

M4P32 Number Theory: Elliptic Curves

Lectured by Prof Toby Gee
Typed by David Kurniadi Angdinata

Autumn 2019

Syllabus

Contents

1	Introduction	3
2	The p-adic numbers	4
3	Basic algebraic geometry	9
4	Plane conics	12
5	The Hasse principle for smooth plane conics over \mathbb{Q}	13
A	Diagonalisation of quadratic forms	16

1 Introduction

Lecture 1
Thursday
03/10/19

The following are books.

- J W S Cassels, Lectures on elliptic curves, 1991
- J H Silverman, The arithmetic of elliptic curves, 1986
- J H Silverman and J Tate, Rational points on elliptic curves, 1992

Note that there are a lot of books on elliptic curves out there, and a lot of them are not relevant to this course, so either different topics, or they will be too advanced. Also, about half of this course will not actually be on elliptic curves. We are going to start off by looking at conics, which are simpler but are a good place to start in order to build intuition and technique. As explained below, we will be essentially following Cassels, although there is quite a lot of material that we will not cover, and our treatment of a 2-descent, that is our method for computing the rank of an elliptic curve over \mathbb{Q} , will be different. The overall aim of this course is to learn more about solving polynomial equations in \mathbb{Z} or \mathbb{Q} . For example,

$$x^2 + y^2 = 5, \quad y^2 = x^3 - x, \quad x^4 + y^4 = 17.$$

Let k be a field, such as \mathbb{Q} , \mathbb{R} , \mathbb{C} , the field of p elements \mathbb{F}_p , or the p -adic numbers \mathbb{Q}_p , and let its polynomial ring be $k[x_0, \dots, x_n]$. A **monomial** is a term $x_0^{a_0} \dots x_n^{a_n}$, which has degree $a_0 + \dots + a_n$. The **degree** of a polynomial is the maximal degree of a monomial occurring in it.

Example. $x_1^5 + x_2x_3 + x_{10}x_{11}^5$ has degree six.

Equations in one variable are easy to solve over \mathbb{Q} .

Example. Let $3x^5 - 9x^3 + x^2 + \frac{148}{81} = 0$, so $243x^5 - 729x^3 + 81x^2 + 148 = 0$. If $x = a/b$ with $(a, b) = 1$, we need $243a^5 - 729a^3b^2 + 81a^2b^3 + 148b^5 = 0$. Then $b \neq 0$, so $a \neq 0$, so $a^2 \mid 148$, so $a \mid 2$, so $a = \pm 1, \pm 2$. Similarly $b^2 \mid 243$, so $b \mid 9$, so $b = \pm 1, \pm 3, \pm 9$. Check each of these, and $x = \frac{2}{3}$.

More than two variables, over \mathbb{Q} , is hopeless, so let x and y be two variables.

- Degree one is very easy, since $ax + by + c = 0$ for $b \neq 0$ gives $y = -c/b - (a/b)x$.
- Degree two and three are in this course.
- Degree four can be reduced to degree three.

Theorem 1.1 (Mordell's conjecture and Falting's theorem). *A general equation in two variables of degree greater than four has only finitely many solutions over \mathbb{Q} .*

General equations are nonsingular, so $(x - y)(x^{100} + 10y + 1) = 0$ and $x^{73} - y^{109} = 0$ are not general.

Example 1.2. Let $x^2 + y^2 = c$ for $c \in \mathbb{Q}$.

- $x^2 + y^2 = -1$ has no solutions in \mathbb{R} .
- $x^2 + y^2 = 0$ has $(x, y) = (0, 0)$ in \mathbb{R} .
- $x^2 + y^2 = 1$ has infinitely many solutions $(x, y) = (\frac{3}{5}, \frac{4}{5}), (\frac{5}{13}, \frac{12}{13}), \dots$, since $(a/c)^2 + (b/c)^2 = 1$ gives $a^2 + b^2 = c^2$, which has infinitely many solutions $(3, 4, 5), (5, 12, 13), \dots$.
- $x^2 + y^2 = 3$ has no solutions in \mathbb{Q} , since $a^2 + b^2 = 3c^2$ has no solutions for $a, b, c \in \mathbb{Z}$ and $c \neq 0$. Suppose a, b, c is such a solution. Then $a^2 + b^2 \equiv 0 \pmod{3}$. But all squares are 0 or 1 modulo 3, so $a \equiv b \equiv 0 \pmod{3}$. Write $a = 3A$ and $b = 3B$ gives $3(A^2 + B^2) = c^2$, so $3 \mid c$. Write $c = 3C$ gives $A^2 + B^2 = 3C^2$, a contradiction, by induction on the biggest power of 3 dividing c . Next week $x^2 + y^2 = 3$ has no solutions in \mathbb{Q}_3 .

Example 1.3. $x^2 + 2y^2 = 6$ has $(x, y) = (2, 1)$, which has line $y - 1 = m(x - 2)$, so

$$(2m(x - 2))^2 + x^2 - 6 = 0 \implies (2m^2 + 1)x^2 + (4m - 8m^2)x + 2(1 - 2m)^2 - 6 = 0.$$

The sum of the roots of $ax^2 + bx + c$ is $-b/a$. So the second root, other than $x = 2$ and $y = 1$, is

$$x = \frac{8m^2 - 4m}{2m^2 + 1} - 2 = \frac{4m^2 - 4m - 2}{2m^2 + 1}, \quad y = \frac{-2m^2 - 4m + 1}{2m^2 + 1}.$$

2 The p -adic numbers

Lecture 2
Monday
07/10/19

Definition 2.1. A **norm** on a field k is a function $|\cdot| : k \rightarrow \mathbb{R}$ such that

1. $|x| \geq 0$ with equality if and only if $x = 0$,
2. $|xy| = |x| \cdot |y|$, and
3. $|x + y| \leq |x| + |y|$.

2 implies that $|1| = |-1| = 1$. So $|x| = |-x|$.

Example. Usual absolute value on \mathbb{R} , that is

$$|x| = \begin{cases} x & x \geq 0 \\ -x & x < 0 \end{cases}.$$

Remark 2.2. Define

$$\begin{aligned} d(\cdot, \cdot) &: k^2 \longrightarrow \mathbb{R} \\ (x, y) &\longmapsto |x - y| \end{aligned}$$

then d is a metric on k^2 . Not every metric comes from a norm.

Definition 2.3. Let $k = \mathbb{Q}$. Then the **p -adic norm** is defined by

$$\begin{aligned} |\cdot|_p &: \mathbb{Q} \longrightarrow \mathbb{R} \\ x &\longmapsto \begin{cases} 0 & x = 0 \\ p^{-n} & x = p^n \frac{a}{b}, n \in \mathbb{Z}, (p, a) = (p, b) = (a, b) = 1 \end{cases}. \end{aligned}$$

Lemma 2.4. $|\cdot|_p$ is a norm, and in fact

$$3^*. |x + y| \leq \max(|x|, |y|).$$

Proof. Without loss of generality, $x, y \in \mathbb{Z}$. Also we may assume $x, y, x + y \neq 0$. Then 3^* is equivalent to, if $p^n \mid x$ and $p^n \mid y$, then $p^n \mid (x + y)$. \square

Definition 2.5. We say that 3^* is the **ultrametric inequality**. If $|\cdot|$ satisfies 3^* , we say that $|\cdot|$ is **non-archimedean**.

We have infinitely many norms on \mathbb{Q} , the one from \mathbb{R} , and the p -adic norm $|\cdot|_p$ for each prime p . Say that two norms $|\cdot|_1$ and $|\cdot|_2$ on k are **equivalent** if there exists $\alpha > 0$ such that $|\cdot|_1 = |\cdot|_2^\alpha$.

Exercise. Check two norms are equivalent if and only if the corresponding metrics give the same topology on k .

Theorem 2.6. Any norm on \mathbb{Q} is equivalent to exactly one of

- the archimedean norm coming from \mathbb{R} ,
- a norm $|\cdot|_p$ for some uniquely determined p , or
- the discrete norm $|x| = 1$ if $x \neq 0$.

Lemma 2.7. If $|\cdot|$ is non-archimedean and $|x| \neq |y|$, then $|x + y| = \max(|x|, |y|)$.

