

Math 326 - Algebra 2

Lectures by Kazuya Kato

Notes by Zev Chonoles

The University of Chicago, Winter 2013

Lecture 1 (2013-01-07)	1	Lecture 16 (2013-02-13)	43
Lecture 2 (2013-01-09)	4	Lecture 17 (2013-02-15)	46
Lecture 3 (2013-01-11)	7	Lecture 18 (2013-02-18)	47
Lecture 4 (2013-01-14)	9	Lecture 19 (2013-02-20)	50
Lecture 5 (2013-01-16)	11	Lecture 20 (2013-02-22)	52
Lecture 6 (2013-01-18)	14	Lecture 21 (2013-02-25)	53
Lecture 7 (2013-01-23)	16	Lecture 22 (2013-02-27)	54
Lecture 8 (2013-01-25)	19	Lecture 23 (2013-03-01)	56
Lecture 9 (2013-01-28)	23	Lecture 24 (2013-03-04)	58
Lecture 10 (2013-01-30)	26	Lecture 25 (2013-03-06)	59
Lecture 11 (2013-02-01)	29	Lecture 26 (2013-03-08)	61
Lecture 12 (2013-02-04)	32	Lecture 27 (2013-03-11)	63
Lecture 13 (2013-02-06)	35	Lecture 28 (2013-03-13)	64
Lecture 14 (2013-02-08)	37	Lecture 29 (2013-03-15)	66
Lecture 15 (2013-02-11)	40		

Introduction

Math 326 is one of the nine courses offered for first-year mathematics graduate students at the University of Chicago. It is the second of three courses in the year-long algebra sequence.

These notes are being live-Texed, though I edit for typos and add diagrams requiring the *TikZ* package separately. I am using the editor TeXstudio.

I am responsible for all faults in this document, mathematical or otherwise; any merits of the material here should be credited to the lecturer, not to me.

Please email any corrections or suggestions to chonoles@math.uchicago.edu.

Lecture 1 (2013-01-07)

The main subject of this course is commutative ring theory, and its relation to algebraic number theory and algebraic geometry. We will also see some more advanced topics such as class field theory and the Weil conjectures, though we will not go into them in depth.

There will be no exams. The assignments will appear on each Friday, on the Chalk site if it can be set up; otherwise, on each Thursday evening, the assignments will be sent by email. They will then be due the following Friday.

If you look on the street, you never meet a commutative ring; that's rather strange. They are rather shy I think. We need to ask them to come to this room. Rings, rings, please come! Rings, rings please come! **shuffles along the floor, playing the part of the ring** Finite fields, come! Rings of functions, come! **hops** I think they are here now.

The Mysterious Analogy Between Prime Numbers and Points

Let A be a commutative ring. We define

$$\max(A) = \{\text{maximal ideals of } A\}.$$

There is a bijection

$$\begin{array}{ccc} \max(\mathbb{Z}) & \longleftrightarrow & \{\text{prime numbers}\} \\ \Downarrow & & \Downarrow \\ (p) = p\mathbb{Z} & & p \end{array}$$

There is also a bijection

$$\begin{array}{ccc} \max(\mathbb{C}[T]) & \longleftrightarrow & \mathbb{C} \\ \Downarrow & & \Downarrow \\ (T - \alpha) & & \alpha \end{array}$$

More generally, there is a bijection

$$\begin{array}{ccc} \max(\mathbb{C}[T_1, \dots, T_n]) & \longleftrightarrow & \mathbb{C}^n \\ \Downarrow & & \Downarrow \\ (T_1 - \alpha_1, \dots, T_n - \alpha_n) & & (\alpha_1, \dots, \alpha_n) \end{array}$$

Note that $(T_1 - \alpha_1, \dots, T_n - \alpha_n) = \{f \in \mathbb{C}[T_1, \dots, T_n] \mid f(\alpha_1, \dots, \alpha_n) = 0\}$.

We can walk on \mathbb{C} , but I think it is hard walking on the prime numbers. I hope someday I can find a pair of shoes that can help. One difficulty is that the points in \mathbb{C} are all the same size, but the primes are like stones of different sizes; 3 is a little bigger than 2, 5 is a little bigger than 3...

Let X be a compact Hausdorff space, and let $A = C(X) = \{\text{continuous maps } X \rightarrow \mathbb{R}\}$. Then there is a bijection

$$\begin{array}{ccc} \max(A) & \longleftrightarrow & X \\ \Downarrow & & \Downarrow \\ \{f \in A \mid f(p) = 0\} & & p \end{array}$$

If X is not compact, this is false. We can see this by considering $X = \mathbb{R}$ for example. In $A = \{\text{continuous maps } \mathbb{R} \rightarrow \mathbb{R}\}$, we can consider the ideal

$$I = \{f \in A \mid \text{there is some } c \text{ such that } f(x) = 0 \text{ if } x > c\}.$$

There is a proposition from commutative ring theory:

Proposition. *If A is a commutative ring and $I \subsetneq A$ is a proper ideal of A , then there is some $\mathfrak{m} \in \max(A)$ such that $I \subset \mathfrak{m}$.*

This proposition requires the Axiom of Choice, so we will skip the proof for the moment. But the proposition implies that there is some maximal ideal of A containing I , and no ideal of the form $\{f \in A \mid f(p) = 0\}$ can contain I , so there must be other maximal ideals.

Now consider $X = \{(x, y) \in \mathbb{C}^2 \mid y^2 = x^3 + 1\}$, and let $A = \{\text{polynomial functions on } X\}$. For example, the function x sends $(a, b) \in X$ to $a \in \mathbb{C}$, and the function y sends $(a, b) \in X$ to $b \in \mathbb{C}$. Note that

$$A = \{\mathbb{C}\text{-valued functions on } X \text{ written as a polynomial over } \mathbb{C} \text{ in the functions } x, y\}.$$

Then $A \cong \mathbb{C}[T, \sqrt{T^3 + 1}]$, where T is the function x . This ring is a quadratic extension of $\mathbb{C}[T]$, which you should think of as being similar to an extension of \mathbb{Z} , such as for example $\mathbb{Z}[\sqrt{26}]$.

There is an isomorphism $A \cong \mathbb{C}[T_1, T_2]/(T_2^2 - T_1^3 - 1)$, where $T_1 \mapsto T$ and $T_2 \mapsto \sqrt{T^3 + 1}$. There is also a bijection

$$\begin{array}{ccc} \max(A) & \longleftrightarrow & X \\ \cup & & \cup \\ \{f \in A \mid f(p) = 0\} & & p \end{array}$$

which can be deduced from the correspondence between $\max(\mathbb{C}[T_1, T_2])$ and \mathbb{C}^2 ,

$$\begin{array}{ccc} \max(\mathbb{C}[T_1, T_2]) & \longleftrightarrow & \mathbb{C}^2 \\ \cup & & \cup \\ \max(A) & \longleftrightarrow & X \end{array}$$

(Recall that there is a bijection

$$\max(A/I) \longleftrightarrow \{\mathfrak{m} \in \max(A) \mid I \subseteq \mathfrak{m}\},$$

where $M \in \max(A/I)$ corresponds to $\{x \in A \mid x \bmod I \in M\}$.)

In the ring $\mathbb{Z}[\sqrt{-26}]$, note that we do not have unique factorization:

$$3^3 = 27 = (1 + \sqrt{-26})(1 - \sqrt{-26}).$$

Writing $\mathfrak{p} = (3, 1 + \sqrt{-26})$ and $\mathfrak{p}' = (3, 1 - \sqrt{-26})$, we can recover unique factorization for ideals:

$$(3) = \mathfrak{p}\mathfrak{p}', \quad (1 + \sqrt{-26}) = \mathfrak{p}^3, \quad (1 - \sqrt{-26}) = \mathfrak{p}'^3$$

$$(\mathfrak{p}\mathfrak{p}')^3 = (27) = \mathfrak{p}^3\mathfrak{p}'^3.$$

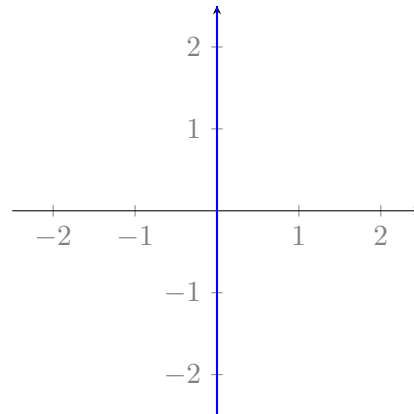
(recall that for ideals I and J , their product is $IJ = \{\sum_{i=1}^n a_i b_i \mid a_i \in I, b_i \in J\}$.)

There is a similar situation in A : we have $x^3 = (y + 1)(y - 1)$. Define

$$\mathfrak{p} = (x, y + 1) = \{f \in A \mid f(0, -1) = 0\} \longleftrightarrow (0, -1) \in X,$$

and similarly $\mathfrak{p}' = (x, y - 1) \longleftrightarrow (0, 1) \in X$. Then $(x) = \mathfrak{p}\mathfrak{p}'$, $(y + 1) = \mathfrak{p}^3$, and $(y - 1) = \mathfrak{p}'^3$.

$$y^2 = x^3 + 1$$

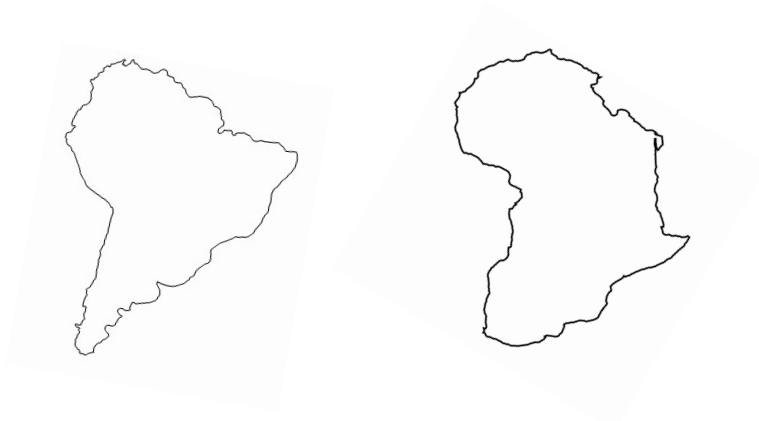


Observe that the function x has a zero of order 1 at $(0, 1)$ and $(0, -1)$, that $y + 1$ has a zero of order 3 at $(0, -1)$, and $y - 1$ has a zero of order 3 at $(0, 1)$.

Kummer was the one who realized that even though there is no unique factorization in the world of numbers, it could be recovered in the world of ideals. This observation was then imported to the world of geometry.

As we've seen, there is an analogy between \mathbb{Z} and $\mathbb{C}[T]$. In fact, the analogy between \mathbb{Z} and $\mathbb{F}_p[T]$ is even stronger; for example the theory of zeta functions is very similar for \mathbb{Z} and $\mathbb{F}_p[T]$. We don't know the true reason why they are so similar; perhaps they are children of the same parents. But we don't know who their parents are; their parents are missing.

In 1912, Wegener compared the west coast of Africa and the east coast of South America,



and hypothesized that at one point they were connected. It took a long time for his theory to be accepted.

Lecture 2 (2013-01-09)

Noetherian rings and integral closure; intro. to algebraic number theory

Let A be a commutative ring with unity $1 \in A$. A subring of A must contain 1; thus, for example, $2\mathbb{Z}$ is not a subring of \mathbb{Z} . We also require that a ring homomorphism respects the unities of the rings.

Integral elements, algebraic integers

The spirit of algebraic number theory:

To study \mathbb{Z} , it is better not only to consider \mathbb{Z} , but also to consider the friends $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{2}]$, ... of \mathbb{Z} , for they are happy to help \mathbb{Z} .

Numbers like i , $\sqrt{2}$, $\sqrt{5}$, ... are algebraic integers. However, $\frac{\sqrt{5}}{2}$ is not an algebraic integer. But even though the shape of $\frac{1+\sqrt{5}}{2}$ is a fraction, it is an algebraic integer, and similarly $\frac{-1+\sqrt{-3}}{2}$ is an algebraic integer. Now we need a precise definition of algebraic integer.

Definition. Let A be a subring of a ring B . Then we say an element $x \in B$ is integral over A when there is an $n \geq 1$ and $a_1, \dots, a_n \in A$ such that $x^n + a_1x^{n-1} + \dots + a_n = 0$.

For example, if we take $A = \mathbb{Z}$ and $B = \mathbb{Q}(\sqrt{5})$, the element $x = \frac{1+\sqrt{5}}{2}$ satisfies $x^2 - x - 1 = 0$. Thus, $\frac{1+\sqrt{5}}{2}$ is integral over \mathbb{Z} .

Definition. Given a field $K \supseteq \mathbb{Q}$, we say that an element $x \in K$ is an algebraic integer when x is integral over \mathbb{Z} .

Definition. Let A be a subring of a ring B . The integral closure of A in B is the set

$$\{x \in B \mid x \text{ is integral over } A\}.$$

When we have a field K that is a finite extension of \mathbb{Q} , we denote the integral closure of \mathbb{Z} in K by \mathcal{O}_K . Sometimes, it is called the ring of integers of K , or the integer ring of K .

When $K = \mathbb{Q}$, we have $\mathcal{O}_K = \mathbb{Z}$. When $K = \mathbb{Q}(i)$, we have $\mathcal{O}_K = \mathbb{Z}[i]$.

Proposition 1. *The integral closure of A in B is a subring of B .*

We will prove this claim later.

Proposition 2. *Let $A \subseteq B \subseteq C$ be rings. Let B' be the integral closure of A in B , and let C' be the integral closure of A in C . Then C' is the integral closure of B' in C .*

We will prove this claim later. When I say that we will prove something later, it either means I will give it later in class, or on the homework, or I will just forget to prove it.

Corollary. \mathcal{O}_K is a ring.

Let $K \supseteq \mathbb{Q}$ be a quadratic extension, so that $K = \mathbb{Q}(\sqrt{m})$ for a squarefree $m \in \mathbb{Z}$. Then

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{m}] & \text{if } m \equiv 2, 3 \pmod{4}, \\ \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right] & \text{if } m \equiv 1 \pmod{4}. \end{cases}$$

Thus, for example, if $K = \mathbb{Q}(\sqrt{5})$, we have $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$.

Now consider $A = k[T]$ and $B = k(T)(\sqrt[n]{f(T)})$ where $f \in k[T]$ is a polynomial with no multiple factors. Then the integral closure of $k[T]$ in B is $k[T, \sqrt[n]{f(T)}]$. For example, the integral closure of $\mathbb{C}[T]$ in $\mathbb{C}(T, \sqrt{T^3+1})$ is $\mathbb{C}[T, \sqrt{T^3+1}]$.

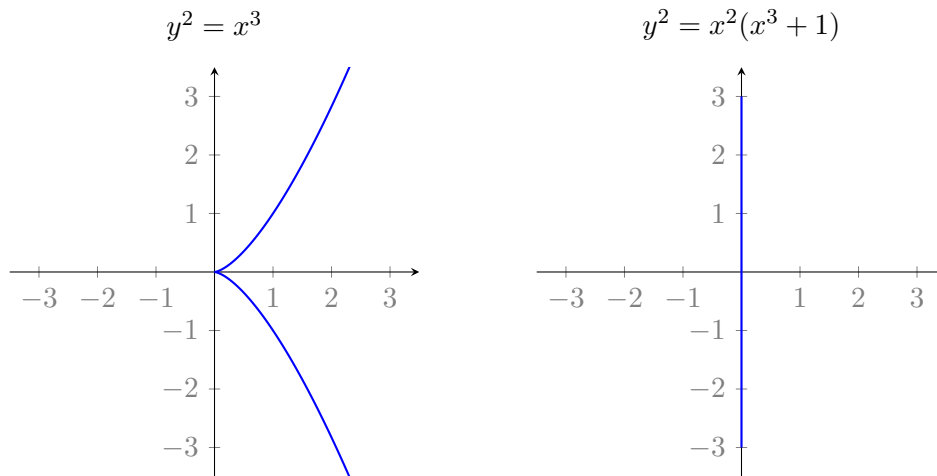
Definition. Let A be an integral domain with field of fractions K . We say that A is integrally closed if the integral closure of A in K is just A . Sometimes we instead say that A is normal.

For example, for any finite extension $K \supseteq \mathbb{Q}$, the ring \mathcal{O}_K is normal.

However, $\mathbb{Z}[\sqrt{5}]$ is not normal, because $\frac{1+\sqrt{5}}{2}$ is in the field of fractions $\mathbb{Q}(\sqrt{5})$ and is integral over $\mathbb{Z}[\sqrt{5}]$, so it is in the integral closure of $\mathbb{Z}[\sqrt{5}]$ in $\mathbb{Q}(\sqrt{5})$, but it is not itself in $\mathbb{Z}[\sqrt{5}]$.

Here is another example of a non-normal ring: $\mathbb{C}[T, \sqrt{T^3}]$. The field of fractions of this ring is $\mathbb{C}(\sqrt{T})$, and $\sqrt{T} \notin \mathbb{C}[T, \sqrt{T^3}]$ even though it is integral over $\mathbb{C}[T, \sqrt{T^3}]$. Note that $\mathbb{C}[T, \sqrt{T^3}] \cong \mathbb{C}[X, Y]/(Y^2 - X^3)$, where $X \mapsto T$ and $Y \mapsto \sqrt{T^3}$.

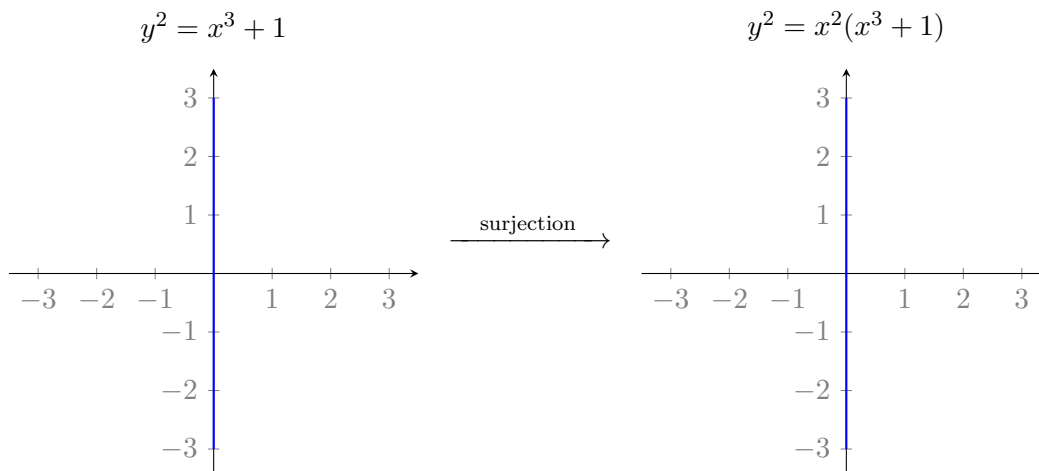
The ring $\mathbb{C}[T, T\sqrt{T^3+1}]$ is not normal, because $\sqrt{T^3+1} \notin \mathbb{C}[T, T\sqrt{T^3+1}]$. Note that $\mathbb{C}[T, T\sqrt{T^3+1}] \cong \mathbb{C}[X, Y]/(Y^2 - X^2(X^3+1))$, where $X \mapsto T$ and $Y \mapsto T\sqrt{T^3+1}$.



The property of not being normal can be thought of as a singularity in the corresponding graph, i.e. the set of maximal ideals has a singularity.

The integral closure of $A = \mathbb{C}[T, T\sqrt{T^3-1}]$ in its field of fractions $\mathbb{C}(T, \sqrt{T^3+1})$ is $\mathbb{C}[T, \sqrt{T^3+1}] \cong \mathbb{C}[X, Y]/(Y^2 - (X^3+1))$. The intersection of a maximal ideal of $\mathbb{C}[T, \sqrt{T^3+1}]$ with A is a maximal ideal of A . This map of maximal ideals corresponds to the map of points

$$\{(x, y) \mid y^2 = x^3 + 1\} \xrightarrow{(x,y) \mapsto (x,xy)} \{(x, y) \mid y^2 = x^2(x^3 + 1)\}.$$



Taking the integral closure is like dissolving the singularity. The same thing is occurring when we take $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ instead of $\mathbb{Z}[\sqrt{5}]$.

Proposition. $\mathbb{C}[T, \sqrt{T^3 + 1}]$ is the integral closure of $\mathbb{C}[T]$ in $\mathbb{C}(T)(\sqrt{T^3 + 1})$

Proof. An element $f \in \mathbb{C}(T)(\sqrt{T^3 + 1})$ is of the form $f = g + h\sqrt{T^3 + 1}$, where $g, h \in \mathbb{C}(T)$. If f is integral over $\mathbb{C}[T]$, then the conjugate $\bar{f} = g - h\sqrt{T^3 + 1}$ is also integral over $\mathbb{C}[T]$, so $f + \bar{f} = 2g \in \mathbb{C}(T)$ and $f\bar{f} = g^2 - (T^3 + 1)h^2 \in \mathbb{C}(T)$ are integral over $\mathbb{C}[T]$. Now using a lemma,

Lemma. *PID's are normal.*

we see that we must have $2g \in \mathbb{C}[T]$ and $g^2 - (T^3 + 1)h^2 \in \mathbb{C}[T]$. Therefore $g \in \mathbb{C}[T]$, hence $(T^3 + 1)h^2 \in \mathbb{C}[T]$, and because $T^3 + 1$ has no repeated factors, this implies that $h \in \mathbb{C}[T]$. Hence $f \in \mathbb{C}[T, \sqrt{T^3 + 1}]$. \square

Lecture 3 (2013-01-11)

The number $x = \frac{1+\sqrt{5}}{2}$ is integral over \mathbb{Z} because it is a root of the polynomial $x^2 - x - 1 = 0$. However, the number $x = \frac{\sqrt{5}}{2}$ is not integral over \mathbb{Z} because it is a root of $4x^2 - 5 = 0$ and not of any monic integer polynomial.

