E_{/K}$ is an elliptic curve, then the Mordell-Weil group $E(K)$ is infinite and divisible.*

Theorem 2.5. *Let K be an algebraically closed field, and let $E_{/K}$ be an elliptic curve.*
a) If $\operatorname{char} K = 0$, then $E(K)[\text{tors}] \cong (\mathbb{Q}/\mathbb{Z})^2$.
b) If $\operatorname{char} K = p > 0$, then $E(K)[\text{tors}]$ is isomorphic to either

$$T_o = \bigoplus_{\ell \neq p} (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^2 \oplus \mathbb{Q}_p/\mathbb{Z}_p$$

or to

$$T_{\text{ss}} = \bigoplus_{\ell \neq p} (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^2.$$

Both possibilities occur over any algebraically closed field K of characteristic p.

Corollary 2.6. *Let K be an uncountable algebraically closed field of characteristic 0.*[2] *Then for any elliptic curve $E_{/K}$, there is an isomorphism*

$$E(K) \cong (\mathbb{Q}/\mathbb{Z})^2 \oplus V,$$

where V is the additive group of a $\mathbb{Q}$-vector space of dimension $\mathfrak{c} = 2^{\aleph_0} = \#\mathbb{R}$.

Exercise 2.9: Prove Corollary 2.6.

Corollary 2.7. *Let K be the algebraic closure of a finite field, and let $E_{/K}$ be an elliptic curve. Then $E(K) = E(K)[\text{tors}] \cong T_o$ or T_{ss}.*

Exercise 2.10: Prove Corollary 7.7.

Corollary 2.8. *Let $E_{/K}$ be an elliptic curve, and let $T \subset E(K)$ be a finite subgroup. Then there are $M, N \in \mathbb{Z}^+$ such that*

$$T \cong \mathbb{Z}/MN\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z}.$$

Exercise 2.11: a) Prove Corollary 2.8.
b) Show that $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is the smallest commutative group which is not a Mordell-Weil group.

Conjecture 2.9. *For a commutative group $(A, +)$, the following are equivalent.*
(i) There is an injection $A[\text{tors}] \hookrightarrow (\mathbb{Q}/\mathbb{Z})^2$.
(ii) There is a field K and an elliptic curve $E_{/K}$ such that $E(K) \cong A$.

2.4. **The Mordell-Weil Theorem.**

2.4.1. *The Statement.*

Few would argue that the following result is "the fundamental theorem of the arithmetic theory of elliptic curves". It was proved when $K = \mathbb{Q}$ by L.J. Mordell [Mo22] and then over an arbitrary number field by A. Weil [We29].

Theorem 2.10. *(Mordell-Weil) Let K be a number field, and let $E_{/K}$ be an elliptic curve. Then the Mordell-Weil group $E(K)$ is finitely generated.*

2.4.2. *A Closer Look at Mordell-Weil Groups Over Number Fields.*

Let $E_{/K}$ be an elliptic curve over a number field. By the Mordell-Weil theorem, $E(K)$ is finitely generated, and thus by Exercise 2.3 we may write

$$E(K) \cong \mathbb{Z}^r \oplus T$$

with $r \in \mathbb{N}$, the **rank** of E, and $T \cong E(K)[\text{tors}]$ a finite subgroup. Much of the last 90 years of elliptic curve theory has been devoted to a careful study of r and T.

If one restricts to elliptic curves over $\mathbb{Q}$, one finds empirically that the torsion subgroup is constrained to lie in a rather small list. It has long been known that the following groups occur as torsion subgroups of elliptic curves over $\mathbb{Q}$:

$$\mathbb{Z}/N\mathbb{Z}, \ 1 \leq N \leq 10, \ N = 12, \tag{2}$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}, 1 \leq N \leq 8. \tag{3}$$

[2]The main example is, of course, $K = \mathbb{C}$.

Exercise 2.12*: Use the fact that the elliptic modular curve $X_1(N)$ has genus zero to show that for $1 \leq N \leq 10$, there are infinitely many elliptic curves over $\mathbb{Q}$ with a rational point of order N.

Theorem 2.11. *(Mazur* [Ma77]*) For any elliptic curve $E_{/\mathbb{Q}}$, the torsion subgroup of $E(\mathbb{Q})$ is isomorphic to one of the groups listed in (2) or (3).*

Of course if we increase K, then more groups can arise as torsion subgroups.

Exercise 2.13: Let G be any finite subgroup of $(\mathbb{Q}/\mathbb{Z})^2$.
a) Use Theorem 2.5 to show that for any number field K and elliptic curve $E_{/K}$, there is a finite extension L/K and an injection $G \hookrightarrow E(L)[\text{tors}]$.
b)* Show that this can be done with $[L : K]$ bounded above in terms of $\#G$.

Theorem 2.12. *(Merel* [Me96]*) There is a function $M : \mathbb{Z}^+ \to \mathbb{Z}^+$ such that: for every number field K with $[K : \mathbb{Q}] \leq n$ and every elliptic curve $E_{/K}$,*

$$\#E(K)[\text{tors}] \leq M(n).$$

Merel's work gives an explicit function $M(n)$ which was later improved by P. Parent [Pa99], but the best known bounds are still quite large. For instance, work of Parent shows that the largest prime power p^a dividing the order of $E(K)[\text{tors}]$ for some elliptic curve E over a field K with $[K : \mathbb{Q}] \leq n$ satisfies

$$p^a \leq 65(3^n - 1)(2n)^6.$$

This bound is exponential in n. On the other hand, it was sort of a folklore result that the size of $E(K)[\text{tors}]$ could be as large as $n\sqrt{\log\log n}$: this was written up in [CX08], for instance. Recently this lower bound has been improved.

Theorem 2.13. *(Breuer* [Br10]*) There exists a sequence of positive integers $n_1 < n_2 < \ldots < n_k < \ldots$, a sequence of number fields $\{K_k\}_{k=1}^{\infty}$ and a sequence of elliptic curves $(E_k)_{/K_k}$ with*

$$\liminf_k \frac{E_k(K_k)[\text{tors}]}{n_k \log\log n_k} > 0.$$

Conjecture 2.14. *(Clark-Cook-Stankewicz* [CCS13]*) There is a constant C such that for all $n \in \mathbb{Z}^+$, all number fields $K/\mathbb{Q}$ with $[K : \mathbb{Q}] \leq n$ and all elliptic curves $E_{/K}$,*

$$\#E(K)[\text{tors}] \leq Cn \log\log n.$$

This conjecture seems to lie far out of current reach.

We now pass to the rank of an elliptic curve. Here there has been even more work and fewer definitive results. In fact, while there *is* an algorithm to compute the torsion subgroup of an elliptic curve over a number field, there is *no algorithm proven* to compute the rank of an elliptic curve over a number field, or even an elliptic curve over $\mathbb{Q}$.

Exercise 2.14*: Show that for any $r \in \mathbb{N}$, there is a number field K and an elliptic curve $E_{/K}$ such that the Mordell-Weil rank of $E(K)$ is at least r.

Remark: So far as I know, if in the previous exercise we replace "at least r" with "exactly r" then we get an open problem.

It is a generally believed folk conjecture that the rank of an elliptic curve $E_{/\mathbb{Q}}$ can be arbitrarily large, and there is a cottage industry of finding explicit elliptic curves $E_{/\mathbb{Q}}$ of large rank. For several years the record has been held by an elliptic curve $E_{/\mathbb{Q}}$ found by N.D. Elkies, which is known to have rank at least 28.

However, it is also generally believed that elliptic curves with rank at least r become more and more sparse among all elliptic curves as r increases. Many people believe that in some sense half of all rational elliptic curves have rank 0 (and in fact, trivial Mordell-Weil group) and half have rank 1 (and in fact, Mordell-Weil group $\mathbb{Z}$). In the last few years there has been dramatic progress towards these conjectures, especially by Bhargava and Shankar. I will try to report more carefully on these recent results by the end of the course.

2.4.3. *Some Generalizations of the Mordell-Weil Theorem.*

The Mordell-Weil Theorem holds verbatim for **abelian varieties** – i.e., smooth, projective geometretically connected group varieties – over a number field K. The proof of this generalization is also due to Weil. Once one has developed the basic foundations of the theory of abelian varieties (which requires more of an algebraic-geometric overhead than that of elliptic curves), modifying the proof of the Mordell-Weil Theorem becomes relatively straightforward. In particular, it follows the same basic strategy: first one proves finitness of $A(K)/nA(K)$, then one develops a theory of height functions on abelian varieties.

The Mordell-Weil Theorem does not in general hold for algebraic groups over number fields which are not abelian varieties. For instance, neither the additive nor the multiplicative groups of $\mathbb{Q}$ are finitely generated. However, by Dirichlet's Theorem the **unit group** of a number field is finitely generated, and this suggests that on nonprojective varieties one should be considering not rational but *integral* points. More on this later, perhaps.

One can also try to generalize the Mordell-Weil Theorem by considering ground fields other than a number field. Recall that a field K is **finitely generated** if it is obtained by adjoining finitely many elements to its prime subfield. Equivalently, a field is finitely generated iff it is the fraction field of a domain of the form $\mathbb{Z}[t_1, \ldots, t_n]/\mathfrak{p}$ for some prime ideal $\mathfrak{p}$.

Theorem 2.15. *(Lang-Néron* [LN59]*) Let E be an elliptic curve (or in fact an abelian variety) over a finitely generated field K. Then $E(K)$ is finitely generated.*

The proof of the Lang-Néron Theorem is probably beyond the scope of this course, but if you're especially interested please let me know and I'll see what I can do.

In fact Lang and Néron proved yet a stronger theorem, albeit one which is rather difficult to state precisely. For instance, for many elliptic curves E defined over the rational function field $\mathbb{C}(t)$ the Mordell-Weil group remains finitely generated, and Lang-Néron proved a nice theorem to this effect. However, certainly there are some elliptic curves $E_{/\mathbb{C}(t)}$ for which $E(\mathbb{C}(t))$ is *not* finitely generated. Namely, start with any elliptic curve $E_{/\mathbb{C}}$, and consider it via basechange as a curve over $\mathbb{C}(t)$. Then

we have an inclusion of Mordell-Weil groups

$$E(\mathbb{C}) \hookrightarrow E(\mathbb{C}(t))$$

and, by Proposition 2.3 $E(\mathbb{C})$ is uncountable infinite, hence so is $E(\mathbb{C}(t))$.

The task of how to exclude examples like the above will become eaiser when we develop the concept of the **j-invariant** of an elliptic curve.

2.5. K-Analytic Lie Groups.

Let K be a nondiscrete, locally compact topological field. It can be shown that K is isomorphic to $\mathbb{R}$, to $\mathbb{C}$, to a finite extension of $\mathbb{Q}_p$, or to $\mathbb{F}_q((t))$.

Having a topology on K allows us to put a useful topology on $\mathbb{A}^n(K)$ and $\mathbb{P}^n(K)$: we call these the K-**analytic topologies** to distinguish them from the (strictly weaker) Zariski topology that exists for any field K. The following exercise develops some basic properties of the analytic topology on $\mathbb{P}^n(K)$.

Exercise 2.15: Let K be a field, and consider $\mathbb{P}^N_{/K}$.
a) For $0 \leq i \leq N$, let $U_i = \{[X_0 : \ldots : 1 : \ldots : X_N] \mid X_i \in K\}$. Show that $\mathbb{P}^N = \bigcup_{i=0}^N U_i$, and that each U_i is canonically isomorphic to $\mathbb{A}^N_{/K}$.
b) Explain how to construct $\mathbb{P}^N$ from $U_0, \ldots, U_N$ via a "glueing construction".
c) Suppose K is a locally compact, nondiscrete topological field (e.g. $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}_p$). Endow each U_i with the product topology on K^N. Say that a subset $A \subset \mathbb{P}^N(K)$ is **analytically open** if $A \cap U_i$ is open in U_i for all $0 \leq i \leq N$. Show that this determines a topology on $\mathbb{P}^N(K)$, called the **analytic topology**.
d) Show that the analytic topology on $\mathbb{P}^N$ agrees with the topology $\mathbb{P}^N$ receives as a quotient space of $K^{N+1} \setminus \{(0, \ldots, 0)\}$ via the standard equivalence relation $v \sim \lambda v$ for $\lambda \in K^\times$. In this way, or otherwise, deduce that $\mathbb{P}^N(K)$ is compact.
e) Suppose $K = \mathbb{R}$. Show that $\mathbb{P}^N(\mathbb{R})$ is a smooth N-manifold. Show that $\mathbb{P}^1(\mathbb{R}) \cong S^1$ is the one-point compactification of $\mathbb{R}$.
f) Suppose $K = \mathbb{C}$. Show that $\mathbb{P}^N(\mathbb{C})$ is a smooth N-dimensional complex manifold. Show also that $\mathbb{P}^N(\mathbb{C})$ admits the structure of a cell complex with exactly one cell in each even dimension $2k \leq 2N$ and no other cells, and use this to show that each $\mathbb{P}^N(\mathbb{C})$ is simply connected and to compute its integal co/homology groups. Show that $\mathbb{P}^1(\mathbb{C})$ is isomorphic to the Riemann sphere S^2.
g) Suppose K is a locally compact, nondiscrete Archimedean field. Show that for all $N \in \mathbb{Z}^+$, $\mathbb{P}^N(K)$ is homeomorphic to the Cantor set.

We state the following results now because we are discussing what is known about the structure of Mordell-Weil groups over various fields. At least some of the proofs will be given later; complete proofs will be given iff there is sufficient interest.

Theorem 2.16. *Let $E_{/K}$ be an elliptic curve. Then, endowed with the K-analytic topology, $E(K)$ has the structure of a one-dimensional compact K-analytic Lie group in the sense of* [LALG].

Corollary 2.17. *a) Let $E_{/\mathbb{C}}$ be an elliptic curve. Then $E(\mathbb{C})$ is connected and is thus a one-dimensional complex torus: it is isomorphic as a $\mathbb{C}$-analytic Lie group to $\mathbb{C}/\Lambda$ for some lattice Λ in $\mathbb{C}$.*
b) Let $E_{/\mathbb{R}}$ be an elliptic curve with Weierstrass equation $E : y^2 = P(x)$. Then:

(i) $\Delta(E) > 0 \iff P(x)$ *has three real roots* $\iff E(R) \cong S^1 \times \mathbb{Z}/2\mathbb{Z}$.
(ii) $\Delta(E) < 0 \iff P(x)$ *has one real root* $\iff E(\mathbb{R}) \cong S^1$.
c) Let $K/\mathbb{Q}_p$ *be a field extension of finite degree* n*, and let* $E_{/K}$ *be an elliptic curve. Then*

$$E(K) \cong \mathbb{Z}_p^n \oplus T, \tag{4}$$

where T *is a finite group.*

Remark: The isomorphism of (4) is proved by finding a finite index subgroup isomorphic to $\mathbb{Z}_p^n$ and applying Exercise 2.4.

Exercise 2.16: Let $K = \mathbb{F}_q((t))$ and let $E_{/K}$ be an elliptic curve. Show that $E(K)$ is *not* (!!) isomorphic to $\mathbb{F}_q[[t]]^n \oplus T$ for any $n \in \mathbb{N}$ and any finite group T. (Hint: think about the torsion subgroup.)

3. Background on Algebraic Varieties

3.1. **Affine Varieties.**

Let K be a field. For $n \in \mathbb{Z}^+$, by **affine n-space** over K we mean K^n, but we give it a fancy new notation: $\mathbb{A}^n_{/K}$. Well, in fact by $mathbbA^n_{/K}$ we mean something a little fancier than this. The easiest way to say this is that we associate the polynomial ring $K[t] = K[t_1, \ldots, t_n]$.

On $\mathbb{A}^n(K)$ we define a topology, the **Zariski topology**, for which a base for the closed sets is given by zero sets of elements $f \in K[t]$. The process of passing from an arbitrary subset $S \subset \mathbb{A}^n(K)$ to its Zariski closure can be viewed as the **closure operation** attached to a canonical **Galois connection** between the set of subsets of $\mathbb{A}^n(K)$ and the set of ideals in $K[t]$. Namely, for any subset $S \subset \mathbb{A}^n(K)$ we attach the ideal

$$I(S) = \{f \in K[t] \mid \forall x \in S, f(x) = 0\},$$

and to any ideal $J \subset K[t]$, we attach the subset

$$V(J) = \{x \in K^n \mid \forall f \in J, f(x) = 0\}.$$

Then the associated closure operations are just the composites of these two processes in either order. I leave it to you to check that for every subset $S \subset K^n$, $V(I(S)) = \overline{S}$, the Zariski closure. What about the other way around?

This works nicely if K is algebraically closed: then for all ideals J of $K[t]$, we have $I(V(J)) = \operatorname{rad} J$ (Hilbert's Nullstellensatz).

In particular, for any proper ideal J of $K[t]$, $I(V(J))$ is proper. This means: for any polynomials $f_1, \ldots, f_m \in K[t]$, either there is $x \in K^n$ with $f_i(x) = 0$ for all i, or there are polynomials $g_1, \ldots, g_m$ such that $g_1 f_1 + \ldots + g_m f_m = 1$. This consequence of Hilbert's Nullstellensatz is often called the **weak Nullstellensatz**.

Still assuming that $K = \overline{K}$, let's introduce the notion of an **afine variety**. Let J be a radical ideal of $\overline{K}[t]$, and let $V(J)$ be the corresponding Zariski-closed subset of $\overline{K}^n$. A polynomial $f \in K[t]$ can of course be thought of as a K-valued function on K^n: further, it can be shown that since K is infinite, different polynomials determine different K-valued functions on K^n. By restriction, each f can also be

thought of as a function on $V(J)$. But now the injectivity is lost, because any element of J evaluates to the zero function on $V(J)$. It is not hard to see that this is the entire source of the ambiguity: namely, elements of the quotient ring $K[t]/J$ give well-defined functions on J, and the natural map

$$K[t]/J \to \text{Maps}(V(J), K)$$

is injective. In this way we see that it is reasonable to regard $K[t]/J$ as the **ring of polynomial functions on** $V(J)$. Thus the quotient ring $K[t]/J$ is an algebraic object which carries equivalent information to the subset J.

Exercise 3.1: Let $K = \overline{K}$. For a Zariski-closed subset $S \subset K^n$, TFAE:
(i) S is **irreducible**: it is not the union of two proper, nonempty Zariski-closed subsets.
(ii) The ideal $I(S)$ of $K[t]$ is prime.
(iii) The quotient ring $K[t]/I(S)$ is a domain.
In Silverman's terminology, a Zariski-closed subset of K^n satisfying these equivalent conditions is called an **affine subvariety** of $\mathbb{A}^n$.

Now suppose that K is *not* algebraically closed. Unfortunately now the Nullstellensatz and most of the above pleasant consequences fail. In particular, since K is not algebraically closed, there is some nonconstant polynomial $f \in K[t_1]$ without a root in K, and then the ideal $J = \langle f \rangle$ is proper but $V(J) = \varnothing$. Thus the Nullstellensatz – or even the weak Nullstellensatz – holds over a field K iff $K = \overline{K}$.

This example suggests that for an arbitrary field K it is convenient to pair the polynomial ring $K[t_1, \ldots, t_n]$ with $\overline{K}^n$. For an ideal J of $K[t_1, \ldots, t_n]$, let $V^a(J)$ be the set of $x = (x_1, \ldots, x_n) \in \overline{K}^n$ with $g(x) = 0$ for all $g \in J$. For $S \subset \overline{K}^n$, let $I(S)$ be the set of $g \in K[t_1, \ldots, t_n]$ such that $g(x) = 0$ for all $x \in S$.

Theorem 3.1. *(Semirational Nullstellensatz) For all ideals J of $K[t_1, \ldots, t_n]$, we have $I(V^a(J)) = \operatorname{rad} J$.*

The moral here is that when dealing with algebraic geometric objects over a nonalgebraically closed field K, if one wants to think in terms of "points" (more precisely, *closed points*), one should take these points to lie in $\overline{K}$. There is another half to this philosophy though: we do want, and need, the notion of a variety *defined over* K. If $S \subset \overline{K}^n$, we need a notion of S being "defined over K". The correct notion on the algebraic side is as follows: we have an extension of rings

$$\iota : K[t] \hookrightarrow \overline{K}[t]$$

and thus for any ideal $\mathfrak{j}$ of $K[t]$, we may **push it forward** to get an ideal $\iota_* \mathfrak{j} = \mathfrak{j}\overline{K}[t]$ of $\overline{K}[t]$. We can also **pull back** ideals of J of $\overline{K}[t]$ via $\iota^* J = J \cap K[t]$. Now it makes sense to say that an ideal J of $\overline{K}[t]$ **is defined over** K if it is *extended* from $K[t]$, i.e., if there is an ideal $\mathfrak{j}$ of $K[t]$ such that

$$J = \iota_* \mathfrak{j}.$$

Theorem 3.2. *Let K be a field. Let $\mathfrak{j}$ be an ideal of $K[t] = K[t_1, \ldots, t_n]$, and let J be an ideal of $\overline{K}[t]$. Let $\iota : K[t] \hookrightarrow \overline{K}[t]$ be the canonical map.*
a) The following are equivalent:
(i) J is defined over K.

(ii) $\iota_* \iota^* J = J$.
b) Let $G = \mathrm{Aut}(\overline{K}/K)$. *The following are equivalent:*
(i) For all ideals J *of* $\overline{K}[t]$, $\iota^* J = J^{\mathfrak{g}_K}$.
(ii) K *is perfect.*
(iii) $\overline{K}^G = K$.

Proof. a) Left as an exercise.
$\neg$ (ii) $\implies$ $\neg$ (i): If K is not perfect, it has characteristic $p > 0$ and there is $\alpha \in K \setminus K^p$. Let $n = 1$ and $J = \langle t - \alpha \rangle$. Then $\iota^* J = \langle (t-\alpha)^p \rangle$ but $t - \alpha \in J^G$.
(ii) $\iff$ (iii): By standard field theory, for any field K, $\overline{K}^G = \bigcup_{n=1}^{\infty} K^{p^{-n}}$ is the **perfect closure** of K. This coincides with K iff $K = K^p$.
(ii) $\implies$ (i): This requires some work: see e.g. [KCd], especially §4. The term for this kind of argument is **Galois descent**. □

Exercise 3.2: Use Theorem 3.2a) to deduce the Semirational Nullstellensatz from Hilbert's Nullstellensatz.

For a field which is not perfect, Galois descent can often be salvaged by replacing an algebraic closure $\overline{K}$ with a *separable* algebraic closure K^{sep}, the key point being that for any field K,

$$(K^{\mathrm{sep}})^{\mathrm{Aut}(K^{\mathrm{sep}}/K)} = K.$$

Exercise 3.3: Let K be any field.
a) Let $\sigma \in \mathrm{Aut}(\overline{K}/K)$. Show that σ restricts to a field isomorphism of K^{sep}.
b) By part a) there is a canonical map $\mathrm{Aut}(\overline{K}/K) \to \mathrm{Aut}(K^{\mathrm{sep}}/K)$. Show that this map is an isomorphism.

The previous exercise justifies writing G for *either* $\mathrm{Aut}(\overline{K}/K)$ or $\mathrm{Aut}(K^{\mathrm{sep}}/K)$, as we shall do from now on.

Exercise 3.4: Show that Galois descent holds for affine varieties. More precisely, let K be a field with separable algebraic closure K^{sep}, let J be an ideal of $K[t]$, and let $V(K) = V(J)$ be the corresponding Zariski-closed subset of K^n. Let $V(K^{\mathrm{sep}})$ be the Zariski-closed subset corresponding to $\iota_* I$, i.e., the pushforward of I to an ideal of $K^{\mathrm{sep}}[t]$. Show:

$$V(K^{\mathrm{sep}})^G = V(K).$$

Of course the worry with the "K^{sep} remedy" is that if K is not perfect, the field K^{sep} is not algebraically closed, so it may not be "large enough" for certain geometric purposes. Very roughly, if we stick not to arbitrary Zariski-closed subsets of projective space but *smooth, geometrically integral varieties*, then K^{sep} tends to behave as if it were algebraically closed. No more on this now...later, perhaps.

A workable definition of an affine K-variety is that the category of affine K-varieties should be the opposite category of the category of integral domains which are finitely generated K-algebras, in which the morphisms are K-algebra maps. In fact we only want to consider varieties which are not only integal but **geometrically integral**, namely such that $K[V] \otimes_K \overline{K}$ is still a domain.

An affine K-variety V comes with a well-defined **dimension** $\dim V \in \mathbb{N}$. This is

either the Krull dimension of the coordinate ring $K[V]$ or the transcendence degree of the field extension $K(V)/K$: see e.g. [CA] to see that these agree. The second definition makes clear that dimension is invariant under base extension: if L/K is any field extension, then $L[V] = K[V] \otimes_K L$ is the coordinate ring of an affine variety $V_{/L}$, and $\dim(V_{/L}) = \dim V$.

An **affine curve** is an affine K-variety of dimension one. A **smooth affine curve** if an affine curve satisfying the Jacobian condition on all of its $\overline{K}$ points.

Exercise 3.5: Let k be a field of characteristic 3, and let $K = k(t)$. Consider the K-algebra $K[C] = K[x,y]/(y^2 - x^3 + t)$.
a) Show that $K[C]$ is a Dedekind domain.
b) Deduce that $K[C]$ is regular: for all $\mathfrak{m} \in \operatorname{MaxSpec} K[C]$, $\dim_{K[C]/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 = 1$.
c) Show that nevertheless the affine curve C is not smooth.

The notion of a morphism of K-varieties can be reduced to that of a regular function on a K-variety: if V, W are affine K-varieties, with $W \subset \mathbb{A}^n_{/K}$, then a morphism $f : V \to W$ is given by a collection of n functions $f_1, \ldots, f_n \in K[V]$ such that for all $x \in V(\overline{K})$, $(f_1(x), \ldots, f_n(x)) \in W(\overline{K})$. We would get more style points for a "schemier" definition, but we'll try to work with this slightly naive one.

3.2. **Projective Varieties.**

Although the class of affine varieties is algebraically very natural, from a geometric perspective we really want (and need) to consider **projective varieties**. The justification for this is that if $V_{/\mathbb{C}}$ is an affine variety of positive dimension, then $V(\mathbb{C})$ endowed with the analytic topology – i.e., the subspace topology of the usual topology on $\mathbb{C}^n$ – is never compact, whereas since $\mathbb{CP}^n$ is a compact manifold, every projective variety over $\mathbb{C}$ is compact. I hope I do not have to argue for the usefulness of compactness as a property of topological spaces: e.g. any compact metric space is complete. In algebraic geometry, projective varieties satisfy important "completeness properties", especially related to intersection theory. As a basic example, two curves in the affine complex plane "usually" intersect in a finite set of points, but exceptionally, need not interset at all: e.g. two lines fail to intersect iff they are distinct and parallel. But as any student of art learns, *parallel lines meet at infinity*. In particular, any two distinct lines in the projective plane $\mathbb{CP}^2$ meet in exactly one point. The unity that this brings to the subject is both elegant and useful.

Projective space $\mathbb{P}^n(K)$: for a field K, we first want to define the point set $\mathbb{P}^n(K)$. This is given by the familiar recipe: we start with the set $K^{n+1} \setminus \{(0, \ldots, 0\}$, and we mod out by the equivalence relation $(x_0, \ldots, x_n) \sim (\lambda x_0, \lambda x_1, \ldots, \lambda x_n)$ for all $\lambda \in K^\times$. We denote the equivalence class of $(x_0, \ldots, x_n)$ by $[x_0 : \ldots : x_n]$.

As for affine space, this gives a functor (at least) on field extensions: for any field extension L/K, we get an injection of sets $\mathbb{P}^n(K) \hookrightarrow \mathbb{P}^n(L)$. And as above it is useful to think especially of the inclusion

$$\mathbb{P}^n(K) \hookrightarrow \mathbb{P}^n(\overline{K}).$$

For $P = [X_0 : \ldots : X_n] \in \mathbb{P}^n(\overline{K})$, we defined the **field of definition** of P as follows: we choose i such that $X_i \neq 0$ and put

$$K(P) = K\left(\frac{X_0}{X_i}, \ldots, \frac{X_n}{X_i}\right).$$

Of course there is something to check here.

Exercise 3.6: Show that this definition is independent of our choice of i.

Does Galois descent hold in projective space? That is, must we have

$$\mathbb{P}^n(K^{\mathrm{sep}})^G = \mathbb{P}^n(K)?$$

This is not an obvious consequence of Galois descent for vector spaces because projective space is defined by a quotient construction, and in general passing to quotients does not commute with taking G-invariants.

Since this is a key idea, let us come at it first in a slightly more abstract (but also simpler) context. For a group G, a **G-module** is a commutative group M on which G acts by group automomorphisms. It turns out that this is not really a generalization of the notion of a module: being a G-module is equivalent to being a left module over the (non-commutative, if G is!) group ring $\mathbb{Z}[G]$. In particular, the G-modules form an abelian category with enough projectives and enough injectives...all of which to say is that co/homological constructions work nicely. Consider a short exact sequence of G-modules

$$0 \to A \to B \to B/A \to 0.$$

For any G-module A, we put

$$A^G = \{x \in A \mid gx = x \ \forall g \in G\}.$$

One swiftly sees that the functor $A \mapsto A^G$ is left exact: applying it to the above short exact sequence, one gets an exact sequence

$$0 \to A^G \to B^G \xrightarrow{\varphi} (B/A)^G.$$

However, in general φ need not be surjective: in fact its image in $(B/A)^G$ is $\frac{B^G}{A^G}$, so what we're saying is that in general we have

$$\frac{B^G}{A^G} \subset (B/A)^G,$$

but this containment may be proper: a G-invariant element of the quotient need not have a G-invariant representative in B. To show you that this is a basic fact of life and not some fancy cohomological phenomenon, consider the following example from linear algebra. Let $B = \mathbb{C}^2 = \langle e_1, e_2 \rangle_{\mathbb{C}}$, and let A be the one-dimensional subspace $\langle e_1 \rangle_{\mathbb{C}}$. Let $G = \mathbb{Z}$, and let G act on B by sending $1 \in \mathbb{Z}$ to the matrix $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ (and thus sending $n \in \mathbb{Z}$ to the matrix $\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$).

Exercise 3.7: Show that:
(i) $B^G = A = A^G$.
(ii) $(B/A)^G = B/A$.
(iii) $B^G/A^G \subsetneq (B/A)^G$.