Proof. Without loss of generality $|x| > |y|$. Write $x = (x + y) + (-y)$, so that 3^* gives us

$$|x| \leq \max(|x + y|, |-y|) \leq \max(|x|, |y|, |-y|) = |x|.$$

So $|x| = \max(|x + y|, |y|)$. But $|x| > |-y| = |y|$, so $|x| = |x + y|$. \square

Exercise 2.8. Check Lemma 2.7 for $|\cdot|_p$ using the definition.

Recall that

- a sequence (x_n) in k is **Cauchy** if for all $\epsilon > 0$ there exists N such that $m, n \geq N$ implies that $|x_m - x_n| < \epsilon$, and
- a sequence (x_n) **converges** to $x \in k$ if for all $\epsilon > 0$ there exists M such that $n \geq M$ implies that $|x_n - x| < \epsilon$.

(x_n) converges implies that (x_n) is Cauchy, but in general (x_n) is Cauchy does not imply that (x_n) converges.

Example.

- \mathbb{R} is complete.
- \mathbb{Q} is not complete with respect to the usual archimedean norm. For example, $3, 3.1, \dots \rightarrow \pi \notin \mathbb{Q}$.

Example 2.9. Let $p = 2$. Then $(x_n) = 3, 33, \dots$ is Cauchy with respect to $|\cdot|_2$, and $x_n = \frac{10^n - 1}{3} \rightarrow -\frac{1}{3}$ as $n \rightarrow \infty$ because $|x_n + \frac{1}{3}|_2 = |\frac{10^n}{3}|_2 = |2^n \frac{5^n}{3}|_2 = 2^{-n} \rightarrow 0$.

Example 2.10. Let $x_n = 5^{2^n}$. If $p = 5$, then $x_n \rightarrow 0$, since $|5^{2^n}|_5 = 5^{-2^n} \rightarrow 0$ as $n \rightarrow \infty$. If $p = 2$, then $x_n \rightarrow 1$ as $n \rightarrow \infty$, since $(1 + y)^2 = 1 + 2y + y^2$.¹

Example. A Cauchy sequence in \mathbb{Q} for $|\cdot|_3$ which does not converge. Take a sequence converging to $\sqrt{7}$. That is, take (x_n) such that $x_n^2 - 7 \rightarrow 0$, that is $|x_n^2 - 7|_3 \rightarrow 0$ as $n \rightarrow \infty$. For example, take $x_n \in \mathbb{Z}$, chosen such that $x_n^2 \equiv 7 \pmod{3^n}$. For example,

$$x_1 = 1, \quad x_2 = 4, \quad x_3 = 13, \quad \dots$$

Exercise 2.11. If $p > 2$ and $t \in \mathbb{Z}$ is not a square but is a quadratic residue modulo p , that is there exists y such that $y^2 \equiv t \pmod{p}$, then there exists a Cauchy sequence (x_n) in \mathbb{Q} with $x_n^2 \rightarrow t$ as $n \rightarrow \infty$, such as $t = 1 - p$. If $p = 2$, then $t = -7$ works.

\mathbb{Q} is not complete with respect to any $|\cdot|_p$. Let k be a field and $|\cdot|$ be non-archimedean. Let

$$R = \{\text{Cauchy sequences in } k\},$$

where $(x_n) + (y_n) = (x_n + y_n)$ and $(x_n)(y_n) = (x_n y_n)$. Let

$$I = \{(x_n) \mid x_n \rightarrow 0 \text{ as } n \rightarrow \infty\}.$$

Exercise.

- Check that I is an ideal in R .
- If $(x_n) \notin I$, then there exists N such that $n \geq N$ implies that $x_n \neq 0$. Show that furthermore the sequence (y_n) defined by

$$y_n = \begin{cases} 0 & n < N \\ \frac{1}{x_n} & n \geq N \end{cases}$$

is Cauchy, and $x_n y_n = 1$ for all $n \geq N$, so $(x_n)(y_n) - 1 \in I$.

That is, I is a maximal ideal of R , so $\widehat{k} = R/I$ is a field. There is a natural map

$$\begin{aligned} k &\longrightarrow \widehat{k} \\ x &\longmapsto (x)_{n \geq 1} \end{aligned}.$$

This is an injection. Call \widehat{k} the **completion** of k . The norm $|\cdot|$ extends to \widehat{k} by defining

$$|(x_n)| = \lim_{n \rightarrow \infty} |x_n|.$$

Exercise.

- Check that this is defined, and is a norm.
- Check that if $x_n \not\rightarrow 0$, then $|x_n|$ is eventually constant, by using Lemma 2.7.

¹Exercise

Lemma 2.12. k is dense in \widehat{k} .

Proof. Need to show that if $x \in \widehat{k}$ and $\epsilon > 0$, then there exists $y \in k$ such that $|x - y| < \epsilon$. Write $x = (x_n)$ for $x_n \in k$, and choose N such that if $m, n \geq N$, then $|x_m - x_n| < \epsilon$. Then take $y = x_N$. Then $|x - y| = \lim_{n \rightarrow \infty} |x_n - x_N| < \epsilon$. \square

Lemma 2.13. \widehat{k} is complete.

Proof. Let (x_n) be a Cauchy sequence in \widehat{k} , so x_n is itself an equivalence class of Cauchy sequences in k . By Lemma 2.12, for each $n \geq 1$ there exists $y_n \in k$ such that $|x_n - y_n| < \frac{1}{n}$. Claim that $y = (y_n)$ is a Cauchy sequence, and $x_n \rightarrow y$ as $n \rightarrow \infty$. Since

$$|y_m - y_n| \leq |y_m - x_m| + |x_m - x_n| + |x_n - y_n| < \frac{1}{m} + \frac{1}{n} + |x_m - x_n|,$$

and (x_n) is Cauchy, so (y_n) is Cauchy. Then

$$|x_n - y| \leq |x_n - y_n| + |y_n - y| < \frac{1}{n} + |y_n - y|.$$

Need to check that $|y_n - y| \rightarrow 0$ as $n \rightarrow \infty$, which is what we did in the proof of Lemma 2.12. \square

Definition 2.14. Let $k = \mathbb{Q}$ and $|\cdot| = |\cdot|_p$. Write the field of p -adic numbers \mathbb{Q}_p for \widehat{k} , the completion of \mathbb{Q} with respect to $|\cdot|_p$, and the ring of p -adic integers

$$\mathbb{Z}_p = \left\{ x \in \mathbb{Q}_p \mid |x|_p \leq 1 \right\} \subset \mathbb{Q}_p.$$

By construction or definition, $\mathbb{Q} \subset \mathbb{Q}_p$, and $\mathbb{Z} \subset \mathbb{Z}_p$.

Exercise 2.15. Show that \mathbb{Z}_p is a subring of \mathbb{Q}_p . More generally, if k is any non-archimedean field, then

$$\{x \in k \mid |x| \leq 1\}$$

is a subring of k .

Note. $\frac{1}{p} \notin \mathbb{Z}_p$, and $\left| \frac{1}{p} \right|_p = p > 1$. In fact $\mathbb{Q}_p = \mathbb{Z}_p \left[\frac{1}{p} \right]$, the field of fractions of \mathbb{Z}_p .

Definition 2.16. If k is any field with a norm $|\cdot|$, then we write

$$\sum_{n=1}^{\infty} a_n = \lim_{m \rightarrow \infty} \sum_{n=1}^m a_n,$$

if this limit exists.

Lemma 2.17. If k is non-archimedean, and $t_1, \dots, t_n \in k$, then

$$\left| \sum_{i=1}^n t_i \right| \leq \max_{1 \leq i \leq n} |t_i|.$$

In particular if $|t_i| \leq R$ for all i , then $|\sum_{i=1}^n t_i| \leq R$.

Proof. Induction on n , where $n = 2$ is 3^* . \square

Corollary 2.18. A sequence (t_n) is Cauchy if and only if $|t_n - t_{n+1}| \rightarrow 0$ as $n \rightarrow \infty$.