Proposition 1. *If B is a ring and $A \subset B$ is a subring, and $x \in B$, then x is integral over A if and only if $A[x] \subset B$ is a finitely-generated A -module.*

Recall that we say an abelian group M is an A -module when for any $a \in A$ and $x \in M$, we define their product $ax \in M$, and this satisfies

$$\begin{aligned}a(x + y) &= ax + ay \\(a + b)x &= ax + bx \\(ab)x &= a(bx) \\1x &= x\end{aligned}$$

An A -module M is finitely generated when there exist $x_1, \dots, x_n \in M$ such that

$$M = \{a_1x_1 + \dots + a_nx_n \mid a_1, \dots, a_n \in A\}.$$

Proof. If x is integral over A , then it satisfies some monic polynomial over A , say

$$x^n + a_1x^{n-1} + \dots + a_n = 0.$$

Then $A[x]$ is generated by $1, x, \dots, x^{n-1}$ as an A -module, because

$$\begin{aligned}x^n &= -(a_n + a_{n-1}x + \dots + a_1x^{n-1}) \\x^{n+1} &= -x(a_n + a_{n-1}x + \dots + a_1x^{n-1}) = -(a_nx + \dots + a_2x^{n-1}) - a_1x^n \\x^{n+2} &= \dots\end{aligned}$$

Conversely, if $A[x]$ is generated by $f_1, \dots, f_m \in A[x]$, then there is some $r \in \mathbb{N}$ such that

$$f_1, \dots, f_m \in A + Ax + \dots + Ax^r$$

(for example, $r = \max \deg(f_i)$). We have $A[x] \subset A + Ax + \dots + Ax^r$, so $x^{r+1} = a_0 + a_1x + \dots + a_rx^r$ for some $a_i \in A$, and therefore x is integral. \square

As an illustration of this proposition, note that $\frac{2}{3} \in \mathbb{Q}$ is not integral over \mathbb{Z} because

$$\mathbb{Z}[\frac{2}{3}] = \bigcup_{n \geq 1} (\mathbb{Z} + \mathbb{Z}\frac{2}{3} + \dots + \mathbb{Z}\frac{2^n}{3^n})$$

cannot be finitely generated as a \mathbb{Z} -module.

Noetherian rings and modules

Definition. A commutative ring A is noetherian when any ideal of A is finitely generated.

Theorem (Hilbert, 1888). *Let A be a commutative ring and B is a finitely generated ring over A . If A is noetherian, then B is noetherian.*

When we say that B is a ring over A , what we really mean is that we have fixed a ring homomorphism $\phi : A \rightarrow B$. Then we say that B is finitely generated (as a ring) over A when there exist $b_1, \dots, b_n \in B$ such that $B = \phi(A)[b_1, \dots, b_n]$.

Hilbert's theorem demonstrates that most of the rings that come up in algebraic geometry or number theory, which are finitely generated rings over either a field k or over \mathbb{Z} , are noetherian.

Definition. Let A be a commutative ring and M is an A -module. Then we say that M is a noetherian A -module when all A -submodules of M are finitely generated as A -modules.

Remark. A commutative ring A can be regarded as an A -module. An ideal of a commutative ring A is precisely an A -submodule of A . Thus, A is a noetherian ring if and only if it is a noetherian module over itself.

Proposition 2. *Let A be a commutative ring, let M be an A -module, and let N a submodule of M .*

$$N \text{ and } M/N \text{ are f.g. } A\text{-modules} \implies M \text{ is an f.g. } A\text{-module} \implies M/N \text{ is an f.g. } A\text{-module}$$

and

$$N \text{ and } M/N \text{ are noetherian } A\text{-modules} \iff M \text{ is a noetherian } A\text{-module.}$$

Proposition 3. *If A is a commutative ring and M is a finitely generated A -module, then M is a noetherian A -module.*

Proof of Prop. 3. Because M is finitely generated, we have $M = Ax_1 + \dots + Ax_n$ for some $x_i \in M$. Then we have a surjection $A^n \rightarrow M$, defined by mapping (a_1, \dots, a_n) to $a_1x_1 + \dots + a_nx_n$. Letting $N = \ker(h)$, we then have $A^n/N \cong M$. An easy induction argument shows that A^n is a noetherian A -module for any n (note that $A^n/(A^{n-1} \oplus 0) \cong A$). Thus, using Proposition 2, $M \cong A^n/N$ is noetherian. \square

Now let's prove Proposition 1 from last time, i.e. that given a ring B and a subring A , the integral closure of A in B is a subring of B .

Proof. First, let's do the case that A is noetherian. Assume that $x, y \in B$ are integral over A . Then $A[x, y]$ is finitely generated as an A -module, because $x^n + a_1x^{n-1} + \dots + a_n = 0$ and $y^m + c_1y^{m-1} + \dots + c_m = 0$ implies that $A[x, y]$ is generated by $x^i y^j$ for $0 \leq i < n$ and $0 \leq j < m$.

Clearly, $x + y, xy \in A[x, y]$. Equivalently, we know that $A[x + y] \subset A[x, y]$ and $A[xy] \subset A[x, y]$. By Proposition 3, $A[x, y]$ is a noetherian A -module, so both $A[x + y]$ and $A[xy]$ are finitely generated as A -modules, and therefore $x + y$ and xy are integral over A by Proposition 1.

Now let's do the general case. Any ring A whatsoever is a union of subrings of A each of which is finitely generated over \mathbb{Z} . This is clear because any finite subset $\{a_1, \dots, a_n\}$ of A is contained in a subring of A which is finitely generated over \mathbb{Z} , specifically, $\phi(\mathbb{Z})[a_1, \dots, a_n]$ where $\phi : \mathbb{Z} \rightarrow A$ is the unique ring homomorphism (specifically $\phi(n) = n \cdot 1$).

Thus, if $x, y \in B$ are integral over A , say $x^n + a_1x^{n-1} + \dots + a_n = 0$ and $y^m + c_1y^{m-1} + \dots + c_m = 0$ for some $a_i, c_i \in A$, then not only are x and y integral over A , they are integral over the subring $A' = \phi(A)[a_1, \dots, a_n, c_1, \dots, c_m]$ of A . Because A' is finitely generated over \mathbb{Z} , it is noetherian. By the noetherian case, we have that $x + y$ and xy are integral over A' , and therefore they are clearly also integral over A . \square

Lecture 4 (2013-01-14)

Accomplishments in algebraic number theory in the 19th century

In the middle of the 19th century, Kummer started the theory of ideals.

Two motivations of Kummer:

1. He hoped to prove Fermat's Last Theorem.
2. He hoped to make progress in class field theory.

Fermat (1601-1665) is the father of modern number theory. As you should all be familiar, he stated Fermat's Last Theorem, that there are no integer solutions to

$$x^n + y^n = z^n$$

when $n \geq 3$ and $xyz \neq 0$. It was written in the margin's of Diophantus' *Arithmetica*, which was written in the 3rd century.

He also wrote other things in the margins; for example, he claimed that any non-negative integer could be written as a sum of four squares, i.e. that for any $n \geq 0$, there exist some $x, y, z, u \in \mathbb{Z}$ such that

$$n = x^2 + y^2 + z^2 + u^2.$$

However, it took people about 100 years to prove this.

Fermat did give a proof of Fermat's Last Theorem for $n = 4$. 100 years after that, Euler gave a proof for the case $n = 3$. Prior to Kummer, the cases $n = 5$ and $n = 7$ were also known.

Fermat's Last Theorem can be reduced to the cases $n = 4$ and $n =$ a prime, because (for example) we can re-express

$$x^6 + y^6 = z^6 \implies (x^2)^3 + (y^2)^3 = (z^2)^3.$$

Theorem (Kummer). *Assume that n is an odd prime number. If the class number of $\mathbb{Q}(\zeta_n)$ is not divisible by n , then Fermat's Last Theorem is true for n .*

The only prime numbers less than 100 which do not have this property (i.e. the class number is divisible) are $n = 37, 59, 67$.

The class number is the order of the group of classes of fractional ideals.

Kummer could prove Fermat's Last Theorem if the ring $\mathbb{Z}[\zeta_n]$ had unique factorization into irreducibles (note that $\mathbb{Z}[\zeta_n] = \mathcal{O}_K$ where $K = \mathbb{Q}(\zeta_n)$), because we can re-express Fermat's Last Theorem as a multiplicative statement in this ring:

$$x^n = z^n - y^n = \prod_{i=0}^{n-1} (z - \zeta_n^i y).$$

The class number measures how badly unique factorization fails.

Let Us Share the Feelings of Kummer

Kummer was very happy when he proved that

$$n \nmid \text{class number of } \mathbb{Q}(\zeta_n) \implies \text{FLT for } n \text{ is true.}$$

But Kummer was not happy that he could not treat the case that $n \mid \text{class number}$.

As an example of this technique, we can prove that

$$x^3 = y^2 + 4 \text{ for } x, y \in \mathbb{Z} \implies (x, y) = (5, \pm 11) \text{ or } (2, \pm 2)$$

by using unique factorization in $\mathbb{Z}[i]$.

We are very happy to prove that

$$x^3 = y^2 + 20 \implies (x, y) = (6, \pm 14)$$

by using the fact that $3 \nmid$ the class number of $\mathbb{Q}(\sqrt{-5})$ (which is 2); the problem can be re-expressed as

$$x^3 = (y + 2\sqrt{-5})(y - 2\sqrt{-5}).$$

However, we are not happy that we have difficulty for $x^3 = y^2 + 26$, because $3 \mid$ the class number of $\mathbb{Q}(\sqrt{-26})$ (which is 6). Note that

$$3^3 = (1 + \sqrt{-26})(1 - \sqrt{-26}),$$

so that in the world of ideals,

$$(3) = \mathfrak{p}\mathfrak{p}'$$

where \mathfrak{p} and \mathfrak{p}' are prime ideals such that $\mathfrak{p}^3 = (1 + \sqrt{-26})$ and $(\mathfrak{p}')^3 = (1 - \sqrt{-26})$.

Let $\mathfrak{q} = (2, \sqrt{-26})$, which is a prime ideal with $\mathfrak{q}^2 = (2)$. The the class group of $\mathbb{Q}(\sqrt{-26})$ consists of the ideal classes

$$\{1, \text{class}(\mathfrak{p}), \text{class}(\mathfrak{p}^2), \text{class}(\mathfrak{q}), \text{class}(\mathfrak{q}\mathfrak{p}), \text{class}(\mathfrak{q}\mathfrak{p}^2)\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}.$$

In the class group, we have $\text{class}(\mathfrak{p})^3 = 1$.

Going back to the problem $x^3 = y^2 + 4$, we can re-express it as

$$x^3 = (y + 2i)(y - 2i).$$

For any prime element $\pi \in \mathbb{Z}[i]$, if $\pi \mid y + 2i$, we have $\pi \mid x^3$, and therefore $\pi \mid x$.

If $\pi \mid y + 2i$ and $\pi \mid y - 2i$, then $\pi \mid (y + 2i) - (y - 2i) = 4i$, so $\pi \mid 2$, so that $(\pi) = (1 + i)$.

For an $\alpha \in \mathbb{Z}[i] \setminus \{0\}$, define

$$\text{ord}_\pi(\alpha) = \text{the exponent } e \text{ such that } \pi^e \mid \alpha, \pi^{e+1} \nmid \alpha$$

where π is a prime element of $\mathbb{Z}[i]$. Then if $\pi \mid y + 2i$,

$$\text{ord}_\pi(y + 2i) = 3 \text{ord}_\pi(x) \text{ if } (\pi) \neq (1 + i),$$

which implies that $3 \mid \text{ord}_\pi(y + 2i)$. If $(\pi) = (1 + i)$, then

$$\text{ord}_\pi(y + 2i) = \text{ord}_\pi(y - 2i)$$

since $y - 2i = \overline{y + 2i}$, so that

$$2 \text{ord}_\pi(y + 2i) = 3 \text{ord}_\pi(x),$$

and therefore $3 \mid \text{ord}_\pi(y + 2i)$. Thus, we have shown that $3 \mid \text{ord}_\pi(y + 2i)$ for all prime divisors π of $y + 2i$. Thus $y + 2i = \alpha^3$ for some $\alpha \in \mathbb{Z}[i]$. We'll finish this next time.

Lecture 5 (2013-01-16)

We claim that the only solutions $x, y \in \mathbb{Z}$ to the equation $x^3 = y^2 + 4$ are $(x, y) = (2, \pm 2)$ and $(x, y) = (5, \pm 11)$.

As we did last time, we factor the left side in $\mathbb{Z}[i]$ (which is a UFD):

$$x^3 = (y + 2i)(y - 2i).$$

We then obtained last time that this implies $(y + 2i) = \alpha^3$ for some $\alpha \in \mathbb{Z}[i]$. If $\alpha = a + bi$, then

$$\begin{aligned} y + 2i &= (a + bi)^3 \\ &= (a^3 - 3ab^2) + (3ab^2 - b^3)i \end{aligned}$$

and therefore

$$\begin{aligned} y &= a^3 - 3ab^2 \\ 2 &= 3a^2b - b^3 = (3a^2 - b^2)b \end{aligned}$$

The second of these equations forces that $b \in \{1, -1, 2, -2\}$.

$$\begin{aligned} b = 1 &\implies 3a^2 - 1 = 2 && \implies a = \pm 1 \implies y = \mp 2 \\ b = -1 &\implies 3a^2 - 1 = -2 && \text{(not OK)} \\ b = 2 &\implies 3a^2 - 4 = 1 && \text{(not OK)} \\ b = -2 &\implies 3a^2 - 4 = -1 && \implies a = \pm 1 \implies y = \mp 11 \end{aligned}$$

Now let's go back to proving that the integral solutions to $x^3 = y^2 + 20$ are $(x, y) = (6, \pm 14)$.

Factoring the equation in $\mathbb{Z}[\sqrt{-5}]$, we get

$$x^3 = (y + 2\sqrt{-5})(y - 2\sqrt{-5}).$$

As before, this implies that there is an $\alpha \in \mathbb{Z}[\sqrt{-5}]$ such that $y + 2\sqrt{-5} = \alpha$. If $\alpha = a + b\sqrt{-5}$, then we obtain that

$$\begin{aligned} y &= a^3 - 3 \times 5ab^2 \\ 2 &= 3a^2b - 5b^3 = (3a^2 - 5b^2)b \end{aligned}$$

Again, we break into cases for each possibility $b \in \{1, -1, 2, -2\}$, and can conclude the result.

Let $K = \mathbb{Q}(\sqrt{-5})$. Then $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ is not a UFD, because

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

The beautiful world of ideals exists behind the ugly world of numbers.

In the world of ideals, this is fixed, because

$$(2) = \mathfrak{p}^2, \quad (3) = \mathfrak{q}\mathfrak{q}', \quad (1 + \sqrt{-5}) = \mathfrak{p}\mathfrak{q}, \quad (1 - \sqrt{-5}) = \mathfrak{p}\mathfrak{q}'$$

where

$$\mathfrak{p} = (2, 1 + \sqrt{-5}) = (2, 1 - \sqrt{-5}), \quad \mathfrak{q} = (3, 1 + \sqrt{-5}), \quad \mathfrak{q}' = (3, 1 - \sqrt{-5}).$$

For a maximal ideal \mathfrak{p} of $\mathbb{Z}[\sqrt{-5}]$ and $\beta \in \mathbb{Z}[\sqrt{-5}]$, recall that $\text{ord}_{\mathfrak{p}}(\beta) = e$ for that integer e for which $(\beta) = \mathfrak{p}^e I$ for some ideal I , but for which there is no ideal I such that $(\beta) = \mathfrak{p}^{e+1} I$.

Considering the equation $x^3 = (y + 2\sqrt{-5})(y - 2\sqrt{-5})$, we can conclude that $\text{ord}_{\mathfrak{p}}(y + 2\sqrt{-5})$ for every maximal ideal \mathfrak{p} of $\mathbb{Z}[\sqrt{-5}]$. This is because if $y + 2\sqrt{-5} \in \mathfrak{p}$ and $y - 2\sqrt{-5} \notin \mathfrak{p}$, then

$$3 \text{ord}_{\mathfrak{p}}(x) = \text{ord}_{\mathfrak{p}}(x^3) = \text{ord}_{\mathfrak{p}}(y + 2i),$$

and if $y + 2\sqrt{-5} \in \mathfrak{p}$ and $y - 2\sqrt{-5} \in \mathfrak{p}$, then $4\sqrt{-5} \in \mathfrak{p}$, which implies that either $\mathfrak{p} = (2, 1 + \sqrt{-5}) = (2, 1 - \sqrt{-5})$, or $\mathfrak{p} = (\sqrt{-5}) = (-\sqrt{-5})$. Thus, we have obtained that $(y + 2\sqrt{-5}) = I^3$ for some non-zero ideal I of $\mathbb{Z}[\sqrt{-5}]$. Because the class number of $\mathbb{Q}(\sqrt{-5})$ is 2 and $\text{class}(I)^3 = 1$, we can conclude that $\text{class}(I) = 1$, because the order of $\text{class}(I)$ is either 1 or 2.

Therefore there is a principal ideal $I = (\alpha)$ such that $(y + 2\sqrt{-5}) = I^3$, so that $y + 2\sqrt{-5} = \text{unit} \cdot \alpha^3$. The units of $\mathbb{Z}[\sqrt{-5}]$ are just $\{\pm 1\}$, so $y + 2\sqrt{-5} = \pm \alpha^3 = (\pm \alpha)^3$.

This method does not work for solving $x^3 = y^2 + 26$, because $\mathbb{Q}(\sqrt{-26})$ has class number 6, which is divisible by 3. Thus, we get everything up to the conclusion that $(y + \sqrt{-26}) = I^3$ for some ideal I , but we do not then obtain that $y + \sqrt{-26} = \alpha^3$ for some element α . For example, $(x, y) = (3, 1)$ is a solution, so

$$3^3 = (1 + \sqrt{-26})(1 - \sqrt{-26}),$$

but $1 + \sqrt{-26}$ is not a cube, i.e. $1 + \sqrt{-26} \neq \alpha^3$ for any $\alpha \in \mathbb{Z}[\sqrt{-26}]$. However, $(1 + \sqrt{-26}) = \mathfrak{p}^3$ where $\mathfrak{p} = (3, 1 + \sqrt{-26})$.

Three big theorems in algebraic number theory in the 19th century

Let K be a number field.

1. Unique factorization in the world of ideals

If I is a non-zero ideal of \mathcal{O}_K , then $I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ in a unique way, where the \mathfrak{p}_i are maximal ideals of \mathcal{O}_K .

2. Finiteness of class number

The ideal class group of K is finite.

3. Dirichlet's unit theorem

The unit group $(\mathcal{O}_K)^\times$ is isomorphic to

$$\mathbb{Z}^{r_1+r_2-1} \oplus \mathbb{Z}/w_K\mathbb{Z}$$

where w_K is the number of roots of unity in K , r_1 is the number of distinct embeddings $K \hookrightarrow \mathbb{R}$, and r_2 is (one half of) the number of distinct embeddings $K \hookrightarrow \mathbb{C}$ whose image is not \mathbb{R} . Note that

$$r_1 + 2r_2 = \#\{K \hookrightarrow \mathbb{C}\} = [K : \mathbb{Q}].$$

Let's look at some examples of Dirichlet's unit theorem.

If $K = \mathbb{Q}(i)$, then there are no embeddings of K into \mathbb{R} , and two embeddings of K into \mathbb{C} (via $i \mapsto i$ and $i \mapsto -i$), so $r_1 = 0$ and $r_2 = 1$, and

$$\mathbb{Z}[i]^\times = \{\pm 1, \pm i\} \cong \mathbb{Z}/4\mathbb{Z}.$$

If $K = \mathbb{Q}(\sqrt{2})$, then $r_1 = 2$ and $r_2 = 0$, and

$$\mathbb{Z}[\sqrt{2}]^\times = \{\pm(1 + \sqrt{2})^n \mid n \in \mathbb{Z}\} \cong \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

If $K = \mathbb{Q}(\sqrt[3]{2})$, then $r_1 = 1$, $r_2 = 1$, and

$$\mathbb{Z}[\sqrt[3]{2}]^\times = \{\pm(1 - \sqrt[3]{2})^n \mid n \in \mathbb{Z}\} \cong \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

The finiteness of class number tells us that the difference between the world of ideals and the world of numbers is finite in some sense.

Recall that Kummer wanted to approach Fermat's Last Theorem by

$$\begin{aligned} x^n &= y^n - z^n \\ &= \prod_{a=1}^n (z - \zeta_n^a y) \end{aligned}$$

Kummer wanted to be able to say that

$$(z - \zeta_n^a y) = I^n \implies (z - \zeta_n^a y) = (\alpha^n)$$

for some α , which we've seen that we can do when the class number of $\mathbb{Q}(\zeta_n)$ is prime to n . However, the next step requires us to understand the unit group because

$$(z - \zeta_n^a y) = (\alpha^n) \implies z - \zeta_n^a y = u\alpha^n$$

for a unit u .