So the burden is on us to explain why this sort of thing does not happen in projective space. First, we need to place ourselves in the context of G-modules: we have $\mathbb{P}^N(K) = K^{N+1} \setminus \{0\}/K^\times$; where is the group structure? Let us first work with the subset $\mathcal{U} = (K^\times)^{N+1}$; its image $\mathcal{U}/K^\times$ is the Zariski-dense subset $U(K)$ of projective space consisting of points *all* of whose projective coordinates are not zero. The point here is that U is a group and $K^\times$ is a subgroup. Working over K^{sep} we get a short exact sequence of $G = \mathrm{Aut}(K^{\mathrm{sep}}/K)$-modules

$$0 \to (K^{\mathrm{sep}})^\times \to ((K^{\mathrm{sep}})^\times)^{N+1} \to \mathcal{U}(K^{\mathrm{sep}}) \to 0.$$

Taking G-invariants, we get

$$0 \to K^\times \to (K^\times)^{N+1} \stackrel{\varphi}{\to} \mathcal{U}(K^{\mathrm{sep}})^G,$$

and now notice that by Galois descent for vector spaces we have $(\mathcal{U}(K^{\mathrm{sep}}))^G = \mathcal{U}(K)$, so our task is reduced to showing that φ is surjective. But a short exact sequence of G-modules induces a long exact sequence in group cohomology, the next term of which is $H^1(G, \mathrm{K}^{\mathrm{sep}\,\times})$. And now we come to the first important result of **Galois cohomology**: it is a famous result of Hilbert, **Hilbert's Theorem 90**, that $H^1(G, \mathrm{K}^{\mathrm{sep}\,\times}) = 0$.

Exercise 3.8: Show that the above argument can be extended to give a Galois descent on all of $\mathbb{P}^N$, not just its open subset U.

We may define a Zariski topology on $\mathbb{P}^N(K)$ in much the same way as on $\mathbb{A}^{N+1}(K)$, except that we need to restrict to homogeneous polynomials: this is because the value of a polynomial $f(X_0, \ldots, X_n)$ does depend upon the representative $(X_0, \ldots, X_n)$. However, if f is homogeneous of degree d, then for all $\lambda \in K$, $f(\lambda X_0, \ldots, \lambda X_n) = \lambda^d f(X_0, \ldots, X_n)$. In particular, the relation $f(X_0, \ldots, X_n) = 0$ is well-defined on the quotient.

Again this gives a Galois connection, and the passage from a subset S of $\mathbb{P}^N(K)$ to the ideal J generated by homogeneous polynomials in $K[T_0, \ldots, T_N]$ vanishing identically on S to the simultaneous zero set in $\mathbb{P}^N(K)$ of the homogeneous elements of J is the closure operator for a topology on $\mathbb{P}^N(K)$, the **Zariski topology**.

Exercise 3.9: Show that Galois descent holds for Zariski-closed subsets of $\mathbb{P}^N(K)$.

3.3. **Homogeneous Nullstellensätze.**

We now pursue analogues of the Nullstellensatz in projective space. (In the lecture I revealed that my understanding / memory of this area is far from complete. Had I spent more time preparing on this topic, I would have seen that in fact most introductory texts in algebraic geometry give at least *some* treatment of this. What follows is a somewhat more complete treatment than is traditional, and in fact more than we will need for our work on elliptic curves, given for penitential reasons.)

Let K be a field, $f \in K[T]$, and $x \in \mathbb{P}^n(K)$. Let

$$q : \mathbb{A}^{n+1}(K) \setminus \{0\} \to \mathbb{P}^n(K)$$

be the quotient map. We say x **is a zero of** f – and write $f(x) = 0$ – if **for all** $\tilde{x} \in q^{-1}(x)$, $f(\tilde{x}) = 0$. Note that in general this condition may be satisfied for one

element of $q^{-1}(x)$ but not for another; however, if f is **homogeneous** then the condition is independent of the choice of $\tilde{x} \in q^{-1}(x)$.

Proposition 3.3. *Let K be an infinite field. Let $f \in K[t]$, and write $f = \sum_{i=0}^{r} f_i(T)$ as a sum of homogeneous components. For $x \in \mathbb{P}^n(K)$, we have $f(x) = 0 \iff \forall 1 \leq i \leq r,\ f_i(x) = 0$.*

Proof. Suppose $f(x) = 0$: that is, for all $\lambda \in K^\times$, $f(\lambda x) = \lambda^r f_r(x) + \ldots + \lambda f_1(x) + f_0(x) = 0$. Since K is infinite, this implies $f_0(x) = \ldots = f_r(x) = 0$. The converse direction is immediate. □

For an ideal J of $K[T]$, let $V_{\mathbb{P}}(J)$ be the set of $x \in \mathbb{P}^n(K)$ such that $f(x) = 0$ for all $f \in J$. On the other hand, for a subset $S \subset \mathbb{P}^N(K)$, let $I(S)$ be the set of all $f \in K[T]$ such that $f(x) = 0$ for all $x \in S$. Note that this is really a special case of our affine construction, namely

$$I(S) = I(q^{-1}(S))).$$

Lemma 3.4. *Let $R = \bigoplus_{i=0}^{\infty} R_i$ be a graded ring. For an ideal I of R, TFAE:*
(i) I is generated by homogeneous elements.
(ii) For every $f = \sum_{i=0}^{r} f_i \in R$, $f \in I$ iff each $f_i \in I$.
*An ideal satisfying these equivalent conditions is called **homogeneous**.*

Exercise 3.10: Prove it.

Lemma 3.5. *Let I be an ideal in a graded ring. If I is homogeneous, so is* $\operatorname{rad} I$.

Exercise 3.11: Prove it.

Proposition 3.6. *Let K be infinite, J an ideal of $K[T]$ and S a subset of $\mathbb{P}^n(K)$.*
a) We have $V_{\mathbb{P}}(I(S))$ is the Zariski closure of S.
b) $I(V_{\mathbb{P}}(J))$ is a homogeneous radical ideal containing J.

Exercise 3.12: Prove it.

Suppose now that K is algebraically closed and that J is a homogeneous ideal of $K[T]$. As in the affine case, knowing only that $I(V_{\mathbb{P}}(J))$ is a homogeneous radical ideal containing J, Occam's razor suggests that we seriously consider the possibility that $I(V_{\mathbb{P}}(J)) = \operatorname{rad} J$.

However, in the projective world there is at least one case where this fails. Namely, let $J = \langle T_0, \ldots, T_N \rangle$. Note that J is indeed a homogeneous, radical (indeed, maximal) ideal of $K[T]$. Then $V(J) = (0, \ldots, 0)$, which does not give a point in projective space. It follows that $I(V_{\mathbb{P}}(J)) = K[T]$.

How do we deal with this counterexample? Simply by excluding it! Namely, the ideal $\langle T_0, \ldots, T_N \rangle$ is called the **irrelevant ideal**; any other ideal is called **relevant**.

Theorem 3.7. *(Homogeneous Nullstellensatz I) Let K be an algebraically closed field, and let $J \subset K[T] = K[T_0, \ldots, T_n]$ be a homogeneous ideal. Then:*
a) We have $V_{\mathbb{P}}(J) = \varnothing \iff \operatorname{rad} J \supset \langle T_0, \ldots, T_n \rangle$.
b) If $V_{\mathbb{P}}(J) \neq \varnothing$, then $I(V_{\mathbb{P}}(J)) = \operatorname{rad} J$.

Proof. Since the radical of a homogeneous ideal is radical and $V_{\mathbb{P}}(J) = V_{\mathbb{P}}(\operatorname{rad} J)$, we may – and shall – assume that J is a radical homogeneous ideal.
a) Note that $V_{\mathbb{P}}(J) = \varnothing \iff V(J) \subset \{(0)\}$; by Hilbert's Nullstellensatz, $V(J) \subset \{(0)\} \iff J \supset (T_0, \ldots, T_n)$.

b) Since J is homogeneous and $V_{\mathbb{P}}(J)$ is nonempty, $I(V_{\mathbb{P}}(J)) = I(q^{-1}(V_{\mathbb{P}}(J))) = I(V(J)) = J$ by Hilbert's Nullstellensatz. □

Theorem 3.8. *(Homogeneous Nullstellensatz II) Let K be an algebraically closed field, and let $f_1, \ldots, f_n \in K[T_0, \ldots, T_n]$ be polynomials of positive degree. Then there is $x \in \mathbb{P}^n(K)$ such that $f_1(x) = \ldots = f_n(x) = 0$.*

We will give two proofs. The first deduces the result from Hilbert's Nullstellensatz. The second deduces it from Theorem 3.7 along with Krull's Hauptidealsatz.

Proof. Step 1: Let $J = \langle f_1, \ldots, f_n \rangle$ and let

$$Z = V(J) = \{x \in k^{n+1} \mid f_1(x) = \ldots = f_n(x) = 0\}.$$

Since each f_i is homogeneous, $Z \supset \{0\}$; seeking a contradiction, we suppose $Z = \{0\}$. Then by Hilbert's Nullstellensatz, $\operatorname{rad} J = I(V(J)) = I(Z) = I(\{0\}) = \langle t_0, t_1, \ldots, t_n \rangle$, i.e., there is $k \in \mathbb{Z}^+$ such that $t_0^k, \ldots, t_n^k \in J$, and thus there are polynomials g_{ij} such that for all $0 \leq i \leq n$,

$$t_i^k = \sum_{j=1}^n g_{ij} f_j$$

we may assume that each g_{ij} is homogeneous of degree $k - \deg f_j < k$.
Step 2: Let $B = k[t_0, \ldots, t_n]$, and let $m_1, \ldots, m_s$ be the monomials in B of degree less than $k(n+1)$. Put $A = k[f_1, \ldots, f_n]$ and $M = \langle m_1, \ldots, m_s \rangle_A$.
We CLAIM $M = k[t_0, \ldots, t_n]$.
SUFFICIENCY OF CLAIM: By the claim, $B = k[t_0, \ldots, t_n]$ is a finitely generated A-module, and thus B/A is an integral extension of domains. Let E and F be the fraction fields of A and B respectively; then F/E is an algebraic field extension. But $\operatorname{trdeg} E/k \leq n$ and $\operatorname{trdeg} F/k = n+1$, contradiction.
Step 3: PROOF OF CLAIM: It suffices to show that M contains all monomials $t_0^{a_0} \cdots t_n^{a_n}$. This is true by definition when $\delta = a_0 + \ldots + a_n < k(n+1)$; in general, we go by induction on δ. Suppose $\delta \geq k(n+1)$; then $a_i \geq k$ for some i; relabelling if necessary, we may assume that $a_0 \geq k$. Since $t_0^k = \sum g_{1j} f_j$, we have

$$t_0^{a_0} \cdots t_n^{a_n} = \sum_{j=1}^n (g_{1j} t_0^{v_0 - k} t_1^{v_1} \cdots t_n^{v_n}) f_j.$$

The coefficient of each f_j is homogeneous of degree less than δ, hence by induction is contained in M. Since M is an A-module, it follows that $t_0^{a_0} \cdots t_n^{a_n} \in M$. □

Proof. Let $J = \langle f_1, \ldots, f_n \rangle$. Note that $J \subset \langle t_0, \ldots, t_n \rangle$, so J is a proper ideal of $K[T]$. As for any proper ideal in a commutative ring, there is at least one minimal prime ideal $\mathfrak{p}$ containing J. Since R is Noetherian and J is generated by n elements, by Krull's Hauptidealsatz $\mathfrak{p}$ has height at most n. Therefore $\mathfrak{p} = \operatorname{rad} \mathfrak{p}$ does not contain the irrelevant ideal $\langle t_0, \ldots, t_n \rangle$, and by Theorem 3.7 $V_{\mathbb{P}}(J) \neq \varnothing$. □

3.4. **Bézout's Theorem.**

Let K be an algebraically closed field, let $f(X, Y, Z) \in K[X, Y, Z]$ be homogeneous of degree $d_f > 0$, and let $g(X, Y, Z) \in K[X, Y, Z]$ be homogeneous of degree $d_g > 0$. Bézout's Theorem is a statement about the common zero locus of f and g,

or equivalently by the Nullstellensatz, a statement about the homogeneous coordinate ring $K[X,Y,Z]/\langle f,g\rangle$.

Step 1: We need to assume that f and g have no (nonunit) common factor in the UFD $K[X,Y,Z]$. Otherwise there is a polynomial $h(X,Y,Z)$ of positive degree such that $I \subset \langle h\rangle$, and $V(I) \supset V(h)$, i.e., $V_{\mathbb{P}}(I)$ contains an entire curve.

Having made the assumption in Step 1, it turns out to be true that $V_{\mathbb{P}}(I)$ is a finite set. Indeed, one can say more: its cardinality, say N, satisfies

$$1 \leq N \leq d_f d_g.$$

Note that $N \geq 1$ by Theorem 3.8. This is one of the advantages of working in $\mathbb{P}^2$ rather than $\mathbb{A}^2$. In fact for those who know some commutative algebra it is a good exercise to try to show that if $f,g \in K[x,y]$ have no common factor, then the affine algebra $K[x,y]/\langle f,g\rangle$ is finite dimensional over K.

At the moment we have an inequality. In some branches of mathematics inequalities are the basic currency of the realm, but in elementary algebraic geometry it is often the case that by working harder an inequality can be refined to an equality. (The other shining instance of this is Riemann's inequality, which was refined by Roch into an equality: the Riemann-Roch theorem.) In this case we probably also have some intuition that there should be "in general" precisely $d_f d_g$ intersection points, and what stops that from happening is accidents of "higher order intersection". For instance, even in $\mathbb{A}^2$ over $\mathbb{R}$, most lines $g = ax - by$ through $(0,0)$ intersect the curve $f(x,y) = y - x^2$ at two points ($2 = d_f d_g$), the exceptions being the vertical line $x = 0$ and the horizontal line $y = 0$, which intersect in only one point. You can – and should – check that the first scenario is repaired by passing to $\mathbb{P}^2$: the point $[0:1:0]$ is also an intersection point. However even in $\mathbb{P}^2_{/\mathbb{C}}$ the projective variety $V_{\mathbb{P}}(\langle y, yz - x^2\rangle)$ consists only of a single point, $[0:0:1]$.

From a geometric perspective, what is special about the line $y = 0$ among all lines passing through the curve $y - x^2$ at $(0,0)$ is, of course, that it is the **tangent line**. In the language of calculus, it is the unique best linear approximation to $f(x) = x^2$ at $x = 0$. It is possible to carry over this analytic intuition to the present algebraic context using the notion of completion of the local ring at $(0,0)$, but let us go for something more elementary and algebraic.

Indeed, consider the affine algebra $\mathbb{C}[x,y]/(y-x^2,y)$. This is a local ring with unique maximal ideal $(0,0)$, which corresponds to the fact that $V_{\mathbb{C}}(\langle y - x^2, y)\rangle) = \{(0,0)\}$. Indeed, a moment's thought shows that this ring is isomorphic to $\mathbb{C}[x]/(x^2)$. But now let us pay attention to exactly what the Nullstellensatz asks us to ignore: namely the difference between the ideal (x^2) and its associated radical ideal (x). Thus we have the algebra $\mathbb{C}[x]/(x^2)$ rather than the corresponding "reduced" (i.e., free of nilpotent elements) algebra $\mathbb{C}[x]/(x^2)$. The nonreduced algebra carries more information – in fact, exactly the information we want. Namely, we have $\dim_{\mathbb{C}} \mathbb{C}[x,y]/(y - x^2, y) = 2$, and this is the 2 we wanted to see: we want to define the **local intersection multiplicity** of y and $y - x^2$ at $(0,0)$ to be 2.

In the same way we can give a general definition of local intersection multiplicity of $f(X,Y,Z)$ and $g(X,Y,Z)$ as the dimension of a certain local ring. First, observe that since the invariant we are trying to define is *local*, we may immediately reduce to the affine case: each of the points of $V_{\mathbb{P}}(\langle f,g\rangle)$ lies in at least one affine coordinate patch U_0, U_1, U_2, and to define the local intersection multiplicity we work in any one affine patch containing the given point. For concreteness we may as well assume that a point lies in the patch $Z \neq 0$, i.e., reduce to the affine case. Then as mentioned above, the hypothesis that $f(x,y), g(x,y) \in K[x,y]$ contain no common factor implies that $V(\langle f,g\rangle)$ is zero-dimensional; equivalently the affine algebra $K[x,y]/(f,g)$ is a **finite-dimensional K-algebra**. In particular it is an **Artinian ring** – i.e., it satisfies the (very strong!) descending chain condition on ideals. We can therefore exploit the structure theory of Artinian rings: every Artinian ring R has finitely many maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$ and is isomorphic to a product of r Artinian local rings:

$$R \cong \prod_{i=1}^{r} R_i,$$

where $R_i = R_{\mathfrak{m}_i}$. In our context then we may factor $K[x,y]/(f,g)$ as a product $\prod_{i=1}^r R_i$ – where $V(\langle f,g\rangle) = \{P_1, \ldots, P_r\}$. We are trying to assign a positive integer to each P_i, so we may simply define the **local intersection multiplicity** $m(f,g)_{P_i}$ to be $\dim_K R_i$. Again, we do this for all points in $V_{\mathbb{P}}(\langle f(X,Y,Z), g(X,Y,Z)\rangle)$. Finally we can state the desired result.

Theorem 3.9. *(Bézout's Theorem) Let $K = \overline{K}$, and let $f, g \in K[X,Y,Z]$ be homogeneous polynomials of degrees $d_f, d_g > 0$ with $\gcd(f,g) = 1$. Then*

$$\sum_{P \in V_{\mathbb{P}}(\langle f,g\rangle)} m(f,g)_{P_i} = d_f d_g.$$

3.5. **Bézout's Theorem and Singular Points.**

There are relations between local intersection multiplicities of an intersection of two curves and multiplicities of singular points on a single curve. Again without proof, we mention some of these.

Let C be a geometrically integral plane curve given by a homogeneous polynomial $f(X,Y,Z) = 0$, and let $P \in C(\overline{K})$. Let ℓ be a line passing through P. There are already some interesting things to say about the local intersection multiplicity $m(f,\ell)_P$.

• Suppose that P is a nonsingular point of C. Then there is a unique line passing through P such that $m(f,\ell)_P > 1$: the tangent line at P. Further, the tangent line can be defined over the field of definition $K(P)$ of P.

• If P is a nonsingular point of C, then we say that P is a **flex point** of C if for some line ℓ through P we have $m(f,\ell)_P \geq 3$. By the above bullet point, if such a line exists, then it must be the tangent line at P.

Flex points are part of the rich **extrinsic geometry** of a plane curve, i.e., the geometry of the curve as it is embedded in the projective plane. Very shortly we will formalize the notion of *projectively equivalent* plane curves, and then it will be

clear that the existence and number of flex points is a projective invariant. It is not an **intrinsic invariant** of a curve: many curves admit multiple inequivalent embeddings into $\mathbb{P}^2$ (and more so, into $\mathbb{P}^n$) and the resulting isomorphism of abstract algebraic curves need not preserve flex points.[3]

For instance, a smooth plane cubic over an algebraically closed field of characteristic different from 3 has precsisely nine distinct flex points. One could try to prove this now using tools of classical geometry like the **Hessian** – indeed, this would be a great exercise – but this becomes much easier when more of the theory of elliptic curves is developed.

• Now suppose that P is a singular point of C. We claim that for *every* line ℓ passing through P we have $m(f,\ell)_P \geq 2$.

This claim has many important and useful consequences for us. Here is one:

Proposition 3.10. *Let $C : f(x,y,z) = 0$ be a geometrically irreducible plane cubic curve. Then C has at most one singular point.*

Proof. Suppose not, and let $P_1 \neq P_2 \in C(\overline{K})$ be distinct singular points. There is a unique line ℓ joining P_1 to P_2. By Bézout's Theorem the sum of the local intersection multiplicities is $d_f d_\ell = 3$. However, the local intersection multiplies $m(f,\ell)_{P_1}$ and $m(f,\ell)_{P_2}$ are both at least 2: contradiction! □

Exercise 3.13 Let $d \in \mathbb{Z}^+$. Show that there is a positive integer $S(d)$ such that no geometrically irreducible plane curve of degree d has more than $S(d)$ singularities.

Since I am not proving my assertions in this section anyway, I cannot resist the temptation to take things a little farther. One wants to associate to any point P on a curve C (say over an algebraically closed field K) a positive integer $m(P)$, which is equal to 1 iff P is a nonsingular point, and in some sense gets larger as the singularity at P gets worse. Assuming the curve is embedded in $\mathbb{P}^2$ (which is, by the way, a big assumption in general: over any infinite field, every algebraic curve can be embedded in $\mathbb{P}^3$, but a nonsingular degree d curve in $\mathbb{P}^2$ has genus $\frac{(d-1)(d-2)}{2}$, whereas for any $g \in \mathbb{N}$ there are nonsingular curves of genus g!) there are two rather concrete ways to do this:

First measure: Without loss of generality we think about affine curves $f(x,y) = 0$. If $P = (x_0, y_0)$ is a singular point, then clearly the change of variables $x \mapsto x - x_0,\ y \mapsto y - y_0$ carries P to $(0,0)$. Consider the defining polynomial (let's still call it f) $f(x,y) = 0$. Like any polynomial, we decompose it in terms of homogeneous polynomials:

$$f(x,y) = \sum_{d=0}^{\infty} f_d(x,y),$$

where $f_d(x,y)$ is homogeneous of degree d (and of course, identically zero for $d \gneq 0$). To say that $(0,0)$ lies on the curve is, of course, to say that $f_0 \equiv 0$. Further, observe that $(0,0)$ is a singular point iff moreover $f_1 \equiv 0$. Thus the least $d \in \mathbb{N}$

[3] In this regard one should perhaps mention **Weierstrass points**, which have a similar flavor to flex points but are part of the **intrinsic geometry** of a curve.

such that f_d is not identically zero is an integer ≥ 2. If you draw some examples of singular points of plane curves, you will quickly convince yourself that the larger this quantity d is the "worse" the singularity is. Thus it is reasonable to regard d as one kind of numerical measure of the singularity: let's call it $m_1(P)$.

Second measure: Above we said that a point $P \in C(K)$ is singular iff for every line ℓ passing through C we have $m(f, \ell)_P \geq 2$. So why not take this a step further: for $P \in C(K)$, we define $m_2(P)$ to be the smallest positive integer d such that for every line ℓ passing through P we have $m(f, \ell)_P \geq d$.

Exercise 3.13: a) Show that the set of lines ℓ passing through P such that $m(f, \ell)_P > m_2(P)$ is finite. Let us call such a line an **exceptional line**. b) Show by example that the set of exceptional lines can be – among finite numbers! – arbitrarily large. c) Is there always at least one exceptional line?

Exercise 3.14: Compare the two invariants $m_1(P)$ and $m_2(P)$. Are they always equal?

3.6. **Projective Equivalence.** Let K be a field, and let V be an $n+1$-dimensional vector space over K. By $\mathbb{P}V$ we will mean the associated projective space obtained as the space of all lines through the origin in V.

As you well know, the group $\mathrm{GL}_{n+1}(K)$ acts on V by linear transformations. This action is **effective**: for any non-identity matrix m, there is $v \in V$ with $mv \neq v$. (In case this is not intimately familiar to you, look at it the other way around: if for every standard basis vector $e_1, \ldots, e_{n+1}$ of V we have $me_i = e_i$, then we see that our matrix is the $(n+1) \times (n+1)$ identity matrix.)

When a group G acts on a set X, there are some naturally induced actions on other sets formed in terms of X. First, G also acts on the set 2^X of all subsets of X: namely $g : Y \subset X \mapsto gY = \{gy \mid y \in Y\}$. This is however a very "large" action. In particular, as long as $X \neq \varnothing$ it is not a transitive action, because the G-orbit of a subset Y of X consists only of subsets Y' of the same cardinality as Y. This motivates the following construction.

For any $k \in \mathbb{Z}^+$, let $S_k(X)$ be the set of k-element subsets of X. Then G acts on $S_k(X)$ simply by $g\{x_1, \ldots, x_k\} = \{gx_1, \ldots, gx_k\}$. These actions come up for instance, in some of the proofs of the Sylow theorems. More broadly useful is the induced action of G on the set $P_k(X)$ of **ordered k-element subsets** of X, or, to be formal about it, injective functions $\iota : \{1, \ldots, k\} \to X$: for $g \in G$, we send $(x_1, \ldots, x_k)$ to $(g(x_1), \ldots, g(x_k))$. Note that for $k = 1$, $S_k(X) = P_k(X) = X$ and we recover the action we started with.

Remark for the nullologists: we allow any group G to act on the empty set $\varnothing$: indeed there is a unique function $G \times \varnothing \to \varnothing$, the empty function. However, let us agree that this action is *not* transitive: in this action there are zero G-orbits, whereas for a transitive action there is one G-orbit.

We say that the action of G on X is **k-transitive** if the induced action of G on $P_k(X)$ is transitive, i.e., there is a single G-orbit. We say that the action is **sharply k-transitive** if the induced action of G on $P_k(X)$ is simply transitive,

i.e., if there is a single G-orbit and trivial stabilizer.

Exercise 3.15: Let $l \leq k$ be positive integers.
a) If the G action on a set X is k-transitive, it is also l-transitive for all $l \leq k$.
b) There is at most one $k \in \mathbb{Z}^+$ for which a given G action on X can be sharply k-transitive.

Exercise 3.16: Let G act on a set X, and let $k \in \mathbb{Z}^+$.
a) If the action is k-transitive, then $\#G \geq \prod_{i=1}^{k} \#X - i + 1$.
b) If the action is sharply k-transitive, then $\#G = \prod_{i=1}^{k} \#X - i + 1$.

Exercise 3.17: Let $n \geq 2$.
a) Show that the natural action of S_n on $\{1, \ldots, n\}$ is sharply n-transitive.
b) Show that the natural action of A_n (alternating group) on $\{1, \ldots, n\}$ is $(n-2)$-transitive but not n-transitive.

Exercise 3.18: A group action on a set is **primitive** if the only G-stable partitions of X are $\{X\}$ and $\{\{x\}_{x \in X}\}$
a) Show that a 2-transitive group action is primitive.
b) Exhibit a primitive group action which is not 2-transitive.

Here is the upshot: already a group action being 2-transitive implies some useful qualitative information. Further, group actions which are k-transitive for $k \geq 3$ are rather rare: if you find one which is different from the examples of S_n and A_n acting on $\{1, \ldots, n\}$, you have a right to be excited. A shining example of this is Matthieu's discovery, in the 1860's and 1870's, of permutation groups M_{11}, M_{12}, M_{22}, M_{23}, M_{24}; in each case the subscript indicates the cardinality on the finite set on which the group acts. Matthieu got excited when he noticed these groups have lots of k-transitivity, specifically:

- M_{11} is sharply 4-transitive.
- M_{12} is sharply 5-transitive.
- M_{22} is 3-transitive.
- M_{23} is 4-transitive.
- M_{24} is 5-transitive.

It turns out that all five of these finite groups are non-commuative and simple: they were the first examples of **sporadic simple groups**. In fact, they were the first by far: in the mid 1960's Janko found 4 more sporadic groups, and in the late 1960's Conway found 3 more. According to **CFSG** (**classification of finite simple groups**) there are precisely 26 sporadic groups, so Matthieu's findings are already a substantial number of them. Conversely, Cameron used CFSG to prove the following remarkable result.

Theorem 3.11. *(Cameron) Let G be a finite group acting 4-transitively on a set X. Then G is isomorphic, as a permutation group, to one of the following:*
(i) S_n for $n \geq 4$.
(ii) A_n for $n \geq 6$.
(iii) M_{11}, M_{12}, M_{23}, M_{24}.

Consider now the action of $\mathrm{GL}_{n+1}(K)$ on V. It is not transitive, since the 0 vector lies in its own orbit, but it acts transitively on $V^\bullet = V \backslash \{0\}$. The action on $V^\bullet$ is not 2-transitive, because the action of G preserves the linear dependence relation: if v, w are linearly dependenent, then so are gv, gw. Once we take this extra structure into account we get very good transitivity properties.

Proposition 3.12. *The action of $\mathrm{GL}_{n+1}(V)$ on V is simply transitive on the set of ordered bases of V.*

In particular, for any $k \leq n+1$, any K-linearly independent vectors $v_1, \ldots, v_k$ and any other K-linearly independent vectors $w_1, \ldots, w_k$, there is $g \in \mathrm{GL}_{n+1}(K)$ such that $gv_i = w_i$ for all $1 \leq i \leq k$; this g is unique iff $k = n+1$.

Corollary 3.13. *For all $0 \leq k \leq n+1$, $\mathrm{GL}_{n+1}(V)$ acts transitively on the set of all k-dimensional subspaces of V.*

Theorem 3.14. *Let K be a field, $n \in \mathbb{Z}^+$, $V = K^{n+1}$, and $G = \mathrm{GL}_{n+1}(K)$.*
a) The action of G on 1-dimensional subspaces of V is 2-transitive.
b) The following are equivalent:
(i) $n = 1$.
(ii) The action of G on 1-dimensional subspaces of V is sharply 3-transitive.
(iii) The action of G on 1-dimensional subspaces of V is 3-transitive.

Proof. a) Let $\ell_1 \neq \ell_2$ and $\ell_3 \neq \ell_4$ be one-dimensional subspacess of V. Choose nonzero vectors $v_i \in V$ such that $\ell_i = \langle v_i \rangle$ for all i. Since $\ell_1 \neq \ell_2$ (resp. $\ell_3 \neq \ell_4$) v_1 and v_2 are linearly independent (resp. v_3 and v_4 are linearly independent). Thus there is an ordered basis $B_1 = \{v_1, v_2, \ldots\}$ of V and an ordered basis $B_2 = \{v_3, v_4, \ldots\}$ of K; by Proposition 3.12, there is $g \in G$ such that $gv_1 = v_3$ and $gv_2 = v_4$ and thus g carries the pair (ℓ_1, ℓ_2) to the pair (ℓ_3, ℓ_4).
b) (i) $\implies$ (ii): This is an elementary calculation that we leave to the reader as an exercise.[4]
(ii) $\implies$ (iii) is immediate.
(iii) $\implies$ (i): We show the contrapositive: i.e., we assume $n > 1$ and show the action of G on lines in V is not 3-transitive. And we hope that the foregoing construction has made the reason for this clear: when $n > 1$, $\dim V \geq 3$, and there is an additional structure on triples of lines which is preserved by G: "generally" (at any rate, sometimes!) three lines will span a three-dimensional subspace, but there are some triples of lines which span a 2-dimensional subspace. Let's check that any two-dimensional vector space over a field K has at least three lines: indeed, the number of lines through the origin is $\#K + 1$ (the number of possible slopes, plus one for a vertical line), and since $\#K \geq 2$, this is indeed at least 3. □

The set of lines through the origin in V is of course the projective space $\mathbb{P}(V) = \mathbb{P}^n(K)$. Many of the above results can therefore be translated into results on projective spaces. First though let us note that the action of $\mathrm{GL}_{n+1}(K)$ on $\mathbb{P}^n(K)$ is no longer effective: there are nonidentity matrices which preserve every line through the origin. Indeed, the subgroup $\mathbb{G}_m$ of scalar matrices preserves every line, and it is easy to see that these are the only invertible matrices with this property (e.g. by

[4]As usual, I am interested in a proof with a clear moral and which avoids calculation. Let me know if you have one.

eigenspace considerations). As for any ineffective group action on a set, there is an induced effective action on the quotient by the kernel of the action; in this case

$$\mathrm{PGL}_{n+1}(K) = \mathrm{GL}_{n+1}(K)/\mathbb{G}_m$$

acts effectively on $\mathbb{P}^n(K)$.