Proof. If $m > n$, then

$$t_m - t_n = (t_m - t_{m-1}) + \dots + (t_{n+1} - t_n),$$

and use Lemma 2.17. \square

Lemma 2.19. *If k is complete non-archimedean, such as $k = \mathbb{Q}_p$, then $\sum_{n=1}^{\infty} x_n$ converges if and only if $x_n \rightarrow 0$ as $n \rightarrow \infty$. If $|x_n| \leq R$ and $x_n \rightarrow 0$ then $|\sum_{n=1}^{\infty} x_n| \leq R$.*

Proof. $\sum_{n=1}^{\infty} x_n$ converges if and only if $(\sum_{n=1}^m x_n)_{m \geq 1}$ converges. Since k is complete, this is if and only if $(\sum_{n=1}^m x_n)_{m \geq 1}$ is Cauchy. By Corollary 2.18, this is if and only if $x_{m+1} \rightarrow 0$. The final statement then follows from Lemma 2.17. \square

Lemma 2.20. *If $a_n \in \mathbb{Z}$ then $\sum_{n=0}^{\infty} a_n p^n$ converges in \mathbb{Q}_p . If $a_n = 0$ for $n < T$ and $a_T \neq 0$, and $p \nmid a_T$, then $|\sum_{n=0}^{\infty} a_n p^n|_p = p^{-T}$.*

Proof. Since $a_n \in \mathbb{Z}$,

$$|a_n p^n|_p = |a_n|_p \cdot |p^n|_p \leq |p^n|_p = p^{-n} \rightarrow 0.$$

Furthermore $|a_T p^T|_p = p^{-T}$ and $|a_n p^n|_p \leq p^{-T-1}$ if $n \geq T+1$, so $|\sum_{n=T+1}^{\infty} a_n p^n|_p \leq p^{-T-1}$, so

$$\left| a_T p^T + \sum_{n=T+1}^{\infty} a_n p^n \right|_p = p^{-T},$$

by Lemma 2.7. \square

Proposition 2.21.

1. If $a_n \in \{0, \dots, p-1\}$, then $\sum_n a_n p^n$ converges to an element of \mathbb{Z}_p . Furthermore if

$$\sum_n a_n p^n = \sum_n b_n p^n, \quad b_n \in \{0, \dots, p-1\},$$

then $a_n = b_n$ for all n .

2. If $\alpha \in \mathbb{Z}_p$ then there exists (a_n) as in 1 such that $\alpha = \sum_n a_n p^n$.

Proof.

1. Lemma 2.20 gives convergence. Suppose that T is minimal such that $a_T \neq b_T$, then by Lemma 2.20, $|\sum_n (a_n - b_n) p^n|_p = p^{-T}$. In particular $\sum_n (a_n - b_n) p^n \neq 0$.
2. By construction, \mathbb{Q} is dense in \mathbb{Q}_p . So there exists $\beta \in \mathbb{Q}$ such that $|\alpha - \beta|_p < 1$. Since $|\alpha|_p \leq 1$, we have $|\beta|_p \leq 1$, so if $\beta = r/s$ with $(r, s) = 1$, then $p \nmid s$. So there exists $\gamma \in \mathbb{Z}$ with $|\gamma - \beta|_p < 1$, if and only if $s\gamma - r \equiv 0 \pmod{p}$, which has solutions because $(s, p) = 1$. There exists $a_0 \in \{0, \dots, p-1\}$ such that $|\gamma - a_0|_p < 1$, so

$$|\alpha - a_0|_p \leq \max(|\alpha - \beta|_p, |\beta - \gamma|_p, |\gamma - a_0|_p) < 1.$$

Then $|(\alpha - a_0)/p|_p \leq 1$, that is $(\alpha - a_0)/p \in \mathbb{Z}_p$. Repeating the argument, there exists $a_1 \in \{0, \dots, p-1\}$ such that $|(\alpha - a_0)/p - a_1|_p < 1$, that is $(\alpha - a_0 - a_1 p)/p^2 \in \mathbb{Z}_p$. By induction, we find a_0, a_1, \dots such that $|\alpha - (a_0 + \dots + a_n p^n)|_p \leq p^{-(n+1)}$. So $\alpha = \sum_{n=0}^{\infty} a_n p^n$. \square

Corollary 2.22. *Any element α of \mathbb{Q}_p can be uniquely written as*

$$\alpha = \sum_{n \geq -T} a_n p^n, \quad a_{-T} \neq 0, \quad a_n \in \{0, \dots, p-1\}.$$

Proof. If $|\alpha|_p = p^T$, then $|p^T \alpha|_p = 1$, so $p^T \alpha \in \mathbb{Z}_p$, and the claim follows from Proposition 2.21.2 applied to $p^T \alpha$. \square

Corollary 2.23. \mathbb{Z} is dense in \mathbb{Z}_p .

Proof. If $\alpha \in \mathbb{Z}_p$, write $\alpha = \sum_n a_n p^n$. Then

$$|\alpha - (a_0 + \dots + a_m p^m)|_p \leq p^{-(m+1)},$$

and $a_0 + \dots + a_m p^m \in \mathbb{Z}$. \square

For all $m \geq 1$, there is a surjective ring homomorphism

$$\begin{aligned} \mathbb{Z}_p &\longrightarrow \mathbb{Z}/p^m\mathbb{Z} \\ \sum_{n=0}^{\infty} a_n p^n &\longmapsto \sum_{n=0}^{m-1} a_n p^n. \end{aligned}$$

In fact

$$\mathbb{Z}_p/p^m\mathbb{Z}_p = \mathbb{Z}/p^m\mathbb{Z}, \quad \mathbb{Z}_p = \varprojlim_m \mathbb{Z}/p^m\mathbb{Z}.$$

Lemma 2.24.

$$\mathbb{Z}_p^\times = \left\{ x \in \mathbb{Z}_p \mid |x|_p = 1 \right\}.$$

Proof. If $|x|_p = 1$ then $x \neq 0$, and so $x^{-1} \in \mathbb{Q}_p$, and $|x^{-1}|_p = 1/|x|_p = 1$, so $x^{-1} \in \mathbb{Z}_p$. Conversely if $x \in \mathbb{Z}_p^\times$ then there exists $y \in \mathbb{Z}_p$ such that $xy = 1$, so $|x|_p|y|_p = 1$. But $|x|_p, |y|_p \leq 1$, so $|x|_p = |y|_p = 1$. \square

Now $\langle p \rangle \subset \mathbb{Z}_p$ is a maximal ideal, because $\mathbb{Z}_p/\langle p \rangle = \mathbb{Z}/p\mathbb{Z}$ is a field. Since $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \langle p \rangle$ by Lemma 2.24, $\langle p \rangle$ is the unique maximal ideal of \mathbb{Z}_p , that is \mathbb{Z}_p is a local ring. In fact it is a discrete valuation ring.

Notation. A unit of \mathbb{Q}_p is a unit in \mathbb{Z}_p , that is an element of $|\cdot|_p = 1$.

Corollary 2.25. Every element of \mathbb{Q}_p other than zero is uniquely of the form $p^n u$ for $n \in \mathbb{Z}$ and u is a unit.

Proof. If $\alpha \in \mathbb{Q}_p$ and $\alpha \neq 0$, write $|\alpha|_p = p^{-n}$ for $n \in \mathbb{Z}$, and set $u = \alpha p^{-n}$. \square

Hensel's lemma is Newton-Raphson in \mathbb{Q}_p . A reminder that if k is any field, and $f(X) \in k[X]$, then we can define $f'(X), f''(X), \dots$ formally by $\frac{d}{dx}(X^n) = nX^{n-1}$.