Lecture 6 (2013-01-18)

There will be no class next Monday.

The first introduction to Dedekind domains

An example of a Dedekind domain is \mathcal{O}_K for any number field K .

Definition. An integral domain A is called a Dedekind domain precisely when

- A is noetherian,
- A is normal (i.e. integrally closed), and
- any non-zero prime ideal of A is a maximal ideal.

Let A be an integral domain, and let K be the field of fractions of A .

Definition. A fractional ideal of A is an A -submodule $I \subset K$ such that $aI \subseteq A$ for some $a \in A \setminus \{0\}$.

For any non-zero ideal $I \subseteq A$, the set

$$I^{-1} := \{a \in K \mid aI \subseteq A\}$$

is a fractional ideal of A .

Theorem (Noether). For an integral domain A , the following conditions are equivalent:

- A is a Dedekind domain.
- $II^{-1} = A$ for any non-zero ideal $I \subseteq A$.
- The non-zero fractional ideals of A form a group for the multiplication

$$IJ = \{\sum_{i=1}^n x_i y_i \mid n \geq 0, x_i \in I, y_i \in J\}.$$

- Any non-zero ideal of A is a finite product of maximal ideals of A .
- Any non-zero ideal of A can be expressed as a finite product of maximal ideals of A .
- All local rings of A are PIDs (this will be explained later).

Lemma. Given a non-zero ideal $I \subseteq A$, then $II^{-1} = A$ implies that I is finitely generated.

Proof. If $II^{-1} = A$, then there are some $a_i \in I$ and $b_i \in I^{-1}$ such that $\sum_{i=1}^n a_i b_i = 1$.

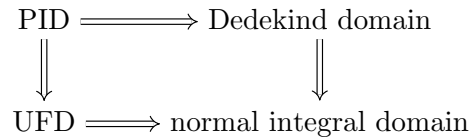
We claim that the a_i generate I . Let $x \in I$. Then

$$x = x \sum_{i=1}^n a_i b_i = \sum_{i=1}^n a_i \underbrace{xb_i}_{\in A}. \quad \square$$

Theorem. Given a Dedekind domain A , let K be its fraction field, let L be any finite extension of K , and let B be the integral closure of A in L . Then B is a Dedekind domain.

Remark. We don't need to assume that L/K is separable.

Corollary. For any number field K , the ring of integers \mathcal{O}_K (which is the integral closure of \mathbb{Z} in K) is a Dedekind domain.



The ring $k[T_1, \dots, T_n]$ for $n \geq 2$ is a UFD, but not a Dedekind domain, because there are non-zero, non-maximal prime ideals. The ring $\mathbb{Z}[\sqrt{-26}]$ is a Dedekind domain, but not a UFD.

Given a Dedekind domain A , we have that A is a UFD $\iff A$ is a PID.

“Dedekind domain” is a good notion. A PID is just a simple-minded Dedekind domain.

Alternatively, you may think “PID” is a good notion, and that a Dedekind domain is a sick PID.

$\mathbb{Z}[\sqrt{5}]$ is not a Dedekind domain, because if $I = (2, 1 + \sqrt{5})$, then

$$I^2 = (2, 1 + \sqrt{5})(2, 1 + \sqrt{5}) = (4, 2(1 + \sqrt{5}), (1 + \sqrt{5})^2) = (2)(2, 1 + \sqrt{5}) = (2)I.$$

This problem is fixed in $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$, because $(2, 1 + \sqrt{5}) = (2)$.

Lecture 7 (2013-01-23)

Ideal class groups

Let A be a Dedekind domain, and let K be its field of fractions. Then the non-zero fractional ideals (which we defined earlier) form a group under multiplication. There's no standard notation for this group, but we'll denote it by I_A .

The non-zero principal fractional ideals, i.e the ones of the form $(a) = aA$ for some $a \in K^\times$, form a subgroup of $I(A)$, which we will denote by $P(A)$.

Definition. The class group $\text{Cl}(A)$ of A is defined to be $I(A)/P(A)$.

If $A = \mathcal{O}_K$ where K is a number field, then the class number of K is defined to be $\#\text{Cl}(A)$. The class number is finite for any number field K .

Note that there is a homomorphism $\theta : K^\times \rightarrow I(A)$ defined by taking a to (a) , and that

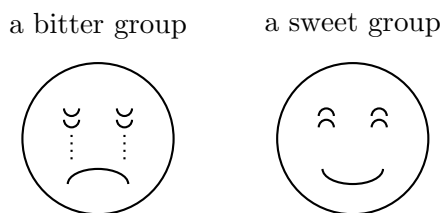
$$\ker(\theta) = A^\times, \quad \text{coker}(\theta) = \text{Cl}(A).$$

These two groups are the most important in number theory. When we understand these, then we are doing well.

Remark. We can identify

$$\text{Cl}(A) \longleftrightarrow \left\{ \begin{array}{l} \text{isomorphism classes of non-zero} \\ \text{ideals of } A \text{ as } A\text{-modules} \end{array} \right\}$$

The class group is a bitter group and a sweet group. It is bitter because when it is non-trivial it makes a mess. It is sweet because it makes things interesting.



There is a cake shop in Balmont, which is north of Chicago. The class group is the same as this cake shop; it is a very nice cake shop.

Class groups have mysterious relations with values of zeta functions. In the 19th century, the class number formula was discovered, which connects zeta functions with both the class number and the unit group. Thus, zeta functions are related to two of the most important groups in number theory.

Another result of the 19th century:

Theorem (Kummer's criterion). *Let p be a prime number. The class number of $\mathbb{Q}(\zeta_p)$ is divisible by p if and only if, for some even integer $2 \leq r \leq p-3$, the numerator of $\frac{\zeta(r)}{\pi^r} \in \mathbb{Q}$ is divisible by p .*

Recall that $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$. Then Euler proved in 1735 that

$$\zeta(2) = \frac{\pi^2}{6}, \quad \zeta(4) = \frac{\pi^4}{90}, \quad \zeta(6) = \frac{\pi^6}{945}$$

and in general, he proved that for any $n \geq 1$,

$$\zeta(2n) = (-1)^{n+1} \frac{B_{2n}(2\pi)^{2n}}{2 \cdot (2n)!} \in \mathbb{Q}\pi^{2n},$$

where the B_{2n} is the $2n$ th Bernoulli number. The Bernoulli numbers are defined by

$$\frac{t}{e^t - 1} = \sum_{m=0}^{\infty} \frac{B_m}{m!} t^m.$$

It turns out that the numerator of $\frac{\zeta(r)}{\pi^r}$ is 1 for $r = 2, 4, 6, 8, 10$. However,

$$\frac{\zeta(12)}{\pi^{12}} = \frac{691}{3^4 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13}.$$

The primes p such that the class number of $\mathbb{Q}(\zeta_p)$ is divisible by p are

$$37, 59, 67, 101, 103, 131, \dots, 691, \dots$$

In the 20th century, people discovered deeper relations between zeta functions and arithmetic groups like the ideal class group (there were also many more zeta functions to think about). For example, Iwasawa theory was developed, and there is the conjecture of Beilinson.

Recall that Kummer's two motivations were

- Hope to prove Fermat's last theorem
- Hope to have progress on "generalized reciprocity law" (we now call this class field theory)

A great stream in number theory

In the 1630's, Fermat proved for an odd prime p , that $p = x^2 + y^2$ for some x and y if and only if $p \equiv 1 \pmod{4}$. For example,

$$5 = 2^2 + 1^2, \quad 13 = 3^2 + 2^2, \quad 17 = 4^2 + 1^2, \quad 89 = 8^2 + 5^2$$

In 1796, Gauss proved the quadratic reciprocity law.

In the 19th century, Kummer and others proved the generalized reciprocity law.

Takagi, my advisor's advisor, and Artin in the 1920's worked on class field theory.

From 1965 forward, Langlands worked on Langland's conjectures (non-commutative version of class field theory).

In 1994, Wiles made big progress on the Langland's conjectures, and proved Fermat's last theorem.

Two motivations of Wiles were

- Hope to prove Fermat's last theorem
- Hope to have progress on Langlands conjectures

Fermat's last theorem has clearly given a lot of energy to mathematicians. In contrast, if Fermat had talked about

$$x^{10} + xy + 6345 = z^{y!} + yz$$

nobody would have cared.

Recall that $p = x^2 + y^2$ implies that $p = (x + yi)(x - yi)$ in $\mathbb{Z}[i]$.

Kummer generalized this by proving that p decomposes "completely" in $\mathbb{Z}[\zeta_n]$ (into $\phi(n)$ distinct primes) if and only if $p \equiv 1 \pmod{n}$.

Lecture 8 (2013-01-25)

Introduction to class field theory and Langlands correspondence

Fermat \rightarrow Gauss $\rightarrow \dots$

Gauss proved the quadratic reciprocity law in 1796.

For p an odd prime number and $a \in \mathbb{Z}$, $p \nmid a$, the Legendre symbol $\left(\frac{a}{p}\right)$ is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \bmod p \text{ has a square root in } \mathbb{F}_p, \\ -1 & \text{otherwise.} \end{cases}$$

We have

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$$

because \mathbb{F}_p^\times is a cyclic group of order $p-1$.

When we fix p and let a vary, it is easy to understand:

$$\left(\frac{a}{5}\right) = \begin{cases} 1 & \text{if } a \equiv 1, 4 \pmod{5}, \\ -1 & \text{if } a \equiv 2, 3 \pmod{5}. \end{cases}$$

This is because $1 = 1^2$, $4 = 2^2$ in \mathbb{F}_5 , but 2 and 3 are not squares.

But if we fix a and let p vary, it seems like this would be very hard to understand:

$$\left(\frac{5}{p}\right) = ?$$

How can we figure out when \mathbb{F}_p has a solution to $x^2 = 5$?

(The case of $x^3 = 5$ is harder; this is a case where we need Langlands correspondence.)

Quadratic Reciprocity Law

Complementary Laws:

$$\text{I: } \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4}, \\ -1 & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

$$\text{II: } \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{if } p \equiv 1, 7 \pmod{8}, \\ -1 & \text{if } p \equiv 3, 5 \pmod{8}. \end{cases}$$

Love song in the land of prime numbers:

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) \cdot (-1)^{\frac{p-1}{2} \frac{q-1}{2}}$$

for distinct odd prime numbers p and q .

$\left(\frac{q}{p}\right)$ is how the girl q is reflected in the heart of the boy p , and $\left(\frac{p}{q}\right)$ is how the boy is reflected in the heart of the girl q . As you may some experience with, these are sometimes not related in our world. But in the world of prime numbers, they are related - this is very mysterious.

We can relate the quadratic reciprocity law as

$$\left(\frac{m}{p}\right) = \chi(p)$$

where $m \in \mathbb{Z}$, m is squarefree. Let

$$N = \begin{cases} |m| & \text{if } m \equiv 1 \pmod{4}, \\ 4|m| & \text{otherwise.} \end{cases}$$

There is a unique homomorphism $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow \{\pm 1\}$ such that

(i) $\chi(-1) = \begin{cases} 1 & \text{if } m > 0, \\ -1 & \text{if } m < 0 \end{cases}$, and

(ii) χ does not factor as

$$\begin{array}{ccc} (\mathbb{Z}/N\mathbb{Z})^\times & \xrightarrow{\quad\quad\quad} & \{\pm 1\} \\ & \searrow & \nearrow \\ & (\mathbb{Z}/N'\mathbb{Z})^\times & \end{array}$$

for any proper divisor N' of N .

When $m = 2$, we have $N = 8$, and $\chi : (\mathbb{Z}/8\mathbb{Z})^\times \rightarrow \{\pm 1\}$ sends 1 and 7 to 1, and 3 and 5 to -1 .

	What happens in finite fields	How primes decompose	Class field theory
Quadratic reciprocity (Gauss, 1796)	$x^2 = m$ has a solution in \mathbb{F}_p $p \nmid m, p \neq 2$	$p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ for distinct $\mathfrak{p}_i \subset \mathcal{O}_K$, where $K = \mathbb{Q}(\sqrt{m})$	$\chi(p) = 1$, where χ is as above
Generalized reciprocity (Kummer, 19 th century)	$x^n = 1$ has n solutions in \mathbb{F}_p $p \nmid n$	$p\mathcal{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ in $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$, where $r = \varphi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}]$	$\chi(p) = 1$ for all $\chi : (\mathbb{Z}/n\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$ ($\iff p \equiv 1 \pmod{n}$)
Class field theory (Tagaki, Artin)	\mathfrak{p} a maximal ideal of $\mathbb{Z}[\zeta_3]$; $x^3 = 2$ has a solution in $\mathbb{Z}[\zeta_3]/\mathfrak{p}$	$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3$ for distinct $\mathfrak{P}_i \subset \mathcal{O}_L$, where $L = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$	exists $\alpha \in \mathbb{Z}[\zeta_3]$ with $\mathfrak{p} = (\alpha)$, $\alpha \equiv 1 \pmod{6}$

For example, in $\mathbb{Z}[\zeta_3]$ we have

$$31 = (1 + 6\zeta_3)(1 + 6\zeta_3^2)$$

and each factor is prime in $\mathbb{Z}[\zeta_3]$, and in \mathcal{O}_L we have

$$1 + 6\zeta_3^a = - \prod_{b=0}^2 (1 - \zeta_3^a + \zeta_3^b \sqrt[3]{2})$$

for each $a = 1, 2$.

Here is another example. Let p be an odd prime and m squarefree, $p \nmid m$. Let $K = \mathbb{Q}(\sqrt{m})$. We have

$$\mathcal{O}_K/p\mathcal{O}_K \cong \mathbb{Z}[\sqrt{m}]/p\mathbb{Z}[\sqrt{m}]$$

because $p \neq 2$. Note that this is isomorphic to

$$\mathbb{Z}[\sqrt{m}]/p\mathbb{Z}[\sqrt{m}] \cong \mathbb{Z}[T]/(T^2 - m, p) \cong \mathbb{F}_p[T]/(T^2 - m).$$

If $\left(\frac{m}{p}\right) = -1$, then $\mathbb{F}_p[T]/(T^2 - m)$ is a field and (p) is maximal.

If $\left(\frac{m}{p}\right) = 1$, then $\mathbb{F}_p[T]/(T^2 - m) \cong \mathbb{F}_p[T]/(T - a)(T - b) \cong \mathbb{F}_p \times \mathbb{F}_p$, and $(p) = (p, a - \sqrt{m})(p, b - \sqrt{m})$.

I saw a book that said class field theory was the greatest theory in number theory, and I misunderstood and thought that number theorists only studied stupid things now, because the greatest theory was already completed. But this was my misunderstanding.

Lecture 9 (2013-01-28)

Today I complete my story about number theory and next class we will return to commutative algebra.

Last time, we discussed the following extensions:

$$\mathbb{Q}(\sqrt{m})/\mathbb{Q}, \quad \mathbb{Q}(\zeta_n)/\mathbb{Q}, \quad \mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}(\zeta_3).$$

Given number fields $L \supseteq K$, how does each maximal ideal \mathfrak{p} of \mathcal{O}_K decompose in \mathcal{O}_L ?

$$\mathcal{O}_L \mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$$

(When at least one of the e_i 's is > 1 , we say that \mathfrak{p} ramifies.)

How the maximal ideal \mathfrak{p} decomposes is related to what happens modulo \mathfrak{p} . This relationship is captured by class field theory. However, class field theory only applies to abelian extensions (all of the ones mentioned above are abelian). Around 1965, Langlands realized the philosophy that modular forms could be used to study non-abelian extensions.

Let p be a prime number. Then

$$x^n = 1 \text{ has } n \text{ solutions in } \mathbb{F}_p \iff p \equiv 1 \pmod{n} \iff (p) \text{ decomposes completely in } \mathbb{Z}[\zeta_n].$$

This is provable using basic ring theory; we know that \mathbb{F}_p^\times is cyclic of order $p - 1$, so

$$\#\{x \in \mathbb{F}_p^\times \mid x^n = 1\} = n \iff n \mid \#(\mathbb{F}_p^\times) \iff p \equiv 1 \pmod{n}.$$

Note that there is an isomorphism $\mathbb{Z}[T]/(\Phi_n(T)) \cong \mathbb{Z}[\zeta_n]$ where $\Phi_n(T)$ is the n th cyclotomic polynomial

$$\Phi_n = \prod_{a \in (\mathbb{Z}/n\mathbb{Z})^\times} (T - \zeta_n^a) \in \mathbb{Z}[T].$$

Thus, we have $\mathbb{Z}[\zeta_n]/(p) \cong \mathbb{Z}[T]/(p, \Phi_n(T))$. Note that $\Phi_n(T) \mid T^n - 1$. Also note that $r = \#(\mathbb{Z}/n\mathbb{Z})^\times = \varphi(n)$, where $r = \deg(\Phi_n(T))$. If we assume that \mathbb{F}_p has n solutions to $x^n = 1$, then

$$\begin{aligned} \mathbb{Z}[\zeta_n]/(p) &\cong \mathbb{Z}[T]/(p, \Phi_n(T)) \\ &\cong \mathbb{F}_p[T]/(\Phi_n(T)) \\ &\cong \mathbb{F}_p[T]/((T - a_1) \cdots (T - a_r)) \\ &\cong \mathbb{F}_p[T]/(T - a_1) \times \cdots \times \mathbb{F}_p[T]/(T - a_r) \\ &= \mathbb{F}_p \times \cdots \times \mathbb{F}_p \end{aligned}$$

Thus, the maximal ideals of $\mathbb{Z}[\zeta_n]$ which contain p are of the form

$$(p, \zeta_n - a_1), \quad \dots, \quad (p, \zeta_n - a_r).$$

Using the fact that $I_1 \cap \cdots \cap I_k = I_1 \cdots I_k$ for coprime ideals I_1, \dots, I_k , we can see that

$$(p) = \prod_{i=1}^r (p, \zeta_n - a_i) = \prod_{c \in (\mathbb{Z}/n\mathbb{Z})^\times} (p, a_i - \zeta_n^c).$$

Let's consider the non-abelian extension $L = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ of \mathbb{Q} (the Galois group is isomorphic to S_3). Let p be a prime, $p \neq 2, 3$. There are three possibilities:

- (1) $x^3 = 2$ has three solutions in \mathbb{F}_p
- (2) $x^3 = 2$ has one solution in \mathbb{F}_p
- (3) $x^3 = 2$ has no solutions in \mathbb{F}_p

By a similar argument,

- (1) $\iff (p)$ decomposes into a product of 6 distinct maximal ideals of \mathcal{O}_L
- (2) $\iff (p)$ decomposes into a product of 3 distinct maximal ideals of \mathcal{O}_L
- (3) $\iff (p)$ decomposes into a product of 2 distinct maximal ideals of \mathcal{O}_L

The Langlands correspondence tells us that

- (1) $\iff a_p = 2$
- (2) $\iff a_p = 0$
- (3) $\iff a_p = -1$

where the numbers a_p are defined as follows, via the Dedekind eta function

$$\eta(z) = q^{1/24} \prod_{n=1}^{\infty} (1 - q^n) \quad q = e^{2\pi iz}$$

(this converges when $\text{Im}(z) > 0$ i.e. $|q| < 1$). We can write $\eta(6z)\eta(18z)$ as a power series

$$\eta(6z)\eta(18z) = q \prod_{n=1}^{\infty} (1 - q^{6n}) \prod_{n=1}^{\infty} (1 - q^{18n}) = \sum_{n=1}^{\infty} a_n q^n,$$

which is a modular form of weight 1 in $\Gamma_1(108)$. Expanding, we see that

$$\eta(6z)\eta(18z) = q - q^7 - q^{13} + q^{19} + q^{25} + 2q^{31} - q^{39} + 2q^{43} + \dots$$

For each prime p , we have $a_p \in \{2, 0, -1\}$, and (for example)

$$\begin{aligned} a_{31} = 2 &\implies (31) \text{ decomposes into 6 maximal ideals} \\ a_5 = 0 &\implies (5) \text{ decomposes into 3 maximal ideals} \\ a_7 = -1 &\implies (7) \text{ decomposes into 2 maximal ideals} \end{aligned}$$

Explicitly,

$$(31) = \prod_{a=1}^2 \prod_{b=0}^2 (1 - \zeta_3^a + \sqrt[3]{2}\zeta_3^b).$$

Compare the following statements:

- in $\mathbb{Q}(\sqrt{m})/\mathbb{Q}$, p decomposes into two $\iff \chi(p) = 1$, i.e. $1 - \chi(p)u = 1 - u$
- in $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}$, p decomposes into six $\iff a_p = 2$, i.e. $1 - a_p u + u^2 = (1 - u)^2$

Let E denote the elliptic curve $y^2 = x^3 + 1$. We define

$$N_p = \#E(\mathbb{F}_p) = \#\{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p \mid y^2 = x^3 + 1\} + \underbrace{1}_{\text{point at infinity}}$$

The set of solutions, together with the point at infinity, form an abelian group.

Let $p \neq 2, 3$. Then

$$N_p = p + 1 - a_p$$

where a_p is defined by expanding the following as a power series:

$$\eta(6z)^4 = q \prod_{n=1}^{\infty} (1 - q^{6n})^4 = \sum_{n=1}^{\infty} a_n q^n.$$

This is a modular form of weight 2. The first few terms are

$$q - 4q^7 + \dots$$

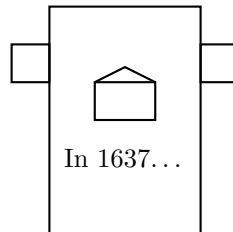
and we correspondingly have $N_5 = 6$ and $N_7 = 12$.