Corollary 3.15. *Let K be a field, $n \geq 1$, and $G = \mathrm{PGL}_{n+1}(K)$.*
a) For any $0 \leq k \leq n$, G acts transitively on k-dimensional linear subvarieties of $\mathbb{P}^n(K)$.
b) The action of G on $\mathbb{P}^n(K)$ is 2-transitive. It is 3-transitive iff $n = 1$, in which case it is sharply 3-transitive.

Exercise 3.19: Let $x \neq y \in \mathbb{P}^1(K)$. By Corollary 3.15, there exists $g \in \mathrm{PGL}_2(K)$ such that $gx = y$ and $gy = x$. Show that any such g is an involution, i.e. $g^2 = 1$.

The property occurring in the previous exercise can be formulated in the context of general group actions: say a group action has the **interchange-involution** property if whenever $x \neq y$ are elements of X and $g \in G$ is such that $gx = y$ and $gy = x$, then g has order 2.

Exercise 3.20 (J. Lurie): Let G be a finite group acting on a finite set X. Suppose that the action is sharply 3-transitive and has the interchange-involution property. Then G is isomorphic as a permutation group to $\mathrm{PGL}_2(\mathbb{F}_q)$ for some finite field $\mathbb{F}_q$.

Consider the action of $\mathrm{PGL}_{n+1}(K)$ on all subsets of $\mathbb{P}^n(K)$. We say that two subsets S_1, S_2 of $\mathbb{P}^n(K)$ are **projectively equivalent** if there is $g \in \mathrm{PGL}_{n+1}(K)$ such that $gS_1 = S_2$.

Thus for example any two lines in $\mathbb{P}^2$ are projectively equivalent.

Note that $\mathrm{GL}_{n+1}(K)$ acts on the polynomial ring $K[T] = K[T_0, \ldots, T_n]$ and hence also on ideals of $K[T]$. It therefore makes sense to say that two projective subvarieties of $\mathbb{P}^n(K)$ are projectively equivalent if their associated homogeneous ideals are projectively equivalent.

The basic idea of projective equivalence is to take advantage of the large symmetry group of projective spaces to put varieties and equations in a canonical form.

Example: Any two three element subsets of $\mathbb{P}^1(K)$ are projectively equivalent; equivalently, every three element subset of $\mathbb{P}^1(K)$ is projectively equivalent to $\{0, 1, \infty\}$. Given a subset of $N > 3$ points in $\mathbb{P}^1(K)$, it is usually a good idea to apply an automorphism of projective space to take the first three points to $0, 1, \infty$: the remaining $N - 3$ points represent "free parameters". In fact, these considerations essentially show that the moduli space of N markes points on $\mathbb{P}^1$ is birational to $(\mathbb{P}^1)^{N-3}$. In particular, the moduli space of 4 marked points on $\mathbb{P}^1$ is birational to $\mathbb{P}^1$ itself. As we will see soon enough, we have essentially found the j-invariant of an elliptic curve via these elementary geometric considerations.

4. The Riemann-Roch Express

Let $C_{/K}$ be a nice curve. A **prime divisor** on C is a closed point. Since every closed point lies in an affine open subset, it suffices to consider the case of an affine

open subset C° of C, with corresponding coordinate ring $K[C^\circ]$. Now a closed point of C° corresponds to a maximal ideal $\mathfrak{m}$ of $K[C^\circ]$. By Zariski's Lemma, the residue field $K[C^\circ]/\mathfrak{m}$ is a finite degree field extension of K, and this degree is by definition the **degree** of the closed point.

A closed point with residue field L gives rise to a point $P \in C(L)$, so in particular $P \in C(\overline{K})$. If $L = K$ then this correspondence is a bijection. In general though the same maximal ideal can induce multiple $\overline{K}$-valued points. Let's try an example: $K = \mathbb{R}$, $C = \mathbb{P}^1$, $C^\circ = \mathbb{A}^1$, and we take the maximal ideal $\mathfrak{m} = (t^2 + 1)$. Then the residue field is $\mathbb{C}$, and the maximal ideal $\mathfrak{m}$ corresponds to the 2 $\mathbb{C}$-valued points i and $-i$. A relatively down-to-earth way to see this is to consider the factorization of $\mathfrak{m}$ in the unramified extension of Dedekind domains $K[C^\circ] \hookrightarrow L[C^\circ]$.

Theorem 4.1. *Let C be a nice curve over a field K. Then closed points on C are naturally in bijection with $G_K = \mathrm{Aut}(K^{\mathrm{sep}}/K)$-orbits of $C(K^{\mathrm{sep}})$.*

For a curve C, the **divisor group** $\mathrm{Div}\, C$ is the free abelian group on the set of prime divisors of C: thus an element of $\mathrm{Div}\, C$ is a finite formal $\mathbb{Z}$-linear combination of closed points of C. We define the degree of a divisor $\sum n_i \mathfrak{m}_i$ as $\sum n_i \deg \mathfrak{m}_i$. This gives a homomorphism

$$\deg : \mathrm{Div}\, C \to \mathbb{Z}.$$

Lemma 4.2. *Let $C_{/K}$ be a nice curve.*
a) Let L/K be an algebraic field extension. Then there is a natural injection

$$\iota : \mathrm{Div}(C) \to \mathrm{Div}(C_{/L})$$

which preserves degrees.
b) If L/K is Galois, then

$$\iota(\mathrm{Div}\, C) = \mathrm{Div}(C_{/L})^{\mathrm{Aut}(L/K)}.$$

In particular, if K is a perfect field, this gives a description of $\mathrm{Div}\, C$ as the Galois-invariant divisors over the algebraic closure. Note that this description of $\mathrm{Div}\, C$ via Galois descent is Silverman's *definition*.

Suppose that C has a K-rational point: e.g. if K is algebraically closed or C is an elliptic curve. Then the corresponding prime divisor has degree one, and thus the degree map is surjective. The converse need not hold: for instance it is known if K is finite, there is necessarily a divisor of degree 1 but not necessarily a K-rational point. In general we define the **index** $I(C)$ of C to be the least positive degree of a divisor on C; thus

$$\deg(\mathrm{Div}\, C) = I(C)\mathbb{Z}.$$

By definition, $\mathrm{Div}^0 C$ is the kernel of the degree map, whence a short exact sequence

$$0 \to \mathrm{Div}^0 C \to \mathrm{Div}\, C \to I(C)\mathbb{Z} \to 0.$$

Let $f \in K(C)^\bullet$ be a nonzero rational function on f. Then we may associate a divisor: roughly, as $\mathrm{div}\, f = f^{-1}(0) - f^{-1}(\infty)$, but with each quantity counted with suitable multiplicities. A precise definition can be given using the fact that since C is nonsingular, the local ring at any closed point P is a DVR, and then we define the local multiplicity of $f^{-1}(0)$ at P as $\mathrm{ord}_P(f)$. To define $f^{-1}(\infty)$ we can use the fact that $f(P) = 0 \iff \frac{1}{f}(P) = \infty$. Note that for any $\alpha \in K^\times$ we have $\mathrm{div}\, f = \mathrm{div}\, \alpha f$.

Lemma 4.3. *For any $f \in K(C)^\times$, we have* $\deg \operatorname{div} f = 0$.

Proof. This comes down to the fact that if $\mathfrak{m}$ is a maximal ideal in a Dedekind domain R with fraction field K, L/K is a finite field extension and S is the integral closure of R in L, then the factorization of $\mathfrak{m}S$ satisfies the basic equation

$$\sum_{i=1}^{g} e_i f_i = [L : K].$$

In particular the sum is independent of $\mathfrak{m}$. □

Lemma 4.4. *For $f \in K(C)^\times$, we have* $\operatorname{div} f = 0 \iff f \in K^\times$.

Proof. Exercise. □

This gives us short exact sequences

$$1 \to K(C)^\times / K^\times \to \operatorname{Div} C \to \operatorname{Pic} C \to 1,$$

i.e., we define $\operatorname{Pic} C$ as the quotient.

4.1. **Riemann-Roch Spaces.**

Let $C_{/K}$ be a nice curve, and let $D \in \operatorname{Div} C$. We define

$$\mathcal{L}(D) = \{f \in K(C)^\times \mid \operatorname{div} f \geq -D\} \cup \{0\}.$$

Proposition 4.5. *Let $C_{/K}$ be a nice curve, and let $D, D' \in \operatorname{Div} C$.*
a) The set $\mathcal{L}(D)$ is a K-subspace of $K(C)$.
b) If $D \sim D'$, then $\mathcal{L}(D) \cong \mathcal{L}(D')$.

For $D \in \operatorname{Div} C$, put

$$\ell(D) = \dim_K \mathcal{L}(D).$$

Proposition 4.6. *Let $D \in \operatorname{Div} C$. We may naturally identify the projectivization $\mathbb{P}\mathcal{L}(D)$ with the set of all* effective *divisors D' which are linearly equivalent to D.*

Exercise: Prove it.

Exercise: Let $D \in \operatorname{Div} C$.
a) Show that if $\ell(D) > 0$, then D is linearly equivalent to an effective divisor.
b) Deduce that if $\deg D < 0$, then $\ell(D) = 0$.
c) Suppose $\deg D = 0$. Show that the following are equivalent:
(i) $\ell(D) = 1$.
(ii) $\ell(D) > 0$.
(iii) $D \sim 0$.

Proposition 4.7. *Let $D \in DivC$, and suppose* $\deg D = d \geq 0$. *Then*

$$\ell(D) \leq \deg D + 1.$$

Proof. Step 0: Let $\iota : \operatorname{Div} C \to \operatorname{Div}(C_{/\overline{K}})$. It is easy to see that the natural map $\mathcal{L}(D) \otimes_K \overline{K} \to \mathcal{L}(\iota(D))$ is an injection (hint: use the fact that the natural map $K(C) \otimes_K \overline{K} \to \overline{K}(C)$ is, almost by definition, an isomorphism), hence $\ell(D) \leq \ell(\iota(D))$. Since $\deg \iota(D) = \deg D$, it is enough to prove this result under the assumption that K is algebraically closed. This simplifies matters – prime divisors now have degree 1. Further, we may assume that D is effective, say $\sum_{i=1}^{d} [P_i]$

(why?).
Step 1: We go by induction on d. The base case, $d = 0$, was handled above.
Step 2: Suppose $d \geq 0$, the result holds for all divisors of degree d, and let $D = D' + [P]$, with D' a divisor of degree d. Let n be the multiplicity of P in D'. We may assume there is $f \in \mathcal{L}(D) \setminus \mathcal{L}(D')$, otherwise there is nothing to show. To show then that $\dim \mathcal{L}(D) = \dim \mathcal{L}(D') + 1$, it suffices to show: for all $g \in \mathcal{L}(D) \setminus \mathcal{L}(D')$, there is $\alpha \in K^\times$ such that $f - \alpha g \in \mathcal{L}(D')$.

To show this, let $t \in K(C)$ be a uniformizing element at P, so $\ord_P(f) = \ord_P(g) = -(n+1)$. Thus $\ord_P(t^{n+1}f) = \ord_P(t^{n+1}g) = 0$, so the functions $t^{n+1}f$ and $t^{n+1}g$ are defined and nonzero at P: say their values are α_1 and α_2. Then $t^{n+1}(f - \frac{\alpha_1}{\alpha_2}g)$ vanishes at P, so $\ord_P(f - \alpha g) \geq -n$ and thus $f - \alpha g \in \mathcal{L}(D')$. □

Let us consider the case of $C = \mathbb{P}^1$. This is almost trivial – but enlightening. First we claim that $\Pic^0 \mathbb{P}^1$ is the trivial group, or, in other words, that every degree zero divisor on $\mathbb{P}^1$ is the divisor of a rational function. Let $D = D_+ - D_0$ be a degree zero divisor written as the difference of two effective divisors of equal degree d. (The case $d = 0$ is trivial, so we may assume $d \geq 1$.) Then D_+ and D_- are very close to corresponding to monic polynomials; the only issue here is the point at ∞ on $\mathbb{P}^1$, i.e., the unique point which does not lie in the standard affine coordinate chart. But no problem: the rational function t has divisor $(0) - (\infty)$, so by multiplying D by $\div t^a$ for a suitable $a \in \mathbb{Z}$, we ensure that D_+ and D_0 are sums of finite closed points (and, of course, modifying our divisor by the divisor of a rational function does not disturb the desired conclusion that D is itself the divisor of a rational function). But then it is clear that D_+ and D_- each correspond to (monic, say) degree d polynomials $f, g \in K[t]$, and thus $D = \div(f/g)$.

Since $\ell(D)$ depends only on the linear equivalence class of D and on $\mathbb{P}^1$ there is a unique linear equivalence class of divisors of any given degree d, to compute $\ell(D)$ in all cases it suffices to compute, say $\ell(d[\infty])$ for all $d \in \mathbb{N}$. And this is a trivial computation: the space of rational functions regular away from $[\infty]$ and with a pole of order at most d at ∞ is precisely the space of polynomials of degree at most d, of dimension $d + 1$. We deduce:

Proposition 4.8. *For any divisor D of non-negative degree on $\mathbb{P}^1$,*

$$\ell(D) = \deg D + 1.$$

4.2. **The Riemann-Roch Theorem.**

Theorem 4.9. *(Riemann-Roch) Let $C_{/K}$ be a nice curve. Then there is $\mathcal{K} \in \Div C$ and $g \in \mathbb{N}$ such that for all $D \in \Div C$,*

$$\ell(D) - \ell(\mathcal{K} - D) = \deg D - g + 1. \tag{5}$$

It is not our place to prove the Riemann-Roch Theorem here, although we mention that there is a nice proof using what are essentially Geometry of Numbers methods. Let us however deduce some important consequences.

- Taking $D = 0$ gives a relation between the mysterious quantities $\mathcal{K}$ and g:

$$\ell(\mathcal{K}) = g.$$

- Taking $D = K$ gives a further relation:

$$\deg K = 2g - 2.$$

Proposition 4.10. *Let $C_{/K}$ be a nice curve.*
a) There is a unique *natural number g such that (5) holds for all $D \in \operatorname{Div} C$, called the* ***genus of C****.*
b) There is a unique *divisor class $[\mathcal{K}]$ such that (5) holds for all $D \in \operatorname{Div} C$ – in other words, if (5) holds for a divisor $\mathcal{K}'$ in place of $\mathcal{K}$, then necessarily $\mathcal{K}' \sim \mathcal{K}$ – called the* ***canonical class of C****.*

Proof. a) For all D with $\deg D > \deg \mathcal{K}$, (5) reads

$$\ell(D) = \deg D - g + 1.$$

Clearly there can only be one natural number g for which this holds.[5]
b) Suppose that $\mathcal{K}' \in \operatorname{Div} C$ is another divisor such that for all $D \in \operatorname{Div} C$,

$$\ell(D) - \ell(\mathcal{K}' - D) = \deg D - g + 1.$$

Taking $D = \mathcal{K}'$ we find $\deg \mathcal{K}' = \deg \mathcal{K} = 2g - 2$. Taking $D = \mathcal{K}$, we find

$$\ell(\mathcal{K} - \mathcal{K}') = 1.$$

Since $\deg(\mathcal{K} - \mathcal{K}') = 0$, we findthat $\mathcal{K} \sim \mathcal{K}'$. □

4.3. **Descent for Riemann-Roch Spaces.**

Theorem 4.11. *(Descent for Riemann-Roch Spaces) Let $C_{/K}$ be a nice curve.*[6]*. Let $D \in \operatorname{Div} C$, let L/K be an algebraic field extension, and let $\iota_L(D)$ be the image of D in $\operatorname{Div}(C_{/L})$. Then*

$$\dim_K \mathcal{L}(D) = \dim_L \mathcal{L}(\iota_L(D)).$$

Proof. See [AEC, Ch. II] for a proof in the case where K is perfect... □

Corollary 4.12. *Let $C_{/K}$ be a nice curve, and let L/K be an algebraic field extension. Then $g(C) = g(C_{/L})$.*

Exercise: Prove it.

4.4. **Some Applications of Riemann-Roch.**

Proposition 4.13. *Let $C_{/K}$ be a nice curve.*
a) If $C \cong \mathbb{P}^1$, then the genus of C is zero.
b) If the genus of C is zero and C has a K-rational point P, then $C \cong \mathbb{P}^1$.

Proof. a) Earlier we saw that for all divisors D of non-negative degree on $\mathbb{P}^1$, $\ell(D) = \deg D + 1$. Comparing with Riemann-Roch we see that $g = 0$.
b) Applying Riemann-Roch to $D = [P]$, we find that there is a rational function $f \in K(C)$ with $\operatorname{div} f = [Q] - [P]$. Thus f gives a degree one map from the smooth curve C to the smooth curve $\mathbb{P}^1$, so f is an isomorphism. □

Proposition 4.14. *For a nice curve $C_{/K}$, the following are equivalent:*
(i) The zero divisor represents the canonical class $\mathcal{K}$.
(ii) $g(C) = 1$.

Proof. (i) $\implies$ (ii): Since $\deg \mathcal{K} = 2g - 2$, this is immediate.
(ii) $\implies$ (i): If $g = 1$, then $\deg \mathcal{K} = 2g - 2 = 0$, and $\ell(\mathcal{K}) = 1$, so $\mathcal{K} \sim 0$. □

[5]As an aside, what Riemann himself knew was that $\ell(D) \geq \deg D - g + 1$ for all D, with equality if $\deg D > \deg K$.

[6]Here, if K is not perfect, it is important that C be *geometrically regular* rather than merely regular

4.5. **The Genus of a Smooth Plane Curve.**

Theorem 4.15. *Let C be a smooth plane curve of degree d. Then*

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

We regard this as a basic algebraic geometric fact and do not give a proof here. However, [AEC, Exc. 2.7] suggests a method of proof using the **Riemann-Hurwitz formula**. We recommend this as an exercise for the interested reader.

Here are three important cases:
• ($d = 1$): A line in $\mathbb{P}^2$ has genus zero. In fact, it is clear that a line in $\mathbb{P}^2$ is isomorphic to $\mathbb{P}^1$ and therefore has genus zero, so we certainly did not need Theorem 4.15 for this.

• ($d = 2$): A smooth conic in $\mathbb{P}^2$ has genus zero. Note that we've already seen that a smooth plane conic is isomorphic to $\mathbb{P}^1$ iff it has a K-rational point, but also that over ground fields K of arithmetic interest (e.g. $\mathbb{R}$, $\mathbb{Q}_p$, $\mathbb{Q}$) there are smooth conics without K-rational points. Here we could avoid the appeal to Theorem **??** by extending the ground field and applying Corollary 4.12. This special case of the latter result is an easy one *except* when K has characteristic 2, and then there is some content to it.

• ($d = 3$): A smooth cubic in $\mathbb{P}^2$ has genus one. This is the case of most interest to us! Shortly we will attempt to prove a *converse* to this.

• ($d = 4$): A smooth quartic in $\mathbb{P}^2$ has genus three.

Note that the case of genus two curves is skipped over here: it is not possible to smoothly embed a genus two curve in the projective plane. (Indeed, the formula shows that for most positive integers g, this is not possible: the ones of the form $\frac{(d-1)(d-2)}{2}$ are obviously in the minority!)

Exercise: Let K be a field and $g \in \mathbb{N}$. Show that there is a nice curve $C_{/K}$ of genus g.

Harder Exercise: Let K be a field and $g \geq 3$. Show that there is a nice, *non-hyperelliptic* curve $C_{/K}$ of genus g.

4.6. **Mappings into Projective Space.**

We have now studied the Riemann-Roch space $\mathcal{L}(D)$ of a divisor in some detail. It was certainly interesting, and we made some connections to interesting issues in the geometry of curves, but we have yet to give an overarching point: what is so important about these Riemann-Roch spaces that we want a big theorem to (almost) compute their dimensions?

Let D be an effective divisor, so $\ell(D) > 0$. We will obtain a map of curves from C to $\mathbb{P}\mathcal{L}(D)$. Namely, let $f_0, \ldots, f_N$ be a K-basis for $\mathcal{L}(D)$. We define the map

$\varphi_D : C \to \mathbb{P}^N$ as

$$P \mapsto [f_0(P) : \cdots f_N(P)].$$

Some comments are in order. First, we made a choice in order to define φ_D: how does the map φ_D depend on this choice? In a very simple way: if we chose a different basis of $K(D)$, then there is a matrix $m \in \mathrm{GL}_{N+1}(K)$ carrying us from one to the other, and a moment's thought shows that the new map φ_D is just the image of the old map φ_D under the linear change of variables m acting on $\mathbb{P}^N$. In summary, the map φ_D is well-defined *up to projective equivalence*.

We do need to check that this gives a well-defined map. First, we will not get a well-defined point of projective space if $f_0(P) = \ldots = f_n(P) = 1$, but since the rational function 1 lies in $\mathcal{L}(D)$, this will never occur. The next thing to worry about is what happens if $f_i(P) = \infty$ for some i. In this case we choose an inde j such that $\mathrm{ord}_P(f_j)$ is minimal and divide all the coordinates by $f_j(P)$ to get an equivalent point in projective space with finite coordinates. (This same argument shows that *every* rational map from a smooth curve to projective space extends uniquely to a morphism.)

The map φ_D need not be an embedding: for instance, if $g(C) > 0$ and $N = 1$, it cannot possibly be. One says that D is **very ample** if φ_D embeds C into $\mathbb{P}^N$. Wasn't that helpful? No, it wasn't. But the following result is.

Theorem 4.16. *Let D be a divisor on a nice curve C of genus g. If $\deg D \geq 2g+1$, then D is very ample, i.e., $\varphi_D : C \to \mathbb{P}^N$ is an embedding.*

Further, we from the embedding φ_D we can recover the set of effective divisors D' linearly equivalent to D (and, in so doing, gain key insight into the meaning of the term "linearly equivalent"): namely, for each hyperplane $H \in \mathbb{P}^N$, if we intersect $\varphi_D(C)$ with H then we get a divisor on C of degree $d = \deg D$. This divisor is, in fact, linearly equivalent to D. (If we choose our basis in a careful way, we may arrange for the hyperplane at infinity $X_N = 0$ to cut out the given divisor D: think about this!) Conversely, as we vary H through all hyperplanes in $\mathbb{P}^N$, the divisors we cut out are precisely the full set of effective divisors $D' \sim D$.

There is a more precise "dual" description of this map into projective space which is often useful: without choosing any bases, there is a map

$$\Phi_D : C \to \mathbb{P}(\mathcal{L}(D)^\vee),$$

i.e., into the projectivization of the dual space of $\mathcal{L}(D)$. Roughly speaking this is obtained by viewing $P \in C(K)$ as a linear form on the Riemann-Roch space: $P \cdot f \mapsto f(P)$ (and similarly for $P \in C(L)$ with L/K any algebraic field extension). Unfortunately this doesn't quite make sense because for some choices of P and f we will have $f(P) = \infty$. This difficulty comes from the fact that our definition of $\mathcal{L}(D)$ is slightly too naive: it should "really" be the space of global sections of the line bundle associated to D. We got around this difficulty above by considering only a basis for $\mathcal{L}(D)$; here we can (inelegantly!) solve this by also choosing a basis and making the same extension argument. In fact, we claim that if $I : \mathbb{P}^{\ell(D)-1} \to \mathbb{P}(\mathcal{L}(D)^\vee)$ is the isomorphism induced by the dual basis $f_0^\vee, \ldots, f_{\ell(D)-1}^\vee$, we have

$$\Phi_D = I \circ \varphi_D.$$

Since $\mathbb{P}(V^{\vee\vee}) = \mathbb{P}(V)$, we may view elements of $\mathbb{P}(\mathcal{L}(D))$ as hyperplanes in $\mathbb{P}^{\ell(D)-1}$; if we choose $f_{\ell(D)-1} = 1$, then the divisor D itself corresponds to the hyperplane at ∞, i.e., to setting the last projective coordinate equal to 0.

Now we see why the Riemann-Roch Theorem is useful: if we have a very ample divisor on a curve C, then we get an embedding of C into some projective space? But which one? Here $N = \ell(D) - 1$, so the Riemann-Roch gives in particular the following result.

Theorem 4.17. *Let $D \in \operatorname{Div} C$ with $\deg D = d \geq 2g + 1$.*
a) Then $\varphi_D : C \hookrightarrow \mathbb{P}^{d-g+1}$ is an embedding.
b) In particular, let D be a divisor of degree $d \geq 3$ on a genus one curve. Then

$$\varphi_D : C \hookrightarrow \mathbb{P}^d.$$

Applying this Theorem in various special cases proves to be extremely enlightening.

Example: $g = 0$. Every divisor D of degree $d > 0$ is very ample, and Riemann-Roch gives an embedding $\varphi_C : C \to \mathbb{P}^d$. In particular:

1) Suppose that $\deg D = 1$. By Riemann-Roch, every divisor of positive degree on C is linearly equivalent to an effective divisor, so the assumption that C admits a degree one divisor is equivalent to the assumption that it admits a K-rational point, which is equivalent to assuming that it is isomorphic to $\mathbb{P}^1$. In this case φ_C is an isomorphism.

2) We claim that C always admits a divisor of degree 2: indeed, a canonical divisor has degree -2, so its negative is a divisor of degree 2, say D, which, up to linear equivalence, we may assume to be effective. Then $\varphi_D : C \to \mathbb{P}^2$ embeds C as a curve with the property that every hyerplane (here, every line!) intersects C to give an effective divisor of degree 2. Thus $\varphi_D(C)$ is a conic.

3) If $C \cong \mathbb{P}^1$ and $\deg D = d$, then the map $\mathbb{P}^1 \to \mathbb{P}^d$ is a very classical one in algebraic geometry, obtained by assembling all monomials of degree d. This is called the **Veronese embedding** (or, in the strangely inelegant terminology of [H], the "d-uple embedding").

(4) When C is a genus zero curve without a rational point, by the above arguments we have divisors of every even degree $d = 2k \geq 0$, and the corresponding maps to $\mathbb{P}^{2k}$ are "K-forms" of the Veronese embedding, meaning that as soon as we extend the base so as to put a rational point on C, the map becomes the Veronese embedding. It seems interesting to attempt to give a more concrete description, but now is not the time or place.)

Example ($g \geq 2$): In this case we may choose an effective canonical divisor $\mathcal{K}$ of degree $2g-2 > 0$. We therefore get a **canonical map** $\varphi : C \to \mathbb{P}^{g-1}$. The major dichotomy here is whether φ is an embedding or not: notice that its degree is too small for this to be automatic from Theorem 4.17.

Suppose $g = 2$, so $\deg \mathcal{K} = 2$. Then we have a map from a curve of positive genus to $\mathbb{P}^1$: this is clearly not an embedding. Because the preimage of a hyperplane (i.e.,

a point!) in $\mathbb{P}^1$ is an effective degree 2 divisor, the map φ is in fact a rational function of degree 2. A Riemann-Hurwitz calculation shows that it has $2g + 2 = 6$ branch points.

If we *must* embed C into projective space, no problem: take $D = 2\mathcal{K}$ instead. This gives a degree 4 embedding of C into $\mathbb{P}^3$.

Suppose $g > 2$. There is at least one curve $C_{/K}$ for which φ is not an embedding: it turns out (less obviously than above) that φ must then be $2:1$ onto its image, which is again isomorphic to $\mathbb{P}^1$. Such curves are said to be **hyperelliptic**.

Further, there is always at least one curve $C_{/K}$ for which the canonical map $\varphi : C \to \mathbb{P}^{g-1}$ *is* an embedding: such curves are called **canonical** (and are in a geometric sense the generic case among curves of genus $g \geq 3$). For instance, if $g = 3$, then the canonical map embeds C into $\mathbb{P}^2$ as a plane quartic, a situation which we've seen before. For a canonical curve of genus 4, φ is a degree 6 map of C into $\mathbb{P}^4$ whose image is the complete intersection of a degree 2 hypersurface and a degree 3 hypersurface. Describing the image of the canonical embedding of a canonical curve of degree g swiftly gets more complicated as g increases. In fact, one soon sees that it is the hyperelliptic curves which are more concrete and easier to understand geometrically!

As an aside: On any curve we have a canonically given divisor...the canonical divisor, of degree $2g - 2$. If $g = 0$, then $-\mathcal{K}$ is a divisor of degree 2, so $I(C) \mid 2$. If $g \geq 2$, then $I(C) \mid 2g - 2$. However, if $g = 1$, then $\mathcal{K}$ is trivial, so we get no help in embedding C into projective space and no *a priori* bound on $I(C)$.

Theorem 4.18. *(Clark, 11/2/04) For any number field K and any $I \in \mathbb{Z}^+$, there is a nice genus one curve $C_{/K}$ with $I(C) = I$.*

Suppose $g = 1$ and C admits a divisor D of degree 1. Then by Riemann-Roch, $\ell(D) = 1$, so D is linearly equivalent to an effective divisor, so without loss of generality $D = [P]$ for a K-rational point P. However, because $\ell(D) = 1$, the corresponding map φ_D is to $\mathbb{P}^0$: nothing to see here!

Suppose $g = 1$ and C admits a divisor D of degree 2. By Riemann-Roch $\ell(D) = 2$, so we get a degree 2 map $\varphi_D : C \to PP^1$. Let us suppose that $\operatorname{char} K \neq 2$. Then since $K(C)/K(t)$ is a quadratic extension, $K(C) = K(t, f(t))$, where we may take $f(t) \in K[t]$ a polynomial. The ramification points of φ_D correspond to the roots of f in $\overline{K}$; a Riemann-Hurwitz calculation shows that there are four roots, thus we get an equation $y^2 = P_4(x)$, and C is a hyperelliptic quartic curve. If one of the ramification points is rational, then we can move it to ∞ on $\mathbb{P}^1$ and get a Weierstrass cubic $y^2 = P_3(x)$. But in general we may not have any K-rational points at all.

Suppose $g = 1$ and C admits a divisor D of degree 3. By Riemann-Roch $\ell(D) = 3$ and $\deg D = 2g + 1$, so $\varphi_D : C \to \mathbb{P}^2$ is a degree 3 embedding, i.e., its image is a plane cubic curve.

Suppose $g = 1$ and C admits a divisor D of degree 4. By Riemann-Roch we get a degree 4 embedding $C \to \mathbb{P}^3$. If this happens to be a complete intersection, then it must be a complete intersection of two quadrics. It turns out that this is

the case, but this involves some further geometric argumentation (Exercise!).