Theorem 2.26 (Hensel's lemma). Let k be a non-archimedean field with norm $|\cdot|$ and $R = \{x \in k \mid |x| \leq 1\}$. For example, $k = \mathbb{Q}_p$, $|\cdot| = |\cdot|_p$, and $R = \mathbb{Z}_p$. Suppose $f \in R[X]$, and $t_0 \in R$ such that $|f(t_0)| < |f'(t_0)|^2$. Then there exists a unique $t \in R$ such that

$$f(t) = 0, \quad |t - t_0| < |f'(t_0)|.$$

Furthermore

$$|f'(t)| = |f'(t_0)|, \quad |t - t_0| = \frac{|f(t_0)|}{|f'(t_0)|}.$$

Proof. Construct a Cauchy sequence t_0, t_1, \dots by

$$t_{n+1} = t_n - \frac{f(t_n)}{f'(t_n)}.$$

It turns out that $|f'(t_n)| = |f'(t_0)|$, so

$$\left| \frac{f(t_n)}{f'(t_0)} \right| = \left| \frac{f(t_n)}{f'(t_n)} \right| = |t_{n+1} - t_n| \rightarrow 0,$$

that is $f(t_n) \rightarrow 0$, that is $f(t) = 0$. \square

Lemma 2.27. If $f(X) \in R[X]$ has a simple root $X = t \in R$, then for any $t_0 \in k$ with $|t - t_0| < |f'(t)|$, we have

$$|f'(t)| = |f'(t_0)|, \quad |f(t_0)| < |f'(t_0)|^2.$$

Exercise 2.28. The equation $X^2 = 7$ has a solution in \mathbb{Z}_3 . Take $f(X) = X^2 - 7$. Then $f'(X) = 2X$. So $|f'(X)|_3 = |X|_3$. So we need to find t_0 such that $|t_0^2 - 7|_3 < |t_0|_3^2$. For example, choose $t_0 \in \mathbb{Z}$ such that $3 \nmid t_0$ and $t_0^2 \equiv 7 \pmod{3}$, for example $t_0 = 1$. Hensel's lemma implies that there exists a unique $t \in \mathbb{Z}_3$ such that $t^2 = 7$ and $|t - 1|_3 < 1$, that is $t \equiv 1 \pmod{3}$. In the same way, show that there exists a unique $s \in \mathbb{Z}_3$ such that $s^2 = 7$ and $s \equiv 2 \pmod{3}$. In fact $s = -t$, since $(-t)^2 = t^2$ and $X^2 - 7 = (X - t)(X + t)$.

Corollary 2.29. Let $u \in \mathbb{Z}_p^\times$. If $p > 2$, then u is a square if and only if it is a square modulo p . If $p = 2$, then u is a square if and only if it is a square modulo 8, if and only if $u \equiv 1 \pmod{8}$.

Proof. Exercise. ² \square

²Exercise

3 Basic algebraic geometry

Lecture 5
Monday
14/10/19

An affine **algebraic curve** over k is an equation

$$f(x, y) = 0, \quad 0 \neq f \in k[x, y].$$

The **degree** $n = \deg f \in \mathbb{N}_{>0}$ of this curve is the total degree, so if $f(x, y) = \sum_{i,j=0}^n a_{ij}x^i y^j$, then

$$\deg f = \max \{i + j \mid a_{ij} \neq 0\}.$$

Algebraic curves of degree one are **lines**. Algebraic curves of degree two are **conics**. Two curves $x = 0$ and $y = f(x)$ for $f(x) \in k[x]$ have intersection points the zeroes of $f(x)$, and a non-zero polynomial of degree n has n roots, but $f(x) = x^2 + 1$ has no real zeroes, so need to work over \mathbb{C} or some algebraically closed field.

Definition 3.1. A field k is **algebraically closed** if any non-zero polynomial $f(x) \in k[x]$ has a zero in k .

By induction on the degree,

$$f(x) = a_n \prod_{j=1}^n (x - \alpha_j), \quad a_n, \alpha_j \in k.$$

Bézout's theorem states that two algebraic curves of degree d_1 and d_2 respectively have $d_1 d_2$ common points.

- We need to assume that k is algebraically closed. For example, the **fundamental theorem of algebra**, by Gauss, states that \mathbb{C} is algebraically closed.
- We need to count multiplicities. There is a definition given for multiplicity. For example, if $\underline{0} = (0, 0)$ is the intersection point of two curves $f(x, y) = 0$ and $g(x, y) = 0$ for $f, g \in \mathbb{C}[x, y]$, so $f(\underline{0}) = g(\underline{0}) = 0$, then the **multiplicity** at $\underline{0}$ is

$$\dim_{\mathbb{C}} \mathbb{C}[[x, y]] / \langle f, g \rangle < \infty.$$

- We need to enlarge the plane to contain points at infinity. For example, the **real projective plane**

$$\mathbb{P}^2(\mathbb{R}) = \mathbb{R}^2 \cup \{\text{points at infinity}\}$$

is the equivalence classes of affine lines through \mathbb{R}^2 modulo parallelism, where if $l_1, l_2 \in \mathbb{R}^2$, then l_1 is parallel to l_2 if and only if $l_1 \cap l_2 = \emptyset$ or $l_1 = l_2$, which is an equivalence relation. There is an injection from points in $\{y = 1\}$ to affine lines through $\underline{0}$, and for any class of parallel affine lines on $\{y = 1\}$ there exists a unique line going through $\underline{0}$ and parallel to these lines, so

$$\mathbb{P}^2(\mathbb{R}) = \{\text{lines from } \{y = 1\}\} \cup \{\text{lines parallel to } \{y = 1\}\}.$$

This collection of subsets are called **projective lines**, which are two-dimensional subspaces in \mathbb{R}^3 , and points are one-dimensional subspaces in \mathbb{R}^3 . The set of points at infinity is a projective line, and any affine line $l \subset \mathbb{R}^2$ gives a projective line $l^\# = l \cup \{\text{parallelism class}\}$. Thus any two different projective lines intersect in exactly one point, and this definition makes sense for any field.

The following is an equivalent description of $\mathbb{P}^2(k)$. Let k be any field. Then

$$\mathbb{P}^2(k) = k^3 \setminus \{\underline{0}\} / \sim$$

is the equivalence classes (x_0, x_1, x_2) such that $x_i \in k$ are not all zero modulo \sim , where $\underline{x} \sim \underline{y}$ if and only if $\underline{x} = \lambda \cdot \underline{y}$ for $\lambda \in k \setminus \{0\} = k^*$.

Definition 3.2. The **projective n -space** is

$$\mathbb{P}^n(k) = k^{n+1} \setminus \{\underline{0}\} / \sim.$$

Notation 3.3. The **homogeneous coordinates** $[x_0 : \cdots : x_n]$ is an equivalence class of non-zero vectors in k^{n+1} modulo \sim , so

$$\mathbb{P}^n(k) = \{[x_0 : \cdots : x_n] \mid x_i \in k \text{ not all zero}\}.$$

Definition 3.4. The **affine n -space** is

$$\mathbb{A}^n(k) = k^n.$$

Lemma 3.5. *Let*

$$\begin{aligned} \phi_i : \quad \mathbb{A}^n(k) &\longrightarrow \mathbb{P}^n(k) \\ (x_0, \dots, x_{n-1}) &\longmapsto [x_0 : \dots : x_{i-1} : 1 : x_{i+1} : \dots : x_{n-1}] \end{aligned}.$$

Then ϕ_i is injective, and

$$\mathbb{P}^n(k) = \bigcup_{i=0}^n \text{Im } \phi_i.$$

Proof. Obvious. □

Exercise 3.6. There is an isomorphism

$$\begin{aligned} \mathbb{P}^{n-1}(k) &\longrightarrow \mathbb{P}^n(k) \setminus \phi_n(\mathbb{A}^n(k)) \\ [x_0 : \dots : x_{n-1}] &\longmapsto [x_0 : \dots : x_{n-1} : 0] \end{aligned}.$$

Definition 3.7. The **points at infinity** of $\mathbb{P}^n(k)$ are the ones not in $\phi_n(\mathbb{A}^n(k))$. They are recognisable as the graph of $X_n = 0$.

Let $\lambda : k^{n+1} \rightarrow k$ be a non-trivial linear function. The image of

$$\text{Ker } \lambda = \{ \alpha_0 x_0 + \dots + \alpha_n x_n = 0 \mid (x_0, \dots, x_n) \in k^{n+1}, \text{ not all } \alpha_i \in k \text{ are zero} \} \subset \mathbb{P}^n(k)$$

with respect to the quotient map $k^{n+1} \setminus \{0\} \rightarrow \mathbb{P}^n(k)$ is a **linear hyperplane**. This can be generalised by taking homogeneous polynomials in general.