Lecture 10 (2013-01-30)

There is still a bit more to say about number theory before we get back to algebra.

On June 23, 1993, Wiles attended a conference in England where he gave three talks. There were rumors, so people knew that something was going to be special, and on the third day he announced his proof. I was one of the organizers of the conference, but I was in Japan at the time.

There were t-shirts made for the occasion,



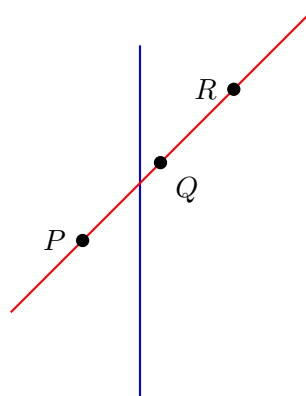
I've received several letters where people who were not professionals claimed to have proven Fermat's Last Theorem. They were all making trivial manipulations until they made a mistake, and thought they had reached a contradiction.

There is a myth of Lorelei, a maiden who lived on a rock in the Rhine river who would distract fishermen with her song so they forgot to control their boat, and they ended up on the bottom of the river. Many people spent their lives in vain trying to prove Fermat's Last Theorem.

Last time, I didn't mention what happens in the number field situation for elliptic curves, only what happens modulo p .

An elliptic curve E/\mathbb{Q} is a curve of the form $y^2 = f(x)$ where $f(x) \in \mathbb{Q}[x]$ is of degree 3, and has no multiple roots.

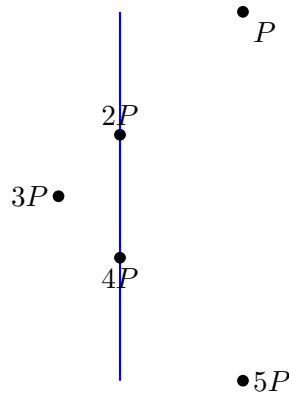
The set $E(K) = \{(x, y) \in K \times K \mid y^2 = f(x)\} \cup \{O\}$ is a group under the operation $+$ defined by setting $P + Q + R = O$ when P , Q , and R are collinear:



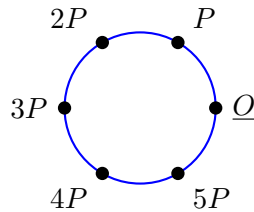
(special cases are needed when the line is tangent to the curve, or is vertical.)

On $E : y^2 = x^3 + 1$, we have that $E[6]$ (the 6-torsion of E) is isomorphic to $\mathbb{Z}/6\mathbb{Z}$, consisting of $\{O, P, 2P, 3P, 4P, 5P\}$ where $P = (2, 3)$:

$$y^2 = x^3 + 1$$



Viewed on the projective plane, you can think of this as simply being



For a natural number n , we define

$$E[n] := \{(x, y) \in E(\overline{\mathbb{Q}}) \mid n \cdot (x, y) = \underline{Q}\} \cong (\mathbb{Z}/n\mathbb{Z})^2.$$

This has a natural action of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on it. There is then a number field $\mathbb{Q}(E[n])$, where we adjoin the x - and y -coordinates of each of the points in $E[n]$ to \mathbb{Q} .

$$\begin{array}{ccc} \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) & \longrightarrow & \text{GL}(2, \mathbb{Z}/n\mathbb{Z}) \\ & \searrow & \swarrow \\ & \text{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}) & \end{array}$$

Let p be an odd prime number.

Frey's elliptic curve takes a hypothetical counterexample to Fermat's Last Theorem, $a^b + b^p = c^p$, and is defined by $y^2 = x(x - a^p)(x - b^p)$. Note that this is of the form

$$(x - A)(x - B)(x - C)$$

where $A - B$, $B - C$, and $A - C$ are all p th powers. This implies that the ramification in $\mathbb{Q}(E[p])/\mathbb{Q}$ is very, very small.

The Taniyama-Shimura conjecture gives a correspondence between elliptic curves and modular forms,

$$E \longleftrightarrow f = \sum_{n=1}^{\infty} a_n q^n$$

where $a_p = 1 + p - \#E(\mathbb{F}_p)$ for almost all p . This is a special case of the Langlands correspondence. Wiles proved a large part of this conjecture.

The property that $A - B$, $B - C$, and $C - A$ are all p th powers implies that $f \bmod p$ has level ≤ 2 , but the correspondence in the Taniyama-Shimura conjecture implies that such an f does not exist. This establishes Fermat's Last Theorem.

The correspondence between E 's and f 's is something like the quadratic reciprocity law. The correspondence between $y^2 = x^3 + \dots$ and a modular form f is like the correspondence between $x^2 = -1$ and $\chi : (\mathbb{Z}/4\mathbb{Z})^\times \rightarrow \{\pm 1\}$ with $\chi(1) = 1$, $\chi(3) = -1$.

Two comments:

1. $\chi : (\mathbb{Z}/n\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$ is a modular form of $\mathrm{GL}(1, \mathbb{Q})$, $f = \eta(6z)\eta(18z)$ is a modular form of $\mathrm{GL}(2, \mathbb{Q})$, etc.
2. The Kronecker-Weber theorem says that any finite abelian extension K of \mathbb{Q} is contained in some cyclotomic field $\mathbb{Q}(\zeta_n)$.

$$\begin{array}{ccc} \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) & \xrightarrow{\cong} & (\mathbb{Z}/n\mathbb{Z})^\times \\ \text{restriction} \downarrow & & \downarrow \chi \\ \mathrm{Gal}(\mathbb{Q}(\sqrt{m})/\mathbb{Q}) & \xrightarrow{\cong} & \{\pm 1\} \end{array}$$

Let p be a prime, and assume $p \nmid n$. Then p decomposes in \mathcal{O}_K completely if and only if $p \bmod N \in H \subset (\mathbb{Z}/n\mathbb{Z})^\times$, where H is the subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$ corresponding to K in the Galois theory correspondence.

Hilbert had a rough idea of class field theory at the end of the 19th century. Takagi was very lucky to be able to study under him, not many people in Japan were able to go to Europe at the time. When he came back, the people of Takagi's village threw a festival, because a great person had returned.

Takagi's thesis under Hilbert established the following result. If $K/\mathbb{Q}(i)$ is a finite abelian extension, then K is contained in a field of the form $\mathbb{Q}(i)(E[n])$ where $E : y^2 = x^3 - x$. Note that $(x, y) \mapsto (-x, iy)$ is an automorphism of E corresponding to multiplication by i . This is a special case of Kronecker's dream-of-youth (Jugendtraum).

Hilbert conjectured that for any number field K , there was a special number field L containing K such that $\mathfrak{p} \subset \mathcal{O}_K$ decomposes completely in \mathcal{O}_L if and only if \mathfrak{p} is principal. For example, if $K = \mathbb{Q}(\sqrt{-5})$, then $L = \mathbb{Q}(\sqrt{-5}, i)$. In this extension, any maximal ideal is unramified, \mathfrak{p} splits if and only if \mathfrak{p} is principal, and \mathfrak{p} remains prime if and only if \mathfrak{p} is not principal.

Lecture 11 (2013-02-01)

Localization, and introduction to algebraic geometry

The spaces $\text{Spec}(A)$ and $\text{max}(A)$

For a commutative ring A , we define

$$\begin{aligned}\text{Spec}(A) &= \{\text{prime ideals of } A\} \\ \text{max}(A) &= \{\text{maximal ideals of } A\}\end{aligned}$$

Recall that an ideal $\mathfrak{p} \subset A$ is prime when $\mathfrak{p} \neq A$, and if $ab \in \mathfrak{p}$ implies that $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. Equivalently, \mathfrak{p} is prime when A/\mathfrak{p} is an integral domain. To have A/\mathfrak{p} a field is equivalent to \mathfrak{p} being maximal.

For example, $\text{Spec}(\mathbb{Z}) = \text{max}(\mathbb{Z}) \cup \{(0)\}$.

To have a good understanding of commutative ring theory, it is nice to think that $\text{Spec}(A)$ and $\text{max}(A)$ are very nice spaces, and we think of A as the ring of functions on these spaces. In number theory, our rings are not really rings of functions; we can't take the derivative of an integer for example. But the analogy is still useful.

Theorem 1. *If k is an algebraically closed field, then $\text{max}(k[T_1, \dots, T_n])$ is in bijection with k^n :*

$$\begin{aligned}\underbrace{(T_1 - a_1, \dots, T_n - a_n)} &\longleftrightarrow (a_1, \dots, a_n). \\ &= \{f \in k[T_1, \dots, T_n] \mid f(a_1, \dots, a_n) = 0\}\end{aligned}$$

Theorem 2. *Let A be a finitely generated ring over a field k (respectively, over \mathbb{Z}), and let \mathfrak{m} be a maximal ideal of A . Then A/\mathfrak{m} is a finite extension of k (respectively, of a finite field).*

We can see that Theorem 2 implies Theorem 1, because any finite extension of an algebraically closed field k must be k itself, so for any maximal ideal \mathfrak{m} of $k[T_1, \dots, T_n]$, we have $k[T_1, \dots, T_n]/\mathfrak{m} \xrightarrow{\cong} k$, and if $T_i \mapsto a_i$, we have $T_i - a_i \in \mathfrak{m}$ for all i , and hence $\mathfrak{m} = (T_1 - a_1, \dots, T_n - a_n)$.

For the proof of Theorem 2, we use the following two propositions.

Proposition 1. *Let K be a finitely generated field over a field k . Then there is an isomorphism of k -algebras between K and a finite extension of $k(T_1, \dots, T_n)$ for some $n \geq 0$, where the T_i 's are indeterminates.*

(We won't prove Proposition 1.)

Proposition 2. *Let B be a commutative ring, and A a subring of B . Assume that B is integral over A . Then B is a field $\implies A$ is a field.*

Proof of Proposition 2. Let $a \in A$ be any non-zero element. Then $\frac{1}{a} \in B$ because B is a field. Because $\frac{1}{a}$ is integral over A , there is some $n \geq 1$ and $c_i \in A$ such that

$$\left(\frac{1}{a}\right)^n + c_1 \left(\frac{1}{a}\right)^{n-1} + \dots + c_n = 0.$$

Thus

$$\frac{1}{a} = -(c_1 + c_2 a + \dots + c_n a^{n-1}) \in A. \quad \square$$

Proof of Theorem 2. Note that it will suffice to prove the theorem in the case that A is a field. In other words, we want to prove that if K is a field that is finitely generated over k (respectively, over \mathbb{Z}), then K is a finite extension of k (respectively, that K is a finite field).

First, let's do the case over k . By Proposition 1, we have that K is a finite extension of $k(T_1, \dots, T_n)$. We want to prove that $n = 0$.

There exist some $b_1, \dots, b_m \in K$ such that K is finitely generated by b_1, \dots, b_m as a ring over k . We have $b_i^{n(i)} + c_{i1}b_i^{n(i)-1} + \dots + c_{in(i)} = 0$ for each i and some $c_{ij} = \frac{f_{ij}}{g_{ij}} \in k(T_1, \dots, T_n)$. Let g be the product of all the g_i . Thus $c_{ij} \in k[T_1, \dots, T_n, \frac{1}{g}]$ for all i, j , and therefore the elements b_i are all integral over $k[T_1, \dots, T_n, \frac{1}{g}]$. Hence all the elements of K are integral over $k[T_1, \dots, T_n, \frac{1}{g}]$. By Proposition 2, this implies $k[T_1, \dots, T_n, \frac{1}{g}]$ is a field; but this is possible only when $n = 0$.

Now we do the case over \mathbb{Z} . The kernel of $\mathbb{Z} \rightarrow K$ is a prime ideal, so it is either (0) or (p) for a prime number p . If it is (p) , then we have that K is a field over \mathbb{F}_p ,

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & K \\ & \searrow & \nearrow \\ & \mathbb{F}_p & \end{array}$$

If it is (0) , we have

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & K \\ & \searrow & \nearrow \\ & \mathbb{Q} & \end{array}$$

so that K is a finite extension of $\mathbb{Q}(T_1, \dots, T_n)$ for some $n \geq 0$. In a similar way, we have that K is integral over $\mathbb{Z}[T_1, \dots, T_n, \frac{1}{g}]$ for some $g \in \mathbb{Z}[T_1, \dots, T_n]$, so $\mathbb{Z}[T_1, \dots, T_n, \frac{1}{g}]$ is a field; but this is impossible unless $n = 0$. \square

Hasse zeta function

Let A be a finitely generated commutative ring over \mathbb{Z} . We define

$$\zeta_A(s) = \prod_{\mathfrak{m} \in \max(A)} \frac{1}{1 - \frac{1}{\#(A/\mathfrak{m})}}$$

which makes sense because A/\mathfrak{m} is a finite field by Theorem 2.

The famous Riemann zeta function is just

$$\zeta_{\mathbb{Z}}(s) = \prod_{p \text{ prime}} \frac{1}{1 - \frac{1}{p^s}} = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Hasse conjectured that $\zeta_A(s)$ has an analytic continuation to all of \mathbb{C} as a meromorphic function.

We have

$$\zeta_{\mathbb{Z}[i]}(s) = \zeta(s)L(s, \chi),$$

where χ is a modular form for $\text{GL}(1, \mathbb{Q})$.

If A is finitely generated over \mathbb{F}_p , then $\zeta_A(s)$ is a rational function in $\frac{1}{p^s}$; for example,

$$\zeta_{\mathbb{F}_p[T]}(s) = \frac{1}{1 - p \cdot \frac{1}{p^s}}.$$

If A is an integral domain and $\mathbb{Z} \subseteq A$, we **expect** that

$$\zeta_A(s) = \frac{\prod L(s, f_i)}{\prod L(s, g_j)}$$

where the f_i, g_j are modular forms for $\mathrm{GL}(n, \mathbb{Q})$.

Lecture 12 (2013-02-04)

I have some comments to add about the Hasse zeta function. Recall that the definition is

$$\zeta_A(s) = \prod_{m \in \max(A)} \frac{1}{1 - \#(A/m)^{-s}}$$

where A is a finitely generated ring over \mathbb{Z} . I mentioned the conjecture of Hasse,

Conjecture 1. There is a meromorphic continuation of ζ_A to all of \mathbb{C} .

But I forgot to mention the generalization of Riemann's hypothesis:

Conjecture 2. The zeros and poles of $\zeta_A(s)$ satisfy $\operatorname{Re}(s) \in \frac{1}{2}\mathbb{Z}$.

Remark. When $A = \mathcal{O}_K$ for a number field K , the function $\zeta_A(s)$ is called the Dedekind zeta function of K . For this case, Conjecture 1 was proved a long time ago; Conjecture 2 is not known.

When A is over a finite field \mathbb{F}_q , Conjecture 1 was proved by Dwork, and then later in a deeper way by Grothendieck (in this case, they were proving that $\zeta_A(s)$ is a rational function in q^{-s}). Conjecture 2 was proved by Deligne in 1973.

Conjecture (Weil conjectures, 1949). Let A be a ring over \mathbb{F}_q , i.e. a ring that is a friend of $\mathbb{F}_q[x]$ like $\mathbb{F}_q[x, y]/(y^2 - x^3 - x - 1)$.

- $\zeta_A(s)$ is a rational function in q^{-s}
- Conjecture 2
- $\zeta_A(s)$ tells us the shape of $A = \mathbb{F}_q[T_1, \dots, T_n]/(f_1, \dots, f_m)$, or rather the shape of the algebraic variety

$$\{x = (x_1, \dots, x_n) \mid f_1(x) = \dots = f_m(x) = 0\}.$$

Over \mathbb{F}_q , this does not have a shape - we can't draw it. But we can think it is over \mathbb{C} , and then we can see the shape.

Great encounters in history

- Young algebraic geometry met Riemann's hypothesis.
- Young Dante met Beatrice.

If A is an integral domain over \mathbb{Z} , i.e. $A \supset \mathbb{Z}$, the Langlands conjectures tell us that

$$\zeta_A(s) = \frac{\prod_{i=1}^m L(s, f_i)}{\prod_{j=1}^n L(s, g_j)}$$

where f_i, g_j are modular forms for $\operatorname{GL}_n(\mathbb{Q})$. Each of these L -functions has a meromorphic continuation to \mathbb{C} , so if we knew the Langlands conjectures, Conjecture 1 would be done.

If $K = \mathbb{Q}(i)$, then $\mathcal{O}_K = \mathbb{Z}[i]$, and

$$\zeta_K(s) = \zeta(s)L(s, \chi)$$

where $\chi : (\mathbb{Z}/4\mathbb{Z})^\times \rightarrow \{\pm 1\}$.

If $K = \mathbb{Q}(\sqrt[3]{2})$, then $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{2}]$, and

$$\zeta_K(s) = \zeta(s)L(s, f)$$

where

$$f(z) = \eta(6z)\eta(18z) = \sum_{n=1}^{\infty} a_n q^n, \quad q = e^{2\pi iz}.$$

Using the nice analytic properties of the function of

$$L(s, f) = \sum_{n=1}^{\infty} \frac{a_n}{n^s},$$

we can show that ζ_K also has a meromorphic continuation.

Now, we will get back to algebra.

Proposition. *Let A be a finitely generated ring over k , an algebraically closed field. Then there are bijections*

$$\max(A) \longleftrightarrow \text{Hom}_k(A, k) \longleftrightarrow \{x = (x_1, \dots, x_n) \in k^n \mid f_1(x) = \dots = f_m(x) = 0\}$$

where A is isomorphic as a k -algebra to $k[T_1, \dots, T_n]/(f_1, \dots, f_m)$.

We know that there is always such a presentation of A because if A is generated by h_1, \dots, h_n over k , then we have a surjective k -algebra map $k[T_1, \dots, T_n] \rightarrow A$ defined by sending T_i to h_i . The kernel I of this map is an ideal of $k[T_1, \dots, T_n]$, and therefore it is finitely generated because this ring is Noetherian. If $I = (f_1, \dots, f_m)$, then we get

$$A \cong k[T_1, \dots, T_n]/(f_1, \dots, f_m).$$

Proof. First, we do the case when $A = k[T_1, \dots, T_n]$. Clearly,

$$\begin{array}{ccc} \text{Hom}_k(k[T_1, \dots, T_n], k) & \longleftrightarrow & k^n \longleftrightarrow \max(k[T_1, \dots, T_n]) \\ \varphi & \longleftarrow & (\varphi(T_i))_i \\ & & a = (a_i)_i \longleftarrow \{f \mid f(a) = 0\} \\ \varphi & \longleftarrow & \{f \mid \phi(f) = 0\} \end{array}$$

Now note that there are bijections

$$\text{Hom}_k(k[T_1, \dots, T_n]/(f_1, \dots, f_m), k) \longleftrightarrow \{x = (x_1, \dots, x_n) \in k^n \mid f_i(x) = 0\}$$

and

$$\text{Hom}_k(k[T_1, \dots, T_n]/(f_1, \dots, f_m), k) \longleftrightarrow \{\varphi \in \text{Hom}_k(k[T_1, \dots, T_n]/(f_1, \dots, f_m), k) \mid \varphi(f_1) = \dots = \varphi(f_m) = 0\}$$

and

$$\max(k[T_1, \dots, T_n]/(f_1, \dots, f_m)) \longleftrightarrow \{\mathfrak{m} \in \max(k[T_1, \dots, T_n]) \mid \mathfrak{m} \ni f_i \text{ for all } i\}$$

□

For any commutative ring A , any $f \in A$ and $\mathfrak{p} \in \text{Spec}(A)$, we define $f(\mathfrak{p})$, the value of f at \mathfrak{p} , to be the image of f in the fraction field $\kappa(\mathfrak{p})$ of A/\mathfrak{p} (this field is called the residue field at \mathfrak{p}). If $\mathfrak{p} \in \max(A)$, then $\kappa(\mathfrak{p}) = A/\mathfrak{p}$.

The idea here is to consider any ring A as a ring of functions on the space $\text{Spec}(A)$. However, the values at different points can take values in different fields. For example, given $f \in \mathbb{Z}$ and $\mathfrak{p} = (p)$ a prime ideal of \mathbb{Z} , then $f(\mathfrak{p}) = f \bmod p \in \mathbb{F}_p$.

Theorem. *Let A be a commutative ring. Then*

$$f(\mathfrak{p}) = 0 \text{ for all } \mathfrak{p} \in \text{Spec}(A) \iff f \text{ is nilpotent,}$$

i.e. $f^n = 0$ for some $n \geq 1$. In the case that A is finitely generated over a field, then in fact

$$f(\mathfrak{m}) = 0 \text{ for all } \mathfrak{m} \in \text{max}(A) \iff f \text{ is nilpotent.}$$

If $A = k[[T]]$ is the ring of formal power series, then $\text{Spec}(A) = \{(T), (0)\}$, and $\text{max}(A) = \{(T)\}$.

For any ring homomorphism $f : A \rightarrow B$, there is a corresponding map $\text{Spec}(B) \rightarrow \text{Spec}(A)$. You should think of f as taking a function on $\text{Spec}(A)$ and pulling it back via this map to a function on $\text{Spec}(B)$.

There is not a corresponding map on sets of maximal ideals; for example, if $f : \mathbb{Z} \hookrightarrow \mathbb{Q}$, then $(0) \in \text{max}(\mathbb{Q})$, but $f^{-1}(0) = (0)$ is not a maximal ideal of \mathbb{Z} .

The world of rings and the world of spaces correspond very nicely.