Suppose $g = 1$ and C admits a divisor D of degree $d \geq 5$. By Riemann-Roch we get a degree d embedding $C \to \mathbb{P}^{d-1}$. It turns out that this embedding is *not a complete intersection*, but rather can be given as an excess intersection of $\frac{d(d-3)}{2}$ quadric hypersurfaces. (Exercise!) When $d = 5$ this can still be described somewhat nicely and classically in turns of **Pfaffians** (Exercise!). Starting in degree 6 so far as I know working with explicit equations begins to get out of hand.

5. Weierstrass Cubics

Let $C : F(X, Y, Z) = 0$ be a plane cubic curve defined over a field K. We will always assume that C is geometrically irreducible: i.e. F does not factor over $\overline{K}$.

A **Weierstrass cubic** over a field K is a plane cubic of the special form

$$C : \alpha Y^2Z + a_1XYZ + a_3YZ^2 = \beta X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 = 0, \tag{6}$$

with $\alpha\beta \in K^\times$, $a_1, a_2, a_3, a_4, a_6 \in K$.

Lemma 5.1. *A Weierstrass cubic is geometrically irreducible.*

Exercise: Prove it.

Proposition 5.2. *a) Let C be a Weierstrass cubic. Then $O = [0 : 1 : 0]$ is a K-rational flex point, with K-rational flex line $Z = 0$.*
b) Let C be an geometrically irreducible plane cubic for which $O = [0 : 1 : 0]$ is a K-rational flex point, with K-rational flex line $Z = 0$. Then C is a Weierstrass cubic.

Proof. a) In other words, if we plug $Z = 0$ into a Weierstrass equation, we get the unique solution $O = [0 : 1 : 0]$: this is clear.
b) Observe that the homogeneous cubic polynomials $f(x, y, z)$ form a 10-dimensional K-vector space. The condition that a given K-rational point, say O, be a flex point is a linear condition which cuts down the dimension of the space by 2, and the condition that the flex line be any given line cuts down the dimension by 1, leaving us with a 7-dimensional linear space. Let us say for the moment that a **generalized Weierstrass cubic** is a plane cubic of the form 6 but without the condition $\alpha\beta \neq 0$. Then the generalized Weierstrass cubics form a 7-dimensional linear space of cubics every element of which has O as a flex pointa and $Z = 0$ as a flex line, so is therefore the most general plane cubic with these properties. We leave it to the reader to show that the condition $\alpha\beta \neq 0$ is equivalent to geometric irreducibility. □

Lemma 5.3. *A Weierstrass cubic $C_{/K}$ is projectively equivalent to a Weierstrass cubic in* ***long Weierstrass form***

$$C : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 = 0. \tag{7}$$

Exercise 3.21: Suppose $\operatorname{char} K \neq 2$. Then via an affine equivalence, we may transform the Weierstrass cubic to a Weierstrass cubic with $a_1 = a_3 = 0$.

Exercise 3.22: Suppose $\operatorname{char} K \neq 2, 3$. Then via an affine equivalence, we may transform the Weierstrass cubic to **short Weierstrass form**:

$$Y^2Z = X^3 + AXZ^2 + BZ^3, \tag{8}$$

with $A, B \in K$. Further, suppose that K is the fraction field of a domain R. Show that the affine equivalence may be chosen so as to have $A, B \in R$.

In particular this makes contact between our concrete definition of an elliptic curve and the ultra-naive definition of an elliptic curve $E_{/\mathbb{Q}}$ as being given by an equation $y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}$.

Proposition 5.4. *Let C be a Weierstrass cubic in long Weierstrass form. Define*

$$b_2 = a_1^2 + 4a_4,$$

$$b_4 = 2a_4 + a_1a_3,$$

$$b_6 = a_3^2 + 4a_6,$$

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,$$

$$\Delta(E) = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_8.$$

Then C is smooth iff $\Delta(E) \neq 0$.

Until further notice we consider only smooth Weierstrass cubics.

Theorem 5.5. *For a smooth plane cubic curve $C_{/K}$, the following are equivalent:*
(i) C is projectively equivalent to a Weierstrass cubic.
(ii) C has a K-rational flex point.
(iii) C has a K-rational flex line.

Proof. (i) $\implies$ (ii): This is immediate from Proposition 5.2.
...

Corollary 5.6. *Over an algebraically closed field, every plane cubic is projectively equivalent to a Weierstrass cubic.*

Exercise: Consider the plane cubic $F_3 : X^3 + Y^3 + Z^3 = 0$ over $\mathbb{Q}$.
a) Show that F_3 has three $\mathbb{Q}$-rational flex points.
b) Give an explicit Weierstrass cubic which is projectively equivalent to C.
c)* Show that there is a plane cubic $C_{/\mathbb{Q}}$ which is isomorphic to F_3 as an algebraic curve but which does not have any $\mathbb{Q}$-rational flex points.

Theorem 5.7. *(Nagell) Let C be a smooth plane cubic with a K-rational point O. Then C is isomorphic to a Weierstrass cubic.*

Proof. See [LEC, pp. 34-35]. □

Exercise:
a) Write a computer program which takes as input a nonsingular plane cubic endowed with a K-rational point and outputs an isomorphic Weierstrass cubic.
b) Does a computer program implementing part a) already exist? If so, find one.

5.1. **Singular Weierstrass Cubics.** Exercise: Let C be a cubic curve over an arbitrary field K, let ℓ be a K-rational flex line, and let $P \in C(\overline{K})$ be the unique intersection point of ℓ with P.
a) Suppose that K is perfect. Show that $P \in C(K)$.
b) Suppose that P is *not* K-rational. Show that K is not perfect and has characteristic 3.
c) Find an example where P is not K-rational.

Exercise: By an affine equivalence – which we mean a projective equivalence fixing the line $Z = 0$ – we may transform the Weierstrass cubic (7) to a Weierstrass cubic with $\alpha = \beta = 1$.

Remark: It turns out that the two parameters in the short Weierstrass form cannot be improved upon over a general ground field. Even to state this result precisely requires some algebraic-geometric sophistication. The following is just for culture: there is no one-dimensional variety $X_{/\mathbb{Q}}$, surface $\mathcal{E}_{/\mathbb{Q}}$ and morphism $f : \mathcal{E} \to X$ with the following property: for every field K of characteristic 0 and every plane cubic curve $C_{/K}$, there is $P \in X(K)$ such that the fiber f_P is isomorphic to C.

5.2. **Covariants of Weierstrass Cubics.**

Let $E = (E, P)$ be an elliptic curve over a field K. As we discussed, the map

$$\varphi_{3[P]} : E \hookrightarrow \mathbb{P}(\mathcal{L}(3[P])^\vee)$$

is an embedding into two-dimensional projective space carrying carrying P to a flex point. This is a nice coordinate-free description. In this section we pursue a more classical, coordinate-full description, which is also useful.

(Insert classical derivation of Weierstrass equation here.)

Now let $(1, x, y)$ and $(1, x', y')$ be two sets of Weierstrass coordinates on E: i.e., both x and x' are degree two rational functions with a single, double pole at O and both y and y' are degree three rational functions with a single, triple pole at 0; and we have arranged for $y^2 = x^3 + O(5)$ and $y'^2 = x'^3 + O(5)$. By pure linear algbra, there must be relations between x and x' and between y and y' of the following form:

$$x = u_1 x' + r,$$
$$y = u_2 y' + s_2 x' + t,$$

for $u_1, u_2 \in K^\times$ and $r, s_2, t \in K$. The relations between y^2 and x^3 and between y'^2 and x'^3 yield $u_1^3 = u_2^2$. We may eliminatea variable by taking

$$u = \frac{u_2}{u_1},\ s = \frac{s_2}{u^2}.$$

Thus we have proven:

Proposition 5.8. *Any two Weiertrass equations for an elliptic curve $E_{/K}$ are related by a change of variables of the following form:*

$$x = u^2 x' + r,$$
$$y = u^3 y' + s u^2 X' + t,$$

with $u \in K^\times$ and $r, s, t \in K$.

If $\operatorname{char} K \neq 2$, then completing the square in y

$$y \mapsto \frac{1}{2}(y - a_1 x - a_3)$$

yields an equation of the (simpler) form

$$y^2 = 4x^3 + b_2 x^2 + 2b_4 x + b_6,$$

where

$$b_2 = a_1^2 + 4a_2,$$
$$b_4 = 2a_4 + a_1 a_3,$$
$$b_6 = a_3^2 + 4a_6.$$

Let us also define

$$c_4 = b_2^2 - 24b_4,$$
$$c_6 = -b_2^3 + 36b_2 b4 - 316b_6,$$
$$\Delta = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6,$$
$$j = c_4^3/\Delta.$$

Note that all of the other quantities are defined for singular Weierstrass cubics, but j is defined precisely when the cubic is nonsingular.

Two relations between these quantities are

$$4b_8 = b_2 b_6 - b_4^2$$

and – more importantly! –

$$1728\Delta = c_4^3 - c_6^2,$$
$$j = \frac{1728 c_4^3}{c_4^3 - c_6^2}.$$

It is useful to record the effect on these quantities of making the most general linear change of variables preserving the Weierstrass form of the cubic equation. Here are some of the nicer formulas:

$$c_4 = u^4 c_4',$$
$$c_6 = u^6 c_6',$$
$$\Delta = u^{12}\Delta',$$
$$j = j'.$$

When $\operatorname{char} K \neq 2, 3$, then the following substitution (directly inspired by the classical study of cubic equations)

$$(x, y) \mapsto \left(\frac{x - 3b_2}{36}, \frac{y}{108}\right)$$

further simplifies the equation, yielding

$$y^2 = x^3 - 27c_4 x - 54c_6.$$

An equation of this latter type is often called **short Weierstrass form**, and is certainly better suited to explicit calculations when it applies. Note that it is traditional to write short Weierstrass form as

$$y^2 = x^3 + Ax + B,$$

so let us record that

$$A = -27c_4,\ B = -54c_6$$

and thus

$$\Delta = -16(4A^3 + 27B^2),$$

$$j = -1728\frac{(4A)^3}{\Delta}.$$

Exercise: Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve in char. different from 2 and 3. Define the **Krumm invariant**

$$k = \frac{B^2}{4A^3 + 27B^2}.$$

a) Show that k is indeed an invariant of an elliptic curve: i.e., independent of the short Weierstrass form chosen.
b) Show that $k = \alpha\frac{c_6^2}{c_4^3 - c_6^2}$ for some constant α. Explain how a different choice of α leads to a definition of an invariant k valid in all characteristics.

Proposition 5.9. *Let K be a field, and let $j \in K$. Then there is an elliptic curve $E_{/K}$ with $j(E) = j$.*

Proof. Step 1: Suppose first that j is neither 0 nor 1728, and consider

$$E_j = y^2 + xy = x^3 - \frac{36}{j - 1728}x - \frac{1}{j - 1728}.$$

Since $j \neq 1728$, E_j is well-defined; moreover

$$\Delta(E_j) = \left(\frac{j}{j - 1728}\right)^3 \neq 0$$

and

$$j(E_j) = j.$$

Step 2: Consider

$$E_0 : y^2 + y = x^3,$$

with

$$\Delta(E_0) = -27,\ j(E_0) = 0,$$

and

$$E_{1728} : y^2 = x^3 + x,$$

with

$$\Delta(E_{1728}) = -64,\ j(E_{1728}) = 1728.$$

• If $\operatorname{char} K \notin \{2, 3\}$, then E_0 is an elliptic curve with j-invariant 0 and E_{1728} is an elliptic curve with j-invariant 1728.
• If $\operatorname{char} K = 2$, then E_0 is an elliptic curve with $j = 0 = 1728$.
• If $\operatorname{char} K = 3$, then E_{1728} is an elliptic curve with $j = 0 = 1728$. □

Exercise: State an prove an analogue for the (possibly rescaled) Krumm invariant.

Theorem 5.10. *For elliptic curves E_1, E_2 defined over a field K, TFAE:*
(i) $(E_1)_{\overline{K}} \cong (E_2)_{\overline{K}}$.
(ii) $j(E_1) = j(E_2)$.

Proof. (i) $\implies$ (ii): Observe that the j-invariant does not change upon base extension: $E_{/K}$ is an elliptic curve and L/K is any field extension, then then $j(E_{/L}) = j(E)$ (more precisely the right hand side is $\iota(j(E))$, where $\iota : K \hookrightarrow L$ is the embedding). This direction now follows immediately: since we know the j-invariant is an invariant, if $(E_1)_{/\overline{K}} \cong (E_2)_{/\overline{K}}$, then

$$j(E_1) = j((E_1)_{/\overline{K}}) = j((E_2)_{/\overline{K}}) = j(E_2).$$

(ii) $\implies$ (i): For simplicity we are going to assume $\operatorname{char} K \neq 2, 3$ and and, in particular, that E and E' can both be put in short Weierstrass form. So suppose we have:

$$E_1 : y^2 = x^3 + Ax + B,$$
$$E_2 : y^2 = x^3 + A'x + B'.$$

Then if $j(E_1) = j(E_2)$, we have

$$\frac{A^3}{4A^2 + 27B^2} = \frac{A'^3}{4A'^3 + 27B'^2}.$$

Clearing denominators and using $\operatorname{char} K \neq 3$ we get

$$A^3B'^2 = A'^3B^2.$$

I leave it to you to check the following:
- $j(E_1) \neq 0, 1728 \iff AB \neq 0$.
- $j(E_1) = 1728 \iff A \neq 0,\ B = 0$.
- $j(E_1) = 0 \iff A = 0,\ B \neq 0$.

Case 1: $j(E_1) \neq 0, 1728$. Then AB, $A'B' \neq 0$. Take

$$u = (\frac{A}{A'})^{\frac{1}{4}} = (\frac{B}{B'})^{\frac{1}{6}}.$$

Then making the change of variables

$$x = u^2X, y = u^3Y,$$

we get

$$y^2 = u^6Y^2 = x^3 + Ax + B = u^6X^3 + u^2AX + B,$$

or

$$Y^2 = X^3 + \frac{A}{u^4}X + \frac{B}{u^6} = X^2 + A'X + B'.$$

Case 2: $j(E_1) = 1728$. Take $u = (\frac{A}{A'})^{\frac{1}{4}}$.
Case 3: $j(E_2) = 0$. Take $u = (\frac{B}{B'})^{\frac{1}{6}}$. □

Exercise: Is there an analogue of Theorem XX from the Krumm invariant?

Let us look more closely at the proof of Theorem XX, first in the (generic) Case 1. Part of the point is that the change of variables

$$u = (\frac{A}{A'})^{\frac{1}{4}} = (\frac{B}{B'})^{\frac{1}{6}}$$

which linked two short Weierstrass cubics with the same j-invariant could not, in general, be performed over the ground field. However, it can manifestly be performed over a much smaller extension than $\overline{K}$! Indeed, the given conditons show that $u^4, u^6 \in K$ and thus $u^2 = \frac{u^6}{u^4} \in K$. Precisely, let

$$d = u^2 = (A/A')^{\frac{1}{2}} = (B/B')^{\frac{1}{3}} \in K.$$

Exercise: Let $E_{/K}$ be an elliptic curve over an algebraically closed field of characteristic different from 2 and 3.
a) Suppose $j(E) \notin \{0, 1728\}$. Show $\mathrm{Aut}(E) \cong \mathbb{Z}/2\mathbb{Z}$.
b) Suppose $j(E) = 1728$. Show $\mathrm{Aut}(E) \cong \mathbb{Z}/4\mathbb{Z}$.
c) Suppose $j(E) = 0$. Show $\mathrm{Aut}(E) \cong \mathbb{Z}/6\mathbb{Z}$.

Remark: Even if $\mathrm{char}\, K \in \{2, 3\}$, if $j(E) \notin \{0, 1728\}$, then $\mathrm{Aut}\, E \cong \mathbb{Z}/2\mathbb{Z}$. However in characteristic 3, if $j(E) = 0 = 1728$, then $\mathrm{Aut}\, E$ is a non-commutative group of order 12; in characteristic 2, if $j(E) = 0 = 1728$, then $\mathrm{Aut}\, E$ is a non-commutative group of order 24.

Exercise: Let K be a field of characteristic not 2 or 3. Let E_1, E_2 be elliptic curves over K with $j(E_1) = j(E_2)$.
a) Suppose $j(E_1) \notin \{0, 1728\}$. Show that E_2 is a quadratic twist of E_1.
b) Suppose $j(E_1) = 1728$.
(i) Show that E_1 and E_2 become isomorphic in some extension $K(d^{\frac{1}{4}})$.
(ii) Show that E_1 has a Weierstrass equation of the form

$$E_d : y^2 = x^3 + dx.$$

(iii) Show that $E_{d_1} \cong E_{d_2} \iff d_1/d_4 \in K^{\times 4}$.
c) Suppose $j(E_1) = 0$.
(i) Show that E_1 and E_2 become isomorphic in some extension $K(d^{\frac{1}{6}})$.
(ii) Show that E_1 has a Weierstrass equation of the form

$$E_d : y^2 = x^3 + d.$$

(iii) Show ....

Exercise: Let K be a field of characteristic not 2 or 3, and let $c \in K^\times$. Consider the plane cubic

$$E : X^3 + Y^3 + cZ^3 = 0.$$

a) Show that if we take $O = [1 : -1 : 0]$, then (E, O) is an elliptic curve.
b) Show that $E_{/\overline{K}}$ admits an automorphism of order 3.
c) Deduce $j(E) = 0$.
d) Show that E is isomorphic to a curve of the form

$$y^2 = x^3 + d_c,$$

and determine d_c in terms of c.

Interpret the previous exercises in terms of Galois Cohomology.
Hint: $H^1(K, \pm 1) \cong K^\times / K^{\times 2}$.

6. The ℓ-adic Tate module

Theorem 6.1. *Let K be a field and $E_{/K}$ be an elliptic curve. Let ℓ be a prime number with $\mathrm{char}\, K \nmid \ell$. There is a pairing $e : T_\ell(E) \times T_\ell(E) \to T_\ell(\mu)$ such that:*
(i) e is bilinear, alternating and nondegenereate.

(ii) e is G_K-equivariant.
(iii) If $\varphi : E_1 \to E_2$ is an isogeny, then φ and $\varphi^\vee$ are adjoints for e:

$$\forall S \in T_\ell E_1, T \in T_\ell E_2,\ e(\varphi S, T) = e(S, \varphi^\vee T).$$

Proof. See [AEC, §III.8]. □

Remark: It is a standard convention in arithmetic geometry that ℓ denotes a prime number which is different from the characteristic of the field over which one's varieties are being defined. Here, when we have an elliptic curve $E_{/K}$, it shall from now on be understood that ℓ means a prime different from $\operatorname{char} K$.

Lemma 6.2. *Let R be any commutative ring, and let $A \in M_2(R)$. Then*

$$\operatorname{tr} A = 1 + \det A - \det(1 - A).$$

Exercise: a) Prove Lemma 6.2.
b) What do you make of it? Is there a generalization to $k \times k$ matrices?[7]

Theorem 6.3. *Let $\varphi \in \operatorname{End} E$, and let $\varphi_\ell \in \operatorname{End} T_\ell E$ be the induced map. Then*

$$\det \varphi_\ell = \deg \varphi,$$

$$\operatorname{tr} \varphi_\ell = 1 + \deg \varphi - \deg(1 - \varphi).$$

In particular, the characteristic polynomial $\chi_\varphi(t)$ of φ_ℓ has coefficients in $\mathbb{Z}$ which are independent of the choice of $\ell \neq \operatorname{char} K$.

Proof. Let v_1, v_2 be a $\mathbb{Z}_\ell$-basis for $T_\ell E$, and write

$$\varphi_\ell(v_1) = av_1 + bv_2,$$

$$\varphi_\ell(v_2) = cv_1 + dv_2.$$

Thus the matrix of φ_ℓ relative to $\{v_1, v_2\}$ is

$$\varphi_\ell = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

Using 6.1, we compute

$$e(v_1, v_2)^{\deg \varphi} = e([\deg \varphi]v_1, v_2) = e(\varphi^\vee)_\ell \varphi_\ell v_1, v_2)$$

$$= e(\varphi_\ell v_1, \varphi_\ell v_2) = e(av_1 + bv_2, cv_1 + dv_2)$$

$$= e(v_1, v_2)^{ad-bc} = e(v_1, v_2)^{\det \varphi_\ell}.$$

Thus

$$e((\deg \varphi - \det \varphi_\ell)v_1, v_2) = 0,$$

and since the pairing is alternating it follows that

$$e((\deg \varphi - \det \varphi_\ell)v_1, T_\ell E) = 0;$$

by nondegneracy, we conclude $\det \varphi_\ell = \deg \varphi$. By Lemma 6.2, we have

$$\operatorname{tr} \varphi_\ell = 1 + \deg \varphi - \deg(1 - \varphi).$$

These are indeed integers which are independent of ℓ. □

[7]Neither of these are precise questions, of course.

7. Elliptic Curves Over Finite Fields

7.1. Hasse's Theorem.

Lemma 7.1. *Let K be a field of characteristic $p > 0$, let $q = p^a$. The isogeny $1 - \mathrm{Fr}_q$ is separable.*

The idea of the proof is the basic fact that a homomorphism of algebraic groups is a separable isogeny iff it induces an isomorphism on co/tangent spaces at the identity. For elliptic curves, the cotangent space at O may be identified with the vector space of **invariant differentials**. If you know about such things, it is easy to check that pulling back a differential by the identity gives the same differential, while pulling back by any Frobenius map gives the zero differential:

$$\mathrm{Frob}_q^* \frac{dx}{2y + a_1 x + a_3} = \frac{dx^q}{2y^q + a_1 x^q + a_3} = \frac{q x^{q-1} dx}{2y^q + a_1 x^q + a_3} = 0.$$

Lemma 7.2. *(Abstract Cauchy-Schwarz) Let R be an ordered ring, A an R-module, and $f : A \to R$ a non-negative quadratic form, with associated bilinear form*

$$\langle x, y \rangle = f(x + y) - f(x) - f(y).$$

Then for all $x, y \in A$,

$$\langle x, y \rangle^2 \leq 4 f(x) f(y).$$

Proof. If $x = 0$, then $\langle x, y \rangle^2 = 4 f(x) f(y) = 0$, and the result holds with equality. So assume $x \neq 0$. For $a, b \in R$, we have

$$0 \leq f(ax + by) = a^2 f(x) + ab \langle x, y \rangle + b^2 f(y).$$

Take

$$a = \langle x, y \rangle, \ b = -\langle x, x \rangle$$

to get

$$0 \leq \langle x, x \rangle \left(\langle x, x \rangle \langle y, y \rangle - \langle x, y \rangle^2 \right).$$

It follows that

$$\langle x, y \rangle^2 \leq \langle x, x \rangle \langle y, y \rangle = 4 f(x) f(y).$$

□

Theorem 7.3. *(Hasse) Let $E_{/\mathbb{F}_q}$ be an elliptic curve. Then*

$$|\#E(\mathbb{F}_q) - (q + 1)| \leq 2\sqrt{q}.$$

Proof. The map $\deg : \mathrm{End}\, E \to \mathbb{Z}$ is a positive quadratic form. We apply Lemma 7.2 to deg and the endomorphisms $x = 1$, $y = \mathrm{Frob}_q$:

$$|\deg(1 - \mathrm{Frob}_q) - \deg(1) - \deg(\mathrm{Frob}_q)| \leq 2\sqrt{\deg 1 \deg \mathrm{Frob}_q} = \sqrt{q}.$$

Further, since $1 - \mathrm{Frob}_q$ is separable, $\deg(1 - \mathrm{Frob}_q)$ is equal to the set of $P \in E(\overline{\mathbb{F}_q})$ such that $(1 - \mathrm{Frob}_q)(P) = 0$, i.e., such that $P = \mathrm{Frob}_q(P)$. This is precisely the set of $\mathbb{F}_q$-rational points on E, so

$$|\#E(\mathbb{F}_q) - (q + 1)| \leq 2\sqrt{q}.$$

□

Theorem 7.4. *(Hasse-Deuring-Waterhouse) Let $q = p^k$ be a prime power, let $a \in \mathbb{Z}$, and put $N = q+1-a$. Then there is an elliptic curve $E_{/\mathbb{F}_q}$ with $\#E(\mathbb{F}_q) = N$ iff* at least one of the following holds*:*
(i) $\gcd(a,p) = 1$.
(ii) n is even and $a = \pm 2\sqrt{q}$.
(iii) n is even, $p \not\equiv 1 \pmod 3$, and $a = \pm\sqrt{q}$,
(iv) n is odd, $p \in \{2,3\}$, and $a = \pm p^{\frac{n+1}{2}}$,
(v) n is even, $p \not\equiv 1 \pmod 4$, and $a = 0$,
(vi) n is odd and $a = 0$.

Theorem 7.5. *(Ruck) Let $E'_{/\mathbb{F}_q}$ be an elliptic curve and put $N = \#E'(\mathbb{F}_q)$. Write $N = p^e n_1 n_2$ with $p \nmid n_1 n_2$, $n_1 \mid n_2$. There is an elliptic curve $E_{/\mathbb{F}_q}$ such that*

$$E(\mathbb{F}_q) \cong \mathbb{Z}/p^e \oplus \mathbb{Z}/n_1 \oplus \mathbb{Z}/n_2$$

iff
a) $n_1 \mid q-1$ in cases (i),(iii), (iv), (v), (vi) above;
b) $n_1 = n_2$ in case (ii) above.

7.2. **The Endomorphism Ring.**

Recall that we showed that if K is any field of characteristic 0 and $E_{/K}$ is any elliptic curve, then $\mathrm{End}^0 E$ is either $\mathbb{Q}$ or an imaginary quadratic field.

First I want to touch up the structure on $\mathrm{End}^0(E)$ a bit.

Let's start with the fact that $x \in \mathrm{End}^0(E) \mapsto \deg x$ is a positive quadratic form such that for all $x, y \in \mathrm{End}^0(E)$, $\deg(xy) = \deg x \deg y$.

Let F be a field, not of characteristic 2. (For our application to elliptic curves, $F = \mathbb{Q}$ no matter what the ground field K is, so this is absolutely a safe assumption!) A unital but not necessarily associative F-algebra C endowed with a nondegenerate, multiplicative quadratic form n is called a **composition algebra**. I actually prefer the term **quadratic algebra**.

As usual, we define $\langle x, y\rangle = n(x+y) - n(x) - n(y)$. We also define the **trace**

$$t : C \to F,\ x \mapsto \langle x, 1\rangle.$$

We now deduce some identities valid in any composition algebra (C, N). Denoting the multiplicative identity of C by 1, we have that for all $x \in C$,

$$N(x) = N(1 \cdot x) = N(1)N(x).$$

Since N is nondegenerate, there exists $x \in X$ with $N(x) \neq 0$, whence

$$N(1) = 1$$

and the quadratic form N is **principal** (i.e., represents 1).

For all $x_1 x_2, y \in C$,

$$N(x_1y+x_2y) = N(x_1y)+N(x_2y)+\langle x_1y, x_2y\rangle = N(x_1)N(y)+N(x_2)N(y)+\langle x_1y, x_2y\rangle$$

and also

$$N(x_1y+x_2y) = N((x_1+x_2)y) = N(x_1+x_2)N(y) = \left(N(x_1) + N(x_2) + \langle x_1, x_2\rangle\right) N(y).$$

Comparing these gives

$$\langle x_1y, x_2y\rangle = \langle x_1, x_2\rangle N(y) \tag{9}$$

and similarly

$$\langle xy_1, xy_2\rangle = N(x)\langle y_1, y_2\rangle. \tag{10}$$

Notice that equation (9) is quadratic in y. Its linearized form is

$$\langle x_1y_1, x_2y_2\rangle + \langle x_1y_2, x_2y_1\rangle = \langle x_1, x_2\rangle\langle y_1, y_2\rangle. \tag{11}$$

Taking $x_1 = x$, $y_1 = y$, $x_2 = z$, $y_2 = 1$ in (11) gives

$$\langle xy, z\rangle + \langle x, zy\rangle = \langle x, z\rangle\langle y, 1\rangle = T(y)\langle x, z\rangle. \tag{12}$$

Taking $x_1 = y_2 = x$, $x_2 = y$, $y_2 = 1$ in (11) gives

$$\langle x, yx\rangle + \langle x^2, y\rangle = \langle x, y\rangle\langle 1, x\rangle = T(x)\langle x, y\rangle. \tag{13}$$

Taking $x_1 = x,\ y_1 = y$, $x_2 = y_2 = 1$ gives

$$\langle xy, 1\rangle + \langle x, y\rangle = \langle x, 1\rangle\langle y, 1\rangle. \tag{14}$$

Theorem 7.6. *Let (C, N) be a composition algebra and $x \in C$. Then*

$$x^2 - T(x)x + N(x)1 = 0. \tag{15}$$

Thus every element of C satisfies a quadratic equation over F.

Proof. Let $y \in C$ be arbitrary and form the inner product of LHS(15) with y:

$$\langle x^2, y\rangle - \langle x, 1\rangle\langle x, y\rangle + \langle 1, y\rangle N(x) = \langle x^2, y\rangle - \langle x, 1\rangle\langle x, y\rangle + \langle x, yx\rangle = 0.$$

Here the first equality is by (9) and the second is by (13). Since this holds for all $y \in C$ and the bilinear form is nondegenerate, this establishes (15). □

Theorem 7.7. *(Hurwitz Classification of Composition Algebras)*
Let $C_{/F}$ be a composition algebra. Then $\dim C \in \{1, 2, 4, 8\}$. *Moreover:*
a) If $\dim C = 1$, *then $C = F$. With respect to the basis* 1 *of C, the norm form is*

$$N(x) = x^2.$$

b) If $\dim C = 2$, *there exists $\alpha \in F^\times$ such that $C \cong \left(\frac{\alpha}{F}\right) = F[t]/(t^2 - \alpha)$. With respect to the basis $1, \alpha$ of C, the norm form is*

$$N = N(x_1, x_2) = x_1^2 - \alpha x_2^2.$$

c) If $\dim C = 4$, *there exist $\alpha, \beta \in F^\times$ such that C is isomorphic to the quaternion algebra $B(\alpha, \beta) = \left(\frac{\alpha,\beta}{F}\right)$. With respect to the standard quaternion basis e_1, e_2, e_3, e_4, the norm form is*

$$N(x_1, x_2, x_3, x_4) = x_1^2 - \alpha x_2^2 - \beta x_3^2 + \alpha\beta x_4^2.$$

d) If $\dim C = 8$, *there exist $\alpha, \beta, \gamma \in F^\times$ such that C is isomorphic to the octonion algebra $O(\alpha, \beta, \gamma) = \left(\frac{\alpha,\beta,\gamma}{F}\right)$. With respect to the standard octonion basis $e_1, e_2, e_3, e_4, e_5, e_6, e_7, e_8$, the norm form is*

$$N(x_1, \ldots, x_8) = x_1^2 - \alpha x_2^2 - \beta x_3^2 - \gamma x_4^2 + \alpha\beta x_5^2 + \alpha\gamma x_6^2 + \beta\gamma x_7^2 - \alpha\beta\gamma x_8^2.$$

Conversely, each of the algebras exhibited above is a composition algebra.