Definition 3.8. A polynomial $F(X_0, \dots, X_n) \in k[X_0, \dots, X_n]$ is **homogeneous** of degree $d \in \mathbb{N}$ if

$$F(X_0, \dots, X_n) = \sum \alpha_{i_0 \dots i_n} X_0^{i_0} \dots X_n^{i_n}, \quad i_0 + \dots + i_n = d,$$

so you only have degree d terms.

- If f is a degree d polynomial in $k[x_1, \dots, x_n]$, then here is how to **homogenise** it. Change x_i to X_i and then introduce a new variable X_0 and multiply each term with a suitable power of X_0 such that the resulting polynomial is homogeneous of the smallest possible degree.
- If F is a degree d homogeneous polynomial in $k[X_0, \dots, X_n]$, then here is how to **dehomogenise** it. Choose i with $0 \leq i \leq n$, set $X_i = 1$ and change all the other X_j to x_j . If we chose $i = 0$ then this recovers the initial equation.

If $f \in k[x_1, \dots, x_n]$ then the **points at infinity** of $f = 0$ are the zeroes of F , the homogenisation of f , which are in $\mathbb{P}^n(k)$ but not in $\mathbb{A}^n(k)$.

If $F \in k[X_0, \dots, X_n]$ is homogeneous of degree d , then

$$Z(F) = \{[x_0 : \dots : x_n] \in \mathbb{P}^n(k) \mid F(x_0, \dots, x_n) = 0\}$$

does not depend on the representative. Homogenisation allows us to extend an algebraic subset in $\mathbb{A}^n(k)$ to $\mathbb{P}^n(k)$.

Example.

- $X^2 + YZ + Z^2 = 0$ is homogeneous of degree two and gives rise to a conic in $\mathbb{P}^2(k)$.
- $x^2 + x^3 = y^2$ and $xy = 1$ homogenises to $X^2Z + X^3 = Y^2Z$ and $XY = Z^2$.
- $X^2 + Y^2 = Z^2$ and $YZ = X^2$ dehomogenises to $x^2 + y^2 = 1$ and $y = x^2$.

Lecture 6
Tuesday
15/10/19

Theorem 3.9 (Bézout's theorem). *If $F, G \in k[X_0, X_1, X_2]$ be homogeneous non-zero polynomials of degree m and n respectively without common factors, so $\gcd(f, g) = 1$ up to associates, then*

$$|\{F = 0\} \cap \{G = 0\}| = m \cdot n,$$

counted with multiplicities, where $m \cdot n$ is always a positive integer.

Let \bar{k} be the **algebraic closure** of k , the smallest algebraically closed field containing k .

Example.

- $\overline{\mathbb{Q}}$ is a subfield of \mathbb{C} .
- If k is algebraically closed, then $k = \bar{k}$, so $\overline{\mathbb{C}} = \mathbb{C}$, and $\overline{\mathbb{R}} = \mathbb{C}$.
- If K is a field and \mathcal{C} is a collection of subfields $k \in \mathcal{C}$ such that k are algebraically closed, then $\bigcap_{k \in \mathcal{C}} k \subseteq K$ is an algebraically closed subfield.

Corollary 3.10. *If F and G are two homogeneous polynomials of degree a and b in $k[X, Y, Z]$, for k any field not necessarily algebraically closed, then either the graphs of $F = 0$ and $G = 0$ in $\mathbb{P}^2(k)$ have at most ab points in common, or F and G have a common factor.*

Proof. Immediate from Bézout applied to \bar{k} . □

Definition 3.11. Let k be a field of $\text{ch } k \nmid d$, and let $f \in k[x_1, \dots, x_n]$ be a polynomial of degree $d > 0$. Let $P \in \mathbb{A}^n(k)$ be a point on $f = 0$, that is $f(P) = 0$. Then we say that P is a **smooth point** or **non-singular point** if one of the partial derivatives of f does not vanish at P , that is if there exists some i with $1 \leq i \leq n$ such that $\frac{\partial f}{\partial x_i}(P) \neq 0$. Note that the definition of a partial derivative is formal, not a limiting process. We say that P is a **singular point** if all the partial derivatives vanish at P .

Definition 3.12. Let k be a field of $\text{ch } k \nmid d > 0$, and let $F \in k[X_0, \dots, X_n]$ be a homogeneous polynomial of degree d . Let $P \in \mathbb{P}^n(k)$. Then P is a **singular point** of $F = 0$ if any of the following conditions is true.

- $\frac{\partial F}{\partial X_i}(P) = 0$ for $i = 0, \dots, n$.
- $F(P) = 0$ and $\frac{\partial F}{\partial X_i}(P) = 0$ for $i = 0, \dots, n$.
- For some of $\phi_i : \mathbb{A}^n(k) \rightarrow \mathbb{P}^n(k)$ such that $P = \phi_i(p)$ for some $p \in \mathbb{A}^n(k)$, if f is a dehomogenisation of F then $f(p) = 0$ and $\frac{\partial f}{\partial x_i}(p) = 0$ for all i .

Example. $x^3 = y^2$ is a **cusp**.

Definition 3.13. If k is as above, then $f = 0$ or $F = 0$ is **non-singular** in $\mathbb{A}^n(k)$ or $\mathbb{P}^n(k)$ if it has no singular points over \bar{k} .

Lecture 7 is a problem class.

We need to compute the multiplicity up to some precision. Let $f \in k[x, y]$, and let $P \in \mathbb{A}^2(k)$ such that $f(P) = 0$. If $P = (a_1, a_2)$ is non-singular, the **tangent line** of $f = 0$ at P is

$$\frac{\partial f}{\partial x}(P)(x - a_1) + \frac{\partial f}{\partial y}(P)(y - a_2) = 0.$$

This is a non-zero equation, by definition, so not both $\frac{\partial f}{\partial x}(P)$ and $\frac{\partial f}{\partial y}(P)$ is zero. Let $f, g \in k[x, y]$ be non-zero polynomials as above, where $f(P) = g(P) = 0$. We say that $f = 0$ and $g = 0$ **intersect transversely** at P if the tangent lines of $f = 0$ and $g = 0$ at P are different.

Theorem 3.14. *If $f(P) = g(P) = 0$ then the multiplicity at P is one if and only if the intersection is transversal at P .*

Lecture 7
Thursday
17/10/19
Lecture 8
Monday
21/10/19

4 Plane conics

Let $X^2 + Y^2 = Z^2$. If $(a, b, c) \in \mathbb{Z}^3$ is a solution, then $(\lambda a, \lambda b, \lambda c)$ is a solution for $\lambda \in \mathbb{Z}$. A **primitive solution** has $\gcd(a, b, c) = \pm 1$. Any solution can be written as a rescaling of a primitive solution by an integer.

Algorithm 4.1 (To find out if a plane conic is singular). *Say $f \in k[x, y]$ is degree two. Then $\frac{\partial f}{\partial x}$ and $\frac{\partial f}{\partial y}$ are both linear so will meet in at least one point, possibly at infinity. Just check whether this point is on $f = 0$.*

By diagonalisation of quadratic forms, if $\text{ch } k \neq 2$, then for $F \in k[X_0, X_1, X_2]$ of degree two homogeneous, after rescaling by a non-zero scalar, and a permutation of variables, we can assume that

$$F(X_0, X_1, X_2) = \alpha_0 X_0^2 + \alpha_1 X_1^2 + \alpha_2 X_2^2.$$

Theorem 4.2. *The following are equivalent.*

1. $F = 0$ is singular.
2. $\alpha_0 \cdot \alpha_1 \cdot \alpha_2 = 0$.
3. F is the product of two linear polynomials over the algebraic closure.