Lecture 13 (2013-02-06)

There is a correspondence

$$\begin{array}{ccc} \text{algebra} & \longleftrightarrow & \text{geometry} \\ \text{commutative rings} & \longleftrightarrow & \text{spaces} \end{array}$$

Let k be an algebraically closed field, and let

$$X = \{x = (x_1, \dots, x_n) \in k^n \mid f_1(x) = \dots = f_m(x) = 0\}$$

for some $f_i \in k[T_1, \dots, T_n]$. Let A be the collection of polynomial functions on X , i.e. the k -valued functions which can be expressed as a polynomial over k in the coordinate functions. Then A is the image of the map

$$\begin{array}{ccc} k[T_1, \dots, T_n] & \longrightarrow & \text{maps}(X, k) \\ f(T_1, \dots, T_n) & \longmapsto & (x = (x_1, \dots, x_n) \mapsto f(x_1, \dots, x_n)) \end{array}$$

If I is the kernel of this map, we therefore have $A \cong k[T_1, \dots, T_n]/I$.

We claim that $\max(A) = X$. On the homework, you have already shown that $\max(A) = \text{Hom}_k(A, k)$ when A is finitely generated over k . Then the bijection from X to $\text{Hom}_k(A, k)$ is given by

$$\begin{array}{ccc} X & \longrightarrow & \text{Hom}_k(A, k) \\ x & \longmapsto & (f \mapsto f(x)) \end{array}$$

If $B = k[T_1, \dots, T_n]/(f_1, \dots, f_m)$, then we have

$$\begin{array}{ccccc} B & \twoheadrightarrow & A & \hookrightarrow & \text{maps}(X, k) \\ & & \searrow & \nearrow & \\ X = \text{Hom}_k(B, k) & \xleftarrow{\text{injective}} & \text{Hom}_k(A, k) & \xleftarrow{\quad} & X \\ & & \searrow & \nearrow & \\ & & & \text{identity} & \end{array}$$

hence the injective map is also surjective.

This universe should be the set of prime ideals of some nice commutative ring; we can dream this is possible. This ring should be a very beautiful ring. If this ring is the integers, then we are prime numbers, like 17.

The correspondence between rings and spaces is

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ \text{Spec}(B) & \longrightarrow & \text{Spec}(A) \\ \mathfrak{p} & \longmapsto & \varphi^{-1}(\mathfrak{p}) \end{array}$$

Remark. If A and B are finitely generated rings over a field k , and $\varphi : A \rightarrow B$ is a homomorphism of k -algebras, or if A and B are finitely generated over \mathbb{Z} , then we have an induced map $\max(B) \rightarrow \max(A)$, also given by $\mathfrak{p} \mapsto \varphi^{-1}(\mathfrak{p})$.

Proof. For the case over k , if $\mathfrak{m} \in \max(B)$, then $A/\varphi^{-1}(\mathfrak{m}) \subset B/\mathfrak{m}$. Because B/\mathfrak{m} is a finite extension of k , we have that $A/\varphi^{-1}(\mathfrak{m})$ is an integral domain that is finite-dimensional over a field, and therefore it is a field. \square

Zariski topology on $\text{Spec}(A)$, on $\max(A)$

Recall that on the homework, you saw that for a compact Hausdorff space X , and

$$A = \{\text{continuous maps } X \rightarrow \mathbb{C}\},$$

then there was a natural identification $X = \max(A)$, and for any subset $S \subseteq X$, we have $\overline{S} = V(I(S))$ where

$$\begin{aligned} I(S) &= \{f \in A \mid f(x) = 0 \text{ for all } x \in S\} \\ V(J) &= \{x \in X \mid f(x) = 0 \text{ for all } f \in J\} = \{\mathfrak{m} \in \max(A) \mid J \subseteq \mathfrak{m}\} \end{aligned}$$

If A is any commutative ring, then the Zariski topology on $\text{Spec}(A)$ is defined by declaring the closed sets to be those of the form

$$V(J) = \{\mathfrak{p} \in \text{Spec}(A) \mid \mathfrak{p} \supseteq J\}$$

for ideals J of A . This gives a topology, because you can check that

$$\bigcap_i V(J_i) = V(J)$$

where J is the ideal generated by all the J_i , and

$$\bigcup_{i=1}^n V(J_i) = V\left(\bigcap_{i=1}^n J_i\right)$$

Then $\max(A)$ gets the subspace topology, as a subset of $\text{Spec}(A)$.

For example, in $\text{Spec}(\mathbb{Z})$, the closed sets are \emptyset , $\text{Spec}(\mathbb{Z})$ itself, or a finite set of maximal ideals. This is a stupid topological space, and we can't recover the ring just from this topological space; this is not as nice as the case of the compact Hausdorff space.

We hope to hear the voice of the ring A . The first person which appears here is the ring of continuous functions on a compact Hausdorff space. I'm a young guy called "commutative ring", but I was originally "the ring of continuous functions on a compact Hausdorff space". Now I am an algebraic object, so I must say goodbye to my home village, the space, but I will always keep it in my heart as a set of maximal ideals.

Polynomials are determined by their values at finitely many points; thus

$$\overline{S} = \{x \in \text{Spec}(A) \mid \text{if } f, g \in A \text{ and } f(y) = g(y) \text{ for all } y \in S, \text{ then } f(x) = g(x)\}$$

At midnight, some people put a candle on their head and **makes hammering motion with hand**... I'm out of time, so I will explain this next time.

Lecture 14 (2013-02-08)

Let's talk more about the spectrum of a ring and the Zariski topology.

In the Zariski topology on $\text{Spec}(\mathbb{C}[T])$, the closed sets are just \emptyset , $\text{Spec}(\mathbb{C}[T])$, and finite sets of maximal ideals (i.e. points of \mathbb{C}). It may seem counterintuitive, but (0) converges to (T) , to $(T - 1)$, to $(T - 2)$, etc. This is because, if $S = \{(0)\}$, then

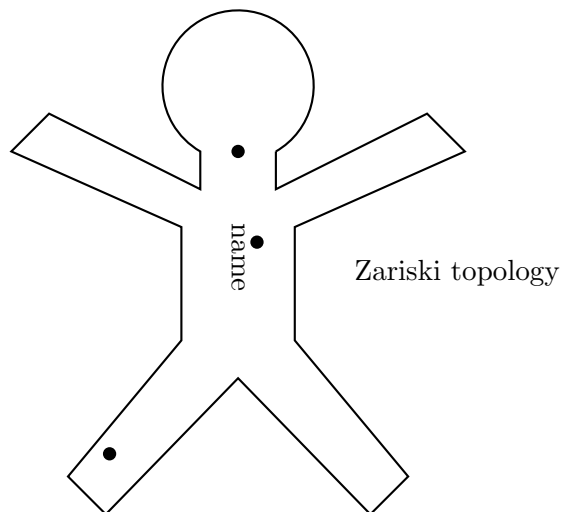
$$I(S) = \{f \in \mathbb{C}[T] \mid f \in (0)\} = \{0\},$$

and thus

$$\overline{S} = V(I(S)) = \{\text{prime } \mathfrak{p} \subset \mathbb{C}[T] \mid \mathfrak{p} \supseteq I(S)\} = \text{Spec}(\mathbb{C}[T]).$$

In general, if A is an integral domain, then we have $\text{Spec}(A) = \overline{\{(0)\}}$.

If you go to the Kifune Shrine in Kyoto (it must be at midnight), you can cut out a piece of paper, write the name of your enemy on it, and hammer nails into it to hurt them. You must have a candle on your head, and there are special white clothes to wear. This is like the Zariski topology; if you take a polynomial and hammer it enough times in \mathbb{C} , it will die.



Localization

Let A be a commutative ring and let S be a multiplicative subset of A , i.e. a subset $S \subset A$ such that $1 \in S$ and $a, b \in S$ implies $ab \in S$. We will define a commutative ring $S^{-1}A$, called the localization of A at S .

In the case when A is an integral domain and $S \subset A \setminus \{0\}$, we have that

$$S^{-1}A = \left\{ \frac{a}{s} \mid a \in A, s \in S \right\} \subset \text{fraction field of } A.$$

Note that $\frac{a}{s} = \frac{a'}{s'}$ if and only if $sa' = s'a$.

In general, we define $S^{-1}A := A \times S / \sim$ where $(a, s) \sim (a', s')$ when there is some $t \in S$ such that $tsa' = ts'a$. This $t \in S$ is necessary to make \sim an equivalence relation. I don't have an example in mind of where this fails without the t . You can prove on your own that \sim is an equivalence relation.

The set $S^{-1}A$ has a ring structure, and in fact a ring structure over A , i.e. we have a ring homomorphism $A \rightarrow S^{-1}A$.

We simply define, as you are used to,

$$\frac{a}{s} + \frac{b}{t} = \frac{ta + sb}{st}, \quad \frac{a}{s} \frac{b}{t} = \frac{ab}{st}.$$

The ring homomorphism $A \rightarrow S^{-1}A$ is defined by $a \mapsto \frac{a}{1}$. This homomorphism has the following universal property:

- Any element of S , considered as an element of $S^{-1}A$, is invertible, and
- If B is a commutative ring and $h : A \rightarrow B$ is a ring homomorphism such that $h(s) \in B^\times$ for all $s \in S$, then there is a unique ring homomorphism $h' : S^{-1}A \rightarrow B$ such that the following diagram commutes:

$$\begin{array}{ccc} A & \xrightarrow{h} & B \\ & \searrow & \nearrow h' \\ & S^{-1}A & \end{array}$$

Note that $h'(\frac{a}{s}) = \frac{h(a)}{h(s)}$. As usual with a universal property, if C is any other ring satisfying the universal property, then $S^{-1}A \cong C$.

When the multiplicative subset S is of the form $S = \{1, f, f^2, \dots\}$, then $S^{-1}A$ is written as $A[\frac{1}{f}]$. There is an isomorphism of rings $A[\frac{1}{f}] \cong A[T]/(fT - 1)$ over A .

The homomorphism $A \rightarrow S^{-1}A$ induces a map $\text{Spec}(S^{-1}A) \rightarrow \text{Spec}(A)$ in the opposite direction, as we've seen.

Proposition. *The map $\text{Spec}(S^{-1}A) \rightarrow \text{Spec}(A)$ is injective, and its image is*

$$\{\mathfrak{p} \in \text{Spec}(A) \mid S \cap \mathfrak{p} = \emptyset\}.$$

Proof. For any ideal I of A , we have its extension to an ideal of $S^{-1}A$, namely

$$S^{-1}I = \{\frac{x}{s} \mid x \in I, s \in S\}.$$

It is easy to check that if $\mathfrak{q} \in \text{Spec}(S^{-1}A)$ has image $\mathfrak{p} \in \text{Spec}(A)$ under the map $\text{Spec}(S^{-1}A) \rightarrow \text{Spec}(A)$, i.e. \mathfrak{p} is the preimage of \mathfrak{q} under the map $A \rightarrow S^{-1}A$, then

$$\mathfrak{p} = \{x \in A \mid \frac{x}{1} \in \mathfrak{q}\}.$$

Clearly, $S^{-1}\mathfrak{p} = \mathfrak{q}$, and $\mathfrak{p} \cap S = \emptyset$.

Conversely, if $\mathfrak{p} \in \text{Spec}(A)$ has $\mathfrak{p} \cap S = \emptyset$, then $S^{-1}\mathfrak{p}$ is a prime ideal of $S^{-1}A$ and

$$\mathfrak{p} = \{x \in A \mid \frac{x}{1} \in S^{-1}\mathfrak{p}\}.$$

□

What happens to the prime ideals $\mathfrak{p} \subset A$ with $\mathfrak{p} \cap S \neq \emptyset$? Then we have $S^{-1}\mathfrak{p} = S^{-1}A$.

Corollary. *The map $\text{Spec}(A[\frac{1}{f}]) \rightarrow \text{Spec}(A)$ is injective. The image is*

$$\begin{aligned} & \{\mathfrak{p} \in \text{Spec}(A) \mid f^n \notin \mathfrak{p} \text{ for all } n \geq 0\} \\ & = \{\mathfrak{p} \in \text{Spec}(A) \mid f \notin \mathfrak{p}\} \\ & = \{\mathfrak{p} \in \text{Spec}(A) \mid f(\mathfrak{p}) = 0\}. \end{aligned}$$

We will identify $\text{Spec}(A[\frac{1}{f}])$ with the image

$$D(f) := \{\mathfrak{p} \in \text{Spec}(A) \mid f(\mathfrak{p}) \neq 0\},$$

which is the complement of $V((f))$. Because $V((f))$ is closed, $D(f)$ is open.

The sets $D(f)$, as f ranges over A , form a basis for the Zariski topology on $\text{Spec}(A)$. Thus, $U \subseteq \text{Spec}(A)$ is open if and only if

$$U = \bigcup_{\lambda} D(f_{\lambda}) = \bigcup_{\lambda} V((f_{\lambda}))^c$$

for some set of $\{f_{\lambda}\} \subseteq A$.

Note that

$$D(f_1) \cap \cdots \cap D(f_n) = D(f_1 \cdots f_n).$$

Theorem. For a commutative ring A ,

$$\{f \in A \mid f(\mathfrak{p}) = 0 \text{ for all } \mathfrak{p} \in \text{Spec}(A)\} = \{\text{nilpotent elements of } A\}.$$

Lecture 15 (2013-02-11)

The rest of the course will cover

- the correspondence between ideals and geometry
- local rings, Dedekind domains, and regular local rings
- completion, p -adic numbers
- algebraic curves
- projective curves
- Weil conjectures and recent big theorems in number theory

Last time, we proved that

$$\text{nil}(A) = \{f \in A \mid f(\mathfrak{p}) = 0 \text{ for all } \mathfrak{p} \in \text{Spec}(A)\} = \bigcap_{\mathfrak{p} \in \text{Spec}(A)} \mathfrak{p}.$$

Now, let's prove that if A is finitely generated over a field, then in fact

$$\text{nil}(A) = \{f \in A \mid f(\mathfrak{p}) = 0 \text{ for all } \mathfrak{p} \in \text{max}(A)\} = \bigcap_{\mathfrak{m} \in \text{max}(A)} \mathfrak{m}.$$

The \subseteq inclusion follows from what we proved last time, so let's prove the \supseteq inclusion.

Assume that $f(\mathfrak{p}) = 0$ for all $\mathfrak{p} \in \text{max}(A)$. We will prove that $A[\frac{1}{f}] = 0$, which suffices to show that f is nilpotent.

If $A[\frac{1}{f}] \neq 0$, then there is some $\mathfrak{m} \in \text{max}(A[\frac{1}{f}])$. Because A is finitely generated over a field, the inverse image of \mathfrak{m} in A is also a maximal ideal, say $\mathfrak{p} \in \text{max}(A)$. Then $\frac{f}{1} \notin \mathfrak{m}$ because $f \in A[\frac{1}{f}]^\times$, but then $f \notin \mathfrak{p}$, which contradicts our assumption.

Ideal \longleftrightarrow Geometry

Let A be a commutative ring. For an ideal I of A , we use \sqrt{I} or $\text{rad}(I)$ to denote

$$\{f \in A \mid \text{there is some } n \geq 1 \text{ such that } f^n \in I\},$$

which is called the radical of I . Note that \sqrt{I} is the inverse image of $\text{nil}(A/I)$ under the quotient map $A \rightarrow A/I$. If $I = \sqrt{I}$, then we say that I is a radical ideal.

Note that $\sqrt{\sqrt{I}} = \sqrt{I}$; this is easy to see from the definition.

Theorem. *Let A be a commutative ring.*

1. *The radical ideals I of A are in bijection with the closed subsets $V(I)$ of $\text{Spec}(A)$.*
2. *If A is finitely generated over a field, then $I = \sqrt{I}$ if and only if $V(I)$ is a closed subset of $\text{Spec}(A)$.*

Proposition. Let A be a commutative ring.

1. For any subset $S \subseteq \text{Spec}(A)$, we have $\overline{S} = V(I(S))$, where recall that

$$I(S) = \{f \in A \mid f(\mathfrak{p}) = 0 \text{ for all } \mathfrak{p} \in S\},$$

$$V(I) = \{\mathfrak{p} \in \text{Spec}(A) \mid f(\mathfrak{p}) = 0 \text{ for all } f \in I\}.$$

2. For any ideal J of A , we have $\sqrt{J} = I(V(J))$.

1' & 2'. If A is finitely generated over a field, then $\text{Spec}(A)$ can be replaced by $\max(A)$.

Proof of part 2 of proposition. By replacing A by A/J , it is enough to prove that

$$\text{nil}(A) = I(V(0))$$

because $\text{nil}(A) = \sqrt{0}$ and there is a bijection

$$\text{Spec}(A/J) \longleftrightarrow \{\mathfrak{p} \in \text{Spec}(A) \mid \mathfrak{p} \supseteq J\}.$$

But we know this is true, because $V(0) = \text{Spec}(A)$, so

$$I(V(0)) = \{f \in A \mid f(\mathfrak{p}) = 0 \text{ for all } \mathfrak{p} \in \text{Spec}(A)\} = \text{nil}(A). \quad \square$$

Note that the theorem follows from the proposition; the bijection is given by

$$\begin{array}{c} V() \\ \curvearrowright \\ I() \end{array}$$

Definition. Let k be an algebraically closed field. A subset of k^n of the form

$$V(f_1, \dots, f_m) = \{x = (x_1, \dots, x_n) \in k^n \mid f_1(x) = \dots = f_m(x) = 0\}$$

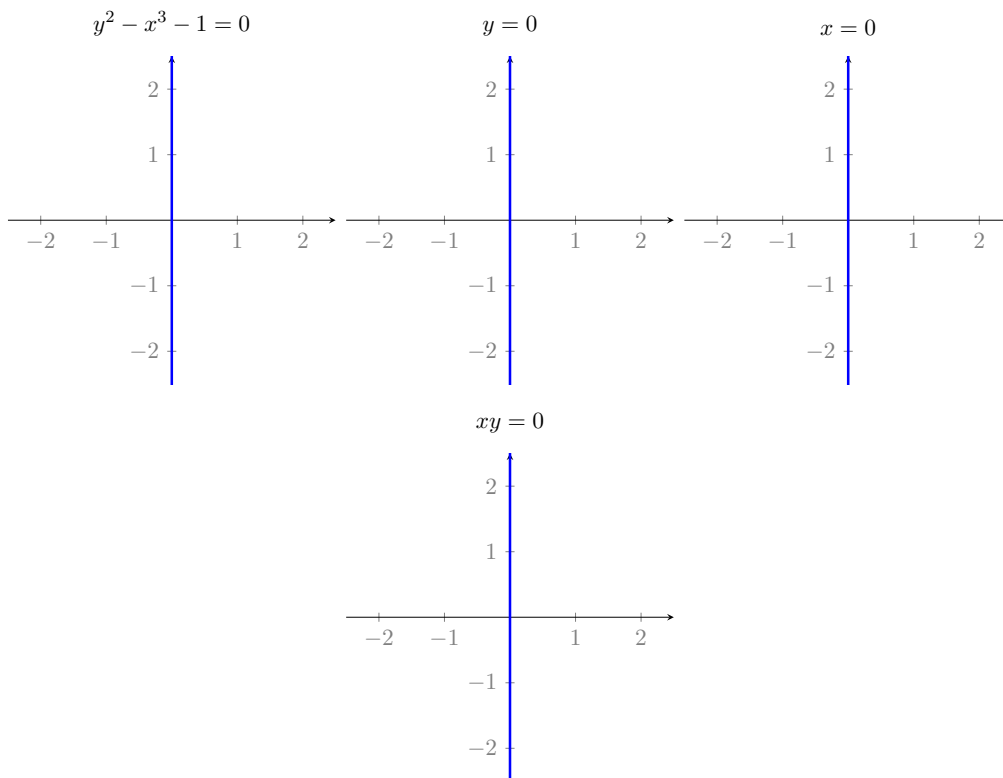
where $f_1, \dots, f_m \in k[T_1, \dots, T_n]$ is called an algebraic subset of k^n . We know there is an identification $k^n = \max(k[T_1, \dots, T_n])$. Then algebraic subsets of k^n are just the closed subsets in the Zariski topology; the above set is just $V(J)$ for $J = (f_1, \dots, f_m)$.

Let S be an algebraic subset of k^n , and let A be the ring of polynomial functions on S , i.e. the functions on S that can be written as polynomials in the coordinate functions. Then we can identify $S = \max(A)$, and there is a bijection

$$\begin{array}{ccc} & V() & \\ & \curvearrowright & \\ \{\text{radical ideals } J \text{ of } A\} & & \{\text{algebraic subsets of } k^n \text{ contained in } S\} \\ & \curvearrowleft & \\ & I() & \end{array}$$

Prime Ideals

In the ring $k[T_1, T_2]$, the ideals (T_1) , (T_2) , and $(T_1^2 - T_2^3 - 1)$ are prime ideals, but $(T_1 T_2)$ is not a prime ideal.