Note in particular that although a composition algebra is *a priori* allowed to be infinite-dimensional over F, it turns out that the only possible dimensions are 1, 2, 4 and 8.

Lemma 7.8. *Let R be an order in the imaginary quadratic field $K = \mathbb{Q}(\sqrt{D})$: that is, R is free of rank 2 as a $\mathbb{Z}$-module and $R \otimes_{\mathbb{Z}} \mathbb{Q} = K$.*
a) R is a finite index subring of $\mathbb{Z}_K$, the full ring of integers of K. We denote this index by f and call it the ***conductor*** *of R.*
b) Conversely, for every $f \in \mathbb{Z}^+$ there is a unique order R in K of conductor f, namely

$$R_f = \mathbb{Z}\left[f\left(\frac{D+\sqrt{D}}{2}\right)\right].$$

c) R_f is a Dedekind domain iff $f = 1$.
d) For any nonzero ideal I in R_f, put $|I| = \#R_f/I$. The ideals of norm prime to f factor (necessarily uniquely) into products of prime ideals.

Theorem 7.9. *Let K be an algebraically closed field of characteristic $p > 0$, and $E_{/K}$ an elliptic curve. TFAE:*
(i) $E[p](\overline{K}) = 0$.
(ii) $E[p^\infty](\overline{K}) = 0$.
(iii) The endomorphism $[p]$ is purely inseparable.
(iv) The isogeny $\mathrm{Frob}_p^\vee$ is inseparable.
(v) $\mathrm{End}^0(E)$ is isomorphic to $B_{p,\infty}$, the definite rational quaternion algebra ramified precisely at p and ∞.

Proof. We have already seen the equivalence of (i) through (iv). Let us call these equivalent conditions "supersingular".
(iii) $\implies$ (v): Seeking a contradiction, we suppose $\dim_{\mathbb{Q}} \mathrm{End}^0(E) \leq 2$.
Step 1: If E is supersingular, every curve isogenous to E is supersingular. Indeed, let $\psi : E \to E'$. Then since $\psi \circ [p]_E = [p]_{E'} \circ \psi$; taking separable degrees gives what we want.
Step 2: Since $j(E) \in \mathbb{F}_{p^2}$, the **isogeny class** of E is finite. Each curve in the isogeny class has endomorphism ring either $\mathbb{Z}$ or an order in an imaginay quadratic field. We may choose a prime $\ell \neq p$ which is inert in each of these guys. We can choose a sequence of subgroups

$$\Phi_1 \subset \Phi_2 \subset \ldots \subset E(K)$$

with $\Phi_i \cong \mathbb{Z}/\ell^i\mathbb{Z}$. Let $E_i = E/\Phi_i$, so these guys are all isogenous to E. Since the isogeny class if finite, we may choose $j > i > 0$ such that $E_i \to E_j$. Thus we get

$$\lambda : E_i \to E_j \xrightarrow{\sim} E_i.$$

$\ker \lambda$ is cyclic of order ℓ^{j-i}, and ℓ is prime in $\mathrm{End}\, E_m$; comparing degrees gives

$$\lambda = u[\ell^{\frac{j-i}{2}}],$$

for some $u \in \mathrm{Aut}\, E_m$. The kernel of the guy on the right is not cyclic!
(v) $\implies$ $\square$

Exercise: Let K be an algebraically closed field, and let $E_{/K}$ be an elliptic curve which is *not* supersingular. Show that the isogeny class of E is countably infinite.

7.3. **The Characteristic Polynomial of Frobenius.**

Let $E_{/K}$ be an elliptic curve. For any prime $\ell \operatorname{char} K$ and any $\varphi \in \operatorname{End} E$, we know from Theorem 6.3 that the characteristic polynomial of $\varphi_\ell \in \operatorname{End} T_\ell E$ is

$$\chi_\varphi(t) = t^2 - (1 + \deg \varphi - \deg(1 - \varphi))t + \deg \varphi.$$

By the way, we have not yet used this result for anything? What's it good for?

For most elliptic curves over a field of characteristic 0, $\operatorname{End} E = \mathbb{Z}$. If we take $\varphi = [n]$, nothing very exciting happens: the characteristic polynomial is

$$t^2 - (1 + \deg[n] - \deg(1-[n])t + \deg[n] = t^2 - (1 + n^2 - (1-n)^2)t + n^2 = t^2 - 2nt + n^2 = (t-n)^2.$$

Well, of course it is: this is the characteristic polynomial of the scalar matrix $\begin{bmatrix} n & 0 \\ 0 & n \end{bmatrix}$, and that's what φ_ℓ is: multiplication by n on $T_\ell E$.

Exercise: If we have an elliptic curve $E_{/\mathbb{C}}$ with $\operatorname{End} E$ isomorphic to an order in an imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$, let $\varphi \in \operatorname{End} E \setminus \mathbb{Z}$ be any "complex multiplication". Show that for any prime number ℓ, the characteristic polynomial of φ_ℓ is precisely the minimal polynomial of φ viewed as an element of the quadratic field $\mathbb{Q}(\sqrt{-d})$.

So what's all the fuss about Theorem 6.3? Can we get a nontrivial example?

Yes. Let $q = p^k$ be a prime power, $E_{/\mathbb{F}_q}$ an elliptic curve, let $\ell \neq p$, and take $\varphi = \operatorname{Frob}_q$, the Frobenius map. Then

$$\chi_{\operatorname{Frob}_q}(t) = t^2 - at + q,$$

where $a = q + 1 - \#E(\mathbb{F}_q)$. This is exactly the quantity we considered in our discussion of Mordell-Weil groups of elliptic curves over finite fields: in particular Hasse's Theorem is equivalent to the bound

$$|a| \leq 2\sqrt{q}.$$

Let π and $\overline{\pi}$ be the roots in $\mathbb{C}$ of the characteristic polynomial of Frobenius. Thus π and $\overline{\pi}$ are algebraic integers, and by the quadratic formula

$$\pi, \overline{\pi} = \frac{-a \pm \sqrt{a^2 - 4q}}{2}.$$

We have a repeated root iff $a^2 = 4q$, i.e., iff $a = \pm 2\sqrt{q}$ (this can only happen if $q = p^k$ with k *even*, but if you look at Theorem XX you see that it can *always* happen in this case). Then we have a repeated root and $\pi = \overline{\pi} = \pm\sqrt{q}$.

Otherwise we have distinct roots $\pi \neq \overline{\pi}$. It is easy to see that we cannot then have $\pi, \overline{\pi} \in \mathbb{Q}$: they would then be in $\mathbb{Z}$; since $\pi\overline{\pi} = q$ we must have

$$\pi = \epsilon p^r, \ \overline{\pi} = \epsilon p^{k-r}$$

with $0 \leq r \leq k$ and $\epsilon \in \pm 1$; without loss of generality $r > \frac{k}{2}$, and then

$$\frac{\pi + \overline{\pi}}{p^{\frac{k}{2}}} = p^{r - \frac{k}{2}} + p^{\frac{k}{2} - r} > p^{\frac{1}{2}} \geq \sqrt{2},$$

contradicting Hasse's Theorem. So $\pi, \overline{\pi}$ are Galois conjugate elements of the quadratic field $\mathbb{Q}(\sqrt{a^2 - 4q})$; by Hasse's Theorem, this is an imaginary quadratic field.

Because they are Galois conjugate, they have the same norm from $K/\mathbb{Q}$, and since this norm is just the square of the usual absolute value on $\mathbb{C}$, it follows that $|\pi| = |\overline{\pi}|$. Finally, because $|\pi\overline{\pi}| = |q| = q$, we conclude $|\pi| = |\overline{\pi}| = \sqrt{q}$. Noting that this also holds in the case of a repeated root, we see that we have proved in all cases that:

Theorem 7.10. *Let $E_{/\mathbb{F}_q}$ be an elliptic curve. Then the complex roots of the characteristic polynomial of* Frob_q *have absolute value $|\sqrt{q}|$.*

This result is in fact the **Riemann Hypothesis** for the Hasse-Weil zeta function of $E_{/\mathbb{F}_q}$, although we have not given the definition of this.

Exercise: Show that in all cases Frob_q as an element of $\mathrm{End}\, V_\ell$ is semisimple, i.e., diagonalizable over the algebraic closure. (Hint: assume not and build an element of $\mathrm{End}\, E$ whose ℓ-adic representation is a nonzero nilpotent matrix.)

Remark: For an elliptic curve $E_{/\mathbb{F}_q}$, each of the following pieces of data immdiately determines the others:
(i) $\#E(\mathbb{F}_q)$.
(ii) a, the trace of Frob_q.
(iii) $\chi(t)$, the characteristic polynomial of Frobenius.
(iv) π, $\overline{\pi}$, the Frobenius eigenvalues.

Corollary 7.11. *Let $E_{/\mathbb{F}_q}$ be an elliptic curve, and let $\pi, \overline{\pi}$ be the roots of the characteristic polynomial of* Frob_q*. Then for all $n \in \mathbb{Z}^+$,*

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - \pi^n - \overline{\pi}^n.$$

Proof. We have $\#E(\mathbb{F}_{q^n}) = q^n + 1 - a_n$, where a_n is the trace of Frob_{q^n}. In particular $a_1 = \pi + \overline{\pi}$ is the trace of Frob_q. But $\mathrm{Frob}_{q^n} = \mathrm{Frob}_q^n$, so if the eigenvalues of Frob_q are $\pi, \overline{\pi}$, the eigenvalues of Frob_{q^n} are π^n, $\overline{\pi}^n$. □

Theorem 7.12. *Let $E_{/\mathbb{F}_q}$ be an elliptic curve. Write $\#E(\mathbb{F}_q) = (q+1) - a$. TFAE:*
(i) $p \mid a$.
(ii) E is supersingular.

Proof. E is ordinary iff there is $n \in \mathbb{Z}^+$ such that

$$p \mid \#E(\mathbb{F}_{q^n}) = q^n + 1 - \pi^n - \overline{\pi}^n,$$

i.e., iff there is $n \in \mathbb{Z}^+$ such that $\pi^n + \overline{\pi}^n \equiv 1 \pmod{p}$.
(i) $\implies$ (ii): Suppose $p \mid a$. Then $\mathrm{tr}\,\mathrm{Frob}_q = \pi + \overline{\pi}$ is divisible by p. Since $\mathrm{tr}\,\mathrm{Frob}_{q^n} = \pi^n + \overline{\pi}^n = (\pi + \overline{\pi})(\ldots)$, it follows that $\mathrm{tr}\,\mathrm{Frob}_{q^n}$ is divisible by p for all n, so E is supersingular.
$\neg$ (i) $\implies$ $\neg$ (ii): Now suppose $\pi + \overline{\pi} \not\equiv 0 \pmod{p}$. Then there is $n \in \mathbb{Z}^+$ such that $(\pi + \overline{\pi})^n \equiv 1 \pmod{p}$. Now, using the relation $\pi\overline{\pi} = q \equiv 0 \pmod{p}$, one can show that for all $n \in \mathbb{Z}^+$,

$$\pi^n + \overline{\pi}^n \equiv (\pi + \overline{\pi})^n \pmod{p}$$

(Exercise!). This suffices. □

Exercise: Let $E_{/\mathbb{F}_p}$ be an elliptic curve; put, as usual, $\#E(\mathbb{F}_p) = p + 1 - a$.
a) Show that when $p = 2$ and $p = 3$ there are elliptic curves with $p \mid a$, $a \neq 0$.
b) Show that if $p \geq 5$, $E(\mathbb{F}_p)$ is supersingular iff $a = 0$.

Exercise: Show that for $E_{/\mathbb{F}_q}$, the following are equivalent:
(i) E is supersingular.
(ii) There is $n \in \mathbb{Z}^+$ such that, as endomorphisms of $E_{\mathbb{F}_{q^n}}$, $\mathrm{Frob}_{q^n} = [q^{\frac{n}{2}}]$.

Theorem 7.13. *(Tate) For elliptic curves $E_1, E_2/\mathbb{F}_q$, the following are equivalent:*
(i) E_1 and E_2 are $\mathbb{F}_q$-isogenous.
(ii) The characteristic polynomials of Frob_q *on E_1 and E_2 are equal.*
(iii) $\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q)$.

Proof. (i) $\implies$ (ii): Let $\varphi : E_1 \to E_2$ be an isogeny, say of degree d. Choose a prime ℓ which does not divide qd. Then $T_\ell(\varphi) : T_\ell(E_1) \to T_\ell(E_2)$ is a $\mathbb{Z}_\ell[G_K]$-module isomorphism, or, otherwise put, the ℓ-adic rep. of G_K on $T_\ell(E_1)$ and on $T_\ell(E_2)$ are isomorphic representations. It follows that the characteristic polynomials of Frob_q in these two representations are equal, and this implies $\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q)$.
(ii) $\iff$ (iii) follows from Remark XX above.
(ii) $\implies$ (i): Since Frob_q is a topological generator of the Galois group of $\mathbb{F}_q$, since the characteristic polynomials are equal and the Frobenius elements are semisimple, $T_\ell E_1$ and $T_\ell E_2$ are isomorphic as representations of $G_{\mathbb{F}_q}$. By a big theorem of Tate that we mentioned earlier, this forces E_1 and E_2 to be isogenous. □

Lemma 7.14. *Let E/K be an elliptic curve. Let $\varphi \in \mathrm{End}_K(E)$ be nonzero and spearable. Let $S \subset E(K)$. Let $L = K(\varphi^{-1}(S))$ be the compositum of all the extensions $K(Q)/K$ as Q ranges over points of $E(\overline{K})$ with $\varphi(Q) \in S$. Then L/K is a Galois extension.*

Proof. Step 1: The map $\varphi : E \to E$ is an unramified covering map (in more precise terminology, a finite étale morphism). By XXX, its fiber over $P \in E(K)$ is a finite etale K-algebra, i.e., a finite product of *separable* field extensions. These are precisely the extensions $K(Q)/K$ for $Q \in \varphi^{-1}(P)$, so L/K is separable.
Step 2: Let $Q \in E(K^{\mathrm{sep}})$ be such that $\varphi(Q) = P \in S$, and let $\sigma \in G_K$. Then

$$P = \sigma(P) = \sigma(\varphi(Q)) = \varphi(\sigma(Q)),$$

so $\varphi(\sigma(Q)) = P$. It follows that $\sigma(L) = L$, i.e., L/K is normal. □

8. The Mordell-Weil Theorem I: Overview

8.1. **Statement.**

Our goal is to prove the following celebrated result.

Theorem 8.1. *(Mordell-Weil) Let $E_{/K}$ be an elliptic curve over a global field. Then $E(K)$ is a finitely generated commutative group.*

8.2. **Outline of the Proof.**

Step 1: One proves the **weak Mordell-Weil Theorem**: for each $n \geq 2$, the **weak Mordell-Weil group** $E(K)/nE(K)$ is finite.

In broadest possible terms, this is proved as follows: there is an easily defined canonical injection ι of $E(K)/nE(K)$ into a group called (you are not expected to understand this notation as yet) $H^1(K, E[n])$. This group is infinite, but there is a subgroup $\mathrm{Sel}(K, E)[n]$ containing $\iota(E(K)/nE(K))$, the **n-Selmer group**. So it suffices to show the finiteness of the n-Selmer group. This uses a mixture of

classical (but nontrivial) alebraic number theory and Galois cohomology.

Step 2: One shows that there is a **height function** $h : E(K) \to \mathbb{R}^{\geq 0}$ with the following properties:

(H1) For all $R \in \mathbb{R}^{\geq 0}$, $h^{-1}([0, R])$ is a finite set;
(H2) For all $Q \in E(K)$, there is $C_2 = C_2(K, E, Q)$ such that for all $P \in E(K)$, $h(P + Q) \leq 2h(P) + C_2$; and for all $n \geq 2$,
(H3n) There is $C_3 = C_3(K, E, n)$ such that for all $P \in E(K)$, $h(nP) \geq n^2 h(P) - C_3$.

Step 3: Let $(A, +)$ be a commutative group. Consider properties of $h : A \to \mathbb{R}$:
(HF1) For all $R > 0$, $h^{-1}((-\infty, R))$ is finite.
(HF2) For all $y \in A$, there is $c_1(y) \in \mathbb{R}^{>0}$ such that for all $x \in A$,

$$h(x + y) \leq 2h(x) + c_1(y).$$

(HF3) For every integer $m \geq 2$,
(HF3m) There is $C_2(m) \in \mathbb{R}^{>0}$ such that for all $x \in A$, $m^2 h(x) \leq h(mx) + C_2(m)$.

A **height function** on a commutative group A is a function $h : A \to \mathbb{R}$ satisfying (HF1), (HF2) and (HF3).

Exercise: Let A be a commutative group which admits a height function. Prove or disprove: $A[\text{tors}]$ must be finite.

For an integer $m \geq 2$, an **m-height function** is a function $h : A \to \mathbb{R}$ satisfying (HF1), (HF2) and (HF3m).

Of these steps, the easy one is Step 3. This is a completely elementary argument that takes slightly under a page: [AEC, Prop. VIII.3.1].

Step 2 involves developing the theory of height functions on varieties over number fields. An acceptable definition of the height of a rational number $\frac{a}{b}$ in lowest terms is $\log(\max(|a|, |b|)$. Constructing a height function over number fields is more involved and is part of Weil's contribution.

Step 1 is probably the deepest. It breaks into enough substeps that it gets an outline of its own in the next section.

9. The Mordell-Weil Theorem II: Weak Mordell-Weil

Convention: Throughout this section, E/K is an elliptic curve, and $m \geq 2$ is an integer which is not divisible by $\operatorname{char} K$.

9.1. **Statement and Outline of the Proof.**

We will prove the following formulation of the Weak Mordell-Weil Theorem.

Theorem 9.1. *a) Let K be a field, let E/K be an elliptic curve, and let $K' = K(E[m])$. Suppose there is a Dedekind domain R with fraction field K' such that:*
(i) The ideal class group $\operatorname{Pic} R$ *is finitely generated, and*
(ii) The unit group $R^\times$ is finitely generated.
Then for every $m \geq 2$ with $\operatorname{char} K \nmid m$, *$E(K)/mE(K)$ is finite.*
b) In particular, for every elliptic curve over a global field K and every $m \geq 2$ with $\operatorname{char} K \nmid m$, *$E(K)/mE(K)$ is finite.*

9.2. **Outline of the proof.**

Here are the major steps of the proof:

Step 1: We reduce to the case $K' = K$.

Let

$$L = K([m]^{-1}E(K))$$

be the compositum of all the fields of definition $K(Q)$ as Q ranges over points of $E(\overline{K})$ such that $[m]Q \in E(K)$. By XXX, $K(Q) \subset K^{\text{sep}}$, so L/K is a separable extension. If $[m]Q = P \in E(K)$, then $P = \sigma(P) = \sigma([m]Q) = [m](\sigma Q)$, so $[m](\sigma Q) \in E(K)$. It follows that L/K is Galois: we write $G_{L/K} = \text{Aut}(L/K)$.

Step 2: We construct the **Kummer pairing**

$$\kappa : E(K) \times G_K \to E[m](K),$$

which has the following properties:
(i) For all $P, Q \in E(K)$ and $\sigma \in G_K$,

$$\kappa(P + Q, \sigma) = \kappa(P, \sigma) + \kappa(Q, \sigma).$$

(ii) For all $P \in E(K)$ and $\sigma, \tau \in G_K$,

$$\kappa(P, \sigma\tau) = \kappa(P, \sigma) + \kappa(P, \tau).$$

(iii) For $P \in E(K)$, we have $\kappa(P, \sigma) = 0$ for all $\sigma \in G_K$ iff $P \in mE(K)$.
(iv) For $\sigma \in G_K$, we have $\kappa(P, \sigma) = 0$ for all $P \in E(K)$ iff $\sigma \in G_L$.

It follows that κ induces injections

$$G_{L/K} \hookrightarrow \text{Hom}(E(K)/mE(K), E[m])$$

and

$$E(K)/mE(K) \hookrightarrow \text{Hom}(G_{L/K}, E[m]).$$

The first injection shows that L/K is abelian of exponent m. The second injection implies that if L/K is finite, so is $E(K)/mE(K)$.

Step 3: We show that L/K is finite.

This step further breaks down as follows.

Step 3a: Choose a Weierstrass Equation $\mathcal{W}$ for E with coefficients in R, and let Δ be the discriminant of $\mathcal{W}$. Let S be the finite set of prime ideals of R dividing $m\Delta$. We show that L/K is unramified outside S.

Step 3b: We show that the maximal abelian extension of exponent m of K which is unramified outside any finite set S of primes of R is finite.

9.3. **The preliminary reduction.**

Let K be a field $E_{/K}$ an elliptic curve, $m \geq 2 \in \mathbb{Z}$, and L/K a field extension. There is a natural map

$$\iota : E(K)/mE(K) \to E(L)/mE(L).$$

Proposition 9.2. *Suppose that* $\operatorname{char} K \nmid m$ *and that* L/K *is Galois (i.e., algebraic, normal and separable, but possibly of infinite degree). There is a canonical injection*

$$\ker \iota \hookrightarrow \operatorname{Map}(G_{L/K}, E[m]).$$

Proof. Let $P \in E(K) \cap mE(L)$, and choose $Q_P \in E(L)$ such that $[m]Q_P = P$. For $\sigma \in G_{L/K}$, we have

$$[m](\sigma(Q_P) - Q_P) = \sigma([m]Q_P) - [m]Q_P = \sigma P - P = 0,$$

and thus $\sigma(Q_P) - Q_P \in E[m]$ Thus we have defined a map

$$\lambda_P : G_{L/K} \to E[m],\ \lambda_P(\sigma) = \sigma(Q_P) - Q_P.$$

(In general λ_P *does* depend on the choice of Q_P; our argument will hold for any choice of Q_P.) Suppose that for $P, P' \in E(K) \cap mE[L]$, $\lambda_P = \lambda_{P'}$. Then

$$\forall \sigma \in G_{L/K},\ \sigma(Q_P - Q_{P'}) = Q_P - Q_{P'},$$

so by Galois descent $Q_P - Q_{P'} \in E(K)$. Thus

$$P - P' = [m](Q_P - Q_{P'}) \in mE(K)$$

Thus

$$\ker r \to \operatorname{Map}(G_{L/K}, E[m]),\ P \mapsto \lambda_P$$

is injective. □

Corollary 9.3. *If* L/K *is finite Galois and* $E(L)/mE(L)$ *is finite,* $E(K)/mE(K)$ *is finite.*

Proof. Exercise! □

Exercise: a) Show that in Corollary 9.3, "finite Galois" can be weakened to "finite separable". (A solution is given in [BG, Lemma 10.2.13].)
b) Does Corollary 9.3 hold if "finite Galois" is weakened to "finite"?
c) Give an example of a field extension L/K and an elliptic curve E/K such that $E(L)/mE(L)$ is finite but $E(K)/mE(K)$ is infinite. (Suggestion: use the fact – see e.g. [Cl09, §3] – that for every free comutative group G, there is a field K and an elliptic curve E/K with $E(K) \cong G$.)

9.4. **The Kummer Pairing.**

Let K be a field, $m \geq 2$ such that $\operatorname{char} K \nmid m$, and let E/K be an elliptic curve such that $E[m] = E[m](K)$. We define the **Kummer pairing**

$$\kappa : E(K) \times G_K \to E[m]$$

by applying the construction of the last section with $L = K^{\mathrm{sep}}$. For $P \in E(K)$, we defined $\lambda_P : G_K \to E[m]$ by choosing $Q_P \in E(K^{\mathrm{sep}})$ with $[m]Q_P = P$ and then putting $\lambda_P(\sigma) = \sigma(Q_P) - Q_P$. We claim that, in contrast to the previous case, the assumption that E has full m-torsion over K implies that λ_P is independent of the

choice of Q_P. Indeed, any Q'_P with $[m]Q'_P = P$ is of the form $Q'_P = Q_P + T$ for $T \in E[m]$. Since $E[m] = E[m](K)$, we have

$$\sigma(Q'_P) - Q_P; = \sigma(Q_P + T) - (Q_P + T) = \sigma(Q_P) - Q_P + \sigma(T) - T = \sigma(Q_P) - Q_P.$$

Thus we put $\kappa(P, \sigma) = \sigma(Q) - Q$.

The next thing to check about the Kummer pairing is its bilinearity: properties (i) and (ii) above. Since we may take $Q_{P+P'} = Q_P + Q_{P'}$, it follows that

$$\kappa(P + P', \sigma) = \kappa(P, \sigma) + \kappa(P', \sigma).$$

On the other hand, if $\sigma, \tau \in G_K$, then

$$\kappa(P, \sigma\tau) = \sigma\tau Q_P - Q_P = \sigma\tau Q_P - \sigma Q_P + \sigma Q_P - Q_P$$

$$= \sigma(\tau Q_P - Q_P) + (\sigma Q_P - Q_P) = \sigma\kappa(P, \tau) + \kappa(P, \sigma) = \kappa(P, \sigma) + \kappa(P, \tau).$$

Let $P \in E(K)$. Then $\kappa(P, \sigma) = 0$ for all $\sigma \in G_K$ iff $\sigma Q_P - Q_P = 0$ for all $\sigma \in G_K$ iff $Q_P \in E(K)$ iff $P \in mE(K)$. This establishes (iii): the left kernel of κ is $mE(K)$.

Let $\sigma \in G_K$. Then $\kappa(P, \sigma) = 0$ for all $P \in G_K$ iff $\sigma Q_P - Q_P = 0$ for all P iff σ pointwise fixes $L = K([m]^{-1}E(K))$ iff $\sigma \in G_L$.

Exercise: Show: these results on Kummer pairings hold with $E_{/K}$ replaced by any commutative group variety $A_{/K}$. (You may use that $A[m](K^{\mathrm{sep}})$ is finite.)

9.5. **Interlude: Weak Mordell-Weil Over Big Fields.**

Let us say that a Galois extension L/K is **small** if for every positive integer d, there are only finitely many subextensions M of L/K with $[M : K] \leq d$.[8] Let us say that a field K is **big** if K^{sep}/K is small.

Exercise: a) Let L/K be a finite and separable. Show: L is big iff K is big.
b) Does part a) still hold if "separable" is omitted?

Exercise: a) Show that the following fields are big:
(i) $\mathbb{C}$, $\mathbb{R}$. (ii) Any field which is algebraically closed, separably closed, or real-closed.
(iii) Any finite field.[9]
(iv) A finite extension of $\mathbb{Q}_p$. (This is not easy: see [NT2, § II.2.5] for a proof.)
b) Let K be a field of characteristic 0. Show that K is big iff $K((t))$ is big.
c) Show that K is *not* big if K is:
(i) A number field.
(ii) Finitely generated but not algebraic over a field k.
(iii) The fraction field of $k[[t_1, \ldots, t_n]]$ for any k and any $n \geq 2$.
(iv) $k((t))$ for any field k of positive characteristic.
(Remark: in parts (i) through (iii) of c), the field K is **Hilbertian**. If you know about Hilbertian fields it should be easy to prove that no Hilbertian field is big.)

[8] This is not such a standard terminology, but there is some precedent for it: one often calls a profinite group G "small" if it has only finite many open subgroups of any given index. Thus we call a Galois extension small if its Galois group $\mathrm{Aut}(L/K)$ is a small profinite group.

[9] Admittedly this is a point against the terminology. If you would like to suggest an alternate adjective for this property of a field, please go ahead.

Theorem 9.4. *Let K be a big field, let $m \geq 2$ be an integer such that* $\operatorname{char} K \nmid m$*, and let A/K be any commutative group variety. Then $A(K)/mA(K)$ is finite.*

Exercise: Prove Theorem 9.4.

Exercise: Let $q = p^a$ and $K = \mathbb{F}_q((t))$.
a) Show that for each positive integer d *prime to* p, there are only finitely many extensions L/K of degree d inside a fixed algebraic closure. (Again, a proof can be found in [NT2, § II.2.5].)
b) Let $m \in \mathbb{Z}^+$ be such that $2 \leq m^2 < p$. Show that for any commutative group variety A/K, $A(K)/mA(K)$ is finite.
c)* Prove or disprove: for any $m \geq 2$ with $p \nmid m$ and any elliptic curve E/K, $E(K)/mE(K)$ is finite.[10]

9.6. **Reduction Modulo a Discrete Valuation.**

Let E/K be an elliptic curve over a field K, and let v be a discrete valuation on K, with valuation ring R and residue field k. In certain circumstances we can define a **reduced elliptic curve** $E_{/k}$ and a reduction map $r : E(K) \to E(k)$.

Exercise: Let R be any domain with fraction field K, and let E/K be an elliptic curve. Show that E admits a Weierstrass equation with coefficients in R.

So let $\mathcal{W}$ be a Weierstrass equation for E with R-coefficients. Using the canonical map $R \to R/\mathfrak{m} = k$ we may view $\mathcal{W}$ as a Weierstrass cubic over k: call it $\mathcal{W}_k$. Note that while $\mathcal{W}$ was by definition nonsingular, the reduced equation $\mathcal{W}_k$ need not be. This is not mysterious: the discriminant Δ of $\mathcal{W}$ is a nonzero element of R; the discriminant of the reduced Weierstrass equation is the image of Δ in k; thus the reduced discriminant is nonzero iff $v(\Delta) = 0$. When this occurs we say that the *Weierstrass elliptic curve* $(E, \mathcal{W})$ has **good reduction**.

By way of contrast, we say that E/K has **good reduction with respect to v** if E admits a Weierstrass equation $\mathcal{W}$ such that $(E, \mathcal{W})$ has good reduction.

The notion of good reduction of an elliptic curve is the more important one, but it is also worryingly abstract: can it happen that the Weierstrass equation that we start with has bad reduction but a different Weierstrass equation has good reduction? Absolutely yes! Equivalently, the reverse can happen: let $(E, \mathcal{W})$ be a Weierstrass equation with good reduction. We can always change variables to get a Weierstrass equation with bad reduction. Let π be a uniformizing element of K, let

$$\mathcal{W} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

be a Weierstrass equation with $v(\Delta) = 0$, and make the change of variables $x' = \pi^2 x$, $y' = \pi^3 y$ to get

$$\mathcal{W}' : y'^2 + \pi a_1 x'y' + \pi^3 a_y y' = x'^3 + \pi^2 a_2 x'^2 + \pi^4 a_4 x' + \pi^6 a_6.$$

The reduced Weierstrass equation is $y'^2 = x'^3$, which has a cusp at $(0, 0)$.