Proof. $F = 0$ is non-singular if and only if the equations $2\alpha_i X_i = \frac{\partial F}{\partial X_i} = 0$ for all i has no non-zero simultaneous zeroes in k^{n+1} , if and only if not all α_i are zero, so 1 and 2 are equivalent. Let us assume 2. After permuting variables

$$F = \alpha_0 X_0^2 + \alpha_1 X_1^2 = (\sqrt{\alpha_0} X_0 + i\sqrt{\alpha_1} X_1)(\sqrt{\alpha_0} X_0 - i\sqrt{\alpha_1} X_1),$$

so 2 implies 3. Converse 3 implies 2 is an exercise. ³ □

Algorithm 4.3 (To find all k -points of a singular plane conic). *Factor the conic into linear factors, possibly over an extension of k , and then find all the k -points on the lines.*

Algorithm 4.4 (To find all k -points on a non-singular plane conic from one point). *Let k be any field of $\text{ch } k \neq 2$, and let $C \neq \emptyset$ be a conic $F = 0$ over k for a degree two homogeneous polynomial $F \in k[X, Y, Z]$ such that $F = 0$ is non-singular. If $O \in C$, then we can construct a bijection between points over k in C and points on a projective line over k not containing O .*

Proof. Let $\pi(P)$ be the projection of O through P onto a line l not containing O . Claim that $P \mapsto \pi(P)$ is a well-defined map. Any line can intersect C only at most two points, and it intersects C in exactly one point if and only if it is a tangent.

- If $P \neq O$, then there is a unique line \overline{OP} between O and P . Then \overline{OP} and l are different as l does not contain O , but \overline{OP} does, so $\overline{OP} \cap l$ is one point $\pi(P)$, so $\pi(P)$ is well-defined in this case.
- The tangent line of C at O intersects C at O with multiplicity at least two, so it does not intersect C in any other point, but it still has a unique intersection point with l , so I take the latter to be $\pi(O)$.

Claim that $P \mapsto \pi(P)$ is a bijection.

- The map is injective, since if $\pi(P) = \pi(P')$, then $\overline{OP} = \overline{OP'}$, so $P, P', O \in \overline{OP} \cap C$, so $P = P'$.
- The map is surjective. If $O \neq Q \in l$, then there is another intersection point in $\overline{OQ} \cap C$ over the algebraic closure. The bad thing is that the line intersects C in two points over the algebraic closure, neither of which is a rational point. Claim that if $0 \neq h \in k[x]$ has degree two, and it has a root over k , then its other root is also defined over k . Let $h = ax^2 + bx + c$. There exists $\alpha \in k$ such that $h(\alpha) = 0$, so I can factor out $x - \alpha$, so $h = (x - \alpha)g$ for $g \in k[x]$. Then $\deg g = 1$, so $g = a(x - \beta)$ for $\beta \in k$, so β is the other root. Thus the other intersection point is another point $P \in C$.

□

Corollary 4.5. *If k is infinite, then either C has no points, or it has infinitely many.*

³Exercise

5 The Hasse principle for smooth plane conics over \mathbb{Q}

Let C be a conic $aX^2 + bY^2 + cZ^2 = 0$ over \mathbb{R} . We rescale each of a, b, c by a non-zero square. Over \mathbb{R} we can assume $\{a, b, c\} = \{1, -1\}$. There are two cases.

- If $X^2 + Y^2 + Z^2 = 0$, then $C(\mathbb{R}) = \emptyset$.
- If $X^2 + Y^2 - Z^2 = 0$, then $C(\mathbb{R}) \neq \emptyset$.

Let C be a conic $aX^2 + bY^2 + cZ^2 = 0$ over \mathbb{Q}_p such that p is an odd prime. After rescaling by a square I can assume that $a, b, c \in \mathbb{Z}_p$. Then $|a|_p, |b|_p, |c|_p \leq 1$. By rescaling by a non-zero even power of p , I can assume the following two cases.

- If $|a|_p, |b|_p, |c|_p = 1$, then C is non-singular. As $a, b, c \in \mathbb{Z}_p$, I can reduce the equation modulo p . Pick $x \neq 0$, and let

$$A = \{ax^2 + by^2 \mid y \in \mathbb{F}_p\}.$$

Assume $A \subseteq \mathbb{F}_p^*$, otherwise for some y , $ax^2 + by^2 + c0^2 = 0$. If $ax^2 + by^2 = ax^2 + by'^2$, then $y^2 = y'^2$, so $y = y' = 0$ or $y = -y' \neq 0$, so $|A| = (p+1)/2$. Let

$$B = \{-cz^2 \mid z \in \mathbb{F}_p\}.$$

Similarly $|B| = (p+1)/2$. If the equation has no solutions, then $A \cap B = \emptyset$, so

$$p-1 = |\mathbb{F}_p^*| \geq |A \cup B| = |A| + |B| = \frac{p+1}{2} + \frac{p+1}{2} = p+1,$$

a contradiction. Then C has a point over \mathbb{F}_p , so it has a non-zero solution by Hensel's lemma. Thus C has a point over \mathbb{Q}_p .

- If $|c|_p = 1/p$ and $|a|_p, |b|_p = 1$, then C is singular, and we could still use Hensel's lemma.

Let C be a conic $aX^2 + bY^2 + cZ^2 = 0$ over \mathbb{Q} . I can assume that

- $a, b, c \in \mathbb{Z}$, by rescaling,
- a, b, c are relatively prime, by rescaling,
- a, b, c are square-free, since we can rescale individual variables by squares, and
- a, b, c are pairwise relatively prime, since if p is a prime number such that $p \mid a$ and $p \mid b$, then pa and pb are divisible by p^2 , so I absorb the p^2 into X and Y .

Now just by looking at the signs you can tell whether C has a solution or not over the reals, and just by looking at the valuations you can tell whether C has a solution or not over the individual p -adic fields, but what can we say about the solutions of C over the rationals?

Lemma 5.1. *Let $U \subseteq \mathbb{R}^n$ be a measurable set, for example open, and assume that it has measure $\mu(U) > m \in \mathbb{N}_{>0}$. Then there exist $c_0, \dots, c_m \in U$ such that $c_i - c_0 \in \mathbb{Z}^n \subset \mathbb{R}^n$ for all $i = 1, \dots, m$.*

Proof. Let $C = [0, 1]^n \subseteq \mathbb{R}^n$. Then C is measurable and $\mu(C) = 1$, and $C + \mathbb{Z}^n = \mathbb{R}^n$. For any set $X \subseteq \mathbb{R}^n$ let

$$\chi_X(\underline{t}) = \begin{cases} 1 & \underline{t} \in X \\ 0 & \underline{t} \notin X \end{cases}$$

be the characteristic function of X . Then

$$m < \mu(U) = \int_{\mathbb{R}^n} \chi_U(\underline{t}) \, d\underline{t} = \sum_{\underline{x} \in \mathbb{Z}^n} \int_{\mathbb{R}^n} \chi_{(C+\underline{x}) \cap U}(\underline{t}) \, d\underline{t} = \int_{\mathbb{R}^n} \sum_{\underline{x} \in \mathbb{Z}^n} \chi_{(C+\underline{x}) \cap U}(\underline{t}) \, d\underline{t} = \int_C \sum_{\underline{x} \in \mathbb{Z}^n} \chi_{C-\underline{x}}(\underline{t}) \, d\underline{t}.$$

The function $\sum_{\underline{x} \in \mathbb{Z}^n} \chi_{C-\underline{x}}(\underline{t})$ is a counting function

$$\underline{x} \in C \mapsto |\{ \underline{y} \in U \mid \underline{x} - \underline{y} \in \mathbb{Z}^n \}|,$$

which is an integer-valued measurable function, and if $\underline{x} < m$ for all points, then its integral over C is less than m , a contradiction. Thus there exists $\underline{x} \in C$ such that $|\underline{x} + \mathbb{Z}^n \cap U| > m$. \square

Definition 5.2.

- $U \subseteq \mathbb{R}^n$ is **symmetric** if for all $\underline{x} \in U$, $-\underline{x} \in U$.
- $U \subseteq \mathbb{R}^n$ is **convex** if for all $\underline{x}, \underline{y} \in U$, there exists $t \in [0, 1]$ such that $t\underline{x} + (1-t)\underline{y} \in U$.