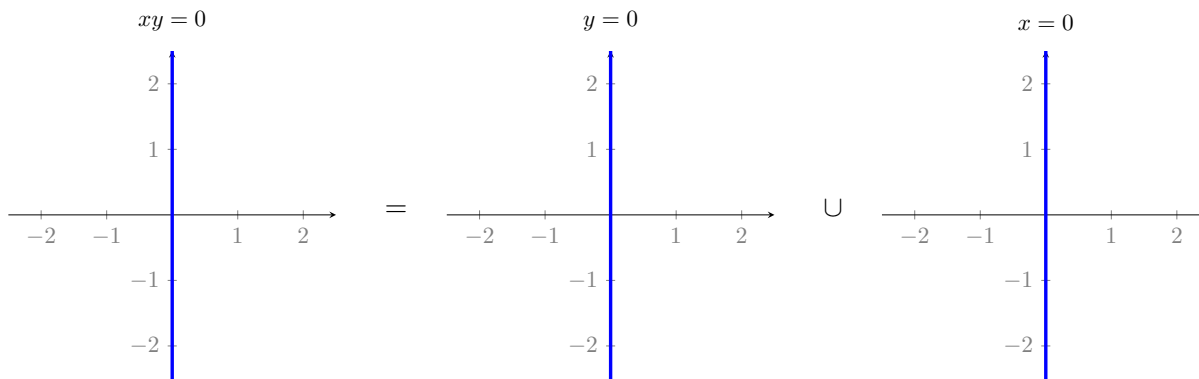
Prime ideals in $k[T_1, \dots, T_n]$ correspond to irreducible algebraic sets, also known as algebraic varieties. These cannot be written as a non-trivial union of smaller algebraic sets. In the same way that a prime number is a number that cannot be divided into two other numbers, an algebraic variety is an algebraic subset that cannot be divided into two other algebraic subsets.

The prime ideal is a princess of the world of ideals. Her father is the prince “Point” in the world of geometry. Her mother is the princess “Prime Numbers” in the world of numbers. She inherits the purity from her parents.

Lecture 16 (2013-02-13)

Definition. A non-empty topological space X is said to be irreducible if, whenever we have $X = Y \cup Z$ where Y and Z are closed subsets of X , then either $X = Y$ or $X = Z$.

For example, the set $V(xy)$ is not irreducible:



Theorem. *Either*

- (i) *let A be a commutative ring, and $X = \text{Spec}(A)$, or*
- (ii) *let A be finitely generated commutative ring over a field k , and $X = \text{max}(A)$.*

Then

1. *In the bijection*

$$\text{radical ideals of } A \longleftrightarrow \text{closed subsets of } X,$$

prime ideals correspond to irreducible subsets.

2. *In case (i), if a prime ideal \mathfrak{p} corresponds to Y , then $Y = \overline{\{\mathfrak{p}\}}$ in $\text{Spec}(A)$.*
3. *In case (i), assume that A is noetherian; this is already true in case (ii). Then X is a finite union of irreducible closed subsets.*

Proof of 1. Let \mathfrak{p} be a prime ideal of A . We will prove that $V(\mathfrak{p})$ is irreducible.

Suppose for the sake of contradiction that $V(\mathfrak{p}) = V(J_1) \cup V(J_2)$. For $i = 1, 2$, because

$$V(J_i + \mathfrak{p}) = V(J_i) \cap V(\mathfrak{p}) = V(J_i),$$

WLOG we can assume that $J_i \supseteq \mathfrak{p}$. We want to prove that either $J_1 = \mathfrak{p}$ or $J_2 = \mathfrak{p}$. If $J_1 \neq \mathfrak{p}$, then we can find some $x \in J_1 \setminus \mathfrak{p}$. Choose any $y \in J_2$. Then $xy \in J_1 \cap J_2$, so

$$V(xy) \supseteq V(J_1 \cap J_2) = V(J_1) \cup V(J_2) = V(\mathfrak{p}).$$

In case (i), this shows that $\mathfrak{p} \in V(\mathfrak{p}) \subseteq V(xy)$, so that $xy \in \mathfrak{p}$. In case (ii), this shows that for any $\mathfrak{m} \in \text{max}(A)$ with $\mathfrak{m} \supseteq \mathfrak{p}$, we have $xy \in \mathfrak{m}$; but

$$\bigcap_{\mathfrak{n} \in \text{max}(A/\mathfrak{p})} \mathfrak{n} = 0$$

because A/\mathfrak{p} has no nilpotents, so

$$\bigcap_{\substack{\mathfrak{m} \in \max(A) \\ \mathfrak{m} \supseteq \mathfrak{p}}} \mathfrak{m} = \mathfrak{p},$$

and thus in case (ii) we also have $xy \in \mathfrak{p}$. Thus, in either case, we have $xy \in \mathfrak{p}$, and because $x \notin \mathfrak{p}$ we must have that $y \in \mathfrak{p}$. Thus $J_2 \subseteq \mathfrak{p}$, and because $J_2 \supseteq \mathfrak{p}$, this shows that $J_2 = \mathfrak{p}$.

Now let's prove the converse. Let $Y \subseteq X$ be a closed subset that is irreducible; we want to prove that $I(Y)$ is a prime ideal of A . By replacing X by Y , it is enough to prove that if X is irreducible, then $I(X) = \text{nil}(A)$ is a prime ideal. By replacing A by $A/\text{nil}(A)$, we may assume that $I(X) = \text{nil}(A) = 0$, so that our goal is now to show that A is an integral domain. We can do this because the map $\text{Spec}(A/\text{nil}(A)) \rightarrow \text{Spec}(A)$ induced by the quotient map $A \rightarrow A/\text{nil}(A)$ is a homeomorphism.

Let $f, g \in A$ satisfy $xy \in I(Y) = 0$. Thus $V(f) \cup V(g) = X$. Because X is irreducible, either $V(f) = X$ or $V(g) = X$, so that either $f = 0$ or $g = 0$. \square

Proof of 2. Easy. \square

We need some preparation for the proof of 3.

Proposition. *If A is a commutative ring, the following two conditions are equivalent:*

- (i) A is noetherian.
- (ii) For any non-empty set Φ of ideals of A , there is a maximal element of Φ (under the ordering given by inclusion).

Proof. First, let's show that (i) \implies (ii); thus, let A be noetherian and let Φ be a non-empty set of ideals of A . Let $I_0 \in \Phi$. If I_0 is not maximal in Φ , then there is some $I_1 \in \Phi$ such that $I_0 \subsetneq I_1$. If I_1 is not maximal in Φ , then there is some $I_2 \in \Phi$ such that $I_1 \subsetneq I_2$. **Continuing**, if Φ doesn't have a maximal ideal, then we have an infinite ascending chain of ideals

$$I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq \dots$$

which contradicts the assumption that A is noetherian because $J = \bigcup_{n=0}^{\infty} I_n$ cannot be finitely generated.

Now, let's show that (ii) \implies (i). For any ideal J , let Φ consist of all the finitely generated ideals contained in J . If J is not finitely generated, then there is no maximal element in this collection, which would contradict our assumption. \square

This proof is a little dangerous. It may take 30 years. We may have to tell our children that, when we were young, we were in a course called "Algebra 2" where we tried to find a maximal ideal in Φ , but that we still are not done. This is not such a good thing for the family. We need to use some sort of axiom of choice.

It never happens that, when we go home and open the refrigerator, we see all infinitely many prime numbers there. We will never observe all of an infinite set, but we know it is there.

Proof of 3. We know that there is a bijection

$$\text{radical ideals of } A \longleftrightarrow \text{closed subsets of } \text{Spec}(A).$$

For any non-empty set Φ of closed subsets of X , we know that Φ has a minimal element.

Now let

$$\Phi = \{\text{closed subsets } Z \subseteq X \mid Z \text{ is not a finite union of irreducible closed subsets of } X\}.$$

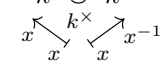
We want to prove that $\Phi = \emptyset$. Suppose for the sake of contradiction that $\Phi \neq \emptyset$. Then Φ has a minimal element Z , and certainly we cannot have that Z is irreducible, so $Z = Y_1 \cup Y_2$ where Y_1, Y_2 are closed and $Y_1, Y_2 \neq Z$. By minimality of Z , we must have that

$$Y_1 = Y_{11} \cup \cdots \cup Y_{1m}, \quad Y_2 = Y_{21} \cup \cdots \cup Y_{2n}$$

for some irreducible closed sets Y_{ij} . But then $Z = \bigcup_{i,j} Y_{ij}$, which contradicts the fact that $Z \in \Phi$. Thus, our assumption was incorrect, and we must have $\Phi = \emptyset$. \square

Let k be an algebraically closed field. An irreducible algebraic set of $k^n = \text{max}(k[T_1, \dots, T_n])$ is called an affine algebraic variety.

There are things which we want to call algebraic varieties which are not affine. For example, if we glue two copies of k together, we can make

$$\mathbb{P}^1(k) = k \cup k$$


Lecture 17 (2013-02-15)

Lecture 18 (2013-02-18)

Last time, we started talking about completion and the p -adic fields.

Definition. Assume we are given sets X_n and maps f_n , as follows:

$$\cdots \xrightarrow{f_3} X_3 \xrightarrow{f_2} X_2 \xrightarrow{f_1} X_1$$

Then the projective (a.k.a. inverse) limit of this system, denoted $\varprojlim X_n$, is defined to be

$$\varprojlim X_n := \{(x_n)_{n \in \mathbb{N}} \mid x_n \in X_n \text{ and } f_n(x_{n+1}) = x_n\}.$$

Definition. Let A be a commutative ring, and let I be an ideal of A . The I -adic completion of A , denoted A_I , is defined to be

$$A_I := \varprojlim A/I^n,$$

where the map $f_n : A/I^{n+1} \rightarrow A/I^n$ is just the quotient map.

Example. If $A = R[T]$ and $I = (T)$, then we have

$$A/I^n = R[T]/(T^n) = \{a_0 + a_1T + \cdots + a_{n-1}T^{n-1} \mid a_i \in R\},$$

and thus

$$\varprojlim A/I^n = R[[T]] = \left\{ \sum_{n=0}^{\infty} a_n T^n \mid a_n \in R \right\},$$

the formal power series ring in the variable T . More generally, if $A = R[T_1, \dots, T_n]$ and $I = (T_1, \dots, T_n)$, then

$$\varprojlim A/I^n = R[[T_1, \dots, T_n]] = \left\{ \sum_{m_1, \dots, m_n \geq 0} a_{m_1, \dots, m_n} T_1^{m_1} \cdots T_n^{m_n} \mid a_{m_1, \dots, m_n} \in R \right\}.$$

If A is a local ring and \mathfrak{m} is its maximal ideal, then $\varprojlim A/\mathfrak{m}^n$ is called the completion of A . This is often denoted \widehat{A} .

Let A be a commutative ring, and $\mathfrak{p} \in \text{Spec}(A)$. The idea of localization is to make things simple; completion makes things even more simple.

$$A \xrightarrow{\text{simple}} A_{\mathfrak{p}} \xrightarrow{\text{simpler}} \widehat{A}_{\mathfrak{p}} = \varprojlim A_{\mathfrak{p}}/(\mathfrak{p}A_{\mathfrak{p}})^n$$

If $\mathfrak{p} \in \max(A)$, then $\widehat{A}_{\mathfrak{p}} = \varprojlim A/\mathfrak{p}^n$ because we have a canonical isomorphism $A/\mathfrak{p}^n \cong A_{\mathfrak{p}}/(\mathfrak{p}A_{\mathfrak{p}})^n$. This is because elements of $A \setminus \mathfrak{p}$ are invertible in A/\mathfrak{p}^n .

Example. Let $a \in \mathbb{C}$. Then

$$\begin{array}{ccc} \mathbb{C}[T]_{(T-a)} & \subset & \widehat{\mathbb{C}[T]}_{(T-a)} \\ \left\{ \frac{f}{g} \mid f, g \in \mathbb{C}[T], g(a) \neq 0 \right\} & & \mathbb{C}[[T-a]] \text{ "Taylor expansions at } a\text{"} \end{array}$$

In 1896, Hensel defined \mathbb{Z}_p and \mathbb{Q}_p where p is a prime number.

$$\mathbb{Z}_p := \varprojlim \mathbb{Z}/p^n\mathbb{Z} = \varprojlim \mathbb{Z}_{(p)}/p^n\mathbb{Z}_{(p)}.$$

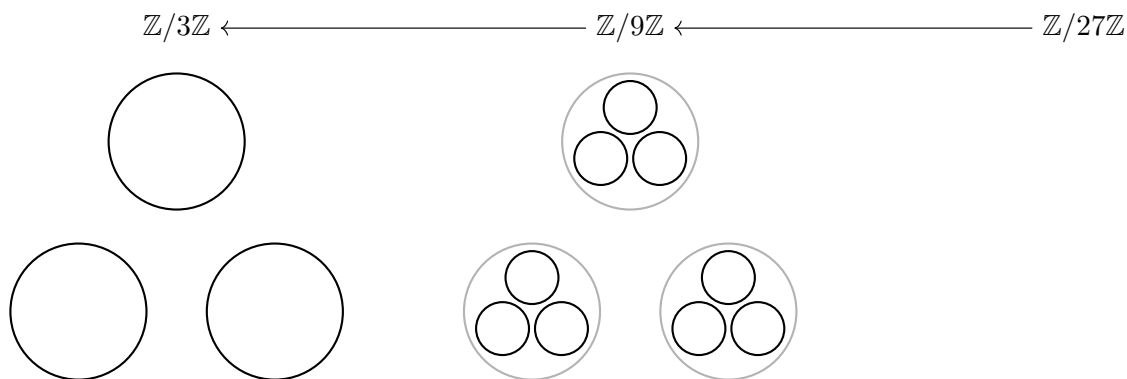
The ring \mathbb{Z}_p is an integral domain, and then we define

$$\mathbb{Q}_p := \text{fraction field of } \mathbb{Z}_p.$$

Thus, we have $\mathbb{Z} \hookrightarrow \mathbb{Z}_{(p)} \hookrightarrow \mathbb{Z}_p$, and $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$. In \mathbb{Q}_p , we have the following relations:

$$\mathbb{Z}_{(p)} = \mathbb{Q} \cap \mathbb{Z}_p, \quad \mathbb{Q}_p = \mathbb{Q} + \mathbb{Z}_p, \quad \mathbb{Z} = \mathbb{Z}[\frac{1}{p}] \cap \mathbb{Z}_{(p)}, \quad \mathbb{Q}_p = \mathbb{Z}[\frac{1}{p}] + \mathbb{Z}_p = \mathbb{Z}_p[\frac{1}{p}].$$

Picture of \mathbb{Z}_3



You can think of an element of \mathbb{Z}_3 as being a choice of one of the three petals at each stage. You can feel that you approach some point, some limit; this is the element of \mathbb{Z}_3 .

This picture also shows us that

$$\mathbb{Q}_p = \coprod_{\substack{a \in \mathbb{Z}[\frac{1}{p}] \\ 0 \leq a < 1}} \mathbb{Z}_p + a = \bigcup_{n \geq 0} p^{-n}\mathbb{Z}_p.$$

image

Moreover, $\mathbb{Q}_p/\mathbb{Z}_p \cong \mathbb{Z}[\frac{1}{p}]/\mathbb{Z}$.

The formal definition of the topology on \mathbb{Q}_p is that x_n converges to a when, for any fixed $n \geq 0$, $x_\lambda - a \in p^n\mathbb{Z}_p$ for all $\lambda \gg 0$.

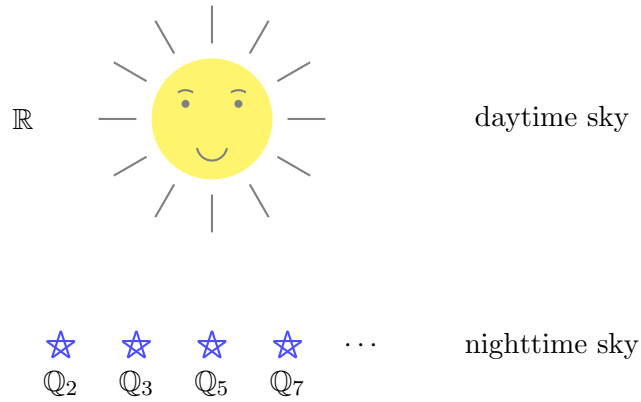
Remark. Arithmetic in \mathbb{R} and in each \mathbb{Q}_p is simpler than in \mathbb{Q} . We can understand \mathbb{Q} by studying the problem in \mathbb{R} and \mathbb{Q}_p first, and then glueing these pieces of local information together. This is known as the Hasse principle.

For example, in \mathbb{Q} , although $\sqrt{1} = 1$ exists in \mathbb{Q} , $\sqrt{1.1}$ and even $\sqrt{1.01}$ do not exist in \mathbb{Q} . In \mathbb{R} , $\sqrt{1.1}$ exists, and it is near to $\sqrt{1}$. In \mathbb{Q}_5 , $\sqrt{1}$ exists, and $\sqrt{1 - \frac{5}{4}} = \frac{\sqrt{-1}}{2}$ exists and is near to 1. We know that $\sqrt{-1}$ exists in \mathbb{Z}_5 because we can find it in each $\mathbb{Z}/5^n\mathbb{Z}$:

$$\begin{array}{ccccc} \mathbb{Z}/125\mathbb{Z} & \longrightarrow & \mathbb{Z}/25\mathbb{Z} & \longrightarrow & \mathbb{Z}/5\mathbb{Z} \\ 57 & \longmapsto & 7 & \longmapsto & 2 \\ 68 & \longmapsto & 18 & \longmapsto & 3 \end{array}$$

If we drop money, we are usually very sad if the money is big. But for example, if we drop 3^{10} dollars, we can relax, because this is very small in the 3-adics. This world is dominated by the real numbers, though, not by the p -adics; we don't live in a p -adic world. That is strange.

\mathbb{R} is like the sun, and the p -adics are like the stars. The sun blocks out the stars during the day, and humans are asleep at night and don't see the stars, even though they are just as important.



Lecture 19 (2013-02-20)

When we complete the ring $\mathbb{C}[T]$ at the prime ideal (T) , we saw last time that we get the ring $\mathbb{C}[[T]]$, the formal power series in the variable T . Its fraction field is denoted $\mathbb{C}((T))$, and elements of $\mathbb{C}((T))$ are called Laurent series in T :

$$\mathbb{C}((T)) = \left\{ \sum_{n=n_0}^{\infty} a_n T^n \mid a_i \in \mathbb{C} \text{ for some } n_0 \in \mathbb{Z} \right\}.$$

We can also form the fields $\mathbb{C}((T-1))$, $\mathbb{C}((T-2))$, \dots but there is one more field, which is $\mathbb{C}((\frac{1}{T}))$. We say that this is the Laurent expansion at ∞ . The field $\mathbb{C}(T)$ is like \mathbb{Q} , the fields $\mathbb{C}((T))$, $\mathbb{C}((T-1))$, etc. are like the p -adic fields \mathbb{Q}_2 , \mathbb{Q}_3 , and \mathbb{R} is like the expansion at ∞ . This analogy is very mysterious.

$$\begin{array}{ccc} \mathbb{C}((\frac{1}{T})) & & \mathbb{R} \\ \cup & & \cup \\ \mathbb{C}(T) \subset \mathbb{C}((T)) & & \mathbb{Q} \subset \mathbb{Q}_2 \\ \vdots \quad \cap \quad \supset & & \vdots \quad \cap \quad \supset \\ & & \mathbb{Q}_3 \\ \mathbb{C}((T-2)) & & \mathbb{Q}_5 \end{array}$$

The Greeks wanted to understand the world using mathematics. But once they realized \mathbb{Q} and \mathbb{R} are different, it was no longer so clear to them how to do that. The student who told others about the existence of irrational numbers was killed by the gods, or perhaps just thrown out of the boat by the other students.

Nowadays, we worry if the weight of our body becomes too small or too large, but we don't worry about whether it is a rational number or an irrational number.

Why does \mathbb{Q} want to grow to \mathbb{R} or \mathbb{Q}_2 or \mathbb{Q}_3 ? Its heart has holes, for example at $\sqrt{2}$ and $\sqrt{3}$. This is similar to mankind; we can grow to be big boys or big girls, but there is still some sadness in our hearts, and we grow to love another person.

Theorem (Hensel's lemma). *Let A be a commutative ring, and let I be an ideal of A . Let $f \in A[T]$, and assume that $a \in A$ has the property that $f(a) \equiv 0 \pmod{I}$, and that $f'(a) \pmod{I}$ is invertible in A/I . Then there exists a unique $b \in \hat{A} := \varprojlim A/I^n$ such that $f(b) = 0$ and $b \equiv a \pmod{I}$. In other words, there exist unique $b_n \in A/I^n$ such that $f(b_n) \equiv 0 \pmod{I^n}$ and $b_n \equiv a \pmod{I}$, and then we have $b = (b_n)_{n \geq 1}$.*

Proof. We proceed by induction on $n \geq 1$. Assume the unique existence of $b_n \in A/I^n$. Fix a choice of $\tilde{b}_n \in A/I^{n+1}$, a lifting of b_n . Then by the general fact that

$$g(T+x) \equiv g(T) + g'(T)x \pmod{x^2}$$

for any polynomial g , we have that

$$f(\tilde{b}_n + x) = f(\tilde{b}_n) + f'(\tilde{b}_n)x + \underbrace{(\text{a multiple of } x^2)}_{\in I^{2n} \subset I^{n+1}}.$$

Because $f'(\tilde{b}_n) \in (A/I^{n+1})^\times$, there is a unique choice of x , namely

$$x = -f'(\tilde{b}_n)^{-1}f(\tilde{b}_n),$$

such that $f(\tilde{b}_n + x) \equiv 0 \pmod{I^{n+1}}$. We then set $b_{n+1} = \tilde{b}_n - f'(\tilde{b}_n)^{-1}f(\tilde{b}_n)$, which is the unique good choice in A/I^{n+1} . Note that we also have that $b_{n+1} \equiv b_n \pmod{I^n}$, because $f(\tilde{b}_n) \in I^n/I^{n+1}$. \square

For example, suppose that we want to find $\sqrt{-1}$ in \mathbb{Z}_5 . We know that we can choose $\sqrt{-1} = 2$ in $\mathbb{Z}/5\mathbb{Z}$ (the other choice is 3). We hope to find the y such that

$$(2 + 5y)^2 \equiv -1 \pmod{25},$$

and this y is the x in the proof. Solving, we get that $y \equiv 1 \pmod{5}$, and we note that $2 + 5 \cdot 1 = 7$ has the property that $7 \equiv 2 \pmod{5}$ and $7^2 \equiv -1 \pmod{25}$.