Exercise: Can we always choose a Weierstrass equation such that the reduction

[10] Off the top of my head, I think I don't know the answer to this.

has a nodal singularity?

Exercise: Show that if an elliptic curve has good reduction, the isomorphism class of the reduced elliptic curve $E_{/k}$ is well-defined independent of the choice of Weierstrass equation.

As we have hinted at, there is a rich theory here, including an algorithm due to Tate to determine whether a given elliptic curve has good reduction (and, if not, to give an elaborate, precise description of the type of bad reduction). We are going to skip this entirely, as we don't need it for the proof of the Mordell-Weil Theorem. Following [LEC], we develop the bare minimum for this.

First, the reduction of a given Weierstrass equation may be singular but, like any Weierstrass cubic, is geometrically irreducible so has at most one singular point. Now is a good time to recall that we discussed the fact that the chord and tangent process on a singular Weierstrass cubic still yields a group law on the set of nonsingular points, and that this group is isomorphic to the additive group of k in the case that the equation has a cuspidal singularity. Let $E^{\mathrm{ns}}(k)$ denote the set of nonsingular k-rational points on the reduced Weierstrass curve.

Let K_v be the completion of K with respect to v. We define a **reduction map**

$$r : E(K_v) \to E(k),$$

as follows: let $P \in E(K) \subset \mathbb{P}^2(K)$. Then we may write $P = [x : y : z]$ with $\min v(x), v(y), v(z) = 0$ and put $[q(x) : q(y) : q(z)] \in E_{\mathfrak{p}}(k(\mathfrak{p}))$.

Let $E^0(K_v)$ be the subset of $E(K_v)$ consisting of points P such that $r(P)$ is a nonsingular point on $E(k)$. (If $(E, \mathcal{W})$ has good reduction, then $E^0(K_v) = E(K_v)$.)

Proposition 9.5. *The restricted reduction map*

$$r : E^0(K_v) \to E^{\mathrm{ns}}(k)$$

is a surjective group homomorphism.

Exercise: Prove it. (Suggestions: the surjectivity is Hensel's Lemma. If you know a suitably high-powered formulation of Hensel's Lemma – e.g. one applying to nonsingular points on varieties – then there is nothign else to say. One can however easily reduce to the simplest version of Hensel's Lemma. See e.g. [AEC, §VII.2] for details. To show that the reduction map is a homomorphism, recall that both group laws are defined by the chord and tangent process. So all you need to do is show that the reduction modulo $\mathfrak{m}$ is compatible with the chord-and-tangent process, which is easier than it may sound.)

Define $E^1(K_v)$ to be the kernel of the (restricted) reduction map, so we have an exact sequence

$$0 \to E^1(K_v) \to E^0(K_v) \to E^{\mathrm{ns}}(k) \to 0.$$

Let's analyze $r : E(K_v) \to E(k)$ a little more. It is immediate that the point $O = [0 : 1 : 0]$ of $E(K_v)$ reduces to the point $O = [0 : 1 : 0]$ of k. Now consider a point $(x, y) = [x : y : 1]$. If $x, y \in R$, then (x, y) simply reduces to the point $(x \pmod m, y \pmod m)$. Otherwise $\min v(x), v(y) = v < 0$, and we write $[x :$

$y : 1] = [\pi^{-v}x : \pi^{-v}y : \pi^{-v}]$, which reduces to $O \in E(k)$. Thus a finite point $(x, y) = [x : y : 1] \in E(K_v)$ lies in $E^1(K)$ iff $x, y \in R_v$. The next result takes things one step further.

Lemma 9.6. *Let (R, v) be a discrete valuation ring with fraction field K, and let $(E, \mathcal{W})$ be a Weierstrass elliptic curve over K with $a_1, a_2, a_3, a_4, a_6 \in R$. Let $(x, y) = [x : y : 1] \in E(K)$. Then:*
a) We have $v(x) \geq 0 \iff v(y) \geq 0$.
b) If $\min v(x), v(y) < 0$, then there is $n \in \mathbb{Z}^+$ such that $v(x) = -2n$, $v(y) = -3n$.

Proof. Exercise. □

Believe it or not, the one fact about reduced elliptic curves that we will actually want to use in the proof of the Mordell-Weil Theorem is the following one.

Theorem 9.7. *Let $m \in \mathbb{Z}^+$ be such that $v(m) = 0$. Then $E^1(K_v)[m] = 0$.*

Proof. (Cassels [LEC]) Step 1: Let $E^0 = E^0(K_v$ and $E^1 = E^1(K_v)$. We will define a sequence of subgroups

$$E^1 \supset E^2 \supset \dots E^n \supset E^{n+1} \supset \dots$$

with the following properties:
(F1) $\bigcap_{n \in \mathbb{Z}^+} E^n = (0)$, and
(F2) for all $n \in \mathbb{Z}^+$, $E^n/E^{n+1} \cong (k, +)$.
This suffices: if $P \in E^1$ is such that $mP = 0$, then since $k[m] = 0$, P maps to 0 in E^1/E^2, i.e., $P \in E^2$. In general, if $P \in E^n$ then since $(E^n/E^{n+1})[m] = 0$, $P \in E^{n+1}$, so by induction $P \in \bigcap_{n \in \mathbb{Z}^+} E^n = (0)$.
Step 2: Now let's do it. By Lemma 9.6 $E^1(K_v)$ consists of O together with all points $(x, y) = [x : y : 1]$ with $v(x), v(y) < 0$, and for every such point we have $v(x) = -2n$, $v(y) = -3n$ for some $n \in \mathbb{Z}^+$. We therefore define E^n to be O together with the set of $(x, y) \in E^0(K_v)$ with $v(y) \leq -3n$. This definition makes clear that $E^n \supset E^{n+1}$ for all n and $\bigcap_{n \in \mathbb{Z}^+ E^n} = \{O\}$.
Step 3: It remains to show that each E_n is a subgroup and that $E_n/E_{n+1} \cong (k, +)$. For each $P = [x : y : 1] \in E(K_v)$, there is a unique $n \in \mathbb{Z}^+$ with $P \in E^n \setminus E^{n+1}$; we call this n the **level** of P and denote it by $\ell(P)$. Now fix $n \in \mathbb{Z}^+$ and make the change of variables

$$x' = \pi^{2n}x, y' = \pi^{3n}y$$

(and thus $P = (x, y) \mapsto P' = (x_n, y_n)$) to get the new Weierstrass equation

$$\mathcal{W}' : y'^2 + \pi^n a_1 x' y' + \pi^{3n} a_y y' = x'^3 + \pi^{2n} a_2 x'^2 + \pi^{4n} a_4 x' + \pi^{6n} a_6.$$

Under this change of variables a point P has the following behavior:
• If $\ell(P) < n$, then $P_n \in \mathcal{W}'$ reduces to the singular point $(0, 0)$.
• If $\ell(P) = n$, then $P_n \in \mathcal{W}$ reduces to a nonsingular finite point of $E(k)$.
• If $\ell(P) > n$, then $P_n \in \mathcal{W}'$ reduces to O.
Thus the isomorphism $E \to E'$ sends E^n to $(E')^0$ and E^{n+1} to $(E')^1$. It follows that E^n is a subgroup for all n and $E^n/E^{n+1} \cong (E')^0/(E')^1 \cong (E')^{\mathrm{ns}}(k) \cong (k, +)$. □

9.7. **The Finiteness of L/K.**

We now know that $L = K([m]^{-1}E(K))$ is an abelian extension of exponent dividing m and that the finiteness of L/K is equivalent to the finiteness of the group $E(K)/mE(K)$. Our goal in this section is to show that $[L : K]$ is finite.

9.7.1. *Bounding the Ramification.*

Choose a Weierstrass equation $\mathcal{W}$ for E with R-coefficients in R. Let $\Delta = \Delta(\mathcal{W})$.

Theorem 9.8. *Let $\mathfrak{p}$ be any nonzero prime ideal of R not dividing $m\Delta$. Then the extension L/K is unramified at $\mathfrak{p}$.*

Proof. The *a priori* infinite algebraic extension L/K is obtained by adjoining to K all fields of definition $K(Q)$ for $Q \in E(K^{\mathrm{sep}})$ such that $[m]Q = P \in E(K)$. If we put $L_P = \prod_{[m]Q=P} K(Q)$, then L_P/K is a finite Galois extension, and the possibly infinite extension L is obtained as the compositum of all the finite Galois extensions L_P. So it will be enough to show that each L_P/K is unramified. To set this up properly, let S be the integral closure of R in L_P, and let $\mathcal{P}$ be a prime of S lying over $\mathfrak{p}$. Let $I = I(\mathcal{P}/\mathfrak{p})$ be the **inertia group**, i.e., the set of $\sigma \in G_{L_P/K}$ such that $\sigma(\mathcal{P}) = \mathfrak{p}$ and σ acts trivially on $S/\mathcal{P}$. It will be enough to show that for all Q such that $[m]Q = P$ and all $\sigma \in I$, $\sigma(Q) = Q$.

Since $P \in E(K)$, $P = \sigma(P) = \sigma[m]Q = [m]\sigma(Q)$, so

$$0 = P - P = [m](\sigma(Q) - Q),$$

i.e., $\sigma(Q) - Q \in E[m]$. Further, because $\sigma \in I$,

$$r(\sigma(Q) - Q) = r(\sigma(Q)) - r(Q) = r(Q) - r(Q) = 0.$$

It follows that $\sigma(Q) - Q$ is an m-torsion element of the kernel of reduction. By the preceding theorem, this implies $\sigma(Q) = Q$. □

9.7.2. *An Algebraic Finiteness Theorem.*

Let S be the finite set of maximal ideals $\mathfrak{p}$ of R not dividing $m\Delta$.

Here is what we know about the field extension $L = K([m]^{-1}E(K))$ of K that we are trying to prove is finite:
(i) L/K is abelian of exponent dividing m.
(ii) L/K is a composite of finite extensions L_Q, each of degree at most m^2, and each unramified outside of S.

This gives us more than enough information to prove by purely algebraic means that L/K is finite! In the case where K is a number field and R is an S-integer ring in K, we can apply a theorem of Hermite-Minkowski directly out of the box.

Theorem 9.9. *(Hermite-Minkowski) Let K be a number field, let $d \in \mathbb{Z}^+$, and let S be a finite set of places of K. Then there are only finitely many field extensions L/K of degree d which are unramified outside of S.*

According to some we have now proved the weak Mordell-Weil Theorem. But I am going to go on with the proof. Why?
• Although the Hermite-Minkowski Theorem is well known to contemporary number theorists and arithmetic geometers (because of this important application, for instance!), it does not seem to be as ubiquitously present in first courses and texts in algebraic number theory. (For instance, it seems to be absent from the excellent text [Ba], upon which several algebraic number theory courses taught at UGA have been based.) The proof can be found, for instance, in [N, Thm. 2.13].
• The Hermite-Minkowski Theorem, as stated above, applies to number fields only.

We are going for a more general weak Mordell-Weil Theorem, including, in particular, the function field case. In fact the Hermite-Minkowski Theorem holds for global fields of positive characteristic, as long we impose the restriction (as we have been throughout) that $\operatorname{char} K \nmid m$. However the proof of this is really not standard – an instance of the second-class citizenship that function fields hold in number theory even unto the present day.[11]

• Our version of weak Mordell-Weil is "abstract": it holds in the fraction field of a Dedekdind domain with finitely generated class group and unit group. So we need to give a proof which works under those hypotheses. As we are about to see, the key is to use the fact that L/K is known to be abelian of exponent dividing m: this allows us to bring our class group and unit group hypotheses to play.[12]

We remove the "bad primes" from R by passing from R to

$$R_S = \bigcap_{v \in \Sigma_R \setminus S} R_v.$$

Then $\operatorname{Pic} R_S$ is naturally the quotient of $\operatorname{Pic} R$ by the subgroup generated by classes of prime ideals $\mathfrak{p}$ corresponding to finite elements of S. In particular, since $\operatorname{Pic} R$ is finitely generated, so is $\operatorname{Pic} R_S$. Actually we would very much like R_S to be a PID, which we can attain by increasing S. Namely, for each of a finite set of generators of $\operatorname{Pic} R_S$ choose a representative ideal I_i, and let S' be S together with all the prime ideals dividing at least one I_i. Then $\operatorname{Pic} R_{S'}$ is a PID. Further, its unit group is still finitely generated: indeed, for each prime $\mathfrak{p}$ we remove from R_S the free rank of the unit group either increases by 1 (if $\mathfrak{p}$ has finite order) or stays the same (if $\mathfrak{p}$ has infinite order).

Remark: In the case of R_S an S-integer ring in a global field, it follows from the Cebotarev Density Theorem that each element of $\operatorname{Pic} R_S$ is represented by a prime ideal (rather than a product of prime ideals). In this case then we can choose S' such that $R_{S'}$ is a PID and

$$\operatorname{rank}_{\mathbb{Z}} R_{S'}^{\times} \leq \operatorname{rank}_{\mathbb{Z}} R_S^{\times} + \#\operatorname{Pic} R_S.$$

Now, let us proceed. Since L/K is an abelian extension of exponent dividing m of a field containing m mth roots of unity, Kummer Theory applies: L is obtained by adjoining to K mth roots of a set of elements of K.

Lemma 9.10. *Let v be a discrete valuation on a field K such that $v(m) = 0$. Then the extension $K(a^{\frac{1}{m}})$ is unramified at v iff $v(a) \equiv 0 \pmod{m}$.*

Proof. We may assume that v is normalized, i.e., $v(K^{\times}) = \mathbb{Z}$. Extend v to a valuation on $L = K(a^{\frac{1}{m}})$. Then L/K is unramified at v iff $v(L^{\times}) = v(K^{\times})$. But the valuation of $a^{\frac{1}{m}}$ is $\frac{1}{m}$ times the valuation of a, so if this valuation is not divisible by m, $v(a^{\frac{1}{m}})$ is not an integer and the extension is ramified.

Conversely, suppose that $v(a)$ is an mth power. Let π be a uniformizer of K and

[11] One of the main steps in the proof of the Hermite-Minkowski Theorem is proved using Geometry of Numbers. The function field analogue can be proved using the Mahler-Eichler-Armitage GoN in the function field case.

[12] It is presumably the case that there are Dedekind domains to which the hypotheses of our theorem apply and for which the Hermite-Minkowski finiteness result does not!

put $a' = \frac{a}{\pi^{v(a)}}$. Then $a/a' = \pi^{v(a)}$ is an mth power, so $K(a^{\frac{1}{m}}) = K(a'^{\frac{1}{m}})$. That is: we may replace a with a', i.e., we may assume that a is a unit in the valuation ring and thus, since R_v is integrally closed, $a \in R_v^{\times m}$. Since $v(m) = 0$, by Hensel's Lemma reduction modulo π induces an isomorphism $R_v^\times / R_v^{\times m} \xrightarrow{\sim} k_v^\times / k_v^{\times m}$. So adjoining the mth root of a unit yields an unramified extension. □

Thus to prove the finiteness of L/K, it is enough to show that the subgroup

$$T_{S'} = \{a \in K^\times / K^{\times m} \mid \operatorname{ord}_v(a) \equiv 0 \pmod m \ \forall v \in \Sigma_R \setminus S'\}$$

is finite.

Lemma 9.11. *The natural map $\psi : R_{S'}^\times \to T_{S'}$ is surjective.*

Proof. Let $\overline{a} \in T_{S'}$ and choose a representative a of $\overline{a}$ in $K^\times$. Then the fractional ideal $aR_{S'}$ is an mth power; since $R_{S'}$ is a PID, there are $b \in K^\times$ and $u \in R_S^\times$ such that $a = ub^m$, and thus

$$\overline{a} = \psi(a) = \psi(u)\psi(b^m) = \psi(u).$$

□

Since $T_{S'} = T_{S'}[m]$, the map ψ factors through a surjective group homomorphism

$$\psi : R_{S'}^\times / R_{S'}^{\times m} \to T_{S'}.$$

Since $R_{S'}^\times$ is finitely generated, $T_{S'}$ is finite.

The proof given here actually works under milder hypotheses.

Theorem 9.12. *Let K be a field, and let $m \geq 2$ be an integer such that* $\operatorname{char} K \nmid m$. *Let E/K be an elliptic curve, and let $K' = K(E[m])$. Suppose there is a Dedekind domain R with fraction field K' such that:*
(i) $(\operatorname{Pic} R)[m]$ *is finite, and*
(ii) $R^\times / mR^\times$ is finite.
Then $E(K)/mE(K)$ is finite.

Exercise: Prove it. The following exercise may be helpful for this.

Exercise: Let $m \geq 2$, let $(A, +)$ be a commutative group, and let B be a subgroup of A. Suppose that $A[m]$ is finite.
a) Show by example that $(A/B)[m]$ may be infinite (indeed, of arbitrarily large cardinality).
b) Suppose that B is finitely generated. Show that $(A/B)[m]$ is finite.

Exercise: a) Let k be an algebraically closed field, $C_{/k}$ an integral curve and $K = k(C)$ the function field of C. Show that K satisfies the hypotheses of the Stronger Weak Mordell-Weil Theorem and thus, for every elliptic curve E/K and every $m \geq 2$ with $\operatorname{char} K \nmid m$, $E(K)/mE(K)$ is finite.
b) With K as in part a), give an example of an elliptic curve E/K such that $E(K)$ is *not* finitely generated.

10. The Mordell-Weil Theorem III: Height Functions

10.1. **Fields With Product Formula.**

Let K be a field and let Σ_K be a set of places v of K such that
(PF1) The subset Σ_K^{Arch} of Archimedean places in Σ_K is finite;
(PF2) For all $x \in K^\times$, the set of $v \in \Sigma_K \setminus \Sigma_K^{\mathrm{Arch}}$ such that $v(x) \neq 0$ is finite.

To every place we can associate an absolute value, unique up to normalization. By definition an Archimedean place is an equivalence class of Archimedean absolute values. To get from a valuation $v : K^\times \to \mathbb{R}$ to a place we need to exponentiate: thus we choose a constant $c_v > 1$ and put $|x|_v = c_v^{-v(x)}$. The data of one absolute value $|\cdot|_v$ for each place $v \in \Sigma_K$ will be referred to as $\mathcal{A}$. We require:
(PF3) For all $x \in K^\times$,

$$\prod_{v \in \Sigma_K} |x|_v = 1. \tag{16}$$

By (PF2), the product appearing on the left hand side of (16) is really a finite product. The equation (16) is called the **product formula**.

Exercise: $(K, \Sigma_K, \mathcal{A})$ be a field satisfying (PF1) and (PF2), and let R be a subring of K such that K is the fraction field of R. Suppose (PF3) holds for all nonzero elements of R. Show that (PF3) holds for all nonzero elements of K.

A triple $(K, \Sigma_K, \mathcal{A})$ is called a **product formula field**.

Remark: Clearly the data of $\mathcal{A}$ determines that of Σ_K: just pass to equivalence classes of absolute values. One may then wonder why we have taken this redundant approach. The answer is that it in practice it is usually quite clear what Σ_K should be, but the choice of an absolute value out of each equivalence class which satisfies (PF3) is more subtle, to the point where it seems to be best to treat it as an additional piece of data. In fact, there are often reasons to consider multiple nomalizations $\mathcal{A}$ on the same pair (K, Σ_K): c.f. the following exercise.

Exercise: Suppose that $(K, \Sigma_K, \mathcal{A})$ is a product formula field. Let $C \in \mathbb{R}^{>0}$, and define $\mathcal{A}_C$ by: for $v \in \Sigma_K$, $|\cdot|_{v,C} = |\cdot|_v^C$. Show that $(K, \Sigma_K, \mathcal{A}_C)$ is also a product formula field.

Example: Let $K = \mathbb{Q}$, let $\Sigma_{\mathbb{Q}}$ be the usual infinite absolute value $\infty|$, and for all primes p let $|\cdot|_p$ be the standard p-adic absolute value: $|x|_p = p^{-\operatorname{ord}_p(x)}$. It is immediate to check (PF1) and (PF2); the best way to check (PF3) is express it as the fact that for any nonzero integer x the standard Archimedean absolute value $|x|_\infty$ is the reciprocal of the product of the p-adic absolute values. Indeed, if $x = \pm \prod_{i=1}^r p_i^{a_i}$, then $|x|_p = 1$ for $p \neq p_i$ and $|x|_{p_i} = p_i^{-a_i}$, so

$$\prod_p |x|_p = \prod_{i=1}^n p_i^{-a_i} = {|x|_\infty}^{-1}.$$

Exercise:
a) Prove or disprove: every PFF structure on $\mathbb{Q}$ is of the form $(\mathbb{Q}, \Sigma_{\mathbb{Q}}, \mathcal{A}_C)$ for some constant C, where $(\Sigma_Q, \mathcal{A})$ is the standard product formula structure.

Example: Let k be any field, let $R = k[t]$ and let $K = k(t)$. We define Σ_K as follows: the nonzero prime ideals of R correspond to monic irreducible polynomials f; as for any nonzero prime ideal in a Dedekind domain there is a corresponding discrete valuation v_f. To get from a valuation to an absolute value, we need to exponentiate, and this involves a choice of base: that is, for each f, we need to choose $c_f > 1$ and then put $|x|_f = c_f^{-v_f(x)}$? Classical valuation theory deemphasizes this choice: two absolute values are **equivalent** if they each arise from the same valuation via different choices of constant, and as long as we work with only one absolute value at a time, the choice of normalization is usually immaterial.

However, a moment's thought shows that it certainly matters if we are trying to get a product formula! We could write down the answer in advance, but let's try something more honest: we'll make a naive guess to start and try to figure out how to modify it if and when things go wrong. Namely, fix any $c > 1$ and put $|x|_f = c^{-v_f(x)}$. We write Σ_R for this set of absolute values on K.

Exercise: Show that, up to equivalence, Σ_R is precisely the set of absolute values on K which are: **regular on R**: for all $x \in k[t]$, $|x| \leq 1$.

The pair (K, Σ_R) clearly satisfies (PF1) and (PF2): what about (PF3)? Let $x = \epsilon f_1^{a_1} \cdots f_r^{a_r} \in k[t]^\bullet$; here $\epsilon \in k^\times$ and the f_i's are monic and irreducible. Then

$$\prod_{v \in \Sigma_R} |x|_v = \prod_{i=1}^r |x|_{f_i} = \prod_{i=1}^r c^{-a_i} = c^{-\sum_{i=1}^r a_i}.$$

Well, first of all, this product clearly need not equal 1: in fact, when f has positive degree it is never 1. If each f_i has degree – as will be the case for all irreducible polynomial iff k is algebraically closed – then $-\sum_{i=1}^r a_i = -\deg x$. This suggests that we should add in one further non-Archimedean absolute value, $v_\infty(\frac{f}{g}) = v_\infty(g) - v_\infty(f)$ and normalize it as $|x|_\infty = c^{-v_\infty(x)}$. For $x \in k[t]^\bullet$ we get $|x| - \infty = c^{\deg x}$, so we do get a product formula this way if $k = \overline{k}$.

We want things to work nicely for arbitrary k though, so it is clear that we have done something slightly wrong...and, luckily, it is almost equally clear *what* we have done wrong. We want $\prod_{v \in \Sigma_R} |x|_v$ to be equal to $c^{-\deg x} = c^{-\sum_{i=1}^r a_i \deg f_i}$, so in fact the right way to exponentiate ord_f is as follows:

$$|x|_f = c^{-\deg(f) \mathrm{ord}_v(f)} = (c^{\deg f})^{-\mathrm{ord}_v f}.$$

Exercise: Prove or disprove that the only product formula structure on $k(t)$ is obtained from the one we constructed above via $\mathcal{A} \mapsto \mathcal{A}_C$.

Exercise: Let $C_{/k}$ be a nice curve, and let $K = k(C)$. Show that there is a product formula structure on $K(C)$ in which Σ_K is the set of valuations v_P as P ranges over closed points of C. (Suggestion: the matter of it, of course, is to work out the choice of constant c_v such that $|x|_v = c_v^{-v(x)}$. This is closely related to the definition of the divisor of $f \in K(C)$: in fact, with the right choice of normalizations, the

product formula is *equivalent* to the fact that the degree of the divisor of a rational function is zero.)

In fact we do not need the result of the previous exercise: we will use the fact that every nice curve admits a separable finite map to the projective line and build the product formula structure out of the finite separable field extension $k(C)/k(t)$.

10.2. **Height on Projective Space Associated to a Product Formula Field.**

Product formula fields (PFF) are used in several different ways in modern number theory. But for us the point is that a PFF $(K, \Sigma_K, \mathcal{A})$ allows us to define, for all $n \in \mathbb{Z}^+$, a **height function**

$$H : \mathbb{P}^n(K) \to \mathbb{R}^{\geq 0}.$$

The definition is simple enough: first let $(x_0, \ldots, x_n) \in \mathbb{A}^{n+1}(K)$. We put

$$H(x_0, \ldots, x_n) = \prod_{v \in \Sigma_K} \max_{0 \leq i \leq n} |x_i|_v.$$

Example: For $n = 1$ and $x \in K$,

$$H(x) = \prod_{v \in \Sigma_K} |x|_v = \begin{cases} 0, & x = 0; \\ 1; & x \neq 0. \end{cases}$$

So that's not very interesting. In fact, the product formula implies:

Lemma 10.1. *a) For any $n \in \mathbb{Z}^+$ and $\lambda \in K^\times$,*

$$H(\lambda x_0, \ldots, \lambda x_n) = H(x_0, \ldots, x_n).$$

b) Therefore H descends to a well-defined function $H : \mathbb{P}^n(K) \to \mathbb{R}^{\geq 0}$.
c) For all $x \in \mathbb{P}^n(K)$, $H(x) \geq 1$.

Exercise: Prove it.

Exercise: a) Let $n = 2$, $K = \mathbb{Q}$, $a, b \in \mathbb{Z} \setminus \{0\}$, $\gcd(a, b) = 1$. Then

$$H(x, 1) = H(\frac{a}{b}, 1) = H(a, b) = \max |a|, |b|.$$

b) State and prove a generalization of part a) to $\mathbb{P}^n(\mathbb{Q})$.
c) State and prove a generalization of part b) to $\mathbb{P}^n(k(t))$.

Notation: In general then, if we have a product formula field K and $x \in K$, then by $H(x)$ we will mean $H(x, 1)$.

Exercise: Let $(K, \Sigma_K, \mathcal{A})$ be a product formula field, and let R be a UFD with fraction field K. We say that $v \in \Sigma_K$ is **regular** on R if $|x|_v \leq 1$ for all $x \in R$.
a) Check that this depends only on v and not the choice of normalization.
b) Let Σ_K^∞ be the places of Σ_K which are *not* regular on R. Show that the height function on $\mathbb{P}^N(K)$ can be computed as follows: for write $P \in \mathbb{P}^N(K)$ as $P = [x_0 : \ldots : x_N]$ with $x_0, \ldots, x_N \in R$ and $\gcd(x_i) = 1$. Then

$$H(P) = \prod_{v \in \Sigma_K^\infty} \max_i |x_i|_v.$$

c) In particular, for $x \in K$,

$$H(x) = H(1,x) = \prod_{v \in \Sigma_K^\infty} |x|_v.$$

d) Let K be a global field and let R be an S-integer ring in K. Show that for $x \in R^\bullet$, $H(x) = \#R/(x)$.

We say that a product formula field has the **Northcott Property** if for all $n \in \mathbb{Z}^+$ and all $N \in \mathbb{R}$, $P(n,N) = \{x \in \mathbb{P}^n(K) \mid H(x) \leq N\}$ is finite.

Exercise: a) Show that $\mathbb{Q}$ has the Northcott Property.
b) Show that $K = k(t)$ has the Northcott Property iff k is finite.

Thus by regarding the rational number $\frac{a}{b}$ as the point $[\frac{a}{b} : 1] = [a : b] \in \mathbb{P}^1(\mathbb{Q})$ we recover the simplest, most natural arithmetic measure of its "arithmetic complexity": $\max |a|, |b|$. Similarly, our definition for the height of a rational function $f = \frac{a(t)}{b(t)}$ is precisely $c^{\deg f}$.

One may well ask why we went to all this trouble when the final formula is so simple. The answer is this: we are not just interested in the fields $\mathbb{Q}$ and $k(t)$ but in *every global field*. The elementary definition of the height function given here exploits several key features of these "prime global fields" which do not persist for an arbitrary global field: especially, it is not always possible to choose a PID R with fraction field K and take Σ_K to be Σ_R together with one further place.

The advantage of the formalism of product formula fields is (precisely?) that it handles passage to a finite field extension in a graceful way. We pursue this next.

10.3. **Finite Extensions of Product Formula Fields.**

Let $(K, \Sigma_K, \mathcal{A})$ be a product formula field, and let L/K be a finite separable field extension of degree d. We will endow L with a product formula structure $(\Sigma_L, \mathcal{A}_L)$.

Let Σ_L be the set of all places of L which extend some place of Σ_K. We recall some of the theory of this: by definition of Σ_L there is a surjective restriction map

$$\Sigma_L \to \Sigma_K;$$

we claim that the fibers of this map have cardinality at most d. Indeed, to find the set of places of L extending a place $v \in \Sigma_K$ we consider the algebra $L_v = L \otimes_K K_v$. Since L/K is separable, by the Primitive Element Corollary we may write $L = K[t]/(f)$ for some irreducible, separable polynomial f, and then $L_v \cong K_v[t]/(f)$. Suppose that f factors over K_v into irreducibles $f_1 \cdots f_r$ (by separability, these irreducible factors must be distinct). Then, by the Chinese Remainder Theorem,

$$L_v = L \otimes_K K_v \cong \prod_{i=1}^r K_v[t]/(f_i) \cong \prod_{w|v} L_w. \tag{17}$$

Thus L_w/K_v is a finite separable extension of complete fields. It is known that there is a unique place w on L_w extending v on K_v; up to normalization, the

corresponding absolute value is $x \mapsto |N_{L_w/K_v}(x)|_v$ [NT2, Thm. 31].

Of course, to get a product formula, the normalization matters. Thus we define

$$|x|_w = |N_{K_w/L_v}(x)|_v^{\frac{1}{d}}.$$

Lemma 10.2. *Let $x \in L$ and $v \in \Sigma_K$. Then*

$$\prod_{w|v} |x|_w = |N_{L/K}(x)|_v^{\frac{1}{d}}. \tag{18}$$

Exercise: Prove it. (Hint: use the definition of the norm in a finite dimensional algebra as the determinant of multiplication by x, and apply (17).)