Corollary 5.3 (Minkowski's geometry of numbers). *Let $\Lambda \subseteq \mathbb{R}^n$ be a subgroup of finite index m . Let $U \subseteq \mathbb{R}^n$ be an open, convex, symmetric set of $\mu(U) > 2^n \cdot m$. Then $\Lambda \cap U \neq \emptyset$.*

Proof. Let

$$V = \frac{1}{2}U = \left\{ \frac{1}{2}\underline{x} \mid \underline{x} \in U \right\},$$

so $\mu(V) = 2^{-n} \cdot \mu(U) > m$. So by the Lemma 5.1 there exist $c_0, \dots, c_m \in V$ such that $c_i - c_0 \in \mathbb{Z}^n$ for all $i = 0, \dots, m$. By the pigeonhole principle, as

$$|\{c_i - c_0 \mid i = 0, \dots, m\}| = m + 1 > [\mathbb{Z}^n : \Lambda],$$

there exist $i \neq j$ such that $c_i - c_0 \equiv c_j - c_0 \pmod{\Lambda}$, so $c_i - c_j = (c_i - c_0) - (c_j - c_0) \in \Lambda$. Then $2c_i \in U$, and $-2c_i \in -U = U$ by symmetry of U , so $\frac{1}{2}(2c_i) + \frac{1}{2}(-2c_i) \in U$, as U is convex. \square

Theorem 5.4. *If $n \in \mathbb{Z}_{>0}$ such that there exists t with $t^2 \equiv 1 \pmod{n}$, then n is a sum of two squares.*

Proof. Define

$$\Gamma = \{(x, y) \mid y \equiv tx \pmod{n}\} \subseteq \mathbb{Z}^2.$$

This has index n , because it is the kernel of

$$\begin{array}{ccc} \mathbb{Z}^2 & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ (x, y) & \longmapsto & y - tx \end{array}.$$

Let

$$V = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 < 2n\}.$$

Then

$$\mu(V) = 2n \cdot \pi > 4n = 2^2 \cdot n = 2^2 \cdot [\mathbb{Z}^2 : \Lambda].$$

Corollary 5.3 implies that there exists $(x, y) \in V \cap \Lambda$ such that $(x, y) \neq (0, 0)$. Then $(x, y) \in V$ implies that $x^2 + y^2 < 2n$, and $(x, y) \in \Lambda$ implies that $y \equiv tx \pmod{n}$, so

$$x^2 + y^2 \equiv x^2 + (tx)^2 \equiv x^2(t^2 + 1) \equiv 0 \pmod{n}.$$

So $x^2 + y^2 = n$. \square

Theorem 5.5 (Hasse-Minkowski). *Let C be*

$$f = ax^2 + by^2 + cz^2, \quad a, b, c \in \mathbb{Z}, \quad abc \neq 0, \quad (a, b) = (b, c) = (c, a) = 1,$$

where a, b, c are square-free. Let $\Sigma = \{p \mid 2abc\}$. Then the following are equivalent.

1. C has infinitely many solutions in $\mathbb{P}^2(\mathbb{Q})$.
2. C has a solution in $\mathbb{P}^2(\mathbb{Q})$.
3. C has a solution in $\mathbb{P}^2(\mathbb{Q}_p)$ for all p , and in $\mathbb{P}^2(\mathbb{R})$.
4. C has a solution in $\mathbb{P}^2(\mathbb{Q}_p)$ for all $p \in \Sigma$.

The problem of solving conics over \mathbb{Q} is algorithmically decidable, so there is a computer program which solves this problem.

Lecture 11
Monday
28/10/19

Proof. 1 implies 2 implies 3 implies 4, and we proved 2 implies 1, so 4 implies 2 is enough. Assume 4. Claim that if $p \mid a$, then there is a solution to

$$b + cz^2 \equiv 0 \pmod{p}.$$

By 4, there exists $(x, y, z) \in \mathbb{P}^2(\mathbb{Q}_p)$ with $ax^2 + by^2 + cz^2 = 0$. Without loss of generality $x, y, z \in \mathbb{Z}_p$, not all divisible by p . If $|y|_p < 1$ then $cz^2 = -(ax^2 + by^2) \equiv 0 \pmod{p}$, so $|z|_p < 1$, then $|ax^2|_p \leq 1/p^2$, so $|x|_p < 1$, a contradiction. So $|y|_p = 1$, so $a(x/y)^2 + b + c(z/y)^2 = 0$, with $x/y, z/y \in \mathbb{Z}_p$. Then $b + c(z/y)^2 \equiv 0 \pmod{p}$.

- Now assume that p is odd and $p \mid a$. Then let $\alpha \in \mathbb{Z}/p\mathbb{Z}$ be a solution to $b + c\alpha^2 \equiv 0 \pmod{p}$, and impose the condition

$$\alpha s + t \equiv 0 \pmod{p}.$$

Then $ar^2 + bs^2 + ct^2 \equiv bs^2 + ct^2 \equiv bs^2 + c(\alpha s)^2 \equiv s^2(b + c\alpha^2) \equiv 0 \pmod{p}$. If p is odd and $p \mid b$ or $p \mid c$, impose the analogous conditions.

- Now assume that $p = 2$.

- Let $2 \mid a$, or by symmetry $2 \mid b$ or $2 \mid c$. We will write a condition to ensure that $ar^2 + bs^2 + ct^2 \equiv 0 \pmod{8}$. We saw in the proof of the claim that there exist $x, y, z \in \mathbb{Z}_2$ with $|x|_2 \leq 1$ and $|y|_2 = |z|_2 = 1$, and $ax^2 + by^2 + cz^2 = 0$. Then $ax^2 + by^2 + cz^2 \equiv ax^2 + b + c \pmod{8}$, that is $ax^2 + b + c \equiv 0 \pmod{8}$.

- * If $|x|_2 = 1$, then $a + b + c \equiv 0 \pmod{8}$. Impose

$$s \equiv t \pmod{4}, \quad r \equiv s \pmod{2}.$$

Then either r, s, t all odd, and $ar^2 + bs^2 + ct^2 \equiv a + b + c \equiv 0 \pmod{8}$, or r, s, t all even, and $ar^2 + bs^2 + ct^2 \equiv bs^2 + ct^2 \equiv 4(b + c) \equiv -4a \equiv 0 \pmod{8}$.

- * If $|x|_2 < 1$, then $ax^2 + b + c \equiv b + c \pmod{8}$, that is $b + c \equiv 0 \pmod{8}$. Impose

$$s \equiv t \pmod{4}, \quad r \equiv 0 \pmod{2}.$$

Then $ar^2 + bs^2 + ct^2 \equiv bs^2 + ct^2 \equiv bs^2 + cs^2 \equiv (b + c)s^2 \equiv 0 \pmod{8}$.

- Let $2 \nmid abc$. Let $(x, y, z) \in \mathbb{P}^2(\mathbb{Q}_2)$ with $ax^2 + by^2 + cz^2 = 0$. Assume $\max(|x|_2, |y|_2, |z|_2) = 1$. Then $ax^2 + by^2 + cz^2 \equiv 0 \pmod{2}$, that is $x^2 + y^2 + z^2 \equiv 0 \pmod{2}$. Then exactly one of x, y, z is even, without loss of generality $|x|_2 < 1$ and $|y|_2 = |z|_2 = 1$. Then $0 = ax^2 + by^2 + cz^2 \equiv by^2 + cz^2 \equiv b + c \pmod{4}$. Impose conditions

$$r \equiv 0 \pmod{2}, \quad s \equiv t \pmod{2}.$$

Then $ar^2 + bs^2 + ct^2 \equiv bs^2 + ct^2 \equiv (b + c)s^2 \equiv 0 \pmod{4}$.