Here is another application. If p is an odd prime and $m \in \mathbb{Z}$ is an integer with $p \nmid m$, then we can show that if $\left(\frac{m}{p}\right) = 1$, then $x^2 = m$ has a solution \mathbb{Q}_p (which is in fact in \mathbb{Z}_p ; one way to see this is that \mathbb{Z}_p is a PID, hence normal). We can see this by applying Hensel's lemma to $f(T) = T^2 - m$; there is an $a \in \mathbb{Z}$ such that $a^2 - m \equiv 0 \pmod{p}$, and $f'(a) = 2a$ which is invertible in $\mathbb{Z}/p\mathbb{Z}$.

We can use Hensel's lemma and the p -adics to better understand number theory.

It may happen that tomorrow, when you wake up, taking three steps returns you close to your starting point, and taking nine steps returns you even closer.

Lecture 20 (2013-02-22)

Lecture 21 (2013-02-25)

Lecture 22 (2013-02-27)

Let $X \subseteq \mathbb{C}^n$ be an affine algebraic variety of dimension d . Recall that an affine algebraic variety is defined to be an irreducible algebraic set.

If A is the coordinate ring of X (the collection of polynomial functions on X), then A is an integral domain, and the transcendence degree of $\text{Frac}(A)$ over \mathbb{C} is d . There is a bijection between points $x \in X$ and maximal ideals $\mathfrak{m} \in \max(A)$. The dimension of the local ring $A_{\mathfrak{m}}$ is d .

If X is non-singular, then X has the structure of a complex analytic manifold. Each element of the local ring $A_{\mathfrak{m}}$ can be considered as a holomorphic function defined on an open neighborhood of x in X , each of which in turn can be considered as an element of $\mathbb{C}[[T_1, \dots, T_d]]$ (via Taylor expansion). The image consists of the **convergent** series. Letting the maximal ideal $\mathfrak{m}A_{\mathfrak{m}}$ of $A_{\mathfrak{m}}$ be $\mathfrak{m}A_{\mathfrak{m}} = (t_1, \dots, t_d)$, we have an isomorphism

$$\mathbb{C}[[T_1, \dots, T_d]] \cong \varprojlim A_{\mathfrak{m}}/(\mathfrak{m}A_{\mathfrak{m}})^r \cong \varprojlim A/\mathfrak{m}^r,$$

where $T_i \mapsto t_i$.

Theorem. *Let A be a noetherian regular local ring. Then*

1. A is an integral domain.
2. A is normal.
3. For all $\mathfrak{p} \in \text{Spec}(A)$, the localization $A_{\mathfrak{p}}$ is a regular local ring.

Proof. These are all very hard results; we won't go over the proofs. □

Definition. Let A be a noetherian integral domain. We will say that A is regular when $A_{\mathfrak{p}}$ is a regular local ring for all $\mathfrak{p} \in \text{Spec}(A)$. In fact, this is equivalent to only requiring that $A_{\mathfrak{m}}$ be a regular local ring for all $\mathfrak{m} \in \max(A)$, by part 3 of the above theorem.

Remark. If A is a noetherian integral domain, then A is normal if and only if $A_{\mathfrak{p}}$ is normal for all $\mathfrak{p} \in \text{Spec}(A)$, and again, we in fact only need to ask that $A_{\mathfrak{m}}$ is normal for all $\mathfrak{m} \in \max(A)$. Thus, putting the above results together, if A is a noetherian integral domain, then

1. A regular $\implies A$ normal.
2. If $\dim(A) \leq 1$, then A is regular if and only if A is normal.

At the singular point of the cone $z^2 = x^2 + y^2$, the local ring **is** normal. However, it is not a regular local ring; the ring is

$$(\mathbb{C}[x, y, z]/(x^2 + y^2 - z^2))_{(x, y, z)},$$

and because $z^2 = x^2 + y^2 = (x + iy)(x - iy)$, we can see that this is isomorphic to $(\mathbb{C}[x, y, z]/(z^2 - xy))_{(x, y, z)}$.

The ring $A = \mathbb{C}[x, y, z]/(z^2 - xy)$ can be thought of as lying between $\mathbb{C}[x, y]$ and $\mathbb{C}[\sqrt{x}, \sqrt{y}]$. It corresponds to $\mathbb{C}[x, y, \sqrt{xy}]$. The Galois group of the extension $\mathbb{C}[\sqrt{x}, \sqrt{y}]$ of $\mathbb{C}[x, y]$ is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and if $\sigma(\sqrt{x}) = -\sqrt{x}$ and $\sigma(\sqrt{y}) = -\sqrt{y}$, then

$$\mathbb{C}[x, y, \sqrt{xy}] = \{f \in \mathbb{C}[\sqrt{x}, \sqrt{y}] \mid \sigma(f) = f\}.$$

Because A is normal, then for any $g \in \text{Frac}(A)$ integral over A , then $g \in \text{Frac}(\mathbb{C}[\sqrt{x}, \sqrt{y}])$ is integral over $\mathbb{C}[\sqrt{x}, \sqrt{y}]$, because $\mathbb{C}[\sqrt{x}, \sqrt{y}]$ is normal.

When I took Itaka's algebraic geometry class, I gave up trying to understand blowing up rings because he thought we understood everything and went very fast, just said "blow up this, blow up that, you all have seen this before" so that is why I am no good at blowing up rings now.

Remember that a Dedekind domain is a noetherian normal integral domain of dimension ≤ 1 . What we've discussed shows that this is equivalent to being a noetherian regular integral domain of dimension ≤ 1 .

If A is a Dedekind domain, and $\mathfrak{m} \in \max(A)$, then $A_{\mathfrak{m}}$ is a regular local ring, and a PID.

Why can we have a decomposition of an ideal I of A into a product of maximal ideals? For any ideal I , we have $IA_{\mathfrak{m}} = (\mathfrak{m}A_{\mathfrak{m}})^{e(\mathfrak{m})}$ where almost all $e(\mathfrak{m})$ are 0, and then we have

$$I = \prod_{\mathfrak{m} \in \max(A)} \mathfrak{m}^{e(\mathfrak{m})}.$$

If I and J are ideals of a commutative ring A and $IA_{\mathfrak{m}} = JA_{\mathfrak{m}}$ for all $\mathfrak{m} \in \max(A)$, then $I = J$. More generally, if M is an A -module, and N, N' are submodules of M such that $N_{\mathfrak{m}} = N'_{\mathfrak{m}}$ for all $\mathfrak{m} \in \max(A)$, then we have that $N = N'$.

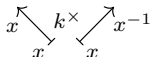
Lecture 23 (2013-03-01)

The homework that was due today will be the last one.

Today we'll talk about algebraic curves.

Let k be a field, and let K be a finite extension of $k(T)$. This is similar to letting K be a finite extension of \mathbb{Q} . In the 19th century, people started to compare these two scenarios. Recall that \mathcal{O}_K denotes the integral closure of \mathbb{Z} in K ; analogously, let A be the integral closure of $k[T]$ in K .

Both A and \mathcal{O}_K are always Dedekind domains. However, the following does not occur in the case of \mathcal{O}_K : we can let A' be the integral closure of $k[\frac{1}{T}]$ in K , and let A'' be the integral closure of $k[T, \frac{1}{T}]$ in K . Then $U'' = \max(A'')$ can be regarded as a subset of both $U = \max(A)$ and $U' = \max(A')$, and we can form $\mathbb{P}^1(k)$ as

$$\mathbb{P}^1(k) = \max(k[T]) \cup_{\max(k[T, \frac{1}{T}])} \max(k[\frac{1}{T}]) = k \cup k$$


It is always the case that $\max(A'')$ is just $\max(A)$ minus a finite set, and also $\max(A')$ minus a finite set.

When $k = \mathbb{C}$, we have that $\mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$ is the Riemann sphere. The ring A' corresponds to $\mathbb{P}^1(\mathbb{C}) \setminus \{0\} \cong \mathbb{C}$. Note how looking at A or A' corresponds to stereographic projection from the north or south pole.

Localization is compatible with taking integral closure; in other words, if A is a domain, K is the fraction field of A , L is a finite extension of K , and B is the integral closure of A in L , then if $S \subset A \setminus \{0\}$ is a multiplicative subset of A , then the integral closure of $S^{-1}A$ in L is $S^{-1}B$. If A is finitely generated over a field k , then B is finitely generated as an A -module, and therefore also finitely generated over k .

In the case of \mathbb{Z} , the best analog we know for \mathbb{P}^1 is taking $X = \max(\mathbb{Z}) \cup \{\infty\}$ where ∞ denotes the embedding of $\mathbb{Q} \hookrightarrow \mathbb{R}$. More generally, for \mathcal{O}_K , we take $\max(\mathcal{O}_K) \cup \{\infty_1, \dots, \infty_r\}$, which we can regard as the set of all embeddings of K into locally compact topological fields with dense image, considered up to a certain equivalence.

Going back to the case of $k = \mathbb{C}$, we have that U and U' are Riemann surfaces (one-dimensional complex analytic manifolds), and $X = U \cup U'$ is a compact Riemann surface. The field of meromorphic functions on $\mathbb{P}^1(\mathbb{C})$ is just $\mathbb{C}(T)$.

For a less trivial example, suppose we have $K = \mathbb{C}(T)(\sqrt{T^3 + 1})$, so that $A = \mathbb{C}[T, \sqrt{T^3 + 1}]$. It may be surprising that $A' = \mathbb{C}[\frac{1}{T}, \sqrt{(\frac{1}{T})^4 + \frac{1}{T}}]$, so that the corresponding sets are

$$\begin{aligned} U &= \{(x, y) \in \mathbb{C}^2 \mid y^2 = x^3 + 1\} \\ U' &= \{(u, v) \in \mathbb{C}^2 \mid v^2 = u^4 + u\} \\ U'' &= U - \{(x, y) \in U \mid x = 0\} \\ &= U - \{(0, \pm 1)\} \\ &= U' - \{(u, v) \in U' \mid u = 0\} \\ &= U' - \{(0, 0)\} \end{aligned}$$

and X is U , together with the point $(0, 0)$ of U' .

Theorem. *There is a bijection between (isomorphism classes of) function fields in one variable over \mathbb{C} and (isomorphism classes of) compact connected Riemann surfaces, where $K \leftrightarrow X$ where K is the field of meromorphic functions on X , and X is constructed from K as above.*

A function field in one variable over \mathbb{C} is a field which is isomorphic over \mathbb{C} to a finite extension of $\mathbb{C}(T)$; however, note that you are free to choose a different T .

The complex topology on the surface X corresponding to $K = \mathbb{C}(T)(\sqrt{T^3 + 1})$ is a torus. In general, if f is a polynomial with no repeated roots, the surface associated with $\mathbb{C}(T)(\sqrt{f})$ is a torus with $\frac{n-1}{2}$ holes if n is odd, and $\frac{n-2}{2}$ holes if n is even.

We say that the number of hole of a donut is g , the genus. Is that how “donut” is spelled? It is too bad, I can eat donuts, but I cannot write it. It turns out that

$$g = \dim_{\mathbb{C}}(A''/(A + A')),$$

and we always know that $A''/(A + A')$ is a finite-dimensional vector space over \mathbb{C} . For example, if $K = \mathbb{C}(T)$, then because $\mathbb{C}[T, \frac{1}{T}] = \mathbb{C}[T] + \mathbb{C}[\frac{1}{T}]$, we have that $g = 0$; if $K(T)(\sqrt{T^3 + 1})$, then $T^{-1}\sqrt{T^3 + 1}$ is a \mathbb{C} -basis for $A''/(A + A')$, so the genus is 1.

Lecture 24 (2013-03-04)

We mentioned last time that there was a correspondence between algebra and geometry,

$$\begin{array}{c} \text{function fields in one} \\ \text{variable over } \mathbb{C} \end{array} \longleftrightarrow \text{compact Riemann surfaces}$$

You can find some good books about this in the Eckhart library, in section QA333. One good book is G. Springer's *Introduction to Riemann Surfaces*.

An algebraic formulation of this correspondence is

$$K \longleftrightarrow X,$$

where

$$X = \{\text{discrete valuation rings } V \mid k \subset V \subset K \text{ and } \text{Frac}(V) = K\}.$$

A discrete valuation ring is a regular local noetherian ring of dimension one. Equivalently, we could define it to be a local ring which is a PID, but not a field. Some examples are $\mathbb{C}[T]_{(T)}$, and $\mathbb{Z}_{(p)}$.

An example of how to think about this correspondence is if

$$X = \text{Spec}(A) \cup_{\text{Spec}(A'')} \text{Spec}(A').$$

Thus, $x \in X$ equals either a maximal ideal $\mathfrak{m} \in \max(A)$, or $\mathfrak{m} \in \max(A')$. Letting $V = A_{\mathfrak{m}}$ or $A'_{\mathfrak{m}}$ as the case may be, this is a DVR, and then the point x corresponds to this V , and X can be understood as the set of such V .

If K is a function field in one variable over \mathbb{C} , we can let

$$V = \{f \in K \mid f \text{ is holomorphic at } x\}.$$

Then V is a PID, with a prime element t (which generates the unique maximal ideal of V) given by a function which vanishes with order 1 at x . Thus, any $f \in K^\times$ can be written uniquely as $f = ut^n$ where $u \in V^\times$, and n is the order of the zero / pole of f at x .

Let's consider the example of $K = \mathbb{C}(T)(\sqrt{f(T)})$ where $f(T) = (T - \alpha_1) \cdots (T - \alpha_n)$, the α_i being distinct. Assume also that n is odd.

Lecture 25 (2013-03-06)

Projective varieties; schemes

Let k be a field. Then n -dimensional projective space over k is defined as

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

where $(a_0, \dots, a_n) \sim (b_0, \dots, b_n)$ when there is some $c \in k^\times$ such that $b_i = ca_i$ for all i . The equivalence class of (a_0, \dots, a_n) is denoted as $(a_0 : \dots : a_n)$.

Suppose that k is algebraically closed. We can define a Zariski topology on $\mathbb{P}^n(k)$ as follows: $Y \subseteq \mathbb{P}^n(k)$ is closed if and only if $Y \cap W_r$ is closed in W_r for all r .

Definition. A closed subset $X \subseteq \mathbb{P}^n(k)$, i.e. a projective algebraic set, is said to be irreducible if

- (i) $X \neq \emptyset$
- (ii) For any closed $Y, Z \subseteq \mathbb{P}^n(k)$ such that $X = Y \cup Z$, we have either $X = Y$ or $X = Z$.

An irreducible projective algebraic set is called a projective algebraic variety.

Example. The subset

$$X = \{(x_0 : x_1 : x_2) \in \mathbb{P}^2(k) \mid x_2^2 x_0 = x_1^3 + x_0^3\}$$

is a projective algebraic variety. Note that U_0 of this X is

$$U_0 = \{(x_1, x_2) \in k^2 \mid x_2^2 = x_1^3 + 1\},$$

and that $X \setminus U_0 = \{(0 : 0 : 1)\}$.

Given a projective algebraic variety $X \subseteq \mathbb{P}^n(k)$, the function field of X is defined as follows: we have $X = \bigcup_{r=0}^n U_r$, and $X \neq \emptyset$ so some $U_r \neq \emptyset$, and because $U_r \neq \emptyset$ we have that U_r is an irreducible algebraic set in k^n . If $U_r \neq \emptyset$ and $U_s \neq \emptyset$, then $U_r \cap U_s \neq \emptyset$. The ring $\mathcal{O}(U_r)$, the “coordinate ring” of $U_r \subseteq k^n$, consists of the polynomial functions on U_r . We can identify $U_r = \max(\mathcal{O}(U_r))$, so that

$$X = \bigcup_{r=0}^n \max(\mathcal{O}(U_r)).$$

The intersection $U_r \cap U_s$ can be identified with $\max(\mathcal{O}(U_r[\frac{1}{x_s}]))$, which is an open subset of $\max(\mathcal{O}(U_r)) = U_r$.

If $U_r \neq \emptyset$, then $\mathcal{O}(U_r)$ is an integral domain, and if $U_r \cap U_s \neq \emptyset$, then

$$\mathcal{O}(U_r[\frac{1}{x_s}]) = \mathcal{O}(U_s[\frac{1}{x_r}]).$$

Therefore their fraction fields are the same as well:

$$\text{Frac}(\mathcal{O}(U_r)) = \text{Frac}(\mathcal{O}(U_r[\frac{1}{x_s}])) = \text{Frac}(\mathcal{O}(U_s[\frac{1}{x_r}])) = \text{Frac}(\mathcal{O}(U_s)).$$

We define the function field K of X to be $\text{Frac}(\mathcal{O}(U_r))$ for any $U_r \neq \emptyset$. We then have that

$$\dim(X) = \dim(\mathcal{O}(U_r)) = \text{tr.deg.}_k(K).$$

Conjecture (Resolution of singularities). Let K be a finitely generated field over k . Then there is a non-singular projective algebraic variety $X \subseteq \mathbb{P}^n(k)$, such that K is the function field of X .

This was proved by Hironaka in the case that $\text{char}(k) = 0$.

The conjecture is true if $\text{tr.deg}_k(K) = 1$. In this case, we have that $X = \max(A) \cup \max(A')$ and that X can be embedded in $\mathbb{P}^3(k)$; sometimes even $\mathbb{P}^2(k)$.

For example,

$$X = \{(x_0 : x_1 : x_2) \in \mathbb{P}^2(\mathbb{C}) \mid x_0^d = x_1^d + x_2^d\}$$

is a non-singular variety of genus $\frac{(d-1)(d-2)}{2}$.

Theorem (Fermat's Last Theorem for $\mathbb{C}(T)$). For $n \geq 3$, there are no non-constant $f, g \in \mathbb{C}(T)$ such that $f^n + g^n = 1$.

Proof. The function field K is $\mathbb{C}(T_1, \sqrt[n]{1 - T_1^n})$. This is the fraction field of $\mathbb{C}[T_1, T_2]/(T_1^n + T_2^n - 1)$. If such an f, g exist, then there is an embedding $K \hookrightarrow \mathbb{C}(T)$, defined by $T_1 \mapsto f$ and $T_2 \mapsto g$, induced from $\mathbb{C}[T_1, T_2]/(T_1^n + T_2^n - 1) \rightarrow \mathbb{C}(T)$. But such an embedding would correspond to a covering $\mathbb{P}^1(\mathbb{C}) \rightarrow X$ of compact Riemann surfaces. This would then induce surjections in homology,

$$H_1(\mathbb{P}^1(\mathbb{C}), \mathbb{Q}) \rightarrow H_1(X, \mathbb{Q}).$$

But $H_1(\mathbb{P}^1(\mathbb{C}), \mathbb{Q}) = 0$ and $H_1(X, \mathbb{Q}) = \mathbb{Q}^{2g}$ where $g = \frac{(n-1)(n-2)}{2} > 0$ when $n \geq 3$, so this is impossible. It's important to use homology over a field, and in particular a field of characteristic 0; if we did it over \mathbb{F}_p and the degree of the covering was a multiple of p , then the map would be the zero map and we would not have a contradiction. Integral homology can also mess up surjectivity, because for example we might have $\mathbb{Z} \rightarrow \mathbb{Z}$, $1 \mapsto n$. \square

Lecture 26 (2013-03-08)

Today we'll discuss recent developments in number theory. Since I'm old, this means what happened in the last 50 years. To me it feels like one day.

Very, very big theorems in number theory appear once in each decade.

In 1973, Deligne proved the Weil conjectures using works of Grothendieck. In 1983, Faltings proved Mordell's conjecture. In 1994, Wiles proved Fermat's Last Theorem. In 2006, Taylor proved a big part of the Sato-Tate conjecture. In 2012, we have the proof of the *abc* conjecture by Mochizuki, though this is still being checked.

If you look at Mochizuki's homepage, you can see that his picture is somewhat strange, it is like **makes face**. But 10 years ago he was normal, and also I still understood his work then. In most pictures of Mochizuki, he looks normal, but for some reason he has chosen a strange picture.

Theorem (Weil, 1941). *Let K be a finite extension of $\mathbb{F}_p(T)$. Let A , A' , and A'' be the integral closures of $\mathbb{F}_p[T]$, $\mathbb{F}_p[\frac{1}{T}]$, and $\mathbb{F}_p[T, \frac{1}{T}]$ in K , respectively. Let $X = \max(A) \cup_{\max(A'')} \max(A')$. Let*

$$\zeta_X(s) = \prod_{x \in X} \left(1 - \frac{1}{\#\kappa(x)^s}\right) = \zeta_A(s) \prod_{x \in X \setminus \text{Spec}(A)} \left(1 - \frac{1}{\#\kappa(x)^s}\right),$$

where $\kappa(x)$ is the residue field at x . Let \mathbb{F}_q be the integral closure of \mathbb{F}_p in K , so that $\mathbb{F}_q = A \cap A'$. Then $\zeta_X(s)$ is of the form

$$\zeta_X(s) = \frac{(1 - \alpha_1 q^{-s}) \cdots (1 - \alpha_{2g} q^{-s})}{(1 - q^{-s})(1 - q^{1-s})},$$

where each α_i satisfies $|\alpha_i| = q^{1/2}$ (this last condition is the analog of the Riemann hypothesis), and g is the genus, which can be obtained as $g = \dim_{\mathbb{F}_q}(A''/(A + A'))$.