Theorem 10.3. *$(L, \Sigma_L, \mathcal{A}_L)$ is a product formula field.*

Proof. (PF1) Since $\Sigma_L \to \Sigma_K$ is finite-to-one and there are only finitely many Archimedean places of Σ_K, there are only finitely many Archimedean places of Σ_L.
(PF2) For $x \in L^\times$, the set of places of K for which $|N_{L/K}(x)|_v \neq 1$ is finite, and hence the set of places of L lying over this set of places of K is finite. For all other places w of L we have $|x|_w = 1$.
(PF3) For $x \in L^\times$, we have

$$\prod_{w \in \Sigma_L} |x|_w = \prod_{v \in \Sigma_K} \prod_{w|v} |x|_w = \left(\prod_{v \in \Sigma_K} |N_{L/K}(x)|_v \right)^{\frac{1}{d}} = 1^{\frac{1}{d}} = 1.$$

□

Evidently we did not need to raise everything to the $(\frac{1}{d})$th power in order for the product formula to hold. Why did we do this? Because of the following result:

Theorem 10.4. *Let $(K, \Sigma_K, \mathcal{A})$ be a product formula field.*
a) Let L/K be a finite separable extension of degree d, and endow it with its product formula structure $(\Sigma_L, \mathcal{A}_L)$. Let $H_K : \mathbb{P}^n(K) \to \mathbb{R}$ and $H_L : \mathbb{P}^n(L) \to \mathbb{R}$ be the associated height functions, and let $\iota : \mathbb{P}^n(K) \hookrightarrow \mathbb{P}^n(L)$ be the natural inclusion. Then for all $P \in \mathbb{P}^n(K)$,

$$H_L(\iota(P)) = H_K(P).$$

b) Therefore there is a well-defined height function

$$H : \mathbb{P}^n(K^{\mathrm{sep}}) \to \mathbb{R},$$

*the **absolute height**.*

Proof. It all comes down to the fact that if $x \in K$, then $N_{L/K}(x) = x^d$. □

Remark: It is possible to extend this discussion to include finite, not necessarily separable extensions L/K. We just need a different normalization of $|x|_w$ in this case: see [LMW, pp. 8-9] for the details. But the proof of weak Mordell-Weil required us to work with K^{sep} anyway, so we may as well stick to that case here.

10.4. **Northcott Implies Strong Northcott.**

The goal of this section is to show that if a product formula field K satisfies the Northcott Property, so do all of its finite extension fields. This is a key step towards the construction of the height function on the Mordell-Weil group.

In fact we will prove a slightly stronger result.

Lemma 10.5. *Let $P \in \mathbb{P}^n(K^{\mathrm{sep}})$. For all $\sigma \in G_K$, $H(P) = H(\sigma(P))$.*

Exercise: Prove it.

For $v \in \Sigma_K$, let ϵ_v be the **Artin constant** of $|\cdot|_v$, i.e., the smallest real number such that for all $x, y \in K$, $|x+y|_v \leq \epsilon_v \max|x|_v, |y|_v$. Then $\epsilon_v = 1$ iff v is non-Archimedean, hence for all but finitely many $v \in \Sigma_K$.

Lemma 10.6. *Let K be a product formula field and $d \in \mathbb{Z}^+$. There is a positive number $M(K,d)$ such that: for any separable polynomial $f(T) = T^d + a_{n-1}T^{d-1} + \ldots + a_1 T + a_0 \in K[T]$, write*

$$f(t) = \prod_{i=1}^{d}(T - \alpha_i),\ \alpha_i \in K^{\mathrm{sep}}.$$

Then

$$H(a_0, \ldots, a_{n-1}, 1) \leq M(K,d) \prod_{i=1}^{d} H(\alpha_i).$$

In fact, we may take

$$M(K,d) = \left(\prod_{v \in \Sigma_K} \epsilon_v \right)^{d-1}.$$

Proof. Put $a_d = 1$.
Step 1: We CLAIM that for all $x \in K$,

$$\max_{0 \leq i \leq d} |a_i|_v \leq \epsilon_v^{d-1} \prod_{i=1}^{d} \max(|\alpha_i|_v, 1). \tag{19}$$

PROOF OF CLAIM We go by induction on d.
Base Case ($d = 1$): If $f(T) = T - a_0$, then the inequality reads $\epsilon_v^{-1} \max|a_0|_v, 1 \leq \max|a_0|_v, 1 \leq \max|a_0|_v$, which is certainly true.
Induction Step: Let $d \geq 2$ and suppose the result holds for all separable polynomials of degree $d-1$. Choose k such that $|\alpha_k|_v \geq |\alpha_i|_v$ for all i, and write

$$f(T) = (T - \alpha_k)g(T) = (T - \alpha_k)(T^{d-1} + b_{d-2}T^{d-2} + \ldots + b_1 T + b_0).$$

Note that $b_{d-1} = 1$; setting also $b_{-1} = b_d = 0$, we get that for $0 \leq i \leq d$,

$$a_i = b_{i-1} - \alpha_k b_i.$$

Thus

$$\max_{0 \leq i \leq d} |a_i|_v = \max_{0 \leq i \leq d} |b_{i-1} - \alpha_k b_i|_v$$

$$\leq \epsilon_v \max_{0 \leq i \leq d} |b_{i-1}|_v, |\alpha_k b_i|_v \leq \epsilon_v \left(\max_{0 \leq i \leq d} |b_i|_v \right) \max(|\alpha_k|_v, 1) \leq \epsilon_v^{d-1} \prod_{i=1}^{d} \max(|\alpha_j|_v, 1);$$

in the last inequality, we applied the induction hypothesis to g.
Step 2: Taking the product of (19) over all $v \in \Sigma_K$, we get the desired result. □

Remark: We will not need it, but one also has the lower bound

$$\left(\prod_{v \in \Sigma_K} \epsilon_v \right)^{-d} \prod_{i=1}^{d} H(\alpha_i) \leq H(a_0, \ldots, a_{n-1}, 1);$$

see [AEC, Thm. VIII.5.9].

Exercise:
a) Let K be a number field. Show that we may take $M(K,d) = 2^{d-1}$.
b) Let K be a function field over a field k. Show that we may take $M(K,d) = 1$.

Theorem 10.7. *(Northcott Implies Strong Northcott)*
Let K be a product formula field satisfying Northcott's Property: for all $n \in \mathbb{Z}^+$, $R \in \mathbb{R}$, $\{P \in \mathbb{P}^n(K) \mid H(P) \leq R\}$ is finite. Then for all $d \in \mathbb{Z}^+$, $n \in \mathbb{Z}^+$, $R \in \mathbb{R}$,

$$\{P \in \mathbb{P}^n(K^{\mathrm{sep}}) \mid [K(P):K] \leq d \text{ and } H(P) \leq R\}$$

is finite.

Proof. Let $P \in \mathbb{P}^n(K^{\mathrm{sep}})$ and choose coordinates $P = [x_0 : \ldots : x_n]$ with some $x_j = 1$, so $K(P) = K(x_0, \ldots, x_n)$. Then

$$H(P) = \prod_{v \in \Sigma_{K(P)}} \max_i |x_i|_v = \prod_{v \in \Sigma_{K(P)}} \max_i \left(\max |x_i|_v, 1\right)$$

$$\geq \max_i \left(\prod_{v \in \Sigma_{K(P)}} \max |x_i|_v, 1 \right) = \max_i H(x_i).$$

Thus if $H(P) \leq C$ and $[K(P):K] \leq d$, then

$$\max_i H(x_i) \leq C, \ \max_i [K(x_i):K] \leq d.$$

It is therefore sufficient to show that the set

$$X(K,C,d) = \{x \in K^{\mathrm{sep}} : H(x) \leq C, \ [K(x):K] \leq d\}$$

is finite. Let $x \in X(K,C,d)$, and put $d' = [K(x):K]$, so $d' \leq d$. Let $f(T) = T^{d'} + a_{d-1}T^{d'-1} + \ldots + a_1 T + a_0 \in K(t)$ be the minimal polynomial of x, say

$$f(T) = \prod_{i=1}^{d'} (T - x_i).$$

With respect to the constant $M(K,d)$ of Lemma 10.6, put

$$M = \max_{1 \leq i \leq d} M(k,i).$$

Then

$$H(a_0, \ldots, a_{d-1}, 1) \leq M \prod_{i=1}^{d'} H(x_i) \leq M H(x)^{d'} \leq M C^d,$$

where in the last inequality we have used Lemma 10.5. Because K has the Northcott Property, there are only finitely many points in $\mathbb{P}^n(K)$ of height at most MC^d, and thus only finitely many possibilities for $a_0, \ldots, a_{d-1}$. □

10.5. **Heights Under a Morphism of Projective Spaces.**

Theorem 10.8. *Let K be a product formula field, and let $f : \mathbb{P}^n \to \mathbb{P}^m$ be a degree d morphism of projective spaces over K. There is a positive number C depending only on K and f such that for all $P \in \mathbb{P}^n(K^{\mathrm{sep}})$,*

$$H(f(P)) \leq CH(P)^d.$$

Proof. For the case of a number field K, see [AEC, Thm. VIII.5.6]. For the general case, see [LMW, p. 13]. □

Exercise: a) Suppose K is a number field. Show that there is a constant c depending only on K and f such that for all $P \in \mathbb{P}^n(K^{\mathrm{sep}})$,

$$cH(P)^d \leq H(f(P)).$$

b) Does the result of part a) hold for a general product formula field?

10.6. **Height Functions on Elliptic Curves.**

So far our discussion of height functions has focused on the case of projective space. However this can be easily adapted to give height functions on anyprojective variety. Indeed, if K is a product formula field and $V_{/K}$ is a variety, choose a morphism $\varphi : V \to \mathbb{P}^n$ which is finite to one onto its image. We then get a height function on $V(K^{\mathrm{sep}})$:

$$h_\varphi : V(K^{\mathrm{sep}}) \to \mathbb{R},\ P \mapsto H(\varphi(P)).$$

If K has the Northcott Property – as we know it does for any global field K – then h_φ has the property that for all $d \in \mathbb{Z}^+$, $R > 0$,

$$\#\{P \in V(K^{\mathrm{sep}}) \mid [K(P) : K] \leq d, h_\varphi(P) \leq R\} < \infty.$$

For what follows we assume that $\mathrm{char}\, K \neq 2$ and discuss at the end what modifications are necessary in that case. The function we choose is the x-coordinate of a Weierstrass model: $x : E \to \mathbb{P}^1$. The significance of this is that it is an *even* function, i.e., for all $P \in E(\overline{K})$, $x(P) = x([-1]P)$. It also turns out to be convenient to take logarithms; thus our precise choice of height function will be

$$h_x : E(K^{\mathrm{sep}}) \to \mathbb{R},\ P = [x : y : z] \in E(K^{\mathrm{sep}}) \mapsto \log H(x(P)).$$

Explicitly, the point at infinity gets mapped under x to the point $[1 : 0]$ of $\mathbb{P}^1$, which has logarithmic height 0. Any other point P gets mapped to $\log H(x(P))$.

Theorem 10.9. *Let K be a product formula field of characteristic different from 2, and let $(E, \mathcal{W})/K$ be a Weierstrass elliptic curve of the form $y^2 = P_3(x)$. Then there is a constant A – depending on K and the Weierstrass coefficients of E – such that for all $P, Q \in E(K^{\mathrm{sep}})$,*

$$h_x(P + Q) + h_x(P - Q) = 2h_x(P) + 2h_x(Q) + A.$$

Proof. Under the additional assumption that E admits a short Weierstrass equation $y^2 = x^3 + ax + b$ – which always holds when $\mathrm{char}\, K \neq 2, 3$ – a very careful proof is given in [AEC, Thm. VIII.6.2]. □

Exercise: Modify the argument of [AEC, Thm. VIII.6.2] so as to work with Weierstrass equations $y^2 = P_3(x)$ in characteristic 3.

Theorem 10.10. *Let K be a global field of characteristic different from 2, and let $E_{/K}$ be an elliptic curve. Choose a Weierstrass equation $y^2 = P_3(x)$ for E. Then $h_x : E(K) \to \mathbb{R}$, $P \mapsto \log H(x(P))$, is a height function on the group $E(K)$.*

Proof. The finiteness property (HF1) has already been established.
(HF2): Fix $Q \in E(K)$. Then for all $P \in E(K)$,

$$h_x(P_+Q) = 2h_X(P) + 2h_x(Q) - h_x(P-Q) + A \leq 2h_X(P) + (2h_x(Q) + A).$$

(HF3) We can show something slightly stronger: for each fixed $m \in \mathbb{Z}$,

$$h_x(mP) = m^2 h_x(P) + O_m(1).$$

Because $h_x(-P) = h_x(P)$, it is enough to assume $m \geq 0$. We prove this by induction on m, the cases $m = 0$ and $m = 1$ being trivial: in these cases we have equality. Now assume that $m \geq 2$ and that the result holds for $m-1$ and m with constants $C(m-1)$ and $C(m)$. Applying Theorem 10.9 with $[m]P$ and P in place of P and Q, we get

$$\begin{aligned} h_x([m+1]P) &= -h_x([m-1]P) + 2h_x([m]P) + 2h_x(P) + O(1) \\ &= (-(m-1)^2 + 2m^2 + 2)h_x(P) + O(1) \\ &= (m+1)^2 h_x(P) + O(1). \end{aligned}$$

□

11. The Mordell-Weil Theorem IV: The Height Descent Theorem

Let $(A, +)$ be a commutative group, and let $m \geq 2$. Recall that a map $h : A \to \mathbb{R}$ is called an m-height function if all of the following hold:

(HF1) For all $R > 0$, $h^{-1}((-\infty, R))$ is finite.
(HF2) For all $y \in A$, there is $c_1(y) \in \mathbb{R}^{>0}$ such that for all $x \in A$,

$$h(x+y) \leq 2h(x) + c_1(y).$$

(HF3) For every integer $m \geq 2$,
(HF3m) There is $C_2(m) \in \mathbb{R}^{>0}$ such that for all $x \in A$, $m^2 h(x) \leq h(mx) + C_2(m)$.

Theorem 11.1. *(Height Descent Theorem) Let $m \geq 2$ be an integer, let A be a commutative group, and let $h : A \to \mathbb{R}$ be an m-height function. If A/mA is finite, then A is finitely generated.*

Proof. Let $r = \#A/mA$, and let $Q_1, \ldots, Q_r$ be a set of coset representatives for mA in A. Let $P \in A$. We define a sequence $\{P_n\}_{n=0}^{\infty}$ as follows: put $P_0 = P$. For $n \in \mathbb{Z}^+$, having defined P_{n-1}, choose $P_n \in A$ such that for some $1 \leq i_n \leq r$,

$$P_{n-1} = mP_n + Q_{i_n}$$

(P_n is unique up to an element of $A[m]$; choose any one.) Thus for all $n \in \mathbb{Z}^+$,

$$P = m^n P_n + \sum_{j=1}^{n} m^{j-1} Q_{i_j}. \tag{20}$$

We CLAIM there is $C \in \mathbb{R}^{>0}$ such that for all $P \in A$ there is $N = N(P)$ such that for all $n \geq P$, $h(P_n) \leq C$. This suffices to establishes the result, because then by

(20), A is generated by the finite set $\{Q_1, \ldots, Q_r\} \cup \{x \in A \mid h(x) \leq C\}$.

PROOF OF CLAIM: Put

$$C_1 = \max_{1 \leq i \leq r} c_1(-Q_i).$$

For $n \in \mathbb{Z}^+$, we have

$$h(P_n) \leq \frac{1}{m^2}(h(mP_n) + C_2(m)) = \frac{1}{m^2}(h(P_{n-1} - Q_{i_{n-1}}) + C_2(m))$$

$$\leq \frac{1}{m^2}(2h(P_{n-1}) + C_1 + C_2(m))$$

$$\leq \frac{1}{m^2}\left(2\left(\frac{1}{m^2}(2h(P_{n-2})) + C_1 + C_2(m)\right)\right)$$

$$\vdots$$

$$\leq \left(\frac{2}{m^2}\right)^n h(P) + \frac{1}{m^2}\left(1 + \frac{2}{m^2} + \frac{2^2}{m^4} + \ldots + \frac{2^{n-1}}{m^{2n-2}}\right)(C_1 + C_2(m))$$

$$< \left(\frac{2}{m^2}\right)^n h(P) + \frac{C_1 + C_2(m)}{m^2 - 2}.$$

This proves the claim for any constant $C > \frac{C_1 + C_2(m)}{m^2 - 2}$; e.g. we may take

$$C = 1 + \frac{C_1 + C_2(m)}{2}.$$

□

12. The Mordell-Weil Theorem V: Finale

12.1. **Completion of the proof.**

The hard work of the previous three sections fits together perfectly to show that for any elliptic curve E over a global field K, $E(K)$ is finitely generated.

Indeed: fix any $m \geq 2$ with $\operatorname{char} K \nmid m$. Let $K' = K(E[m])$. When K' is a number field, we may take $R = \mathbb{Z}_{K'}$: then $\operatorname{Pic} R$ is finite and $R^\times$ is finitely generated. When $K' = \mathbb{F}_q(C)$ is a function field we may take any affine open subset C° of C and let $R = \mathbb{F}_q[C^\circ]$: again $\operatorname{Pic} R$ is finite and $R^\times$ is finitely generated. Therefore Theorem 9.1 applies to show that $E(K)/mE(K)$ is finite. By Theorem 10.10, $h_x : E(K) \to \mathbb{R}$ is an m-height function. Applying the Height Descent Theorem to $E(K)$ and h_x, we conclude that $E(K)$ is finitely generated.

12.2. **Explicit Upper Bounds.**

12.3. **Effectivity.**

13. More On Heights

13.1. **Weil's Height Machine.**

13.2. **Néron Tate Canonical Heights.**

13.3. **The Canonical Height Descent Theorem.**

Theorem 13.1. *Let $(A,+)$ be a commutative group, and let $h : A \to \mathbb{R}$ be a quadratic form. Suppose:*
(i) There is $m \geq 2$ such that A/mA is finite.
(ii) For all $R \in \mathbb{R}$, $\{x \in A \mid h(x) \leq R\}$ is finite.
Let $y_1, \ldots, y_r$ be a set of coset representatives for mA in A. Put $C_0 = \max_{1 \leq i \leq r} h(y_i)$. Then A is generated by the finite set $\{x \in A \mid h(x) \leq C_0\}$.

Proof. Step 0: For any quadratic map $f : A \to B$ of commutative groups, we have $f(A[\text{tors}]) \subset B[\text{tors}]$. Since $\mathbb{R}$ is torsionfree, we have $f(A[\text{tors}]) = 0$. Thus, if $x \in A$ is such that $h(x) < 0$, then the elements $x, 2x, 3x, \ldots$ are distinct and for all $n \in \mathbb{Z}^+$, $h(nx) = n^2 h(x) < 0$, contradicting (ii). Thus $h(A) \subset \mathbb{R}^{\geq 0}$.[13]
Step 1: Let $\langle , \rangle : A \times A \to \mathbb{R}$ be the associated bilinear form: $\langle x, y \rangle = \frac{1}{2}(f(x+y) - f(x) - f(y))$. (We divide by 2 first because we can – $(\mathbb{R}, +)$ is uniquely 2-divisible – and second so that $\langle x, x \rangle = f(x)$ for all $x \in \mathbb{R}$.) Let $A_{\mathbb{R}} = A \otimes_{\mathbb{Z}} \mathbb{R}$. There is a unique extension of $\langle , \rangle$ to an $\mathbb{R}$-bilinear map on $A_{\mathbb{R}}$: for $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n \in \mathbb{R}$, $x_1, \ldots, x_n, y_1, \ldots, y_n \in \mathbb{A}$, we put

$$\langle \alpha_1 x_1 + \ldots + \alpha_n x_n, \beta_1 y_1 + \ldots + \beta_n y_n \rangle = \sum_{1 \leq i,j \leq n} \alpha_i \beta_j \langle x_i, y_j \rangle.$$

Then extend $h : A_{\mathbb{R}} \to \mathbb{R}$ by $h(x) = \langle x, x \rangle$. We leave it as an exercise to check that for all $x \in A_{\mathbb{R}}$, $h(x) \geq 0$. Thus the Cauchy-Schwarz inequality applies. Equivalently, we may define $|\cdot| : A_{\mathbb{R}} \to \mathbb{R}$ by $|x| = \sqrt{h(x)}$ and then

$$\forall x, y \in A_{\mathbb{R}}, |x + y| \leq |x| + |y|.$$

Put $c_0 = \max_{1 \leq i \leq r} |y_i|$, and let A' be the subgroup generated by all $x \in A$ with $|x| \leq c_0$. The assertion of the theorem is equivalent to $A' = A$. Step 2: Let $x_0 \in A$. If $|x_0| \leq c_0$, then $x_0 \in A'$, so suppose $|x_0| > c_0$. We define a sequence $\{x_n\}_{n \in \mathbb{N}}$: for $n \in \mathbb{Z}^+$, having defined x_{n-1}, choose $x_n \in A$ and $1 \leq i_n \leq r$ such that

$$x_{n-1} = m x_n + y_{i_n},$$

and then

$$x_0 = m^n x_n + \sum_{j=1}^{n} m^{j-1} y_{i_j}.$$

We claim that for some $n \in \mathbb{Z}^+$ we have $|x_n| \leq c_0$; since also $|y_{i_j}| \leq c_0$, this gives $x_0 \in A'$ and we're done. If not, then for all $n \in \mathbb{N}$,

$$m|x_{n+1}| = |x_n - y_{i_{n+1}}| \leq |x_n| + |y_{i_{n+1}}| \leq |x_n| + |c_0| < 2|x_n|.$$

Since $m \geq 2$, we get $|x_{n+1}| < |x_n|$ and thus

$$h(x_0) > h(x_1) > h(x_2) > \ldots > h(x_n) > \ldots,$$

so that there are infinitely many $x \in A$ with $h(x) < h(x_0)$: contradiction! □

[13]We will not need it to complete the proof, but it seems helpful to remark that similar arguments show: (i) for $x \in A$, $h(x) = 0 \iff x \in A[\text{tors}]$ and (ii) $A[\text{tors}]$ is finite.

14. Diophantine Approximation

14.1. Classical Diophantine Approximation.

The basic problem of **Diophantine Approximation** is as follows: let $\alpha \in \mathbb{R}$. We wish to find infinitely many rational numbers $\frac{p}{q}$ such that

$$|\frac{p}{q} - \alpha| < \frac{C}{q^d}$$

where $C > 0$ and $d \geq 1$ are fixed constants. When this is possible, we say α is (d, C)-approximable.

Exercise: Let $\alpha \in \mathbb{R}$. Show: α is (d, C)-approximable, then α is (d, C')-approximable for all $C' \geq C$ and (d', C') approximable for all $d' \leq d$ and all $C' > 0$.

We define the **approximation exponent** of α to be the infimum over all d such that α is (d, C)-approximable for some C.

Exercise: a) For all $\alpha \in \mathbb{R}$, show $d(\alpha) \geq 1$.
b) Show that $d(\sum_{n=1}^{\infty} \frac{1}{10^{n!}}) = \infty$.
c) Show that for any $\alpha \in \mathbb{Q}$, $d(\alpha) = 1$.

Theorem 14.1. *(Dirichlet) Let $\alpha \in \mathbb{R} \setminus \mathbb{Q}$. Then α is $(2, 1)$-approximable.*

Proof. Step 1: Since for any rational number $\frac{x}{y}$ and any $n \in \mathbb{Z}$ we have $\frac{x}{y} - n = \frac{ny - x}{y}$, we may assume $\alpha \in [0, 1)$. Divide the interval $[0, 1)$ into n half-open subintervals of equal length:

$$[0, 1) = \bigcup_{i=0}^{n-1} [\frac{i}{n}, \frac{i+1}{n}).$$

Consider the fractional parts of $0, \alpha, 2\alpha, \ldots, n\alpha$. By the Pigeonhole Principle there are $0 \leq j < k \leq n$ such that the fractional parts of $j\alpha$ and $k\alpha$ both lie in $[\frac{i}{n}, \frac{i+1}{n})$ for some i and hence

$$|k\alpha - \lfloor k\alpha \rfloor - (j\alpha - \lfloor j\alpha \rfloor)| < \frac{1}{n}.$$

Taking $x = \lfloor j\alpha \rfloor - \lfloor k\alpha \rfloor$ and $y = k - j$, we get

$$|x - y\alpha| < \frac{1}{n}$$

or

$$|\frac{x}{y} - \alpha| < \frac{1}{ny} < \frac{1}{y^2},$$

since $y = k - j < n$. This gives one solution to $|\frac{x}{y} - \alpha| < \frac{1}{y^2}$.
Step 2: Since α is irrational, $|\frac{x}{y} - \alpha| > 0$. By choosing n sufficiently large in Step 1 we can find a rational number $\frac{x'}{y'}$ such that $|\frac{x'}{y'} - \alpha| < \min \frac{1}{y'^2}, |\frac{x}{y} - \alpha|$. Continuing in this way we get an infinite sequence of rational numbers, showing that α is $(2, 1)$-approximable. □

We remark in passing that a strengthening of Dirichlet's Theorem is known.

Theorem 14.2. *(Hurwitz) a) Every irrational real number is* $(2, \frac{1}{\sqrt{5}})$*-approximable.*
c) The quadratic irrational $\frac{1-\sqrt{5}}{2}$ *is* not $(2, C)$*-approximable for any* $C < \frac{1}{\sqrt{5}}$.

Proof. See e.g. [GoN]. □

Theorem 14.3. *(Liouville* [Li44]*) Let* $\alpha \in \mathbb{R}$ *be algebraic of degree* d.
a) Then there exists $C > 0$ *such that* α *is* not (d, C)*-approximable.*
b) Thus $d(\alpha) \leq d$.

Proof. If $\alpha \in \mathbb{Q}$, we know already that $d(\alpha) = 1$, so we may assume that α is algebraic of degree $d > 1$. Let

$$P(t) = a_d t^d + \ldots + a_1 t + a_0 \in \mathbb{Z}[t]$$

be the minimal polynomial for α over $\mathbb{Q}$: we have $a_0, \ldots, a_d \in \mathbb{Z}$ (in order to make P unique we require $a_d > 0$). Let M be the maximum value of $|P'(t)|$ on the interval $[\alpha - 1, \alpha + 1]$. For $\frac{p}{q} \in [\alpha - 1, \alpha + 1]$, we apply the Mean Value Theorem:

$$\left| P\left(\frac{p}{q}\right) \right| = \left| P\left(\frac{p}{q}\right) - P(\alpha) \right| \leq M \left| \frac{p}{q} - \alpha \right|.$$

On the other hand, $q^d P(\frac{p}{q})$ is a nonzero integer, so

$$\left| P\left(\frac{p}{q}\right) \right| \geq \frac{1}{q^d}.$$

Combining, we find that if $|\frac{p}{q} - \alpha| \leq 1$, then

$$\left| \frac{p}{q} - \alpha \right| \geq \frac{1}{M} \left| P\left(\frac{p}{q}\right) \right| \geq \frac{M^{-1}}{q^d}.$$

Taking $C = \min(1, \frac{1}{M})$, we find that for all $\frac{p}{q} \in \mathbb{Q}$,

$$\left| \frac{p}{q} - \alpha \right| \geq \frac{C}{q^d}.$$

□

Corollary 14.4. *The real number* $\sum_{n=1}^{\infty} \frac{1}{10^{n!}}$ *is transcendental.*

Exercise: Prove it.

Remark: The converse of Corollary 14.4 is false: there are transcendental numbers with finite approximation exponent. Kurt Mahler made a deep study of transcendental numbers by their Diophantine approximation properties. However, as we shall see, for applications to Diophantine geometry we are interested only in approximation exponents of algebraic numbers.

Combining the results of Liouville and Dirichlet, we get:

Corollary 14.5. *For any quadratic irrational* $\alpha \in \mathbb{R}$, $d(\alpha) = 2$.

This leaves open the determination of the approximation exponent for algebraic numbers of degree $d \geq 3$. Improvements on Liouville's Theorem were given by several leading mathematicians in the first half of the 20th century. Finally, the problem was completely solved by Klaus Roth in 1955 in work which awarded him the Fields Medal in 1958.

Theorem 14.6. *Let α be a real algebraic number of degree d.*
a) (Thue [Th09]*)* $d(\alpha) \leq \frac{d}{2} + 1$.
b) (Siegel [Si21]*)* $d(\alpha) \leq 2\sqrt{d}$.
c) (Gelfond, Dyson [Dy47]*)* $d(\alpha) \leq \sqrt{2d}$.
d) (Roth [Ro55]*)* $d(\alpha) = 2$.

14.2. **Diophantine Approximation Applied to Diophantine Equations.**

What does Diophantine Approximation have to do with finiteness of integral solutions to Diophantine Equations? We give two examples illustrating the key difference between quadratic numbers and algebraic numbers of higher degree.