Let $\Lambda \subseteq \mathbb{Z}^3$ be the subgroup defined by all of these congruence conditions for $p \in \Sigma$. Then

$$[\mathbb{Z}^3 : \Lambda] = |4abc| = 4 \prod_{p|abc} p,$$

using the Chinese remainder theorem. If $(r, s, t) \in \Lambda$ then $ar^2 + bs^2 + ct^2 \equiv 0 \pmod{4abc}$. Let

$$V = \{|a|x^2 + |b|y^2 + |c|z^2 < 4|abc|\}.$$

If $(r, s, t) \in \Lambda \cap V$ then $|ar^2 + bs^2 + ct^2| < 4|abc|$, so $ar^2 + bs^2 + ct^2 = 0$. By Corollary 5.3, we just need to check that $\mu(V) > 2^3 \cdot |4abc|$, and

$$\mu(V) = \frac{\frac{4}{3}\pi\sqrt{|4abc|}^3}{\sqrt{|abc|}} = \frac{\pi}{3} \cdot 2^3 \cdot |4abc| > 2^3 \cdot |4abc|.$$

□

Let $X \subseteq \mathbb{P}^n(\mathbb{Q})$ be a projective algebraic variety, such as hypersurfaces or plane curves. The **local-global principle** holds for X if $X(\mathbb{Q}) \neq \emptyset$ if and only if $X(\mathbb{Q}_p) \neq \emptyset$ for all p prime number and $X(\mathbb{R}) \neq \emptyset$. Hasse-Minkowski implies that conics satisfy the local-global principle, but $3X^3 + 4Y^3 + 5Z^3 = 0$ does not.

A Diagonalisation of quadratic forms

Definition A.1. Let k be any field, and let V be a k -linear vector space. A **symmetric bilinear pairing** on V is a map $(\cdot, \cdot) : V \times V \rightarrow k$ such that for all $\alpha_1, \alpha_2 \in k$ and $\underline{v}_1, \underline{v}_2, \underline{v}_3 \in V$,

- $(\alpha_1 \underline{v}_1 + \alpha_2 \underline{v}_2, \underline{v}_3) = \alpha_1 (\underline{v}_1, \underline{v}_3) + \alpha_2 (\underline{v}_2, \underline{v}_3)$,
- $(\underline{v}_3, \alpha_1 \underline{v}_1 + \alpha_2 \underline{v}_2) = \alpha_1 (\underline{v}_3, \underline{v}_1) + \alpha_2 (\underline{v}_3, \underline{v}_2)$, and
- $(\underline{v}_1, \underline{v}_2) = (\underline{v}_2, \underline{v}_1)$.

Example A.2. Dot product in \mathbb{R}^n over \mathbb{R} .

Definition A.3. If $\text{ch } k \neq 2$, then the associated **quadratic form** to a symmetric bilinear pairing is

$$\begin{aligned} B &: V \longrightarrow k \\ \underline{v} &\longmapsto (\underline{v}, \underline{v}) \end{aligned}$$

Remark A.4. Then B is uniquely determined by (\cdot, \cdot) , but the converse is also true, since

$$B(\underline{v}_1 + \underline{v}_2) = (\underline{v}_1 + \underline{v}_2, \underline{v}_1 + \underline{v}_2) = (\underline{v}_1, \underline{v}_1) + (\underline{v}_1, \underline{v}_2) + (\underline{v}_2, \underline{v}_1) + (\underline{v}_2, \underline{v}_2) = B(\underline{v}_1) + B(\underline{v}_2) + 2(\underline{v}_1, \underline{v}_2),$$

by bilinearity and symmetry, so

$$(\underline{v}_1, \underline{v}_2) = \frac{1}{2} (B(\underline{v}_1 + \underline{v}_2) - B(\underline{v}_1) - B(\underline{v}_2)).$$

Example A.5. Let $V = k^n$, and let A be a symmetric $n \times n$ matrix over k . Then

$$(\underline{v}_1, \underline{v}_2) = \underline{v}_1^\top A \underline{v}_2 \in k, \quad \underline{v}_1, \underline{v}_2 \in V$$

is a symmetric bilinear pairing. More generally, let V be any finite-dimensional vector space, so $V = \langle \underline{e}_1, \dots, \underline{e}_n \rangle_k$ for $\{\underline{e}_i\}$ a k -basis, and let the (i, j) -th entry of A be $(\underline{e}_i, \underline{e}_j)$. Under the unique isomorphism

$$\begin{aligned} \phi &: V \longrightarrow k^n \\ \underline{e}_i &\longmapsto (0, \dots, 0, 1, 0, \dots, 0) \end{aligned}$$

we get a symmetric bilinear pairing

$$(\underline{v}, \underline{w}) = \phi(\underline{v})^\top A \phi(\underline{w}) \in k, \quad \underline{v}, \underline{w} \in V.$$

Definition A.6. A **quadratic space** over k is an ordered pair $(V, (\cdot, \cdot))$ for V a finite-dimensional k -linear vector space, and $(\cdot, \cdot) : V \times V \rightarrow k$ a symmetric bilinear pairing. Two quadratic spaces $(V, (\cdot, \cdot))$ and $(W, (\cdot, \cdot))$ are **isometric** if there exists $\phi : V \rightarrow W$ an isomorphism such that $(\underline{v}, \underline{w}) = \langle \phi(\underline{v}), \phi(\underline{w}) \rangle$ for all $\underline{v}, \underline{w} \in V$, so any quadratic space is isometric to a specimen from the example.

Remark A.7. Change of basis has the following effect. Let A be the matrix of the symmetric bilinear pairing (\cdot, \cdot) in the basis $\underline{e}_1, \dots, \underline{e}_n$. If the matrix of the change of basis is B , in the basis the matrix of the symmetric bilinear pairing is $B^\top A B$, since $(B\underline{v})^\top A (B\underline{w}) = \underline{v}^\top (B^\top A B) \underline{w}$.

Theorem A.8 (Gram-Schmidt orthogonalisation process). *If $(V, (\cdot, \cdot))$ is a quadratic space, then V has a basis $\underline{e}_1, \dots, \underline{e}_n$ in which the matrix of (\cdot, \cdot) is diagonal.*

Proof. Two cases. If $B \equiv 0$, then $(\cdot, \cdot) \equiv 0$. Otherwise for all $\underline{v} \in V$ such that $B(\underline{v}) \neq 0$. Let $\underline{e}_1 = \underline{v}_1$ and

$$\underline{v}^\perp = \{\underline{w} \in V \mid (\underline{v}, \underline{w}) = 0\}.$$

This is an k -linear subspace, which is trivial as $\underline{w} \mapsto (\underline{v}, \underline{w})$ is k -linear. Then $\underline{v} \notin \text{Ker}(\underline{v}, \cdot)$, so $\dim \underline{v}^\perp = \dim V - 1$. We apply the process to $(\underline{v}^\perp, (\cdot, \cdot)|_{\underline{v}^\perp})$, by using induction on the dimension. \square

Remark A.9. The general linear group

$$\mathrm{GL}_{n+1}(k) = \mathrm{Aut}_k k^{n+1}$$

acts on $\mathbb{P}^n(k)$, and maps scalar multiples to scalar multiples, so maps equivalence classes under rescaling to equivalence classes, so have an induced action on $\mathbb{P}^n(k)$. The centre $Z_{n+1}(k)$ of $\mathrm{GL}_{n+1}(k)$ is the scalar matrices $\{\lambda I_3 \mid \lambda \in k^*\}$, which acts trivially on $\mathbb{P}^n(k)$. This is a normal subgroup, so I can form the quotient group

$$\mathrm{PGL}_{n+1}(k) = \mathrm{GL}_{n+1}(k) / Z_{n+1}(k),$$

the **projective linear group** of rank $n + 1$. Projective algebraic geometry is invariant under projective linear transformations. If $F = 0$ is non-singular, then its image under $\mathrm{PGL}_{n+1}(k)$ is also non-singular, and multiplicities in Bézout's theorem does not change under $\mathrm{PGL}_{n+1}(k)$, etc.

Theorem A.10. *If $\mathrm{ch} k \neq 2$, then for $F \in k[X_0, \dots, X_n]$ of degree two homogeneous, there exists a linear transformation, such that after the change of variables, F is of the form*

$$\alpha_0 X_0^2 + \dots + \alpha_n X_n^2, \quad \alpha_0, \alpha_1, \alpha_2 \in k.$$

Proof. Let $F(X_0, \dots, X_n) = \sum_{i < j} a_{ij} X_i X_j$ for $a_{ij} \in k$. It is the quadratic form on k^{n+1} associated to the bilinear pairing in the standard basis with matrix $A = (b_{ij})$, where

$$b_{ij} = \begin{cases} \frac{1}{2}a_{ij} & i \leq j \\ \frac{1}{2}a_{ji} & i > j \end{cases}.$$

Now apply the Gram-Schmidt theorem. □