Example. Let $K = \mathbb{F}_5(T)(\sqrt{T^3 + 1})$. Then you showed on the homework that

$$\zeta_A(s) = \frac{1 + 5^{1+2s}}{1 - 5^{1-s}} = \zeta_A(s) \cdot \underbrace{\frac{1}{1 - 5^{-s}}}_{\substack{\text{contribution of } \infty, \\ \text{where } X \setminus \text{Spec}(A) = \{\infty\}}} = \frac{(1 + i\sqrt{5} \cdot 5^{-s})(1 - i\sqrt{5} \cdot 5^{-s})}{(1 - 5^{-s})(1 - 5^{1-s})}.$$

Note that from this we can see that the genus is 1.

Example. Let $K = \mathbb{F}_3(T)(\sqrt{T^5 + 1})$. Then

$$\zeta_A(s) = \frac{\prod_{a=1,3,5,7} (1 - \sqrt{3}\zeta_8^a \cdot 3^{-s})}{(1 - 3^{-s})(1 - 3^{1-s})},$$

from which we can see that the genus is 2.

The theorem of Weil was conjectured by Artin in 1934, and proved by Hasse in the case $g = 1$ around 1934.

It is amazing that the zeta function describes the geometric shape that appears over \mathbb{C} .

In 1949, Weil formulated the Weil conjectures. Grothendieck's new algebraic geometry came about around 1960-1965. In 1973 the conjectures were proved by Deligne.

Let X be a non-singular projective algebraic variety over \mathbb{F}_q , and $d = \dim(X)$. Assume that the total constant field (i.e. closure of \mathbb{F}_q in the function field) is just \mathbb{F}_q . Then

$$\zeta_X(s) = \frac{p_1(q^{-s}) \cdots p_{2d-1}(q^{-s})}{p_0(q^{-s})p_2(q^{-s}) \cdots p_{2d}(q^{-s})},$$

where $p_0(u) = 1 - u$ and $p_{2d}(u) = 1 - q^d u$, and

$$p_i(u) = \prod_{j=1}^{b_i} (1 - \alpha_{ij} u)$$

where every $|\alpha_{ij}| = q^{i/2}$. If $X = \mathfrak{X}_{\mathbb{F}_q}$ for some \mathfrak{X} satisfying a certain condition, then $b_i = \dim_{\mathbb{Q}} H^i(\mathfrak{X}_{\mathbb{C}}, \mathbb{Q})$. This number is known as a Betti number. The algebraic geometry of the time did not have the ability to define cohomology for varieties over finite fields.

Complements for non-singular points

Let k be a field, let $f_1, \dots, f_m \in k[T_1, \dots, T_n]$, and let $A = k[T_1, \dots, T_n]/(f_1, \dots, f_m)$, where $m \leq n$. Let $\mathfrak{p} \in \text{Spec}(A)$. Assume that the image of the matrix $\left(\frac{\partial f_i}{\partial T_j}\right)_{ij}$ in $\kappa(\mathfrak{p})$ has rank m . Then $A_{\mathfrak{p}}$ is a regular local ring. If $\mathfrak{p} = (T_1 - a_1, \dots, T_n - a_n)$, and $f_i(a) = 0$ for all $i = 1, \dots, m$, then for any subset $S \subset \{1, \dots, n\}$ with $\#S = m$ such that the image of $\left(\frac{\partial f_i}{\partial T_j}\right)_{i,j \in S}$ has rank m , the image of $T_i - a_i$ for $i \in \{1, \dots, n\} \setminus S$ generates the maximal ideal of $A_{\mathfrak{p}}$.

As an easy application, we can see that the curve $f = y^2 - x^3 - 1$ is non-singular because the matrix $\left(\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}\right)$ always has rank 1 at any point on the curve.

Lecture 27 (2013-03-11)

Lecture 28 (2013-03-13)

On Friday, attendance will be optional. I'll give the definition of etale cohomology.

Let R be a commutative ring, and let $f_1, \dots, f_m \in R[T_0, \dots, T_n]$ be homogeneous polynomials. The projective scheme over R defined by $f_1 = \dots = f_m = 0$ is $\bigcup_{r=0}^n \text{Spec}(A_r)$, where

$$A_r = R[T_1, \dots, T_{r-1}, T_{r+1}, \dots, T_n] / (f_{1,r}, \dots, f_{m,r})$$

and

$$f_{i,r} = f_i(T_1, \dots, T_{r-1}, T_{r+1}, \dots, T_n).$$

For $r \neq s$, we have

$$\text{Spec}(A_r) \cap \text{Spec}(A_s) = \text{Spec}(A_r[\frac{1}{x_s}]),$$

which is an open subset of $\text{Spec}(A_r)$. Here x_s denotes the image of T_s in A_r .

Example 1. We can take $R = \mathbb{C}[t]$, and $f = T_2^2 T_0 - T_1^2 - t T_0^3$. For any $a \in \mathbb{C}$, we have a map $\mathbb{C}[t] \rightarrow \mathbb{C}$ defined by sending $t \mapsto a$, and then we get the projective scheme over \mathbb{C} defined by the image of f , i.e. the projective scheme over \mathbb{C} defined by $T_2^2 T_0 - T_1^2 - a T_0^3$. In general the closed points of this projective scheme over \mathbb{C} are

$$X_a := \{(x, y) \in \mathbb{C}^2 \mid y^2 = x^3 + a\} \cup \{\infty\}.$$

If $a = 0$, then this becomes $y^2 = x^3$, which has a singularity. We can see this problem in the cohomology:

$$H_1(X_a, \mathbb{Q}) \cong H^1(X_a, \mathbb{Q}) \cong \begin{cases} \mathbb{Q}^2 & \text{if } a \neq 0, \\ 0 & \text{if } a = 0. \end{cases}$$

Example 2. An analogous example in the case of $R = \mathbb{Z}$ would be $f = T_2^2 T_0 - T_1^3 - 3T_0^3$.

If $R = k$ is an algebraically closed field, then we can identify

$$\{x = (x_0 : \dots : x_n) \in \mathbb{P}^n(k) \mid f_1(x) = \dots = f_m(x) = 0\} = \bigcup_{r=0}^n \max(A_r) \subset \bigcup_{r=0}^n \text{Spec}(A_r),$$

where

$$\bigcup_{r=0}^n \max(A_r) = \left\{ x \in \bigcup_{r=0}^n \text{Spec}(A_r) \mid \{x\} \text{ is closed} \right\}.$$

We can define a condition (**): for any r and any $\mathfrak{p} \in \text{Spec}(A_r)$ (you can also use $\max(A_r)$ without changing the condition), the image of $\left(\frac{\partial f_{i,r}}{\partial T_j} \right)_{1 \leq i \leq m, 0 \leq j \leq n, j \neq r}$ in $\kappa(\mathfrak{p})$ has rank m .

- If $R = \mathbb{C}[t, \frac{1}{t}]$, and f is the same as in our earlier example, and (**) is satisfied.
- If $R = \mathbb{Z}[\frac{1}{6}]$, and f is the same as in our earlier example, then (**) is satisfied.
- If $R = \mathbb{C}[t]$ and we consider the maps $R \rightarrow \mathbb{C}$ sending $t \mapsto a$ and $t \mapsto b$ respectively, where $a, b \neq 0$, then when (**) is satisfied, we have $H^1(X_a, \mathbb{Q}) \cong H^1(X_b, \mathbb{Q})$. In general, if (**) is satisfied and if R is an integral domain finitely generated over \mathbb{C} , then $H^i(X_a, \mathbb{Q}) \cong H^i(X_b, \mathbb{Q})$ for any ring homomorphisms $a, b : R \rightarrow \mathbb{C}$ and any i .

Grothendieck's étale cohomology

Let k be a separably closed field (this means algebraically closed when $\text{char}(k) = 0$). Let ℓ be a prime number, $\ell \neq \text{char}(k)$. Let X be a scheme of finite type over k , which just means that there is an open covering $X = \bigcup_{s=1}^n \text{Spec}(A_s)$ where each A_s is finitely generated over k . Then we have finite-dimensional vector spaces over \mathbb{Q}_ℓ , denoted $H_{\text{et}}^i(X, \mathbb{Q}_\ell)$, for all $i \geq 0$.

If $k = \mathbb{C}$, then $H_{\text{et}}^i(X, \mathbb{Q}_\ell) \cong H^i(X_{\text{cl}}, \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$, where X_{cl} is the closed points of X with the topology coming from \mathbb{C} .

If R is an integral domain satisfying condition (**) and we have any ring homomorphisms $a : R \rightarrow k_1$, $b : R \rightarrow k_2$ where the k_i are separably closed fields, then

$$H_{\text{et}}^m(\mathfrak{X}_a, \mathbb{Q}_\ell) \cong H_{\text{et}}^m(\mathfrak{X}_b, \mathbb{Q}_\ell),$$

where \mathfrak{X}_a is the scheme over k_1 defined by the images of the f_i in $k_1[T_0, \dots, T_n]$.

If R is a finite field and (**) is satisfied, then we can express the zeta function as

$$\zeta_X(s) = \prod_{\substack{x \in X \\ x \text{ closed point}}} \left(1 - \frac{1}{\#\kappa(x)^s}\right)^{-1} = \prod_{i=0}^{2 \dim(X)} \det \left(1 - \varphi^{-1}u : H_{\text{et}}^i(X_{\overline{\mathbb{F}}_q}, \mathbb{Q}_\ell)\right)^{(-1)^{i-1}}$$

where $u = q^{-s}$. There is an action of

$$\text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \cong \varprojlim_n \text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \varprojlim_n \mathbb{Z}/n\mathbb{Z}.$$

Let $P_i(u) = \det(1 - \varphi^{-1}u : H^i)$ as in above. Then

$$\zeta_X(s) = \frac{P_1(q^{-s}) \cdots P_{2d-1}(q^{-s})}{P_0(q^{-s}) \cdots P_{2d}(q^{-s})},$$

where $d = \dim(X)$.

If K is a number field and X is a scheme of finite type over K , then because we have $K \hookrightarrow \overline{K} = \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$, we have

$$H_{\text{et}}^m(X_{\overline{K}}, \mathbb{Q}_\ell) \cong H_{\text{et}}^m(X_{\mathbb{C}}, \mathbb{Q}_\ell) \cong H^m(X_{\mathbb{C} \text{ cl}}, \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell.$$

and there is a Galois action of $\text{Gal}(\overline{K}/K)$ on the left.

If we have a donut over \mathbb{C} , then we cannot hear the action of the Galois group. We can eat it and enjoy the taste though.

The Langlands correspondence

Lecture 29 (2013-03-15)

A sheaf gives information that connects local and global. Cohomology can tell us the difference between local and global.

The geometric space of a space X is usually considered to be how open sets in X exist. This is not so good for schemes though, because there are too few open sets.

The right idea for schemes is taking the geometric shape of a scheme X to be how étale morphisms to X exist. This gives rise to the idea of étale cohomology.

For example, let $X = \mathbb{S}^1 = \mathbb{R}/\mathbb{Z}$. For each open $U \subseteq X$, define $\mathcal{A}(U) = C^\infty$ functions from U to \mathbb{R} , and $\mathcal{B}(U) = C^\infty$ differential forms on U . These form sheaves \mathcal{A}, \mathcal{B} of abelian groups.

There is a map $d : \mathcal{A} \rightarrow \mathcal{B}$ which is a morphism of sheaves of abelian groups. For any open $U \subseteq X$, we take $d(U) : \mathcal{A}(U) \rightarrow \mathcal{B}(U)$ to be the map $f \mapsto df$.

It turns out that $\mathbb{R} = \ker(d)$. Here, \mathbb{R} denotes the sheaf defined by taking $\mathbb{R}(U) =$ locally constant functions from U to \mathbb{R} for each open $U \subseteq X$. The sequence

$$0 \longrightarrow \mathbb{R} \longrightarrow \mathcal{A} \xrightarrow{d} \mathcal{B} \longrightarrow 0$$

is an exact sequence of sheaves of abelian groups. For sheaves $\mathcal{F}, \mathcal{G}, \mathcal{H}$ of abelian groups on a space, we say that

$$0 \longrightarrow \mathcal{F} \longrightarrow \mathcal{G} \longrightarrow \mathcal{H} \longrightarrow 0$$

is exact when

$$0 \longrightarrow \mathcal{F}(U) \longrightarrow \mathcal{G}(U) \longrightarrow \mathcal{H}(U) \longrightarrow 0$$

is exact for all open $U \subseteq X$. For each U and $a \in \mathcal{H}(U)$, there exists an open cover $U = \bigcup U_\lambda$ and $b_\lambda \in \mathcal{G}(U_\lambda)$ such that $b_\lambda \mapsto a|_{U_\lambda}$.

Returning to our example, we have $X = \mathbb{S}^1$, and the map $\mathcal{A}(X) \rightarrow \mathcal{B}(X)$ is not surjective because (for example) there is no C^∞ function on X whose differential is $d\theta$. Thus, local and global are different; $d\theta$ locally comes from \mathcal{A} , but not globally.

If we have an exact sequence

$$0 \longrightarrow \mathcal{F} \longrightarrow \mathcal{G} \longrightarrow \mathcal{H} \longrightarrow 0$$

of sheaves of abelian groups on a space, we get a long exact sequence of abelian groups

$$0 \longrightarrow H^0(X, \mathcal{F}) \longrightarrow H^0(X, \mathcal{G}) \longrightarrow H^0(X, \mathcal{H}) \longrightarrow H^1(X, \mathcal{F}) \longrightarrow H^1(X, \mathcal{G}) \longrightarrow H^1(X, \mathcal{H}) \longrightarrow \dots$$

where we define $H^0(X, \mathcal{K}) = \mathcal{K}(X)$ for any sheaf \mathcal{K} .

In our exact sequence

$$0 \longrightarrow \mathbb{R} \longrightarrow \mathcal{A} \xrightarrow{d} \mathcal{B} \longrightarrow 0$$

we get the long exact sequence

$$0 \longrightarrow \mathbb{R}(X) \longrightarrow \mathcal{A}(X) \xrightarrow{d} \mathcal{B}(X) \longrightarrow H^1(X, \mathbb{R}) \longrightarrow H^1(X, \mathcal{A}) \longrightarrow \dots$$

where $H^1(X, \mathbb{R}) \cong \mathbb{R}$. This is because, for any abelian group M and topological space X , the sheaf M defined by $M(U) =$ locally constant functions $U \rightarrow M$ satisfies $H^m(X, \text{sheaf } M) =$ the usual $H^m(X, M)$ from algebraic topology.

Let X be a \mathbb{C}^∞ manifold, or complex analytic space. Let \mathcal{O}_X be the sheaf of \mathbb{C} -valued \mathbb{C}^∞ functions, or holomorphic functions respectively. For any $n \geq 1$, we get an exact sequence

$$0 \longrightarrow \mathbb{Z}/n\mathbb{Z} \xrightarrow{1 \mapsto e^{2\pi i/n}} \mathcal{O}_X^\times \xrightarrow{f \mapsto f^n} \mathcal{O}_X^\times \longrightarrow 0$$

If $X = \mathbb{C} \setminus \{0\}$, and $z \in \mathcal{O}_X^\times(X)$ denotes the coordinate function, then z is locally $(z^{1/n})^n$, but it is not an n th power globally. We have that $H^1(\mathbb{C} \setminus \{0\}, \mathbb{Z}/n\mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}$, where $z^m \in \mathcal{O}_X^\times(X)$ corresponds to $m \in \mathbb{Z}/n\mathbb{Z}$. If $H^1(X, \mathbb{Z}/n\mathbb{Z}) = 0$, then all elements of $\mathcal{O}_X^\times(X)$ are n th powers. This is very powerful.

Now we turn the second part of the story. The Zariski topology is good sometimes, but not always. For example, it is bad that $H^1(\text{scheme}, \mathbb{Z}/n\mathbb{Z}) = 0$ usually, when the scheme has the Zariski topology. If the sheaf is nice, like \mathcal{O}_X , then if we have $X = U \cup U'$ with $U = \text{Spec}(A)$ and $U' = \text{Spec}(A')$ open subsets of X , then the Mayer-Vietoris sequence is true,

$$0 \longrightarrow \mathcal{O}_X(X) \longrightarrow \underbrace{\mathcal{O}_X(U)}_A \oplus \underbrace{\mathcal{O}_X(U')}_{A'} \longrightarrow \underbrace{\mathcal{O}_X(U \cap U')}_{A''} \longrightarrow H^1(X, \mathcal{O}_X) \longrightarrow \dots$$

and $k^g = H^1(X, \mathcal{O}_X) = A''/(A + A')$.

Étale morphisms

I will assume that you know the definition of a morphism of schemes. We say that a morphism $f : X \rightarrow Y$ of schemes is smooth of relative dimension d when there are open covers $X = \bigcup \text{Spec}(B_\lambda)$ and $Y = \bigcup \text{Spec}(A_\mu)$ such that for all λ and μ , $f(\text{Spec}(B_\lambda)) \subseteq \text{Spec}(A_\mu)$, which corresponds to a map $A_\mu \rightarrow B_\lambda$, such that over A_μ ,

$$B_\lambda \cong A_\mu[T_1, \dots, T_{m+d}]/(f_1, \dots, f_m)$$

such that the image of the matrix $\left(\frac{\partial f_i}{\partial T_j}\right)_{ij}$ in $\kappa(\mathfrak{p})$ has rank m for any $\mathfrak{p} \in \text{Spec}(B_\lambda)$. Then we say that a morphism is étale when it is smooth of relative dimension 0.

If $f : X \rightarrow Y$ is smooth of relative dimension d , then $\{f^{-1}(y)\}_{y \in Y}$ is a family of non-singular varieties of dimension d , parametrized by Y .

If X and Y are of finite type over \mathbb{C} and $f : X \rightarrow Y$ is étale, then $X_{\text{cl}} \rightarrow Y_{\text{cl}}$ is locally a homeomorphism. Here X_{cl} denotes the closed points of X with the topology coming from the topology of \mathbb{C} . The converse implication is almost true.

Let X be a scheme. We say that something holds “étale locally” when there are étale morphisms $f_\lambda : U_\lambda \rightarrow X$ with $\bigcup f_\lambda(U_\lambda) = X$ such that it holds on each U_λ .

Thus, if $Y = \text{Spec}(\mathbb{C}[T, \frac{1}{T}])$, then T is étale locally an n th power, because there is an étale morphism from $X = \text{Spec}(\mathbb{C}[T^{1/n}, T^{-1/n}])$ to Y . If $B = \mathbb{C}[T^{1/n}, T^{-1/n}]$, then $B = A[S]/(S^n - T)$. This map

corresponds to the map $X_{\text{cl}} = \mathbb{C} \setminus \{0\}$ to $Y_{\text{cl}} = \mathbb{C} \setminus \{0\}$ given by $w \mapsto w^n$. However, T not Zariski locally an n th power (localizing the ring $\mathbb{C}[T, \frac{1}{T}]$ will never add in an n th root of T).

We have

holds Zariski locally \implies holds étale locally \implies holds for classical topology

The second implication is very close to also having \longleftarrow , but the first implication is very far from having \longleftarrow .

Now we can define étale cohomology. We say that \mathcal{F} is a sheaf on $X_{\text{ét}}$ when we define every $\mathcal{F}(Y, f)$ for étale morphisms $f : Y \rightarrow X$, and for any $g : Y' \rightarrow Y$ with

$$\begin{array}{ccc} Y' & \xrightarrow{g} & Y \\ & \searrow f' & \swarrow f \\ & & X \end{array}$$

we have a corresponding $\mathcal{F}(X, f) \rightarrow \mathcal{F}(Y', f')$, and we require the analog of the open covering condition for usual sheaves.

Given a sheaf \mathcal{F} of abelian groups on $X_{\text{ét}}$, we define

$$H_{\text{ét}}^0(X, \mathcal{F}) = \mathcal{F}(X).$$

There are a variety of ways of defining higher étale cohomology groups, but we can just say that

$$H_{\text{ét}}^m(X, \mathcal{F}) = \text{Ext}_{\mathcal{C}}^m(\mathbb{Z}, \mathcal{F})$$

where \mathcal{C} is the category of sheaves of abelian groups on $X_{\text{ét}}$.

If X is a scheme over k , a separably closed field, then we define

$$H_{\text{ét}}^m(X, \mathbb{Q}_\ell) = \left(\varprojlim_n H_{\text{ét}}^m(X, \mathbb{Z}/\ell^n \mathbb{Z}) \right) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$$

for any $\ell \neq \text{char}(k)$, where $\mathbb{Z}/\ell^n \mathbb{Z}$ denotes the constant sheaf. This is a finite-dimensional \mathbb{Q}_ℓ vector space. If $k = \mathbb{C}$, then it is isomorphic to $H^m(X_{\text{cl}}, \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$.

As an example, let $X = \text{Spec}(\mathbb{C}[T, \frac{1}{T-a_1}, \dots, \frac{1}{T-a_m}])$. We have a long exact sequence of étale cohomology

$$0 \longrightarrow \mathbb{Z}/n\mathbb{Z}(X) \longrightarrow \mathcal{O}_X^\times(X) \xrightarrow{n} \mathcal{O}_X^\times(X) \longrightarrow H_{\text{ét}}^1(X, \mathbb{Z}/n\mathbb{Z}) \longrightarrow \dots$$