Theorem 14.7. *(Pell's Equation) Let d be a positive integer which is not a square. Then there are infinitely many $(x, y) \in \mathbb{Z}^2$ such that $x^2 - dy^2 = 1$.*

Proof. Step 1: We claim that there is a constant $M > 0$ and infinitely many pairs of positive integers (x, y) such that $|x^2 - dy^2| < M$. To see this, note that since d is not a square, $\alpha = \sqrt{d}$ is irrational, so by Dirichlet's Theorem there are infinitely many $(x, y) \in \mathbb{Z}^2$ such that

$$\left|\frac{x}{y} - \sqrt{d}\right| < \frac{1}{y^2},$$

or, multiplying through by y, such that

$$|x - \sqrt{d}y| < \frac{1}{y}.$$

Since $\sqrt{d} > 0$, we may assume $x, y > 0$. Now observe

$$|x + \sqrt{d}y| = |x - \sqrt{d}y + 2\sqrt{d}y| \leq |x - \sqrt{d}y| + 2\sqrt{d}y < \frac{1}{y} + 2\sqrt{d}y.$$

Thus

$$|x^2 - dy^2| = |x - \sqrt{d}y||x + \sqrt{d}y| < \left(\frac{1}{y}\right)\left(\frac{1}{y} + 2\sqrt{d}y\right) = \frac{1}{y^2} + 2\sqrt{d} \leq 1 + 2\sqrt{d} = M.$$

Step 2: We begin by further exploiting the pigeonhole principle. Namely, since we have infinitely many solutions (x, y) to $|x^2 - dy^2| < M$, there must exist some integer m, $|m| < M$ for which we have infinitely many solutions to the equality $x^2 - dy^2 = m$. And once again: we must have two different solutions, say (X_1, Y_1) and (X_2, Y_2) with $X_1 \equiv X_2 \pmod{|m|}$ and $Y_1 \equiv Y_2 \pmod{|m|}$ (since there are only m^2 different options altogether for $(x \pmod{|m|}, y \pmod{|m|})$ and infinitely many solutions). Let us write

$$\alpha = X_1 + Y_1\sqrt{d}$$

and

$$\beta = X_2 + Y_2\sqrt{d};$$

we have $N(\alpha) = N(\beta) = m$. A first thought is to divide α by β to get an element of norm 1; however, $\alpha/\beta \in \mathbb{Q}(\sqrt{d})$ but does not necessarily have integral x and y coordinates. However, it works after a small trick: consider instead

$$\alpha\beta' = X + Y\sqrt{d}.$$

I claim that both X and Y are divisible by m. Indeed we just calculate, keeping in mind that modulo m we can replace X_2 with X_1 and Y_2 with Y_1:

$$X = X_1X_2 - dY_1Y_2 \equiv X_1^2 - dY_1^2 \equiv 0 \pmod{|m|},$$

$$Y = X_1Y_2 - X_2Y_1 \equiv X_1Y_1 - X_1Y_1 \equiv 0 \pmod{|m|}.$$

Thus $\alpha\beta' = m(x + y\sqrt{d})$ with $x, y \in \mathbb{Z}$. Taking norms we get

$$m^2 = N(\alpha)N(\beta') = N(\alpha\beta') = N(m(x + y\sqrt{d})) = m^2(x^2 - dy^2).$$

Since $m \neq 0$ (why?), this gives

$$x^2 - dy^2 = 1.$$

Moreover $y \neq 0$: if $y = 0$ then the irrational part of Y, namely $X_1Y_2 - X_2Y_1$, would be zero, i.e., $\frac{X_1}{Y_1} = \frac{X_2}{Y_2}$, but this is impossible since $(X_1, Y_1) \neq (X_2, Y_2)$ are both coprime pairs: they cannot define the same rational number. We are done. □

Exercise: a) Show that the integral solutions to $x^2 - dy^2 = 1$ are precisely the norm one units in the ring of integers of $\mathbb{Q}(\sqrt{d})$.
b) Deduce from Theorem 14.7 that the norm one units in $\mathbb{Q}(\sqrt{d})$ form an infinite cyclic group.[14]
c) Let $a \in \mathbb{Z}^\bullet$. Show that the set of integral solutions to $x^2 - dy^2 = a$ is a **principal homogeneous space** under the group of solutions to $x^2 - dy^2 = 1$. In plainer terms, this means: if there are any solutions at all to $x^2 - dy^2 = a$, then by choosing any one solution one can define a bijection from the group of solutions to $x^2 - dy^2 = 1$ to the set of solutions to $x^2 - dy^2 = a$.
d) For which squarefree positive integers d does $x^2 - dy^2 = -1$ have any integral solutions?

Theorem 14.8. *Let $k \geq 3$ be an integer, d a positive integer which is not a kth power, and let a be a nonzero integer. Then there are only finitely many $(x, y) \in \mathbb{Z}^2$ such that $x^k - dy^k = a$.*

Proof. Let ζ_k be a primitive cube root of unity in $\mathbb{C}$, and suppose $x, y \in \mathbb{Z}$ are such that $x^k - dy^k = a$. Then

$$\left(\frac{x}{y} - d^{\frac{1}{k}}\right)\left(\frac{x}{y} - \zeta_k d^{\frac{1}{k}}\right)\cdots\left(\frac{x}{y} - \zeta_k^{k-1} d^{\frac{1}{k}}\right) = \frac{a}{y^k}. \tag{21}$$

Since for $0 < i < k$, $\zeta_k^i d^{\frac{1}{k}}$ is not real, all the factors in the left hand side of (21) are bounded away from zero, we find that

$$\left|\frac{x}{y} - d^{\frac{1}{k}}\right| \leq \frac{C}{y^k}$$

for some constant C. Because the approximation exponent of the degree k algebraic number $d^{\frac{1}{k}}$ is less than k – this follows from Roth's Theorem; in fact, it already follows from Thue's Theorem, but Liouville's Theorem is not enough. It follows that the equation $x^k - dy^k = a$ has only finitely many solutions. □

[14]This is, of course, the first nontrivial case of the Dirichlet Unit Theorem.

14.3. **The Roth-Ridout Theorem.**

In order to prove Siegel's Theorem we will want a generalization of Roth's Theorem to number fields and to approximation with respect to any norm $|\cdot|_v$ for $v \in \Sigma_K$.

Let K be a number field $v \in \Sigma_K$ and choose some extension of v to $\overline{K}$. We say $\alpha \in \overline{K}$ is (d, C, v)-approximable if there are infinitely many $x \in K$ such that

$$|x - \alpha|_v \leq \frac{C}{(H_K(x))^d};$$

here $H_K(x) = H([1, x])^{[K:\mathbb{Q}]}$ is the "relative height" of x.

We define the approximation exponent of α with respect to v as above.

Exercise: Check that this agrees with the case $(K, v) = (\mathbb{Q}, \infty)$.

Theorem 14.9. *(Roth-Ridout) For all $\alpha \in \overline{K}$, $d_v(\alpha) \leq 2$.*

Exercise: Find an analogue of Dirichlet's Theorem in this context.

Remark: In fact one can go further and consider a finite subset $S \subset \Sigma_K$. Instead of $|x - \alpha|$ we consider $\prod_{v \in S} \min(|x - \alpha|_v, 1)$.

14.4. **Siegel-Mahler S-Unit Theorem.**

Theorem 14.10. *(Siegel-Mahler) Let $K/\mathbb{Q}$ be a number field, let $S \subset \Sigma_K$ be a finite set of places of K including all the Archimedean places, and let $R = \mathbb{Z}_{K,S}$ be the corresponding S-integer ring. Then the* ***S-Unit Equation***

$$U + V = 1 \tag{22}$$

has only finitely many solutions $(U, V) \in (R^\times)^2$.

Proof. [HS, pp. 346-349].

□

15. Siegel's Theorems on Integral Points

15.1. **Statement of the Theorem.** One version of Siegel's Theorem – certainly an important and nontrivial version – simply states that if $y^2 = x^3 + Ax + B$ is an affine Weierstrass elliptic curve with $A, B \in \mathbb{Z}_K$, the ring of integers of some number field K, then there are only finitely many points $(x, y) \in \mathbb{Z}_K$ satisfying the Weierstrass equation. In fact this is already a deep and interesting result over $\mathbb{Q}$.

Over $\mathbb{Q}$, it is natural to compare this to the Lutz-Nagell Theorem, which says that torsion points on $y^2 = x^3 + Ax + B$ are integral points.

Here is the full extent of what Siegel proved.

Theorem 15.1. *(Big Siegel Theorem) Let K be a number field, let S be a finite set of places of K containing all the Archimedean places, and let $R = \mathbb{Z}_{K,S}$ be the ring of S-integers. Let $C_{/K}$ be a nice curve, and let $f \in K(C)$ be a nonconstant rational function. If C has genus zero, we assume that f has at least three distinct poles in $C(\overline{K})$. Then $\{P \in C(K) \mid f(P) \in R\}$ is finite.*

In these notes we will give a proof of Theorem 15.1 in the cases $g(C) = 0$ and $g(C) = 1$ relying on the (unproved, by us) Roth-Ridout Theorem and its consequence, the Siegel-Mahler S-Unit Theorem. The proof of Siegel's Theorem in higher genus – or at least, one modern proof exposed in [HS] – runs along broadly similar lines to the genus one Siegel Theorem but uses the Weak Mordell-Weil Theorem and some machinery of height functions on the **Jacobian** $J(C)$, an abelian variety of dimension $g(C)$. There are already enough technical details in the genus one case that we will leave the abelian variety case for another course.

15.2. **Siegel's Theorem in Genus Zero.**

Theorem 15.2. *(Genus Zero Siegel Theorem) Let K be a number field, let $S \subset \Sigma_K$ be a finite set of places containing all infinite places, and let $R = \mathbb{Z}_{K,S}$. Let $C_{/K}$ be a nice curve of genus zero, and let $\varphi \in K(C)$ be a nonconstant rational function such that $\#\{P \in C(\overline{K}) \mid \varphi(P) = \infty\} \geq 3$. Then*

$$\#\{P \in C(K) \mid \varphi(P) \in R\} < \infty.$$

Proof. If $C(K) = \varnothing$ the result holds trivially, so we may assume $C(K) \neq \varnothing$ and thus $C \cong_K \mathbb{P}^1$. We may write $\varphi = \frac{f(x,y)}{g(x,y)}$, where f, g are homogeneous of degree d without common roots in $\mathbb{P}^1(\overline{K})$. By enlarging K and S we may assume:
• $f = a(x - \alpha_1 y)^{d_1} \cdots (x - \alpha_m y)^{d_m}$,
$g = b(x - \beta_1 y)^{e_1} \cdots (x - \beta_n y)^{e_n}$,
• $\alpha_i, \beta_j \in R$,
• $a, b, \alpha_i - \beta_j \in R^\times$,
• $\beta_i - \beta_j \in R^\times$ for all $i \neq j$,
• R is a PID.
Suppose $\varphi(P) \in R$. Since R is a PID we may write $P = [X : Y]$ with $\gcd(X, Y) = 1$. Note that

$$(x - \alpha_i y) - (x - \beta_j y) = (\alpha_i - \beta_j)y,$$

$$-\beta_j(x - \alpha_i y) + \alpha_i(x - \beta_j)y = (\alpha_i - \beta_j)x.$$

Since $\alpha_i - \beta_j \in R^\times$ and $\gcd(x, y) = 1$, it follows that

$$\gcd(x - \alpha_i y, x - \beta_j y) = 1.$$

It follows that $f(x, y)$ and $g(x, y)$ are coprime. Since $\varphi(P) = \frac{f(x,y)}{g(x,y)} \in R$, $g(x, y) \mid f(x, y)$. Therefore $g(x, y) \in R^\times$ and hence $x - \beta_j y \in R^\times$. Because g has at least 3 distinct roots we may consider **Siegel's Identity**

$$\frac{\beta_2 - \beta_3}{\beta_2 - \beta_1} \cdot \frac{x - \beta_1 y}{x - \beta_3 y} - \frac{\beta_3 - \beta_1}{\beta_2 - \beta_1} \cdot \frac{x - \beta_2 y}{x - \beta_3 y} = 1.$$

Both terms on the left hand side are units, so by Siegel-Mahler they take on only finitely many values; in particular $\frac{x - \beta_1 \gamma}{x - \beta_3 \gamma}$ takes on only finitely many values. Fix a value $\gamma = \frac{x - \beta_1 y}{x - \beta_3 y}$; then

$$(1 - \gamma)x = (\beta_1 - \gamma\beta_3)y,$$

so we get only one point

$$P = [x : y] = [\beta_1 - \gamma\beta_3 : 1 - \gamma].$$

□

15.3. **v-adic Distance Functions.**

Let K be a field, and let $|\cdot|_v$ be a norm on K. If $V_{/K}$ is any variety, then $V(K)$ admits a natural topology, called the **v-adic topology**. This is defined as follows: on K^n we have a natural norm function, $|(x_1, \ldots, x_n)| = \max |x_i|_v$. This induces a metric and the metric induces a topology. For an affine subvariety $V \subset \mathbb{A}^n$ we endow $V(K) \subset \mathbb{A}^n$ with the subspace topology. (One does need to show that this is independent of the chosen affine embedding, and we omit this for now.) Finally, an arbitrary variety can be covered by affine open subvarieties. Given a set X, a family $\{Y_i\}_{i \in I}$ of subsets, and topologies τ_i on Y_i, there is a natural topology τ on X: a subset U of X lies in τ if for all $i \in I$, $U \cap Y_i \in \tau_i$.

If $(K, |\cdot|_v)$ is a normed field, then the norm can be extended in at least one way to the algebraic closure $\overline{K}$. We fix such an extension and continue to denote it by $|\cdot|_v$.

Let C/K be a nice curve. Fix a point $Q \in C(K)$. Choose a function $t_Q \in \overline{K}(C)$ which has a zero of order $e \geq 1$ at Q and no other zeros. (By Riemann-Roch, such a function exists for all $e \geq g(C)+1$.) For $P \in C(K)$, we define the **v-adic distance from P to Q** by

$$d_v(P, Q) = \min(|t_Q(P)|_v^{\frac{1}{e}}, 1).$$

If t_Q has a pole at P, weput $|t_Q(P)|_v = \infty$, so that $d_v(P, Q) = 1$.

Note: One should not read too much into this definition: in particular it certainly does depend upon the choice of t_Q so is in no way canonical. The point of d_v is to measure the rate of convergence of a sequence of points $\{P_n\}$ to a fixed point Q.

Proposition 15.3. *Let $Q \in C(\overline{K})$ and $F \in \overline{K}(C)$ be a function such that $F(Q) = 0$. Let $\{P_n\}$ be a sequence of points in $C(\overline{K})$ converging to Q. Then*

$$\lim_{n \to \infty} \frac{\log |F(P_n)|_v}{\log d_v(P_n, Q)} = \operatorname{ord}_Q(F).$$

Proof. Choose $t_Q \in \overline{K}(C)$ vanishing only at Q, and put $e = \operatorname{ord}_Q(t_Q)$, $f = \operatorname{ord}_Q(F)$. Then $\varphi = \frac{F^e}{t_Q^f}$ is regular and nonvanishing at Q so $|\varphi(P_n)|_v$ is bounded away from 0 and ∞ as $P_n \to Q$. Thus

$$\lim_{n \to \infty} \frac{\log |F(P_n)|_v}{\log d_v(P_n, Q)} = \lim_{n \to \infty} \frac{\log |F(P_n)|_v}{\log |t_Q(P_n)|_v^{\frac{1}{e}}} = \lim_{n \to \infty} \frac{\log |\varphi(P_n) t_Q(P_n)^f|_v^{\frac{1}{e}}}{\log |t_Q(P_n)|_v^{\frac{1}{e}}}$$

$$= \lim_{n \to \infty} \frac{\frac{1}{e} \log |\varphi(P_n)|}{\log |t_Q(P_n)|_v^{\frac{1}{e}}} + f = 0 + f = f.$$

□

Proposition 15.4. *Let C_1/K and C_2/K be curves, and let $\varphi : C_1 \to C_2$ be a finite morphism. Let $Q_1 \in C_1(\overline{K})$, and let e be the ramification index of φ at Q. Let $\{P_n\}$ be a sequence in $C_1(\overline{K})$ such that $P_n \to Q$. Then*

$$\lim_{n \to \infty} \frac{\log d_v(\varphi(P_n), \varphi(Q))}{\log d_v(P_n, Q)} = e.$$

Proof. Put $Q_2 = \varphi(Q_1)$. Let $t_1 \in \overline{K}(C_1)$ vanish only at Q_1 and put $e_1 = \operatorname{ord}_{Q_1}(t_1)$. Let $t_2 \in \overline{K}(C_2)$ vanish only at Q_2 and put $e_2 = \operatorname{ord}_{Q_2}(t_2)$. Then

$$\operatorname{ord}_{Q_1} t_2 \circ \varphi = e \operatorname{ord}_{Q_2} t_2 = ee_2.$$

So the functions $(t_2 \circ \varphi)^{e_1}$ and $t_2^{ee_2}$ vanish to the same order at Q_1, and

$$f = \frac{(t_2 \circ \varphi)^{e_1}}{t_1^{ee_2}} \in K_v(C_1)$$

is finite and nonzero at Q_1, so $\{|f(P_n)|_v\}$ is bounded away from 0 and ∞. Thus

$$\lim_{n\to\infty} \frac{\log d_v(\varphi(P_n), \varphi(Q))}{\log d_v(P_n, Q)} = \lim_{n\to\infty} \frac{\log |t_2(\varphi(P_n))|_v^{\frac{1}{e_2}}}{\log |t_1(P)|_v^{\frac{1}{e_1}}}$$

$$= \lim_{n\to\infty} \frac{e \log |t_1(P_n)|_v^{\frac{1}{e_1}} + (\frac{1}{e_1 e_2}) \log |f(P_n)|_v}{\log |t_1(P_n)|_v^{\frac{1}{e_1}}} = e.$$

□

Now let K is a number field, v a place of K and $|\cdot|_v$ is the corresponding normalized absolute value. As above we extend to a norm $|\cdot|_v$ on $\overline{K}$.

Theorem 15.5. *Let C/K be a curve, $v \in \Sigma_K$, $f \in K(C) \setminus K$ and let $Q \in C(\overline{K})$. Let $\{P_n\}$ be a sequence of distinct points in $C(K)$ converging v-adically to Q. Then*

$$\liminf_n \frac{\log d_v(P_n, Q)}{\log H(f(P_n))} \geq -2[K : \mathbb{Q}].$$

Proof. First note that $H_K(f(P)) = H_K(\frac{1}{f}(P)$, so by replacing f by $\frac{1}{f}$ if necessary we may assume $f(Q) \neq \infty$. Let $e = \operatorname{ord}(f - f(Q)) \geq 1$. Applying Proposition 15.3 with $F = f - f(Q)$ gives

$$\lim_{n\to\infty} \frac{\log |f(P_n) - f(Q)|_v}{d_v(P_n, Q)} = e.$$

It follows that

$$\liminf_n \frac{\log d_v(P_n, Q)}{\log H_K(f(P_n))} = \frac{1}{e} \liminf_n \frac{\log |f(P_n) - f(Q)|_v}{H_K(f(P_n))}$$

$$= \frac{1}{e} \liminf_n \frac{\log \left(H_K(f(P_n))^{2+\epsilon} |f(P_n) - f(Q)|_v\right)}{\log H_K(f(P_n))} - (2 + \epsilon).$$

By the Roth-Ridout Theorem, for all sufficiently large n we have

$$H_K(f(P_n))^{2+\epsilon} |f(P_n) - f(Q)|_v \geq 1.$$

It follows that

$$\liminf_n \frac{\log d_v(P_n, Q)}{\log H(f(P))} \geq \left(-\frac{2+\epsilon}{e}\right) [K : \mathbb{Q}].$$

Since $e \geq 1$ and this holds for all $\epsilon > 0$, the result follows. □

15.4. **Siegel's Theorem in Genus One.**

Theorem 15.6. *(Siegel) Let E/K be an elliptic curve over a number field with infinitely many K-rational points. Let $Q \in E(K)$, and let v be a place of K. Then*

$$\lim_{P \in E(K),\ h_x(P) \to \infty} \frac{\log d_v(P,Q)}{h_x(P)} = 0.$$

Proof. Choose a sequence $\{P_n\}$ of distinct points in $E(K)$ satisfying

$$\lim_{n \to \infty} \frac{\log d_v(P_n,Q)}{h_x(P_n)} = L = \liminf_P \frac{\log d_v(P,Q)}{h_x(P)}.$$

Since $d_v(P,Q) \leq 1$ and $h_x(P) \geq 0$ for all $P \in E(K)$, we have $L \leq 0$. Therefore it suffices to prove that $L \geq 0$.

Step 1: Let $m \in \mathbb{Z}^+$. By Weak Mordell-Weil, $E(K)/mE(K)$ is finite, and thus some coset of $mE(K)$ in $E(K)$ contains infinitely many $\{P_n\}$. After passing to a subsequence we may assume

$$P_n = [m]P_n' + R$$

with $P_n', R \in E(K)$ and R independent of n. Using the basic properties of height functions, we find that

$$m^2 h_x(P_n') = h_x([m]P_n') + O(1) = h_x(P_n - R) + O(1) \leq 2h_x(P_n) + O(1). \tag{23}$$

Step 2: If $\{P_n\}$ is bounded away from Q in the v-adic topology then $\log d_v(P_n,Q)$ is bounded and thus $L = 0$. Otherwise, by passing to a subsequence we may assume $P_n \to Q$ (all convergence is with respect to the v-adic topology). Then $[m]P_n' \to Q - R$, so at least one of the mth roots of $Q - R$ is an accumulation point of $\{P_n'\}$. Passing to a subsequence, there is a point $Q' \in E(\overline{K})$ such that $P_n' \to Q'$ and $Q = [m]Q' + R$. The map $E \to E$ defined by $P \mapsto [m]P + R$ is unramified, so by Proposition 15.4

$$\lim_{n \to \infty} \frac{\log d_v(P_n,Q)}{\log d_v(P_n',Q')} = 1. \tag{24}$$

Combining (23) and (24) we get

$$L = \lim_{n \to \infty} \frac{\log d_v(P_n,Q)}{h_x(P_n)} \geq \lim_{n \to \infty} \frac{\log d_v(P_n',Q')}{\frac{m^2}{2} h_x(P_n') + O(1)} = \lim_{n \to \infty} \frac{\log d_v(P_n',Q')}{\frac{m^2}{2} h_x(P_n')}. \tag{25}$$

(The numerators $\log d_v(\cdot,\cdot)$ are negative, which flips the inequality.) We now apply Theorem 15.5 to the sequence $\{P_n'\}$, getting

$$\liminf_n \frac{\log d_v(P_n',Q')}{h_x(P_n')} \geq -2[K:\mathbb{Q}]. \tag{26}$$

Combining (25) and (26) we deduce

$$L \geq \frac{-4[K:\mathbb{Q}]}{m^2}.$$

Since m was arbitrary, this shows $L \geq 0$. □

Exercise: a) Show that the case $K = \mathbb{Q}$, $v = \infty$ of Theorem 15.6 can be proved using the classical Roth Theorem rather than the Roth-Ridout Theorem.
b) Show that we need only the "qualitative classical Roth Theorem", namely that the supremum of all approximation exponents of real algebraic numbers is finite.
c) Of course Siegel in 1929 did not have even the qualitative classical Roth Theorem

but only the result that a real algebraic number of degree d has approximation exponent at most $2\sqrt{d}$. How do you deduce Theorem 15.6 from this?[15]

Corollary 15.7. *Let E/K be a Weierstrass elliptic curve. Then*

$$\#\{P \in E(K) \mid x(P) \in R\} < \infty.$$

Proof. We apply Theorem 15.6. Supppose there is a sequence of distinct points $\{P_n\}$ in $E(K)$ with $x(P_n) \in R$ for all n. Then

$$h(x(P_n)) = \sum_{v \in S} \log \max(1, |x(P_n)|_v)$$

since for all places $v \notin S$ we have $|x(P_n)|_v \leq 1$. After passing to a subsequence, there is at least one $v \in S$ such that for all $n \in \mathbb{Z}^+$,

$$h_x(P_n) \leq (\#S) \log |x(P_n)|_v.$$

In particular $|x(P_n)|_v \to \infty$, and thus $d_v(P_n, O) \to 0$. The function x has a pole of order 2 at O and no other poles, so we may take as our distance function

$$d_v(P_n, O) = \min(|x(P_i)|_v^{\frac{-1}{2}}, 1).$$

For all sufficiently large n, we have

$$\frac{\log d_v(P_n, O)}{h_x(P_n)} \leq \frac{-1}{2\#S},$$

contradicting Theorem 15.6. □

Corollary 15.8. *Let $C_{/K}$ be a nice genus one curve, let $f \in K(C) \setminus K$. Then*

$$\#\{P \in C(K) \mid f(P) \in R\} < \infty.$$

Proof. As usual, if it helps us to enlarge K and/or S, we are free to do so. We may thus assume that $C(K)$ contains a pole O of f. Taking O to be the identity element, we view (C, O) as an elliptic curve. Let x, y be coordinate functions for a Weierstrass model of (C, O) which we may of course take in short Weierstrass form:

$$y^2 = x^3 + Ax + B.$$

We have $f \in K(C) = K(x, y)$ and $[K(x, y) : K(x)] = 2$, so we can write

$$f(x, y) = \frac{\varphi(x) + \psi(x)y}{\eta(x)}$$

for $\varphi, \psi, \eta \in K[x]$. Since $\mathrm{ord}_O(x) = -2$, $\mathrm{ord}_O(y) = -3$ and $\mathrm{ord}_Q(f) < 0$, we have

$$2 \deg \eta < \max(2 \deg \varphi, 2 \deg \psi + 3). \tag{27}$$

Now observe the identity

$$(f\eta(x) - \varphi(x))^2 = (\psi(x)y)^2 = \psi(x)^2(x^3 + Ax + B).$$

Writing this out as a polynomial in x with $K[f]$-coefficients, we see that the highest power of x comes from one of the terms $f^2\eta(x)^2$, $\varphi(x)^2$ or $\psi(x)^2x^3$. By (27) the first of these has lower degree in x than the other two, while the leading terms of $\varphi(x)^2$ and $\psi(x)^2x^3$ cannot cancel, since the former has even degree and the latter has odd

[15] I don't know the answer. The point of this exercise is to underscore the fact that Siegel in 1929 had to work *much harder* to prove his theorem than we have here!

degree. We deduce that x satisfies a monic polynomial with $K[f]$-coefficients hence is integral over $K[f]$. Multiply through by a nonzero element of R to get a relation

$$a_0 x^N + a_{N-1}(f)x^{N-1} + \ldots + a_1(f)x + a_0(f) = 0$$

with $a_0 \in R^\bullet$ and $a_i(f) \in R[f]$ for $1 \leq i \leq N$. By enlarging S, we may assume $a_0 \in R^\times$; dividing by a_0 we may assume $a_0 = 1$.
Now suppose $P \in C(K)$ satisfies $f(P) \in R$. Then $P \neq O$, so P is not a pole of x, and the relation

$$x(P)^N + a_{N-1}(f(P))x(P)^{N-1} + \ldots + a_0(f(P)) = 0$$

show that $x(P)$ is integral over R. Since $x(P) \in K$ and R is integrally closed in K, it follows that $x(P) \in R$. Thus

$$\{P \in C(K) \mid f(P) \in R\} \subset \{P \in C(K) \mid x(P) \in R\},$$

so the finiteness of the first set follows from Corollary 15.7. □

15.5. **Siegel's Theorem for Hyperelliptic Curves.**

References

[AEC] J.H. Silverman, *The arithmetic of elliptic curves*. Second edition. Graduate Texts in Mathematics, 106. Springer, Dordrecht, 2009.

[Ba] M.H. Baker, *Algebaic Number Theory. Course Notes (Fall 2006), Math 8803, Georgia Tech*. available at `http://people.math.gatech.edu/~mbaker/pdf/ANTBook.pdf`.

[Ba36] R. Baer, *The subgroup of the elements of finite order of an abelian group*. Ann. of Math. 37 (1936), 766-781.

[BG] E. Bombieri and W. Gubler, *Heights in Diophantine Geometry*.

[Br10] F. Breuer, *Torsion bounds for elliptic curves and Drinfeld modules*. J. Number Theory 130 (2010), 1241-1250.

[CA] P.L. Clark, *Commutative algebra*, `http://math.uga.edu/~pete/integral.pdf`.

[CCS13] P.L. Clark, B. Cook and J. Stankewicz, *Torsion points on elliptic curves with complex multiplication*. International Journal of Number Theory, *to appear*.

[Cl09] P.L. Clark, *Elliptic Dedekind domains revisited*. Enseign. Math. (2) 55 (2009), 213-225.

[Co06] B. Conrad, *Chow's K/k-image and K/k-trace, and the Lang-Néron theorem*. Enseign. Math. 52 (2006), 37-108.

[CX08] P.L. Clark and X. Xarles, *Local bounds for torsion points on abelian varieties*. Canad. J. Math. 60 (2008), 532-555.

[Dy47] F.J. Dyson, *The approximation to algebraic numbers by rationals*. Acta Math. 79 (1947), 225-240.

[GoN] P.L. Clark, *Geometry of numbers with applications to nubmer theory*. `http://math.uga.edu/~pete/geometryofnumbers.pdf`

[H] R. Hartshorne, *Algebraic Geometry*.

[HS] M. Hindry and J.H. Silverman, *Diophantine geometry. An introduction*. Graduate Texts in Mathematics, 201. Springer-Verlag, New York, 2000.

[KCd] K. Conrad, *Galois descent*. Notes available at `http://www.math.uconn.edu/~kconrad/blurbs/galoistheory/galoisdescent.pdf`

[LALG] J.-P. Serre, *Lie algebras and Lie groups*. Lectures given at Harvard University. W. A. Benjamin, Inc., New York-Amsterdam 1965.

[LEC] J.W.S. Cassels, *Lectures on elliptic curves*. London Mathematical Society Student Texts, 24. Cambridge University Press, Cambridge, 1991.

[LMW] J.-P. Serre, *Lectures on the Mordell-Weil theorem*. Aspects of Mathematics, E15. Friedr. Vieweg & Sohn, Braunschweig, 1989.

[LN59] S. Lang and A. Néron, *Rational points of abelian varieties over function fields*. Amer. J. Math. 81 (1959), 95-118.

[Li44] J. Liouville, *Sur les classes très étendues de quantités dont la valeur n'est ni algébrique, ni même réductible à des irrationelles algébriques*. C.R. Acad. Sci. Paris 18 (1844), 883-885; 910-911.

[Ma33] K. Mahler, *Zur Approximation algebraischer Zahlen*. Math. Ann. 107 (1933), 691–730.
[Ma97] Yu. I. Manin, *Mordell-Weil problem for cubic surfaces*. Advances in mathematical sciences: CRM's 25 years (Montreal, PQ, 1994), 313-318, CRM Proc. Lecture Notes, 11, Amer. Math. Soc., Providence, RI, 1997.
[Ma77] B.C. Mazur, *Modular curves and the Eisenstein ideal*. Inst. Hautes Études Sci. Publ. Math. No. 47 (1977), 33-186.
[Ma78] B.C. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*. Invent. Math. 44 (1978), 129-162.
[Me96] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*. Invent. Math. 124 (1996), 437-449.
[Mo22] L.J. Mordell, *On the rational solutions of the indeterminate equations of the third and fourth degrees*. Proc. Cambridge Philos. Soc. 21 (1922), 179–192.
[N] J. Neukirch, *Algebraic Number Theory*.
[NT2] P.L. Clark, *Algebraic Number Theory II: Valuations, Local Fields and Adeles*. Notes available at `http://math.uga.edu/~pete/8410FULL.pdf`
[Pa99] P. Parent, *Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres*. J. Reine Angew. Math. 506 (1999), 85-116.
[Ri58] D. Ridout, *The p-adic generalization of the Thue-Siegel-Roth theorem*. Mathematika 5 (1958), 40-48.
[Ro55] K.F. Roth, *Rational approximations to algebraic numbers*. Mathematika 2 (1955), 120; corrigendum, 168.
[Rü87] H.-G. Rück, *A note on elliptic curves over finite fields*. Math. Comp. 49 (1987), 301-304.
[Si21] C.L. Siegel, *Approximation algebraischer Zahlen*. Math. Z. 10 (1921), 173-213.
[Ta66] J.T. Tate, *Endomorphisms of abelian varieties over finite fields*. Invent. Math. 2 (1966), 134-144.
[Th09] A. Thue, *Über Annäherunswerte Algebraischer Zahlen*. J. Reine Anew. Math. 135 (1909), 284–305.
[Wa69] W.C. Waterhouse, *Abelian varieties over finite fields*. Ann. Sci. École Norm. Sup. 2 (1969), 521-560.
[We29] A. Weil, *L'arithmétique sur les courbes algébriques*. Acta Math 52 (1929), 281–315.